UNIVERSIDAD ESTATAL DE GUAYAQUIL

Facultad de Ciencias Administrativa

"DISEÑO DE PORTAL CAUTIVO PARA EL USO DEL INTERNET A TRAVÉS DE LA RED WLAN PARA LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL."

PROYECTO DE IMPLEMENTACIÓN

Previo a la obtención del Título de:

INGENIERIO EN SISTEMA ADMINISTRATIVO COMPUTARIZADO

Presentado por:

MICHEL ALEXANDER VIDAL PINARGOTE

JAMES ROGGER PESANTES PIGUAVE

Tutor:

BRYAN NAGIB ZAMBRANO MANZUR

Guayaquil – Ecuador

AÑO: 2016

REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO: "DISEÑO DE PORTAL CAUTIVO PARA EL USO DEL INTERNET A TRAVÉS DE LA RED WLAN PARA LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL."		
AUTORES: Michel Alexander Vidal Pinargote; James Rogger Pesantes Piguave.	**REVISORES:** Ing. Cesar Barrionuevo Delarosa Ing. César Vallejo de la Torre.	
INSTITUCIÓN: Universidad de Guayaquil.	**FACULTAD:** Facultad de Ciencias Administrativas	
CARRERA: Ingeniería en Sistemas Administrativos Computarizados.		
FECHA DE PUBLICACIÓN:	**N° DE PÁGS.:** 124	
ÁREA TEMÁTICA: Tecnología – redes.		
PALABRAS CLAVES: Administración de navegación, Administración de perfiles, WLAN, Portal cautivo.		
RESUMEN: En el ámbito de la infraestructura de red WLAN el tema de seguridad, es algo que en la última década se ha convertido en algo muy relevante para los administradores de red. Y con los avances tecnológicos se puede tener muchas alternativas para poder suplir esta brecha, en la cual para este proyecto hemos escogido la del portal cautivo. En la Facultad de Ciencias Administrativas se ha encontrado esta falencia o brecha de seguridad, para lo cual se propuso realizar mediante este proyecto el análisis y diseño de una solución viable. Lo cual se describe desde el análisis de la problemática hasta los objetivos que se quiere lograr con este estudio, dado que desde la parte de IT se desea.		
N° DE REGISTRO(en base de datos):	**N° DE CLASIFICACIÓN:**	
DIRECCIÓN URL (tesis en la web):		
ADJUNTO PDF:	✓ SI	NO
CONTACTO CON AUTOR:	**Teléfono:** 0991120770	**E-mail:** michaelvidalp@hotmail.com james.pesantes@hotmail.com
CONTACTO DE LA INSTITUCIÓN	**Nombre:**	
	Teléfono:	

CERTIFICACIÓN DEL TUTOR

Habiendo sido nombrado **Bryan Nagib Zambrano Manzur**, como tutor de tesis de grado como requisito para optar por título de **Ingeniería en Sistemas Administrativos Computarizados** presentado por los egresados: **Michel Alexander Vidal Pinargote y James Rogger Pesantes Piguave** con C.I #**09295092263; 0930756887.**

TEMA"**DISEÑO DE PORTAL CAUTIVO PARA EL USO DEL INTERNET A TRAVÉS DE LA RED WLAN PARA LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL."**

El presente trabajo ha sido revisado por el programa de Urkund teniendo un porcentaje del 5%.

Certifico que he revisado y aprobado en todas sus partes, encontrándose apto para su sustentación.

Atentamente,

_____

Bryan Nagib Zambrano Manzur.

TUTOR DE TESIS

RENUNCIA DE DERECHOS DE AUTOR

Por medio de la presente certifico que los contenidos desarrollados en esta tesis son de absoluta propiedad y responsabilidad de: **Michel Alexander Vidal Pinargote y James Rogger Pesantes Piguave, con c.c. # 0930493796** cuyo tema es**:**

DISEÑO DE PORTAL CAUTIVO PARA EL USO DEL INTERNET A TRAVÉS DE LA RED WLAN PARA LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL.

Derechos que renuncio a favor de la Universidad de Guayaquil, para que haga uso como a bien tenga.

MICHAEL ALXANDER VIDAL PINARGOTE
CI: 0930493796

JAMES ROGGER PESANTES PIGUAVE
CI: 0930756887

El Honorable Jurado Calificador

Otorga a este trabajo de Titulación

La Calificación de: _____

Equivalente a: _____

_____ _____

_____

AGRADECIMIENTO

A Dios y a nuestros padres por apoyarnos siempre y esforzarse para ofrecerme la oportunidad de llegar hasta este punto de nuestras vidas.

MICHEL ALEXANDER VIDAL PINARGOTE

JAMES ROGGER PESANTES PIGUAVE

DEDICATORIA

A nuestros padres, hermanos y familiares, que sin duda alguna fueron pilares fundamentales para nuestra formación académica, profesional y personal

MICHEL ALEXANDER VIDAL PINARGOTE

JAMES ROGGER PESANTES PIGUAVE

RESUMEN

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS ADMINISTRATIVAS

TEMA: "DISEÑO DE PORTAL CAUTIVO PARA EL USO DEL INTERNET A TRAVÉS DE LA RED WLAN PARA LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL."

En el ámbito de la infraestructura de red WLAN el tema de seguridad, es algo que en la última década se ha convertido en algo muy relevante para los administradores de red. Y con los avances tecnológicos se puede tener muchas alternativas para poder suplir esta brecha, en la cual para este proyecto hemos escogido la del portal cautivo.

En la Facultad de Ciencias Administrativas se ha encontrado esta falencia o brecha de seguridad, para lo cual se propuso realizar mediante este proyecto el análisis y diseño de una solución viable. Lo cual se describe desde el análisis de la problemática hasta los objetivos que se quiere lograr con este estudio, dado que desde la parte de IT se desea.

El uso de las WLAN ha incrementado exponencialmente, dado a este lugar a unas de las más utilizadas en la mayoría de las instituciones, compañías o industrias para brindar a sus usuarios finales.

PALABRAS CLAVES: Administración de navegación, Administración de perfiles, WLAN, Portal cautivo.

ABSTRACT

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS ADMINISTRATIVAS

TOPIC: "DISEÑO DE PORTAL CAUTIVO PARA EL USO DEL INTERNET A TRAVÉS DE LA RED WLAN PARA LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL."

In the field of network infrastructure WLAN security issues, it is something that in the last decade has become very important for network administrators. And with technological advances you can have many alternatives to fill this gap, which for this project have chosen the captive portal.

In the Faculty of Administrative Sciences it has found this failure or security breach, for which were proposed by this project the analysis and design of a viable solution. Which is described from analyzing the problem to the objectives to be achieved in this study, because you want from the part of IT.

The use of WLAN has increased exponentially, given this place to one of the most used in most institutions, companies or industries to provide their end users

KEYWORDS: Navigation Administration, Administration profiles, Wlan, Captive Portal.

CUERPO PRELIMINAR

ÍNDICE GRÁFICO.

Introducción

En los últimos tiempos las soluciones tecnológicas con referencia a las redes móviles se han visto en un crecimiento. Y, lugares sociales como restaurantes, universidades, centros comerciales están implementado el uso de la red Wi-Fi abierta para que sus usuarios puedan tener acceso a internet y así brindar un plus a sus servicios.

Dentro del Ecuador, en las diversas ciudades y en las diferentes localidades que brindan algún tipo de servicio se pueden encontrar con una red Wireless (Wi-Fi) abierta que los administradores o dueños implementan para poder atraer y brindar un plus en su localidad. Sin embargo en algunos de estos lugares no es factible dejar al libre albedrío el uso de este recurso.

Las diferentes seguridades que han existido para este tipo de tecnología han quedado obsoletos en el transcurso de los avances tecnológicos y es así que los administradores de red que se han quedado en el pasado no pueden ofrecer alternativas a sus instituciones, ya que las mismas se apalancan en un método de restricción total del recurso lo cual no es a lo que se quiere llegar implementado un hotspot. Muchas de las instituciones no prestan la debida atención a este tipo de seguridades, creyendo que con una implementación de seguridad WPA (Wi-Fi Protected Access) es más que suficiente.

Capítulo 1

Diseño teórico

Respondiendo a las diversas necesidades de la administración de las redes Wi-Fi abiertas, se ha ideado diseñar un portal cautivo, con el fin de poder contribuir a la mejor administración de una de las redes más utilizadas en las Facultades o en cualquier institución que es el Wi-Fi; esto sin afectar la calidad de la misma.

Por medio de este proyecto, no solo estaremos aportando un método de administración de redes Wi-Fi, sino que se fomenta el mejor uso a este tipo de redes ya que los usuarios estarán limitados al uso del ancho de banda y de las páginas que la administración defina.

En base a la propuesta de este proyecto, se debe hacer referencias a diversos temas técnicos-informáticos, desde cómo se estudia la comunicación de redes computacionales hasta cuáles son los componentes de una red inalámbrica. Esto para poder comprender desde donde se realizó el estudio para este proyecto hasta llegar al objetivo del mismo.

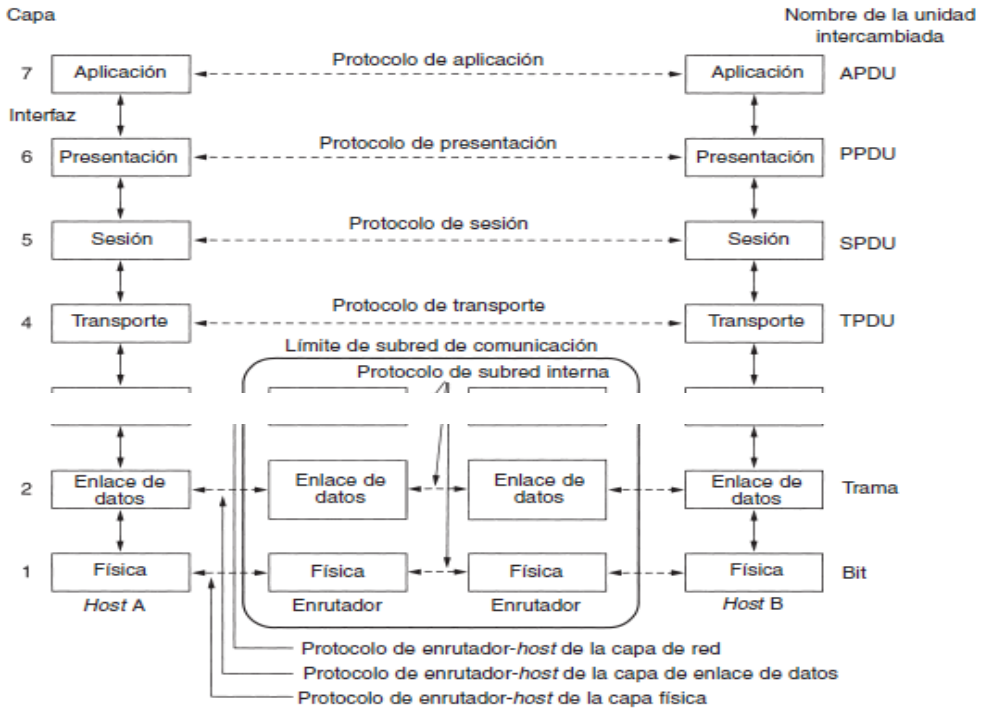
En este documento se va describir el modelo referencial OSI el cual está diseñado para poder entender cómo se da la comunicación desde el nivel más bajo hasta su nivel más complejo , también se incluye concepto de las redes inalámbricas, sus protocolos , componentes , los tipos de conexiones que existen y conceptos de los mismos, las ventajas de utilizar las redes inalámbricas y sus desventajas , los tipos de seguridades que existen en redes WLAN, concepto de portal cautivo con sus respectivos conceptos técnicos y funcionalidades.

Modelo OSI.

Una red informática, es un conjunto de computadoras que están conectadas entre ellas para poder compartir cualquier tipo de recurso sea este una impresora, escáner o medio de almacenamiento y de esta manera mantener flexibilidad en tareas o procesos que los usuarios realizan dentro de una organización.(Carballeiro, 2012)

Para poder entender el funcionamiento de una red informática, se creó un modelo referencial para poder comprender, interpretar, analizar y brindar soluciones en cada una de sus capas. Este modelo llamado referencia de interconexión de sistemas abiertos (OSI) es un estándar creado por la Organización Internacional de la Normalización (ISO) la cual se compone por siete capas que se describen a continuación en la imagen 1.1.

Imagen 1-1 Modelo referencial OSI



Fuente: Redes de Computadoras.

Capas de aplicación.

La capa de aplicación contiene varios protocolos que la mayoría de usuarios utilizan con frecuencia. Uno de los protocolos más utilizados es HTTP (Hyper Text Transfer Protocol) que es la base de World Wide Web. Existen más protocolos como el DNS (Domain Name Server), DHCP (Dynamic Host Configuration Protocol) entre otros.

Esta capa es la más cercana al usuario, suministra servicios de red a las aplicaciones de los usuarios, difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a las aplicaciones. Adicional establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de integridad de los datos.

En esta capa se define las aplicaciones de red y la mayoría de los servicios de internet estándar que pueda utilizar un usuario. Aquellos servicios utilizan la capa de transporte para enviar y recibir datos. Existen varios protocolos de la capa de aplicación, a continuación se enlistan ejemplos de protocolos de capa de aplicación:

-Servicios TCP/IP estándar como los comandos ftp, tftp y telnet.

-Comandos UNIX "r" como rlogin o rsh.

-Servicios de nombres, como INS o el sistema de nombre de dominio DNS.

-Servicio de directorio (LDAP).

-Servicio de archivos, como el NFS

-Protocolo simple de administración de red (SNMP), que permite administrar la red.

-Protocolo RDISC (Router Discovery Server) y protocolo RIP (Routing Information Procotol).

Capa de presentación.

La capa de presentación como su nombre mismo indica se encarga de la presentación de los datos transportados es decir la sintaxis y la semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar, las estructuras de datos que se intercambiarán se pueden definir de una manera abstracta, junto con una codificación estándar para su uso "en el cable". La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de un nivel más alto (por ejemplo, registros bancarios).(Tanenbaum, 2003)

Un ejemplo típico de servicio de capa de presentación es la codificación de datos en una forma estándar acordada. La mayor parte de los programas de usuario no intercambia cadenas de bits al azar, intercambian cosas como: nombres de personas, fechas, cantidades de dinero, cuentas. Estos elementos se representan como cadenas de caracteres, enteros, cantidades de puntos flotantes y estructura de datos compuestas por varios elementos. A continuación se detalla las operaciones de la capa de presentación:

-Traducir entre varios formatos de datos utilizando un formato común.

-Definir la estructura de datos a transmitir.

-Definir el código a usar para representar una cadena de caracteres.

-Dar formato a la información para visualizarlo o imprimirlo.

-Comprimir los datos si es necesario.

-Aplicar a los datos procesos criptográficos.

Capa de sesión.

La capa de sesión permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen diversos servicios, como el control de diálogo (Dar seguimiento a quién le toca transmitir), administración de Token (Que impide que los las dos partes traten de realizar las mismo operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a transmisiones largas para permitirles continuar desde donde se encontraban después de una caída).(Tanenbaum, 2003)

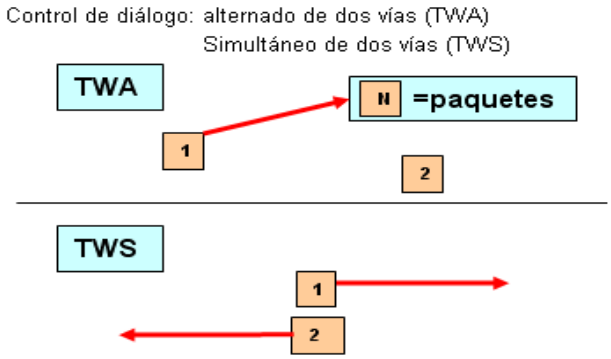
El direccionamiento usado en esta capa es lógica a diferencia del direccionamiento físico empleado en la capa de enlace de datos que es física. Este direccionamiento lógico permite mantener abiertos diferencias servicios o puertos a una o ciertas dirección de la capa de red.

La capa de sesión establece, administra y termina las sesiones entre las aplicaciones. Esto incluye el inicio, la terminación y la resincronización de dos equipos que están manteniendo una sesión. La capa de sesión coordina las aplicaciones mientras interactúan en dos hots que se comunica entre sí. La comunicación de datos se transporta a través de redes conmutadas por paquetes, al contrario de lo que ocurre con las llamadas telefónicas que se transportan a través de redes conmutadas por circuitos.

La capa de sesión decide si va a utilizar la conversación simultánea de dos vías o la comunicación alternada de dos vías. Esta decisión se la conoce como control de diálogo. Si se permite comunicaciones simultáneas de dos vías, entonces la capa de sesión poco puede hacer en

cuanto al manejo de la conversación, es posible que en la capa de sesión se produzcan colisiones cuando un mensaje pasa a otro, causando confusión en uno de los hots que se comunican, o en ambos. Si estas colisiones de la capa de sesión se vuelven intolerable, entonces el control de diálogo cuenta con otra opción: La comunicación alternada de dos vías que involucran el uso de un token de datos de la capa de sesión que permite cada hots se comuniquen por turno.

Imagen 1-2 Manejo de Token



Fuente: Biblia TCP/IP.

La capa-5 tiene una serie de protocolos importantes. Debemos ser capaces de reconocer estos protocolos cuando aparezcan en un procedimiento de conexión o en una aplicación. Los siguientes son ejemplos de protocolos de capa-5:

-Sistema de archivos de red(NFS).

-Lenguaje de consulta estructurado (SQL).

-Llamada de procedimiento remoto (RPC).

-Sistema X-Windows.

-Protocolo de sesión Apple Talk(ASP).

-Protocolo de control de sesión de arquitectura de red digital (DNA SCP)

Capa de transporte.

La capa de transporte tiene como función principal aceptar los datos provenientes de las capas superiores y separarlos en unidades más pequeñas si es necesario, lo cual se conocen como segmentos y estos enviarlos a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo, además todo esto debe hacerse con eficiencia y de manera que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware. La capa de transporte también es la que determina qué tipo de servicio va a proporcionar la capa de sesión y finalmente a los usuarios de la red(Tanenbaum, 2003).

La capa de transporte en sí es una conexión de extremo a extremo en toda la ruta. Demos un simple ejemplo cuando una máquina origen quiere llevar a cabo una conversación con un programa similar en una máquina destino. Las capas inferiores operan en sus propias máquinas con sus vecinos inmediatos sean estos los superiores o inferiores cual sea la forma de que se la analice. Esto quiere decir que desde la capa-3 hacia abajo las capas trabajan en conjunto en sus propias estaciones, mientras que las capas superiores trabajan de extremo a extremo.

Los protocolos más comunes de la capa de transporte del conjunto de protocolos TCP/IP son el protocolo de control de transmisión (TCP) y el protocolo de datagrama de usuarios (UDP). Ambos protocolos gestionan la comunicación de múltiples aplicaciones.

UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP

se llaman datagramas. Este protocolo de la capa de transporte envía estos datagramas como mejor intento. Entre las aplicaciones que utilizan UDP son:

-Sistema de nombre de dominio (DNS).

-Streaming de video.

-Voz IP.

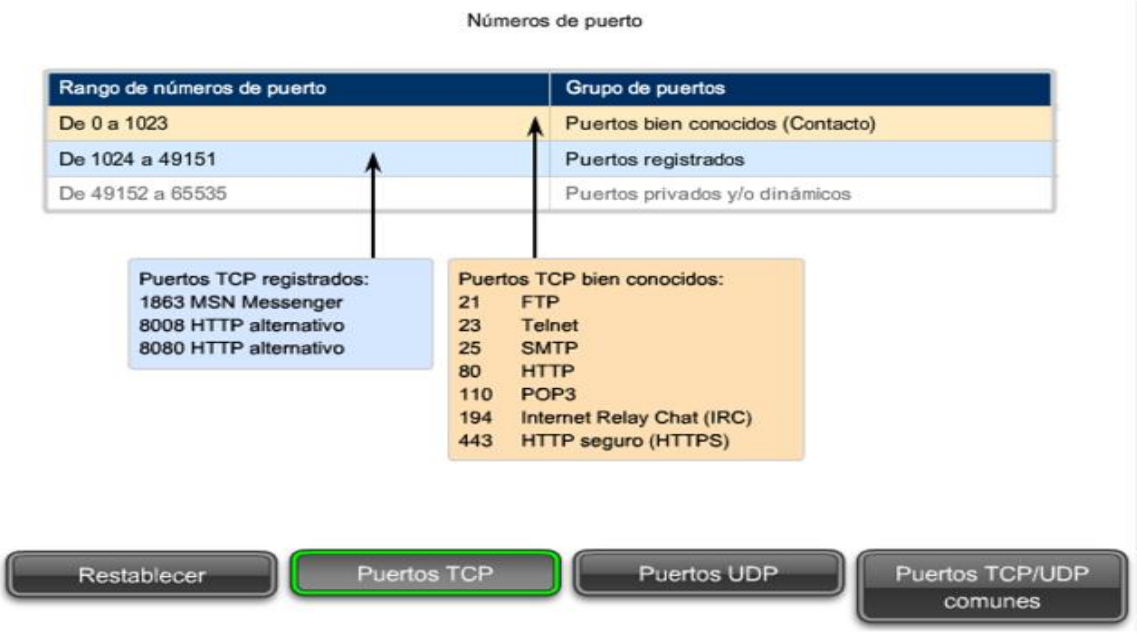
TCP es un protocolo orientado a la conexión, descrito en la RFC 793. Este incurre en el uso adicional de recursos para agregar funciones adicionales especificadas por TCP, las cuales están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento TCP posee 20 bytes de carga en el encabezado, que encapsulan los datos de la capa de aplicación, mientras que cada segmento UDP solo posee 8-bytes de carga.

Los servicios basados en TCP y UDP mantienen un seguimiento de las varias aplicaciones que se comunican. Para diferenciar los segmentos y datagramas para cada aplicación, tanto TCP como UDP cuentan con campos de encabezado que pueden identificar de manera exclusiva estas aplicaciones, estos identificadores únicos son los números de los puertos.

En el encabezado de cada segmento o datagrama hay un puerto de origen y de destino, el número de puerto de origen es el número para esta comunicación asociada con la aplicación que origina la comunicación en el host local, el número de puerto de destino es el número para esta comunicación asociada con la aplicación de destino en el host remoto.

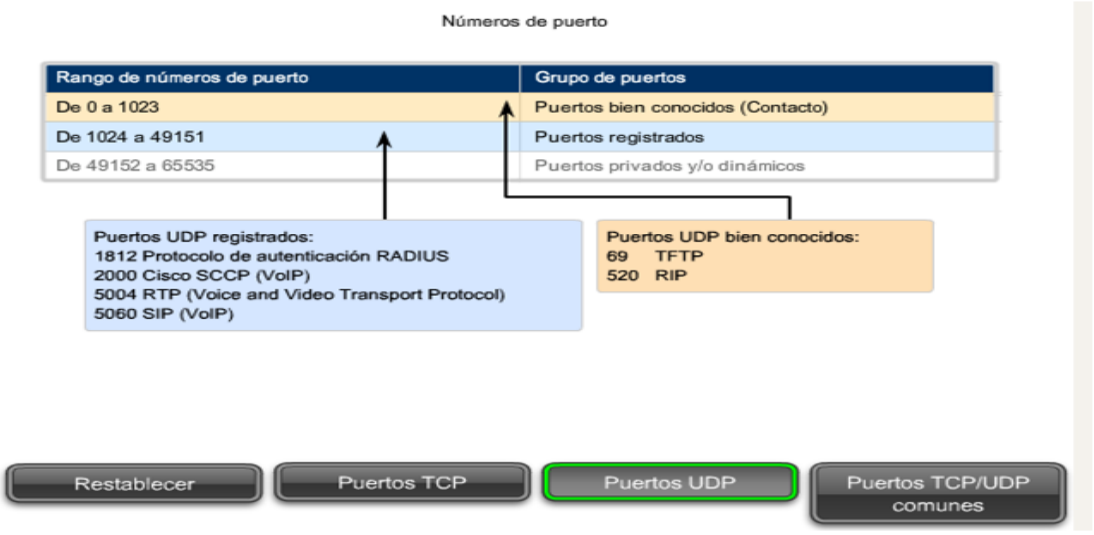
La autoridad de números asignados de Internet (IANA) asigna números de puerto. IANA es un organismo de estándares responsable de la asignación de varias normas de direccionamiento.

Imagen 1-3 Puertos TCP



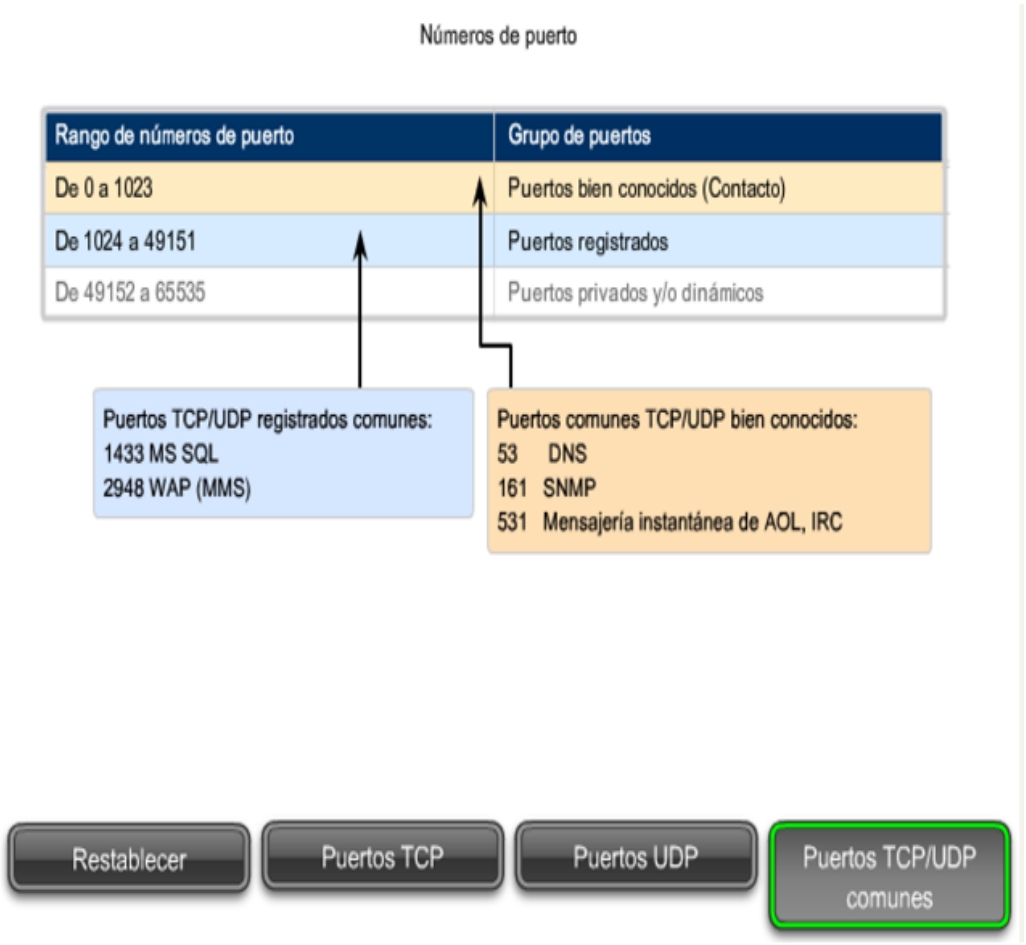
Fuente: La biblia de TCP/IP.

Imagen 1-4 Puerto UDP.



Fuente: La biblia de TCP/IP.

Imagen 1-5 Puertos UDP.



Fuente: La biblia de TCP/IP.

Las diferencias entre TCP y UDP es la confiabilidad de la comunicación TCP que se lleva a cabo utilizando sesiones orientadas a la conexión, antes de que un host que utiliza TCP envíe datos a otro host, la capa de transporte inicia un proceso para crear una conexión con el destino. Esta conexión permite el rastreo de una sesión o stream de comunicación entre los hots, este proceso asegura que cada host tenga conocimiento de la comunicación y se prepare.

Una conversación TCP completa requiere el establecimiento de una sesión entre los hosts en ambas direcciones.

Luego establecida la sesión, el destino envía acuses de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP. Cuando el origen recibe un acuse de recibo, reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos. Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado.

Capa de red.

La siguiente capa a nombrar es la capa de red la cual está encargada de controlar las operaciones de la subred. Al momento de diseñar una red de manera lógica es indispensable determinar cómo van a ser enrutados los paquetes IP desde su origen hacia su destino. (Tanenbaum, 2003) Las rutas pueden estar basadas en tablas estáticas codificadas en la red y que rara vez cambian.

(Tanenbaum, 2003) El concepto básico del enrutamiento estático, es que la ruta que van a seguir los paquetes desde su origen hacia su destino será definida por el administrador de red. Las rutas también pueden determinarse cuando los enrutadores cambian información de enrutamiento (Enrutamiento dinámico).

Al momento de que un paquete IP deba viajar desde una red hacia otra para poder llegar al destino deseado, pueden surgir muchos inconvenientes. El direccionamiento de la segunda red puede ser diferente que la de la primera, la cual no podría aceptar paquetes demasiados largos, o los protocolos podrían ser diferente, etc. Todo lo antes mencionado debe resolver la capa de red

para que redes heterogéneas se puedan comunicar. La capa-3 del modelo OSI realiza cuatro procesos básicos:

-Direccionamiento, donde debe proveer un mecanismo para direccionar dispositivos finales.

-Encapsulamiento, la capa de red debe proveer un mecanismo de encapsulación. Los dispositivos no deben ser identificados solo con una dirección.

-Enrutamiento, el cual es la función de router ya que debe seleccionar las rutas y dirigir paquetes hacia un destino

-Desencapsulamiento, es aquí donde el paquete llega al host de destino y es procesado por la capa-3. El host examina la dirección de destino para verificar que el paquete fue direccionado al dispositivo correspondiente. Si la dirección es correcta, el paquete es desencapsulado por la capa de red y la PDU de la capa-4 contenida en el paquete pasa hasta el servicio adecuado en la capa de transporte.

En la capa de red se encuentra dos métodos para realizar el enrutamiento, los cuales son: Enrutamiento estático, el cual es una ruta fija predeterminada por el administrador de red, estas rutas no se actualizan automáticamente ya que deben actualizarse por el mismo administrador de red. Las mismas poseen algunas ventajas y desventajas.

Ventajas.

-Se configura manualmente.

-Son más estables.

-Manejan rutas por defecto.

-Fácil de configurar en redes pequeñas.

-Usan menos ancho de banda.

Desventajas.

-El administrador debe tener una gran comprensión de la red.

-Si se agrega una nueva red debe agregarse en todos los ruteadores.

-En grandes redes la actualización puede ser más complicada de realizar.

El enrutamiento dinámico, es facilitar el intercambio de información, esto permite compartir información de redes remotas y agregarlas automáticamente a la tabla de enrutamiento. Un protocolo de enrutamiento dinámico requiere menos sobrecarga administrativa, pero en cambio consumirá parte de los recursos del router, como tiempo del CPU y ancho de banda de los enlaces. En una red con más de una ruta posible al destino podría usarse este tipo de enrutamiento

Una ruta dinámica es construida por información intercambiada por los protocolos de enrutamiento. Los protocolos son diseñados para distribuir información, únicamente ajustan las rutas reflejadas en las condiciones de la red. Los protocolos de enrutamiento manejan complejas situaciones de enrutamiento más rápido de lo que el administrador del sistema podría hacerlo.

Ventajas.

-Menos carga de trabajo para agregar o quitar redes.

-Ajuste automático ante cambios en la topología.

-Menos propenso a errores de configuración.

-Escalable, el crecimiento de la red no es un problema.

Desventajas.

-Requiere recursos del router.

-Requiere más conocimiento para la configuración y solución del problema.

En esta capa existen algunos dispositivos que trabajan, comenzando desde un routeador, un switch multicapa, firewall y servidores AAA (Authentication, Autorization, Accounting)

Capa de enlace de datos.

(Tanenbaum, 2003) La siguiente capa es la de enlace de datos, la cual es la responsable de transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red aparezca libre de errores de transmisión, esto logra haciendo que el emisor fragmente los datos de entrada en tramas de datos y transmitiendo las tramas de manera secuencial. Si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción.

Las principales funciones de la capa de enlace de datos son:

-Delimitar marcos.

-Mantener la integridad de los marcos.

-Proveer transparencia de datos.

-Detectar de errores.

-Retransmitir de marcos para recuperarse de errores.

-Permitir el control de flujo.

-Supervisar las funciones de enlace.

La capa de enlace de datos se encuentra dividida en dos subcapas las cuales son:

-Control de acceso al medio (MAC).
-Control de enlace lógico (LLC).

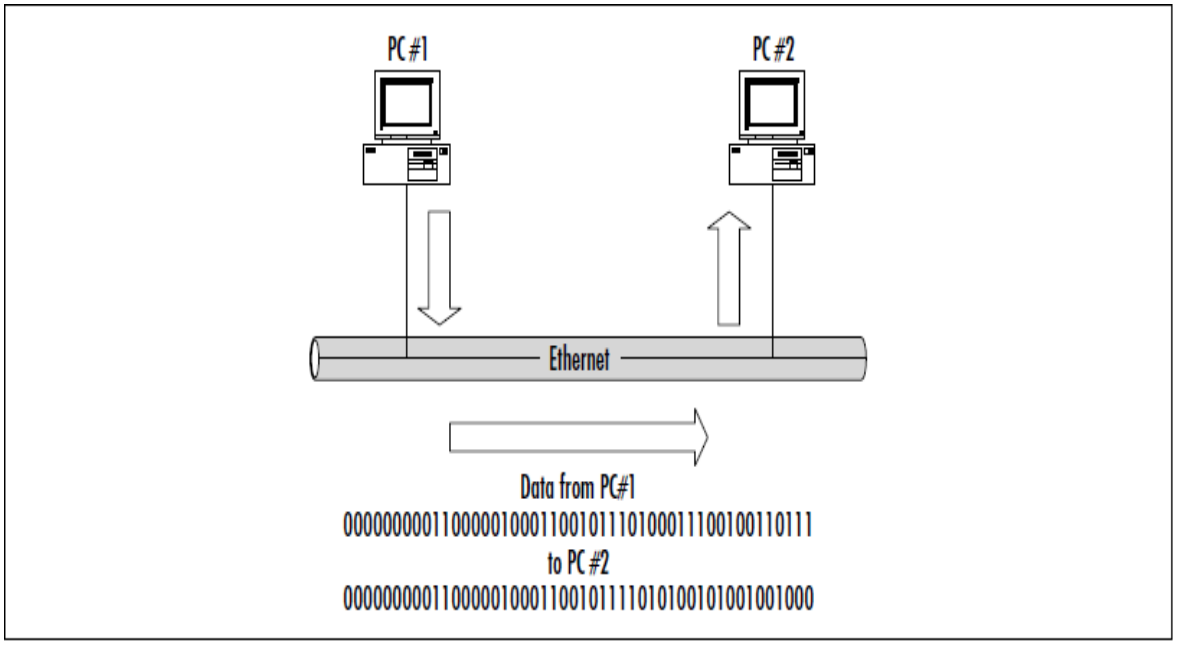
Estas dos subcapas juegan un papel fundamental en la operación de una red.

La sub-capa de control de acceso al medio es el encargado de identificar los dispositivos en una red informática. Ya que según el estándar del sistema de modelo OSI, cuando una interface de red en una router, switch, PC, servidor u otro dispositivo que se conectan a las LAN llevan con ellos una dirección única global de 48-bits que se encuentra en la ROM de la interface la cual debe ser única en la red. La subcapa MAC es la más baja de las subcapas y es el responsable de determinar el método de acceso al medio tales como contador de pasar (Token Ring o FDDI) o contención (CSMA / CD).(Ouellet, Padjen, Pfund, Fuller, & Blankenship, 2002).

En caso de las redes inalámbricas porque se especifica el protocolo de acceso al medio propiamente dicho así como una serie de peculiaridades propias de las redes inalámbricas como el envío de acuses de recibo, la posibilidad de realizar segmentación de las tramas y los mecanismo de encriptación para dar confidencialidad a los datos transmitidos. En esta subcapa no se utiliza el CSMA/CD sino el CSMA/CA ya que según este protocolo, el emisor antes de transmitir envía una trama RTS (Request to send), indicando la longitud de datos que desea enviar. El receptor contesta con una trama CTS (Clear to Send) repitiendo la longitud. El emisor

al recibir el CTS envía sus datos. A continuación se muestra la imagen 2.1 donde se muestra un ejemplo de direcciones MAC.

Imagen 1-6 Capa MAC.



Fuente: Cisco Wireless LAN

La siguiente sub-capa es la de control de enlace lógico que es aquella que se encarga de la manipulación de control errores, control de flujo, el encuadre, y direccionamiento de la sub-capa MAC. El protocolo más común en la sub-capa de control de enlace lógico es IEEE 802.2, este mismo define servicio de puntos de acceso (PAE) a través de un campo en la Ethernet. Estas PAE en conjunto con la dirección MAC puede identificar de forma exclusiva el destinatario de una trama, por lo general LLC se utiliza para protocolo tales como Sistema Arquitectura de RED (SNA) que no tienen una capa de red correspondiente.(Ouellet, Padjen, Pfund, Fuller, & Blankenship, 2002).

En esta capa trabaja un protocolo más conocido como ARP (Address Resolution Protocol). Cada equipo conectado a la red tiene un número de identificación de 48-bits. Este es un número único establecido de fábrica, sin embargo la comunicación en el internet no utiliza directamente este número, para que las direcciones físicas se puedan conectar con las direcciones lógicas, el protocolo ARP realiza una interrogación a los equipos conectados a la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché.

Los dispositivos que intervienen en la capa dos del modelo OSI son los siguientes:

-Tarjeta de red o NIC.

-Bridge o Puente.

-Switch de Capa 2.

Una de las características de la capa de enlace de datos es el control de errores, los cuales se realizan al momento de enviar los datos, ya que se codifica en un formato especial, que consiste normalmente en añadir información (Overhead) al final. Los códigos en función de la distancia de Hamming pueden ser:

Detectores: Tienen menos overhead, pues necesitan incorporar menos redundancia.

Correctores: Estos se utilizan bien en conexiones simplex, bien en multicast o bien en tiempo real.

En esta capa existe un mecanismo necesario para no agobiar al receptor conocida como control de flujo, este utiliza diferentes mecanismos de retroalimentación para mandar señales de

control de flujo, y por tanto requiere un canal semi-duplex o full-duplex. Estas señales pueden ser activación de líneas de hardware(RTS,CTS), caracteres especiales(XON,XOFF) o tramas especiales conocida como acknowledgment (ACK) de reconocimiento, para notificar la recepción correcta. Lo envíos de los ACKS permiten controlar al transmisor, de forma que si no se le reconoce las tramas enviadas, este espera hasta que se le reconozcan, además también se envía aprovechando la transmisión de datos en sentido contrario la cual se conoce a esta técnica como piggybacked o llevar de espaldas.

Capa física.

Nosotros vamos a comenzar por analizar el funcionamiento de la capa física, ya que es la capa en donde se estudia cual va hacer el medio o el mecanismo por el cual se va a transmitir los 0`s y los 1`s de la data binaria, es decir donde se define el medio físico sea este por cable o por ondas electromagnéticas. En esta capa también deben asegurarse al momento de su diseño , cuando de un lado se envía un bit 1 , el otro lado lo recibe como tal y no como bit 0.

En esta capa es donde se delimita el ancho de banda, es decir, que la mayor capacidad va a estar definida por el medio físico en el cual se transporten los datos y todo va a depender del grosor, la construcción y longitud de dicho medio. Aquí podemos citar los medios de comunicación guiados:

Par trenzado, es el medio de comunicación más viejo y el más común actualmente el cual consiste en dos alambres de cobre aislado, por lo general de 1mm de grueso. Los alambres se trenzan de forma helicoidal, parecida a una molécula de ADN. Su velocidad dependerá del grosor del cable y de su longitud, a veces pueden llegar a algunos megabits/seg. Existen varios

tipos de cable de par trenzado que lo nombraremos como es categoría-3, categoría-5, categoría-6, categoría-7.

Cable coaxial, a comparación con el par trenzado mantiene mejor blindaje, por lo cual alcanza mayores tramos de longitud a velocidades superiores. Este cable consiste en un alambre de cobre rígido como núcleo, rodeado por materiales aislantes. El aislante está forrado con un conductor cilíndrico, que con frecuencia es una malla de tejido fuertemente trenzado. El conductor externo se cubre con una envoltura protectora de plástico. Los cables modernos tiene un ancho de banda cerca de 1 GHz(Tanenbaum, 2003).

Fibra óptica, es un sistema de transmisión óptico que mantiene tres componentes: la fuente de luz, el medio de transmisión y el detector. Básicamente, un impulso de luz indica un bit-1 y la ausencia de luz indica un bit-0. El medio de transmisión es una fibra de vidrio ultra delgada. El detector genera un pulso eléctrico cuando la luz incide en él.

El cable de fibra se parece al coaxial, excepto por el trenzado, en el centro se encuentra el núcleo de vidrio, a través de la cual se propaga la luz. En las fibras multimodo el diámetro es de 50 micras, aproximadamente el grosor de un cabello humano. En las fibras mono modo el núcleo es de 80 a 10 micras.(Tanenbaum, 2003)

El medio de la capa física que se tratará en este proyecto, es la transmisión inalámbrica, pues aquí es donde la capa física del modelo referencial OSI cambia.

El concepto se basa en que una onda electromagnética es la forma de propagación de la radiación electromagnética a través del espacio, son ondas producidas por el movimiento de una carga eléctrica, son disturbios ondulatorios que se repiten en una distancia determinada, llamada longitud de onda. A diferencia de una onda mecánica, las ondas electromagnéticas no dependen

de un medio físico para propagarse, se propagan libremente por el aire. La comunicación inalámbrica se basa en un principio, que al conectar una antena de tamaño apropiado a un circuito eléctrico, las ondas electromagnéticas pueden ser difundidas de manera eficiente y receptadas a cierta distancia.

En este tipo de comunicación el modelo OSI cambia, siendo estas afectadas la capa física y la subcapa enlace de datos. La capa física se divide en dos sub-capas, la inferior llamada PMD (Physical Media Dependent), que depende a cada uno de los sistemas de transmisión a nivel físico. La subcapa superior, PLCP (PhysicalLayerConvergenceProcedeure) la cual se encarga de homogénear de cara a la capa MAC las peculiaridades de las diversas especificaciones de la subcapa PMD.

Existen muchos organismos internacionales y nacionales, organismo de regulación gubernamental y compañías privadas que intervienen en el establecimiento y el mantenimiento de los estándares de la capa física. Por ejemplo los siguientes organismos definen y rigen los estándares de hardware, medios, codificación y señalización de la capa física:

-Organismo internacional para la Estandarización (ISO).

-Telecommunications Industry Association/Electronic Industries Association (TIA/EIA).

-Unión Internacional de Telecomunicaciones (UIT).

-American National StandardsInstitute (ANSI)

-Instituto de Ingenieros en Electricidad y Electrónica (IEEE)

-Autoridades nacionales reguladoras de las telecomunicaciones, incluida la Federal Communication Commission (FCC) de los EE. UU. y el European Telecommunications Standards Institute (ETSI)

Imagen 1-7 Estándares de capa Física y sus organismos.

Organismo de estandarización	Estándares de red
ISO	• ISO 8877: adoptó oficialmente los conectores RJ (p. ej., RJ-11, RJ-45). • ISO 11801: Estándar de cableado de red similar a EIA/TIA 568.
EIA/TIA	• TIA-568-C: estándares de cableado de telecomunicaciones, utilizados en casi todas las redes de datos, voz y video. • TIA-569-B: estándares de construcción comercial para rutas y espacios de telecomunicaciones. • TIA-598-C: código de colores para fibra óptica. • TIA-942: estándar de infraestructura de telecomunicaciones para centros de datos.
ANSI	568-C: Diagrama de pines RJ-45. Desarrollado conjuntamente con EIA/TIA.
ITU-T	G.992: ADSL
IEEE	• 802.3: Ethernet • 802.11: LAN inalámbrica (WLAN) y malla (certificación Wi-Fi) • 802.15: Bluetooth

Fuente: Cisco Networking Academy.

Protocolos IPV4 IPV6

Protocolo IPV4.

Es la primera versión de IP que es implementada en forma extensiva. IPV4 es el principal protocolo utilizado a nivel de red de modelo TCP/IP y fue creado por la IETF (Internet Engineering Task Force).

Una de las características del protocolo IP es brindar una dirección lógica única a cada equipo ya sea este físico o virtual y con esto poder generar un direccionamiento lógico para la entrega de los paquetes transmitidos por la red.

IPV4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones de paquetes. Tienen las siguientes características:

-Es un protocolo de un servicio de datagrama no fiable.

-No proporciona garantía en la entrega de datos.

-No proporciona garantía sobre la corrección de datos.

-Puede resultar paquetes duplicados o en desorden y la fiabilidad depende del protocolo con el que se esté trabajando.

En este protocolo se hace el uso del broadcast, por aquello hay ataques de denegación de servicios como tormenta de broadcast. Todos los problemas antes mencionados se solventan en niveles superiores.

El protocolo IPV4 utiliza direcciones de 32-bits(4-Bytes) u ocho octetos que limitan el número de direcciones posibles a utilizar. Pero muchas de estas están reservadas para propósitos especiales como redes privadas.

Las redes IPV4 se dividen en redes públicas y privadas, de las cuales las privadas tienen tres rangos especiales que no tienen encaminamiento hacia redes públicas

-10.0.0.0 a 10.255.255.255
-172.16.0.0 a 172.16.255.255
-1923.168.0.0 a 192.168.255.255

Los tres rangos de redes públicas son:
-1.0.0.0 a 126.255.255.255(Clase A).
-128.0.0.0 a 191.255.255.255(Clase B).
-192.0.0.0 a 223.255.255.255(Clase C).

Protocolo IPV6.

Debido al crecimiento del internet y a la sofisticación de los dispositivos electrónicos las diferentes soluciones propuestas para escalar el espacio de direccionamiento IPV4 no será suficiente para cubrir la necesidad de la misma. Es así como nace la nueva versión del protocolo IP diseñados por el grupo especial de ingeniería de internet (Internet Engineering Task Force o IETF), la cual ahora se la conoce como IPV6.

Las características de IPV6 son las siguientes:

-Esquema de direcciones de 128-bits provee con la posibilidad de asignar direcciones únicas globales a nuestros dispositivos.

-Tiene un paquete más ligero.

-Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al internet.

-El proceso de autoconfiguración permite que los nodos de la red IPV6 configuren sus propias direcciones IPV6, facilitando su uso.

-La transición entre proveedores de IPV6 es transparente para los usuarios finales con el mecanismo de remunerado.

-La difusión ARP es reemplazada por el uso de multicast en el link local.

-El encabezado de IPV6 es más eficiente que el de IPV4: tiene menos campos y se elimina la suma de verificación del encabezado.

-Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.

-Las nuevas extensiones de encabezado reemplazan el campo opciones de IPV4 y proveen mayor flexibilidad.

-IPV6 fue esbozado para manejar mecanismos de movilidad y seguridad de manera más eficiente que protocolo IPV4.

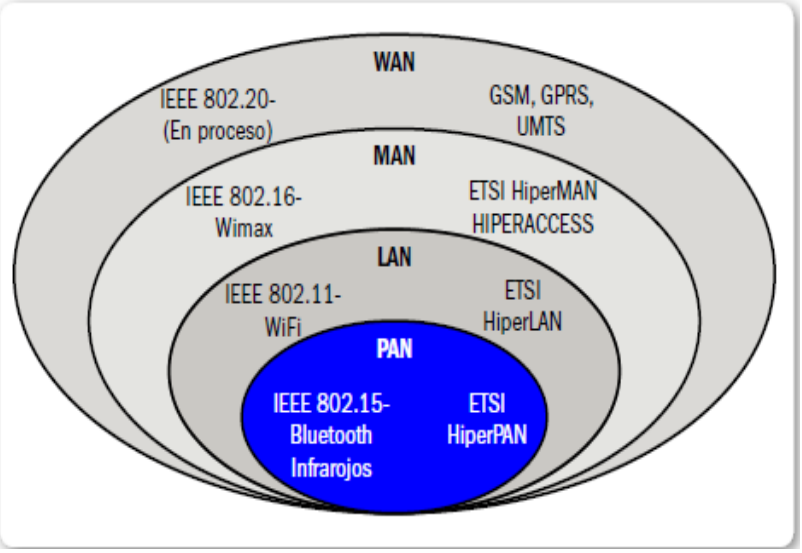
-Se crearon varios mecanismos junto con el protocolo para tener unas transición sin problemas de la redes IPV4 a las IPV6.

Debido a la mayor distribución de direcciones se posibilita el uso de un solo prefijo grande para toda la red de una organización y así el ISP puede agregar todos los prefijos de sus clientes y anunciarlos a internet IPV6. Este también incluye la configuración automática de dirección sin estado IPV6 que permite que el ruteador envíe a través del enlace local, la información de la red a sus computadoras.

Redes inalámbricas.

Siempre cuando escuchamos la palabra inalámbrico, se habla de conexión de equipos o dispositivos de red sin la necesidad de un cable físico. Estas mismas se dividen idénticamente como las redes LAN cableadas, basándonos en el alcance que posee cada una de ellas: redes WAN, redes MAN, redes LAN y redes PAN. A continuación en la imagen 2.2 se pueden visualizar las diferentes tecnologías inalámbricas con sus estándares:

Imagen 1-8 División de tecnologías Inalámbricas con sus Protocolos.



Fuente: Redes Wi-Fi en entornos Windows.

Existen dos tipos de tecnologías que emplean la radiofrecuencia, la banda estrecha y la banda ancha, también conocida como espectro ensanchado, esta última es la que más se utiliza. Consiste en difundir la señal de la información a lo largo del ancho de banda disponible, en otras palabras, en vez de concentrar la energía de las señales alrededor de una portadora concreta lo

que hace es difundirla por toda la banda disponible. Se comparte con el resto de usuarios. Existes dos tipos de tecnologías espectro ensanchado:

DSSS (Direct Sequence Spred Spectrum). El espectro ensanchado de secuencia directa es una técnica que genera un patrón redundante para cada uno de los bits que componen la señal. Para que la señal sea un poco más resistente a las interferencias, la misma debe ser mayor.

El estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado de secuencia directa, la modulación DBPSK (Differenctial Binary Phase Shift Keying) que proporcionan una velocidad de transferencia de 1-Mbps y la modulación DQPSK (Differenctial Quadrature Phase Shift Keying) que proporciona una velocidad de transferencia de 2-Mbps La IEEE ha revisado este estándar conocida como 802.11b que aporta mejoras de seguridad, aumenta la velocidad hasta 11-Mbps.

FHSS (Frequency Hosping Spread Spectrum), conocida como espectro ensanchado por salto en frecuencias la cual consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada dwell time a inferior a 400-ms. Pasado este tiempo se cambia de frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

La zona de 2,4-GHz también utiliza esta técnica, la cual se organiza en setenta y nueve canales con un ancho de banda de 1-MHz cada uno.

OFDM (Orthogonal Frequency Division Multiplexing), la multiplexión por división de frecuencias ortogonales, es una tecnología en enviar un conjunto de portadoras de diferentes frecuencias donde cada una transporta información. La modulación OFDM es muy robusta

frente al multitrayecto, que es lo más normal en canales de radiodifusión confrontando las atenuaciones selectivas en frecuencia y frente a las interferencias de RF.

Imagen 1-9 Medios de nivel físico en 802.11

Medio físico	Infrarrojos	FHSS	DSSS	OFDM
Banda	850 – 950 nm	2,4 GHz	2,4 GHz	2,4 y 5 GHz
Velocidades* (Mb/s)	1 y 2 (802.11)	1 y 2 (802.11)	11 (802.11b)	54 (802.11a) 54 (802.11g) 300 (802.11n)
Alcance (a vel. Max.)	2 m	20 m	100 m	100 m
Utilización	Muy rara hoy	Poca. A extinguir	Mucha	Mucha
Características	No atraviesa paredes	Interferencias Bluetooth y hornos microondas	Buen rendimiento y alcance	Buen rendimiento y mejor alcance

Fuente: Redes inalámbricas WI-Fi.

En este proyecto nos concentraremos en el estudio de la redes WLAN, en la que por lo general se describe de una red de área local que tiene por medio de transmisión el aire. A este tipo de red inalámbrica se la conoce en el mercado como Wi-Fi y opera en la banda de 2,4-GHz(Carballeiro, 2012)

Protocolos de redes inalámbricas.

La familia de protocolos 802.11 que se conocen como circuito cerrado Wi-Fi es la tecnología que se utiliza hoy en día para la construcción de redes inalámbricas de bajo costo. Existen muchos protocolos de la familia 802.11 y no todos se encuentran relacionados con el protocolo de radio. Los tres estándares implementados en la mayoría de equipos disponibles son los que se detallan a continuación. (Aichele, y otros, 2007)

802.11b, ratificado por IEEE EL 16 de septiembre de 1999, el protocolo de redes inalámbricas 802.11b es el más asequible. La mayoría de los dispositivos que lo utilizan han sido vendidos desde 1999. Este protocolo utiliza una modulación conocida como espectro expandido por secuencia directa, la cual es una porción de las banda ISM (Industrial, Scientific and Medical) desde 2400-MHz a 2484-MHz. Mantiene como tasa de transmisión 11-Mbps. con una velocidad real de datos utilizable un poco más de 5-Mbps. (Aichele, y otros, 2007)

802.11g, este protocolo estuvo finalizado en junio del 2003, y se entiende que el protocolo como tal llegó un poco tarde al mercado inalámbrico. Sin embargo este protocolo es por defecto en las redes inalámbricas utilizado como característica estándar virtualmente todas las laptops y mucho de los dispositivos handheld. Utiliza el mismo rango ISM que 802.11b, pero con la diferencia que utilizan como Orthogonal Frequency Division Multiplexing (OFDM)-Multiplexaje por división de frecuencias ortogonales. Tiene una tasa de transmisión máxima de 54-Mbps y mantiene compatibilidad con el protocolo 802.11 b gracias al soporte de velocidades inferiores. (Aichele, y otros, 2007)

(Aichele, y otros, 2007)802.11a, también ratificado por la IEEE el 16 de septiembre de 1999, este protocolo igual que el 802.11g utiliza OFDM. Tiene una tasa de transmisión máxima de 54-

Mbps (Con un rendimiento real de hasta 27-Mbps). El 802.11a opera en la banda ISM entre 5725-MHz y 5850-MHz, y en una porción de la banda UNII entre 5.15-GHz y 5.35-GHz .Estas características hace incompatible con el 802.11b o el 802.11g, y su alta frecuencia implica un rango más bajo implica un rango más bajo comparado con el 802.11b/g al mismo nivel de potencia. Esta porción del espectro es casi no utilizada comparada con la 2.4-GHz, pero desafortunadamente su uso es legal solo en unos pocos lugares del mundo.

Componentes de una red WLAN.

En esta parte conoceremos los componentes que forman una red inalámbrica, hablando técnicamente del hardware como tal. Por lo general una red WLAN se conforma de un AP (Access Point), router inalámbrico, antenas, tarjeta de red inalámbrica.

Access Point o punto de acceso, es considerada como el punto principal de emisión y recepción de datos. Este equipo concentra la señal de los nodos inalámbricos y centraliza el reparto de información de toda la red local. También es el encargado de realizar el vínculo de la red inalámbrica con la red cableada.

Imagen 1-10 Punto de acceso.

Fuente: Redes Wi-Fi en entornos Windows**.**

Para entender mejor este concepto, coloquémonos de parte del cliente (Laptop, celulares, dispositivos móviles) y observemos al punto de acceso como un cable virtual desde cada cliente hacia él. De esta forma el Access point nos conecta a la red cableada como a cada uno de los usuarios conectados por cable.

Router inalámbrico, más utilizadas en conexiones ADSL (Asymmetric Digital Subscriber Line) que sirve para dar acceso a internet desde una línea telefónica y será este equipo el que nos va a conectar, aunque no es la única función que realiza ya que el mismo es una combinación de router y Access point y por lo tanto también podemos distribuir internet de manera cableada. Adicional este equipo puede restringir el acceso por usuarios, por MAC, servicios y horarios entre otras opciones.

Imagen 1-11 Router inalámbrico.

Fuente: Redes Wi-Fi en entornos Windows

Antena, es uno de los componentes más fundamental que existen dentro de este tipo de redes, ya que de él va a depender la calidad de la conexión para un dispositivo de comunicación. Este

equipo convierte la corriente de energía de corriente alterna, en un campo electromagnético. Al momento de diseñar una red inalámbrica debemos tener en cuenta que este componente debe ser bueno o superior.

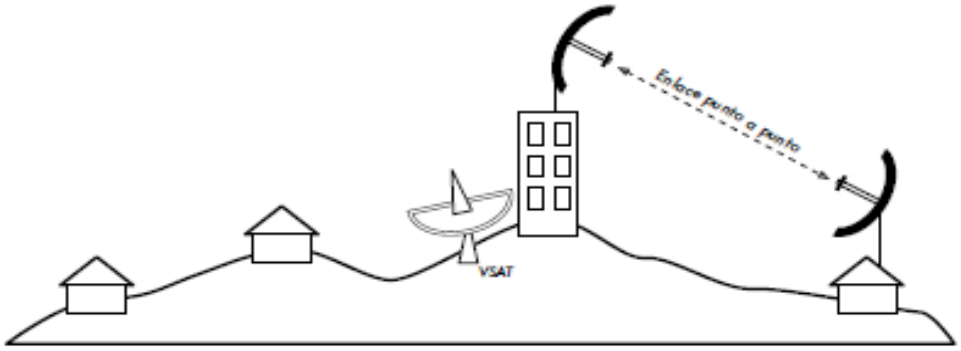
Tipos de conexiones.

El diseño de la red física va a depender netamente de la problemática que se nos presente. Debido al uso de las redes WLAN a nivel general y por la magnitud del espacio físico que actualmente mantiene la Facultad de Ciencias Administrativas de la Universidad de Guayaquil se realizó el análisis de los diferentes esquemas de conexiones de redes WLAN y se identificó la más viable. A continuación se detalla y se explica la forma en que trabajan lo diferentes esquemas.

Conexión punto a punto.

Este esquema es uno de los más comunes utilizados por las empresas que mantienen el edificio principal cerca de su sucursal, en lo cual su implementación se da para comunicar los edificios teniendo una línea visual disponible libre obstáculos físicos. Uno de los lados del enlace de punto a punto se encuentra conectado al internet para de esa forma poder dar salida a su otro extremo sin embargo no es un requisito para poder implementarlo debido a que el enlace se puede utilizar netamente para brindar algún servicio que tenga activo atrás del punto inicial. Con antenas apropiadas y existiendo línea visual, se pueden hacer enlaces punto a punto seguros de más de treinta kilómetros.

Imagen 1-12 Conexión Punto a Punto

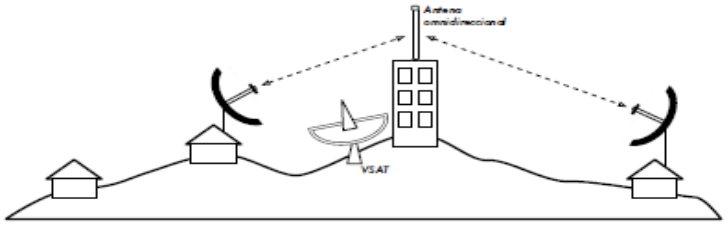


Fuente: Redes Inalámbricas en los Países en Desarrollo

Conexión punto a multipunto.

Este esquema es el comúnmente más utilizado, donde varios nodos se conectan con un punto de acceso principal que brinda la salida a internet, siendo este un AP (Access Point) o un router doméstico según sea la situación. El ejemplo que se identifica con este esquema es la de un punto de acceso inalámbrico que provee conexión a varias computadoras portátiles. Las computadoras portátiles no se comunican directamente las una con las otras

Imagen 1-13 Conexión Punto a Multipunto.



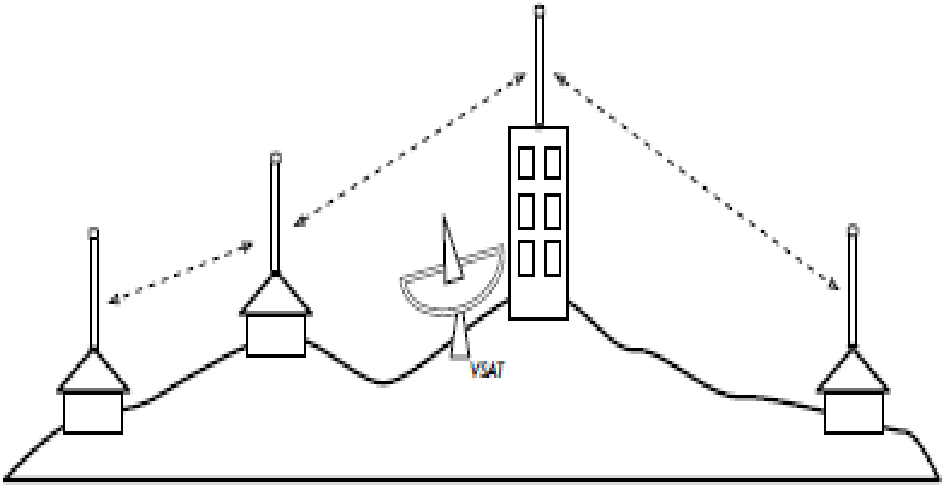
Fuente: Redes Inalámbricas en los Países en Desarrollo

Esta conexión también se la puede implementar de igual forma que la conexión punto a punto, pero con la diferencia de que los puntos externos se comuniquen al nodo principal teniendo en cuenta que podrían ser dos o más sin la necesidad de instalar varias conexiones punto a punto para poder realizar este tipo de comunicaciones. Existen muchas desventajas con esta conexión al momento de aplicarla en distancia muy extensas.

Conexión multipunto a multipunto.

El tercer tipo de esquema es el de Multipunto a Multipunto, el cual también se lo conoce como red Ad-hoc o en malla. En este tipo de esquema no existe una autoridad (Equipo) central que sea indispensable para los demás equipos conectados. Para este esquema se necesitan de equipos de radiofrecuencia que en su infraestructura puedan comunicarse entre ellos, para poder tener conexiones sin caída del servicio.

Imagen 1-14 Conexión Multipunto a Multipunto.



Fuente: Redes Inalámbricas en los Países en Desarrollo.

Este tipo de esquema tiene dos grandes desventajas, que son el aumento de la complejidad y la disminución del rendimiento. El tema de seguridad de esta red es muy importante, ya que todos los participantes pueden transportar potencialmente el tráfico. La solución de los problemas e inconvenientes que se dan en las redes Multipunto siempre tienden a ser muy complejas debido a la administración del gran número de variables, adicional que mantienen una sobrecarga adicional de administrar el enrutamiento de la red, y el uso más intensivo del espectro del radio.

El beneficio de este esquema es que sin importar que alguno de los nodos sea alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí. En la imagen 1.14 se visualiza un esquema Multipunto a Multipunto.

Para este proyecto con relación a lo que se analizó el esquema más idóneo sería el punto a multipunto, ya que lo que se necesita conseguir que los equipos finales se conecten a cualquiera de los dispositivos Wireless para de esa forma tener una salida al internet. Bajo este esquema se realizó el diseño para el uso del internet atreves de la red WLAN para la Facultad de Ciencias Administrativas de la Universidad de Guayaquil (FCA-UG).

Ventajas de redes inalámbricas.

Las ventajas de utilizar redes inalámbricas son las siguientes:

-Movilidad.

-Portabilidad.

-Flexibilidad.

-Escalabilidad.

Dentro de la movilidad nos encontramos, que a diferencia de los usuarios que se encuentran conectados a una red cableada, en la inalámbrica los usuarios pueden movilizarse dentro del área de conexión o de la cobertura que brinden la misma.

Portabilidad va de la mano con la movilidad, ya que el usuario puede movilizarse junto con sus dispositivos, sean estos notebook´s o netbook`s o similares, sin perder la conexión a la red a la cual nos encontramos conectados.

Poder colocar tu equipo de cómputo en el escritorio y luego por alguna emergencia trasladarte al escritorio de tu compañero sin realizar ningún cambio a nivel de configuración dentro del equipo o a nivel de red, pues a ese factor se lo conoce como flexibilidad.

Dentro de las redes WLAN añadir uno o más equipos a la misma no tiene ninguna dificultad a nivel técnico, ni cambios o adicionales luego de su instalación. Esta característica se llama escalabilidad y es una de la más importante a nivel de costos que le da mucha ventaja a una red cableadas ya que en esta última se deben realizar adiciones a nivel de infraestructura y son más costosas.

Desventajas de utilizar redes inalámbricas.

Las redes inalámbricas actualmente mantienen cinco desventajas muy bien reconocidas por los expertos en redes, las cuales se mencionan a continuación:

-Menor Velocidad.
-Mayor inversión inicial.
-Seguridad.
-Alcance.

-Interferencias.

La primera desventaja de este tipo de redes es algo muy técnico que se observa en la rapidez de una red WLAN vs LAN ya que las últimas mantiene velocidad de 100-Mbps a 10.000-Mbps dependiendo del tipo de cable que se utilicen para sus conexiones. A diferencia, las redes WLAN reducen sus velocidades de 11-Mbps a 108-Mbps, aunque existen soluciones y estándares propietarios que llegan a mejores velocidades aunque a un precio muy elevado.(Carballeiro, 2012)

La siguiente desventaja de las redes inalámbricas es un inversión inicial más alta que en la de redes cableadas, debido a que los equipos inalámbricos mantienen un costo de inversión más alto.

Debido a que las conexiones de una red inalámbrica se dan por medio de radio frecuencia, cualquier equipo que se encuentre dentro del alcance de nuestra red WLAN podría conectarse, burlando las medidas de seguridad que se ha implementado y esta desventaja se la conoce como seguridad, en la cual se debe trabajar mucho al momento de implementarla.

(Carballeiro, 2012).El alcance de una red inalámbrica está determinado por la potencia de los equipos y la ganancia que caracterice a las antenas. Así, si estos parámetros no son suficientes, encontraremos puntos en nuestra casa oficina donde no tendremos la cobertura adecuada.

La mayoría de las redes inalámbricas trabajan en la banda de 2,4-GHz ya que esta banda no demanda de una licencia administrativa para su uso por lo que muchos equipos inalámbricos utilizan esta misma frecuencia incluyendo todas las redes Wi-Fi. Debido a este suceso no hay una garantía que nuestro medio radioeléctrico esté totalmente libre para que nuestra red inalámbrica funcione a su mayor nivel de rendimiento, a mayor interferencia que produzcan las

redes inalámbricas de otros equipos mayor es la probabilidad de que reduzca el rendimiento de nuestra red, pero a pesar de esto no quiere decir que sea una real afectación, la mayoría de las redes inalámbricas trabajan afinadamente sin mayores complicaciones en este aspecto..(Carballeiro, 2012)

Seguridad de topología WLAN.

(Rojas & Rivera & Quispe, 2008)Las redes inalámbricas WLAN utilizan el aire como medio de datos de transmisión mediante la propagación de ondas de radio y esto genera nuevas amenazas de seguridad. Si estas ondas de radio se propagan fuera del edificio donde está ubicada su red, expone su información a posibles intrusos los cuales podrán manipularla.

De este hecho se derivan algunos riesgos como el que se pueda generar de forma constante una irrupción bien de un usuario que no esté autorizado, o por la ubicación de un punto de acceso ilegal que capte las estaciones cliente en vez del punto de acceso legítimo accediendo a la red inalámbrica, otro problemas que se puede generar malintencionadamente interferencias y una posible negación del servicio con solo introducir un dispositivo que genere ondas de radio a una frecuencia de 2.4-GHz que es la frecuencia mayormente utilizada por las redes inalámbricas.

La opción de comunicarse entre las estaciones cliente directamente sin transitar por el punto de acceso consentiría atacar directamente a una estación cliente creando problemas si esta estación da servicios TCP/IP, existe también la posibilidad de duplicar las direcciones IP o MAC de estaciones clientes legítimas los puntos de acceso estarían vulnerable a un ataque de fuerza bruta para indagar las contraseñas por lo que se debe tener cuidado en la configuración de estos para no facilitar la invasión por parte de intrusos.

A pesar de lo expuesto existen varios mecanismos de seguridad para reprimir que puedan introducirse en la red los cuales veremos para estar al tanto de sus beneficios.

Tipos de seguridades.

CNAC (Control de Acceso de Red Cerrada) Impide que los dispositivos que quieren unirse a la red lo hagan si no conoces previamente el SSID (Services Set Identidifier) y es una cadena de treinta y dos caracteres máximos que identifica a cada red inalámbrica.(Villegas, Paredes, & CH., 2008)

El SSID es el mecanismo para identificar redes inalámbricas que por sí solo no da una protección y en la mayoría de las ocasiones se emplea el de default un uso inteligente es eliminar el broadcast del SSID es decir la emisión de este por lo tanto queda oculto por lo tanto quien quiera conectarse deberá conocerlo brindando algo de seguridad entre los usuarios de la red pero no obstante hay programas que pueden detectar redes ocultas.

ACL (Lista de Control de Acceso) conocido como filtro de MAC es el método mediante el cual solo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas. El filtrado por direcciones permite hacer una lista de equipos que tienen acceso al AP o bien denegar ciertas direcciones la principal desventaja radica en que la dirección de la tarjeta por lo regular es intercambiable clonada lo que permite una obtención de una entrada valida en el AP. Las ACL también permitirán controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

WEP (Wire Equivalente Privacy) Privacidad equivalente a cableado es el sistema de cifrado incluido con el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite proporcionando un cifrado a nivel-2. Está basado en el algoritmo de cifrado RC4 y utiliza claves de 64-bits. Los mensajes de difusión de las redes inalámbricas de transmiten por ondas de radio lo que los hace más susceptible frente a las redes cableadas de ser captadas con relativa facilidad presentada en 1999 para proporcionar confidencialidad comparada a la de una red tradicional cableada.

Con el sistema WEP se puede utilizar dos métodos de autenticación que son el sistema abierto y el de clave compartida. En la autenticación del Sistema Abierto, el cliente WLAN no tiene que identificarse en el punto de acceso durante la autenticación, cualquier cliente independiente de su clave WEP podrá verificarse en el punto de acceso y conectarse. Después de la autenticación y la asociación WEP podrá ser usado para cifrar los paquetes de datos en este punto el cliente deberá tener las claves correctas.

En la autenticación mediante clave compartida WEP primero la estación cliente envía una petición de autenticación en el punto de acceso, el punto de acceso enviará de vuelta un texto modelo y el cliente deberá cifrar el texto modelo usando la clave WEP ya configurada y reenviando al punto de acceso en otra petición de autenticación. El punto de acceso descifra el texto codificado y lo compara con el texto modelo que envió dependerá de esta comparación para que el punto de acceso envíe una confirmación o denegación después de la autenticación y la asociación WEP podrá ser usado para cifrar los paquetes de datos.

WPA (Wi-Fi Protected Access) Acceso Protegido Wi-Fi es un sistema para proteger las redes inalámbricas Wi-Fi creado para corregir las deficiencias del sistema previo WEP tales como la

reutilización del vector IV vector de inicialización del cual se deriva ataques estadísticos que permite recuperar la clave WEP.

WPA fue creado por la Wi-Fi ALLIANCE, fue diseñado para utilizar un servidor de autentificación que distribuye claves diferentes a cada usuario sin embargo también se puede utilizar en un modo menos seguro de clave pre compartida para usuarios de casa o pequeña oficina la información es cifrada utilizando el algoritmo RC4 debido a que WPA no elimina el proceso de cifrado WEP sino que lo fortalece con una clave de 128-bits y un vector de inicialización de 48-bits.

Portal cautivo.

Un portal cautivo es una aplicación utilizada generalmente en redes inalámbricas abiertas para controlar el acceso a la misma, aunque también puede utilizarse en redes cableadas. Por un lado, se utiliza para presentar al usuario alguna información de interés (información corporativa, políticas de uso, etc.) y por otro le permite al usuario facilitar al sistema sus credenciales de acceso. Al utilizar un navegador web en lugar de un programa personalizado para la interacción entre el usuario y el sistema, se consigue una gran versatilidad en cuanto a equipos y sistemas operativos.

Cuando un usuario, una vez seleccionada la red Wi-Fi y establecida la conexión inalámbrica, intenta acceder a una página web utilizando cualquier navegador, el portal cautivo captura esta solicitud y en lugar de la página solicitada le presenta al usuario la página de registro al sistema,

bloqueando cualquier otro tipo de tráfico. Una vez que el usuario introduce sus datos y estos son comprobados se le permite el acceso a la red facilitándole la página web inicialmente solicitada.

Conceptos y funcionalidades de un portal cautivo.

(Aichele, y otros, 2007)Una herramienta común de autenticación utilizada en las redes inalámbricas es el portal cautivo. Este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

Para comenzar, el usuario enciende su computadora portátil busca y selecciona la red objetivo. Su computadora solicita una dirección mediante DHCP y le es otorgada. Luego usa su navegador web para ir a cualquier sitio en Internet.

El usuario solicita una página web y es redireccionado, en lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña, simplemente oprime el botón de “registro” (login) o ingresa cualquier otra credencial que solicite el administrador de red. El punto de acceso u otro servidor en la red verifica los datos.

Cualquier otro tipo de acceso a la navegación se bloquea hasta que se verifiquen las credenciales. Las credenciales se verifican antes de brindar acceso al resto de la red. El servidor de autenticación puede ser el punto de acceso mismo, otra computadora en la red local, o un servidor en cualquier lugar del Internet. Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red, y en general es redireccionado al sitio web que solicitó originalmente.

Un portal cautivo no provee encriptación para los usuarios de redes inalámbricas, en su lugar confían en las direcciones MAC e IP del cliente como identificadores únicas. Si bien esto no es necesariamente muy seguro, muchas implementaciones van a solicitar que el usuario se re-autentique periódicamente.

Esto puede hacerse automáticamente, minimizando una ventana emergente (pop-up) del navegador, cuando el usuario se registra por primera vez. En redes públicas o semipúblicas, las técnicas de encriptación como WEP y WPA son realmente inútiles.

Capítulo 2

Diseño metodológico

Tipo de investigación.

Según el proyecto propuesto y los objetivos planteados, el tipo de investigación que se realiza determina una investigación descriptiva ya que este proyecto se basa en el comportamiento que se da en la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG) sobre el uso de las redes inalámbricas.

Descriptiva.

Este proyecto propone una solución tecnológica frente a la necesidad del uso del internet a través de dispositivos móviles que muestra una tendencia creciente en los últimos tiempos y que con las respectivas medidas puede ser dirigida a campos con enfoques educativos, científicos, culturales para beneficio de la población de la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG).

Apoyados del actual red Ethernet de la (FCA-UG) y adicionando Hardware y software a esta estructura, se desea dar evolución dentro de nuestra área de estudio al uso y enfoque del internet que es considerada la red inalámbrica más amplia a nivel mundial.

La búsqueda de un aporte tecnológico donde se reflejen conocimientos adquiridos a lo largo de la carrera y de manera personal nos conduce al estudio de uno de varios problemas dentro de

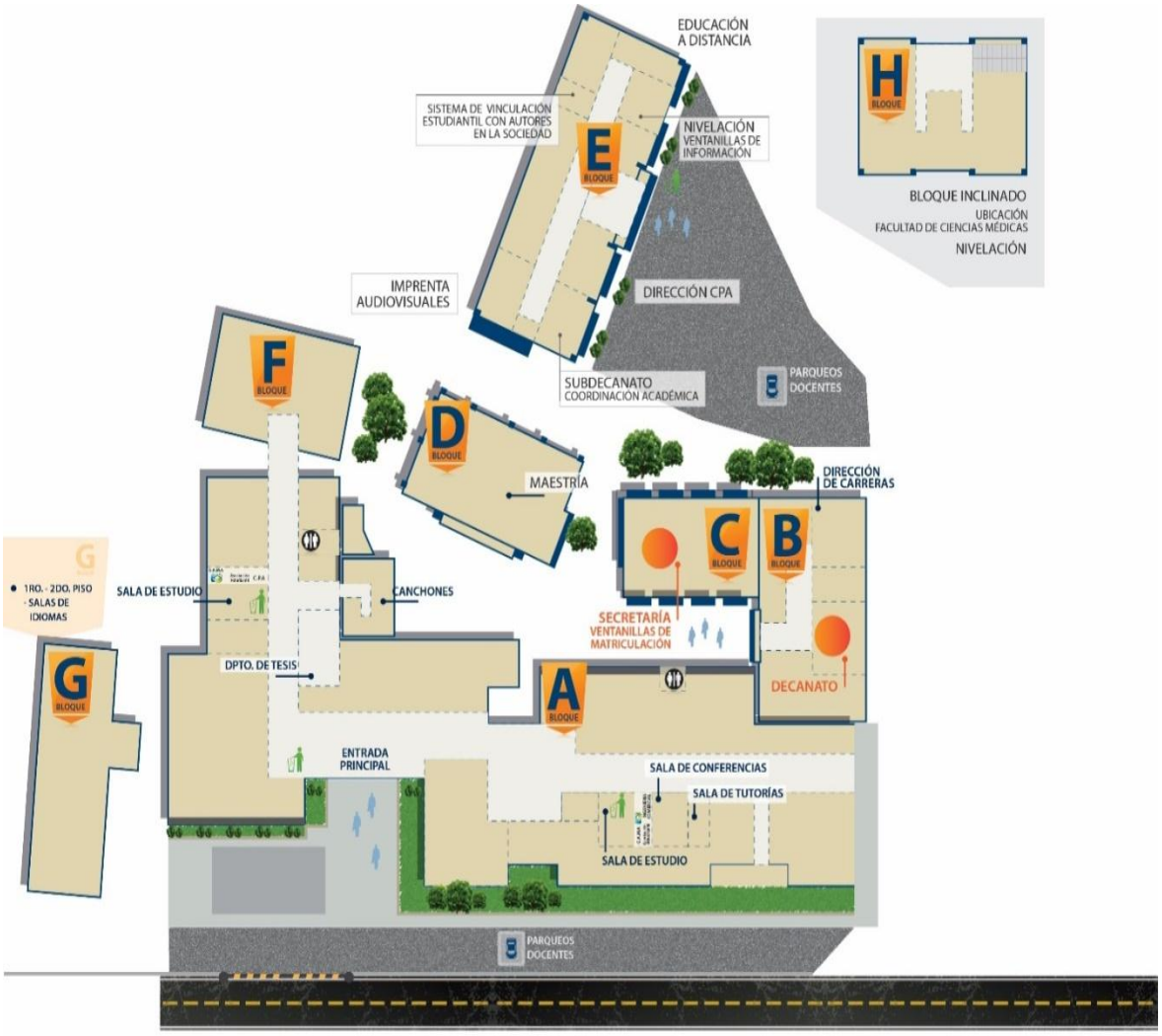
la (FCA-UG) que es, el no disponer de manera gratuita y libre la facilidad de constar con internet considerado como un recurso el cual puede ser usado para la adquisición de conocimientos de manera más dinámica y apegada a la realidad del mercado.

Diseño de investigación.

***Investigación de campo*.**

Para un mejor entendimiento y mayor apego de la realidad de los objetos de investigación se realizó visitas de campo en la (FCA-UG) con la finalidad de adquirir información que facilite el desarrollo de este proyecto uno los métodos para la recolección de información fueron encuestas y entrevistas realizadas tanto a estudiantes, docentes y administrativos con la finalidad de poder tener información relevante y de vital utilidad para la determinación de las normas y políticas que se detallan en el capítulo-4.Por medio de las visitas de campo también se hizo el levantamiento de información correspondiente a la infraestructura de la universidad y su organización a continuación en la imagen 2.1 se puede observar la estructura de la (FCA-UG) compuesta por los diversos departamentos y clasificada por bloques respectivamente, donde por cada bloque se colocará un access point o dispositivo repetidor de señal de la red de internet, para tener una cobertura total dentro de la (FCA-UG) y que así todos los usuario o personas correspondientes a este campus puedan tener el acceso a la red de internet de manera simple en sus dispositivos que tengan la habilidad para conexión a redes inalámbricas o con capacidad Wi-fi.

Imagen 2-1 Infraestructura de (FCA-UG)



Fuente: Facultad de Ciencias Administrativas de la Universidad de Guayaquil

Propósito de la Investigación.

El propósito de este proyecto es el aporte de una solución tecnológica para la (FCA-UG) que busca obtener un alto grado de satisfacción de los usuarios, a través del diseño de un portal cautivo para la (FCA-UG), que permitirá administrar y proporcionar seguridad al uso de internet por medio de hardware y software que se implementará a su red actual.

Área de estudio.

El área de estudio está constituida por la Facultad de Ciencias Administrativa de la Universidad de Guayaquil, debido a que es en donde se desea aplicar lo investigado y se realizarán pruebas de errores donde participaran los estudiantes, docentes y administrativos para la comprobación del mismo.

Población y muestra.

Población.

Se realizó una división en base a los tipos de usuarios que pueden tener la Facultad de Ciencias Administrativa de la universidad de Guayaquil, en tres grupos bien definidos que son: Administrativos, docentes y estudiantes.

Se realizó el cálculo de la muestra y distribución, está proporcionalmente por extractos

Tabla 1

Usuarios (FCA-UG)

Administrativo	255	1.94%
Docentes	550	4.18%
Estudiantes	12360	93.88%
Total	**13165**	**100%**

Fuente: Realizado por los integrantes del proyecto de tesis

Muestra.

Para el análisis de las necesidades del portal cautivo en la Facultad de Ciencias Administrativa de la Universidad de Guayaquil, se dirigieron encuestas a una muestra correspondiente a un0.03 % del personal que integran la Facultad de Ciencias Administrativa de la Universidad de Guayaquil.

Debido a que la población es definida y limitada, el error admisible puede variar entre uno y el diez por ciento, para el cálculo de la muestra, se escogió al cinco por ciento como error máximo admisible, para obtener un grado de confianza del noventa y cinco por ciento en los resultados de las encuestas.

Aplicando la siguiente fórmula:

$$n = \frac{m}{e^2 (m-1) + 1}$$

Donde:

n= tamaño de la muestra.

m=población total

e=máximo error admisible

Reemplazamos:

$$n = \frac{13165}{(0.05)^2 (13165-1) + 1} \qquad n = \frac{13165}{0.0025\ (13164) + 1}$$

$$n = \frac{13165}{33.91} \qquad n = 388$$

Distribución Muestral:

n= 388 x 1.94%= 8 administrativos

n= 388 x 4.18%= 16 docentes

n= 388 x 93.88%= 364 estudiantes

n= 8+16+364 n= 388

Fracción Muestral

$$f = \frac{n}{m}$$

Reemplazamos:

$$f = \frac{388}{13165} \qquad f = 0.03$$

Métodos e instrumento de recolección de datos.

Las técnicas de recolección de datos usados en este proyecto fueron:

Observación.

Por medio de la observación se pudo determinar una necesidad real en el estudiantado correspondiente a la Facultad de Ciencias Administrativas de la Universidad De Guayaquil, (FCA-UG).

"La observación se refiere a la capacidad, indicación que se hace sobre alguien o algo; anotación o comentario que se realiza sobre un texto"(Editors of Larousse, 2005).

(MEYER, 1981) "consideran que la observación juega un papel muy importante en toda la investigación; los hechos".

Encuesta.

Por medio de la encuesta se ha recolectado información necesaria que nos ayuda para determinación de condiciones, y estándares que se establecerán en el proyecto de implementación que promueve proporcionar un servicio gratuito a favor de los futuros usuarios dentro de la facultad de Ciencias Administrativas de la Universidad de Guayaquil."La encuesta es una técnica de investigación cuantitativa. En ella, el encuestador se pone en contacto con el encuestado con el fin de obtener información, ya sea escrita o verbal. Ese proceso de comunicación se realiza mediante un cuestionario"(Sanz, 2010)

Entrevista.

Por medio de la entrevista se obtuvo datos e información adicional para definir de manera puntualizada las normas que se incluirán dentro de la implementación.

"La entrevista consiste, en esencia, en una conversación entre entrevistador y entrevistado, que se dinamiza con una serie de preguntas o cuestiones".(Manuel, 2008)

Capítulo 3

Propuesta

Título de la propuesta.

"Diseño de portal cautivo para el uso del internet a través de la red WLAN para la Facultad de Ciencias Administrativas de la universidad de Guayaquil"

Objetivos de la propuesta.

Objetivo general.

Diseñar un portal cautivo con los servicios de autenticación y puerta de enlace, dentro de la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG) para que se pueda ofrecer el uso de la red WIFI a usuarios que pertenezcan específicamente dentro del recinto educativo. Con el nivel de seguridad y garantizando a los usuarios la integridad de su información al momento de que se utilice el recurso.

Objetivos específicos.

-Poder establecer el método de seguridad que se acople a nuestra necesidad y estructura**.**

-Definir los equipos inalámbricos que mejor se acople al rendimiento para ser utilizado en este proyecto.

-Configurar un router Mikrotik de autenticación que pueda validar todas las restricciones y validaciones.

-Realizar la instalación del portal cautivo en una zona donde sea factible realizar pruebas de comunicación y administración.

-Comparar ventajas de un portal cautivo usando Mikrotiks software propietario implementado en un servidor.

Justificación de la propuesta.

Justificación práctica.

Este proyecto es conveniente para el estudio, análisis y en un futuro su debida implementación para el buen manejo y viabilidad a través del conocimiento adquirido, que ayudará a administrar y salvaguardar el buen funcionamiento de las redes WLAN, para así demostrar que existen alternativas tecnológicas que nos permitirán aplicar una buena administración no solo en nuestras redes Ethernet sino en las móviles, ya que según estudios estas últimas son las más propensas a recibir ataques informáticos y las menos respaldadas con métodos de seguridad ya existentes.

Generalmente las instituciones u organizaciones aplican al menos una red WLAN dentro de su organización, lo cual en la práctica es de mucha utilidad otro método de seguridad y administración para poder solventar los inconvenientes que se dan dentro de ese tipo de redes es

la aplicación de un portal cautivo, el cual se orienta a garantizar que los usuarios que pertenezcan a la institución utilicen el recurso única y exclusivamente.

Se observa la parte de la instalación de un sistema, debido a que nos proporciona un ahorro a nivel de software significativamente, además que se está siguiendo las directrices de las instituciones públicas al elegir herramientas libres de licenciamiento. Adicional que la herramienta que se escogerá para el desarrollo de este proyecto posee las mismas capacidades y desempeño que cualquier otra herramienta bajo licencia.

En resumen tendrá un impactante alcance técnico, funcional y administrativo a nivel de IT de la institución, dándole más seguridad al administrador de red para el mejor desempeño de la WLAN que administra.

***Justificación* teórica.**

Respondiendo a las diversas necesidades de la administración de las redes Wi-Fi abiertas, se ha ideado diseñar un portal cautivo, con el fin de poder contribuir a la mejor administración de una de las redes más utilizadas en las facultades o en cualquier institución que es el Wi-Fi; esto sin afectar la calidad de la misma.

Además por medio de este proyecto, no solo estaremos aportando un método de administración de redes Wi-Fi, sino que se fomenta el mejor uso a este tipo de redes ya que los usuarios estarán limitados al uso del ancho de banda y de las páginas que la administración defina.

Justificación metodológica

Esta investigación tiene como propósito fundamental, describir las configuraciones para un buen diseño de portal cautivo. Por lo cual para el desarrollo de este proyecto también se utilizará la investigación exploratoria debido a que en la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG) no existen investigaciones previas sobre el objeto del estudio, por lo tanto se quiere indagar y explorar un territorio desconocido, con el fin de llegar al objetivo deseado.

Este estudio propone escudriñar, explorar o investigar en un tema o territorio total o parcialmente desconocido para el investigador, que nos ayudará a diseñar una nueva herramienta de administración/seguridad de WLAN para la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG).

En el proyecto que desarrollaremos se va a exponer y explicar un método para administración de la red WLAN que no se ha utilizado con anterioridad dentro de la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG), esto sin afectar la infraestructura ya instalada ni el medio y forma de comunicación que existen entre las diferentes áreas de la institución en las redes que forma parte de las mismas.

El motivo principal de trabajar en este método, es por la falta de importancia principalmente en el estudio y análisis de una de las redes que ha crecido potencialmente en la última década, y realizando las investigaciones correspondientes se pudo encontrar el método más idóneo para poderla aplicar en una institución educativa con las directrices que utilizan las instituciones gubernamentales.

Descripción de la propuesta

Este proyecto se centra en diseñar un modo seguro y confiable de gestionar la conexión de internet dentro de la Facultad de Ciencias Administrativas de la Universidad de Guayaquil (FCA-UG) con los métodos de comunicación que tenemos en la actualidad y utilizando la infraestructura tecnológica que nos brindan el mercado de IT. estudiando y analizando las distintas técnicas de seguridad para poder elegir la más apropiada cubriendo las necesidades que mantiene la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG) dentro de este ámbito tecnológico y de comunicación.

Esto incluye:

- Encontrar el equipo que va a realizar toda la gestión de comunicación y seguridad a nivel perimetral. Esto implica:

-Realizar la búsqueda dentro de las opciones de autenticación que pueda ser implementado dentro de un servidor dentro de nuestra LAN.

-Realizar pruebas de instalación dentro de un servidor local y analizar si el mismo cumple con lo necesitado.

-Realizar pruebas de comunicación, para validar si la salida con el internet se cumple, y de esta manera poder realizar las configuraciones de validaciones necesitadas.

-Buscar dentro del mercado IT los equipos de comunicación y de infraestructura que sean lo suficientemente consistentes para el procesamiento que van a realizar en caso de que alguien desee realizar la implementación.

-Realizar una prueba total si puede converger tanto el software seleccionado como los equipos tecnológicos que fueron escogidos y así ver el análisis más global o como un todo.

-Comparar tanto costos como beneficios con las alternativas de esto proyecto que son de propietario (Licencias) y dar las respectivas recomendaciones para una futura implementación.

Realmente todo lo que se cita anteriormente se encuentra resumido en palabras muy generales técnicamente ya que el proyecto se viene definiendo mucho por el contrato de ISP que la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG) posea, y sin contar que hay que analizar cuáles son las redes privadas que cuenta dicha institución para poder de esta forma dividir (subnetting) la misma y poder conocer si la máscara de subred no es factible para el número de usuario que vayamos a tener actualmente y de esta forma el servidor DHCP pueda asignar a cada uno una dirección lógica.

El servicio DHCP ya viene inmerso el ruteador que es instalado físicamente en la institución, este también cuenta con el servidor de porta cautivo y de los DNS, sin embargo este se propaga por un switch no administrable hacia los diferentes puntos de acceso que debería ser instalados en puntos estratégicos para asegurar la propagación respectiva de la red WI-FI,

Adicional se protegerá dicha red con credenciales únicas para cada usuario, y serán establecidas por normas para las mismas. Estas credenciales tendrán un tiempo límite para su uso, y será restringida para un solo dispositivo esto basándonos en precautelar la caída de la red por demasiados.

Impacto de la propuesta.

Impacto administrativo.

El proyecto tendrá un impacto fuerte en la administración de tipo de red que aún no ha sido ni siquiera implementada en la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG).

Tendrá un gran impacto a nivel administrativo, ya que se podrá controlar el uso del internet, verificar que sitios webs son los más consultados por los estudiantes y así tener una retroalimentación para un buen control. Se realizará exclusividad para docentes y demás personal de la administración de la institución para que puedan tener una apertura amplia a nivel de navegación y poder crear sus propios perfiles de usuarios.

El departamento de cómputo podrá tener un control definitivo, verificando las restricciones y los accesos de cada usuario, ya sea este con perfil de estudiante o docente.

Las partes que conforman está solución planteada se encuentra el servicio de ISP que mantiene contratada la Facultad de Ciencias administrativa de la universidad de Guayaquil (FCA-UG) ya que dependemos de la misma para poder ofrecer el servicio de internet hacia nuestros estudiantes y docentes, luego de aquello de instalar un routerBoard que hará de routeador y de control de acceso hacia el servicio de internet y a su vez la respectiva configuración de sus interfaces para poder administrar las redes. Luego de aquello debemos estudiar qué redes maneja la institución para luego poder subnetear y dar a nuestra red Wi-Fi un pool de direcciones lógicas.

Impacto académico.

A nivel académico el impacto será mucho más alto, ya que con esta alternativa los estudiantes pueden realizar sus trabajos de investigación sin la necesidad de pagar por un servicio de internet en algún centro de cómputo, y a su vez poder aprovechar a los docentes para realizar las consultas respectivas por las investigaciones ya realizadas en el momento. Desde este punto de vista el proyecto abarca además las investigaciones, la posibilidad de que a futuro la (FCA-UG) maneje diferentes servicios, los cuales pueden ser propagados por este tipo de red.

Además de brindar un apoyo a los estudiantes, también se lo brindan a los docentes en busca de las innovaciones a nivel académico que la web ofrece, esto sin necesidad de que los mismos abandonen el centro académico.

Impacto Institucional.

Es importante mencionar que a nivel institucional, la Facultad de Administración de la Universidad de Guayaquil (FCA-UG), ha mantenido un retraso tecnológico debido a muchos factores económicos.

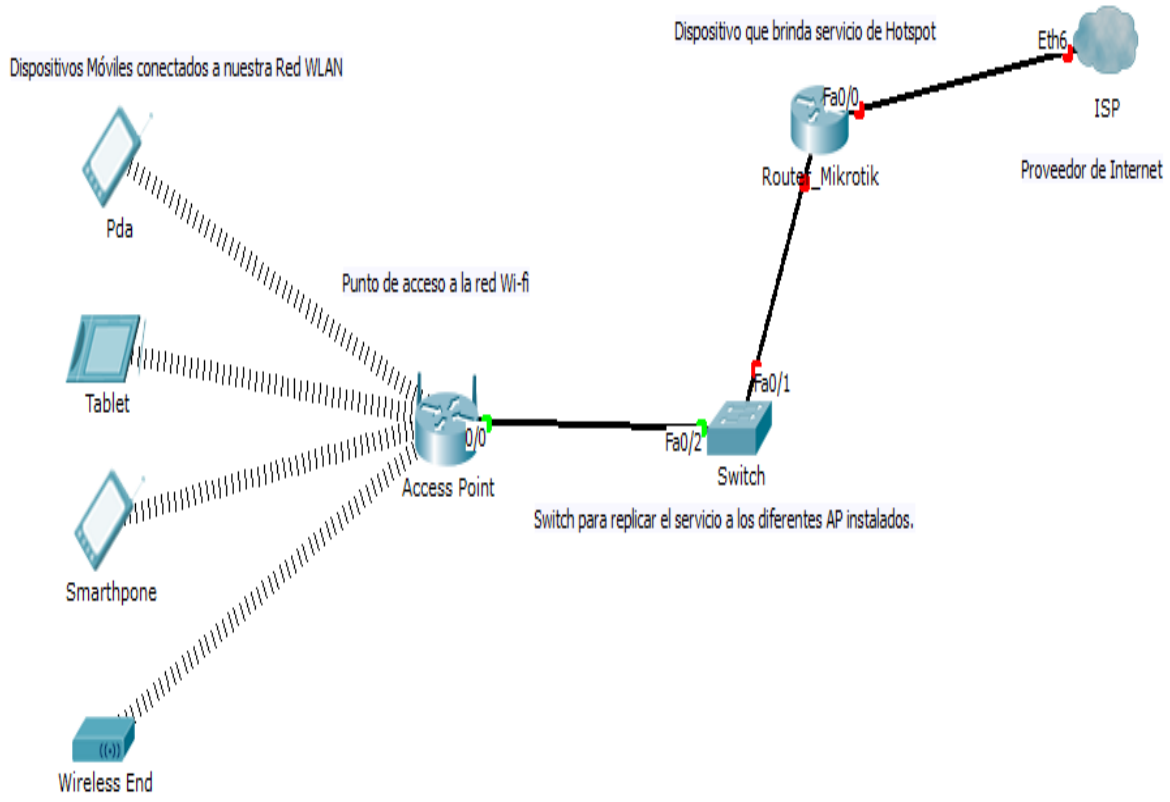
Este proyecto busca causar un gran impacto institucional, ya que se coloca a un nivel tecnológico de universidades de clase A, tratando de realizar un proyecto como el que se está desarrollando, por ende la misma será observada desde otro punto a nivel de implementación de proyectos.

Capítulo 4

Diseño de la solución

Para una mejor exposición del proyecto se muestra el diseño de la solución que este llevará, a continuación en la imagen 4.1 exponemos el esquema con la estructura que determinará este proyecto.

Imagen 4-1 Esquema de red WLAN de (FCA-UG)



Fuente: Realizado por los integrantes del proyecto de tesis.

A través del esquema gráfico podemos interpretar que cuando los usuarios (Docentes, administrativos, estudiantes) cuenten con dispositivos como: Tablets, Smartphone`s, Laptops, y otros que tengan hábil la opción de un mecanismo de conexión de dispositivos electrónicos de manera inalámbrica y deseen conectarse a un punto de acceso manteniendo el servicio, deberán pasar por un Login, es decir que para poder tener acceso a internet deberán identificarse a través una página HTML donde deberán ingresar los datos de sus credenciales ya asignadas.

Partimos de la red Ethernet de la Facultad de Ciencias Administrativas de la Universidad De Guayaquil, donde se implementará una red Wi-Fi que se controlará dentro de un hostspot a través de un dispositivo mikrotik, el dispositivo a usar será un Router Board 750 de cinco interfaces con software Mikrotik que tiene embebido un servicio de portal cautivo disponible para ser configurado en cualquier red que posea el mismo.

La red también constará con un Switch el cual estará enlazado con el Router mikrotik. Este Switch no administrable de veinticuatro puertos que servirá para la conexión de los diversos Access Point con la finalidad de mantener una cobertura global del área ya que deberán estar ubicados estratégicamente dentro de los distintos puntos de la Facultad de Ciencias Administrativas de la Universidad De Guayaquil (FCA-UG).

Normas y políticas.

Es necesaria la definición de normas y/o políticas debido a que el consumo del enlace con internet irá aumentando progresivamente con el pasar del tiempo.

Por esta razón la conexión a internet puede llegar a saturarse lo que complicaría la utilización de este recurso de manera eficaz y eficiente, sino se crean políticas el resultado en un corto

tiempo sería una respuesta lenta al momento de acceder a páginas web o descargar archivos, por ende la creación de normas y/o políticas serán imprescindibles en este proyecto.

Rango de direcciones IP.

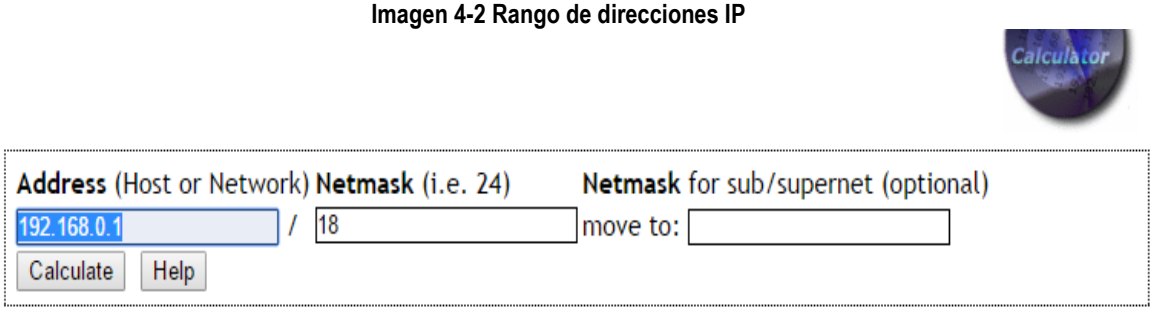
El cálculo del rango de las direcciones IP estará basado en la media de la población total de la Facultad de Ciencias Administrativas de la Universidad de Guayaquil (FCA-UG), que es de trece mil ciento sesenta y cinco personas por lo que hemos determinado que se usará una Netmaskslash (/18) la cual nos proveerá una cantidad de 16382-i direcciones IP`S diferentes en caso de ser requeridas por que se excluyen la dirección de red y de broadcast ya que se realizó subnetting. En nuestro caso trabajaremos con una red de clase C con dirección 192.168.0.1.

Se realiza esta división de la red que también es conocida como subneteo, analizando el universo de estudiantes y docentes que pertenecen y forman parte de la institución, ya que según la teoría de subneteo una red con máscara /19 nos brinda un pool de 8191-i direcciones, sin embargo no es suficiente para la cantidad de usuarios que maneja la institución ya que aproximadamente la misma conserva más de doce mil estudiantes en todas sus carreras y quinientos docentes, por esto es que ampliamos nuestra sección de host disponible quedándonos con una red /18.

Es posible que todos los usuarios no se encuentren conectados recurrentemente, pero en la práctica la porción de red es mayor o menor a la que se necesita y para no tener complicaciones hemos elegido mantener una mayor porción de host de los que se necesitaran en realidad.

En la teoría, a esta red se la debería subdividir para poder tener una mejor administración pero en el caso de este proyecto no aplica, ya que el servicio que se brinda es uno solo y la administración la realizó el dispositivo OnBoard.

Imagen 4-2 Rango de direcciones IP



Fuente: jodies.de/ipcalc

Según las imagen4.2 nos muestra que la dirección de nuestra red será la 192.168.0.1, esta dirección no es utilizable para algún host o equipo ya que será configurada en nuestra interfaz, adicional también nos indica la dirección de broadcast, que tampoco puede ser utilizable para algún host. Podemos observar que la dirección más baja será la 192.168.0.1 y la más alta será la 192.168.63.254.

Control de accesos.

El control de los accesos estará determinado por credenciales y direcciones físicas (MAC ADRESS) ya que cada usuario solo tendrá una sesión disponible es decir que para cada sesión de usuario solo podrá conectarse un dispositivo con su respectiva NIC. Las IP`S se asignarán de forma automática, ya que vamos a tener un servicio DHCP activado para las credenciales. No se mantiene ninguna reservación DHCP ya que sería mucha carga administrativa y de recursos hacia nuestro administrador de redes.

El hotspot manejará a través de sus credenciales el control de acceso por completo a la red, ya que sin duda cualquier podría engancharse a ella pero no podrá hacer uso de la misma por completo.

La porción de red que tendrán nuestros usuarios será toda la configurada e la interfaz asignada para nuestro hotspot, es decir que las direcciones serán asignadas dentro de las 16.382-i direcciones lógicas posibles a cualquier dispositivo, ya que para nosotros es transparente que dirección le asigne nuestro DHCP, debido que habrá control de transmisión de bajada y subida por medio de usuarios creados para cada credencial asignada.

Credenciales.

La concesión de credenciales será centralizada a través de un responsable o administrador de red el cual definirá un user y password por cada usuario existente; conformado de la siguiente manera:

User.

Para el usuario se va a utilizar el número de cédula del usuario, ya que por ser un piloto vamos a trabajar de esta forma.

Password.

Número de cédula. Ejemplo: 0930756887

Tenemos como ejemplo user: 0930756887password: 0930756887

La finalidad de esta metodología de concesión de credenciales es que no sea repetible en ningún caso, es decir, que sea única por usuario.

Sesiones.

Con el objetivo de minimizar los colapsos de la red se definirá una única sesión recurrente por usuario.

Tiempo límite por sesión.

Estudiantes.- 60 minutos por sesión (1 hora)

Docentes y administrativos.- 240 minutos por sesión (4 horas)

Ancho de Banda.

Estudiantes.- 512KB de Bajada y 256 de subida

Docentes y administrativos.- 1024 KB de bajada y 512 de subida

Ahora se explicará por qué la definición de nuestras sesiones, si es verdad un usuario puede estar conectado a nuestro hotspot todo el día, también debemos conocer que el mismo en su

momento se encontrará ocupado por sus responsabilidad académicas y esto hará que se encuentre conectado sin ninguna necesidad, así que se ha programado que cada sesión que no envié ninguna petición relevante se desconectara de la red, liberando recursos y una dirección lógica, sin embargo el trato con los docentes difiere en parte ya que ellos necesitan más de este recursos por aquello permitimos a este perfil de usuario que mantenga una sesión durante cuatro horas.

De igual forma el manejo de ancho de banda se lo realiza por medio de perfil de usuarios, cada perfil tiene un ancho de banda asignado, en nuestro caso el de los estudiantes hemos asignado un ancho de banda muy inferior a la del perfil de docente por su comportamiento y adicional por la cantidad de usuarios que existirían en dicho perfil ya que es significativo.

Para todos los usuarios sin importar al perfil que pertenezcan, solo podrán mantener una sesión recurrente por usuario, esto para poder salvaguardar la integridad de la red y prever de que cualquier agente que no pertenezca a la institución se pueda conectar y adicional que los usuarios finales se pueden conectar con más de un dispositivo a la red, ya que esto haría que la cantidad de usuario se multipliquen significativamente.

Failover.

Tomando en cuenta que en este proyecto se utilizará la actual Ethernet de la Facultad de Ciencias Administrativas de la Universidad De Guayaquil (FCA-UG).

No contaremos con FAILOVER debido a que el enfoque de este proyecto se basa en adherir un servicio para la población de esta área y no en cambios de estructura de esta red.

Si más adelante se piensa plantear esta estructura en la (FCA-UG) pero sin depender de la infraestructura ya montada, se podría pensar en un failover ya que el dispositivo que realiza todo el trabajo puede manejar alta disponibilidad, y pudiendo colocar un enlace de internet de respaldo podríamos tener el failover disponible, es decir dos Router`sOnBoard funcionando en un interfaz de sincronización y a su vez contratar dos proveedores de internet los cuales deben aplicar entre ellos un protocolo para poder levantar la alta disponibilidad de enlaces.

Conclusiones.

-Demostrar cómo es posible implementar un portal cautivo dentro de una institución educativa de tercer nivel, y cuáles serán sus grandes ventajas en ella.

- Demostrar que se puede realizar una implementación viable de tecnología de desarrollo abierto, sin complicaciones a nivel de configuración.

- Resaltar el grado de complicación, dedicación y compromiso que conlleva para el administrador de red una implementación física del mismo.

-Constatar la importante contradicción entre lo existente a nivel de infraestructura con lo que en su momento se desearía realizar físicamente.

- Aprovechar que en la actualidad las universidades públicas cuentan con un mayor apoyo por la parte del gobierno, lo cual nos ha motivado a realizar este tipo de investigación para que en algún momento con inversión pública se pueda ejecutar.

- Mostrar que la puesta en marcha de este tipo de iniciativas demandan un contexto institucional, profesional y organizativo adecuado. Debe existir una coherencia entre lo que se exige al administrador de red con lo que se vive en la realidad de la Facultad de Ciencias Administrativa de la Universidad de Guayaquil.

-Considerar también consistentemente que los usuarios de internet se oponen a ser regulados en su navegación diaria, y por consiguiente que sean restringido su acceso.

Recomendaciones.

Por parte de los desarrolladores de este proyecto, nuestras recomendaciones son las siguientes:

- Realizar una división de redes antes de realizar la implementación del portal cautivo en una WLAN, esto para poder organizar en una sola red la que vaya a ser asignada la WLAN.

.- Realizar una buena inspección del área física donde se va realizar la instalación de los equipos Wireless, esto para poder evitar que dentro de la misma existan medios físicos que no permitan propagar las ondas electromagnéticas.

- Realizar las verificaciones pertinentes con los perfiles de usuarios, sus accesos y demás. Esto evitará que exista algún hueco de seguridad.

- Evitar colocar claves de acceso a los usuarios comunes, preferible que sea el mismo usuario que la coloque o la digite.

-Evitar al momento de realizar la instalación de servidor con el servicio de portal cautivo, no complicarse con software libre de difícil uso, ya que lo que se necesita es que este mismo sea amigable para la administración y configuración.

- Evitar enfocarse en la marca de los equipos de infraestructura, sino en sus características y rendimiento basados en la demanda de recursos y de la red WLAN.

Referencias

Carballeiro, G.J. (2012). *Redes Wi-Fi en entornos Windows.* Málaga, España: Fox Andina.

Tanenbaum, G.J. (2003). *Redes de computadoras.* México, México: Pearson Educación.

Aichele, Corinna Elektra; Flickenger, Rob; Fonda, Carlo; Forster, Jim; Howard, Ian; Krag, Tomas; Zennaro, Marco. (2007). *Redes Inalámbricas en los países en Desarrollo.* Londres, Inglaterra: Limehouse Book Sprint Team

Editors of Larousse. (2005). *El Pequeño Larousse Ilustrado*. México, México

Acuña B. P. (1981). *La Observación como Herramienta Científica*. Madrid, España: Acci.

Sanz M. M (2010). *Introducción a la investigación de Mercados.* Madrid, España: Esic Editorial

Saavedra M. J. (2008). *Elaboración de Tesis Profesionales.* México, México: Pax México

On-line

Ouellet, Eric; Padjen, Robert; Pfund, Arthur; Fuller, Ron; Blankenship, Tin.(2002)*Cisco Redes Wireless* Recuperado de. https://books.google.com.ec/books?id=LN1xako6zIwC&printsec=frontcover&hl=es#v=onepage&q&f=false

ANEXO Nº1

Instalación del Router Onboard.

En este apartado se describe como se debe realizar la configuración de nuestro router mikrotik desde el principio, y partiendo de ahí realizar la respectiva configuración de nuestro portal cautivo.

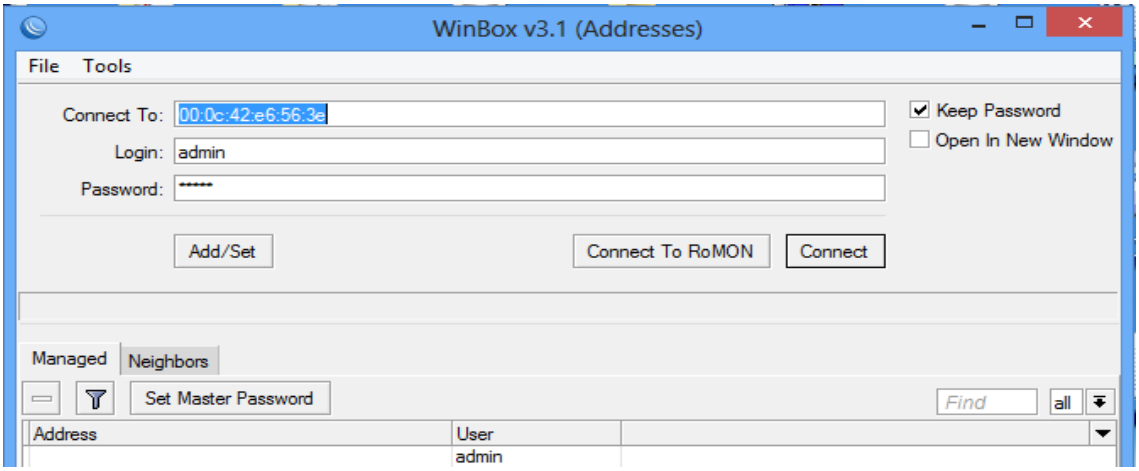
El dispositivo que vamos a utilizar es un router mikrotik 750, el cual posee cinco interfaces y además un gran número de servicios de networking.

Imagen 4-1 Router Mikrotik-750

Conexión Dispositivo.

El primer paso que se realiza es entrar a nuestro dispositivo, esto se lo logra conectándonos por cable de red a una de las interfaces del mismo, y por medio de la herramienta del fabricante

“WinBox” conectarnos apuntando a la dirección física del equipo como se puede ver a continuación:

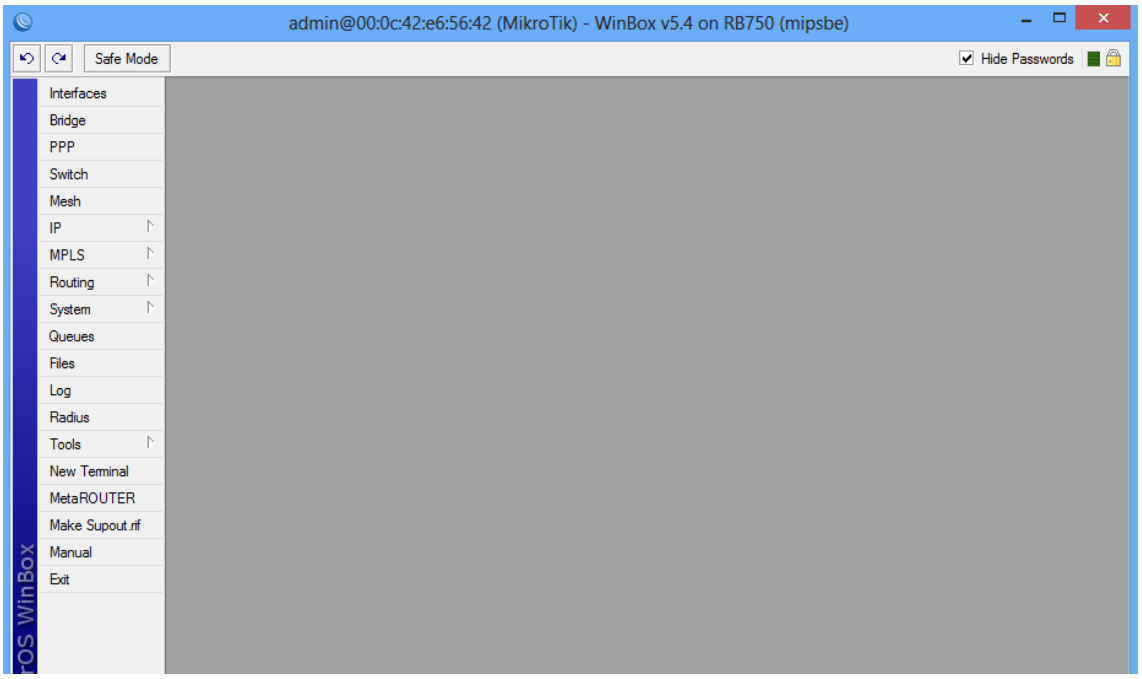


El login por defecto las credenciales son las siguientes:

Login: admin

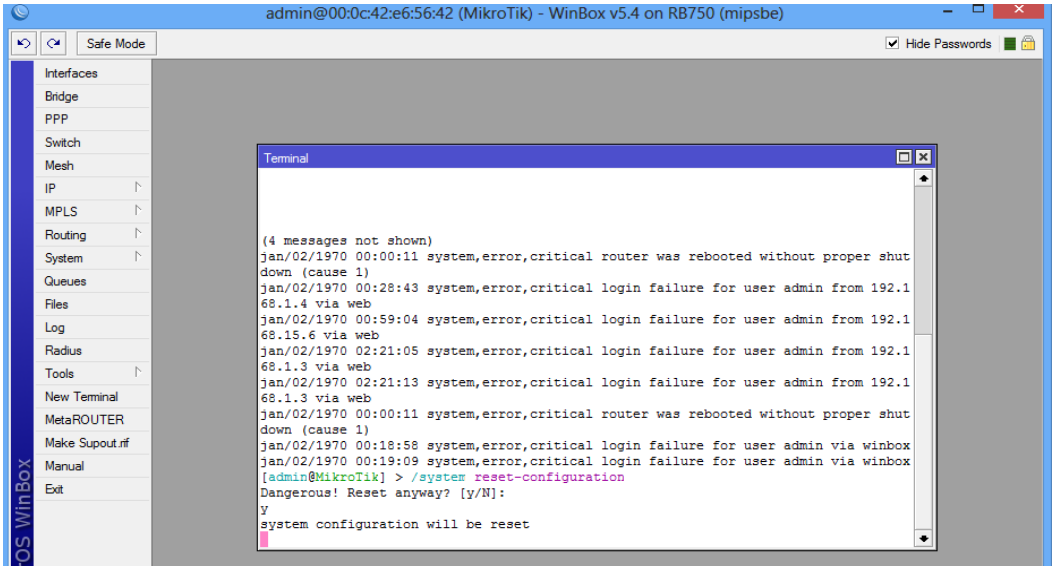
Password: (en blanco)

Una vez conectados les aparecerá la siguiente imagen:



Como vamos a configurar el dispositivo desde cero, y para asegurarnos que no hay ninguna configuración en el dispositivo, lo mandamos a reiniciar de fábrica, de tal forma el dispositivo quedará sin ninguna configuración que pueda tener, esto se lo hace por rutina.

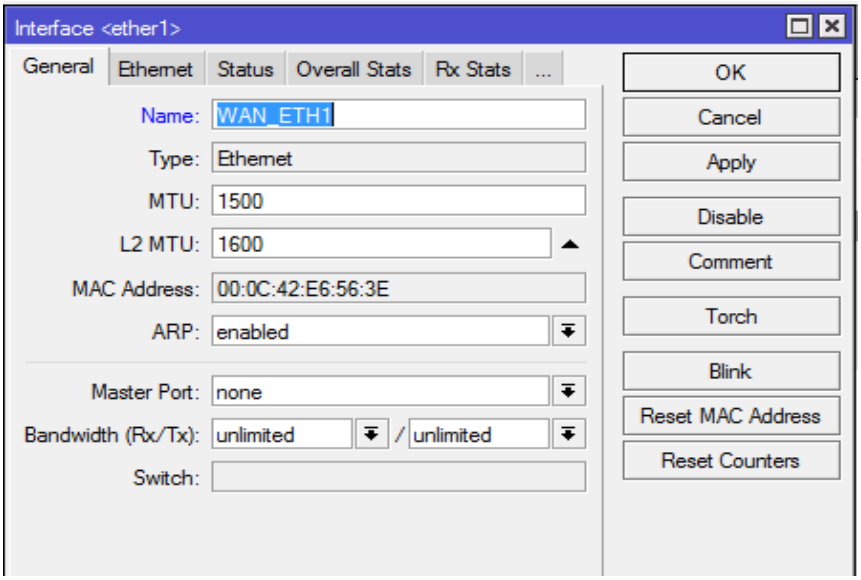
Esto se lo realiza con el comando **system reset-configuration**.



Configuración de interfaces.

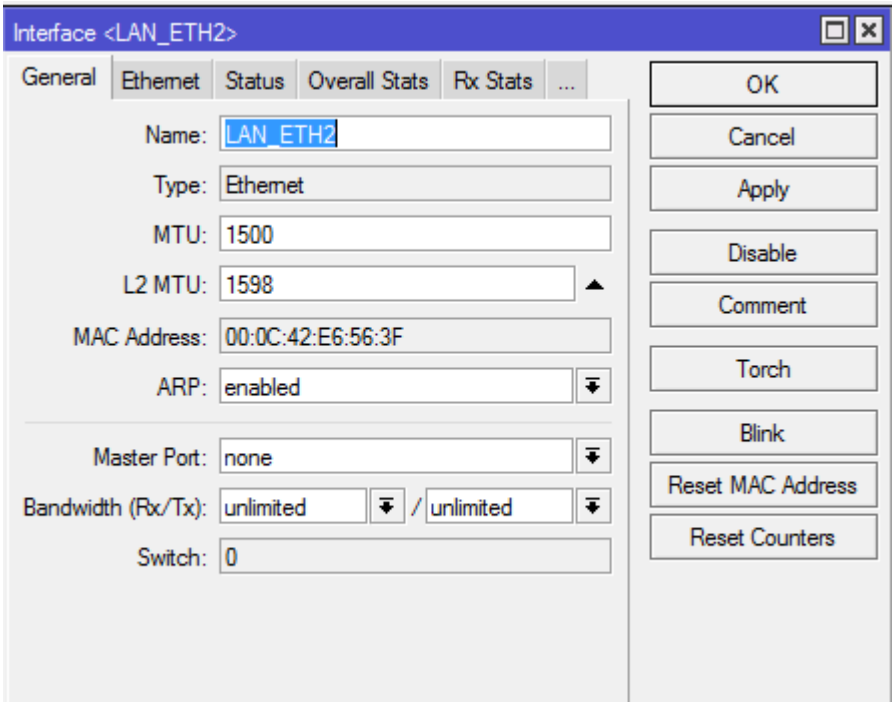
Vamos a realizar la configuración de las interfaces del dispositivo, por lo general se realiza un configuración de un Ethernet WAN(Salida a Internet), una red LAN y una red Wireless.

La primera interfaz configurada será la interfaz eth1, que ahora la llamaremos WAN_ETH1.

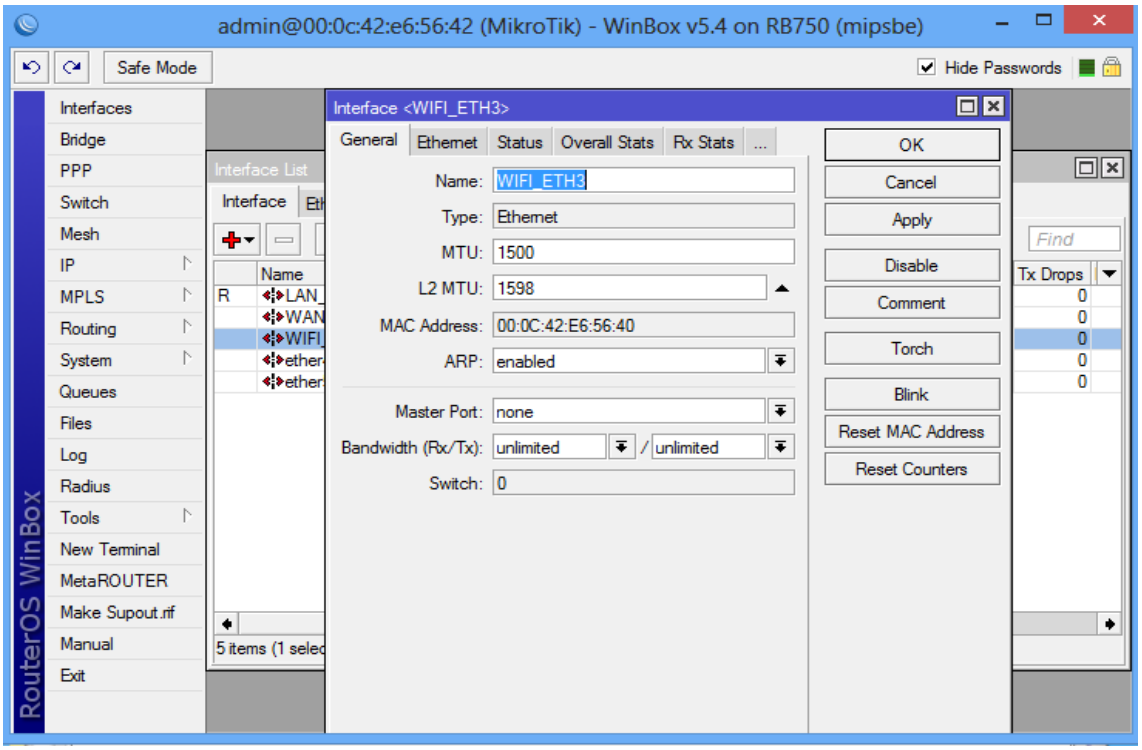


Luego de renombrar la interfaz, damos click en APPLY y finalmente OK.

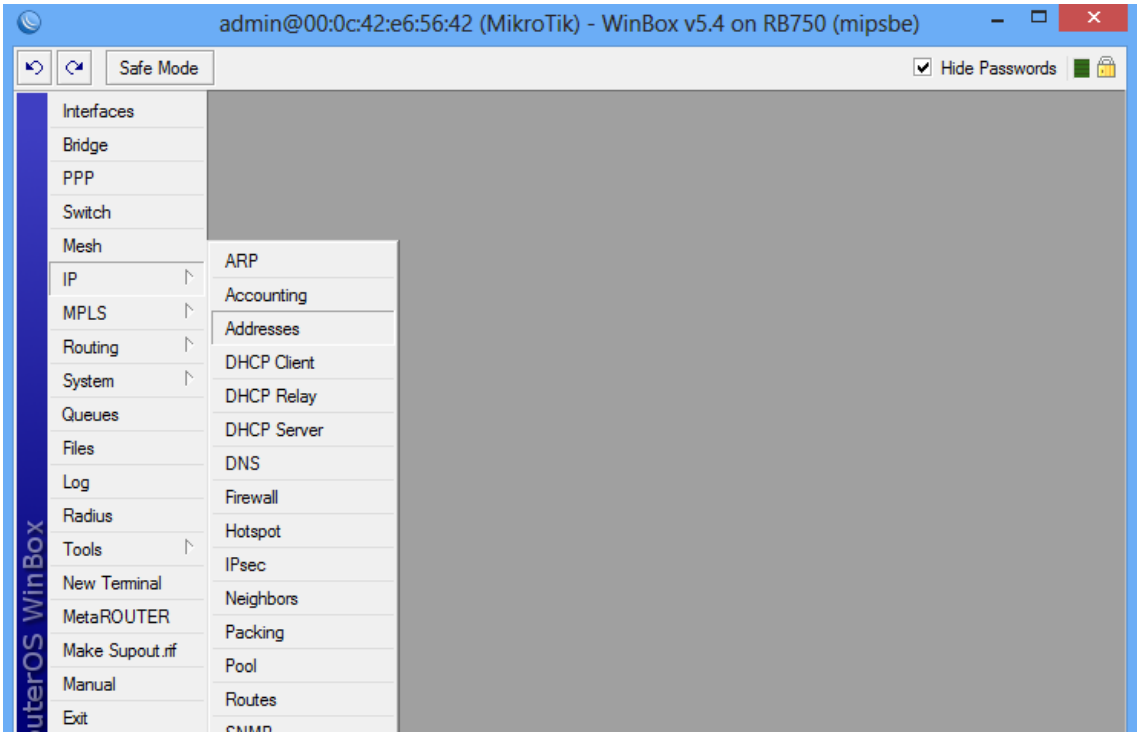
Lo mismo que se realizó en la eth1, lo realizamos en la eth2, la cual la vamos a conocer como LAN_ETH2.



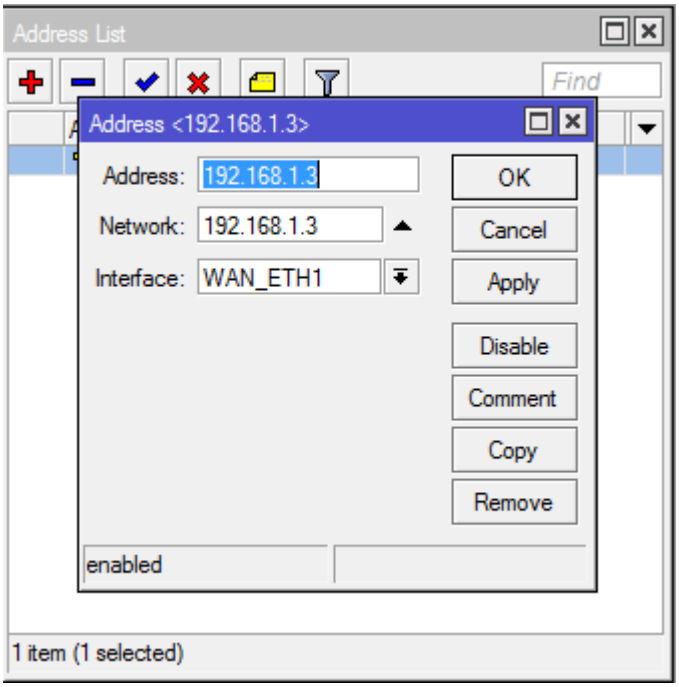
Y finalmente realizamos el cambio en la eth3, que ahora la conoceremos como WIFI_ETH3.



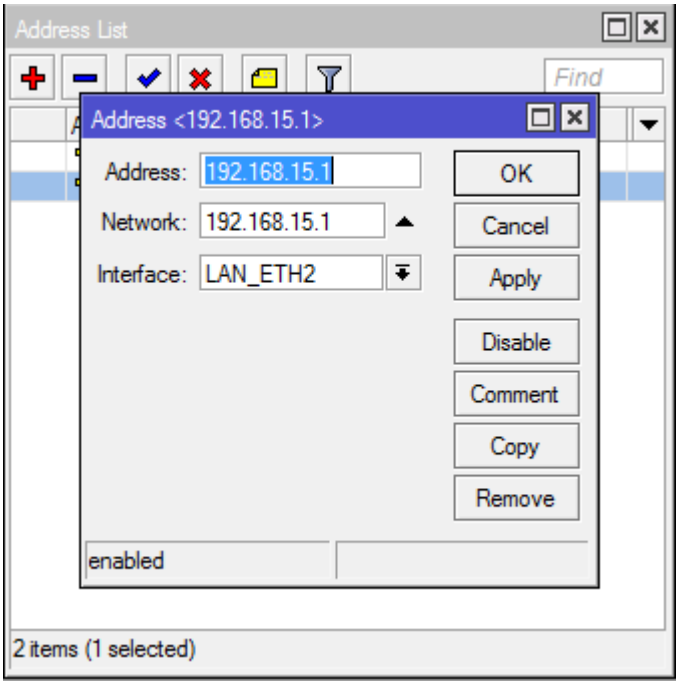
Ahora configuraremos las direcciones de nuestras interfaces, esto se lo realiza en la sección IP, Addresses.



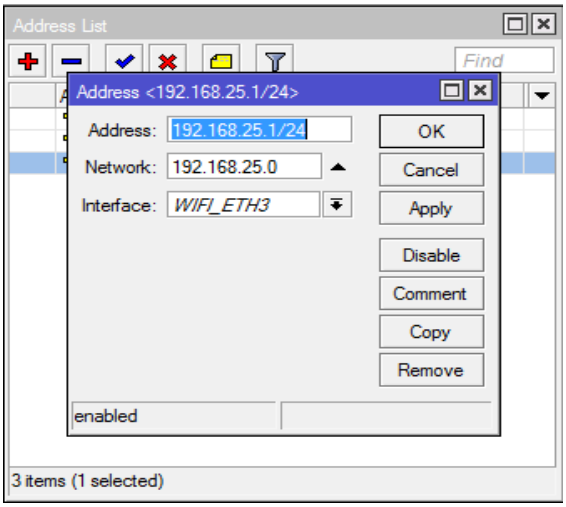
La primera dirección configurada será para nuestra interfaz WAN_ETH2, la cual vamos asignar la dirección 192.168.1.3/24.



La segunda dirección configurada será la 192.168.15.1, esto para realizar un subneteo de la red que nos proporciona nuestro ISP.

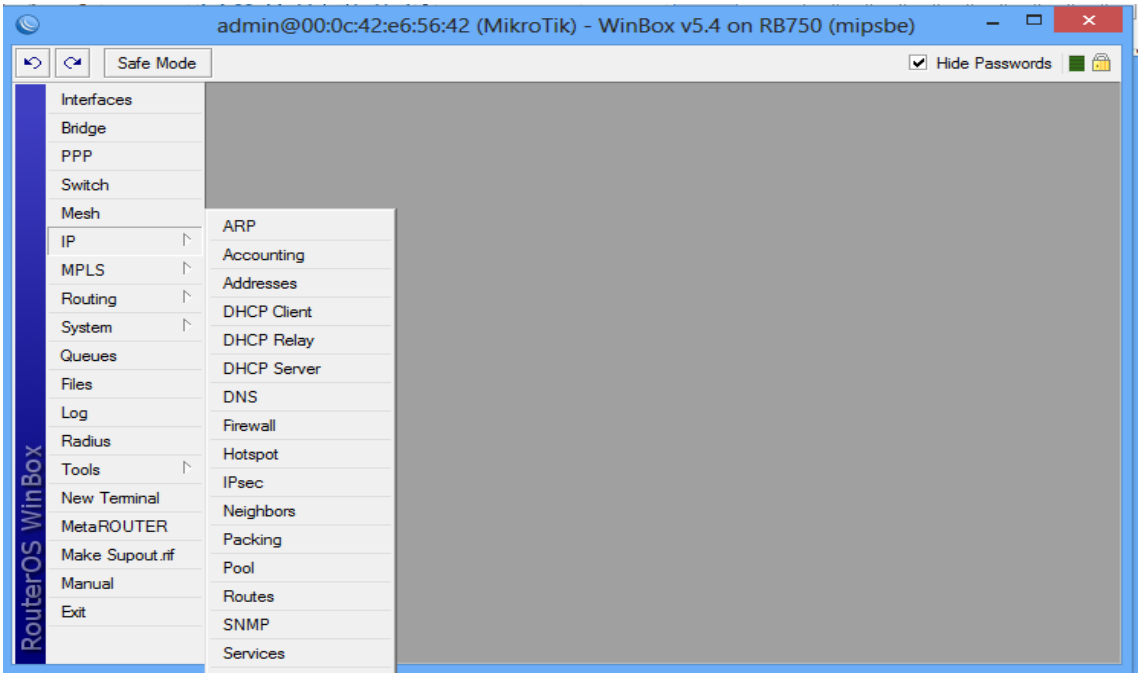


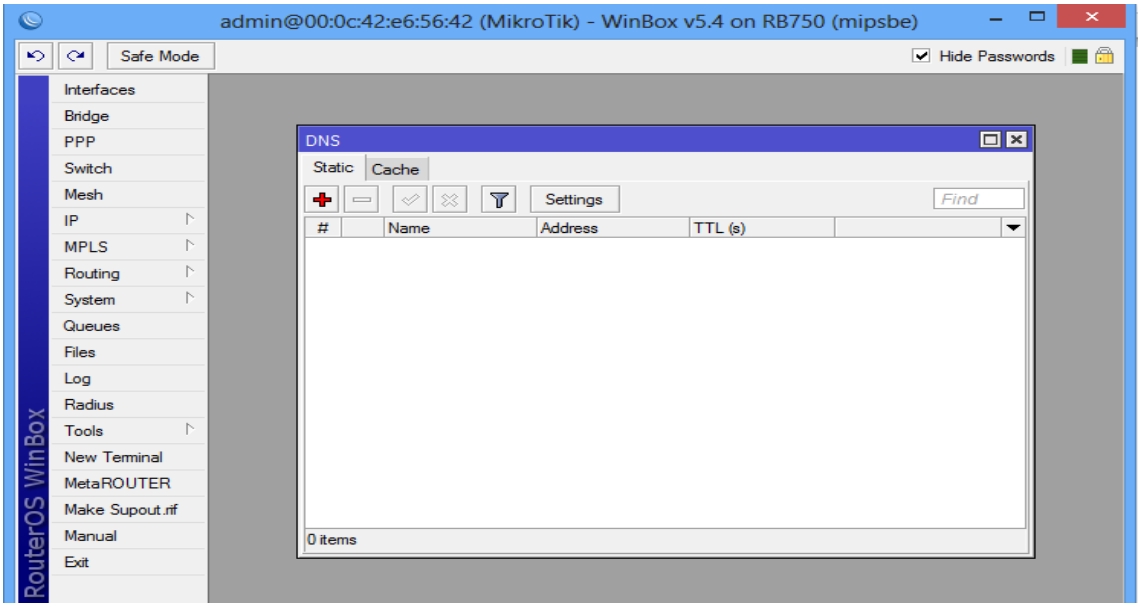
La tercera dirección será para nuestra red WIFI_ETH3 que será la 192.168.25.1.



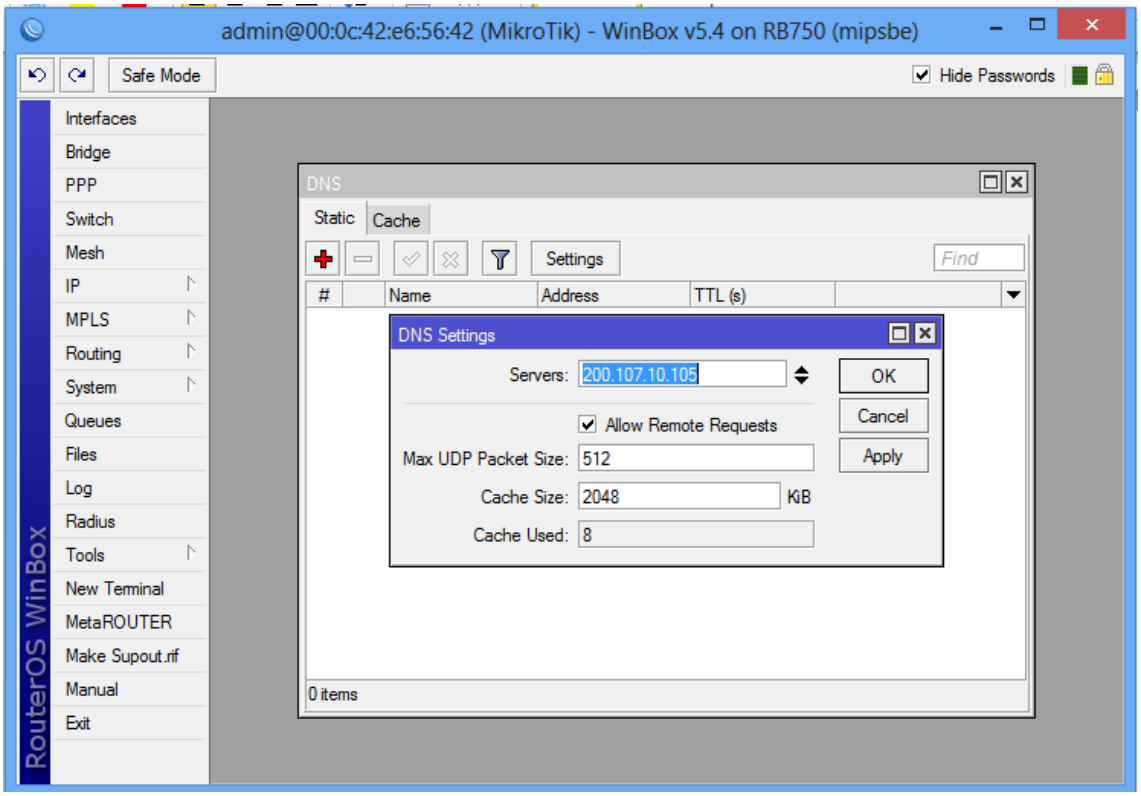
Configuración DNS.

Luego de haber realizado la configuración de nuestras redes e interfaces, vamos a configurar nuestro servidor DNS que necesita el Router Mikrotik para que cualquier equipo conectado a él, o el mismo pueda navegar. Nos dirigimos a IP / DNS.



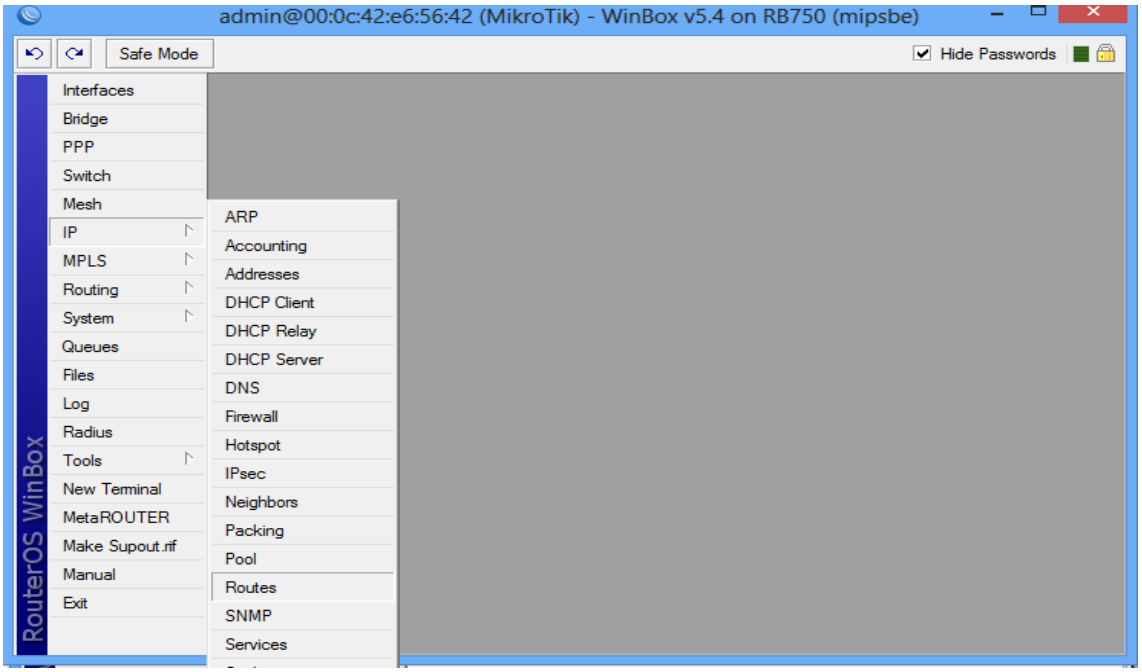


Nos dirigimos a Settings, y agregamos nuestro servidor DNS que poseamos, en este caso va hacer el del proveedor de internet que mantengo por el momento.

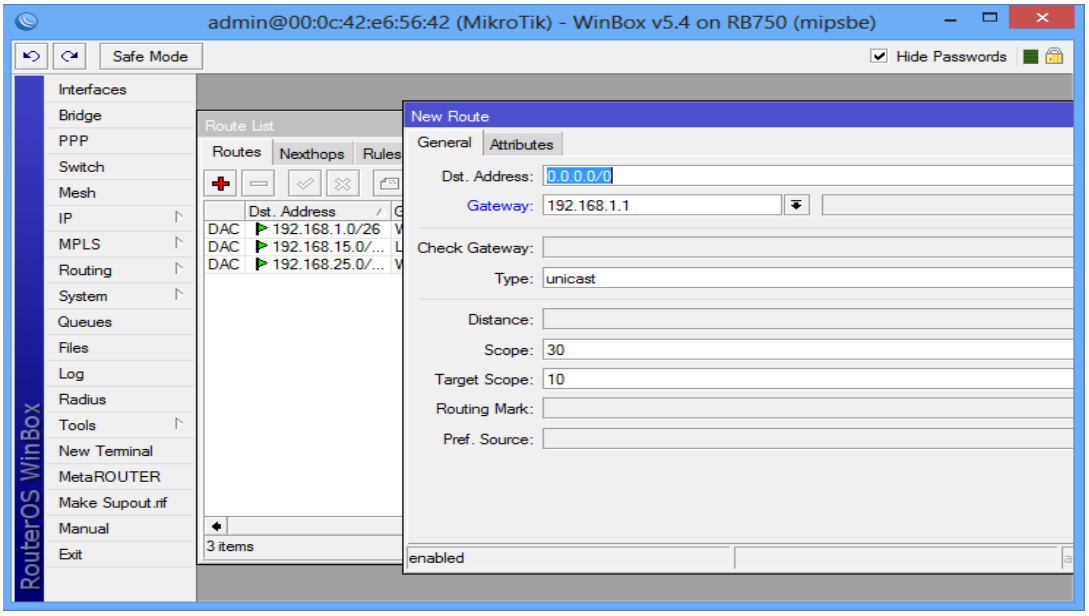


Configuración de Puerta de enlace.

Para que cualquier petición de navegación pueda realizarse con satisfacción, se debe configurar la puerta de enlace que es la que nos da acceso a salir de nuestra red LAN.

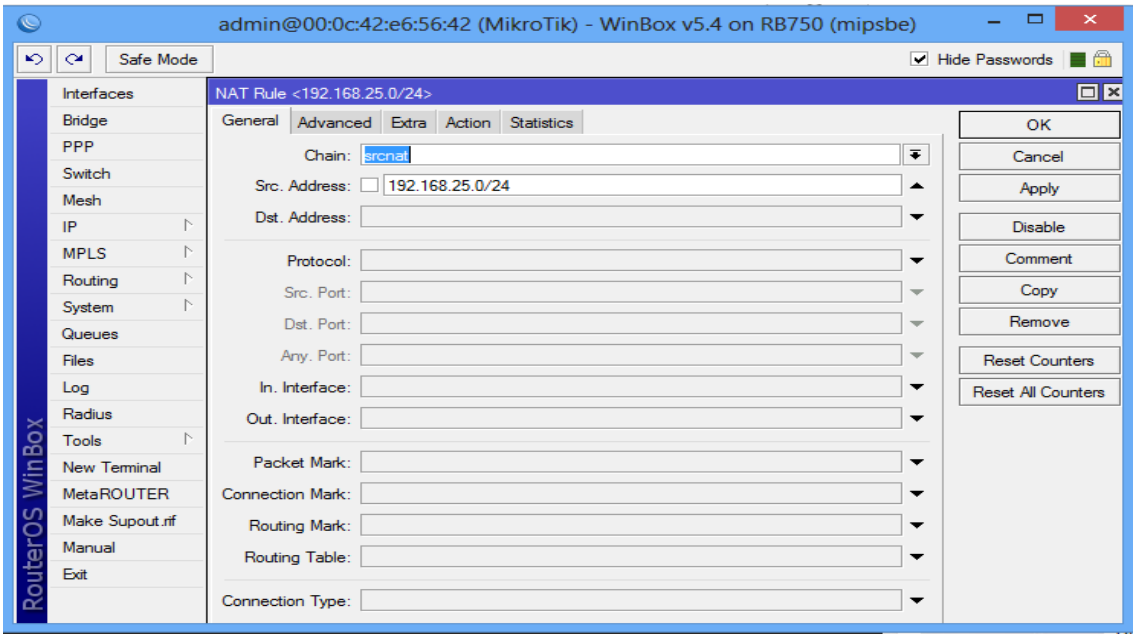


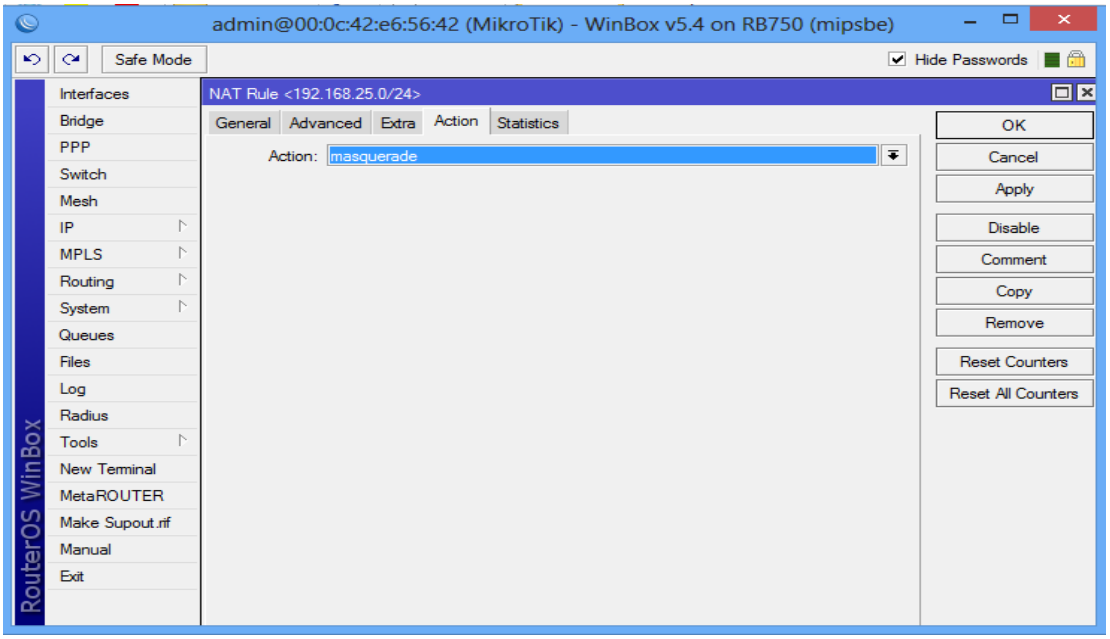
Nuestra puerta de enlace va a ser la 192.168.1.1, ya que es la que nos va a dar la salida a internet.



Reglas para enmascaramiento.

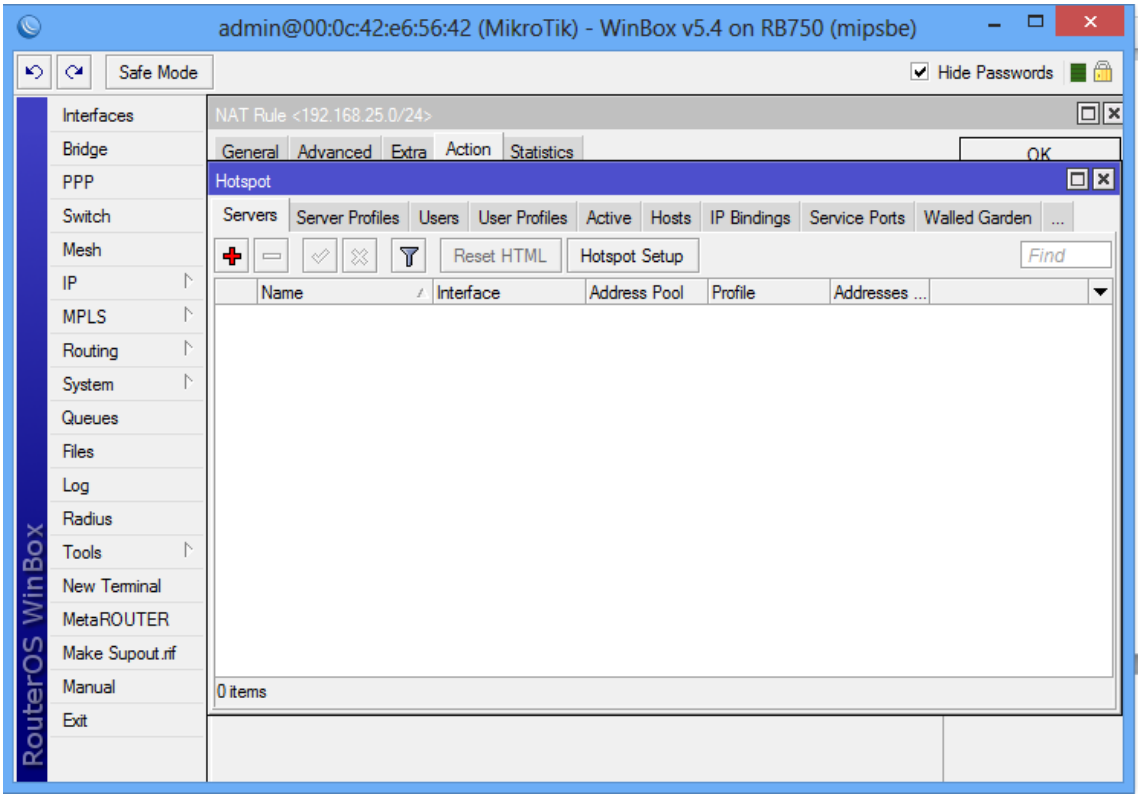
Para que cualquier petición que realice un dispositivo que esté conectado a las interfaces LAN_ETH2 o WIFI_ETH3 se debe establecer reglas NAT que permitan enmascarar las peticiones. Esto se lo realiza en IP/Firewall/NAT se crea la regla.



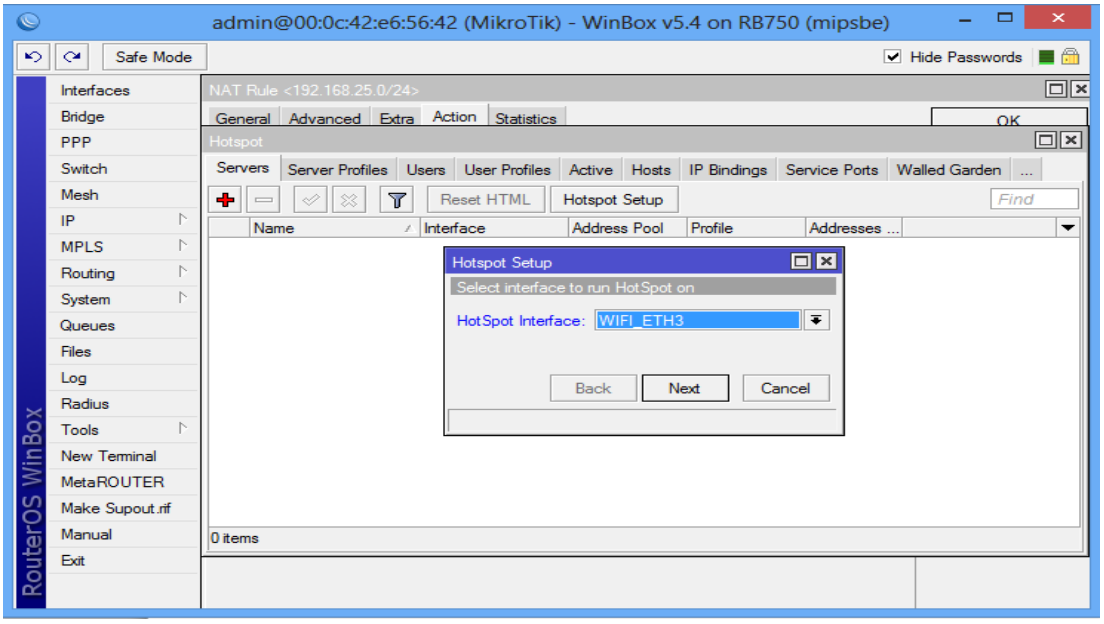

admin@00:0c:42:e6:56:42 (MikroTik) - WinBox v5.4 on RB750 (mipsbe)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit
NAT Rule <192.168.25.0/24>
General
Advanced
Extra
Action
Statistics
Action:
masquerade
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Configuración de hotspot.

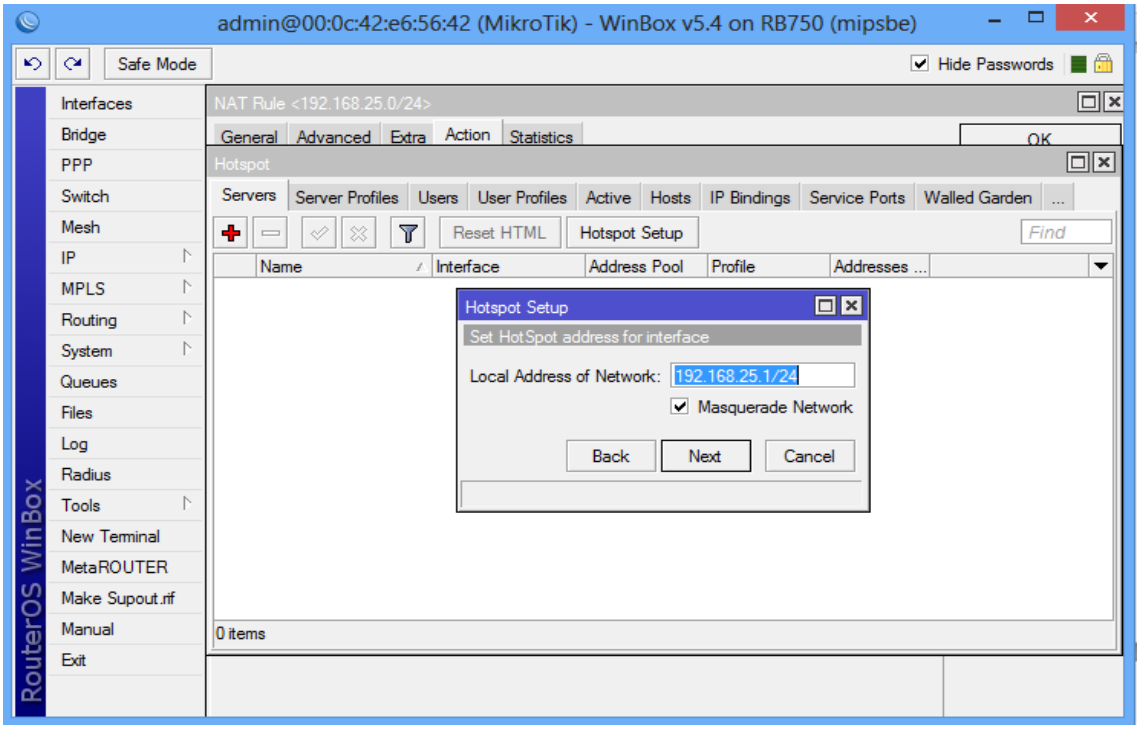
Nos dirigimos a IP/Hotspot. Para no cometer algún error nos ayudaremos con HotpostSetup.



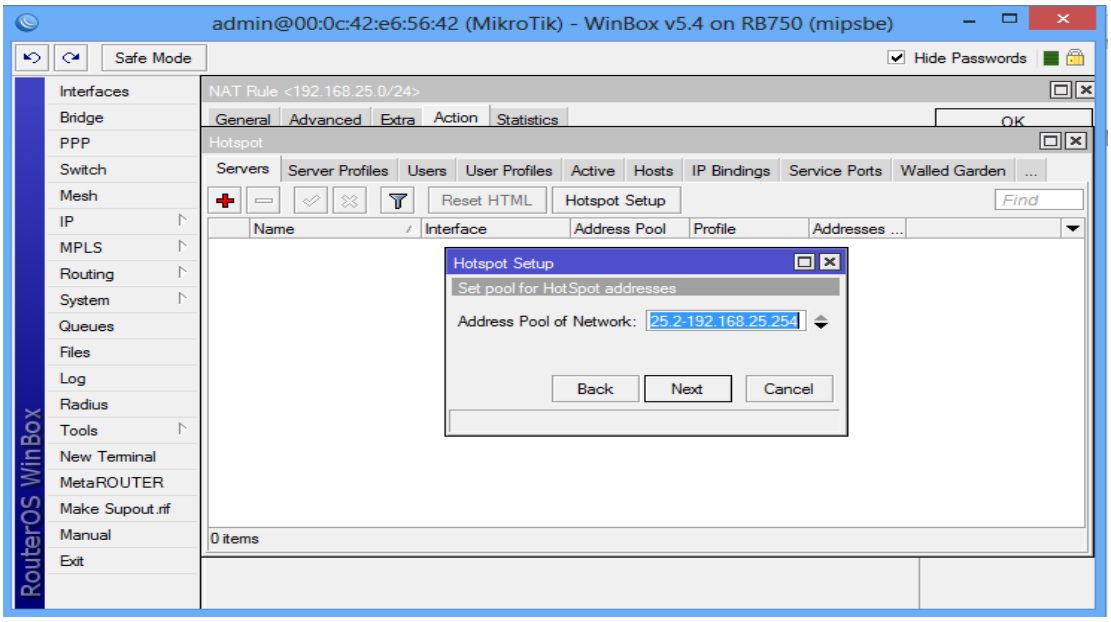
Escogemos a que interfaz deseamos realizarle la configuración de Hotspot.



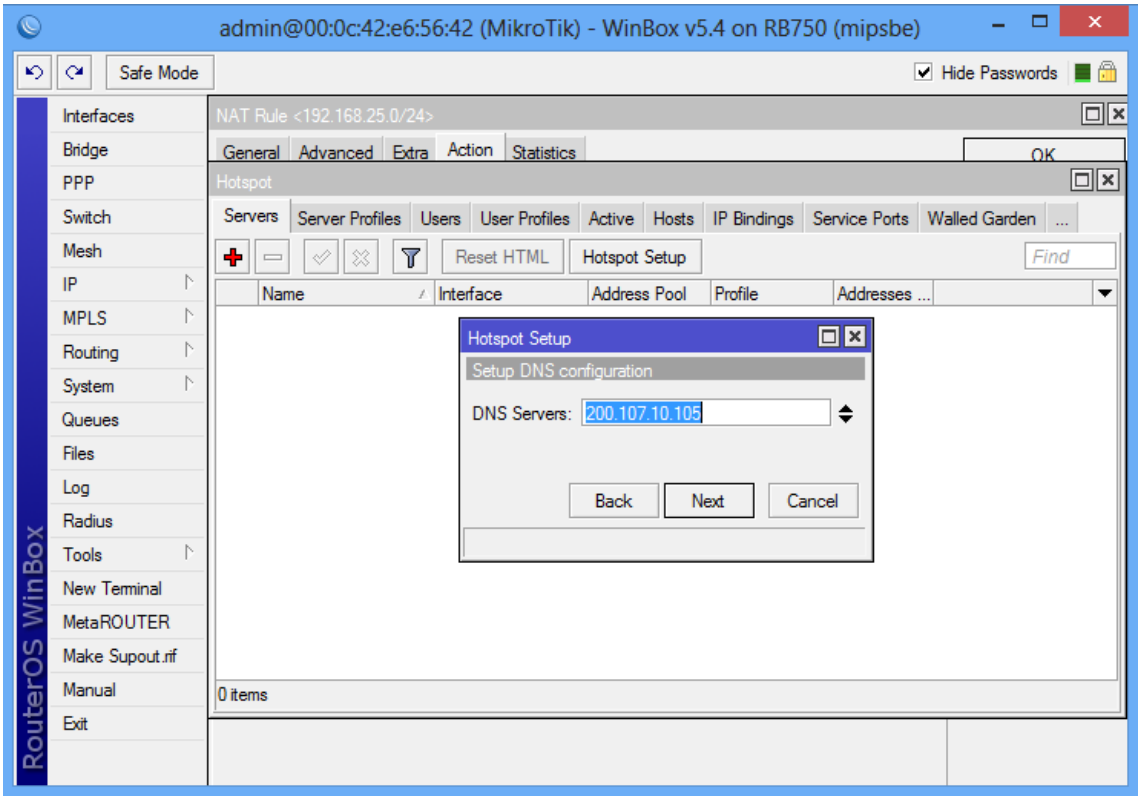
Se indica que red es la que vamos a escoger para la configuración y damos Check a la opción de enmascarar la red.



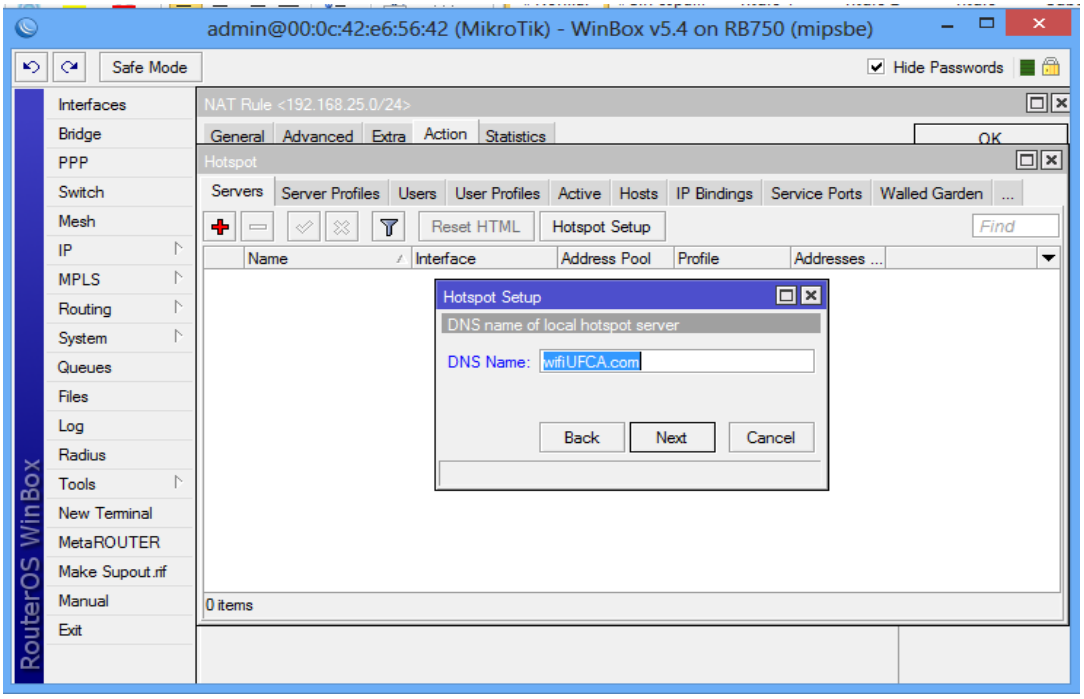
Se indica cual va hacer el rango de las direcciones que el Hotspot va a brindar.



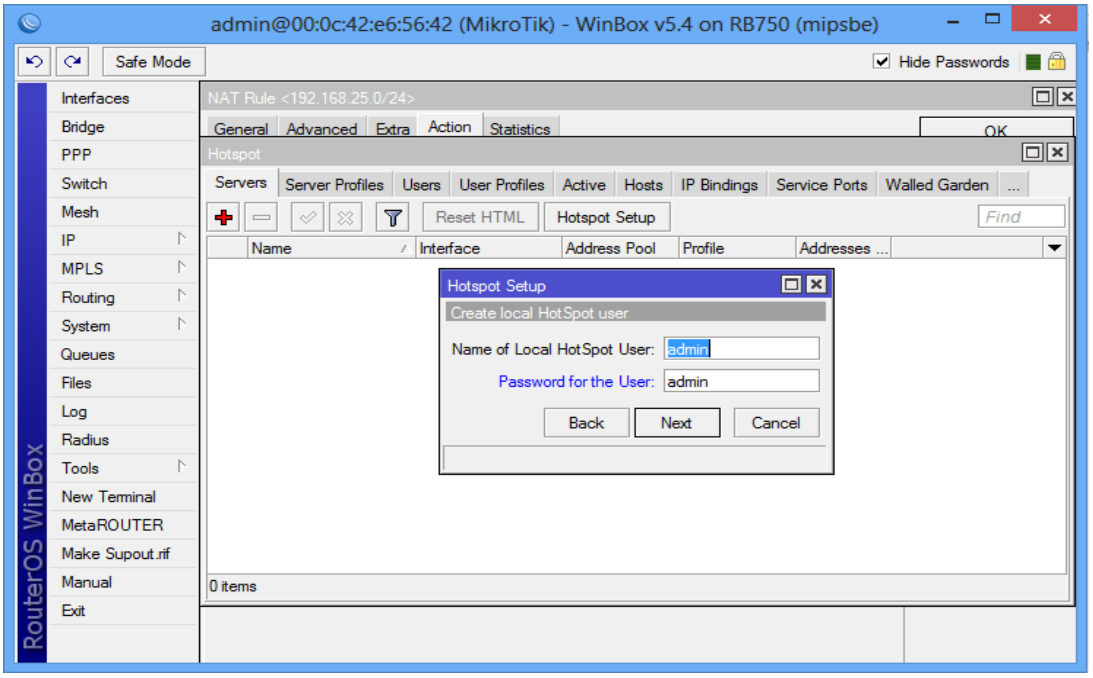
Indicamos también cual va a ser nuestro servidor DNS.



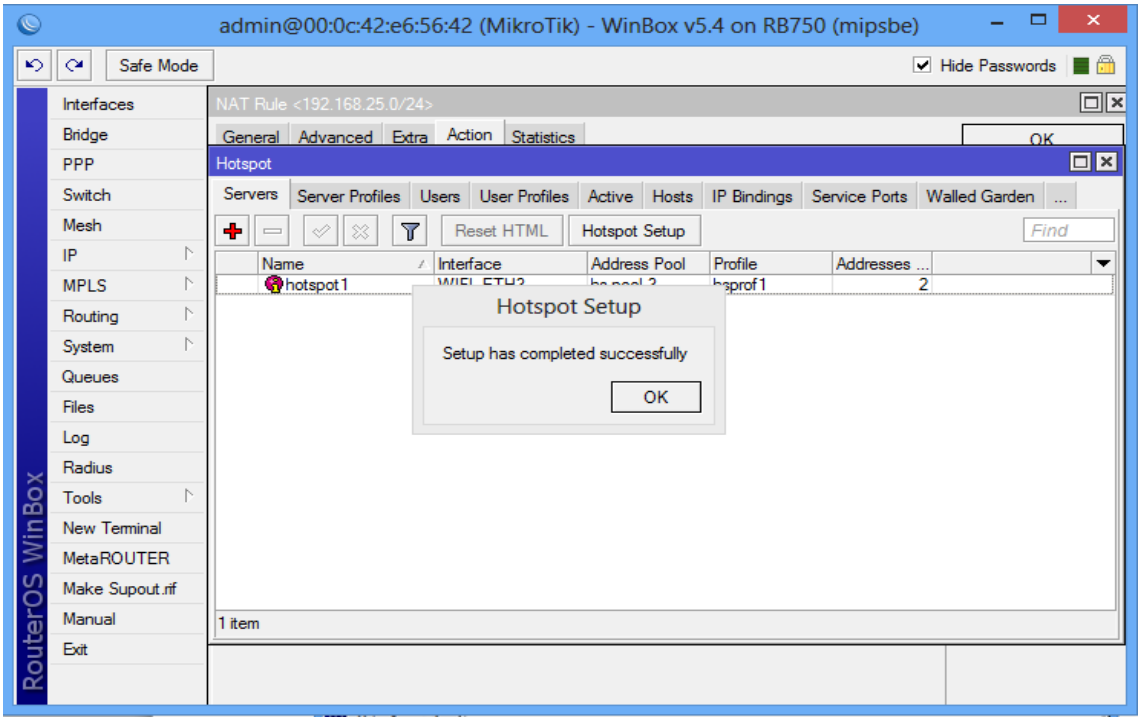
Le indicamos cual va a ser nuestro nombre de dominio para nuestro servidor local.



Definimos un nombre y una clave para el usuario de HostPost local.

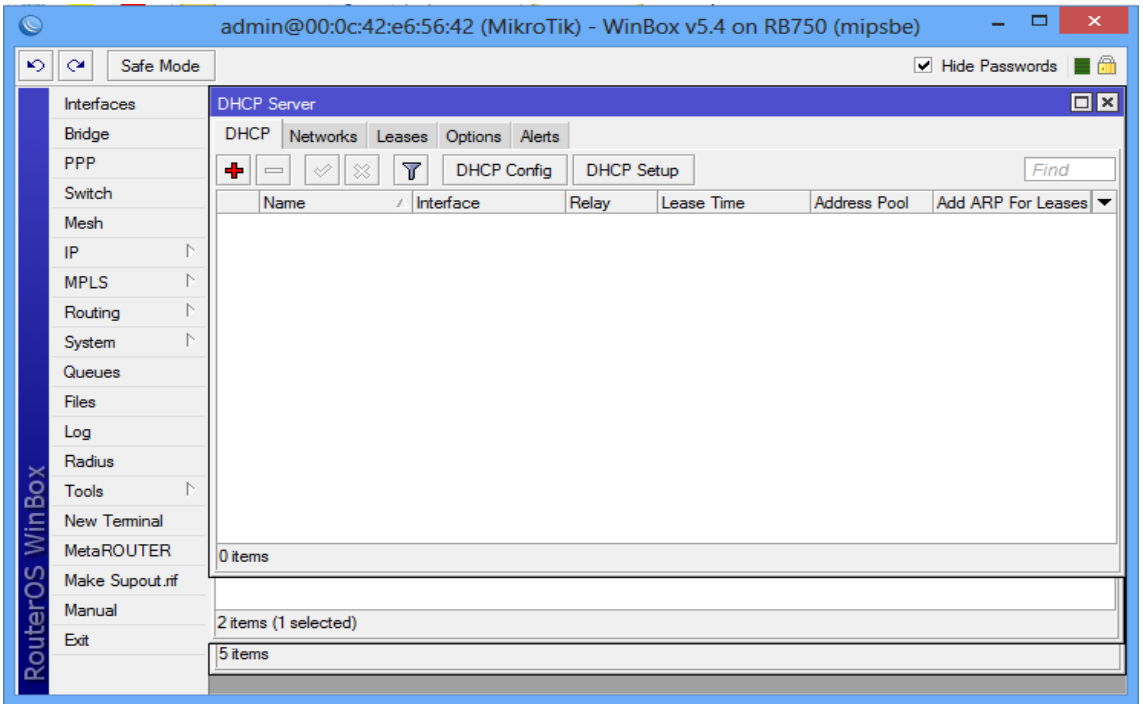


Y la configuración de nuestro Hotpost se finaliza satisfactoriamente.

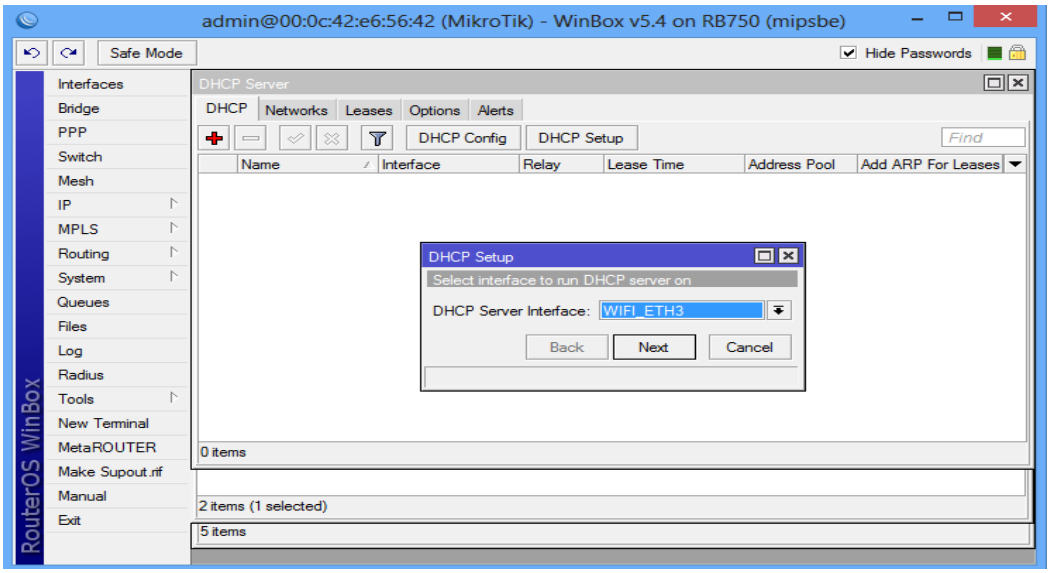


Configuración de Server DHCP.

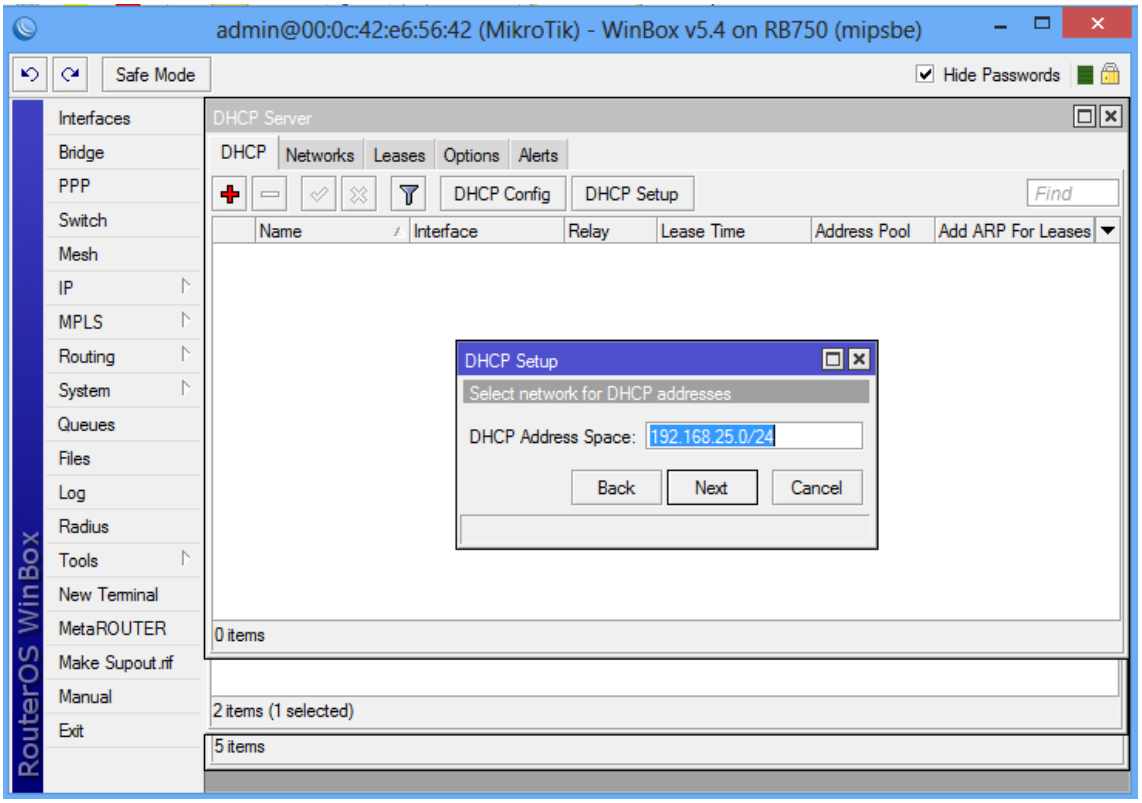
Para evitar la configuración manual de red en nuestros dispositivos, configuramos un servidor DHCP con un rango de direcciones, la puerta de enlace y su servidor DNS.



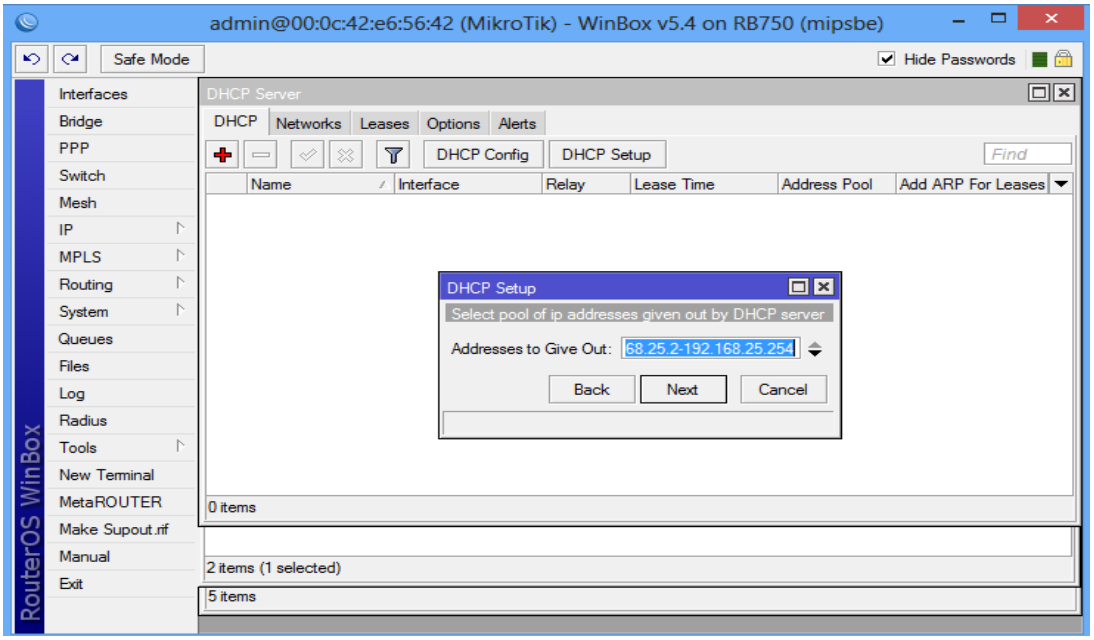
En la siguiente imagen, se denota a que interfaz vamos a dar el servicio DHCP en nuestro caso a la WIFI_ETH3.



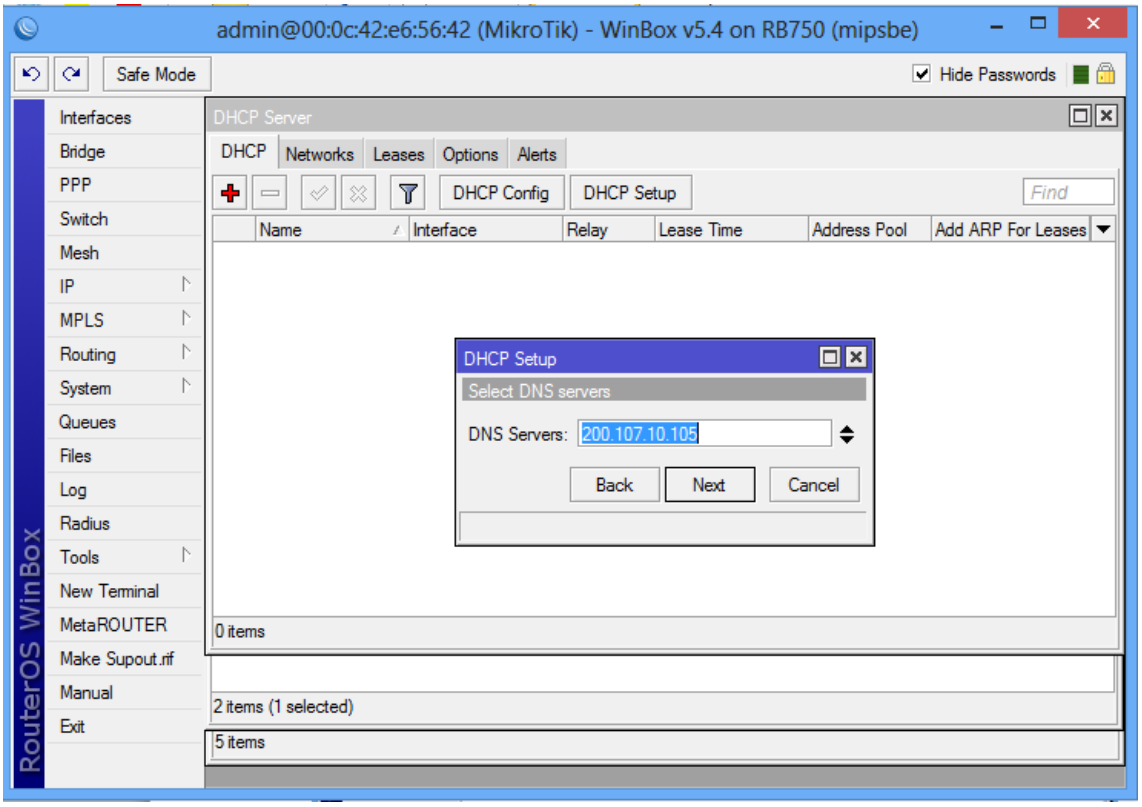
Aquí detallamos cual va hacer la red a cual vamos a entregar el servicio DHCP. En nuestro caso es 192.168.25.0/24.



En esta sección indicamos cual va hacer nuestra puerta de enlace. En este caso es 192.168.25.1.



Aquí se define el Servidor DNS.

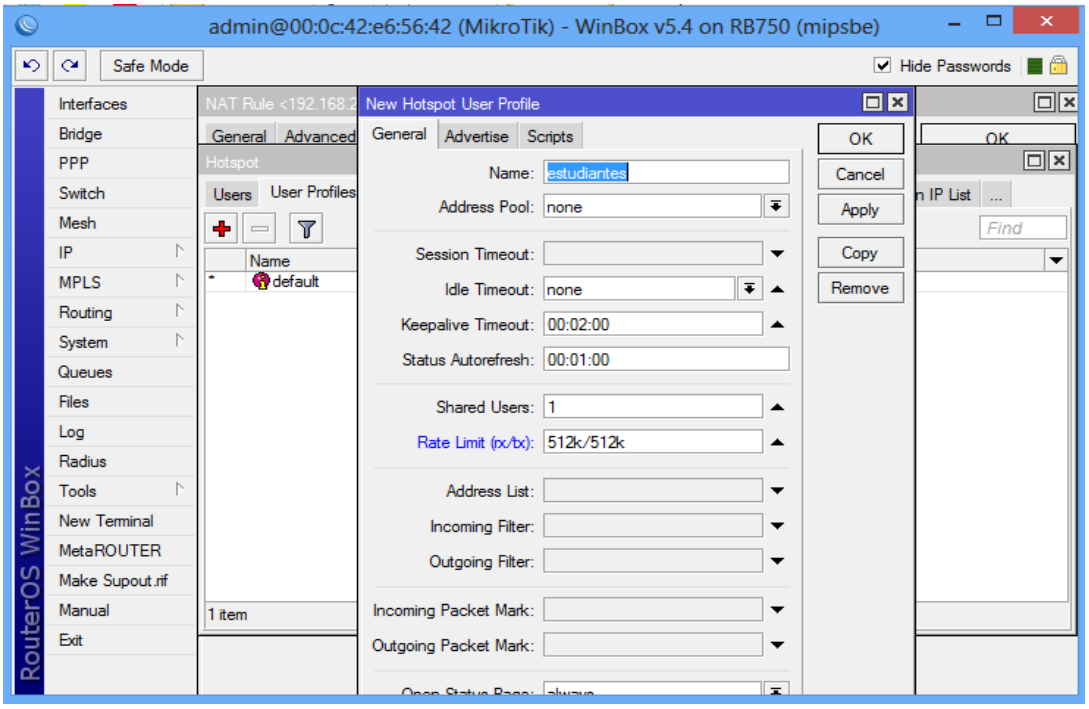


De esta forma dejamos configurado nuestro servidor DHCP para nuestro Hotspot.

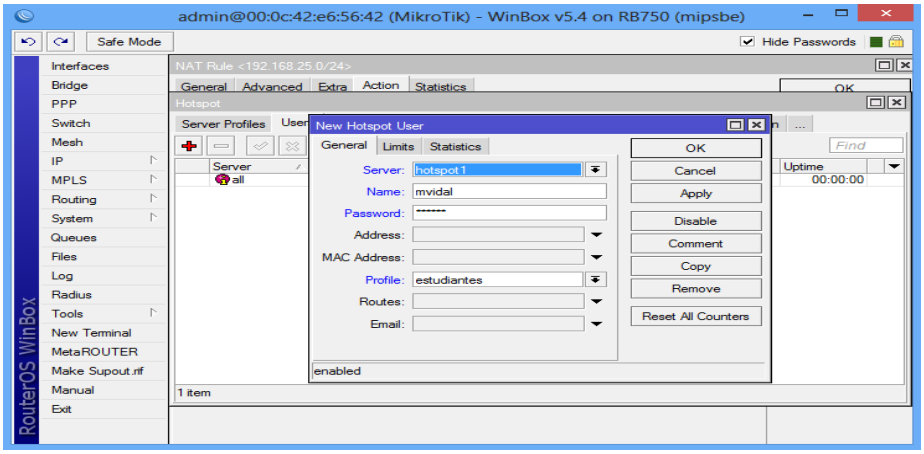
Perfil de usuarios.

Ahora crearemos un perfil de usuario donde determinamos los parámetros de navegación y velocidad que tendrá el mismo.

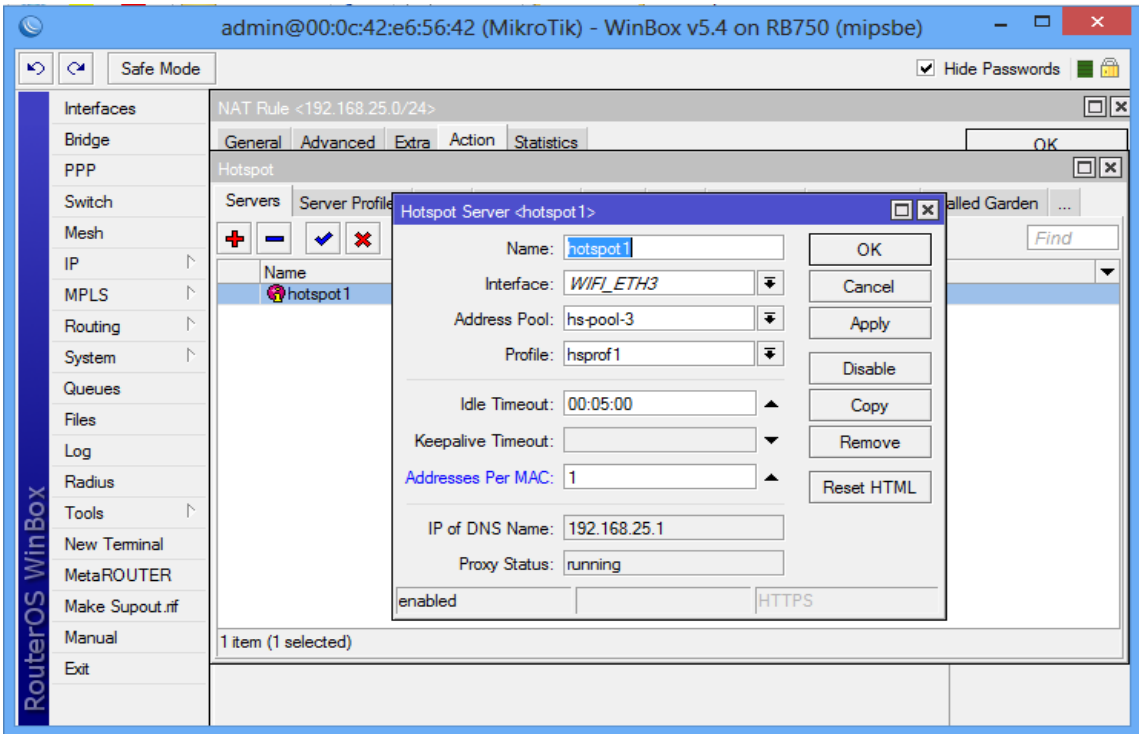
Tendrá como nombre estudiantes, y le daremos una velocidad de transmisión de 1024kb.



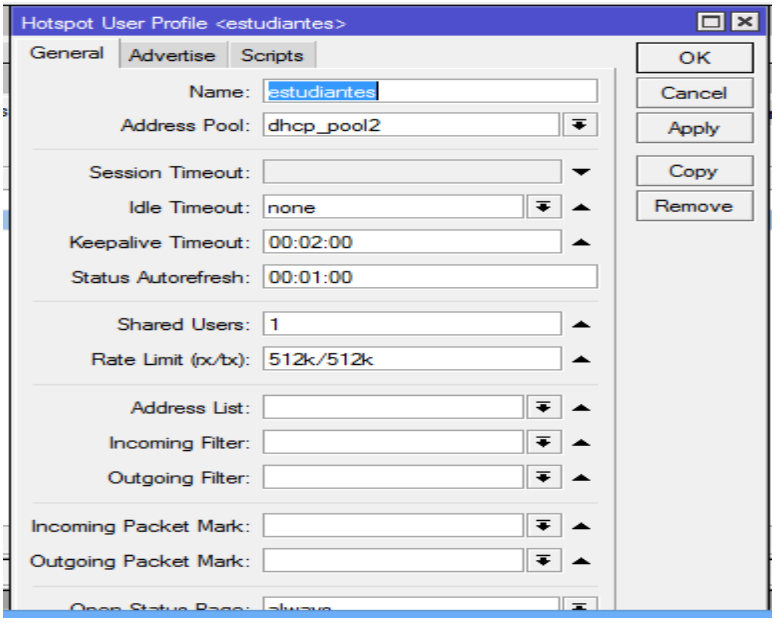
Ahora para el perfil de estudiantes, vamos a crear un usuario para acceder a nuestro Hotspot.



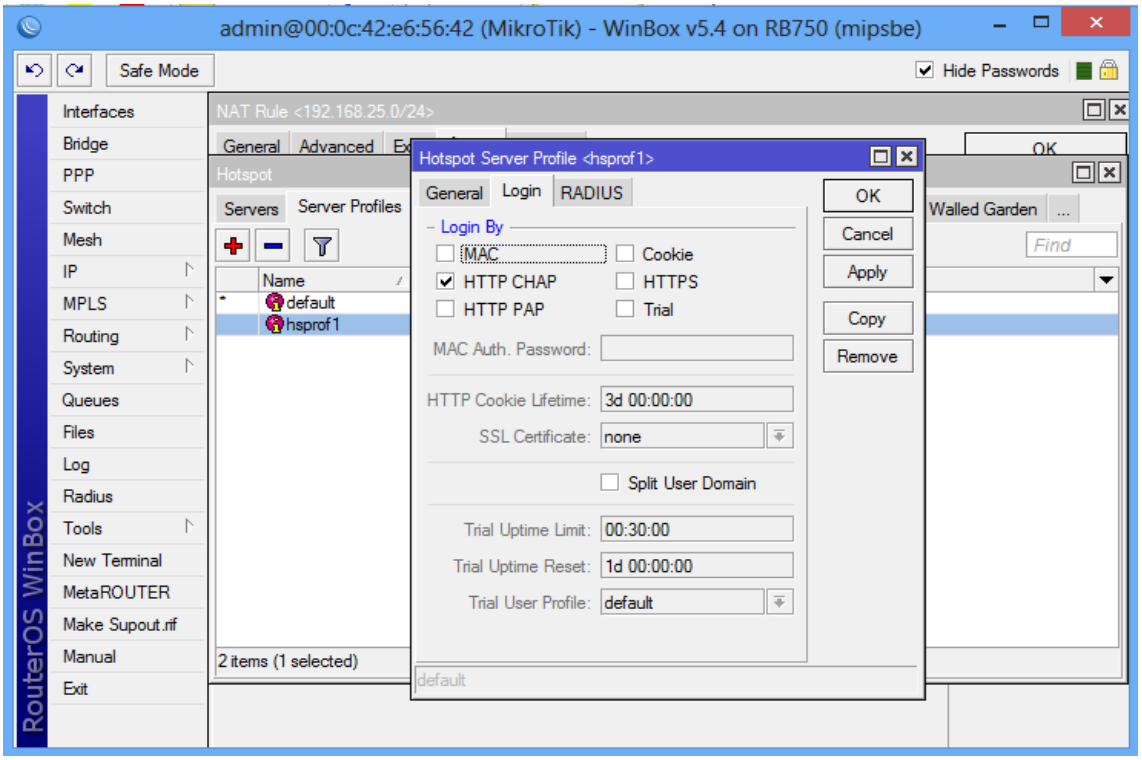
Definimos cuantas direcciones por MAC van a existir, es decir, cuantos dispositivos se pueden conectar con el mismo usuario.



En esta sección escogemos cual va hacer nuestro pool DHCP, como ya configuramos anteriormente un servidor DHCP escogemos el nombre del mismo. En nuestro caso dhcp_pool2.



Para evitar que las credenciales se queden guardadas en los temporales o cookies, desactivamos aquello en el apartado de LOGIN del server de Hotspot.



Consideraciones Técnicas.

Para realizar la debida instalación de todo el proyecto se deben tomar algunas consideraciones técnicas, las cuales serán nombradas y expuestas a continuación:

- Seleccionar un router Onboard capaz de soportar toda la carga de recursos debido a la magnitud de la cantidad de usuarios conectados recurrentemente y las peticiones en la red.

- Conocer la infraestructura de la red, como las direcciones de sus servidores DNS, a que subred se va enganchar nuestro dispositivo.

- Realizar un subneteo de tal forma queden el suficiente número de direcciones IP para el número de usuario que maneja la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG).

- Verificar que la dirección IP asignada a nuestra interfaz WAN del dispositivo de comunicación debe poseer todos los permisos necesarios para la salida hacia el internet por parte del centro de cómputo de la Facultad de Ciencias Administrativa de la Universidad de Guayaquil (FCA-UG).

- Tener muy claro que las interfaces del dispositivo se configuran con sus nombres y en las mismas se subnetean, luego de aquello a las mismas se le aplica el servicio de hotpost las cuales deben coincidir con la división de red que le fue asignada a la misma y el servicio DHCP que fue configurado.

- Configurar que las sesiones recurrentes por usuario deberían ser una sola.

- Configurar el firewall del dispositivo Onboard para que cualquier peticiones que viene de nuestra red de hotspot pasen sin ningún inconveniente, en nuestro caso dejamos pasar cualquier petición por cualquier puerto ya que todo va hacer peticiones hacia internet.

-Crear en la misma sección de Firewall la regla de NAT, esto para poder ocultar nuestras peticiones con la dirección de nuestro dispositivo Router hacia el internet.

- Tener claro cuáles son nuestras interfaces ya sean estas las de WAN, LAN o la de hotspot ya que por mucha confusiones en la práctica da para que se conecte los punto de acceso en algunas interfaz que no sea la indicada, y de ahí para delante no va a funcionar ningún tipo de configuración para que pueda funcionar correctamente.

ANEXO N°2

Encuesta sobre uso del WI-FI

1. ¿Qué tipo de equipos utiliza para navegar en internet?

    A. Computadora de escritorio.

    B. Laptops – Netbooks.

    C. Teléfonos inteligentes.

    D. Tablets.

    E. Otros

2. ¿Qué tan concurrente hace el uso del internet dentro de la FCA?

    A. Nunca

    B. Muy poco

    C. A menudo

    D. frecuentemente

    E. Siempre

3. ¿Qué tipo de páginas web visita a menudo al momento de utilizar el internet conectado a una red WI-FI?

    A. Redes sociales.

    B. Páginas de investigación.

    C. Páginas Educativas.

    D. Otros.

4. Si existiera una red WI-FI dentro de la FCA estaría de acuerdo en que esta sea reservada únicamente para los docentes, estudiantes y personal administrativo de la facultad?

    A. SI.

    B. NO

5. ¿Está de acuerdo que el acceso a las redes WI-FI que se implementen en la F.C.A. sean abiertas (Sin Clave)?

    A. SI.

    B. NO.

6. ¿Está de acuerdo en que el acceso para el uso de internet se realice mediante usuario y contraseña?

    A. SI.

    B. NO.

7. De los siguientes ítems seleccione dónde le parece adecuado disponer de redes WI-FI.

    A. Bibliotecas de la F.C.A.

    B. Bloques de la F.C.A.

    C. Secretaría.

    D. Entrada Principal.

    E. Todos los anteriores.

8. ¿Está de acuerdo en que el internet mediante WI-FI esté disponible en todas las jornadas educativas que mantiene la F.C.A?

    A. SI.

    B. NO.

9. ¿Está de acuerdo en que se establezca a los usuarios un tiempo de uso del WI-FI para no congestionar el ancho de banda (velocidad del internet)?

    A. SI.

    B. NO.

10. ¿En caso de implementar una red WI-FI en la FCA, está de acuerdo en que se restringa el acceso a páginas de redes sociales o cualquier otra que no tenga que ver con ciencia y educación?

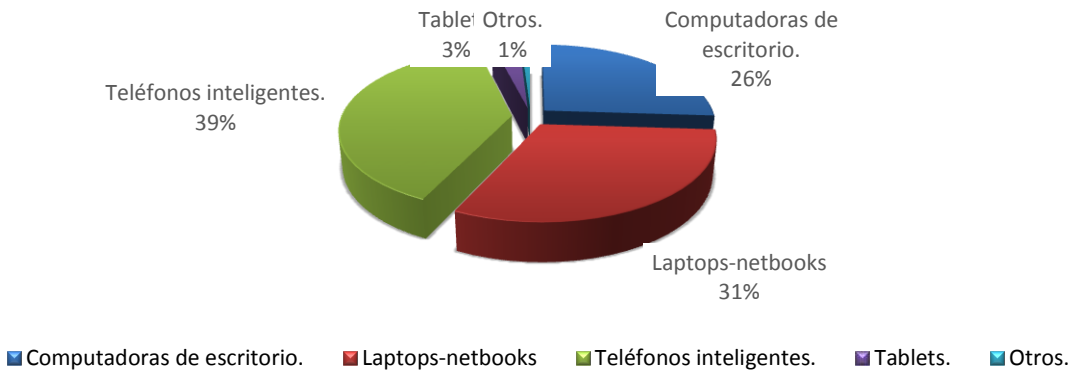
    A. SI.

    B. NO.

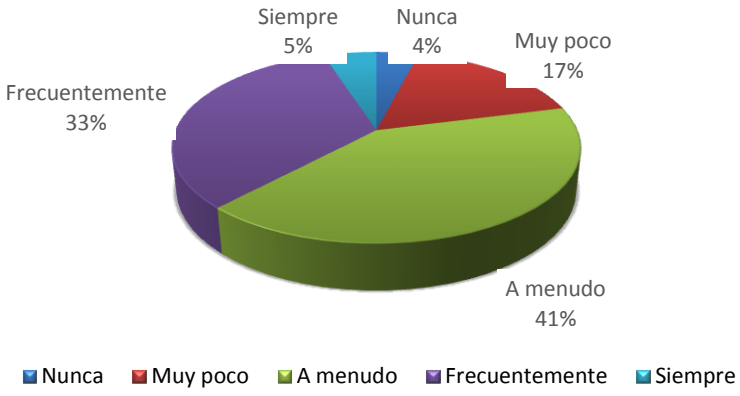
ANEXO N°3

Resultados de la encuesta sobre uso del WI-FI

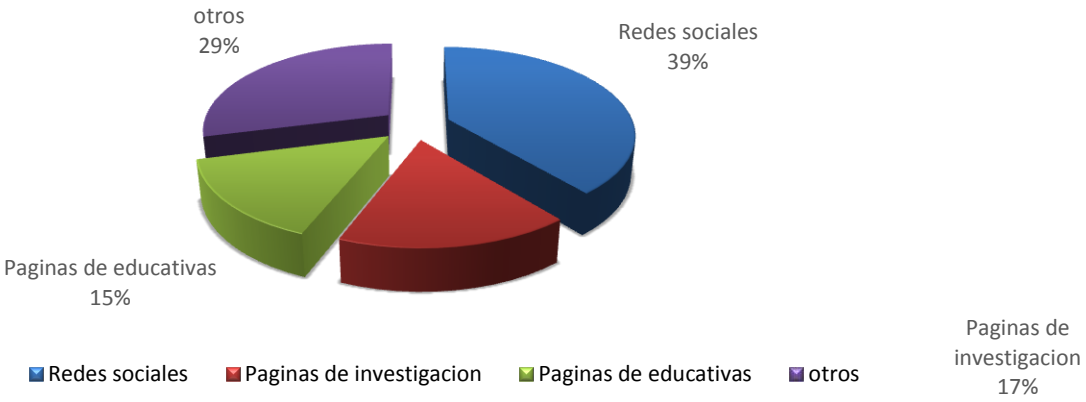
1. ¿Qué tipo de equipos utiliza para navegar en internet?



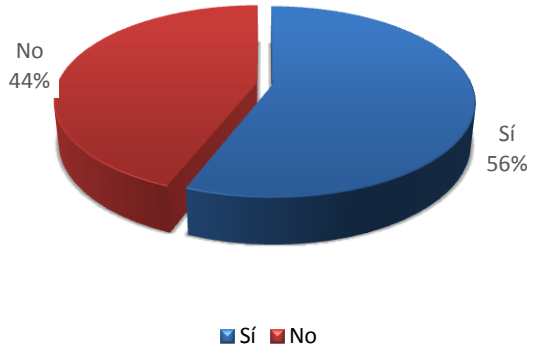
2. ¿Qué tan concurrente hace el uso del internet dentro de la FCA?



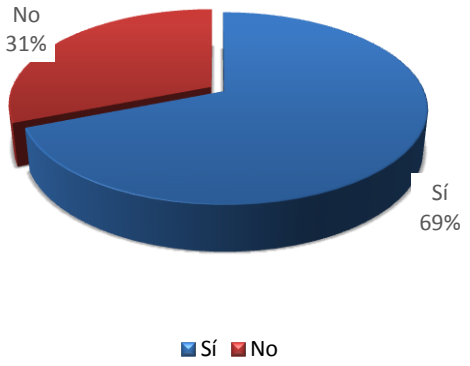
3. ¿Qué tipo de páginas web visita a menudo al momento de utilizar el internet conectado a una red WI-FI?



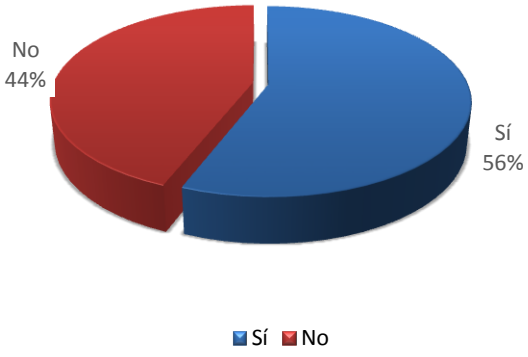
4. Si existiera una red WI-FI dentro de la FCA estaría de acuerdo en que esta sea reservada únicamente para los docentes, estudiantes y personal administrativo de la facultad?



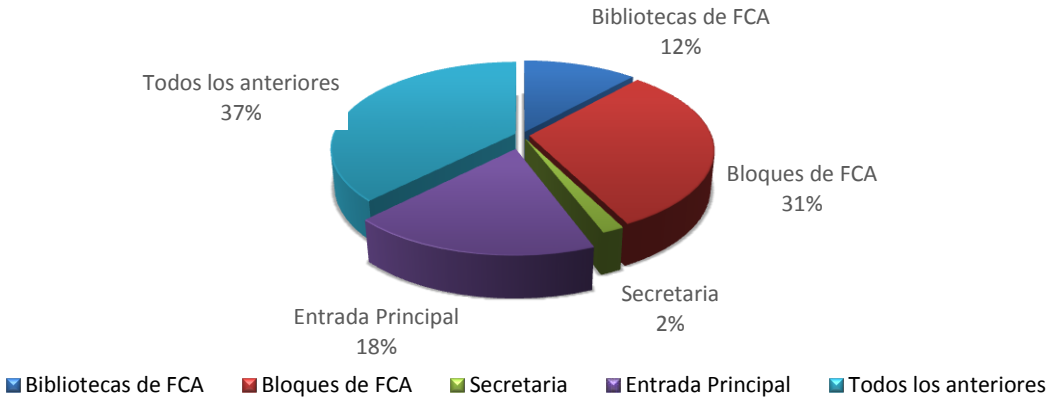
5. ¿Está de acuerdo que el acceso a las redes WI-FI que se implementen en la F.C.A. sean abiertas (Sin Clave)?



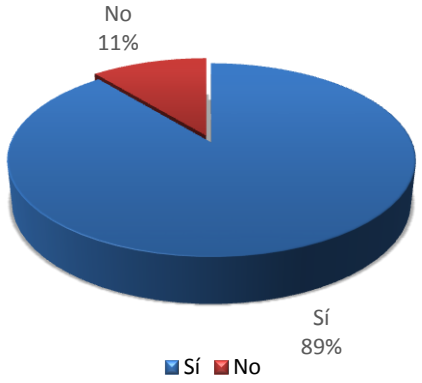
6. ¿Está de acuerdo en que el acceso para el uso de internet se realice mediante usuario y contraseña?



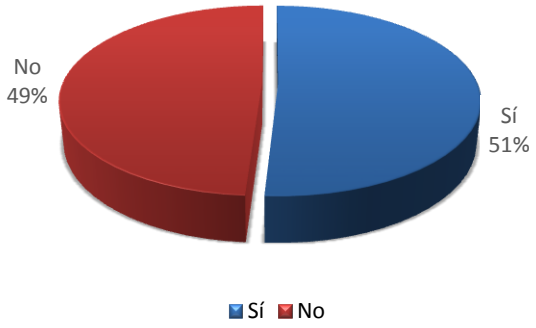
7. De los siguientes ítems seleccione dónde le parece adecuado disponer de redes WI-FI.



8. ¿Está de acuerdo en que el internet mediante WI-FI esté disponible en todas las jornadas educativas que mantiene la F.C.A?



9. ¿Está de acuerdo en que se establezca a los usuarios un tiempo de uso del WI-FI para no congestionar el ancho de banda (velocidad del internet)?



10. ¿En caso de implementar una red WI-FI en la FCA, está de acuerdo en que se restringa el acceso a páginas de redes sociales o cualquier otra que no tenga que ver con ciencia y educación?