DISEÑO E IMPLEMENTACION DE UNA RED INALAMBRICA PARA LA COMUNIDAD ACADEMICA DE LA CORPORACION UNIVERSITARIA MINUTO DE DIOS SEDE NUEVA

INGRID MILENA CARDENAS ARCINIEGAS

DIEGO FRANCISCO BALLEN LEON

COORPORACION UNIVERSITARIA MINUTO DE DIOS

FACULTAD DE INGENIERIA

TECNOLOGIA DE REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA

GIRARDOT

2011

DISEÑO E IMPLEMENTACION DE UNA RED INALAMBRICA PARA LA COMUNIDAD ACADEMICA DE LA CORPORACION UNIVERSITARIA MINUTO DE DIOS SEDE NUEVA

INGRID MILENA CARDENAS ARCINIEGAS

DIEGO FRANCISCO BALLEN LEON

PROYECTO PARA OPTAR EL TITULO DE TECNOLOGO EN REDES

EFRAIN MASMELA

DOCENTE

COORPORACION UNIVERSITARIA MINUTO DE DIOS

FACULTAD DE INGENIERIA

TECNOLOGIA DE REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA

GIRARDOT

2011

AGRADECIMIENTOS

Un gran agradecimiento a todos los profesores que nos guiaron en este proyecto a Mauricio Rodríguez y Juan Murillo quienes nos dieron pautas importantes para la implementación y a todos aquello que compartieron su sabiduría con nosotros en especial a Oscar Díaz… a todos ellos muchas gracias.

CONTENIDO

Pag.

TABLAS

Pag.

INTRODUCCION

En la Corporación Universitaria Minuto de Dios sede Girardot, en los 10 años de estar presente en la ciudad como universidad reconocida, aun estando sin sede propia, se ha dado a la tarea de orientar diversas carreras en varios niveles académicos, que en la actualidad presentan mucho demanda, pero sin ningún servicio inalámbrico de internet para su estudiantado, solo con una red cableada y unos equipos de cómputo con los que cuenta la universidad.

Debido al cambio y avances la universidad brindo temporalmente internet a la comunidad académica atreves de una red inalámbrica mediante 2 A.P. (Access Point), uno en la Antigua Sede García Herreros, pero el cual ya no está disponible y el otro en la Nueva Sede, que poseía una infraestructura de seguridad inalámbrica atraves de una autenticación Mac, esto la hacía segura pero sin un sistema de autenticación a la vanguardia de hoy en día a nivel de redes de datos, pero el cual ha sido cancelado.

En la actualidad la universidad no cuenta con una red inalámbrica para los estudiantes, pero si se implementó una red cableada e inalámbrica para los profesores y coordinadores, estas redes funcionan por medio de dos equipos un Linksis en la sala de coordinadores y una D-link en la sala de profesores, estas redes se encuentran con claves, a las cuales los estudiantes no tienen acceso.

Dada que la falta de una red inalámbrica es necesaria y que la seguridad es primordial hoy en día, evitando no solo la entrada de personas no ligadas a la institución sino para brindar una sistematización a la hora de entrar a la red inalámbrica, ya no necesitando quien configure nuestro equipo sino acceder a la red y dando un usuario y una clave que nos vincule directamente a la internet al entrar al navegador.

Este proyecto busca crear un red inalámbrica que simplifique esta parte haciéndola más sencilla y segura para usuarios, sin que tengan extensos conocimientos de redes.

1. PROBLEMA

1.1 FORMULACION DEL PROBLEMA

¿Cómo diseñar e implementar una red inalámbrica con un nivel de seguridad óptimo para la comunidad académica de la Corporación Universitaria Minuto de Dios en la Nueva Sede?

1.2 DESCRIPCION DEL PROBLEMA

Actualmente la Corporación Universitaria Minuto de Dios no cuenta con una red inalámbrica para los estudiantes.

Anteriormente tenía una red inalámbrica que manejaba algunas pautas de seguridad a la hora de accesar a la red, pero no contaba exactamente con algún tipo de infraestructura de seguridad que estipule los protocolos de acceso a la misma; lo que se quiere con este proyecto es crear una red inalámbrica que simplifique este proceso brindando un acceso simple y a la vez seguro en la universidad, atreves de un servidor Mikrotik para brindar autenticación, este prototipo le dará a la comunidad académica una ventaja de poder tener acceso cuantas veces quiera pero ya con un usuario y una clave asignada, sin tener que esperar configuraciones del encargado de la clave de acceso en la universitaria.

2. JUSTIFICACION

El desarrollo de este proyecto es algo muy importante en toda nuestra etapa formativa no solo por ser requisito fundamental para nuestra graduación sino que por medio de este proyecto seremos parte de toda la evolución que ha logrado la Universidad Minuto de Dios a lo largo de todos estos años, dejando así un gran aporte no solo para la universidad sino para aquellas generaciones futuras que ingresen y puedan beneficiarse con este gran proyecto.

Este trabajo es una prueba muy importante, donde se pondrán a prueba los conocimiento no solo aquellos que nos proporcionaron los profesores en las diversas áreas referentes a las redes sino también aquellos que poseemos o adquirimos por nosotros mismo así como nuestro ingenio y dedicación y los demás aspectos que tenemos que tener el momento de trabajar o hacer alguna actividad de este tipo, aspectos tales como la puntualidad, el cumplimiento la responsabilidad y las actitudes que estemos dispuestos probar. Además de querer innovar un servicio con el que se cuenta actualmente en la universidad, brindando seguridad y simplicidad en este, garantizando a la comunidad académica el acceso de este; facilitando a la comunidad académica un nivel investigativo, teniendo muy en cuenta que uno de los objetivos principales de la universidad minuto de dios es formar profesionales altamente competentes, éticamente responsables líderes de procesos de transformación social.

3. OBJETIVO DEL PROYECTO

❖ OBJETIVO GENERAL

Diseñar e implementar una red Inalámbrica con un nivel de seguridad optimo, para la comunidad académica de la Corporación Universitaria Minuto de Dios de la Sede Nueva Girardot.

❖ OBJETIVOS ESPECIFICOS

- Analizar las diferentes necesidades a nivel inalámbrico actual en la Corporación Universitaria Minuto de Dios Nueva Sede recolectando información para su debido proceso.

- Analizar diferentes alternativas de solución prácticas a la necesidad actual que presenta la universidad con las evidencias que se recolectaron anteriormente.

- Diseñar la solución que mejore la infraestructura de seguridad existente de la red.

- Implementar el prototipo diseñado con sus especificaciones en la fase de diseño

4. MARCOS DE REFERENCIA

8.1. MARCO LEGAL

Este proyecto se enmarca en el Decreto 2566 del 10 de Septiembre de 2003, que reglamentó las condiciones mínimas de calidad y demás requisitos para el ofrecimiento y desarrollo de programas académicos de educación superior, en el Articulo 10 opción e es nombrado, esto es reglamentado por el estado que vela por el adecuado ofrecimiento de educación superior.

También se deja presente que todos los derechos de este proyecto le pertenecen a la Corporación Universitaria Minuto de Dios, nuestra participación en dicho proyecto es simplemente de coautores.

8.2. MARCO TEORICO

- Red inalámbrica

El término red inalámbrica (Wireless networks en inglés) es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.

Una de sus principales ventajas es notable en los costos, ya que se elimina todo el cable ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

En la actualidad las redes inalámbricas son una de las tecnologías más prometedoras.

Categorías

Existen dos categorías de las redes inalámbricas.

1. Larga distancia: estas son utilizadas para distancias grandes como puede ser otra ciudad u otro país.

2. Corta distancia: son utilizadas para un mismo edificio o en varios edificios cercanos no muy retirados.

Tipos

Según su cobertura, se pueden clasificar en diferentes tipos:

Wireless Personal Area Network

En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth (protocolo que sigue la especificación IEEE 802.15.1); ZigBee (basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo); RFID (sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

Wireless Local Area Network

En las redes de área local podemos encontrar tecnologías inalámbricas basadas en HiperLAN (del inglés, High Performance Radio LAN), un estándar del grupo ETSI, o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.

Wireless Metropolitan Area Network

Para redes de área metropolitana se encuentran tecnologías basadas en WiMAX (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service).

Wireless Wide Area Network

En estas redes encontramos tecnologías como UMTS (Universal Mobile Telecommunications System), utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología GSM (para móviles 2G), o también la tecnología digital para móviles GPRS (General Packet Radio Service).

Características

Según el rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser las ondas de radio, las microondas terrestres o por satélite, y los infrarrojos, por ejemplo. Dependiendo del medio, la red inalámbrica tendrá unas características u otras:

- Ondas de radio: las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30 Hz, hasta la banda UHF que va de los 300 a los 3000 MHz, es decir, comprende el espectro radioeléctrico de 30 - 3000000000 Hz.

- Microondas terrestres: se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar en enlaces punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.

- Microondas por satélite: se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal (denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuenciales de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta frecuencia se mezclan bastante, así que pueden haber interferencias con las comunicaciones en determinadas frecuencias.

- Infrarrojos: se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz.

- Protocolo Informático

En informática, un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. En su

forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, un protocolo define el comportamiento de una conexión de hardware.

Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma. El protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet es necesario que tenga instalado este protocolo de comunicación.

Estrategias para mejorar la seguridad (autenticación, cifrado).

Cómo se construye una red física.

Cómo los computadores se conectan a la red.

- Políticas De Seguridad

Hoy es imposible hablar de un sistema cien por cien seguro, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. "Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares".

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la

mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

- Seguridad Informática

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Objetivos de la seguridad informática

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

La información contenida

Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

La infraestructura computacional

Una parte fundamental para el almacenamiento y gestión de la información, asi como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y preveer en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios

Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general. y como principal contribuyente al uso de programas realizados por programadores

- RADIUS

RADIUS es un protocolo ampliamente usado en el ambiente de redes, para Dispositivos tales como routers, servidores y switches entre otros.

RADIUS (Remote Authentication Dial-In User Server) es una colección y definición de normas para la creación de sistemas o protocolo que nos permite gestionar la “autenticación, autorización y registro” de usuarios remotos sobre un determinado recurso, ampliamente usado en el ambiente de redes, para dispositivos tales como routers, servidores y switches entre otros. La tupla “autenticación, autorización y registro” es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa “Authentication, Authorization, and Accounting”.

Estos términos se refieren a:

- Autenticación (authentication) hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario nos permite acceder a determinados recursos. El nombre de usuario es nuestra identidad, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante nuestra identidad. Otros tipos más avanzados de credenciales son los certificados digitales.

Existen muchos métodos concretos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son:

- Autenticación de sistema (system authentication), típica en un sistema Unix, normalmente realizada mediante el uso del fichero /etc/passwd;
- Los protocolos PAP (Password Authentication Protocol), y su versión segura CHAP (Challenge Handshake Authentication Protocol), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP;
- LDAP (Lightweight Directory Access Protocol), un protocolo a nivel de aplicación (sobre TCP/IP) que implementa un servicio de directorio ordenado, y muy empleado como base de datos para contener nombres de usuarios y sus contraseñas;
- Kerberos, el famoso método de autenticación diseñado por el MIT;
- EAP (Extensible Authentication Protocol), que no es un método concreto sino un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto;
- Por último, también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

En la fase de autenticación se produce un mensaje inicial de solicitud de acceso desde el equipo NAS al servidor de autenticación en forma de:

- Access – Request (solicitud de acceso): El usuario envía el nombre de usuario y la contraseña cifrada, si procede hacia el NAS. Este envía entonces al servidor de autenticación el mensaje de Access-Request solicitando además el puerto de acceso para el usuario.

- Autorización (authorization) se refiere a conceder servicios específicos (entre los que se incluye la “negación de servicio”) a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples “logins” de un mismo usuario.

  El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

  Los métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen bases de datos LDAP, bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor.

  No se debe confundir los términos autenticación con autorización. Mientras que la autenticación es el proceso de verificar un derecho reclamado por un individuo (persona o incluso ordenador), la autorización es el proceso de verificar que una persona ya autenticada tiene la autoridad para efectuar una determinada operación.

  E n esta fase el servidor de autenticación, tras conocer todos los atributos necesarios para el solicitante, responderá a su solicitud de autenticación mediante un mensaje estándar enviado al equipo NAS para permitir, denegar o volver a preguntar sobre su acceso:

  - Access - Accept (Aceptación del acceso): El fin mismo de la solicitud de autenticación es la aceptación del acceso. Si el mecanismo de acceso ha sido correcto, se le envía este mensaje al NAS con los atributos necesarios para regular el acceso del usuario de forma personalizada.
  - Access – Reject (Denegacion del acceso): Debido a las circunstancias que pueden no permitir el acceso de un usuario, como por ejemplo: usuario inexistente, contraseña incorrecta, derechos revocados, etc. Se le deniega de forma incondicional el acceso a este solicitante. Se puede incluir en este mensaje el motivo de la denegación del servicio. El NAS que recibe este mensaje no permite el

acceso al usuario, enviando un mensaje (si se incluye) al solicitante o usuario.

- Access – Challenge (Solicitud de información adicional para el acceso): Se le solicita al usuario o solicitante información adicional, como contraclave, tarjeta de acceso, PIN de acceso, o cualquier otro método alternativo o adicional de acceso. El NAS transmite la solitud al usuario. Este mensaje puede ser intercambiado en múltiples ocasiones dependiendo del tipo de autenticación y de la información que se precisa

- Registro (accounting, a menudo traducido también como contabilidad) se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio.

  Durante la fase de registro se producen los siguientes mensajes:

  - Accounting - Request [Start] (Solicitud de inicio de registro): Es una solicitud de inicio enviada desde el equipo NAS al servidor, para indicar que ha comenzado la fase de registro, y comienza a recolectar los datos de la sesión del usuario.
  - Accounting - Response [Start] (Respuesta de asentimiento al inicio de registro): El servidor de autenticación responde a la solicitud inicial, registrando la información de inicio y enviando este paquete al NAS para mostrar su conformidad.
  - Accounting - Request [Stop] (Solicitud de final de registro): El NAS comprueba la desconexión del usuario y envía al servidor un mensaje de final de la fase de registro con los datos de la sesión de usuario.
  - Accounting – Response [Stop] (Respuesta de asentimiento al final del registro): El servidor tras almacenar la información anterior, envía al NAS su conformidad al final de la fase de registro, admitiendo haber recibido correctamente toda la información de la sesión.

Es interesante el uso del protocolo RADIUS cuando tenemos redes de dimensiones considerables sobre las que queremos proporcionar un servicio de acceso centralizado (aunque posiblemente jerarquizado por medio de diversos servidores RADIUS). Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan

acceso a Internet o grandes redes corporativas, en un entorno con diversas de tecnologías de red (incluyendo módems, xDSL, VPNs y redes inalámbricas) no sólo para gestionar el acceso a la propia red, sino también para servicios propios de Internet (como e-mail, Web o incluso dentro del proceso de señalización SIP en VoIP).

Un uso de RADIUS que queremos enfatizar, al ser el que realizaremos en esta práctica, es la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (pre-shared key, PSK), que son bastante limitados al gestionar una red cuando ésta alcanza un determinado tamaño.

Aunque RADIUS es el protocolo para AAA más extendido en la actualidad, ya existe un nuevo protocolo que está llamado a sustituir a RADIUS. Su nombre es DIAMETER, y también proporciona manejo de errores y comunicación entre dominios.

Es utilizado para proveer autenticación centralizada, autorización y manejo de cuentas para redes de acceso dial-up, redes privadas virtuales (VPN) y, recientemente, para redes de acceso inalámbrico.

Puntos importantes:

- Los sistemas embebidos generalmente no pueden manejar un gran número de Usuarios con información diferente de autenticación. Requiere una gran cantidad de almacenamiento.

- RADIUS facilita una administración centralizada de usuarios. Si se maneja una enorme cantidad de usuarios, continuamente cientos de ellos son agregados o eliminados a lo largo del día y la información de autenticación cambia continuamente. En este sentido, la administración centralizada de usuarios es un requerimiento operacional.

- Debido a que las plataformas en las cuales RADIUS es implementado son frecuentemente sistemas embebidos, hay oportunidades limitadas para soportar protocolos adicionales. Algún cambio al protocolo RADIUS deberá ser compatible con clientes y servidores RADIUS pre-existentes.

Un cliente RADIUS envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS al servidor. Éste autentica y autoriza la solicitud del cliente y envía de

regreso un mensaje de respuesta. Los clientes RADIUS también envían mensajes de cuentas a servidores RADIUS.

Los mensajes RADIUS son enviados como mensajes UDP (User Datagram Protocol). El puerto UDP 1812 es usado para mensaje de autenticación RADIUS y, el puerto UDP 1813, es usado para mensajes de cuentas RADIUS. Algunos servidores usan el puerto UDP 1645 para mensajes de autenticación y, el puerto 1646, para mensajes de cuentas.

Esto último debido a que son los puertos que se usaron inicialmente para este tipo deservicio.

- NAS

Un Network Access Server (NAS) es un sistema que proporciona acceso a la red. En algunos casos también se conoce como Remote Access Server (RAS) o Terminal Server. En general, NAS es un elemento que controla el acceso a un recurso protegido, que puede ser desde un sencillo teléfono para VoIP o una impresora, hasta el acceso a una red inalámbrica o a Internet (proporcionado por un ISP).

Cuando un cliente quiere hacer uso de uno de estos servicios se conecta a NAS, quien a su vez se conecta a un servidor de AAA (típicamente RADIUS) preguntando si los credenciales proporcionados por el cliente son válidos. Basándose en su respuesta, NAS le permitirá acceder o no a este recurso protegido. El sistema NAS no contiene ninguna información sobre los usuarios que se pueden conectar ni sus credenciales, sino que utiliza esta información para enviarla a RADIUS, y que éste le informe sobre los permisos del cliente.

Observa que nos encontramos en un escenario en el que hay dos niveles de la arquitectura cliente-servidor. Desde un punto de vista más global, tenemos la típica arquitectura en la que un usuario quiere acceder a un servicio, siendo el usuario el cliente, y el servidor el sistema que proporciona dicho servicio.

Una ventaja del uso de RADIUS es que sus clientes tan sólo tienen que implementar el protocolo de comunicación con RADIUS, y no todas las posibilidades de AAA existentes (PAP, CHAP, LDAP, kerberos, mySQL, etc.). En el ejemplo del punto de acceso, tan sólo

necesitamos implementar una solución NAS que realice las consultas a RADIUS.

Otra ventaja del protocolo RADIUS es que, en su comunicación con NAS, nunca transmite las contraseñas directamente por la red (lo que se conoce como en cleartext), ni siquiera al usar PAP, sino que usa algoritmos para ocultar las contraseñas como MD5. Sin embargo, al no ser considerado MD5 un sistema de protección de credenciales demasiado seguro, es aconsejable utilizar sistemas adicionales de protección para cifrar el tráfico de RADIUS, como puede ser túneles de IPsec.

NOTA: Es importante no confundir la definición de NAS que hemos dado en este apartado con el NAS como "Network-Attached Storage", que comúnmente se refiere a discos duros conectados directamente a una red.

- Seguridad en tecnologías de red inalámbrica

En redes inalámbricas con infraestructura se utiliza un punto de acceso (wireless access point, WAP o simplemente AP) para interconectar todos los dispositivos inalámbricos de la red. Usualmente un AP se conecta también a una red cableada, transmitiendo datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

La seguridad es un tema importante en las redes inalámbricas porque, al contrario que en una red cableada a la que sólo tienen acceso las personas que físicamente pueden conectarse, cualquier persona de la calle o pisos o edificios vecinos pueden conectarse a una red inalámbrica o ver el contenido de los paquetes que circulan por ella si ésta no está convenientemente protegida.

Algunos de los principales protocolos estándar para proporcionar seguridad en redes inalámbricas IEEE 802.11 son:

- WEP (Wired Equivalent Privacy). Fue introducido en 1997 con objeto de proporcionar un nivel de confidencialidad similar al de las redes cableadas. Usa una clave estática de 64 ó 128 bits con el algoritmo RC4. Su uso se desaconseja completamente, ya que aunque es muy fácil de configurar y está muy extendido al ser el primero que surgió, presenta graves fallos de seguridad.

- WPA (Wi-Fi Protected Access) fue creado para corregir los múltiples fallos detectados en el protocolo WEP. WPA fue diseñado por el consorcio Wi-Fi Alliance basándose en un borrador del estándar 802.11i (es un subconjunto del mismo), y utiliza TKIP (Temporal Key Integrity Protocol) como protocolo de cifrado que sustituye a WEP sin necesidad de modificar el hardware existente (podría funcionar actualizando el firmware).

  En concreto, WPA sigue usando RC4 como algoritmo de cifrado con claves de 128 bits, pero usa TKIP para cambiar dinámicamente estas claves.
  WPA fue diseñado para ser usado junto a un servidor AAA (habitualmente RADIUS), de manera que se le asignan claves distintas a cada uno de los posibles usuarios. Sin embargo, para entornos domésticos o pequeñas oficinas también se puede usar, de forma menos segura, con una única clave compartida (pre-shared key, PSK). En este caso hablamos de WPA-PSK.

- WPA2 se basa en el nuevo estándar 802.11i, y el cambio más significativo respecto a WPA es que usa el protocolo de cifrado AES en lugar de RC4. Mientras que WAP puede ejecutarse en el hardware que soporte WEP (tras actualizar el firmware), WAP2 necesita un hardware más nuevo (posterior al 2004). Sin embargo, se sabe que WAP también terminará siendo comprometido a medio plazo y por tanto sólo se recomienda como transición a WAP2.

  Otro concepto relacionado con la seguridad en redes inalámbricas que merece la pena destacar es EAP (Extensible Authentication Protocol). EAP es un marco general de autenticación, y no un mecanismo de autenticación concreto. EAP proporciona algunas funciones comunes y un método para negociar el mecanismo de autenticación a usar. Actualmente hay más de 40 métodos distintos. En esta práctica haremos uso del denominado EAP protegido (PEAP) para la autenticación de nuestro usuario en la red inalámbrica. Como nuestro suplicante es una máquina con WindowsXP, usaremos MSCHAPv2, la versión de PEAP empleada por Microsoft en este S.O.

8.3 MARCO CONCEPTUAL

La terminología que se maneja en este proyecto no es muy compleja a lo largo del mismo generalmente se encontraran algunas abreviaturas como por ejemplo:

- ✓ WLAN: Que significa “Red de área local Inalámbrica” es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN.
- ✓ Protocolo: Normas o reglas a seguir en las Redes de Computadores.
- ✓ ANSI: El Instituto Nacional de Normalización Estadounidense (ANSI por su sigla en inglés) es una organización privada sin fines lucrativos que administra y coordina la normalización voluntaria en distintos ámbitos.
- ✓ IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (USA). Su Comité de Estándares para las Tecnologías Educativas trabaja con el objetivo de desarrollar estándares técnicos, prácticas recomendadas y guías para la implementación informática de sistemas de formación y educación.
- ✓ TIA: Asociación de la Industria de las Telecomunicaciones que rige normalizaciones del entorno tecnológico.
- ✓ EIA: Asociación de las Industria Eléctrica que rige normalizadores del entorno tecnológico.
- ✓ Red: es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos) y recursos.
- ✓ Host: El término Host, es usado para referirse a los computadores conectados a la red, que proveen y utilizan servicios de ella.

- ✓ Telecomunicaciones: es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser en ambos sentidos.
- ✓ Lógica: Es una secuencia de operaciones realizadas por el hardware o por el software
- ✓ Estación de Trabajo: Puesto de trabajo o computadora de un usuario.
- ✓ Seguridad: El término seguridad proviene de la palabra securitas del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.
- ✓ Inalámbrico: o Wireless Que no utiliza cables. Cualquier tecnología que permite una comunicación entre dispositivos sin ninguna conexión física visible.
- ✓ Mikrotik: El principal producto de Mikrotik es el sistema operativo conocido como Mikrotik RouterOS basados en Linux. Permite a los usuarios convertir un ordenador personal PC en un router, lo que permite funciones como firewall, VPN Server y Cliente, Gestor de ancho de banda, QoS, punto de acceso inalámbrico y otras características comúnmente utilizado para el enrutamiento y la conexión de redes. El sistema operativo es licenciada en la escalada de niveles, cada uno de ellos en libertad a más de los disponibles RouterOS características como el nivel número se eleva. La concesión de licencias es la base y la tasa aumenta con los elementos puestos en libertad. Existe un software llamado Winbox que ofrece una sofisticada interfaz gráfica para el sistema operativo RouterOS. El software también permite conexiones a través de FTP y Telnet, SSH y acceso shell. También hay una API que permite crear aplicaciones personalizadas para la gestión y supervisión
- ✓ Radius: Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.
- ✓ Servidor: Un ordenador o software que ofrece servicios a máquinas de cliente distantes o a aplicaciones, como el suministro de contenidos de

páginas (textos u otros recursos) o el retorno de los resultados de consultas

- ✓ Autenticación: es simplemente la verificación de la identidad y se solicita con frecuencia para tener acceso a los sistemas o redes de computadoras comúnmente con un usuario y una contraseña.
- ✓ Contraseña: Código utilizado para accesar un sistema o servicio. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos.
- ✓ Usuario: Nombre que se utiliza en un registro para accesar a un servicio.
- ✓ AP: o Punto de Acceso Dispositivo que permite que los dispositivos de comunicación inalámbrica se conecten a una red inalámbrica mediante Wi-Fi
- ✓ Software: son los programas, incluyendo procedimientos, utilidades, sistemas operativos, programas de aplicación y paquetes informáticos, implementados para un sistema informático
- ✓ Wi-Fi: Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz
- ✓ Licencia: Permiso otorgado por una Administración para usar un software de pago.
- ✓ Firewall: es una parte de una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- ✓ NAS: Sistema que proporciona acceso a la red, cuando un cliente quiere hacer uso de uno de estos servicios se conecta a NAS, quien a su vez se conecta a un servidor de AAA preguntando si los credenciales proporcionados por el cliente son válidos.

5. METODOLOGIA DE DESARROLLO DEL PROYECTO

5.1 PARTICIPANTES

- ✓ Ingrid Milena Cárdenas Arciniegas
- ✓ Diego Francisco Ballén León
- ✓ Mauricio Rodríguez (Docente)
- ✓ Ana Lucia Forero (Docente)
- ✓ Juan Murillo (Monitor)

5.2 MATERIALES

RECURSOS **TECNOLOGIA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA**	
CANTIDAD	**DESCRIPCION**
2	Computadores
1	Impresora
2	Memorias USB
2	Celulares
1	Software Administración Inalámbrica

Tabla 1: Recursos

5.3 PROCEDIMIENTO

- Fase de Planeación

Donde se toma una vista general de todo el espacio en general, y se realizaron recolección de pruebas, asesorías y todas las demás actividades que son correspondientes y pertinentes a esta fase, examinando las ventajas y desventajas con las que se cuenta.

En la presente fase se realizaron las siguientes actividades:

- Inspección de la Nueva Sede de la Universidad, para tener una vista general del entorno que se maneja a nivel físico.
- Consultar con administrativos y personal encargado de UNIMINUTO, de cuáles son las Políticas de Seguridad que existen o se manejan a nivel de red.
- Investigar modelos de redes administrables que se basen en servidores Mikrotik con autenticación Radius, para conocer el adecuado manejo de ellos, conociendo generalidades para tener en cuenta a aplicar en el desarrollo del proyecto.
- Investigar el flujo de usuarios posibles en la Nueva Sede.

- Fase de Análisis

Es la cual se reflexiono acerca de todos los posibles aspectos que se pueden usarse a la hora de crear esta innovación basándose en asesorías de cómo se podría realizarlo y en general investigar información que respalde y refuerce dicho concepto.

En la presente fase se realizaron las siguientes actividades:

- Investigación de manuales y tutoriales de creación y administración de redes inalámbricas, implementación de servidores Mikrotik que se pueden aplicar en el proyecto.
- Análisis y elección de herramientas de trabajo

- Búsqueda de asesoría en los diversos temas que se generen y requieran de la misma, teniendo la opinión de una persona que tienen experiencia en este tema.
- Consultar manuales de Diseño para implementar una interfaz amigable para usuario.

- Fase de Diseño

En esta parte se plasmó el diseño estructural a nivel lógico las políticas de seguridad y su implementación a nivel físico, innovando lo existente, teniendo en cuenta parámetros estudiados anteriormente en la fase de planeación.

En la presente fase se realizaron las siguientes actividades:

- Solicitud formal a la universidad de los planos de la Nueva Sede.
- Creación de planos independientes, de la estructura del edificio ubicando el lugar ideal de instalación del proyecto en la Universidad.
- Creación del diseño de la infraestructura de seguridad de la red inalámbrica.
- Creación de la metodología a seguir para la implementación física del proyecto

- Fase de Desarrollo

Aquí el proyecto tomo un curso real, nos proporcionara la posibilidad de aplicar la solución final, desarrollada previamente de una manera eficaz para el mejoramiento de los niveles administrativos de la red.

En la presente fase se realizaron las siguientes actividades:

- Implementación del diseño que se adapte a las necesidades y condiciones del entorno.

- Configuración la red de tal forma que cumpla las necesidades de innovación que se requieren.
- Realización de las pruebas necesarias durante el desarrollo de la red para detectando los fallos corrigiéndolos antes de finalizar el proyecto.

- Fase de Documentación

Esta fase se adiciona para brindar un manual de manejo general del prototipo desde el software Mikrotik como también del servidor Radius, tomando su instalación, configuración y mantenimiento del mismo brindado un soporte necesario para que el administrador o monitor de la universidad sepa que hacer en caso de algún percance.

En la presente fase se realizaron las siguientes actividades:

- Recolección de toda la información usada para la configuración e implementación del Mikrotik.
- Creación de un manual administrativo de usuario con la información seleccionada.
- Entrega en medio digital del manual en PDF y planos del proyecto debidamente corregidos.

5.4 ANALISIS DE LA SITUACION ACTUAL

- DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

La Nueva Sede de la Corporación Universitaria Minuto de Dios contaba con una red inalámbrica con la empresa ETB (Empresa de Telecomunicaciones de Bogotá) con MODEM+ROUTER WI-FI 802.11G (54 MBy) ADSL 2+ con 4 puertos de salida RJ45, marca HUAWEI EchoLife HG520b, la persona propietaria que solicito la línea fue el Ingeniero Mauricio Mora, quien estuvo a cargo en el transcurso de la construcción de la Sede, solicito la línea para mantener conectado en el lugar; la línea paso a ser manejada y pagada por la universidad sin ninguna infraestructura compleja, solo el modem que se encuentra ubicado en una de las oficinas que están remodelando en Universidad.

Imagen. 1

Pero este servicio solo brindaba cobertura al sector de la cafetería y los salones 1 desde afuera.

Imagen. 2

La persona que estaba encargada del manejo del acceso a la red era el Ingeniero Juan Murillo quien administra la contraseña para comunidad académica en la Universidad.

Imagen. 3

Quien nos informó que la red inalámbrica contratada presentaba problemas de tierra, con lo que se perdía el internet por días, y se tiene que llamar a servicio técnico a ETB para que hagan la revisión correspondiente, que dura por unos días bien y vuelve a presentar problemas nuevamente.

Imagen. 4

En la mayoría de los casos no había internet con los constantes problemas de tierra que se presentan por los cambios de clima.

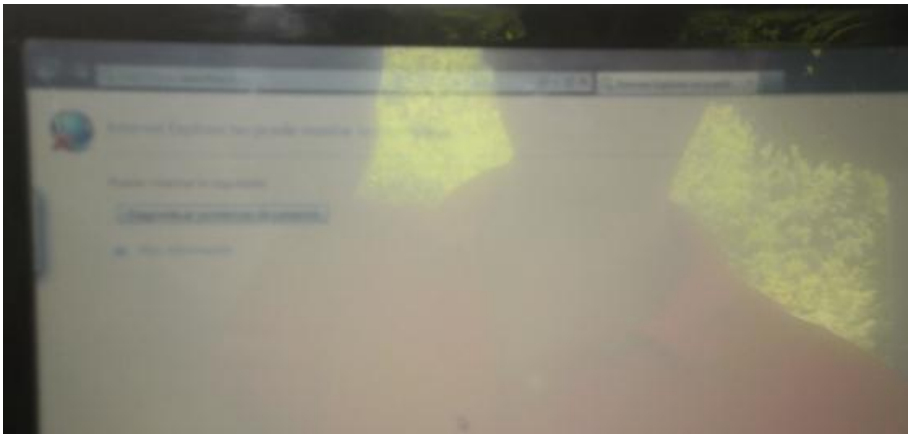


Imagen. 5

Según las recolección de datos en la universidad, aunque la red funcionaba en forma irregular, ahí un flujo regular de estudiantes con portátiles que ingresan a la sede. Con solo una toma en la cafetería para poder conectar el portátil si se queda sin batería.

Imagen. 6

La mayor parte de los estudiantes tiene su propio modem para poder tener el servicio de internet.

Imagen. 7

Los lugares que son de concurrencia en la sede son la biblioteca y las terrazas, pero lamentablemente no tenían la cobertura del servicio a acceso a internet.

Imagen. 8

Imagen. 9

Además estos sitios si tienen toma eléctrica especial a las cuales conectar los portátiles cuando se les acaba la batería, siguiendo las normas para exteriores.

Imagen. 10

En resumen la mayoría de los salones en todo el edificio de la universidad estaban sin la cobertura de la red inalámbrica.

Imagen. 11

Pero en la actualidad este MODEM ya no está en funcionamiento puesto que la línea fue cancelada por la universidad, aunque una no han recogido el equipo.

Imagen. 12

La universidad instalo una red para los profesores y administrativos, tanto cableada como inalámbrica (como se muestra en la imagen 13), los equipos están instalados en el segundo piso del edificio, uno en el salón de profesores (como se muestra en la imagen 14) y el otro en salón de coordinadores (como se muestra en la imagen 15).

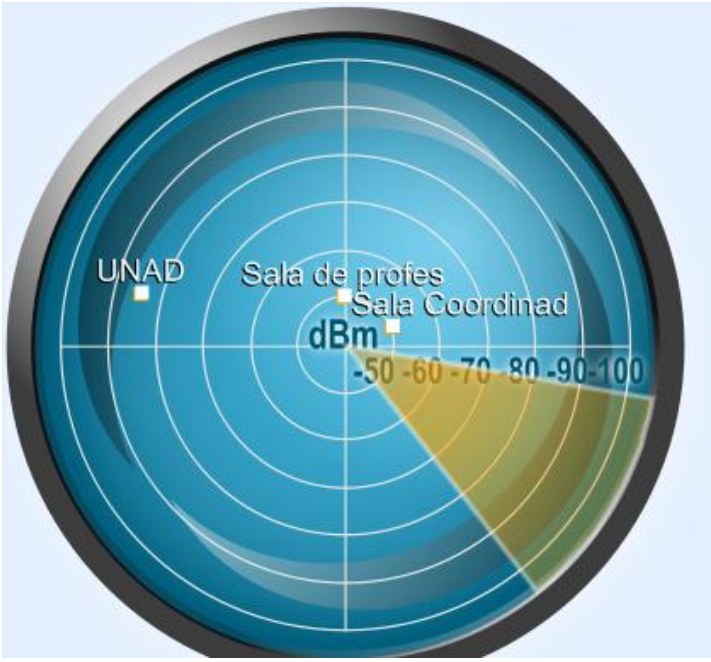


Imagen. 13

Imagen. 14

Imagen. 15

Pero los estudiantes de la universidad no tienen acceso a ellas puesto que están con clave.

5.5 DISEÑO DE LA SOLUCIÓN PROPUESTA

- DESCRIPCION DE PROCESOS DEL SISTEMA PROPUESTO

Observando la problemática actual de la Comunidad Académica en la Nueva Sede de la Corporación Universitaria Minuto de Dios, con respecto a su red inalámbrica de internet, se desarrollaron unas propuestas de las cuales se elegirá la más partica, cumpliendo con lo que se desea emplear y que será implementada por los alumnos desarrolladores del proyecto como prototipo.

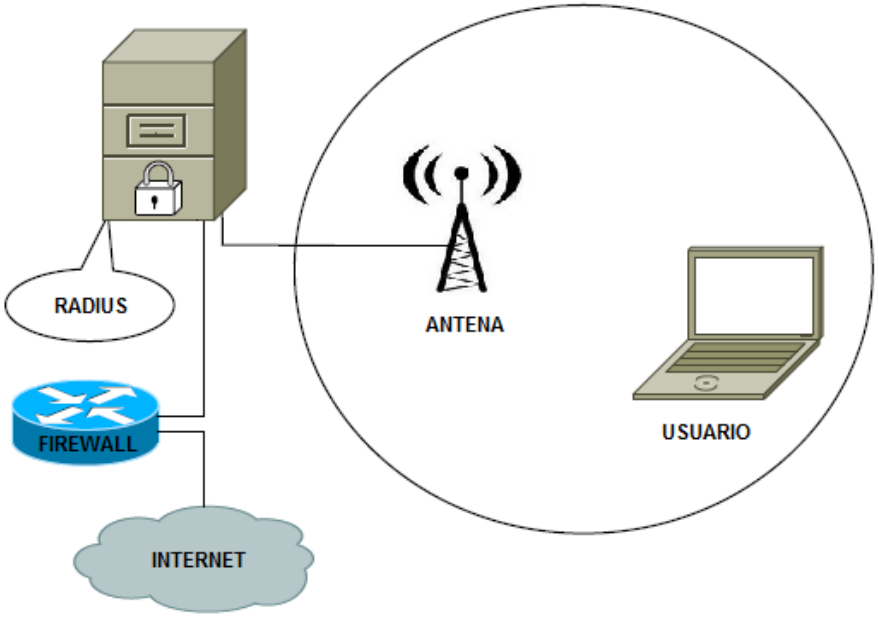


Imagen 16. Diseño del prototipo 1

Maneja un firewall que realiza el filtro de contenido y bloque de páginas en la red inalámbrica y que con ayuda de servidor Radius como es Freeradius que se instala en un sistema operativo Linux realiza la autenticación en la red. El total de costos de los equipos incluirían el router y una antena de alta potencia, con un total de $700.000 mil pesos que sería muy costoso y más complicado de su configuración.

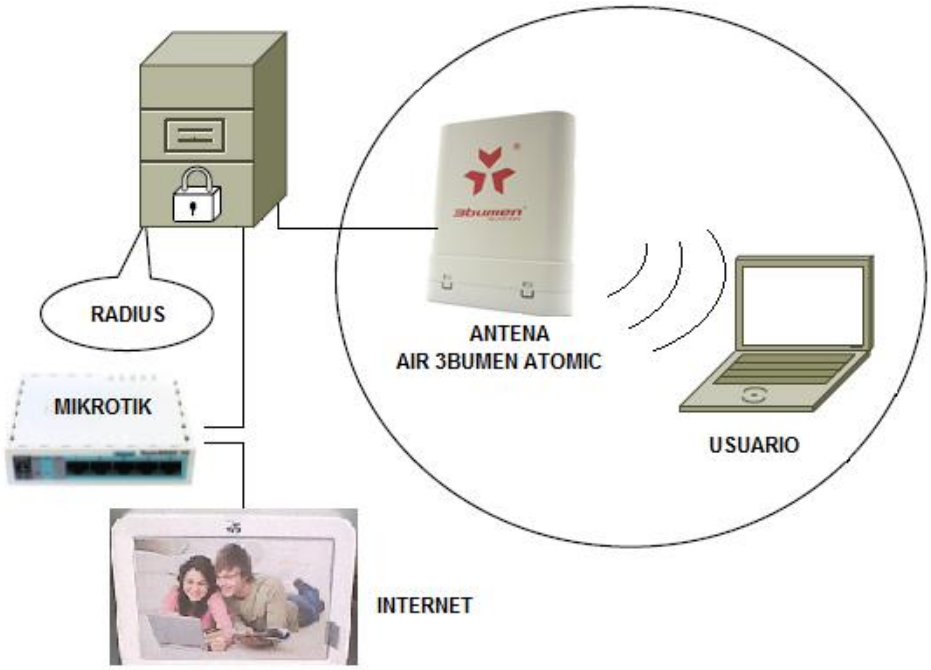


Imagen 17. Diseño del prototipo 2

Este diseño consta de un Mikrotik que y una antena para exteriores, que con un servidor Radius realizan la autenticación y bloqueo que se quiere realizar en la red. El costo total del diseño incluye la compra de la antena y del mikrotik el total seria $500.000 mil pesos un costo alto y mucha más configuración.

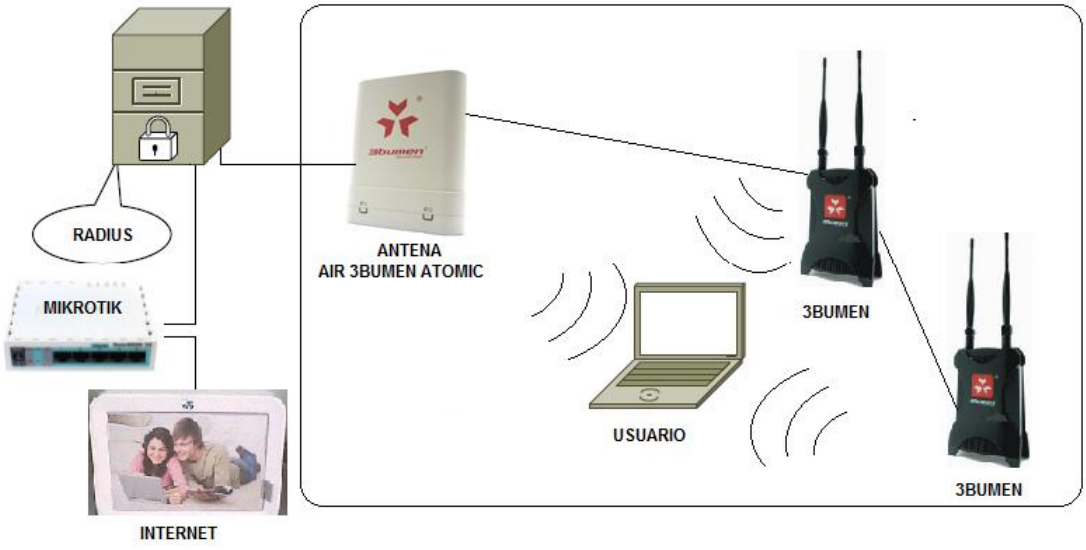


Imagen 18. Diseño del prototipo 3

Este fue el diseño completo que se le presento a la universidad para dar cobertura a toda la universidad que tenía un costo total de 2’000.000 de pesos el cual fue rechazado para ser implantado en la misma.

Por ultimo encontramos una propuesta que consiste es un prototipo que consta de un servidor MIikrotik que tiene integrado un radius, el cual se encargara de la autenticación de usuarios mediante un usuario y una clave que se manejara, además administrara la red y se configurara con las políticas de navegación que la universidad quiera manejar para la comunidad académica, por ultimo encontramos la antena 3-bomen atomic air con alcance de una kilometro a la redonda que servirá como hotspot(punto caliente o punto de acceso frecuente) por donde podrá acceder la comunidad estudiantil (como lo muestra la imagen 19). Que al cumplir con todos los servicios que requerimos y su costo total es de $300.000 mil pesos, es la solución q más se acomoda a dicha necesidad.

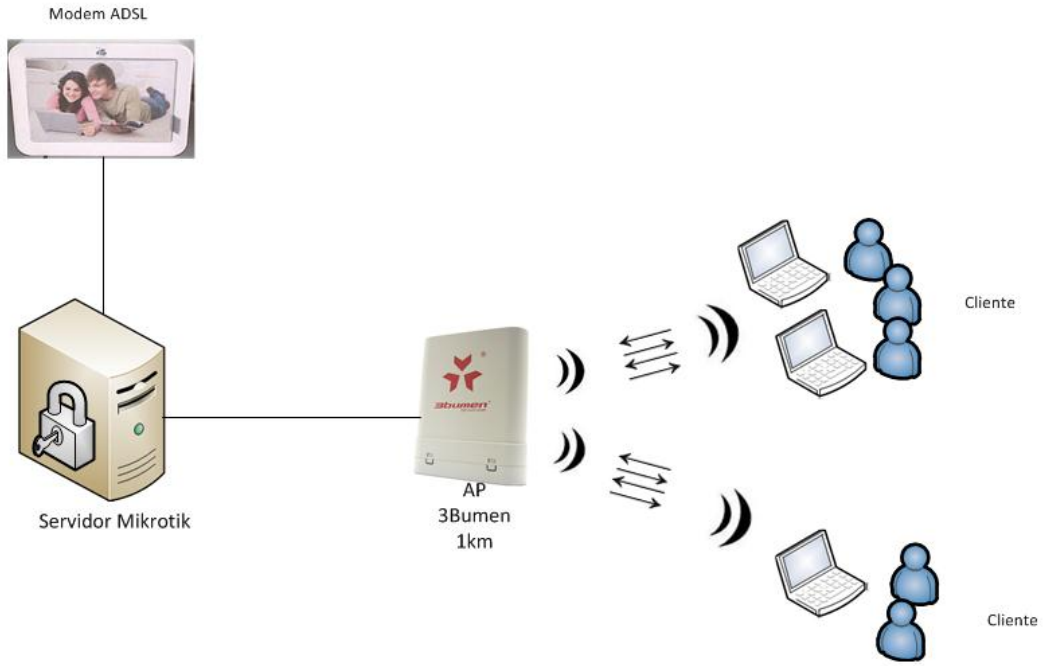


Imagen 19. Diseño del prototipo 4

El diseño consta de montar la red inalámbrica en la Sede Nueva de la Universidad mediante hotspot o (punto caliente), el cual es un A.P. (punto de acceso) en el cual circula todo el flujo la red el area de cobertura. Para crear este hotspot se utilizara un AP CPE ROUTER ATOMIC AIR para exteriores marca 3BUMEN, de un alcance de 1 Km, con 2 antenas de 12dBi cada una y una velocidad de hasta 300 Mbps (como se muestra en las imágenes 20,21 y 22).

Imagen 20. AP

Imagen 21. Interior del AP

Imagen 22. AP vista posterior

Este AP se configura por medio de una interfaz WEB en el navegador y viene con el idioma español por defecto, con una IP: 192.168.1.2 y actuara como puente en su modo de operación:

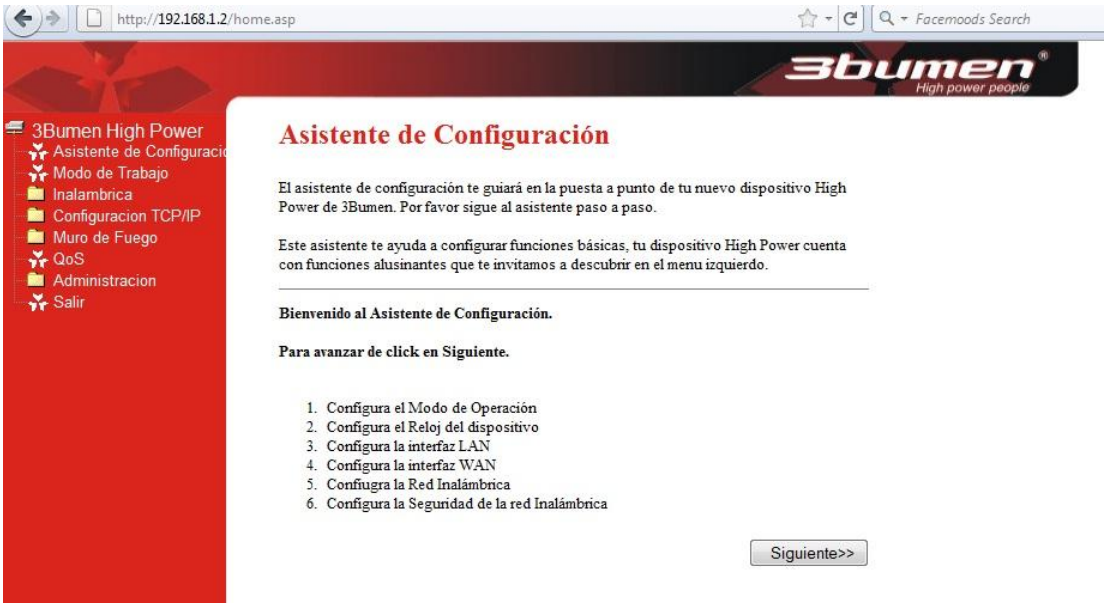


Imagen 23

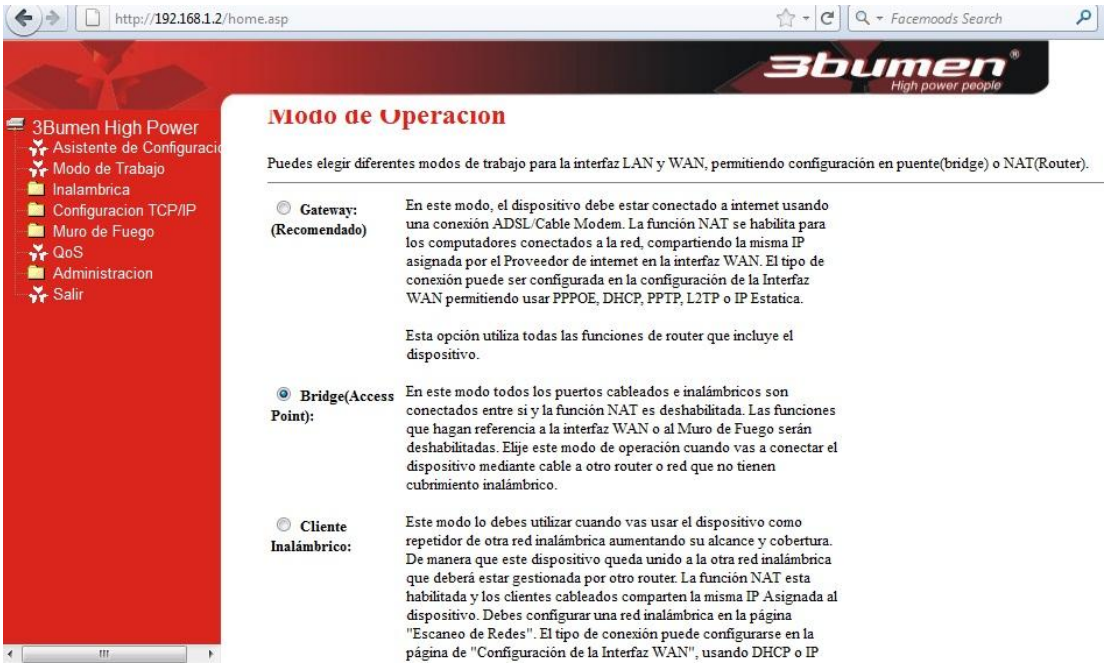


Imagen 24

Imagen 25

Imagen 26

Este A.P. funcionará apoyado y administrado por un servidor mikrotik, para el servicio, comodidad y seguridad de la comunidad, en otras palabras más exactas; El hotspot actuara como punto de acceso para que la comunidad académica pueda conectarse a través de él.

Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Pero todo realizan la misma función autenticación, que se hace al momento de acceder, para nuestro proyecto será por medio de un usuario y la clave será una clave general que se cambiara cada semestre de esta parte se encargara el Mikrotik.

La metodología de acceso que se usara el usuario será una secuencia de pasos:

1. Primero el usuario envía su usuario/contraseña. Esta información es encriptado con una llave secreta y enviada en un access-request al servidor radius (Fase de autenticación).

2. Cuando la relación usuario/contraseña es correcta, entonces el servidor envía un mensaje de aceptación, access-accept, con información extra (Fase de autorización).

3. Tercero el usuario ahora envía un mensaje de accounting-request (Start) con la información correspondiente a su cuenta y para indicar que el usuario está reconocido dentro de la red (Fase de accounting).

4. El servidor radius responde con un mensaje accounting-response, cuando la información de la cuenta es almacenada.

5. Cuando el usuario ha sido identificado, este puede acceder a los servicios proporcionados. Finalmente cuando desee desconectarse, enviará un mensaje de accounting-request (Stop).

6. El servidor radius responde con un mensaje de accounting-response cuando la información de cuenta es almacenada.

Mikrotik este dispositivo servirá para la administración de la red desde filtros de contenidos, bloque de páginas de descargas y de Chad, calidad de servicio, entre otros servicios que trae este para el mejor desempeño de la red.

Para ello se necesita un equipo de cómputo dedicado a exclusivamente para el servidor Mikrotik con las siguientes características técnicas para tener un servidor con óptimo funcionamiento:

CANTIDAD	DECRIPCION
1	COMPUTADOR (PENTIUM 4, CON 1GB DE RAM Y MÍNIMO 50GB DE ESPACIO EN DISCO DURO).
1	TARJETA DE RED
2	CABLES CRUZADOS
1	CABLE DIRECTO

Tabla 2: Detalles Técnicos

Además que además maneje dos tarjetas de red (como se muestra en la imagen 16) y otro computador con el cual se hará configuración de Mikrotik a través de una herramienta llamada Winbox (como se muestra en la imagen 17).

Imagen 27. Tarjeta de red

Solo es necesario comprar una puesto que el computador tiene integrada en la board.

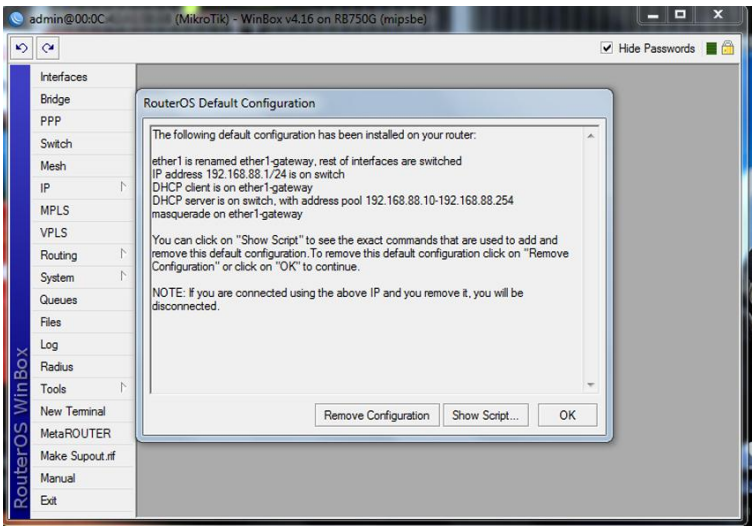


Imagen 28. Winbox

Al accesar al Winbox configuramos nuestro servidor Mikrotik de acuerdo a las pautas que se manejen en la universidad, para el desarrollo y aplicación de este proyecto la universidad nos brindó un puerto de internet en la biblioteca para ponerlo a prueba mientras obtiene un equipo en el cual instalar el servidor, con la configuración que se usa en la red tanto de la IP: 10.10.11.180 como el proxy: 192.168.101.7, DNS: 10.0.0.3 y la Puerta de Enlace: 10.10.11.1 que se maneja, puesto que todo el acceso se maneja directamente desde Bogotá en la sede central. Además se selecciona y configura un Pool de direcciones: 192.168.1.2:192.168.1.254, el cual manejara la tarjeta de red que va a la antena repartiendo automáticamente cuando acceda a la red el usuario.

CONFIGURACION

Antes de nada, descargamos el Winbox (herramienta gráfica para configurar RouterOS) en este enlace se puede descargar este programa: http://www.mikrotik.com/download/winbox.exe.

Al descargarlo conectamos un cable UTP cruzado al puerto de un PC y la otra una de las tarjetas de red de equipo en donde instalamos Mikrotik. Luego conectamos otro cable UTP cruzado desde la otra tarjeta de red al puerto de la antena.

Abrimos Winbox y nos saldrá una pantalla como esta:

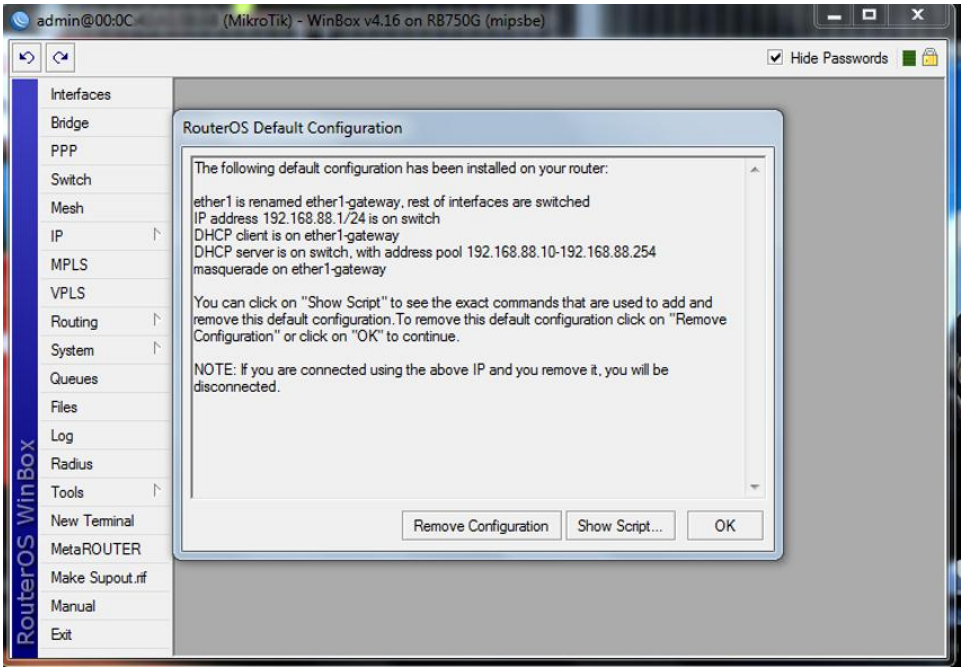


Imagen 29

Uno de los primeros pasos es nombra las interfaces a nuestro gusto, para ello hacemos click en Interfaces se abrirá el cuadro don están todas las interfaces con las que trabaja actualmente el servidor Mikrotik.

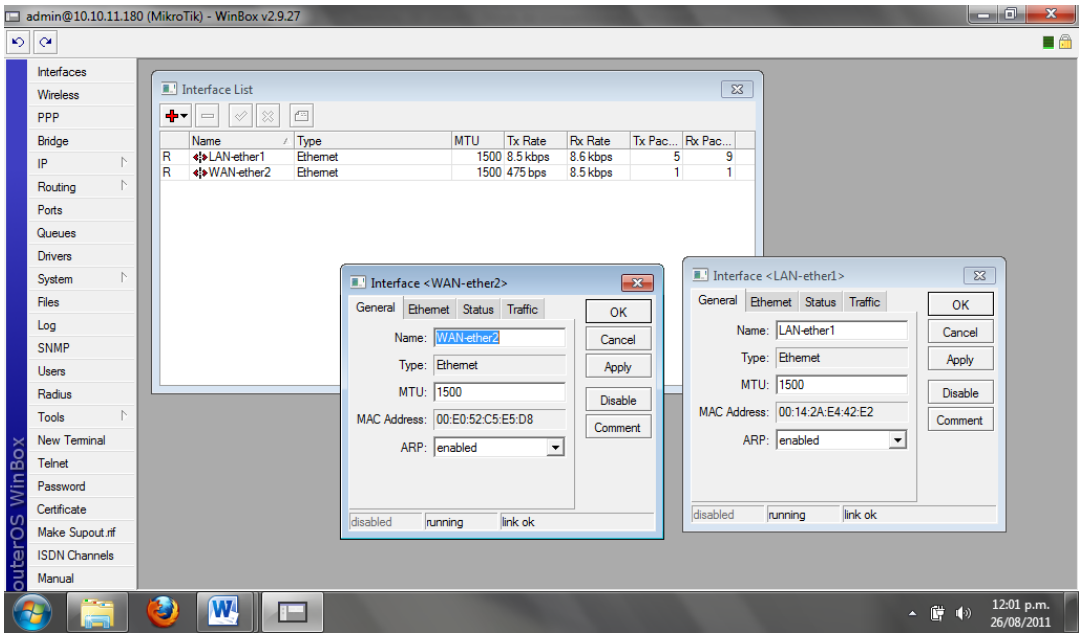


Imagen 30

Nos dirigimos a IP>>Address verificamos y agregamos las IP que haces fatal por configurar

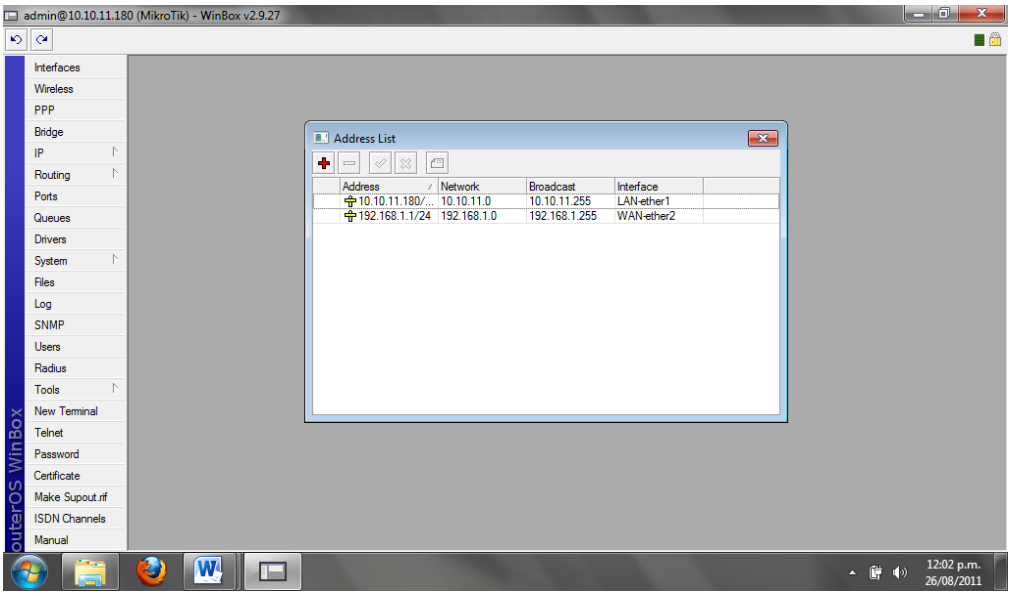


Imagen 31

Luego nos dirigimos a IP>>Firewall seleccionamos la pestaña NAT luego hacemos click en el signo '+', damos click en la pestaña Action y en el menú desplegable colocamos la opción masquerade y damos aceptar

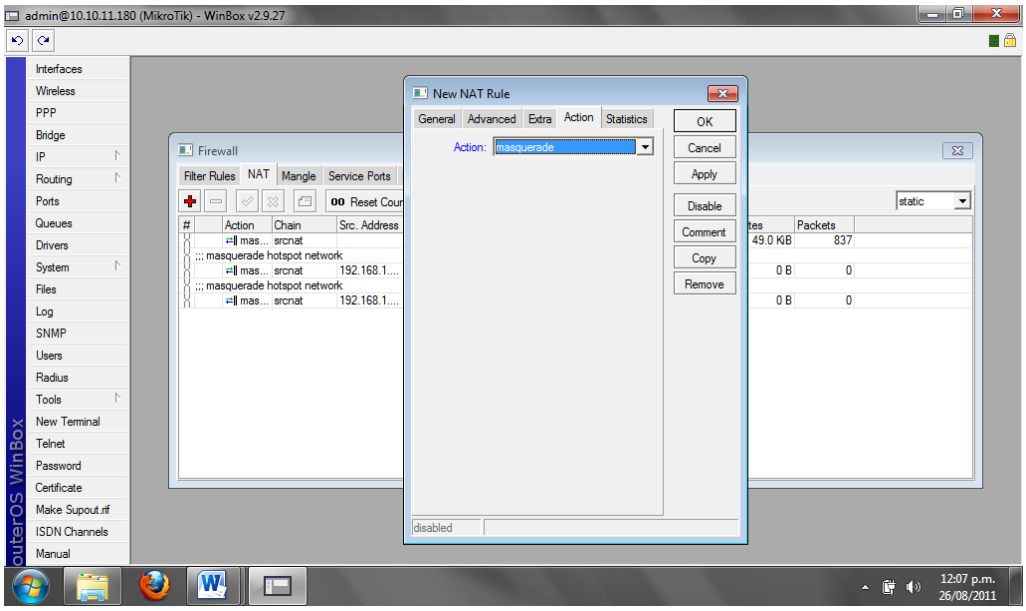


Imagen 32

Luego nos dirimos a IP>>Pool selescionamos el '+' y ahí nos aparece un menu donde damos un nombre al pool de direcciones y colocamos su respectiva IP inicial y su respectiva IP final.

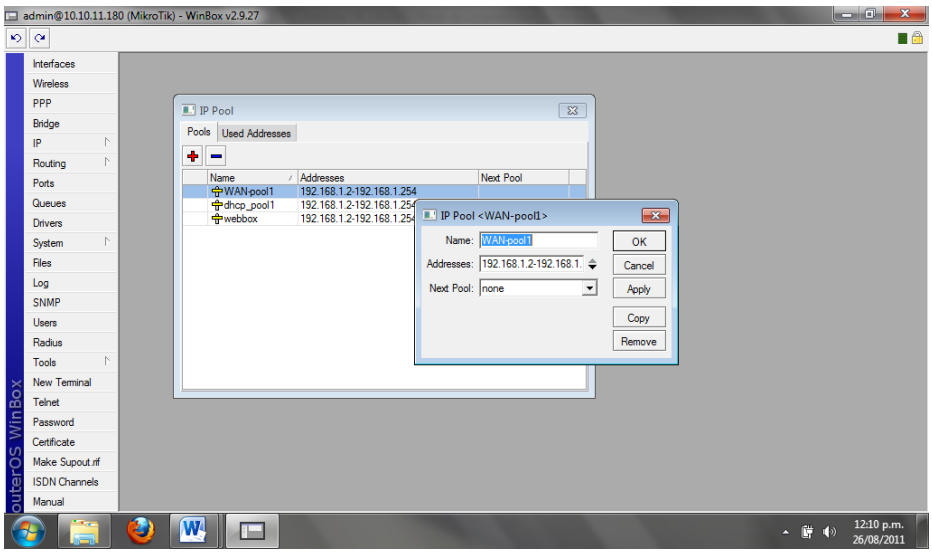


Imagen 33

Después nos dirigimos a IP>>Routes y ahí colocamos la puerta de enlace de la Ip que maneja el internet

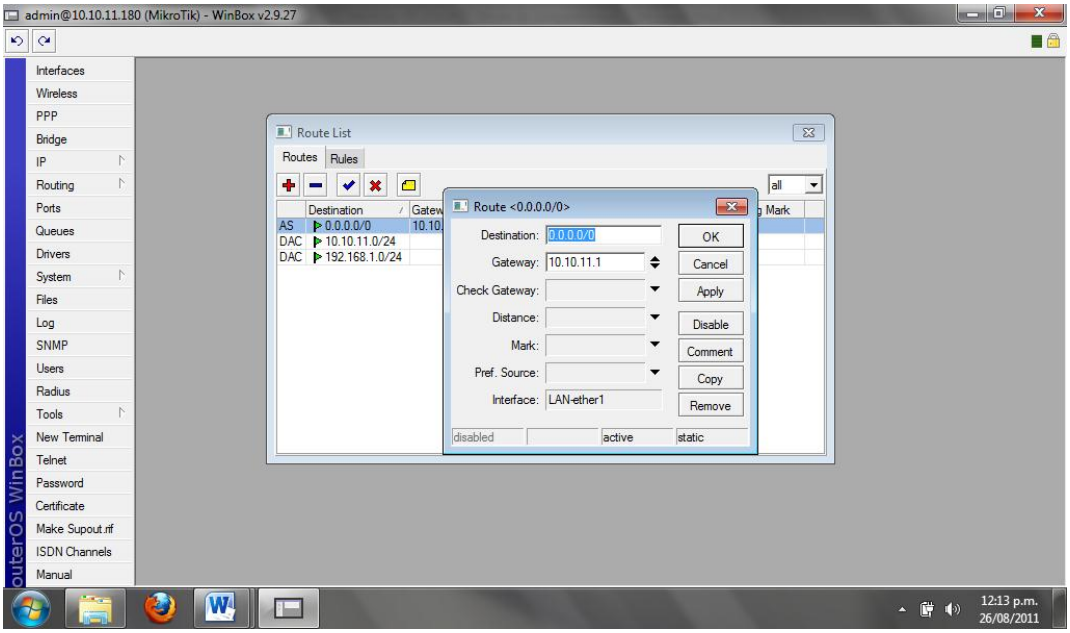


Imagen 34

Ahora nos dirigimos IP>>DNS y colocamos el DNS que maneja la red del internet

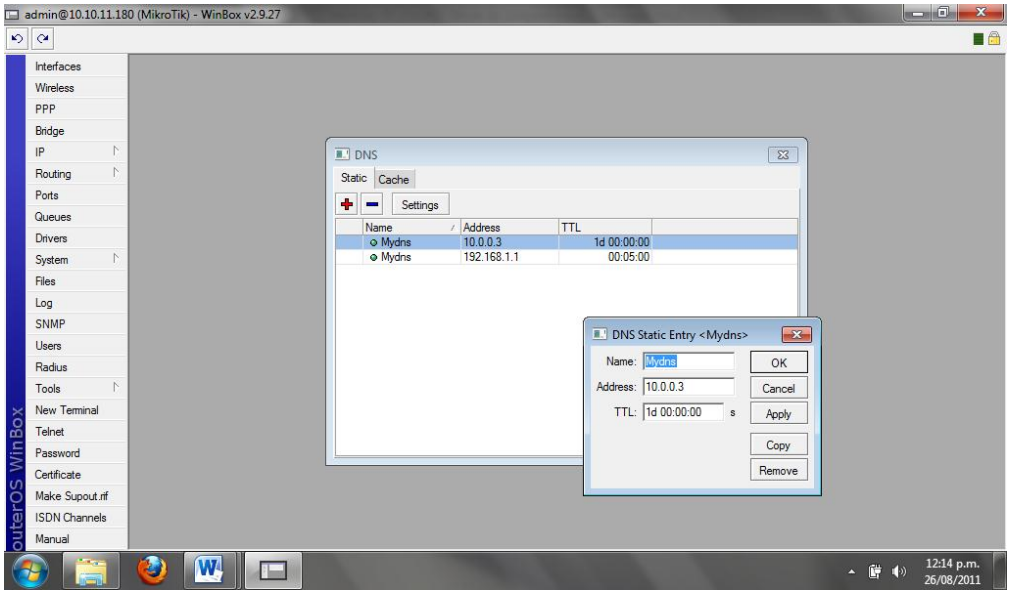


Imagen 35

Ahora vamos a configurar el servidor DHCP de la interfaz de nuestra antena, para que entregue direcciones IP a todo equipo que se conecte por esa boca. Nos dirigimos a IP>DHCP Server y damos click en DHCP Setup.

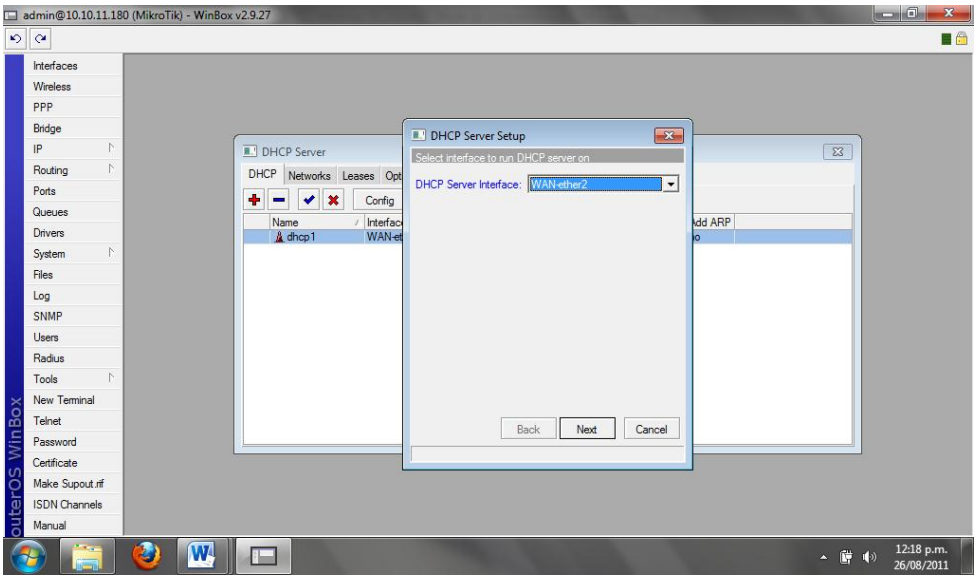


Imagen 36

Seleccionamos la interface que configuramos para la salida a internet por cable, en mi caso WAN ether2.

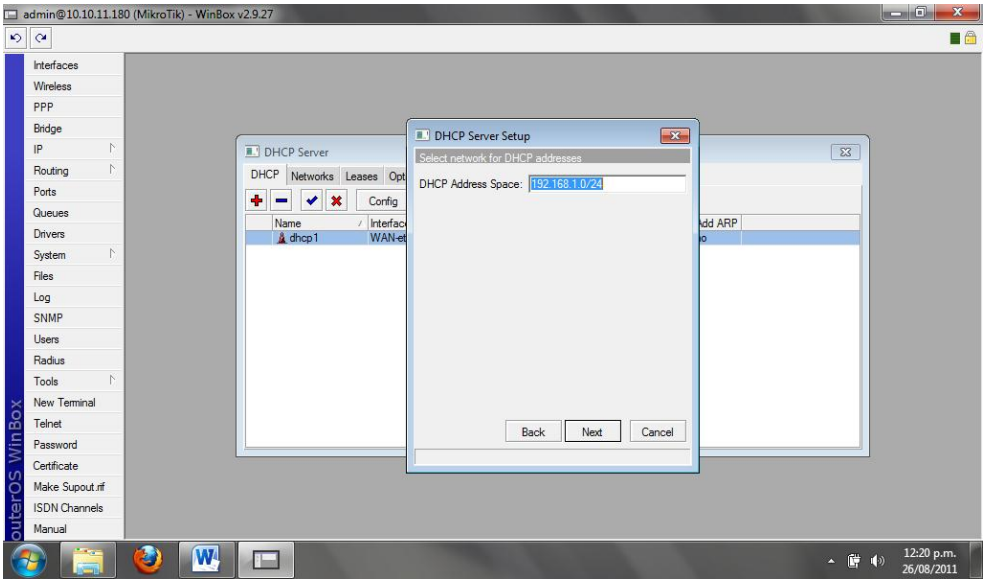


Imagen 37

Ahora seleccionamos el rango de direcciones IP que queremos entregar por la

WAN ether2, en este caso he seleccionado el rango 192.168.1.0/24, esto quiere decir que entregaré 255 IP del tipo 192.168.1.x

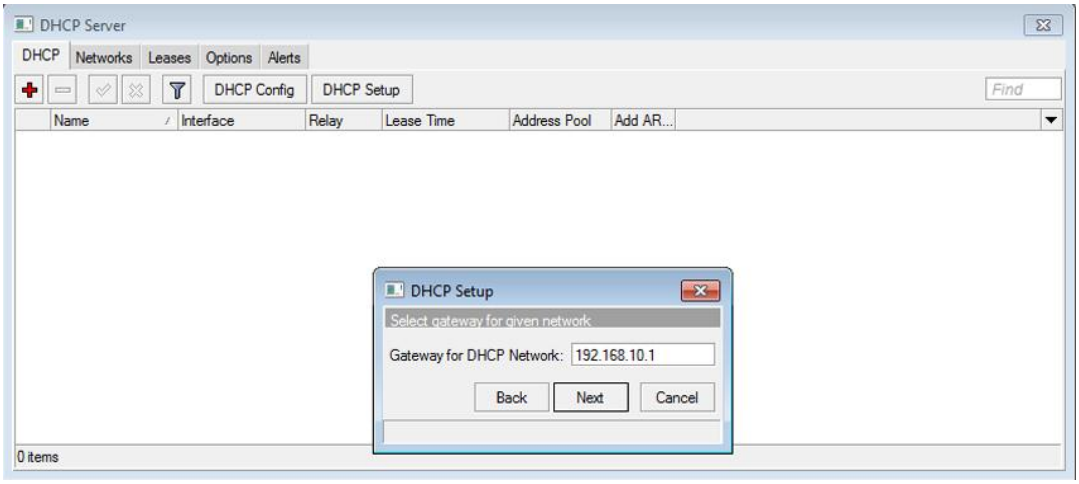


Imagen 38

La puerta de enlace os aparecerá de forma automática.

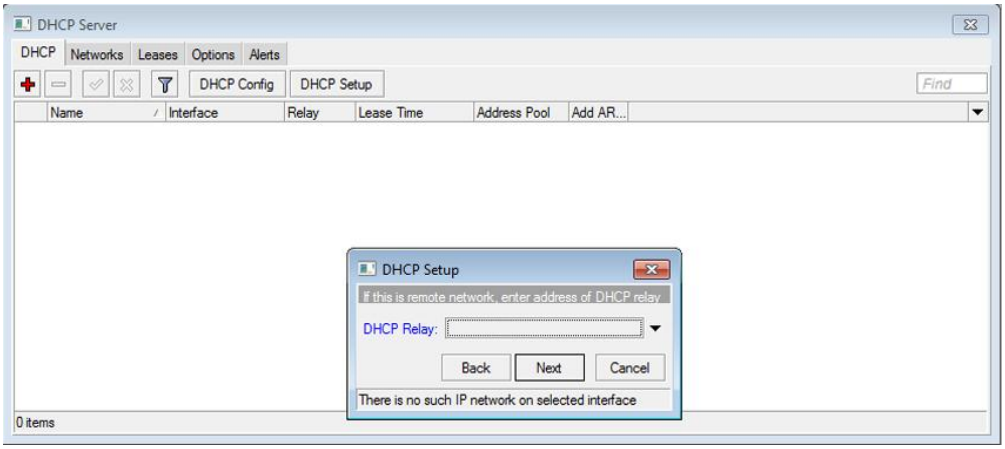


Imagen 39

El DHCP Relay lo desactivamos pulsando en la flecha negra hacia arriba.

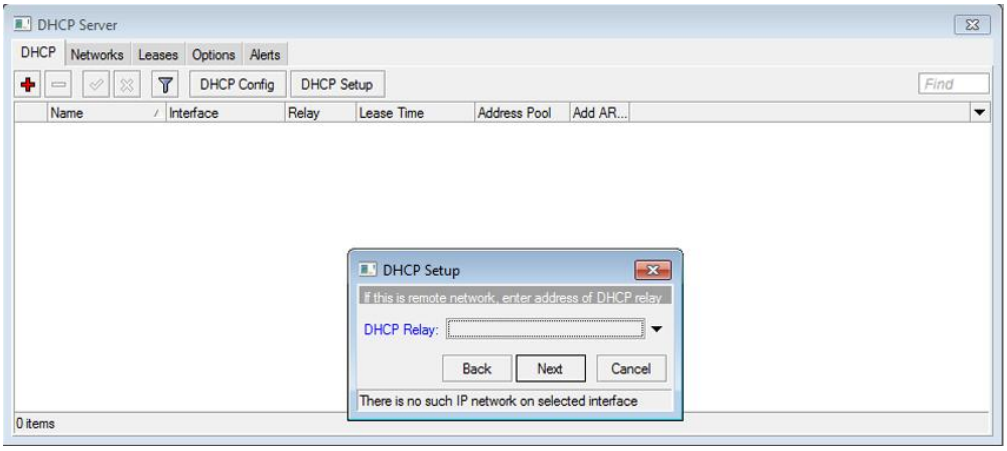


Imagen 40

Aquí tienes lo del rango de IP, entregaremos 255 IP, desde la 192.168.1.2 hasta la 192.168.1.254

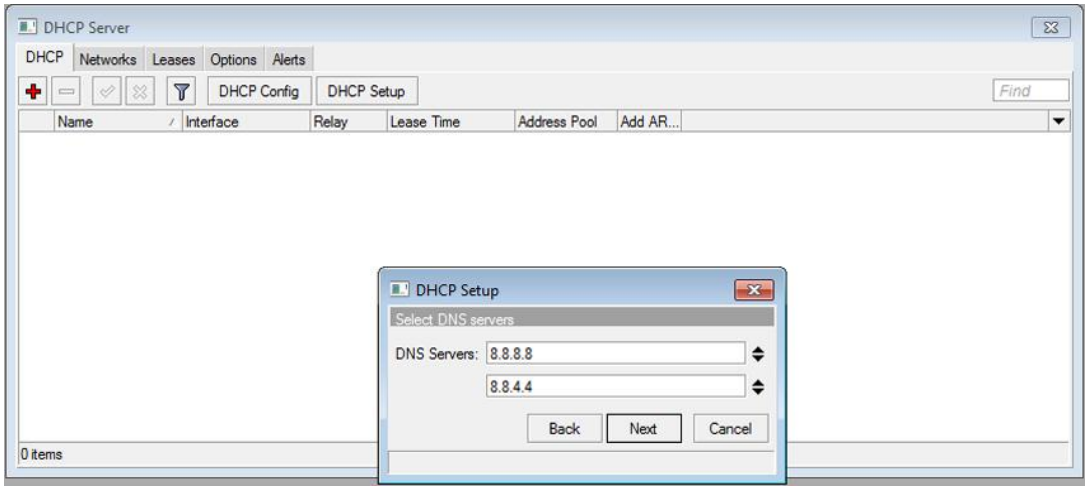


Imagen 41

Aquí las DNS, os saldrán automáticamente, ya que las hemos configurado anteriormente.

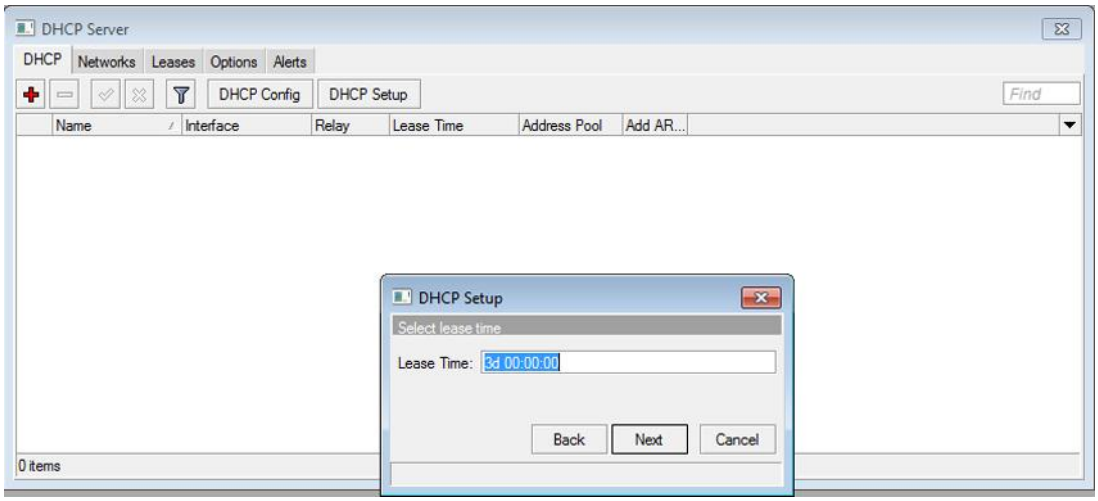


Imagen 42

Lease Time lo dejamos por defecto y seguimos.

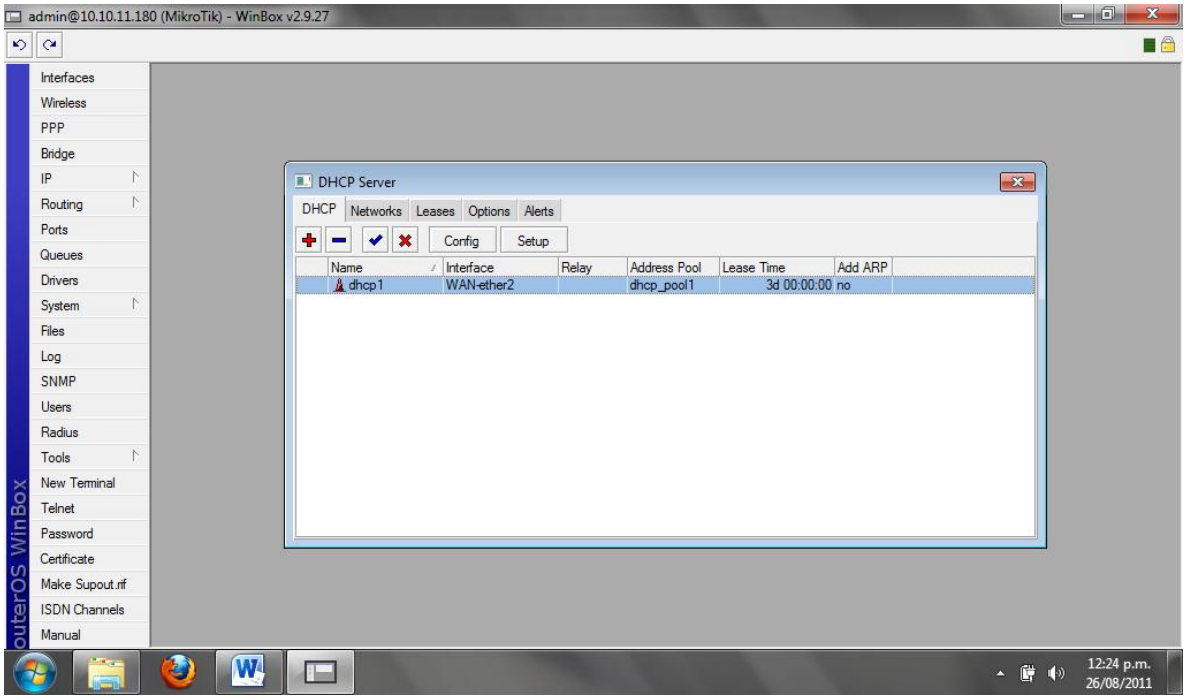


Imagen 43

Ylisto quedoconfigurado nuestro servidor DHCP

Después vamos a crear el Hotspot vamos a IP>Hotspot y damos click en Hotspot Setup.

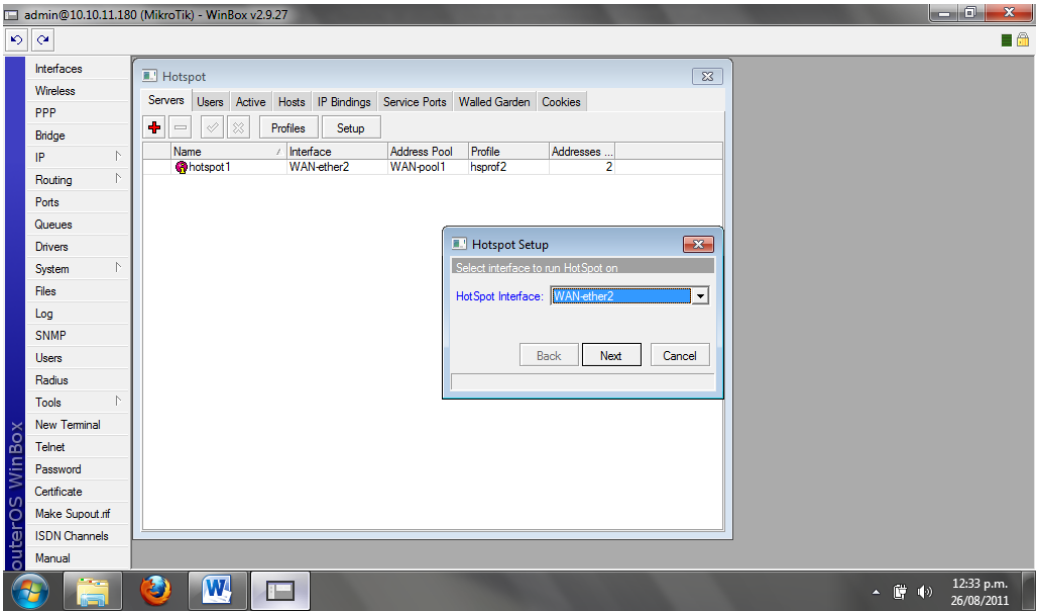


Imagen 44

Elegimos la interface que creamos al principio para el Hotspot.

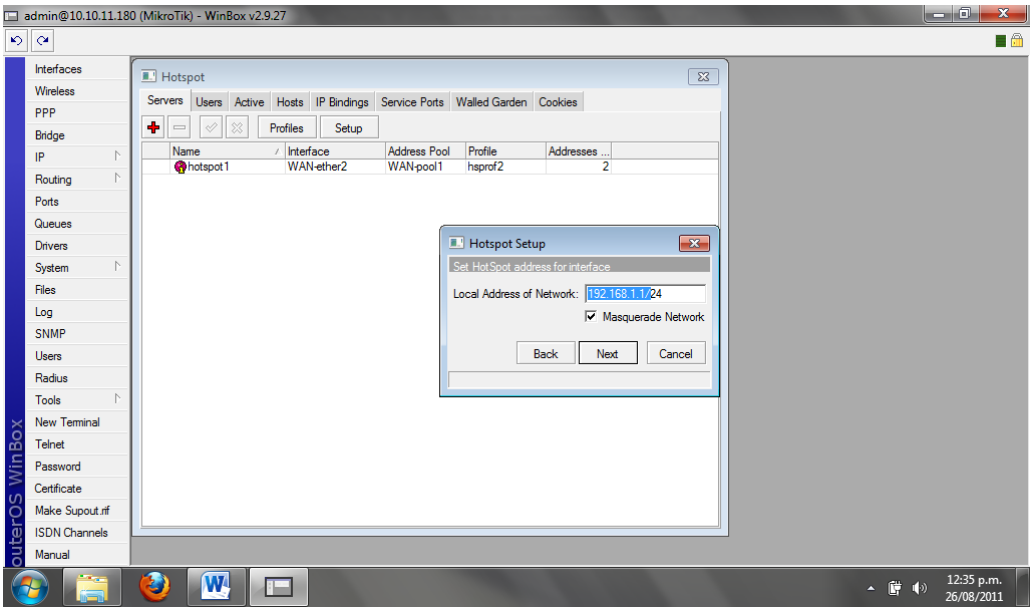


Imagen 45

Elegimos el rango de IP que queremos que de nuestro Hotspot, y le damos a la opción Masquerade Network.

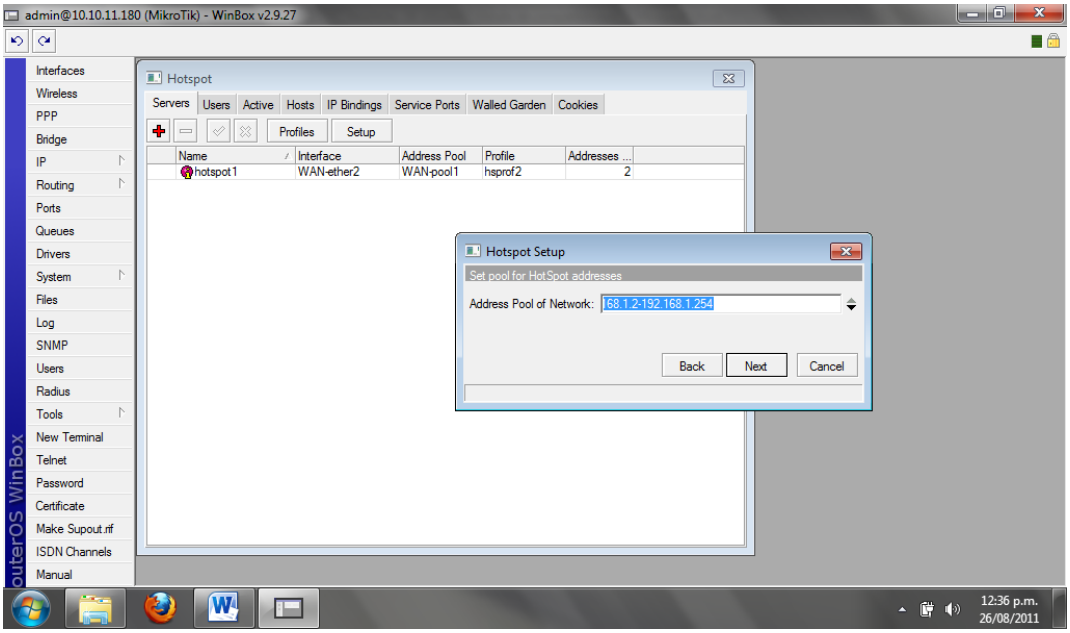


Imagen 46

Aquí tienes el rango de IP que va a entregar vuestro Hotspot, en mi caso entregará hasta 255 IP desde la 192.168.1.2 hasta la 192.168.1.254.

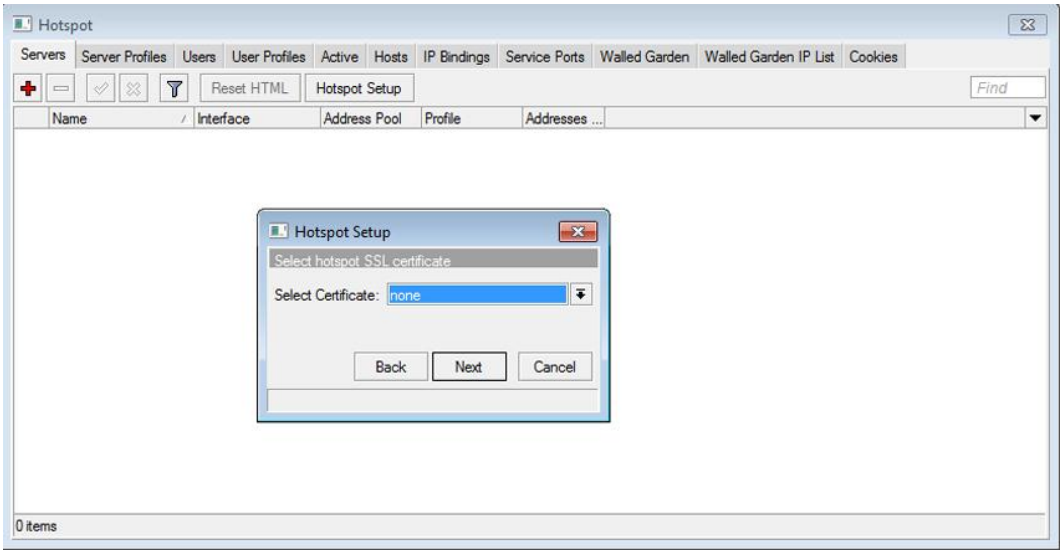


Imagen 47

Dejamos la opción por defecto none y continuamos.

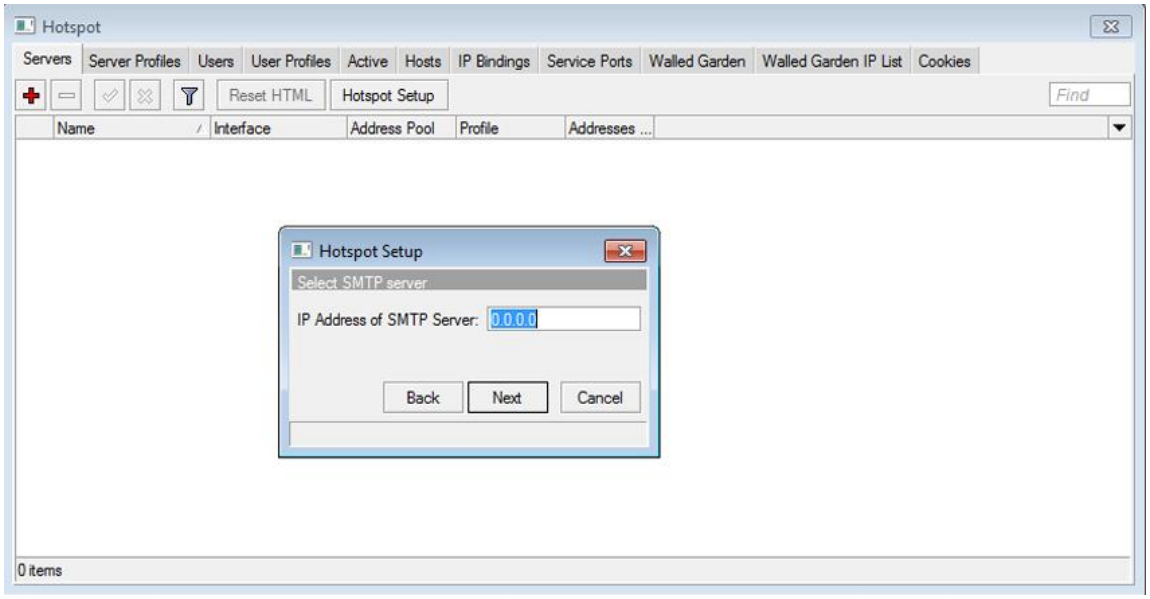


Imagen 48

Opción por defecto y seguimos, ya falta menos.

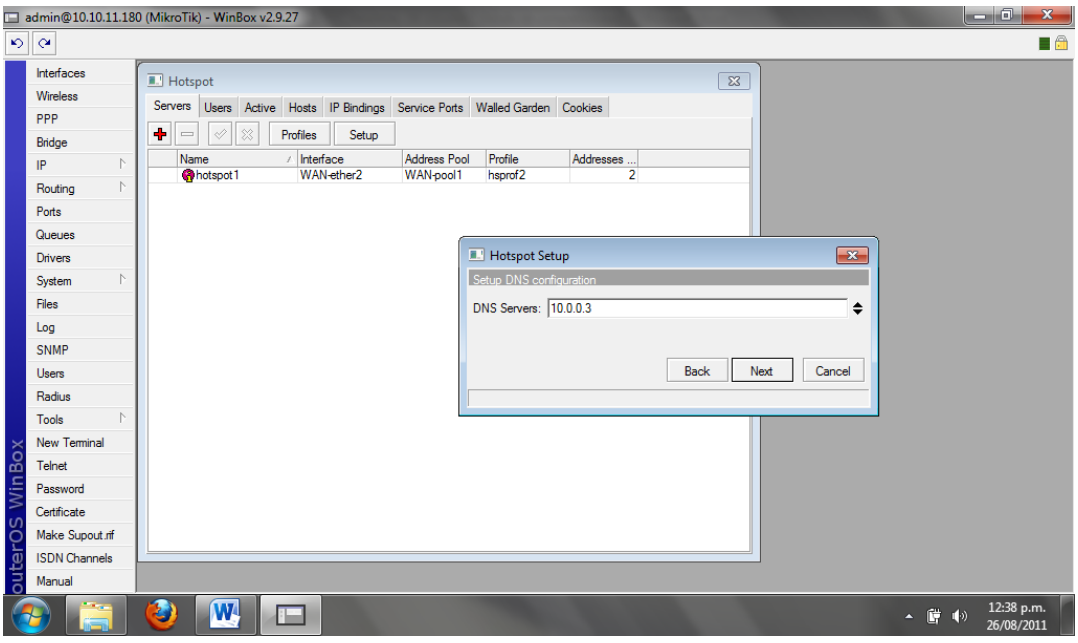


Imagen 49

Las DNS saldrán automáticamente, ya que las teníamos configuradas de antes.

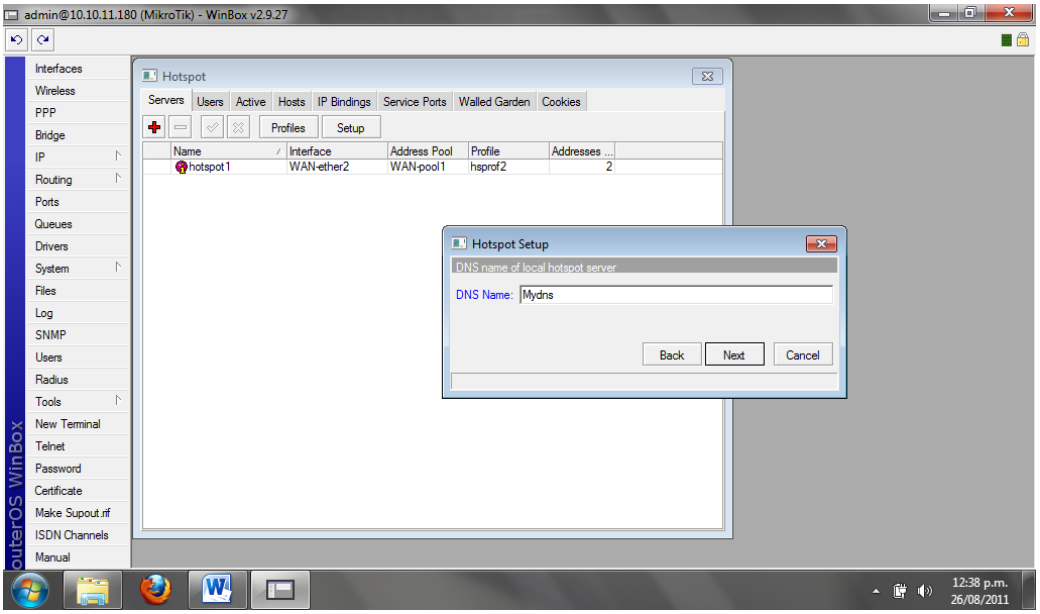


Imagen 50

En DNS Name ponemos cualquier nombre, es la página interna del Hotspot a la que nos redirecciona al intentar conectarnos a internet.

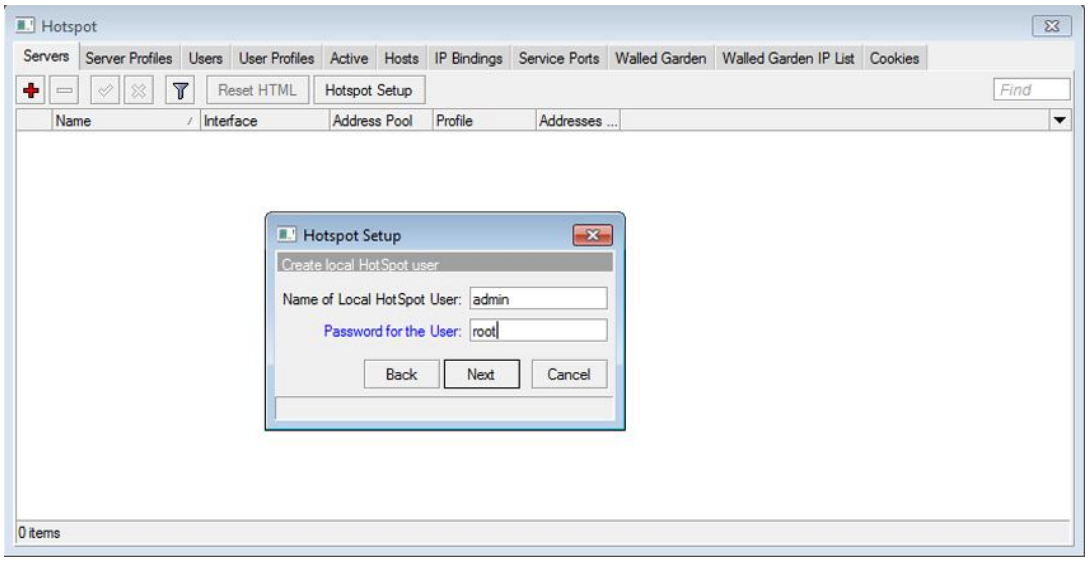


Imagen 51

Este usuario que no tendrá limitaciones al navegar por el Hotspot

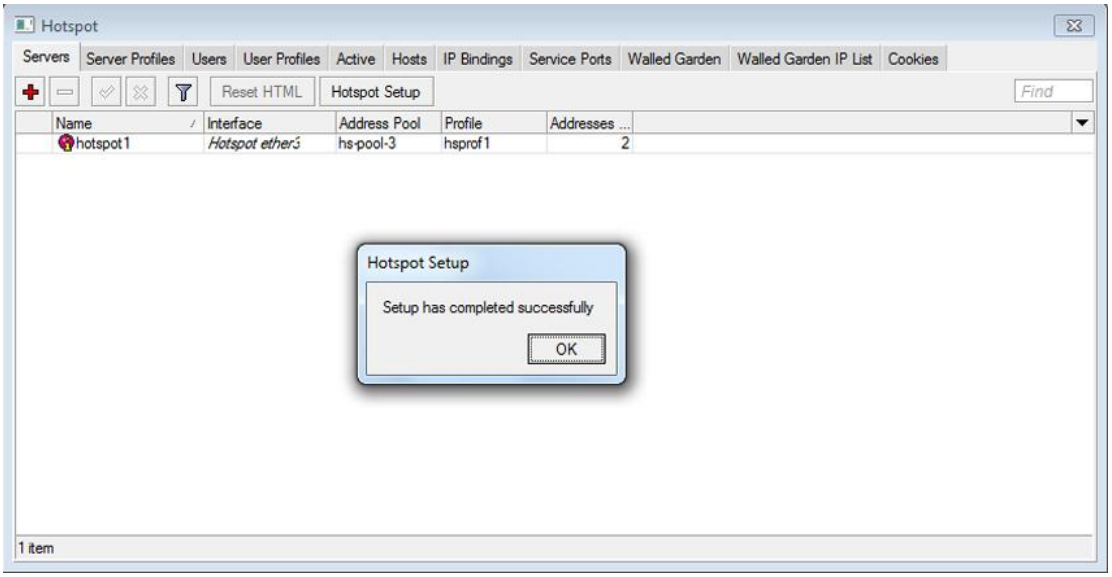


Imagen 52

Ya hemos creado nuestro Hotspot.

Ahora vamos a crear usuarios, para ello IP>Hotspot>Users

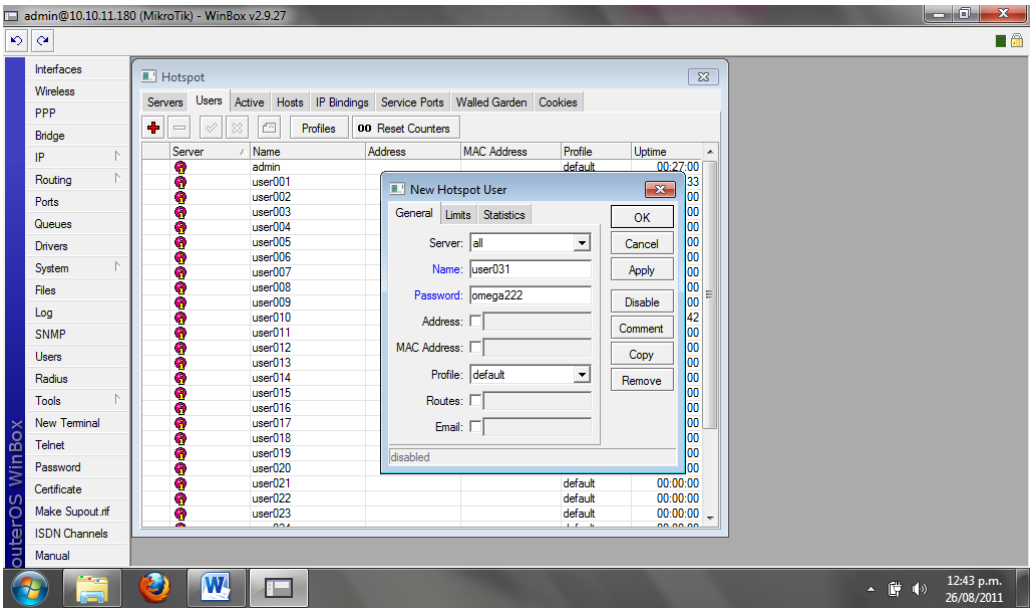


Imagen 53

Aquí he creado un usuario de nombre user031, con una contraseña

Para cambiar la interfaz de autenticación que nos arroja Mikrotik por defecto nos dirigimos a Files copiamos la carpeta entera de hotspot en el escritorio de nuestro pc y la modificamos a nuestro gusto cuando ya la tenemos lista entramos de nuevo a files borramos todo los archivos hasta q quede en blanco y copiamos la misma carpeta con las modificaciones. Por seguridad de la configuración se le coloco una clave al servidor: “IngridyDiego123456789”.

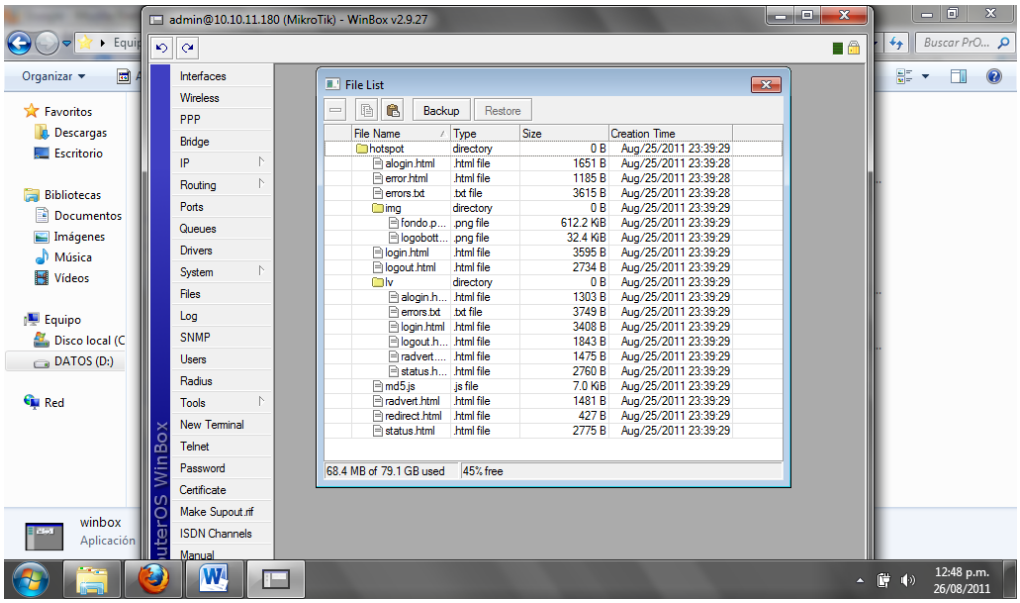


Imagen 54

Para probar la efectividad del servicio que queremos brindar a la comunidad, repartimos estos usuarios con sus contraseñas correspondientes y enseñamos como utilizar este servicio, puesto que el puerto es de la red académica, utiliza el proxy que también se tiene que configurar en el navegador (como se muestra en proxy) y al solicitar un página en el navegador, automáticamente se redirecciona a la página de inicio de nuestro servidor la cual solicita el usuario y la clave (como se muestra en Interfaz), teniendo presente que la sesión de cada usuario solo se puede efectuar una sola vez, no permitiendo sesiones múltiples, ni errores al introducir el usuario y la clave que sea incorrectamente (en caso de que sea alguno de estos errores en la parte de abajo saldrá un mensaje en rojo de cuál fue el error que ocurrió) y son correctos los datos introducidos de automáticamente entra a la página que solicito el navegador, claro está si esta no está bloqueada por el proxy.

Imagen 55

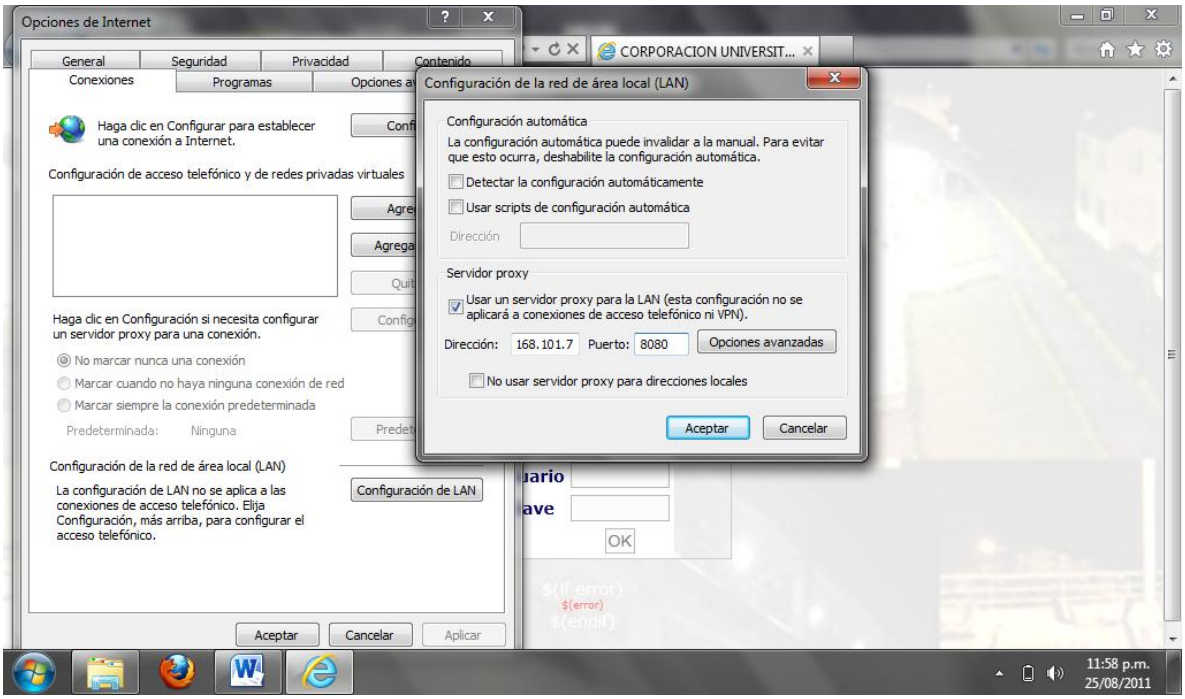


Imagen 56. Proxy

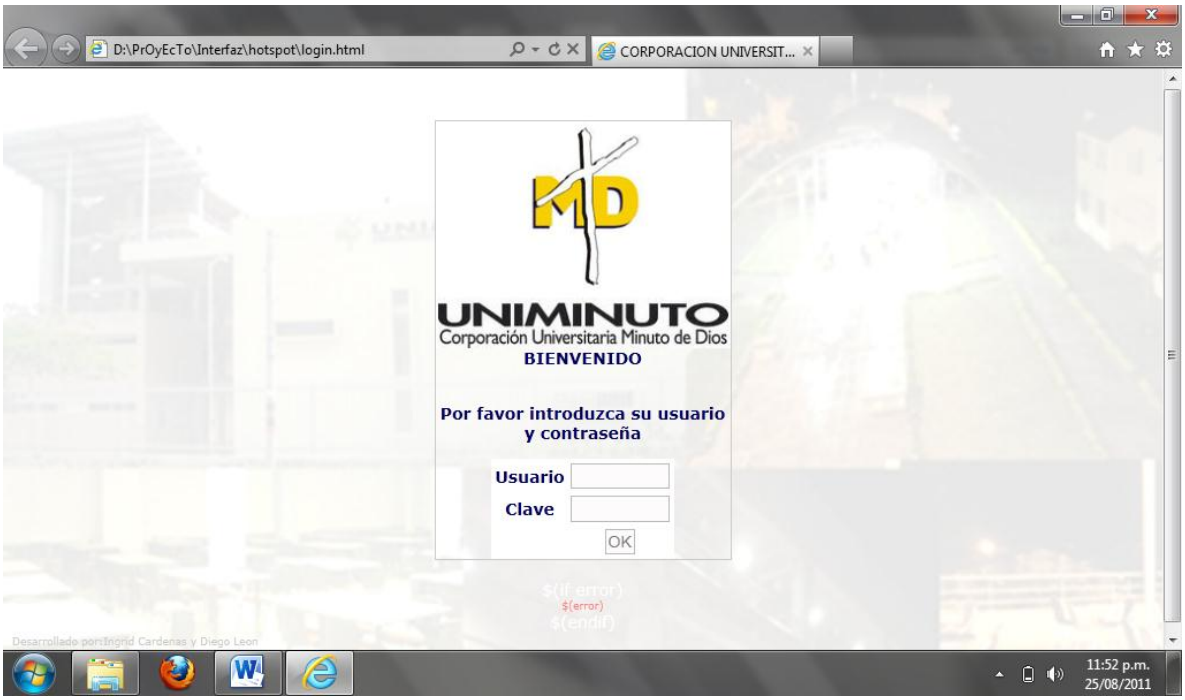


Imagen 57. Interfaz

La configuración utilizada en toda la configuración seria la siguiente:

TABLA DE DIRECCIONAMIENTO	
192.168.101.7	PROXY DE LA UNIVERSIDAD
192.168.1.3-192.168.1.254	POOL DE DIRECCIONES DEL SERVIDOR DHCP
10.10.11.1	PUERTA DE ENLACE DE LA RED DE LA UNIVERSIDAD
10.0.0.3	DNS
10.10.11.180	DIRECCIÓN IP QUE PROVEE EL INTERNET AL SERVIDOR INTERFACE 2 LAN
192.168.1.1	DIRECCIÓN DE LA TARJETA DE RED INTERFACE 2 WAN
192.168.1.2	DIRECCIÓN DE LA ANTENA O A.P. QUE HACE DE HOTSPOT

Tabla 3: Direccionamiento

Nuestro único inconveniente es la localización del puerto, puesto que la antena es aérea y al estar en la biblioteca pierde potencia, según las medidas de alcance que se realizaron: el todo el primer piso hasta el parqueadero y el segundo piso tiene acceso, ya en el tercer, cuarto y quinto piso no logra tener alcance en los salones, pero si se logra tener en las terrazas y pasillos que son los lugares de mayor concurrencia junto con la biblioteca que eran nuestra en un principio nuestra meta de cobertura anteriormente mencionada en el análisis de la situación actual.

6. CONCLUSIONES

- Este es un gran proyecto lleva consigo muchos propósitos y beneficios desde probar los conocimientos adquiridos durante todo este tiempo por los alumnos desarrolladores del mismo, pasando por la innovación en el campo de las redes hasta otorgar un beneficio a la comunidad estudiantil y a la misma Universidad Minuto de Dios.

- De las falencias y sugerencias de la implementación de nuestro prototipo:

  - ✓ La localización que aprovecha mejor la cobertura de la AP es en la casa donde estaba la línea de internet de ETB.

  - ✓ Para tener mejor aprovechamiento de todas las capacidades que nos brinda el servidor Mikrotik sería mejor tener un internet sin restricciones o una línea dedicada para este.

  - ✓ Para prevenir accidentes por ser lugar público sería mejor tener un cuarto dedicado a equipos de cómputo y conexión a internet.

  - ✓ Para tener una eficiencia como servicio sería ideal tener una UPS que permita terminar y guardar investigaciones a los usuarios cuando falle la energía eléctrica.

BIBLIOGRAFÍA

- García-Moran Maglaya, Jean Paul, Ramos Varón, Antonio Angel, Fernández Hansen, Yago RADIUS / AAA / 802.1x Sistemas basados en la Autenticación en Windows y Linux/GNU Seguridad Máxima, 1ª Ed. Alfaomega, 2009. ISBN 978-970-15-1455-9.

- Stallings, William: Comunicaciones y Redes de Computadores, 7ª Ed. Prentice Hall, 2000. ISBN 978-84-205-4110-5.

- Black, Uyless: Tecnologías emergentes para Redes de Computadoras, 2ª Ed. Prentice Hall, 1999. ISBN 970-17-0268-9.

- Derfler y Freed, Les: Así funcionan las comunicaciones. 1994.

- Derfler, Frank: Descubre redes LAN y WAN. Prentice Hall, 1998. ISBN 84-8322-091-1.

- Ford, Merilee y Kim Lew, H.: Tecnologías de interconectividad de redes. Cisco Press, 1998. ISBN 970-17-0171-2.

- Kim Lew, H. y otros: Interconectividad Manual para la Resolución de problemas. Cisco Press, 2000. ISBN 970-17-0351-9.

- Black, Uyless: Redes de ordenadores, protocolos, normas e interfaces, 2ª Ed.,,1995.

- Parnell, T.: LAN Times Guía de redes de área extensa. 1997. ISBN 84-481-1012-9

- Parnell, T.: LAN Times Guía de redes de alta velocidad. 1997. ISBN 84-481-0825-6.

- Habraken, Joe: Routers Cisco. Serie Práctica. Prentice Hall, 2000. ISBN 84-205-2952-4.

- Huitema, C.: Routing in the Internet. Prentice Hall, 1995.

- Shaugnessy, Tom y Velte, Toby: Manual de CISCO. McGraw-Hill, 2000. ISBN 84-481-2727-7.

- Alonso, J.M. : TCP/IP en UNIX. 1998. ISBN 84-7897-307-9.

- Casad, John y Wilsey, Bob: Aprendiendo TCP/IP en 24 Horas. Prentice Hall, 1997. ISBN 970-17-0339-1.

- Comer, Douglas E.: Redes Globales de información con Internet y TCP/IP. Vol. 1, 3ª Ed. Prentice-Hall, 1996. ISBN 968-880-541-6.

- Comer, Douglas E.: Redes de Computadoras, Internet e Interredes. Prentice Hall, 1997. ISBN 970-17-0021-X.

- Comer, Douglas E.: El libro de Internet. 1995.

- Feit, Sidnie.: TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill. 1998. ISBN 84-481-1531-7

- Miller, M. A. Troubleshooting TCP/IP. M&T Books, 1996

- Parker, Timothy: Aprendiendo TCP/IP en 14 días, 2ª Ed. Prentice Hall, 1997. ISBN 968-880-865-2.

- Piscitello, D.M. y Chapin, A.L.: Open Systems Networking. TCP/IP and OSI. Addison-Wesley, 1993.

- Cheswick, W.R. y Bellovin, S.M.: Firewalls and Internet Security, 1994.

- Hafner, K. y Markoff, J.: Cyberpunk. Outlaws and hackers on the Computer Frontier. Simon & Schuster Inc., 1995.

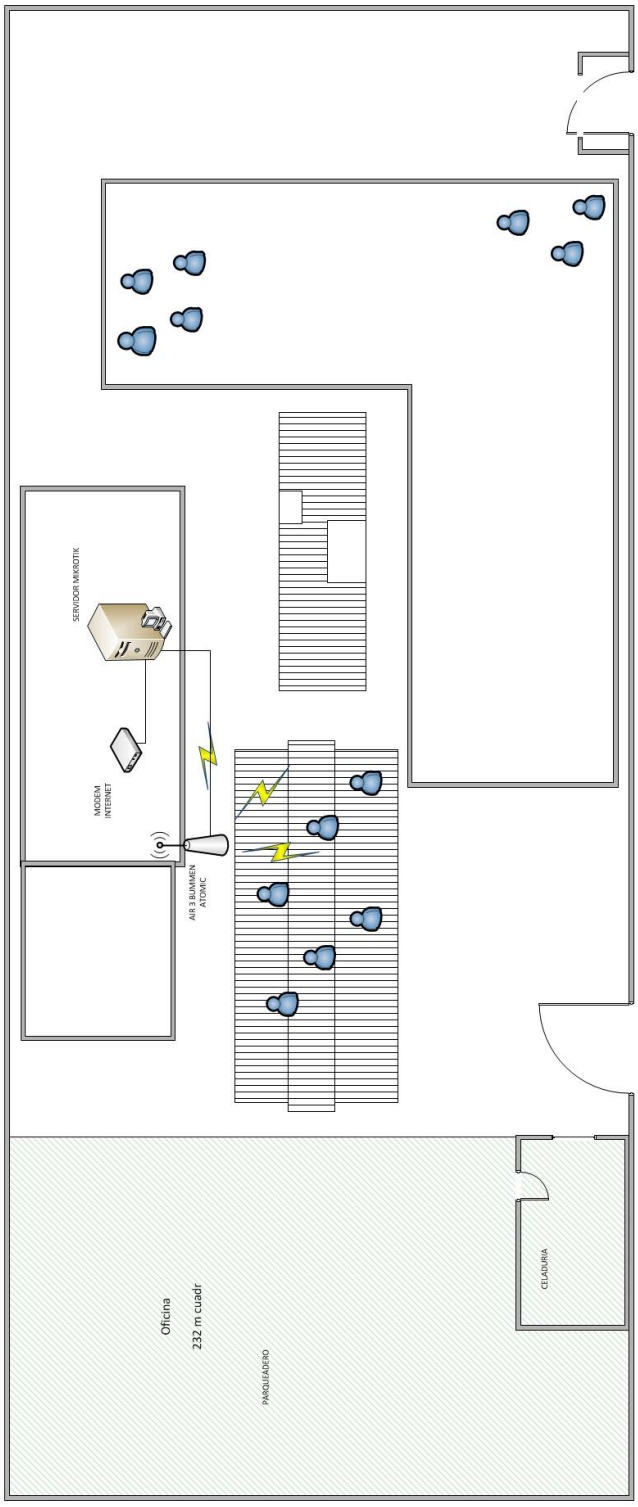
- Kaufman, C., Perlman, R. y Speciner, M.: Network Security. Private Communication in a Public World. Prentice Hall, 1995.

- Schneier, B.: E-Mail Security. How to keep your electronic messages private. John Wiley & Sons, Inc., 1995

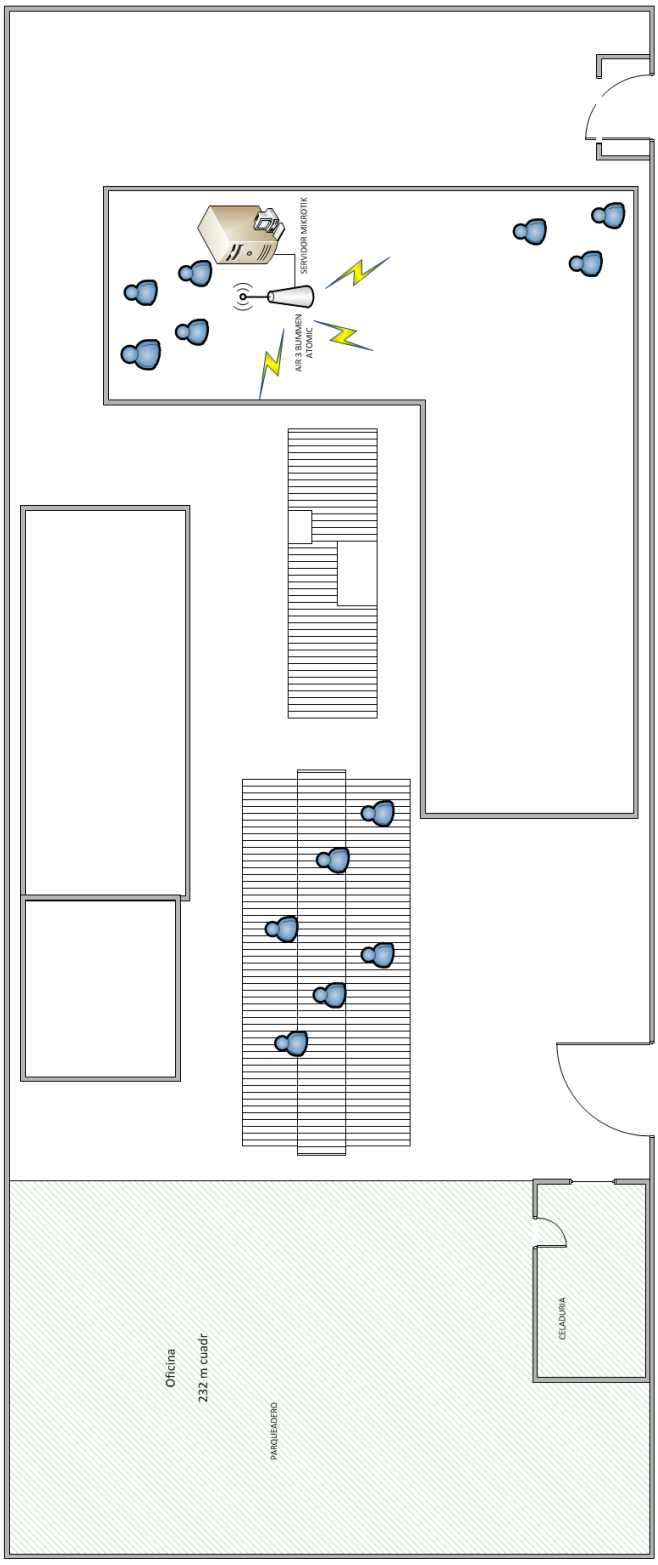
- W. Stallings. Network and Internet Network Security. Principles and Practice. Prentice Hall 1995

- SENN J. (1990). Análisis y Diseños de Sistemas de Información. Traducción de Edmundo Gerardo Urbina Medal. México: Editorial McGraw Hill.

ANEXOS



Diseño ideal de Localizacion



Diseño actual de Localizacion

MANUAL DE USUARIO PARA SERVIDOR MIKROTIK DE LA COMUNIDAD ACADEMICA DE LA CORPORACION UNIVERSITARIA MINUTO DE DIOS

INTEGRANTES

INGRID MILENA CARDENAS ARCINIEGAS

DIEGO FRANCISCO BALLEN LEON

PRESENTADO A

UNIMINUTO

GIRARDOT - 2011

CAPITULO

DEFINICIONES, CONCEPTOS Y TEORIA

RADIUS

RADIUS es un protocolo ampliamente usado en el ambiente de redes, para dispositivos tales como routers, servidores y switches entre otros.

RADIUS (Remote Authentication Dial-In User Server) es una colección y definición de normas para la creación de sistemas o protocolo que nos permite gestionar la "autenticación, autorización y registro" de usuarios remotos sobre un determinado recurso, ampliamente usado en el ambiente de redes, para dispositivos tales como routers, servidores y switches entre otros. La tupla "autenticación, autorización y registro" es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa "Authentication, Authorization, and Accounting".

Estos términos se refieren a:

- Autenticación (authentication) hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

  Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario nos permite acceder a determinados recursos. El nombre de usuario es nuestra identidad, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante nuestra identidad. Otros tipos más avanzados de credenciales son los certificados digitales.

  Existen muchos métodos concretos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son:

  - Autenticación de sistema (system authentication), típica en un sistema Unix, normalmente realizada mediante el uso del fichero /etc/passwd;
  - Los protocolos PAP (Password Authentication Protocol), y su versión segura CHAP (Challenge Handshake Authentication Protocol), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP;

- LDAP (Lightweight Directory Access Protocol), un protocolo a nivel de aplicación (sobre TCP/IP) que implementa un servicio de directorio ordenado, y muy empleado como base de datos para contener nombres de usuarios y sus contraseñas;
- Kerberos, el famoso método de autenticación diseñado por el MIT;
- EAP (Extensible Authentication Protocol), que no es un método concreto sino un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto;
- Por último, también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

En la fase de autenticación se produce un mensaje inicial de solicitud de acceso desde el equipo NAS al servidor de autenticación en forma de:

- Access – Request (solicitud de acceso): El usuario envía el nombre de usuario y la contraseña cifrada, si procede hacia el NAS. Este envía entonces al servidor de autenticación el mensaje de Access-Request solicitando además el puerto de acceso para el usuario.

- Autorización (authorization) se refiere a conceder servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "logins" de un mismo usuario.

  El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

  Los métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen bases de datos LDAP, bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor.

No se debe confundir los términos autenticación con autorización. Mientras que la autenticación es el proceso de verificar un derecho reclamado por un individuo (persona o incluso ordenador), la autorización es el proceso de verificar que una persona ya autenticada tiene la autoridad para efectuar una determinada operación.

E n esta fase el servidor de autenticación, tras conocer todos los atributos necesarios para el solicitante, responderá a su solicitud de autenticación mediante un mensaje estándar enviado al equipo NAS para permitir, denegar o volver a preguntar sobre su acceso:

- Access - Accept (Aceptación del acceso): El fin mismo de la solicitud de autenticación es la aceptación del acceso. Si el mecanismo de acceso ha sido correcto, se le envía este mensaje al NAS con los atributos necesarios para regular el acceso del usuario de forma personalizada.
- Access – Reject (Denegacion del acceso): Debido a las circunstancias que pueden no permitir el acceso de un usuario, como por ejemplo: usuario inexistente, contraseña incorrecta, derechos revocados, etc. Se le deniega de forma incondicional el acceso a este solicitante. Se puede incluir en este mensaje el motivo de la denegación del servicio. El NAS que recibe este mensaje no permite el acceso al usuario, enviando un mensaje (si se incluye) al solicitante o usuario.
- Access – Challenge (Solicitud de información adicional para el acceso): Se le solicita al usuario o solicitante información adicional, como contraclave, tarjeta de acceso, PIN de acceso, o cualquier otro método alternativo o adicional de acceso. El NAS transmite la solitud al usuario. Este mensaje puede ser intercambiado en múltiples ocasiones dependiendo del tipo de autenticación y de la información que se precisa

- Registro (accounting, a menudo traducido también como contabilidad) se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio.

  Durante la fase de registro se producen los siguientes mensajes:

- Accounting - Request [Start] (Solicitud de inicio de registro): Es una solicitud de inicio enviada desde el equipo NAS al servidor, para indicar que ha comenzado la fase de registro, y comienza a recolectar los datos de la sesión del usuario.
- Accounting - Response [Start] (Respuesta de asentimiento al inicio de registro): El servidor de autenticación responde a la solicitud inicial, registrando la información de inicio y enviando este paquete al NAS para mostrar su conformidad.
- Accounting - Request [Stop] (Solicitud de final de registro): El NAS comprueba la desconexión del usuario y envía al servidor un mensaje de final de la fase de registro con los datos de la sesión de usuario.
- Accounting – Response [Stop] (Respuesta de asentimiento al final del registro): El servidor tras almacenar la información anterior, envía al NAS su conformidad al final de la fase de registro, admitiendo haber recibido correctamente toda la información de la sesión.

Es interesante el uso del protocolo RADIUS cuando tenemos redes de dimensiones considerables sobre las que queremos proporcionar un servicio de acceso centralizado (aunque posiblemente jerarquizado por medio de diversos servidores RADIUS). Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan acceso a Internet o grandes redes corporativas, en un entorno con diversas de tecnologías de red (incluyendo módems, xDSL, VPNs y redes inalámbricas) no sólo para gestionar el acceso a la propia red, sino también para servicios propios de Internet (como e-mail, Web o incluso dentro del proceso de señalización SIP en VoIP).

Un uso de RADIUS que queremos enfatizar, al ser el que realizaremos en esta práctica, es la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (pre-shared key, PSK), que son bastante limitados al gestionar una red cuando ésta alcanza un determinado tamaño.

Aunque RADIUS es el protocolo para AAA más extendido en la actualidad, ya existe un nuevo protocolo que está llamado a sustituir a RADIUS. Su nombre es DIAMETER, y también proporciona manejo de errores y comunicación entre dominios.

Es utilizado para proveer autenticación centralizada, autorización y manejo de cuentas para redes de acceso dial-up, redes privadas virtuales (VPN) y, recientemente, para redes de acceso inalámbrico.

Puntos importantes:

- Los sistemas embebidos generalmente no pueden manejar un gran número de Usuarios con información diferente de autenticación. Requiere una gran cantidad de almacenamiento.

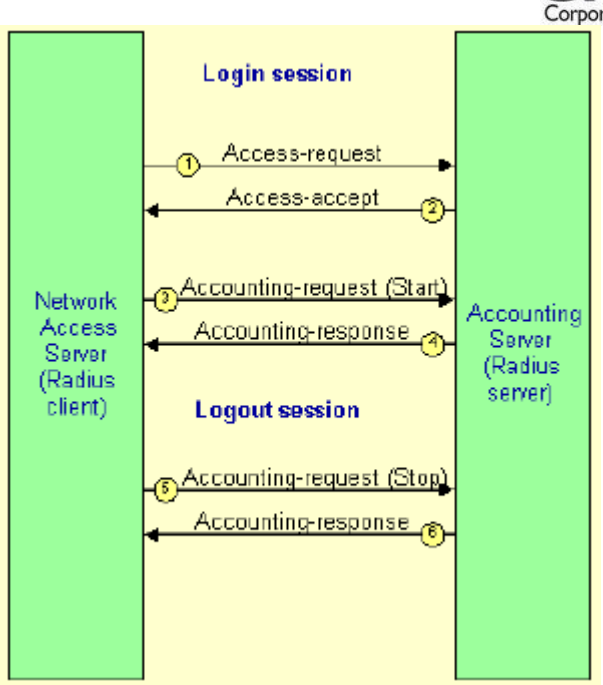
- RADIUS facilita una administración centralizada de usuarios. Si se maneja una enorme cantidad de usuarios, continuamente cientos de ellos son agregados o eliminados a lo largo del día y la información de autenticación cambia continuamente. En este sentido, la administración centralizada de usuarios es un requerimiento operacional.

- Debido a que las plataformas en las cuales RADIUS es implementado son frecuentemente sistemas embebidos, hay oportunidades limitadas para soportar protocolos adicionales. Algún cambio al protocolo RADIUS deberá ser compatible con clientes y servidores RADIUS pre-existentes.

Un cliente RADIUS envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS al servidor. Éste autentica y autoriza la solicitud del cliente y envía de regreso un mensaje de respuesta. Los clientes RADIUS también envían mensajes de cuentas a servidores RADIUS.

Los mensajes RADIUS son enviados como mensajes UDP (User Datagram Protocol). El puerto UDP 1812 es usado para mensaje de autenticación RADIUS y, el puerto UDP 1813, es usado para mensajes de cuentas RADIUS. Algunos servidores usan el puerto UDP 1645 para mensajes de autenticación y, el puerto 1646, para mensajes de cuentas.

Esto último debido a que son los puertos que se usaron inicialmente para este tipo deservicio.



Inicio de sesión

CAPITULO

INSTALACION

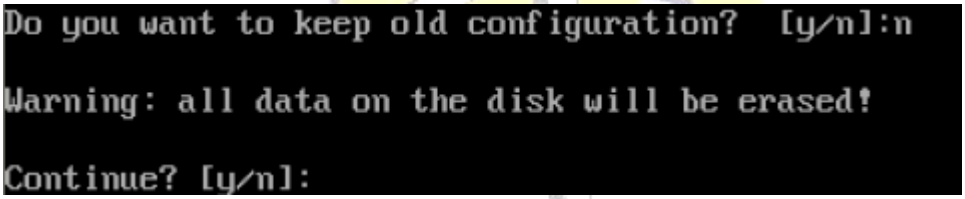
INSTALACION DE MIKROTIK ROUTER OS

Para la instalación de Mikrotik, ya contando con el equipo preparado con dos tarjetas de red y requerimientos de hardware suficientes para que nuestro Mikrotik funcione sin ningún inconveniente, junto con el CD de instalación de software, se procede iniciando el booteo del PC por el CD. Al arrancar por el CD nos arroja este pantallazo en el cual se seleccionan los servicios que se instalaran por lo general se seleccionan todos con la letra ‘a’ y el paquete de servicio que no se quiere instalar se le quita la marca de selección.

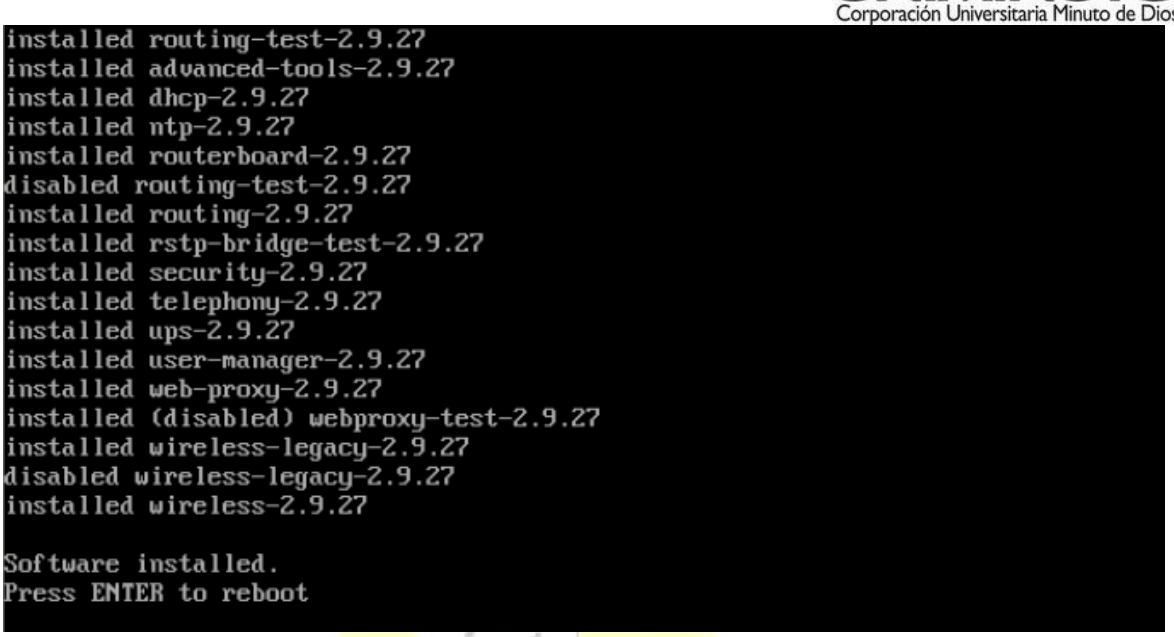
- ✓ System: Paquete principal que posee los servicios básicos al igual que los drivers básicos.
- ✓ Ppp: Provee de soporte para PPP, PPTP, L2TP, PPPoE e ISDN PPP.
- ✓ Dhcp: Servidor y cliente DHCP.
- ✓ Hotspot: provee de un hot spot.
- ✓ Hotspot-fix: Provee el parche para actualizar el modulo hot spot que tiene problemas en las versión 2.9.27.

- ✓ Ntp: Servidor y cliente NTP.
- ✓ Routerboard: provee de las utilidades para el routerboard.
- ✓ Routing: Provee soporte para RIP, OSPF y BGP4.
- ✓ Rstp-bridge-test: provee soporte para Rapid Spanning Tree Protocol.
- ✓ Security: Provee soporte para IPSEC, SSH y conectividad segura con Winbox.
- ✓ Telephony: Provee soporte para H.323.
- ✓ Ups: provee soporte para UPS APC.
- ✓ User-manager: Servicio de usuario del RouterOs
- ✓ Web-Proxy: Paquete para realizar un Web Proxy.
- ✓ wireless-legacy: Provee soporte para placas Cisco Aironet, PrismII, Atheros entre otras.

Al terminar la selección con la letra 'i' damos comienzo al proceso de instalación, luego nos pregunta si estamos seguros de borrar el disco, entonces damos 'n' y para continuar de nuevo 'y' como se muestra en la siguiente imagen.

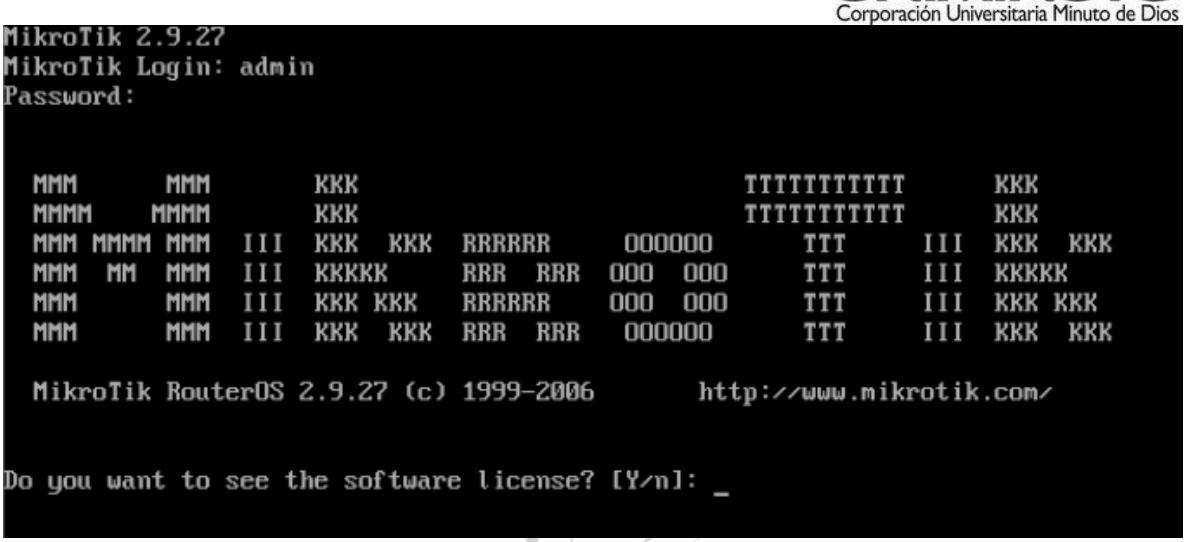


Así comienza el formateo del disco (esto puede demorarse un tiempo), luego la instalación de los paquetes correspondientes, al terminar nos pide reiniciar el equipo entonces damos 'enter', como se muestra en la siguiente imagen.

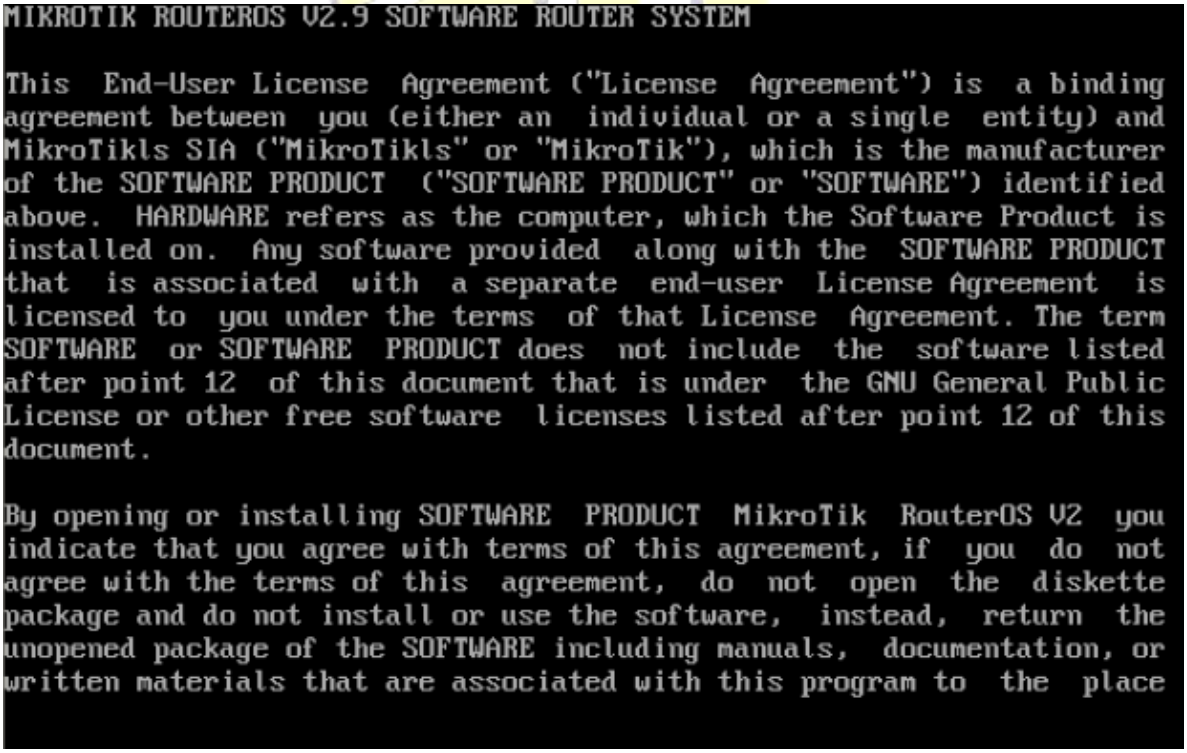


Después que se reinicia nuestro equipo, si no sufrió ningún error carga todos los paquetes y se comprueba automáticamente el funcionamiento del Sistema Operativo.

Nos carga inicialmente una consola que nos pide el usuario y contraseña, la cual por defecto dicho nombre de usuario es: *admin* y para la contraseña se deja el casillero en blanco y se presiona enter.



A continuación nos da la bienvenida y nos pregunta si deseamos leer la licencia lo cual contestamos que si ´Y´. Luego de haber leído la licencia ya nos queda la consola para comenzar a configurar nuestro Mikrotik.



CAPITULO

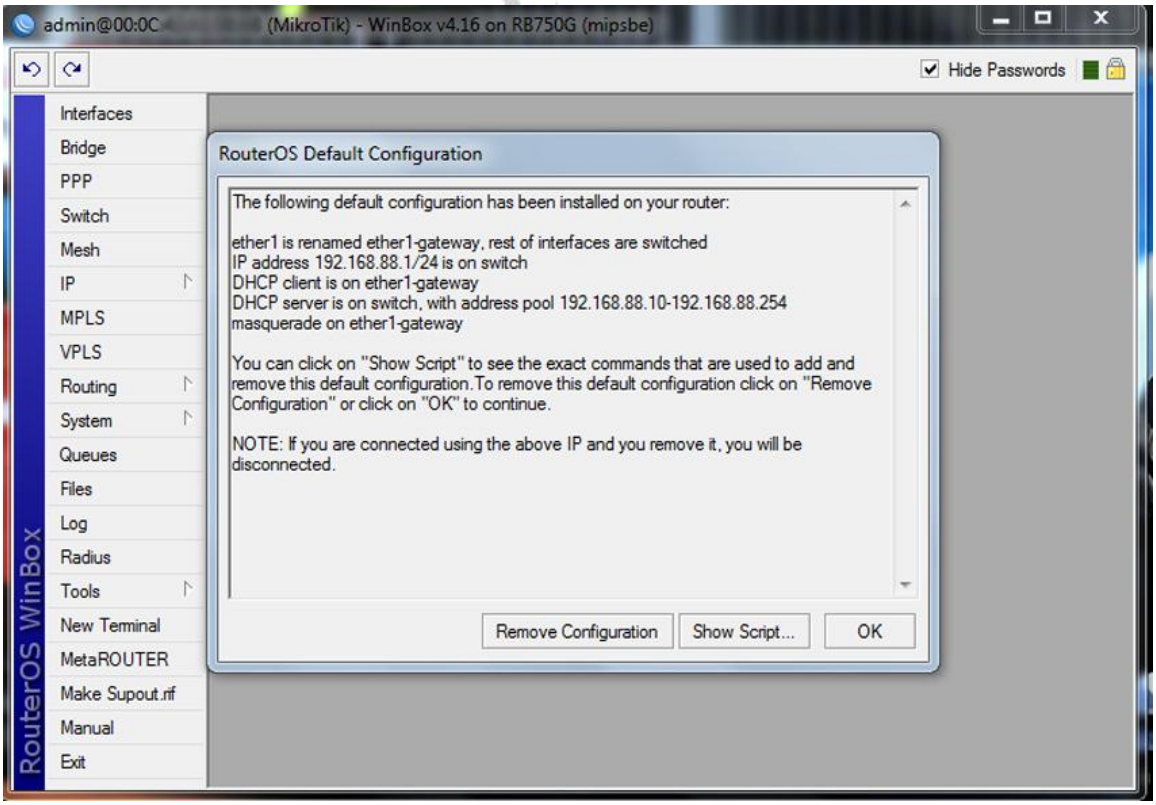
CONFIGURACION

CONFIGURACION

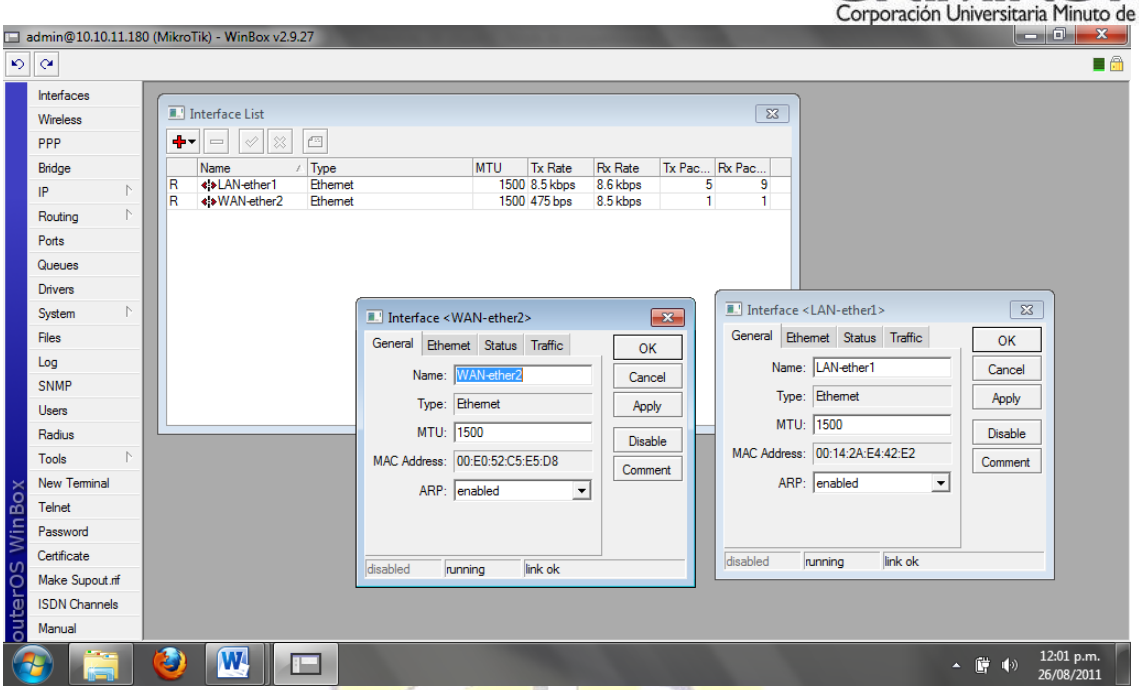
Antes de nada, descargamos el Winbox (herramienta gráfica para configurar RouterOS) en este enlace se puede descargar este programa: http://www.mikrotik.com/download/winbox.exe.

Al descargarlo conectamos un cable UTP cruzado al puerto de un PC y la otra una de las tarjetas de red de equipo en donde instalamos Mikrotik. Luego conectamos otro cable UTP cruzado desde la otra tarjeta de red al puerto de la antena.

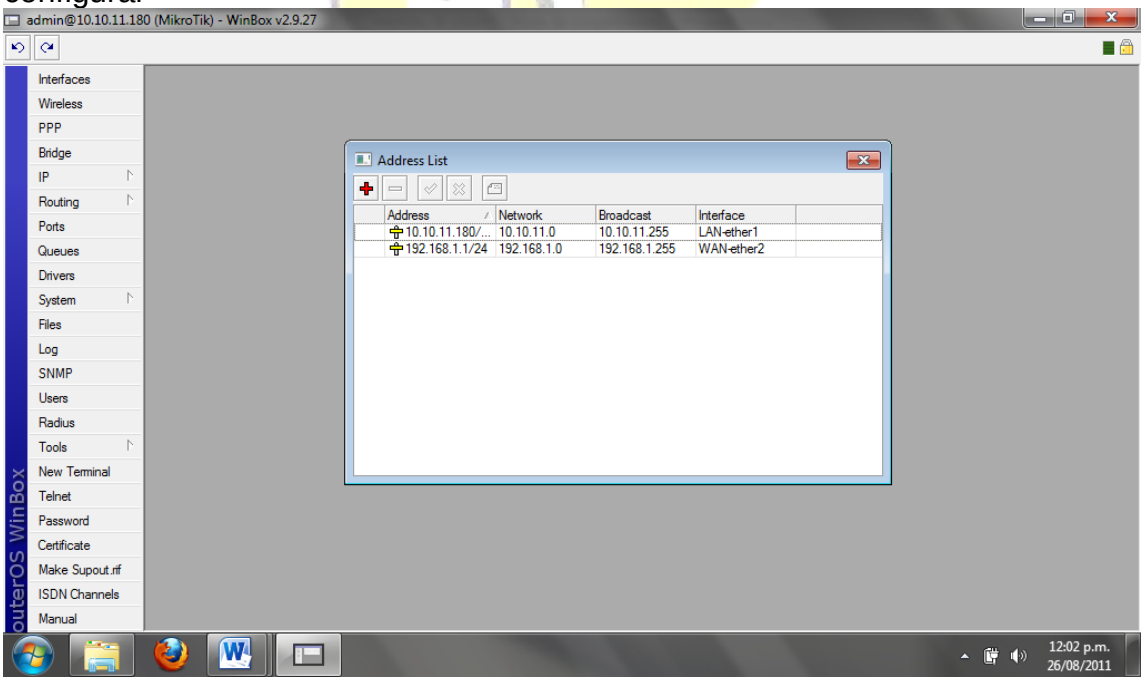
Abrimos Winbox y nos saldrá una pantalla como esta:



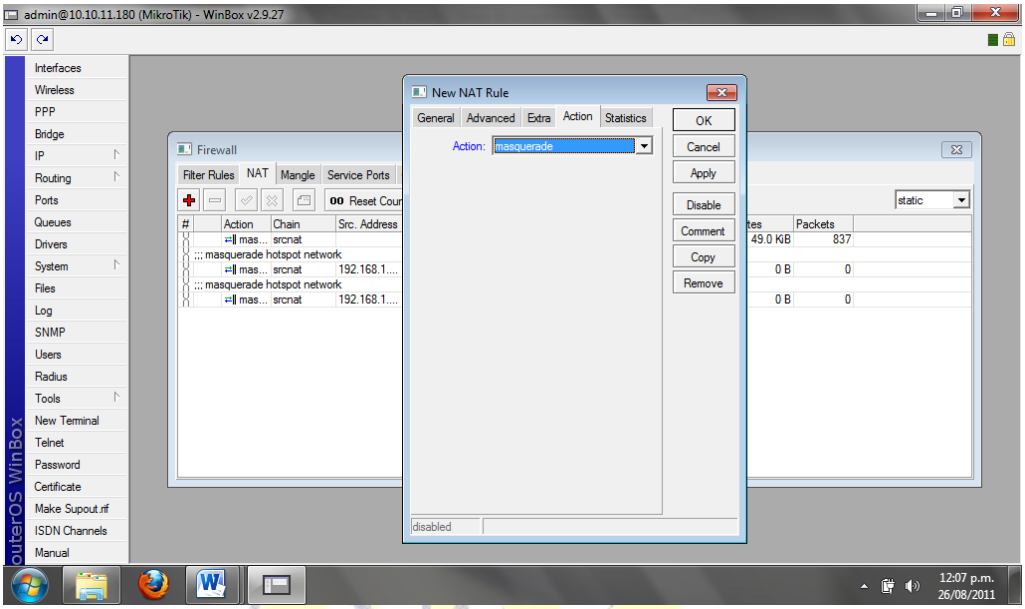
Uno de los primeros pasos es nombra las interfaces a nuestro gusto, para ello hacemos click en Interfaces se abrirá el cuadro don están todas las interfaces con las que trabaja actualmente el servidor Mikrotik.



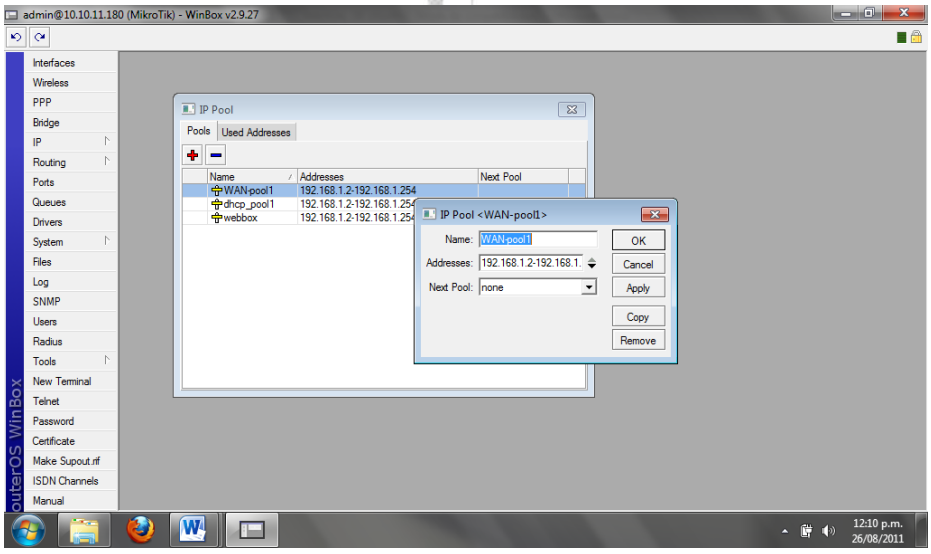
Nos dirigimos a IP>>Address verificamos y agregamos las IP que haces fatal por configurar



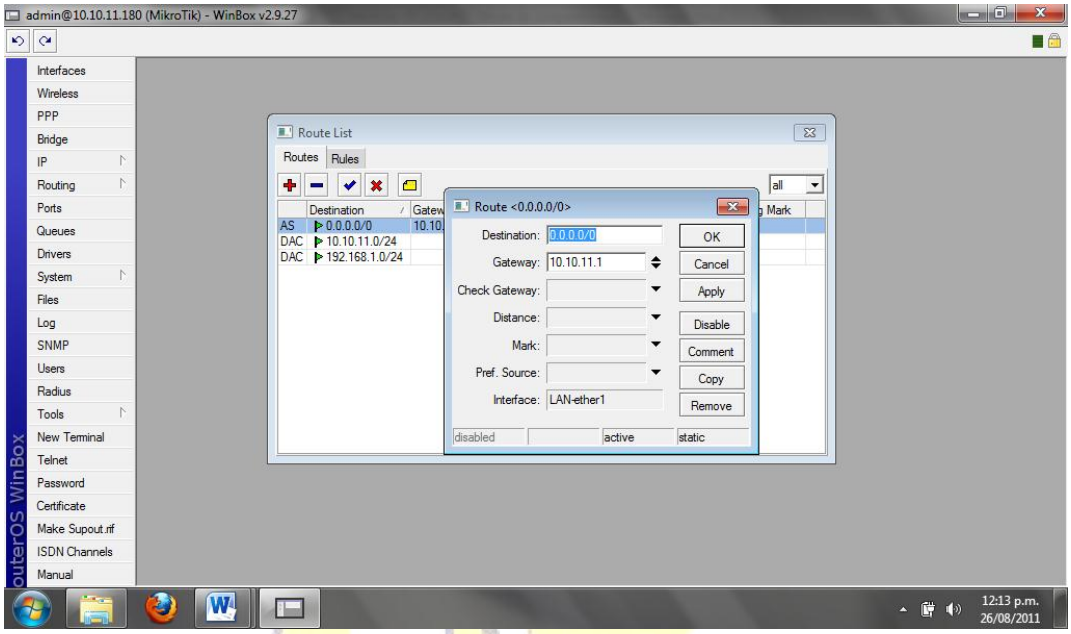
Luego nos dirigimos a IP>>Firewall seleccionamos la pestaña NAT luego hacemos click en el signo '+', damos click en la pestaña Action y en el menú desplegable colocamos la opción masquerade y damos aceptar



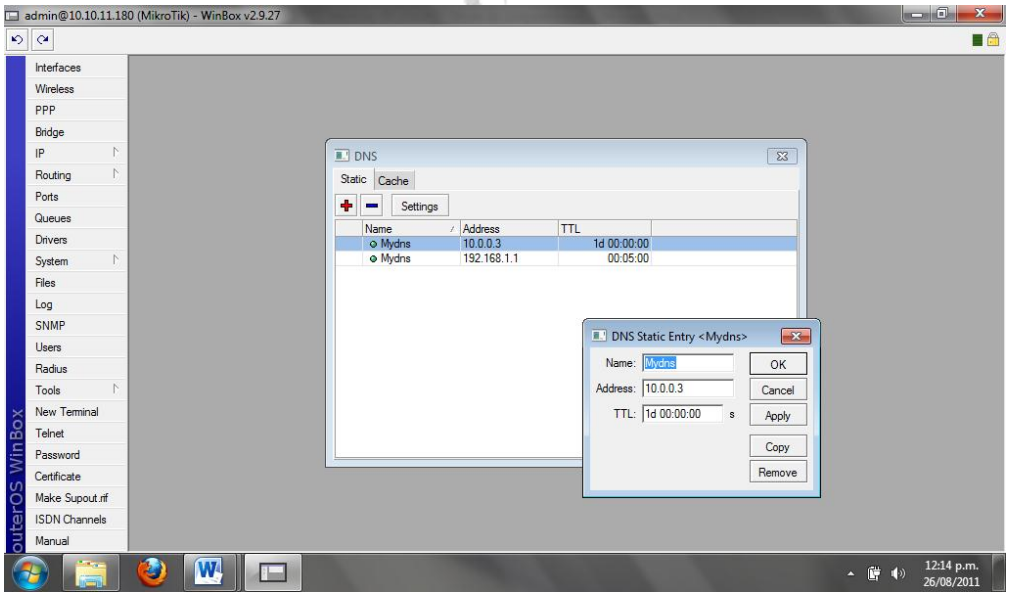
Luego nos dirimos a IP>>Pool selescionamos el '+' y ahí nos aparece un menu donde damos un nombre al pool de direcciones y colocamos su respectiva IP inicial y su respectiva IP final.



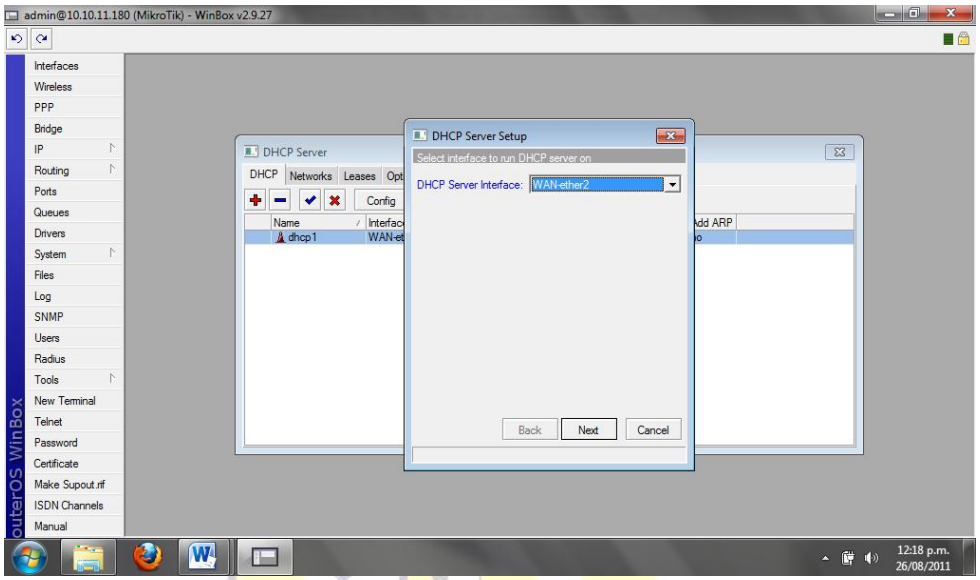
Después nos dirigimos a IP>>Routes y ahí colocamos la puerta de enlace de la Ip que maneja el internet



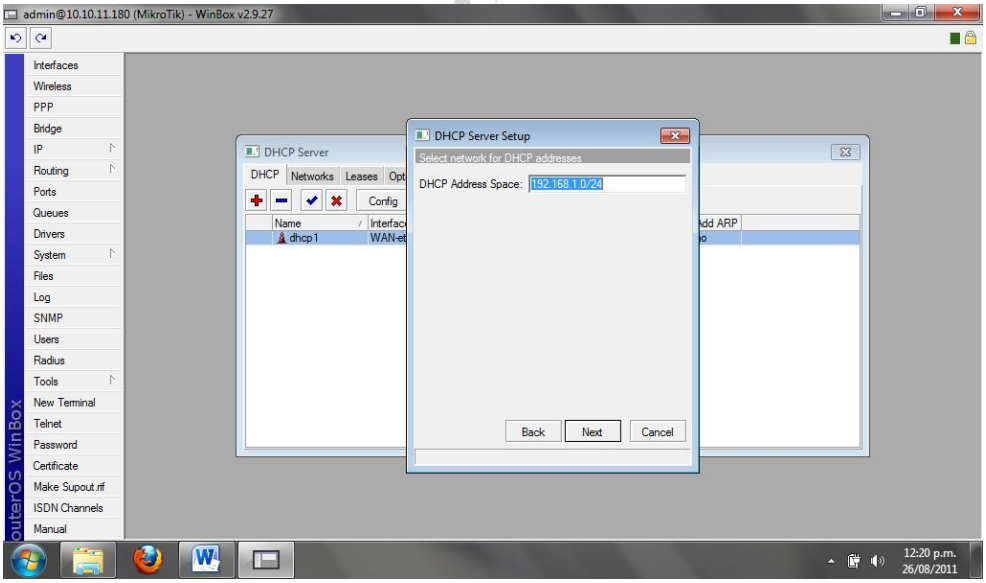
Ahora nos dirigimos IP>>DNS y colocamos el DNS que maneja la red del internet



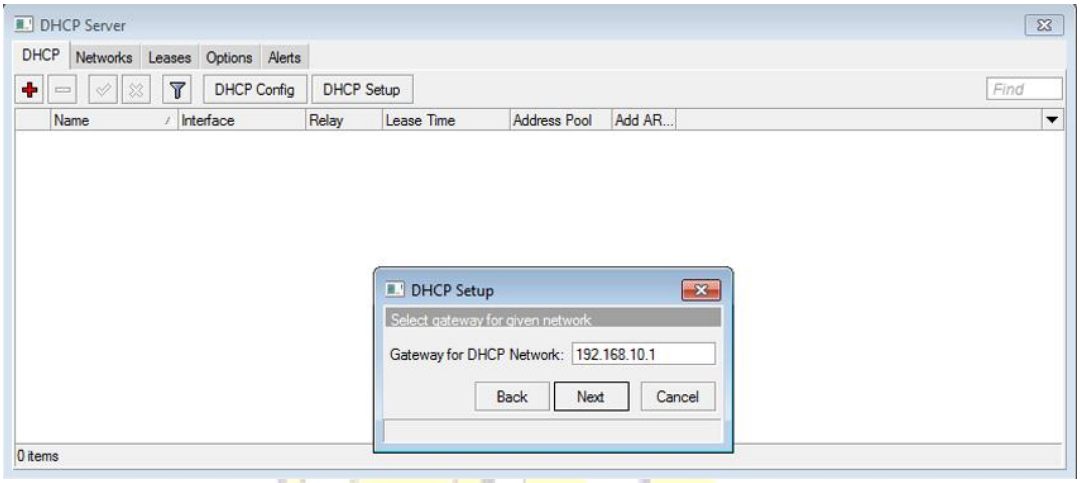
Ahora vamos a configurar el servidor DHCP de la interfaz de nuestra antena, para que entregue direcciones IP a todo equipo que se conecte por esa boca. Nos dirigimos a IP>DHCP Server y damos click en DHCP Setup.



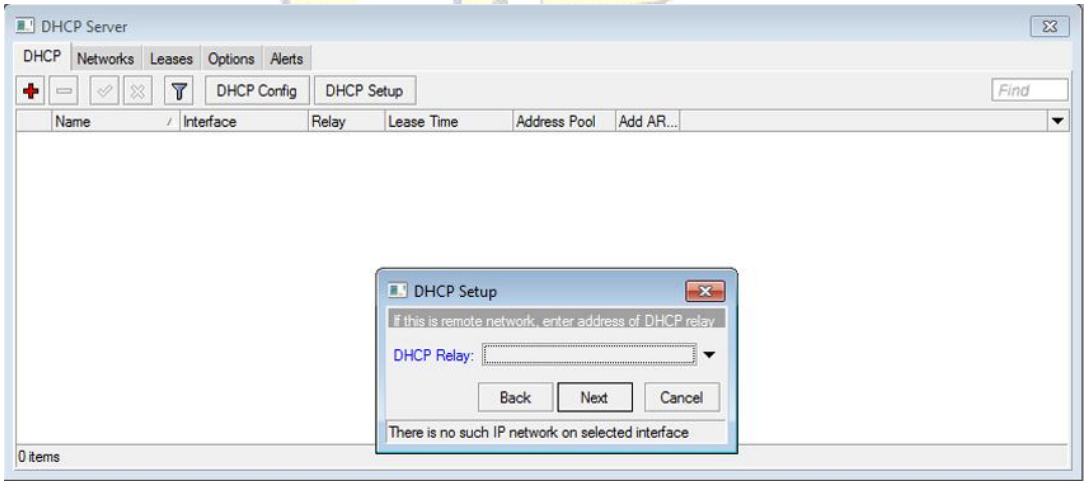
Seleccionamos la interface que configuramos para la salida a internet por cable, en mi caso WAN ether2.



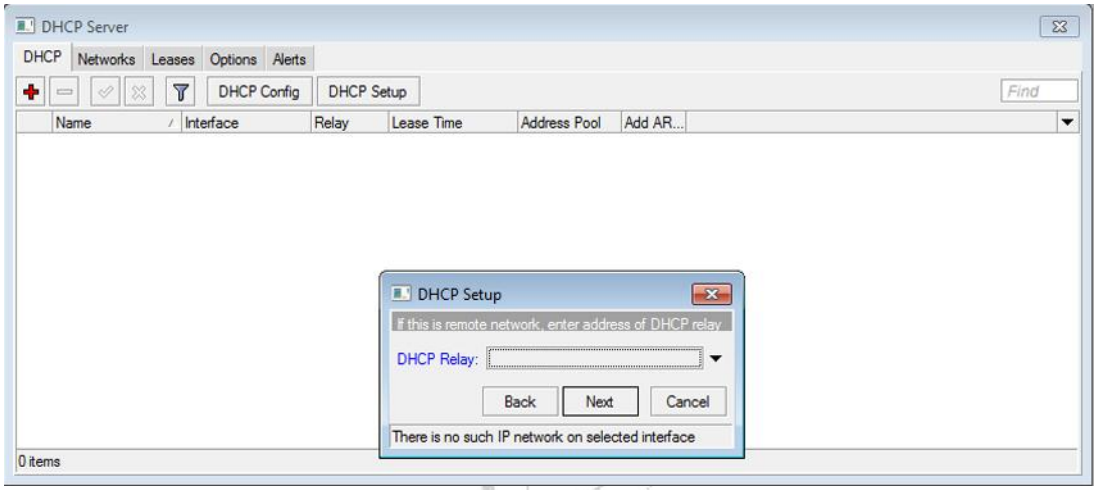
Ahora seleccionamos el rango de direcciones IP que queremos entregar por la WAN ether2, en este caso he seleccionado el rango 192.168.1.0/24, esto quiere decir que entregaré 255 IP del tipo 192.168.1.x



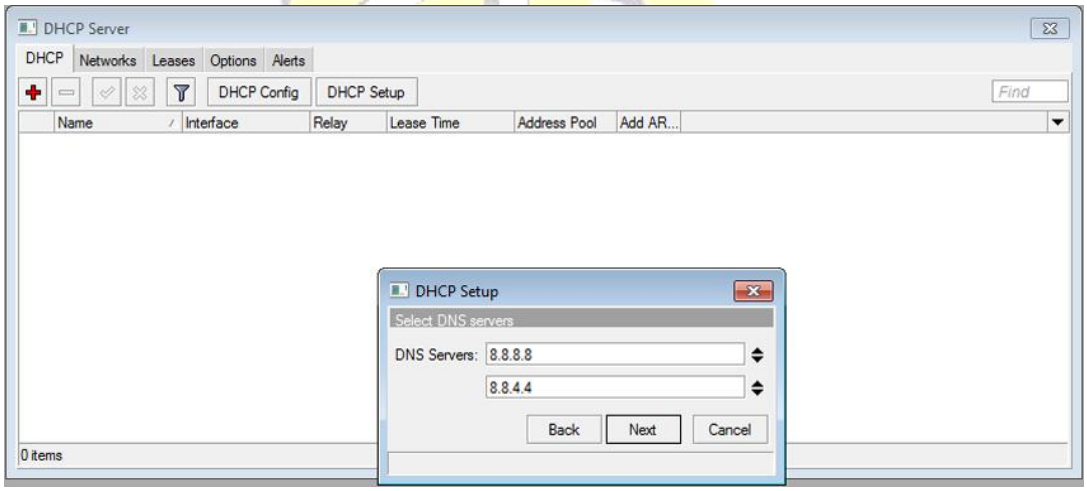
La puerta de enlace os aparecerá de forma automática.



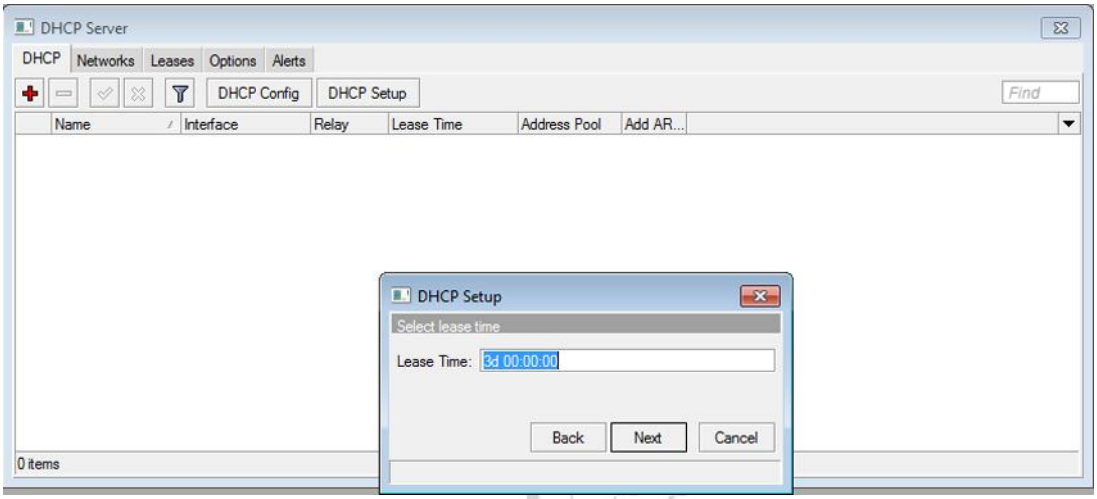
El DHCP Relay lo desactivamos pulsando en la flecha negra hacia arriba.



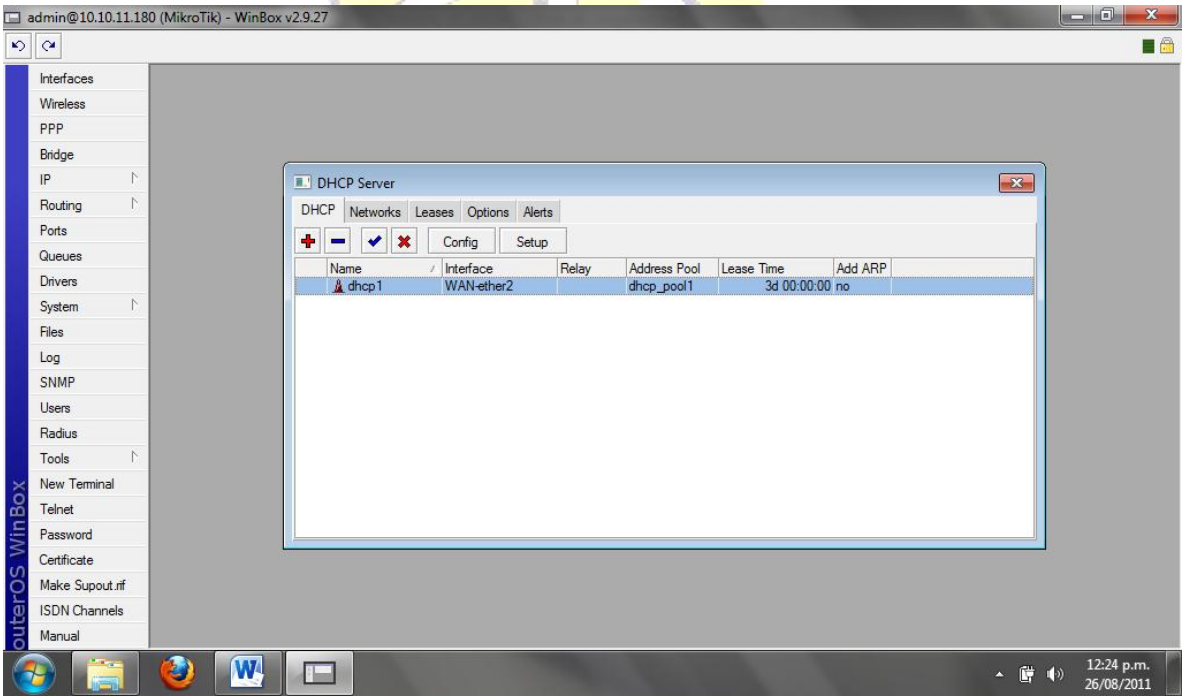
Aquí tienes lo del rango de IP, entregaremos 255 IP, desde la 192.168.1.2 hasta la 192.168.1.254



Aquí las DNS, os saldrán automáticamente, ya que las hemos configurado anteriormente.

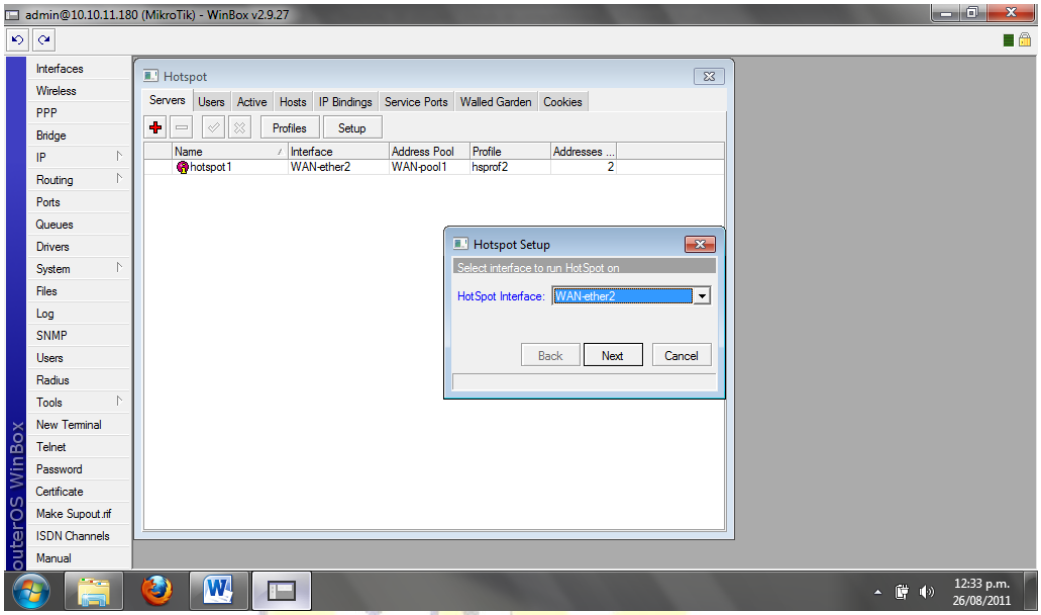


Lease Time lo dejamos por defecto y seguimos.

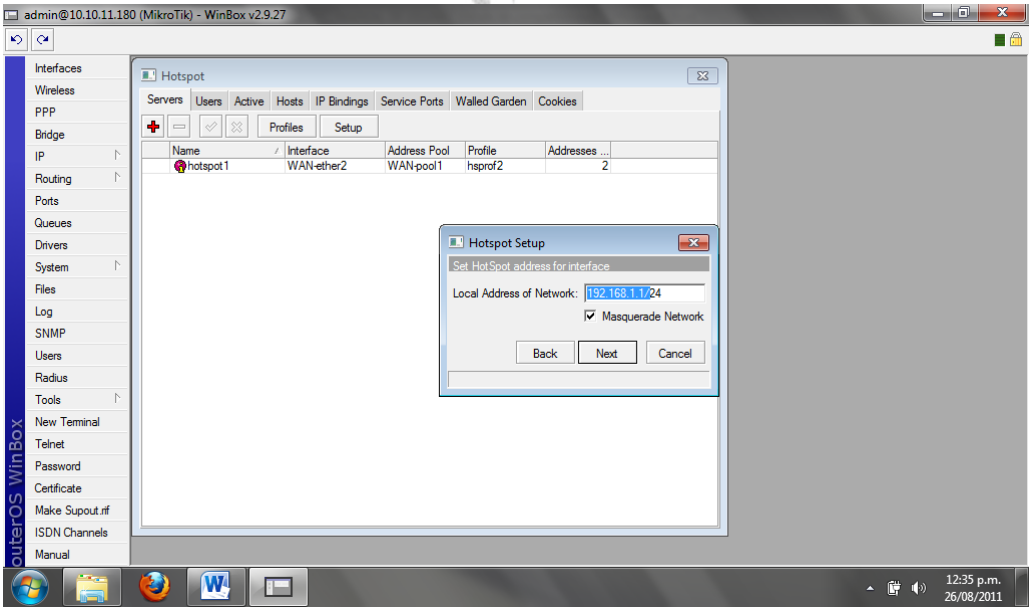


Ylisto quedoconfigurado nuestro servidor DHCP

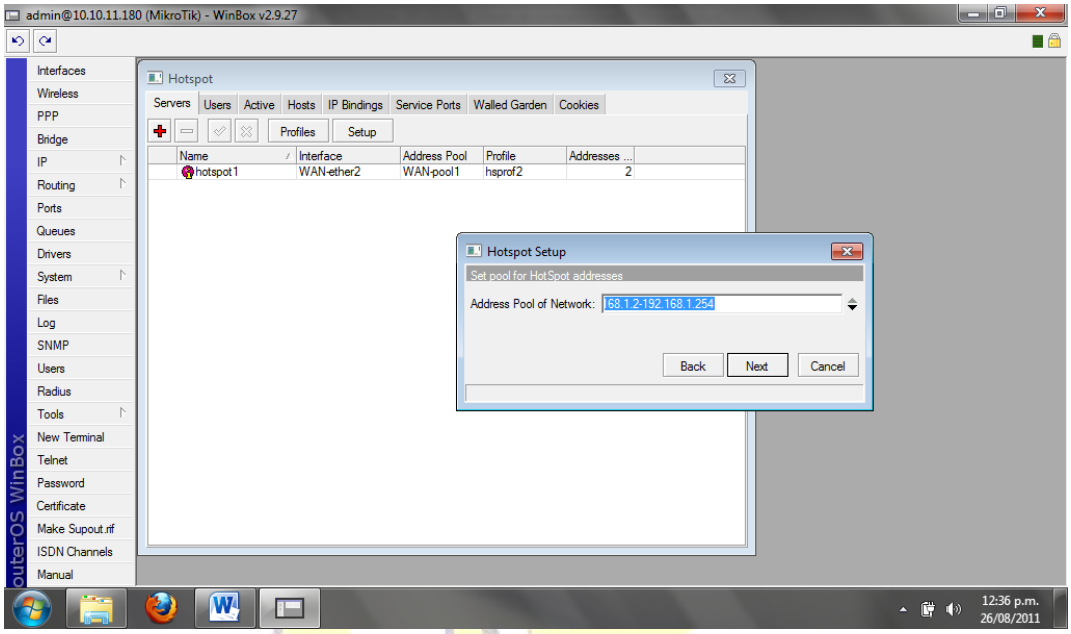
Después vamos a crear el Hotspot vamos a IP>Hotspot y damos click en Hotspot Setup.



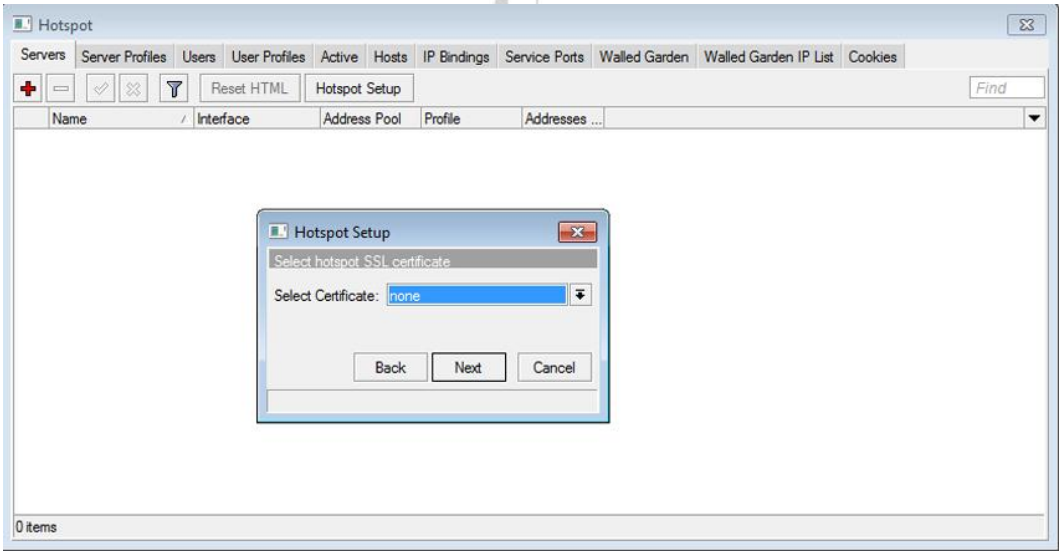
Elegimos la interface que creamos al principio para el Hotspot.



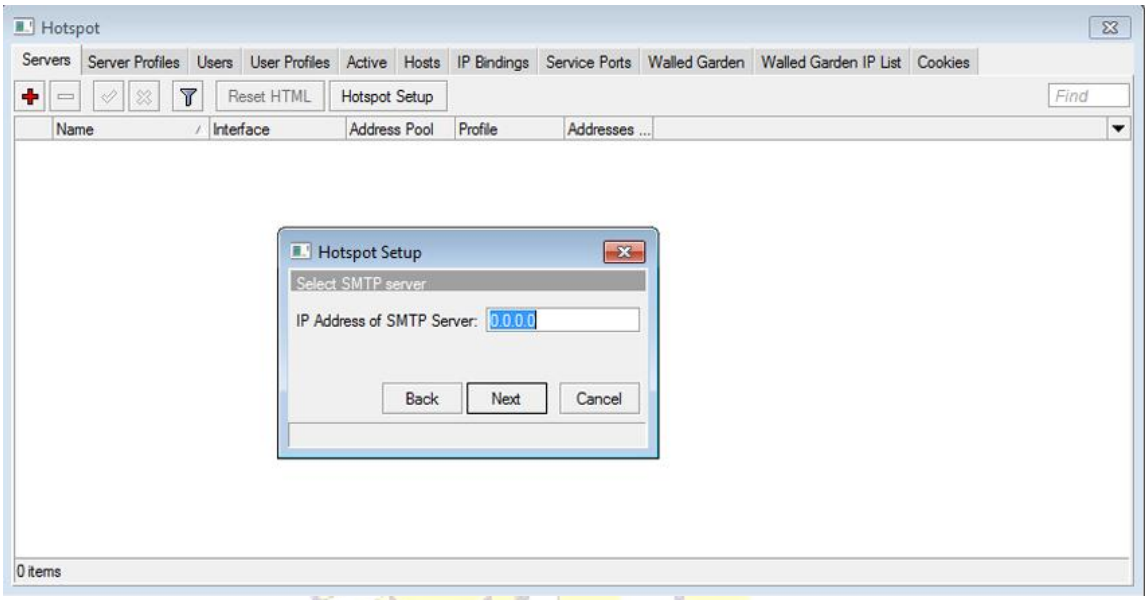
Elegimos el rango de IP que queremos que de nuestro Hotspot, y le damos a la opción Masquerade Network.



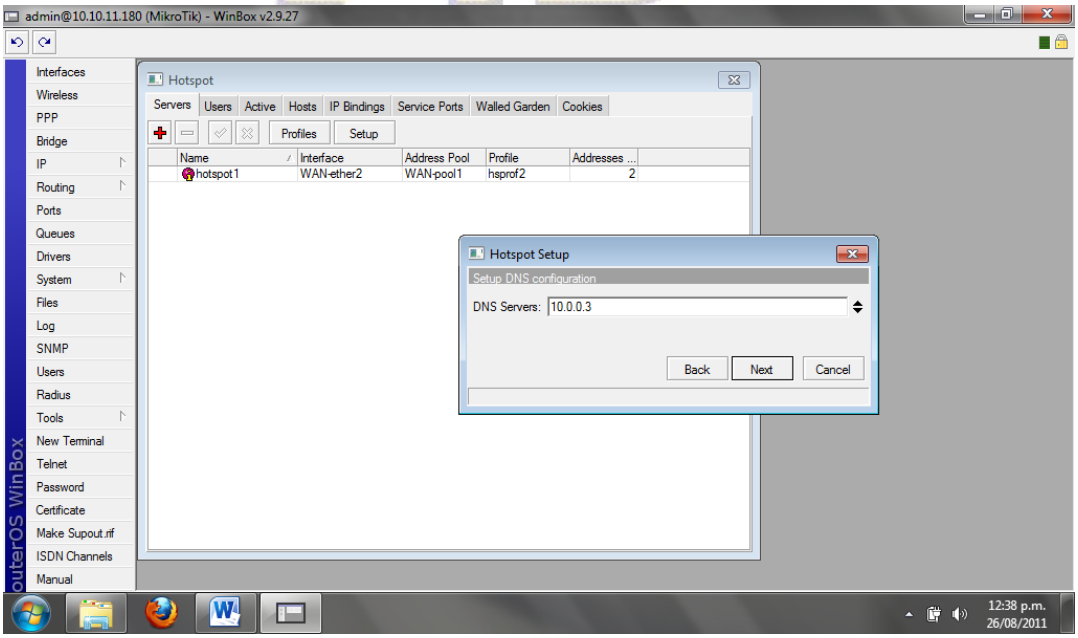
Aquí tienes el rango de IP que va a entregar vuestro Hotspot, en mi caso entregará hasta 255 IP desde la 192.168.1.2 hasta la 192.168.1.254.



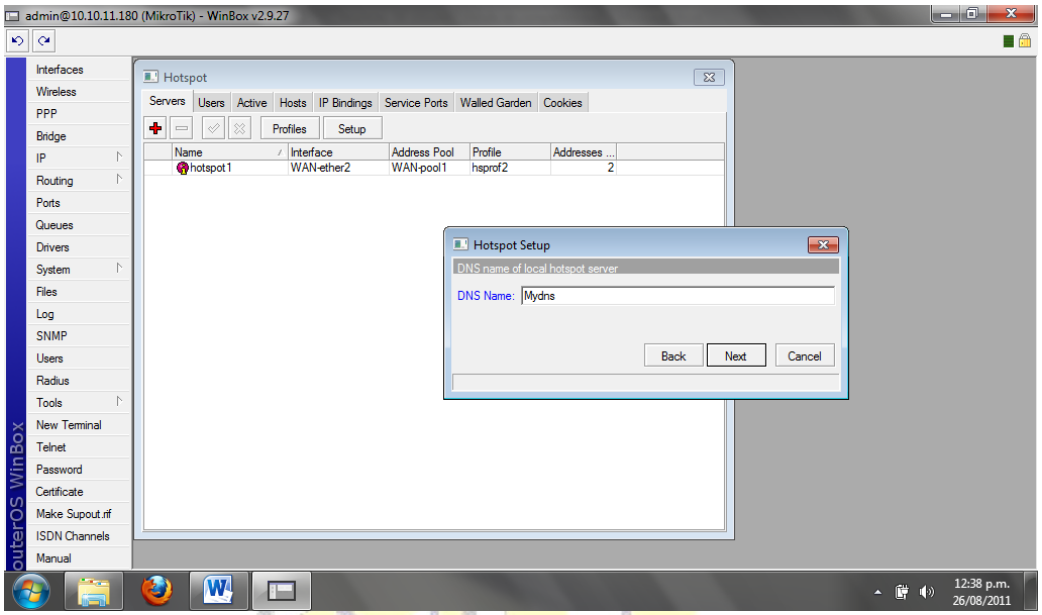
Dejamos la opción por defecto none y continuamos.



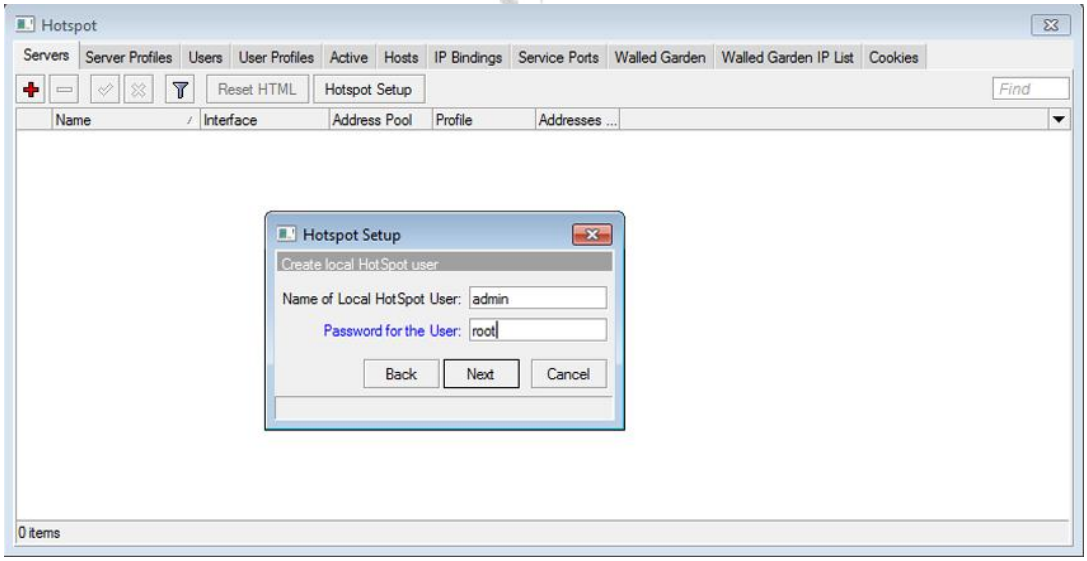
Opción por defecto y seguimos, ya falta menos.



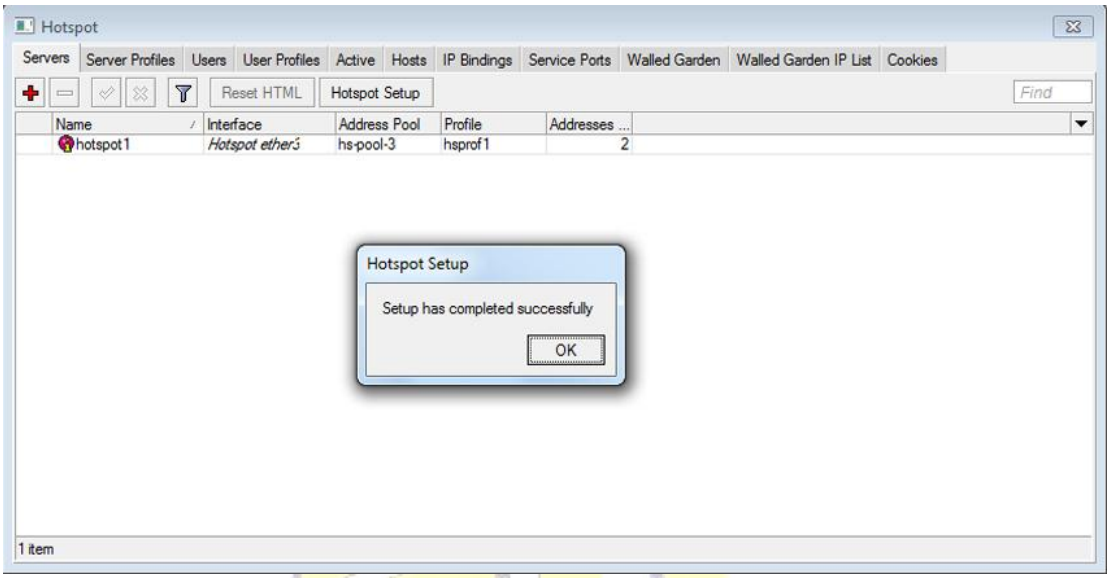
Las DNS saldrán automáticamente, ya que las teníamos configuradas de antes.



En DNS Name ponemos cualquier nombre, es la página interna del Hotspot a la que nos redirecciona al intentar conectarnos a internet.

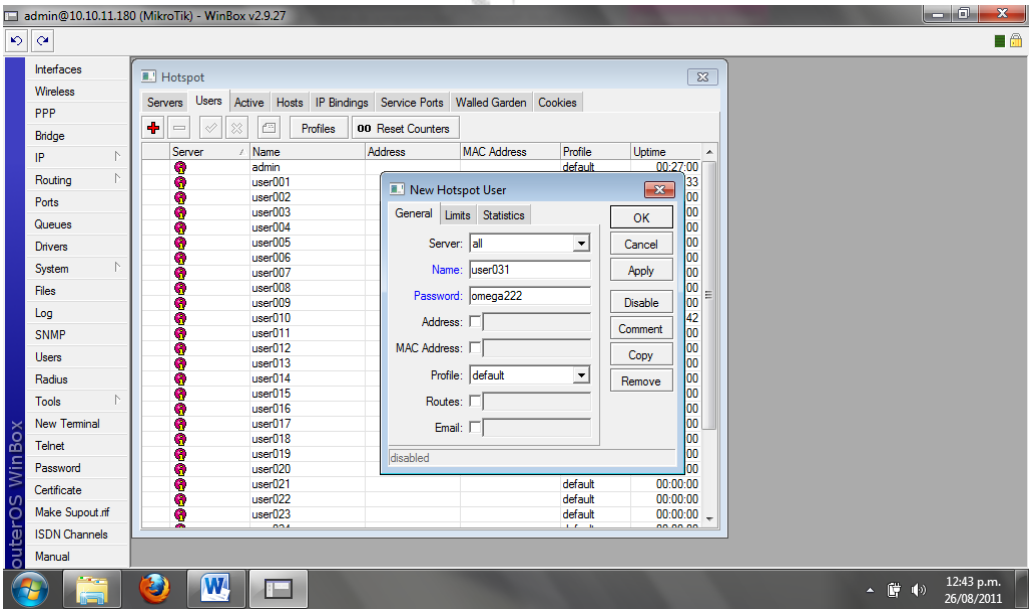


Este usuario que no tendrá limitaciones al navegar por el Hotspot



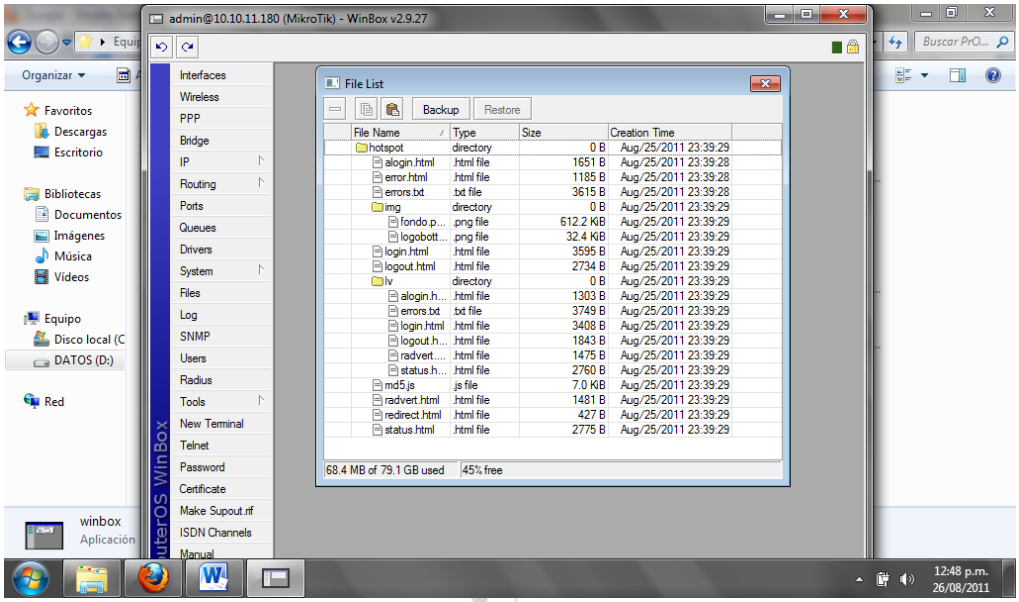
Ya hemos creado nuestro Hotspot.

Ahora vamos a crear usuarios, para ello IP>Hotspot>Users



Aquí he creado un usuario de nombre user031, con una contraseña

Para cambiar la interfaz de autenticación que nos arroja Mikrotik por defecto nos dirigimos a Files copiamos la carpeta entera de hotspot en el escritorio de nuestro pc y la modificamos a nuestro gusto cuando ya la tenemos lista entramos de nuevo a files borramos todo los archivos hasta q quede en blanco y copiamos la misma carpeta con las modificaciones.



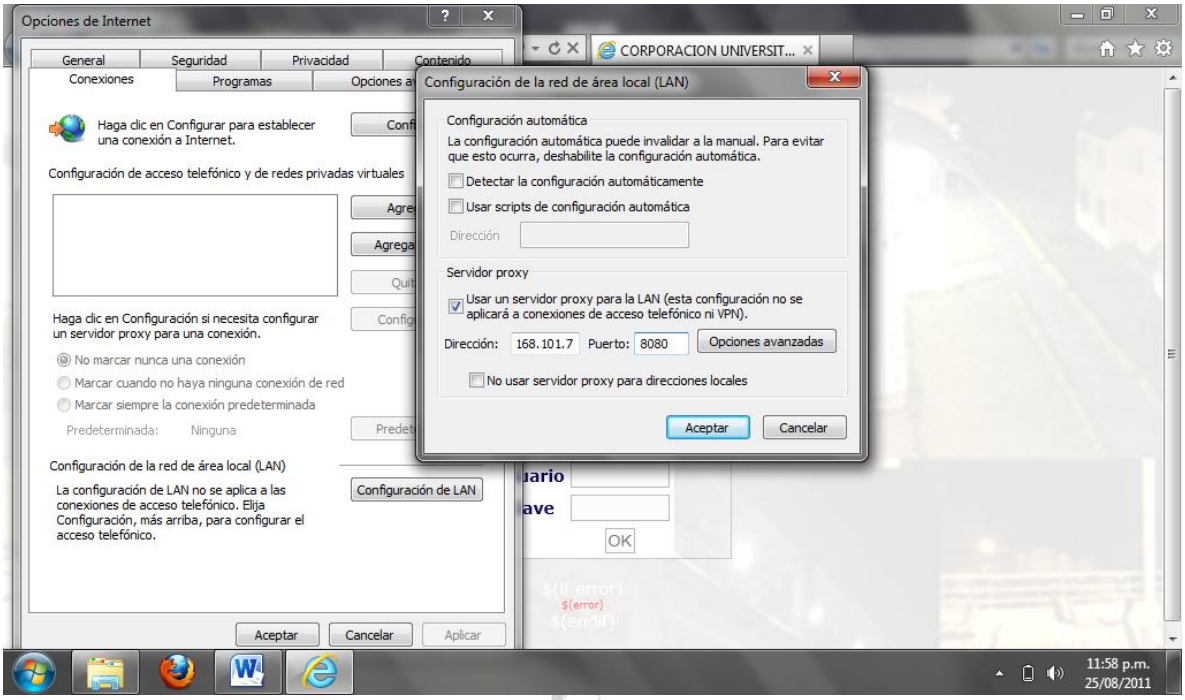
Listo se comprueba que todo funcione correctamente

CAPITULO

FUNCINAMIENTO

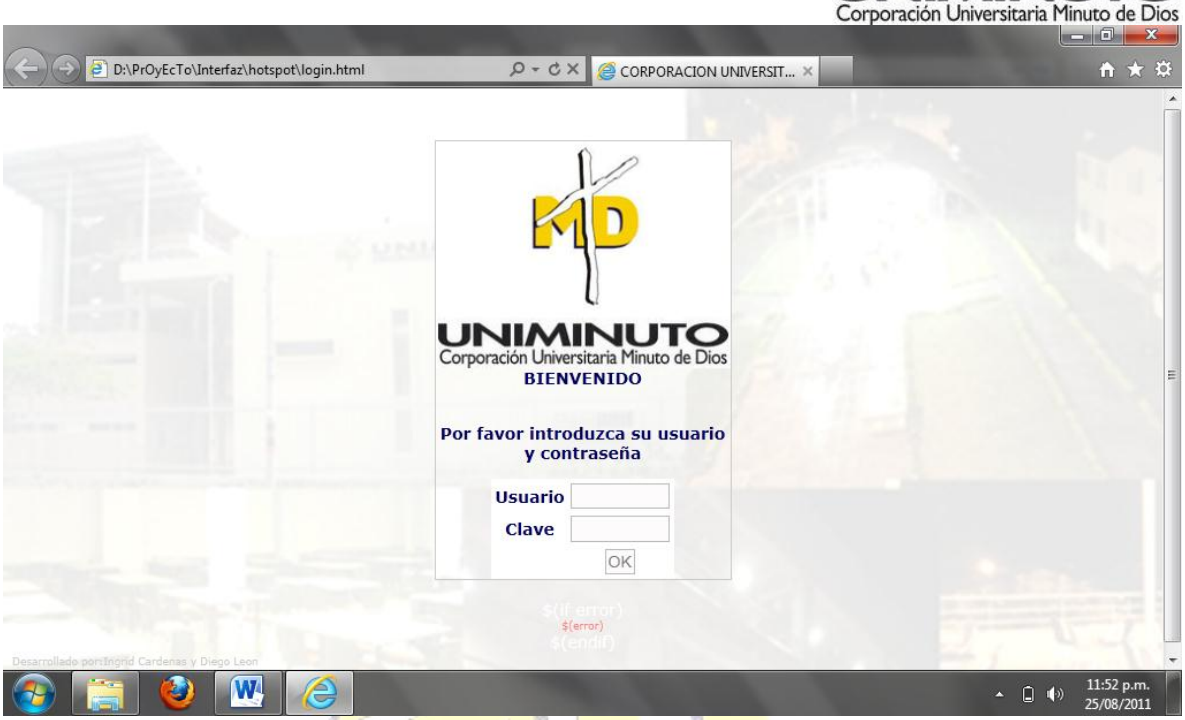
FUNCIONAMIENTO

El funcionamiento sera muy facil, pero debido a que por el momento se maneja un puerto que se deriba del proxy es necesario configurarle en el navegador para que pueda acceder al internet como se muestra en la siguiente imagen:



Configuracion del proxy

Despues de esto automaticamente cuando se escriba una direccion en URL del navegador nos aparecera la pagina inicial para autenticarnos del servidor Mikrotik, se introduce el usuario y la contraseña, y automaticamente nos carga la pagina que solicitamos en el URL del navegador teniendo presente que la sesión de cada usuario solo se puede efectuar una sola vez, no permitiendo sesiones múltiples, ni errores al introducir el usuario y la clave que sea incorrectamente (en caso de que sea alguno de estos errores en la parte de abajo saldrá un mensaje en rojo de cuál fue el error que ocurrió) y son correctos los datos introducidos de automáticamente entra a la página que solicito el navegador, claro está si esta no está bloqueada por el proxy.


D:\PrOyEcTo\Interfaz\hotspot\login.html
CORPORACION UNIVERSIT...
UNIMINUTO
Corporación Universitaria Minuto de Dios
BIENVENIDO
Por favor introduzca su usuario y contraseña
Usuario
Clave
OK
$(if error)
$(error)
$(endif)
Desarrollado por:Ingrid Cardenas y Diego Leon
11:52 p.m.
25/08/2011