DISEÑAR UN SISTEMA DE SEGURIDAD PARA PROTEGER LA TRANSMISIÓN DE DATOS DE LA EMPRESA XYZ CON SUS SEDES UTILIZANDO ROUTEROS MIKROTIK

LUIS RAFAEL ARGEL GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ - CUNDINAMARCA
2020

DISEÑAR UN SISTEMA DE SEGURIDAD PARA PROTEGER LA TRANSMISIÓN DE DATOS DE LA EMPRESA XYZ CON SUS SEDES UTILIZANDO ROUTEROS MIKROTIK

LUIS RAFAEL ARGEL GONZÁLEZ

Proyecto de grado para optar por el título:
Especialista en seguridad informática

Director de proyecto:
John Freddy Quintero Tamayo. MS (C)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ - CUNDINAMARCA
2020

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 2020

DEDICATORIA

Este proyecto de grado está dedicado principalmente a Dios, por la bendición del conocimiento y la fuerza para culminar con satisfacción este proceso.

A mis padres por la inspiración para ser cada día mejor.

A mi hija y a mi esposa que me han acompañado en este camino del conocimiento.

AGRADECIMIENTOS

Mis agradecimientos a todos los profesores de la Escuela de Ciencias Básicas Tecnología e Ingeniería de la Universidad Nacional Abierta y a Distancia que me han acompañado en este proceso de aprendizaje, en especial al ingeniero John Freddy Quintero Tamayo, que con paciencia y experticia me orientó en la elaboración de este proyecto. A mi esposa por ofrecerme apoyo en esta etapa de mi vida. A Dios por darme la salud y la oportunidad de seguir aprendiendo.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

La empresa de cobranza XYZ tiene cuatro sedes en diferentes ciudades del país (Bogotá, Bucaramanga, Medellín y Cali), cada una de ellas tiene su propia base de datos para hacer sus actividades y son independientes, ya que no tienen correspondencia con los datos de las otras, por tratarse de bases de datos distribuidas y no centralizadas. La sede principal está en la ciudad de Bogotá, en ella está el clúster de servidores (servidor de telefonía IP, servidor web, servidor FTP, servidor dedicado).

El objetivo es interconectar de manera protegida las otras tres sedes (Medellín, Bucaramanga y Cali) con la ciudad de Bogotá, para que puedan acceder a los servidores de la empresa y centralizar los datos para que cada sede tenga la información completa de todos clientes.

Palabras claves: Firewall, Reuters, servidores, enrutamiento, infraestructura, red, interconectar, clúster, centralizado, telefonía ip, ftp, web, internet, ancho de banda, vpn, swiches.

ABSTRACT

The collection company XYZ has four offices in different cities of the country (Bogotá, Bucaramanga, Medellin and Cali), each of them has its own database to do their activities and they are independent, since they do not have communication with the information of the others, because they are distributed and non-centralized databases. The main headquarters is the city of Bogotá, where the server cluster is located (IP telephony server, web server, FTP server, dedicated server).

The objective is to interconnect in a protected way the other three locations (Medellin, Bucaramanga and Cali) with the city of Bogotá, so that they can access the company's servers and centralize the data so that each headquarters has the complete information of all clients.

Keywords: Firewall, Router, servers, routing, infrastructure, network, interconnect, cluster, centralized, ip telephony, ftp, web, internet, bandwidth, vpn, swiches.

INTRODUCCIÓN

Las empresas están expandiendo su actividad comercial en un mundo cada vez más estricto, y la empresa de cobranza XYZ no es la excepción, esta tiene su centro principal en la ciudad de Bogotá y ha incursionado en otras ciudades de Colombia entre las que se encuentran Medellín, Cali y Bucaramanga. El hecho de tener varias sedes, le implica contar con una buena estructura de intercomunicación entre sí y seguridad en la entrega de los datos que se manejan.

No obstante, la situación que se presenta en la empresa de cobranza XYZ es que las sedes de Medellín, Cali y Bucaramanga no tienen la forma de acceder de manera segura a los servidores que están en el centro principal situada en la ciudad de Bogotá, lo cual constituye un riesgo para la integridad de los datos. Por ende, el objetivo trazado es crear un método que ofrezca la seguridad de la transmisión de los datos, evitando que personas ajenas o no autorizadas tengan acceso a la información. Para el efecto, el proyecto necesita respaldarse en el uso de procesos que permita reducir errores y extender su efectividad. La metodología que se utiliza es el Diagrama de Gantt, porque el proyecto se realizara por faces.

De las opciones para hacer que las sedes de la empresa de cobranza XYX puedan comunicarse de forma segura entre sí, se enfatizará en una solución que consiste en crear una red privada virtual en la cual participen todas las dependencias de la empresa, como si estuvieran en una misma red LAN, para lo anterior, el elemento que se utiliza es el RouterOS Microtik, dispositivo que tiene varias configuraciones que ayudan a la protección de la red y los datos compartidos entre las sedes.

Resulta fundamental para la empresa fiscalizar las acciones de los beneficiarios de la red, siendo el mecanismo idóneo para ello el RoutersOS Mikrotik, ya que permite crear grupos separados y asignar a cada grupo un ancho de banda acorde a su necesidad. Otra configuración importante es la creación de pool de direcciones de IP`s para cada tarjeta de Ethernet que tenga el router, para identificar los equipos (pc’s, servidores, teléfonos ip, impresoras) que están conectados en cada uno de las interfaces del router.

Es importante también aplicar la configuración de control del tiempo que cada equipo (pc’s) de usuario requiere para estar conectado a internet, lo cual amplía la seguridad en la red y limita los posibles puntos de acceso que podría utilizar los atacantes para infiltrarse en la misma. Para controlar lo que puede asociarse o salir de la red de cada una de las sedes, y lograr que solo pase el tráfico de información deseada es necesario crear un firewall que aporta una función muy importante en la seguridad de la redes de la empresa XYZ.

1. PLANTEAMIENTO DEL PROBLEMA

Las empresas de todo el mundo cada día tienden a ampliar su cobertura de mercado, maximizar sus ganancias y obtener reconocimiento que les permita sostenibilidad y crecimiento a largo plazo, lo cual también implica asumir retos y controlar los riesgos latentes en el camino. Los riesgos son diferentes para cada empresa, dependiendo del ámbito en que se desarrolle la actividad económica.

La empresa de cobranza XYZ por su actividad maneja bases de documentos, con datos personales de sus clientes y por ende se encuentra inmersa en el mundo de la tecnología e involucrada con la aplicación de la regulación colombiana relacionada con el manejo de datos personales. Entonces sus peligros están relacionados con la seguridad de los datos que por disposición legal debe garantizar.

En esa búsqueda de mejora continua la empresa de cobranza XYZ ha encontrado que las sedes de Medellín, Cali y Bucaramanga no tienen la forma de acceder de manera segura a los servidores que están en el despacho principal situada en la ciudad de Bogotá, motivo por el cual está en riesgo no solo la información de sus clientes sino la razón de ser de la organización. En la sede principal de la empresa está el clúster de servidores (web, dhcp, ftp, dns, correo) que contiene toda la información de la organización y las otras sedes acceden a la misma por medio de llamadas telefónicas (línea fija, celular) y correo electrónico que no son de dominio de la empresa o por sistemas que no están conectados directamente con la empresa XYZ.

Al utilizar esta forma de comunicación los procesos que realizan cada una de las sedes (Medellín, Bucaramanga y Cali) son muy lentos y están afectando el funcionamiento correcto de las actividades programadas por la organización, porque están en función del tiempo de respuesta de la sede principal. Esta forma de operación ha demostrado ineficiencia, porque está poniendo en riesgo la inversión económica hecha a cada una de las sedes (Medellín, Bucaramanga y Cali).

Para mejorar la efectividad en cada una de las actividades, resulta necesario para la empresa XYZ crear un sistema seguro de transmisión de datos y comunicación eficiente para que las sedes de Medellín, Bucaramanga y Cali puedan acceder al clúster de servidores en despacho principal situada en la ciudad de Bogotá.

2. JUSTIFICACIÓN

Actualmente la empresa XYZ tiene su despacho en la ciudad de Bogotá, en el cual ha desarrollado su actividad desde hace 20 años. Para expandir su servicio abrió tres nuevas sucursales en Medellín, Bucaramanga y Cali, ciudades donde ya tiene un número considerable de clientes. Las bases de datos de las cuatro sedes no tienen comunicación entre sí, por lo cual hacen uso del teléfono y correo electrónico para compartir la información que necesiten.

No manejar la información en línea tiene desventajas para la compañía, ya que no se comparten los datos en tiempo real, sino en la medida de la disponibilidad de tiempo tanto del emisor y receptor, conllevando a retrasos en las actividades y a la duplicidad de funciones por la doble digitación.

Dentro de los objetivos de la empresa XYZ están los de mejorar sus ingresos y ser líder en el mercado, para lo cual es prioritario subsanar el tema de comunicación online entre las bases de datos de las cuatro sedes, a través de infraestructura segura. Adicionalmente se obtienen los siguientes beneficios:

- Mejor estructura y las operaciones o actividades estarían integradas.
- Comunicación protegida entre las sedes.
- Información de los movimientos de cada sede en tiempo real.

Por otra parte, en Colombia existe normatividad o regulación respecto de la defensa de los documentos personales contenida en la Ley 1581 de 2012, a la cual debe ceñirse la empresa de cobranzas XYZ por manejar bases de datos que contienen información de personas naturales. Garantizar la protección de la información que le ha sido confiada, le evita sanciones.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de seguridad para proteger la transmisión de datos de la empresa XYZ con sus sedes utilizando routerOS mikrotik.

3.2 OBJETIVOS ESPECÍFICOS

- Instalar en cada una de las sedes un routerOS mikrotik.
- Instalar el winbox en el equipo administrador en todas las sedes para el acceso al mikrotik.
- Limitar el ancho de banda, hora y fecha de uso para algunos usuarios.
- Activar el servidor SNTP y SNTP CLIENT al router mikrotik.
- Crear relación de IP y Mac.
- Crear el firewall para controlar el tráfico de información con las reglas establecidas por la organización.
- Asegurar el programa winbox en cada una de las sedes.
- Bloquear el ICMP en el equipo router mikrotik.
- Crear el servidor DHCP en el router mikrotik en cada una de las sedes.
- Crear una VPN para establecer conexión con todas las sedes.
- Crear el backup del router mikrotik

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

En el presente las redes de comunicación están presentes en cualquier actividad humana. Las redes son un complejo sistema formados por muchos y diferentes dispositivos (pc, impresores, teléfonos) trabajando y comunicándose entre ellos, e intercambiando información de toda clase como por ejemplo: documentos, fotos, música, videos. Esta información es usada y manipulada por personas. (Alonso, 2014).

El mundo de los sistemas de información está compuesto por una gran variedad de arquitectura de redes complejas, y ha tomado un gran papel en las empresas hoy en día para agilizar sus actividades comerciales o de producción, y esto ha llevado a las compañías que sean más profesionales en el mercado. (Carpentier, 2016).

Una red de información también es un conjunto de varios elementos debidamente organizados, relacionados y coordinados, encargados de proporcionar el funcionamiento de una empresa o de cualquier actividad que implique el manejo de datos. Estos elementos son: primero sería los recursos. Pueden ser físicos, como ordenadores, sus periféricos y conexiones, los lógicos como sistemas operativos y programas de aplicaciones. Segundo el equipo humano, que está compuesto por las personas que trabajan para la empresa. Y por último la Información. Conjunto de datos organizados que tienen un fin. (López, 2010)

Otro concepto de una red es un recurso de conexión que deja a personas o un grupo de ellas compartir información y sus servicios. La tecnología que usan las redes informáticas están compuestas por un conjunto de herramientas que permiten a los equipos (pc, impresoras) compartir información y recursos. Una red está formada por equipos (pc) llamados nodos. Para comunicarse entre los nodos utilizan protocolos o lenguajes que se puedan entender entre ellos. (Bertolín, 2008).

Entendiendo el significado de red en el área de la informática, el siguiente tema que se debe comprender es sobre la seguridad y se puede interpretar como seguridad una propiedad de algún sistema (informático o no) que nos advierte que ese sistema está exento de toda amenaza, perjuicio o fatalidad, y que es, en cierta forma, eficaz. Como esta propiedad, individualizando para el tema de los sistemas

operativos o redes de activos (impresoras, teléfonos, computadores), es muy complicado de alcanzar (según la mayoría de peritos, irrealizable). (Huerta, 2002). La seguridad informática es la disciplina que con base en políticas y normas interiores y exteriores de la empresa se encargan de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. (Urbina, 2016).

La seguridad tangible envuelve todo lo relacionado a los equipos informáticos: computadores de propósito corriente, servidores con funciones especiales e infraestructura de red. La seguridad lógica se trata de las diferentes aplicaciones que trabajan en cada uno de estos equipos como los sistemas operativos, programas de aplicación. (Buendía, 2013).

Cuando se habla de seguridad en un sistema informático se puede encontrar con diferentes tipos de seguridad, que puede ser activa o pasiva (Santos, 2014). Se puede entender que la seguridad activa consiste en aquellas medidas que se usan para encontrar las amenazas, y en el caso que se encuentres generar los mecanismos apropiados para evitarlo. Un ejemplo de seguridad activa puede ser la detección de una clave débil de acceso. Seguridad pasiva consiste en un conjunto de medidas para que cuando se presente un ataque en un sistema informático tenga un impacto lo menor posible y activar los mecanismos de recuperación. Por ejemplo son los Backup o copias de seguridad de la información que es relevante para la compañía. (Molina, 2004).

La inestabilidad de las estructuras informáticas y de las redes de computadores va mucho más allá de los programas informáticos maliciosos que son conocidos. El uso de dispositivos de defensa es una prioridad para las empresas. Los delincuentes de una red de computadores no requieren estar en contacto directo con un equipo que está conectado a la red; los datos pueden ser sencillamente duplicados, transferidos, cambiados o arruinados cuando son difundidos por la red. Como consecuencia, si no se tiene de los dispositivos de defensa apropiado resulta complicado determinar al delincuente: no hay huellas y el marco legal no está adecuadamente renovado para enfrentar esta clase de amenazas. (Soriano, 2014).

Los atacantes pertenecen a un mundo escondido que es llamado mundo underground, porque es una asociación de sujetos que se mantienen «ocultos» para mostrarse entre ellos sus competencias y destrezas (Asensio, 2006). Estos conocimientos y experiencias sobre como han hecho los abusos informáticos de los sistemas son compartidas en foro.

Una de las primeras definiciones sobre los abusos informáticos, fue la mostrada por PARKER, que precisó como “cualquier accidente vinculado con la tecnología de los computadores en el que la víctima padeció o pudo haber padecido un daño y el autor, deliberadamente, logró o pudo haber logrado un beneficio. (Hernández, 2009).

Cada día, se crean nuevos métodos de intentos de intrusión. Los intentos de intrusión son aquellos intentos que pueden afectar negativamente a la confiabilidad, integridad y disponibilidad de la información de un equipo (PC) o que intente evitar los mecanismos de seguridad que se hay establecido (Tejada, 2015). Es por ello la obligación de una táctica perfecta de seguridad, de manera de impedir pérdidas y defectos en los sistemas. A lo antes mostrado se agregan inseguridades internas (misma corporación), que son un elemento de peligro no menor, y por lo tanto, coexiste alta posibilidad de desgaste de capital y repercusiones en la confianza por parte de beneficiarios, consumidores y accionistas de negocios. (Salazar, 2008).

El primero de los tres principios de la seguridad de la información que usamos es la integridad, la cual nos posibilita certificar que el dato no ha sido afectado en su contenido, por tanto, esta intacto. El principio de la confidencialidad de la información tiene como intención el asegurar que sólo el individuo correcto entre a la información que deseamos mostrar. El método que se sutiliza para cumplir los primeros principios (la integridad y la confidencialidad) es la criptografía asimétrica que opera con un par de claves (una pública y otra privada) para la transferencia de datos. Las dos claves son creadas en el mismo instante, la clave pública se da a las terceras partes, y la clave privada se habrá de almacenar de modo que nadie tenga acceso a ella. (Sarubbi, 2008).

Una vez que nos certificamos que el dato correcto llegue a los receptores o personas correctas, ahora lo que debemos asegurar es que llegue en el tiempo adecuado, y exactamente de esto trata el tercer principio de la seguridad de la información: la disponibilidad. Para que los datos se puedan utilizar, deberán estar libres o disponibles. (Clavijo, 2006). (Sánchez, 2014).

La información es uno de los activos más valiosos de las organizaciones, por ello se diseñan políticas que permitan el manejo o tratamiento adecuado y garantizar su seguridad. En el diseño del sistema de seguridad de la información es necesario conocer algunos conceptos básicos y aplicarlos de forma correcta, entre los cuales se señalan los siguientes:

Firewall (cortafuego): Es un sistema de red que está encargado de separar redes informáticas, controlando el tráfico existente entre ellas. Este control permite o deniega el paso de la comunicación entre redes. (Castellanos, 2014)

Criptografía: Es la aplicación de los métodos matemáticos para proteger los datos que son enviados por la red de modo que no pueda ser leída por personas no autorizadas. (Granados, 2006)

Exploit: Es un programa usualmente escrito en el lenguaje C o ensamblador, que busca las situaciones necesarias para explotar una fragilidad de seguridad. (Gallo, 2011)

Sniffer: Es un programa que intercepta toda la información que pase por la interfaz de red. Con la información obtenida se almacena en un dispositivo para después ser analizada. (Hernández, 2000)

DDoS: (Denegación de servicio distribuido) es una arremetida a una red que causa que un servicio sea inaccesible por cualquier usuario. (Rus, 2007)

MAN: (Redes de área metropolitana), es una red que está en una ciudad o una zona suburbana. Está formada de 2 o más LAN adentro de un plano geográfico. (Kurose, 2010)

SAN: (Redes de área de almacenamiento) Es una red de servidores que se usa para transportar información. (Argonza, 2017)

WAN: (Redes de área amplia). Relacionan redes de beneficiarios dentro de un área geográfica muy grandes como por ejemplo: pises. (Kurose, 2010)

VPN: Es una red privada virtual que se crea dentro de una instalación de red pública. (Tenelema, 2016)

Vulnerabilidad: Es una deficiencia de un programa que puede permitir que una persona no autorizada entre a un sistema. (Aguilera, 2010)

VoIP: Es una señal de voz digitalizada que es enviada por la red utilizando el protocolo IP. (Domínguez, 2016)

VLAN: Es una red de zona virtual o VLAN (Virtual Local Area Network) es una red lógica independiente dentro de una red física. (Molina, 2012)

TCP/IP: Protocolo de control de transmisión/Protocolo Internet.

Routers: También es llamado enrutador. Es un hardware que permite interconectar computadoras. Su objetivo es establecer qué ruta es la más apropiada para mandar un paquete de datos a un destino. (Kurose, 2004).

Ancho de banda: Es la conjunto de información (bits) de datos que se logra mandar a través de un enlace de red en un período definido. Por ejemplo MegaBits/segundos (Mbps). (Longoria, 2005).

Dirección IP: Es un número que es asignado a un equipo para poder identificarlo en la red.

Mac: (Media Access Control) es un número de 6 bloques de dos caracteres hexadecimales que se le asigna a una tarjeta de red.

ICMP: Es un protocolo de control de mensajes de Internet (Internet Control Message Protocol), es parte del conjunto de protocolos IP. Este es utilizado para mandar avisos de equivocación e información, por ejemplo, que un equipo no puede ser localizado. (Peláez, 2002).

DHCP: Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol) es un protocolo de red de modelo cliente/servidor, donde un servidor DHCP establece activamente una dirección IP. (Velásquez, 2013).

NTP: (Network Time Protocol) protocolo de tiempo de red. Es un protocolo de Internet para coincidir los relojes de los sistemas informáticos. (Skeie)

NTP CLIENT: Es una aplicación cliente / servidor. Cada estación de trabajo, enrutador o servidor debe estar equipado con un software cliente NTP para concordar su reloj con el servidor de hora de la red. (Skeie)

Winbox: Es una aplicación que se utiliza para configurar los equipos router mikrotik

PPTP: Point-to-Point Tunneling Protocol. Admite crear un túnel de forma transparente al distribuidor de Internet. (Ternero, 2003)

L2TP: (Layer 2 Tunneling Protocol). Protocolo dirigido al proveedor. Admite crear un túnel de modo transparente al cliente (habitualmente se emplea junto con IPSec). (Ternero, 2003)

4.2 MARCO TEÓRICO

La información es uno de los activos más valiosos para toda organización, por ende requiere protección y salvaguardarla de posibles ataques informáticos para sustraerla ilegalmente. Los datos personales que fueron encomendados a otras personas naturales o jurídicas deben ser tratados de tal forma que se evite el menoscabo o la pérdida de los mismos. Cuando se efectúa el tratamiento adecuado de datos y se controlan los riesgos para preservar la información, es porque las empresas tienen establecidas políticas de seguridad de la información idóneas.

En la seguridad informática existen muchos temas a tener en cuenta para proteger la información contenida en un equipo o dispositivo informático. En la actualidad no hay un lugar donde no haya un computador con información importante almacenada, la cual es de propiedad del dueño o usuario del equipo; así mismo la responsabilidad del cuidado del equipo y custodia de los datos se ha extendido a todos los usuarios, ya que tener un equipo como es la computadora implica una serie de cuidados y manejo de riesgos, desde mantenerlo limpio hasta proteger su contenido; son diversos aspectos a tener en cuenta, empezando por el sistema de alimentación eléctrica, se debe prevenir cualquier falla que pueda suceder, como suspensión del servicio**,** cambios bruscos de voltaje que conllevan a dañar el equipo y por ende la información que contiene.

Para prevenir incidentes relacionados con el suministro de energía, es necesario conectar la PC en una UPS, que es un dispositivo que proporciona electricidad por un tiempo determinado, con el objetivo de disponer de tiempo para guardar los documentos y apagar el equipo de modo adecuado, sin el temor de perder información. Si el sistema es más complejo como un conjunto de servidores que deben estar en servicio las 24 horas al día, los 7 días de la semana, el sistema de protección eléctrica será mucho más robusto como una planta de energía eléctrica, ya que tendrá que suministrar voltaje hasta que se solucione el problema.

El segundo tema a tratar es sobre los programas maliciosos o virus, los cuales consisten en códigos que pueden interferir en las actividades personales o laborales realizadas a través de la computadora. En este aspecto el riesgo es alto, ya que se puede eliminar información histórica o actual de alta importancia. La forma de evitar o prevenir este riesgo es instalando en el equipo un antivirus, este proceso de protección cuando se trata de equipos individuales, es decir no conectados en red local ni por internet.

La protección de equipos comunicados en red o conectados a través de internet, es más compleja dado que usan más herramientas para la ejecución de sus actividades. Cuando los equipos están conectados a internet, existe mayor riesgo de tener ataques a los sistemas, por ejemplo: DDoS o interceptación de la información que es enviada por correo, etc. Para evitar estos riegos se debe crear un sistema de seguridad eficiente, empezando por controlar la entrada de tráfico a la red instalando un firewall, y por otra parte encriptar los datos privados para que solo logren ser examinados por las personas a las que van destinadas y no por los intrusos. El proceso de encriptación se efectúa mediante un algoritmo que usa una clave y produce un mensaje cifrado, el cual llega al destino para que se aplique el proceso inverso y obtener el mensaje original.

Por su parte, para que una empresa mantenga una conexión de forma segura con sus sucursales que están otra ciudad o país, debe crear una red privada virtual (VPN) que puede unir las agencias con la sede principal y formar una sola red. Al crear esta VPN, tiene todas las protecciones adecuadas para conservar y compartir la información de forma segura.

El principal elemento que se utiliza para crear una red privada virtual (VPN), es un router. Este dispositivo debe estar instalado en cada una de las sedes que pertenecerán a la VPN. La ventaja de usar el router, es que se puede configurar según las necesidades, por ejemplo: restringe el ancho de banda a un equipo o a un grupo de equipos que no necesitan estar conectados a internet para hacer las actividades asignadas y pasarlos a otras que si lo necesitan. Controlando el acceso a internet a los equipos, aumenta la seguridad en la red porque también se puede controlar el tiempo que los equipos tengan conexión a internet, disminuyendo los puntos de entrada de los atacantes que quieran ingresar a la red.

Otras configuraciones que se pueden hacer en el router y que son muy relevantes en creaciones de redes son: Crear un firewall para controlar el tráfico de información tanto de salida como de entrada, logrando así que solo entre y salga la información necesaria incluyendo los mensajes ICMP (protocolo de control de mensajes de Internet). Y por último la creación de un servidor DHCP (Dynamic Host Configuration Protocol) que asigne grupos de direcciones IP a cada uno de los puertos Ethernet que tenga habilitados el router.

Para hacer las configuraciones en el router mikrotik se puede hacer de varias forma, la primer es utilizando un navegador (Chrome, Firefox, etc.), y el segundo utilizando un programa que está instalado en el equipo del administrador de sistema. Este programa es el winbox, y este debe estar asegurado de tal forma que solo lo pueda usar las personar autorizadas, porque de no estarlo correría un gran riesgo la configuración de seguridad de la red.

5. MARCO LEGAL

La mayoría de las empresas utilizan la tecnología para enviar de forma instantánea información privada de mucho valor, requiriendo que esos datos sean conocidos solamente por las personas involucradas en el asunto, pero hay terceros ajenos que están interesados y dedicados a acceder a la misma para hacer actividades ilícitas, como acceso abusivo, obstaculización ilegítima a un sistema informático, interceptación de datos, suplantación, etc. Existen leyes que castigan o condenan esas actuaciones ilícitas, para el caso de Colombia se ha creado la Ley 1273 de 2009, que crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

La empresa de cobranzas XYZ maneja información personal de sus clientes, por lo tanto debe sujetarse a la siguiente normatividad:

5.1 ARTÍCULO 15 CONSTITUCION POLITICA DE COLOMBIA (ALCALDIA MAYOR de Bogotá, 2018)

El artículo 15 de la carta magna Colombiana establece que "*todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas*.

Por lo anterior la empresa de cobranzas XYZ debe estar en capacidad de administrar los datos privados recogidos de sus clientes y por ende manejar su política de tratamiento de datos personales.

5.2 LEY 1273 DE 2009

La Ley 1273 de 2009, consta de dos capítulos, el primero reglamenta las sanciones respecto de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; mientras que el capítulo segundo trata de los atentados informáticos y otras infracciones.

Las sanciones que estipula esta Ley consisten en pena de prisión y multa. De acuerdo a la gravedad de la actuación ilícita la pena de prisión oscila entre treinta y seis (36) a ciento veinte (120) meses y las multas entre 100 y 1500 salarios mínimos legales mensuales vigentes.

Los empleados de la empresa XYZ están expuestos a incurrir en cualquiera de las infracciones por el acceso a los datos personales de los clientes, siendo los principales los siguientes:

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La ley 273 de 2009 también señala las circunstancias de agravación punitiva, que consiste en aumentar las penas imponibles si la conducta se comete:

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Los atentados informáticos y otras infracciones que se castigan son:

Hurto por medios informáticos y semejantes.

Transferencia no consentida de activos.

5.3 LEY 1581 DE 2012

La ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, establece como objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Constituye una responsabilidad para la empresa XYZ centralizar y organizar sus bases de datos, de tal forma que la información para las cuatro sucursales sea la misma.

5.4 DECRETO 1377 DE 2013

El Decreto 1377 de 2013 tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Trata aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información.

Para la empresa XYZ resulta fundamental este decreto, por cuanto puntualiza la política de manejo de datos personales y enfatiza en la aprobación por parte del titular de la información.

6. MARCO ESPACIAL

La empresa XYZ abarca cuatro ciudades de Colombia: Bogotá, Medellín, Cali y Bucaramanga, las cuales estarán interconectadas virtualmente y formarán una LAN. En el próximo año estará abriendo otras sucursales en otros países como Ecuador, Perú, Brasil y Argentina. El sistema de Seguridad de la información debe proteger la transmisión de datos entre las cuatro sedes.

7. MARCO METODOLÓGICO

7.1 METODOLOGÍA

La metodología que es utilizada es llamada diagrama de Gantt, la cual es una herramienta gráfica y permite mostrar el tiempo del proyecto que se trabajará en fases, cada una con su tiempo de ejecución. En este proyecto tendrá 4 fases que son las siguientes:

Fase 1: Levantamiento de activos en cada sede.

Con el fin de efectuar la configuración del router Microtik, se recopilará la información de todos los activos informáticos que tiene la empresa XYZ (servidores, impresoras, computadores) en cada una de las sedes (Bogotá, Medellín, Bucaramanga y Cali).

Fase 2. Diseño.

En esta parte se describe como debe funcionar el sistema después de que se haya instalado el routers Mikrotik en cada una de las sucursales, y porque es el apropiado para la empresa.

Fase 3. Instalación y configuración de los routers Mikrotik en las sedes.

En esta fase se harán las configuraciones a los routers Mikrotik de las sedes (Bogotá, Medellín, Bucaramanga y Cali). Para la configuración de los routers Mikrotik se empleará un computador en cada sede que tendrá instalado una aplicación llamada Winbox que facilita la programación de los routers Mikrotik.

Fase 4. Resultado y Prueba de comunicación de las sedes.

En esta fase se muestra como queda conectada físicamente los equipo (router Mikrotik, modem, switches, PC`s) en cada una de las sedes que tiene la empresa XYZ, y se validaran las comunicaciones de cada uno de los routers Microtik de las sedes de Medellín, Cali y Bucaramanga con la sede principal que está en la ciudad de Bogotá. Para saber que errores se encuentran en las configuraciones de dada uno de los routers Mikrotik y corregirlos.

Fase 5. Recomendaciones.

Se harán las recomendaciones necesarias para que los routers mikrotik y los elementos que forman parte de la red de la empresa XYZ funcionen adecuadamente.

7.2 METODOLOGÍA EMPLEADA EN EL PROYECTO

El proyecto se desarrollará en las siguientes fases:

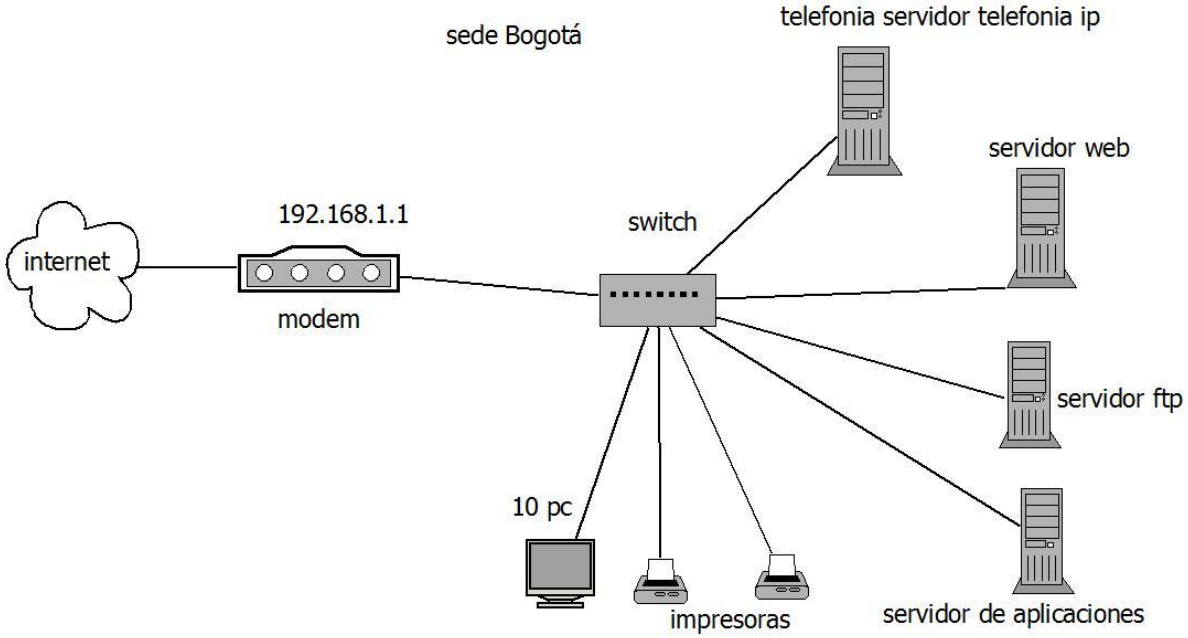
Fase 1. Levantamiento de activos.
Fase 2. Diseño.
Fase 3. Instalación y configuración de los routers Mikrotik en las sedes.
Fase 4. Resultado y pruebas de comunicación.
Fase 5. Recomendaciones.
.

7.2.1 Fase 1. Levantamiento de activos en las sedes de Bogotá, Medellín, Bucaramanga y Cali.

Se procede al levantamiento de los activos de la empresa Cobranzas XYZ en sus diferentes sedes:

Sede Bogotá

Figura 1. Diagrama de la red de la sede de Bogotá



Fuente. El autor

En la figura 1 están especificadas las conexiones de los activos de la sede de Bogotá como son: Servidores web, ftp, servidor de aplicaciones, PC`s, switch, modem, teléfonos IP`s. En la sede de la ciudad de Bogotá se está usando la tipología estrella, porque todos los dispositivos están conectados a un punto central, en este caso a un switch, y el switch se comunica con el modem que es suministrado por la empresa que esta prestado el servicio de internet.

Tabla 1. Descripción de activos de la sede Bogotá

Equipos	Descripción
Un servidor de telefonía IP	Encargado de administrar el Call Center. A través del cual se encuentran configuradas todas las extensiones de los agentes y personal administrativo de la empresa, así como los planes de marcación establecidos para el enrutamiento de las llamadas.
Un servidor Web	En el cual se encuentra el sitio web de la empresa y algunos servicios de mercadeo.
Un servidor FTP	Destinado para almacenar y compartir entre los funcionarios toda la información interna de empresa.

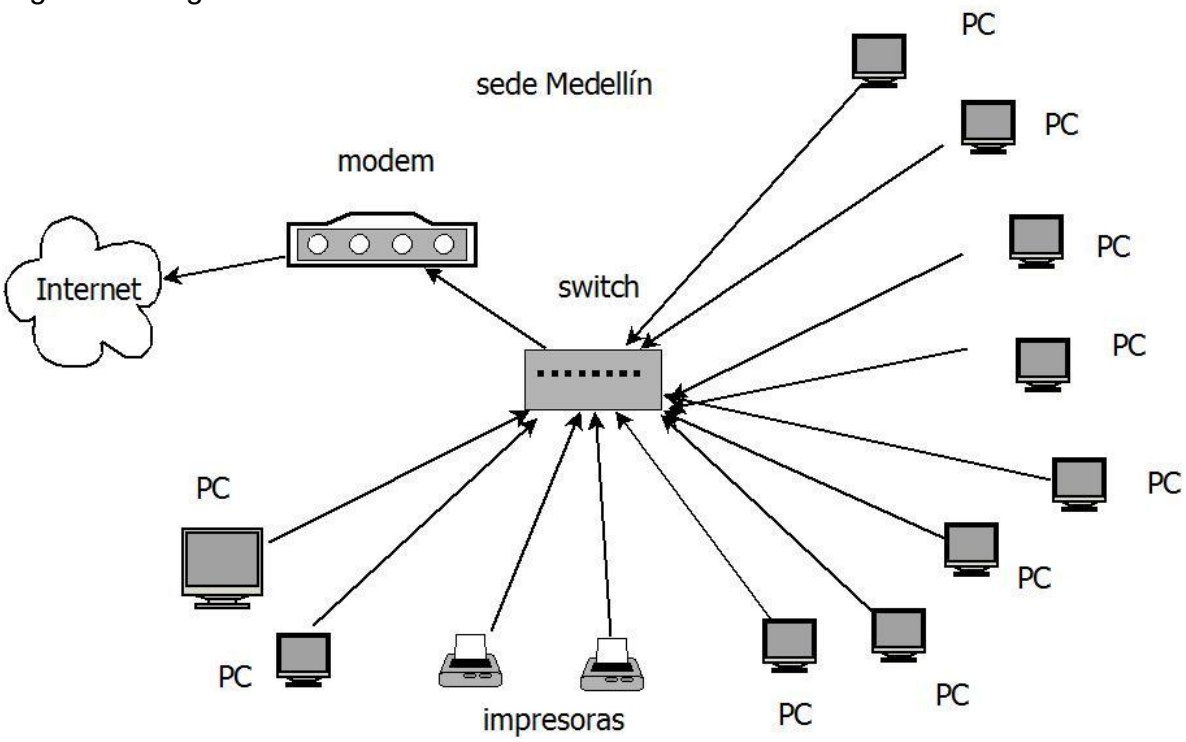
Un servidor de aplicativo	Encargado de la gestión de la información suministrada por los Bancos y a través de la cual, se realizan los procesos de consulta de los clientes por parte de cada agente, orientada a la recuperación de cartera.
10 pc Intel Core i7 Nehalem	Actividades comerciales
2 impresoras Epson Ecotank L4160	Para imprimir los documentos soporte requeridos en forma impresa.

Fuente. El autor

En la tabla 1 se encuentran registrados todos los activos (PC's, impresoras, servidores) que fueron encontraron en cada una de las oficinas que conforman la sede de la ciudad de Bogotá con su respectiva descripción. La información contenida en la tabla 1 se utilizará para asignar las restricciones solicitadas por la empresa XYZ.

Sede Medellín.

Figura 2. Diagrama de la red de la sede de Medellín



Fuente. El autor

La figura 2 refleja cómo están conectados los activos de la sede de Medellín. Se observa que a diferencia de Bogotá no cuenta con servidores. La tipología que se está usando en la sede de la ciudad de Medellín es la tipología estrella, porque todos los dispositivos están conectados a un punto central, en este caso a un switch. El switch se comunica con el modem que es suministrado por la empresa que esta prestado el servicio de internet.

Tabla 2. Activos de la sede de Medellín

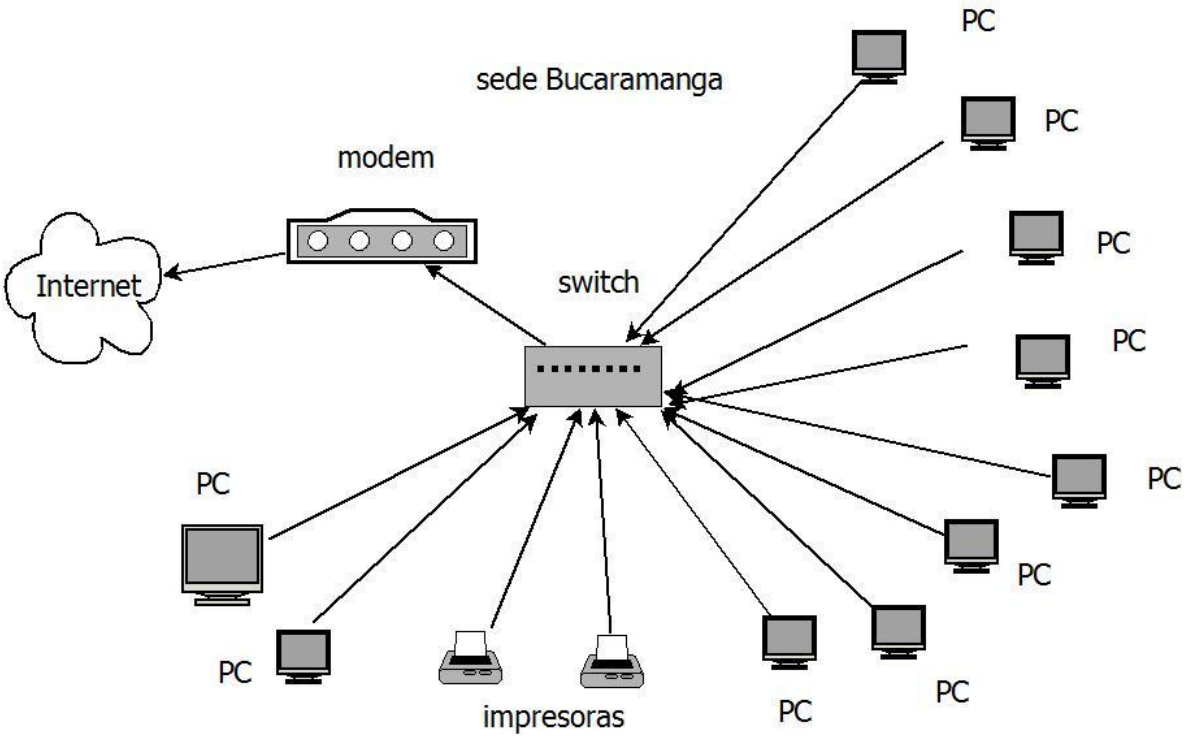
Equipos	Descripción
10 pc Intel Core i7 Nehalem	Actividades comerciales
2 impresoras Epson Ecotank L4160	Para imprimir los documentos soporte requeridos en forma impresa.

Fuente. El autor

En la tabla 2 se hallan registrados todos los activos (PC's, impresoras) que fueron encontraron en cada una de las departamentos que conforman la sede de la ciudad de Medellín con su descripción. La información presentada en la tabla 2 se utilizará para asignar las limitaciones solicitadas por la empresa XYZ.

Sede Bucaramanga.

Figura 3. Diagrama de la red de la sede de Bucaramanga



Fuente. El autor

En la figura 3 se visualiza como están conectados los activos de la sede de Bucaramanga. La tipología que se está usando en la sede de la ciudad de Bucaramanga es la tipología estrella, porque todos los dispositivos están conectados a un punto central, en este caso a un switch. El switch se comunica con el modem que es suministrado por la empresa que esta prestado el servicio de internet. Se observa que a diferencia de la sede de Bogotá, esta no cuenta con servidores.

Tabla 3. Activos de la sede de Bucaramanga

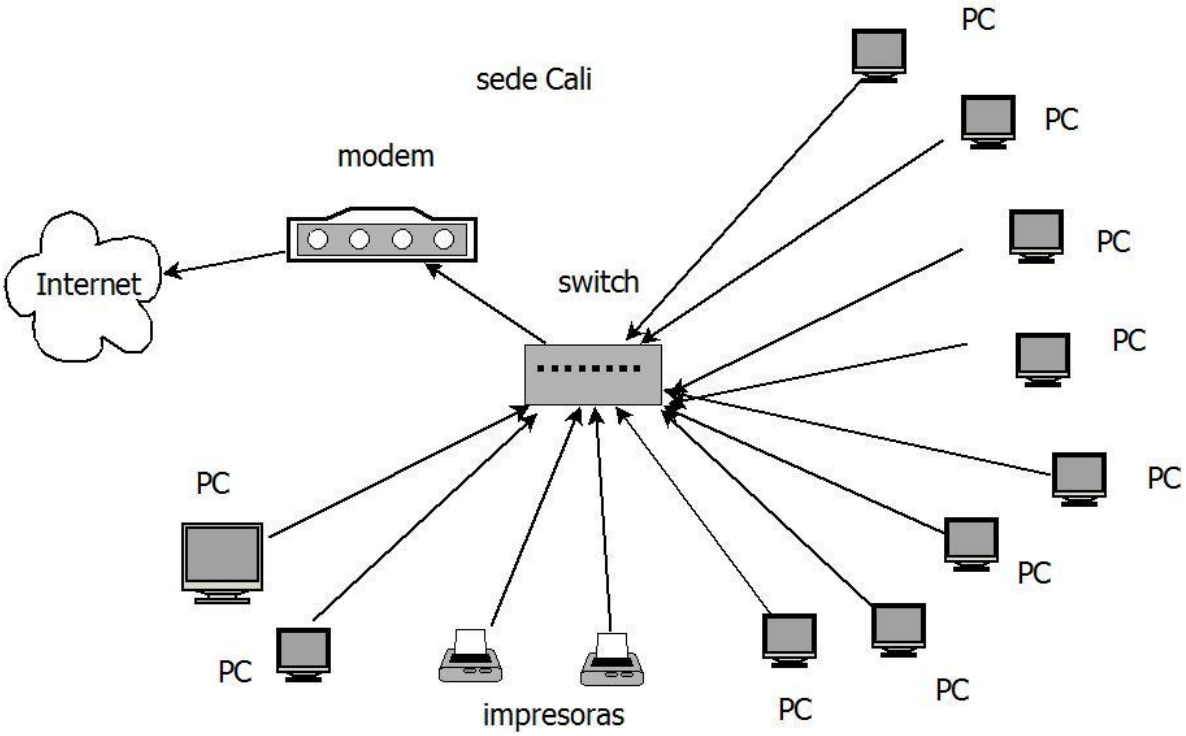
Equipos	Descripción
10 pc Intel Core i7 Nehalem	Actividades comerciales
2 impresoras Epson Ecotank L4160	Para imprimir los documentos soporte requeridos en forma impresa.

Fuente. El autor

En la tabla 3 se muestran todos los activos (PC's, impresoras) que fueron encontraron en cada una de los sitios de trabajos que conforman la sede de la ciudad de Bucaramanga con su respectiva descripción. La información contenida en la tabla 3 se utilizará para determinar las restricciones solicitadas por la empresa XYZ.

Sede Cali

Figura 4. Diagrama de la red de la sede de Cali



Fuente. El autor

En la figura 4 se visualiza como están conectados los activos de la sede de Cali. La tipología que se está usando en la sede de la ciudad de Cali es la tipología estrella, porque todos los dispositivos están conectados a un punto central, en este caso a un switch. El switch se comunica con el modem que es suministrado por la empresa que esta prestado el servicio de internet. Se observa que a diferencia de la sede de Bogotá, esta no cuenta con servidores.

Tabla 4. Activos de la sede de Cali

Equipos	Descripción
10 pc Intel Core i7 Nehalem	Actividades comerciales
2 impresoras Epson Ecotank L4160	Para imprimir los documentos soporte requeridos en forma impresa.

Fuente. El autor

En la tabla 4 se encuentran registrados todos los activos (PC's, impresoras) que fueron localizados en cada una de las oficinas o departamentos que conforman la sede de la ciudad de Cali con su respectiva descripción. La información incluida en la tabla 4 se utilizará para asignar las restricciones solicitadas por la empresa XYZ.

7.2.2 Fase 2. Diseño.

En este punto se describe rápidamente los procesos que debe de cumplir el sistema para desarrollar su función de forma correcta y transparente para el usuario.

7.2.2.1 utilizar diferentes programas para la configuración del sistema.

El sistema puede ser configurado utilizando diferentes aplicaciones como por ejemplo: Google crome, Telnet, que son aplicaciones que están instaladas en cualquier computador. También puede instalar otras aplicaciones como Winbox, Putty.

7.2.2.2 Selección de servidores.

El sistema debe de facilitar la selección de servidores que se necesitan en la empresa en el momento solicitado.

7.2.2.3 Control de dispositivos en la red.

Limita la cantidad de dispositivos que puede haber en una red, controlando la conexión de dispositivos no deseados.

7.2.2.4 Asignación de rangos de direcciones ip.

Puede asignar grupos de direcciones de ip a cada una de las sedes para poder identificar cada equipo. Las direcciones de ip pueden ser de cualquier clase (A, B, C).

7.2.2.5 Control del tiempo de una pc para estar conectado a internet.

Los equipos quedan desconectados de internet en horarios no laborales para evitar posibles ataques.

7.2.2.6 Asignación de ancho de banda.

Se asignaran el ancho de banda a los pc según sus actividades, para dar prioridad a los pc que utilizan más el internet. El ancho de banda se puede asignar a un grupo de pc o a un equipo especifico.

7.2.2.7 Relacionar una dirección ip con una mac de un pc

Para aumentar la seguridad en la red las direcciones de ip quedan relacionadas con la mac de una pc. Esto quiere decir que una dirección ip se le asignará siempre a una pc que tenga determinada mac.

7.2.2.8 Reglas para asegurar la red.

Para controlar el acceso a ciertas páginas y las descargas de archivos no autorizados se usa un firewall para disminuir el riego de infección de virus en el sistema.

7.2.2.9 Comunicación de las sedes por medio de una red privada virtual (VPN)

La información que es enviada entra las sedes se hará utilizando una VPN, porque los datos que viaja por la red son encriptados, evitando que estos sean leídos por posibles intrusos.

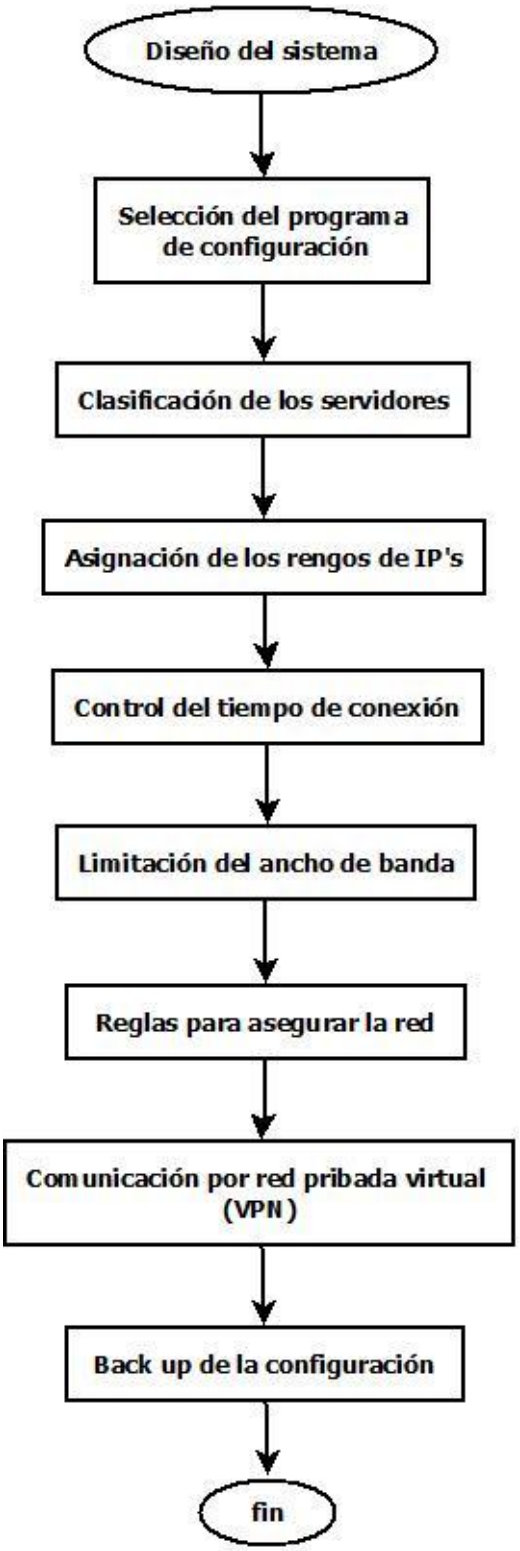
7.2.2.10 Backup de configuración del sistema.

Se puede hacer una copia de seguridad de la configuración del sistema. Cuando el sistema tenga problemas de funcionamiento causados por fallas eléctricas o una actualización mal realizada, se pueda restablecer el sistema sin ningún problema.

7.2.2.11 Diagrama

En el siguiente diagrama (figura 5) se muestra el orden de los procesos que se deben de seguir para tener una configuración correcta, y no presentar inconvenientes en el funcionamiento del sistema que pueda afectar las actividades y seguridad los datos de la empresa. El beneficio de tener un diagrama de diseño, es que facilita a los nuevos ingenieros o a los administradores del sistema vinculados a la empresa a seguir los mismos pasos que se utilizaron en el diseño para hacer revisiones y actualizaciones del sistema, y es una buena estrategia para tener un orden de procedimientos de configuración.

Figura 5. Diseño del sistema



En el diagrama de la figura 5 muestra cómo será diseñado del sistema de la empresa XYZ, para que pueda alcanzar los objetivos de seguridad que necesita para el buen desempeño en las actividades diarias.

Como se ve en el diagrama, el primer proceso que se debe de hacer es escoger el programa que se va a utilizar para hacer la configuración en el sistema de forma segura. Los programas que se pueden utilizar son: Winbox, Chrome que tienen interfaz gráfica, y Telnet o Putty que usan comandos para la configuración. En este diseño el programa que se usará en el winbox.

Teniendo el programa para hacer la configuración del sistema, el segundo proceso que se debe de realizar es seleccionar los servidores que son requeridos por la empresa XYZ, por ejemplo uno de ellos es el protocolo de configuración dinámica de host (DHCP), que entregará las direcciones IP`s a los equipos que se conecten a la red de la empresa.

El tercer proceso asignar las direcciones IP`s a los equipos que estén conectados a la red. Las direcciones IP`s pueden ser de cualquier clase (A,B,C,D), facilitando a la empresa XYZ la elección de las direcciones IP`s de cada una de las sucursales para su fácil identificación y control de sus actividades.

El cuarto proceso del diagrama, es controlar el acceso de internet a los equipos que están conectados a la red, con el objetivo que los equipos usen este servicio solo en horarios de trabajo, evitando que utilicen estos equipos para ingresar a la red de forma ilegal, aumentando las seguridad en el sistema.

El quinto proceso es restringir el ancho de banda para los equipos que no lo necesiten en sus actividades de la empresa, y asignar más a los equipos que si lo necesitan para tener un buen desempeño y que sean más productivos en sus actividades empresariales.

El sexto paso se incrementa la seguridad en los equipos de la red, controlando la descarga de archivo no deseados en las actividades de la empresa, bloqueando la descarga de música, imágenes o pelicular que pueden tener un programa malicioso que pueda perjudicar a la empresa en su funcionamiento. También son bloqueadas las páginas web que no están relacionados con la empresa.

El séptimo paso es la creación de una comunicación segura entre las sedes de la empresa XYZ, para que puedan compartir recursos e información sin temor de

que pueda ser interceptada y manipulada con fines perjudiciales. La forma de hacer esto es crear una red privada virtual (VPN), lo cual provee la seguridad que la empresa y sus sucursales necesita para el manejo de la información confidencial que tienen.

El último proceso es guardar la información de la configuración del sistema, esto facilita la recuperación casi inmediata del sistema de posibles fallos que se pueden presentar en cualquier momento, evitando retrasos en las actividades de la empresa. Otra ventaja de tener una copia de respaldo del sistema, es que se puede hacer actualizaciones de configuración e instalarlo sin tener que suspender las actividades de la empresa por un tiempo prolongado.

7.2.2.12 Por qué este diseño es la mejor opción.

Porque utiliza la tecnología de red privada virtual (VPN), que facilita a las sedes de la empresa el intercambio de los datos de forma fácil y segura, manteniendo su integridad, disponibilidad y confidencialidad, mejorando así sus actividades diarias.

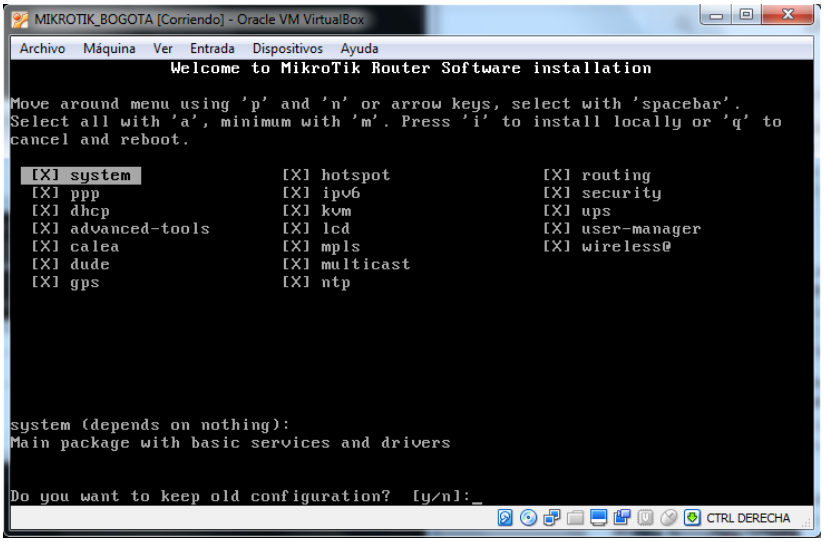
Este diseño tiene la capacidad de cambiar su dimensión o configuración para ajustarse a las nuevas necesidades de la empresa sin perder su calidad y sin que las actividades internas tengan que ser suspendidas por un periodo largo de tiempo, porque el hardware que se utiliza puede ser configurado con las características que desee la empresa sin estar conectado a la red, disminuyendo el tiempo de instalación del hardware en el sistemas. Será como si tuviera la tecnología plug and play.

7.2.3 Fase 3. Instalación y configuración de los routers Mikrotik en las sedes de Bogotá, Medellín, Bucaramanga y Cali.

En esta fase 3 se hace la Instalación y configuración de los routers Mikrotik en cada una de las sedes (Bogotá, Medellín, Cali y Bucaramanga) que forman parte de la empresa XYZ, para poder comunicarse entre sí, y tener acceso a los servidores de la empresa. Unos de los paquete más importante es el PPP (protocolo punto a punto), este es un protocolo que se utiliza para que dos puntos se puedan comunicar. Su objetivo es mantener la autenticidad y seguridad de la información que es enviada por la red y no sea afectada. (RAMIREZ, 2004). En la figura 6 se evidencia la selección de los paquetes que tendrá el dispositivo Router Mikrotik en cada una de las sedes. Los principales paquetes que se usaran en esta configuración son: system para la configuración del sistema operativo que

tiene el Router Mikrotik, ppp (protocolo de punto a punto) es un protocolo que se utiliza para establecer una conexión directa con otro dispositivo (router), dhcp (protocolo de configuración dinámica de host) este protocolo es utilizado para asignar las direcciones ip's a los pc's, impresoras, servidores. Serán modificados según las necesidades de la empresa XYZ. (Di Rienzo, 2010).

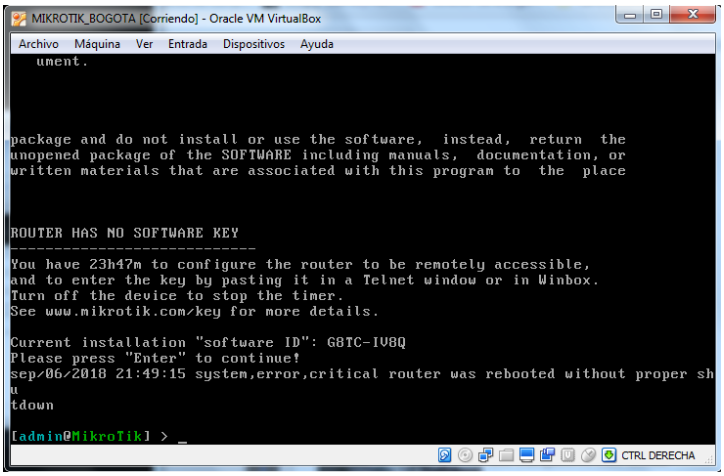
Figura 6. Selección de servidores de Mikrotik



Fuente. El autor

Finalizada la instalación el router Mikrotik queda en la ventana de comandos para hacer las configuraciones. Hay dos formas de hacer la configuración al router, la primera es ingresa los comandos directamente en la ventana de comando del equipo Router Mikrotik, y la segunda es usar el programa de Winbox que utiliza interface gráfica para hacer los ajustes en el Router Mikrotik. El programa Winbox puede ser instalado en el equipo del administrador de la red. En la figura 7 se visualiza la ventana de comandos que se utiliza para la programación del Mikrotik, es similar a la ventana de comandos que utiliza el sistema operativo de Windows.

Figura 7. Entrar al Mikrotik para confirmar su funcionamiento



Fuente. El autor

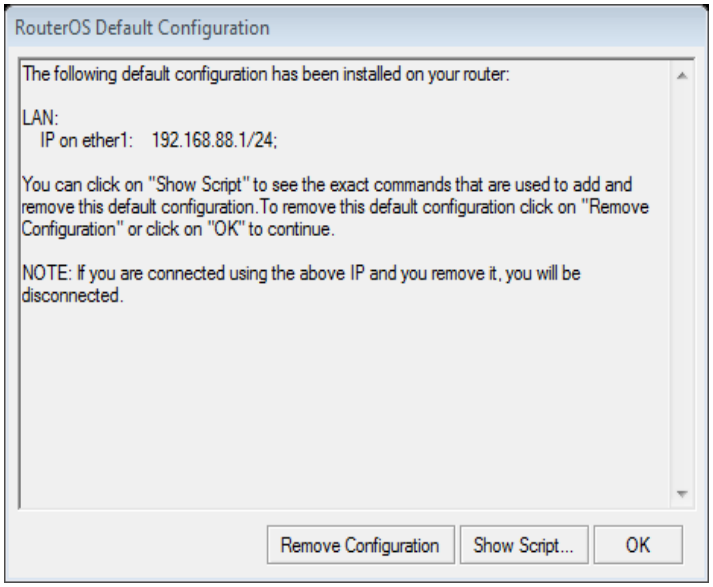
Este proyecto utiliza el programa de winbox para la configuración del router Mikrotik, porque tiene una interfaz gráfica que facilita la programación del equipo. Al ejecutar winbox detecta automáticamente la Mac del router Mikrotik, y solo hay que ingresar el usuario que viene por defecto que es “admin”, y la clave se deja vacio.

7.2.3.1 Configurando la Ethernet en el routerboard

El router Mikrotik es el dispositivo que usará la red de cada una de las sedes de la empresa XYZ para poder ingresar a internet, y lo primero que debe hacer es configurar el router para que pueda ejecutar esta función. El router tiene instalada 4 tarjetas de red, y una de ellas será la que utilizará el router para que sea parte de la red WAN.

Para poder hacer la configuración en el equipo router mikrotik, se debe resetear para eliminar cualquier programación que esté dispuesta por el fabricante. Es necesario abrir el programa Winbox y hacer clic en el menú New terminal, digitar el siguiente comando: *system reset,* el equipo genera un mensaje de remover configuración, que informa que es peligroso hacerlo y preguntará si desea continuar (figura 8). El router mikrotik se reiniciará e ingresará otra vez al equipo router mikrotik con el Winbox.

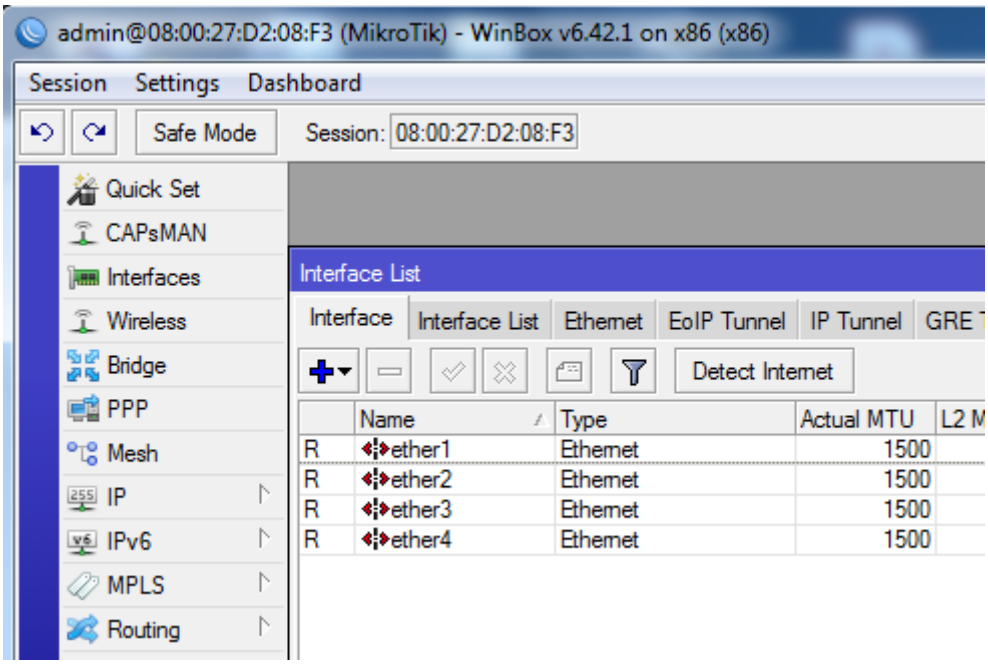
Figura 8: Consola de winbox



Fuente. El autor

Para conocer cuántas tarjetas de red están habilitadas, se debe dar clic en el menú interfaces y se visualiza las interfaces que se pueden utilizar. La figura 9 visualiza la ventana donde las tarjetas de Ethernet del equipo router mikrotik están con los nombres que fueron asignados por el fabricante. La tarjeta "ether1", se va a utilizar como la puerta de salida a internet, y será utilizada para que el equipo router mikrotik se comunique con las otras sedes de la empresa XYZ (figura 8).

Figura 9. Actualizado el nombre de las ether1 y ether2

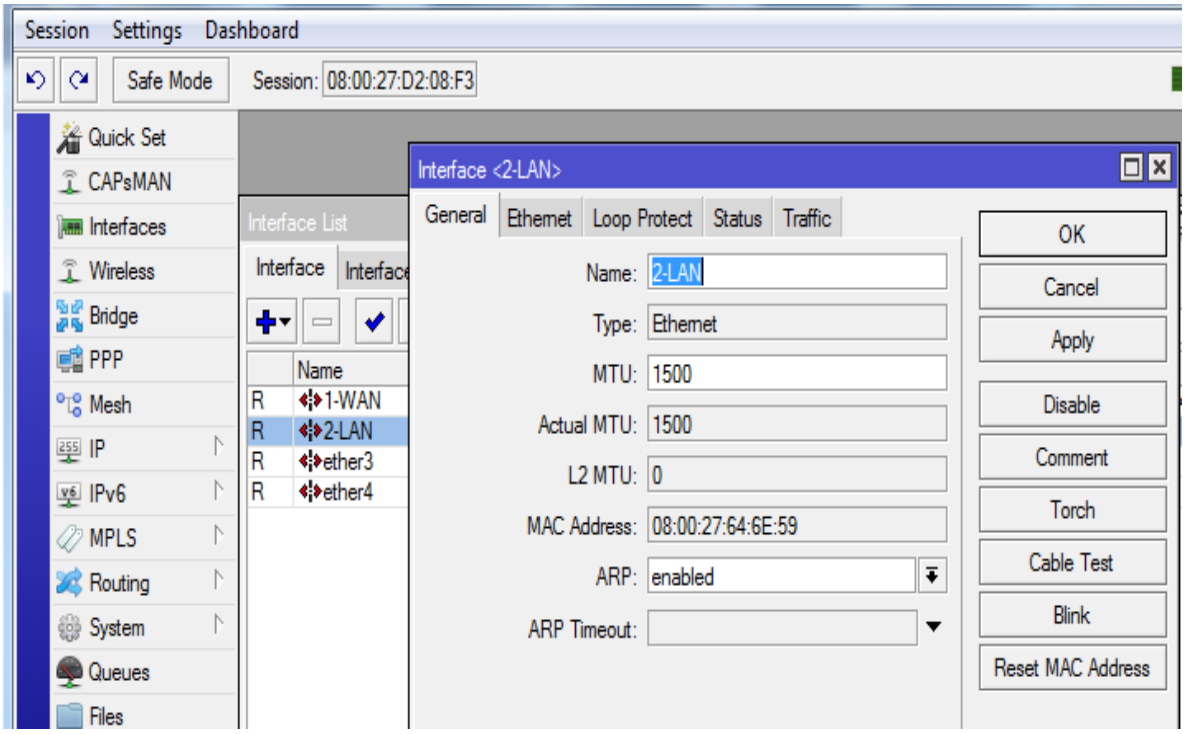


Fuente. El autor

7.2.3.2 Configurar las tarjetas de la red WAN y LAN para tener acceso a internet

Detectadas las interfaces que tiene el router mikrotik, se debe seleccionar cuál de las tarjetas funcionará como red WAN y cual trabajará como red LAN, para que las sedes puedan formar una gran red, y poder tener acceso a los servidores que tiene la empresa XYZ. En la figura 10 nuestra los nombres que están asignadas por defecto a las tarjetas de red (ether1, ether2, ether3 y ether4) en el router Mikrotik. Para cambiar el nombre a cada una de las tarjetas de red del router Mikrotik se debe ingresar al menú interfaces, ejecutar dos clic en el nombre de la tarjeta de red y en la pestaña general en el cuadro de texto name, se escribe el nuevo nombre que en este caso es 1-WAN para la primera Ethernet y 2-LAN para la segunda y se hace clic en ok. (Londoño Velásquez, 2015).

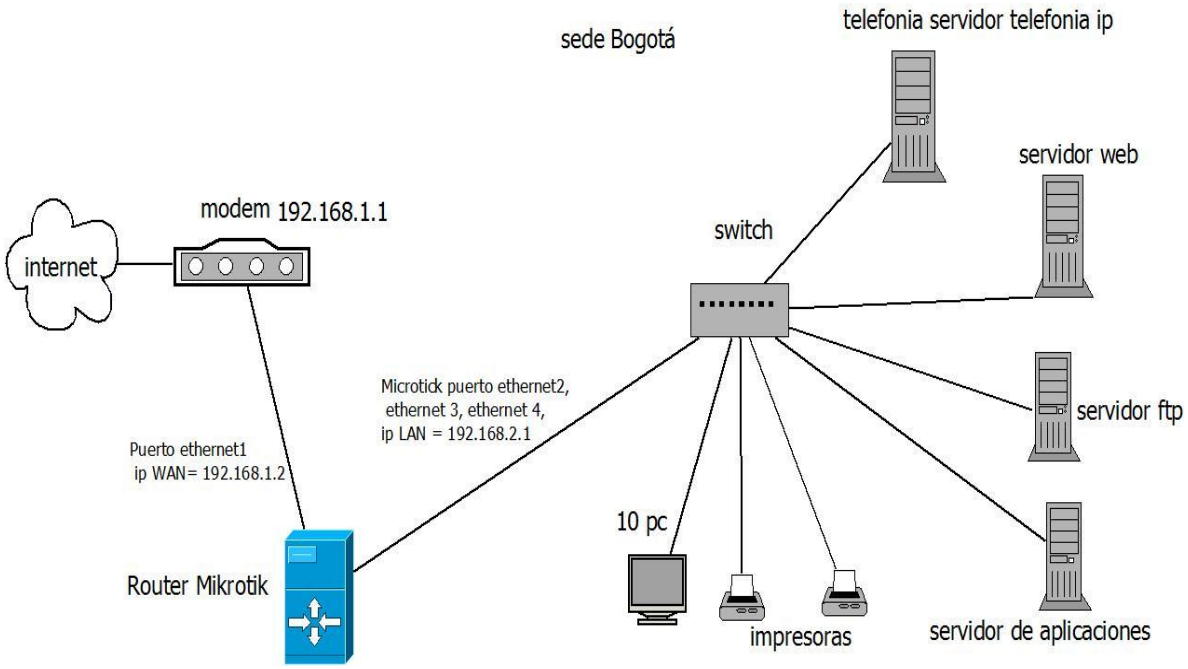
Figura 10. Opción de interface



Fuente. El autor

En la figura 11 está el diagrama de conexión del dispositivo router mikrotik que será integrado en la estructura de la red de la sede de Bogotá. La conexión que hay entre el modem que es instalado por la compañía que da el servició de internet y el router mikrotik hace parte de la red WAN, y la conexión del router Mikrotik al swich hacer parte de la red LAN. Esto quiere decir, que cualquier equipo que esté conectado a la red y quiera comunicarse con el exterior (internet) y mandar o recibir una información, tiene que pasar por el router mikrotik, que ahora tiene el control de la comunicación que sale y entra a la red de la empresa XYZ.

Figura 11. Diagrama de la red con el Mikrotik en la sede de Bogotá

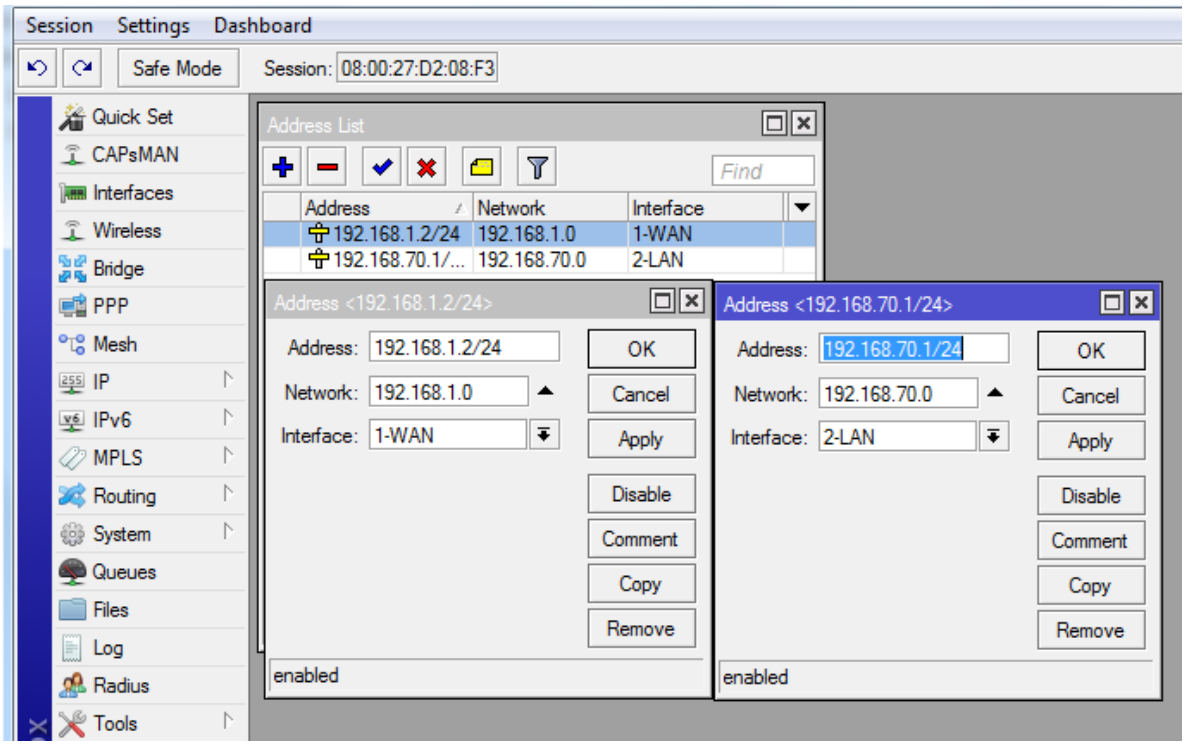


Fuente. El autor

7.2.3.3 Configurar la WAN y LAN

Después de haber asignado el nombre a las tarjetas de red. Se debe dar clic en el menú ip, addresses y hacer clic en el signo “+” y asignar las IP’s a cada una de ellas (figura 12) (Castro, 2019). La IP asignada a la red WAN debe pertenecer al rango de las IP’s que son suministradas por el modem de la compañía que facilita el servicio de internet. En este caso la ip que tiene el modem es 192.168.1.1, y se le asigna la ip siguiente al equipo router Mikrotik, que en este caso será 192.168.1.2. En la tarjeta que se ha escogido para trabajar en la red LAN puede tener cualquier clase de ip. Existen varios tipos de clase de IP’s y estas son: A, B, C, D, E. (Mejía, 2011). A la tarjeta LAN se le asigna la clase C.

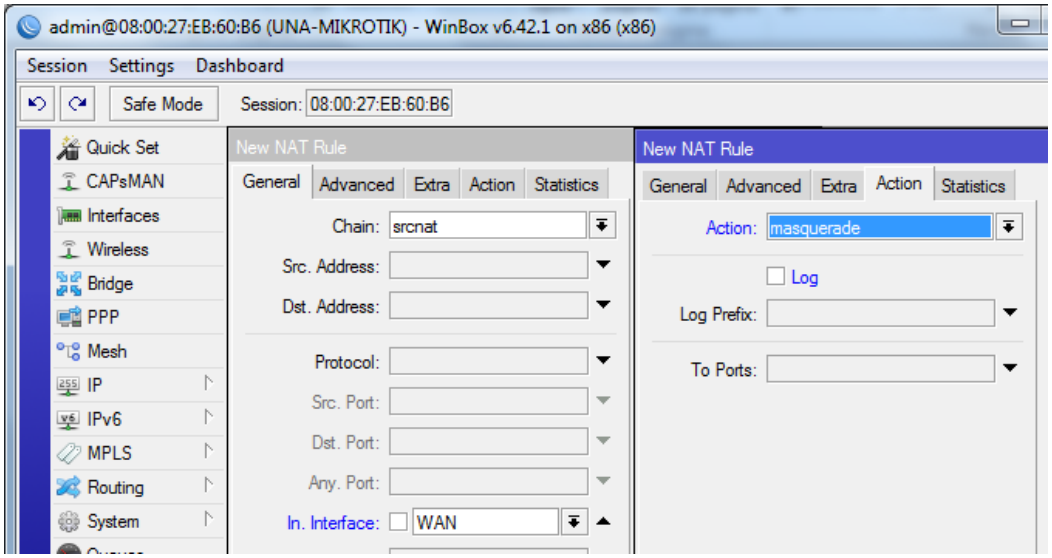
Figura 12. Se asigna la IP a la WAN y a la LAN



Fuente. El autor

Seleccionadas las IP’s, ahora se debe crear la reglas de NAT (Network Address Translation) es el recurso que se dio para solucionar el problema de la escases de direcciones ipv4 en la actualidad. NAT realiza la conversión de las direcciones privadas de los equipos de una empresa hacia las públicas. (Becerra, 2013). La configuración de esta función se hace de la siguiente forma: se hace clic en ip, firewall, aparecerá una ventana, a continuación hace clic en la revorde NAT y posteriormente en el signo “+” y se visualiza una nueva ventana. En la pestaña general, en el cuadro de texto Chain, se selecciona scrnat, en Out Interface se asigna la interfaz WAN y en la pestaña action, en el cuadro de texto action se la asigna el valor de masquerade, clic en apply y después en ok. (Figura 13). (Vásquez, 2019).

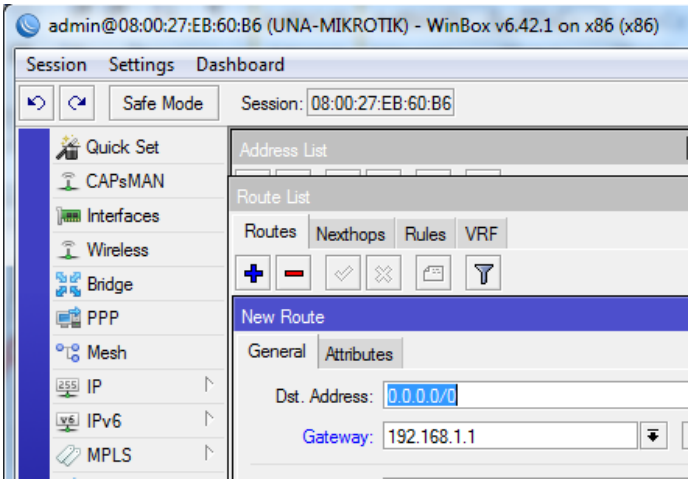
Figura 13. Crear la regla de NAT



Fuente. El autor

Lo último que falta para que el equipo router Mikrotik tenga internet, es decirle que ip suministra el servicio. La única ip que puede prestar el servicio de internet es la que tiene el modem que pertenece a la empresa de la línea telefónica, en este caso 192.168.1.1, que sería la puerta de enlace. Para hacer la configuración se hace clic en ip, Route y después en el signo “+”, se anotar en el rectangulo de texto Gateway la ip 192.168.1.1, y clic en ok, (figura 14). (Ureta, 2019).

Figura 14. Puerta de enlace

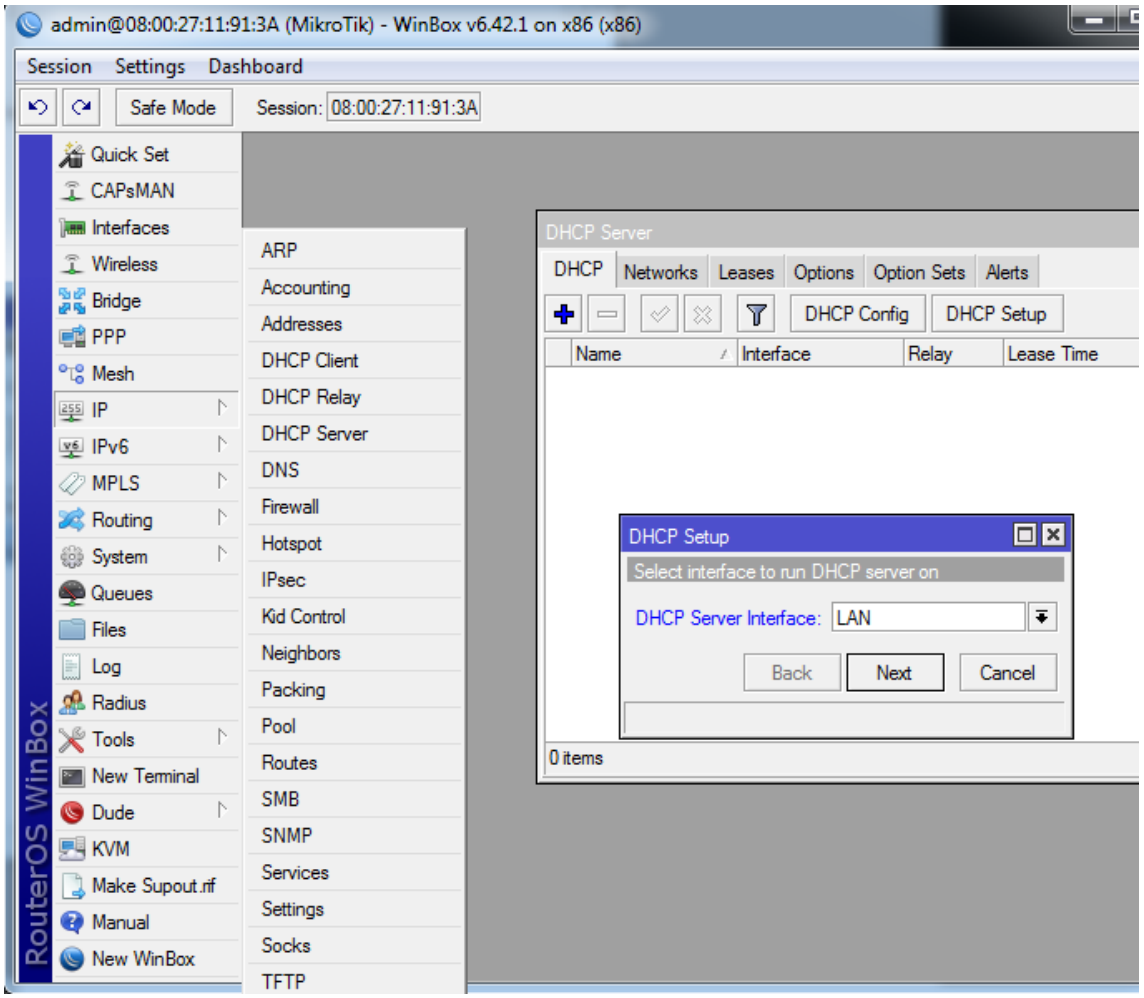


Fuente. El autor

7.2.3.4 Configuración del servidor DHCP en mikrotik

Al colocar el Router Mikrotik entre la red y el modem, la red no queda directamente conectada al modem, y no tendría quien le suministre las IP's para identificar cada uno de los equipo, lo cual se tendría que poner una ip estática a cada uno de los equipos. El equipo de Mikrotik debe tener un servidor DHCP que será asignado a la tarjeta de red para que suministre las ip's de forma dinámicas a los equipos que están conectados. Para crear el servidor DHCP en el router se debe hacer clic en ip, DHCP server, DHCP setup y se visualizará una ventana para seleccionar la interface (figura 15). (Salguero, 2015)

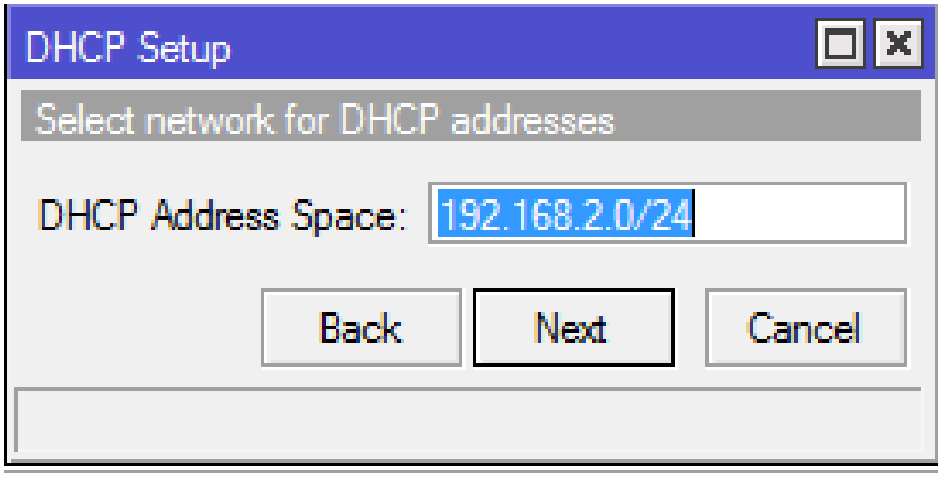
Figura 15. Configuración DHCP



Fuente. El autor

Establecida la tarjeta que estará relacionada con el servidor DHCP que en este caso es la tarjeta LAN, se debe seleccionar la red que tendrá las ip's dinámicas (figura 16). Cada tarjeta de red (LAN) que se detecte en el equipo de Mikrotik se le debe asignar diferentes pool de DHCP para tener organizadas cada una de las redes LAN que forman cada interface del router mikrotik. Como cada tarjeta tiene un nombre que las identifica, también puede tener su propio rango de ip.

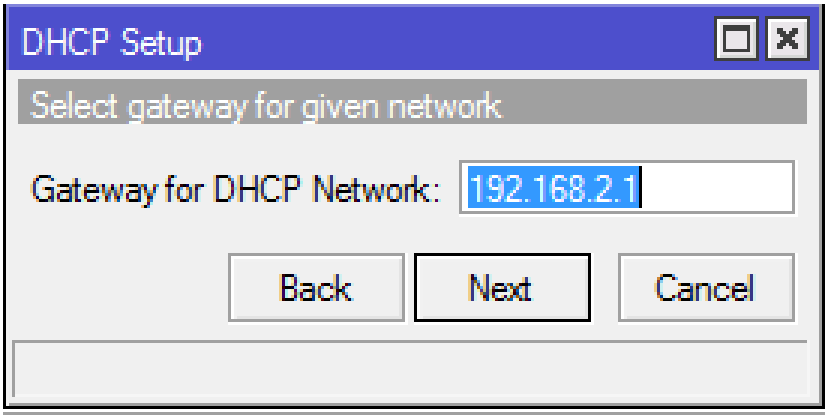
Figura 16. Ip del DHCP



Fuente. El autor

Seleccionada la red que va a trabajar el servidor DHCP, se asigna la puerta de enlace (figura 17), y esta será la ip que se le asignó a la tarjeta de red donde estarán conectados. Si la ip no es igual al de la tarjeta donde fue conectado no tendrán la posibilidad de comunicarse con las sedes de las otras ciudades para compartir información.

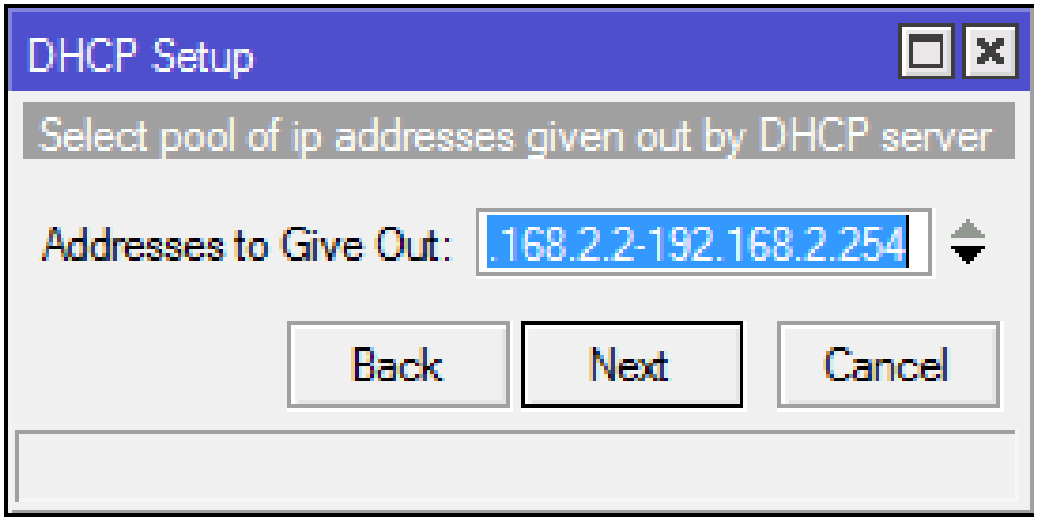
Figura 17. Gateway para el DHCP



Fuente. El autor

Para controlar la cantidad de dispositivos que tendrá cada tarjeta de red detectada en el equipo de Mikrotik y tener más control de los equipos de las oficinas de cada sede, se configura el servido DHCP que de un número terminado rango de ip. El rango puede estar entre 192.168.2.2 hasta 192.18.2. 254 (figura 18).

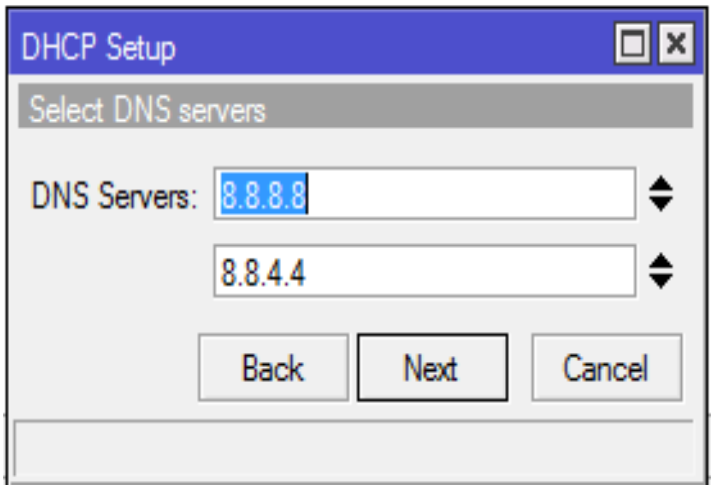
Figura 18. Rango de ip DHCP



Fuente. El autor

Creado el servidor DHCP para que asigne las IP's a los equipo de forma dinámica, también se necesita configurar los DNS (servidor de nombre de dominio). La empresa XYZ no tiene servidor de domino. Los proveedores que ofrecen el servicio de internet tienen sus servidores de DNS predeterminados, pero en este caso se utilizarán los servidores de DNS públicos, en este caso se puede usar los DNS públicos como por ejemplo los de Google 8.8.8.8 y 8.8.4.4, para configurarlo se da clic en ip, después en DNS. En el cuadro de texto servers se escriben las IP's de los DNS. (Figura 19). (Vásquez, 2019).

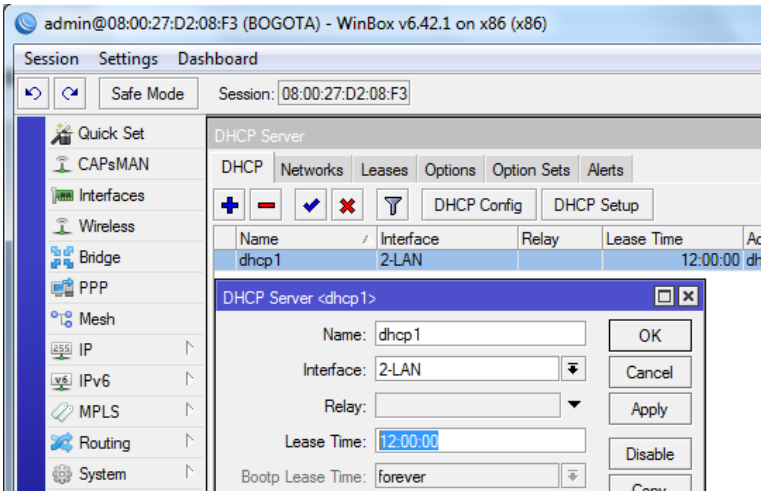
Figura 19. DNS públicas asignadas



Fuente. El autor

Una de las cualidades que tiene el router Mikrotik es que puede controlar el tiempo que está el equipo (PC) de un usuario conectado a la red, por ejemplo: se puede programar que un equipo (PC) esté conectado a la red solamente 12 horas, evitando que el equipo sea usado en horas que no estén en servicio los usuarios. Para programar el tiempo se ingresa al menú IP, DHCP server, y se hace doble clic en el grupo de DHCP creada y se asigna el límite del tiempo, clic en ok (figura 20).

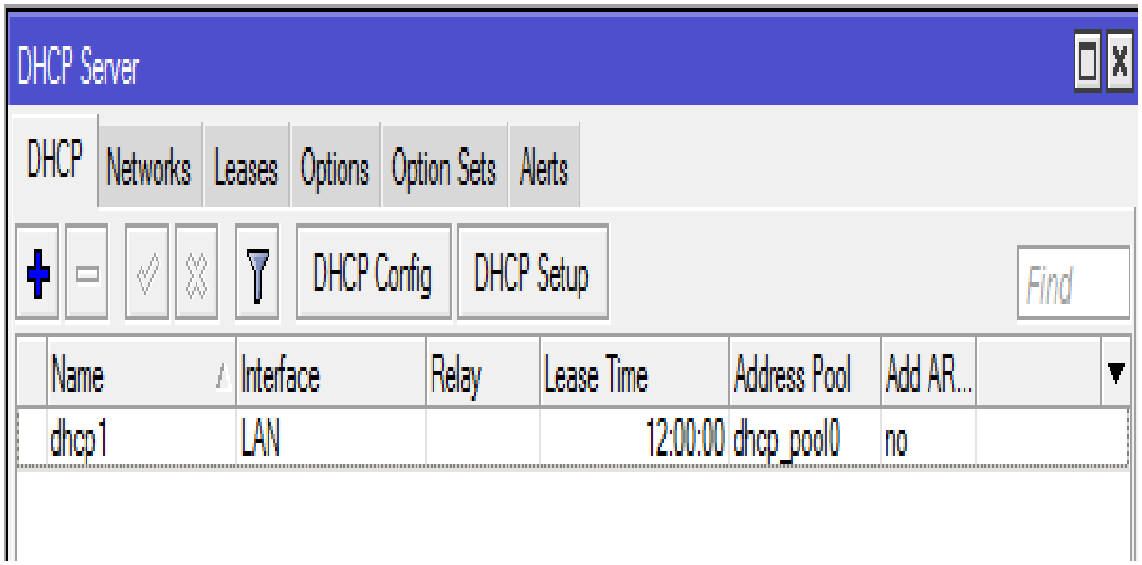
Figura 20. Control del tiempo



Fuente. El autor

Programado el último paso, que es el tiempo de conexión, el servidor DHCP ya queda totalmente configurado para que la red que estará conectada a la tarjeta LAN (figura 21) tenga sus IP's dinámicas y su control de tiempo. Se puede hacer la configuración de un servidor DHCP para cada una de las tarjetas de red que se detecten en el router Mikrotik.

Figura 21. Creado el servidor DHCP para la LAN

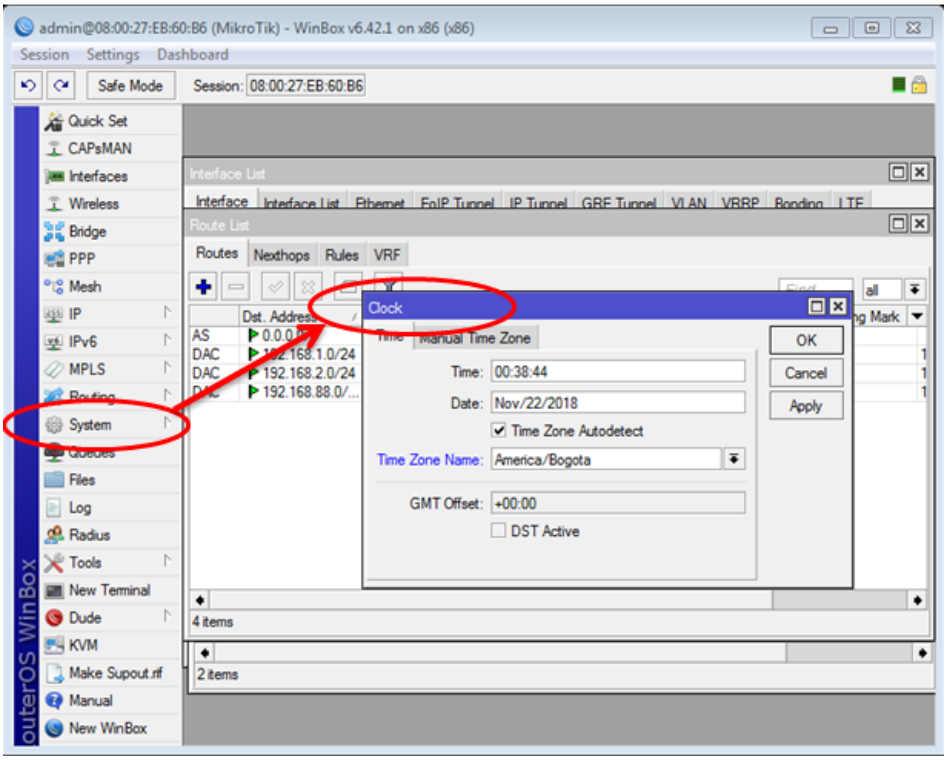


Fuente. El autor

7.2.3.5 Asignación de ancho de banda

Controlar el amplio de banda de una red es muy primordial, porque se puede asignar la cantidad de amplio de banda depende de la actividad del sector de la red. Para poder asignar el ancho de banda a los equipos que están en la red se debe configurar hora y fecha del equipo router Mikrotik. Se hace clic en el menú system, después clock y se visualiza una ventana donde se ingresa la fecha y hora deseada y se confirma con ok (figura 22).

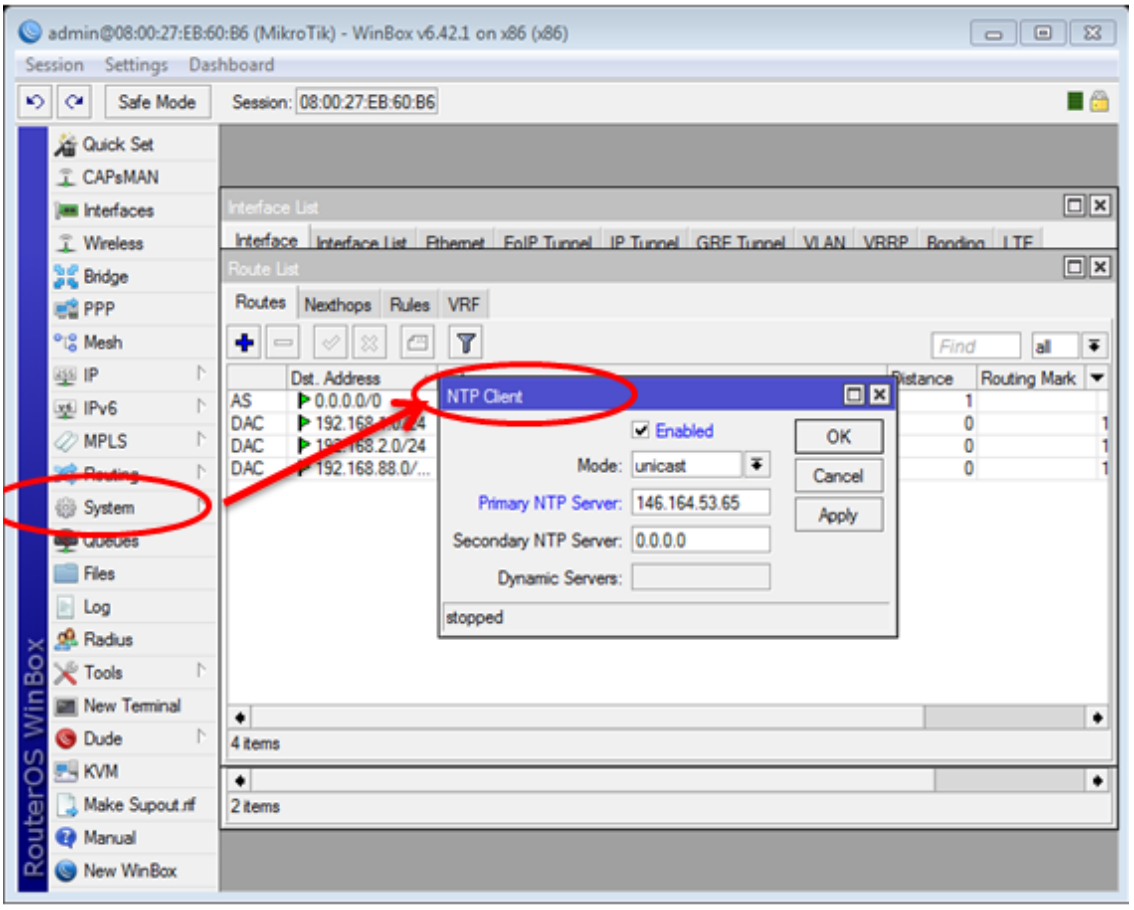
Figura 22. Configuración de la hora y fecha.



Fuente. El autor

Un inconveniente que tiene el equipo Mikrotik es que no tiene batería para mantener la información de hora y fecha como lo tienen las computadoras cuando se apaga o se reinicia. Para solucionar este problema, se activa el servidor NTP (*Protocolo de tiempo en la red)*. Es el protocolo que transfiere el tiempo por la red. Que en otras palabras es un servidor que da la hora a terminales que se encuentren vinculados a la red. Para configurar el NTP client (cliente porque va a recibir la hora), se debe activar el SNTP Client y digitar la ip del servidor que suministrará la hora que en este caso es ip 146.164.53.65 para que el equipo mikrotik este siempre con el tiempo actualizado. Para configurar el router Mikrotik se ingresa al menú system y después en SNTP Client y se escribe la ip del servidor que suministrará la hora y fecha. (Figura 23).

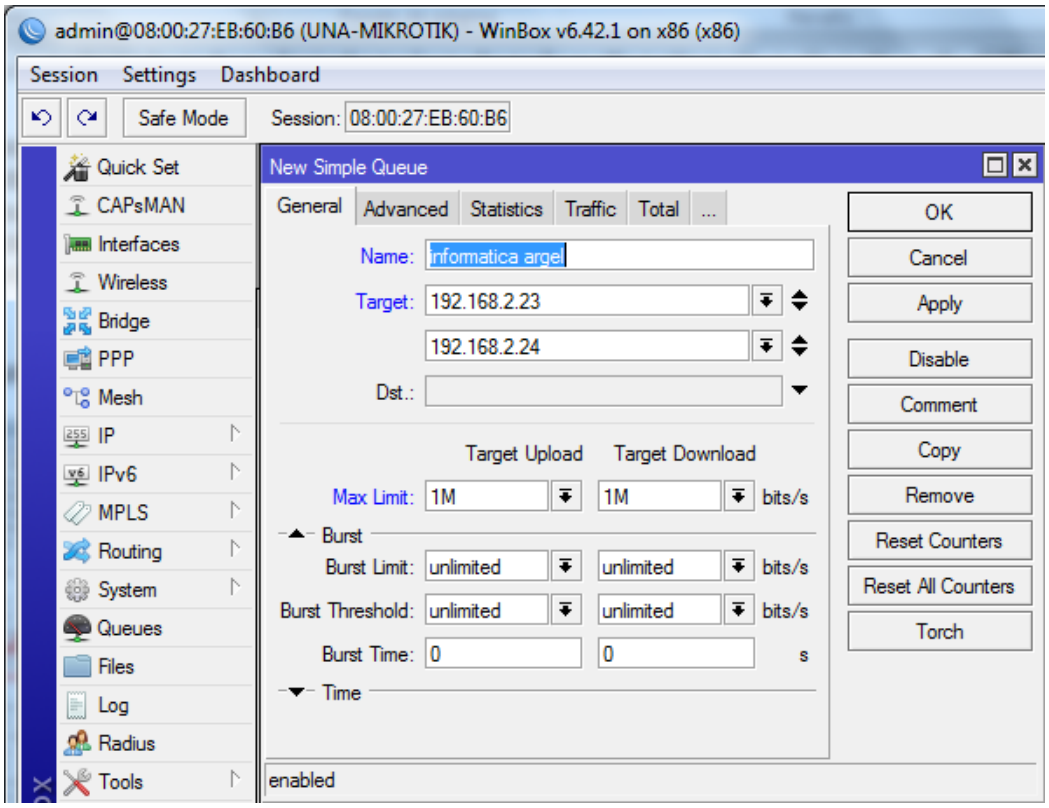
Figura 23. Activar el SNTP Client



Fuente. El autor

Ahora se puede hacer la configuración para controlar o distribuir el ancho de banda en la red, lo cual es muy indispensable, ya que hay páginas web que consumen mucho el ancho de banda y pone lenta la red. El equipo router mikrotik se puede configurar para limitar el ancho de banda a un equipo o grupo de ellos en la red. Para controlar el ancho de banda se ingresa al menú Queues, en la pestaña Simple que use, se da clic en el signo “+” y se mostrará una ventana que tiene los siguientes cuadros de textos: Name, donde se escribe el nombre del grupo de equipos que tendrá limitada el ancho de banda, el target donde se escribe el rengo de IP’s que tendrá la limitación el ancho de banda, los cuadros de texto donde se escribe el valor del ancho de banda y se da clic en ok. (Figura 24). (Salguero, 2015).

Figura 24. Limitación de ancho de banda individual y por grupo

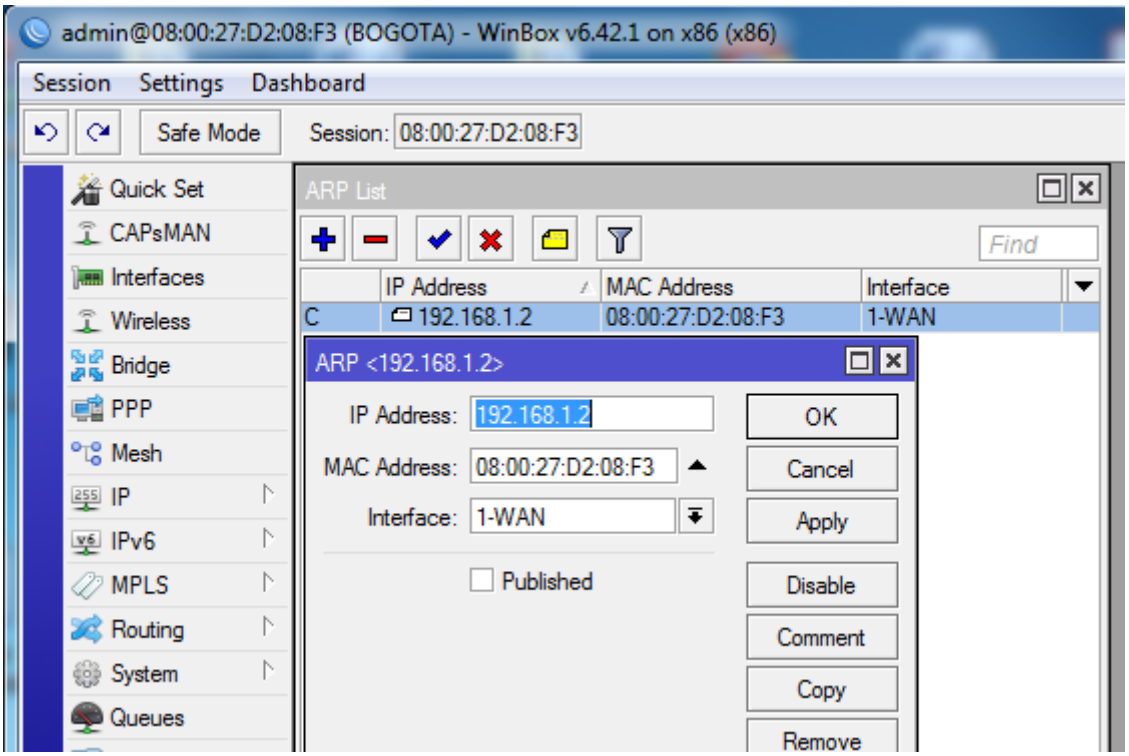


Fuente. El autor

7.2.3.6 Unión de ip y la Mac

Realizada la configuración del servidor DHCP, se puede empezar a relacionar la ip de un equipo (PC) con su Mac. Cuando los PC's quieren enviar alguna información a otra pc, necesitan conocer la ip y la Mac de los equipos (PC) de destinos. Los dispositivos (PC) tratan de entablar comunicación con otros computadores de la empresa con direcciones IP's conocidas, se deben encontrar la MAC del equipo (PC) receptor. El TCP/IP tiene el protocolo ARP, y su función es encontrar la dirección Mac del pc destino. El equipo router Mikrotik posee una tabla ARP en donde almacena las IP's y lo asigna a las MAC. Para agregar direcciones ip con su respectiva Mac se debe ingresar al menú IP, después a ARP, se da clic en el signo "+" y se digita la ip y la Mac del equipo (PC) y ok, como lo visualiza la figura 25. (Muñoz, 2018).

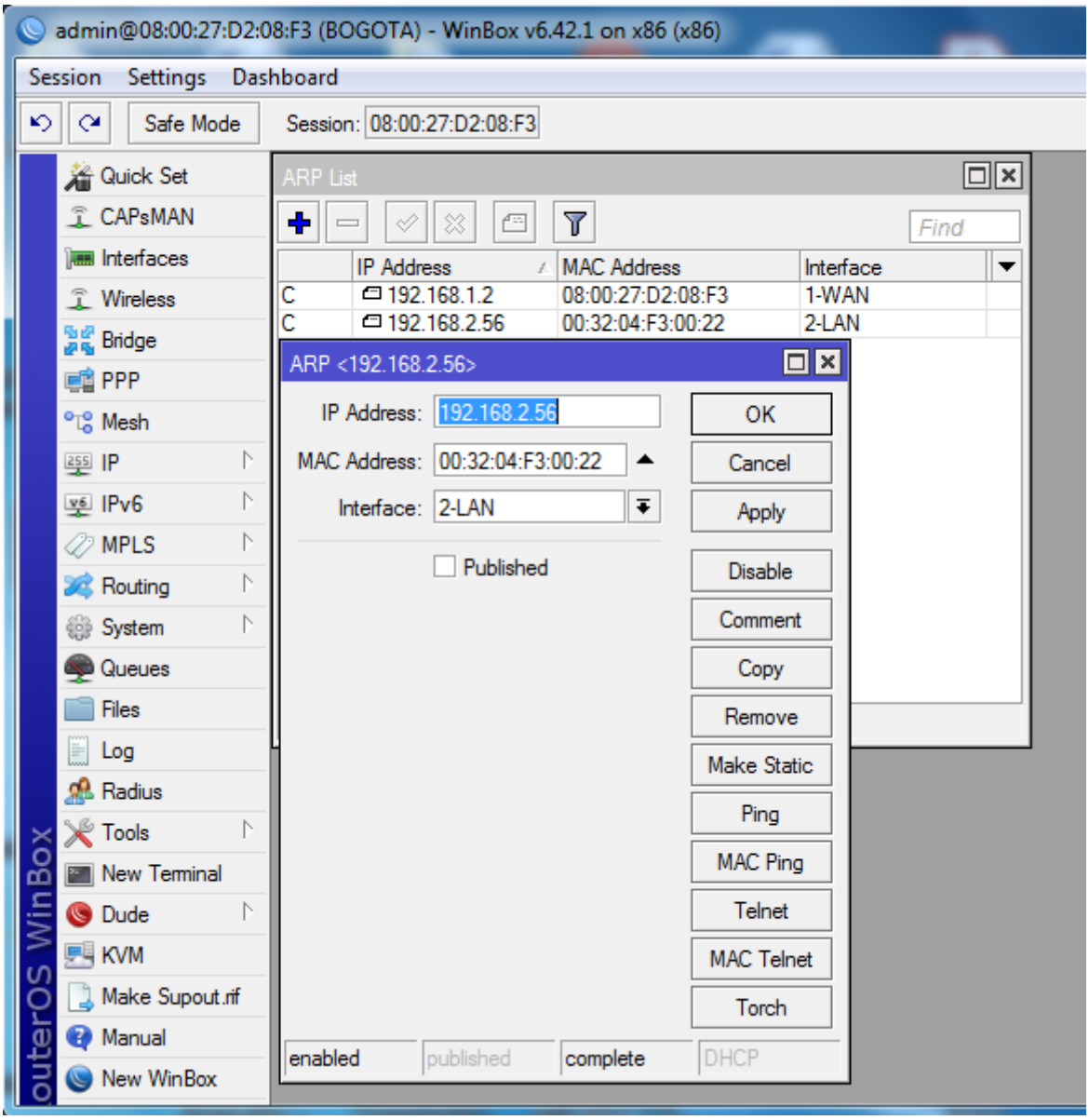
Figura 25. Unión de IP y el Mac



Fuente. El autor

Al ingresar a la tabla ARP del equipo de Mikrotik para crear la relación se visualiza la Mac y la IP que han sido relacionadas, en este caso solo muestra la interface que se ha escogido como WAN (1-WAN). Al lado izquierdo de la ip aparecerá una letra "C", lo cual indica que la ip está relacionada con un Mac de un equipo. Para configurar la interface LAN se hace de la misma forma como se realizó la configuración de la WAN (figura 26).

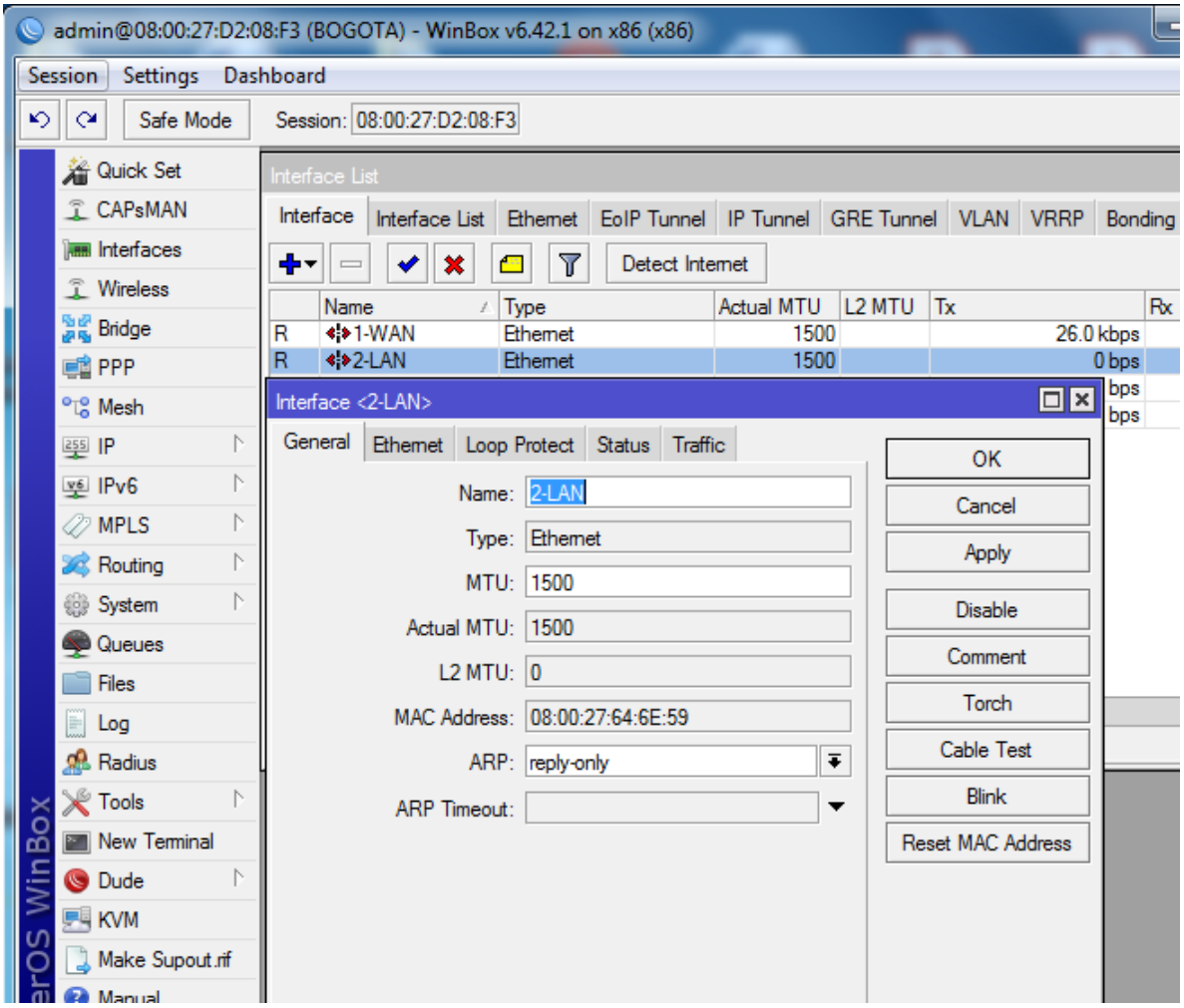
Figura 26. ARP



Fuente. El autor

Al validar que los dispositivos (PC) mostrados en la tabla son los que se configuraron, se ingresa a la Interface LAN y se cambia el valor del campo ARP por *reply only*. Si el valor que está asignado es *enabled*, significa que está abierta la red, requiriendo cerrarla, con el objetivo de que solo puedan entrar a internet los equipos (PC) que están en la lista de ARP. Para hacer esta configuración se debe ingresar al menú interfaces, doble clic en el nombre de la interfaz (2-LAN), (figura 27).

Figura 27. Interface LAN

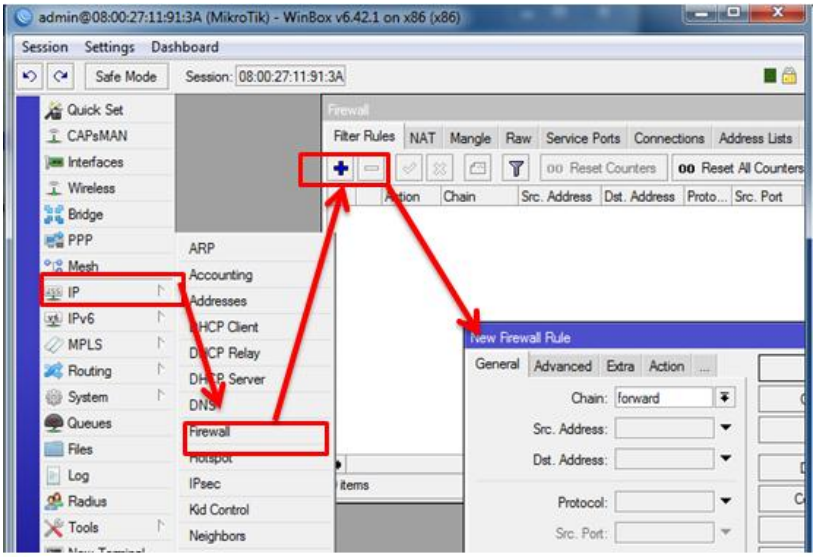


Fuente. El autor

7.2.3.7 Reglas para asegurar la red utilizando firewall

Para asegurar la red se requiere crear normas generales en el equipo router Mikrotik, y para lograrlo, se necesita hacer algunas restricciones de acceso a determinados sitios web que indique la empresa XYZ, como por ejemplo: negar o bloquear el ingreso a redes sociales. Para crear las restricciones se debe ingresar al menú IP, Firewall, como lo visualiza la figura 28.

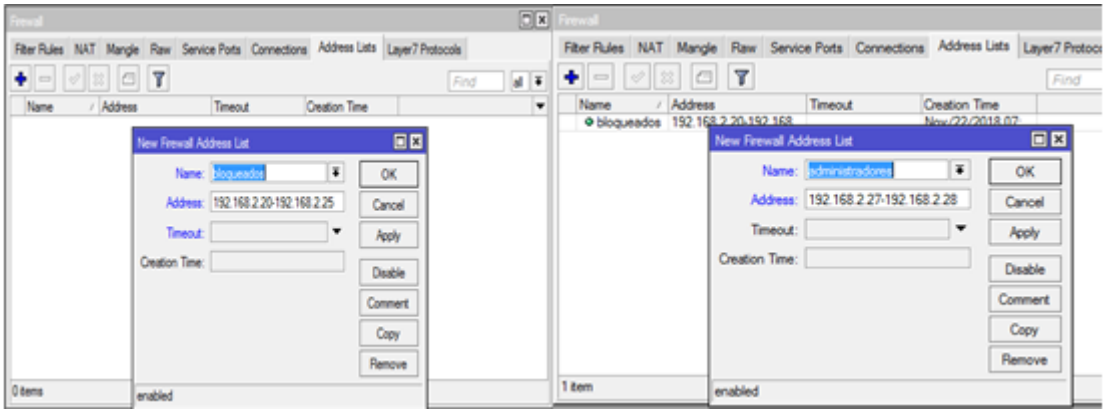
Figura 28. Crear reglas en el Firewall



Fuente. El autor

Para poder aplicar las restricciones que son solicitadas por la empresa XYZ, se debe crear los grupos de ip's para asígnales las reglas que tendrá cada grupo de usuario, en este caso se crearan dos grupos, un grupo se llamará "bloqueados" y las direcciones que abarca son 192.168.2.20 hasta 192.168.2.25, y el otro grupo se llamará administradores, que tendrá las IP's 192.168.2.27 a 192.168.2.28. para realizar la configuración de restricciones se debe ingresar al menú IP, Firewall, se da clic en la reborde address lists y en el signo "+", aparecerá una ventana donde se ingresará el nombre del grupo a crear y el rango de IP's que tendrá , como lo visualiza la figura 29.

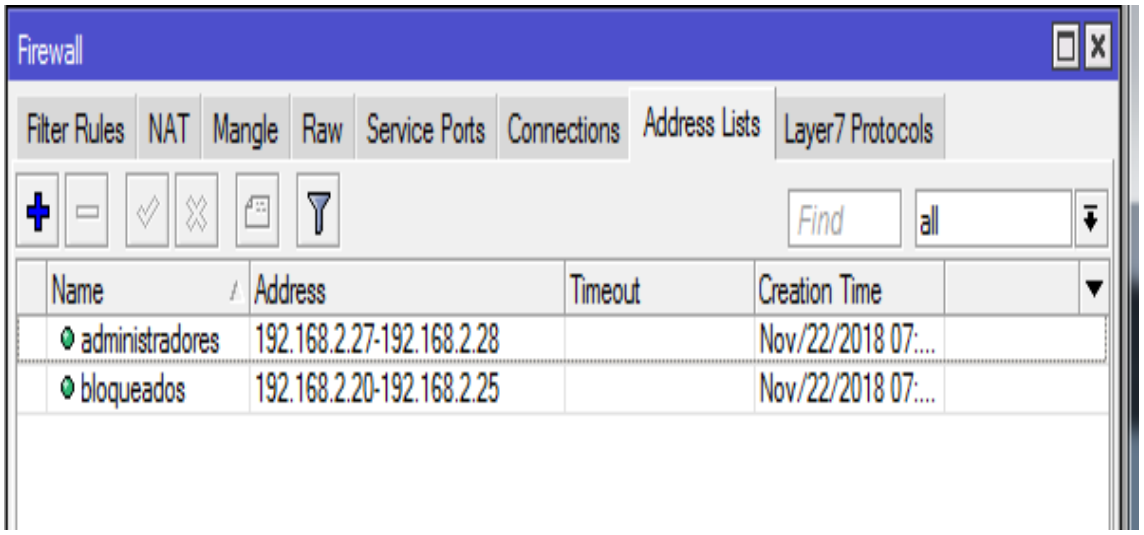
Figura 29. Creación de los grupos para el firewall



Fuente. El autor

Cuando los grupos de IP’s se han creado (figura 30), se les aplicaran las reglas del firewall. Se podrá crear las restricciones de entrada y salida de información, controlando las funciones de los grupos y mejorando la protección de la red de la compañía XYZ y disminuyendo los riesgos infección de los virus informáticos.

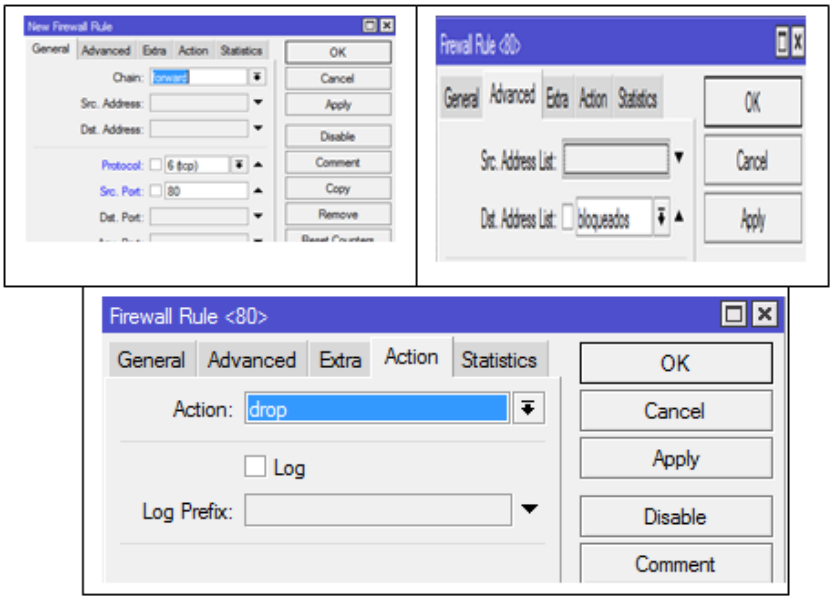
Figura 30. Grupos creados



Fuente. El autor

La primera regla que se crea es para el grupo llamado bloqueados, y es prohibir el tráfico http que se conectan en el puerto 80. El protocolo que se debe prohibir es el de tcp que pase (forward) por el firewall y provenga del grupo de bloqueados, y la acción que se va a tomar es bloquear (drop). Para realizar esta configuración se debe dar clic en IP, Firewall, y en la pestaña filter rulers, se da clic en el signo “+” y se mostrará una ventana. La ventana tiene varias pestañas. En la pestaña general, en el cuadro de texto Chain se selecciona la opción forward, en el cuadro de texto protocol se elige la opción 6 (tcp) y en el cuadro de texto port se escribe el número 80. En la pestaña advanced, en el cuadrode texto dst address list se selecciona el nombre de la lista que se quiere bloquear, que en este caso es el grupo de bloqueados. En la pestaña action, en el cuadro de texto action se selecciona la palabra drop. (Figura 31).

Figura 31. Crear regla en el firewall



Fuente. El autor

7.2.3.8 Creación de la vpn en la Empresa XYZ

Las vpn son redes de IP's privadas que son seguras que utilizan la estructura de otra red ip pública que no es segura. Al utilizar una VPN (red privada virtual) se tiene varios beneficios como por ejemplo: es de bajo costo, es muy segura, de fácil interconexión, puede tener usuarios móviles, es fácil de administrar, es muy flexible y es escalable. Una vpn debe garantizar algunas condiciones como por ejemplo: confidencialidad, autenticidad e integridad. Si no cumple estas condiciones entonces no sería adecuado usarla. (Dobladez, 2009)

Hay varios tipos de vpn, la primera son las redes ruteables que trabaja en la capa 3, son eficientes, son escalables y su configuración es sencilla de realizar. El segundo tipo son las redes bridgeadas que trabajan en la capa dos, en este tipo de red no se configura enrutamiento, se puede utilizar cualquier protocolo y hay broadcast a través de la red. (Dobladez, 2009)

Hay diferentes protocolos que se utilizan en las VPN`s. algunos de ellos son: PPTP (Point to Point Tunneling Protocol) es un protocolo que está obsoleto. L2TP (Layer 2 Tunneling Protocol), que es el sucesor de PPTP. Estos protocolos tienen las siguiente características: Suministra Autenticación y Encriptación, el Mikrotik

RouterOS aguanta PPTP / L2TP Cliente y Server, es simple de configurar, Interoperatibilidad (Windows, Linux, Mac, etc), acceso Remoto, direccionamiento IP & Firewall. (Dobladez, 2009)

IPSEC tienen las siguientes características: tiene alta seguridad criptográfica en la información que son transmitidos por la red, estándar de Internet , tiene inconveniente con NAT, es compatible entre distintas plataformas, puede trabajar en base en políticas entre peers, de pendiendo de la configuración de la red , la configuración es compleja en algunos casos (Dobladez, 2009)

Las configuraciones que se realizaron en los routers Mikrotik de la ciudad de Bogotá, también fueron hechas en las otras sedes (Medellín, Cali y Bucaramanga), para tener las direcciones ip de las WAN de cada router y poder crear la VPN de la empresa XYZ. Las direcciones de IP`s de las WAN's que se generaron en cada son las siguientes:

Ip WAN de Bogotá: 192.168.1.1

Ip WAN de Medellín: 192.168.2.1

Ip WAN de Bucaramanga: 192.168.3.1

Ip WAN de Cali: 192.168.4.1

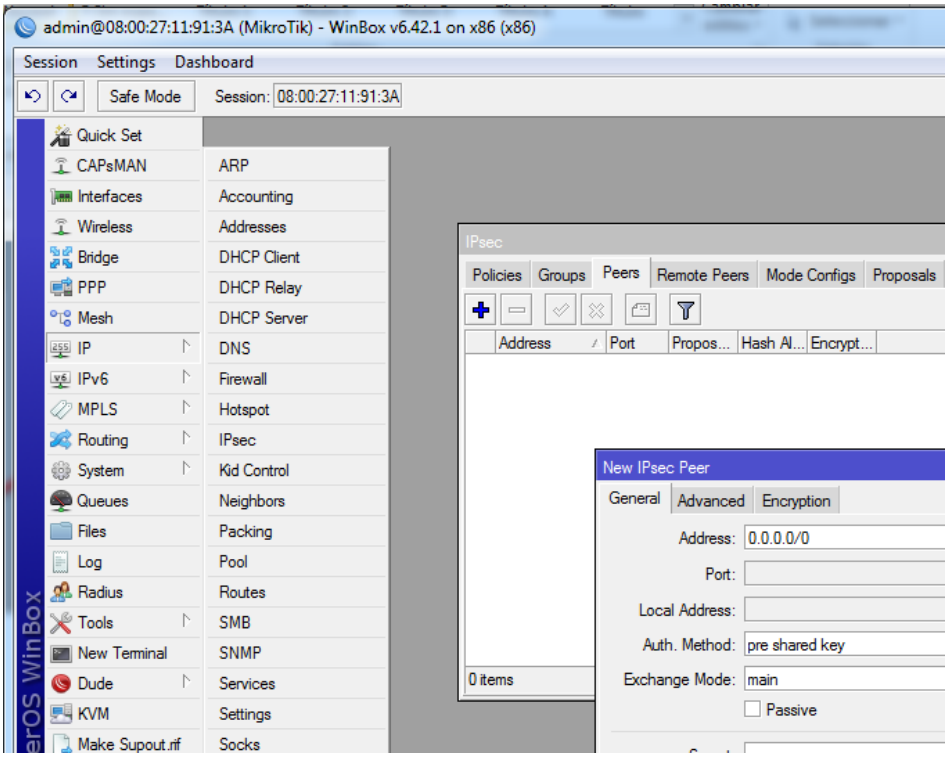
Se ha escogido el tipo de VPN (red privada virtual) ruteables con IPSec por tener varios protocolos y su función principal es brindar seguridad a las comunicaciones IP, cifrando cada paquete IP enviado. IPSec ofrece muchos beneficios como por ejemplo: Facilita nuevas servicios para el acceso fiable y transparente de un punto IP remoto, aportar una infraestructura segura sobre la que efectuar transacciones, (Iglesias, 2001)

7.2.3.8.1 Configuración del router mikrotik de la sede de Medellín

Con la configuración efectuada en la ciudad de Bogotá, y teniendo la ip de su red WAN, ya se puede hacer la programación de la VPN IPSec en el dispositivo router Mikrotik en la sede de Medellín (figura 32). Esta sede se debe comunicar con la sede principal que está en la cuidad de Bogotá, ya que esta sede tiene toda la información almacenada en el clúster de servidores. Para hacer la configuración de debe ingresar al programa Winbox que debe estar instalado previamente en el

equipo (PC) del administrador de red. Debe ir al menú IP, IPsec y se mostrará una ventana que tiene varias pestañas. Se selecciona la pestaña Peers, y en el signo “+” se da clic para visualizar la ventana New IPsec Peer para ingresar los datos que se necesitan para crear la conexión con la agencia principal que está en la ciudad de Bogotá y formar la red privada virtual o VPN.

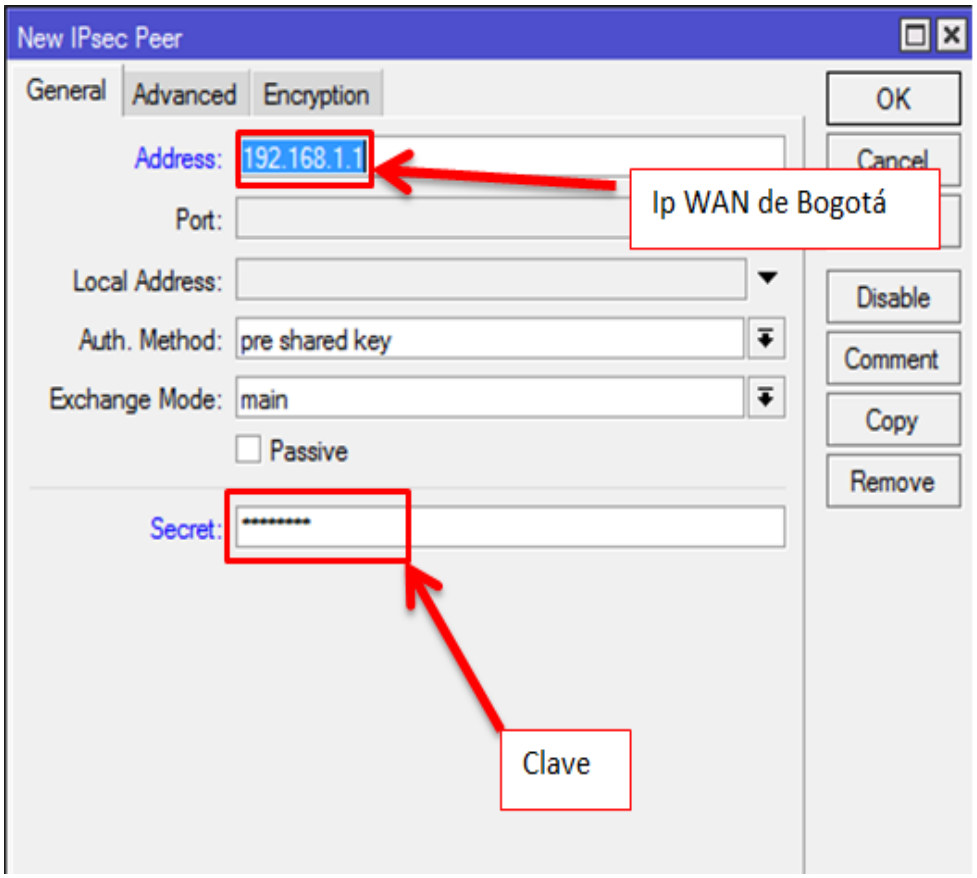
Figura 32. Página peers



Fuente. El autor

En el cuadro de texto address de la pestaña General se pone la ip de la red WAN de destino (192.168.1.1), que en este caso es la sede que está en la ciudad de Bogotá, y se crea una clave de seguridad para la creación de la VPN que tendrá la empresa XYZ. Logrando que los equipos (PC, impresoras) que están en la sede de la ciudad de Medellín pertenezcan a la red de la sede la ciudad de Bogotá (figura 33).

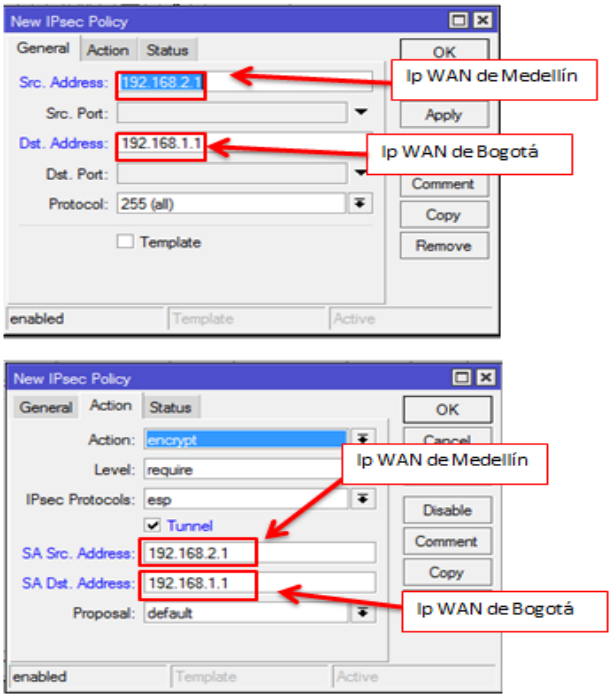
Figura 33. Página general



Fuente. El autor

Ahora falta crear las políticas, que consiste en informar al router Mikrotik cuáles son las IP's que participaran en el túnel de comunicación, que en este caso son: la ip de la WAN de Medellín (192.168.2.1) y la ip de la WAN de Bogotá (192.168.1.1). Con estos datos registrados la sede de Medellín ya podrá comunicarse con el clúster de servidores que tienen la sede de Bogotá. Para realizar la configuración en el router de la ciudad de Medellín, se da clic en el menú IP, después en IPsec y se mostrará una ventana para digitar la ip 192.168.2.1 de origen (Medellín) y la ip (192.168.1.1) de destino (Bogotá) en la pestaña general y la pestaña action. (Figura 34).

Figura 34. Página police – general

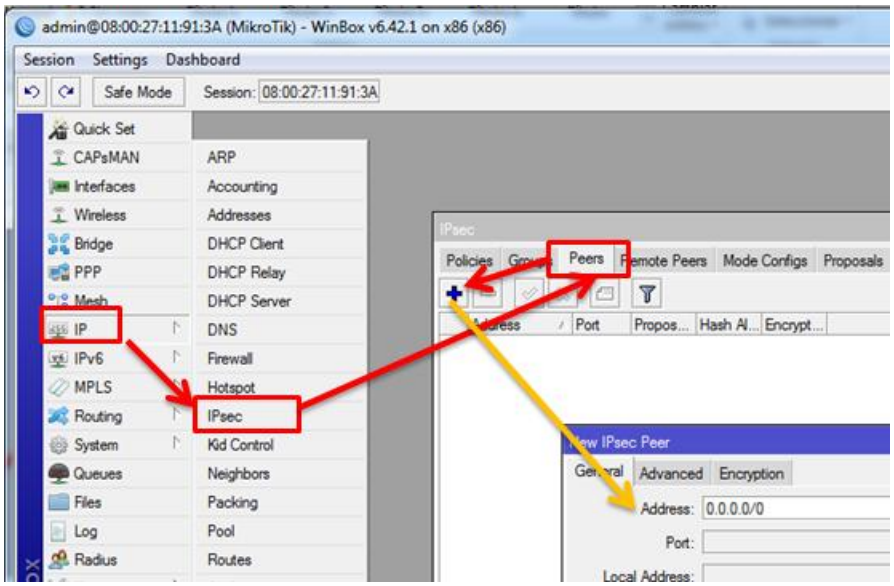


Fuente. El autor

7.2.3.8.2 Configuración del router mikrotik de la sede de Bucaramanga

Concluida la programación del router Mikrotik en la ciudad de Medellín, se continúa con la configuración del router Mikrotik de la sede de la ciudad de Bucaramanga. Con la ip de la red WAN de la sede de la ciudad de Bogotá, se inicia la programación de la VPN IPSec en el dispositivo router Mikrotik utilizando el programa Winbox (figura 35). Esta sede (Bucaramanga) se debe comunicar con la sede principal de la cuidad de Bogotá, ya que esta sede tiene el clúster de servidores. Para realizar la configuración ingresamos al programa Winbox y se ingresa al menú IP, IPsec, clic en la pestaña Peers, clic en el signo “+”.

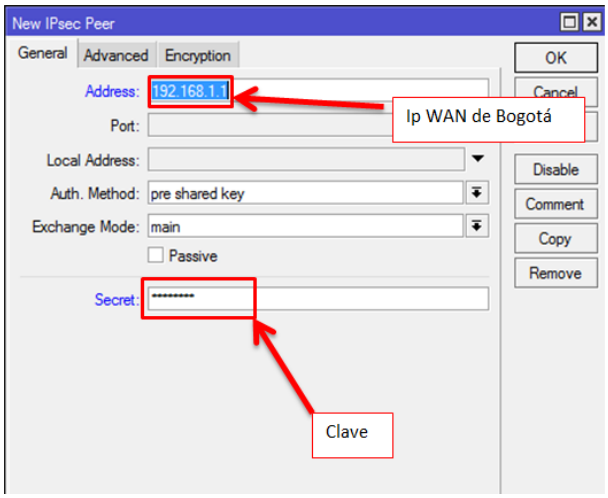
Figura 35. Mikrotik de la sede de Bucaramanga



Fuente. El autor

En el cuadro de texto address de la pestaña General se pone la ip de la red WAN de destino (192.168.1.1), que en este caso es la sede de la cuidad de Bogotá, y se crea una clave de seguridad como se hizo en la sede de la ciudad de Medellín para la creación de la VPN que tendrá la empresa XYZ. Logrando que los equipos (PC, impresoras) que están en la sede de Bucaramanga pertenezcan a la red de la sede de Bogotá (figura 36).

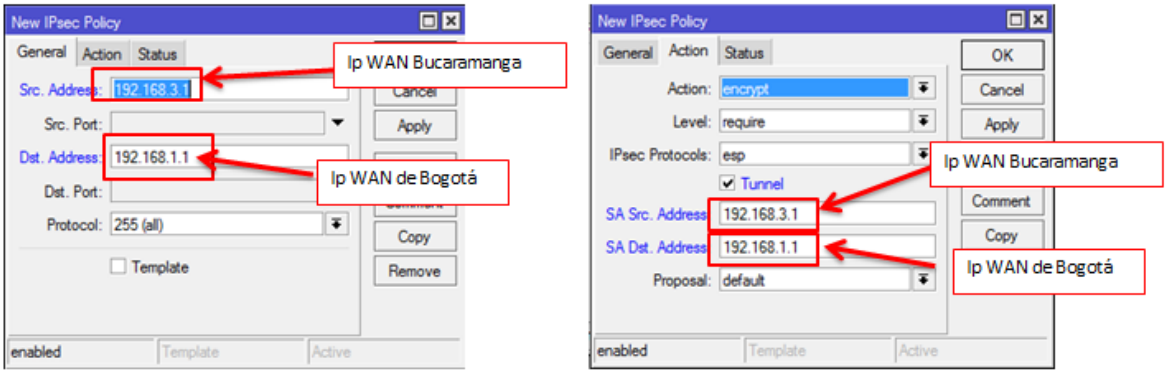
Figura 36. Página general



Fuente. El autor

Para crear las políticas, que consiste en informar al router Mikrotik cuáles son las ip's que participaran en el túnel de comunicación, que en este caso son la ip de la WAN de Bucaramanga (192.168.3.1) y la ip de la WAN de Bogotá (192.168.1.1). Con estos datos registrados la sede de Bucaramanga ya podrá comunicarse con el clúster de servidores que tienen la sede de Bogotá. Para configurar las políticas en el router Mikrotik se debe ingresar al menú IP, IPsec, y en el borde policies se da clic en el signo "+". En la ventana que aparece en la pestaña General se ingresan las IP's de origen y de destino. En la pestaña action en el cuadro de texto action se escoge la opción encrypt (encriptar), para que la información enviada sea protegida. En el cuadro de texto de dirección de origen y destino se ingresen las IP's correspondiente, que en este caso son la de origen 192.168.3.1 (Bucaramanga) y la de destino 192.168.1.1 (Bogotá). (Figura 37).

Figura 37. Página police – general

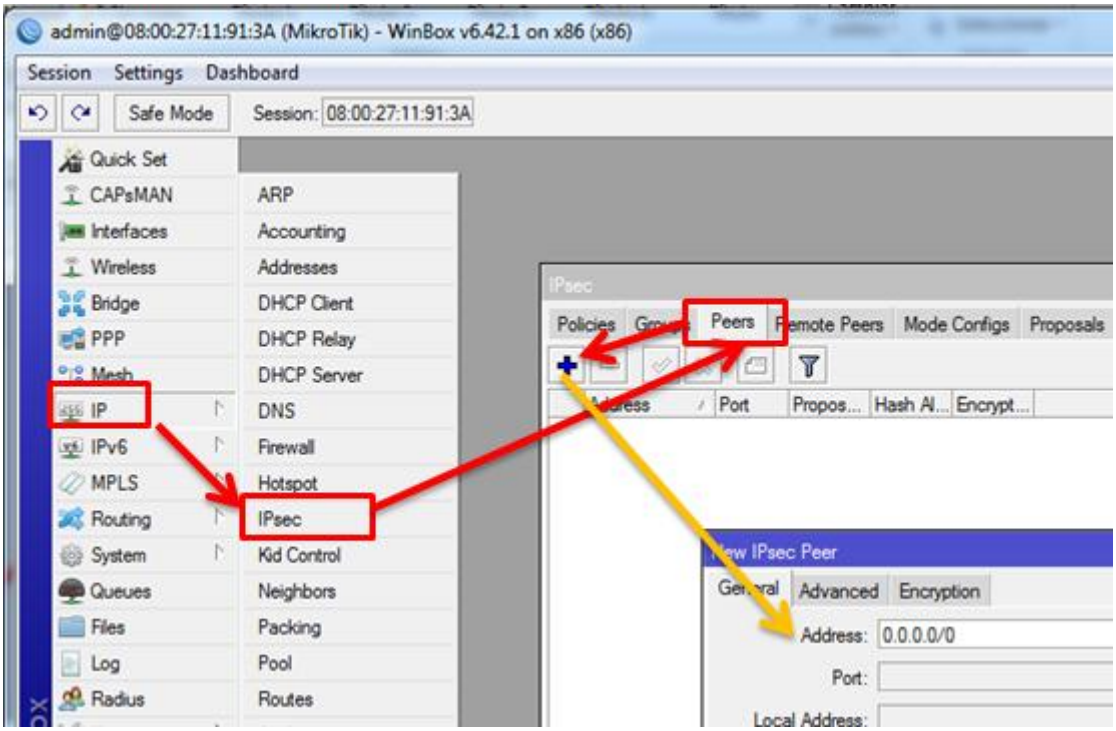


Fuente. El autor

7.2.3.8.3 Configuración del router mikrotik de la sede de Cali

Concluida la configuración la sede de la ciudad de Bucaramanga, se continúa con la programación del router Mikrotik de la sede de la ciudad de Cali. Con la ip de la red WAN de la sede de la ciudad de Bogotá, se inicia la programación de la VPN IPSec en los dispositivos router Mikrotik (figura 38). Esta sede se deberá comunicarse con la sede principal de Bogotá, ya que esta sede tiene toda la información almacenada en el clúster de servidores. Para hacer la configuración se abre el programa Winbox. Se hace clic en el menú IP, IPsec. Aparece una ventana, se da clic en el borde Peers y clic en el signo "+".

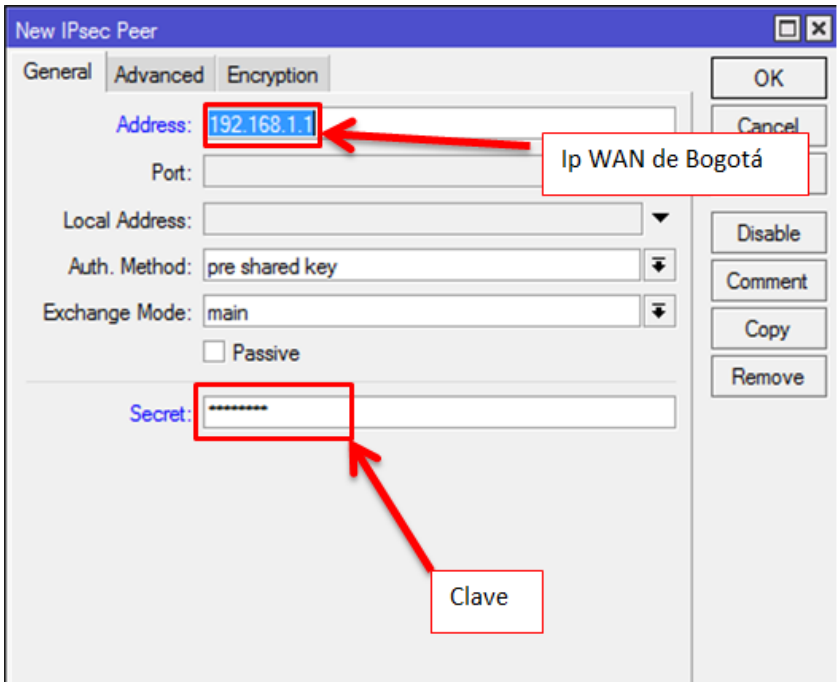
Figura 38. Mikrotik de la sede de Cali



Fuente. El autor

En el cuadro de texto address se ingresa la ip de la red WAN de destino, que en este caso es la sede de Bogotá, y se escribe una clave de seguridad para la creación de la VPN que tendrá la empresa XYZ. Logrando que los equipos (PC) que están en la sede de Cali pertenezcan a la red de la sede de Bogotá (figura 39).

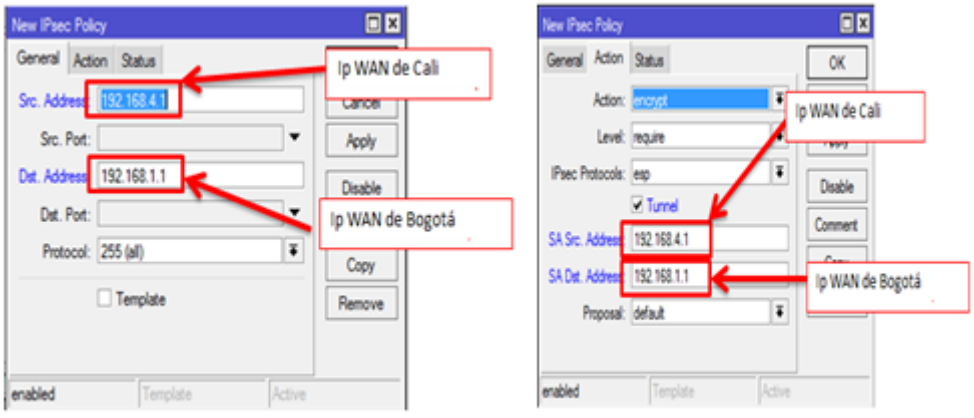
Figura 39. Página peers – general



Fuente. El autor

Se continua con la creación de las políticas para que el router Mikrotik de la ciudad de Cali que tiene la ip 192.168.4.1 se puede comunicar con el router Mikrotik de la ciudad de Bogotá que tiene asignada la ip 192.168.1.1. Para hacer la configuración, se deben hacer los mismos pasos que se realizaron en las ciudades de Medellín Y Bucaramanga. (Figura 40)

Figura 40. Página police – general

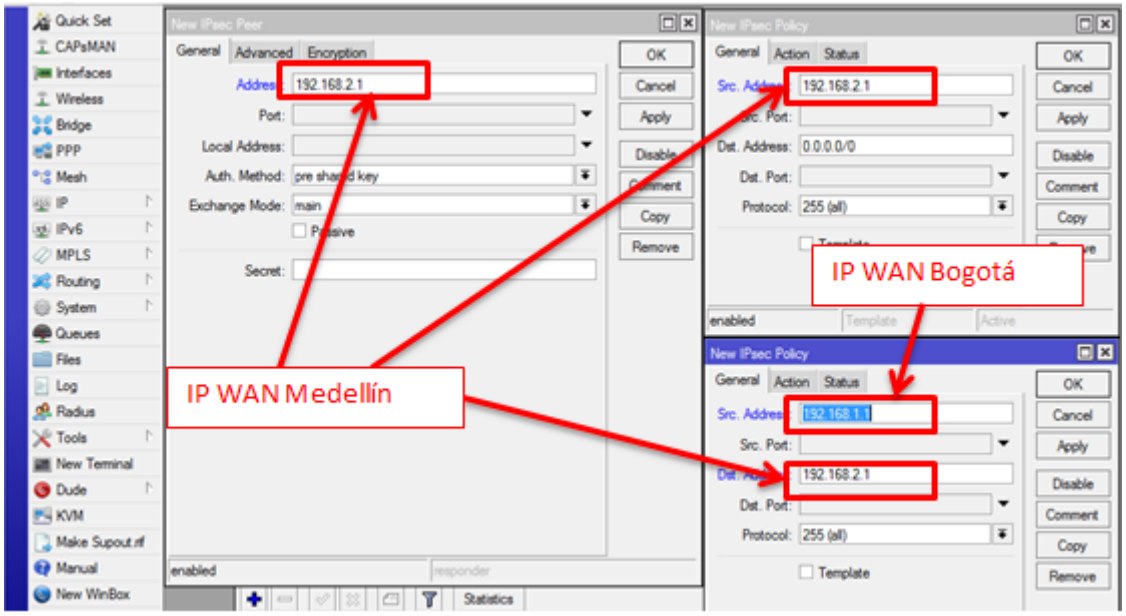


Fuente. El autor

7.2.3.8.4 Configuración de la VPN del router mikrotik desde la sede de Bogotá

Configurados los parámetros de los routers Mikrotik para la creación de la VPN en cada una de las sedes (Medellín, Bucaramanga y Cali), se empezará la configuración del router Mikrotik de la ciudad de Bogotá para completar la VPN de la empresa XYZ (figura 41). Se hará la configuración de las políticas de la conexión de la sede de Bogotá con la sede de Medellín, lo cual se realizan los mismos pasos que se realizaron en la ciudad de Medellín Bucaramanga y Cali.

Figura 41. Router Mikrotik de la sede de Bogotá



Fuente. El autor

Configuración de la sede de Bogotá a la sede de Bucaramanga.

Configurado los parámetros del router de Mikrotik de la sede la ciudad de Bogotá hacia la sede de la ciudad de Medellín, se continuará con la configuración del router de la ciudad de Bogotá hacia el router de la sede de la ciudad de Bucaramanga para que haya una apropiada comunicación entre los equipo de cómputo de cada una de las sedes (figura 42).

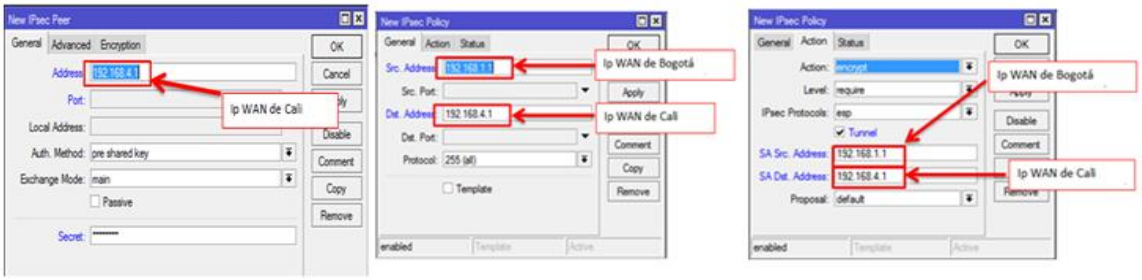
Figura 42. Página peer – general

Fuente. El autor

Configuración de la sede de Bogotá a la sede de Cali.

Configurado los parámetros del router de Mikrotik de la sede la ciudad de Bogotá hacia la sede de la ciudad de Bucaramanga, se continuará con la configuración del router de la ciudad de Bogotá hacia el router de la sede de la ciudad de Cali para que haya una apropiada comunicación entre los equipo de cómputo de cada una de las sedes (figura 43).

Figura 43. Página peer – action



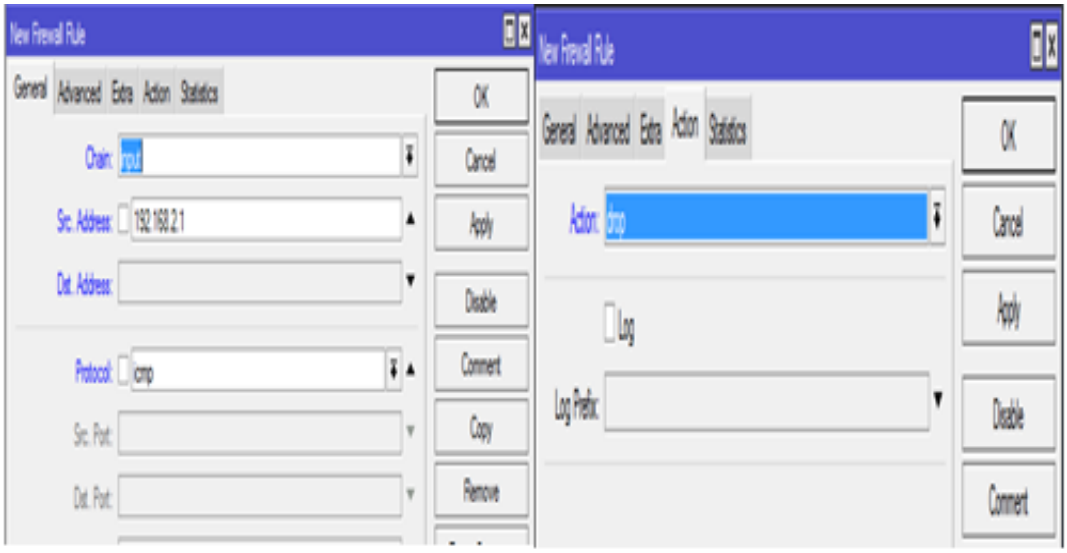
Fuente. El autor

7.2.3.8.5 Bloqueo de ICMP

El ICMP (Internet Control Messaging Protocol) es utilizado para notificar mensajes, y constan de muchos tipos de avisos que permiten tanto anunciar situaciones de error, como ejecutar peticiones de información (Peláez, 2002), y se debe evitar que envié información que podría ser utilizado para ser atacado. Para realizar la configuración de este parámetro se ingresa al menú IP, Firewall, se hace clic en el signo “+”. Aparecerá una ventana donde en la pestaña general en el cuadro de

texto chein se selecciona input, en el cuadro de texto de IP de origen se escribe la IP del dispositivo de red, que en este caso es 192.168.2.1. en el cuadro de protocol se selecciona ICPM. En la pestaña action, en el cuadro de texto action se escoge la opción drop y aceptamos (ok). (Figura 44).

Figura 44. Bloqueo ICMP

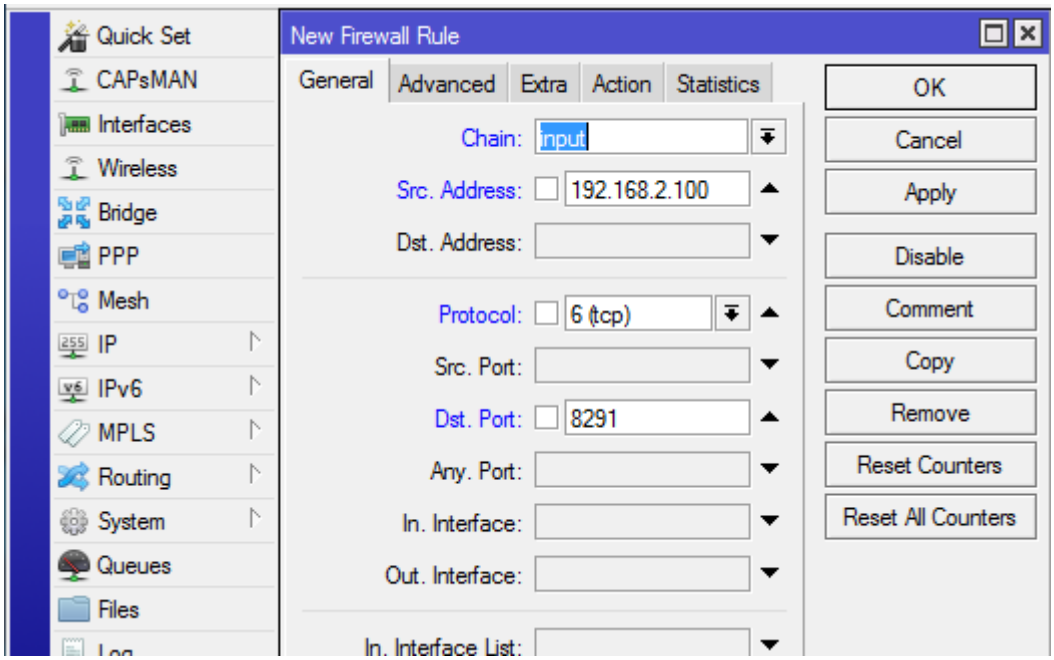


Fuente. El autor

7.2.3.9 Asegurar el winbox

Es importante que todas las aplicaciones que son utilizadas en un sistema informático tengan su método de seguridad. El programa Winbox se puede configura para que tenga su protección, y evitar que personas ajenas al departamento de sistema puedan controlar el router mikrotik, y salvar la configuración que se hicieron en el router mikrotik de las sedes de la empresa XYZ. Para proteger la configuración que se ha realizado con el programa Winbox , se ingresa al menú IP, firewall. En el reborde filter rulers se da clic en el signo “+” y mostrará una ventana. En la pestaña general, en los campos chain se selecciona la opción input, en el rectangulo src address (dirección salida) se escribe la IP, en el campo protocol se escoge la opción 6-tcp, en el campo port se escribe el puerto 8291 y se guarda los cambios. Con esta información, el router mikrotik solo se podrá configurar desde la pc que tenga esta ip 192.168.2.100. Está configuración se hace desde la sede de la ciudad de Bogotá. (Figura 45).

Figura 45. Winbox página general

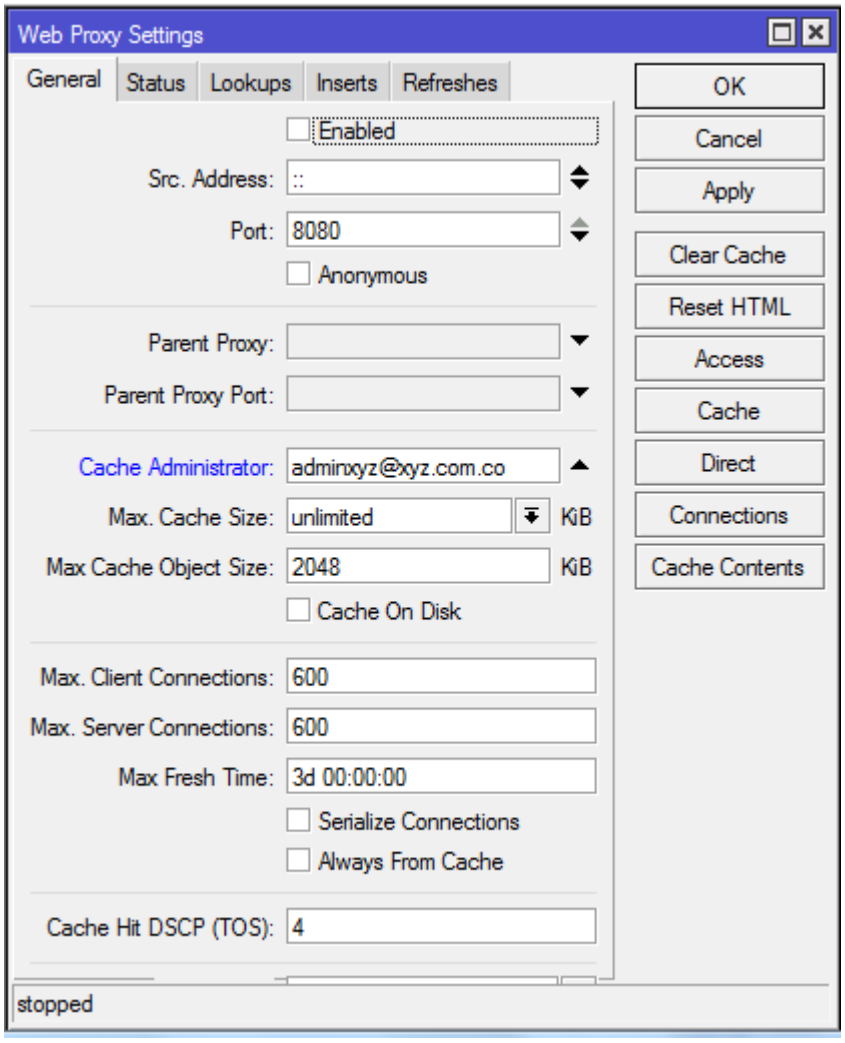


Fuente. El autor

7.2.3.10 Creación de servidor web proxy.

Un servidor proxy puede ser un programa o un equipo que se encarga de recibir las consultas o peticiones que hacen los usuarios de la red hacia el internet. El servidor proxy realiza el trabajo de acceso a Internet en lugar del usuario. El servidor proxy está conectado entre un usuario o equipo (PC) y el equipo que suministra el servicio de internet (modem). Para configurar el servidor web proxy en el equipo de mikrotik se ingresa al menú ip y después se ingresa al menú web proxy. Se ingresan los siguientes datos: en port se pone el 8080, en cache administrator se pone el correo del administrador, que en este caso es adminxyz@xyz.com.co, en max. Cahe size se selecciona unlimited (ilimitado), en max cache object size se digita 2048, en max. conexiones de clientes 600, en max. Conexiones del servidor 600 y finalmente se da clic en ok (figura 46).

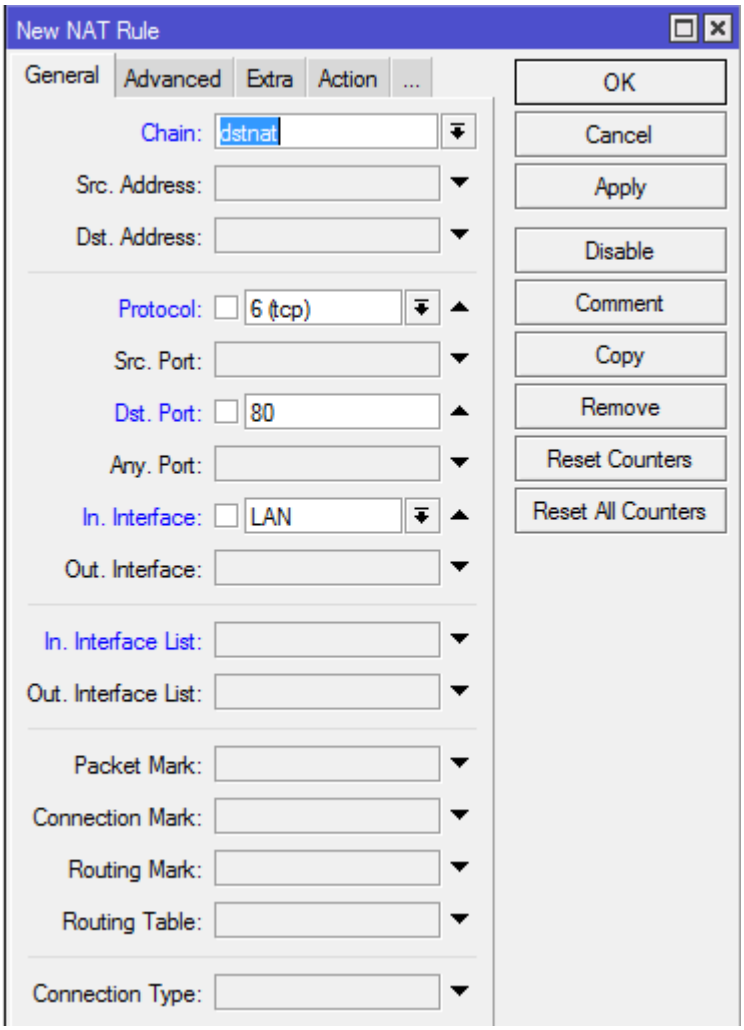
Figura 46: Creación servidor web proxy



Fuente. El autor

El siguiente paso se debe generar un criterio en el firewall para que realice un redireccionamiento al servidor Proxy cuando los usuarios quieran ingresar a internet. Para ello se dirige al menú ip y después a firewall, en la ventana de configuración se hace clic en la pestaña NAT, en seguida clic en el botón (+). La ventana que se muestra se configura de la siguiente forma: en chain se selecciona dstnat, en protocol se escoge tcp, puerto de destino se escribe 80, e interfaz de entrada se selecciona LAN y por último se da clic en ok (figura 47).

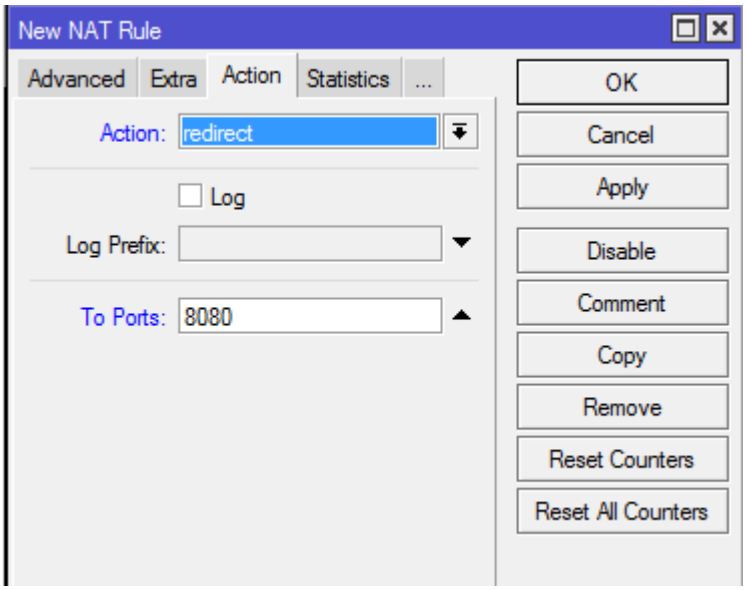
Figura 47: creación de regla general en el servidor web proxy



Fuente. El autor

Configurada esta sección, se da clic en la pestaña action para hacer los últimos cambios en las reglas. Los datos ingresados son los siguientes: en action se selecciona redirec, que toda información que le esté llegando lo redirecciones al puerto que se especifica en el campo port, que en este caso es el 8080, asegurando así, que todas las solicitudes hacia internet que hagan los usuarios tengan que pasar por el servidor proxy (figura 48)

Figura 48: Creación de regla action en el servidor web proxy

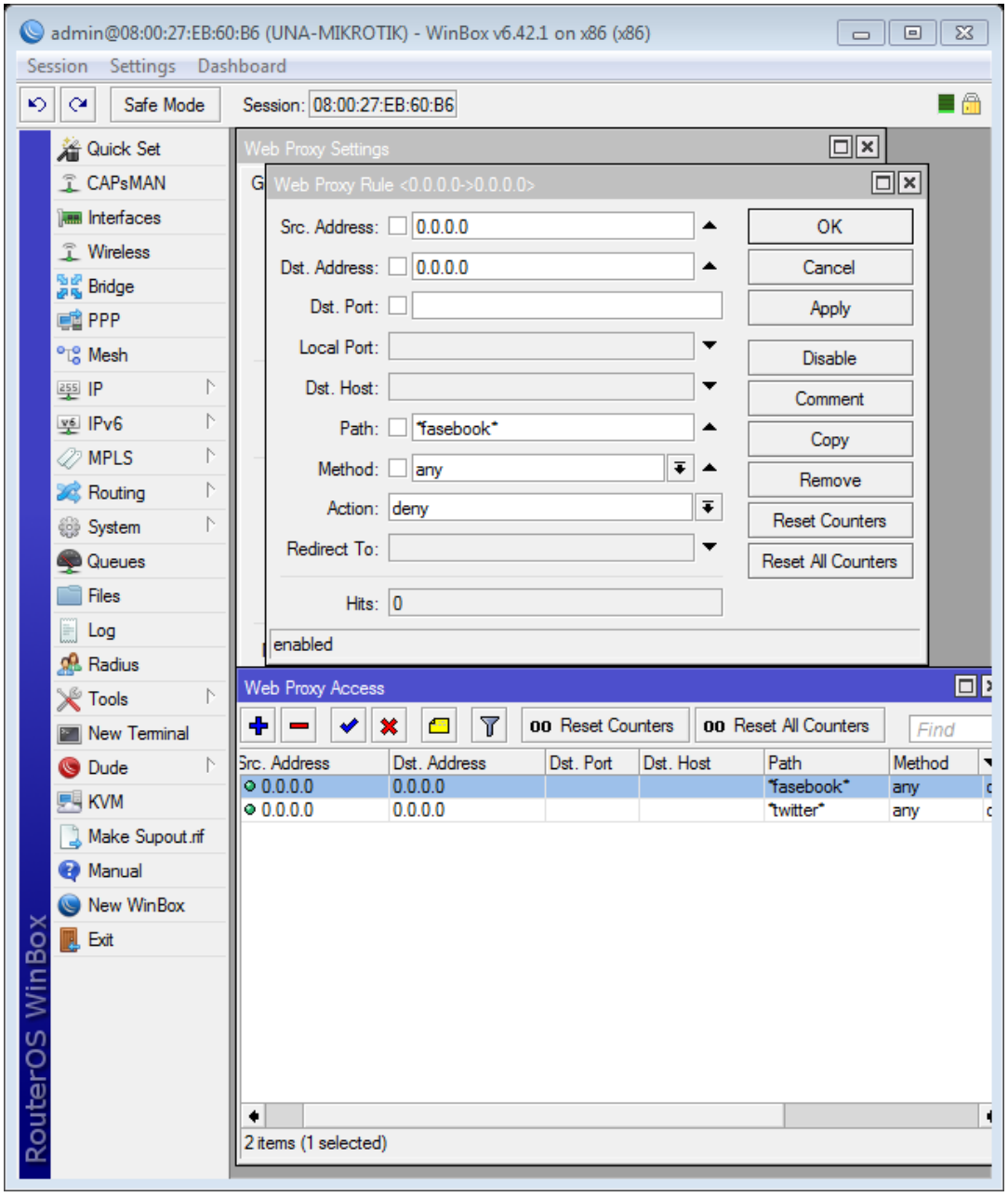


Fuente. El autor

7.2.3.10.1Bloqueo de páginas en el servidor proxy.

Otra forma de bloquear páginas en las oficinas de la empresa xyz para evitar distracciones en horarios laborales y evitando que los empleados disminuyan su rendimiento en sus actividades asignadas, es creando reglas de bloqueo en el servidor proxy. Para hacer los bloqueos de los sitios web no autorizados se realiza la siguiente configuración en el router mikrotik: se da clic en el menú IP, después en Web Proxy. En la ventana que se muestra, se da clic en el Access, aparece una nueva ventana, se da clic en el icono (+). Se mostrará una ventana donde se ingresan los siguientes datos, en Src. Address se escribe 0.0.0.0, en dst address 0.0.0.0, en Path se coloca entre asteriscos la palabra que tenga el sitio web que se quiere bloquear (*Facebook* o *twitter*) y la acción que se debe ejecutar es deny (denegar). Este filtro obstruirá cualquier sitio que tenga la término *Facebook * o *twitter* en su alias. También se aplica en Google, debido a que si un usuario busca algo con estas palabras o cualquier otro buscador también se bloquea la búsqueda (figura 49). (Delgado, 2018).

Figura 49: bloqueo de página en el servidor web proxy



Fuente. El autor

7.2.3.10.2 Bloqueo de descarga directa de archivos.

En la actualidad se han creado diferentes formas de esconder un virus que pueda pasar las barreras de seguridad en un sistema. Y uno de los métodos que se utilizan es esconder un virus en una foto, en un archivo ejecutable, en un archivo de música, en un archivo comprimido, etc. Para disminuir el ingreso de los virus por este medio, el router mikrotik se debe configurar para que niegue la descarga de estos tipos de archivo de internet.

La configuración es igual a la que se hizo en el bloqueo de las páginas web en el servidor proxy. El único parámetro que se cambia es el de “path”, que en vez de poner la palabra que se debe bloquear para evitar ingresar a sitio, se pone la extensión del archivo a denegar. En este caso serán bloqueados los ficheros que posean las siguientes extensiones: avi (video), mp3 (música), mp4 (video), exe (programas) como se visualiza en la figura 50. (Delgado, 2018).

Bloqueo archivos. Mp3

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- Path: *.mp3
- Method: any
- Action: deny

Bloqueo Archivos. Avi

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- Path: *.avi
- Method: any
- Action: deny

Bloqueo Archivos RAR

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- Path: *.rar
- Method: any
- Action: deny

Bloqueo Archivos ZIP

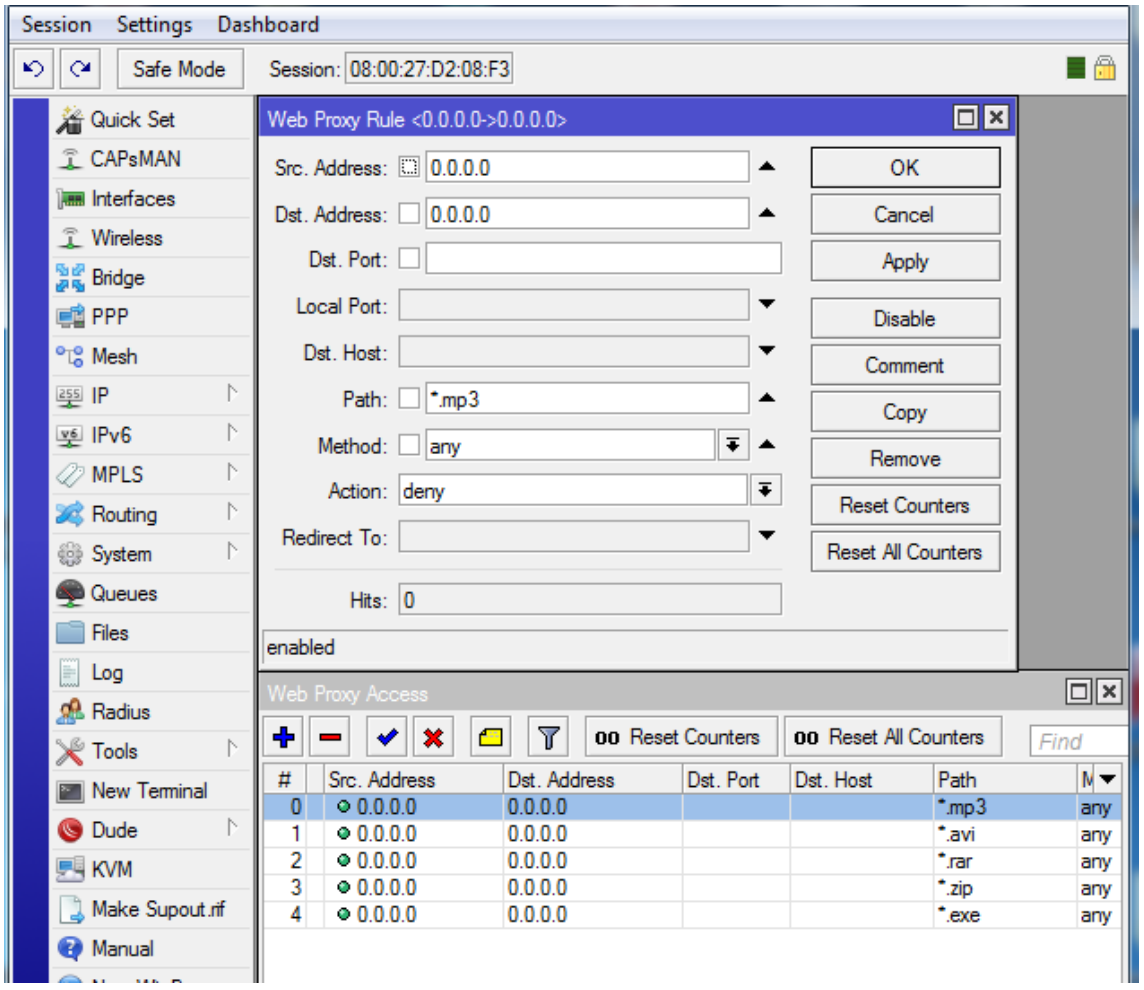
- Src. Address: 0.0.0.0/0

- Dst. Address: 0.0.0.0/0
- Path: *.zip
- Method: any
- Action: deny

Bloqueo Archivos EXE

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- Path: *.exe
- Method: any
- Action: deny

Figura 50: configuración de bloqueo de archivo

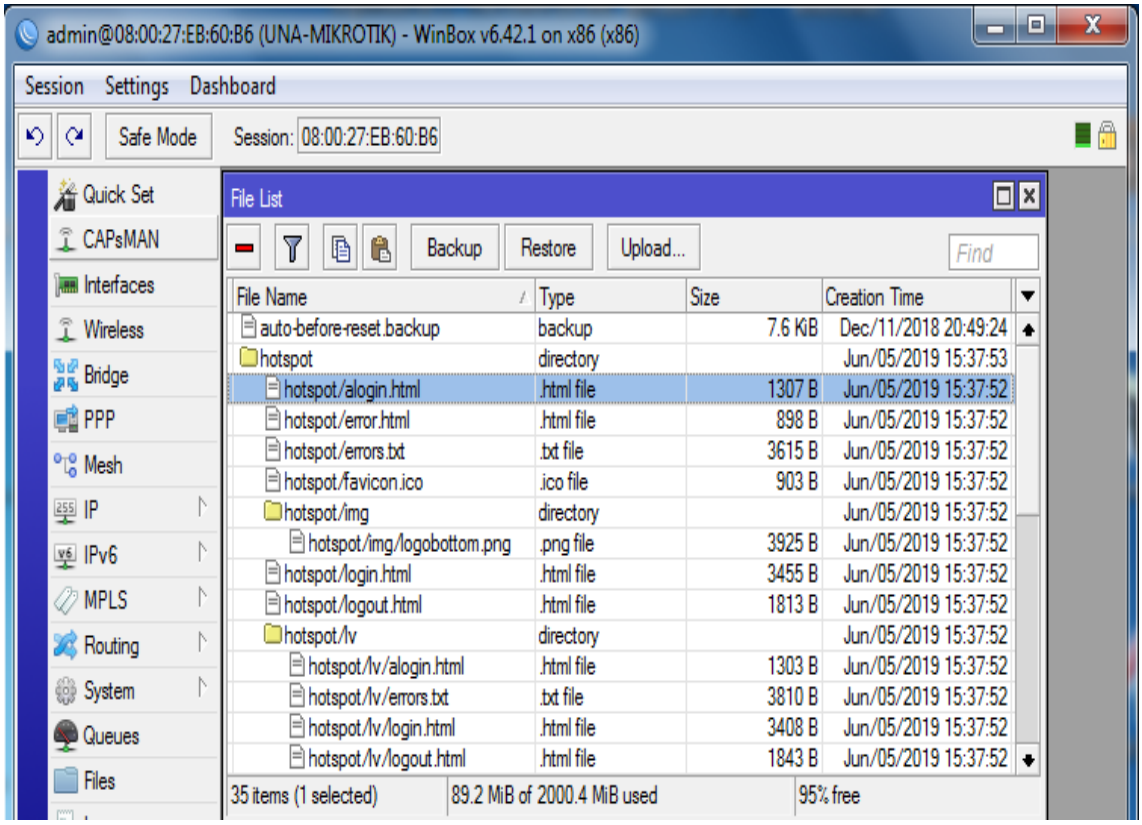


Fuente. El autor

7.2.3.11 Crear el backup de router mikrotik

Cuando se instala un equipo como el router Mikrotik cuenta con parámetros que son configurados por el administrador del sistema, es necesario hacer una copia de seguridad (backup) a la configuración establecida, con el objetivo de usarlo cuando el router mikrotik presenta falla como por ejemplo: programación mal realizada, facilitando la reconfiguración de forma casi inmediata, evitando pérdidas considerables de tiempo de funcionamiento de la red de computadores que depende de el. Para hacer un backup de la configuración del router mikrotik por medio del programa Winbox, se ingresa a la pestaña file (figura 51) y se da clic en backup. (Ramos, 2013).

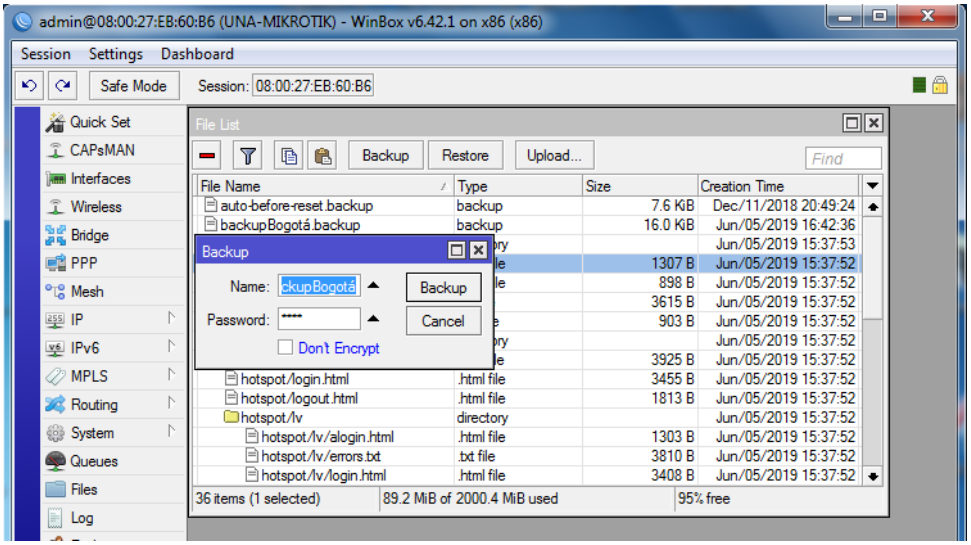
Figura 51: crear un backup



Fuente. El autor

Se muestra una segunda ventana (figura 52) donde se debe digitar el nombre del archivo del backup que se va a crear en este caso se llama backupBogota, ingresar una contraseña. Si se quiere que el archivo sea encriptado no se debe marcar la opción don't encrypt, y hacer clic en el botón backup. El archivo aparecerá en la lista de los archivos que se han creado en el router mikrotik y se almacenara como un archivo binario (figura 52).

Figura 52: nombre del archivo backup

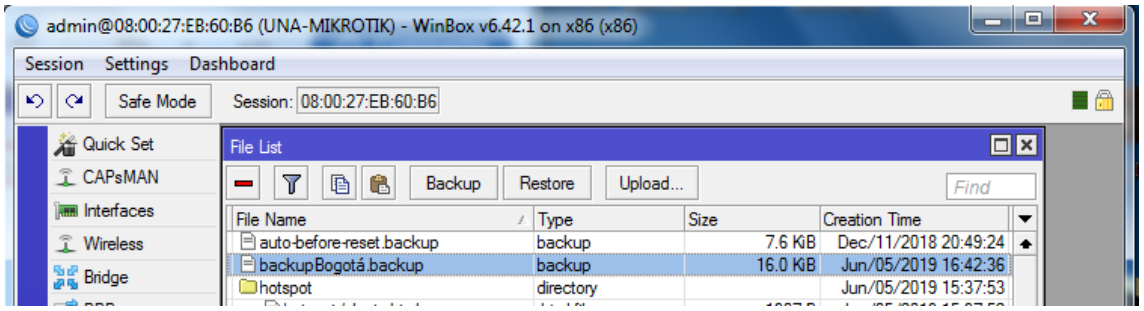


Fuente. El autor

7.2.3.12 Guardando el backup en el computador del administrador.

Cuando se crea el archivo de seguridad de la configuración, este se puede extraer del router mikrotik y almacenarlo en otro lugar. Para extraer el archivo y almacenarlo en el computador del administrador, se hacen lo siguiente: se ingresa al menú file, se selecciona el archivo, que este caso se llama backupBogotá, y se da clic en el botón copiar. El botón copiar es el que tiene el dibujo de hojas de papel en blanco, y se pega en el lugar deseado del computador del administrador (figura 53)

Figura 53: exportar archivo backup

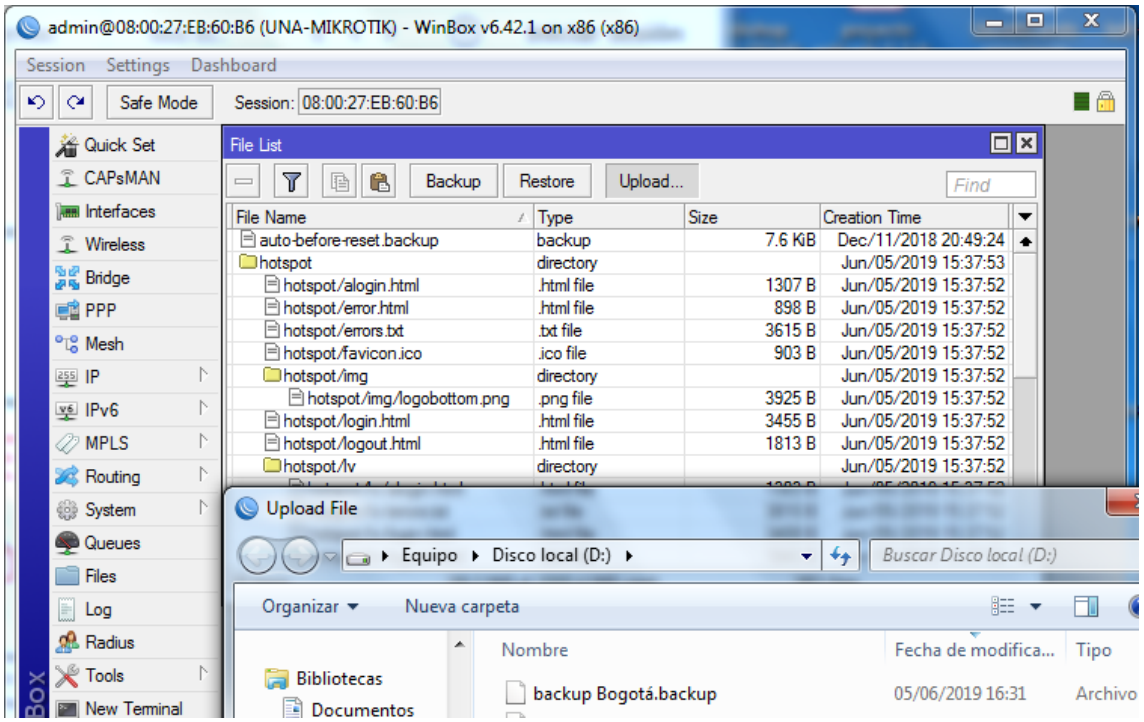


Fuente. El autor

7.2.3.13 Importar y restaurar la configuración.

Cuando se quiera cargar un archivo de configuración que se ha almacenado en un lugar fuera del router mikrotik, se hace los siguientes pasos: se ingresa al menú file y se da clic en upload para buscar el archivo de configuración deseada, este archivo tiene una extensión .backup. Este archivo se ha copiado en el disco D del equipo del administrador (figura 54). (Di Rienzo, 2010).

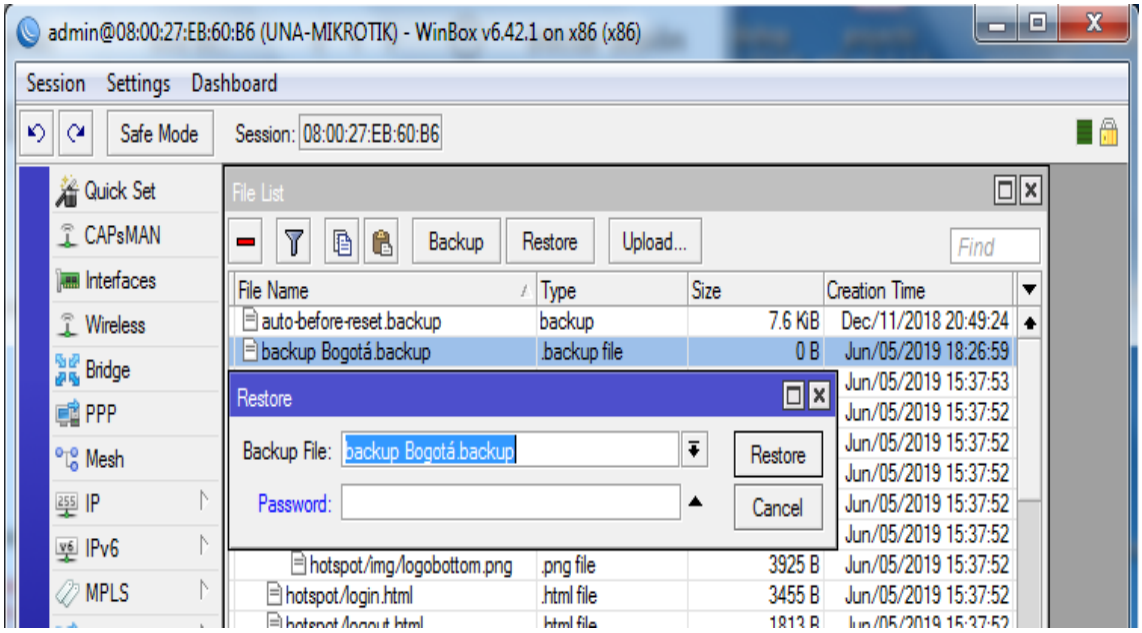
Figura 54: importar archivo de backup



Fuente. El autor

Cuando el archivo está cargado en el router mikrotik, ya se puede utilizar el archivo para poder restaurar la configuración del router mikrotik. Para hacer la restauración del router mikrotik, se debe escoger el archivo y dar clic en restore y después en la ventana emergente clic en restore (figura 55) (Di Rienzo, 2010).

Figura 55: restaurar configuración del router

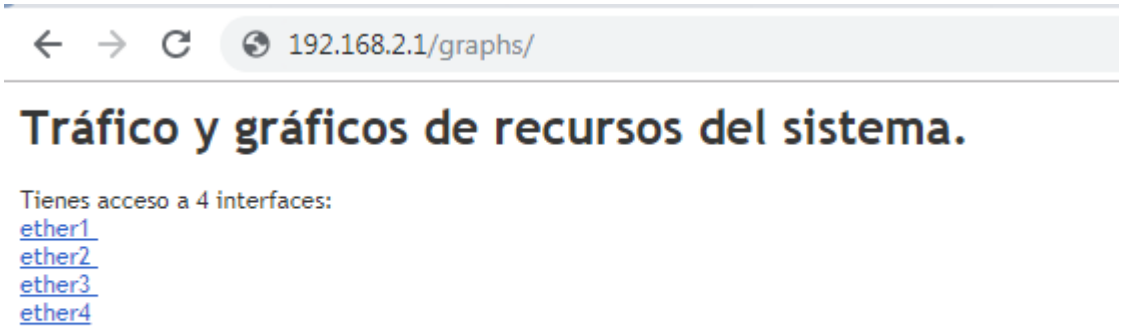


Fuente. El autor

7.2.3.14 Ver de forma gráfica el tráfico en la tarjeta de red del router mikrotik.

Es importantes tener un informe de forma gráfica sobre el tráfico que está pasando por todas las interfaces que tiene habilitada el router mikrotik. Con el objetivo de conocer si se hizo una buena configuración con la asignación de ancho de banda a cada una de las interfaces del router Mikrotik. Uno de los métodos para conocer que las tarjetas de red están disponibles en el router, solamente se necesita un dato y es la ip que se le asignó al router Mikrotik en cada una de las sedes de la empresa xyz. Por ejemplo, si desean visualizar el tráfico que ha tenido la sede de la ciudad de Bogotá, se abre un navegador (Chrome, Firefox, etc.) y se escribe la ip del router Mikrotik en la barra de dirección (figura 56). (Delgado, 2018).

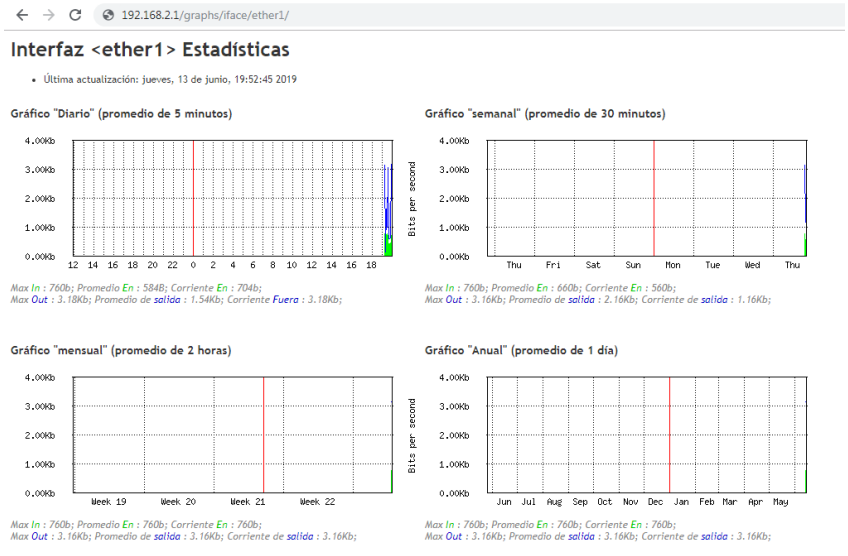
Figura 56: tarjeta de red activas



Fuente. El autor

Al digitar la dirección ip del router Mikrotik en un navegador (Chrome), se mostrará cuales interfaces están activas en el equipo router de mikrotik. Para conocer el movimiento que ha tenido cada una de las interfaces, solo vasta en dar un clic en el alias de la tarjeta deseada, y mostrará un gráfico de su actividad. Son 4 los gráficos que se visualizan, cada uno visualiza una estadística, que está en función del tiempo, en el primer grafico muestra un promedio diario de funcionamiento, el segundo está el grafico del promedio estadístico semanal que tiene la tarjeta de red, el tercer grafico contiene el promedio mensual y el cuarto grafico describe el promedio anual que ha tenido (figura 57).

Figura 57: gráfico de funcionamiento de tarjeta de red



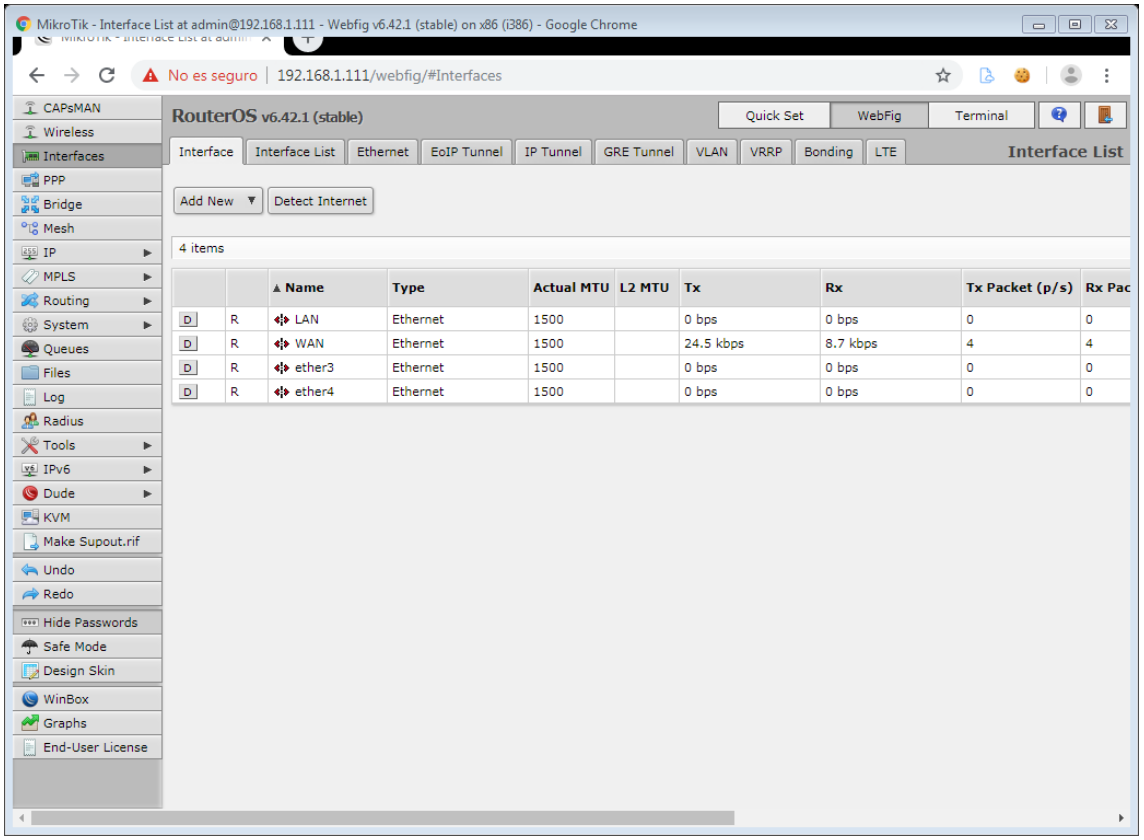
Fuente. El autor

Este método es muy eficiente, porque muestra en cualquier momento como está el tráfico en la red, facilitando su estudio y poder hacer las mejoras de configuración que se necesiten en el caso de ser necesario, y hacer un informe de forma inmediata de cómo ha sido su funcionamiento en el periodo de su actividad.

7.2.3.15 Otros programas que se utilizan para configurar el router mikrotik

Los programas que se utilizan para hacer las configuraciones del router mikrotik, son aplicaciones que trabajan en la capa 7 (aplicación) en el modelo OSI (interconexión de sistemas abiertos) o en la capa 4 del modelo tcp/ip (protocolo de comunicación de trasmisión/ internet protocolo). El primer programa que se usará para la conexión con el router mikrotik es un navegador (chrome). Se digita la ip que fue asignada al router Mikrotik, se escribe la clave y contraseña, se ingresa al router para hacer las configuraciones deseadas (figura 58). (García, 2017).

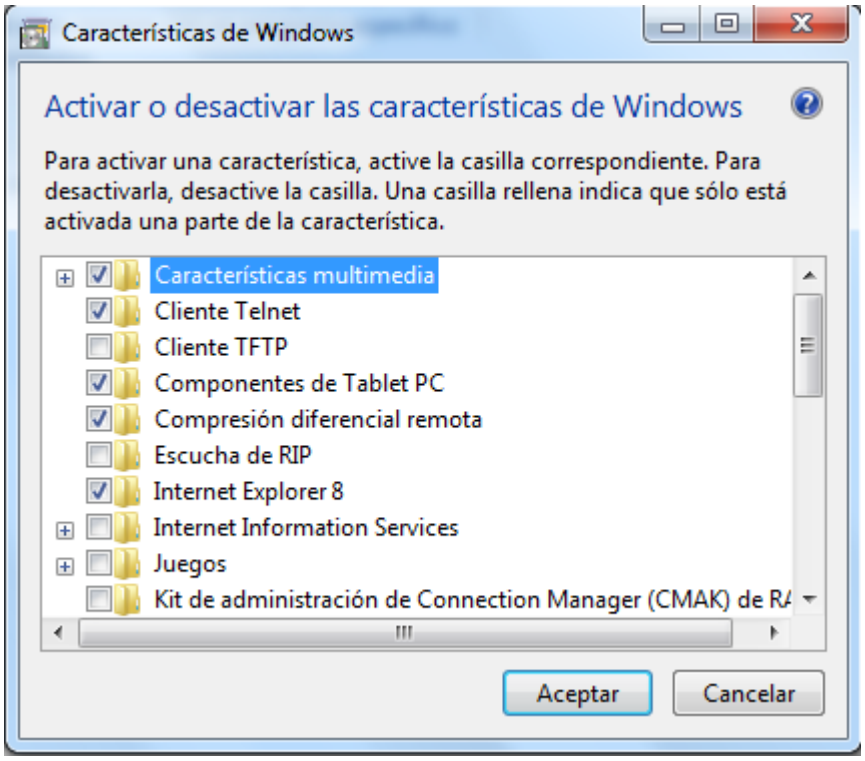
Figura 58: utilizando chrome para configurar el router mikrotik



Fuente. El autor

Existe protocolo que se puede utilizar para hacer las configuraciones del router mikrotik, es telnet. Por defecto el router tiene habilitado el servidor telnet. En los equipo que tienen instalado el sistema operativo Windows tiene deshabilitado el telnet cliente, para actívalo se debe ingresar a panel de control, programa, activar y desactivar características de Windows y habilitar la opción de cliente telnet (figura 59)

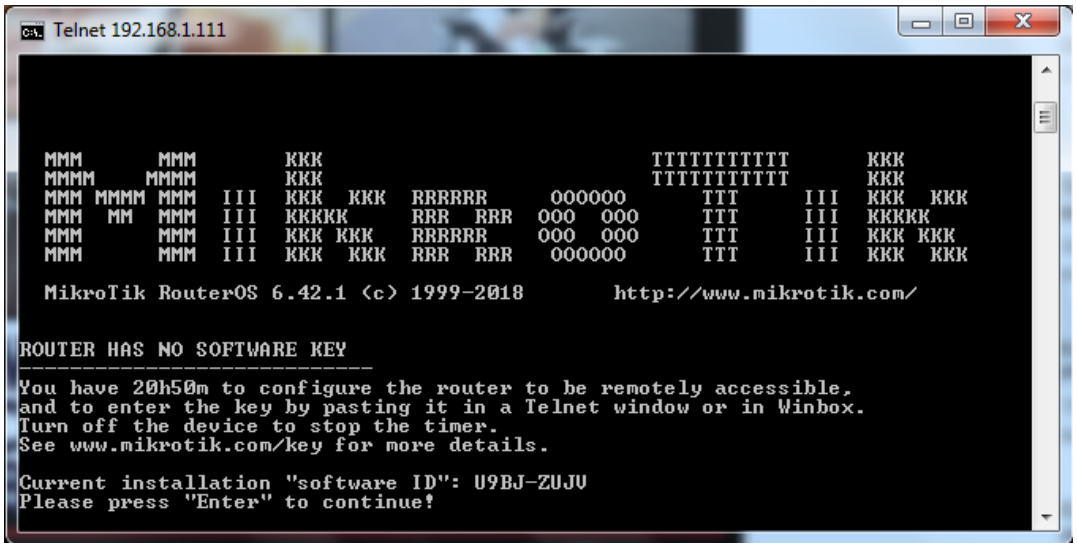
Figura 59: habilitando telnet en Windows



Fuente. El autor

Habilitado el cliente telnet de Windows, se ejecuta el cmd y se escribe el comando telnet seguido de la ip del router mikrotik. Se digita la clave y contraseña, mostrando la consola de comando, la versión del sistema operativo que tiene el router y esperar que le ingresen las instrucciones de configuración (figura 60). El inconveniente que tiene este programa es que no encripta la información que es enviada, lo cual lo hace vulnerable.

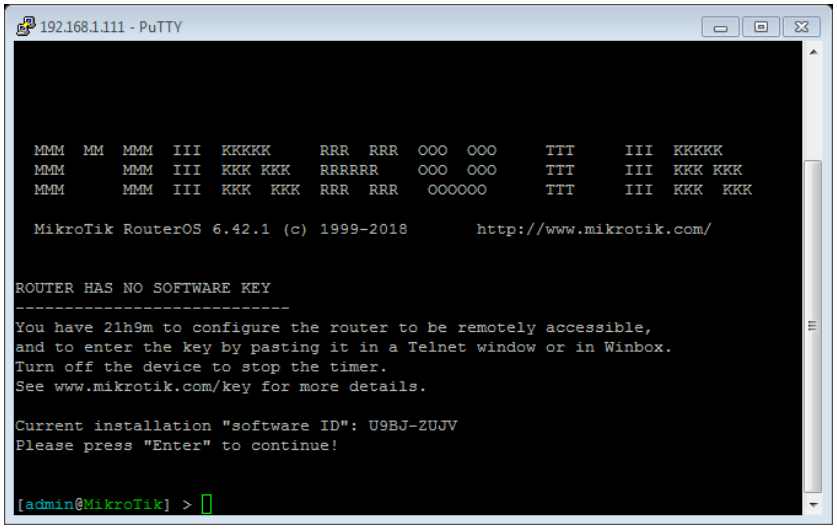
Figura 60: utilizando telnet para configurar el router mikrotik



Fuente. El autor

El siguiente programa que se puede usar es Putty. Este programa es mejor que el protocolo telnet, porque Putty encripta la información enviada, aumentando la seguridad de los datos. El programa Putty como el telnet no tiene interfaz gráfica, lo cual lo hace un poco difícil de utilizar, porque solo se usan comandos y los resultados los muestra en pantalla (figura 61)

Figura 61: utilizando Putty para configurar el router mikrotik

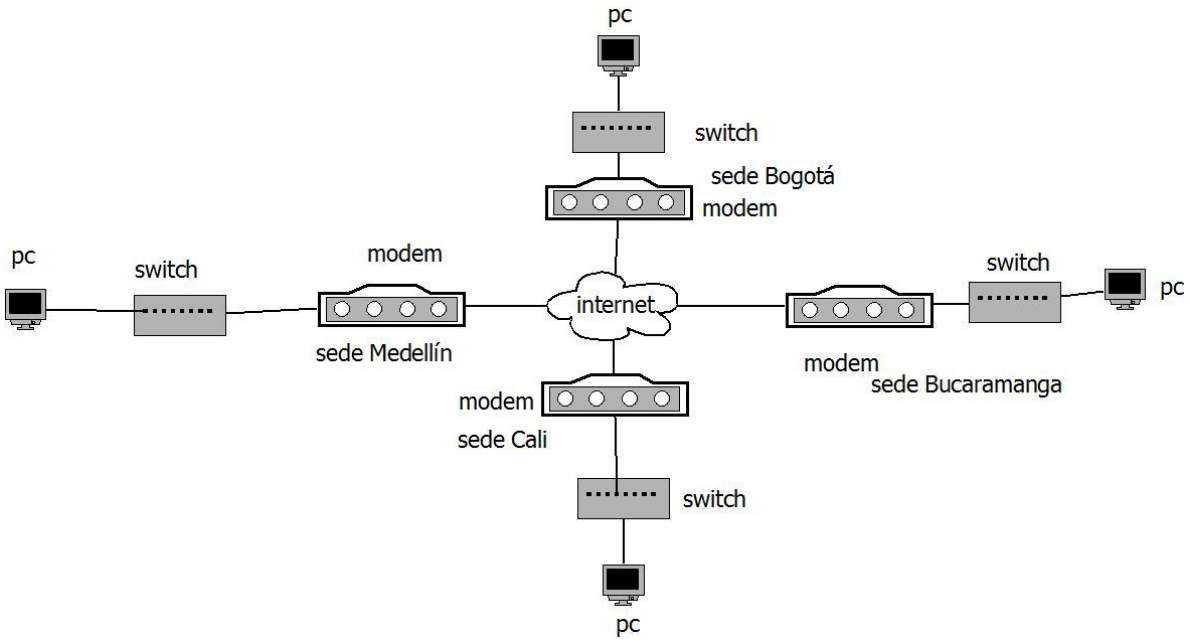


Fuente. El autor

7.2.4 Fase 4. Resultado y Prueba de comunicación de las sedes.

Antes de empezar el proyecto, las sedes trabajaban como LAN's independientes, y no tenían comunicación directa con el clúster de servidores que esta instalados en la agencia principal en la ciudad de Bogotá. Esta situación estaba disminuyendo la efectividad de sus actividades laborales. En la figura 62 se muestra como estaban las redes.

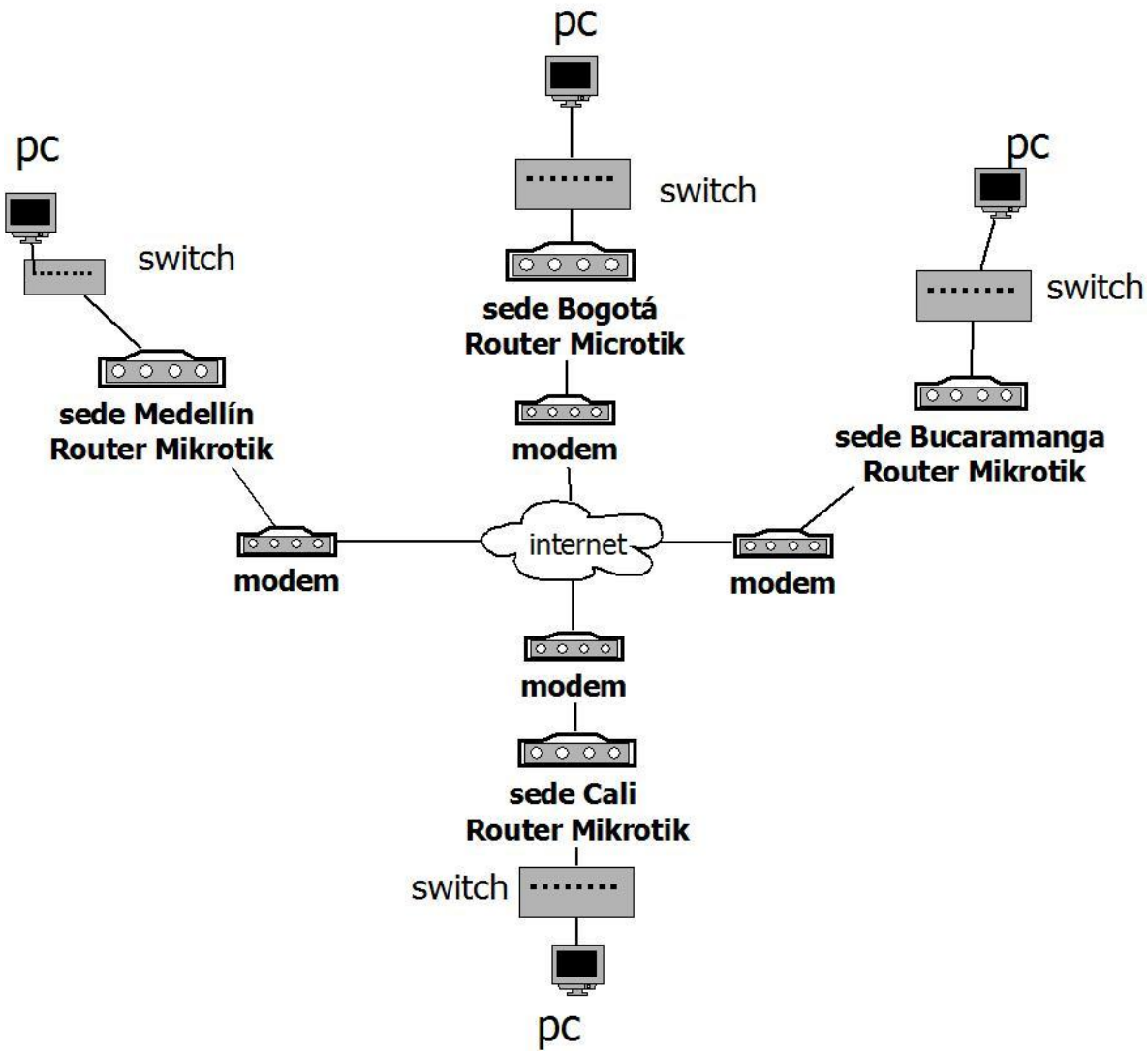
Figura 62. Red de la empresa sin Mikrotik



Fuente. El autor

Al terminar el proyecto, las redes que se veían distanciadas, ahora forman una sola LAN virtual, lo que facilita la comunicación entre las sedes (Bogotá, Medellín, Cali, Bucaramanga), logrando que todas las oficinas de la empresa XYZ transfieran de forma segura la información privada y usar todos los servidores que están centralizados en la sede principal de Bogotá, así lo visualiza la figura 63.

Figura 63. Red con Mikrotik



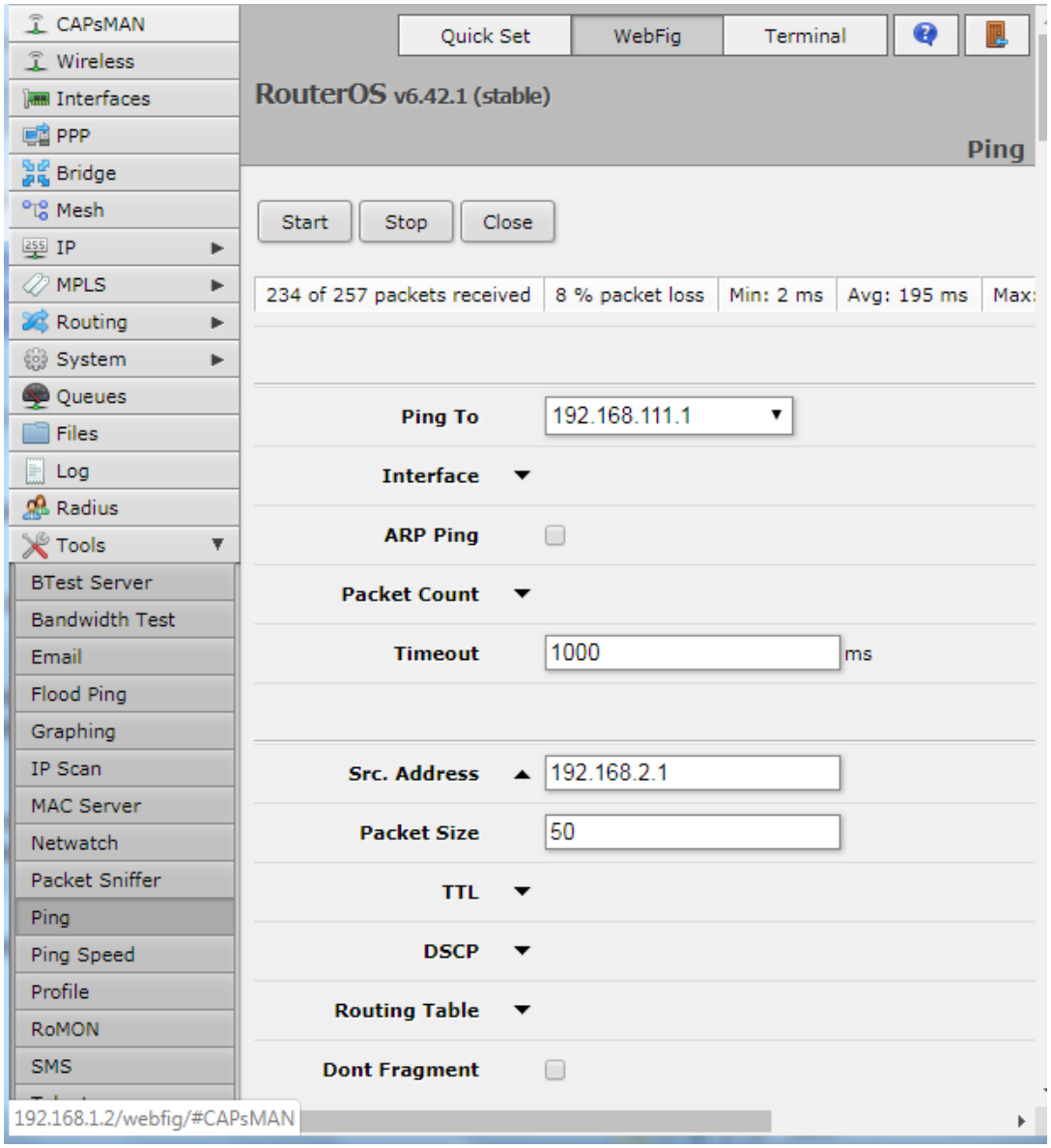
Fuente. El autor

7.2.4.1 Prueba de comunicación.

Para validar la comunicación entre la sede de la ciudad de Bogotá con la sede de la ciudad de Medellín, se realiza un ping a la LAN que está conectada al router Mikrotik de la sede de la ciudad de Bogotá desde la LAN que está conectada del router Mikrotik de la sede de Medellín. La ip de origen es 192.168.2.1 (LAN de Medellín) y la ip de destino es 192.168.111.1 (LAN de Bogotá). La validación se hace utilizando el navegador Chrome digitado en la barra de direcciones la ip que

fue asignada al router Mikrotik, se escribe el usuario con la contraseña, se hace clic en el menú tool, y después clic en ping. En la ventana que aparece se escribe la ip de origen y la de destino. Se da clic en el botón start y se presenta el número de los paquetes que se han enviado y el porcentaje de paquetes que se han perdido. En la validación que se realizó se muestra que se enviaron 257 paquetes de los cuales se recibieron 234 y se perdió el 8% de paquetes (figura 64).

Figura 64: validación de comunicación



Fuente. El autor

7.2.5 Fase 5. Recomendaciones

- Si desean crear más sedes en otras ciudades en Colombia o en otro país, se sugiere utilizar el mismo equipo de Mikrotik.

- Utilizar criptografía asimétrica porque este método utiliza dos claves, una privada y otra publica y mejorará aún más la seguridad en la transmisión de información.

- No utilizar otro medio de comunicación como por ejemplo: wifi públicos, para enviar información de la empresa, solo usar la VLAN que pertenezca a la empresa XYZ.

- Extraer una copia de la configuración del router cada vez que se actualice alguno de los parámetros. Con el propósito de tener una duplicado de seguridad en caso tal de que el dispositivo presente un daño físico como una sobre carga eléctrica.

- Complementar la seguridad utilizando programas de escaneo de vulnerabilidades en la red. Para encontrar posibles errores de configuración como puertos abiertos sin ninguna función.

- Utilizar programas que detecten de intrusos en la red, para conocer en qué momento se produce y como evitarlo. Esta herramienta es muy importante porque alerta al administrador de la red que están intentando ingresar al sistema.

- Se debe crear políticas de seguridad informáticas a medida que se vaya actualizando los sistemas de información, para poder disminuir los peligros de pérdida o daño que puede tener los datos almacenados en los equipos de la empresa XYZ.

CONCLUSIONES

Cuando en una empresa solicita el servicio de internet, es instalado un modem que tiene alguna configuraciones que son realizadas por la ISP (Internet service provider) o proveedor de servicios de Internet, y no son suficientes para brindar una seguridad adecuada a una empresa que piensa ampliar sus actividades económicas a nivel nacional o internacional. Las configuraciones que se le podrán hacer a este dispositivo (modem) son muy básicas como por ejemplo: bloquear determinados puertos, habilitar el DHCP para que asigne las direcciones ip a los equipos que se puedan conectar, habilitar el WIFI, etc. Y estas configuraciones solo lo puede hacer el distribuidor de servicios de Internet. Esto quiere decir que la compañía que está utilizando el modem no puede habilitar o deshabilitar alguna función que necesite.

Con la instalación del router mikrotik se tendrá un control total de la red de computadores de la empresa XYZ, haciendo las configuraciones que se desea sin la necesidad de estar llamando al proveedor de servicios de Internet para que haga alguna configuración que se necesite. El modem solo servirá para conectarse a internet.

Para controlar o hacer alguna configuración al router mikrotik se puede hacer de dos formas: la primera es estar conectado al router directamente y la segunda es instalar un programa en el computador del administrador del sistema para que no tenga que estar físicamente conectado al router y hacer las configuraciones deseadas. El programa que se usa para la configuración remota del router estará instalado en el equipo del administrador del sistema es Winbox. Con este software se puede configurar el router mikrotik de una forma gráfica pero también se puede hacer las configuraciones por medio de comando utilizando una consola o terminal que este programa tiene.

La empresa XYZ en sus diferentes sedes (Bogotá, Medellín, Bucaramanga y Cali) ha contratado el servicio de internet con el ISP, lo cual puede controlar el router mikrotik; con el router mikrotik se puede asignar el ancho de banda a los equipos según sus necesidades laborales, evitando así el desperdicio de ancho de banda en algunos equipos que no lo necesitan.

El router mikrotik para estar actualizado en la hora y fecha utiliza un servidor SNTP (Simple Network Time Protocol). El router mikrotik se está comunicando periódicamente con un servidor externo que le está mandando información sobre

la hora y fecha actual. Esto debe ser así, porque si en algún momento falla por algún motivo el suministro de energía y se restablece, se pueda actualizar la fecha y hora de forma automática.

Para evitar que cualquier equipo se conecte a la red de la empresa XYZ sin autorización, se relacionó la MAC (Media Access Control) de los equipo de la empresa con la ip asignada, evitando que suplanten equipos en la red para extraer información valiosa en cada una de las sedes que podría perjudicar la empresa en sus actividades diarias.

Con la configuración del firewall se controla el paso a sitios web que puedan atacar la seguridad de la información que esta almacenada en la red, evitando que descarguen archivos a los equipos de los usuarios. También se controla el acceso a sitios que pueden distraer a los usuarios en sus actividades laborales, como por ejemplo: a redes sociales.

Cuando se instala el programa Winbox en el equipo del administrador en cada una de las sedes (Bogotá, Medellín, Bucaramanga y Cali), se aseguró para que solo lo pueda usar la persona autorizada en hacer las configuraciones al router, que en este caso solo el administrador de sistema. Con el objetivo de que solo una persona lo pueda configurar y evitar que terceras personas modifique la configuración.

Con la configuración de ICMP (Internet Control Message Protocol), se evita que el router mande cualquier información, que pueda ser utilizada para hacer ataques, como por ejemplo: DoS (Denial of Service) o DDoS (Distributed Denial of Service), que se usa para sacar de servicio cualquier equipo que responda al protocolo de avisos de control de internet.

Al crear un servidor DHCP en el router facilita la identificación de los equipos que pertenecen a las redes de cada una de las sucursales (Bogotá, Medellín, Bucaramanga y Cali), porque se puede asignar rango de ip's diferentes sin que haya conflicto en las comunicaciones, como por ejemplo: se puede asignar el ip a la red de la sede de Bogotá 192.168.1.0 y a la red de la sede de Cali 192.168.2.0.

Cuando una empresa tiene varias sedes en diferentes partes del país o del mundo, y quiere que se comunique entre sí, sin generar mucho costo. La única forma de hacerlo es creando una red privada virtual. Porque no tiene que invertir en infraestructura, porque estará utilizando la infraestructura de ISP.

Cuando se configura un equipo como el router mikrotik se debe tener una duplicado de respaldo de configuración, para estar preparado en caso de que el equipo mikrotik tenga una falla y se pierda la configuración. Teniendo una copia de respaldo, se puede configurar un nuevo router mikrotik sin demora alguna para tener una respuesta casi inmediata sin perjudicar gravemente las actividades de los servicios de la red de la compañía XYZ.

BIBLIOGRAFÍA

AGUILERA LÓPEZ, Purificación. Seguridad informática. Editex, 2010.

ALCALDIA MAYOR de Bogotá. Ley 1273 de 2009. {En línea}. {15 octubre de 2018} disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp.

ALONSO, C. G. M., Gabriel, D. O., Ignacio, A. A., & Elio, S. R. (2014). Procesos y herramientas para la seguridad de redes. Editorial UNED. Disponible en: https://books.google.es/books?hl=es&lr=&id=dG4lAwAAQBAJ&oi=fnd&pg=PP1&dq=seguridad+inform%C3%A1tica+en+redes&ots=N63OyRM7xd&sig=dshylTphjP8v7mT2kdJvIQni5ds#v=onepage&q=seguridad%20inform%C3%A1tica%20en%20redes&f=false

ARGONZA, Javier Salazar. Dispositivos para el almacenamiento de grandes volúmenes de información “Big data”. Revista Digital Universitaria, 2017, vol. 13, no 12, p. 9-10.

ASENSIO, G. (2006). Seguridad en internet. Ediciones Nowtilus SL. Disponible en: http://tecnologiasemergentesnegocios2012.pbworks.com/w/file/fetch/54228387/descarga_promo_SEGURIDAD%20EN%20INTERNET,%20Nowtilus.pdf

BERTOLÍN, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información. Editorial Paraninfo. Disponible en : https://books.google.es/books?hl=es&lr=&id=Huwy1L0PEq8C&oi=fnd&pg=PA19&dq=seguridad+inform%C3%A1tica+en+redes&ots=N_1ndo8Rbz&sig=yIapp2EGHCaVGSxpVZA1496FoSA#v=onepage&q=seguridad%20inform%C3%A1tica%20en%20redes&f=false

BUENDÍA, J. F. R. (2013). Seguridad informática. McGraw-Hill España. Disponible en: https://s3.amazonaws.com/academia.edu.documents/34758985/Seguridad_Informatica_McGraw-Hill_2013_-_www.FreeLibros.me_-_copia.pdf?response-content-disposition=inline%3B%20filename%3DSeguridad_Informatica_Mc_Graw-Hill_2013.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190722%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190722T213744Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=e6a63215582225b05691fda5d198ea0136f3fd1d3a9e11be4651908988aecefa

CAMACHO TRUJILLO, J. R. (2018). Implementación de seguridades, controles de acceso, ancho de banda y servicio DHCP del equipo principal de la red de la Carrera Sistemas de Información de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil en el año 2017 (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Licenciatura en Sistemas de Información.). Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/30435/1/Tesis%20-%20Camacho%20Trujillo%20Jose%20Ricardo.pdf

CARPENTIER, J. F. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. Ediciones ENI. https://books.google.es/books?hl=es&lr=&id=LKE5_6gzBmgC&oi=fnd&pg=PA15&dq=seguridad+inform%C3%A1tica+en+redes&ots=51t3l7V36G&sig=wCmv33e97jK-sicLr4NWtOwgVhM#v=onepage&q=seguridad%20inform%C3%A1tica%20en%20redes&f=false

CASTELLANOS H, Luis R. Seguridad en Informática. España: Editorial Académica Española. 2014.

CASTRO CUBA, Sayco, D. H. (2019). Diseño e Implementación de la Interconexión de Sucursales de HP-STORE en las ciudades de Arequipa y Cusco mediante VPN con MIKROTIK ROUTER. Disponible en: http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/8663/IEcsdh.pdf?sequence=1

CLAVIJO, C. A. D. (2006). Políticas de seguridad informática. Entramado, 2(1), 86-92. Disponible en: https://www.redalyc.org/pdf/2654/265420388008.pdf

DELGADO PROAÑO, J. J. (2018). *Rediseño de la red inalámbrica e implementación de mecanismo de seguridad utilizando mikrotik router os basado en un servidor hotspot aplicando las normas IEEE 802.11 fundación damas del honorable cuerpo consular centro médico Sur* (Bachelor's thesis). Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/15961/1/UPS-GT002232.pdf

DI RIENZO, V. (2010). Mikrotik Tutorial. Victor Di Rienzo. Disponible en: https://books.google.es/books?hl=es&lr=lang_es&id=GKjWfRDzel8C&oi=fnd&pg=PA4&dq=manual+de+mikrotik&ots=hsgDG1FSED&sig=S3klG566pdoc8_t7MkyRXXsun6w#v=onepage&q=manual%20de%20mikrotik&f=false

DOBLADEZ, M. (27 de 11 de 2009). *https://mum.mikrotik.com/.* Recuperado el 10 de 01 de 2019, de https://mum.mikrotik.com/: https://mum.mikrotik.com//presentations/AR09/VPN-MUM-ARG-09.pdf

DOMÍNGUEZ, Oscar Gil. Fundamentos de Redes de Voz IP: 2ª Edición. IT Campus Academy, 2016.

GALLO, Facundo; UNNAMED, Igor. Inseguridad informática. {En línea}. {10 octubre de 2018} disponible en: https://books.google.com.co/books?hl=es&lr=lang_es&id=4Dd_AgAAQBAJ&oi=fnd&pg=PA5&dq=Gallo,+F.,+%26+Unnamed,+I.+(2011).+Inseguridad+inform%C3%A1tica.+Lulu.+com&ots=FSpeyt5Dxm&sig=AvHl06jgLFaH6B3houAC0fFFgUc&redir_esc=y#v=onepage&q&f=false.

GARCIA RUIZ, J. H., & Ruiz Posada, H. B. (2017). Desarrollo de un esquema para la implementación de un servicio personalizado de un servidor HOTSPOT usando user-manager para redes hoteleras (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matematicas y Fisicas. Carrera en Ingenieria en Networking y Telecomunicaciones). Didponible en: http://repositorio.ug.edu.ec/bitstream/redug/19794/1/B-CINT-PTG-N.174.John%20Henrygarcia%20Ruiz%2C%20Henry%20Bryan%20Ruiz%20Posada.pdf

GRANADOS PAREDES, Gibrán. “Introducción a la Criptografía”. {En línea}. {10 septiembre de 2018} disponible en: https://profecd.webnode.es/_files/200000079-90fc291f71/Introduccion%20a%20la%20criptografia.pdf

HERNÁNDEZ DÍAZ, L. (2009). El delito informático. Disponible en: https://addi.ehu.es/bitstream/handle/10810/24953/18-Hernandez.indd.pdf?sequence=1

HERNÁNDEZ, J. C., et al. Técnicas de detección de Sniffers. Rev. SIC. Agorasic, 2000.

HUERTA, A. V. (2002). Seguridad en Unix y redes. Versión, 1, 81. Disponible en: http://www.sysadmin.org.mx/sites/default/files/unixsec.pdf

IGLESIAS, Santiago Pérez. Análisis del protocolo IPsec: el estándar de seguridad en IP. Comunicaciones de telefónica I+ D, 2001, no 23, p. 51-64. Disponible en: http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf

KUROSE, J., & ROSS, K. (2004). Redes de computadores. Madrid: Edit Pearson Addison Wesley.

KUROSE, James F., et al. Redes de computadoras: un enfoque descendente. Pearson, 2010.

LONDOÑO VELÁSQUEZ, J. H. (2015). Diseño de una red para la empresa compañía comercial universal Surtitodo sa basada en Mikrotik. Disponible en: http://repositorio.ucp.edu.co/bitstream/10785/2881/1/CDMIST107.pdf

LONGORIA, J. F. (2005). La Educación en línea: El uso de la tecnología de informática y comunicación en el proceso de enseñanza-aprendizaje. Universidad Autónoma del Carmen. Disponible en: https://www.researchgate.net/profile/Jose_Longoria/publication/228607914_La_Educacion_en_linea_El_uso_de_la_tecnologia_de_informatica_y_comunicacion_en_el_proceso_de_ensenanza-aprendizaje/links/5408c9390cf2822fb737db1b.pdf

LÓPEZ, P. A. (2010). Seguridad informática. Editex. Disponible en : https://s3.amazonaws.com/academia.edu.documents/39361818/Seguridad_informatica_UD01.pdf?response-content-disposition=inline%3B%20filename%3DSeguridad_informatica_-_por_CF.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190722%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190722T200931Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=cf68238abf979a9154ace2933b59430659ff266e839c35a2d76bbfb1a73d6d78

MEJIA, O. A. (2011). Migración del protocolo IPv4 a IPv6. ContactoS, 79, 55-60. Disponible en: http://www2.izt.uam.mx/newpage/contactos/anterior/n79ne/ipv6.pdf

MOLINA RUIZ, Julio Edgar. Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio Planta Norte. 2012.

MOLINA, J. M. M. (2004). Seguridad en redes inalámbricas 802.11. disponible en: https://books.google.es/books?hl=es&lr=&id=c8kni5g2Yv8C&oi=fnd&pg=PA1&dq=seguridad+inform%C3%A1tica+en+redes&ots=3pzWFDt7Xr&sig=wOTgi6s5qEWpBk3bi7l6HYastHU#v=onepage&q=seguridad%20inform%C3%A1tica%20en%20redes&f=false

MUÑOZ LÓPEZ, J. O. (2018). Implementación de balanceo de carga de internet con Mikrotik en la dirección de Red de Salud Conchucos Sur-Huari; 2017. Disponible en: http://repositorio.uladech.edu.pe/xmlui/bitstream/handle/123456789/1978/BALANCEO_DE_CARGA_INTERNET_MUNOZ_LOPEZ_JUAN_ORLANDO.pdf?sequence=1&isAllowed=y

PELÁEZ, R. S. (2002). Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados.
PELÁEZ, Raúl Siles. Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados. 2002. http://ftp.nluug.nl/ftp/pub/os/Linux/doc/LuCaS/Manuales-LuCAS/doc-seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf

RAMOS TICONA, C. F. (2013). Implementación de una red Lan en base Mikrotik Routeros para brindar servicio de Internet ADSL a la zona este de La Paz (Doctoral dissertation). Disponible en: https://repositorio.umsa.bo/bitstream/handle/123456789/10735/EG-1397-Ramos%20Ticona%2C%20Cindy%20Fiorela.pdf?sequence=1&isAllowed=y

RUS, Juan José González, et al. Delito e informática: algunos aspectos. Universidad de Deusto, 2007.
SALAZAR, J. B., & CAMPOS, P. G. (2008). Modelo para Seguridad de la Información en TIC. Concepción, Chile: Universidad del Bío-Bío. Disponible en: http://ceur-ws.org/Vol-488/paper13.pdf

SALGUERO REINOSO, D. O. (2015). Administración y distribución efectiva del internet a través de Mikrotik (Bachelor's thesis, Quito: Universidad Israel, 2015). Disponible en: http://157.100.241.244/bitstream/47000/749/1/UISRAEL-EC-SIS-378.242-139.PDF

SÁNCHEZ, A. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. Atención Primaria, 46(4), 214-222. Disponible en: https://www.sciencedirect.com/science/article/pii/S0212656714000067

SANTOS, J. C. (2014). Seguridad y alta disponibilidad. RA-MA Editorial. Disponible en: https://s3.amazonaws.com/academia.edu.documents/54527072/libro_seguridad.pdf?response-content-disposition=inline%3B%20filename%3DLibro_seguridad.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190723%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190723T172840Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=6880e51af43cf7f7d6c3fc66b3b123a88dea2ffeff3794eb5144084de90e47c8

SARUBBI, J. P. (2008). Seguridad informatica Tecnicas de defensa comunes bajo variantes del sistema operativo Unix. Luján,(Buenos Aires, República Argentina). Disponible en: http://tesis.blanque.com.ar/tesis/Home_files/Tesis_Pablo_Sarubbi.pdf

SKEIE, T., Johannessen, S., Løkstad, T., & Holmeide, Ø. A la misma hora. Disponible en: https://www.researchgate.net/profile/Tor_Skeie/publication/28061832_Sincronizacion_precisa_para_la_automatizacion_a_la_misma_hora_en_otro_lugar/links/544118820cf2a76a3cc79b04.pdf

SORIANO, M. (2014). Seguridad en redes y seguridad en la información. Obtenido de http://improvet. cvut. cz/project/download/C2ES/Seguridad_de_Red_e_Informacion. pdf. Disponible en: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

TEJADA, E. C. (2015). Gestión de incidentes de seguridad informática. IFCT0109. IC Editorial. Disponible en: https://books.google.es/books?hl=es&lr=&id=y63KCQAAQBAJ&oi=fnd&pg=PT4&dq=seguridad+inform%C3%A1tica+en+redes&ots=znExvdHejS&sig=5cWR7w8vG9yAaz-Tf95HcYebPlc#v=onepage&q=seguridad%20inform%C3%A1tica%20en%20redes&f=false

TENELEMA, Aguaiza, et al. Propuesta de rediseño de la infraestructura de red de la Universidad Laica" Eloy Alfaro" de Manabí, para ofrecer un modelo de servicios con calidad de servicio (QOS). 2016. Tesis de Maestría. PUCE.

TERNERO, M. R. (2003). Seguridad en redes y protocolos asociados. Recuperado de http://www.sistemamid.com/panel/uploads/biblioteca/1/619/672/673/675/4105.pdf

URBINA, G. B. (2016). Introducción a la seguridad informática. Grupo editorial PATRIA. Disponible en: https://books.google.es/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=seguridad+inform%C3%A1tica+en+redes&ots=0WQxaxxfLr&sig=B6tsvQ3R2KPj1JcWBUjRjn1HPIE#v=onepage&q=seguridad%20inform%C3%A1tica%20en%20redes&f=false

URETA, O., & Elvis, J. (2019). DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y BALANCEO DE CARGA, EN ROUTERS MIKROTIK PARA MEJORAR LA CALIDAD DE SERVICIO (QoS) DE LA EMPRESA ZONA VIP, UBICADA EN EL DISTRITO DE AMARILIS, PROVINCIA DE HUÁNUCO 2015. Disponible en. http://200.37.135.58/bitstream/handle/123456789/1616/ORTEGA%20URETA%2C%20JHON%20ELVIS.pdf?sequence=1&isAllowed=y

VÁSQUEZ FLORES, D. R. (2019). Diseño e implementación de una red wireless con el estándar IEEE 802.11 ac con calidad de servicio y seguridades para la administración del servicio de comunicación de una empresa de venta de automóviles, basado en tecnología mesh con equipos ubiquiti y mikrotik (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería En Networking y Telecomunicaciones). Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/40125/1/B-CINT-PTG-N.423%20V%C3%A1squez%20Flores%20Danny%20Rodolfo.pdf

VELÁSQUEZ, J. G. P. (2013). Protocolos de Descubrimiento de Servicio. Revista Pensamiento Americano, 4(6). https://s3.amazonaws.com/academia.edu.documents/47441713/63-59-1-PB.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1559350219&Signature=3oG1A0FNCrjvz%2BEQW3UHLf9DrQs%3D&response-content-disposition=inline%3B%20filename%3DProtocolos_de_Descubrimiento_de_Servicio.pdf

ANEXO

Link del video

https://www.youtube.com/watch?v=OMtn7rDmacQ