UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA DE CIENCIAS Y TECNOLOGÍA

CARRERA DE INGENIERÍA INFORMÁTICA

"ADMINISTRACIÓN DEL SERVICIO DE INTERNET DEL CAMPUS UNIVERSITARIO DE LA U.A.P."

TRABAJO DIRIGIDO PRESENTADO PARA OPTAR AL TITULO ACADÉMICO DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Elaborado por: Univ. Lorena Calizaya Ledezma

Tutor : Ms.C. Lic. Humberto Fernández Calle

Supervisor : Ing. Senta Soneland Valdivia Rodríguez

Cobija - Pando – Bolivia

2012

Agradecimientos.

A Dios por dame la vida para realizar mis sueños, a mis padres por su apoyo, a mi nena por estar siempre conmigo, a la familia de mi hermana Tina por su apoyo en el transcurso de mi Carrera, a mis amigos por acompañarme en los buenos y malos momentos de mi vida y a todos mis Docentes del Área de Ciencias y Tecnología, Gracias…

Dedicatoria.

A Dios por darme la vida para poder realizar mi Carrera Universitaria, a mi princesa hermosa Karla Lorena Calizaya, a mis padres y hermanos por tener la confianza en mí y a los Docentes del ACYT por haberme transmitido sus conocimientos.

RESUMEN

Internet como una red de redes, es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí, es una de las herramientas de mayor capacidad de información a distancia que ha traído consigo la tecnología mundial se ha convertido en medio idóneo para impartir conocimiento y de progreso, se ha notado el progresivo avance del uso de Internet en los hogares, empresas, instituciones que cada vez hacen un uso más sofisticado de la Red.

Uno de los aspectos más importantes en el camino hacia el éxito radica en el manejo de la información la necesidad de compartir recursos e intercambiar información, durante el proceso de informe final del Trabajo Dirigido se emprendió la investigación sobre la Administración del Servicio de Internet y la aplicabilidad en nuestro medio para la implementación del servidor MikroTik para la administración de la Red de Datos y el servicio de Internet de acuerdo al análisis que se realizo a los problemas presentados en la DRDI (División de Redes de Datos e Internet) se determina que el problema principal es la deficiente administración del servicio de Internet, para lo cual se plantea como objetivo principal Mejorar el servicio de Internet con la eficiente administración y el acceso a usuarios del Campus Universitario de la U.A.P. utilizando la metodología "Modelo Funcional Para la Administración de Redes", el cual se logra con la implementación del Servidor Mikrotik, permitiendo utilizar algunas de sus herramientas, para mejorar el servicio de Internet se trabaja con calidad de servicios QoS del MikroTik se utiliza Simples Queues, para restricción de ancho de banda por usuario, el Web Proxy para restricción de páginas web, el servicio de autenticación de usuarios a través ARP de amarre de IP/MAC para la Red LAN y HotSpot para la Wifi inalámbrica, etc.

El servicio de Internet mejoro con la administración de la Red de Datos e Internet permitiendo el control de acceso de usuarios, regulando el ancho de banda, restringiendo páginas web, monitoreo y control del uso de internet, etc.

ÍNDICE

ÍNDICE DE FIGURA

ÍNDICE DE TABLA

ÍNDICE DE GRAFICO

CAPÍTULO I

MARCO REFERENCIAL

1. INTRODUCCIÓN.

Con el avance tecnológico de la comunicación, también crece la inseguridad en la navegación a sitios web, en la actualidad el internet es muy utilizado por las grandes empresas, gobiernos, etc. Tomando en cuenta en el mundo actualmente funciona entorno a internet para lo cual se hace presente la administración de redes que es definida como la suma total de todas las políticas y procedimientos que intervienen en la planeación, configuración, control y monitoreo de los elementos que conforman una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos, lo cual se verá reflejado en la calidad de los servicios ofrecidos, incrementando la eficiencia y productividad de las personas. El uso del internet es un medio de comunicación muy importante que nos provee tecnologías de información y comunicación, que contribuye a todo campo de investigación.

El trabajo dirigido consiste en la Administración del Servicio de Internet en el Campus Universitario de la Universidad Amazónica de Pando (U.A.P.), en el cual se identifica que el problema principal está en la administración deficiente del internet, para el cual se plantea el objetivo principal de Administrar el servicio de internet para mejorar y dar acceso a usuarios del Campus Universitario de la U.A.P. utilizando la metodología "Modelo Funcional Para la Administración de Redes", especificando también los objetivos específicos, la justificación y los alcances que tendrá el trabajo en su desarrollo y ejecución.

1.1. ANTECEDENTES.

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada, que pueden ser redes de cableado físico a través de la Ethernet y redes inalámbricas como ser la Wifi, Internet es una "red de redes", es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas

telefónicas, etc.) con el objeto de compartir recursos, de esta manera, Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una "red global". Esta red global tiene la característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes participantes, este lenguaje común o protocolo (un protocolo es el lenguaje que utilizan las computadoras al compartir recursos) se conoce como TCP/IP[1].

Trabajos relacionados en el campo de estudio:

(Huaygua, 2005) Hace referencia en el trabajo de grado "Administración de la red de datos e internet (DIA)", mejorar la administración de la red de datos y el servicio de internet del predio central de la UAP.

(Zenteno, 2009) En el trabajo de grado "Servidor de Administración de ancho de banda en la Universidad Amazónica de Pando", hace referencia a la implementación de una aplicación MikroTik que permita gestionar el ancho de banda.

(Mendez, 2011) Implementación de un Servidor Proxy para la Administración de la red de datos e Internet en el Consulado del Brasil en Cobija.

Dentro la unidad de Redes de Datos e Internet del campus universitario dependiente de la USIC[2] (Unidad de Sistemas de Información y Comunicación), el servicio de internet que ofrece a la comunidad universitaria se ve afectada por los cortes frecuentes de internet por parte del proveedor y la inadecuada administración del internet en el control de acceso de usuarios, el control de rendimiento de ancho de banda, etc. Dentro la unidad se cuenta con el hardware necesario que ayudara en la administración, lo mismos fueron adquiridos en gestiones anteriores, a los cuales se realizara configuraciones requeridas para la administración de redes del servicio de internet utilizando la metodología del Modelo Funcional.

[1]Es el Protocolo de Transmisión y Comunicación y Protocolo de Internet.
[2] Unidad de Sistemas de Información y Comunicación.

Antecedente institucional.

A partir del mes de abril del año 2000 la Universidad Amazónica de Pando está conectada a la red más grande del mundo de información, desde entonces se ofrece el servicio de acceso a internet Online a toda la comunidad universitaria y población en general siendo la primera institución en prestar este servicio en la ciudad de Cobija. La U.A.P.[3] puso a disposición una Sala de Internet con cinco equipos con una velocidad de acceso de 19kbps, La demanda de conexión a internet tanto de usuarios académicos y estudiantes fue creciendo, es por eso que en septiembre de 2001 se incremento la velocidad a 32kbps y se mantuvo hasta junio del 2002, luego de las gestiones del Departamento de Red LAN e Internet se llega a incrementar a 64kbps, hasta el 2005 que nuevamente se incremento el ancho de banda a 256KB,durante el transcurso de los años y la demanda de usuarios poco a poco fue incrementado la velocidad para el internet, en el año 2007 se incremento nuevamente el ancho de banda a 1Mb de velocidad, firmándose un contrato de 2 años con la empresa proveedora Coteco, en el año 2009 se incremento a 2 Mb de velocidad y a partir de junio de 2012 actualmente se cuenta con 3 Mb de velocidad de ancho de banda para el servicio de Internet.

1.2. DESCRIPCIÓN DEL PROBLEMA.

En el Campus Universitario de la Universidad Amazónica de Pando se ofrece el Servicio de Internet[4] a la comunidad Universitaria, el cual no cuenta con una administración adecuada en el control de acceso de usuarios, la distribución y control del rendimiento del ancho de banda que eviten bajos rendimientos durante el uso del Internet, se tiene tres sub redes de distribución de internet dentro del campus universitario las cuales son la sub red de la Sala de Internet de conexión por cableado físico, la sub red de la Red Local de conexión por cableado físico e inalámbrico, cuenta con tres puntos de acceso Wifi

[3] Universidad Amazónica de Pando.
[4] Es un conjunto descentralizado de redes de comunicación interconectadas que utiliza la familia TCP/IP.

a internet que son (Vice_uap, Netgear, Postgrado) y la subred de la Wifi U.A.P. de conexión inalámbrica.

Las causas identificadas en el servicio de Internet que ofrece a la comunidad universitaria son:

- ✓ Administración inadecuada del servicio de Internet.
- ✓ Control deficiente en el acceso y permiso de usuarios.
- ✓ Control deficiente del rendimiento del ancho de banda.
- ✓ Navegación lenta en Internet.
- ✓ Congestionamiento y tráfico de la información.
- ✓ Falta de monitoreo del ancho de banda a nivel de usuarios.
- ✓ Cortes frecuentes del Internet por parte del proveedor.
- ✓ Incremento de demanda por usuarios.
- ✓ Incremento de puntos de acceso a Internet.
- ✓ Parches de red de datos no optimo para el envió de información.
- ✓ Acceso a internet por cableado e inalámbrico (Wifi).
- ✓ Velocidad Insuficiente del ancho de banda para la demanda de usuarios.

Estas causas mencionadas anteriormente provocan cuantiosos efectos como ser:

- ✓ El indiscriminado uso del servicio de Internet.
- ✓ Acceso de usuarios a Internet por cableado físico e inalámbrico como ser las Zonas Wifi.
- ✓ Acceso de usuarios no registrados y no permitidos a Internet.
- ✓ Saturación constante del ancho de banda.
- ✓ Degradaciones en el rendimiento del ancho de banda.
- ✓ Tiempos no autorizados en Internet.
- ✓ Insatisfacción del servicio por parte de los usuarios.
- ✓ Descargas de datos no académicos para el Universitario (Música, juegos, Fotos, etc.).

Debido a los problemas descritos se plantea el siguiente problema principal.

"Deficiencia en la Administración del Servicio de Internet del Campus Universitario de la U.A.P."

Lo anterior lleva a lo siguiente: configurar servidores en el RouterBoard Mikrotik, para mejorar la administración del Servicio de Internet, realizando el control de acceso de usuarios, restricción de usuarios no permitidos, control del ancho de banda, etc. Que eviten inconvenientes problemas que se da durante el uso de Internet.

1.3. OBJETIVOS.

1.3.1. Objetivo general.

Mejorar el servicio de Internet con la eficiente administración y el acceso a usuarios del Campus Universitario de la U.A.P. utilizando la metodología "Modelo Funcional Para la Administración de Redes"

1.3.2. Objetivos específicos.

Los objetivos específicos que nos llevaran a alcanzar el objetivo general son:

- ✓ Diagnosticar el funcionamiento del uso de Internet en el Campus Universitario para mejorar el servicio en los usuarios.
- ✓ Administrar usuarios para dar acceso a internet dentro el Campus Universitario a través de procesos y procedimientos.
- ✓ Controlar y restringir sitios Web, Monitorear el uso de ancho de banda y acceso a Internet por niveles de usuarios.

1.4. JUSTIFICACIÓN.

La Unidad de Redes de Datos e Internet que proporciona el servicio de Internet a la Universidad Amazónica de Pando, requiere de un área especializada que concentre sus esfuerzos en la administración eficiente de la misma, porque la distribución del Internet dentro del Campus Universitario se da por conexiones de tipo inalámbrico y

cableado físico. Esta Unidad que integra los servicios de Redes e Internet, deberá operar en un esquema de 24/365 (horas por días al año), ya que se proporciona como herramientas de apoyo a las actividades docentes, investigación, administrativa y comunidad universitaria en general.

La administración de Redes en la Unidad es muy importante para mantener una red óptima, para el envió y recepción de la información y distribución de Internet a los usuarios, el cual este constantemente monitoreado, ya que se tiene diferentes puntos de acceso por conexión inalámbrica que son las Zonas Wifi del Campus, y conexiones por cableado físico, la conexión de cableado físico fue diseña anteriormente e implementada como una red pequeña, que con el crecimiento de la Universidad y el incremento de demanda por los usuarios, fue añadiendo a la red mas redes de comunicación de datos (los llamados parches de red) una solución rápida que se da no planificada la cual no es muy optima, es por ello que se requiere de una administración adecuada de redes, para mejorar el acceso a Internet utilizando herramientas propias del RouterOS Mikrotik (HopSpot, Web Proxy, Dhcp, etc.) y otros software de monitoreo de red como: The Dude, Radmin, Cain, etc. que nos ayuden en la administración para brindar un buen servicio en beneficio de la comunidad Universitaria en su conjunto.

Dentro del campus universitario se cuenta con 230 PC entre portátiles y de escritorio que forman parte laboral de las distintas funciones que se desempeña en cada Dirección, beneficiando con la administración del Internet a una cantidad variable de usuarios que dependa del ancho de banda, como ser: Directores, Consultores, administrativos, Universitarios y a toda la comunidad universitaria su conjunto.

1.5. METODOLOGÍA.

La metodología empleada en trabajo dirigido es el “Modelo Funcional para la Administración de Redes”, esta metodología es recomendable en trabajos dirigidos puesto que es un es un cargo en base a funciones.

Esta metodología contiene cinco procesos que son los siguientes: (configuración, fallas, rendimiento, contabilidad y seguridad) cada proceso tiene sus propias actividades. En base al trabajo dirigido se considera cuatro de los cinco procesos de la metodología que

ayudaran a alcanzar la solución al problema y la administración del servicio de Internet las cuales son: (configuración, fallas, rendimiento y seguridad) cada actividad de la metodología tiene por objetivo relacionar con los objetivos específicos.

1.6. ALCANCES.

De acuerdo al ámbito geográfico, el alcance del trabajo dirigido contempla el Campus Universitario de la Universidad Amazónica de Pando y sus diferentes infraestructuras que se benefician del servicio de Internet, que cuenta con una velocidad de 3Mb de ancho de banda, existe tres subredes de distribución y acceso a Internet, por conexiones de cableado físico e inalámbrico, las cuales son la Subred de la Sala de Internet de conexión por cableado físico, la subred de la Red Local de conexión por cableado físico e inalámbrico, cuenta con tres puntos de acceso inalámbrico a Internet que son (Vice_uap, Netgear, Postgrado).

Los alcances que se pretende lograr con el presente trabajo son:

- ✓ Diagnostico total del servicio de Internet, la configuración del Servidor HotSpot para la autorización y acceso de usuarios al Internet, del Servidor Web Proxy para la restricción y control de accesos a sitios web y la administración de altas, bajas y modificaciones de usuario a través de procedimientos y el control de ancho de banda por usuario.
- ✓ Control y monitoreo de la velocidad, servicio y uso de Internet.
- ✓ Asistencia técnica a usuarios a través de entrevistas y sugerencias.
- ✓ Seguridad al servidor y elaboración de políticas para la administración del servicio de Internet.

1.7. ORGANIZACIÓN DEL DOCUMENTO.

Capítulo I: Es la etapa donde se establece la parte introductoria del Trabajo Dirigido donde se describe la introducción, el problema, los objetivos planteados, la metodología utilizada y alcances.

Capítulo II: Hace referencia a los fundamentos teóricos y conceptuales del tema, la metodología, herramientas y técnicas aplicadas en el desarrollo del presente Trabajo Dirigido.

Capítulo III: En este capítulo se realiza la ejecución del proyecto en base a la metodología, sus etapas y actividades como ser el análisis previo, planeación del diseño de implementación, configuración, monitoreo y administración del servicio de Internet.

Capítulo IV: este capítulo refleja las conclusiones obtenidas del proyecto de trabajo dirigido, en base a los objetivos, alcances y las recomendaciones para mejorar o ampliar este servicio dentro de la institución.

CAPÍTULO II

MARCO TEÓRICO

En este capítulo tiene por finalidad mostrar el sustento teórico que fundamenta el Trabajo Dirigido para ello se describe algunos conceptos de la administración de redes, gestión de calidad, conceptos de herramientas de MikroTik, políticas, etc.

2.1. ADMINISTRACIÓN DE REDES.

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada. (Prudencio Nieves, 2012)

Sus principales objetivos de la administración de redes son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de red opera bajo los siguientes pasos básicos:

1.- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.

2.- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.

3.- Transportación de la información del equipo monitoreado al centro de control.

4.- Almacenamiento de los datos coleccionados en el centro de control.

5.- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.

6.- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de la administración de redes moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.

2.2. GESTIÓN DE CALIDAD.

Un Sistema de Gestión de la Calidad es una serie de actividades coordinadas que se llevan a cabo sobre un conjunto de elementos (Recursos, Procedimientos, Documentos, Estructura organizacional y Estrategias) para lograr la calidad de los productos o servicios que se ofrecen al cliente, es decir, planear, controlar y mejorar aquellos elementos de una organización que influyen en satisfacción del cliente y en el logro de los resultados deseados por la organización.

Una organización debe de tomar en cuenta la siguiente estructura:

- **Estrategias:** Definir políticas, objetivos y lineamientos para el logro de la calidad y satisfacción del cliente. Estas políticas y objetivos deben de estar alineados a los resultados que la organización desee obtener.
- **Procesos:** Se deben de determinar, analizar e implementar los procesos, actividades y procedimientos requeridos para la realización del producto o servicio, y a su vez, que se encuentren alineados al logro de los objetivos planteados. También se deben definir las actividades de seguimiento y control para la operación eficaz de los procesos.
- **Recursos:** Definir asignaciones claras del personal, Equipo y/o maquinarias necesarias para la producción o prestación del servicio, el ambiente de trabajo y el recurso financiero necesario para apoyar las actividades de la calidad.

- **Estructura Organizacional:** Definir y establecer una estructura de responsabilidades, autoridades y de flujo de la comunicación dentro de la organización.
- **Documentos:** Establecer los procedimientos documentos, formularios, registros y cualquier otra documentación para la operación eficaz y eficiente de los procesos y por ende de la organización.

También existen varias normativas estandarizadas que establecen requisitos para la implementación de un Sistema de Gestión de la Calidad, y que son emitidas por organismos normalizadores como la ISO, DIS, entre otros. Ejemplos de estas normativas están:

- **ISO 9001** - Requisitos para un Sistema de Gestión de la Calidad (Aplicable a cualquier organización, sin importar tamaño o sector).

2.2.1. Procesos y procedimientos.

Un proceso efectivamente es un conjunto de actividades interrelacionadas que convierten entradas en salidas, generalmente una salida es la entrada de otro proceso, la norma ISO 9001 utiliza este enfoque para poder gestionar de una manera fácil una organización y de esta forma saber cómo se interrelacionan las partes constituyentes de una organización.

Un procedimiento es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias.

Donde el Proceso es la actividad que transforma entradas en salidas y el procedimiento es la forma de describir cómo se lleva a cabo una serie de actividades que puede ser todo un proceso o sólo parte de él.

2.2.2. Políticas.

Son normas y procedimientos que sirven para orientar la acción criterios o lineamientos generales a observar en la toma de decisiones, sobre problemas que se repiten una y otra vez en el ambiente de una organización. (Torrico, 2011)

Son los documentos que describen principalmente la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos tanto de los usuarios y administradores, describe lo que se va a proteger y de lo que se está tratando de proteger.

a) Etapas de desarrollo de una política.

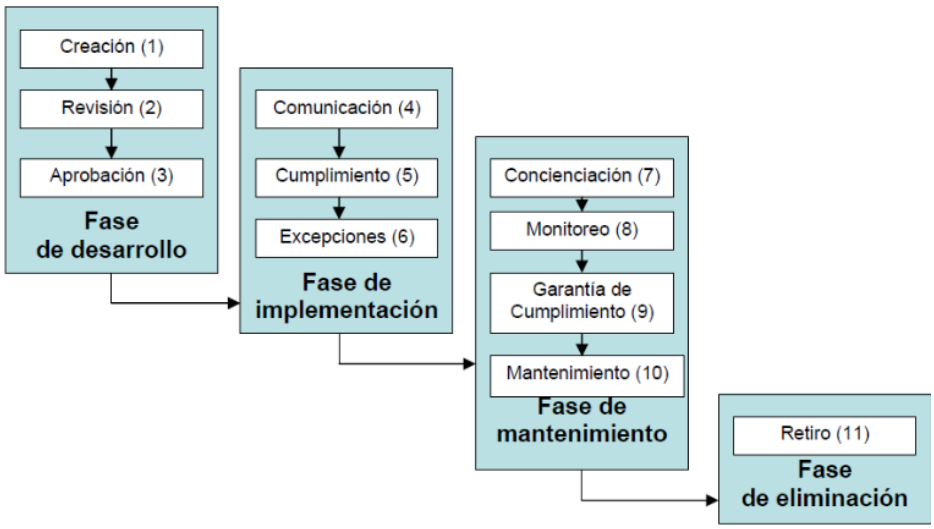


Figura 2.1: Etapas para el desarrollo de una Política.

Fuente: Guía de Elaboración de Políticas de Seguridad 2003.

- **Fase de desarrollo:** durante esta fase la política es creada, revisada y aprobada.
- **Fase de implementación:** en esta fase la política es comunicada y acatada.
- **Fase de mantenimiento:** los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se debe actualizar.
- **Fase de eliminación:** la política se retira si deja de ser útil para la organización.

Para garantizar que todas las etapas del ciclo sean realizadas de manera apropiada y las responsabilidades para la ejecución sean asignadas adecuadamente, la universidad debe establecer un marco de referencia para facilitar el entendimiento, promover la aplicación consistente, establecer una estructura jerárquica para soportar

mutuamente los distintos niveles de políticas y acomodar efectivamente los frecuentes cambios tecnológicos y organizacionales.

2.3. REDES E INTERNET.

2.3.1. Internet.

Es un conjunto descentralizado de redes de comunicación interconectadas que utiliza la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que componen funcionen como una red lógica única, de enlace mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera computadora conocida como ARPANET, entre tres universidades en california y una en Utah, Estados Unidos. (Ramos, 2011)

Uno de los servicios que más éxito ha tenido en Internet ha sido el World Wide Web (WWW, o la Web), hasta tal punto que es habitual la confusión entre ambos términos. La WWW[5] es un conjunto de protocolos que permite, de forma sencilla la consulta remota de archivos de hipertexto. Esta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Existen por tanto mucho otros servicios y protocolos en Internet, aparte de la Web: el envió de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia –telefonía (VoIP), televisión (IPTV), los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

2.3.2. Wifi e Internet.

La Wifi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wifi, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica.

---

[5]World Wide Web Uno de los servicios que más éxito ha tenido en Internet

Compartir Internet en una red Wireless es más fácil que en las redes de cables gracias al hecho de que no es necesario ver la disposición de estos en la estructura que tengamos. En muchas ciudades del mundo ya está disponible la implementación de la tecnología Wireless. Este el caso de lugares públicos que ofrecen acceso a Internet en forma inalámbrica, como avenidas, estaciones de servicios y aeropuertos donde podemos acceder a la red de redes mediante una PDA o Notebook.

2.3.3. Redes inalámbricas.

Las redes inalámbricas son aquellas que carecen de cables, esta tecnología facilita en primer lugar el acceso a recursos en lugares donde se imposibilita la utilización de cables, como zonas rurales poco accesibles, además estas redes pueden ampliar una ya existente y facilitar el acceso a usuarios que se encuentren en un lugar remoto, sin la necesidad de conectar sus computadoras a un **hub** o a un **Switch** por intermedio de cables.

2.3.4. Seguridad en Redes.

En redes de computadoras, como en otros sistemas, su propósito es de reducir riesgos a un nivel aceptable, con medidas apropiadas. La seguridad comprende los tópicos siguientes:

- **Identificación:**(ID) es la habilidad de saber quién es el usuario que solicita hacer uso del servicio.
- **Autentificación:** Es la habilidad de probar que alguien es quien dice ser; prueba de identidad. Por ejemplo un password secreto que solo el usuario debe conocer.
- **Control de Acceso:** una vez que se sabe y se puede probar que un usuario es quien es, es sistema decide lo que le permite hacer.
- **Confidencialidad:** Es la protección de la información por la que garantiza que esta accesible únicamente a personal autorizado, para que no pueda ser vista ni entendida por personal no autorizado.
- **Integridad:** Es la cualidad que asegura que el mensaje es seguro, que no ha sido alterado. La integridad provee la detección del uso no autorizado de la información y de la red.

- **No repudiación:** La no repudiación es la prevención de la negación de que un mensaje ha sido enviado o recibido y asegura que él enviador del mensaje no pueda negar que lo envió o que el receptor niegue haberlo recibido. La propiedad de no repudiación de un sistema de seguridad de redes de cómputo se basa en el uso de firmas digitales.

2.4. ROUTEROS MIKROTIK.

Mikrotik RouterOS es un sistema operativo basado en Linux que permite a los usuarios convertir un ordenador personal PC en un router, con funcionalidades como Gestor de ancho de banda, QoS, punto de acceso inalámbrico, firewall, VPN Server y Cliente y otras características comúnmente utilizado para el enrutamiento y la conexión de redes.

El sistema RouterOS fue creado por dos estudiantes de Latvia país ex integrante de Unión soviética como tesis universitaria para diseñar un Routers basado en Linux que permita equiparar las funcionalidades de otros Router que se encontraban en el mercado. Con el pasar del tiempo se han integrado otras funciones dentro del sistema como: soluciones de telefónica IP, administración de protocolo BGP, integración de Ipv6, servidor de VPN's, administración de ancho de banda, calidad de servicios QoS, administración de HotSpot, puntos de acceso inalámbrico, backhaul inalámbrico, etc.

A partir del año 2002 se enfocaron en la creación del hardware que permita simplificar su operación, creando el RouterBoard 230, luego desarrollaron una amplia gama de RouterBoard RB, como: RB500, RB100, RB300, RB600, RB400, y RB1000 las cuales difieren entre si las características como: la velocidad del procesador, el número de puertos Ethernet, el número de Slot Mini-PCI, capacidad de memoria, capacidad de almacenamiento de datos, nivel de licencia, etc.

Mikrotik es actualmente considerada como una de las grande s empresas de Networking, compitiendo con las grandes fábricas como: Cisco, Juniper, 3Com, o D-Link, etc., entre sus clientes y casos de éxito se puede nombrar a: SIEMENS, IPASS, HP,

ERICCSON, Mitshubishi, RIPE, El departamento de Estado de los Estados Unidos de América, Motorola, Vodafone, FBI y la NASA.

2.4.1. Características principales de RouterOS.

RouterOS es Basado en el Kernel 2.6 de Linux, soporta multi-core (varios núcleos), y computadores multi-CPU (SMP-SymmetricMultiprocessing), la instalación y ejecución pueden ser desde discos IDE, HDDs, CF, memorias USB, SSB disk. Soporta varios métodos acceso a configuración: acceso local, con teclado y monitor por consola mediante puerto serial, Telnet, secure SSH, interface WEB, además de una interfaz GUI (Grapicaluser interface) propia llamada winbox; también soportauna conexión a nivel de MAC address llamada mac-Telnet.

2.4.2. Calidad de servicios QoS.

- Tipo de colas: RED (Randon Early Detection), BFIFO (Byte Limited First In, First Out queue), PFIFO (Packet Limited First In, First Out queue), PCQ (Packet Classification and Queuing).
- Colas simples: por origen/destino de red, dirección IP de cliente, por interface.
- Arboles de colas: por protocolo por puerto, por tipo de conexión.

2.4.3. Protocolo de Configuración de Host Dinámico (DHCP).

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

2.4.4. Firewall.

El Firewall implementa filtrado de paquetes que es usado para administrar el flujo de datos, desde y a través del router. Junto con el NAT (Network Address Translation) previene el acceso no autorizado a redes internas, autorizando solo el tráfico de salida, es

decir el tráfico generado desde la red interna hacia el Internet, por ejemplo HTPP (Hypertex Transfer Protocol) o envió de correo electrónico.

RouterOS permite crear un firewall Statefull lo que significa que realiza una inspección de estado de paquetes y realiza un seguimiento de estado de conexiones de estado de conexiones que pasan a través de él. También soporta Source and Destination NAT (Network Address Translation). El firewall provee características para hacer uso de conexiones internas, ruteando y marcando paquetes, permite detectar ataques por denegación de servicio (DoS).

El filtrado de paquetes puede ser por direcciones IP, rango de direcciones IP, por puerto, rango de puerto, protocolo IP, DSCP (differentiatedServicesCode Point) y otros parámetros. Soporta también direccionamiento IP estático y dinámico, además de implementar características de capa 7 (layer 7).

2.4.5. Wireless.

RouterOS soporta una variedad de tecnologías inalámbricas, puede trabajar con diferentes configuraciones para diferentes aplicaciones por ejemplo: Backhaul para enlaces de punto a punto, Access Point para enlaces de mutipuntos, HotSpot.

Soporta estándares IEEE802.11a/b/g/n, con modulaciones; OFDM (Orthogonalfrequency-divisionmultiplexing), BPSK (BinaryPhaseShiftkeying), QPSK (QuadraturePhaseShiftkeying), 16 QAM (Quadrature Amplitud Modulation), 64 QAM, DSSS (DirectSequence Spread Spectrum), DBPSK (DifferentialBinaryPhaseShiftKeying), DQPSK (DifferentialQuadraturePhaseShiftKeying), CCK (ComplementaryCodeKeying).Maneja protocolos propietarios: Nstreme, protocolo que permite extender el rango de coberturay velocidad de los radios y Nstream2 (dual) utiliza dos tarjetas de radiouna para transmisión y otra para recepción con la cual se pueda duplicar la transmisiony otra para recepción con la cual se pueda duplicar la capacidad de ancho de banda.

Mediante el uso de radios que soportan estándar 802.11n, RouterOS tiene la capacidad de implementar la reciente tecnología MIMO (Multiple-input, Multiple-output),

que permite mediante diversidad de antenas (dos antenas simultaneas en diferentes frecuencias) incrementar el ancho de banda hasta una velocidad teorica de 600Mbps. Puede administrar redes Wireless MESH (malla) y HWMP (Hybrid Wireless MeshProtocol)para incrementar zonas de cobertura de red inalámbrica.

Soporta RTS/CTS (RequesttoSend/Clear toSend) para disminuir las colisiones, WDS (Wireless DistributionSystem), para extender una red multipunto con varios puntos de acceso (AP`s) con un mismo SSID (Service set identifier) conservando las mismas direcciones MAC (Media Access Control) en los clientes.

Implementa seguridad WEP (WredEquivalentPrivacy), WAP (Wireless AplicattionProtocol), WPA2 (802.11i), además incorpora una lista de control de acceso de clientes mediante filtrado de direcciones MAC con seguridad mediante un algoritmo de 104bits con WEP, permite la creación de puntos de acceso virtuales utilizando las mismas características de frecuencia que el AP primario.

2.4.6. Control de Ancho de Banda.

El control de ancho de banda es un mecanismo que controla la asignación de la velocidad de los datos, tiempo de retraso, entrega oportuna de paquetes, confiabilidad en la entrega, es decir prioriza y da forma al tráfico de red.

Algunas características de RouterOS para el control de tráfico son las siguientes.

- Limitación de tráfico por direcciones IP, subredes por protocolo, por puerto y otros parámetros.
- Limitación de trafico peer to peer.
- Priorización de determinados flujos de paquetes sobre otros.
- Uso de trafico de colas para mayor rapidez de navegación.
- Aplicación de colas en intervalos de tiempos fijos.
- Manejo dinámico de cantidad de tráfico dependiendo de la carga del canal.

- RouterOS soporta HierarchicalTockenBukent (HTB), es un tipo de sistema jerárquico de servicio con CIR (CommittedInformationRate) y MIR (MaximunInformationRate), ráfagas de datos y prioridad.

2.4.7. Servidor/Cliente.

RouterOS incorpora varios servicios como servidor o cliente:

- DHCP (Dynamic Host Configuration Protocol): usado para la asignacion dinamica de direcciones IP.
- Tuneles tipo PPPoE (Point to Point Protocol over Ethernet) utilizado para acceso DSL encapsulando tramas PPP dentro de trmas Ethernet.
- Tuneles PPPTP (Point to Point Tunneling Protocol): permite la transmision de datos clilente-servidor sobre la plataforma TCP/IP.
- Relay de DHCP (Dinamic Host Configuration Protocol): utilizado para administrar reenvios de solicitudes de asignacion Ipde un cliente DHCP hacia un servidor DHCP.
- Cache Web-proxy: utilizado para el almacenamiento temporal de archivos rrecurentes.
- Gateway de HotSpot Provee Autenticacion, autorizacion y seguridad para el uso de una red inalambrica de acceso publico.
- VPN (Virtual Private Netword) server, permite establecer conexiones seguras sobre redes abiertas (sin seguridad), ó Internet.

2.4.8. Licenciamiento.

RouterOS para ser activado requiere de una licencia de nivel de aplicaciones, es decir existen varias licencias con limitaciones o caracteristicas adicionales dependiendo del tipo de aplicación de red que se requiera.

Las licencias de nivel 0 es un licencia demo, habilita todas sus funciones durante un periodo de 24 hors. La licencia de nivel 2 fue una licencia de trnsicion e investigacion, por lo que no se encuentran disponible. La licencia de nivel 3 fue una

licencia que opera con caracteristicas limitadas y permitia el uso de interfaces inalambricas solo para trabajar en modo cliente.

La principal diferencia entre las licencias de nivel 4,5 y 6 son la cantidad de tuneles permitidos por nivel, a continuacion se muestra una tabla con los niveles y caracteristicas.

NIVEL (Características)	0 (Gratis)	1 (DEMO)	3(WISP CPE)	4(WISP)	5(WISP)	6(Servidor Control)
PPPoE túneles	24h limite	1	200	200	500	Ilimitados
PPTP túneles	24h limite	1	200	200	500	Ilimitados
L2TP túneles	24h limite	1	200	200	500	Ilimitados
HotSpot Usuarios Activos	24h limite	1	1	200	500	Ilimitados
Sesiones Activas de Administración	24h limite	1	10	20	50	Ilimitados
EoIPtúneles	24h limite	1	Ilimitados	Ilimitados	Ilimitados	Ilimitados
OVPN túneles	24h limite	1	200	200	Ilimitados	Ilimitados
VLAN Interfaces	24h limite	1	ilimitados	Ilimitados	Ilimitados	Ilimitados
Colas QoS	24h limite	1	ilimitados	Ilimitados	Ilimitados	Ilimitados
Wireless AP	24h limite	-	-	Si	Si	Si
Wireless Client y Brydge	24h limite	-	Si	Si	Si	Si
RIP, OSPF, BGP protocolo	24h limite	-	Si	Si	Si	Si
RADIUS client	24h limite	-	Si	Si	Si	Si
Web Proxy	24h limite	-	si	Si	Si	Si
Sincrónicas Interfaces	24h limite	-	-	Si	Si	Si
Actualizable	-	No	ROS v4.x	ROS v4.x	ROS v5.x	ROS v5.x
Soporte Online	-	-	-	15dias	30dias	30dias

Tabla 2. 1: Licenciamiento RoterOS.

Fuente: Elaboracion propia.

2.4.9. Servidor Proxy Web.

La instalación de un servidor proxy de cache web en una red beneficia a la organización en muchos sentidos. En primer lugar los usuarios acceden a las páginas web con mayor rapidez, en segundo lugar el incremento del tamaño y del coste de la conexión a

Internet se reduce o cuando menos controla. El servidor proxy mantiene la conexión a Internet a un nivel y según un criterio constante. Sin servidor proxy los usuarios saturarían la conexión en determinados momentos del día, lo que impondría un incremento de la capacidad.

"El servidor proxy es muy tenaz y paciente. Puede examinar y almacenar miles de páginas web, y cuando un usuario local de la LAN reclama una página especifica almacenada, la página en cuestión sale volando de la unidad local o cache sin retardos en la transmisión Internet. El servidor proxy utiliza de manera eficiente la conexión Internet, lo que implica un ahorro considerable si se comparte la conexión entre varios usuarios aprovechándola al máximo. Aunque un servidor proxy no dispone la avanzada flexibilidad de un cortafuegos especializado, constituye una barrera impermeable entre la red y el exterior". (Derfler , 1998, pág. 242)

2.4.10. HotSpot.

Un HotSpot, traducido del inglés al español como "punto caliente", corresponde a un punto, generalmente ubicado en un lugar público, donde las personas pueden acceder a Internet en forma gratuita, a través del sistema de Internet inalámbrico denominado Wi-Fi.

Los HotSpot, como ya se mencionaba, por lo general, se ubican en lugares públicos, específicamente en bibliotecas, aeropuertos, cafeterías, hoteles, etc. y se configuran como zonas de cobertura Wi-Fi en el que uno o varios puntos de acceso puedan conectarse a Internet y disfrutar de los beneficios de la navegación en la World Wide Web a través de la autenticación de usuarios.

2.4.11. Ingreso a RouterOS.

Una vez realizada la instalación RouterOS este puede ser configurado mediante la interface CLI (Interface de Línea de Comandos), también se puede acceder mediante telnet (capa3), SSH, interface web (Webbox), mediante puerto serial, MAC – Telnet usado solamente por equipos con RouterOS en (capa 2) y por una interface propietaria Mikrotik llamada WINBOX.

Winbox es una herramienta que ejecuta telnet hacia el equipo a configurar, pero presenta la interface gráfica, lo que hace más cómoda e intuitiva la configuración del equipo.

Para el ingreso mediante Winbox se puede usar el IP del equipo asociado; para esto el equipo debe estar configurado dentro de la misma red IP o existir rutas hacia este equipo, caso contrario se puede usar el MAC Address del equipo para ingresar directamente por MAC – Telnet. Si no se conoce la dirección IP del equipo se puede hacer click en (…), esto hara que el Winbox busque el MAC Address del equipo instalado y ejecutando RouterOS.

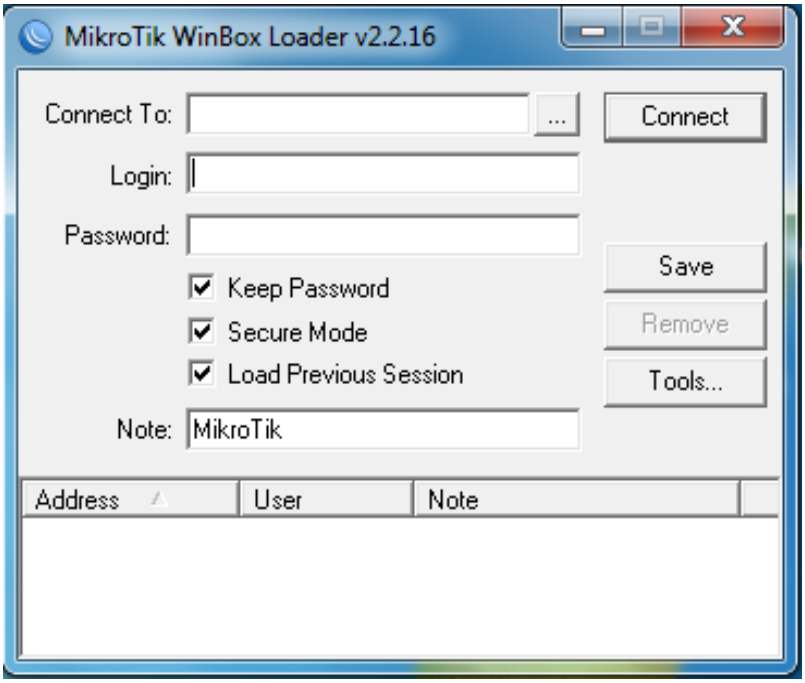


Figura 2.2: Pantalla de ingreso a Winbox.

Fuente: Elaboración propia.

2.5. METODOLOGÍAS PARA ADMINISTRAR REDES.

Se describe una metodología de redes de datos basada en modelos funcionales estándar de la ITU y de la ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes. (Untiveros, 2004)

2.6. Administración de redes.

El término **administración de redes** es definido como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

Tres dimensiones de la administración de redes.

a) Dimensión Funcional. Se refiere a la asignación de tareas de administración por medio de áreas funcionales.

b) **Dimensión Temporal.** Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.

c) **Dimensión del escenario.** Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

2.5.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN.

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

2.5.1.1 Planeación y diseño de la red.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación. El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

a) Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológico de una red pueden ser

- Multicast,
- Voz sobre IP (VoIP),
- Calidad de servicio (QoS), etc.

Algunas necesidades cuantitativas pueden ser

- Cantidad de nodos en un edificio
- Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la implementación de nuevas tecnologías de red como el cambiar de ATM a GigabitEthernet, o cambiar los protocolos de ruteo interno.

b) Diseñar la topología de la red

c) Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.

d) Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.

e) Si el diseño y equipo propuesto satisfacen la necesidades, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

2.5.1.2. Selección de la infraestructura de red.

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta.

Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo más recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

2.5.1.3. Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

a) Instalaciones de hardware

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

- Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- Notificar anticipadamente a los usuarios sobre algún cambio en la red.
- Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
- Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.
- Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.
- Documentar el cambio para futuras referencias.

b) Administración del software.

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.

Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requiere especial cuidado.

Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de tftp.

2.1.4. Provisión

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

- Algunos elementos de hardware más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

2.1.5. Políticas y procedimientos relacionados

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

2.5.2. ADMINISTRACIÓN DEL RENDIMIENTO.

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

2.5.2.1. Monitoreo.

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) Utilización de enlaces

Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.

b) Caracterización de tráfico.

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) Porcentaje de transmisión y recepción de información.

Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) Utilización de procesamiento

Es importante conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

2.5.2.2 Análisis.

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

a) *Utilización elevada.*

Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

b) *Tráfico inusual.*

El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

c) *Elementos principales de la red.*

Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia.

Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

d) *Calidad de servicio.*

Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

e) Control de tráfico.

El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

2.5.2.3 Interacción con otras áreas.

La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

2.5.3. ADMINISTRACIÓN DE FALLAS.

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases.

- *Monitoreo de alarmas.* Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
- *Localización de fallas.* Determinar el origen de una falla.
- *Pruebas de diagnóstico.* Diseñar y realizar pruebas que apoyen la localización de una falla.
- *Corrección de fallas.* Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- *Administración de reportes.* Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

2.5.3.1. Monitoreo de alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red.

También conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red.

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla.

Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

a) Tipo de las alarmas

- *Alarmas en las comunicaciones.* Son las asociadas con el transporte de la información, como las pérdidas de señal.

Alarmas de procesos. Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.

- *Alarmas de equipos.* Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.
- *Alarmas ambientales.* Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.
- *Alarmas en el servicio.* Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

b) Severidad de las alarmas.

- *Crítica.* Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.
- *Mayor.* Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- *Menor.* Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor.

Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.

- *Indefinida.* Cuando el nivel de severidad no ha sido determinado por alguna razón.

2.3.2. Localización de fallas.

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

c) Pruebas de diagnóstico

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

- *Pruebas de conectividad física.*

Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

- *Pruebas de conectividad lógica.*

Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

- *Pruebas de medición.*

Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

2.3.3. Corrección de fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.

- *Reemplazo de recursos dañados. Hay equipos de red* que permiten cambiar módulos en lugar de cambiarlo totalmente.

- *Aislamiento del problema.* Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- *Redundancia.* Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- *Recarga del sistema.* Muchos sistemas se estabilizan si son reiniciados.
- *Instalación de software.* Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- *Cambios en la configuración.* También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

2.3.4. Administración de reportes.

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T.

d) Creación de reportes.

Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte debe contener al menos la siguiente información:

- El nombre de la persona que reportó el problema
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema.
- Comentarios acerca de la problemática.
- Fecha y hora del reporte

e) Seguimiento a reportes.

La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc, y ésta debe poder ser consultada en cualquier momento por el administrador.

f) Manejo de reportes.

El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

g) Finalización de reportes.

Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

2.5.4. ADMINISTRACIÓN DE LA CONTABILIDAD.

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP.

2.5.5. ADMINISTRACIÓN DE LA SEGURIDAD.

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

2.5.5.1. Prevención de ataques.

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de

control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

2.5.5.2. Detección de intrusos.

El objetivo es detectar el momento en que un ataque se está llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

2.5.5.3. Respuesta a incidentes.

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

2.5.5.4. Políticas de Seguridad.

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.
Entre otras, algunas políticas necesarias son:

- Políticas de uso aceptable
- Políticas de cuentas de usuario
- Políticas de configuración de ruteadores
- Políticas de listas de acceso
- Políticas de acceso remoto.
- Políticas de contraseñas.
- Políticas de respaldos.

2.5.5.5. Servicios de seguridad

Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de *mecanismos de seguridad.* Identifica el "*que".*

De acuerdo a la Arquitectura de Seguridad OSI, un *servicio de seguridad* es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de las políticas de seguridad.

2.5.5.6. Mecanismos de seguridad.

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso, cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure shell o IPSec; Mecanismos de integridad como MD5, entre otras.

Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

2.5.5.7. Proceso.

Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones:

- Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.
- Definir, de acuerdo a las políticas de seguridad, los servicios de necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.
- Implementar las políticas de seguridad mediante los mecanismos adecuados.

CAPÍTULO III

MARCO APLICATIVO

Para llevar a cabo la implementación de la administración de redes de datos y la distribución del servicio de Internet, se realizo haciendo seguimiento a la Metodología Funcional para la Administración de Redes, la cual se describe detalladamente en el marco metodológico, para el análisis implementaciones se utilizo las herramientas como registro de usuarios, encuestas sobre el servicio de Internet, observación y el diseño lógico de la red de datos del Campus Universitario de la U.A.P.

3.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN.

A continuación se describen las actividades realizadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

3.1.1. Planeación y diseño de la red.

Como parte de la planificación se vio la necesidad de contar con información inicial del estado en el que se encontraba la Red de Datos y el servicio de Internet, para la obtención de la información se realizó el análisis a través de un diagnóstico, ya que por el aumento de personal, equipos y peticiones de conexión a Internet, también creció la dificultad para esquematizar la red LAN actual, la cual en su diseño inicial no contempló el crecimiento del personal y las peticiones de red, utilizando la metodología funcional para la administración de redes, también el registro físico de usuarios para así poder hacer el estudio de uso de Internet con los datos adquiridos describir el funcionamiento de la red y la descripción de cada usuario del servicio de Internet.

Las actividades relacionadas en la planificación para la administración del Internet son:

3.1.1.1. Diagnóstico de la Red de Datos.

El servicio de análisis y diagnóstico de redes permite encontrar deficiencias en la red de datos y sus causas, u oportunidades de mejora, y formular acciones correctivas y

de mejoramiento. Este servicio se complementa con el de optimización de la red, en donde se implementan estas acciones mediante un plan acordado con el cliente.

3.1.1.2. Diagnóstico del uso de Internet actual.

El diagnostico del uso del servicio de Internet sirvió para apreciar la situación en la que se encontraba la conexión a Internet y por ende la red de datos, toda la información que fue adquirida de los usuarios fue concerniente a el uso del servicio de Internet que ofrece la universidad a sus administrativos, consultores y demás profesionales que prestan su servicio en la U.A.P.

Se realizó el levantamiento de registro de datos físico de usuarios y se aplicó encuesta para diagnosticar el uso actual del Internet, fueron registrados y encuestados los usuarios que gozan del servicio de Internet, para así poder tener un diagnostico actual de las problemáticas e inquietudes de cada usuario que tiene acceso a Internet. El diagnostico total del uso de Internet ayudo a detectar un conjunto de problemas los cuales surgen como una necesidad por parte de los usuarios, para lo cual se decidió tener dos tipos de usuarios de Internet: usuarios con privilegios y usuarios sin privilegios, donde los que gozan del servicio con privilegio son los directores y jefes de unidad y los que gozan del servicio de Internet sin privilegios son todos aquellos demás usuarios que se tiene con acceso a Internet.

A continuación se muestra en la figura 3.1, en la cual se evidencia el estado de conexión a Internet al hacer un ping a www.google.com existe retardación y pérdidas de información.

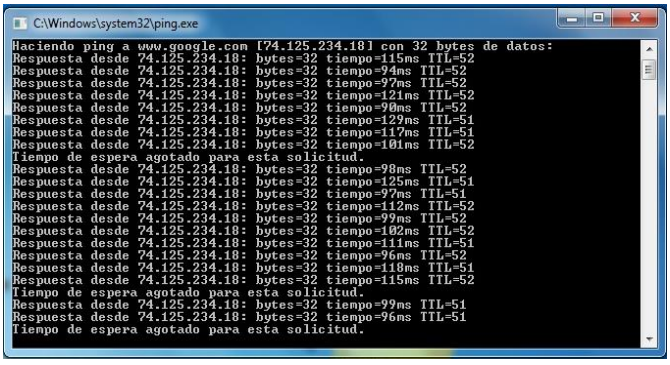


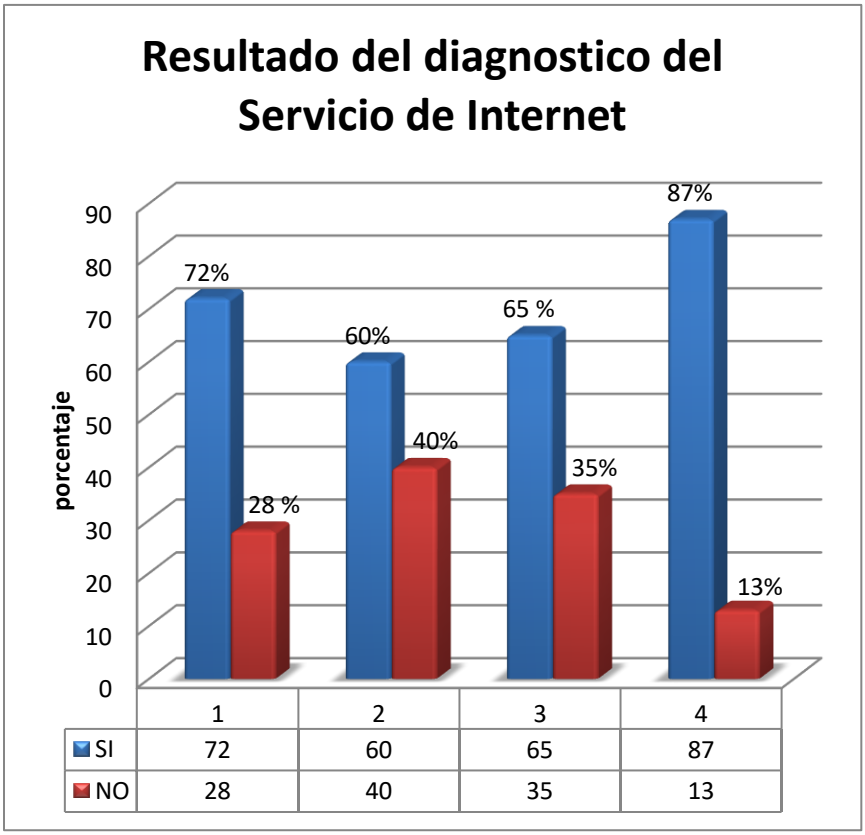
Figura 3.1: Test del conexión a Internet.

Fuente: Elaboración propia.

3.1.1.3. Evaluación de la situación del servicio de Internet.

a) Diagnostico inicial del servicio de Internet.

A través de la información obtenida en el diagnostico se muestra una representación grafica que resume el uso del servicio de Internet en el Campus Universitario de la U.A.P. se dividió en dos partes, la primera muestra el grafico con preguntas cerradas que se realizo al usuario y la segunda con preguntas de selección múltiple a continuación se muestra la grafica de preguntas cerradas.



Nº	Preguntas
1	¿Cuenta con el servicio de Internet?
2	¿Cuenta con asistencia técnica de alguna duda que tenga con el servicio de Internet?
3	¿Sabe los tipos de virus que existe?
4	¿Desearía tener información sobre temas relacionado a los virus informáticos?

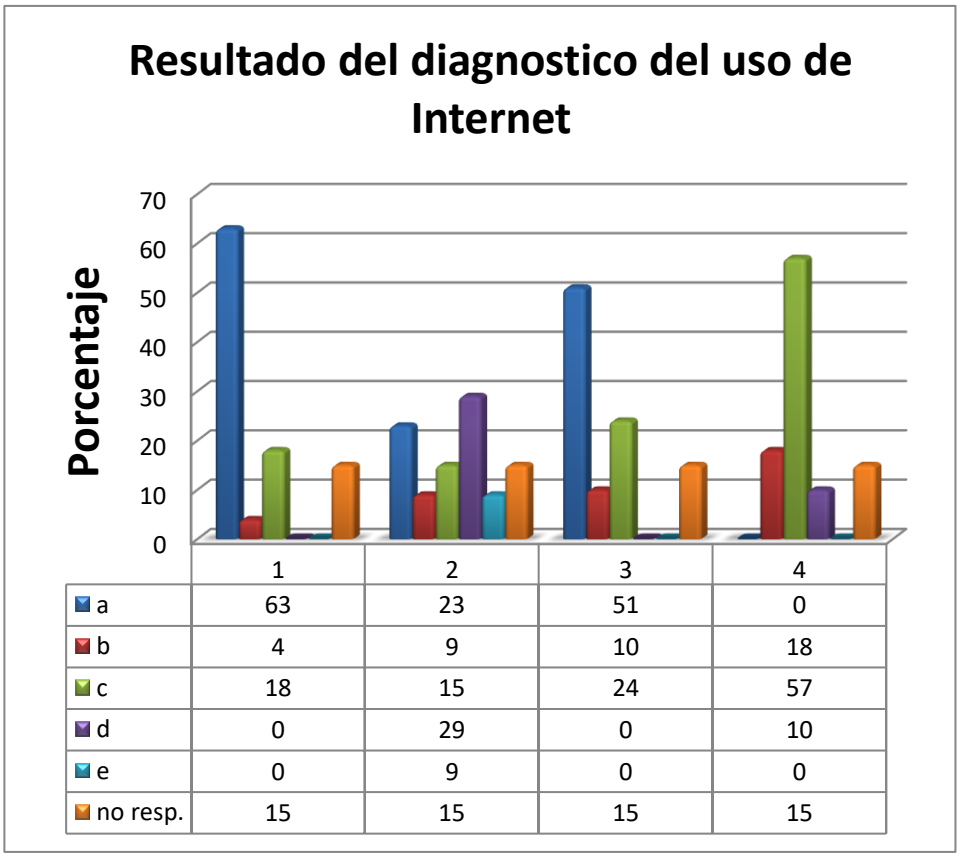
Grafico 3.1: Resultado del diagnostico del uso de Internet 1.1.

Fuente: Elaboración propia.

Como se menciono anteriormente el diagnostico se aplico a los usuarios que tienen acceso a Internet los cuales actualmente son 81 donde se refleja en la grafica que del total de los usuarios el 72% cuenta con conexión a Internet y el 28% no tiene conexión a Internet mas cuenta con el servicio a Internet, el 60% cuenta con asistencia técnica y el

40% no cuenta con asistencia técnica para la conexión a Internet, el 65% conoce los tipo de virus que existen el 35% no conoce ningún tipo de virus malicioso existente, el 87% de los usuarios desearían tener información sobre temas relacionados con los virus informáticos y el 13% ya tiene conocimiento sobre los tipos de virus informáticos existentes.

Se observa a continuación la grafica de las preguntas de selección múltiple hechas al usuario.



	1	2	3	4
a	63	23	51	0
b	4	9	10	18
c	18	15	24	57
d	0	29	0	10
e	0	9	0	0
no resp.	15	15	15	15

Grafico 3.2: Resultado del diagnostico del uso de Internet 1.2

Fuente: Elaboración propia

Nº	Preguntas	Opciones de respuesta
1	¿Con que finalidad utiliza el servicio de Internet?	a. Investigativo b. Entretenimiento c. Otros
2	¿Qué tipo de servicio utiliza en Internet?	a. Correo electrónico b. Video conferencia c. chat d. Descargas e. Otros
3	¿En qué horario utiliza con frecuencia el servicio de Internet?	a. Cuando hay necesidad b. Horario especifico c. En cualquier momento
4	¿Cómo calificaría al servicio de Internet de la U.A.P.?	a. Excelente b. Bueno c. Regular d. Malo e. Pésimo

- Del total de las personas entrevistadas, 63% de usuarios utiliza el Internet con la finalidad de investigación, 4% de usuarios especifican que para entretenimiento, 18% de usuarios con otros motivos y 15% de usuarios se reservaron a la opinión.
- Del total de las personas entrevistadas, 23% de usuarios utiliza el Internet para correo electrónico, 9% de usuarios para videos conferencias, 15% de usuarios para chat, 29% de usuarios para descargas de datos, 9% de usuarios para otros servicios y 15% de usuarios se reservaron a la opinión.
- Del total de las personas entrevistadas, 51% de usuarios utiliza Internet con más frecuencia cuando hay necesidad, 10% de usuarios en horarios específicos, 24% de usuarios en cualquier momento y 15% de usuarios se reservaron a la opinión.
- Del total de las personas entrevistadas, ningún usuarios califica que el servicio de Internet es excelente, 18% de usuarios califican al servicio de Internet como bueno, 57% de usuarios consideran que es regular, 10% usuarios califican el servicio de Internet como malo y 15% de usuarios se reservaron a la opinión.

b) Diagnostico actual del servicio de Internet.

Para la aplicación del diagnostico del servicio de Internet actual se trabajo bajo una muestra estadística sistémica a diferencia del diagnostico inicial que se trabajo con

datos reales de la cantidad de usuarios de Internet existentes, para la recolección de datos de la muestra se tomo un usuario de cada cinco usuarios para ser encuestado lo que significa que la cantidad de usuarios para la muestra es de 17 usuarios puesto que se cuenta con un total de 81 usuarios, con los datos obtenidos del diagnostico actual del servicio de Internet se llega a concluir que se ha alcanzado una mejoría considerable del 21% en el rendimiento del servicio de Internet.

A continuación se muestra en la siguiente grafica la diferencia del resultado del diagnostico inicial y actual.

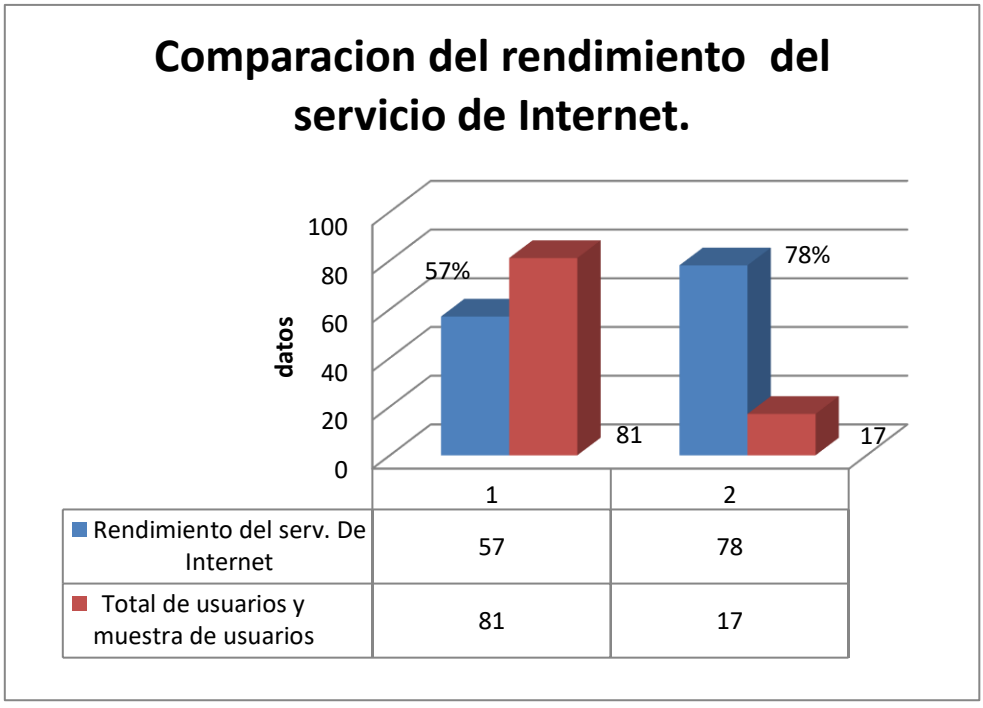


Grafico 3.3: Comparación del diagnostico del servicio de Internet inicial y actual.

Fuente: Elaboración propia.

En la grafica 3.3 se muestra el porcentaje del rendimiento del servicio de Internet y la cantidad de usuarios encuestados en el diagnostico inicial y actual, con el resultado conseguido del rendimiento del servicio de Internet en el diagnostico inicial se tiene que el 57% de 81 usuarios evalúan que el servicio de Internet es regular, haciendo la diferencia con el diagnostico actual de la muestra se tiene que el 78% evalúan que el

servicio de Internet es bueno, lo que significa que la conexión a Internet ha mejorado en un 21% del rendimiento del servicio de Internet inicial.

Para el planteamiento de las preguntas se tomo solo aspectos del servicio de Internet para lo cual se elaboro preguntas concernientes al Internet, con preguntas cerradas y de selección múltiple y a través de la información y resultados obtenidos se tienen las conclusiones del diagnostico, detalle de diagnostico en (Anexo B).

3.1.1.4. Conclusiones de diagnóstico.

De acuerdo al análisis de la información que se obtuvo y tomando en cuenta que el uso de Internet es necesario en el ámbito laboral de la institución y los constantes cortes frecuentes por parte del proveedor (Coteco), y el uso indebido del Internet, es necesario la implementación de un servidor proxy, ya que los usuarios hacen visitas a paginas no autorizadas por la institución (pág. Sociales), paginas de conexión en línea (juegos en línea), etc. Es por eso que se debe de evitar las descargas de diferentes tipos de páginas como por ejemplo P2P, youtube, facebook, dilan dau, orkut y otros, etc.

Diseñar e implementar políticas del servicio de Internet con la finalidad de reglamentar el uso adecuado del Internet además de contra restar los virus informáticos mediante limpiezas periódicas y capacitación a los usuarios de esta actividad.

Brindar asistencia técnica a los usuarios de forma rápida e inmediata para la resolución de problemas de conexión a la red y por tanto a Internet o de otros percances que se puedan presentar, controlar y monitorear el funcionamiento de la red a fin de priorizar las prestaciones del servicio de Internet.

Contar con más Switch para la conexión de predios y reemplazar los que están en mal estado, actualmente se cuenta con 14 Switch y 5 Acces Point en funcionamiento en todo el campus, el cual no abastece la demanda que se tiene de usuarios, que actualmente existe 81 usuarios de Internet y 9 usuarios de la red de datos, que hace un total de 90 usuarios de red de datos en el campus universitario de la U.A.P.

3.1.1.5. Diseño de la topología de la Red de datos del Campus Universitario.

El diseño de la Red de Datos del Campus Universitario actualmente está compuesto por 14 Switch de conexión por cableado y 5 Acces Point de conexión inalámbrica, los cuales están distribuidos en los diferentes predios del campus como muestra la figura 3.2, la cantidad de Switch y Acces Point en funcionamiento actual no satisface las necesidades de conexión, motivo generado por el crecimiento de la demanda y el incremento laboral dentro en la Universidad.

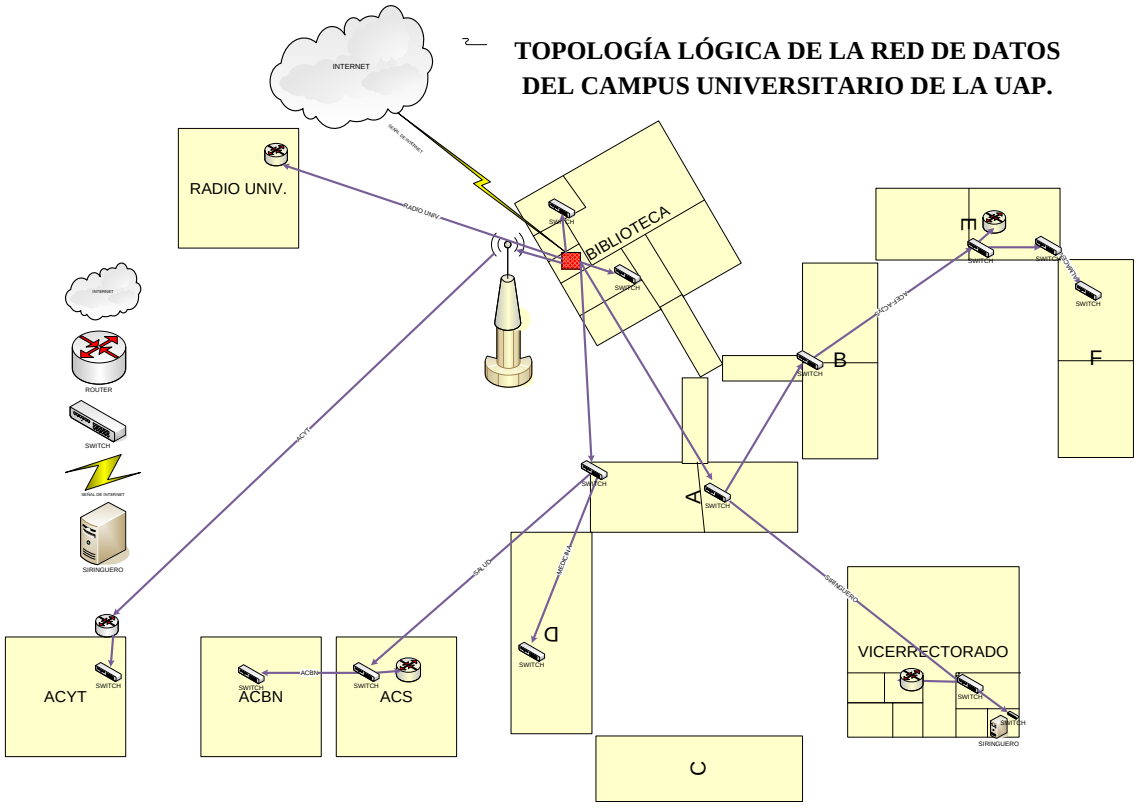


Figura 3.2: Topología lógica de la Red de Datos del Campus Universitario de la U.A.P.

Fuente: Elaboración propia

De acuerdo a la demanda de conexiones de red e Internet y los inconvenientes que se tiene a través de la conexión inalámbrica, se determina la selección de la infraestructura de red basado en los requerimientos técnicos y en la topología propuesta, que se muestra a continuación en la figura 3.3.

Se hace mención de los materiales requeridos para la implementación de la nueva estructura y reemplazo de algunos Switch en mal estado, que tumban la conexión a la red.

Nº	Material	Cantidad
1	Switch de 8 puertos	04
2	Switch de 16 puertos	04
3	Switch de 24 puertos	04
4	Cable UTP (Caja de 300m)	04

Tabla 3.1: Material requerido para la nueva estructura de la Red de Datos.

Fuente: Elaboración propia

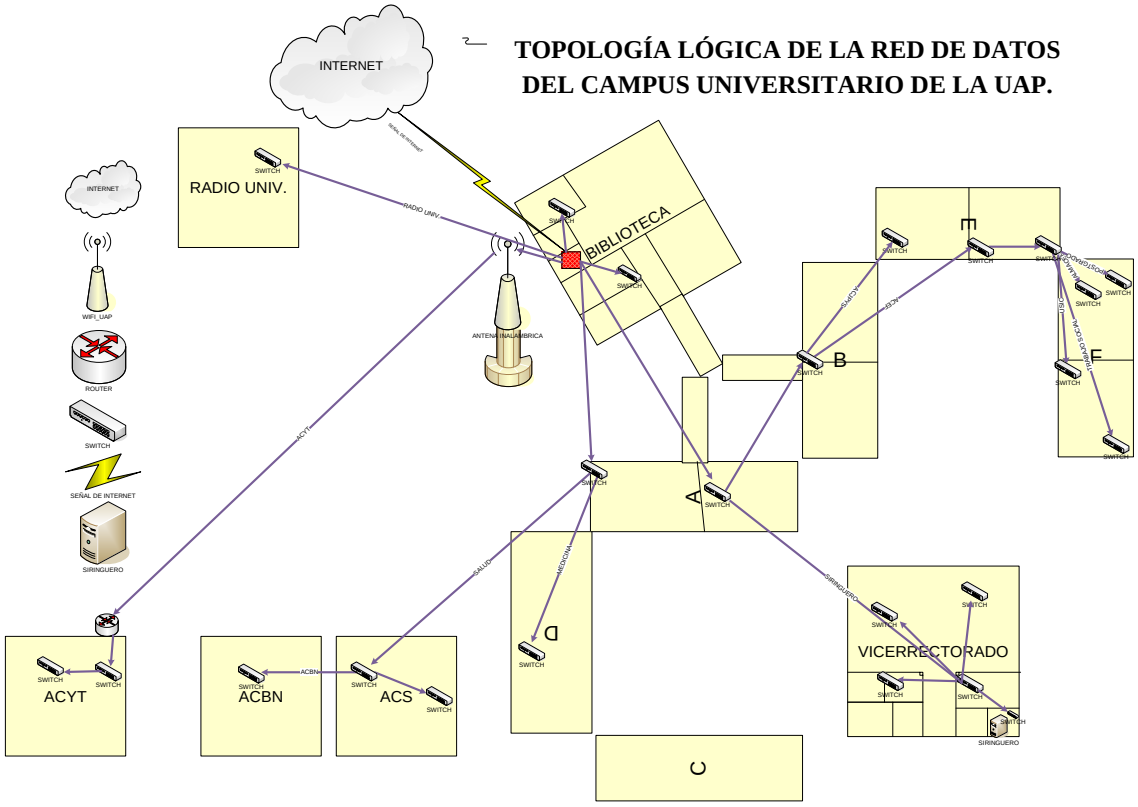


Figura 3.3: Topología lógica de la Red de Datos del Campus Universitario de la U.A.P. (Propuesta).

Fuente: Elaboración propia

La nueva estructura de la Red de Datos está basado en los requerimientos de conectividad a la red e Internet y por las problemáticas presentadas en las conexiones inalámbricas se plantea la nueva estructura a base de 25 Switch y un Acces Point el cual significa que el 90% de los usuarios accederán a la red a través de conexión por cableado, esto para mejorar y garantizar la conexión a la red e Internet y el 10% por conexión inalámbrica a través de zona WIFI_UAP que la U.A.P. ofrece a su comunidad estudiantil. La nueva estructura de la red se está implementando parcialmente en los diferentes predios del Campus Universitario donde ya se abarco los predios de Bloque F (Recursos Humanos, Oficina de Acjpys, Usic, PostGrado), Bloque E (Acef y Acjpys).

3.1.2. Selección de la infraestructura de red.

La selección de la infraestructura de red se realizo de acuerdo a la propuesta del diseño de la Red, los equipos de red y de computación existentes que están en buen funcionamiento para reorganizar sus posiciones.

- Infraestructura para la administración de usuarios del Servicio de Internet y la Red de Datos

Nº	Características	Detalle
1	Laptop	HP de 16px
2	Disco duro	100,00 GB
3	Procesador	Intel(R) Core(TM)2 1.83GHZ
4	Memoria RAM	1,00 GB
5	Tarjeta de red	Integrada

Tabla 3.2: Características de la PC- Laptop utilizada.

Fuente: Elaboración propia

- Infraestructura utilizada para el monitoreo de red y el servicio de Internet.

Nº	Características	Detalle
1	PC de Escritorio	01
2	Tarjeta madre	Asus
3	Memoria RAM	2GB
4	Disco duro	200GB
5	Procesador	1.87GHZ
6	Monitor	Gaba
7	Mouse	Gaba-Optico
8	Tarjeta de red	Integrada a la PC
9	Adaptador de Red	TP-Link

Tabla 3.3: Características de la PC de escritorio utilizado.

Fuente: Elaboración propia

- Infraestructura para la implementación, administración y funcionamiento de la red de datos y el Servicio de Internet.

Nº	Material	Cantidad	Detalle
1	MIkrotik RB1100(Existente)	01	
2	MIkrotik RB1100(Nuevo)	01	
3	MIkrotik RB450G(Existente)	01	
4	Switch de 8 puertos (nuevo)	04	
5	Switch de 16 puertos (Existente)	08	
6	Switch de 16 puertos(nuevo)	04	
7	Switch de 24 puertos(Existente)	03	
8	Switch de 24 puertos(nuevo)	04	
9	Cable UTP (Caja de 300m) (nuevo)	04	
10	Conectores RJ45(nuevo)	300	
11	Antena bullet2 Ubiquiti	01	
12	Roseta de red (Existente)	35	

Tabla 3.4: Material disponible para la Red de Datos.

Fuente: Elaboración propia

- Selección del nuevo Rango de IP, Para la Migración de la red existente a la nueva estructura de red, la distribución de rangos de IP`S pertenece a la clase C, por su tamaño que se utiliza para redes pequeñas.

Nº	Características	Detalle
1	192.168.5.1-192.168.5.254	Para la red LAN interna
2	192.168.5.1	Para el Servidor Mikrotik
3	192.168.5.2	Para la el Sistema Siringuero
4	192.168.5.47	Para la conexión a Wifi
5	192.168.5.3-192.168.5.127	Para sin privilegios
6	192.168.5.128-192.168.5.254	Para con privilegios
7	192.168.20.100-192.168.20.200	Red LAN interna, Para la Zona WIFI_UAP

Tabla 3.5: Nuevos rangos de IP`S en la Red de Datos del Campus Universitario.

Fuente: Elaboración propia

3.1.3. Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

3.1.3.1. Instalación de hardware.

Dentro la USIC (Unidad de Sistemas de Información y Comunicación) en la DRDI (División de Datos e Internet) se contaba con un servidor RouterBoard MikroTik RB1100 y RouterBoard MikroTik RB450, que fueron utilizados para la implementación de la zona Wifi y la Administración de la Red de Datos e Internet de toda la U.A.P. la misma que administra la red de datos del Campus Universitario, para asegurar que la parte que será instalada es compatible con los componentes ya existentes se realizo un estudio previo antes de realizar el análisis de la Red de Datos e Internet el Diseño Lógico era tal cual se muestra en la Figura 3.4.

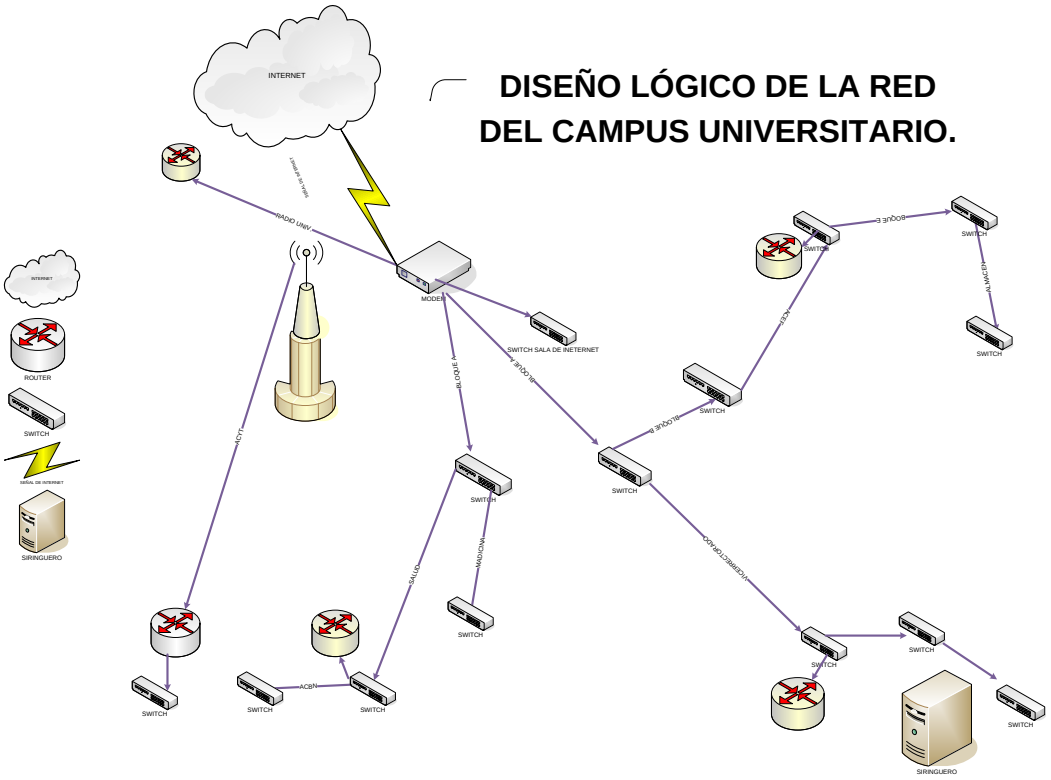


Figura 3.4: Diseño lógico de la red del Campus Universitario.

Fuente: Elaboración propia

Este diseño lógico de la red de datos del Campus Universitario tenía deficiencia con el servicio de Internet e intranet porque no existía control de acceso a ciertas páginas web por la inexistencia de políticas de uso de Internet y el mal estado y funcionamiento de algunos accesorios de red que obstaculizaba brindar un buen servicio al usuario.

Para la instalación del hardware se trabajo en base al nuevo diseño propuesto que enlaza todos los predios del Campus Universitario como se muestra en la Figura 3.5.

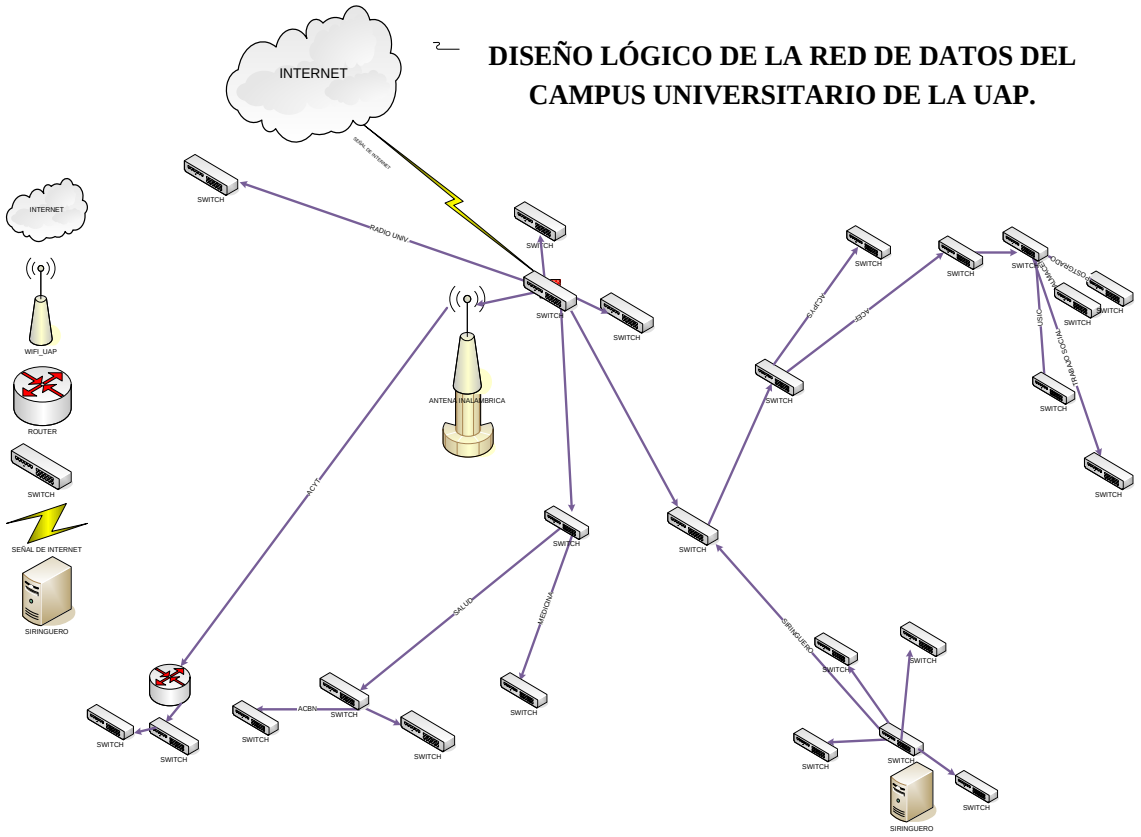


Figura 3.5: Diseño lógico de la red del Campus Universitario de la U.A.P.

Fuente: Elaboración propia.

Para garantizar el funcionamiento de la Red de Datos, del sistema Siringuero en todos los predios y del servicio de Internet se vio por conveniente reorganizar el cableado de algunos predios del Campus Universitario de acuerdo al nuevo diseño.

Posteriormente se contó con otro MikroTik RB1100, que es utilizado como servidor de respaldo del servidor actual, que contiene las mismas configuraciones, para ser utilizado en caso de alguna falla en el Servidor MikroTik, tanto de hardware, software o error de usuario en alguna configuración que se realice.

3.1.3.2. Administración del software.

En la instalación del Software, se administró el RouterBoard MikroTik RB1100 y RB450 bajo las siguientes configuraciones que se muestra en la siguiente tabla:

Configuración en Mikrotik	Descripción	Detalle
Interfaces/puertos	Configuración de la interfaz con el IP Address de la Red WAN y LAN interna en un puerto del MiKroTik.	Configuración de las interfaces, definiendo el puerto para la red interna y el puerto para el proveedor de Internet. Interfaz Puerto Ether0 IP/address Red WAN IP publica. Interfaz Puerto Ether4 IP/address Red LAN interna 192.168.5.0/24.
ARP	**Address Resolution Protocol**, protocolo de capa 2, crea una tabla para interconectar las IP`S con la MACs.	Para el premiso a Internet a través de IP/adrress y MAC/address.
Firewall	**Corta Fuegos**, elemento de red, hardware o software que controla las políticas de seguridad para el acceso o restricción de comunicación.	Pared de control entre Internet de llagada e Internet de salida en la red LAN interna.
NAT	**Network Address Translation,** permite el enrrutamiento de IP`S.	Para enrrutar red LAN interna por la Web proxy.
Web Proxy	Bloquea y permite contenido de capa7, gestiona acceso y niveles de usuarios, permite administrar el cache de acceso web, permite rastreo de contenido web.	Para la restricción de páginas Web.
HotSpot	**Portal Cautivo**, permite agregar un nivel de autenticación para el acceso a red, se maneja con usuario y password.	Para la Zona WIFI_UAP del Campus Universitario de la UAP.
QoS	**Quality of Service**, permite gestionar la calidad del servicio a otorgarse, priorización y creación de colas por tipo de tráfico, distribución equitativa.	Queues simples y queue tree.
DHCP	**Dinamic Host Configuration Protocol**, permite la asignación de IP`S automáticamente a un segmento de red, proveniente de un pool de Direcciones, permiten agregar IP address, Netmask, Gateway y DNS.	Asignacion de IP address, Netmask, Gateway y DNS a usuarios de la Zona WIFI_UAP, en la red LAN interna 192.168.20.0/24

Tabla 3.6: Configuración en MikroTik para la administración de la Red de Datos.

Fuente: Elaboración propia

Para ver detalle de la administración de la configuración en Mikrotik ver (Anexo E).

- **Configuración del protocolo TCP/IP en los equipos informáticos de los usuarios.**

Para la configuración del protocolo TCP/IP se siguió los siguientes criterios que se detalla en la Tabla.

Nº	Descripción	Detalle
1	Dirección IP	192.168.5.x, perteneciente a la clase c donde x es el numero de la nueva dirección IP que se asigna cada vez que solicita un usuario.
2	Gateway o puerta de enlace	La puerta de enlace asignada es la dirección IP 192.168.5.1
3	DNS	El DNS preferido asignado es 192.168.5.1 y el alterno 8.8.8.8.

Tabla 3.7: Descripción de la configuración del protocolo TCP/IP.

Fuente: Elaboración propia.

- **Configuración de IP/MAC en el RouterBoard MikroTik.**

Para la configuración de la IP/MAC en el ARP del servidor se realizo bajo el siguiente criterio, el cual permite al usuario tener acceso al Servicio de Internet en dos diferentes tipos de usuarios que son:

- **Usuario con privilegio.-** Gozan de servicio con ciertos permisos de acceso ejemplo: páginas sociales, youtube, etc. en la navegación, pero con restricciones a páginas pornográficas.
- **Usuario sin privilegio.-** Gozan el servicio de Internet con ciertas restricciones a ejemplo: páginas sociales, páginas pornográficas, youtube, etc.

A continuación se muestra en la siguiente tabla.

Característica	Rango IP/MAC	Privilegios	Detalle
Para el registro de usuarios se considero. • **Nombre usuario** • **IP** • **MAC**	IP: 192.168.5.128-192.192.168.5.254 MAC: xx:xx:xx:xx:xx:xx	Usuario con privilegio	Directores, Jefes de Unidad y autorizados por el responsable de la USIC.
	IP: 192.168.5.1-192.192.168.5.127 MAC: xx:xx:xx:xx:xx:xx	Usuario sin privilegio	Aquellos que no son Directores ni Jefes de Unidad.

Tabla 3.8: Descripción de la configuración del ARP.

Fuente: Elaboración propia

- **Configuración de nuevos usuarios para la zona WIFI en MikroTik.**

Para la configuración de nuevos usuarios de la Zona WIFI (WIFI_UAP) se considero los siguientes datos que se muestran en la siguiente tabla 3.9.

Característica	usuario	password	Detalle
Nombre usuario	CI	RU	CI y RU serán para la autenticación del usuario en el servidor HotSpot y para acceder al servicio de Internet.

Tabla 3.9: Descripción de registro de nuevos usuarios de la zona Wifi.

Fuente: Elaboración propia

- **Respaldo de Backup de las configuraciones en MikroTik.**

Se realiza la extracción de Backup de respaldo de las configuraciones del servidor al finalizar la jornada de trabajo del día, guardándose las configuraciones que se haya realizado durante el día de trabajo.

Muestra de Backup de respaldos detallada en la siguiente tabla.

Mes	Fecha	Capacidad
Septiembre	17/09/12	67kb
	18/09/12	76kb
	19/09/12	89kb
	20/09/12	92kb
	21/09/12	96kb
Octubre	22/10/12	117kb
	23/10/12	119kb
	24/10/12	126kb
	25/10/12	167kb
	26/10/12	183kb
Noviembre	12/11/12	184kb
	13/11/12	184kb
	14/11/12	191kb
	15/11/12	193kb
	16/11/12	196kb

Tabla 3.10: Tabla de Backup de respaldo de las configuraciones.

Fuente: Elaboración propia

3.1.4. Aprovisionamiento.

Para el aprovisionamiento, se cuenta con algunos recursos de respaldo de hardware, software y elementos de Red, dentro de la División de Redes de Datos e Internet se tienen disponibles un RouterBoard RB1100 y Backup de las configuraciones para el aprovisionamiento del servidor, un Switch de 16 y 24 puertos, antenas inalámbricas (Linsys(2), Cisco(1)), adaptadores de red 10 unidades y algunas herramientas y componentes de Red para realizar los cableados (canaletas, rosetas, alicates de red, destornilladores, escalera metálica), todos materiales son utilizados para dar una solución inmediata cuando ocurre alguna falla en la red, hasta efectuar una solución permanente y estable.

3.1.4.1. Recomendaciones.

Tomando en cuenta los requerimientos y la demanda de usuarios se recomienda aumentar el aprovisionamiento de recursos de elementos de red en la DRDI.

- Contar con Switch de 8 y 16 puertos.
- Contar con Cable UTP y conectores RJ45 disponibles de Reserva, para agregar puntos de Red o atender cualquier falla de cableado de Red.

- Contar con herramientas y componentes de Red disponibles como ser: alicates de red, Tester de red, taladro, juego de brocas de diferentes medidas milimétricas, tornillos de diferentes tamaños, sujetadores de tornillos de acuerdo a los diferentes tamaños de los tornillos, etc.

3.1.5. Políticas y procedimientos relacionados.

La División de Redes de Datos e Internet no contaba con políticas y procedimientos relacionados al uso del servicio de Internet, debido a esta dificultad se vio la necesidad de realizar las políticas de uso del servicio de Internet y procedimientos de uso y registros de usuarios de Internet.

Las políticas de uso del servicio de Internet fueron elaboradas de acuerdo a los requerimientos de las instancias superiores que plantea para los usuarios, fue presentado a la Unidad de Sistemas de Información y Comunicación (USIC), para su revisión y/o modificación si se tiene errores y /o fallas, para luego ser presentado a instancias superiores y posteriormente contar con su aprobación.

Para ver políticas de uso de Internet ver (Anexo D).

Los procedimientos y formularios se planteo para la administración de usuarios de Internet, para así tener registro físico, control de usuarios y una administración eficiente del servicio de Internet, brindando información práctica y eficiente al usuario a través de procesos y procedimientos.

Para ver procedimientos ver (Anexo C).

3.1.6. Conclusión de administración de la configuración.

Durante la fase de administración de la configuración se realizo las actividades de planeación y diseño de la red, donde se elaboro el diseño lógico de la red actual y el diseño lógico propuesto de acuerdo al requerimiento de la demanda, se realizo el diagnostico inicial y actual a través de encuestas aplicadas a los usuarios del servicio de Internet, con una diferencia de rendimiento del servicio de Internet en el diagnostico actual del 21% al resultado del diagnostico inicial, se realizo configuraciones para la administración del servicio de Internet y la red de datos en el servidor MikroTik, como ser

el servidor Web proxy para la restricción de páginas web, el HotSpot para el ingreso por autenticación a la zona Wifi de la U.A.P. se administro constantemente las herramientas del ARP en el MikroTik realizando el amarre de IP/MAC para dar acceso a Internet a los usuarios, para la administración de usuario y el control de ancho de banda se trabajo con calidad de servicios, realizando restricciones de ancho de banda por usuario de acuerdo al nivel jerárquico que ocupa dentro las funciones laborales de la U.A.P. en el Campus Universitario, para el control y registro de usuarios se administro bajo el enfoque de gestión de calidad rigiéndonos únicamente en lo que concierne a procedimientos y políticas de uso, para lo cual se elaboro procedimiento de de altas bajas y modificaciones y sus respectivos formularios, se elaboro la propuesta de las políticas de uso puesto que la unidad no contaba con ello.

La administración mejoro porque se aplico en el periodo del Trabajo Dirigido la administración con gestión de calidad y el uso de políticas ya que la unidad anterior a la ejecución del trabajo no contaba con esos elementos en la administración del servicio de Internet.

3.2. ADMINISTRACIÓN DEL RENDIMIENTO.

La administración del servicio de Internet y la Red de Datos se realizó en dos etapas que son: Monitoreo y Análisis, por la necesidad de recolectar y analizar el tráfico generado que circula por la red en un momento en particular (tiempo real) o en un intervalo de tiempo, el cual permitió tomar decisiones pertinentes de acuerdo al comportamiento encontrado, las mismas se explican a continuación: (Untiveros, 2004)

3.2.1. Monitoreo.

El monitoreo del servicio de Internet y la Red de Datos consiste en observar y recolectar la información referente al comportamiento de la red en los siguientes aspectos.

3.2.1.1. Monitoreo del servicio de Internet (Red Wan Externa).

Este proceso de monitoreo del servicio de Internet se realizo bajo un plan de actividades para el testeo del ancho de banda del servicio de Internet que nos brinda la empresa proveedora (COTECO Ltda).

Hacer un test de velocidad es la forma más rápida de probar el rendimiento de una conexión de banda ancha para lo cual se realizo utilizando herramientas de testeo de páginas de web, que se detalla más adelante, lo que significa que no son un 100% seguros en los resultados testeados de la velocidad del ancho de banda, pero nos dan un aproximado de la velocidad del ancho de banda que nos llega desde el proveedor hasta el usuario.

Para el monitoreo del Internet se realizo en dos instancias que son:

- **Monitoreo de ancho de banda sin usuario.**

  Se desconectan físicamente todos los equipos de la Red de Datos y del servicio de Internet, se conecta un equipo directamente al conmutador (Switch) principal, el cual recibe la señal de internet por cable de fibra óptica, las herramientas utilizadas para la verificación del ancho de banda disponibles de forma gratuita son la siguientes direcciones web.

  http://www.testdevelocidades.es/

  http://wwwspeedtest.com

  http://www.internauta.com

  Para ello se muestra en la siguiente tabla el cronograma elaborado de fecha, hora y resultado para la medición del ancho de banda.

Mes	Fecha	Hora	Resultado
Septiembre	10/09/12	8:30 am	529kbps
	11/09/12	11:30 am	426kbps
	12/09/12	10:00 am	376kbps
	13/09/12	10:30 am	364kbps
	14/09/12	9:00 am	552kbps
			Promedio 449.4 Kbps
Octubre	22/10/12	16:30 pm	549kbps
	23/10/12	12:00 pm	526kbps
	24/10/12	12:30 pm	625kbps
	25/10/12	9:00 am	637kbps
	26/10/12	12:45 pm	798kbps
			Promedio 1607 Kbps

Noviembre	12/1112	9:00 am	992kbps
	13/1112	12:30 pm	1462kbps
	14/1112	12:00 pm	1090kbps
	15/1112	12:45 pm	1354kbps
	16/1112	12:30 pm	1455kbps
			Promedio 1270.6 Kbps

Tabla 3.11: Cronograma y resultados de testeo de fecha, hora y resultado en la medición del ancho de banda sin usuarios.

Fuente: Elaboración propia

- **Monitoreo de ancho de banda con usuarios.**

  Se realiza cuando se conectan todos los equipos a la Red de Datos al mismo tiempo que usan el servicio de Internet, se conecta un equipo directamente al conmutador (Switch) principal, el cual recibe la señal de Internet por cable de fibra óptica, las herramientas utilizadas para la verificación del ancho de banda disponibles de forma gratuita son la siguientes direcciones web.

  http://www.testdevelocidades.es/

  http://wwwspeedtest.com

  http://www.internauta.com

Figura de testeo.

Figura 3.6: Pantalla de testeo de http://www.testdevelocidades.es/ probando la velocidad de bajada de ancho de banda con usuarios.

Fuente: Elaboración propia.

Para ello se muestra en la siguiente tabla el cronograma elaborado de fecha, hora y resultado para la medición del ancho de banda con usuarios navegando en Internet.

Mes	Fecha	Hora	Resultado
Septiembre	10/09/12	8:30 am	196kbps
	11/09/12	11:30 am	168kbps
	12/09/12	10:00 am	246kbps
	13/09/12	10:30 am	266kbps
	14/09/12	9:00 am	132kbps
			Promedio 201.6 Kbps
Octubre	22/10/12	16:30 pm	246kbps
	23/10/12	12:00 pm	272Kbps
	24/10/12	12:30 pm	275Kbps
	25/10/12	9:00 am	279Kbps
	26/10/12	12:45 pm	268Kbps
			Promedio 268 Kbps
Noviembre	12/1112	9:00 am	334Kbps
	13/1112	12:30 pm	483kbps
	14/1112	12:00 pm	541kbps
	15/1112	12:45 pm	773kbps
	16/1112	12:30 pm	1158kbps
			Promedio 657.8 Kbps

Tabla 3.12: Cronograma y resultados de testeo de fecha, hora y resultado en la medición del ancho de banda con usuarios.

Fuente: Elaboración propia.

3.2.1.2. Monitoreo de los cortes del servicio de Internet.

Se llevo a cabo cuando el servicio de Internet, tenía cortes o lentitud (saturación) en la navegación a Internet, esta actividad se realiza haciendo el llamado correspondiente vía telefónica a la empresa responsable Coteco Ltda, con el objetivo de preguntar sobre el problema del servicio de Internet corte o lentitud, en coordinación entre ambas partes interesadas se da la solución del problema. Como resultado del control y

monitoreo del servicio de Internet, se observan los datos obtenidos durante los meses de septiembre, octubre y noviembre de la gestión 2012 como se observa en la siguiente tabla.

Mes	Fecha de reclamo	Tipo de reclamo	Motivo del corte
Septiembre	03/09/12	Corte del servicio de Internet	Problema de Brasil telecom
	05/09/12	Lentitud del servicio de Internet	Interferencia de la señal del Internet
	08/09/12	Corte del servicio de Internet	Configuración de equipos
	11/09/12	Corte del servicio de Internet	Ajustes técnicos
	13/09/12	Corte del servicio de Internet	Problema de Brasil telecom
	17/09/12	Lentitud del servicio de Internet	Interferencia de la señal del Internet
	19/09/12	Corte del servicio de Internet	Problema de Brasil telecom
	20/09/12	Corte del servicio de Internet	Ajustes técnicos
	25/09/12	Corte del servicio de Internet	Problema de Brasil telecom
	31/09/12	Lentitud del servicio de Internet	Interferencia de la señal del Internet
Octubre	05/10/12	Corte del servicio de Internet	Problema de Brasil telecom
	09/10/12	Corte del servicio de Internet	Ajustes técnicos
	13/10/12	Lentitud del servicio de Internet	Interferencia de la señal del Internet
	19/10/12	Lentitud del servicio de Internet	Interferencia de la señal del Internet
	24/10/12	Corte del servicio de Internet	Problema de Brasil telecom
	30/10/12	Lentitud del servicio de Internet	Interferencia de la señal del Internet
Noviembre	06/11/12	Corte del servicio de Internet	Problema de Brasil telecom
	15/11/12	Corte del servicio de Internet	Problema de Brasil telecom
	21/11/12	Lentitud del servicio de Internet	Interferencia de la señal del Internet
	26/11/12	Corte del servicio de Internet	Ajustes técnicos
	29/11/12	Corte del servicio de Internet	Problema de Brasil telecom

Tabla 3.13: Control y monitoreo de cortes de servicio de Internet.

Fuente: Elaboración propia.

De la misma manera se realiza el monitoreo internamente de cortes del servicio de Internet dentro la Red interna de Datos, que podrían estar afectados por el mal funcionamiento de algún hardware que hace corte en la conexión a la red, también el monitoreo de conexión a la red desde el punto de acceso hasta la base o inversamente hasta encontrar el problema, ping de conexión a la red, testeo del funcionamiento del cable UTP

de conexión, testeo de funcionamientos de puertos de Switch, ping de conexión de la base al punto de acceso, etc.

3.2.1.3. Monitoreo del servicio de Internet (Red LAN Interna).

Se denomino control y monitoreo del servicio de Internet al constante monitoreo del Internet que la U.A.P. brinda a los usuarios del Campus Universitario para realizar este control se utilizo como herramientas los Queues y tráfico en MikroTik, el programa de monitoreo BitMeter (control y monitoreo de ancho de banda en descargas de datos), también se realizo ping la Red para verificar la conectividad de los equipos y el tiempo de transmisión de los paquetes enviados.

Control y monitoreo de uso de Internet por usuarios a través de MikroTik con la herramienta Queues, que nos permite visualizar la saturación de ancho de banda que nos genera el usuario y en trafico de usuarios se observa la velocidad de datos de bajada y subida y el numero de paquetes enviados y recibidos como se muestra en las siguientes figuras 3.7 a 3.9.

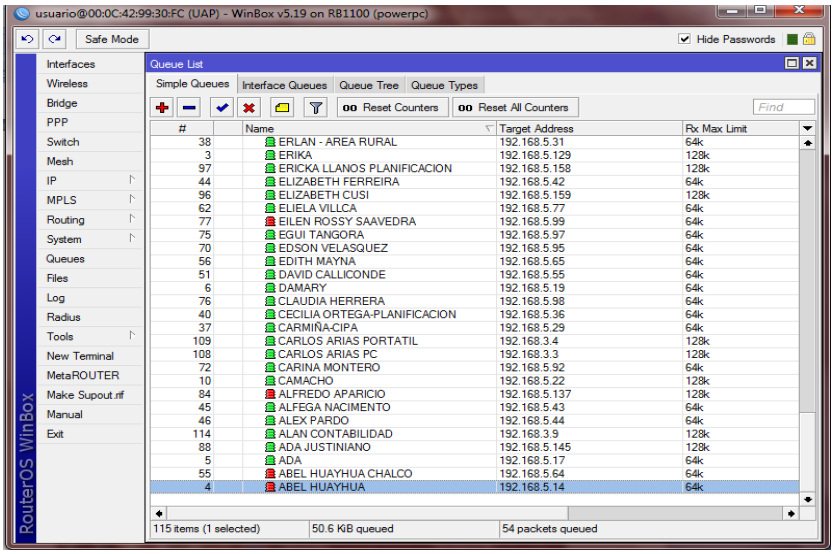


Figura 3.7: Control y monitoreo de ancho de banda por usuarios en Queues.

Fuente: Elaboración propia

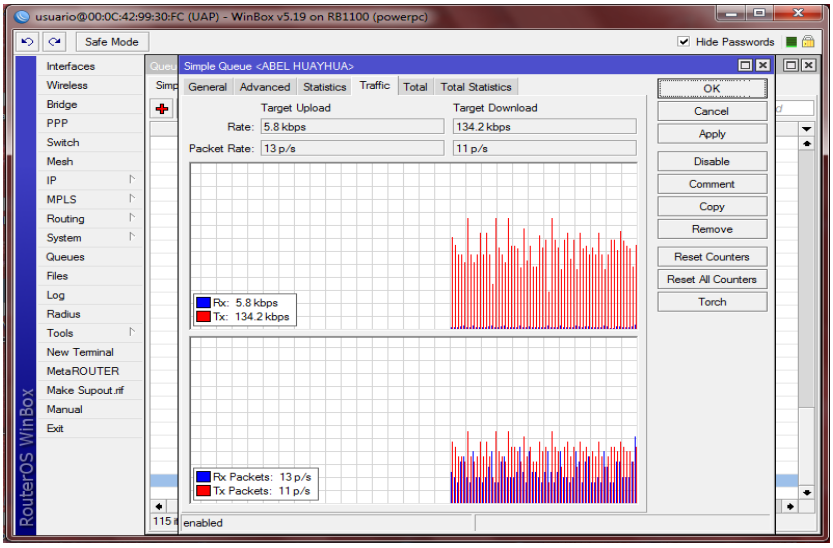


Figura 3.8: Control de tráfico de paquetes.

Fuente: Elaboración propia.

Monitoreo con BitMeter software de monitoreo de descarga de datos, nos monitorea las peticiones de carga, descarga y el tiempo combinado entre ambos.

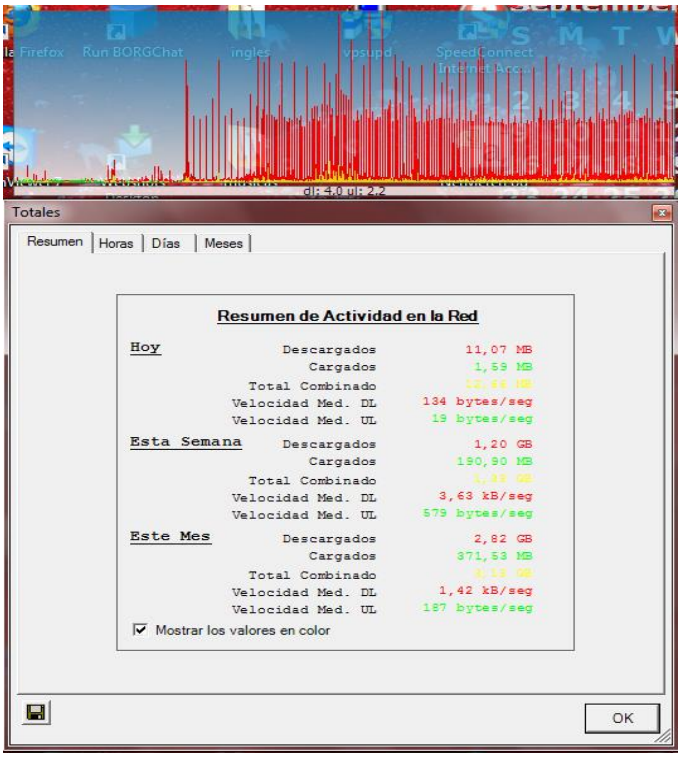


Figura 3.9: Monitoreo con BitMeter.

Fuente: Elaboración propia.

Detalle de datos monitoreados con BitMeter por mes de consumo de carga, descarga y velocidad de Internet.

Mes	Descargados	Cargados	Ambas	Velocidad de Descarga	Velocidad de Carga
Sep. 2012	1,74 GB	583,50 MB	2,31 GB	2,34 kb/seg	786 bytes/seg
Oct. 2012	5,68 GB	914,58 MB	6.57 GB	2,22 kb/seg	358 bytes/seg
Nov. 2012	4,75 GB	845,53 MB	5,43 GB	2.17 kb/seg	613 bytes/seg

Tabla 3.13: Datos monitoredos por mes con BitMeter.

Fuente: Elaboración propia.

3.2.2. Análisis.

Se realiza el análisis, una vez recolectada la información con el análisis de monitoreo es necesario interpretarla para determinar el comportamiento de la Red y tomar decisiones adecuadas que ayuden a mejorar su desempeño, el proceso de análisis se realizo al comportamiento de lo siguiente.

3.2.2.1. Análisis del servicio de Internet.

Respecto al análisis del servicio de Internet se tomo en cuenta los datos obtenidos en el monitoreo del ancho de banda con usuarios y el consumo del mismo.

3.2.2.2. Análisis de ancho de banda real.

Se realizo el análisis del ancho de banda real sacando una muestra de datos de una semana del mes y su promedio respectivo de los meses de septiembre, octubre y noviembre datos reflejados en la tabla 3.11 y 3.12, de acuerdo a ello se muestra los siguientes gráficos.

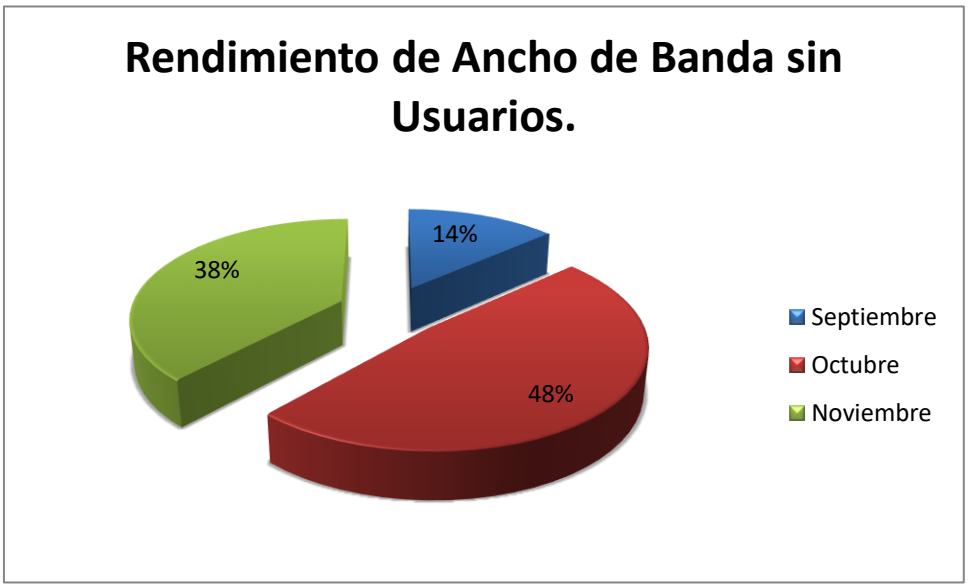


Grafico 3.4: Análisis de rendimiento de ancho de banda sin usuarios.

Fuente: Elaboración propia.

Grafico 3.5: Análisis de rendimiento de ancho de banda con usuarios.

Fuente: Elaboración propia.

Antes de la implementación con diagnostico de testeo de velocidad de ancho de banda se obtuvo un promedio respecto a la velocidad de 187,5 kbps y luego durante la administración y con la implementación del servidor MikroTik se obtuvo un promedio

respecto a la velocidad de 375.8 kbps, respecto a los meses descritos en la tabla 3.12, es decir en septiembre, octubre y noviembre, haciendo la diferencia respecto al diagnostico inicial de 188.3 Kbps, lo que significa que la velocidad de la navegación en Internet tuvo una gran mejoría.

3.2.2.3. Análisis de consumo de Internet.

El análisis de consumo de Internet se realizo con los datos obtenidos a través del software de monitoreo BitMeter, alcanzando un consumo de datos de descargas como se muestra en la siguiente grafica.

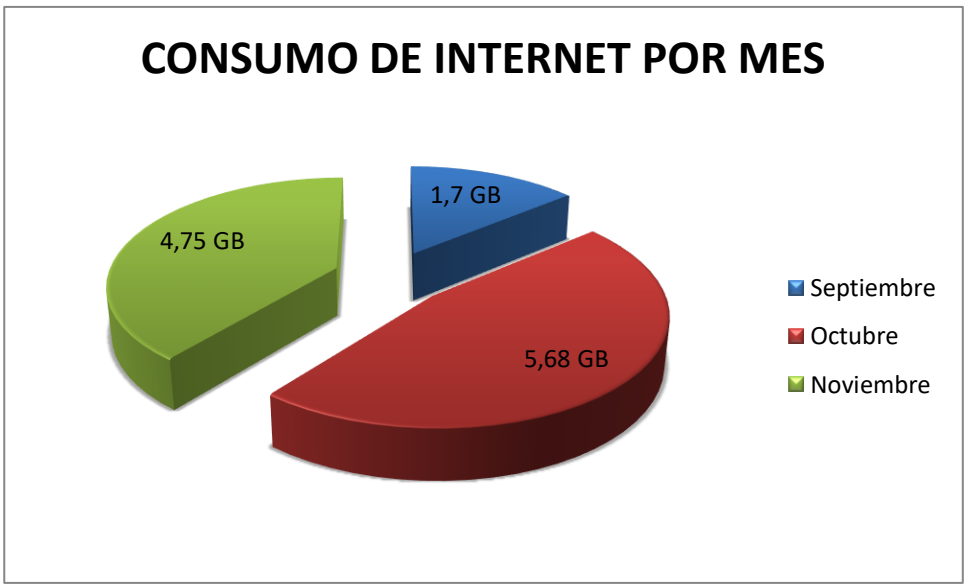


Grafico 3.6: Análisis de rendimiento de ancho de banda con usuarios.

Fuente: Elaboración propia.

3.2.3. Conclusión de administración de rendimiento.

Durante la fase de la administración del rendimiento se realizo actividades constantes como ser el monitoreo del servicio de Internet, haciendo el testeo en la medición de la velocidad del ancho de banda sin usuarios obteniendo como resultado el promedio 1109 Kbps de los meses monitoreados de septiembre, octubre y noviembre, también se obtuvo los datos del monitoreo con usuarios con un promedio de 595, 06 Kbps, se detalla también en la tabla 3.13 el monitoreo de cortes del servicio de Internet, monitoreo y control

de usuarios por Queues de MikroTik, monitoreo de consumo de ancho de banda con BitMeter, con sus respectivos análisis de datos.

3. 3. ADMINISTRACIÓN DE FALLAS.

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en el servicio de Internet y la red de datos. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

La administración de fallas también llamada asistencia técnica en el Trabajo Dirigido (Administración del Servicio de Internet del Campus Universitario de la U.A.P.), fue una actividad constante durante la ejecución del Trabajo Dirigido, para lo cual se administraron las siguientes actividades.

3.3.1. Corrección de fallas.

Es la actividad donde se recuperan las fallas y se plantean las soluciones para corregir el error en la red, PC, Switch, Servidor, RouterBoard, etc. para dar solución es necesario la asistencia técnica.

3.3.1.1. Asistencia técnica por fallas del servicio de Internet y de Red.

Existen un sin fin de problemas causados por la falla de conexión de la computadora con la red de datos, se mencionaran los más ocurridos durante la ejecución del Trabajo Dirigido en la USIC.

a) Configuración de IP`S.

Las configuraciones de IP`S en las computadoras de los usuarios se las realizo cada vez que el usuario lo requería, tanto como para asignar un IP a una maquina nueva dentro la red como para configurar el IP asignado a la máquina correspondiente, para así poder identificar cada uno de los equipos informáticos (computadoras) de los usuarios, esta configuración se realizo en el protocolo de red TCP/IP.

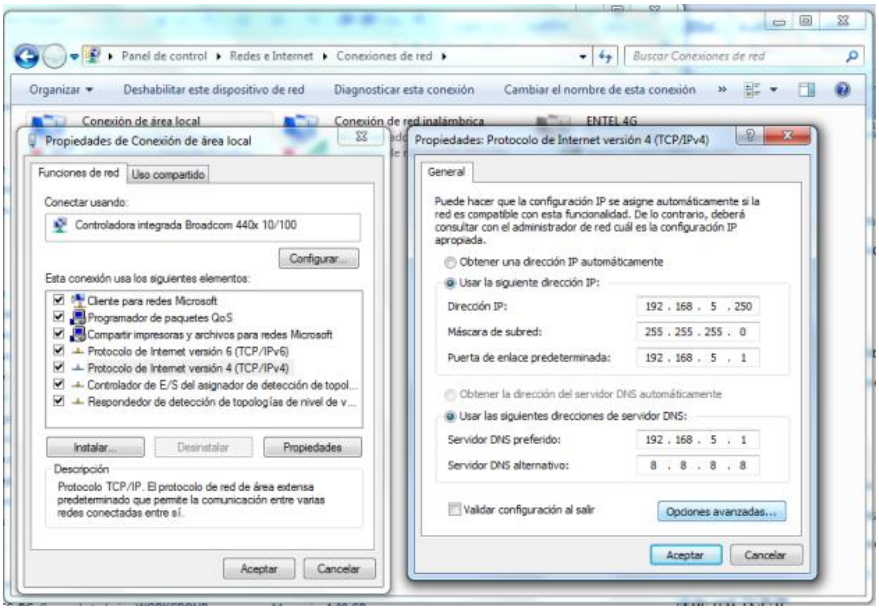


Figura 3.10: Ventana de configuración de protocolo TCP/IP.

Fuente: Elaboración propia.

b) Asistencia técnica de conexión a la Red.

La asistencia técnica de conexiones a la Red se realizó, verificando la duplicidad de IP, configurando las IP`S en las computadoras, configurando las tarjetas USB inalámbricas en la PC`S, adición de nuevos puntos en la Red, reemplazo de cableado en puntos existentes, verificación de conexión y comunicación de la computadora en la red, verificación del funcionamiento y estado de los puertos del Switch, verificación del funcionamiento y configuración de las antenas inalámbricas.

3.3.1.2. Asistencia técnica por fallas de conexión a Internet.

Se realiza en las computadoras de los usuarios que tienen permiso y acceso al servicio de Internet, se verifica la conexión a la Red ya sea por cableado o inalámbrico, la configuración del IP asignado y la MAC (dirección física del equipo) de la computadora a través del estado de conexión como se observa en la siguiente figura, para revisar la MAC y la dirección IP de la maquina y corroborar el registro de la misma en el Servidor y verificar que coincida con la dirección IP/MAC de la PC, se realiza pruebas de diagnóstico de conexión a Internet haciendo ping a www.google.com.bo y a la red haciendo ping a la dirección IP del Servidor y se verifica en cualquier navegador que tenga instalado la

computadora que realice una búsqueda de datos para confirmar que la falla se ha solucionado.

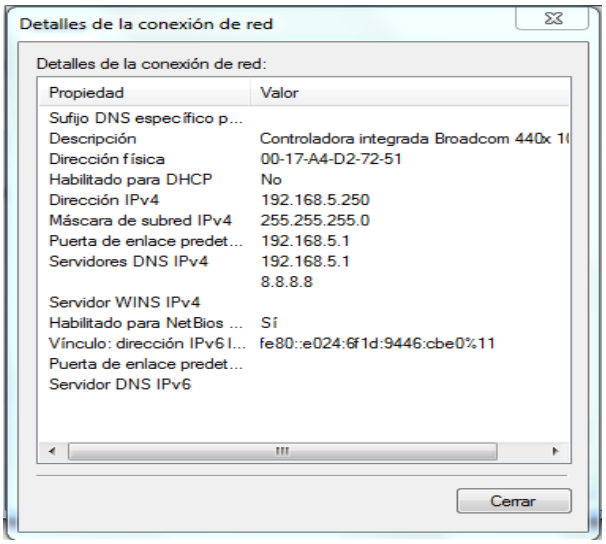


Figura 3.11: Ventana de verificación del Estado de conexión de la PC.

Fuente: Elaboración propia.

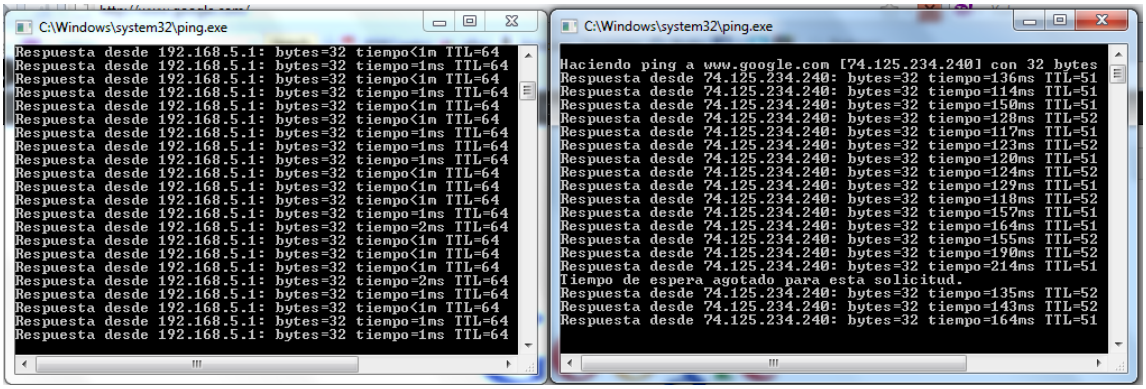


Figura 3.12: Ping de conexión al Servidor y a Internet www.google.com.bo.

Fuente: Elaboración propia.

3.3.3.3. Fallas con respecto a otros aspectos.

Aparte de las fallas ocurridas con el servicio de Internet y la Red de Datos durante el periodo del Trabajo Dirigido también se presentaron otras fallas con relación a otros aspectos una de ellas se da cuando ocurre cortes eléctricos el cual está fuera de nuestro alcance para dar una solución que provoca la inestabilidad de la Red, puertos de Switch quemados, antenas inalámbricas apagadas y otros como cortes del servicio de Internet que se da desde el Proveedor, etc.

3.3.3.4. Fallas Atendidas durante en Trabajo Dirigido.

Durante la ejecución del periodo de Trabajo Dirigido se realizo la asistencia técnica bajo los siguientes aspectos que el usuario requería.

A continuación se muestra la tabla y el grafico detallando el servicio técnico realizado en los diferentes meses siguiendo la ejecución del trabajo.

MES	ACTIVIDAD	Nº ATENDIDOS
Septiembre	Asistencia técnica por fallas de la Red de Datos.	8
	Asistencia técnica por fallas del servicio de Internet.	12
	Fallas con relación a otros aspectos	2
Casos atendidos en el mes de septiembre		**22**
Octubre	Asistencia técnica por fallas de la Red de Datos.	5
	Asistencia técnica por fallas del servicio de Internet.	9
	Fallas con relación a otros aspectos	1
Casos atendidos en el mes de octubre		**15**
Noviembre	Asistencia técnica por fallas de la Red de Datos.	6
	Asistencia técnica por fallas del servicio de Internet.	14
	Fallas con relación a otros aspectos	1
Casos atendidos en el mes de noviembre		**21**
Total de fallas atendidas		**58**

Tabla 3.14: Fallas atendidas de la Red de Datos y el servicio de Internet.

Fuente: Elaboración propia.

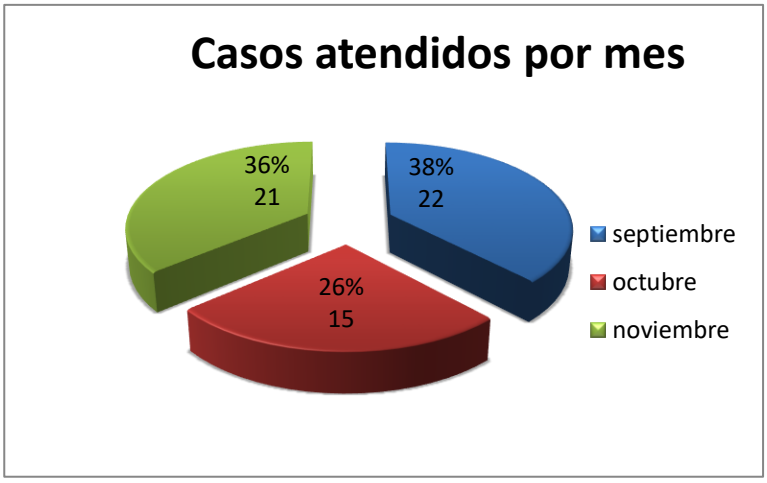


Grafico 3.7: Casos de fallas atendidos por mes.

Fuente: Elaboración propia.

El total de casos atendidos por distintas fallas en la Administración del servicio de Internet son 58 y observando el grafico se deduce que:

- El mes de Septiembre fue donde hubo más solicitudes de asistencia técnica por parte de los usuarios, donde se dio solución a los problemas producidos a un 38% de asistencia técnica realizada.
- El mes de Octubre se soluciono menos problemas a las solicitudes en un 26% de asistencia técnica a usuarios.
- El mes de Noviembre se soluciono más problemas debido a las solicitudes en un 26% de asistencia técnica a usuarios.

3.3.2. Conclusión de administración de fallas.

En la fase de administración de fallas se realizo la corrección de fallas presentadas durante el periodo de Trabajo Dirigido, los casos de asistencia técnica atendidos fueron por: fallas de servicio de Internet y la red, donde se realizo actividades contantes de configuración de IP`S a maquinas nuevas y formateadas que perdían su configuración asignada de IP`S o mala configuración de su IP asignado, monitoreo de conexión a la red verificando la configurando las IP`S, la duplicidad de IP, las tarjetas USB inalámbricas en la PC`S, etc. Otro de los casos atendidos fue por: fallas de conexión a Internet que se realizo con la observación del estado de conexión del adaptador de red para

confirmar que la configuración este correcta, luego se realiza ping de conexión servidor y al Internet y por último se hace la verificación y actualización del registro de la IP/MAC en el servidor, como resultado de la asistencia técnica se tiene un total de 58 casos atendidos satisfactoriamente brindando una buena atención eficiente al usuario.

3.4. ADMINISTRACIÓN DE LA SEGURIDAD.

Su objetivo es ofrecer seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para las respuestas a incidentes de seguridad.

En cuanto a la seguridad de la red se limito en la prevención de ataques, de intrusos (acceso de usuarios no permitidos), limitándonos a dar el permiso a la red con la asignación de IP`S a cada equipo e Internet a través del registro de usuarios en el ARP del MikroTik (amarre de IP/MAC del equipo), eso en cuanto a la red cableada e inalámbrica que conforman la red LAN del Campus, en cuanto al servicio de Internet de la zona WIFI_UAP, se tomo por seguridad la autenticación del usuario a través del servidor HotSpot, para evitar el ingreso de intrusos (personas ajenas a la Universidad), puesto que es un servicio que se da para Comunidad Universitaria.

3.4.1. Prevención de ataques.

Para la prevención de ataques al servidor MikroTik como estrategia se considero bloquear algunos puertos de entrada al servidor.

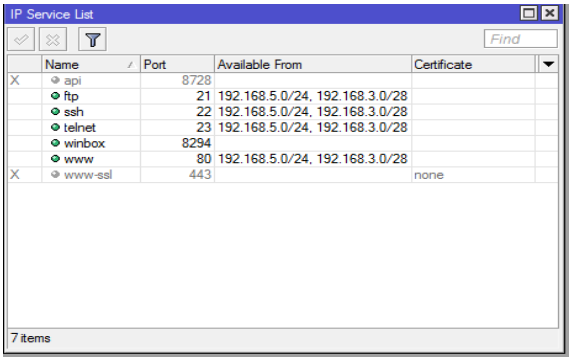


Figura 3.13: Bloqueo de puertos.

Fuente: Elaboración propia.

3.4.2. Detección de intrusos.

Para la detección de intrusos se monitoreo y logro mediante el mensaje del protocolo TCP/IP de red de duplicidad de IP´S, para confirmar el mensaje se realizo el escaneo de IP´S con el programa IPScan Software de escaneo de IP´S.

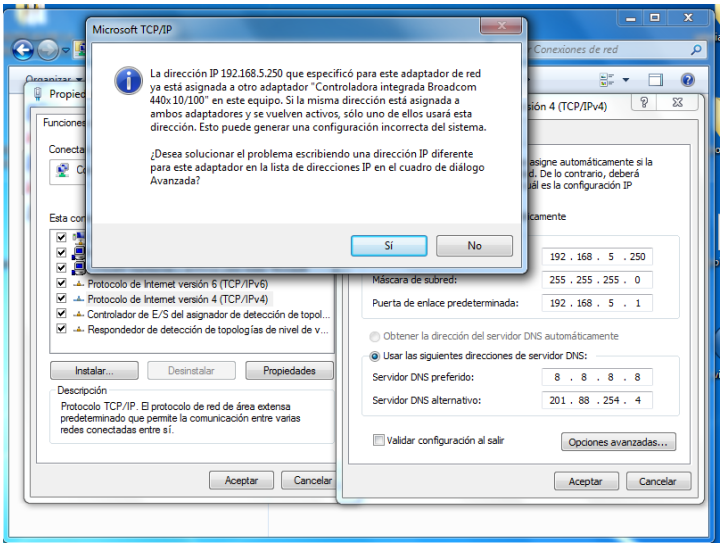


Figura 3.14: Mensaje del protocolo TCP/IP de red de duplicidad de IP´S.

Fuente: Elaboración propia.

3.4.3. Políticas de Seguridad.

Tomando en cuenta que en la USIC (Unidad de Sistemas de Información y Comunicación) no existían políticas de ningún tipo para la administración, se elaboro las siguientes Políticas de Uso para la administración del servicio de Internet.

- Políticas de uso de Internet.
- Políticas de cuentas de usuario.
- Políticas de configuración de ruteadores.
- Políticas de listas de acceso.
- Políticas de contraseñas.
- Políticas de respaldos.

Para ver los detalles de las políticas ver (Anexo D).

3.4.4. Servicios de seguridad.

Los servicios de seguridad implementados en la administración del servicio de Internet y la Red de datos son:

- **Confidencialidad:** Solo el administrador del servidor puede acceder a la información que se encuentre en el servidor.
- **Autenticación:** A través de la implementación del servidor HotSpot en el MikroTik para la Zona Wifi de la UAP y de amarre de IP/MAC en la red por cableado.
- **Integridad:** El servicio de integridad de los datos se da en el registro de los datos de usuarios bajo el formulario de registro de usuarios el cual es llenado por el mismo usuario y en el caso de usuarios de la zona Wifi bajo la fotocopia de la matrícula Universitaria.
- **Control de acceso:** El control de acceso al servicio de Internet se da por tipos de usuarios, los cuales son usuarios con privilegios y usuarios sin privilegios esto en la Red LAN y usuarios de la zona Wifi a través de la conexión inalámbrica.

3.4.5. Proceso.

Para la mejor administración de usuarios se elaboro procedimientos el cual fue mencionado en la fase de configuración en su subtitulo de políticas y procedimientos relacionados, para ver a mejor detalle ver (Anexo C).

3.4.6. Conclusión de administración de la seguridad.

En la fase de administración de seguridad se protegió al servidor con el bloqueo de puertos de conexión a la red (SSH,Telnet, etc.), la detección de intrusos a través del escaneo a la red con el software de escaneo IpScan, para proteger al usuario, dar seguridad de uso de Internet y manejo de la red se elaboraron políticas y procedimientos con las que no contaba la unidad al iniciar el Trabajo Dirigido lo que mejoro significativamente la administración y control de los usuarios, el servicio de Internet y el control de la red de datos.

CAPITULO IV
CONCLUSIONES Y RECOMENDACIONES

4. CONCLUSIONES Y RECOMENDACIONES.

4.1. CONCLUSIONES.

Como resultado obtenido a través de las actividades realizadas se ha llegado a las siguientes conclusiones:

- ✓ Como consecuencia del trabajo, se llego a la conclusión principal donde el servicio de Internet mejoro con la administración de la red de datos e Internet permitiendo el control de acceso de usuarios, regulando el ancho de banda, restringiendo páginas web, monitoreo y control del uso de internet, etc.
- ✓ La administración mejoro porque en el periodo del Trabajo Dirigido durante la administración de la configuración se realizo las actividades de planeación y diseño de la red, se realizo el diagnostico inicial y actual con una diferencia de rendimiento del servicio de Internet en el diagnostico actual del 21% al resultado del diagnostico inicial, se realizo configuraciones para la administración del servicio de Internet, como ser el servidor Web proxy para la restricción de páginas web con un total de 252 restricciones, el HotSpot para el ingreso por autenticación a la zona Wifi de la U.A.P. con un total de 109 usuarios registrados, el amarre de IP/MAC para dar acceso a Internet, los Queues para restricciones de ancho de banda por usuario, para el control y registro de usuarios se administro bajo el enfoque de gestión de calidad rigiéndonos únicamente en lo que concierne a procedimientos y políticas de uso,

- ✓ En la administración del rendimiento se realizo actividades constantes de monitoreo del servicio de Internet, haciendo el testeo de la velocidad del ancho de banda con y sin usuarios con promedios de velocidad en los meses de septiembre, octubre y noviembre de 1109 Kbps y 595,06 Kbps respectivamente, se detalla también el monitoreo de cortes del servicio de Internet, control de usuarios por Queues, monitoreo de consumo de ancho de banda con BitMeter de los meses mencionados anteriormente de 1.7Gb, 5.68Gb y 4.75Gb respectivamente.

- ✓ En la administración de fallas se realizo la corrección de fallas, los casos de asistencia técnica atendidos fueron por: fallas de servicio de Internet y la red, donde se realizo actividades contantes de configuración de IP`S, la verificación de la duplicidad de IP, las tarjetas USB inalámbricas, fallas de conexión a Internet que se realizo con la verificación y actualización del registro de la IP/MAC en el servidor, como resultado de la asistencia técnica se tiene un total de 58 casos atendidos satisfactoriamente brindando una buena atención eficiente al usuario.
- ✓ En la administración de seguridad se protegió al servidor con el bloqueo de puertos de conexión a la red (SSH, Telnet, etc.), la detección de intrusos con el software de escaneo IpScan, para proteger al usuario se elaboraron políticas y procedimientos con las que no contaba la unidad al iniciar el Trabajo Dirigido.

4.2. RECOMENDACIONES.

Concluido el Trabajo Dirigido se consideran las siguientes recomendaciones:

- ✓ Considerando una cantidad de 81 usuarios y tomando en cuenta que visitan diferentes o mismos sitios web, se recomienda realizar la investigación para la integración de un Servidor Cache al Mikrotik, para ganar ancho de banda mejorando la velocidad en las peticiones y respuestas del usuario la conexión a Internet.
- ✓ Considerando que existen usuarios que se dedican a realizar descargas o saturar el ancho de banda se recomienda realizar el Monitoreo de usuarios, abocado al ancho de banda, rendimiento de Internet, descargas de datos, logs de páginas visitadas, trafico de información, envió de paquetes, etc. Para tener el control del servicio en los usuarios y tomar decisiones apropiadas y fundamentadas.
- ✓ Considerando la inseguridad en la red de datos y tomando en cuenta el manejo del Sistema Siringuero en la red, se recomienda para evitar su vulnerabilidad incorporar un personal que se dedique a dar Seguridad en la red para optimizar todas las debilidades habidas y por haber.

REFERENCIAS Y BIBLIOGRAFÍA.

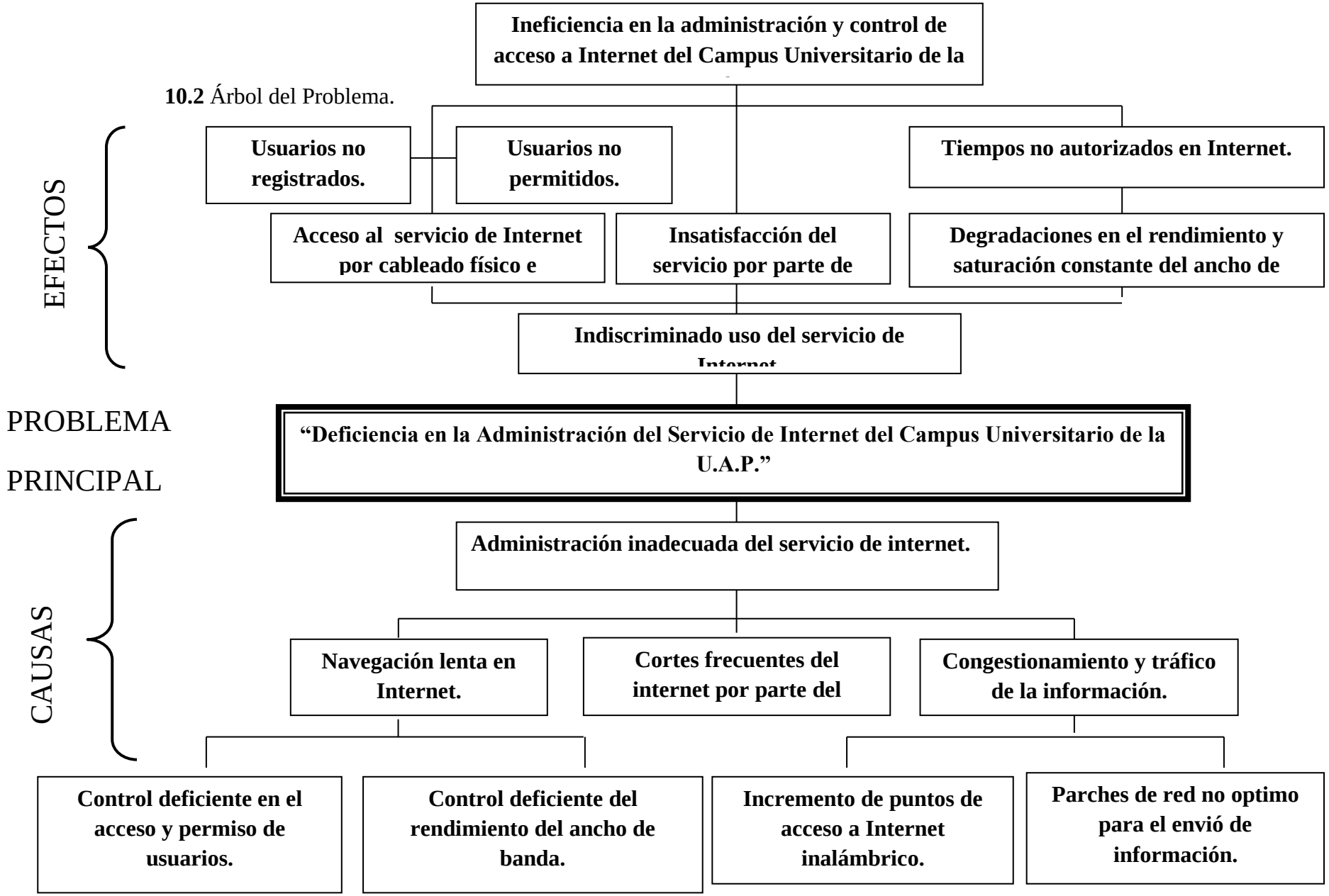
- Derfler , F. (1998). *Redes Lan & Wan.* Madrid, España: Prentice Hall.
- Huaygua, A. C. (2005). *Administracion de la Red de Datos e Internet.* Cobija - Pando.
- Mendez, A. A. (2011). *Implementacion de un servidor proxy para la administracion de la Red de Datos e Internet en el Consulado del Brasil en Cobija.* Cobija - Pando.
- Prudencio Nieves, J. (31 de Agosto de 2012). *Instituto de Educacion Superior Tecnologico privado "San Santiago" - ITSAN - Huaraz.* Obtenido de http://jcpn-itsan.blogspot.com.br/2012/08/administracion-de-redes.html
- Ramos, F. G. (03 de Octubre de 2011). *Tecnologias de la Informacion y la comunicacion Unidad III Internet.* Obtenido de Scrib: es.scribd.com
- Torrico, D. (2011). *Administracion de la Red de Datos e Internet del Gobierno Municipal de Cobija.* Cobija.
- Untiveros, s. (Julio de 2004). *Aprenda-Redes.* Obtenido de www.aprendaredes.com
- Zenteno, D. (2009). *Servidor de Administracion de ancho de Banda en la Universidad Amazonica de Pando.* Cobija - Pando.

Anexos

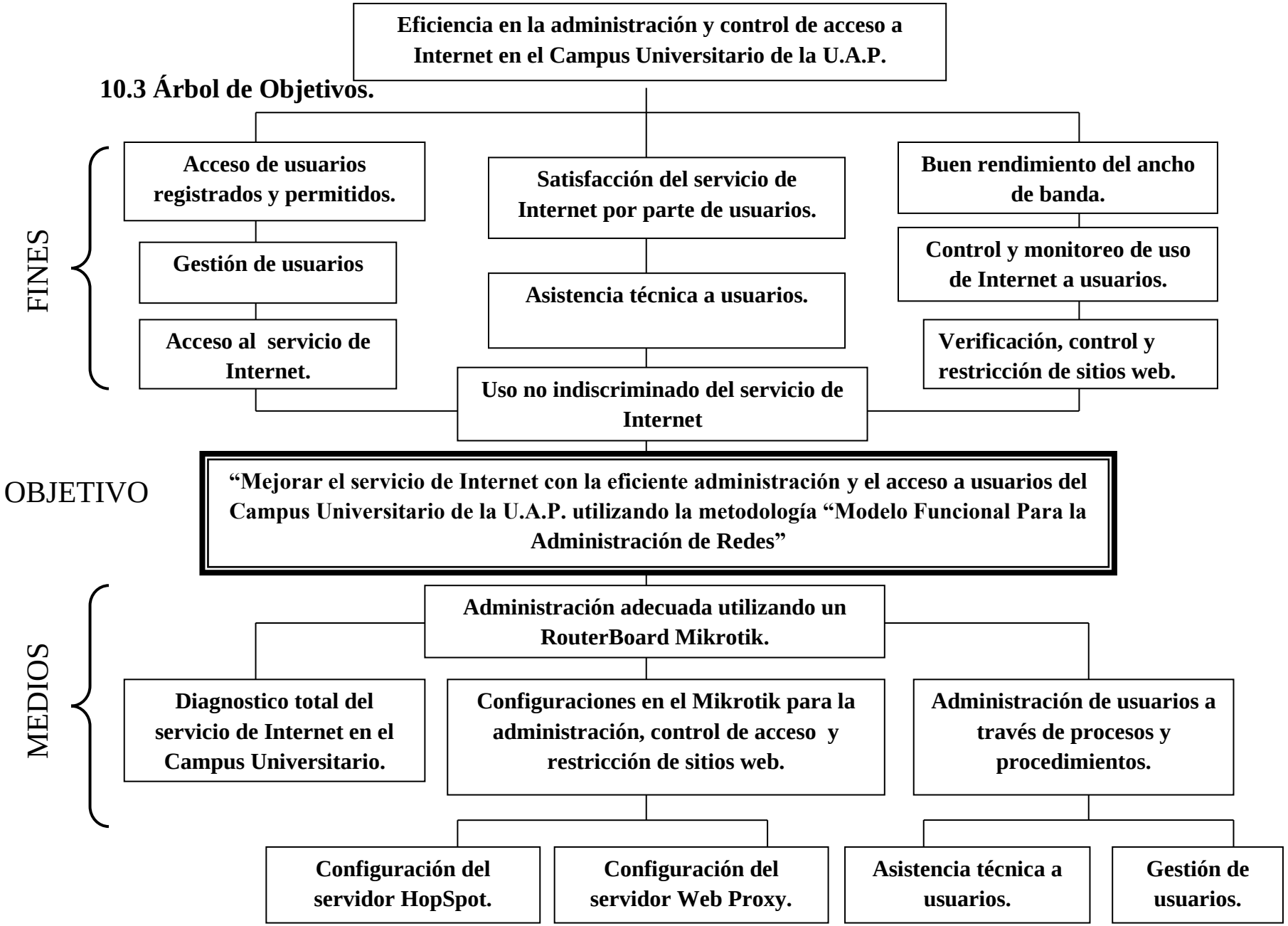
Anexo A

Árbol del problema y objetivos

10.2 Árbol del Problema.



10.3 Árbol de Objetivos.



Anexo B

Diagnostico del servicio de Internet

PREGUNTAS CONCERNIENTES AL SERVICIO DE INTERNET

Predio al que corresponde: ……..

1.- ¿Cuenta con el servicio de Internet?

En caso de responder no fin de la encuesta.

Si ◯ no ◯

2.- ¿Cuenta con asistencia técnica de alguna duda que tenga con el servicio de Internet?

Si ◯ no ◯

3.- ¿Con que finalidad utiliza el servicio de Internet?

d. Investigativo
e. Entretenimiento
f. otros

4.- ¿Qué tipo de servicio utiliza en Internet?

f. Correo electrónico
g. Video conferencia
h. chat
i. Descargas
j. Otros……

5.- ¿En qué horario utiliza con frecuencia el servicio de Internet?

d. Cuando hay necesidad
e. Horario especifico
f. En cualquier momento

6.- ¿Cómo calificaría al servicio de Internet de la UAP?

f. Excelente
g. Bueno
h. Regular
i. Malo
j. Pésimo

7.- ¿Sabe los tipos de virus que existe?

Si ◯ no ◯

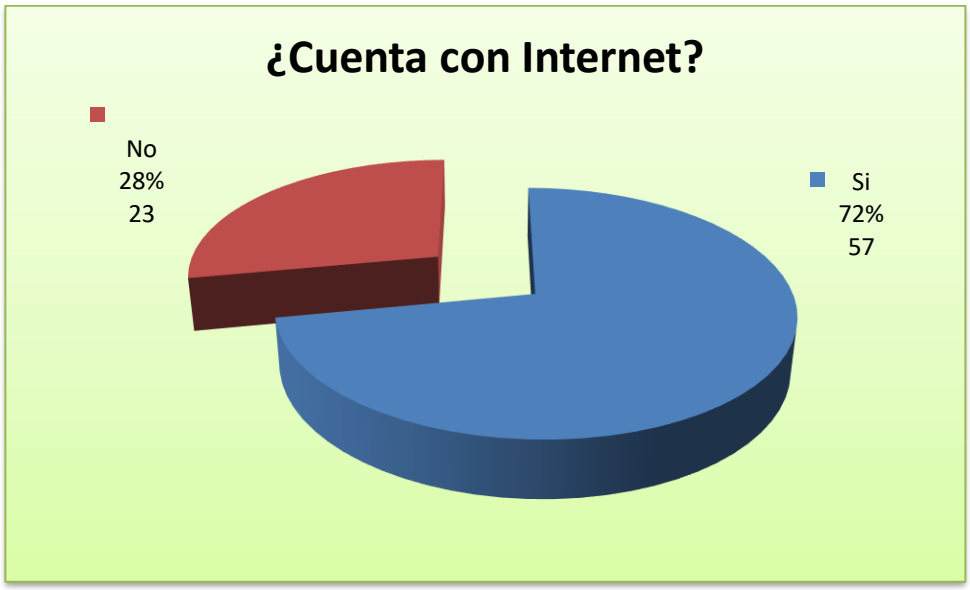
8.- ¿Desearía tener información sobre temas relacionado a los virus informáticos?

Si ◯ no ◯

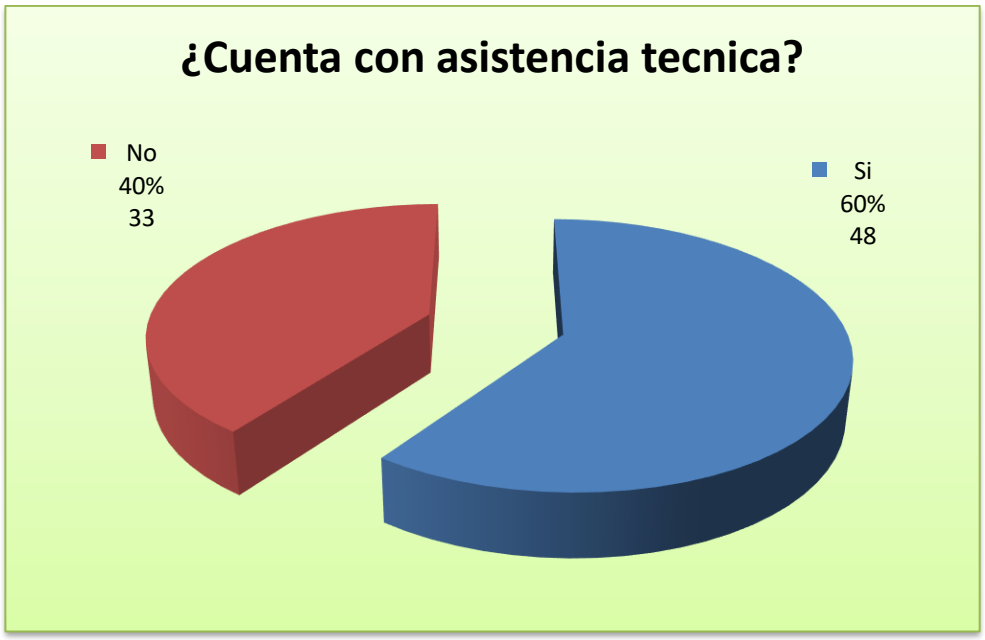
A continuación se observa el diagnostico realizada con respecto al uso de Internet, a los usuarios en el Campus Universitario de la U.A.P. cabe recalcar que los usuarios encuestados son 81 con tendencia incrementar.

PREGUNTAS CONCERNIENTES AL SERVICIO DE INTERNET

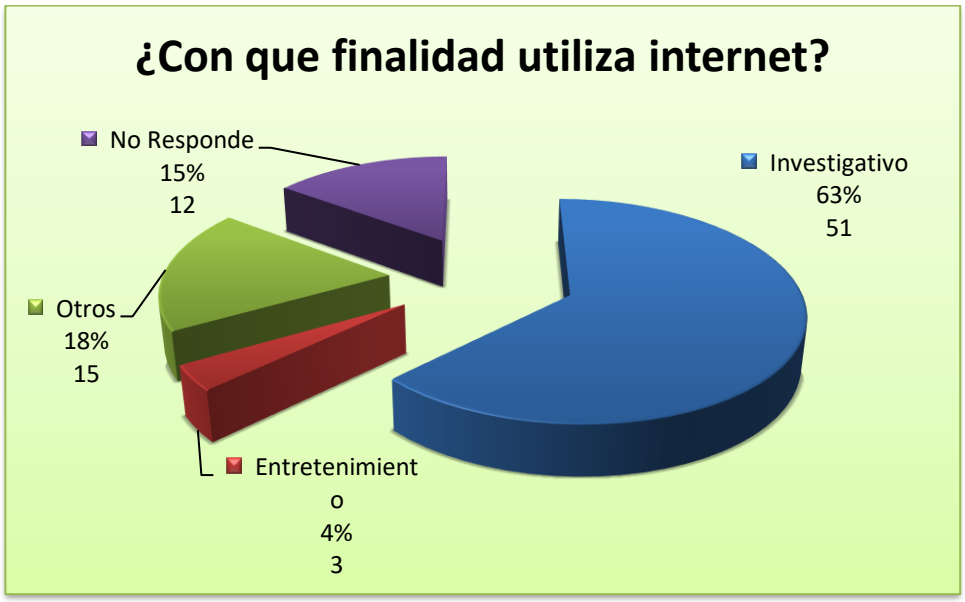
1.- ¿Cuenta con el servicio de Internet?



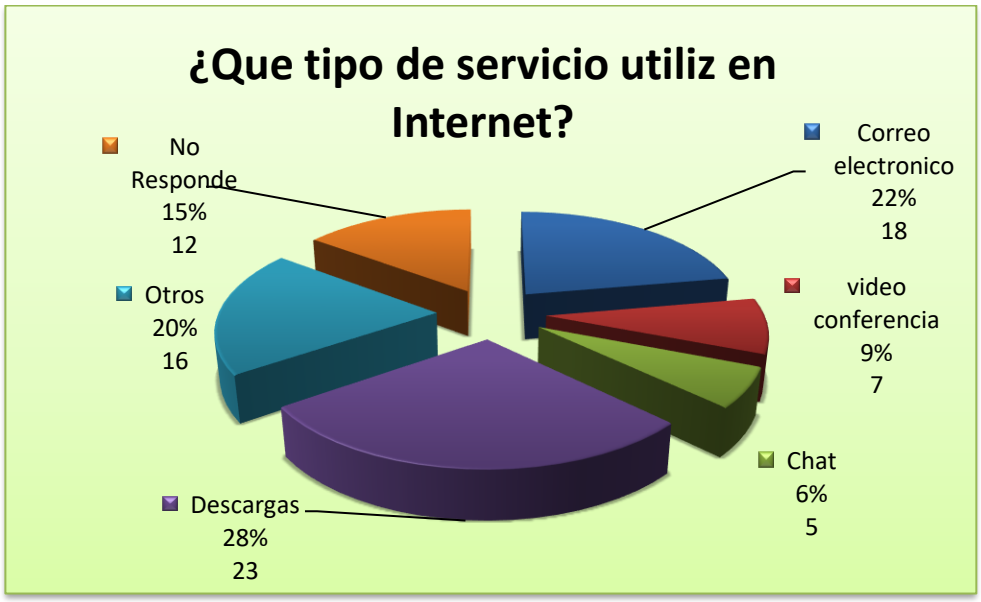
2.- ¿Cuenta con asistencia técnica de alguna duda que tenga con el servicio de Internet?



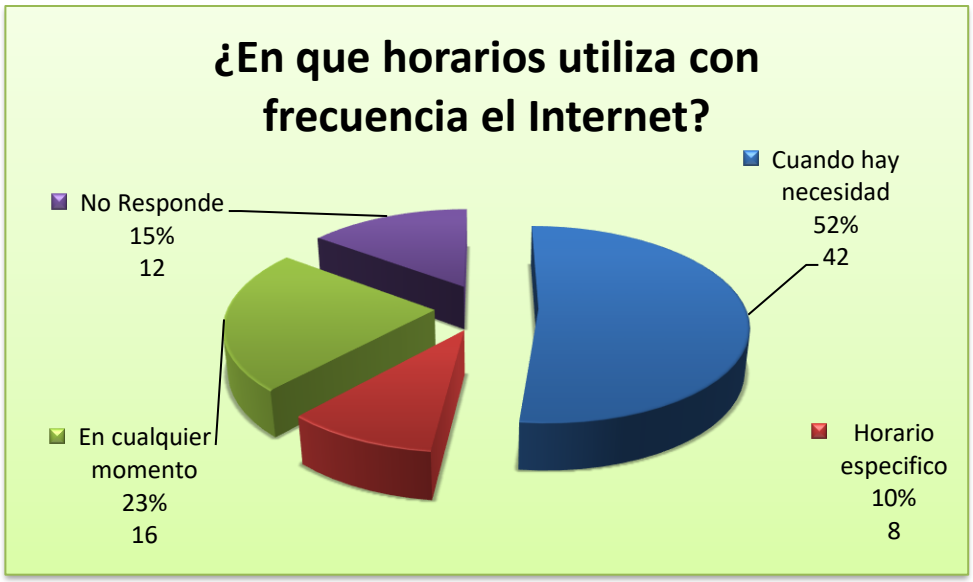
3.- ¿Con que finalidad utiliza el servicio de Internet?



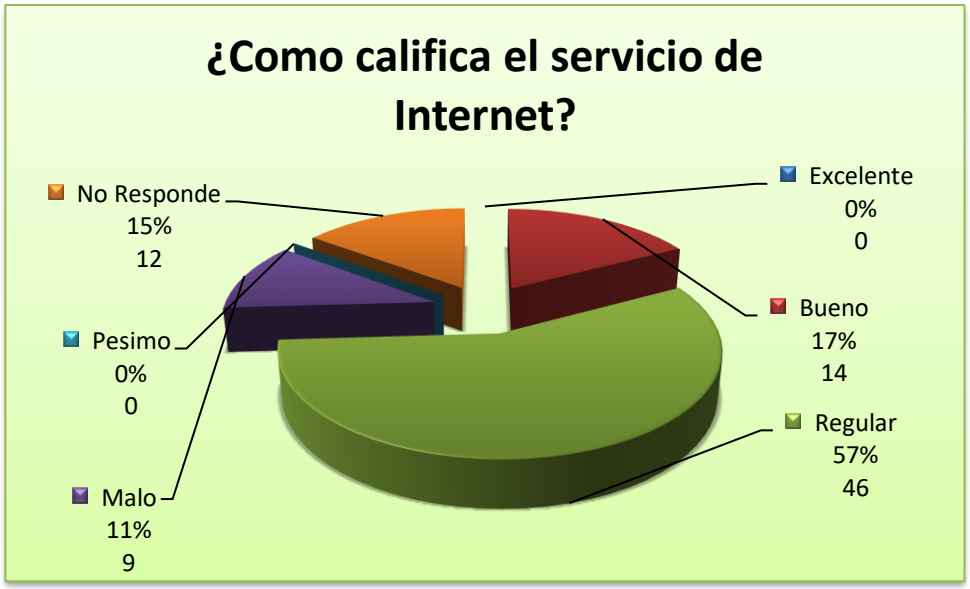
4.- ¿Qué tipo de servicio utiliza en Internet?



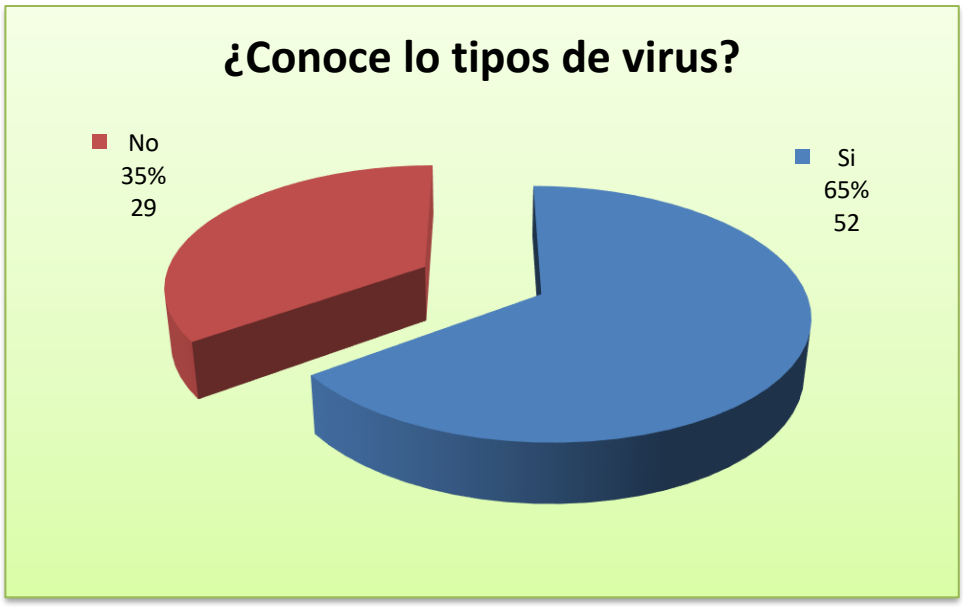
5.- ¿En qué horario utiliza con frecuencia el servicio de Internet?



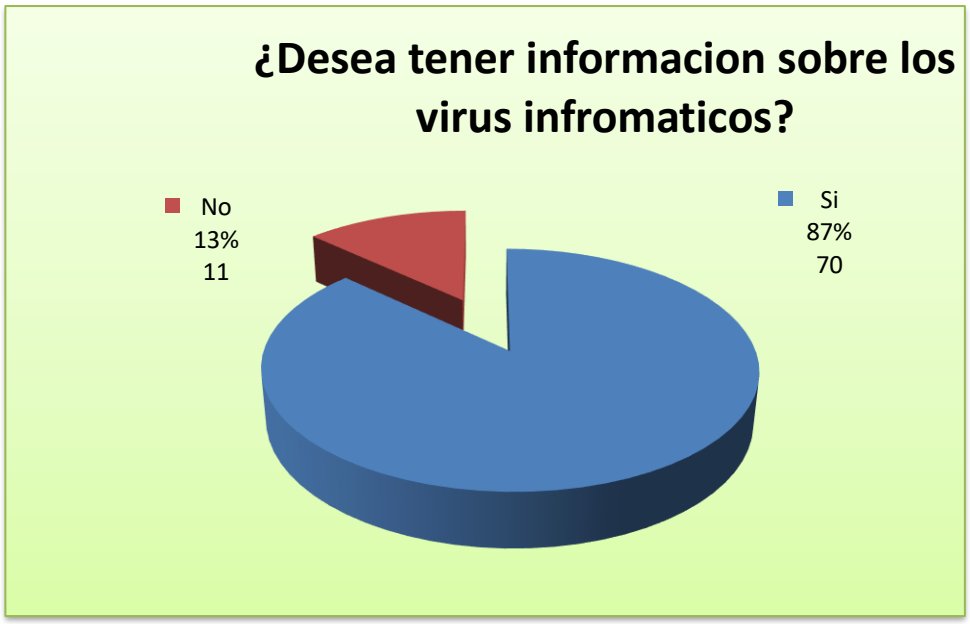
6.- ¿Cómo calificaría al servicio de Internet de la U.A.P.?



7.- ¿Sabe los tipos de virus que existe?



8.- ¿Desearía tener información sobre temas relacionado a los virus informáticos?



Conclusiones del diagnostico.

De acuerdo a los requerimientos que se obtuvo del levantamiento de la información se plantea lo siguiente.

- Mejorar el Servicio de Internet.
- Elaborar e implementar políticas de uso de Internet.
- Brindar asistencia técnica a los usuarios de forma rápida e inmediata.
- Reestructurar parcialmente la red de datos.

Anexo C

Procedimientos y formularios

Anexo D

Políticas

U.A.P.	UNIVERSIDAD AMAZÓNICA DE PANDO UNIDAD DE SISTEMAS DE INFORMACION Y COMUNICACIÓN – DRDI	POLITICAS USIC-001 VIGENCIA 16/09/12

POLÍTICAS DE GESTIÓN DE CALIDAD

POLÍTICA GENERAL

Las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos, es la primera línea de protección para el usuario. Una contraseña mal elegida o protegida puede resultar en un agujero de seguridad para toda la organización. Por ello, todos los usuarios de la red de la Universidad Amazónica de Pando son responsables de velar por la seguridad de las contraseñas seleccionadas por ellos mismos para el uso de los distintos servicios ofrecidos a la comunidad universitaria.
Todas las contraseñas de cuentas que den acceso a recursos y servicios de la Universidad Amazónica de Pando deberán seguir las siguientes directrices generales:

POLÍTICAS GENERAL DE CONTRASEÑAS

- Todas las contraseñas del servidor de la Red de Datos deben ser cambiados al menos una vez cada seis meses.
- Todas las contraseñas de usuario (cuentas de zonas Wifi, cuentas de administrador, etc…) deben ser cambiadas al menos una vez cada seis meses. Sin embargo, se recomienda cambiarla con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.
- Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica.
- Las contraseñas no deben ser almacenadas por escrito nunca.
- Las cuentas y contraseñas de U.A.P no deberán ser compartidos con nadie, incluyendo administrativos, secretarias, etc.
- Todas las contraseñas deben ser tratadas como información sensible y confidencial.

NOTA: El incumplimiento de la presente Política puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la Universidad Amazónica de Pando.
Será la USIC la que decida las acciones a tomar en el caso de incumplimiento de la presente política.

ELABORADO POR:	REVISADO POR:	APROBADO POR:

U.A.P.	**UNIVERSIDAD AMAZÓNICA DE PANDO** **UNIDAD DE SISTEMAS DE INFORMACION Y COMUNICACIÓN – DRDI**	**POLITICAS** **USIC-001** **VIGENCIA** **16/09/12**

POLÍTICAS DE GESTIÓN DE CALIDAD

POLÍTICA GENERAL

La gestión de cuentas de usuarios es una parte critica en el mantenimiento de la seguridad, se declara que todo usuario de la institución deberá poseer una **cuenta de usuario** personal, que actuará como una credencial que lo identifique unívocamente, y que le permitirá tener acceso a los recursos de la red informática institucional. El usuario deberá señalar quién es (identificación), y luego deberá comprobar que es quien dice ser (autenticación). La identificación se realizará normalmente por un "Código de Usuario". La autenticación se realizará mediante algo que sólo el usuario conoce (Contraseña) y/o algo que sólo él posee.

POLÍTICAS DE CUENTAS DE USUARIOS

- Todas las cuentas de usuarios son generadas a partir de la solicitud de uso del servicio del Sistema de Información, Internet u otro recurso que requiera el acceso por autenticación de usuario.
- Toda cuenta de usuario generada para el servicio de Internet en la Zona Wifi, debe ser a través del procedimiento de registro de usuario y el llenado del formulario de usuario.
- Deberán tener cuentas de usuarios del servidor de administración de la red de datos e Internet solo el personal autorizado como el administrador y jefe de unidad.
- Las cuentas de usuarios serán generadas de acuerdo al nivel de cada usuario y el rol que desempeña en la institución.
- Las cuentas de usuarios no deben ser almacenadas por escrito nunca.
- Las cuentas de usuarios de U.A.P no deberán ser compartidos con nadie, deben ser tratadas como información sensible y confidencial de cada usuario.

NOTA: El incumplimiento de la presente Política puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la Universidad Amazónica de Pando.
Será la USIC la que decida las acciones a tomar en el caso de incumplimiento de la presente política.

ELABORADO POR:	REVISADO POR:	APROBADO POR:

U.A.P.	**UNIVERSIDAD AMAZÓNICA DE PANDO** **UNIDAD DE SISTEMAS DE INFORMACION Y COMUNICACIÓN – DRDI**	**POLITICAS** **USIC-001** **VIGENCIA** **16/09/12**

POLÍTICAS DE GESTIÓN DE CALIDAD

POLÍTICA GENERAL

En la DRDI (División de Redes de Datos e Internet) dependiente de la USIC (Unidad de Sistemas de Información y Comunicación) se establece las políticas para efectuar los respaldos en servidores, equipos y unidades de almacenamiento, de la información, programas, bases de datos y otros como medida de seguridad básica.
Estos no aplicarán para la restauración de archivos de paquetería Office por corrección de versiones o eliminación.

POLÍTICAS DE RESPALDOS

- Se establece la responsabilidad de la DRDI para efectuar respaldo de información en servidores, así como la asistencia a usuarios bajo Requerimiento para la información correspondiente al equipo asignado.
- La DRDI es responsable exclusivo de realizar los respaldos correspondientes a configuración, información, estructura de datos y bases de datos localizado en los servidores dentro de la Red.
- La DRDI es responsable de realizar un respaldo incremental semanal de las configuraciones en los servidores.
- Todos los respaldos efectuados se conservarán bajo custodia del jefe de la unidad dependiente.

NOTA: El incumplimiento de la presente Política puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la Universidad Amazónica de Pando.
Será la USIC la que decida las acciones a tomar en el caso de incumplimiento de la presente política.

ELABORADO POR:	REVISADO POR:	APROBADO POR:

U.A.P.	**UNIVERSIDAD AMAZÓNICA DE PANDO** **UNIDAD DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN – DRDI**	**POLÍTICAS** **USIC-001** **VIGENCIA** **16/09/12**

POLÍTICAS DE GESTIÓN DE CALIDAD

POLÍTICA GENERAL

La configuración de los Routers es importante dentro de la Red de Datos para lo cual se estipula que los ruteadores de cualquier modelo y tipo de marca con el que cuenta la unidad deberán ser configurados para uso exclusivo dentro de la red como repetidores de señal o ruteadores para dar acceso a Internet.

POLÍTICAS DE RUTEADORES

- Se deberán configurar como repetidores de señal a todos los Routers que formen parte de la Red Lan interna de la U.A.P.
- Se deberán configurar los Routers como ruteadores solo en caso de eventos que requieran de conexión a Internet con zonas Wifi y habilitar durante el periodo de realización del evento.
- El nombre de los Routers de acuerdo que predio que pertenezca deberá ser seguido del símbolo (_) y de la palabra UAP escrito con mayúscula.
- Se designaran IP´S a los Routers para que formen parte de la red Lan interna.

NOTA: El incumplimiento de la presente Política puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la Universidad Amazónica de Pando.
Será la USIC la que decida las acciones a tomar en el caso de incumplimiento de la presente política.

ELABORADO POR:	REVISADO POR:	APROBADO POR:

U.A.P.	**UNIVERSIDAD AMAZÓNICA DE PANDO** **UNIDAD DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN – DRDI**	**POLÍTICAS** **USIC-001** **VIGENCIA** **16/09/12**

POLÍTICAS DE GESTIÓN DE CALIDAD

POLÍTICA GENERAL

La Universidad Amazónica de Pando, ofrece el servicio de Internet a todo el personal y alumnos que lo soliciten, en la medida de los accesos disponibles. La utilización de estos recursos por personas ajenas a la misma queda terminantemente prohibida, deberán cumplirse todas las normas específicas dictadas por la DRDI dependiente de la USIC.

Dichas normas se comunicarán por los diferentes medios disponibles, e incluso directamente a los interesados.

POLÍTICA DE USO DE INTERNET

- El servicio de Internet está destinado a mejorar el desenvolvimiento laboral y académico, además del acceso a información científica, técnica u otra temática relativa a la universidad.
- Los usuarios del servicio de Internet, estarán sujetos al monitoreo por parte del responsable de la red de datos y el servicio de Internet, a través del servidor proxy cuya función principal es registrar los accesos a páginas de Internet (web).
- Es indispensable que se utilice el servicio de Internet para propósitos que puedan influir positivamente en la imagen de la universidad o de sus autoridades y personal de la institución.
- Está prohibido el acceso y propagación de material con contenido pornográfico o ilegal.
- Está prohibido el bajar archivos de video y música, a no ser que se utilicen para una función determinada de la universidad y que este con autorización previa del Responsable del DRDI.
- Está prohibido el infiltrarse a los equipos teleinformáticas (switch, router, servidor proxy, etc.) de manera indebida y que puedan ocasionar alteraciones en la configuración además de conflictos.
- Está estrictamente prohibido cualquier uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral o educativo que dio origen a la habilitación del servicio.

NOTA: Las políticas de uso del servicio de Internet serán aplicados a todos los usuarios de la comunidad universitaria con acceso a Internet de los predios del Rectorado, Vicerrectorado y el Campus universitario.

ELABORADO POR:	REVISADO POR:	PROBADO POR:

POLÍTICAS DE GESTIÓN DE CALIDAD

POLÍTICA GENERAL

El propósito de esta política es establecer normas que aseguren los tipos de acceso al servicio de Internet, para facilitar sus labores con el buen funcionamiento del Internet.

POLÍTICAS DE CUENTAS DE USUARIOS

- Todas las listas de acceso son generadas a partir de la solicitud de uso del servicio de Internet que de acuerdo al rol y la jerarquía de trabajo se habilita bajo las siguientes listas de acceso:
- Usuarios con privilegios, solo para jefes de unidad y directores.
- Usuarios sin privilegios, para técnico y demás usuarios del Internet.
- Usuarios de zona Wifi, para universitario y la comunidad universitaria en general.

NOTA: El incumplimiento de la presente Política puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la Universidad Amazónica de Pando.
Será la USIC la que decida las acciones a tomar en el caso de incumplimiento de la presente política.

Anexo E

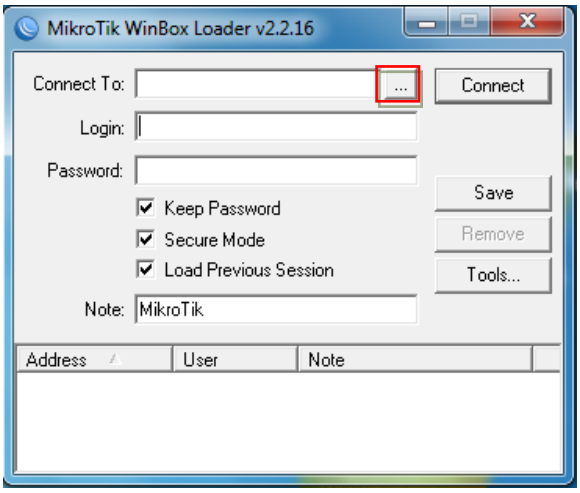
Manual de Usuario

Manual de Usuario de MikroTik RouterOS

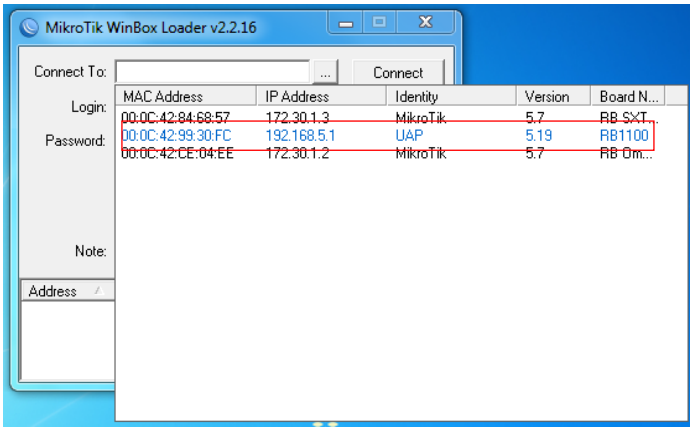
MikroTik RouterBoard es un Sistema Operativo muy complejo, que nos facilita en la administración de redes pequeñas o grandes.

Winbox es un software propio de MikroTik que nos facilita el ingreso al RouterOS y ver sus herramientas a través de su interfaz grafica, como verán enseguida el icono de acceso de Winbox.

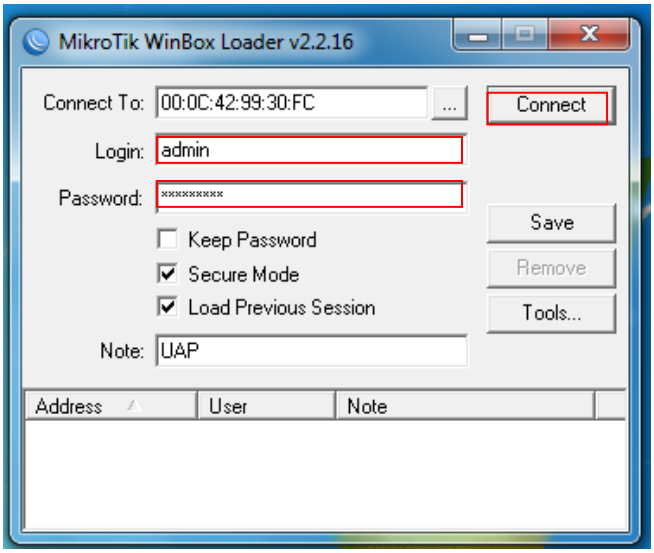
Al hacer doble clip en el icono nos muestra la siguiente ventana en la cual seleccionamos donde (…).



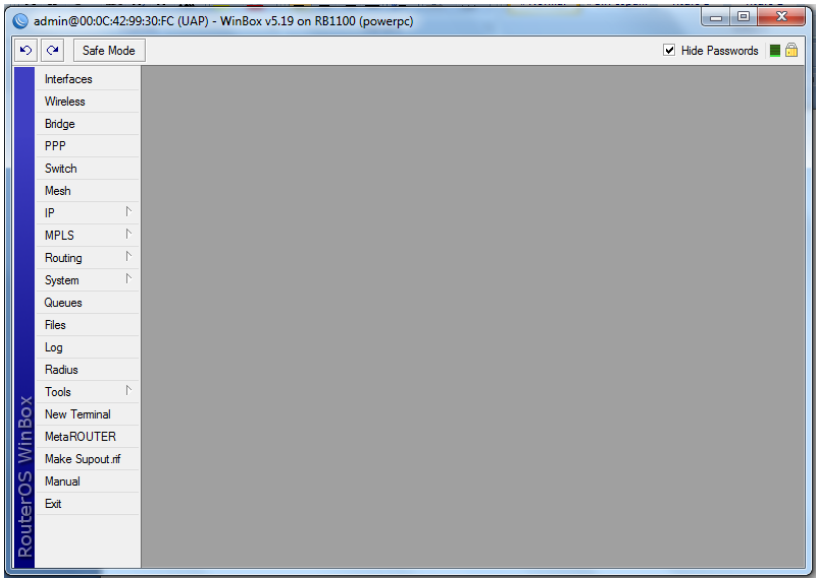
Nos muestra una lista en el que seleccionamos la y IP o MAC de nuestro servidor.



En **login** ponemos el nombre del usuario y en **password** el password del usuario luego hacemos clip en **connect**.



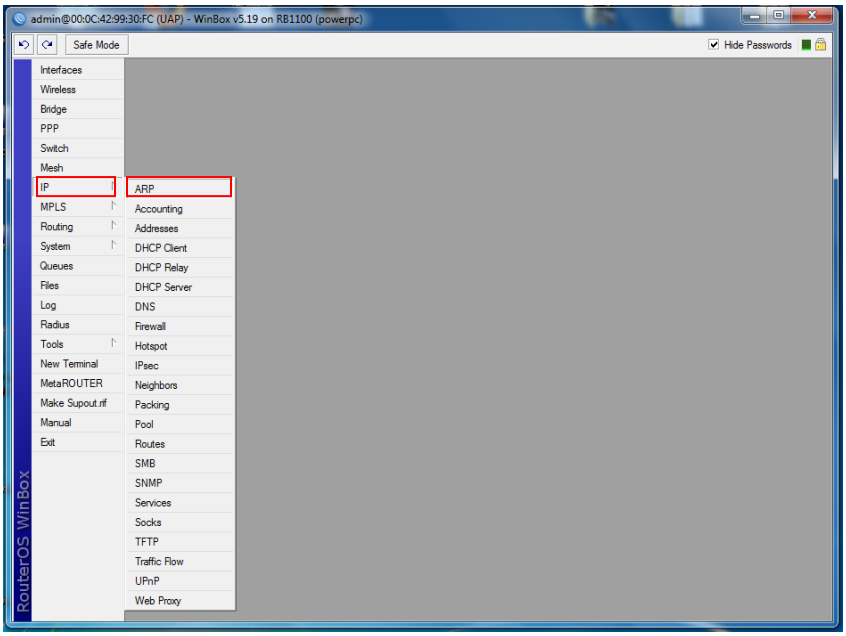
Entrando a la pantalla principal del MikroTik.



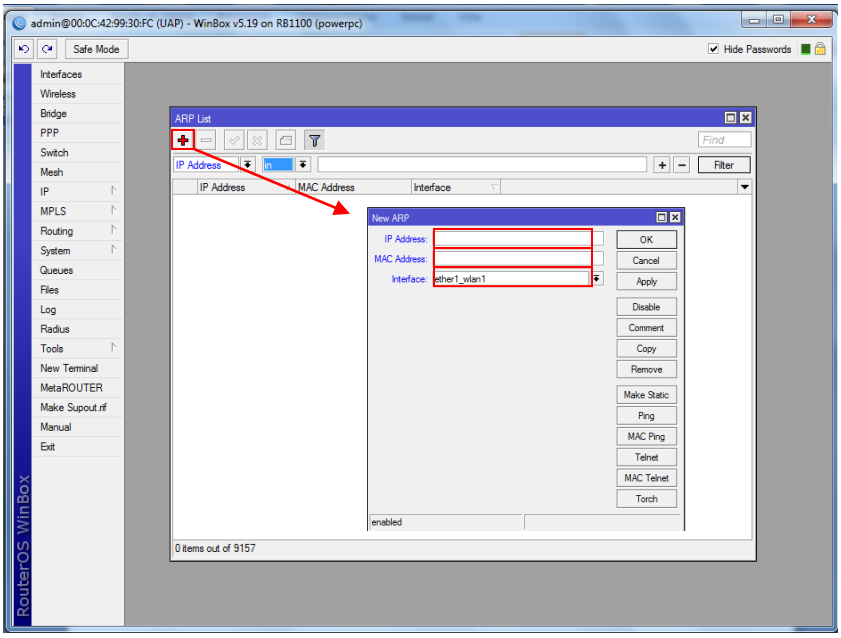
Este manual de usuario nos sirve para administrar usuarios en ARP, en HOTSPOT, QUEUES, y restricción de páginas web en WEB PROXY.

Administración de ARP.

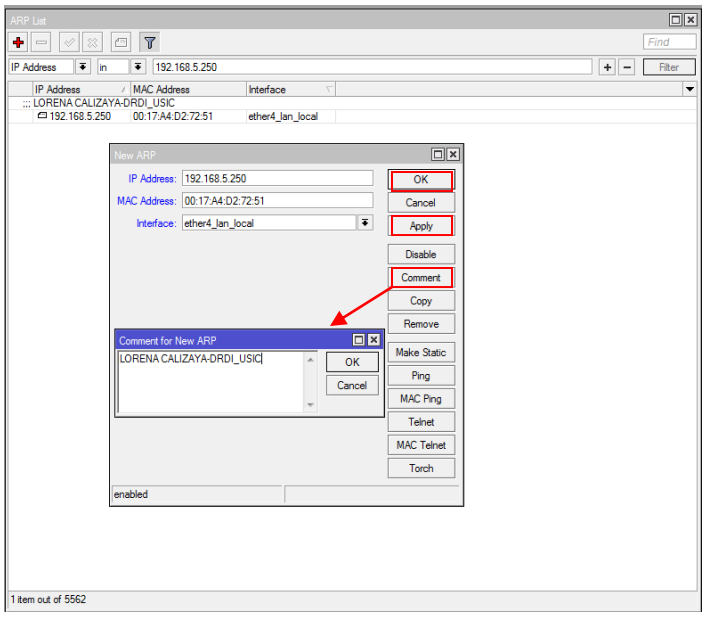
Seleccionamos la pestaña **IP** luego **ARP.**



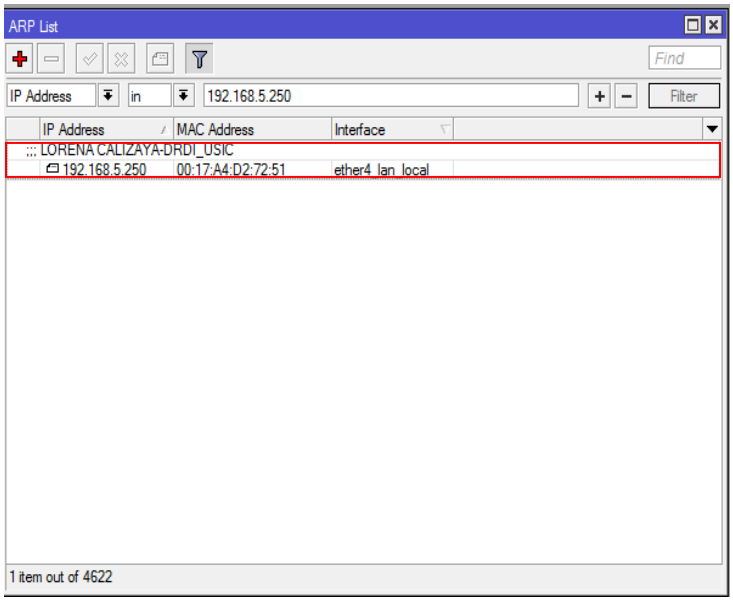
Hacemos clip en ARP y luego nos aparece la siguiente pantalla donde cliqueamos en (+) y luego registramos la **IP** y **MAC** del equipo y seleccionamos la **Interfaz** de nuestra red.



Una vez registrado la dirección IP, MAC y seleccionada la interfaz agregamos o no un **comment** (comentario) y luego cliqueamos **apply** y **ok.**

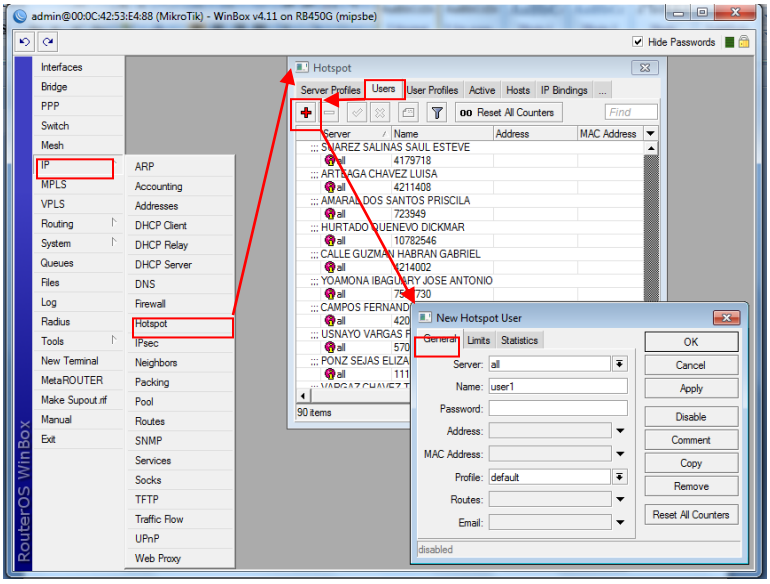


Si el procedimiento se realizo correctamente el registro se grabara y tendremos la siguiente pantalla con el primer usuario registrado en nuestro ARP.

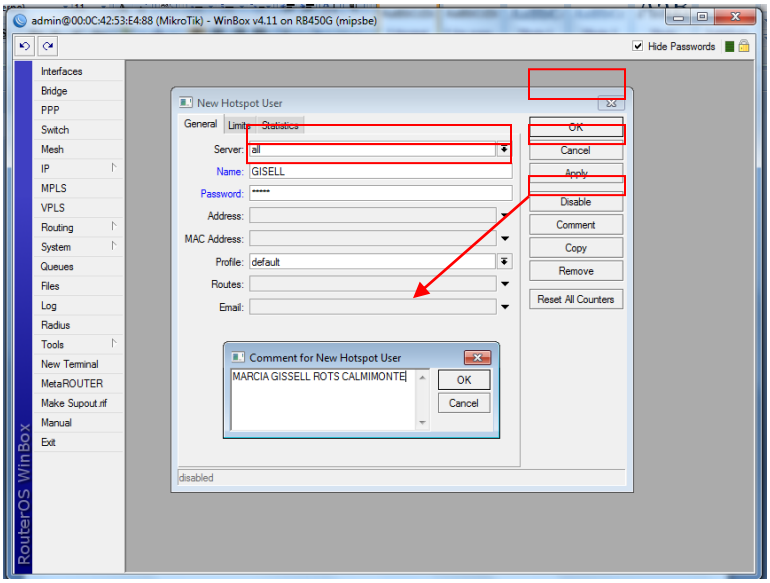


Administración de HotSpot

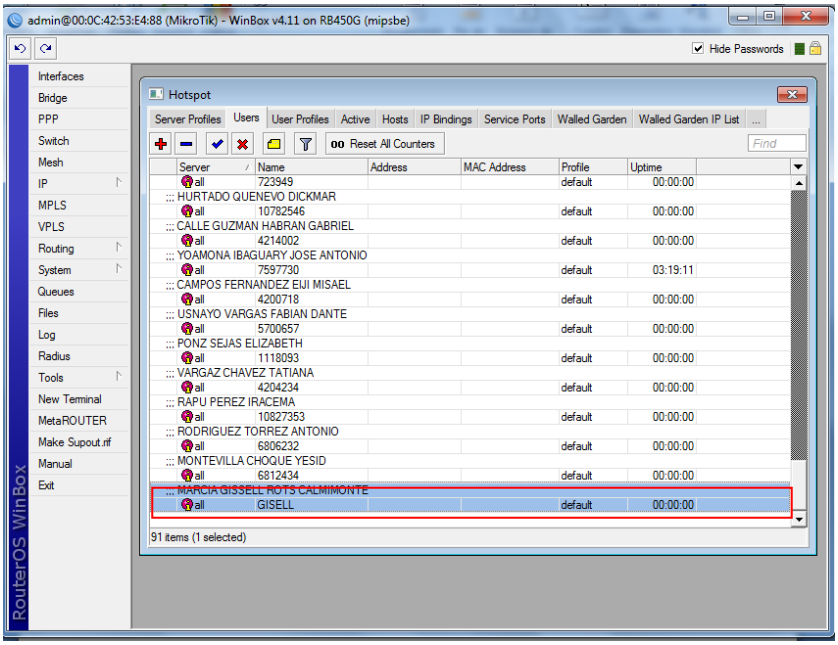
Seleccionamos la pestaña **IP** y luego **HotSpot hacemos** doble clip y nos muestra la ventana de **HotSpot**, seleccionamos **Users** y le damos doble clip al icono **(+)** y nos aparece la pantalla de registro de usuarios donde seleccionamos la pestaña **General** como se muestra en la siguiente figura.



Una vez en la pantalla de registro de usuario agregamos en **Name** el nombre de usuario y en **Password** el password del usuario y agregamos un comentario en **Comment** para identificar al usuario, luego aplicamos para grabar el registro en el servidor en **Apply** y O**k.**

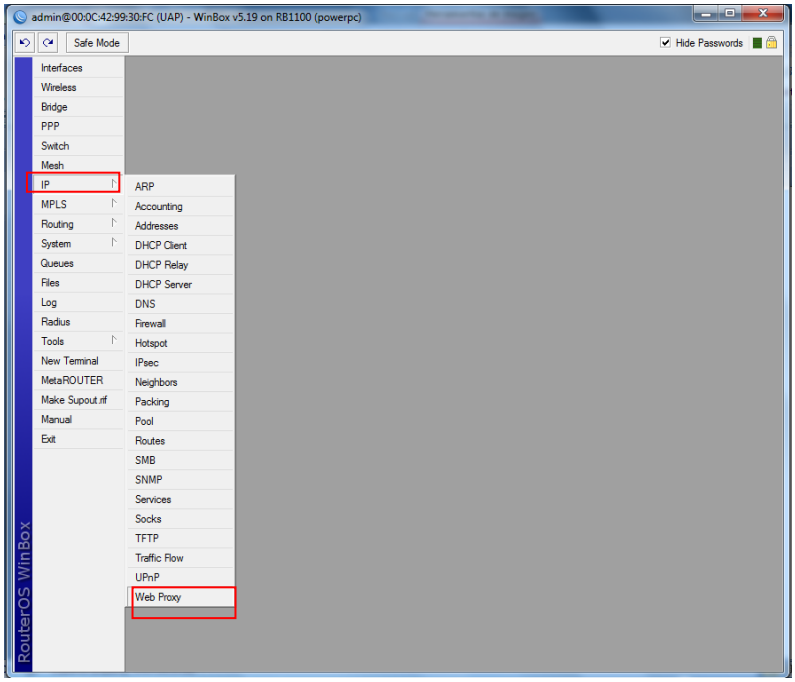


Al finalizar el proceso de registro se mostrara al usuario registrado en la lista de usuarios para ser autenticados y permitidos a navegar a Internet como se observa en la siguiente figura.

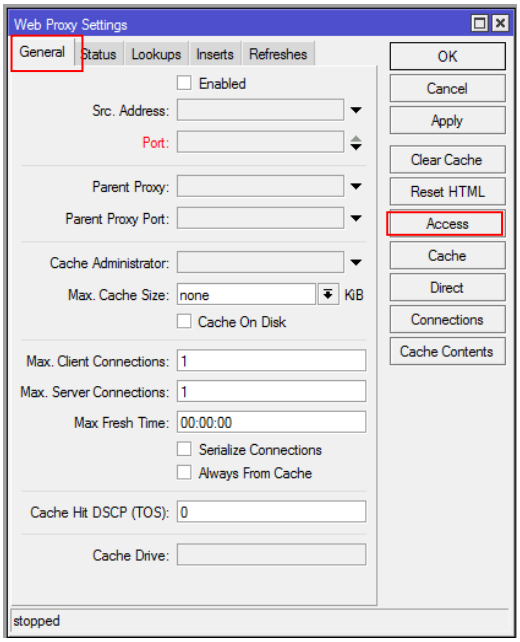


Administración de Web Proxy

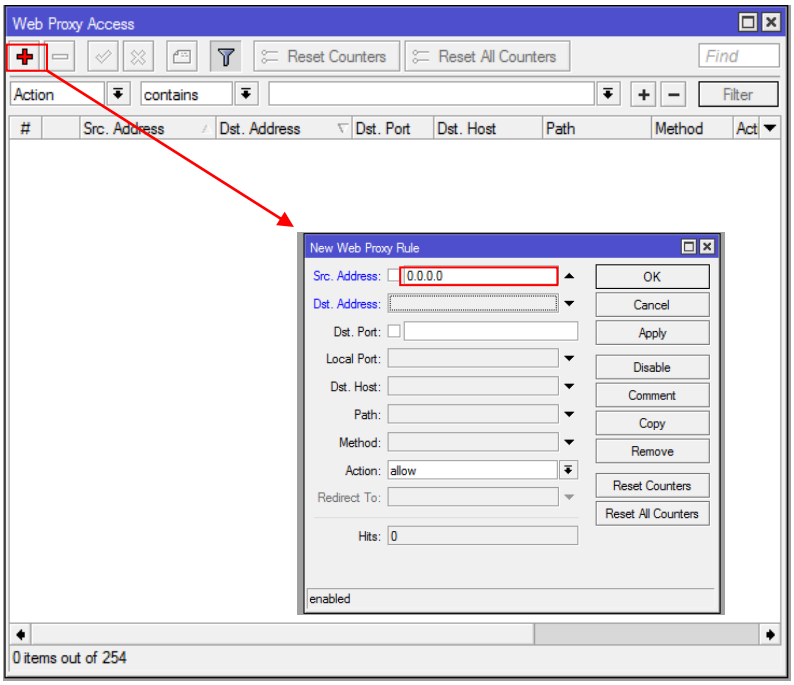
Seleccionamos la pestaña **IP** luego **Web Proxy** y hacemos doble clip.



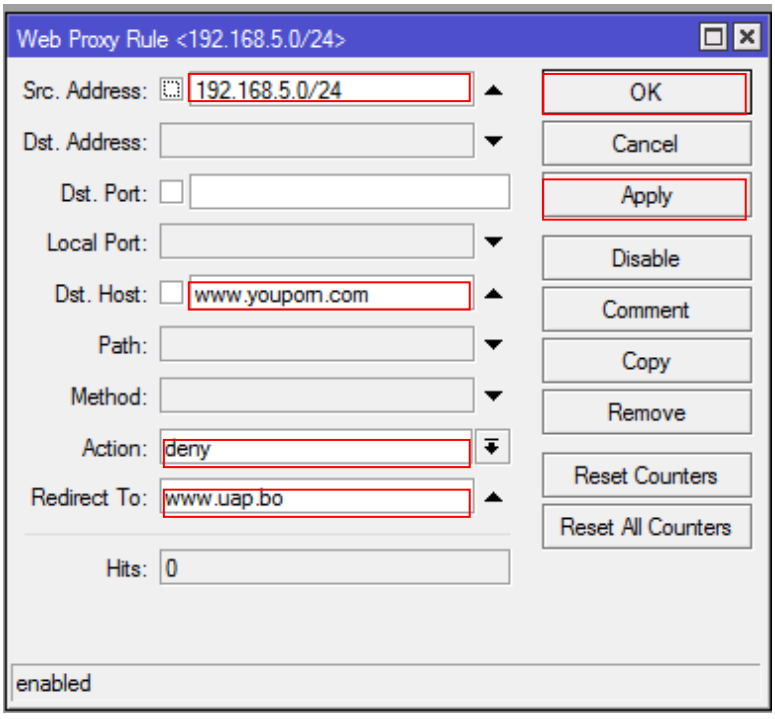
En la pantalla seleccionamos **General** y luego doble clip en **Access** como se observa en la siguiente figura.



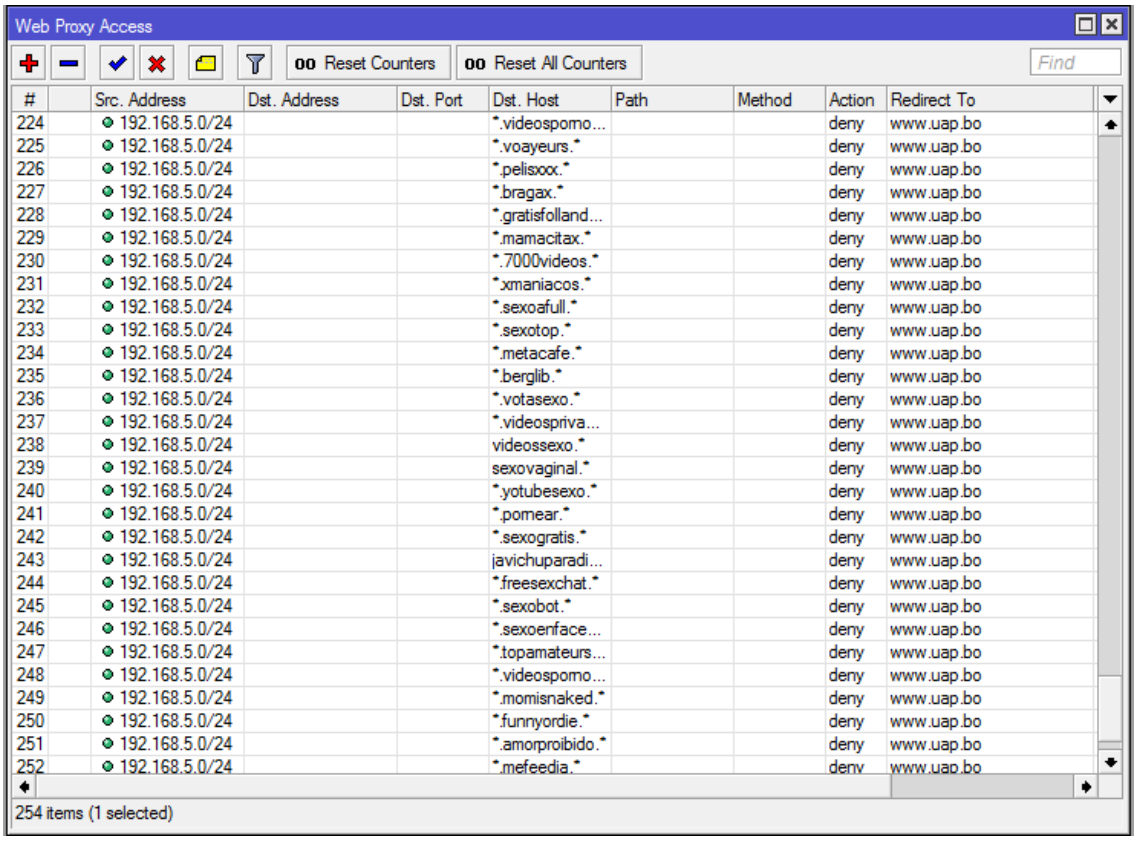
Una vez dentro en Access hacemos doble clip en (+) y nos aparecerá una nueva ventana.



Introducimos el número de **IP** a restringir en **Src. Address**, luego en **Dst. Host** ponemos la dirección web a ser restringido, en **Action** seleccionamos **deny** y en **Redirect To** ponemos la dirección Web de la pagina que será cargada en lugar de la pagina restringida y hacemos doble clip en **Apply** y **ok.**



depues de realizar todo el procedimiento como resultado obtendremos la lista de paginas web restringidas y redireccionada a la pagina web nuestra Universidad www.uap.bo.



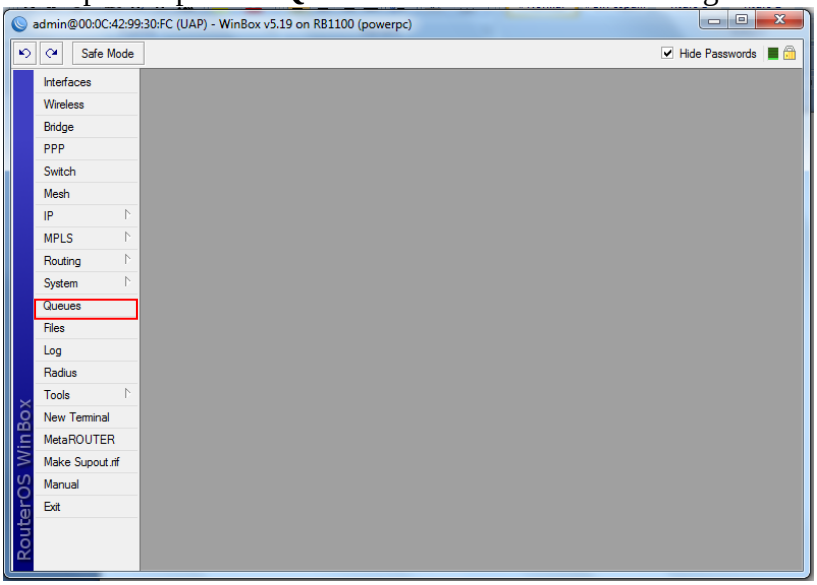
#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To
224	192.168.5.0/24			*.videospomo...			deny	www.uap.bo
225	192.168.5.0/24			*.voayeurs.*			deny	www.uap.bo
226	192.168.5.0/24			*.pelisxxx.*			deny	www.uap.bo
227	192.168.5.0/24			*.bragax.*			deny	www.uap.bo
228	192.168.5.0/24			*.gratisfolland...			deny	www.uap.bo
229	192.168.5.0/24			*.mamacitax.*			deny	www.uap.bo
230	192.168.5.0/24			*.7000videos.*			deny	www.uap.bo
231	192.168.5.0/24			*.xmaniacos.*			deny	www.uap.bo
232	192.168.5.0/24			*.sexoafull.*			deny	www.uap.bo
233	192.168.5.0/24			*.sexotop.*			deny	www.uap.bo
234	192.168.5.0/24			*.metacafe.*			deny	www.uap.bo
235	192.168.5.0/24			*.berglib.*			deny	www.uap.bo
236	192.168.5.0/24			*.votasexo.*			deny	www.uap.bo
237	192.168.5.0/24			*.videospriva...			deny	www.uap.bo
238	192.168.5.0/24			videossexo.*			deny	www.uap.bo
239	192.168.5.0/24			sexovaginal.*			deny	www.uap.bo
240	192.168.5.0/24			*.yotubesexo.*			deny	www.uap.bo
241	192.168.5.0/24			*.pornear.*			deny	www.uap.bo
242	192.168.5.0/24			*.sexogratis.*			deny	www.uap.bo
243	192.168.5.0/24			javichuparadi...			deny	www.uap.bo
244	192.168.5.0/24			*.freesexchat.*			deny	www.uap.bo
245	192.168.5.0/24			*.sexobot.*			deny	www.uap.bo
246	192.168.5.0/24			*.sexoenface...			deny	www.uap.bo
247	192.168.5.0/24			*.topamateurs...			deny	www.uap.bo
248	192.168.5.0/24			*.videospomo...			deny	www.uap.bo
249	192.168.5.0/24			*.momisnaked.*			deny	www.uap.bo
250	192.168.5.0/24			*.funnyordie.*			deny	www.uap.bo
251	192.168.5.0/24			*.amorproibido.*			deny	www.uap.bo
252	192.168.5.0/24			*.mefeedia.*			deny	www.uap.bo

254 items (1 selected)

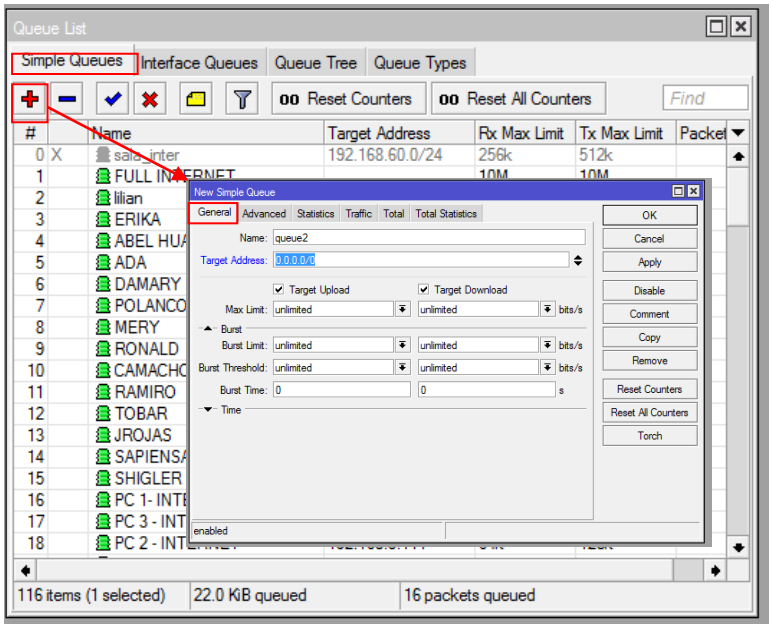
Administración de Queues

Para restricción y control de ancho de banda.

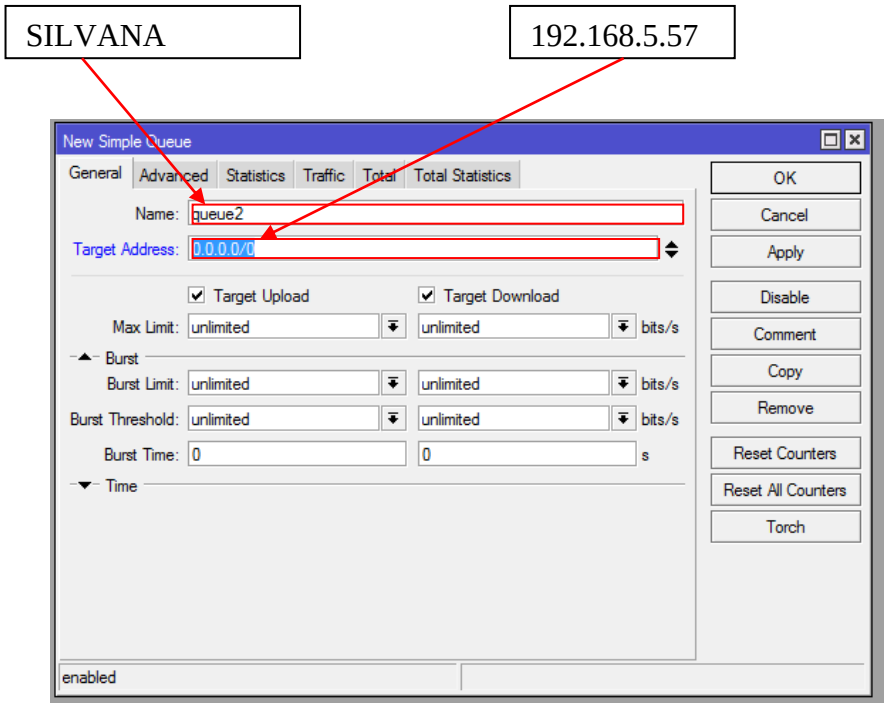
Hacemos doble clip en la pestaña **Queues** como se muestra en la siguiente figura.



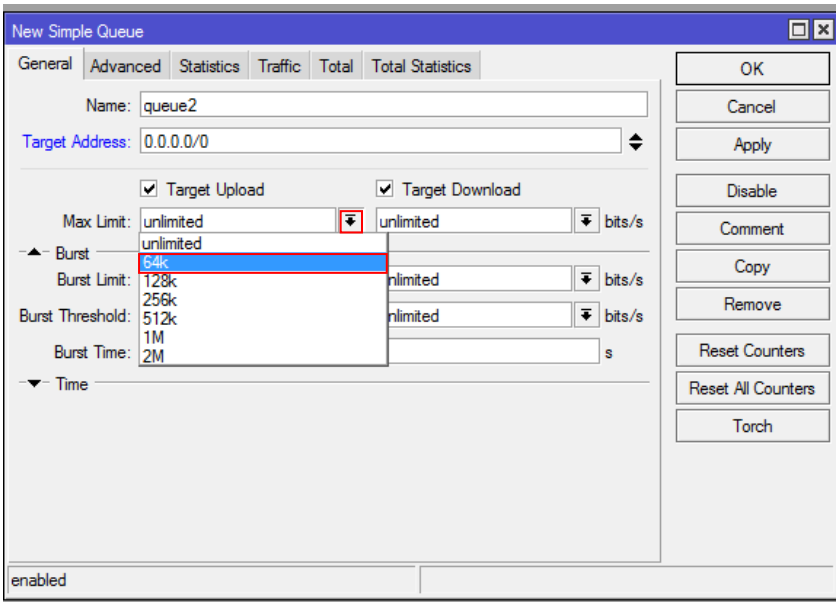
Luego en la nueva ventana que nos aparece seleccionamos **Simple Queues** y hacemos doble clip en el icono **(+)** y nos mostrara otra ventana como se muestra en la figura en la cual seleccionamos **General**.



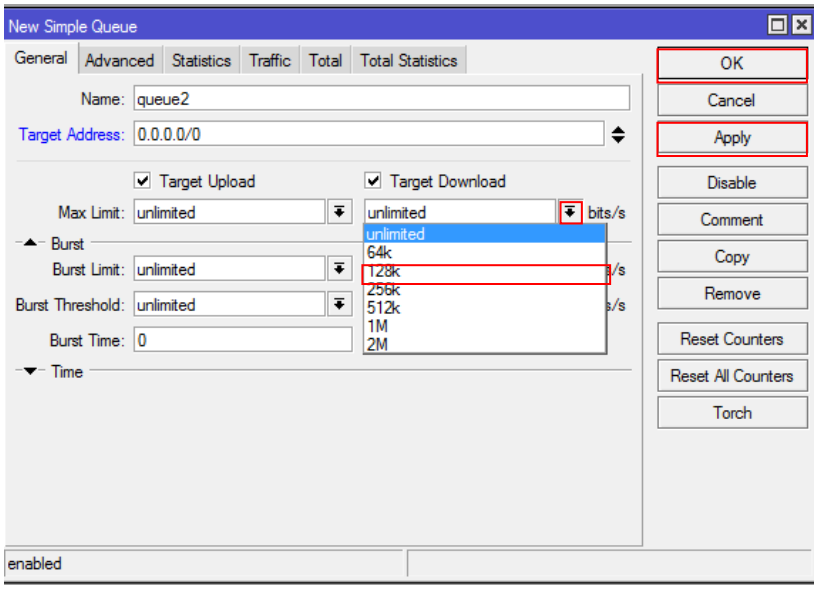
En **Name** ponemos un nombre para identificar la restricción del ancho de banda, en **Target Address** la dirección IP que será restringida, Como se muestra en la siguiente figura.



Luego en **Max Limit** seleccionamos o personalizamos el ancho de banda máximo de velocidad de carga como se muestra en la figura.



Una vez seleccionado o personalizado el ancho de banda máximo de velocidad de carga seleccionamos el de descarga, luego hacemos doble clip en **Apply** y **Ok** para grabar el registro en el servidor.



Despues de realizar todo el procedimiento como resultado obtendremos la lista de IP´S con ancho de banda limitados como se muestra en la siguiente figura.