ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESTUDIO DE CATALOGACIÓN DE LAS APLICACIONES Y ESTRUCTURACIÓN DEL ANCHO DE BANDA EN LA RED INTERNA INSTITUCIONAL DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE SANGOLQUÍ BASADA EN MIKROTIK PARA GARANTIZAR LOS SERVICIOS DE RED

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR:

XIMENA ANDREA JARAMILLO

SANGOLQUÍ, Enero 2013

CERTIFICACIÓN DE ELABORACIÓN DEL PROYECTO

Certificamos que el presente proyecto “ESTUDIO DE CATALOGACIÓN DE LAS APLICACIONES Y ESTRUCTURACIÓN DEL ANCHO DE BANDA EN LA RED INTERNA INSTITUCIONAL DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE SANGOLQUÍ BASADA EN MIKROTIK PARA GARANTIZAR LOS SERVICIOS DE RED” fue realizado en su totalidad por la Srta. XIMENA ANDREA JARAMILLO JAYA, como requerimiento parcial para la obtención del título de Ingeniera en Sistemas e Informática.

_____	_____
Ing. Fernando Galárraga	Ing. Arturo De la Torre
DIRECTOR	**CODIRECTOR**

Sangolquí, Enero 2013

DEDICATORIA

Este proyecto va dedicado a cada persona que directa e indirectamente han sido, al personal del Departamento Ciencias de la Computación que me brindaron su ayuda y su colaboración. Al Ing. Mauricio Campaña quien con su conocimiento siempre me ha extendido una mano y ha sido indispensable con su colaboración. A Javier Morales quien con su amor ha formado parte de mi vida en estos últimos meses y me apoyado para que todo esto sea posible.

Ximena Andrea Jaramillo

AGRADECIMIENTOS

Agradezco de manera especial a mi hermana Pamela Jaramillo que gracias a su apoyo y confianza brindada durante toda mi vida se ha hecho todo posible, mediante su ejemplo ha sido mi guía para encaminarme profesionalmente. A mis padres, por la oportunidad de permitirme participar de este gran viaje llamado vida, por su esfuerzo y sacrificio a lo largo de este recorrido. A mis tíos que han sido mis segundos padres que me han respaldado de diferentes maneras y siempre han estado presentes durante mi vida. A mis profesores que me han brindado sus conocimientos, confianza y apoyo para que este proyecto sea posible, por su paciencia y amistad que han sido una gran base y respaldo en esta fase de mi vida.

Ximena Andrea Jaramillo

AUTORIZACIÓN

Yo, Ximena Andrea Jaramillo Jaya alumna egresada de la Institución, responsable del proyecto “ESTUDIO DE CATALOGACIÓN DE LAS APLICACIONES Y ESTRUCTURACIÓN DEL ANCHO DE BANDA EN LA RED INTERNA INSTITUCIONAL DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE SANGOLQUÍ BASADA EN MIKROTIK PARA GARANTIZAR LOS SERVICIOS DE RED” autorizo al personal responsable para la publicación del proyecto en el catálogo On-line Biblioteca Alejandro Segovia – ESPE.

Ximena Andrea Jaramillo Jaya

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Hoy en día la realidad dice que las redes informáticas, se han vuelto indispensables, tanto para las personas como organizaciones ya sean grandes o pequeñas. Les da oportunidad de interactuar con el resto del mundo, sea por motivos comerciales, personales o emergencias. En este entorno, los departamentos de la Institución de educación superior se enfrentan cada vez más al desafío de distribuir equitativamente los recursos de la red y tratar de garantizar que las aplicaciones académicas legítimas cuenten con el ancho de banda que necesitan. El uso compartido de archivos con fines recreativos es el principal responsable del consumo excesivo de ancho de banda. Muchas instituciones también se enfrentan a la amenaza de que sus redes de alto ancho de banda se conviertan en perfectos trampolines de lanzamiento de virus y gusanos de rápida propagación, que pueden generar cantidades enormes de tráfico inútil e interrumpir los servicios esenciales. Las universidades necesitan contar con nuevas estrategias para controlar de manera más justa y eficaz el uso del ancho de banda entre estudiantes, profesores y aplicaciones. Al proporcionar un control completo del ancho de banda, estas estrategias pueden garantizar que las aplicaciones fundamentales cuenten siempre con los recursos que necesitan, que se permitan las actividades recreativas pero con la debida asignación de prioridad y limitación. No obstante, las modernas herramientas de control de ancho de banda para redes educativas banda deben ser lo suficientemente inteligentes como para permitir a los educadores definir reglas con distintos niveles de granularidad, según el tipo de tráfico, la naturaleza de las aplicaciones y el área de la red. Además, para brindar un auténtico control del ancho de banda en toda

la institución, estas herramientas deben caracterizarse por su escalabilidad y facilidad de administración. La optimización de recursos en el uso de los sistemas informáticos es uno de los elementos de interacción y desarrollo que rige los destinos de la informática. Gracias a ello se tiene día a día la aparición de las plataformas de interconexión de equipos de computación o redes informáticas. Las mismas resultan ser uno de los elementos tecnológicos más importantes al momento de definir un sistema informático en una organización. Entre las principales ventajas que le brinda a una empresa el uso de redes informáticas, es compartir recursos especialmente información (datos), proveer la confiabilidad, permitir la disponibilidad de programas y equipos para cualquier usuario de la red que así lo solicite sin importar la localización física del recurso y del usuario. Permite al usuario poder acceder a una misma información sin problemas llevándolo de un equipo a otro. También es una forma de reducir los costos operativos, compartiendo recursos de hardware y/o de software entre las diversas computadoras de cualquier empresa.

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

El crecimiento de Internet y la necesidad de servicios IP requieren que las redes corporativas vayan incrementando paulatinamente pero de forma constante el ancho de banda para lograr que sus servicios trabajen de forma adecuada y sobre todo maximizar el rendimiento de las comunicaciones de la Escuela Politécnica del Ejército. Para la comunidad politécnica que utiliza Internet continuamente, preocupa la velocidad en la navegación, descarga de programas y papers, ocasionando que se tenga una percepción negativa del servicio. Cuando no existe control de ancho de banda, se hace prácticamente improbable que se logre acceder a la red, teniendo como consecuencia que los usuarios prefieran utilizar el servicio en lugares externos. El rendimiento de una conexión nunca es del 100%. Hay que tener en cuenta que en estos tipos de conexiones se utilizan varios protocolos (PPP, TCP/IP) que ocupan ancho de banda (entre un 2% y un 20% del 100% del total, según el tipo de conexión y protocolo utilizado), con lo que se reduce el ancho de banda útil para la descarga de datos, esto equivale a la velocidad de transferencia de información, y no a la velocidad de acceso. Adicionalmente, existen otros factores no medibles que pueden contribuir a reducir la velocidad de la conexión, como son la congestión en la red e interferencias electromagnéticas que también influyen el resultado final. Las videoconferencias de alta calidad, comunes en las redes de alto desempeño como Internet 2, pueden consumir hasta 2 o 3Mbps, mientras que videoconferencias con usos especializados y calidad de televisión de alta

definición requieren de 10 a 20 Mbps de ancho de banda por sitio, sin embargo, una gran ventaja de la videoconferencia por IP es que usa de forma dinámica el ancho de banda, así al inicio de la sesión se necesitará la cantidad nominal de bits por segundo, monto que irá disminuyendo conforme transcurra, dependiendo del movimiento en el video y las muestras de audio que se digitalicen (dicho de otra forma: si un sitio en la videoconferencia no habla y cancela sus cámaras, el ancho de banda empleado puede ser tan bajo como solo el 20% de bits por segundo del monto inicial que permite mantener la conexión).

1.2 OBJETIVOS

1.2.1 Objetivo General

- Proponer una solución basada en Mikrotik para garantizar QoS a los servicios de la red interna de la Escuela Politécnica del Ejército sede Sangolquí.

1.2.2 Objetivos Específicos

- Analizar el Sistema Operativo Mikrotik RouterOS.
- Investigar los factores establecidos para la Institución que afectan el rendimiento del servicio de red.
- Realizar la catalogación de las aplicaciones y asignar el ancho de banda
- Aplicar conceptos de QoS y etiquetado de paquetes para mejorar el rendimiento de los servicios de la red interna.

1.3 JUSTIFICACIÓN

La administración de los recursos de red, especialmente el ancho de banda es una tarea cada vez más solicitada a los administradores, pues de ello depende

disponer de servicios con cierto grado de calidad y sobre todo que permitan una comunicación oportuna y confiable. La necesidad de disponer de una infraestructura de red robusta, no debe ser entendida únicamente desde la perspectiva del hardware, sino de la calidad de servicios que ofrece; para ello es indispensable realizar tareas de ingeniería de tráfico, administración del ancho de banda a nivel de aplicación, es decir, asignar a cada aplicativo el recurso que requiere para operar de forma adecuada. Las solicitudes hacia internet pasan a través de un gateway por lo que podrá controlar y administrar el tráfico que ingresa y sale de la red, lo que permitirá definir el ancho de banda que cada aplicación requiere para un óptimo desempeño. La Escuela Politécnica del Ejército (ESPE), como institución de educación superior, requiere que los servicios de red sean oportunos y de calidad para todos sus usuarios y así permita realizar investigaciones, consultas, publicaciones y demás actividades propias de un centro de investigación; esto obliga a implementar una administración más fina de los usos del ancho de banda de acceso a internet.

1.4 ALCANCE

El desarrollo del proyecto se enmarca dentro de los servicios de red con los que cuenta actualmente la Institución y tiene como alcance realizar la investigación de las tecnología Mikrotik como medio necesario y óptimo para la medición de tráfico mediante herramientas de hardware, software y brindar una solución a la medida de las necesidades que requiera la red interna de la Institución.

1.5 HIPÓTESIS DE TRABAJO

Los resultados obtenidos de la investigación mediante Hardware y Software podrán ser utilizados como base para la comparación con los resultados actuales que se obtiene mediante equipos con los que trabaja la Institución.

1.6 METODOLOGÍA

A continuación se describen los pasos a seguir:

- Investigar y analizar la tecnología Mikrotik como: equipos, software y herramientas para alcanzar la catalogación de servicios de red.
- Configurar el sistema Mikrotik para lograr la aplicación de los servicios de red interna de la Escuela Politécnica del Ejército sede Sangolquí.
- Verificar los resultados.
- Evaluar y discutir los resultados.

CAPÍTULO 2

MARCO TEÓRICO

2.1 REDES LAN

Una red de área local, red local o LAN (*local area network*) es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro.

2.1.1 **Características**

- Tecnología broadcast (difusión) con el medio de transmisión compartido.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 5 km (una FDDI puede llegar a 200 km).
- Uso de un medio de comunicación privado.
- La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica).
- La facilidad con que se pueden efectuar cambios en el hardware y el software.
- Gran variedad y número de dispositivos conectados.
- Posibilidad de conexión con otras redes.
- Limitante de 100 m, puede llegar a más si se usan repetidores.

2.1.2 **Topologías de la red**

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios.

La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

2.1.2.1 **Topologías físicas**

- Una **topología de bus circular** usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
- La **topología de anillo** conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- La **topología en estrella** conecta todos los cables con un punto central de concentración.
- Una **topología en estrella extendida** conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
- Una **topología jerárquica** es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La **topología de malla** se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. En esta topología, cada host tiene sus propias conexiones con los demás hosts. Aunque Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.
- La **topología de árbol** tiene varias terminales conectadas de forma que la red se ramifica desde un servidor base.

2.1.2.2 **Topologías lógicas**

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

- La **topología broadcast** simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada, es como funciona Ethernet.
- La **topología transmisión de tokens** controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir.

2.1.3 **Medios de Transmisión**

2.1.3.1 **Medios de Transmisión guiados**

Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace. Dentro de los medios de transmisión guiados, los más utilizados en el campo de las comunicaciones y la interconexión de ordenadores son:

- El par trenzado
- El cable coaxial.
- La fibra óptica.

2.1.3.2 **Medios de Transmisión no guiados**

En este tipo de medios tanto la transmisión como la recepción de información se lleva a cabo mediante antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio. Por el contrario, en la recepción la antena capta las ondas electromagnéticas del medio que la rodea. La configuración para las transmisiones no guiadas puede ser direccional y omnidireccional. En la direccional, la antena transmisora emite la energía electromagnética concentrándola en un haz, por lo que las antenas emisora y receptora deben estar alineadas. En la omnidireccional, la radiación se hace de manera dispersa, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. Generalmente, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional. Según el rango de frecuencias de trabajo, las transmisiones no guiadas se pueden clasificar en tres tipos: radio, microondas y luz (infrarrojos/láser). [1]

2.2 WLAN

Su uso, podría estar vinculado a cualquier tipo de comunicación que no requiere de un medio de propagación físico. Sin embargo la noción de wireless se utiliza principalmente para nombrar a las comunicaciones inalámbricas en el marco de las tecnologías informáticas. En una comunicación wlan, por lo tanto el emisor y el receptor no están unidos por cables, sino que apelan a la modulación de ondas electromagnéticas a través del espacio para el envío y la recepción de datos. [2]

2.2.1.1 **Tipos de redes inalámbricas**

- LAN Inalámbrica: Red de área local inalámbrica. También puede ser una Red de área metropolitana inalámbrica.
- GSM (Global System for Mobile Communications): La red GSM es utilizada mayormente por teléfonos celulares.
- PCS (Personal Communications Service): Es una franja de radio que puede ser usada para teléfonos móviles en Estados Unidos de América.
- D-AMPS (Digital Advanced Mobile Phone Service): Está siendo remplazada por el sistema GSM.
- Wi-Fi: Es uno de los sistemas más utilizados para la creación de redes inalámbricas en computadoras, permitiendo acceso a recursos remotos como internet e impresoras. Utiliza ondas de radio.
- Fixed Wireless Data: Es un tipo de red inalámbrica de datos que puede ser usada para conectar dos o más edificios juntos para extender o compartir el ancho de banda de una red sin que exista cableado físico entre los edificios. [3]

2.2.2 **ESTÁNDARES INALÁMBRICOS**

2.2.2.1 **802.11**

El estándar '*IEEE 802.11'* define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana. La versión original del estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

802.11 especifica dos velocidades de transmisión *teóricas* de 1 y 2 megabits por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR). IR sigue siendo parte del estándar, si bien no hay implementaciones disponibles. El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas.

2.2.2.2 **802.11a**

La revisión 802.11a fue aprobada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadora sorthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto.

2.2.2.3 **802.11b**

Artículo principal: IEEE 802.11b*.*

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4 GHz. Debido al espacio ocupado por la codificación del

protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 Mbits sobre TCP y 7,1 Mbit/s sobre UDP.

2.2.2.4 **802.11 c**

Es menos usado que los primeros dos, pero por la implementación que este protocolo refleja. El protocolo ‘c’ es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. El protocolo ‘c’ es más utilizado diariamente, debido al costo que implica las largas distancias de instalación con fibra óptica, que aunque más fidedigna, resulta más costosa tanto en instrumentos monetarios como en tiempo de instalación.

2.2.2.5 **802.11d**

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil.

2.2.2.6 **802.11e**

La especificación IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, esta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que

mantiene compatibilidad con ellos. Estas prestaciones resultan fundamentales para las redes domésticas y para que los operadores y proveedores de servicios conformen ofertas avanzadas. El documento que establece las directrices de QoS, define los primeros indicios sobre cómo será la especificación que aparecerá a finales de 2001. Incluye, asimismo, corrección de errores y cubre las interfaces de adaptación de audio y vídeo con la finalidad de mejorar el control e integración en capas de aquellos mecanismos que se encarguen de gestionar redes de menor rango. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) *Enhanced Distributed Channel Access*, equivalente a DCF.
- (HCCA) *HCF Controlled Access*, equivalente a PCF.

En este nuevo estándar se definen cuatro categorías de acceso al medio.

- *Background* (AC_BK)
- *Best Effort* (AC_BE)
- *Video* (AC_VI)
- *Voice* (AC_VO)

2.2.2.7 **802.11f**

Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras

está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red.

2.2.2.8 **802.11g**

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Que es la evolución del estándar 802.11b, Este utiliza la banda de 2,4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

2.2.2.9 **802.11h**

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite. El desarrollo del 802.11h sigue unas recomendaciones que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ECC/DEC/(04)08). Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

2.2.2.10 **802.11i**

Está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

2.2.2.11 **802.11j**

Es equivalente al 802.11h, en la regulación Japonesa.

2.2.2.12 **802.11k**

Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión. Está diseñado para ser implementado en software, para soportar el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

2.2.2.13 **802.11n**

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 300 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios

canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (3).

2.2.2.14 **802.11p**

Este estándar opera en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

2.2.2.15 **802.11r**

También se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función, que una vez enunciada parece obvia e indispensable en un sistema de datos inalámbricos, permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

2.2.2.16 **802.11v**

IEEE 802.11v servirá para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías:

mecanismos de ahorro de energía con dispositivos de mano VoIP Wi-Fi en mente; posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación; temporización, para soportar aplicaciones que requieren un calibrado muy preciso; y coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

2.2.2.17 **802.11w**

Todavía no concluido. Las LANs inalámbricas envían la información del sistema en tramas desprotegidos, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u. [4]

2.3 SERVICIOS DE RED

La finalidad de una red es que los usuarios de los sistemas informáticos de una organización puedan hacer un mejor uso de los mismos mejorando de este modo el rendimiento global de la organización. Así las organizaciones obtienen una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser:

- Mayor facilidad de comunicación.
- Mejora de la competitividad.
- Mejora de la dinámica de grupo.
- Reducción del presupuesto para proceso de datos.

- Reducción de los costos de proceso por usuario.
- Mejoras en la administración de los programas.
- Mejoras en la integridad de los datos.
- Mejora en los tiempos de respuesta.
- Flexibilidad en el proceso de datos.
- Mayor variedad de programas.
- Mayor facilidad de uso. Mejor seguridad.

Para que todo esto sea posible, la red debe prestar una serie de servicios a sus usuarios, como son:

- Acceso.
- Ficheros.
- Impresión.
- Correo.
- Información.
- Otros. [5]

2.3.1 **ANCHO DE BANDA**

Ancho de banda es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él (ciento setenta y dos, Mbit/s, entre otros). Ancho de banda puede referirse a la capacidad de ancho de banda o ancho de banda disponible en bit/s, lo cual típicamente significa el rango neto de bits o la máxima salida de una huella de comunicación lógico o físico en un sistema de comunicación digital. La razón de este uso es que de acuerdo a la Ley de Hartley, el rango máximo de transferencia de datos de un enlace físico de comunicación es proporcional a su ancho de banda (procesamiento de señal)

en hertz, la cual es a veces llamada "ancho de banda análogo" en la literatura de la especialidad. Ancho de banda puede también referirse a ancho de banda consumido (*consumo de ancho de banda*), que corresponde al uso de descarga o colocación; por ejemplo, el rango promedio de transferencia de datos *exitosa* a través de una huella de comunicación.[6]

2.3.2 **LÍNEAS DEDICADAS**

2.3.2.1 **Línea Dedicada de Cobre**

Conocida comúnmente como LTR ó LD es la extensión de un par de cobre de un punto a otro.

Beneficios

- Enlace no conmutado.
- Permite transmisiones de Voz, Datos, Video y Fax
- El canal contratado es para uso exclusivo del cliente

2.3.2.2 **Línea dedicada de fibra óptica**

Es un servicio de alquiler de líneas dedicadas de Fibra Óptica para interconexiones físicas en las configuraciones punto a punto y punto multipunto, remplazando a las líneas de cobre, teniendo una comunicación más confiable en cuanto al ancho de banda y alcance.

Beneficios

- Atenuación muy baja.
- Transmite señales analógicas y digitales.
- Mayor seguridad en los enlaces. [7]

2.3.3 **ELEMENTOS ACTIVOS – PASIVOS DE UNA RED**

Los elementos que constituyen la capa física de Ethernet son de dos tipos: Activos y Pasivos. Los primeros generan y/o modifican señales, los segundos simplemente la transmiten.

Pasivos:	**Activos:**
Cables	Transceptores
Jacks / Conectores	Repetidores
Patch panels	Repetidores multipuerto (Hubs). [8]

2.4 DIRECCIÓN IP

Una Dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina *dirección IP dinámica*. Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una *dirección IP fija* (comúnmente, *IP fija* o *IP estática*). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web

necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

2.4.1 **Direcciones IPv4**

Las direcciones IPv4 se expresan por un número binario de 32 bits, permitiendo un espacio de direcciones de hasta 4.294.967.296 (2^{32}) direcciones posibles. Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el rango de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255]. En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255, salvo algunas excepciones. Los ceros iniciales, si los hubiera, se pueden obviar.

- Ejemplo de representación de dirección IPv4: 10.128.001.255 o 10.128.1.255.

En las primeras etapas del desarrollo del Protocolo de Internet, los administradores de Internet interpretaban las direcciones IP en dos partes, los primeros 8 bits para designar la dirección de red y el resto para individualizar la computadora dentro de la red. Este método pronto probó ser inadecuado, cuando se comenzaron a agregar nuevas redes a las ya asignadas. En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases (classful network architecture). En esta arquitectura hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} - 2 (se excluyen la dirección reservada para broadcast (últimos octetos en 255) y de red (últimos octetos en 0)), es decir, 16.777.214 hosts.
- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} - 2, o 65.534 hosts.
- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^{8} - 2, o 254 hosts.

Tabla 2.1 Clases de Direcciones IP

Clase	Rango	N° de Redes	N° de Host Por Red	Máscara de Red	Broadcast ID
A	1.0.0.0 - 126.255.255.255	126	16.777.214	255.0.0.0	x.255.255.255
B	128.0.0.0 - 191.255.255.255	16.384	65.534	255.255.0.0	x.x.255.255
C	192.0.0.0 - 223.255.255.255	2.097.152	254	255.255.255.0	x.x.x.255
(D)	224.0.0.0 - 239.255.255.255	histórico			
(E)	240.0.0.0 - 255.255.255.255	histórico			

- La dirección 0.0.0.0 es reservada por la IANA para identificación local.
- La dirección que tiene los bits de host iguales a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.

- La dirección que tiene los bits correspondientes a host iguales a uno, sirve para enviar paquetes a todos los hosts de la red en la que se ubica. Se denomina dirección de broadcast.
- Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina dirección de bucle local o loopback.

El diseño de redes de clases (classful) sirvió durante la expansión de internet, sin embargo este diseño no era escalable y frente a una gran expansión de las redes en la década de los noventa, el sistema de espacio de direcciones de clases fue reemplazado por una arquitectura de redes sin clases Classless Inter-Domain Routing (CIDR) en el año 1993. CIDR está basada en redes de longitud de máscara de subred variable (variable-length subnet masking VLSM) que permite asignar redes de longitud de prefijo arbitrario. Permitiendo una distribución de direcciones más fina y granulada, calculando las direcciones necesarias y desperdiciando las mínimas posibles.

2.4.2 **DIRECCIONES PRIVADAS**

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).

- Clase B: 172.16.0.0 a 172.31.255.255 (12 bits red, 20 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- Clase C: 192.168.0.0 a 192.168.255.255 (16 bits red, 16 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Por ejemplo, los bancos pueden utilizar TCP/IP para conectar los cajeros automáticos que no se conectan a la red pública, de manera que las direcciones privadas son ideales para estas circunstancias. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles. Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles

2.4.3 **MÁSCARA DE SUBRED**

La máscara permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP. Dada la dirección de clase A 10.2.1.2 que pertenece a la red 10.0.0.0 y el host al que se refiere es el 2.1.2 dentro de la misma. La máscara se forma poniendo a 1 los bits que identifican la red y a 0 los bits que identifican el host. De esta forma una dirección de clase A tendrá como máscara 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0. Los dispositivos de red realizan un AND entre la dirección IP y la máscara para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada. Por ejemplo un router necesita saber cuál es la red a la que pertenece la dirección IP del datagrama destino para poder consultar la tabla de encaminamiento y poder

enviar el datagrama por la interfaz de salida. Para esto se necesita tener cables directos. La máscara también puede ser representada de la siguiente forma 10.2.1.2/8 donde el /8 indica que los 8 bits más significativos de máscara están destinados a redes, es decir /8 = 255.0.0.0. Análogamente (/16 = 255.255.0.0) y (/24 = 255.255.255.0).

2.4.4 **Creación de Subredes**

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas. Un ejemplo de uso es cuando se necesita agrupar todos los empleados pertenecientes a un departamento de una empresa. En este caso se crearía una subred que englobara las direcciones IP de estos. Para conseguirlo hay que reservar bits del campo host para identificar la subred estableciendo a uno los bits de red-subred en la máscara. Por ejemplo la dirección 172.16.1.1 con máscara 255.255.255.0 indica que los dos primeros octetos identifican la red (por ser una dirección de clase B), el tercer octeto identifica la subred (a 1 los bits en la máscara) y el cuarto identifica el host (a 0 los bits correspondientes dentro de la máscara). Hay dos direcciones de cada subred que quedan reservadas: aquella que identifica la subred y la dirección para realizar broadcast en la subred (todos los bits del campo host en 1).

2.4.5 **IP DINÁMICA**

Una dirección IP dinámica es una IP asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente. DHCP apareció como protocolo estándar en octubre de 1993. El estándar RFC

2131 especifica la última definición de DHCP (marzo de 1997). DHCP sustituye al protocolo BOOTP, que es más antiguo. Debido a la compatibilidad retroactiva de DHCP, muy pocas redes continúan usando BOOTP puro. Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado.

2.4.5.1 **Ventajas**

- Reduce los costos de operación a los proveedores de servicios de Internet.
- Reduce la cantidad de IP asignadas (de forma fija) inactivas.

2.4.5.2 **Desventajas**

- Obliga a depender de servicios que redirigen un host a una IP.

2.4.6 **DIRECCIONES IPv6**

La función de la dirección IPv6 es exactamente la misma que la de su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la Tierra tenga asignados varios millones de IPs, ya que puede implementarse con 2^{128} (3.4×10^{38} hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento. Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas de notación acerca de la representación de direcciones IPv6 son:

- Los ceros iniciales, como en IPv4, se pueden obviar.

Ejemplo: *2001:0123:0004:00ab:0cde:3403:0001:0063* -> 2001:123:4:ab:cde:3403:1:63.

- Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación sólo se puede hacer una vez.

Ejemplo: *2001:0:0:0:0:0:0:4* -> ***2001::4***. [9]

2.4.7 **FORMATOS DE INFORMACIÓN**

Los datos y la información de control que se transmite a través de las redes toman una gran variedad de formas. Los términos usados para referirse a estos formatos de información no se usan consistentemente en la industria de la interconectividad. Algunas veces pueden ser intercambiables. Los formatos de información más comunes son los siguientes:

- Trama (frame)
- Paquete (packet)
- Data grama (datagram)
- Segmento (segment)
- Mensaje (message)
- Celda (cell)
- Unidad de Datos (data unit)

TRAMA. Una trama es una unidad de información la cual su fuente y su destino es la entidad de la capa de enlace de datos. Una trama se compone de los siguientes dos elementos: Header de la capa de enlace de datos (y posiblemente un trailer); el header y el trailer contienen información de control entendible para la entidad de la capa de enlace de datos en el sistema de destino.

PAQUETE. Un paquete es una unidad de información cuya fuente y destino es la entidad de la capa de red. Un paquete se compone de los siguientes dos elementos: Header de la capa de red (y posiblemente un trailer); el header y el trailer contienen información de control entendible por la unidad de la capa de red en el sistema de destino.

DATAGRAMA. El término datagrama se refiere usualmente a la unidad de información cuya fuente y destino es la entidad de la capa de red usando un información cuya fuente y destino son las entidades de la capa de transporte.

MENSAJE. Un mensaje es una unidad de información cuyas entidades de fuente y destino están arriba de la capa de red (como la capa de aplicación).

CELDA. Una celda es una unidad de información de tamaño fijo cuya fuente y destino son las entidades de la capa de enlace de datos. Las celdas son usadas en ambientes de conmutación, tales como las redes en Modo de Transferencia Asíncrona (ATM) y Servicio Conmutado Multimegabit de Datos (SMDS). Una celda se compone de los siguientes dos elementos: Header; el header contiene información de control entendible para la entidad de la capa de enlace de datos destinataria. El header de una celda típicamente mide 5 bytes. Carga útil; la carga útil contiene datos de las capas superiores que son encapsulados en el header de la celda. La carga útil (Payload) de la celda mide típicamente 48 bytes.

UNIDAD DE DATOS. Unidad de datos es un término genérico referido a una variedad de formatos de información. Algunos ejemplos de las unidades de datos son los siguientes: Unidad de datos de servicio (SDU); son unidades de información de los protocolos de las capas superiores que solicita un

requerimiento de servicio al protocolo de las capas bajas. Unidad de datos de protocolo (PDU); es una terminología de OSI para los paquetes. [10]

2.4.8 **Calidad de servicio (QoS)**

QoS o Calidad de Servicio (*Quality of Service*, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz. [11]

2.4.9 **Calidad de servicio – MIKROTIK**

Calidad de Servicio (QoS) significa que el router puede priorizar y dar forma al tráfico de red. Algunas de las características del mecanismo de control tráfico de Mikrotik RouterOS son los siguientes:

- El límite de velocidad de datos para ciertas direcciones IP, subredes, protocolos, puertos, y otros parámetros.
- El límite de peer-to-peer de tráfico.
- Dar prioridad a algunos flujos de paquetes sobre los demás.
- Uso de colas ráfagas para la navegación web más rápida.
- Aplicar las colas en los intervalos de tiempo fijos.
- Compartir el tráfico disponible entre los usuarios por igual, o en función de la carga del canal. [12]

2.5 PROVEEDORES DE SERVICIOS DE INTERNET

Un proveedor de servicios de Internet (ISP, por la sigla en inglés de *Internet Service Provider*) es una empresa que brinda conexión a Internet a sus clientes.

Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cable módem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios y servidores de noticias. Ecuador consta con los siguientes proveedores de internet:

Tabla 2.2 Proveedores de internet de Ecuador

Proveedor	Ciudad
Andinanet	Quito
Cablemodem	Quito
Claro	Todo el país
Interactive	Quito
Movistar - Telefónica	Todo el país
Panchonet	Quito
Proveedores de internet	Quito
Satnet	Quito
Telconet	Guayaquil, Quito – Cuenca [13]

2.5.1 **TIPOS DE CONEXIONES**

Los ISP utilizan un gran número de tecnologías para permitir al usuario conectarse a sus redes. Conexiones a Internet típicas para usuarios residenciales:

- Dial-up (Banda estrecha).
- Red Digital de Servicios Integrados (ISDN).
- Módem.
- Banda ancha.
- DSL (normalmente del tipo Asymmetric Digital Subscriber Line o ADSL).
- Banda Ancha Móvil.
- Banda ancha inalámbrica (Wi-Fi).
- Cable módem.

- Fiber To The Home (FTTH).

Conexiones típicas para empresas medianas o grandes:

- DSL.
- Ethernet, Metro Ethernet o Gigabit Ethernet.
- Frame Relay.
- ISDN.
- ATM.
- Internet satelital.
- Red Óptica Síncrona (SONET). [14]

2.5.2 **ENLACE DE ÚLTIMA MILLA**

Para casi todos los operadores de telecomunicaciones y de las empresas en la actual economía global, el acceso a comunicaciones de alta velocidad es clave para un rápido y constante crecimiento. Hoy en día las redes de comunicaciones de banda ancha son la columna vertebral de las empresas que dependen del análisis y difusión de información crítica. De hecho, la mayoría de las organizaciones tienen en proyección extender y ampliar sus redes de comunicaciones para fomentar el cumplimiento de sus objetivos de negocios. Pero este crecimiento los enfrenta a un desafío importante: el costo. La serie de equipos de última milla proveen a las soluciones inalámbricas la capacidad de abordar la necesidad de la banda ancha y brindan el apoyo máximo para los operadores de red y las empresas con proyectos próximo de crecimiento. Adicionalmente, ofrecen la escalabilidad de las actualizaciones sencillas y accesibles que proporcionan mayor rendimiento y estabilidad en el momento justo. Los puentes de la Serie PTP utilizan un programa de modulación de

plataforma de banda ancha inalámbrica punto-a-multipunto para ofrecer conectividad de banda ancha hasta una distancia de 250 km y un procesamiento constante en configuraciones de visibilidad directa.

CAPÍTULO 3

FACTORES QUE AFECTAN EL SERVICIO DE RED

3.1 ESTUDIO DESCRIPTIVO DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE SANGOLQUÍ EN EL AÑO 2011

Hoy en día, en la Institución se utilizan una nueva clase de aplicaciones de medios dinámicos para facilitar y fortalecer el proceso educativo. No obstante, a medida que proliferan las aplicaciones de voz y video de alto ancho de banda, también aumenta la demanda de recursos de ancho de banda. Por otra parte, las redes de alto ancho de banda son un blanco atractivo para los hackers y los ataques emergentes de denegación de servicio (DoS) y gente que no pertenece a la Institución pueden aprovechar los entornos de alto ancho de banda, propagarse con una rapidez sin precedentes e inundar los recursos de la red. La Institución debe adoptar nuevas estrategias de seguridad de con el fin de protegerse contra estos problemas. La solución de control de ancho de banda para la red LAN ofrece un potente conjunto de herramientas a fin de implementar y aplicar políticas de control de ancho de banda en toda la institución, así como aprovechar todo el potencial que brindan las redes académicas de alto ancho de banda. No es una opción realizar a futuro una administración de ancho de banda ya que no se ha realizado un análisis, la proyección que se tiene a futuro próximo es aumentar el ancho de banda de la Institución donde actualmente cuenta con 40Megas y se aumentará a 65Megas, como resultado habrá el aumento de ancho de banda con la ausencia de control donde no garantiza la disminución de tráfico y satisfacción completa para cada usuario. Después de realizar un análisis exhaustivo de la estructura de la ESPE (Escuela Politécnica del Ejército) se puede

diagramar la estructura de cómo se encuentra conformada dicha empresa. En las aulas y edificios del campus, los departamentos de la Institución deberán modelar y colocar los teléfonos IP en colas de estricta prioridad. La cola de estricta prioridad ayuda a garantizar que la red siempre asigne al tráfico de voz la máxima prioridad. La cola de estricta prioridad proporciona el ancho de banda dedicado que el tráfico de voz necesita para reducir al mínimo la latencia y las fluctuaciones. Si bien el tráfico de voz es muy sensible a la latencia y a las fluctuaciones, no requiere gran cantidad de ancho de banda (menos de 100 Kbps). En la figura 3.1 se ilustra una red universitaria típica.

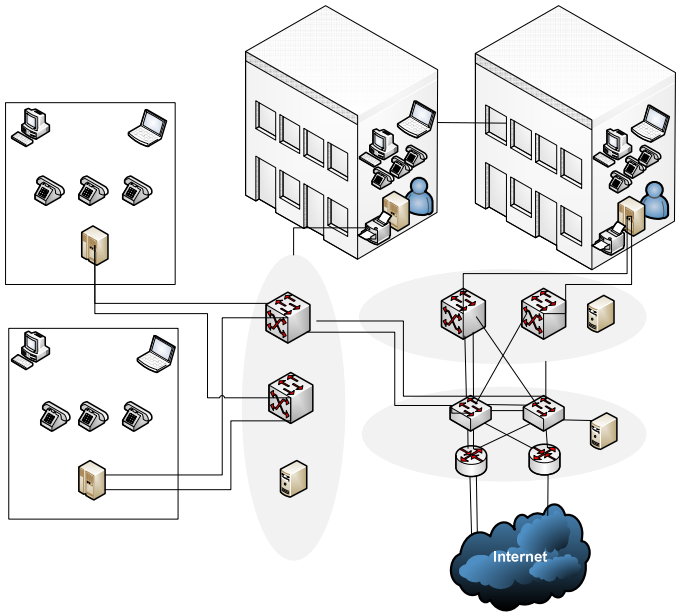


Figura 3.1 Red universitaria típica

Los administradores pueden preferir asignar el mayor ancho de banda a determinados edificios o centros de distribución según las necesidades de ancho de banda. (También pueden utilizar otros criterios, por ejemplo, pueden definir límites de velocidad más altos para los departamentos que pagan una suma adicional por más ancho de banda). En general, los administradores asignan más ancho de banda en el tramo comprendido entre la capa de distribución de los

edificios del campus y el core que entre la capa de distribución de los dormitorios y el core de la red. Las oficinas de profesores, los centros de investigación de estudiantes de postgrado y los centros de trabajo de estudiantes de grado que desarrollan un alto nivel de actividades y están ubicados en los edificios del campus suelen necesitar un mayor ancho de banda de la red y un enlace WAN superior con la red.

Existen 4 segmentos (véase en la figura3.2) que son:

- **Web:** Página web, correo electrónico y telefonía IP.
- **Laboratorios:** Todos los laboratorio que comprende como servicio para los estudiantes.
- **Financiero:** Todo el personal administrativo, servidores públicos que en su mayoría trabaja a tiempo completo.
- **General:** Aquí se encuentra todo el alumnado y biblioteca.

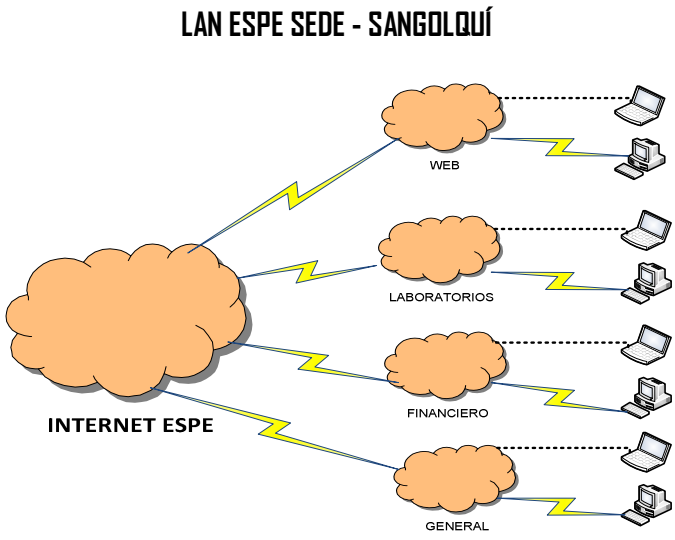


Figura 3.2 LAN actual

El segmento General es el que tiene mayor número de usuarios de todos los segmentos por lo cual tiene más tráfico de datos, en varios casos existen alumnos que no pueden obtener conexión a internet, mientras los alumnos que

tienen conexión a internet, tienen un servicio muy lento y restringido a gran número de páginas. En cada departamento existen 3 tipos de usuarios: Estudiantes, docentes y administrativos donde no existe una validación de alta seguridad donde se garantice que el usuario que ingresó pertenezca al departamento. No existe una administración donde se pueda asegurar el tipo de usuario del Departamento y así ofrecer servicios necesarios por cada segmento y cumplir sus requerimientos. También existe la ausencia de un plan de direccionamiento IP del segmento **General.** Para cumplir con el servicio de videoconferencia se asigna 1Mega cada vez que se hace uso del aula virtual, donde se retira el servicio de ancho de banda de otros segmentos hasta que termine la videoconferencia, eso conlleva insatisfacción a otros usuarios, ya que el internet como herramienta es de uso diario durante las horas laborales de la Institución (de 7:15am a 9:30pm). Entre los servicios que se tienen como proyecto a futuro son: wireless que se desea ampliar y videoconferencia que se quiere tomar como un segmento para no interrumpir otros servicios. En la actualidad el Departamento Ciencias de la Computación (DCC) cuenta con el direccionamiento IP que se detalla en la tabla 3.1, el mismo que indica desperdicio de direcciones y poco orden para poder administrar.

Direccionamiento IP del Departamento Ciencias de la Computación[1]

Tabla 3.1 Asignación de IP'S para la red 10.1.16.0 de los laboratorios generales de computación

10.1.16.1	Utic's	10.1.16.51	10.1.16.101		10.1.16.151	RemoteDesktop	10.1.16.201	ToshibaLABS(L.B.)
10.1.16.2		10.1.16.52	10.1.16.102		10.1.16.152	RemoteDesktop	10.1.16.202	Luis(ServidoresL.B.)
10.1.16.3	SwR8-3C4500-00164	10.1.16.53	10.1.16.103		10.1.16.153	RemoteDesktop	10.1.16.203	
10.1.16.4	SwR8-3C4500-00163	10.1.16.54	10.1.16.104		10.1.16.154	RemoteDesktop	10.1.16.204	SwitchDCC-BloqueH.P.B
10.1.16.5	SwR8-3CWX1200-00166	10.1.16.55	10.1.16.105		10.1.16.155	RemoteDesktop	10.1.16.205	CeciliaHinojosa
10.1.16.6	Sw3C4500-E13	10.1.16.56	10.1.16.106		10.1.16.156	RemoteDesktop	10.1.16.206	
10.1.16.7	Sw3C4200-Ofic.Recepción	10.1.16.57	10.1.16.107		10.1.16.157		10.1.16.207	FaustoGranda
10.1.16.8	SwR10-3C4500-LabsP.B.	10.1.16.58	10.1.16.108		10.1.16.158		10.1.16.208	IlianaSolís
10.1.16.9	Sw3C4200-Ofic-P.B.	10.1.16.59	10.1.16.109		10.1.16.159		10.1.16.209	PedroCasame
10.1.16.10	Sw3C4500-RackServidores	10.1.16.60	10.1.16.110	Temporal	10.1.16.160		10.1.16.210	HugoYépez
10.1.16.11		10.1.16.61	10.1.16.111	Temporal	10.1.16.161		10.1.16.211	MarcoRivera
10.1.16.12		10.1.16.62	10.1.16.112	Temporal	10.1.16.162		10.1.16.212	LucíaNinahualpa
10.1.16.13		10.1.16.63	10.1.16.113	Temporal	10.1.16.163		10.1.16.213	EdgarPérez
10.1.16.14		10.1.16.64	10.1.16.114	Temporal	10.1.16.164		10.1.16.214	CarlosRojas
10.1.16.15		10.1.16.65	10.1.16.115	Temporal	10.1.16.165		10.1.16.215	TatianaNoboa
10.1.16.16		10.1.16.66	10.1.16.116	Temporal	10.1.16.166		10.1.16.216	FaustoGranda
10.1.16.17		10.1.16.67	10.1.16.117		10.1.16.167		10.1.16.217	FaustoGranda
10.1.16.18		10.1.16.68	10.1.16.118		10.1.16.168		10.1.16.218	
10.1.16.19		10.1.16.69	10.1.16.119		10.1.16.169		10.1.16.219	
10.1.16.20		10.1.16.70	10.1.16.120		10.1.16.170		10.1.16.220	FibreCatsx80-Ctrl-A
10.1.16.21		10.1.16.71	10.1.16.121		10.1.16.171		10.1.16.221	
10.1.16.22		10.1.16.72	10.1.16.122		10.1.16.172		10.1.16.222	FibreCatsx80-Ctrl-B
10.1.16.23		10.1.16.73	10.1.16.123		10.1.16.173		10.1.16.223	ServidordeArchivos
10.1.16.24		10.1.16.74	10.1.16.124		10.1.16.174		10.1.16.224	PrimePower250
10.1.16.25		10.1.16.75	10.1.16.125		10.1.16.175		10.1.16.225	ServidordeLicencias
10.1.16.26		10.1.16.76	10.1.16.126		10.1.16.176		10.1.16.226	ServidorBPC
10.1.16.27		10.1.16.77	10.1.16.127		10.1.16.177		10.1.16.227	ServidorAntivirus
10.1.16.28		10.1.16.78	10.1.16.128		10.1.16.178		10.1.16.228	Brocade300A
10.1.16.29		10.1.16.79	10.1.16.129		10.1.16.179		10.1.16.229	ActiveDirectory-01

[1] Año 2011

10.1.16.30	10.1.16.80	10.1.16.130	10.1.16.180	10.1.16.230 Brocade300B
10.1.16.31	10.1.16.81	10.1.16.131	10.1.16.181	10.1.16.231 ActiveDirectory-02
10.1.16.32	10.1.16.82	10.1.16.132	10.1.16.182	10.1.16.232 Primergy05
10.1.16.33	10.1.16.83	10.1.16.133	10.1.16.183	10.1.16.233
10.1.16.34	10.1.16.84	10.1.16.134	10.1.16.184	10.1.16.234 Primergy04
10.1.16.35	10.1.16.85	10.1.16.135	10.1.16.185	10.1.16.235
10.1.16.36	10.1.16.86	10.1.16.136	10.1.16.186	10.1.16.236 Primergy03
10.1.16.37	10.1.16.87	10.1.16.137	10.1.16.187	10.1.16.237
10.1.16.38	10.1.16.88	10.1.16.138	10.1.16.188	10.1.16.238 Primergy01

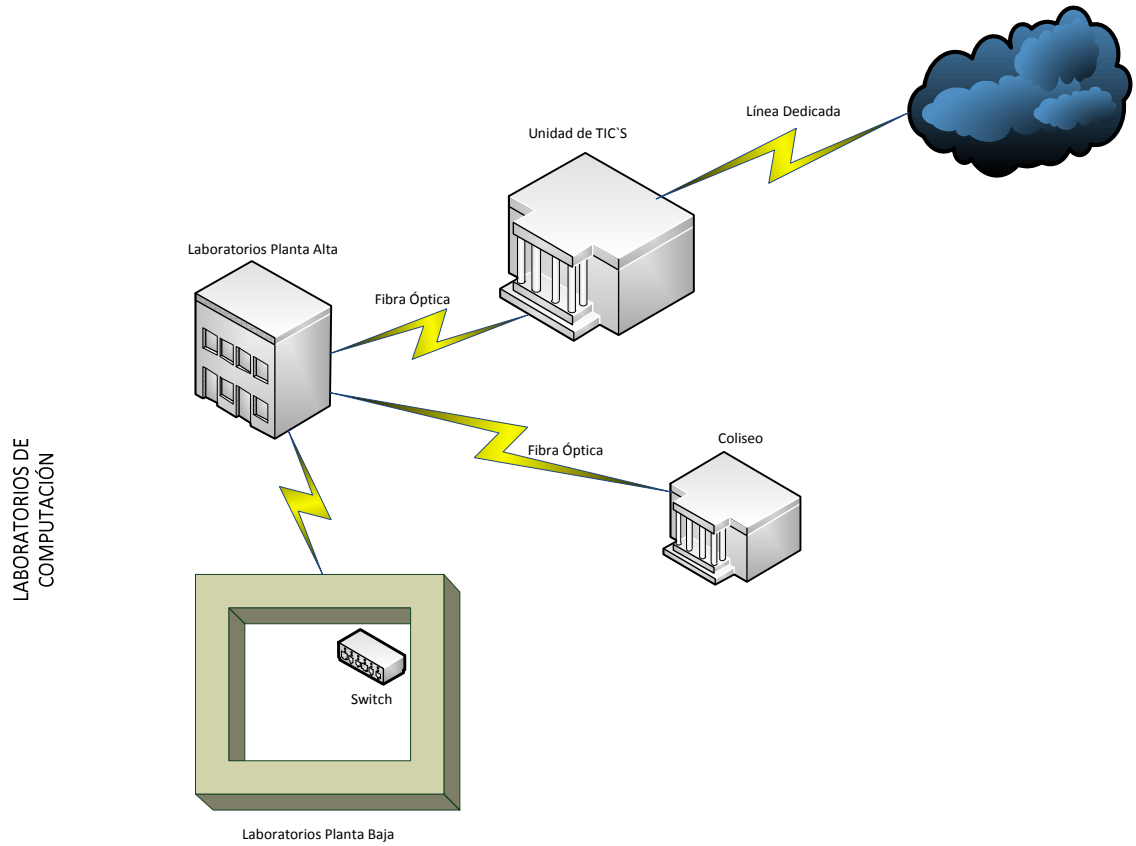


Figura 3.3 Enlace global crossing- laboratorios de computación[2]

Dentro del enlace global se aprecia que mediante fibra óptica desde la Unidad de las TIC`S llega al segundo piso del edificio de la MED, donde se recepta y mediante un switch se distribuye a todas las aulas que corresponden a los laboratorios de computación (véase la figura 3.3).

[2] Año 2011

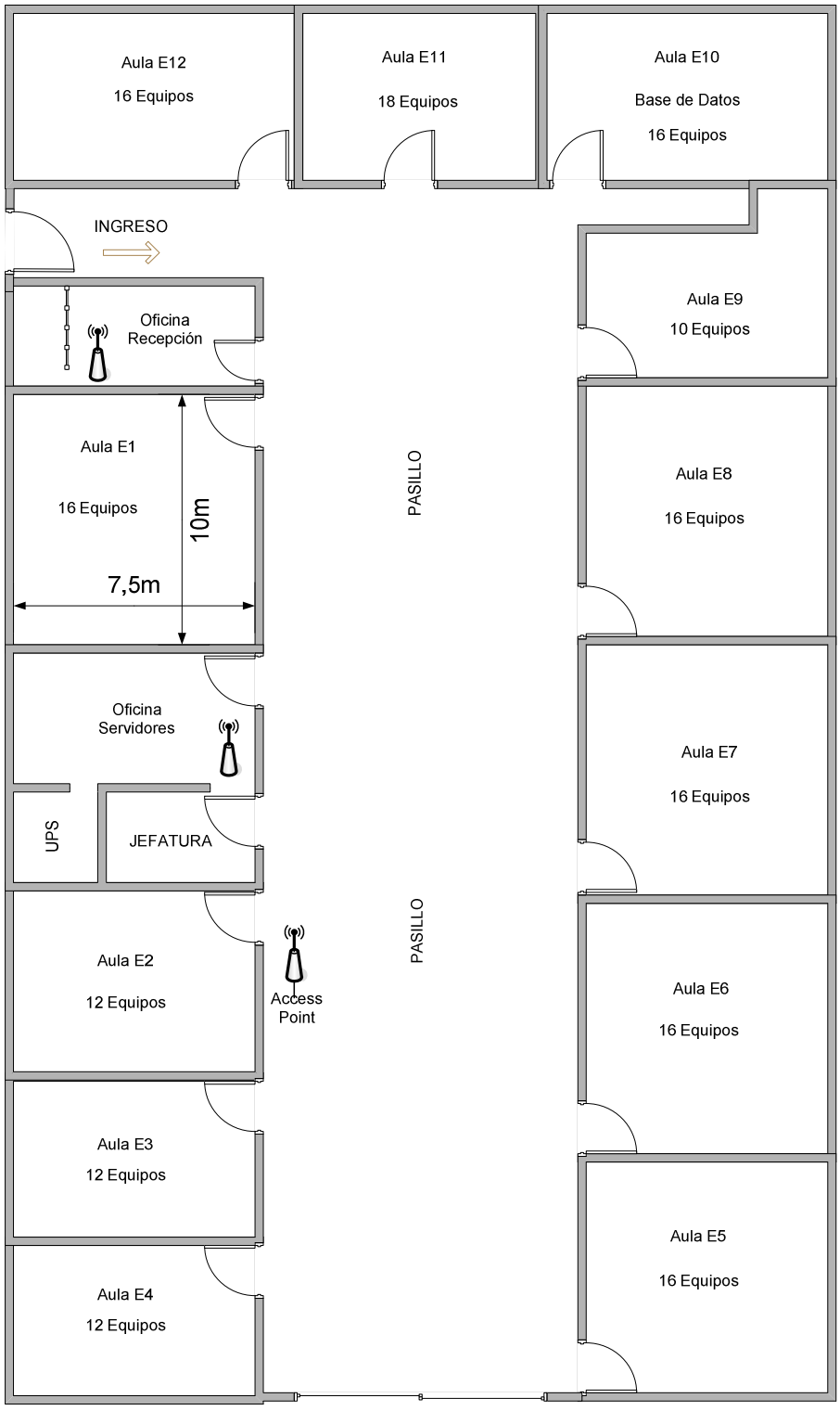


Figura 3.4 Laboratorios de computación-segundo piso[3]

[3] Año 2011

Se puede observar mediante la figura 3.4 como está distribuidos los laboratorios que pertenecen al edificio de la MED, donde señala el número de equipos que tiene cada aula, la ubicación de cada AP para brindar internet vía wireless. En el segundo piso se encuentra la oficina de servidores donde se administran los recursos para todos los laboratorios de computación, se puede observar la figura 3.5 como está distribuido y la ubicación de los servidores.

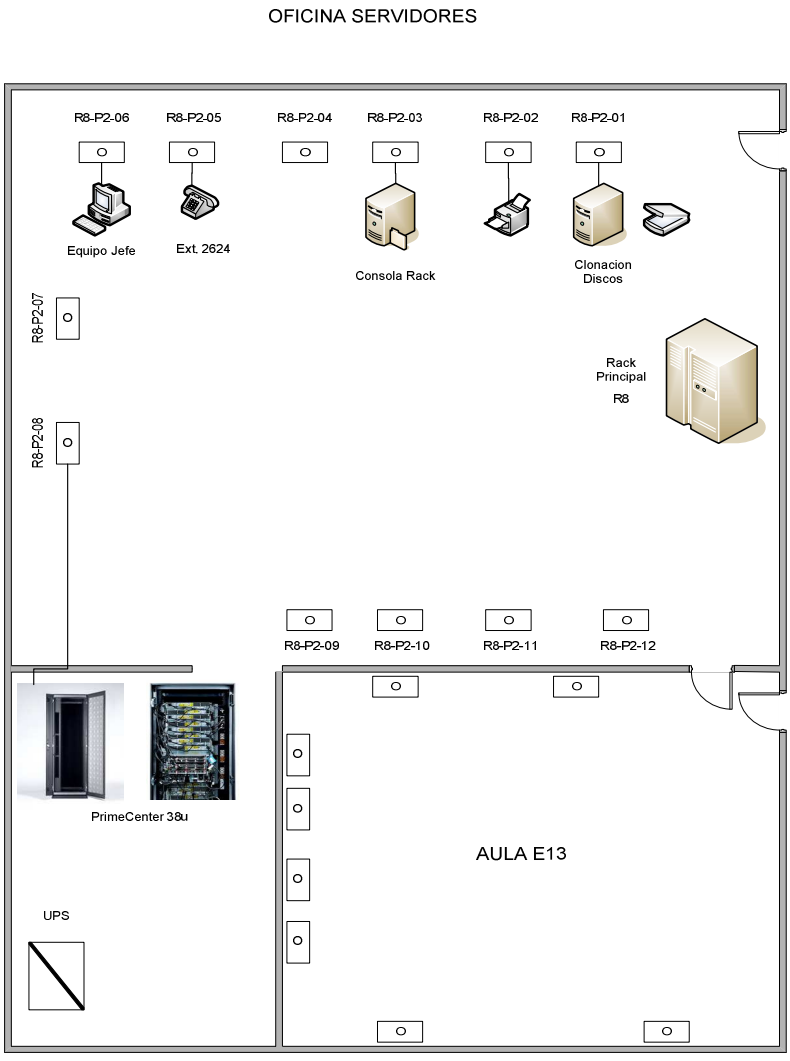


Figura 3.5 Oficina de servidores

En la figura 3.6 Se puede apreciar de manera detallada como está compuesto el servidor de aplicaciones.

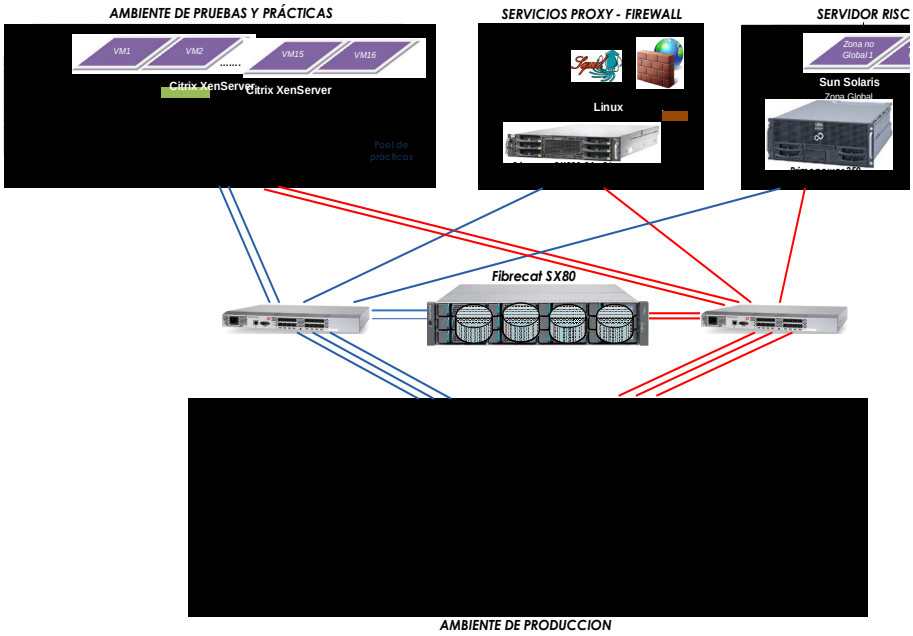


Figura 3.6 Servidor de Aplicaciones Fujitsu

El Control de ancho de banda que se propone para las redes que pertenecen a la Institución, combina diversas estrategias inteligentes y herramientas escalables, ofrece una solución completa para implementar y aplicar políticas de control del ancho de banda en toda la LAN de la Institución. Mediante estas estrategias, los departamentos pueden asignar con mayor eficacia y razonabilidad los recursos de la red.

3.1.1 Switch principal del DCC

En la actualidad se trabaja con un switch de capa 3 para la distribución de red en el Departamento (véase la figura 3.7).

Información del Producto:

Clave de Artículo:	57889
Modelo del Fabricante:	3CR17761-91

3com [1]

Figura 3.7 Switch principal

3.1.1.1 **Características y Ventajas**

Para un análisis con mayor profundidad se consideró conocer las características de este equipo para poder proporcionar información real del mismo.

- **Conectividad Gigabit Ethernet de alto desempeño, segura y preparada para voz**

El 3Com® Switch 4500G es un switch 10/100/1000 Ethernet agrupable en cluster que proporciona una conectividad de LAN segura y flexible, así como funcionalidades avanzadas optimizadas para voz tales como VLAN automática de voz y QoS. El soporte de enlaces ascendentes 10-Gigabit opcionales mediante módulos de conexión local o transceptores XFP proporciona conexiones de alta velocidad con otros dispositivos equipados de forma similar. El Switch 4500G ofrece switching de Capa 2 y routing dinámico de Capa 3, así como robustas funcionalidades de seguridad, Calidad de Servicio (QoS) y administración para proporcionar una conectividad de extremo inteligente para las aplicaciones empresariales esenciales. Este switch ofrece una escalabilidad apilable con administración mediante una única dirección IP.

- **Seguridad avanzada**

Las funcionalidades de seguridad de clase empresarial incluyen login de red IEEE 802.1X, login de dispositivo encriptado SSH/SSL, listas de control de acceso (ACLs) y RADA (acceso a dispositivos autenticados mediante RADIUS), protegiendo así las aplicaciones empresariales de misión crítica.

- **Conectividad de red preparada para voz**

Minimiza el coste y la complejidad asociados con la instalación adicional o el traslado de teléfonos IP: el Switch 4500G detecta la presencia de teléfonos IP, y asigna dinámicamente puertos de switching a la VLAN de voz, permitiendo así una configuración y priorización automatizadas del tráfico de voz sobre IP (VoIP).

- Acceso y distribución avanzados para pequeñas y medianas empresas que desean construir una red convergente segura.
- 24 puertos 10BASE-T/100BASE-TX/1000BASE-T con auto-negociación, 4 de los cuales son Gigabit de uso dual 10/100/1000 o SFP.
- Desempeño a velocidad de cable sin bloqueo: capacidad agregada de switching de hasta 128 Gbps.
- Switching de Capa 2; el routing dinámico de Capa 3 incrementa el desempeño y mejora la seguridad de la red.
- Añada switches al cluster cuando sea necesario sin incrementar la dificultad y el gasto de administración y adminístrelos todos como una única entidad.
- Se pueden agrupar 32 dispositivos en cluster (Switch 4200G, 4500G y switches 5500 y 5500G).
- El control de acceso de red IEEE 802.1X ofrece seguridad basada en estándares.
- El RADA (acceso a dispositivo autenticado mediante RADIUS) permite la autenticación de los dispositivos conectados mediante la

dirección MAC, para un nivel adicional de seguridad de los puntos de entrada a la red.

- La asignación automática de tráfico VoIP a VLANs dedicadas, ayuda a garantizar que el tráfico crítico sensible al tiempo consigue la prioridad necesaria para unas comunicaciones de calidad.
- 2 ranuras traseras para módulos 10-Gigabit de 2 puertos, conexión local CX4 o basada en XFP. [2]

El switch se encuentra en el rack del segundo piso de la MED, como lo indica la figura 3.8 en la oficina de servidores.

Figura 3.8 Switch principal - Oficina de Servidores

En la figura 3.9 se aprecia de mejor manera un acercamiento al switch principal del DCC.

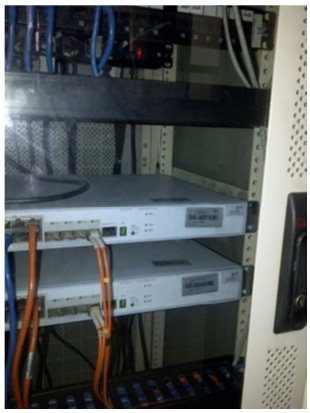


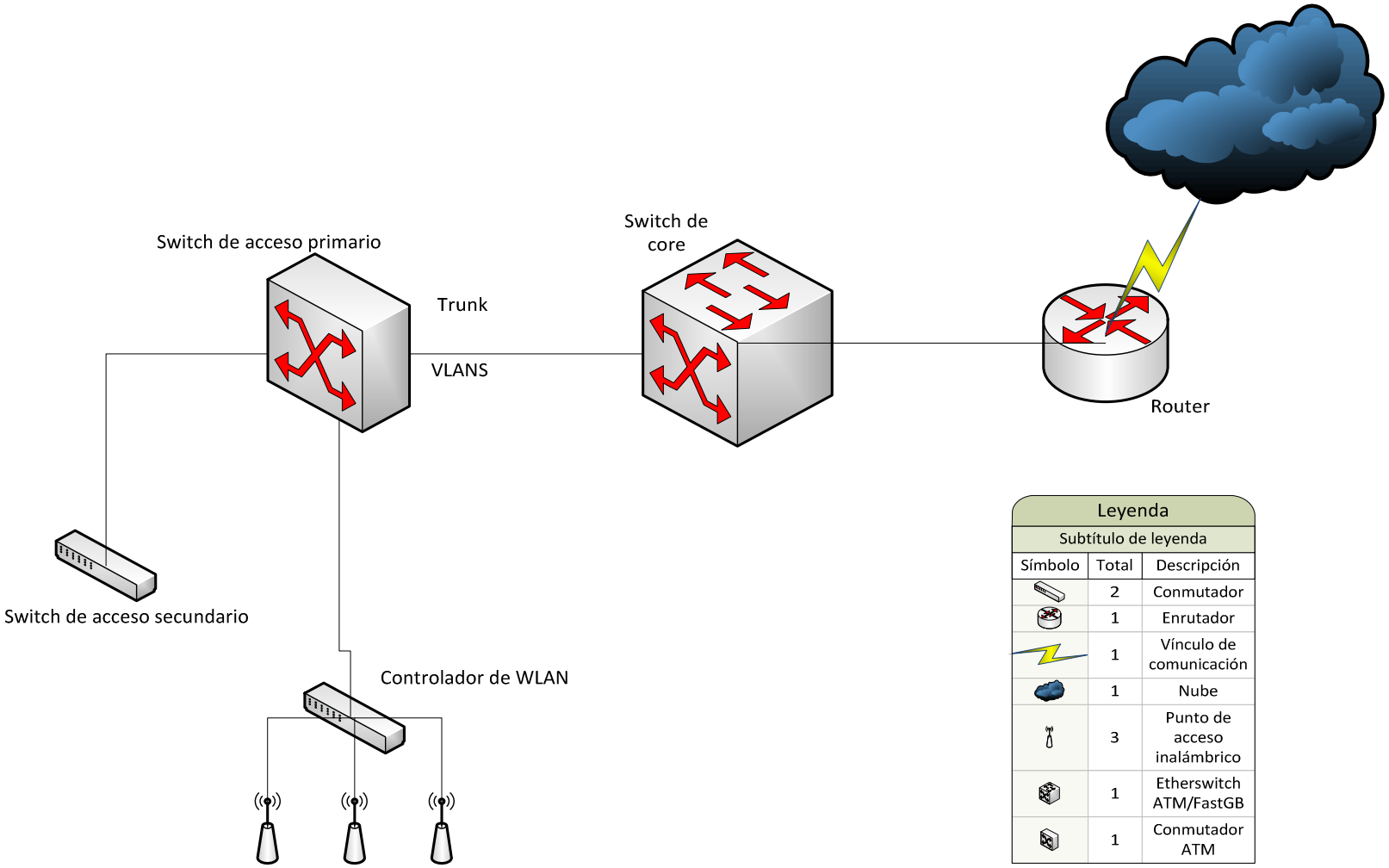
Figura 3.9 Switch principal – Acercamiento

3.2 RED 2011 DCC

Dentro de la red actual la UTIC cuenta con la administración del router principal y de un switch que por medio de fibra óptica proporciona servicios de red a toda la Institución. En el DCC se recibe la fibra por medio del switch principal y existe otro switch que se utiliza para la distribución en los laboratorios que corresponden al DCC que se encuentran en la MED. Se puede apreciar en la figura 3.10 la red actual que actualmente trababa el DCC.

ESPACIO EN BLANCO INTENCIONAL

Figura 3.10 LAN ACTUAL



3.3 INDICADORES DE RENDIMIENTO DEL SERVICIO.

Los indicadores permiten compararlos con los objetivos fijados y si fuera necesario mejorar el propio plan o sus resultados en el futuro. Para este proyecto se obtendrá los indicadores de rendimiento en base a encuestas. Para tomar medidas reales se ha obtenido información por medio de encuestas, con un muestreo sistemático por lo cual se dividió la población en 3 segmentos que son: alumnos, docentes y administrativos, como se puede apreciar en la tabla 3.2 que indica el número de su población.

Tabla 3.2 Población total DCC 2011

Segmento	Población
Alumnos[4]	700
Docentes[5]	102
Administrativos[6]	10

Se ha realizado una encuesta para cada segmento, tres encuestas donde el número de encuestas realizadas será tomado de una muestra poblacional con su respectivo segmento bajo la siguiente fórmula estadística:

$$\boldsymbol{n = \frac{Z^2 * p * q * N}{N * e^2 + Z^2 * p * q}}$$

Dónde:

N: Es el tamaño de la población o universo (número total de posibles encuestados).

p: Proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p=q=0.5 que es la opción más segura.

q: Proporción de individuos que no poseen esa característica, es decir, es 1-p.

[4] Fuente: Director DCC
[5] Fuente: Director DCC
[6] Fuente: Director DCC

$Z_{\alpha/2}$: Valor de Z correspondiente al riesgo α fijado. El riesgo α fijado suele ser 0,05 y $Z_{\alpha/2}$ de 1,96.

e: Es el error muestral deseado. El error muestral es la diferencia que puede haber entre el resultado que obtenido preguntando a una muestra de la población y el que se obtendrá si preguntara al total de ella. Por lo general se trabaja con el 5%.

3.3.1 **Muestra de cada segmento**

3.3.1.1 **Alumnos**

Se conoce que la población del segmento es de 700 y por medio de la aplicación de la fórmula se sabrá el número de encuestas que se realizará al alumnado del DCC. Se tomó la muestra de los últimos niveles de la carrera, porque ellos tienen mayor conocimiento y apoyará con un su criterio técnico sobre el tema a tratar en las encuestas.

Se remplaza los datos que ya se conoce:

3.3.1.2 **Docentes**

La población de este segmento es de 102 donde 35 docentes son tiempo completo y 67 docentes son de horas clase. Como los docentes tiempo completo utilizan la mayoría de los servicios de red se ha tomado la muestra de 35 docentes haciendo referencia a los docentes a tiempo completo.

Se remplaza los datos que ya conoce:

3.3.1.3 **Administrativos**

Como la población es muy pequeña se realizará la encuesta a las 10 personas que están a cargo de lo administrativo en el DCC. Por lo tanto se obtiene esta tabla de valores sobre el número de personas que será una ayuda con la encuesta. Por medio de los cálculos realizados se obtuvo la tabla 3.3.

Tabla 3.3 Población

Segmento	Tamaño de la muestra
Alumnos	169
Docentes	33
Administrativos	10

3.3.2 **Encuesta**

Las encuestas son elaboradas por usuarios que pertenecen solo al Departamento Ciencias de la Computación que utilizan los servicios proporcionados por la Institución, lo cual son una herramienta esencial combinada con los indicadores, para el análisis de la situación actual de los servicios de red. Este documento se ha basado en los indicadores de rendimiento para señalar directamente los factores que afectan el rendimiento del servicio de red y evidenciar la aprobación de los usuarios. La misma encuesta es realizada a los tres segmentos, solo se varió la última

pregunta ya que los servicios de red que tiene cada segmento no son los mismos. Donde los docentes y administrativos realizaron una encuesta igual y los estudiantes elaboraron una encuesta similar. Las cuatro primeras preguntas son las mismas en las 2 diferentes encuestas y así se podrá apreciar de mejor manera que diferencias existe en los segmentos propuestos. La quinta pregunta varía para poder diferenciar las necesidades que tiene cada segmento y así dar prioridad de servicios a cada uno de los segmentos sin olvidar que también se considerará el número de usuarios que pertenecen a cada uno de ellos. También se ha considerado a personas que tienen mayor contacto con los servicios ofrecidos por la Institución y así poder obtener datos reales por medio de las encuestas, cada pregunta utilizada en la encuesta cumple un objetivo que ayudará al análisis de este proyecto y así evidenciar claramente los pros y contras que se sostienen en los servicios de red. Dentro de las encuestas no se pidió ningún tipo de datos a todos los encuestados para que no sientan compromiso con sus respuestas y contesten con honestidad.

3.3.2.1 **Resultados de las encuestas**

El resultado de las encuestas elaboradas a los usuarios del Departamento Ciencias de la Computación se mide mediante índices de difusión. El conteo de todas las encuestas fue de forma manual para tener mayor veracidad y seguridad sobre los resultados de las mismas. Se puede observar las plantillas de las encuestas que se realizaron a los 3 segmentos en el ANEXO D donde se encuentran las encuestas realizadas a los usuarios del DCC. El conteo de los datos se los puede apreciar en las tablas: 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17 y 3.18. Para conocer el

porcentaje de los resultados de los diferentes segmentos se puede apreciar en los gráficos: 3.11, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.19, 3.20, 3.21, 3.22, 3.23, 3.24 y 3.25.

Resultados de las encuestas realizadas a los estudiantes

- **Pregunta 1.**

  ¿Considera que los servicios de red de la ESPE son?

Tabla 3.4 Pregunta 1 - Estudiantes

Opciones	Conteo
Excelente	0
Muy bueno	0
Bueno	13
Regular	61
Malo	95
TOTAL	**169**

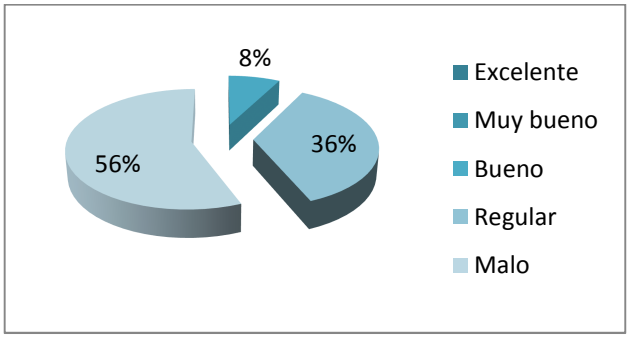


Figura 3.11 Conteo Pregunta 1 – Estudiantes

En su mayoría la opción *Malo* marca una gran insatisfacción del alumnado donde claramente se evidencia la desaprobación que existe y se requiere una mejora en los servicios que se ofrece.

- **Pregunta 2.**

¿Considera que el acceso de servicio web de la ESPE es?

Tabla 3.5 Pregunta 2 - Estudiantes

Opciones	Conteo
Rápido	0
Intermedio	34
Lento	135
TOTAL	**169**

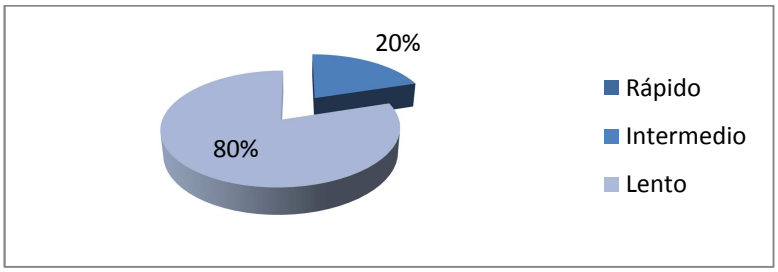


Figura 3.12 Conteo Pregunta 2 – Estudiantes

Esta pregunta va de la mano con la pregunta número 1, se indica uno de los motivos por el cual existe desaprobación de los usuarios, señala directamente una gran expectativa que tiene el usuario y donde se pueda arreglar una parte del problema que existe actualmente.

- **Pregunta 3.**

¿Considera que debe mejorar el acceso de servicio web de la ESPE?

Tabla 3.6 Pregunta 3 - Estudiantes

Opciones	Conteo
Si	165
No	4
TOTAL	**169**

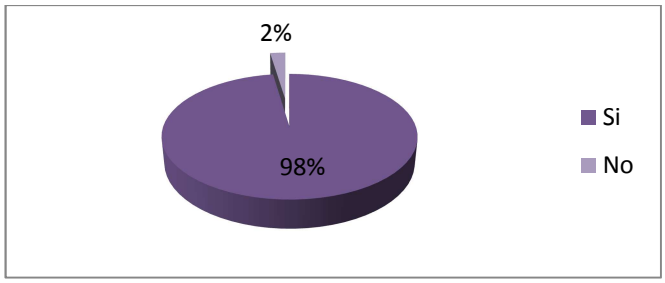


Figura 3.13 Conteo Pregunta 3 – Estudiantes

En relación a la figura 3.13 se puede considerar que el alumnado espera que exista mejora del acceso de servicio web, por lo cual en base a este resultado se requiere un cambio, por lo general muchos alumnos asocian con la velocidad. Mediante este resultado se considerará los cambios que se podrá realizar en este proyecto.

- **Pregunta 4**

¿Está de acuerdo con las restricciones de acceso que hay en los servicios de red?

Tabla 3.7 Pregunta 4 - Estudiantes

Opciones	Conteo
Si	7
No	162
TOTAL	**169**

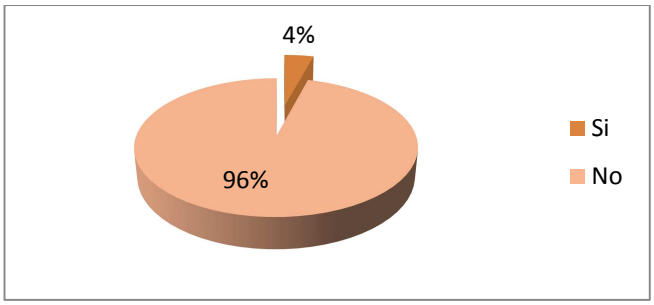


Figura 3.14 Conteo Pregunta 4 – Estudiantes

Mediante este resultado, relacionado con la pregunta número 4 de la encuesta presenta que el grupo de usuarios encuestados presentan desacuerdo a las restricciones establecidas actualmente por lo cual se deberá reconsiderar la población de usuarios y los servicios que se utilizan con fin académico, así cada restricción será validada antes de ser establecida.

- **Pregunta 5**

¿Qué servicios de internet más utiliza?

Tabla 3.8 Pregunta 5 - Estudiantes

Opciones	Conteo
MSN	116
Facebook	74
Buscadores	133
Correo	134

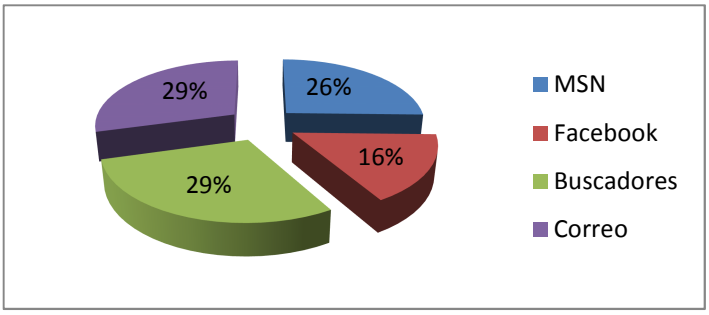


Figura 3.15 Conteo Pregunta 5 – Estudiantes

Las opciones que lleva a una mayoría son: Correo, Buscadores y Messenger.

Las tres opciones son herramientas de trabajo y de estudio, actualmente existe restricciones en las tres opciones. Se debe considerar como objetos claves para el alumnado y retomar las restricciones existentes.

Resultados de las encuestas realizadas a los Docentes

- **Pregunta 1.**

¿Considera que los servicios de red de la ESPE son?

Tabla 3.9 Pregunta 1 – Docentes

Opciones	Conteo
Excelente	0
Muy bueno	0
Bueno	9
Regular	16
Malo	8
TOTAL	**33**

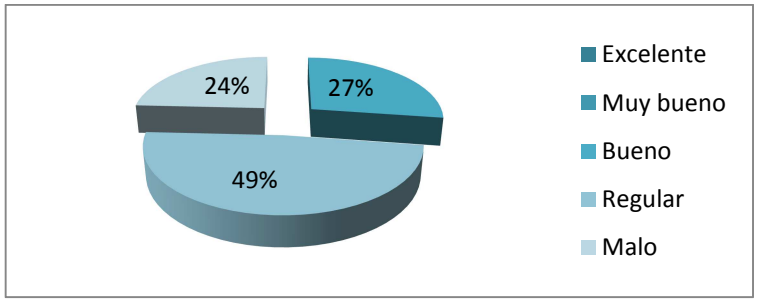


Figura 3.16 Conteo Pregunta 1 – Docentes

El resultado obtenido varía con respecto al análisis de la encuesta anterior ya que se aprecia la opción *regular* que representa la mayoría con 49%, aun así solo se sube un escalón porque se aprecia la inconformidad del usuario, tomando en cuenta que el personal que comprenden los docentes cuentan con mayores privilegios que el alumnado.

- **Pregunta 2.**

¿Considera que el acceso de servicio web de la ESPE es?

Tabla 3.10 Pregunta 2 - Docentes

Opciones	Conteo
Rápido	0
Intermedio	8
Lento	25
TOTAL	**33**

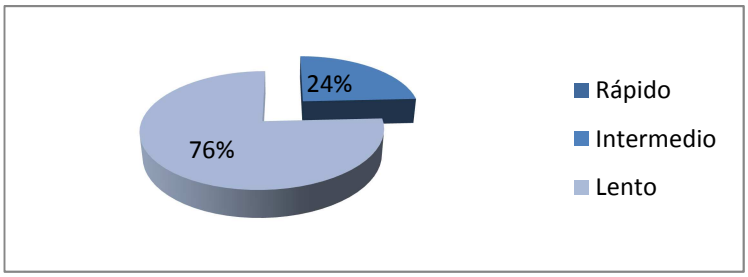


Figura 3.17 Conteo Pregunta 2 – Docentes

Se mantiene una gran diferencia dentro de las repuestas entre alumnado y docentes, la determinación como *lento* evidencia la inconformidad de ambos segmentos marcando un gran porcentaje.

- **Pregunta 3.**

¿Considera que debe mejorar el acceso de servicio web de la ESPE?

Tabla 3.11 Pregunta 3 - Docentes

Opciones	Conteo
Si	0
No	33
TOTAL	**33**

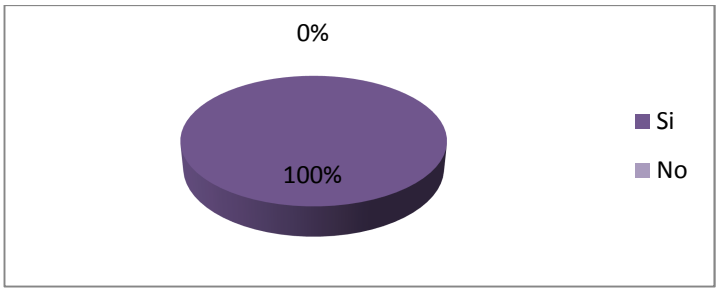


Figura 3.18 Conteo Pregunta 3 – Docentes

Por medio del resultado obtenido, se puede evidenciar que la población considerada para la encuesta requiere mejoras para el acceso de servicio web y por medio de este resultado se considerará el desacuerdo de los docentes de este segmento.

- **Pregunta 4.**

¿Está de acuerdo con las restricciones de acceso que hay en los servicios de red?

Tabla 3.12 Pregunta 4 - Docentes

Opciones	Conteo
Si	4
No	29
TOTAL	**33**

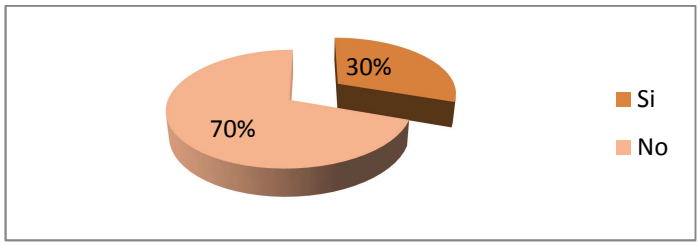


Figura 3.19 Conteo Pregunta 4 – Docentes

Se mantiene la gran diferencia entre respuestas, en este segmento también se debe considerar la restructuración de restricciones, se debe tomar en

cuenta la calidad en los servicios de red para que el usuario se sienta a gusto con los servicios prestados.

- **Pregunta 5.**

Enumere los servicios de red que más utiliza

Tabla 3.13 Pregunta 5 - Docentes

Opciones	Conteo
MAIL	29
DHCP	5
HTTP	41
FTP	3
DNS	3

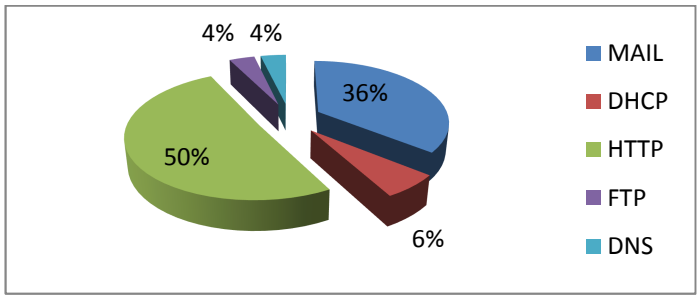


Figura 3.20 Conteo Pregunta 5 – Docentes

Se aprecia que los servicios más utilizados son: Mail y HTTP. Actualmente los dos servicios son herramientas de trabajo, mail es la herramienta más importante ya que así se mantiene comunicación entre alumnos-docentes o docentes-docentes, en base a estos resultados se obtiene información básica para poder administrar y considerar los privilegios que se puede otorgar a los docentes.

Resultados de las encuestas realizadas a los Administrativos

- **Pregunta 1.**

¿Considera que los servicios de red de la ESPE son?

Tabla 3.14 Pregunta 1 - Administrativos

Opciones	Conteo
Excelente	0
Muy bueno	1
Bueno	6
Regular	2
Malo	1
TOTAL	**10**

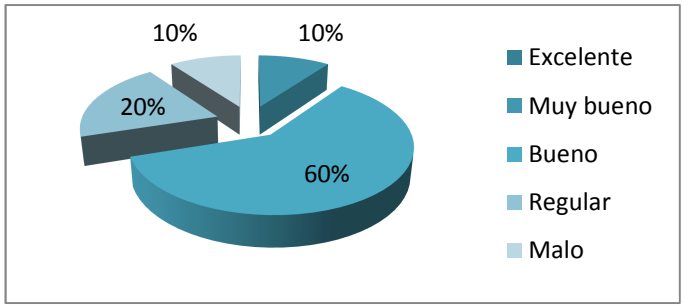


Figura 3.21 Conteo Pregunta 1 – Administrativos

Dentro de este segmento se realizó la encuesta a las secretarias y a los administrativos que brindan su servicio en el edificio de la MED, aquí existe una mezcla de resultados ya que parte de las secretarias del DCC tienen menor conocimiento sobre el tema. De todas maneras el resultado obtenido se marca con la mayoría y los otros resultados, los trabajadores administrativos tienen más servicios a su disponibilidad, ellos lo pueden manejar y las restricciones que tienen son en menor grado.

- **Pregunta 2.**

¿Considera que el acceso de servicio web de la ESPE es?

Tabla 3.15 Pregunta 2 - Administrativos

Opciones	Conteo
Rápido	1
Intermedio	4
Lento	5
TOTAL	**10**

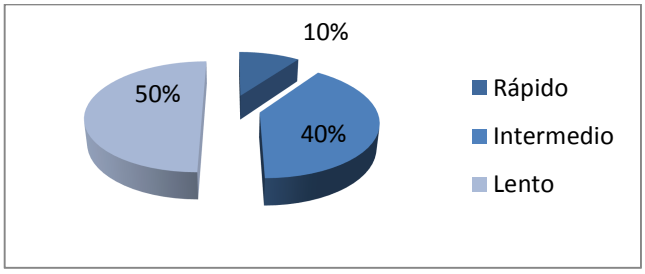


Figura 3.22 Conteo Pregunta 2 – Administrativos

Con el resultado del tercer segmento muestra que existe inconformidad general. Claramente la mayoría de los resultados obtenidos verifica que existe inconformidad en cada uno de los segmentos por la velocidad.

Mediante este resultado ayudará a direccionar un problema a nivel de usuario final.

- **Pregunta 3.**

¿Considera que debe mejorar el acceso de servicio web de la ESPE?

Tabla 3.16 Pregunta 3 - Administrativos

Opciones	Conteo
Si	10
No	0
TOTAL	**10**

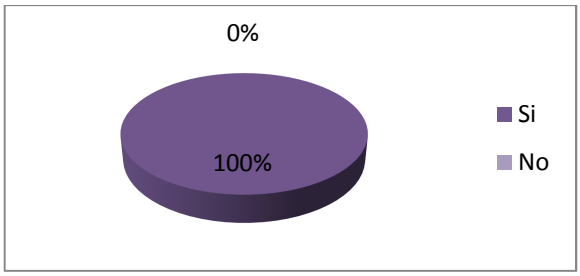


Figura 3.23 Conteo Pregunta 3 – Administrativos

Al obtener 100% indica la desaprobación total de los servicios ofrecidos, en relación a los otros 2 segmentos se puede detallar que es muy evidente la insatisfacción de su mayoría de usuarios.

- **Pregunta 4**

¿Está de acuerdo con las restricciones de acceso que hay en los servicios de red?

Tabla 3.17 Pregunta 4 - Administrativos

Opciones	Conteo
Si	4
No	6
TOTAL	**10**

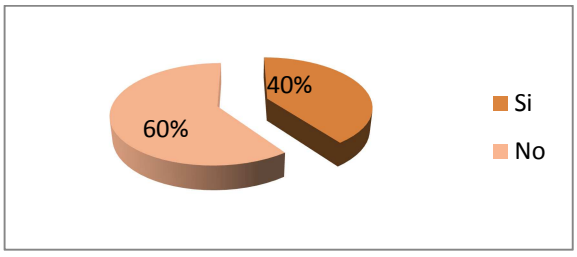


Figura 3.24 Conteo Pregunta 4 – Administrativos

Sobre las restricciones existe una menor diferencia ya que todos los usuarios no cuentan con las mismas restricciones que otros, cabe recalcar que en la misma pregunta la mayoría presenta insatisfacción y esto lleva a retomar las restricciones existentes. Las restricciones pueden existir pero se

debe realizar un análisis previo para aplicarlas y así evitar la incomodidad al usuario y brindar un servicio de calidad.

- **Pregunta 5**

Enumere los servicios de red que más utiliza

Tabla 3.18 Pregunta 5 - Administrativos

Opciones	Conteo
MAIL	7
WEB	8
DNS	2
FTP	2
DHCP	1

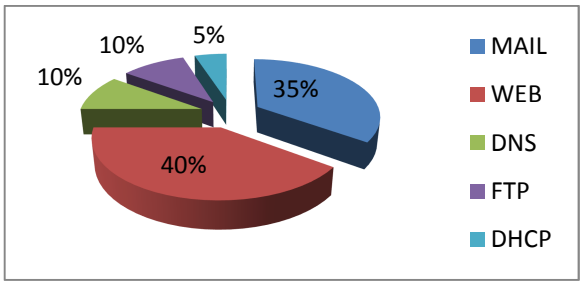


Figura 3.25 Conteo Pregunta 5 – Administrativos

Con este resultado se muestra los servicios más utilizados del segmento "administrativos", dentro de este segmento como herramientas básicas de trabajo son la Web y Mail, tomando en cuenta la utilidad de estos servicios se debe mantener como gran prioridad, eso no quiere decir que no se tomará en cuenta el resto de servicios ofrecidos, cada servicio tiene su importancia, tan solo que con estos resultados se dará prioridad a los servicios más utilizados.

3.3.2.2 **Conclusiones Generales en base a los resultados de las encuestas.**

- En base a la pregunta No. 1 analizado de manera global la mayoría de los resultados obtenidos se enmarca entre regular y malo como calificación de los servicios de red, mediante este resultado se resalta que esta calificación debe variar ya que los usuarios requieren mejoras pero se debe determinar cuáles son los factores que causan los desacuerdos de la población.
- En relación al resultado obtenido de la pregunta No.2 existe un indicador de rendimiento que es la velocidad, muchos usuarios relacionan la calidad con la velocidad, marcando que la velocidad es un factor que ayudará mejorar.
- En atención a la pregunta No.3 se puede apreciar que existe una calificación negativa al respecto sobre el acceso de servicio web, ya que al configurar el proxy para tener acceso a internet no muestra un ambiente amigable para el usuario ya que varios de los mismos no tienen conocimiento de dicha configuración.
- Mediante los resultados obtenidos de la pregunta No.4 se establece que en su mayoría de la población no están de acuerdo con las restricciones establecidas, se debería considerar que el servicio brindado es hacia personas que pertenecen a una comunidad universitaria, por lo cual su grado de cultura es de alto nivel y estas no deberían ser necesarias para los usuarios que pertenecen a la Institución.

- Por medio de los resultados obtenidos en la pregunta No.5 se puede determinar cuáles son los servicios de red que son más utilizados por diferentes tipos de usuarios y así relacionar los privilegios que tendrá cada usuario para que sus necesidades sean atendidas.

En conclusión mediante los datos adquiridos en base de los resultados de las encuestas realizadas y las conclusiones que se han detallado, se ha determinado como indicadores de rendimiento a los datos presentados en la tabla 3.19.

Tabla 3.19 Indicadores de rendimiento

Indicadores
Índice de Satisfacción del Usuario
Facilidad de Acceso
Disponibilidad
Restricciones
Velocidad de Servicio de Internet

3.4 CAPTURA DEL TRÁFICO DE RED

Para realizar el análisis de tráfico de red que existe en el DCC que pertenece a la Escuela Politécnica del Ejército sede Sangolquí se utilizó el software Wireshark 1.6.2, mediante varias opciones se podrá apreciar el tráfico que existe en un día normal de clases. Para la instalación de software se implementó un manual de usuario que se encuentra en el ANEXO B. En las siguientes figuras se puede observar unos contenedores, y se comenzará a capturar todo el tráfico que llegue a nuestro equipo donde está instalado Wireshark. Cabe mencionar que la captura que se presenta en los siguientes figuras son datos tomados en el horario de la mañana, se estima que existe mayor tráfico de red, porque el mayor número de estudiantes

tienen clases en este horario (de 7:15 a 14:00) y en su mayoría el personal administrativo labora mayor tiempo en la mañana ya que su horario comprende de 7:15 a 15:30. Mediante estos datos se procederá obtener y se realizará una comparación para demostrar si lo antes mencionado es sustentado y así encontrar soluciones para mejorarlo.

3.4.1 **Captura de tráfico de red en el horario de la mañana**

En la figura 3.26 se observa el procedimiento de la captura, durante una hora y treinta y un minutos (01:31), se aprecia el porcentaje marcado por cada protocolo indicado. También indica el número total de paquetes capturados señalando el tiempo de corrida del programa.

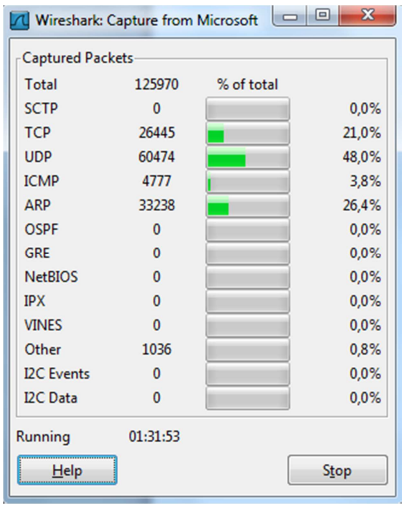


Figura 3.26 Primera captura - Mañana

En la figura 3.27 se observa de cómo se detuvo la captura y así se conoce directamente los datos obtenidos con sus respectivos porcentajes, indicando sus porcentajes, el tiempo transcurrido total es de dos horas y treinta minutos (2:30).

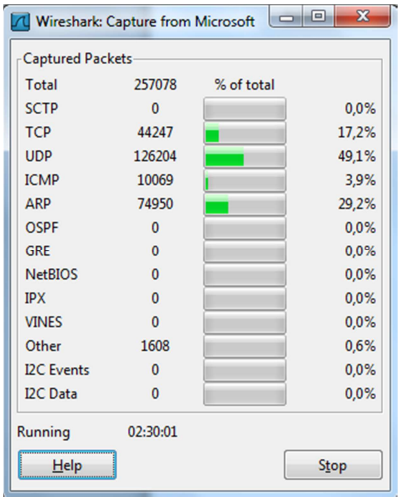


Figura 3.27 Segunda captura - Mañana

Si ya se desea detener el proceso de captura se presiona el botón **Stop** y se procede a guardar los datos con los que se realizará el análisis, con esto se obtiene un respaldo para realizar un robusto estudio del tráfico que existe en la red que pertenece al DCC como muestra la figura 3.28.

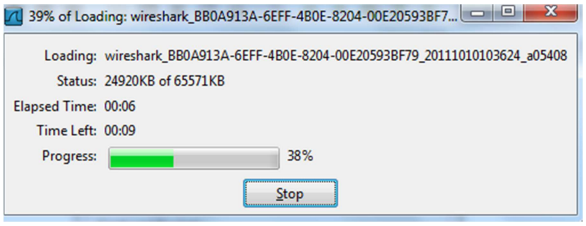


Figura 3.28 Detener captura – Mañana

Wireshark presenta los resultados de la siguiente manera:

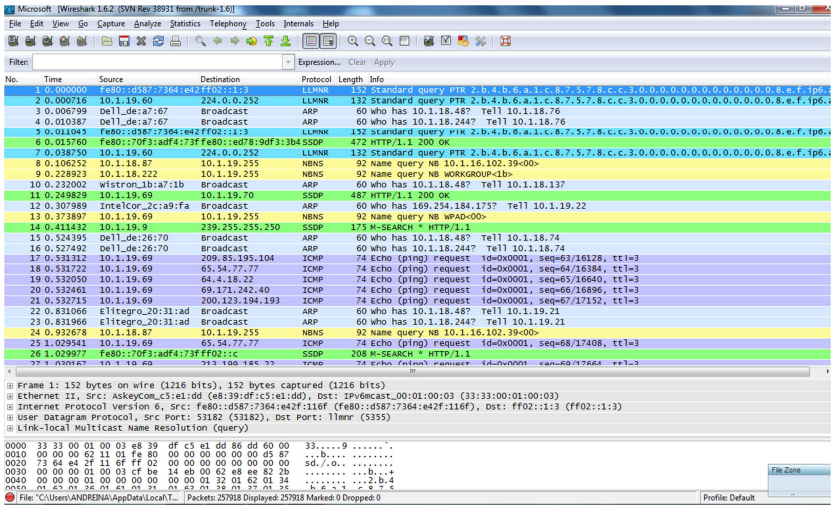


Figura 3.29 Resultado de la captura- Mañana

Como se puede apreciar en la figura 3.29, es la pantalla principal donde se puede apreciar los datos que brinda Wireshark para el análisis del tráfico de red.

3.4.2 **Captura de tráfico de red en el horario de la tarde**

Se realizó el mismo proceso para la captura de paquetes en el horario de la tarde, tomando el mismo tiempo para que la comparación entre los dos horarios sea más pareja. Se puede observar las diferencias entre los porcentajes que se puede observar en la figura 3.30, se aprecia la diferencia entre el tiempo de captura.

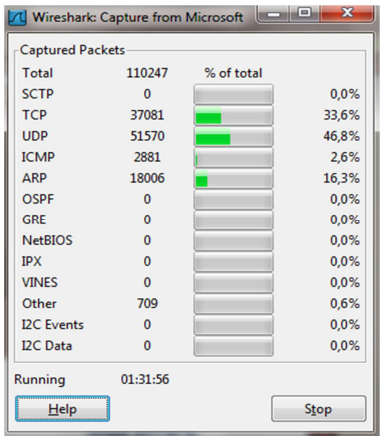


Figura 3.30 Primera captura – Tarde

Con los resultados que muestra la figura 3.31, se trabajó para el análisis del horario de la tarde que tiene la Institución, por medio de estos datos se conocerá el estado actual y se determinará la administración que debe existir. Por medio de estos resultados se conoce el porcentaje de cada protocolo y en base a estos se podrá realizar cálculos que ayudará para el estudio de este proyecto que está basado en el Departamento Ciencias de la Computación (DCC).

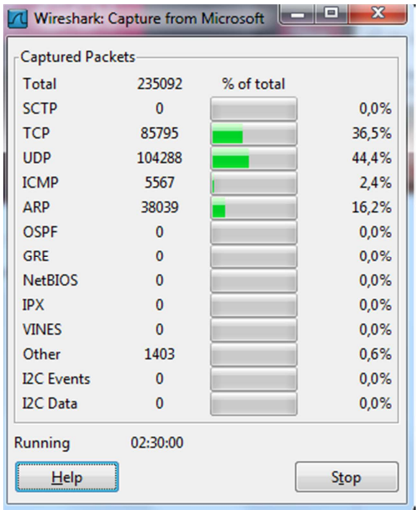


Figura 3.31 Segunda captura- Tarde

Los datos tomados de la medición son del horario vespertino, donde su horario de clases es de 15:00 a 21h30, se considera que esta sección tiene menor tráfico por el menor número de usuarios, en la sección de la mañana asisten otros departamentos que hacen uso de la red que pertenece al DCC. Cumpliendo el objetivo de obtener la captura de algunas tramas, se procede a detener. Cuando se hace clic en el botón **Stop**, el proceso de captura finaliza mostrando la pantalla que muestra la figura 3.32.

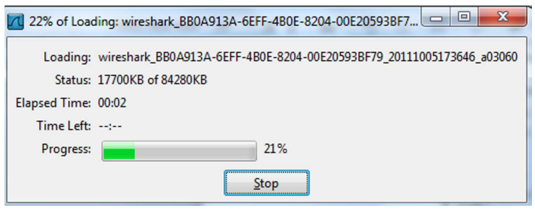


Figura 3.32 Opciones para capturar paquetes

Finalmente llegando a la pantalla principal de visualización de Wireshark donde se muestra todos los paquetes obtenidos a detalle (véase en la figura 3.33).

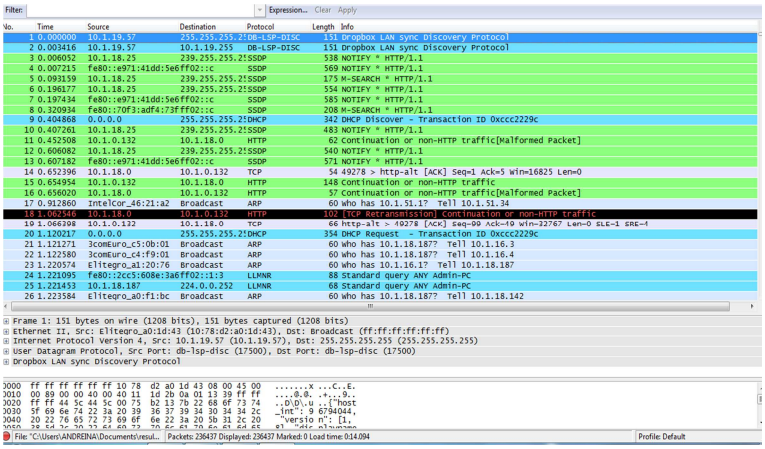


Figura 3.33 Resultado de la captura- Tarde

3.5 DIFERENCIAS Y SIMILITUDES EN LOS RESULTADOS DE LAS CAPTURAS MEDIANTE WIRESHARK

3.5.1 Datos básicos en horarios de la mañana y la noche

En base a las dos capturas de tráfico con la herramienta Wireshark (mañana y tarde) se puede realizar comparaciones estadísticas entre ellas. Dentro de la capturación de tráfico se implementó filtros para obtener información íntegra sobre el estado actual en el que se encuentra la Institución, mediante las dos capturas se realizará el análisis de cada una de ellas y así proceder al reconocimiento de las diferencias y similitudes que existen entre ellas. Desde WireShark se analizó opciones estadísticas de red que son accedidas desde el menú ***Statistics*** que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo. Se manejó estadísticas generales para el estudio del tráfico mediante las opciones que ofrece la herramienta. Los análisis estadísticos realizados son:

- **Summary**, resumen sobre la cantidad de paquetes capturados (véase en la figura 3.34).

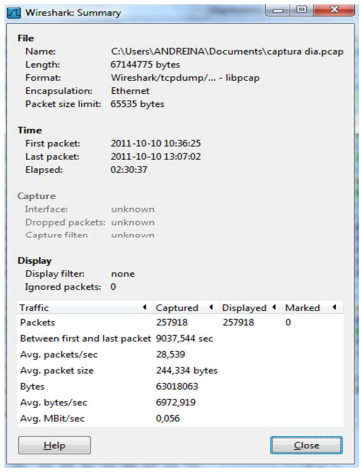


Figura 3.34 Summary – mañana

Mediante esta opción se obtiene un resumen sobre la captura realizada en el horario matutino. Durante el transcurso de 2:30:37, en base a los datos obtenidos de la mañana se obtiene la tabla 3.20 basada en la figura 3.35.

Tabla 3.20 Resultado Summary - mañana

Longitud	67144775 bytes
Límite de tamaño del paquete	65535 bytes

Tráfico	**Capturado**
Paquetes	257918
Promedio de paquetes/seg	28,539
Promedio de tamaño de paquetes	244,334 bytes
Bytes	63018063
Promedio de bytes/seg	6972,919

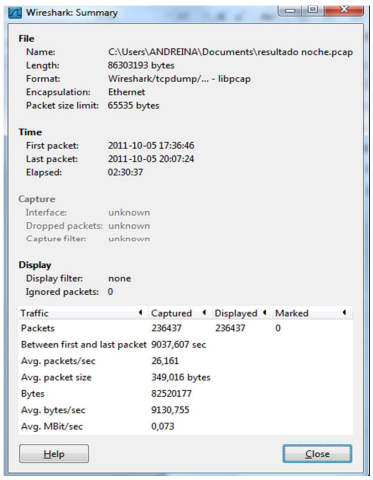


Figura 3.35 Summary – tarde

Durante el transcurso de 2:30:37, mediante el horario vespertino se obtiene los siguientes resultados que describe la tabla 3.21.

Tabla 3.21 Resultado Summary - tarde

Longitud	86303193 bytes
Límite de tamaño del paquete	65535 bytes

Tráfico	**Capturado**
Paquetes	236437
Promedio de paquetes/seg	26,161
Promedio de tamaño de paquetes	349,016bytes
Bytes	82520177
Promedio de bytes/seg	9130,755

Para las capturas tanto la mañana como la tarde se realizó durante el mismo lapso de tiempo que son de 2:30:37. Es evidente que existe mayor tráfico en el horario de la mañana, el número de paquetes capturados es mayor y en base a eso se manifiesta los resultados, se puede observar en las tablas 3.20 y 3.21 muestran el resumen de resultados adquiridos en ambos horarios cada uno, al compararlas existe diferencia en todos los resultados. Cabe mencionar que los datos adquiridos son tomados en un día normal de funcionamiento de la Institución, al finalizar cada parcial dentro de la semana de exámenes existe un tráfico mucho mayor al que se muestra en este proyecto, ya que también comprende entrega de proyectos y una gran cantidad de estudiantes permanecen más tiempo de lo usual dentro de la Institución utilizando servicios. Todos los docentes tienen un tiempo límite para registrar las notas y todo esto ayuda a aumentar el tráfico de red.

3.5.2 **Filtros de protocolos**

Por medio de este resultado se puede concluir el porcentaje de utilización que se tiene en la web, por lo cual se ve la acogida que tiene de todos los

usuarios. Al realizar dos tomas de información a diferentes horarios y compararlas, se conoce cuáles son las horas pico en las que se requiere mayor ancho de banda. Se podrá comparar cuales son las diferencias que existen y bajo qué esquema se podrá tomar diferentes medidas dependiendo de los resultados que existan.

3.5.2.1 **Filtros del horario de la mañana**

Con la captura obtenida en el horario de la mañana se aplicó unos filtros para verificar de cierta forma los resultados de las encuestas y que se pueda determinar qué servicios requieren para asignar mayor prioridad. Según los resultados de las encuestas el servicio mayormente utilizado es HTTP por lo cual se consideró verificar la muestra tomada, el resultado se puede apreciar gráficamente por medio del tiempo transcurrido en líneas, señalando los picos que existen a diferentes intervalos de tiempo. Se consideró a un intervalo de tiempo de 10 segundos para el gráfico que muestra la figura 3.36.

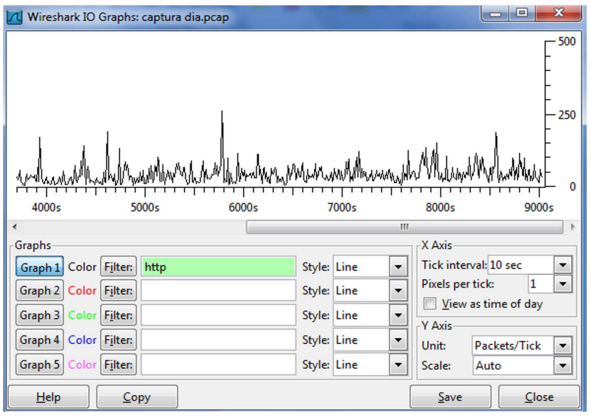


Figura 3.36 Protocolo HTTP – mañana

Por medio de la herramienta se conoce el número de paquetes HTTP obtenidos, tanto como paquetes de solicitud y paquetes de respuesta, señalando el porcentaje de cada uno de ellos, también existe la opción de

otros paquetes HTTP con su respectivo porcentaje como lo muestra figura 3.37.

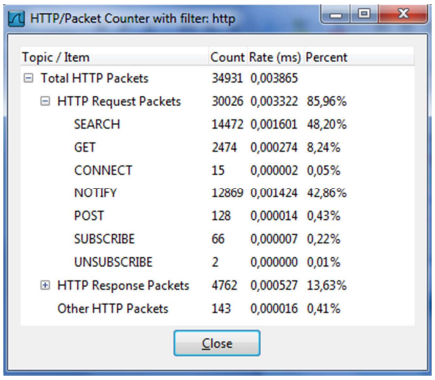


Figura 3.37 Contador de paquetes con filtro – mañana

De manera más resumida se presenta la distribución de carga del protocolo HTTP mediante la figura 3.38.

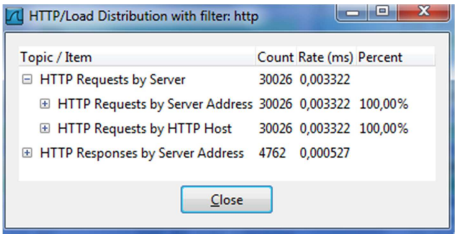


Figura 3.38 Distribución de la carga con filtro – mañana

Una vez obtenida la captura se puede mostrar cada petición de usuarios, se puede mostrar cada página de todos los usuarios que se encontraban utilizando a ciertas horas los servicios, con el conteo del número de usuarios que están ingresados a ciertas direcciones web con promedio mediante porcentaje y la velocidad con la se tiene acceso en cada una de ellas (véase en la figura 3.39). Por medio de estos datos se puede conocer la seguridad establecida que en la actualidad existe, también se conoce el uso institucional y fines académicos que se pueden conseguir con las páginas que está desplegado, mediante los datos obtenidos, también se puede

determinar el comportamiento de los usuarios para acudir a mayores o menores restricciones.

Figura 3.39 Peticiones con filtro – mañana

Se ha considerado dos protocolos y se obtuvo el resultado señalado en el gráfico que plasma en la figura 3.40. Se puede considerar la ausencia de los otros protocolos, se puede estimar que los docentes y administrativos del Departamento Ciencias de la Computación en este intervalo de tiempo no tienen acceso a la web por ser un horario de clase o los usuarios realmente no están usando otros servicios de los que no están indicados en las encuestas.

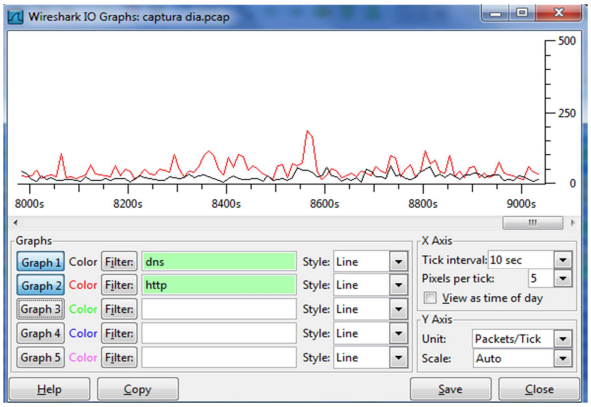


Figura 3.40 HTTP y DNS – mañana

3.5.2.2 **Filtros del horario de la tarde**

Para tener una comparación real se consideraron los mismos datos en los horarios: matutino y vespertino. En el horario vespertino se aprecian picos más elevados y la utilización del servicio es constante (véase en la figura 3.41).

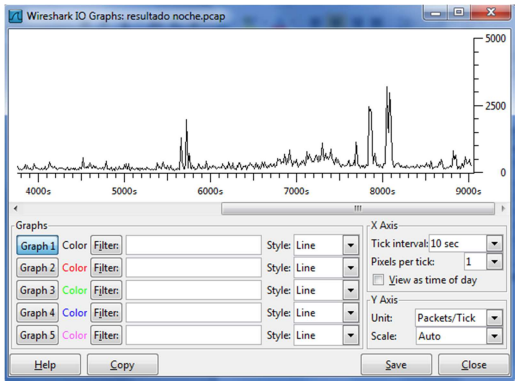


Figura 3.41 Protocolo HTTP – tarde

Por medio de este resultado se puede apreciar que existe menor uso de servicios, la diferencia entre los diferentes horarios es notable su poco porcentaje como muestra la figura 3.42.

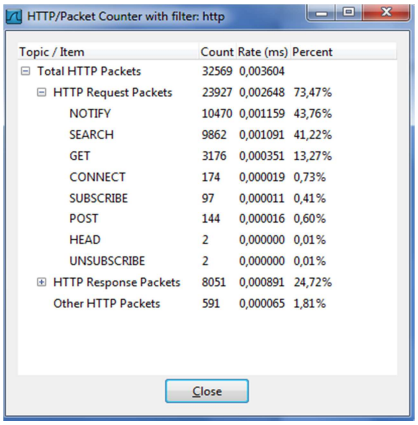


Figura 3.42 Contador de paquetes con filtro – tarde

Mediante de la figura 3.43 se puede asegurar que existe mayor porcentaje de uso de servicios en el horario de la mañana pero con poca diferencia en relación al horario de la tarde de la distribución de carga tanto en los requerimientos como las respuestas.

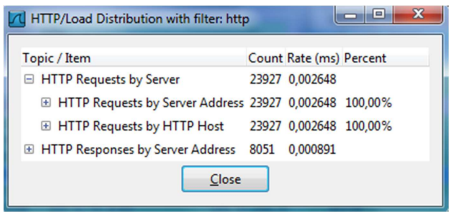


Figura 3.43 Distribución de carga con filtro – tarde

Existen diferencias en las páginas web solicitadas entre los horarios de mañana y tarde, por medio de estos datos se dará constancia si los servicios son utilizados con fin académico y mediante estas especificaciones se podrá validar las restricciones que se encuentran actualmente establecidas. Gracias al conteo (count) presentado en la figura 3.44 se podrá establecer cuáles son las páginas más visitadas por los usuarios de la red del Departamento Ciencias de la Computación y mediante la velocidad de acceso que indica de cada una de ellas.

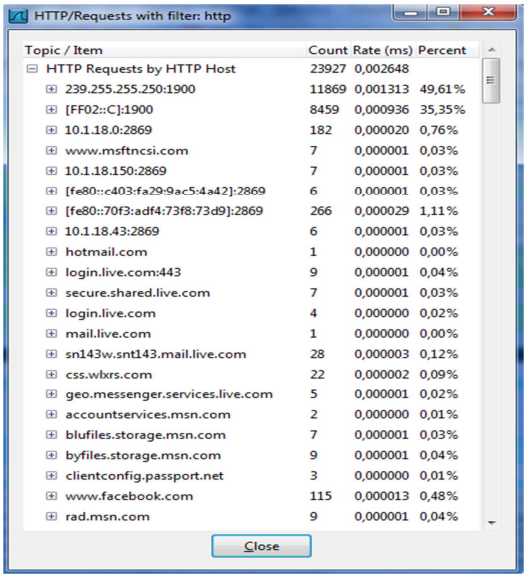


Figura 3.44 Peticiones con filtro – tarde

Al igual que en el horario de la mañana solo se ha encontrado los protocolos HTTP y DNS dentro de la captura realizada, en los resultados de las encuestas están señalados otros protocolos pero tan solo se encuentra los dos antes mencionados, por lo cual se concluye que son protocolos usualmente utilizados en el Departamento Ciencias de la Computación. En el horario de la mañana tanto HTTP como DNS se presentan de comportamiento variable, pero DNS presenta picos más elevados que HTTP, por lo cual el comportamiento es mucho más variable del que se presenta en la tarde. En el horario de la tarde el uso del protocolo DNS permanece constante en un nivel bajo, mientras que HTTP presenta un comportamiento variable con varios picos a diferentes intervalos de tiempo (véase la figura 3.45). Se considera que en la mañana existe mayor número de usuarios ya que varios usuarios son de diferentes departamentos que utilizan las instalaciones ubicadas en el edificio de la MED, lugar donde se encuentran los laboratorios de computación. Y en este mismo horario hay mayor asistencia de estudiantes que se encuentran recibiendo clases.

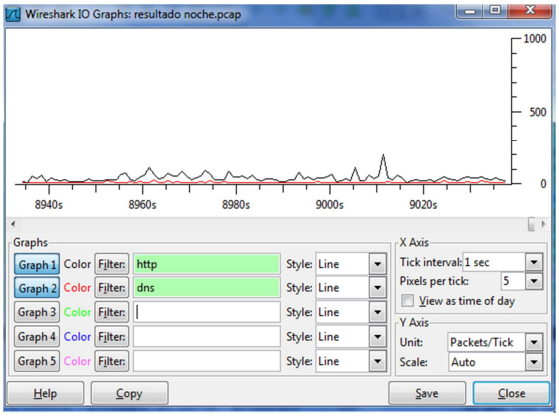


Figura 3.45 HTTP y DNS – tarde

3.6 UBICACIÓN ACTUAL DE LOS PUNTOS DE ACCESO

En los laboratorios del DCC, ubicados en la MED existen 3 puntos de acceso por cada piso. Hay que priorizar la existencia de la red inalámbrica como diseñadores, administradores y propietarios de las instalaciones de las redes inalámbricas, hay que recalcar y dar importancia sobre la existencia del: punto muerto o el agujero de cobertura. Dentro del edificio de la MED se obtiene una cobertura Wi-Fi, pero en ciertos lugares, la cobertura inexplicablemente desaparece o es muy pobre. El punto muerto se encuentra en o cerca del punto más alejado del rango de cobertura del punto de acceso. Los puntos de acceso instalados dentro de cada piso del edificio de la MED no alcanza el rango máximo que sus fabricantes afirman, porque el alcance efectivo se reduce por la interferencia de obstáculos de las cosas tales como paredes, otras redes y dispositivos inalámbricos. Incluso dentro del alcance efectivo de un punto de acceso, una interferencia fuerte como la red inalámbrica de un AP que se encuentra cerca de otro, utilizando el mismo canal que causa manchas localizadas muertas. Señales de radio transmitidas en el interior dividir y seguir varias rutas a su destino, a medida

que rebotan o atraviesan paredes, otros obstáculos de diferentes maneras y en diferentes ángulos. El resultado es que las señales múltiples, algunos más débiles, algunos más fuertes, llegan a su destino en diferentes momentos interfieren unas con otras, a veces lo suficiente como para causar interrupciones o la conectividad es inaceptable. [5] Se considera de mejor manera colocar cada AP en un lugar céntrico para abarcar más espacio dentro del piso donde esté situado, en el caso del piso donde se encuentran los laboratorios del Departamento Ciencias de la Computación actualmente cuentan con 3 AP`s pero en base a la ubicación que tiene no es aprovechado al máximo cada equipo por lo cual es indispensable la redistribución de los AP`s (véase la figura 3.46). Se puede observar que la cobertura no cumple las expectativas al tener 3 equipos para brindar servicio.

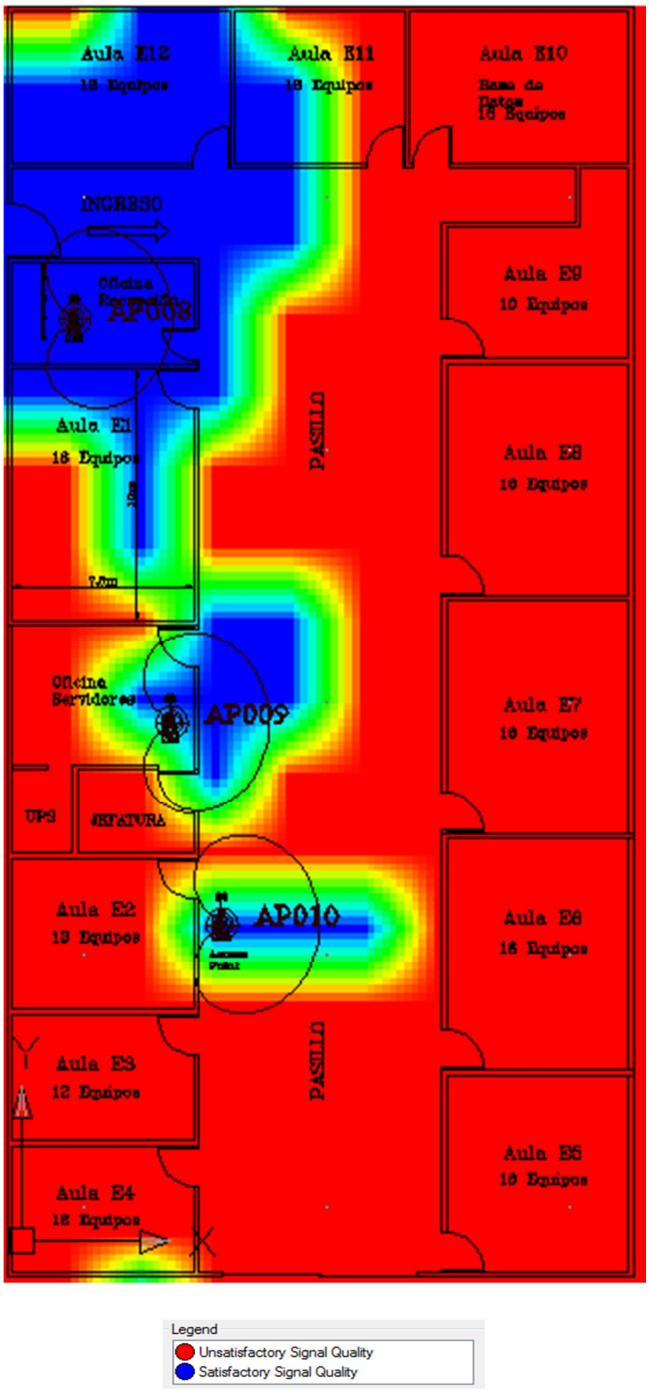


Figura 3.46 Situación actual de la ubicación de APs

3.7 PROBLEMAS DE CABLEADO

Se encuentran varios detalles donde se confirma que no existe un control de funcionamiento y la instalación de cada equipo, en este caso también se aprecia como el cableado estructurado se ausenta dentro de la parte

administrativa del DCC, en este departamento se encuentra varios docentes, personal administrativo y como autoridad el Director de Carrera. Por lo general no existen quejas sobre cómo se encuentran los equipos mientras estos cumplan su funcionamiento y cada miembro del Departamento Ciencias de la Computación tengan los servicios necesarios. Existen detalles inadecuados ya que no cumplen ningún estándar de seguridad, como se trata de una Institución muy prestigiosa se debe evitar estos episodios y llevar un control de cada evento realizado para evitar daños. En las figuras 3.47 y 3.48 se puede observar los eventos antes mencionados.

Figura 3.47 Cableado del DCC

Se aprecia como el techo falso no se encuentra en condiciones no adecuadas para el funcionamiento. Se estima que el departamento de UTICs se hará cargo de estos detalles, mientras el Departamento ya se encuentra trabajando así más de un año.

Figura 3.48 Cableado del Switch

CAPÍTULO 4

SOLUCIÓN PROPUESTA

4.1 BENEFICIOS DEL CONTROL DEL ANCHO DE BANDA

El Control de ancho de banda para la red LAN ofrece varios beneficios que son:

- **Control eficaz del ancho de banda en cada área funcional de la red:** Se puede administrar los enlaces ISP más utilizados, en tanto que las funciones de limitación de la velocidad del software Mikrotik RouterOS, como por ejemplo QoS de clase Scavenger, UBRL y los mecanismos de limitación de la velocidad basados en el switch del extremo, controlan el ancho de banda en las capas del core de distribución y del extremo de la red.
- **Reducción de costos:** La institución pueden realizar servicios de mayor ancho de banda y eliminar la necesidad de actualizar la infraestructura de la red de manera prematura.
- **Reducción de la congestión de la red:** El Control de ancho de banda basado en Mikrotik ofrece la flexibilidad, la granularidad y la inteligencia para controlar estrechamente las aplicaciones recreativas.
- **Aumento del rendimiento de la red y las aplicaciones:** al restringir el tráfico y garantizar que las aplicaciones y los usuarios fundamentales cuenten siempre con los recursos de la red que necesitan.

- **Máxima escalabilidad:** mediante herramientas como Mikrotik RouterOS, los departamentos pueden utilizar con facilidad QoS y políticas de control de ancho de banda en toda la red institucional, así como preservar y controlar con mayor eficacia el ancho de banda del campus.

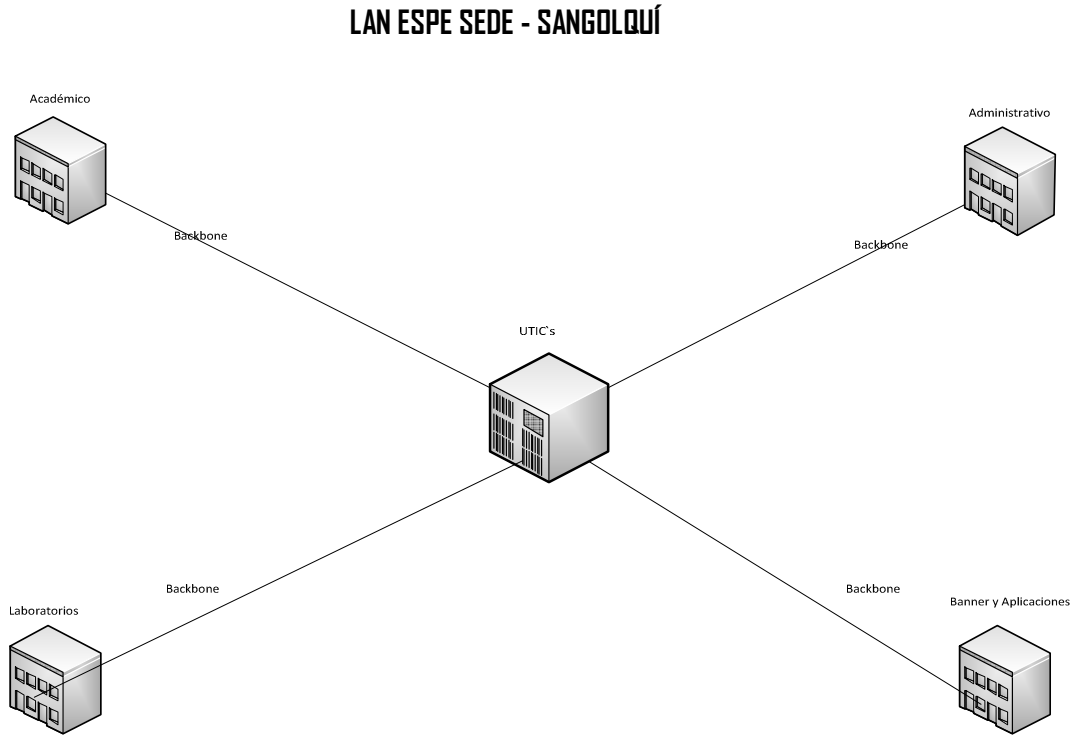


Figura 4.1 Lan Propuesta

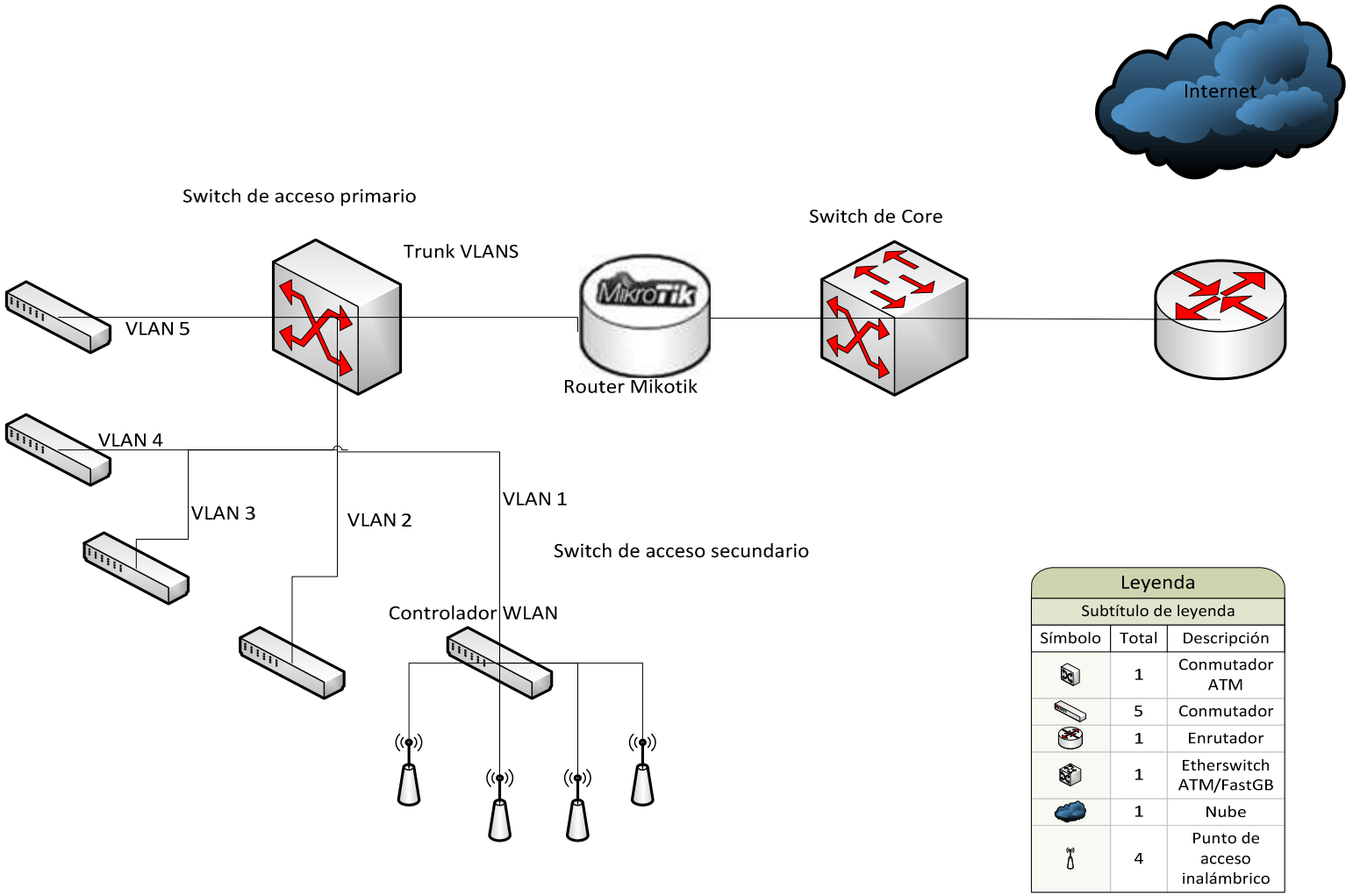
La nueva red planteada posee 4 segmentos que abarca toda la red LAN de la Institución, donde se puede dividir por VLAN`S los segmentos, se aplicará seguridad mediante hotspot donde se asegurará que todos los usuarios pueden ingresar a internet (véase la figura 4.1). Donde también como fuente de documentación y administración se realizará un plan de direccionamiento para usarlo como guía.

4.2 DISEÑO DE LA RED PROPUESTA DEL DCC

La red propuesta permite administrar el ancho de banda, se ha considerado al DCC que será nuestra guía para garantizar los servicios de red, evitando tráfico de red ya que se otorgarán servicios por tipo de usuario (alumno, docente, administrativo e investigador). La propuesta planteada (véase en la figura 4.2) con Mikrotik RouterOS será una solución de fácil administración para los usuarios, se utilizará los recursos con los que actualmente cuenta la Institución, siendo un resultado económico pequeño, grandes ventajas y beneficios para cada usuario.

ESPACIO EN BLANCO INTENCIONAL

Figura 4.2 Red Propuesta



4.3 USO DE INSTRUMENTOS

4.3.1 Direccionamiento IP

El estándar TCP/IP para el direccionamiento de subred reconoce que no todas las entidades tienen la misma necesidad de jerarquía de direcciones, por lo tanto permite una gran flexibilidad al poder escoger como asignarlas.

Para permitir la máxima flexibilidad al particionar las direcciones de subred del DCC, el estándar TCP/IP de subred permite que la interpretación de la dirección IP se escoja de forma independiente para cada red física. La red utilizada es 10.1.16.0/22, por lo cual se procedió a subnetear. En base a la Tabla 4.1 para conocer el número de usuarios y la asignación que pertenece a cada uno de los segmentos.

Tabla 4.1 Población total DCC

Segmento	Población
Alumnos	700
Docentes	102
Administrativos	10

4.3.1.1 Segmento estudiantes

En este segmento se obtuvo varias nuevas IP`s con /24, se considera la dirección 10.1.16.0/24 para el segmento estudiantes y la dirección 10.1.17.0/24 para obtener direcciones con menor población. La dirección de estudiantes es considerada para los laboratorios de computación que pertenecen al Departamento.

10.1.16.0/22

700 HOST	**RED**
2^n-2>=700	2^n=(# SubRedes)
2^10-2>=700	2^14=(# SubRedes)
1024-2>=700	16384=(# SubRedes)

10.1.16.0/24 ESTUDIANTES
10.1.17.0/24

4.3.1.2 **Segmentos docentes, investigadores, administradores y telefonía IP**

10.1.17.0/24

102 HOST	**RED**
2^n-2>=102	2^n=(# SubRedes)
2^7-2>=102	2^3=(# SubRedes)
128-2>=102	8=(# SubRedes)

10.1.17.0/26 DOCENTES
10.1.17.64/26 INVESTIGADORES
10.1.17.128/26 TELEFONÍAIP
10.1.17.192/26 ADMINISTRATIVOS

Como se puede observar en la figura 4.3 se puede apreciar que jerárquicamente se asignó el direccionamiento IP. En la Tabla 4.2 se determina más detalladamente las redes donde se puede apreciar las características necesarias para la asignación. Sin embargo no se pudo realizar encuestas a las personas que pertenecen al segmento de investigadores que pertenecen al DCC ya que se desconoce quién pertenece a este segmento pero se consideró un número de 100 personas para que puedan utilizar exclusivamente de los servicios propuestos.

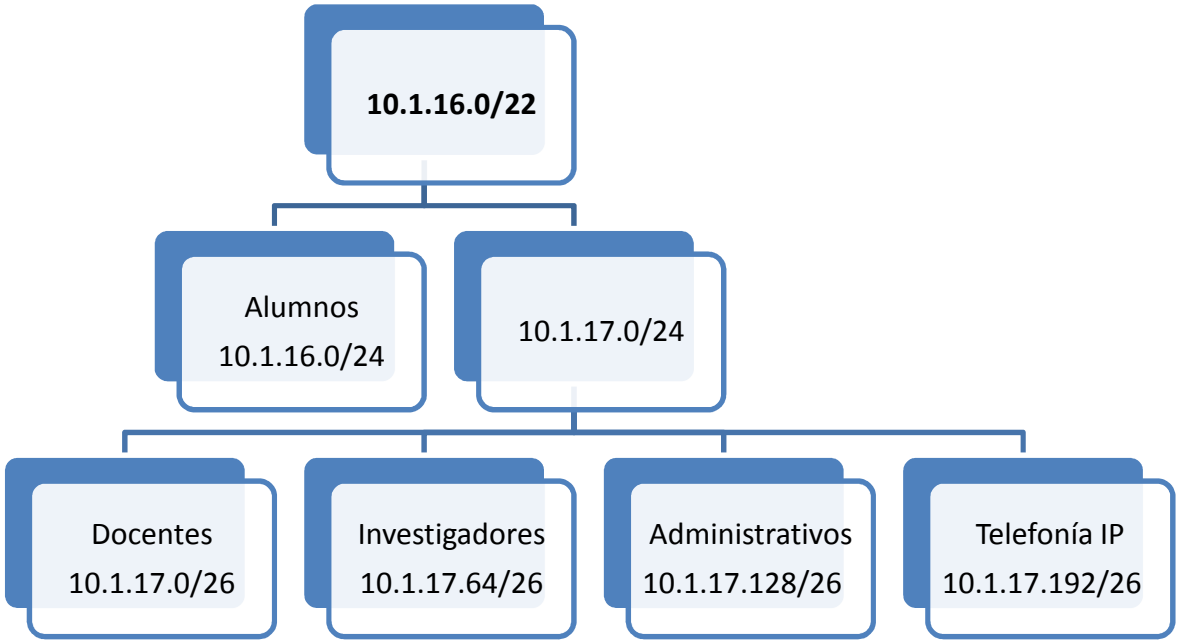


Figura 4.3 Direccionamiento

Tabla 4.2 Direccionamiento DCC

USUARIOS\IP'S	DIRECCIÓN DE RED	PRIMERA DIRECCIÓN VÁLIDA	ÚLTIMA DIRECCIÓN VÁLIDA	BROADCAST	MÁSCARA	/
ESTUDIANTES	10.1.16.0	10.1.16.1	10.1.16.254	10.1.16.255	255.255.252.0	22
DOCENTES	10.1.17.0	10.1.17.1	10.1.17.62	10.1.17.63	255.255.255.0	24
INVESTIGADORES	10.1.17.64	10.1.17.65	10.1.17.126	10.1.17.127	255.255.255.192	26
ADMINISTRATIVOS	10.1.17.128	10.1.17.129	10.1.17.190	10.1.17.191	255.255.255.192	26
TELEFONÍA IP	10.1.17.192	10.1.17.193	10.1.17.254	10.1.17.255	255.255.255.192	26

4.4 INSTALACIÓN Y MANEJO DE HERRAMIENTAS

Como fundamento básico para proceder al desarrollo de este proyecto se instalaron seis tarjetas PCI. El equipo permanecerá en el segundo piso del edificio que pertenece a la MED, en la oficina de servidores como indica la figura 4.4 (imagen tomada desde el pasillo del segundo piso).

Figura 4.4 Oficina de Servidores

Mediante las siguientes figuras se redactará la instalación de las tarjetas en cada ranura, considerando desde que se encontraban empacadas con los accesorios adicionales con las que adquirió cada una de ellas. En la figura 4.5 se enmarca en la presentación de las tarjetas.

Figura 4.5 Tarjetas PCI – Empacadas

Dentro del contenido de cada caja se encuentra (véase en la figura 4.6):

- Tarjeta Gigabit PCI
- CD de instalación de la tarjeta
- Manuales de instalación
- Placa protectora

Figura 4.6 Tarjetas PCI – Contenido

Al abrir el equipo se aprecia que se cuenta con seis ranuras PCI pero dos de ellas ya se encontraban ocupadas (véase la figura 4.7), por lo cual se procedió retirarlas y remplazarlas.

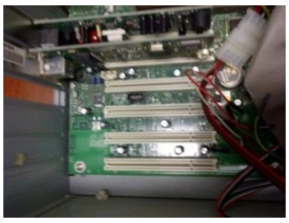


Figura 4.7 Tarjetas PCI – Originales

Una vez ya ubicadas correctamente las tarjetas como se aprecia en las figuras 4.8 y 4.9 se procede la instalación del software Mikrotik Router, para conocer a detalle la instalación del mismo se encuentra en el ANEXO C.

Figura 4.8 Tarjetas PCI-Instaladas

De esta manera permanecerá el equipo de ahora en adelante, trabajará brindando la funcionalidad de un router donde ayudará a solucionar problemas bajo las mismas condiciones.

Figura 4.9 Tarjetas PCI-Utilizadas

Una vez ya instalado el software Mikrotik RouterOS, al digitar el comando **interface** y luego al digitar **print** se presenta como el equipo ya reconoce cada uno de las tarjetas y las enumera del 0 al 5, considerando que son tarjetas Ethernet. Las seis tarjetas utilizadas son totalmente iguales, tanto como la marca como las características de cada una, para conocer sus características más a detalle se puede ver en el ANEXO E.

4.5 CATALOGACIÓN DE APLICACIONES

4.5.1 Catalogación de Wireshark

Mediante la utilización de esta herramienta se han obtenido datos, que mediante ellos se ha concretado los resultados de las encuestas, se ha detallado más a fondo las conclusiones que se proporcionó. También se pudo detectar que tan verídico es el resultado señalado por las encuestas. Se analizó a detalle la herramienta y se la catalogó de la siguiente manera:

- **Software Libre:** se lo puede adquirir fácilmente y su utilización es de manera indefinida.
- **Software Empresarial:** está orientado a ayudar a una empresa a mejorar su productividad.
- **Software de Aplicación:** permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido.
- **Software de Productividad:** ayuda a las personas a realizar su trabajo con más eficiencia.
- **Software de Confiabilidad:** la capacidad del software realiza su función de la manera prevista.

- **Software de Disponibilidad:** está disponible de ser encontrado o utilizado.
- **Software de Escalabilidad:** tiene la propiedad deseable del sistema.

4.5.2 Catalogación de Mikrotik RouterOS

Por medio de las características de esta herramienta se estima que brinda al usuario una manera más amigable de interactuar, ofreciendo los mismos resultados que cualquier otro equipo (router). Mediante el análisis previo realizado a continuación se detalla las características en las cuales se lo ha catalogado:

- **Software Propietario:** existe la versión de prueba que solo se puede utilizar por 24 horas, para realizar durante mayor tiempo las configuraciones necesarias es recomendable adquirir la licencia.
- **Software Empresarial:** está orientado a ayudar a una empresa a mejorar su productividad.
- **Software de Aplicación:** permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido.
- **Software de Productividad:** ayuda a las personas a realizar su trabajo con más eficiencia.
- **Software de Confiabilidad:** la capacidad del software realiza su función de la manera prevista.
- **Software de Disponibilidad:** está disponible de ser encontrado o utilizado.
- **Software de Escalabilidad:** tiene la propiedad deseable del sistema.

4.6 AJUSTE Y SOLUCIÓN

4.6.1 Consideraciones para la ubicación de AP`s

- **No colocar el punto de acceso ni cerca de paredes ni objetos metálicos:** El metal afecta considerablemente a la señal, produciendo inesperados efectos rebote. Los muros, suelos y paredes, pueden afectar y reducir el rendimiento esperado del equipo.
- **Remplazar la antena del router:** En el 90% de los casos, las antenas que incorporan los routers wireless, son antenas omnidireccionales. Significa que la señal se emite en todas direcciones alrededor de la antena del equipo (véase la figura 4.10). Si el equipo se encuentra ubicado en una zona cerca de un muro que en caso de ser atravesado la emisión se está desperdiciando. Es recomendable cambiar la antena por una direccional que emite en el sentido que interesa y remplazarla por la antena omnidireccional existente.

Figura 4.10 Señal de antenas

4.6.1.1 Actualizar los dispositivos 802.11b a 802.11g u 802.11n

Los dispositivos 802.11b prácticamente ya son obsoletos hoy en día y por tanto si se piensa en adquirir nuevo hardware con tecnología wireless lo mejor es decidirse por el estándar 802.11g, a pesar que hoy la norma 802.11n está cada vez más extendida. Es la tecnología conocida también como MIMO (Multiple Input, Multiple Output). [1]

4.6.2 **Reubicación de AP`s**

Considerando las recomendaciones para la ubicación de AP`s y al simular las ubicaciones se puede notar que al utilizar un solo AP se aprovecha el rendimiento del equipo en relación a la cobertura (véase la figura 4.11), otra solución puede ser utilizar los 3 AP`s cambiando el canal de cada uno de ellos. Con esto se obtiene una mejora rápida sobre la cobertura proporcionada del equipo.

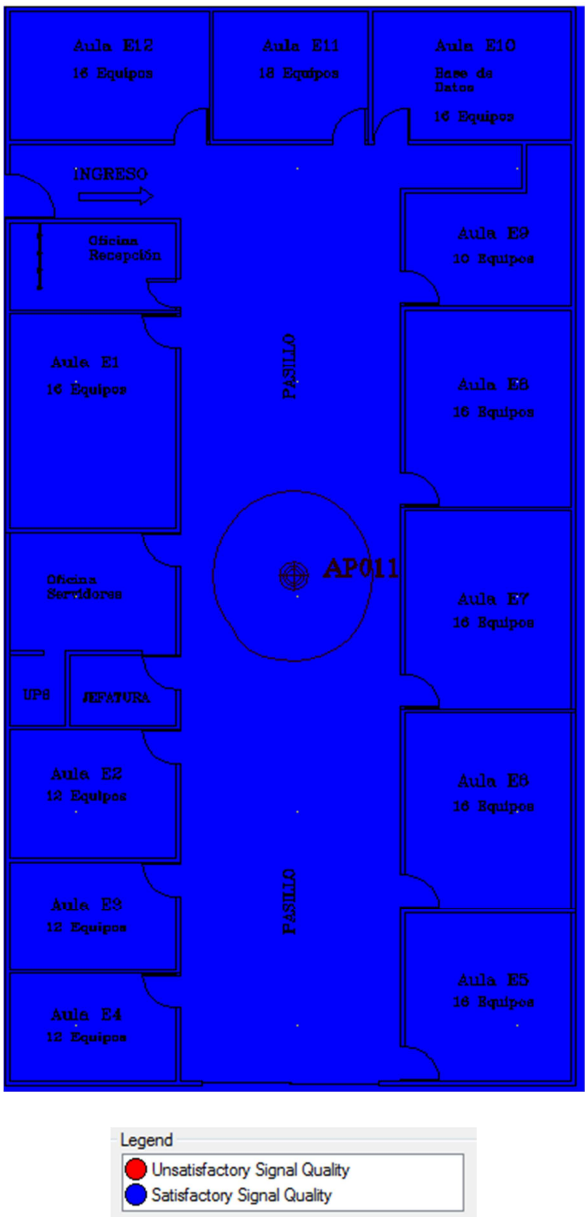


Figura 4.11 Reubicación de APs

4.6.3 **Configuración del Sistema RouterOS**

Mikrotik RouterOS es el sistema operativo y software router por cual convierte a una PC Intel o un Mikrotik RouterBOARD™ en un router dedicado. Con este potente router se podrá dar solución a la red Institucional, ya que ayudará administrar el 100% de los recursos de Ancho de Banda de la red, además se podrá monitorear en forma gráfica el tráfico de red y en tiempo real mediante el software Winbox. El Mikrotik RouterOS puede realizar varias opciones para satisfacer con las necesidades de red, además de cierta funcionalidad como servidor. Al inicializar Mikrotik mediante Winbox se presenta una ventana que señala que el software está corriendo para presentar la interface principal como muestra la figura 4.12.

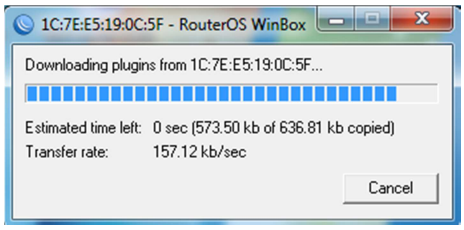


Figura 4.12 Dowloading plugins

Existe la posibilidad que esta descarga de módulos puede llegar a fallar, por lo que se debería repetir la operación hasta que logre establecer la correcta comunicación entre winbox y el servidor. Cuando la conexión esté establecida, se debería tener la ventana principal de winbox lista para proceder a licenciar el software, configurar, administrar y monitorizar a nuestros clientes. Cuando se ha descargado el software y no se ha obtenido licencia para el software Mikrotik, el sistema va a notificar cuanto tiempo ha transcurrido durante el uso (véase en la figura 4.13), la licencia gratis de nivel 1 que se descarga desde la página web tiene duración de 24 horas.

4.6.3.1 **Licenciamiento**

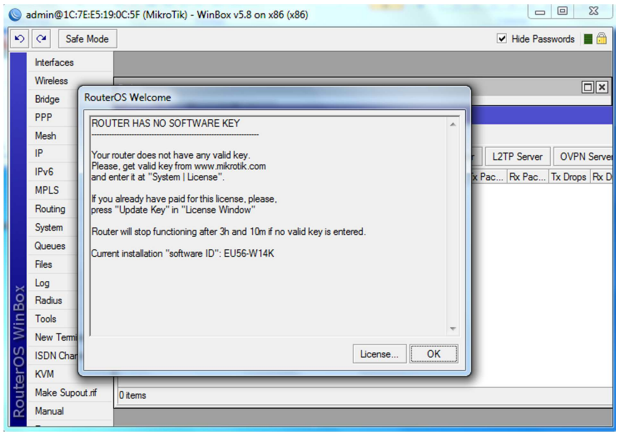


Figura 4.13 Bienvenida de RouterOS

Se puede apreciar el ID para obtener la licencia deseada una vez ya probado el producto. Por ejemplo en este proyecto el ID utilizado es ***EU56-W14K***. Para trabajar en este proyecto se trabajó bajo una licencia de nivel 4 (véase la figura 4.14), ya que la licencia que Mikrotik brinda sus servicios durante 24 horas, se puede utilizar con la distribución de tiempo que se deseé. Se realizó la instalación de Mikrotik sobre una plataforma x86. Las características de la licencia con las que se trabajó en este proyecto son las siguientes:

```
MikroTik RouterOS Licensed Key (Software ID: EU56-W14K)

License: WISP AP (Level 4)
Software ID: EU56-W14K
The software Key is:
-----BEGIN MIKROTIK SOFTWARE KEY------------
p2/gwsBkIU1yKR6p+4vv3ROETPusMJx/BF7C9tyG4oFz
+iJuU/gkcAccb2GtaI0EZpdylrgx5U5xhfHgWphwNA==
-----END MIKROTIK SOFTWARE KEY--------------
```

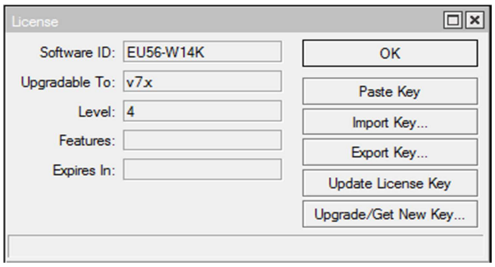


Figura 4.14 Registro de Licencia

- **Nivel de licenciamiento**

  Nivel 1: Licencia SOHO, gratis pero se debe registrar en www.mikrotik.com, tienen algunas limitaciones (1src-nat, 1dst-nat, 1 pppoe).

  Nivel 4: WISP, cliente inalámbrico, punto de acceso inalámbrico, gateway de Hotspot.

  Nivel 5: WISP AP, punto de acceso inalámbrico, Gateway de Hotspot (más conexiones soportadas).

  Nivel 6: Controller, todo sin límite.

  Para un amplio concepto se describe la tabla 4.3.

Tabla 4.3 Tipos de licencia - Mikrotik

Level number	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP 3Y)	6 (Controller 3Y)
Upgrade time	-	1 year	1 year	3 years	3 years
Initial Config Support	-	-	15 days	30 days	30 days
Wireless Client and Bridge	-	yes	yes	yes	yes
Wireless AP	-	-	yes	yes	yes
Synchronous interfaces	-	-	yes	yes	yes
EoIP tunnels	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	1	200	200	500	unlimited
PPTP tunnels	1	200	200	unlimited	unlimited
L2TP tunnels	1	200	200	unlimited	unlimited
VLAN interfaces	1	unlimited	unlimited	unlimited	unlimited
P2P firewall rules	1	unlimited	unlimited	unlimited	unlimited
NAT rules	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	1	1	200	500	unlimited
RADIUS client	-	yes	yes	yes	yes
Queues	1	30	unlimited	unlimited	unlimited
Web proxy	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	-	yes	yes	yes	yes

[2]

La licencia adquirida es la versión 5.11, una de las nuevas versiones de Mikrotik, ya que como característica adicional tiene la opción de poder manejar IPV6. Para conocer la instalación de Mikrotik se puede observar el ANEXO C. Algunas funcionalidades requieren cierto nivel de licenciamiento, el router puede ser actualizado durante un período de actualización (un año que cuenta desde la compra de la licencia). El período de actualización puede ser extendido a un 60% del costo original de la licencia. En el equipo que se está utilizando para este proyecto no se realizó ninguna partición, se

formateó por completo el equipo ya que solo servirá como ruteador y administrador. Existe varias formas de configurar el Router Mikrotik que son: por medio de interfaz gráfica y por líneas de código. Para manipular de una manera más fácil el Mikrotik RouterOS, es aconsejable instalar el software Winbox para trabajar de una manera más amigable al manipular el equipo. El manual de usuario sobre la instalación del software winbox se encuentra en el ANEXO D donde explica la instalación y pasos a seguir para la configuración.

4.6.4 **Reconocimiento de las tarjetas PCI por el Sistema RouterOS**

Mediante Winbox es necesario registrar la MAC del equipo con el que se va trabajar, ya que la licencia de Mikrotik RouterOS tan solo sirve para una máquina, una vez ya instalado captura la MAC y tan solo va a trabajar con el equipo que corresponda a la MAC reconocida que se instaló la primera vez. Para reconocer las tarjetas de red que tiene instaladas físicamente y que nombre tienen según MikroTik, se debe tomar en cuenta que por defecto MikroTik nombra a las tarjetas como ether1, ether2, ether3 y así hasta el número de tarjetas instaladas, en este proyecto de instalaron 6 tarjetas por lo cual se obtiene hasta ether6 (véase en la figura 4.15). Si fueran tarjetas wireless conectadas, a estas las nombra como wlan1, wlan2, wlan3...

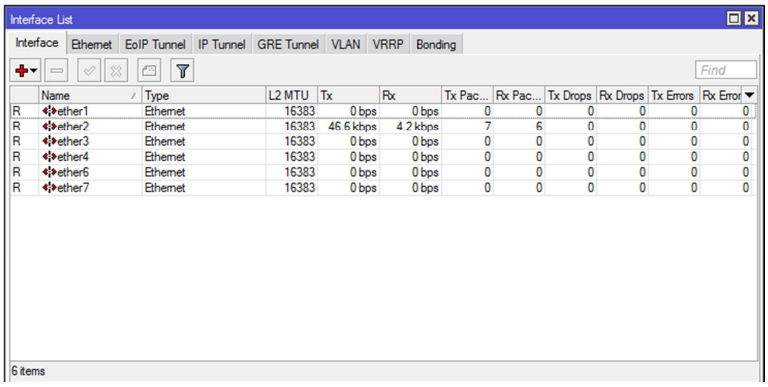


Figura 4.15 Tarjetas PCI reconocidas mediante Winbox

Mikrotik brinda la opción de observar las características técnicas de las tarjetas PCI que han sido instaladas en el equipo, esto ayudará a verificar si las tarjetas tienen las mismas características (véase la figura 4.16).

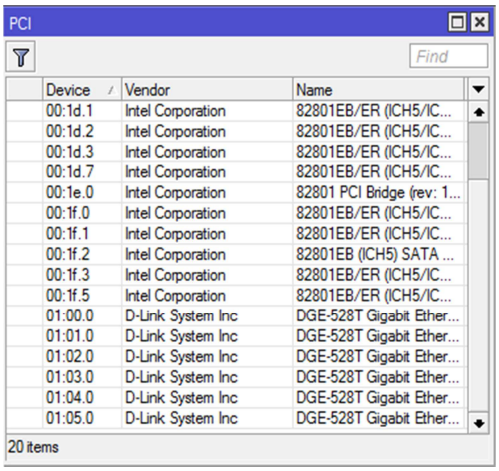


Figura 4.16 Tarjetas PCI características mediante Winbox

Nota 1: Si no se puede llevar a cabo la conexión entre winbox y el servidor a punto tal que no aparezca la MAC en el escaneo de dispositivos MikroTik, puede deberse a una falla de la tarjeta de red, cable de red en mal estado, un firewall activado, un antivirus agresivo o virus de red.

Nota 2: Si se tiene un RouterBOARD, tendrá una preconfiguración, donde el ether1 siempre tendrá bloqueado el acceso desde el exterior, así que conéctense desde el ether2 en adelante.

Mediante la herramienta Winbox se accede. Se ingresa mediante la opción **Interfaces** y determinar las configuraciones necesarias.. Hacer clic sobre la **ehter1**. Se puede asignar un nombre a la interface, por mantener orden se ha establecido y se ha utilizado el nombre de ether1 (véase en la figura 4.17).

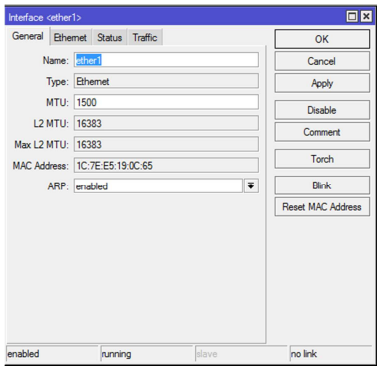


Figura 4.17 Interface ether1

Aquí se puede ver la velocidad con que está conectada, señalando las opciones de auto negoción y full dúplex como muestra la figura 4.18.

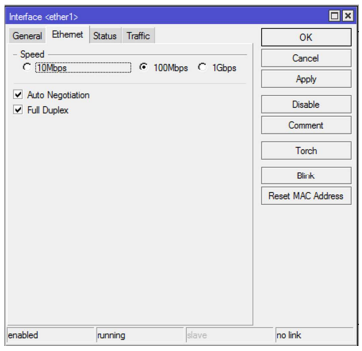


Figura 4.18 Interface ether1 - Viñeta Ethernet

Dentro de la viñeta estado, dice que la autonegoción está realizada, por la asignación de la dirección IP, la **Rate** es la tasa de transferencia de 10Mbps (véase la figura 4.19).

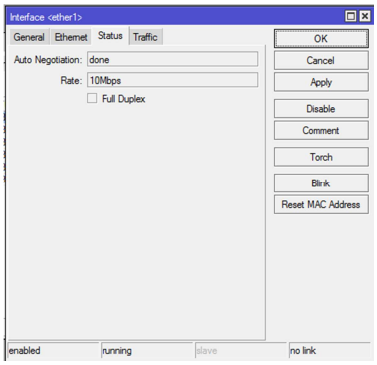


Figura 4.19 Interface ether1 - Viñeta Status

Se realiza la misma configuración para todas las Ethernet que están registradas.

4.6.5 **Configuración de Direcciones IP**

En base a los resultados obtenidos se debe considerar que el tráfico de red que existe en el Departamento Ciencias de la Computación es más saturado en el horario de matutino que el horario vespertino ya que el número de usuarios es mayor. El porcentaje de broadcast es otro dato muy importante y como se tenía estimado existe un mayor porcentaje en el horario matutino, uno de los factores indica donde está un problema significativo y donde se puede aplicar solución para la administración y control. Para la asignación de direcciones IP a cada Ethernet se consideró el direccionamiento IP que se realizó y como resultado se obtuvo la tabla 4.4 donde se detalla el puerto PCI que pertenece cada Ethernet, ya que no coincide el número de puerto con la Ethernet asignada. También se consideró los segmentos para detallar su Ethernet correspondiente y por último la dirección IP que se asignará a cada interface y para coordinar de mejor manera con su respectiva máscara de subred solo que se encuentra en diferente nomenclatura. Con estos cuatro datos será la base para la asignación necesaria de cada interface y así no se desconocerá ningún detalle.

Tabla 4.4 Asignación de IP

N° puerto PCI	Ethernet	Segmentos	Dirección IP
1	2	Alumnos	10.1.16.1/24
2	3	Docentes	10.1.17.1/26
3	4	Investigadores	10.1.17.64/26
4	1	Administrativos	10.1.17.128/26
5	5	Telefonía IP	10.1.17.192/26
6	6		

Se selecciona la opción **Interface** para observar las Ethernet que están reconocidas por el router Mikrotik. Se selecciona **IP,** luego la opción

Addresses, seleccionar la Ethernet que se desea asignar la dirección IP en relación a la tabla 4.4 para la asignación de cada una de ellas como se observa en las figuras 4.20, 4.21, 4.22 y 4.23.

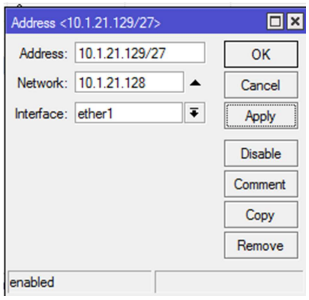


Figura 4.20 Asignación de dirección IP- Ethernet1

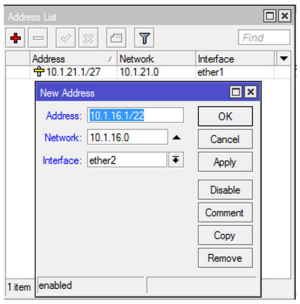


Figura 4.21 Asignación de dirección IP – Ethernet2

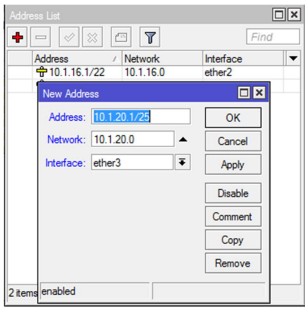


Figura 4.22 Asignación de dirección IP – Ethernet3

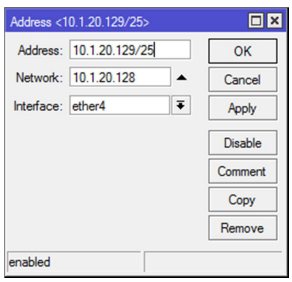


Figura 4.23 Asignación de dirección IP – Ethernet4

Después de la asignación de direcciones IP a cada interface el Mikrotik RouterOS presentará la siguiente interface donde muestra la dirección IP (véase la figura 4.24) y la red que pertenece dicha dirección a cada una de las interfaces Ethernet con las que se trabaja en este proyecto como presenta la figura 4.25.

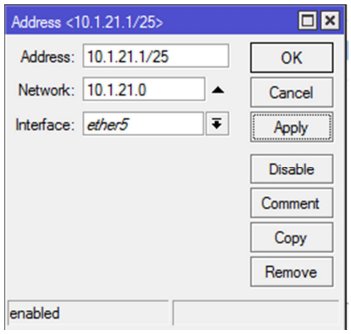


Figura 4.24 Asignación de dirección IP – Ethernet5

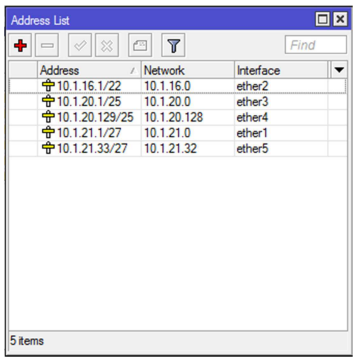


Figura 4.25 Asignación de dirección IP – Ethernet5

4.6.6 **Configuración DHCP**

Primero se debe habilitar al cliente, para la asignación de cliente DHCP a cada interface Ethernet se selecciona la opción **IP** y se selecciona **DHCP Client,** por medio de la Ethernet se determina el nombre de cada uno, según la segmentación establecida en el proyecto por tipo de usuarios. Se procede el mismo proceso con cada una de las interfaces Ethernet. El asistente de configuración ayudará a tener nuestro DHCP correctamente configurado. Se

selecciona la interfaz de red en donde se instalará el DHCP, aquí se escoge la interfaz de red LAN o la tarjeta de red desde donde se conectan nuestros clientes. Se señala la interface que corresponde a cada Ethernet. Se marca **Use Peer DNS** y **Use Peer NTP** para que haga cascada con los DNS y actualice el DNS. Se hace clic en **apply** y luego en **OK**. Realizar los mismos pasos para cada interfaz y marcar los datos que se presentan en las figuras 4.26, 4.27, 4.28, 4.29 y 4.30.

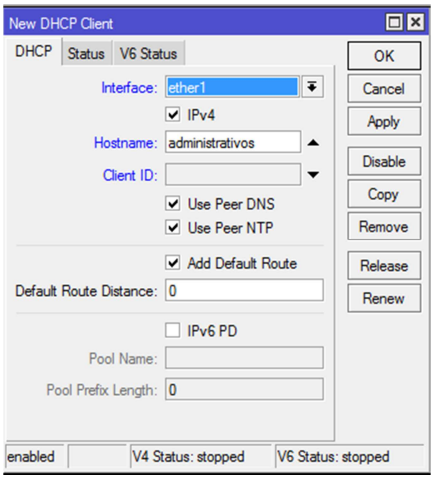


Figura 4.26 DHCP– Ethernet1

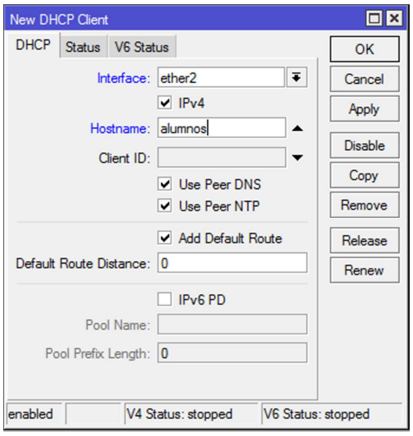


Figura 4.27 DHCP– Ethernet2

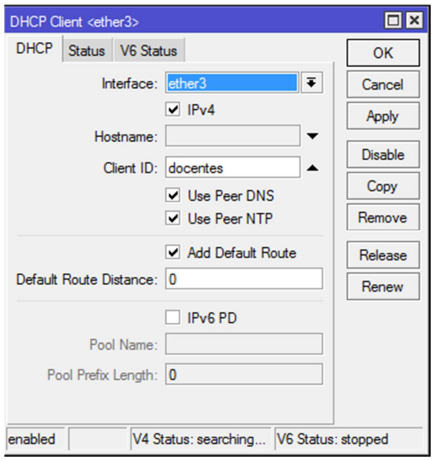


Figura 4.28 DHCP– Ethernet

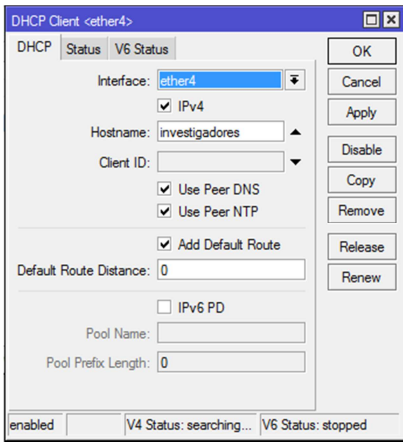


Figura 4.29 DHCP– Ethernet4

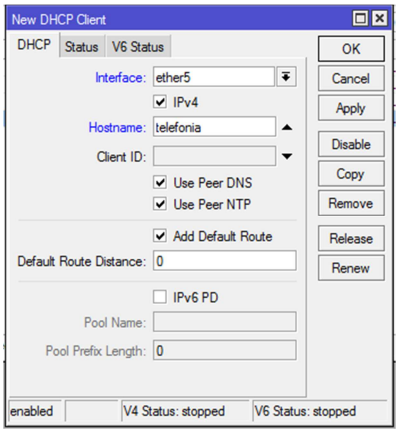


Figura 4.30 DHCP– Ethernet5

Como resultado después de la asignación de DHCP se muestra la interface que indica la figura 4.31 donde si es necesario se puede agregar o eliminar clientes DHCP.

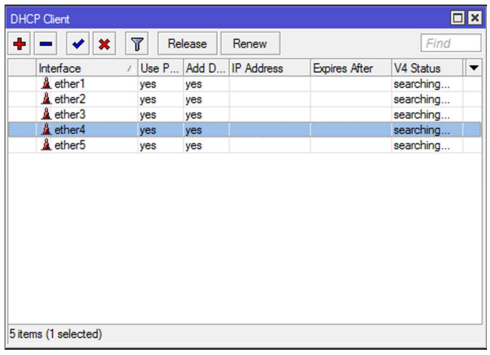


Figura 4.31 Clientes DHCP

Para presentar todas las configuraciones realizadas se presenta la figura 4.32 donde se presentan las características de cada Ethernet.

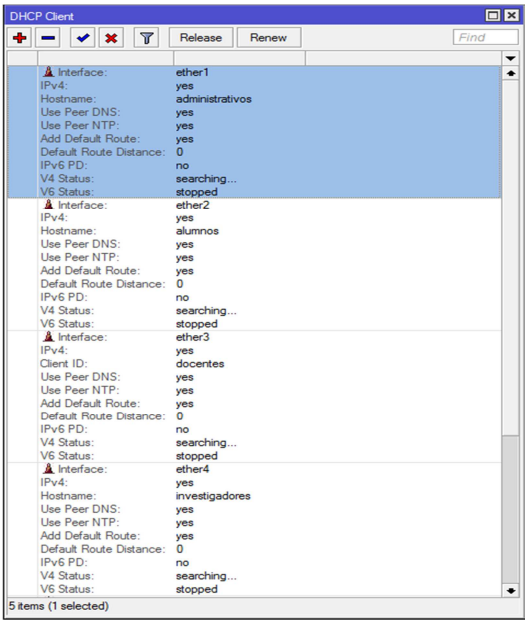


Figura 4.32 Clientes DHCP

Hacer clic en la opción **IP** y luego en **DNS**, presionar el botón **Settings.** Para que Mikrotik responda a solicitudes DNS, marcar la opción **Allow Remote Requests.** Con el fin de que Mikrotik abra el puerto 53 y empiece a escuchar peticiones por la dirección interna (véase la figura 4.33).

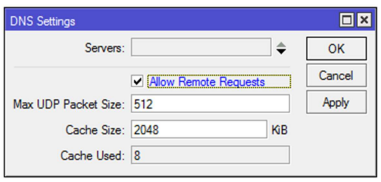


Figura 4.33 DNS Settings

4.6.7 **Firewall**

El Firewall se suele utilizar como herramienta de seguridad para evitar el acceso no autorizado a la red interna o al acceso al propio router, el bloqueo de varios tipos de ataques y controla el flujo de datos de entrada y salida. El firewall llevará a cabo varias funciones importantes, como la clasificación y marcado de los paquetes para el uso de herramientas de calidad de servicio.

La clasificación del tráfico realizado el servidor de seguridad puede basarse en los clasificadores distintos, tales como direcciones MAC, direcciones IP, (broadcast, Multicast) puertos de origen, destino de rango, protocolos, tipo de servicio (tos), tamaño de los paquetes y contenido de los paquetes.

Principios generales del firewall y cadenas default. Un firewall opera por medio de reglas de firewall. Una regla es una expresión lógica que le dice al router que hacer con determinado tipo de paquete. Las reglas son organizadas en cadenas (chains) existe 3 cadenas predefinidas que son:

- INPUT: responsable del tráfico que va hacia el router.
- FORWARD: responsable por el tráfico que pasa el router.
- OUTPUT: responsable por el tráfico que sale del router.

Notas:

1. Las reglas del firewall son siempre procesadas por el canal, en el orden que son listadas, en otras palabras de arriba hacia abajo.
2. Las reglas funciones como en programación se las menciona expresiones condicionales.
3. Si un paquete no tiene todas las condiciones de una regla esta pasa para la siguiente regla.

4. Cuando un paquete tiene todas las condiciones de una regla es tomada la acción que la regla tiene, no es importante las reglas que están debajo de esa cadena, pues estas no serán procesadas.
5. La excepción al criterio anterior se puede realizar cuando la opción “passthrogh” está disponible para transmitir.
6. Un paquete que no se encuentre en cualquier regla del canal, será por default aceptada.

4.6.7.1 **Firewall de Mikrotik: Filter Rules**

En esta pantalla se puede observar todas las reglas que en firewall se están procesando. Básicamente las reglas se dividen en: estáticas y dinámicas, pueden ser visualizadas por separado, también pueden ser visualizados por separados la cadena input, forward y output.

Nota: A medida que son creados son actividades los servicios nuevos que demandan reglas dinámicas en el firewall, son creados también canales dinámicos que aparecen en la lista de opciones del filter rule.

Las opciones que se pueden tomar en las reglas de filtrado son:

- **Accept:** acepta los paquetes.
- **Passthrough**: ignora las reglas (pero contabiliza) y pasa para la siguiente reglas,
- **Drop:** descartar silenciosamente los paquetes.
- **Reject:** descarta los paquetes y responde con un mensaje de icmp p tcp reset.
- **Connection tracking**

Seguimiento de conexiones se refiere a la habilidad del router a mantener el estado de la información relativa a las conexiones, tales como

direcciones de IP de origen, destino, pares de puertos, estados de conexión, tipos de protocolos y timerout. Firewall que hacen connection trancking son llamados “stateful” y son más seguros que aquellos que hacen procesamiento “stateless” (véase la figura 4.34).

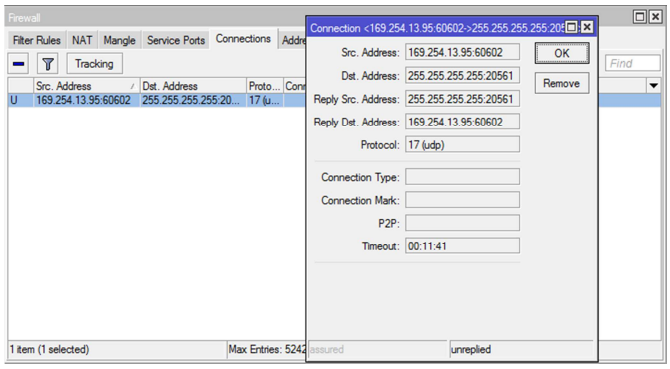


Figura 4.34 Connection

- El sistema de connection trancking o conntrack es el corazón del firewall, mantiene la información sobre las conexiones activas.
- Cuando se deshabilita la función de connection trancking se pierde las funcionalidades de NAT y marcado de paquetes que dependan de la conexión.
- Cada entrada en la tabla conntrack representa el intercambio de datos bidireccional.
- Conntrack y exigente de recursos de hardware, cuando el equipamiento trabaja por ejemplo como AP-bridge (véase la figura 4.35).

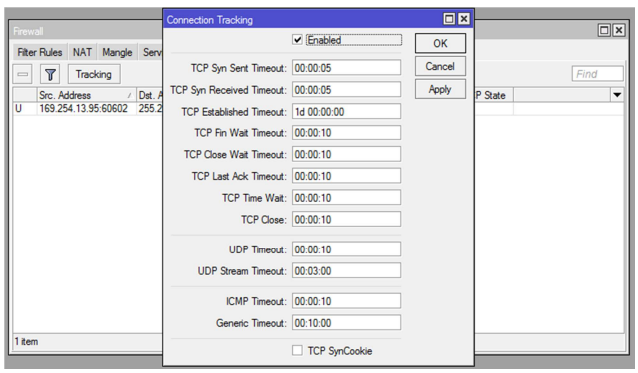


Figura 4.35 Connection Trancking

El estado de una conexión puede ser:

- **Estabilished**: significa que el paquete es parte de una conexión ya establecida anteriormente.
- **New:** significa que el paquete está iniciando una nueva conexión o parte de una conexión que viaja en ambas direcciones.
- **Valid**: significa que el paquete inicia una nueva conexión pero que está asociada a una conexión existente como por ejemplo FTP.
- **Invalid**: significa que el paquete no pertenece a ninguna conexión conocida ni está iniciando en otra.

Reglas canal INPUT

- Descarta conexiones inválidas.
- Acepta conexiones establecidas.
- Acepta conexiones relacionadas.
- Acepta todas las conexiones en redes internas.
- Descarta lo restante.

Reglas en el canal INPUT-COUNT

- Permitir el acceso al winbox externo.
- Permitir acceso SSH.
- Permitir acceso Telnet.
- Reubicar las reglas para que funcionen.

Protecciones básicas de un router

Filtros de firewall, no filtran grupos de MAC, por eso es necesario deshabilitar la MAC telnet a MAC winbox por lo menos en la interface pública. Se tiene que desactivar el “network discovery” también para que el router no se revele más. Dentro de la opción **Tools** se hace clic y

seleccionar la opción **MAC server**, dentro del campo de interfaces abrir el combobox, se selecciona la opción **all** (todas), deshabilitar con la opción **disable**. Luego clic en **IP** y **Neighbors**, en cada interface hacer clic derecho y se selecciona la opción **disable** para cada una de ellas (véase la figura 4.36).

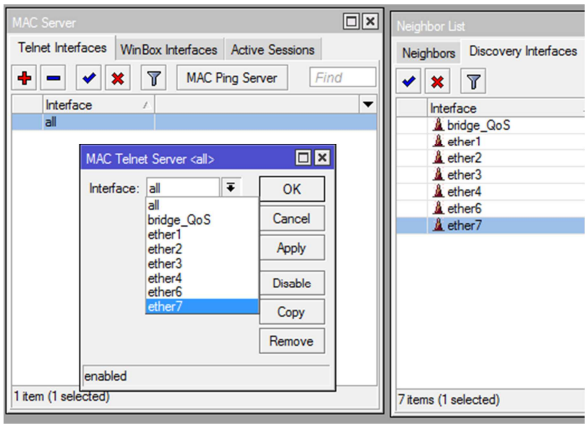


Figura 4.36 Protecciones Básicas del Router

Acceder a **IP** luego en **Services** y se deshabilita todo lo que no es utilizado (véase la figura 4.37).

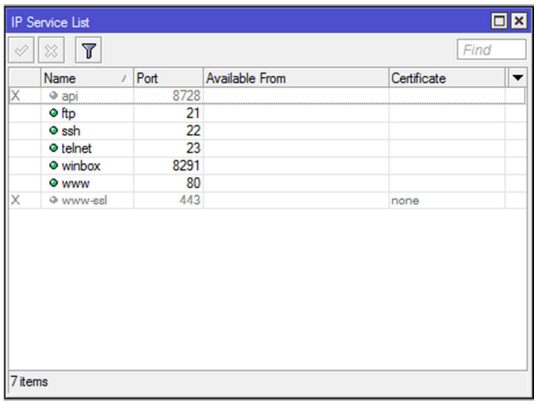


Figura 4.37 Sevice List

Reglas en el canal forward

- Descartar conexiones inválidas.
- Acepta conexiones establecidas.
- Acepta conexiones relacionadas.

Filtros de puertos de virus

- Bloquea puertos más utilizados por virus TCP y UDP.
- En la actualidad existen algunas centenas de troyanos activos y no menos de 50 tipos de virus activos.
- En el Site de Mikrotik hay una lista con las puertas y protocolos que utilizan virus.

Ataques DoS

- El principal objetivo de los ataques DoS es el consumo de los recursos como el CPU y el ancho de banda.
- Usualmente el router es inundado con peticiones de conexión TCP/SYN causando la respuesta TCP/SYN-ACK y queda a la espera de paquetes de TCP/ACK.
- Todas las IP s con más de 10 conexiones con el router pueden ser considerados atacantes.

Ataques DoS-Cont

- Si simplemente descarta las conexiones, permite que el atacante cree una nueva conexión.
- La protección puede ser implementada en dos estados.
- Detención – creando una lista de atacantes DoS con base en la con base en la **connection limit**.
- Supresión – de las restricciones para los que se detectan.

Hacer clic en **IP**, luego en **Firewall**, crear una nueva regla firewall con el botón (+) y agregar los datos que se puede observar en las figuras 4.38 y 4.39.

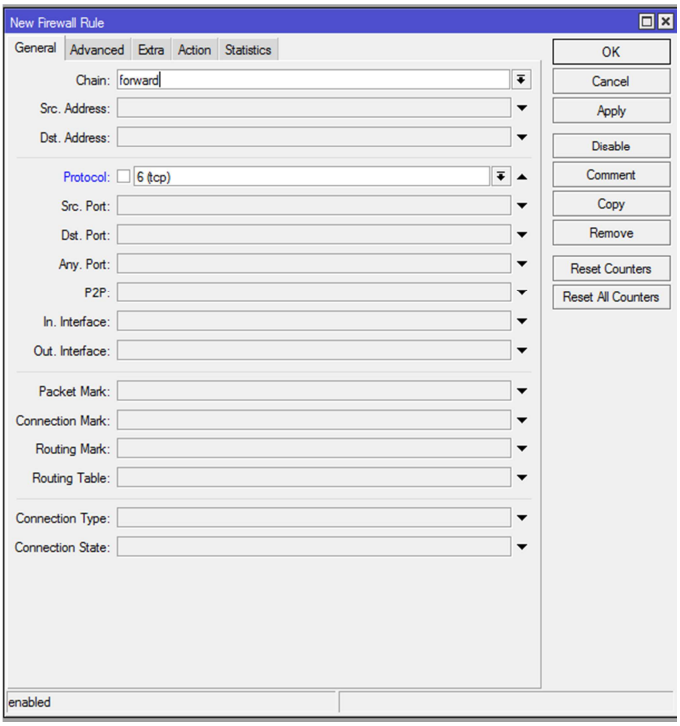


Figura 4.38 Nueva Regla Firewal – General

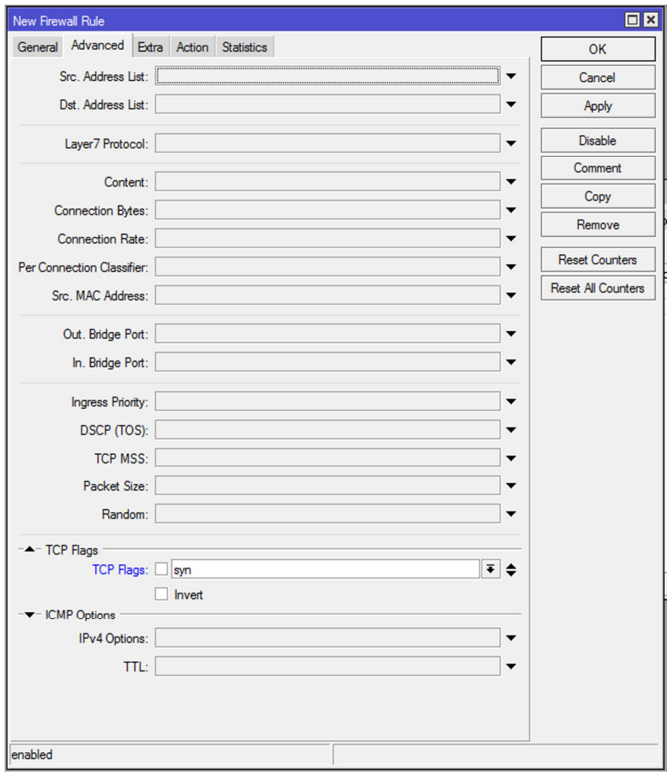


Figura 4.39 Nueva Regla Firewall – Advanced

Seleccionar el límite de 20, en otras palabras así señalar 20 conexiones simultáneas por cada cliente (véase las figuras 4.40 y 4.41).

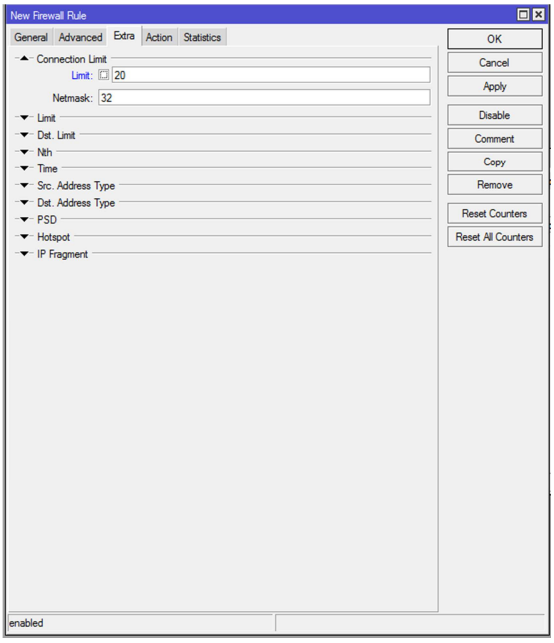


Figura 4.40 Nueva Regla Firewall – Extra

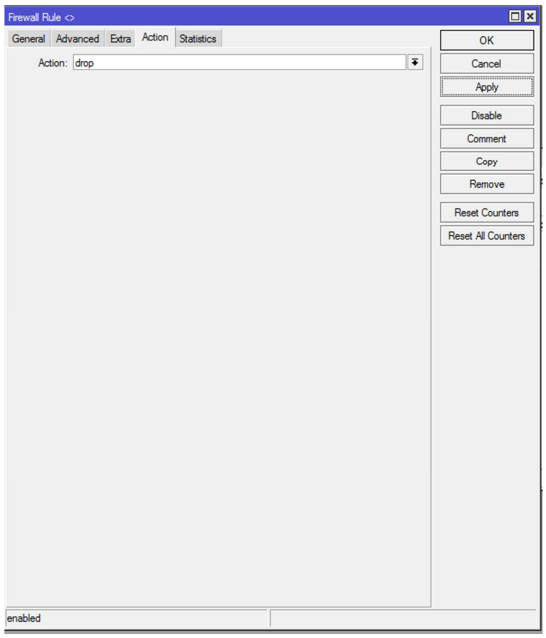


Figura 4.41 Nueva Regla Firewall – Action

4.6.7.2 **Firewall NAT**

NAT: es una técnica que permite que un host en una LAN use un conjunto de direcciones IP para la comunicación interna y otro para la comunicación externa. Existen dos tipos de NAT que son:

- **Source nat (srcnat):** Nat de origen, cuando el router vuelve a escribir la IP de origen y el puerto, por otro IP de destino.
- **Destination NAT (dstnat):** Nat de destino cuando el router reescribe la dirección o el puerto de destino.

Las reglas de NAT son organizadas en cadenas:

- DNS-NAT permite cambiar la dirección y el puerto del receptor a alguna otra dirección y puerto conocido localmente por el ruteador o se llegue vía ruteo.
- Típicamente usado para acceder servicios en una red privada desde direcciones públicas accediendo las direcciones públicas que enmascaran alguna red.
- SRC-NAT permite el cambio de dirección origen y puerto a la dirección local y puerto del router (enmascaramiento, o alguna otra dirección y puerto especificado).
- Aplicación típica de SRC-NAT esconde una red privada detrás de una o más direcciones públicas.
- La dirección origen trasladada debe pertenecer al router, a menos que otras medidas sean tomadas para asegurar el uso de diferentes direcciones.

Ingresar interfaces y verificar que existan los enlaces. Asignar internet para los clientes, hacer clic en **IP**, luego en **firewall**, seleccionar la viñeta NAT (véase la figura 4.42). Habilitar una regla, hacer clic en el ícono +.

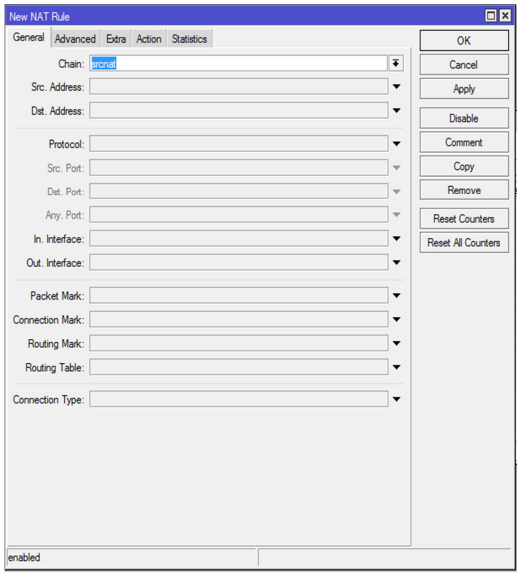


Figura 4.42 Nueva Regla NAT

En la opción de salida, seleccionar cada interfaz, con esto se va a enmascarar como indica la figura 4.43.

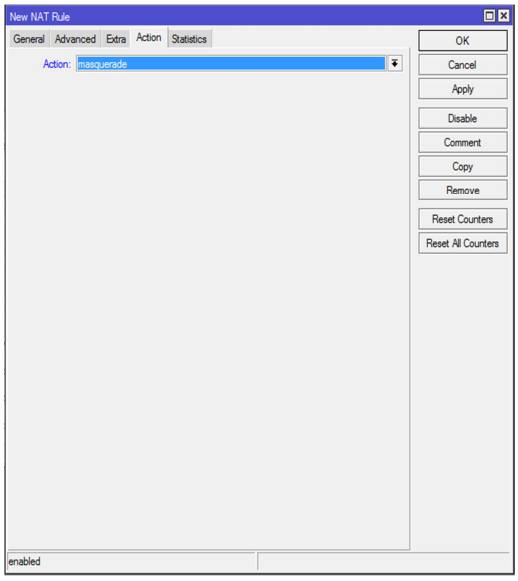


Figura 4.43 Nueva Regla NAT – Viñeta Action

Con estas reglas se obtendrá que todas las personas conectadas a cada interface, vayan a tener salida a internet de manera transparente sin ninguna restricción. Por el momento se tiene la salida, DNS. Habilitar algunos servicios, en la parte de **System** se tiene los servicios del sistema como tal, revisar todos los servicios que tiene el sistema, en la parte de IP existen los

servicios basados en IP, para eso observar las rutas que presenta la figura 4.44.

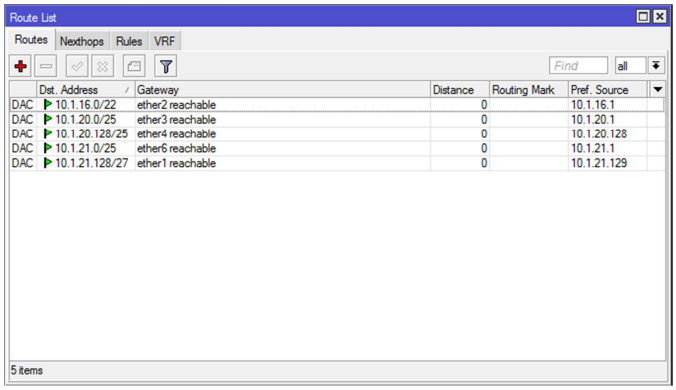


Figura 4.44 Lista de enrutamiento

Para activar la navegación se escoge la opción **Filtre Rules,** aquí se puede agregar todas las políticas deseadas, controlarla en puertos y renvío de paquetes.

4.6.7.3 **Firewall Mangle**

Mangle RouterOS, permite introducir marcas en las conexiones en paquetes IP en función de comportamiento específicos. Las marcas introducidas por el Mangle son utilizadas en el procesamiento futuro y hacen uso de estas herramientas como el control de ancho de banda, herramientas de QoS y NAT, que solo se ponen en el router, no se envían. Es posible poner el cambio MANGLE ciertos campos en el encabezado IP, como ToS (type of service) y campos de TIL (time to live)

Estructura del Mangle:

- Las reglas de mangle son organizadas en cadenas y obedecen las mismas reglas generales de las reglas de filter rules.
- Es posible crear cadenas por usuarios.
- 5 cadenas en padrón.
- Prerouting: marca antes de la cola Global-in.

- Postrouting: marca antes de la cola Global-out.
- Forward: marca antes del filtro Forward.

Acciones de Mangle

Las opciones de marcado incluyen:

- **Mark-connection**: solo el primer paquete.
- **Mark-packet:** marca un flujo (todos los paquetes).
- **Mark-routing:** marca paquetes para políticas de ruteamento.

Marcado de conexiones:

- Use mark-conecction para identificar un grupo de conexiones con una marca específica de conexión.
- Las marcas de conexión son almacenadas en la tabla de connection tracking.
- La facilidad de connection tracking ayuda a asociar cada paquete a una conexión específica.

Los paquetes pueden ser marcados:

- Indirectamente, usando la facilidad de connection tracking, con base en marcas de conexión previamente creadas (más rápido y más eficiente).
- Directamente, sin connection tracking. No es necesario pedir marcas para la conexión y el router se compara cada paquete con ciertas condiciones.

Se asignaron marcas en los paquetes para su proceso. Marcar es la única manera de identificar paquetes dentro de los queues de árbol y se puede utilizar como un clasificador para diferentes políticas de ruteo. Las marcas

mangle solo existen dentro del router, ya que no se transmiten por la red. Se debe considerar los siguientes puntos:

- Mangle facilita la marcación de paquetes especiales por IP.
- Estas marcas son usadas por las instalaciones de otro router como enrutamiento y gestión de ancho de banda para identificar los paquetes.
- Mangle facilita la modificación de varios campos de la cabecera IP, como TOS (DSCP) y campo TTL.

Se puede realizar marcado de paquetes basándose en:

- Dirección IP Origen y Destino
- Puerto Origen y Destino T
- Protocolo de transporte (TCP o UDP)
- Cabecera TOS / DS

Hacer clic en **IP**, dentro del menú de opciones seleccionar **Firewall**. Comenzar entonces creando las conexiones y sus respectivos Packet Marks en el Mangle. Al ingresar al menú de firewall se tiene la interfaz que proyecta la figura 4.45. Estas reglas vienen por default dentro de la instalación de Mikrotik RouterOS.

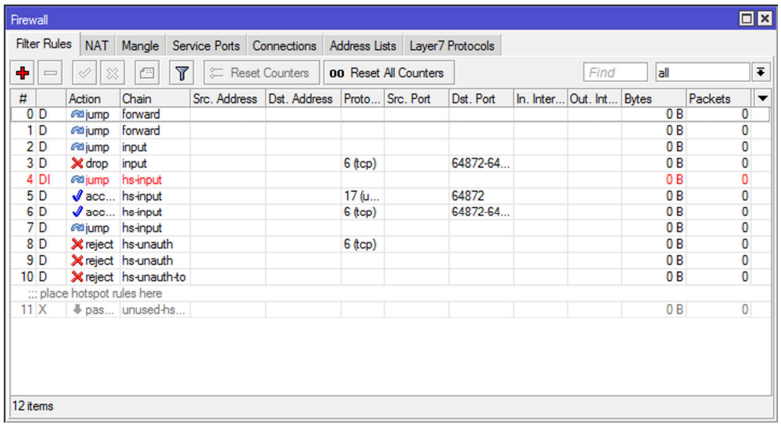


Figura 4.45 Menú principal Filter Rules

Se procedió a borrar estas configuraciones para crear nuestras propias reglas, considerando los objetivos que se han establecido para este proyecto. Para borrar las reglas hacer clic en el botón (-). Dentro la pestaña **Mangle** como índica la figura 4.46. Seleccionar el botón (+) para añadir una regla nueva.

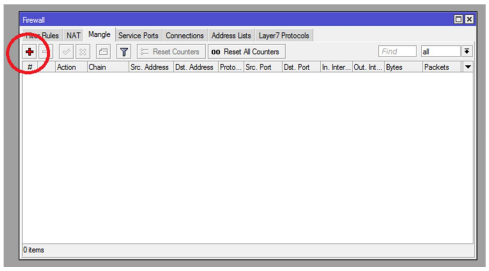


Figura 4.46 Mangle

Cuando agrega una de las nuevas reglas mangle aparece una ventana (véase en la figura 4.47).

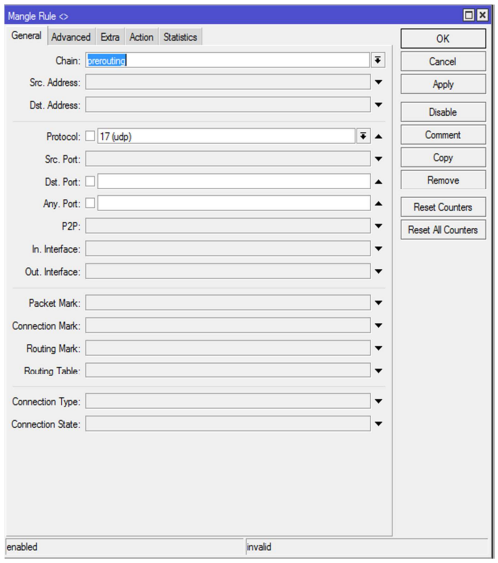


Figura 4.47 Configuración Mangle

Dentro de la viñeta **Action** existe la opción seleccionar la acción que realizará la nueva regla mangle, en este caso se ha seleccionado marcado de paquetes (mark packet). Hacer clic en **Apply** y luego en **OK**, de esta manera se agregará nuestra nueva regla (véase las figuras 4.48 y 4.49).

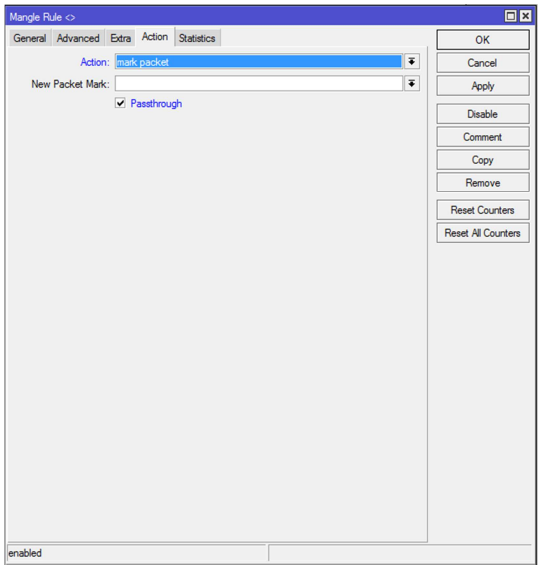


Figura 4.48 Marcación de paquetes

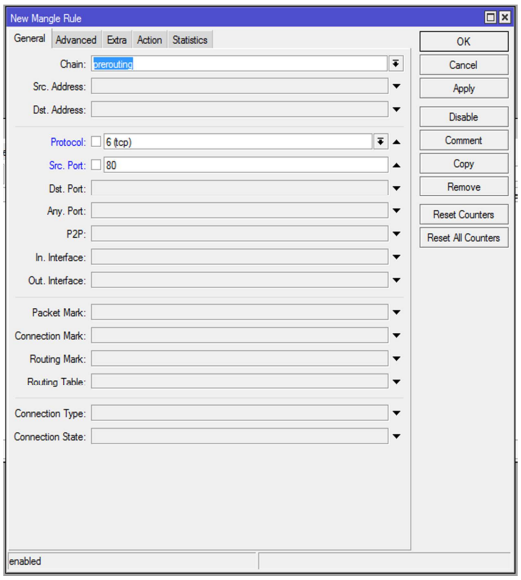


Figura 4.49 Nueva Regla Mangle – routing

Se identificará con www_in, poniendo un comentario (véase la figura 4.50).

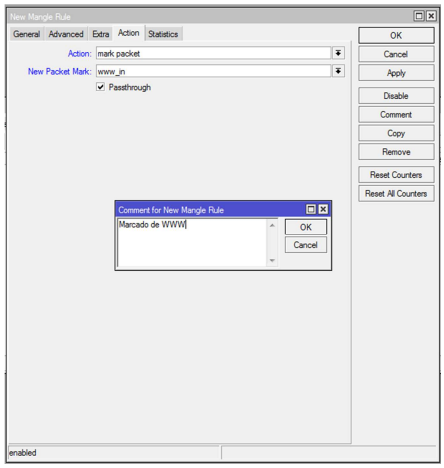


Figura 4.50 Nueva Regla Mangle routing – viñeta Action

Ya se obtiene la primera regla de marcación de paquetes, la marcación que se está realizando son los más básicos que se puede utilizar con la herramienta Mikrotik. Hacer clic en el botón + para agregar una nueva regla, repetir el mismo procedimiento en esta regla, escoger la opción de postrouting como indica la figura 4.51.

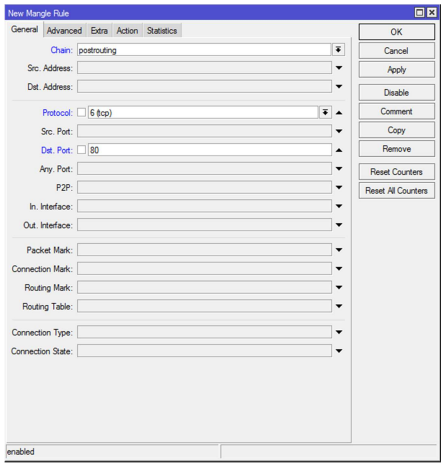


Figura 4.51 Nueva Regla Mangle – postrouting

En la viñeta **Action** seleccionar la opción de **mark Packet** (marcación de paquetes), hacer clic en **Apply** y luego en **OK**. En el campo **New Packet Mark** se colocó www_out (véase las figuras 4.52, 4.53, 4.54, 4.55 y 4.56).

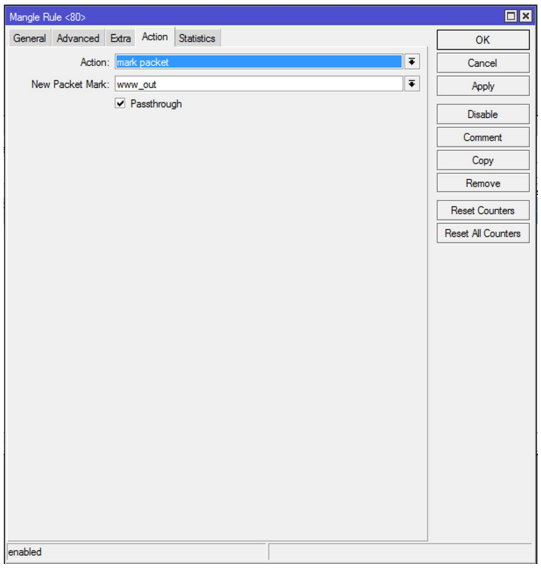


Figura 4.52 Nueva Regla Mangle postrouting – viñeta Action

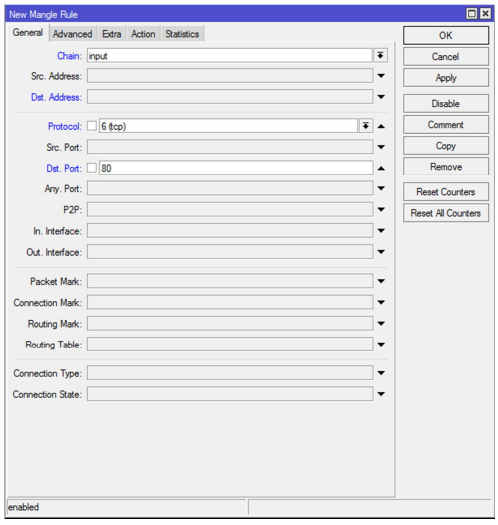


Figura 4.53 Nueva Regla Mangle input – viñeta General

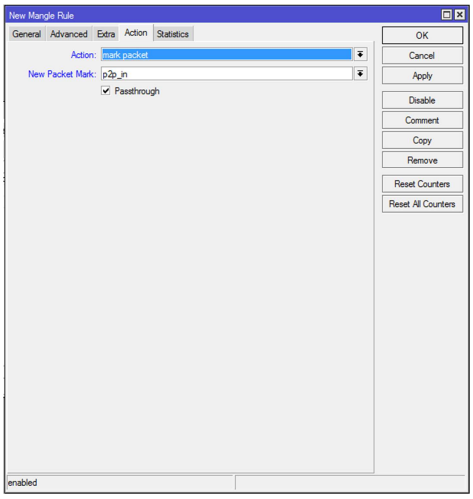


Figura 4.54 Nueva Regla Mangle input – viñeta Action

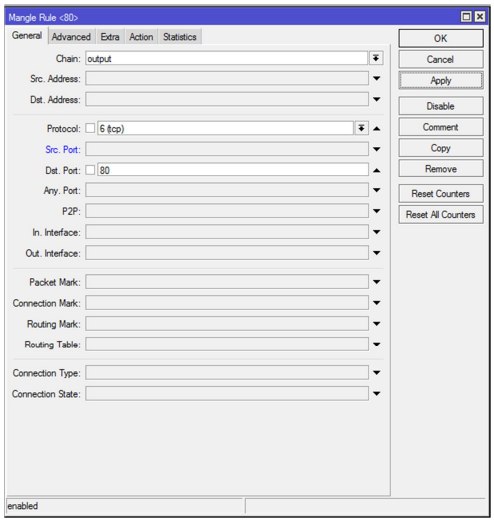


Figura 4.55 Nueva Regla Mangle input – viñeta Action

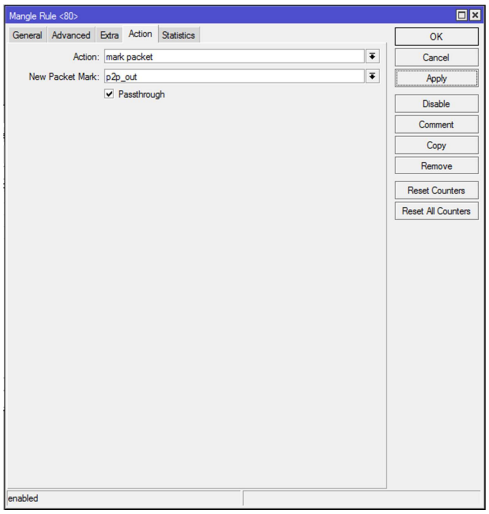


Figura 4.56 Nueva Regla Mangle input – viñeta Action

4.6.7.4 **QoS y Control de Ancho de Banda**

Calidad de servicio (QoS) significa que el router debe priorizar y controlar el tráfico en la red. Restricciones diferentes de control de ancho de banda o QoS tiene la misión de racionalizar los recursos de red, balanceando el flujo de datos con la mejor velocidad posible, evitando la saturación del canal.

Los mecanismos para proveer QoS del mikrotik son:

- Limitar el ancho de bandas para ciertas IP`s, subredes, protocolos, puertos y otros parámetros.

- Limitar tráfico p2p.
- Priorizar ciertos tipos de flujo de datos en relación a otros.
- Utilizar burst`s para mejorar el desempeño de acceso WEB.
- Aplicar colas en intervalos de tiempos fijos.
- Compartir el ancho de banda disponible entre los usuarios de forma moderada y dependiendo de la carga del canal.

Para ordenar y controlar el flujo de datos es aplicada una política de colas de los paquetes. Que son dejados en el router a través de una interface real (las colas son aplicadas en la interface de salida, considerando el flujo del tráfico) o una de las 3 interfaces virtuales adicionales (global-out y global-in). La limitación de ancho de banda es hecha mediante el descarte de paquetes. En el caso del protocolo TCP, los paquetes descartados serán reenviados, de forma que no hay que preocuparse con la relación de pérdida de datos. Los principales términos utilizados para describir el nivel de QoS para aplicaciones de red son:

- Queuing discipline (qdisc), disciplina de colas: es un algoritmo que mantiene y controla las colas de los paquetes, ellas especifican el orden de los paquetes que salen (pudiendo inclusive reordenarlos) y determinan que paquetes serán descartados.
- Limit At CIR (Commnitted Information Rate), Tasa de datos garantizada, velocidad mínima que ofrece un circuito.
- Max Limit MIR (Maximal Information Rate): Banda máxima que será ofrecida, es decir límite que se deja para hacer el descarte de paquetes.

- Priority, Prioridad: Es el orden de importancia de tráfico que será procesado, puede determinar cuál es el tipo de tráfico que será primero procesado.
- Contention Ratio, Radio de Contención: Es la relación en que la banda será compartida entre los usuarios, por ejemplo contention rate de 1:4 significa que la banda total asignada puede ser compartida entre 4 usuarios.

4.6.7.5 **Calidad de Servicio**

Se implementará el marcado y clasificación de paquetes que se dan prioridad para el manejo del tráfico, de esta forma se aplica QoS en el Mikrotik RouterOS. Se ha considerado la marcación de paquetes como objeto clave para la configuración como explica la figura 4.57.

Figura 4.57 Figura referencial

4.6.7.6 **Interfaces Virtuales**

Más allá de las interfaces reales, son definidas 3 interfaces virtuales en el RouterOS (véase la figura 4.58):

- **Glogal_in:** Representa todas las interfaces de entrada en general (INGRESS queue) las colas vinculadas a global-in reciben todo el tráfico entrante en el router, antes del filtrado de los paquetes. “global-in queueing” es ejecutado luego después de mangle y dst-nat.
- **Global-out:** Representa todas las interfaces de salida general, las colas asociadas a esa interface preceden a aquellas asociadas a una interface específica.
- **Global-total:** Representa una interface virtual a través de la cual pasa todo el flujo de datos, cuando se asocia una política de colas a global-total, la limitación es hecha en ambas direcciones

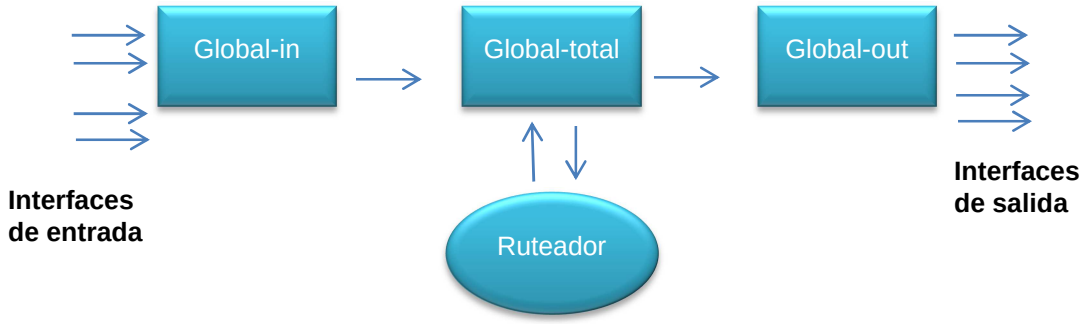


Figura 4.58 Interfaces Virtuales

4.6.7.7 **Tipos de colas**

Las disciplinas de colas son clasificadas por su influencia en el flujo de paquetes de la siguiente forma:

Schedulers: Solo reordenan los paquetes de acuerdo con un determinado algoritmo y descartan aquellos que se encuadran en la disciplina (véase la figura 4.59). Disciplina “Sheduler” son:

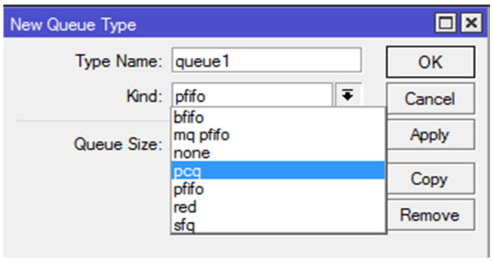


Figura 4.59 New Queue Type

- *PFIFO y BFIFO*

Estas disciplinas de colas son basadas en algoritmo de FIFO (Firts-In First-Out). La diferencia entre PFIFO y BFIFO es que uno es medido en paquetes y otro en Bytes. Existe unos parámetros llamados pfifo-limit (bfifo-limit) que determina a la cantidad de datos de la cola FIFO puede tener, todos los paquetes que no pueden ser puesto en las colas (si la cola se llena) serán descartados, tamaño grande de las colas pueden aumentar la latencia. Se recomienda el uso de este tipo de colas en links no congestionados.

- *RED*

Ramdom Early Detection, Detención Aleatoria anticipada: es un mecanismo de colas que tiende a evitar los congestionamientos de link controlando el tamaño medio de las colas. Cuando el tamaño medio de la cola llega al valor configurado en red-min-threshold, el RED aleatoriamente escoge el paquete para descartar las probabilidades de número de paquetes que serán descartados, crece según la medida de tamaño de la cola que también crece, si el tamaño medio de la cola llega red-max-threshold, entonces todos los paquetes que exceden red-limit serán descartados. RED es indicado en links congestionado y solamente para el control de TCP (no funciona bien para UDP).

- *SFQ*

Stochastic Fairness Queuing, Cola Estocástico. No limita el tráfico, el objetivo es ecualizar los flujos de tráfico (secciones TCP y Streaming UDP) cuando el link está completamente lleno. SFQ es asegurado por logaritmos de hashing y round-robin. Algoritmos de hashing dividen el tráfico de sección en un número limitado de sub-colas, después de alcanzado el tiempo en segundo y configurado en stq-peturb el algoritmo de hashing muda y divide la sección en otras subcolas. El algoritmo de round-robin reencola esas subcolas conforme como está configurado en pcq-allot bytes.

- *PCQ*

Per Connection Queuing: Colas por conexión fue creado para resolver algunas imperfecciones de SFQ (Stochastic Fairness Queuing), es el único tipo de colas de bajo nivel que puede hacer limitaciones siendo una mejoría de SFQ, sin la naturaleza estocástica, PCQ también crea sub-colas considerando el parámetro pcq-classifier. Cada sub-cola tiene una tasa de transmisión establecida en pcq-rate y el tamaño del paquete máximo igual a pcq-limit. El tamaño total de una cola PCQ se limita a lo que se ha configurado en pcq-total-limit. Si los paquetes están ordenados por la dirección de origen, entonces todos los paquetes con diferentes direcciones se dividirá en diferentes sub-colas. En este caso, es posible que la limitación o la estabilización en cada sub-cola con el parámetro pcq-rate. Puede ser que lo más significante es decidir en cual interface se utilizará este tipo de disciplina. Si se utiliza en la interfaz local, todo el tráfico de la interface pública será agrupada por la dirección de origen si es aplicada en la interface publica todo el tráfico de nuestros clientes será agrupado por la

dirección de origen, esto hace más fácil estabilizar o limitar el upload de dos clientes.

- *HTB*

Hierachiral Token Bucket es una disciplina de colas jerárquica que se utiliza para aplicar diferentes políticas para diferentes tipos de tráfico, generalmente es posible hacer una cola para una interface, pero las colas de Mikrotik se asocian con HTB y por lo tanto pueden heredar las propiedades de algunos de los padres de una cola, por ejemplo se podría configurar un total máximo de ancho de banda para un grupo de trabajo y luego distribuirlos entre los miembros.

4.6.7.8 **Queue Simple**

- Las queues simples son la manera más fácil de controlar las velocidades de los clientes, estas permiten configurar las velocidades de upload y download.
- HTB están localizadas justo debajo de ROOT.
- Los filtros de queue simple son ejecutados completamente por HTB en las interfaces global-out (queue direct) y global-in (queue reverse).
- Filtros, consulta las instrucciones de los paquetes IP de la misma manera en que aparecía en el firewall.
- Hotspot y PPP crean dinámicamente las queue simples.

La figura 4.60 muestra la ventana de presentación del software.

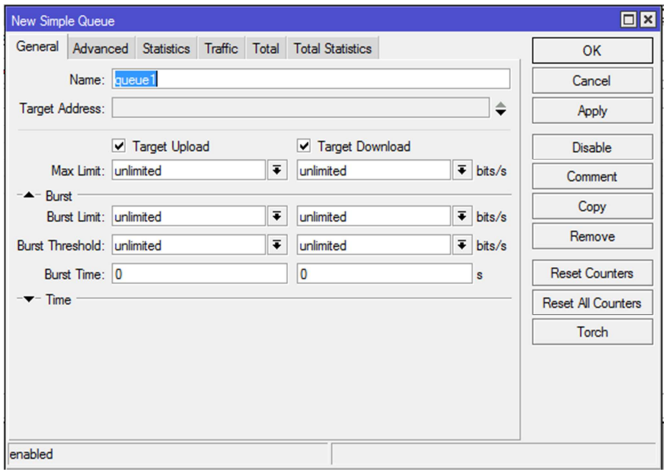


Figura 4.60 New Simple Queue – General

Las propiedades configurables de una queue simples son:

- Límite por dirección IP de origen o destino.
- Interface de cliente.
- Tipo de cola.
- Configuraciones de limit-at, max-limit, priotiry y bursts para download y upload.
- Configuraciones de limit-at, limit, priority y bursts para velocidades agregadas.

- **Utilización de PCQ**

PCQ: Per Connection Queue- Colas por conexión

- PCQ es utilizado para ecualizar a cada usuario en particular o cada conexión en particular.
- Para utilizar PCQ, un nuevo tipo de cola debe ser adicionado como argumento “kina=pcq”
- Deben ser escogido los parámetros:
    - pcq-classifier
    - pcq-rate

Con los rates fijos en cero las subqueue no se limitan o pueden utilizar el máximo ancho de banda disponible en el max-limit. Si se configura un rate para PCQ la Subqueue será limitada en ese rate, hasta el total de max-limit (véase las figuras 4.61 y 4.62).

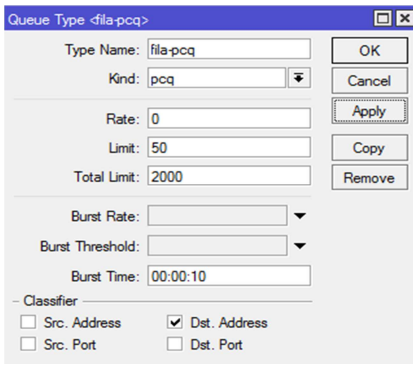


Figura 4.61 Queue Type

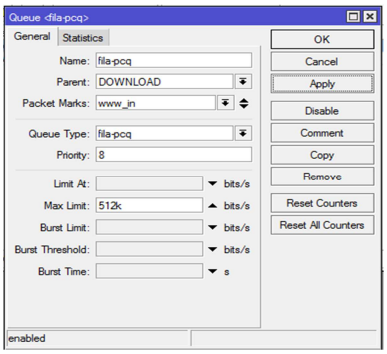


Figura 4.62 Queue fila_pcq

En este caso como en la rate la cola es de 0, no existe limit-at y tiene un total de 512K. La banda total será de 512K. Al crear una subcola se relaciona el parentesco con la cola madre como señala la figura 4.63

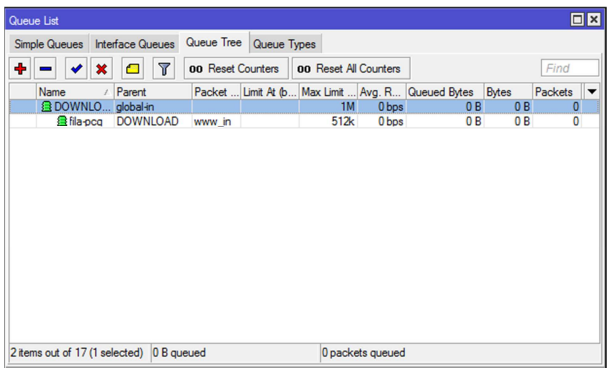


Figura 4.63 Queue fila_pcq

- ***Creación de colas PCQ***

Se crea 2 colas: pcq-dowload y pcq-upload, siguiendo los siguientes pasos que señalas las figuras 4.64, 4.65, 4.66 y 4.67.

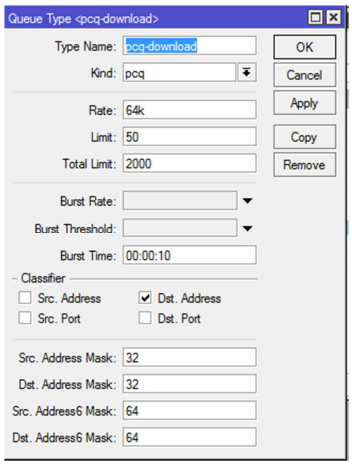


Figura 4.64 Queue Type – pcq download

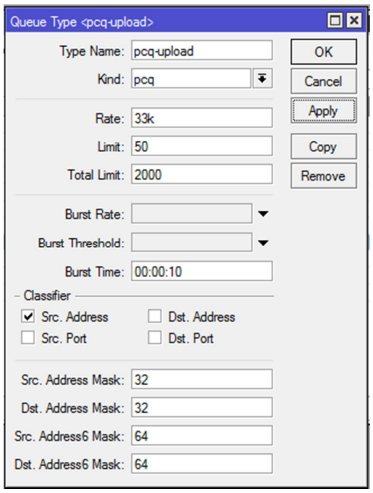


Figura 4.65 Queue Type – pcq upload

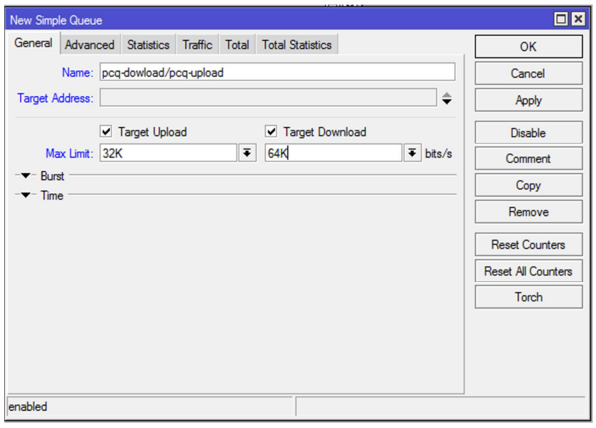


Figura 4.66 New simple Queue - General

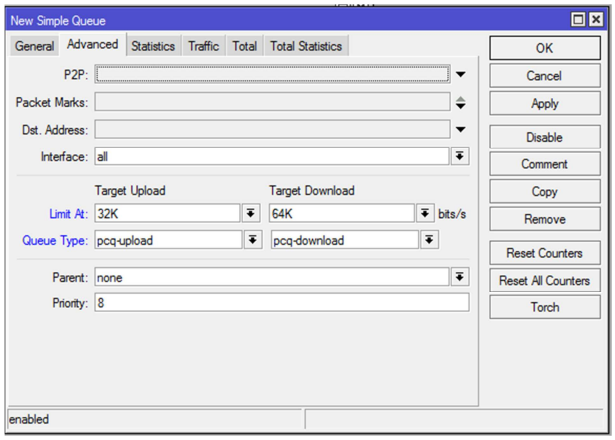


Figura 4.67 New simple Queue – General

4.6.7.9 **Queue tree**

- Trabajar con árboles de colas es una de la manera más elaborada de administrar el tráfico, con ellos es posible construir una medida de jerarquías de clases.
- Los filtros de árboles de colas son aplicados en las interfaces especificadas, los filtros son solo marcas que el firewall, es el flujo de paquetes en los filtros de mangle opción de ver los paquetes en el orden en que llegaron en el router.
- Los filtros en las interfaces globa-in y global-out son ejecutados antes de los filtros simples, fijarse que los queue simple están separadas en 2 partes: direct en global-out y reverse en global-in.
- Se hacen a las configuraciones con doble queue, considerando que no puede ser superior a los límites mínimos de activos.

4.6.7.10 **Manipulación y clasificación del tráfico**

Para otorgar Calidad de Servicio y manipular el tráfico de red, se manejan procedimientos básicos de clasificación y asignación de prioridad. Al

implementar calidad de servicio, los paquetes ya se encuentran marcados. Esta marcación se realiza dentro del campo TOS del paquete IP y en base a esta marcación se indica al router que paquetes tienen más o menos prioridad. En este proyecto se usará Mangle y Queue Tree ya que presenta los siguientes objetivos:

- Marcar el tráfico por tipo en la cadena mangle "prerouting".
- Priorizar y limitar el tráfico por tipo de Global-in HTB.
- Vuelve a marcar el tráfico de clientes en la cadena mangle
- Forward o Postrouting.
- Limitar el tráfico por cliente en la interfaz HTB.

Es necesario mantener las reglas mangle en un mínimo de colas para así aumentar el rendimiento de la misma.

- **Configuración de encolamiento**

La figura 4.68 muestra la presentación de la pantalla de presentación de Queue List.

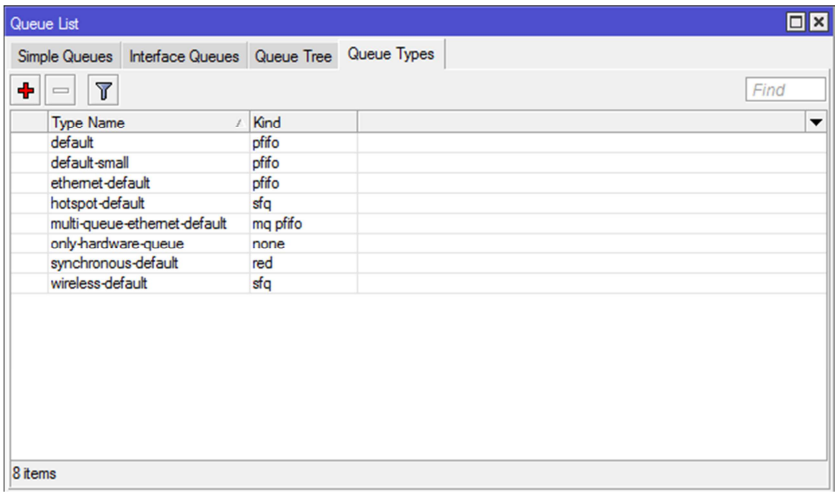


Figura 4.68 Queue List

Al hacer doble clic sobre la función se abrirá la siguiente ventana (véase la figura 4.69):

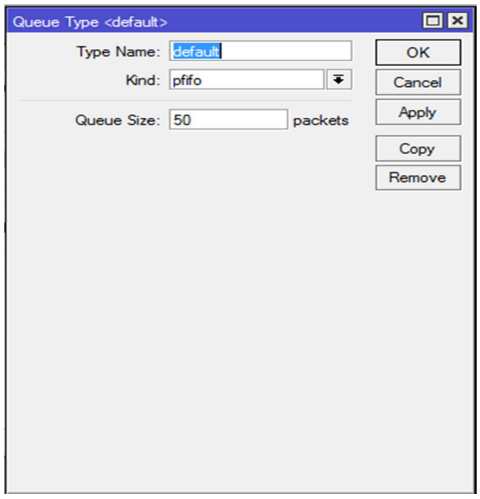


Figura 4.69 Configuración de Queue List

pfifo - Packet First-In First-Out – Es el algoritmo más simple de colas. Los paquetes se sirven en el mismo orden en que se reciben.

bfifo – Al igual que PFIFO, excepto que este algoritmo es basado en bytes pero no basada en paquetes.

red - Random Early Detection – Un algoritmo para evitar la congestión en las redes de conmutación de paquetes.

sfq - Stochastic Fair Queuing.

none – (Igual que default) El tipo de cola, ya que es de forma predeterminada para la interfaz específica.

Queue tree

Para la configuración seguir los pasos descritos en las figuras 4.70 y 4.71.

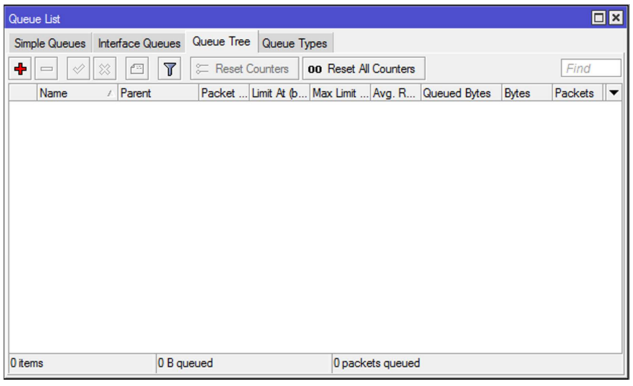


Figura 4.70 Ventana principal de Queue List

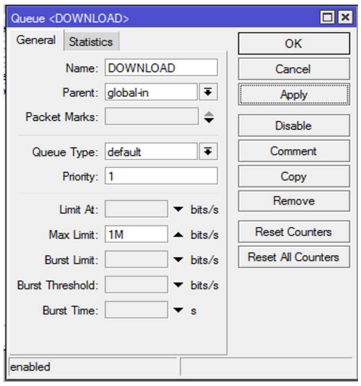


Figura 4.71 Queue Download

4.6.7.11 **Configurar QoS transparente**

Hacer clic en Bridge y en la nueva ventana hacer clic en el botón (+), asignar el nombre, en este caso se le asignó bridge_QoS y aceptar (véase la figura 4.72).

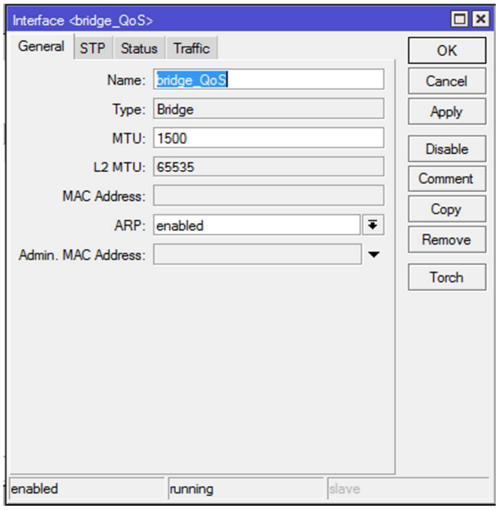


Figura 4.72 Interface Bridge_QoS

En la viñeta Ports hacer clic en el botón +, asignar la Ethernet que corresponda, en este caso seleccionar la ether1 pero se debe repetir el proceso para cada una de ellas (véase la figura 4.73).

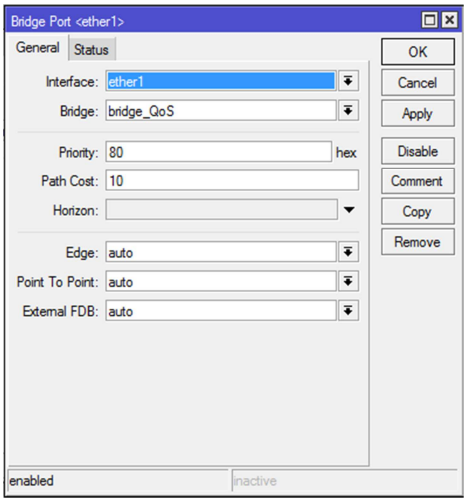


Figura 4.73 Bridge Port –ether1

Una vez que se realice el mismo paso para cada una de las interfaces, una vez ya realizado el proceso dentro de la ventana Bridge deberá estar como indica la figura 4.74.

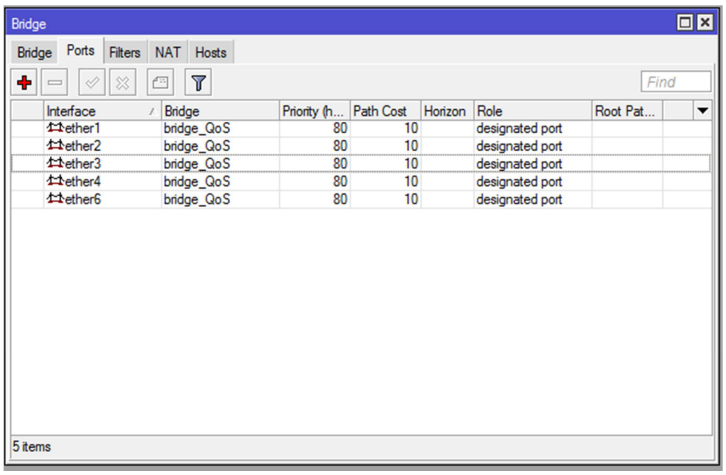


Figura 4.74 Bridge Port – todas las Ethernet

Para comprobar que se realizó bien la configuración, hacer clic en la opción **interfaces** y aparecerá un nuevo espacio del bridge que recientemente se lo creó (véase la figura 4.75).

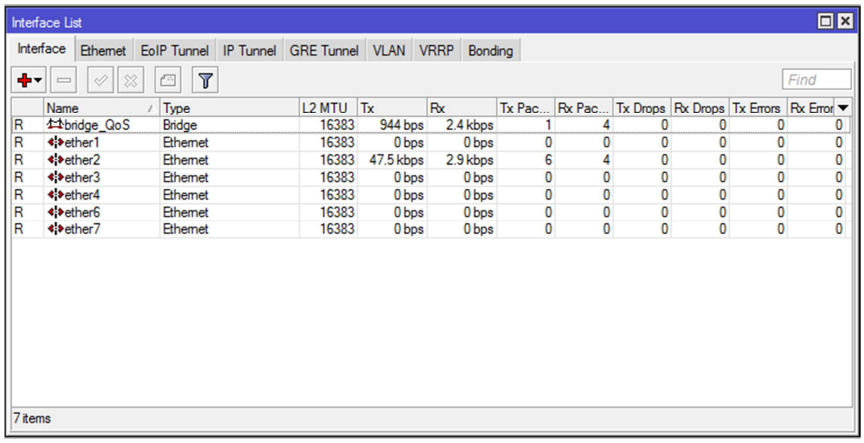


Figura 4.75 Bridge QoS en la lista de interfaces

4.6.7.12 **Configuración Hotspot**

Hotspot es un término utilizado para referirse a un área pública donde está disponible un servicio de acceso a internet, normalmente a través de una red WI-FI, aplicaciones típicas incluyendo el acceso en hoteles, aeropuertos, universidades, etc. El concepto de Hotspot puede ser usado en tanto para dar acceso controlado a una red cualquiera, con o sin cable, a través de autenticación basada en nombre de usuario y contraseña. Cuando en un área de cobertura de un Hotspot, un usuario que usa una laptop y trata de navegar por la web, es redireccionado a una página del Hotspot que pide sus credenciales normalmente nombre de usuario y contraseña, si está autenticado el usuario gana acceso a Internet logrando que su actividad sea controlada por tiempo y uso. Se debe considerar que un hotspot está disponible para ser utilizado en lugares relativamente pequeños. En el menú principal seleccionarla opción **IP** donde se desplegará varias opciones, seleccionar la opción **Hotspot** como señala la figura 4.36 para proceder a la configuración necesaria. Seleccionar **IP** y se desplegará más opciones donde se selecciona **Hotspot**, en la parte superior se escoge la pestaña

Servers y luego en el botón **Hotspot Setup**, para iniciar con el asistente de configuración de Hotspot Server (véase la figura 4.76).

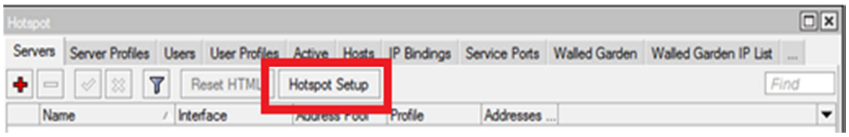


Figura 4.76 Hotspot Setup

HotSpot Interface, se debe especificar la interfaz donde se configurará el Hotspot server, elegir la interfaz de red LAN o tarjeta de red de los clientes. En este caso se ha seleccionado la ether1 porque se está realizando cada una de las configuraciones en completo orden para que luego no exista conflictos de información. Dentro la interfaz ejecutar Hotspot y hacer clic en **Next.**

Local Address of Network, aparecerá automáticamente la puerta de enlace de los clientes, está tomando los datos del IP de ether1.

Aquí se puede establecer la dirección IP en la interfaz del Hotspot, aquí se ha instalado la red IP con su respectiva máscara de subred (véase la figura 4.77). Hacer clic en **Next** y continuar con la configuración.

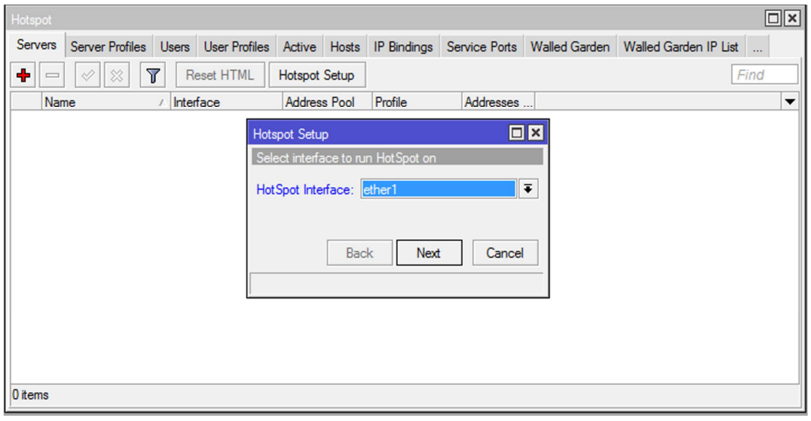


Figura 4.77 Select interface to run Hotspot on

Dentro de **Set pool for Hotspot addresses** se señala el rango que estará disponible para los clientes, que se ajustará automáticamente de la IP y la

máscara de subred que se ha definido en el anterior paso. ***Masquerade Network***, desmarca ya que se tiene el servidor funcionando, por lo tanto ya se cuenta con el enmascarado. Si se activa este check, que creará otro enmascarado, pero en este caso será por rango de red (véase la figura 4.78). Hacer clic en **Next**.

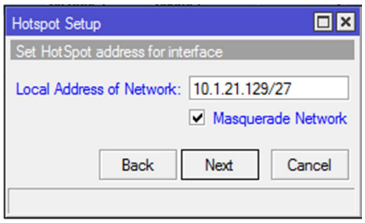


Figura 4.78 Set Hotspot address for interface

Address Pool of Network, aparecerá un rango de IP's que serán asignados a los clientes para que así obtengan un IP automáticamente. En este caso apareció un rango ya definido, este rango lo tomó de una configuración previa ya que tenía configurado un servidor DHCP. Si no hubiera un servidor DHCP funcionando, este paso activaría uno obligatoriamente. Ya más adelante se podrá deshabilitar (véase la figura 4.79). Hacer clic en **Next**.

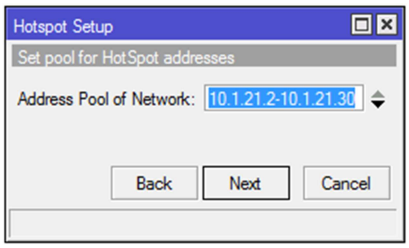


Figura 4.79 Set pool for Hotspot addresses

Al ingresar a **Select hotspot SSL certificate**, escoger la opción **none** (véase en la figura 4.80), ya que no se cuenta con un certificado SSL. Estos certificados son utilizados para validar una página web cuando se utiliza el protocolo el certificado digital es una forma de asegurarse de que el sistema es seguro para los usuarios, el sistema funciona Mikrotik certificado digital.

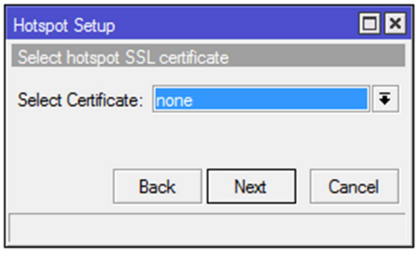


Figura 4.80 Select hotspot SSL certificate

Este paso está relacionado directamente con el paso anterior, esta interface es para la asignación de la IP del servidor SMTP, por lo tanto al ingresar a la interface **Select SMTP Server** dejar tal como está en la IP 0.0.0.0 como indica la figura 4.81, ya que esta configuración no interrumpe los servicios SMTP y no se cuenta con un servidor SMTP. Hacer clic en **Next**.

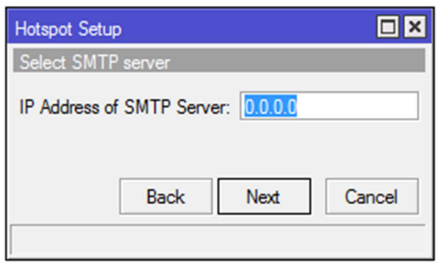


Figura 4.81 Select SMTP server

Dentro de esta opción se deja en blanco la opción porque no se cuenta con un servidor DNS (véase la figura 4.82). Hacer clic en **Next.**

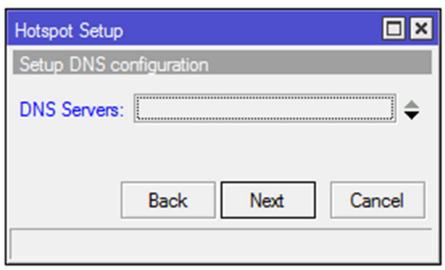


Figura 4.82 Setup DNS configuration

En la interface **DNS name of local hotspot server** también se deja en blanco, en el paso anterior no se asignó ningún servidor por lo cual no tiene sentido configurar esta sección (véase la figura 4.83). Hacer clic en **Next**

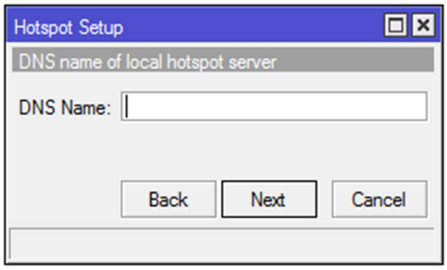


Figura 4.83 DNS name of local hotspot server

Dentro de esta opción se deja tal como lo indica en la figura 4.84 ya que en las siguientes configuraciones asignará usuarios con sus respectivas contraseñas.

Name of Local Hotspot User, por defecto, el nombre de usuario administrador para el logueo en el hotspot es ***admin***, aunque si lo quieren cambiar, no existe conflicto, pero se debe recordar ya que con ese nombre se autenticarán al hotspot por primera vez. Hacer clic en **Next** y finalizar con la configuración del Hotspot.

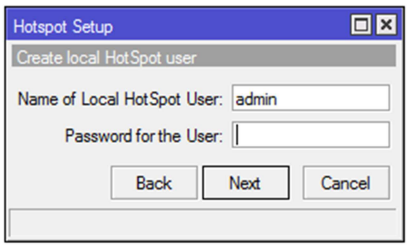


Figura 4.84 Create local Hostspot user

Una vez que se concluya la configuración del Hotspot saldrá un mensaje que nuestro hotspot fue configurado satisfactoriamente (véase en la figura 4.85), si nuestro WinBox estaba conectado al servidor MikroTik por IP, seguramente se desconectará inmediatamente. Si se encuentra conectado por MAC, seguirá conectado. En todo caso, el servidor hotspot ya se encuentra configurado (véase la figura 4.85) y si se intenta abrir una nueva página, este mostrará el portal cautivo de MikroTik.

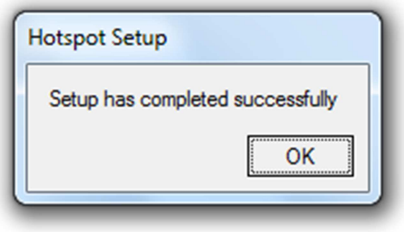


Figura 4.85 Mensaje de finalización de la configuración de Hostspot

Se procede a la configuración de la misma manera que se acaba de indicar con todas las interfaces y como resultado se debe presentar la interface que está representada por la figura 4.86.

Nota: Cada configuración debe tener relación con la tabla 4.4 para que luego no exista conflicto dentro de las configuraciones

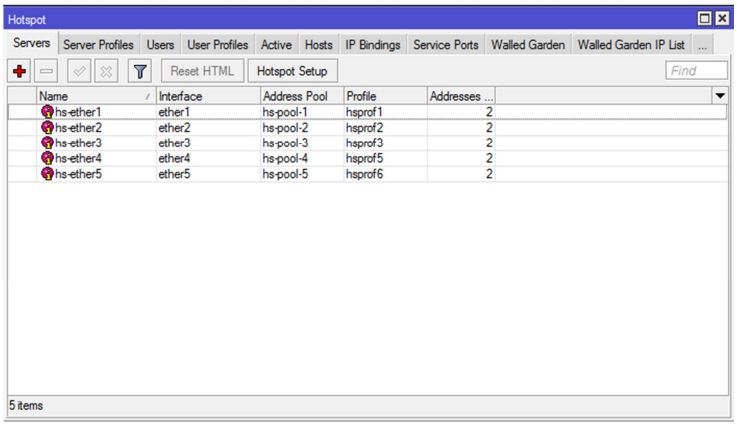


Figura 4.86 Configuraciones de hotspot de todas las interfaces

4.6.7.13 **Creación de perfiles de usuarios**

Para la utilización más óptima de hotspot se crearon perfiles de usuario, haciendo referencia a cada segmento por tipo de usuario. Los perfiles definen el punto de acceso como un grupo que se utilizará para acceder a ese perfil. Dentro del menú del Hotspot, seleccionar la viñeta **User profiles**.

Se presentará la interface que se aprecia en la figura 4.87.

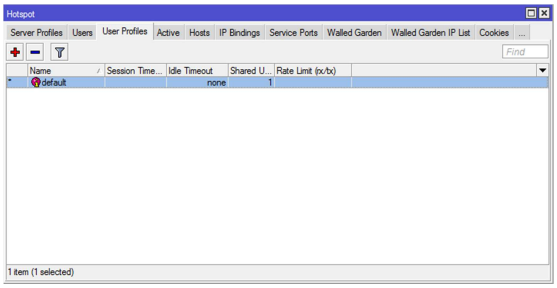


Figura 4.87 Pantalla principal – User profiles

Hacer clic en la opción para agregar perfiles, según la figura 4.88 hay un botón con el símbolo (+) donde permite esta opción.

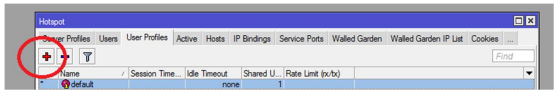


Figura 4.88 Agregar perfiles

Una vez que ya seleccionar esta opción aparecerá la siguiente ventana (véase en la figura 4.89).

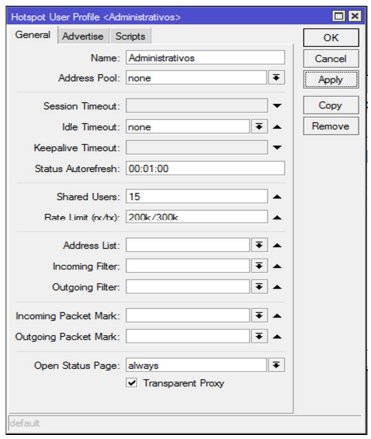


Figura 4.89 Nuevo perfil Hotspot

La pestaña **General** brinda las siguientes opciones:

Name: Es la opción donde se asigna el nombre del perfil.

Address pool: Lugar del pool creado en el proceso de la configuración del punto de acceso.

Session Timeout: Es el tiempo permitido para el usuario.

Idle Timeout: Tiempo de espera del sistema, la mejor opción es dejar en blanco y no manipular este campo.

keepalive Timeout: Aquí seleccionar la opción que está por default.

Status Autorefresh: Es el período en que el sistema actualiza todos los datos del punto de acceso.

Shared Users: Número de usuarios permitidos, este comparte funciones del mismo usuario para el número de clientes que se define.

Rate Limit (tx/rx): Limitación de velocidad. El ajuste de la velocidad debe ser transmisión / recepción de velocidad o de carga / descarga y la velocidad será definido por poner K al final de la velocidad. En la pestaña **Advertise** solo se tiene tres opciones, aquí se establece el perfil básico y se agrega los nuevos usuarios.

Advertise URL: Página que se muestra al cliente y esta puede ser en secuencia.

Advertise Interval: Intervalo para mostrar pop-up.

Advertise Timeout: Advertencia para encerrar a los usuarios.

Para definir el perfil que puede entrar en tantos perfiles como desee su ISP (véase la figura 4.90). Hacer clic en **apply** y luego hacer clic en **OK**.

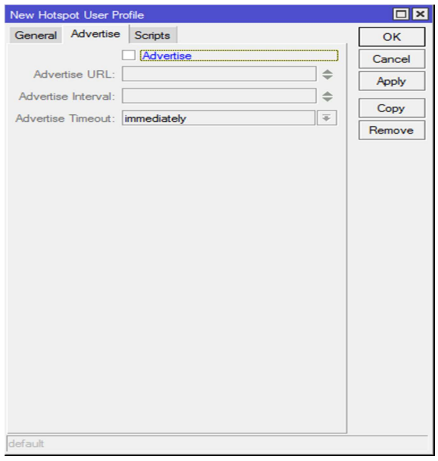


Figura 4.90 Anuncios Hotspot

Cuando ya se configure los cuatro perfiles, siguiendo los mismos pasos para cada perfil Mikrotik RouterOS presentará la siguiente ventana (véase en la figura 4.91) donde se aprecia los perfiles correspondientes a los segmentos:

- Administrativos
- Alumnos
- Docentes
- Investigadores

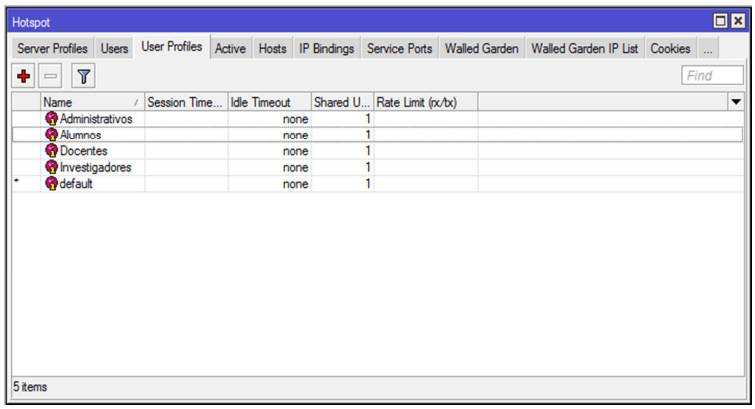


Figura 4.91 Perfiles Hostpot

4.6.7.14 **Administración de usuarios**

Después de crear los perfiles necesarios por cada segmento de tipo de cliente, así como ver los datos relevantes sobre el mismo tiempo de uso, la cantidad del tráfico de paquetes y muchas otras opciones relevantes. Dentro del menú del Hotspot se tiene varias viñetas de opciones, dentro de la viñeta **Users** hacer clic en el botón (+) para agregar un nuevo usuario y concatenar cada uno de ellos con los perfiles creados anteriormente (véase la figura 4.92).

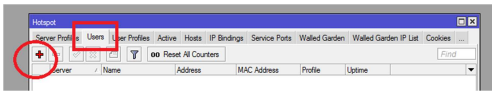


Figura 4.92 Agregar nuevo usuario Hotspot

Señalar **all** en servicios, poner el nombre y el perfil con el que se vaya a trabajar (véase la figura 4.93).

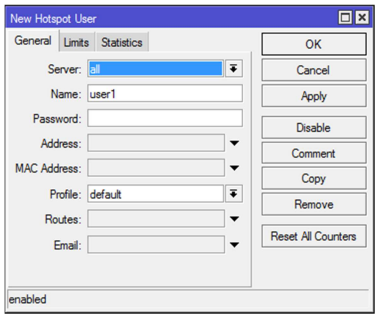


Figura 4.93 Nuevo usuario Hotspot

Dentro de la Viñeta General se tiene:

Server: Aquí se indica el servidor o el punto de accesos que usará exclusivamente el usuario.

Name: Nombre de usuario, se asignó los nombres de los segmentos establecidos por tipo de usuario.

Password: Contraseña, existe la opción en blanco pero como se trata de administrar a los usuarios se consideró aplicar contraseña en cada uno de los segmentos. Se aplicó contraseñas para cada uno de los segmentos como indica la tabla 4.5.

Tabla 4.5 Usuario-Contraseña

Usuario	Contraseña
Administrativo	administrativos1
Alumno	alumnos1
Docente	docentes1
Investigador	investigadores1

Address: No se asignó dirección IP alguna ya que Mikrotik automáticamente asigna una IP a sus clientes.

MAC Address: Esta opción se dejó en blanco ya que solo si se tiene una cuenta MAC se puede atar el MAC de inicio de sesión.

Profile: Dentro de esta opción se escoge uno de los perfiles creados anteriormente de acuerdo con el plan de cada cliente.

Routes: Esta opción se dejó en blanco ya que define una ruta específica para el cliente.

Email: Dentro de esta opción también se dejó en blanco porque este cliente van a usar varias personas por lo cual no tendría sentido asignar.

Por medio de la tabla 4.5 asignar nombre de usuario y contraseña. La figura 4.94 muestra el contenido de toda la pantalla.

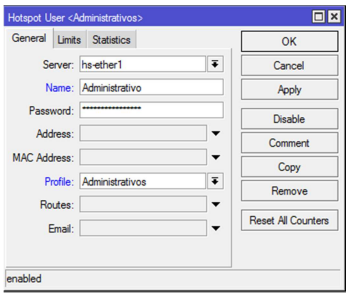


Figura 4.94 Nuevo Usuario Hotspot – Administrativo

En la viñeta Limits hay opciones de más servicios para los clientes, se puede establecer un contrato de tráfico de datos mensual y se puede limitar el uso de tiempo a los clientes. Excelente opción para un servicio prepago o de oferta o de un servicio de pruebas para un futuro cliente.

La viñeta **Limits** ofrece las siguientes opciones:

Limit Uptime: Limita el tiempo de conexión al cliente.

Limit Bytes In: Limita la cantidad para que el cliente realice upload.

Limit Bytes Out: Limita la cantidad para que el cliente realice download.

Limit Bytes Total: Es la suma de todos los límites anteriores.

Dejar las opciones de límites en blanco (véase en la figura 4.95).

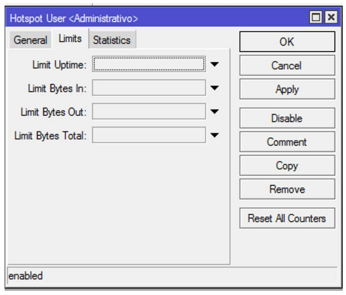


Figura 4.95 Límites usuarios Hotspot

Se crea un usuario por cada segmento, tomando como guía la tabla 4.5 para usuario y contraseña, siguiendo los pasos antes señalados. Una vez ya que ya se han creado a todos los usuarios haciendo referencia con sus respectivos perfiles se presentará la interfaz de la siguiente manera (véase en la figura 4.96).

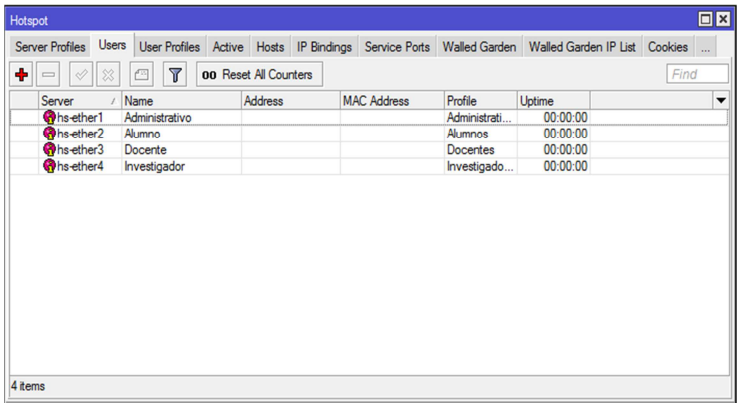


Figura 4.96 Usuarios Hotspot

Para observar quién está conectado mediante Mikrotik, el tiempo de uso y la cantidad de tráfico que existe, ingresar nuevamente al menú de **Hotspot**.

Ingresar a la viñeta **Active** y aparecerá la interfaz que indica el figura 4.97.

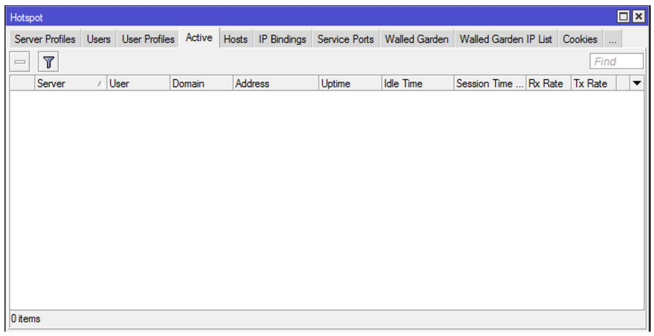


Figura 4.97 Usuarios activos

Se podrá observar a cada cliente que esté activo dentro de la ficha, aquí se detallará quién está concetrado, su tasa de transferencia y la dirección IP.

4.7 EXTRUCTURACIÓN DEL ANCHO DE BANDA DE LA RED INTERNA DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO

Hoy en día, tanto estudiantes como docentes de la Institución esperan como mínimo contar con acceso a redes confiables de alta velocidad. La universidad necesita contar con nuevas estrategias para controlar de manera más justa y eficaz el uso del ancho de banda entre estudiantes, docentes, administrativos e investigadores. Al proporcionar un control completo del ancho de banda, estas estrategias pueden garantizar que las aplicaciones fundamentales cuenten siempre con los recursos que necesitan, que se permitan las actividades recreativas pero con la debida asignación de prioridad. Sin embargo, el software Mikrotik RouterOS es una herramienta de control de ancho de banda y se puede aplicar para redes educativas. **Nota**: La administración institucional general cuenta con 40 Megas (véase en la figura 4.98).

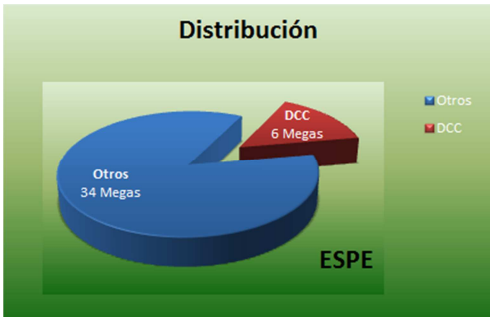


Figura 4.98 Administración de ancho de banda institucional – actual

El ancho de banda debe ser administrado para permitir a los administrativos de la Institución puedan definir reglas con distintos niveles de granularidad, según el tipo de tráfico, la naturaleza de las aplicaciones y el área de la red.

Además, para brindar un auténtico control del ancho de banda en toda la institución, estas herramientas deben caracterizarse por su escalabilidad y facilidad de administración. Para resolver estos problemas, se aplicó una alternativa para controlar, proteger y optimizar los recursos de las redes del campus, se consideró los siguientes puntos:

- Número de usuarios.
- Prioridad de servicios.

Considerando que el Departamento Ciencias de la Computación (DCC) maneja a diario un ancho de banda de 6 Megas donde se procedió a la siguiente distribución (véase en la figura 4.99), considerando la tabla 4.6.

Tabla 4.6 Usuarios vs requerimientos

	Alumnos	**Docentes**	**Administrativos**	**Investigadores**
Población	700	102	10	100
Servicios	HTTP DNS	HTTP DNS	HTTP DNS	HTTP DNS
Horarios	Matutino Vespertino	Matutino Vespertino	Matutino Vespertino	Matutino
Megas	2	2	1	1

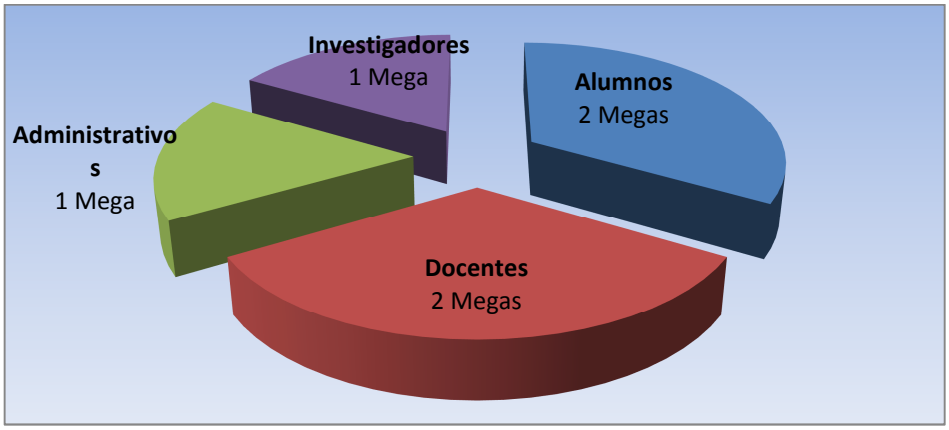


Figura 4.98 Administración de ancho de banda

En relación al Departamento Ciencias de la Computación, el ancho de banda administrado se ha realizado con las 6 Megas que cuenta hoy en día dicho

departamento. Por seguridad se considera la restricción de varias páginas web pero este no debe ser un limitante para el uso adecuado de los servicios ya que la actualidad se encuentra un gran número de restricciones mediante proxy, que pueden ser burlados por otro tipo de software que se encuentra de manera libre en el internet. Con la administración del Mikrotik RouterOS se tiene mayor dificultad de burlarse del sistema ya que es un sistema nuevo de administración y las restricciones aplicadas serán realmente necesarias. Se consideran herramientas de estudio las siguientes opciones:

- Messenger
- Correo electrónico
- Redes sociales
- Buscadores

Al brindar un servicio de mayor ancho de banda a los estudiantes (la población más numerosa) y restricciones necesarias cada usuario (alumno) notará la mejora inmediatamente y calificará a los servicios de una manera más amigable. A la sección de docentes se asignó el mismo ancho de banda que de estudiantes tomando en cuenta que la población es mucho menor pero los servicios de cada docente tienen mayor prioridad, por ejemplo al pasar notas hasta una fecha límite, por lo general en esas fechas el sistema se satura por la demanda de servicios y se precisa velocidad para el servicio del banner. Tantos investigadores como administrativos requieren de servicios constantes con menor prioridad, por lo tanto se asignó 1Mega a cada segmento. La suma de ambos segmentos no es considerable como para ofrecer mayor velocidad de ancho de banda pero aun así ya existe mejoras de servicios de red. Ingresar a la opción **Queues**, con la opción (+)

agregar una nueva regla, en este caso dejar el nombre que sale por default, colocar la IP del usuario que en este caso es para el segmento de los administrativos, la opción de **Burst time** es el tiempo con el que inicia el **Burst Limit** hasta llegar a **Max Limit**, realizar una regla para cada segmento basándose en la IP que debe llevar cada Ethernet y el ancho de bando que se estableció para cada uno de ellos (véase la figura 4.100).

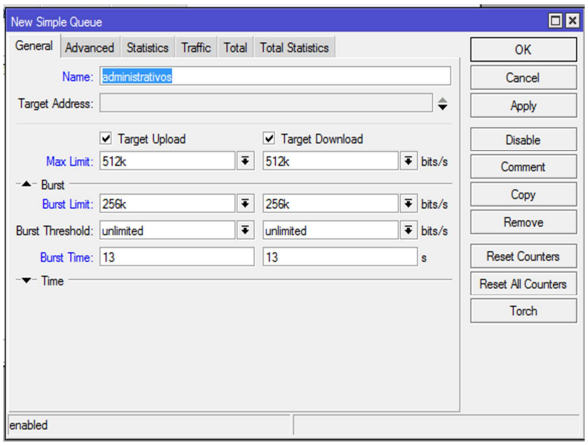


Figura 4.100 Nueva cola simple

En la opción de **Advanced** seleccionar a la interface que pertenece, en este caso es la ether1 que se refiere al segmento de Administrativos (véase la figura 4.101).

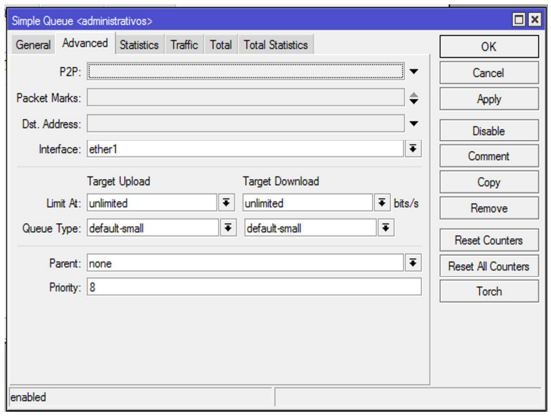


Figura 4.99 Cola simple – administrativos

Una vez asignado cada regla para cada Ethernet el cuadro de **Queue List** debe contener las reglas recientemente establecidas, como se ve en la figura 4.102.

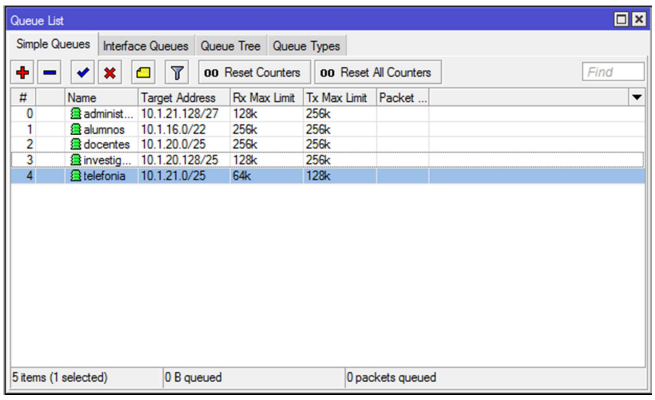


Figura 4.100 Lista de colas

4.8 CONFIGURACIÓN DEL SWITCH

Tras la necesaria aparición de los computadores en las áreas de trabajo. Las redes representan la vital comunicación entre computadores y dispositivos como impresoras en una empresa sea privada o pública. Cuando la red crece de forma exponencial y que se encuentre disponible en todo momento y para cualquier computador o dispositivo, crece la necesidad de una correcta administración de los recursos de esa red y un control de la misma que evite colapsos que puedan incomunicar los elementos de la red. Existen numerosas herramientas que ayudan a la tarea del administrador de la red. Se ha simulado la configuración con un switch cisco catalyst 2950, esta configuración corresponderá a la del switch principal del Departamento Ciencias de la Computación. Antes de proceder a las pruebas para verificar resultados de las configuraciones antes realizadas se deberá configurar el switch administrable que tendrá establecidas las 4 VLAN`s que pertenecen a

cada segmento antes establecido. Cabe recalcar que el switch utilizado tiene 24 puertos y se estableció tal como indica la tabla 4.7.

Tabla 4.7 Asignación de puertos del switch

SEGMENTO	NÚMERO DE PUERTOS
Alumnos	1,2,3,4,5,6
Docentes	7,8,9,10,11,12
Investigadores	13,14,15,16,17,18
Administrativos	19,20,21,22,23,24
Telefonía IP	25

El problema es el siguiente: Se espera administrar un dispositivo intermedio en una red. Se supone que se encuentra como administrador de una red, con una topología no muy compleja. Como paso previo se debería conocer y diseñar una estrategia para la correcta administración y posteriormente documentarla. La documentación de esa red y de las decisiones que se tome deberá ser documentada para los posteriores responsables. Tras el conocimiento de nuestra red, se deberá tomar decisiones para la correcta administración y la toma de decisiones para mejorarla, si presentara un problema para reparar los fallos a los que se puede enfrentar o plantear estrategias frente a posibles complicaciones de seguridad a los que se puede enfrentar. Para este proyecto se utilizará el switch Cisco como centro de la red. Para ello se deberá conocer que posibilidades ofrece. Ya que un conocimiento exhaustivo del mismo podría ser de gran utilidad para cumplir el objetivo.

Nota: Es necesario considerar que no se ha percatado aún de un problema que puede surgir, se encuentra hablando de un dispositivo a nivel de enlace (consulta la pila de protocolos de TCP/IP). Por tanto como es posible tener

una dirección IP que es de un nivel superior. Cuando el dispositivo está sin configurar, la única manera de poder acceder al switch es a través del puerto CONSOLE. De esta manera se puede configurar una IP al dispositivo. Por lo tanto, si se desea que el switch (véase la figura 4.103) no sea transparente y asignarle una IP.

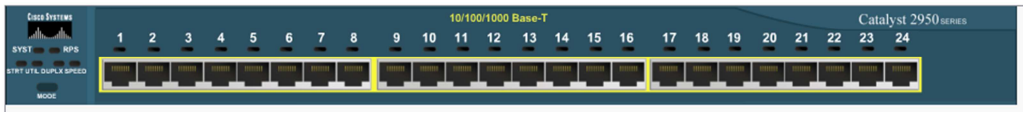


Figura 4.101 Switch Cisco Catalyst 2950

Considerando los 4 segmentos y que cada uno de ellos cuenta con un swtich, se ha considerado la topología conformada solo por switches para la configuración del switch principal (véase la figura 4.104).

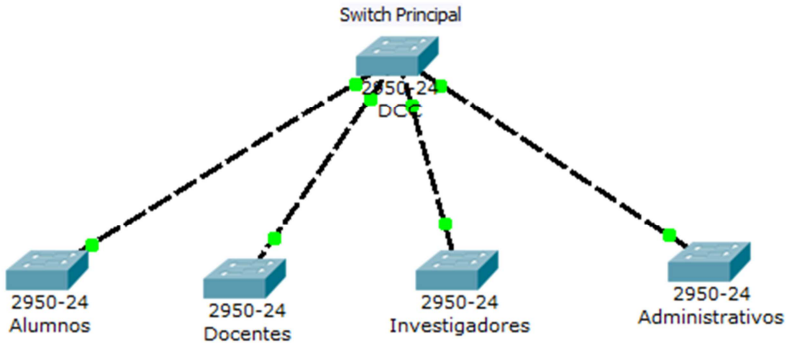


Figura 4.102 Topología considerando solo swtiches

Para el segmento Alumnos se tomará la Vlan2, ya que la Vlan1 es de administración. Según la configuración establecida se armó la tabla 4.8 que indica su número con sus respectivos nombres.

Tabla 4.8 Vlans del switch

VLAN No	VLAN Name
1	default
2	Alumnos
7	Docentes
13	Investigadores
19	Administrativos
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

Para tener una mejor coordinación se elaboró la tabla 4.9 como objetivo de una guía.

Tabla 4.9 Asignación Vlan

Segmento	Vlan	Direcciones IP
Alumnos	2	10.1.16.1/24
Docentes	7	10.1.17.1/26
Investigadores	13	10.1.17.65/26
Administrativos	19	10.1.17.129/26
Telefonía IP	25	10.1.17.193/26

Por medio de la tabla 4.10 se determinó los accesos que tiene cada segmento.

Tabla 4.10 Acceso de VLANs

	ALUMNOS	DOCENTES	ADMINISTRATIVOS	INVESTIGADORES	TELEFONÍA IP
POBLACIÓN	700	102	10	100	15
ACCESO	VLAN2	VLAN7 VLAN2 VLAN25	VLAN13 VLAN2 VLAN25	VLAN19 VLAN2	VLAN25 VLAN2

Mediante las necesidades planteadas el switch principal tendrá la siguiente configuración:

Ingreso al switch: Switch>enable

Ingreso a modo global
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Creación de Vlan y asignación de nombre:
Switch(config)#vlan 2
Switch(config-vlan)#name Alumnos
Switch(config-vlan)#exit
Switch(config)#vlan 7
Switch(config-vlan)#name Docentes
Switch(config-vlan)#exit
Switch(config)#vlan 13
Switch(config-vlan)#name Investigadores

```
Switch(config-vlan)#exit
Switch(config)#vlan 19
Switch(config-vlan)#name Administrativos
Switch(config-vlan)#exit
Switch(config-vlan)#name Telefonia
Switch(config-vlan)#exit
```

Asignación de IPs a cada Vlan

```
Switch(config)#interface vlan2
Switch(config-if)#ip address 10.1.16.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 7
Switch(config-if)#ip address 10.1.17.1 255.255.255.192
Switch(config-if)#exit
Switch(config)#interface vlan 13
Switch(config-if)#ip address 10.1.17.65 255.255.255.192
Switch(config-if)#exit
Switch(config)#interface vlan 19
Switch(config-if)#ip address 10.1.17.129 255.255.255.192
Switch(config-if)#exit
Switch(config)#interface vlan 25
Switch(config-if)#ip address 10.1.17.193 255.255.255.192
Switch(config-if)#exit
```

Asignación de puertos a cada Vlan

```
Switch#configure terminal
Switch(config)#interf range f0/2,f0/3,f0/4,f0/5
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan2
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#interf range f0/7,f0/8,f0/9,f0/10,f0/11,f0/12
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan7
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#interf range f0/13,f0/14,f0/15,f0/16,f0/17,f0/18
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan 13
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#interface range f0/19, f0/20, f0/21,f0/22, f0/23, f0/24
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan 19
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#interface range f0/25
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan 25
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
```

CAPÍTULO 5

CONCLUSIONES, RECOMENDACIONES

5.1 CONCLUSIONES GENERALES

- Se abre alternativas de gestión de red, infraestructura de nertworking, competitividad y estabilidad tecnológica considerando recursos económicos y prestaciones para el crecimiento de la Institución. Mediante este proyecto se abre la posibilidad a nuevas alternativas rentables en equipos de Telecomunicaciones como es Mikrotik.
- Dentro del Departamento no se trabajó bajo ningún estándar, lo que da como resultados gastos innecesarios como es el caso de los AP`s, al mantener 3 de ellos en el mismo canal crea vacíos y desperdicio de rendimiento de los equipos.
- El mejoramiento o adquisición de un equipo tecnológico de una empresa necesariamente no debe significar realizar una gran inversión, sino la ocasión de analizar nuevas alternativas para el mejoramiento en la administración del ancho de banda.
- La institución cuenta con 40 Megas de ancho de banda de lo cual se proporciona 6 Megas para todo el DCC incluido laboratorios de computación que son utilizados por todo el alumnado de la ESPE, esta distribución no es suficiente para las necesidades de este departamento.
- El sistema operativo Mikrotik RouterOS permitió el desarrollo de la propuesta por el proyecto, pese a ser una herramienta con valor

de licenciamiento moderado vs a otros equipos propietarios, se obtiene beneficios bajo un costo menor, una instalación y administración (mediante Winbox) amigable.

- Mediante la implantación de calidad de servicio (QoS) se posibilita la opción de obtener mayor seguridad y servicios de calidad para aplicaciones avanzadas, tan solo el tráfico de las aplicaciones deben tener prioridad en relación con aplicaciones de uso básico.
- Una buena infraestructura para una empresa garantiza la estabilidad tecnológica, así no habrá dependencia y se puede administrar el ancho de banda según la conveniencia.
- Para una eficaz administración y facilidad en la gestión de una red depende esencialmente de las herramientas administrativas que los dispositivos de red incorporen, estas herramientas deben permitir detectar problemas a tiempo considerable y su solución debe ser en poco tiempo e intuitiva.
- La aplicación de mecanismos de medición de tráfico y de diferenciación de servicios no resulta suficiente para la provisión de garantías de QoS sino se evita que la red llegue a una situación de sobreutilización de sus recursos, inevitablemente provocando congestión. Por lo cual es necesario aplicar mecanismos de control de admisión.
- Hubiera sido considerable realizar las pruebas con el switch principal que pertenece al Departamento Ciencias de la Computación y así poder constatar la gran utilidad y beneficios que se puede ofrecer por medio de este estudio.

5.2 RECOMENDACIONES

- La aplicación de Mikrotik permite establecer a futuro una fácil configuración y validar políticas de gestión para su uso de campo educativo y estabilidad.
- Se debe mantener la utilización de equipos bajo estándares para que a futuro sea más fácil el mantenimiento de los equipos y así aprovechar la utilidad de cada uno.
- Antes de realizar una inversión en un nuevo equipo tecnológico es recomendable investigar alternativas que ofrece el mercado, evaluando su disponibilidad y el alcance de soporte técnico que ofrece la empresa proveedora de equipos posterior a la implementación de los enlaces.
- Se debería realizar una nueva redistribución de ancho de banda para el DCC, considerando que se brinda servicio de laboratorios de computación para toda la comunidad politécnica ya que para todo el alumnado se puede proporcionar tan solo 2Megas.
- Para la captura de tráfico de red, la mejor opción es utilizar un computador que contenga un sniffer, en el centro de la nube ya que ahí se realizará una captura de tráfico real que se está generando en la red.
- Realizar un análisis previo de cuáles son los requerimientos de ancho de banda, con el fin de tomar una opción de crecimiento a mediano y largo plazo, que emite requerir una inversión a un plazo menor a lo evaluado.

BIBLIOGRAFÍA

BIBLIOGRAFÍA CAPÍTULO II

- **[1]** Redes LAN

  http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

- **[2]** Medios de transmisión

  http://es.wikipedia.org/wiki/Medios_de_transmisi%C3%B3n

- **[3]** Wireless

  http://definicion.de/wireless/

- **[4]** Estándares inalámbricos

  http://es.wikipedia.org/wiki/IEEE_802.11

- **[5]** Servicios de red

  http://vgg.sci.uma.es/redes/servicio.html

- **[6]** Ancho de banda

  http://es.wikipedia.org/wiki/Ancho_de_banda_(inform%C3%A1tica)

- **[7]** Líneas dedicadas

  http://www.comteco.com.bo/index.php?option=com_content&view=article&id=24&Itemid=334

- **[8]** Elementos activos – pasivos de una red.

  http://www.zator.com/Hardware/H12_4.htm

- **[9]** Dirección IP

  http://es.wikipedia.org/wiki/Direccion_IP

- **[10]** Formatos de información

  http://www.arghys.com/construccion/informacion-intercambio.html

- **[11]** Calidad de servicio (QoS)

  http://es.wikipedia.org/wiki/Calidad_de_servicio

- **[12]** Proveedores de internet http://www.enlinea.ec/resultados.asp?tema=proveedores%20de%20internet&nivel=2
- **[13]** Tipos de conexiones PSI http://es.wikipedia.org/wiki/Proveedores_de_servicios_de_Internet
- **[14]** Enlaces de última milla http://www.netdatanetworks.com/product-list.php?scheme=1&section=2&subsection=8&article=41

BIBLIOGRAFÍA CAPÍTULO III

- **[1]** Imagen Switch principal. http://www.google.com.ec/imgres?imgurl=http://static.amkert.com/280-280/70/td/647782-9601.jpg&imgrefurl=http://www.amkert.com/3Com-Switch-4500G24port-p-129340.htm&usg=__ZCUzB8CT9T2y1sgT3r
- **[2]** Características del swirch principal. http://www.pcenlinea.com/mp/57889.html
- **[3]** Características tarjeta PCI http://www.dlinkla.com.do/home/productos/producto.jsp?idp=722
- Tutorial Mikrotik http://www.4shared.com/document/GK17Hjpy/livro_provedor_completo_mikrot.htm
- **[4]** Clasificación y Selección de Indicadores http://portal.veracruz.gob.mx/pls/portal/docs/PAGE/CGINICIO/PORTLETS_VERACRUZ_/MANOS_LIMPIAS/MANUAL%20GENERAL%20PARA%20LA%20CONSTRUCCI%D3N%20DE%20INDICADOR_.PDF
- **[5]** Ubicación de puntos de acceso

http://foro.seguridadwireless.net/noticias-wireless/como-reanimar-a-los-puntos-muertos-en-redes-wi-fi/

BIBLIOGRAFÍA CAPÍTULO IV

- **[1]** Mejoras el rendimiento de la red wireless http://www.adslnet.es/index.php/2007/08/21/mejorar-el-rendimiento-de-nuestra-red-wireless/
- **[2]** Configuración de reglas Mangle http://dspace.espoch.edu.ec/bitstream/123456789/316/1/18T00402.pdf
- **[3]** User Manager http://www.laserwifi.com/foros/showthread.php?t=28