PROYECTO DE GRADO

Presentado ante la ilustre UNIVERSIDAD DE LOS ANDES como requisito final para obtener el Título de INGENIERO DE SISTEMAS

Efectos del enrutamiento y de la calidad de servicio en la red metropolitana 802.11 de Fundacite Mérida

Por

TSU. Iris Uzcátegui
Tutor: Prof. Andrés Arcia
Asesor industrial: Ing. Histerlee Ramírez

Julio 2012

Efectos del enrutamiento y de la calidad de servicio en la red metropolitana 802.11 de Fundacite Mérida

T.S.U Iris Uzcátegui

Proyecto de Grado – Sistemas Computacionales, 116 páginas

Resumen: La red de Fundacite Mérida cubre gran parte del Estado y presta servicio a instituciones que contribuyen al desarrollo del país.

Esta red tiene entre sus objetivos, proporcionar servicio de Internet a instituciones públicas y gubernamentales así como dar cobertura a todos aquellos lugares que, por su geografía, son de difícil acceso y los proveedores comerciales de servicio de Internet no llegan, o no logran prestarles un servicio adecuado a sus necesidades.

Actualmente, la red de Fundacite Mérida presta servicio a 110 instituciones públicas y la cantidad de tráfico aumenta constantemente. Debido a esto se hace indispensable realizar estudios para determinar la forma de mejorar el uso del ancho de banda. Es por ello que se realiza un perfil de tráfico donde especificamos volumen, cantidad y tipo de tráfico. Además, se hace por primera vez un levantamiento completo de la topología y organización de la red metropolitana de Fundacite.

En este proyecto se busca entender el funcionamiento actual de la red para proponer mejoras que luego podrán ser implementadas, todo esto se logrará a través del método de desarrollo para el proceso de soluciones de problemas de ingeniería; el cuál nos va a permitir determinar las necesidades y posibles soluciones que se pueden implementar en dicha red.

En le capítulo 1 se habla de la institución donde se desarrolló el proyecto, lo objetivos planteados en base a las necesidades detectadas en la red de la institución, la metodología aplicada y el alcance que tiene el presente proyecto de grado.

Para el capítulo 2 se realizará una breve descripción de los conceptos más importantes investigados durante el desarrollo del proyecto.

El capítulo 3 describe el resultado del levantamiento de información de la topología física y lógica de la red de Fundacite.

Ya en el capítulo 4 se describe cómo se obtuvo las mediciones y se realiza un análisis de estas mediciones, análisis que permite obtener un perfil de la red de Fundacite para, finalmente, llegar a conclusiones y recomendaciones para que lograr un mejor funcionamiento de la red.

Palabras Claves: Red inalámbrica, Red de Área Metropolitana, perfil de tráfico.

Dedicatoria

A mis padres, la razón principal por la cual continué adelante en mi carrera profesional.

Índice

Índice de Tablas

Índice de Figuras

Agradecimientos

A Dios, por darme la fortaleza y la voluntad de continuar y finalizar con éxito mi carrera profesional.

A la ilustre Universidad de Los Andes, por haberme abierto las puertas hacia el conocimiento.

A Fundacite Mérida, por permitirme crecer profesionalmente durante mis años de estudio en la Universidad de Los Andes.

Al CDCHTA de la ULA, por el financiamiento dado al presente proyecto identificado con el código I-1288-11-02-F.

A mi tutor, profesor Andrés Arcia, quien dedico horas invaluables de tutoría para lograr un buen proyecto de grado.

A los profesores del jurado, Gilberto Díaz y Laudin Molina, quienes se tomaron la molestia de revisar y corregir este proyecto para garantizar un proyecto de calidad.

Al personal de Fundacite, Alberto Yañez, Gabriel Oballos y Histerlee Ramírez.

A mi esposo, Joger Quintero, quien siempre me ha apoyado, especialmente durante el desarrollo de mi proyecto de grado.

Un especial agradecimiento a mi familia y amigos por apoyarme siempre.

Capítulo 1

Introducción

El Presente capítulo contiene la descripción de la fundación donde se realizó el estudio; fundación para el desarrollo de la ciencia y la tecnología del Estado Mérida (Fundacite Mérida). Se definirán los antecedentes hallados sobre este proyecto, así como también, el planteamiento del problema que dio pie a su realización, la justificación y los objetivos que encaminan su desarrollo, el alcance del proyecto, la metodología usada para su desarrollo y finalmente, una descripción de la estructura del presente documento.

1.1 Definición de la institución

La fundación para el desarrollo de la ciencia y la tecnología (Fundacite Mérida) se creó bajo el decreto presidencial N° 373 publicado en gaceta oficial el 28 de agosto del año 1989 y fue legalmente registrada el 13 de agosto de 1990.

Fundacite es una institución adscrita al ministerio del poder popular para la ciencia y tecnología e industrias intermedias (MCTI) de la República Bolivariana de Venezuela, de carácter público, sin fines de lucro, cuya misión está orientada a ser el ente rector y gestor de la política científico - tecnológica del Estado Mérida.

La Fundación para el desarrollo de la ciencia y la tecnología del Estado Mérida, desde el año 1997, a venido prestando el servicio de Internet a través de una de las redes inalámbricas, en su tipo, más grandes del país; la red teleinformática de ciencia, tecnología e innovación del Estado Mérida (RETICyTIEM), con repetidores distribuidos en diferentes municipios del Estado, señalados en la Figura 1.1, logrando

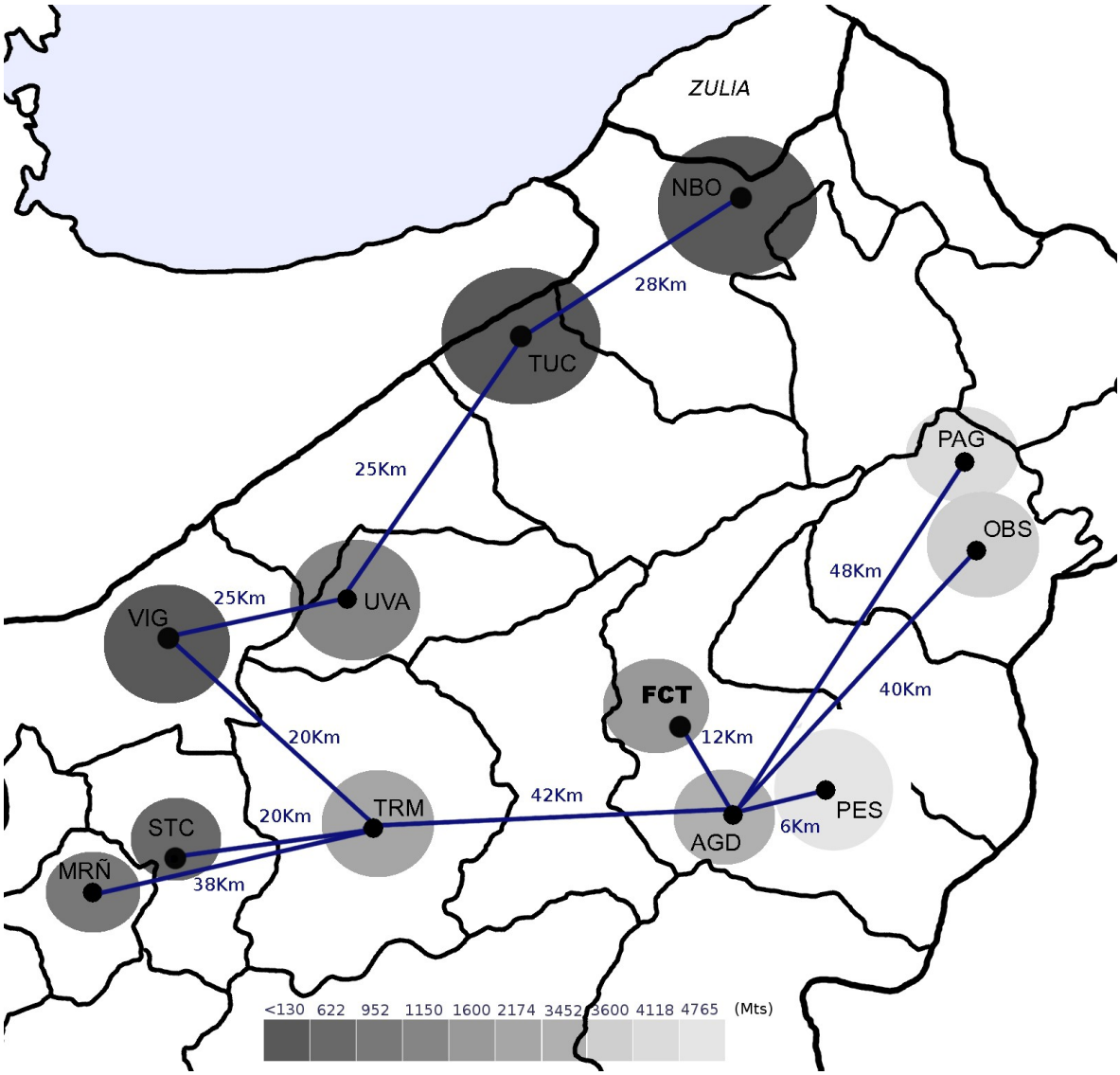

Figura 1.1: Mapa del Estado Mérida y la red de Fundacite Mérida
Fuente: Propia

prestar servicio de acceso a Internet a más de 110 instituciones públicas, con lo cual se pueden sumar alrededor de 1500 usuarios beneficiados.

El objetivo de la red de Fundacite Mérida es ser una herramienta productiva que contribuya al desarrollo político, económico, social, cultural y educativo del Estado Mérida. Para lograrlo, Fundacite presta el servicio a varias instituciones públicas como alcaldías, centros de diagnóstico integral (CDI), liceos, escuelas, instituto autónomo de servicios de bibliotecas e información del Estado Mérida (IBIME), policía, guardia nacional, bomberos, hospitales, comunidades organizadas, así como también, a comunidades que no cuentan con ninguno de los sistemas actuales de conexión.

1.1.1 Ubicación

Fundacite Mérida, como se puede apreciar en la Figura 1.2, se encuentra ubicada en la avenida Alberto Carnevalli, vía La Hechicera, edificio Fundacite de la cuidad de Mérida. Estado Mérida, Venezuela.

1.1.2 Sus instalaciones

Fundacite Mérida cuenta con 2 edificios; A y B. Presidencia y otras áreas administrativas se ubican en el edificio A. La Fábrica del Software Libre, la Academia de Software Libre, la administración de la red y otras áreas técnicas se encuentran en el edificio B.

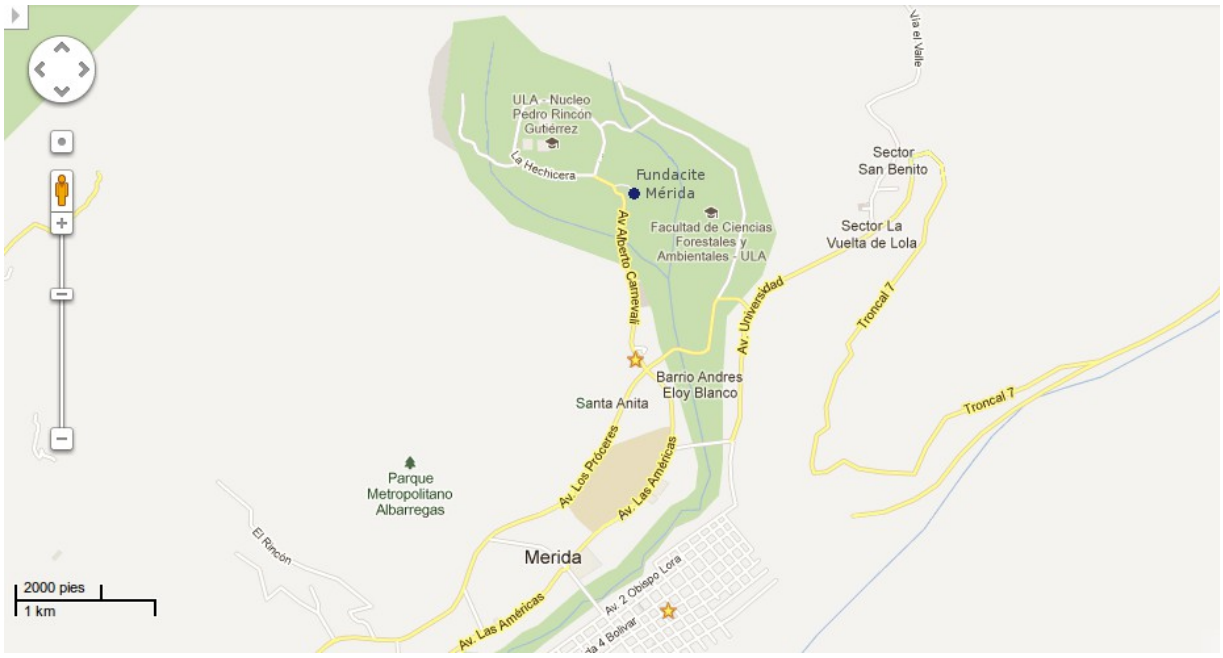

Figura 1.2: Ubicación de Fundacite Mérida
Fuente: http://www.googlemAP.com

1.1.3 Organización

Fundacite Mérida es una Unidad Territorial del MCTI que apoya el desarrollo del Proyecto Nacional Simón Bolívar; plan de desarrollo económico y social de la nación que busca la creación de una nueva nación, con bases en un modelo socialista he igualdad de condiciones, la satisfacción de necesidades sociales y la creación de modelos que le permitan a las sociedades la adquisición de conocimiento, capacitación y desarrollo endógeno.

Misión:

Promover y orientar el desarrollo del sistema científico y tecnológico del Estado Mérida, en función de dar soporte al desarrollo social y económico de esta Región.

Visión:

Ser el ente rector en ciencia, tecnología e innovación en el Estado Mérida.

Objetivos:

- Consolidar a Fundacite Mérida como el ente coordinador para vincular los sectores de ciencia y tecnología del Estado Mérida.
- Fomentar y estimular una cultura en ciencia y tecnología.
- Identificar las necesidades de los distintos sectores de la región en ciencia y tecnología.

Organigrama

La institución gestiona sus actividades a través de diversas unidades de forma centralizada y poco compleja, pues la palabra final, en la mayoría de los casos, la tiene el presidente de la fundación o la junta directiva que es la máxima instancia de autoridad.

En la Figura 1.3 se muestra las forma organizativa de la institución y a continuación se mencionan los departamentos más importantes que forman a Fundacite:

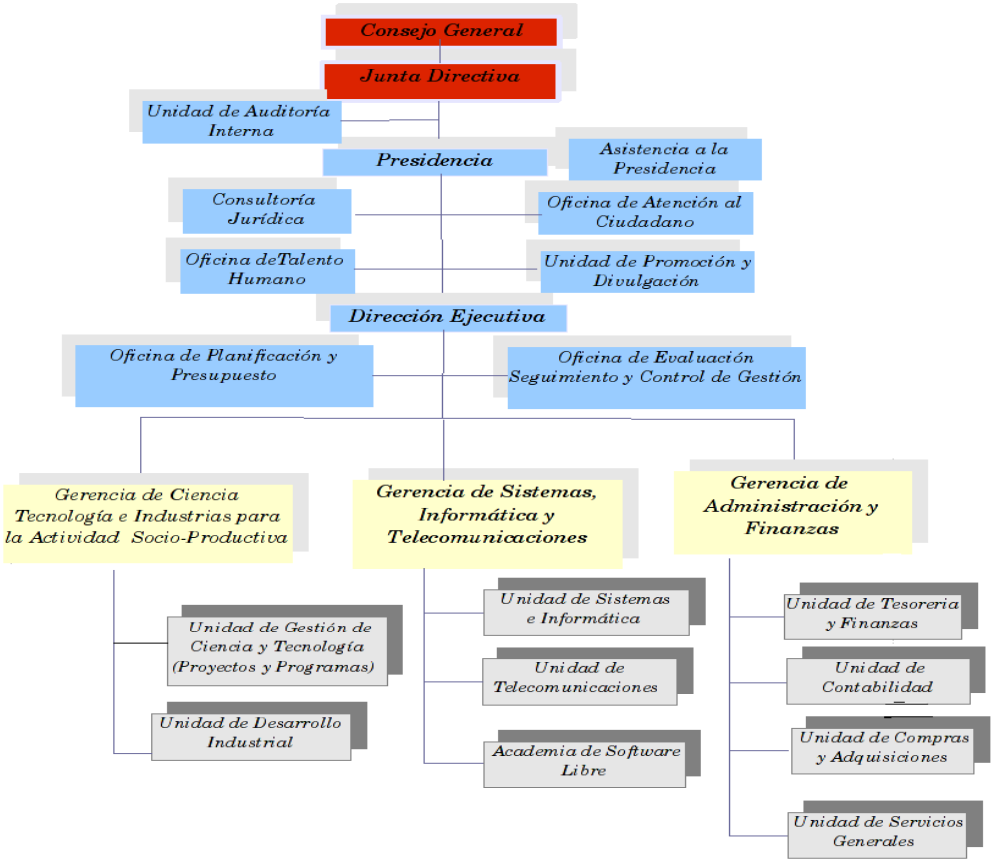

Figura 1.3: Organigrama de Fundacite Mérida.
Fuente: http://Fundacite-merida.gob.ve/

- En el *nivel ejecutivo* es donde se establecen las políticas de funcionamiento para garantizar que la fundación cumpla con sus objetivos. Este nivel se conforma por: Junta directiva, unidad de auditoría interna, presidencia, asistencia a la presidencia, consultoría jurídica, oficina de atención al ciudadano, oficina de talento humano, unidad de promoción y divulgación, dirección ejecutiva, oficina de planificación y presupuesto y la oficina de evaluación, seguimiento y control de gestión.

- A *nivel de gerencia* se presta apoyo a todo aquello que contribuya al desarrollo de los proyectos planteados en el nivel ejecutivo. El nivel está conformado por: la gerencia de ciencia, tecnología e industrias para la actividad socio-productiva, la gerencia de sistemas, informática y telecomunicaciones y la gerencia de administración y finanzas. A su vez, cada una de estas gerencias cuentan con el apoyo de diferentes unidades, tal como lo muestra la Figura 1.3.

1.1.4 Servicios

La fundación busca apoyar el desarrollo social en áreas como la científica, la tecnológica, la innovación y el área de las comunicaciones e información, donde los protagonistas son aquellas personas que tienen una necesidad de conocimiento o una idea innovadora y que no cuentan con el apoyo necesario para desarrollar eficientemente su potencial creativo.

Entre los proyectos encaminados a impulsar y fortalecer el desarrollo de las comunidades se tienen los siguientes:

- En el área de la ciencia y la tecnología se ubican los siguientes proyectos:
  - Redes socialistas de innovación productiva.
  - Casas de los saberes.
  - Programa de reconocimiento a la excelencia y esfuerzo de la población escolar del Estado Mérida (FORTALENTO).
  - Programa de subvenciones.

- Programa de apoyo a la inventiva tecnológica popular.
- Premios regionales de ciencia y tecnología.

- Proyectos para el desarrollo de las comunicaciones e información:
  - Red teleinformática de ciencia, tecnología e innovación del Estado Mérida (Fundacite).
  - Academia de software libre (ASL).
  - Fábrica de software libre.

1.2 Antecedentes del proyecto

Quiroz Alberto (2011), Universidad Nacional Experimental de Táchira (UNET) realizó un informe de pasantías de final de carrera titulado: "*Actualización del esquema de enrutamiento y direccionamiento IP de la red inalámbrica de Fundacite Mérida en la zona Panamericana y Valle de Mocoties del Estado Mérida*", el cual tuvo como basamento la actualización del esquema de enrutamiento, aplicando enrutamiento estático en una red inalámbrica mediante el uso de tecnología *Mikrotik* basada en *RouterOS* y manejada con software libre bajo la distribución *Ubuntu*.

Nechaev Boris (2008), Helsinki Institute for Information Technology (HIIT) realizó un estudio del perfil de tráfico titulado "*From Traffic Measurements to Conclusions*" donde realizó capturas de trazas y usó herramientas libres para determinar la usabilidad de la red a través del análisis de datos.

Jiménez Gladys y Pazmiño Carlos (2009), Escuela Politécnica Nacional de Quito en Ecuador; realizaron su tesis de grado titulada "*Análisis, implementación y*

evaluación de un prototipo router dual IPv4/IPv6 con soporte de QoS e IPsec sobre linux, usando AHP para la selección del hardware e IEEE 830 para la selección del software" donde se estudió los algoritmos de enrutamiento estáticos y dinámicos, se analizó la capa de red y se realizó un estudio para la implementación de calidad de servicio (QoS) con el fin de darle prioridad al tráfico más relevante.

1.3 Definición del problema

La red de Fundacite Mérida cuenta con repetidores que brindan cobertura a 16 sectores en 13 municipios del Estado Mérida. La ubicación de estos repetidores y sus sectores de cobertura se puede ver en la Tabla 1.1.

La red está configurada usando equipos *Motorola Canopy Backhaul* (BH) 5700, *Motorola Canopy* AP 5700, *Mikrotik 411, Mikrotik 433* y *Mikrotik 433AH.* Algunos equipos caseros como *Linksys* y *Buffalo* también forman parte de la topología de la red junto con el sistema operativo *GNU/Linux* distribución *Debian Lenny* para los servidores.

La plataforma teleinformática de Fundacite es una solución compuesta por tecnología *Mikrotik* y *Canopy*, e implementada por Fundacite. Actualmente cuenta con enrutamiento estático en equipos *Mikrotik* a través de una red de área local virtual (VLAN, estándar 802.1q) en la mayor parte de la red, marcado de ruta en la zona Sur de la red que comprende las zonas de Mariño, El Vigía (de La Trampa hacia la Panamericana) y el Páramo.

Municipio	Sector
Alberto Adriani, El Vigía	Aeropuerto
Alberto Adriani, El Vigía	Buenos Aires
Andrés Bello, La Azulita	Páramo de la Uva
Antonio Pinto Salinas	Santa Cruz de Mora
Arzobispo Chacón	Canaguá
Caracciolo Parra Olmedo	Tucaní
Libertador	Aguada - Fundacite
Miranda	Timotes
Rangel	Apartaderos
Rangel	Misintá - Mucuchíes
Rangel	Llano el Hato (Observatorio)
Rivas Dávila, Bailadores	Páramo de Mariño
Santos Marquina	Tabay
Sucre, Lagunillas	La Trampa
Tovar	Tovar
Tulio Febres Cordero	Nueva Bolivia

Tabla 1.1: Sectores de cobertura de la red de Fundacite.

En el caso de La Aguada, donde se concentra el mayor tráfico de la red, el flujo de tráfico se hace a nivel de capa 2 en los enlaces punto a punto y a nivel de capa 3 (con VLAN) en enlaces multipunto, lo que trae como consecuencia que el ancho de banda con que se cuenta para los enlaces inalámbricos no sea aprovechado de la mejor manera debido a tormentas de *broadcast*.

Actualmente se aplica en toda la red el criterio de calidad de servicio (QoS) a nivel de usuario final para controlar el ancho de banda de subida y de bajada.

Tanto el enrutamiento como la QoS que se ha aplicado a la red se ha realizado sin previas pruebas de medición de la capacidad de los enlaces inalámbricos que permitan determinar si, tomando en cuenta los servicios prestados, esta configuración es la adecuada para la red.

1.4 Justificación

Para lograr un mejor funcionamiento de la red y aprovechar la plataforma teleinformática instalada por Fundacite, es necesario realizar mediciones de tráfico para conocer su performance y a futuro, realizar pruebas que permitan proponer un esquema de enrutamiento y QoS adecuado.

Al mejorar el servicio de Internet, se estarían beneficiando instituciones gubernamentales, educativas y las localidades alejadas de la ciudad que, por su difícil acceso, no cuentan con el servicio de telecomunicaciones que prestan los proveedores comerciales.

La optimización en la transmisión de paquetes es de vital importancia para aprovechar de manera mas eficiente los recursos y agilizar tareas que deben ser ejecutadas a tiempo.

El intercambio de información entre instituciones y el continuo avance en el campo de la tecnología a nivel global obligan a que los servicios de datos deban tener mayor fiabilidad en cuanto a tiempo y disponibilidad del servicio.

Debido al crecimiento de la red y a la mayor demanda del servicio por parte de los usuarios, se hace necesario presentar una optimización en el enrutamiento de los

datos y en la configuración de QoS que permita mejorar el control del ancho de banda, disminuir la tormenta de *broadcast* presente en los segmentos de la red inalámbrica de la Aguada y garantizar el continuo crecimiento de la red de Fundacite.

1.5 Objetivos

1.5.1 Objetivo general

Caracterizar y determinar los mecanismos a aplicar en la red de Fundacite para el mejoramiento de la capacidad.

1.5.2 Objetivos específicos

- Realizar estudios para conocer la configuración topológica de la red de Fundacite Mérida.
- Hacer un levantamiento detallado de la topología de la red.
- Conocer los distintos protocolos que intervienen en la capa enlace.
- Analizar la configuración del direccionamiento IP.
- Realizar estudios sobre los protocolos de enrutamiento estáticos y dinámicos.
- Determinar el perfil del tráfico de la red.
- Realizar pruebas basadas en redes de área local virtual (VLAN) para determinar el mejor rendimiento de los servicios de la red.
- Realizar pruebas que permitan determinar las políticas de calidad de servicio (QoS).

- Determinar la mejor tecnología que se debe aplicar a la red de Fundacite Mérida para mejorar el ancho de banda disponible para las aplicaciones.

1.6 Metodología

El desarrollo del proyecto se lleva a cabo bajo la metodología conocida como el P*roceso de diseño de ingeniería* [7]. Esta metodología permite regresar a cualquier etapa previa y retomar el proceso de diseño en caso de ser necesario, tal como lo podemos observar en la Figura 1.4, teniendo en cuenta que este retorno a procesos previos, puede incrementar los costos de tiempo y recursos.

El proceso de diseño de ingeniería contiene seis etapas las cuales serán explicadas a continuación:

- *Formulación del problema*: Se debe describir el problema en forma general, prestando especial atención a información de problemas similares ya resueltos y a información que se pueda prestar a confusión y así lograr tener una idea clara del problema. Se debe hacer un reconocimiento general del problema a resolver sin entrar en detalle de los procesos presentes de lo que se desea solucionar.
- *Análisis del problema*: En base a la información obtenida en el paso anterior, se debe detallar el problema a resolver. Se hace necesario obtener las características cuantitativas y cualitativas presentes en el problema, sus variables y restricciones. Durante la etapa de análisis se puede obtener un conjunto de soluciones incluidas en las restricciones del problema, donde la

solución final viene dada por la evaluación de cada una de las posibles soluciones.

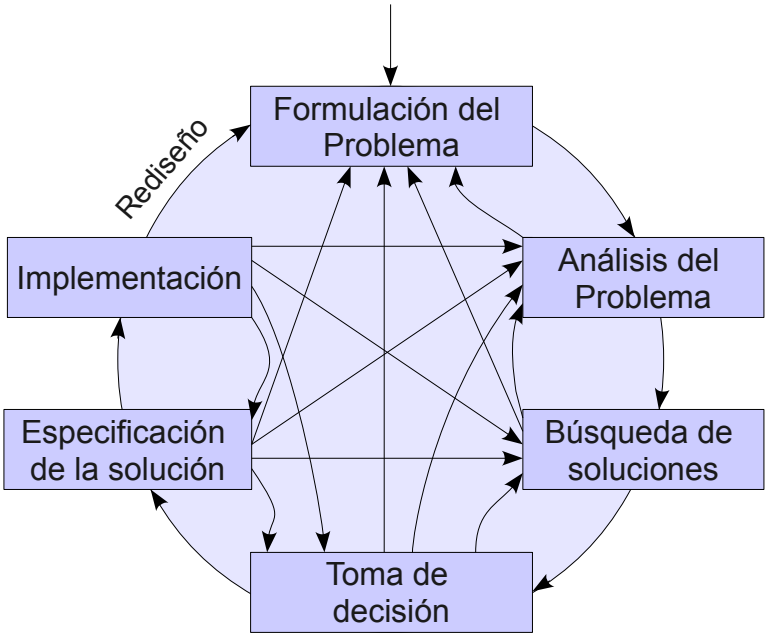

Figura 1.4: Proceso de diseño de ingeniería
(Fuente: Randall, J. y Charles, T. (1979). Software Engineering)

- *Búsqueda de soluciones*: Durante la etapa de búsqueda se debe maximizar el conjunto de posibles soluciones de las cuales, una de estas debería ser la solución final aplicada al problema. Al realizar el análisis del problema pueden surgir posibles soluciones las cuales deben ser recolectadas y guardadas durante la etapa de búsqueda.
- *Toma de decisión*: En esta etapa se debe definir el criterio de selección, el valor que tendrán sus elementos y establecer una medida de evaluación con la cual comparar cada una de las soluciones propuestas hasta obtener, de una manera objetiva, la mejor solución posible.

- *Especificación de la solución*: Se debe especificar la solución con detalle para que pueda ser revisado, analizado y verificado por las personas que llevarán a cabo la implementación de dicha solución teniendo en cuenta que estas personas podrían no ser las mismas que trabajaron en las etapas previas.
- *Implementación*: En esta última etapa se debe implementar y entregar la solución especificada durante la etapa anterior. Dependiendo del producto desarrollado, puede ser necesario que éste se evalúe, modifique y/o que se le haga mantenimiento en su ambiente operacional.

1.7 Alcance

Para este proyecto, se llevará a cabo el estudio de la configuración de la red y se realiza un análisis de tráfico para determinar un esquema de enrutamiento que permita optimizar la transmisión de paquetes y la disminución de *broadcast* que actualmente afectan el rendimiento de la red.

También se realizará un estudio para determinar una configuración adecuada de QoS en toda la red de Fundacite ,que permita delimitar el ancho de banda e implementar VLAN en los enlaces que lo requieran.

Una vez finalizado el proyecto, Fundacite contará con un informe detallado sobre el perfil de tráfico y ancho de banda de la red junto con una propuesta para optimizar la transmisión de paquetes y ofrecer un nivel de QoS adecuado.

1.8 Estructuración del documento

Capítulo 1, Introducción. Para el capítulo introductorio se realiza una descripción de la Fundación donde se realiza el proyecto de grado, fundación para el desarrollo de ciencia y tecnología (Fundacite). Luego se mencionan los antecedentes que son la base para la realización del proyecto, así como también, el planteamiento del problema, la justificación, los objetivos, el alcance del proyecto y la metodología aplicada para su desarrollo.

Capítulo 2, Marco Teórico. Contiene los fundamentos teóricos necesarios para la comprensión del proyecto. Se describe de forma puntual los conceptos básicos de las redes inalámbricas, enrutamiento, QoS y las herramientas libres usadas durante el desarrollo de este proyecto.

Capítulo 3, Topologías y políticas de QoS aplicadas en la red de Fundacite. Se describe la topología lógica y física de la red, la forma como están dispuestos los equipos y la configuración que tiene cada uno de estos. También se describe las políticas de QoS aplicadas en la red de Fundacite al momento de realizar el estudio del perfil de tráfico.

Capítulo 4, Medición y análisis de resultados. En este capítulo se describe el procedimiento realizado para la captura de los datos y luego se analiza los resultados obtenidos. Para el análisis de los datos, se tienen gráficas que muestran las principales características de la red de Fundacite.

Capítulo 5, Conclusiones y recomendaciones. Teniendo el perfil de tráfico de la red y las características de QoS, se plantea en este capítulo, las conclusiones a las

que se ha llegado y las recomendaciones realizadas para mejorar el ancho de banda de la red.

Capítulo 2

Marco Teórico

Los conceptos tratados a continuación proporcionan las nociones básicas sobre redes inalámbricas, topología de una red, direccionamiento IP, protocolos, algoritmos de enrutamiento, calidad de servicio y una breve descripción de las herramientas usadas para realizar este proyecto.

2.1 Modelo TCP/IP

El modelo protocolo de control de transmisión/protocolo de Internet (TCP/IP) divide el funcionamiento de la red en 4 capas [1]. La información debe pasar por cada una de estas capas, en forma descendente desde el *host* origen y ascendente hacia el destino. Cada capa que recibe los datos, los procesa y le agrega o elimina el encabezado para que puedan ser comprendidos por la siguiente capa.

En la Figura 2.1 se muestran las 4 capas y sus principales protocolos

Descripción de las capas:

- *Capa aplicación*: Su función es proporcionar servicios para las aplicaciones de los usuarios. Mantiene comunicación con la capa transporte para entregarle la información en un formato entendible.

- *Capa transporte*: Encargada de asegurar que el segmento sea enviado entre los *host* origen y destino sin importar el tipo de red.
- C*apa de Internet*: Capa responsable de convertir los segmentos en datagramas y enrutarlos desde el origen hasta el destino según su dirección IP.
- *Capa de acceso de red*: Gestiona el acceso al medio físico y transmite datos binarios (bits) a través de la fibra óptica, atmósfera, cable coaxial u otro.

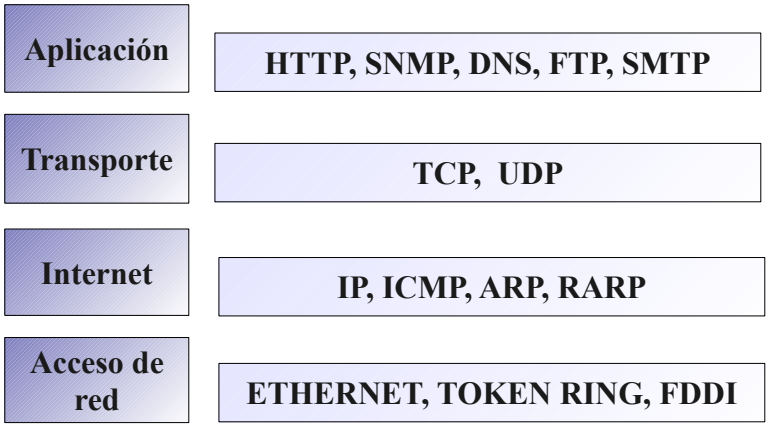

Figura 2.1: Modelo de referencia TCP/IP

2.2 Protocolos de capa Internet del modelo TCP/IP

La capa Internet cuenta con protocolos para asegurar el correcto enrutamiento de los datos y evitar la congestión en los nodos intermedios.

Los protocolos que pertenecen a la capa Internet son descritos a continuación:

2.2.1 Protocolo de Internet (IP)

Protocolo no orientado a conexión encargado seleccionar la mejor ruta para que los datos lleguen a su destino. Maneja un control de comprobación (*Checksums*) que le proporciona seguridad a las cabeceras transmitidas mas no a los datos.

2.2.2 Protocolo de mensajes de control de Internet (ICMP)

Protocolo encargado de diagnosticar y enviar los mensajes de error de Internet. Entre los controles realizados por este protocolo está el de controlar el tiempo de vida de un paquete, el control de si el paquete alcanzó o no su destino, y otros.

2.2.3 Protocolo de resolución de direcciones (ARP)

Este protocolo se encarga de traducir una dirección IP a dirección control de acceso al medio (MAC), es decir, descubrir a qué equipo de la red pertenece una determinada dirección lógica y obtener su dirección física.

Este protocolo entra en funcionamiento cuando un equipo de la red necesita comunicarse con otro y la dirección física no se encuentra registrada en su tabla ARP. En este caso, el protocolo ARP envía una solicitud a todos los equipos de la red y cada uno de estos equipos compara la dirección lógica enviada en el paquete ARP con su propia dirección lógica. Sólo el equipo que encuentra coincidencia con esta dirección, responde con su dirección física. Este nuevo par de direcciones, lógica y física, es almacenada en la tabla ARP para futuras conexiones.

2.2.4 Protocolo de resolución de dirección inversa (RARP)

Realiza el trabajo inverso al realizado por el ARP, es decir, a partir de una dirección MAC, determina la dirección IP del equipo de red.

2.3 Red inalámbrica

La forma de transmitir información entre usuarios ubicados en sitios geográficamente distantes, es a través de redes de comunicación las cuales pueden ser inalámbricas o cableadas. Nuestro interés se centra en las redes inalámbricas. Este tipo de red trae consigo importantes beneficios como son la eliminación de los cables, la facilidad a la hora de instalar equipos y la movilidad proporcionada a los usuarios y sus equipos. Entre sus principales desventajas tenemos una menor velocidad de transmisión y mayor complejidad a la hora de ofrecer seguridad al usuario.

Las redes inalámbricas pueden ser clasificadas según su cobertura en:

- Red inalámbrica de área personal (WPAN)
- Red inalámbrica de área local (WLAN)
- Red inalámbrica de área metropolitana (WMAN) y
- Red inalámbrica de área amplia (WWAN).

2.3.1 Topología de una red inalámbrica

La topología de una red puede ser física que sería la distribución de los dispositivos de la red, y topología lógica que configura la forma de transmisión de datos entre los nodos.

En cuanto a la topología física, ésta se puede clasificar de la siguiente forma:

- *Estrella*: Contiene un nodo central y dispositivos conectados a éste.
- *Bus*: Todos los nodos están conectados a través del mismo enlace.
- *Anillo*: Cada nodo está conectado solamente con un nodo adyacente.
- *Anillo doble*: Formado por dos anillos concéntricos y cada nodo está conectado a ambos anillos.
- *Árbol*: Contiene un nodo enlace al cual están conectados los primeros nodos y a partir de éstos, se ramifican los nodos restantes.
- *Malla*: Todos los nodos se comunican entre sí.
- *Malla parcial*: Parte de la red se comunican unos nodos con otros pero no todos los nodos de la red.

2.4 Estándar 802.11

El protocolo 802.11 es un estándar internacional que corresponde a las reglas que rigen el funcionamiento de la red inalámbrica y define las especificaciones técnicas en la capa Internet.

Bajo este protocolo se definen dos forma de operar en la red. La primera es en forma de *infraestructura* donde se requiere un punto de acceso (AP) para que los

usuarios puedan conectarse. Los AP pueden verse como dispensadores de señal inalámbrica de Internet. La segunda forma es la *ad-hoc* que no requiere AP para la comunicación entre los nodos y el acceso a Internet.

Los protocolos de comunicación inalámbrica más usados en la actualidad son 802.11a, 802.11b y el 802.11g también llamados estándares físicos 802.11.

2.4.1 802.11a

Ofrece un mayor desempeño para aplicaciones que requieren más ancho de banda. Basado en la tecnología de multiplexación por división de frecuencias ortogonales (OFDM). Por trabajar en la frecuencia de 5 Ghz tiene menos interferencia pero su alcance es menor, por lo que redes grandes requiere mayor cantidad de AP. Su velocidad máxima de transferencia es de 54 Mbps con 8 canales de radio no solapados. El estándar físico 802.11a no es compatible con el 802.11b.

2.4.2 802.11b

Su frecuencia de operación es la 2.4 Ghz con una velocidad máxima de transferencia de 11 Mbps la cual se reduce si detecta errores. Su rango de operación puede estar entre los 500 y 100 metros dependiendo de las condiciones del entorno.

2.4.3 802.11g

Entró en funcionamiento en el año 2003 bajo la frecuencia de operación de 2.4 Ghz con una velocidad máxima de 54 Mbps y codificación OFDM. La banda 2.4 Ghz es la más usada y por lo tanto, se corre el riesgo de tener mayor interferencia. El estándar físico 802.11b resulta compatible con el estándar 802.11g.

2.5 Control de acceso al medio

La capa de enlace de datos del modelo de interconexión de sistemas abiertos (OSI) está dividida en dos subcapas; la capa de control de enlace lógico (LLC) y la capa de control de acceso al medio (MAC).

La capa MAC funciona de forma diferente en redes cableadas y redes inalámbricas ya que no pueden detectar una colisión hasta tanto haya finalizado la transferencia generando así, mayor desperdicio de ancho de banda.

El algoritmo encargado de prevenir la colisión se denomina “acceso múltiple sensible a la portadora con prevención de colisiones” (CSMA/CA). Este algoritmo puede trabajar en conjunto con las técnicas de solicitud y aceptación de permisos para transmitir, listo para enviar/listo para recibir (RTS/CTS) y la confirmación de recepción del paquete a través de la trama de reconocimiento (ACK).

Entre cada trama enviada, bien sea de control, de datos o de gestión, se manejan unos espacios entre tramas (IFS) para evitar la concatenación de los datos y para dar prioridad a tramas de control.

Los tiempos entre tramas varían de tamaño generando diferentes tipos de IFS: espacio corto entre tramas (SIFS), IFS distribuido (DIFS) y punto de coordinación IFS (PIFS).

Se debe manejar la contienda para la transferencia de una trama cuando se tienen varias estaciones compitiendo por el medio de transmisión. La contienda es la competencia por el medio de forma que la posibilidad de colisión sea mínima y si ocurre, sea con una trama pequeña para no desperdiciar mucho ancho de banda.

La estación que desea transmitir debe escanear el medio de transmisión para ver si éste está libre o si se encuentra transmitiendo. Aquí pueden ocurrir dos cosas: que el canal este libre o que esté ocupado. Si está ocupado, la estación debe esperar un tiempo para poder transmitir (esto se explicará mas adelante).

Si el canal está libre, la estación que desea transmitir debe esperar un tiempo DIFS y luego volver a escanear el medio y si continua libre, puede iniciar la transferencia de la trama.

Cuando una estación que desea transmitir nota que el canal está ocupado, bien sea porque detectó ocupado el medio al realizar la primera evaluación o porque después de transcurrido el tiempo DIFS el canal resultó estar ocupado, la estación debe esperar un tiempo indicado en la trama que se está transmitiendo y luego otro tiempo aleatorio llamado *backoff* antes de volver a escanear el canal.

El modo de funcionamiento de RTS/CTS, usado para solucionar los problemas de estación oculta y estación expuesta, es el siguiente:

Una estación antes de transmitir envía una trama RTS la cual es escuchada por todas las estaciones que se encuentran en su *hostport*, incluyendo por supuesto a la estación receptora la cual responde con una trama CTS que es escuchada por las estaciones que se encuentran dentro del área *hostport* del receptor evitando así el problema de la estación oculta que no puede ser vista por el emisor. El emisor al recibir la trama CTS y pasado el tiempo SIFS, inicia la transferencia. Al finalizar con éxito la transferencia, el receptor le notifica al emisor con una trama ACK que todo ha salido bien.

2.6 Direccionamiento IP

El direccionamiento IP es la forma como se identifica el destinatario del paquete que se va a enviar a través de la red. Para identificar este destinatario se usa una dirección IP con una longitud de 32 bits en IPv4 mientras que para IPv6, se usa una dirección IP de 128 bits. La dirección IPv4 está formada por un identificador de red (netID) y un identificador del *host* (host-ID).

Las direcciones IP están divididas en clases para facilitar la búsqueda de equipos en la red:

- **Clase A:** Comprende el rango de direcciones desde 1.0.0.0 hasta 126.0.0.0. Tiene reservado 7 bits para el netID y 24 bits para el host-ID, como se muestra en la Figura 2.2. Se puede formar 128 redes y alrededor de 16 millones de *host* por red.
- **Clase B:** Su rango de direcciones va desde la dirección 128.0.0.0 hasta la 191.255.0.0. Distribuye 2 bits para la red, 14 bits para el netID y 16 bits para el host-ID lo que permite crear una cantidad mayor de redes, más de 16000 y más de 65 *host* por red.
- **Clase C:** Las redes disponibles para la clase C van desde la dirección IP 192.0.0.0 hasta la 223.255.255.0 dejando los 3 primeros bits para la red, 21 bits para el netID y los 8 bits restantes para el host-ID. Esta distribución de bits permite la creación de más de 2 millones de redes con 254 equipos cada red.

- **Clase D:** Reservada para servicios de multidifusión donde una estación envía simultáneamente información a un grupo de estaciones.
- **Clase E:** Destinada para hacer pruebas.

Las direcciones de red que inician en 127 son usadas para indicar el *host* local.

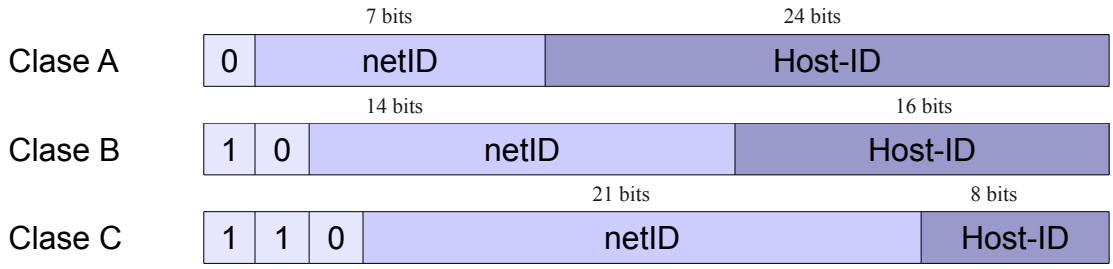

Figura 2.2: Clases A, B y C de direcciones IP

2.7 Enrutamiento

El enrutamiento de los datos a través de la red se realiza en la capa Internet del modelo TCP/IP y consiste en hacer llegar los datos desde un origen hasta un destino, haciendo pasar el paquete por diferentes elementos de red de ser necesario.

Las decisiones de enrutamiento son tomadas por los routers a través de algoritmos y tablas de enrutamiento donde se almacena información sobre la topología de la red.

Cuando un dispositivo de enrutamiento recibe el paquete, éste busca en su tabla de enrutamiento para determinar si dicho paquete es para él o si debe redireccionarlo al siguiente dispositivo. Si la dirección no existe en su tabla, la puede agregar de forma dinámica si es su configuración lo permite, de lo contrario, la tabla sería estática y no cambiaría al cambiar al topología de la red.

Se han diseñado diferentes formas de enrutamiento: el enrutamiento estático y el enrutamiento dinámico.

2.7.1 Enrutamiento estático

Este tipo de enrutamiento es configurado manualmente en la tabla de enrutamiento por el administrador de la red y permanece así hasta que el administrador vuelva a realizar cambios en la tabla, es decir, este tipo de enrutamiento no tiene la capacidad de adaptarse por sí mismo a los cambios sufridos en la topología de la red; por lo cual resulta muy útil para redes pequeñas que tengan pocos enrutadores ya que un enrutamiento dinámico generaría consumo de recursos y de ancho de banda.

2.7.2 Enrutamiento dinámico

El enrutamiento dinámico funciona muy bien en redes grandes con diferentes caminos para llegar a un mismo destino. La ruta es construida dinámicamente por la información compartida entre los routers vecinos, lo que le da la capacidad de adaptarse a los cambios en la topología de la red y de realizar el enrutamiento de los datos de forma mucho más rápida que si se realizara de forma manual por el administrador de la red.

2.8 Algoritmos y protocolos de enrutamiento

La parte del software perteneciente a la capa Internet que se encarga de realizar el enrutamiento de los datos son los algoritmos de enrutamiento y estos pueden ser

de tipo estáticos (no adaptativos) o dinámicos (adaptativos).

Los algoritmos de enrutamiento dinámico más comunes son:

- *Enrutamiento por vector de distancia* el cual determina la dirección y distancia hacia cualquier enlace de red a través de información enviada por sus routers vecinos.
- Por *estado de enlace* donde cada dispositivo calcula la ruta más corta a los otros routers.

Los protocolos son las reglas que existen en Internet para garantizar un óptimo funcionamiento de la red. Las organizaciones que estandarizan los protocolos de red son el instituto de ingenieros eléctricos y electrónicos (IEEE) y el grupo de ingeniería de Internet (IETF).

Algunos protocolos de enrutamiento dinámico son:

- Protocolo de información de enrutamiento (RIP): Es un protocolo de enrutamiento *gateway* interior basado en el algoritmo de enrutamiento por *vector distancia*.
- Primero la ruta más corta (OSPF): Es un protocolo de enrutamiento *gateway* interior por *estado de enlace*.
- Protocolo de enrutamiento de *gateway* interior (IGRP): Protocolo *gateway* interior por *vector distancia* propiedad de *CISCO*.
- Protocolo de enrutamiento de *gateway* interior mejorado (EIGRP): Versión mejorada del protocolo IGRP que cuenta con las ventajas ofrecidas por los protocolos *vector distancia* y *estado de enlace*.

- Protocolo de *gateway* fronterizo (BGP): Protocolo de enrutamiento exterior por *vector distancia*.

2.9 Broadcast

Son datagramas enviadas en capa Internet a los equipos que se encuentran en la misma subred y que pertenecen a un mismo dominio de *broadcast*. Este tipo de tramas es usada cuando se desconoce la ubicación del destinatario en la red. El equipo que debe redirigir la trama busca en su tabla de direcciones MAC la ubicación del destinatario en su red y si no lo encuentra, envía un *broadcast* a todos los segmentos de red para preguntar a todos los *host* a quién le pertenece el paquete y el destinatario al identificar que el paquete es para él, responde con su dirección MAC.

2.9.1 Dominio de broadcast

Es el área de la red donde todos los equipos que pertenecen a la misma red, pueden recibir un mismo *broadcast* de forma simultanea.

2.10 Colisión

Ocurre cuando dos o más equipos compiten por acceder al mismo tiempo a un medio de transmisión compartido. Al ocurrir una colisión, se pierden los paquetes de ambos emisores y éstos deben intentar nuevamente la transmisión.

2.10.1 Dominio de colisión

Área lógica donde las tramas de diferentes emisores pueden colisionar por acceder al medio de transmisión al mismo tiempo. Estos dominios de colisión pueden ser divididos, a través de la segmentación, en áreas más pequeñas disminuyendo las colisiones y la perdida de paquetes.

2.11 Segmentación de redes

Una red grande se puede dividir en redes pequeñas llamadas segmentos de red. El objetivo principal de segmentar una red es para poder aislar el tráfico, dividir el dominio de colisión e incrementar el ancho de banda por segmento de red.

Se puede realizar segmentación de redes de forma física usando equipos como repetidores, switch, routers y de forma lógica con redes virtuales (VLAN).

2.11.1 Repetidores

Son equipos usados para extender el alcance de la red. La potencia de la señal pierde intensidad al extender la longitud del medio y se debe usar equipos como los repetidores para repotenciar la señal y lograr tener un medio de transmisión con mayor longitud.

Estos equipos trabajan a nivel de capa acceso de red por lo que no realizan enrutamiento de datos ni control de tráfico pero sí hacen segmentación de red obteniendo un mismo dominio de colisión para todos los segmentos pertenecientes a la red.

2.11.2 Switch

Permiten crear diferentes segmentos de red con un único dominio de *broadcast* y un dominio de colisión para cada segmento.

Los switches trabajan a nivel de capa acceso de red y pueden ser configurados en modo *bridge* (puente) para segmentar las redes o para unir segmentos de red, dejando paras sólo las tramas pertenecientes a cada segmento en base a la dirección física (MAC).

Se tienen 2 tipos de switches; los no administrables que son switches sencillos que no permiten configuración y los switches administrables aceptan configuración y son capaces de reconocer VLAN.

2.11.3 Router

Elemento de Internet que permite segmentar la red en subredes mas pequeñas y crear un dominio de *broadcast* para cada segmento de red. Por trabajar a nivel de capa Internet, pueden realizar enrutamiento de paquetes de forma más inteligente como por ejemplo, dirigir el tráfico por rutas más cortas.

Los routers, al igual que los switches, pueden ser configurados en modo *bridge* para segmentar las redes y transmitir las tramas en base a la dirección física.

2.11.4 VLAN

Con las redes virtuales se crea un cable lógico entre uno o varios emisores y receptores. Al crear una VLAN, entre un grupo reducido de *host*, se crea un dominio de *broadcast* menor, aprovechando el ancho de banda por segmento de red.

2.12 Calidad de servicio (QoS)

La QoS se aplica a través de tecnologías y protocolos para implementar reglas que permitan mejorar el servicio ofrecido a los usuarios. Entre los principales servicios de mayor consumo de recursos son las aplicaciones de voz y vídeo que requieren de reglas de QoS más robustas para poder garantizar la transmisión de la información en un tiempo optimo.

La QoS puede ser evaluada según las siguientes categorías: tiempo, volumen de tráfico, precisión, robusteza, confiabilidad, manejabilidad y seguridad.

Dentro de la categoría del volumen de tráfico, se tiene los parámetros de *throughput* y picos de volumen, los cuales pueden ser evaluados a través del estudio del perfil de tráfico de red.

Las reglas a aplicar para mejorar la QoS en una red, debe estar basada en estudios previos que permitan determinar el perfil de red y así diseñar reglas orientadas a mejorar los recursos de esa red en especial.

2.13 Herramientas

Las herramientas usadas para determinar el perfil de tráfico, se basan en las siguientes herramientas de software libre.

2.13.1 Tcpdump

Herramienta libre para la captura y monitoreo de tráfico de red. Entre las principales ventajas de esta herramienta está el uso de la librería *Libpcap* para la captura de paquetes los cuales pueden ser almacenados para estudios posteriores,

el consumo de pocos recursos por funcionar a nivel de línea de comandos, el funcionar perfectamente sobre el sistema operativo GNU/Linux y el permitir el uso de filtros para obtener información especifica según las necesidades de estudio.

La información obtenida con esta herramienta depende del protocolo capturado. Por ejemplo, para el protocolo TCP se puede obtener el tiempo en que fue capturado el paquete, las direcciones IP y puertos origen y destino, protocolo, tamaño de la ventana, número de secuencia del bytes, y más.

2.13.2 Tcpstat

Herramienta de línea de comandos diseñada para obtener estadísticas sobre la red a través de la monitorización de la red o a partir de archivo de entrada capturados con aplicaciones que usan la librería *Libpcap*, como por ejemplo, *Tcpdump*.

Entre las principales estadísticas obtenidas con *Tcpstat* tenemos: estadísticas del protocolo de transferencia de hipertexto (HTTP), promedio del tamaño de los paquetes en bytes, número total de bytes por segundo, total de paquetes de protocolo de control de transmisión (TCP), protocolo de datagramas de usuario (UDP), protocolo de mensajes de control de Internet (ICMP), protocolo de resolución de direcciones (ARP), entre otros.

2.13.3 CoralReef

CoralReef está formada por un conjunto de software diseñados para analizar tráfico de Internet. Cuenta con aplicaciones para el análisis de tráfico como *crl_flow*.

Crl_flow es una aplicación que permite obtener estadísticas del flujo de datos tomando en cuenta las IP origen, destino y los puertos origen y destino de los paquetes capturados.

2.13.4 Awk

Lenguaje de programación que permite procesar texto. Alguna de sus funciones es la de permitir la búsqueda de patrones y realizar una acción cada vez que encuentra coincidencia con un patrón o simplemente extraer información desde un archivo de texto.

Resulta muy útil a la hora de querer extraer, de un grupo de columnas, sólo aquellas columnas que resultan de interés para el estudio realizado.

Este lenguaje puede ser ejecutado desde la línea de comandos o a partir de un archivo si el código a ejecutar es grande. La salida puede ser enviada a otro archivo de texto plano.

2.13.5 Iperf

Aplicación que permite obtener datos estadísticos sobre los enlace de red para determinar su ancho de banda y calidad del enlace. *Iperf* funciona a nivel de línea de comandos y cuenta con una versión gráfica llamada *Jperf*.

Funciona en modo cliente/servidor, es decir, se necesita 2 maquinas en los extremos del enlace a medir; una como cliente y la otra como servidor.

Se pueden enviar paquetes de tipo TCP o UDP. Al enviar paquetes TCP se puede determinar el ancho de banda y con UDP, el jitter y la perdida de paquetes.

2.13.6 Perfsonar

Performance gocused service oriented network monitoring architecture. Herramienta para el monitoreo y medición del rendimiento de la red cuando intervienen varios dominios de red entre los extremos a evaluar.

Entre sus principales características se encuentra que permite almacenar las medidas realizadas.

2.13.7 Ping

Herramienta que funciona a nivel de línea de comandos. Es muy útil a la hora de evaluar la conexión entre 2 equipos de la misma red. Con esta herramienta se obtiene también la latencia o RTT al enviar paquetes de tipo ICMP hacia un destino.

2.13.8 R

Aplicación a nivel de línea de comandos que permite realizar cálculos matemáticos y estadísticos. A través de esta herramienta, se obtiene la media, mediana y cuartiles de datos con gran cantidad de volumen, datos que no pueden ser procesados por aplicaciones gráficas.

2.13.9 Gnuplot

Herramienta libre diseñada para realizar gráficos. Funciona a nivel de línea de comandos o con archivos que contengan todas las líneas a ejecutar. Su principal ventaja es la versatilidad para añadirle parámetros que permitan configurar la presentación de las gráficas.

Capítulo 3

Topologías y políticas de QoS aplicadas en la red de Fundacite

La Red teleinformática de ciencia, tecnología e innovación del Estado Mérida (Fundacite) es una red jerárquica que abarca gran parte del Estado Mérida y que funciona con tecnologías híbridas entre *Canopy* de *Motorola* y *Mikrotik*.

Para la realización de mediciones fue necesario conocer y hacer un levantamiento detallado de la topológica física y lógica de la red.

En la topología física se describe la forma como están distribuidos los equipos en los enlaces punto a punto y multipunto ubicados en diferentes Municipios de Estado.

La topología lógica describe la configuración de las redes y subredes de los enlaces punto a punto y multipunto de la red de Fundacite Mérida.

3.1 Topología física

En la Figura 3.1 se observan los 12 principales nodos repetidores de la red de Fundacite con enlaces punto a punto.

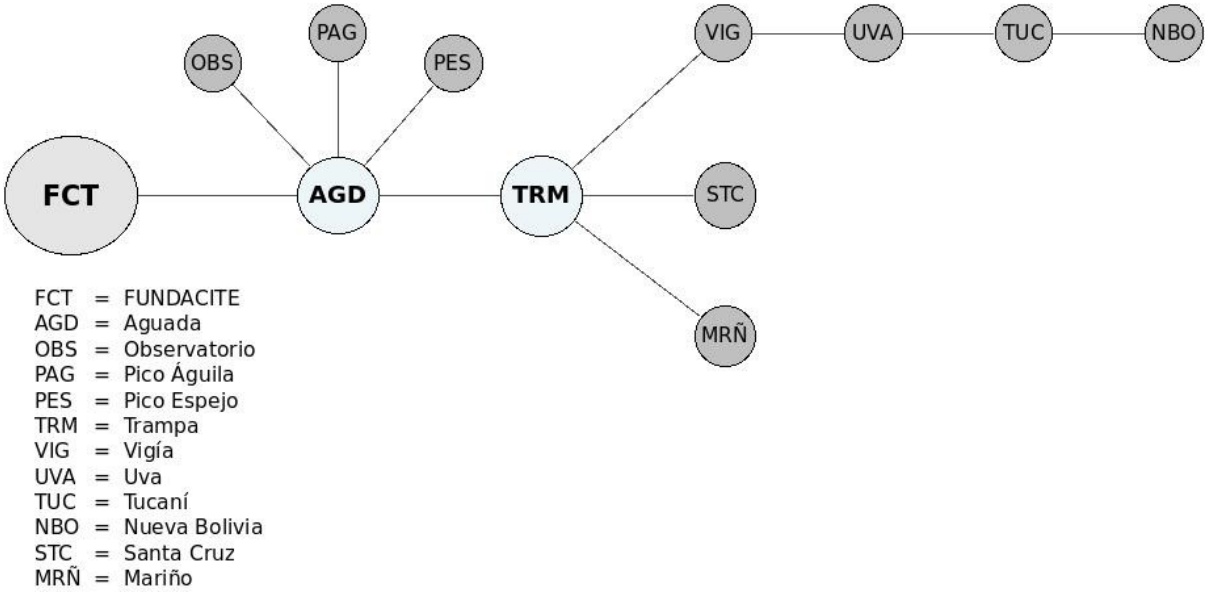

Figura 3.1: Diagrama físico de la red Fundacite

La red de Fundacite cuenta con dos *Frame Relay* E1, enlaces dedicados hasta Caracas, que salen a través del centro nacional de innovación tecnológica (CENIT) y dos conexiones ABA de la compañía anónima nacional teléfonos de Venezuela (CANTV). Cada una de estas conexiones tiene una capacidad de 2 Mbps para dar salida a Internet a través de los equipos ubicados en FCT.

En la Figura 3.2 se tiene un diagrama más detallado de la topología física de los 2 principales enlaces de Fundacite; enlaces FCT-AGD y AGD-TRM.

Se puede observar que FCT se tiene un switch, identificado en la Figura 3.2 como SW-DMZ, y que está en lo que llaman la zona desmilatarizada (DMZ) por estar protegida con *firewall* a la entrada y salida tanto para la red WLAN de FCT, como en la conexión que va hacia la Internet.

Los módulos de administración de clústeres, conocidos como “caja de sincronismo”, se encuentran en los diferentes nodos de la red, identificadas en la Figura 3.2 como CMM. Estas cajas cuentan con un switch incorporado de 8 puertos donde llegan los enlaces, una antena de sistema de posicionamiento global (GPS) y un sistema de alimentación a través de Ethernet (PoE) para los enlace punto a punto y multipunto.

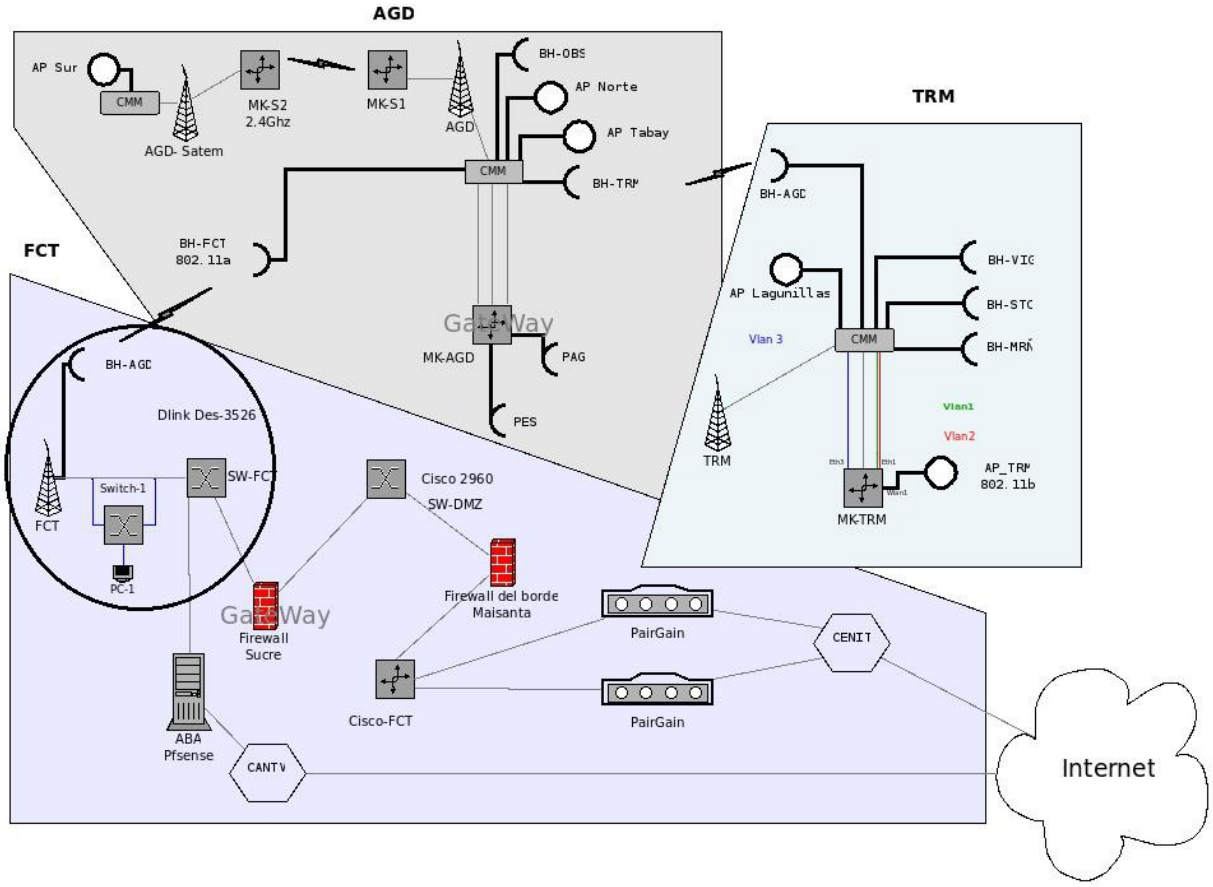

Figura 3.2: Enlaces FCT-AGD-TRM
Fuente: Propia

3.1.1 Enlaces unto a punto

El nodo ubicado en Fundacite, identificado como FCT, es el principal nodo del cual salen enlaces hacia AGD a través de un enlace punto a punto y desde la AGD, se tienen enlaces hacia otros nodos los cuales están representados en la Figura 3.1.

Estos enlaces se realizan con equipos *BH Canopy 5700* de *Motorola* y un plato reflector en cada uno de ellos, proporcionando mayor alcance de señal.

La capacidad de los enlaces es de 10 Mbps tanto de subida como de bajada. Algunos funcionan bajo el protocolo 802.11a y otros bajo el protocolo el protocolo 802.11b.

Nodos	Distancia (Km)
FCT – AGD	12
AGD – OBS	40
AGD – PAG	48
AGD – PES	6
AGD – APM	12
AGD – TRM	42
TRM – VIG	20
TRM – STC	20
TRM – MRÑ	38
VIG – UVA	25
UVA – TUC	25
TUC – NBO	28

Tabla 3.1: Distancias entre los principales nodos

Cada nodo se encuentra a diferentes distancias (kilómetros) uno del otro y cuentan con línea de vista entre ellos. Las distancias en kilómetros están tabuladas en la Tabla 3.1.

En los nodos, excepto NBO, se tienen equipos router *Mikrotik* 433 configurados con un enrutamiento sencillo y puerta de enlace en el salto siguiente.

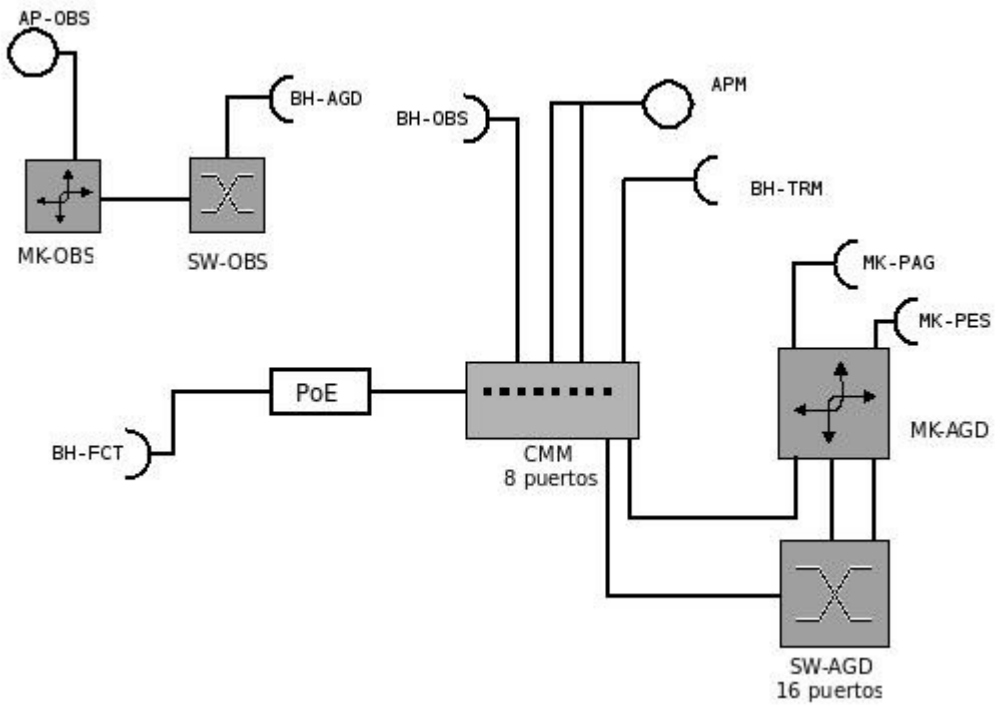

Figura 3.3: Nodo de la AGD con el enlace punto a punto hacia OBS
Fuente: Propia

Leyenda de la Figura 3.3:

- BH-FCT: Equipo BackHaul *Canopy* 5700 de *Motorola* para realizar el enlace punto a punto entre FCT y AGD.
- BH-OBS: Equipo BH-*Canopy* 5700 para realizar el enlace punto a punto entre OBS y AGD

- BH-TRM: Equipo BH-*Canopy* 5700 para realizar el enlace punto a punto entre TRM y AGD
- MK-PAG: Equipo *Mikrotik* 433 para realizar el enlace punto a punto entre PAG y AGD
- MK-PES: Equipo *Mikrotik* 433 para realizar el enlace punto a punto entre PES y AGD
- AP-OBS: Equipo AP *Mikrotik* para realizar el enlace multipunto hacia el OBS. Entre el OBS y Mucuchies se tiene un enlace punto a punto con un equipo BH de *Motorola*.
- APM: Equipos AP *Motorola* para realizar el enlace multipunto hacia las zonas de Tabay, Norte y Sur del Municipio Libertador.
- PoE: Fuente de poder de la caja de sincronismo.
- CMM: Caja de sincronismo con switch incorporado de 8 puertos de los cuales se están usando 7.
- SW-AGD: Switch no administrable de 16 puertos ubicado en AGD (funciona en capa 2)
- MK-AGD: Equipo routerBoard *Mikrotik* donde se administran las VLAN y se configura la puerta de enlace por defecto hacia el siguiente salto, es decir, hacia FCT.
- SW-OBS: Switch no administrable de 16 puertos ubicado en OBS (funciona en capa 2)

- MK-OBS: Equipo routerBoard *Mikrotik* donde se administran las VLAN y se configura la puerta de enlace por defecto hacia el siguiente salto, es decir, hacia AGD.

De la CMM de la Figura 3.3 salen enlaces punto a punto hacia el OBS y la TRM, tres enlaces multipunto hacia el área metropolitana y una conexión hacia el MK-AGD del cual salen dos enlaces punto a punto; uno hacia PAG y otro hacia PES. Cada uno de estos enlaces tiene a su vez enlaces secundarios para dar servicio a otras zonas.

Los enlaces punto a punto hacia el PAG y PES se realizan con equipos *Mikrotik* 433 los cuales funciona bajo los protocolos 802.11b y 802.11a respectivamente.

En la TRM hay un Kit *Mikrotik*, identificado en la Figura 3.2 como MK-TRM. Este equipo, al igual que el MK-AGD, está conectado al CMM de 8 puertos. En esta CMM se tienen enlaces punto a punto hacia el VIG, STC, MRÑ y la AGD, además de un enlace multipunto hacia Lagunillas.

El nodo del VIG cuenta con un enlace punto a punto hacia el nodo UVA, ubicado en La Azulita, y un enlace multipunto hacia Buenos Aires en el Vigía.

En la Figura 3.4 se tienen los nodos UVA, TUC y NBO, con enlaces punto a punto entre ellos, siendo el nodo NBO el último nodo de la red de Fundacite. El servicio a usuarios en este último nodo, se da con un router *Linksys* bajo el protocolo 802.5.

Los enlaces se han colocado con diferentes tipos de líneas para diferenciar hacia dónde va dirigido el tráfico que llega a cada enlace.

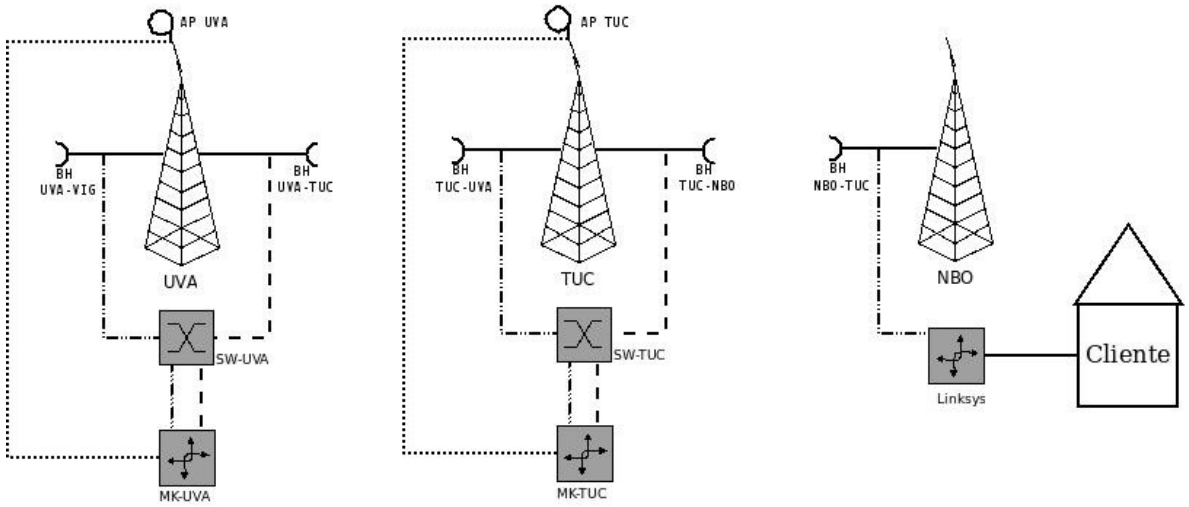

Figura 3.4: Topología física de UVA, TUC y NBO

Leyenda:

- Antena venteada: Identificada en la figura con los nombres de los nodos: UVA, TUC y NBO. Es la estructura metálica donde se montan las antenas para los enlaces punto a punto y multipunto.
- BH UVA-VIG: Equipo BH-*Canopy* 5700 para realizar el enlace punto a punto entre UVA y VIG
- BH UVA-TUC: Equipo BH-*Canopy* 5700 para realizar el enlace punto a punto entre UVA y TUC.
- BH TUC-NBO: Equipo BH-*Canopy* 5700 para realizar el enlace punto a punto entre TUC y NBO.
- AP UVA: Equipo AP *Mikrotik* para realizar el enlace multipunto hacia la UVA
- AP TUC: Equipo AP *Mikrotik* para realizar el enlace multipunto hacia TUC
- SW-UVA: Switch no administrable de 16 puertos ubicado en UVA

- MK-UVA: Equipo routerBoard *Mikrotik* donde se administran las VLAN y se configura la puerta de enlace por defecto hacia el siguiente salto, es decir, hacia VIG.
- SW-TUC: Switch no administrable de 16 puertos ubicado en TUC.
- MK-TUC: Equipo routerBoard *Mikrotik* donde se administran las VLAN y se configura la puerta de enlace por defecto hacia el siguiente salto, es decir, hacia UVA.
- Conexión cableada hacia el *Linksys*.
- *Linksys*: Equipo configurado en capa 2 y GW en FCT.

3.1.2 Enlaces multipunto

Para realizar los enlaces multipunto se utilizan equipos *Motorola* y *Mikrotik*.

En los enlaces con equipos *Motorola*, se tienen los AP *Motorola* que le dan señal al módulo subscriptor (SM) *Canopy* de *Motorola* el cual funciona como transmisor-receptor.

Un ejemplo de esto lo podemos ver en la Figura 3.5 para el APM en la AGD, donde se tiene, por cada enlace, un AP *Motorola* que le da señal a uno o varios *Motorola* SM ubicados en diferentes puntos del Municipio Libertador.

El APM representa los tres enlaces multipunto del Municipio Libertador; AP-Norte, AP-Sur y AP-Tabay. Estos AP están conectados directamente a la CMM de la AGD y de allí, van hacia el BH-FCT por lo que el *broadcast* es replicado hacia FCT, MK-AGD y SW-AGD.

Para el caso de Tabay, se tiene un AP-Tabay, Figura 3.5, que le da servicio a 3 SM ubicados; uno en la biblioteca, otro en un CDI y el último en El Valle.

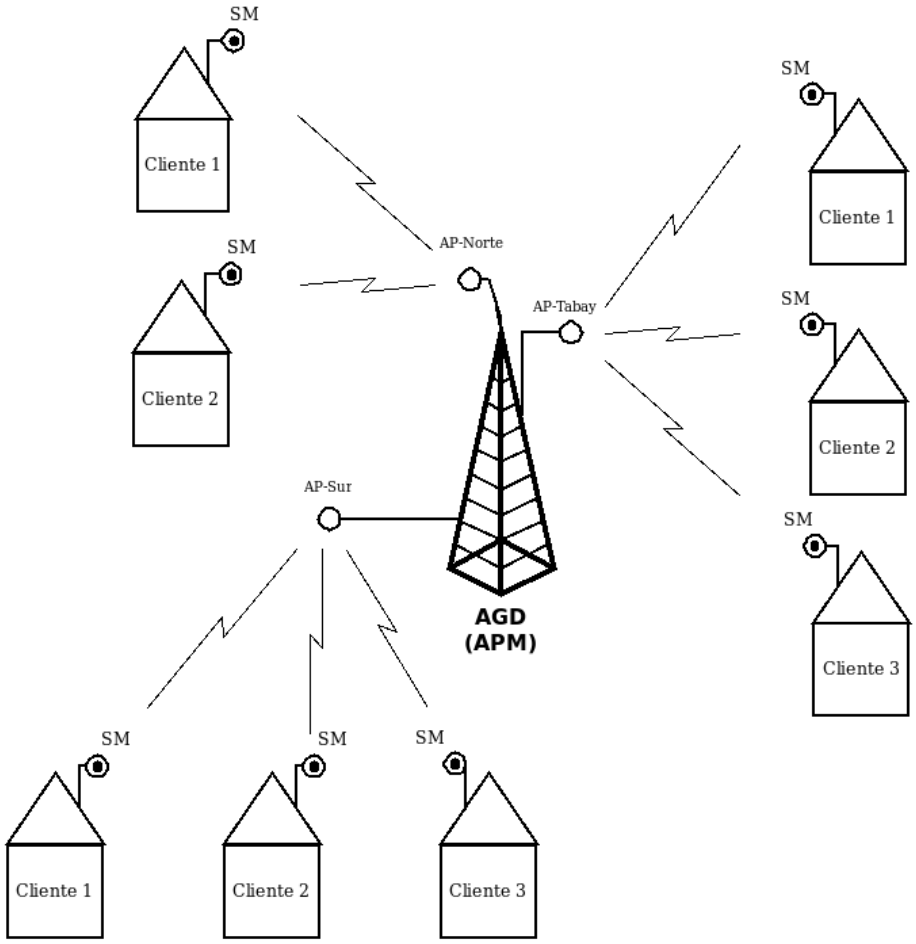

Figura 3.5: Enlace multipunto AGD – APM con equipos Motorola
Fuente: Propia

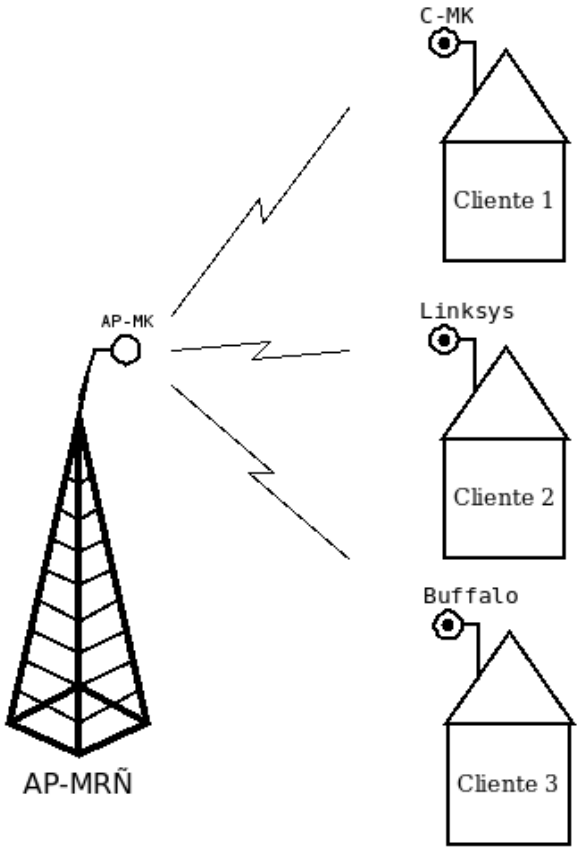

Figura 3.6: Enlace multipunto con AP Mikrotik
Fuente: Propia

Los equipos *Mikrotik*, a diferencia de los *Motorola*, permiten trabajar con diferentes tecnologías como *Linksys*, *Buffalo* y, por supuesto, equipos *Mikrotik* (Figura 3.6).

Los enlaces multipunto con equipos *Mikrotik* están presentes en el resto de los nodos donde se tiene un equipo AP *Mikrotik* y clientes *Mikrotik* en algunos casos y en otros, clientes con equipos sencillos como *Linksys.*

3.2 Topología lógica

En todos los repetidores se tienen switches o conexiones a nivel de capa 2 donde llegan los enlaces punto a punto cuyo tráfico es procesado por los *Mikrotik* para poder identificar, por medio de VLAN, la ruta hacia donde se debe enviar la solicitud según el destino correspondiente.

La red de Fundacite, a excepción del nodo NBO, cuenta con un enrutamiento sencillo y puerta de enlace en el salto siguiente. El tráfico generado por los AP es enrutado a través de VLAN, luego este tráfico pasa hacia los *Mikrotik* donde es filtrado el paquete según la VLAN a la que pertenezca.

Los equipos *Mikrotik*, como por ejemplo MK-AGD y MK-TRM, tienes tres interfaces por donde van las redes y las VLAN.

Fundacite cuenta con redes para la administración de los AP y los BH, estas redes son la 10.248.x.x/24 y la 169.254.x.x/24 respectivamente.

Para el direccionamiento IP se tiene direcciones de IP públicas pertenecientes al rango de IP 150.1x.x.x para cada uno de los nodos de la red. Las VLAN están identificadas con direcciones IP públicas pertenecientes a este rango.

Este direccionamiento se puede ver en la Figura 3.7 a la cual, por seguridad, se le ha cambiado las direcciones IP y se le ha colocado direcciones de IP ficticias.

Los usuarios detrás de los AP se encuentran configurados con el mecanismo de traducción de dirección de red (NAT) para permitir el acceso a Internet a través de las direcciones IP privadas.

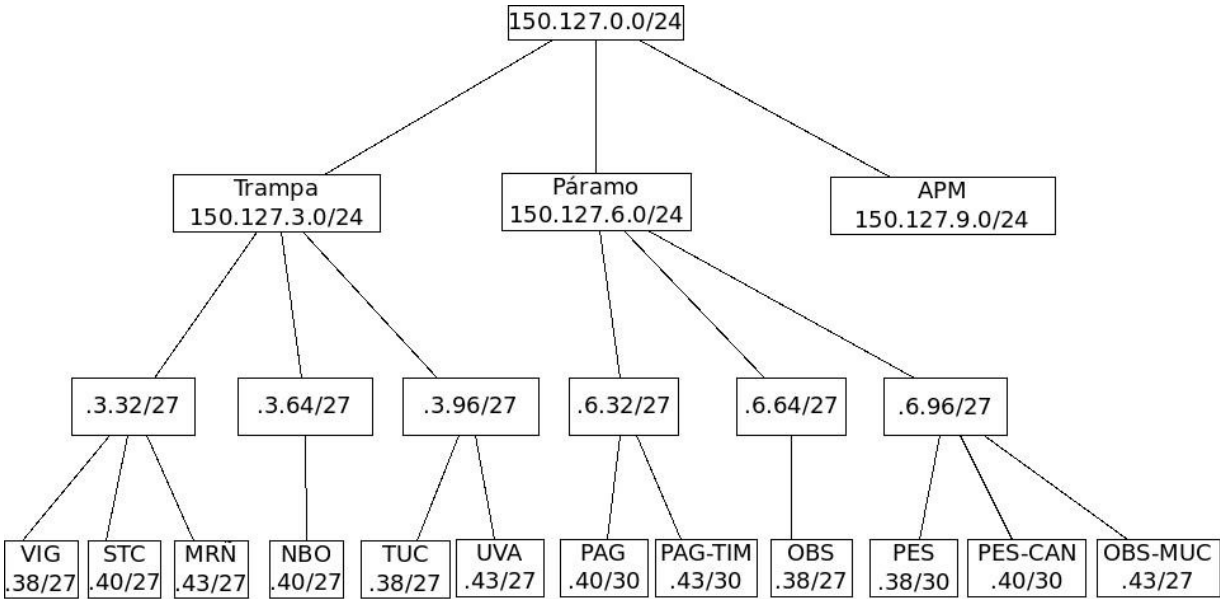

Figura 3.7: Direccionamiento IP

El manejo del tráfico en los nodos se realiza a través de los switches y los *Mikrotik*. Por ejemplo, en el nodo de TUC, Figura 3.4, todo el tráfico que viene de NBO, pasa hacia el SW-TUC y luego hacia el MK-TUC. El tráfico generado por los clientes de TUC, llega al AP-TUC y luego pasa hacia el MK-TUC el cual se encarga de enrutar el tráfico, tanto del AP-TUC como el del SW-TUC, de acuerdo a la VLAN a la que pertenezca este tráfico.

En el nodo UVA, se tiene un enlace punto a punto con VIG y el tráfico pasa hacia el SW-UVA luego va hacia el MK-UVA donde es filtrado y enrutado. Este nodo tiene otro enlace punto a punto con TUC y pasa lo mismo con el tráfico, es decir, el tráfico entre TUC y UVA es enviado al switch y luego pasa al *Mikrotik* para realizar el filtro por VLAN.

El tráfico generado por los clientes de NBO, Figura 3.4, pasa hacia el *Linksys* el cual tiene configurado su puerta de enlace (*Gateway*) en FCT. Este enlace no pertenece a ninguna VLAN, es decir, funciona en capa 2 lo que significa que al hacer una solicitud, por ejemplo hacia FCT, ejemplo que se puede observar en la Figura 3.8, envían un *broadcast* que se ve en gran parte de la red. Al recibir una respuesta, se inunda igualmente de *broadcast* al AP VIG en Buenos Aires, MRÑ, STC y OBS, todo esto debido a que en cada repetidor se tiene una conexión física con dispositivos de capa 2.

En los repetidores de UVA, TUC, PAG y PES, se tienen equipos *Mikrotik* que evitan la propagación de *broadcast*.

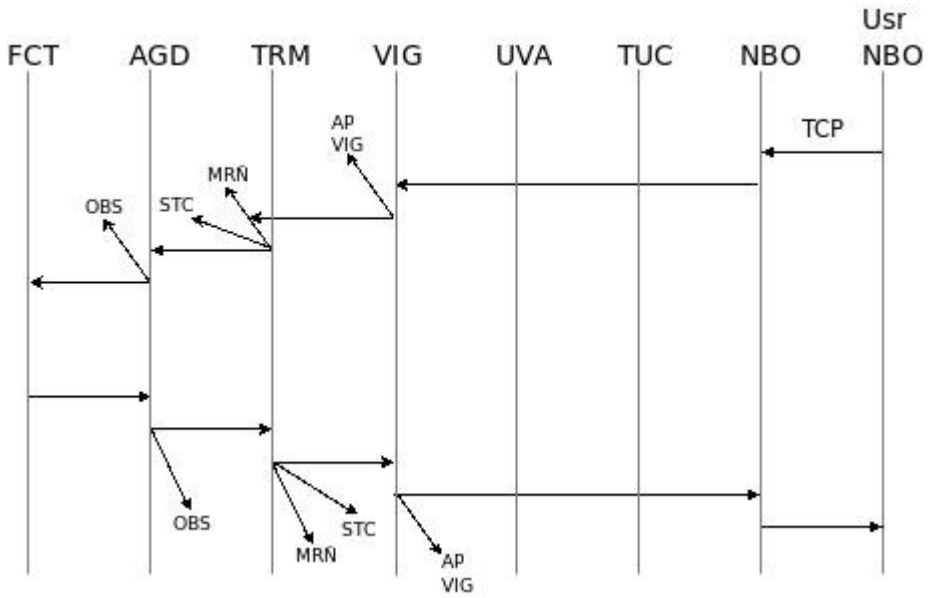

Figura 3.8: Envío de un paquete desde un usuario de NBO hacia FCT
Fuente: Propia

Los AP configurados con VLAN, al enviar un paquete, envían *broadcast* que es visto solamente por los equipos pertenecientes a esa VLAN. En el ejemplo mostrado en la Figura 3.9, donde los usuarios de TUC al hacer una petición a FCT, envían

broadcast que es visto por la UVA ya que pertenecen a la misma VLAN. Una vez que el paquete llega a la TRM, éste es enviado hacia FCT a través de una ruta estática. Al recibir respuesta desde FCT, el paquete es enrutado hasta TRM y luego sale por la VLAN correspondiente.

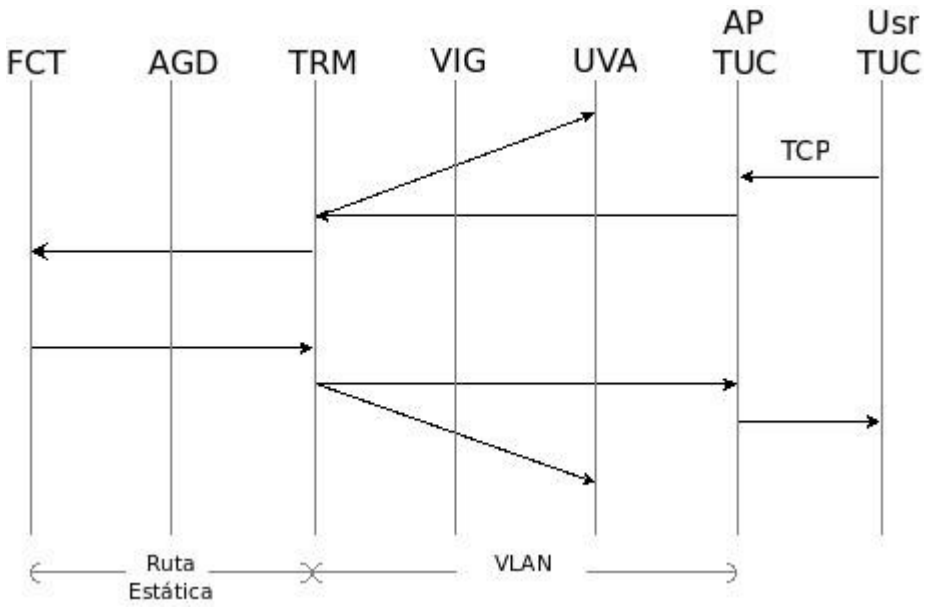

Figura 3.9: Envío de un paquete desde un usuario de TUC hacia FCT
Fuente: Propia

3.3 Políticas de QoS aplicadas en Fundacite

La red de Fundacite utiliza equipos *Motorola* y *Mikrotik* para realizar los enlaces multipunto que es donde se tiene configurada las políticas de QoS.

En los enlaces realizados con equipos *Motorola*, el QoS se aplica en el cliente, es decir, en cada SM. Allí se configura el equipo para que cada cliente tenga un ancho de banda que por lo general son 256Kbps. Cada cliente puede tener uno o más

usuarios conectados a la red cuya cantidad es desconocida para los administradores de la red.

En la Figura 3.5 se tiene un enlace multipunto con equipos *Motorola*. Por ejemplo, en el enlace AP Tabay se tiene configurado el QoS en cada uno de estos SM con un ancho de banda asignado a cada uno de los SM (por ejemplo, 64Kbps para cada cliente).

En los AP *Mikrotik* se maneja el QoS con colas. Cada cola se le asigna un ancho de banda específico y a cada cliente, se le asigna un ancho de banda que debe corresponder con el asignado a una de las colas para que de esta manera, el cliente pase a formar parte de esa cola. Si no se le asigna ancho de banda al cliente, éste consume todo el ancho de banda disponible en el enlace y no el asignado a las colas.

Un ejemplo de este funcionamiento lo podemos ver en la Figura 3.6 donde se tiene un AP-MK que le da servicio a 3 clientes. Supongamos que se configuran 2 colas con un ancho de banda de 256 y 64Kbps respectivamente. A los clientes 1 y 3 se le configura un ancho de banda de 256Kbps con lo cual se les está indicando que estos clientes pertenecen a la cola 1. El cliente 2 se le configura un ancho de banda de 64Kbps y pasa a formar parte de la cola 2.

Los equipos AP *Mikrotik* son mas robustos y tienen mejor procesador que los equipos cliente *Mikrotik*.

Para el manejo de QoS no se tiene prioridad por paquetes ni se bloquean servicios como los de red punto a punto (p2p). Tampoco se limita la tasa de descarga en horas determinadas.

Se plantea un estudio con equipos que se encuentran en la red de Fundacite para determinar el funcionamiento de éstos junto con las VLAN.

Con estas pruebas se espera obtener el rendimiento de los equipos y las reglas de QoS que se deben aplicar para un mejor funcionamiento de la red.

3.3.1 Diseño de pruebas

La red de Fundacite actualmente tiene configurado VLAN para direccionar el tráfico y disminuir tormentas de *broadcast*.

Los switches a los que se encuentran conectados la mayoría de AP y los equipos BH son swhitches no administrables, es decir, son switches sencillos que no distinguen VLAN.

Se tiene la sospecha de que la configuración implementada a través de VLAN para disminuir el *broadcast*, no está funcionando correctamente y que esta solución puede estar generando mayor cantidad de *broadcast* de lo que se podría generar con una configuración en modo bridge.

Para tener pruebas que demuestren cuál debe ser la configuración adecuada, se ha diseñado un modelo a pequeña escala de lo que se tiene en la red inalámbrica el cual se puede observar en la Figura 3.10.

Este modelo representa la configuración de una pequeña porción de la red. Para realizar las pruebas se requieren los siguientes equipos:

- 2 equipos *Mikrotik RouterBOARD* RB433-AH
- 1 switch no administrable *Dlink* (No reconoce VLAN)
- 1 switch administrable *CISCO* (Reconoce VLAN)

- 2 computadoras mini *laptops* con sistema operativo *Windows* y *Linux*
- 1 regulador de voltaje
- cables de red.

Las pruebas pueden realizarse conectando las pc a la red de forma inalámbrica o de forma cableada. Se prefiere realizar las pruebas con una conexión cableada para disminuir interferencias y efectos del ambiente.

Para tener un ambiente más real, se le inyectó el tráfico interno de Fundacite al switch en prueba.

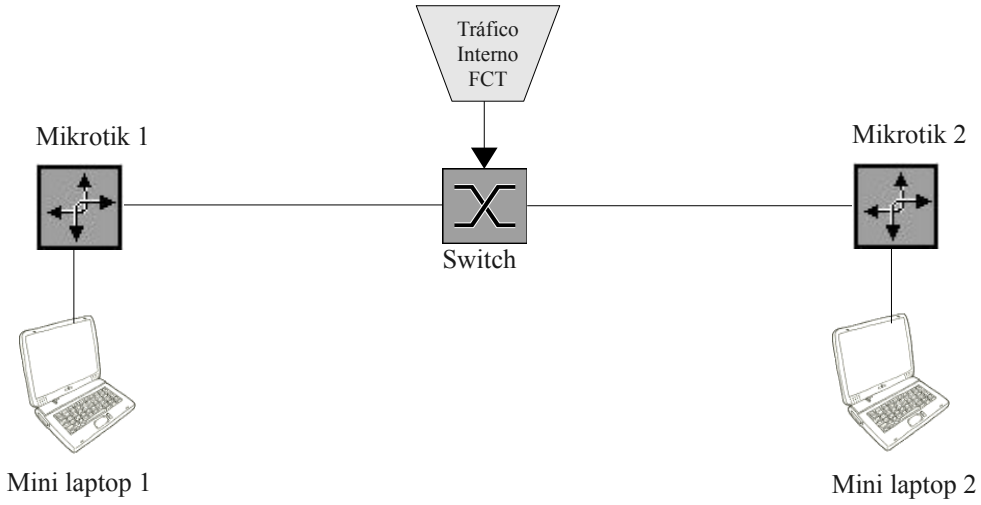

Figura 3.10: Diagrama del modelo de red

Para las pruebas planteadas, se debe cambiar el switch entre uno administrable y uno no administrable. También se configura los *Mikrotik* para poder determinar el rendimiento con VLAN y en capa 2. Al hacer estos cambios se tendrían 4 tipos de pruebas las cuales se describen a continuación:

Prueba 1

Los equipos *Mikrotik* configurados en modo bridge y conectados a un switch no administrables.

Prueba 2

Los equipos *Mikrotik* configurados en modo bridge y conectados a un switch administrable.

Prueba 3

Los equipos *Mikrotik* configurados en modo VLAN y conectados a un switch no administrable.

Prueba 4

Los equipos *Mikrotik* configurados en modo VLAN y conectados a un switch administrable.

3.3.2 Pruebas en curso

Para la realización de las pruebas, se configuró los equipos *Mikrotik* en modo bridge y luego de realizar las primeras pruebas con los switches, se procedió a configurar las VLAN con un enrutamiento al siguiente salto.

También se configuró los switches administrables para que reconocieran las VLAN configuradas en los *Mikrotik*.

Para determinar el rendimiento del enlace se toman los siguientes parámetros:

- Throughput
- Retardo
- Tiempo de ida y vuelta (RTT)

- Pérdida de paquetes

Las herramientas que permiten evaluar cada uno de estos parámetros son *Iperf* y *Ping* descritas en el capítulo 2.

Con *Iperf* obtenemos el *throughput*, retardo y la cantidad de paquetes perdidos. El tiempo de ida y vuelta se obtiene con *Ping*.

3.3.3 Resultados de la investigación

Fundacite cuenta con equipos aptos para soportar políticas de QoS y que no han sido configurados hasta el momento.

También cuenta con routers *Cisco* que pueden ser configurados y usados en los enlaces que tienen mayor tráfico como los nodos de AGD y TRM.

Los problemas de tráfico ARP pueden ser solucionados al configurar VLAN en los enlaces causantes de problemas.

Capítulo 4

Medición y análisis de resultados

Para determinar el perfil de tráfico, rendimiento de los enlaces y reglas de QoS que permitan mejorar la calidad del servicio, se realizaron mediciones de la red inalámbrica de Fundacite y se han analizado los resultados obteniendo un perfil del tráfico de la red.

4.1 Mediciones

La red de Fundacite está formada por una parte inalámbrica y otra cableada. La parte cableada corresponde al nodo identificado en el diagrama de la Figura 3.1 como FCT, que es por donde se da salida de la red inalámbrica hacia la Internet.

La captura de datos se realizó con un switch que soporta *port mirror* unido a un computador para almacenar todo el tráfico de subida proveniente del enlace punto a punto de FCT-AGD y el DMZ de FCT tal como se indica en la Figura 3.2.

Se realizó mediciones durante 100 horas continuas, desde el 31 de enero a las 9am hasta el día sábado 4 de febrero a la 1pm. Las trazas obtenidas en cada hora de medición ocupa alrededor de 400 MB al capturar sólo las cabeceras de los paquetes. Se estima que el volumen de datos a capturar, podría ocupar 30 GB y el procesamiento de los datos podría tornarse complicada y hasta imposible de

procesar por las herramientas usadas. Para solucionar esto, fue necesario almacenar las capturas separando en un archivo por cada hora de medición.

Al final de las capturas, se obtuvo 100 archivos que corresponden a las 100 horas de medición y cada uno de éstos ocupa entre 200 y 400 MB.

4.2 Tráfico de red

En este apartado se estudia el tráfico generado por los nodos principales de la red de Fundacite. Se determina cuáles son los nodos que presentan mayor consumo de recursos de red y cuáles son los servicios más demandados por los usuarios.

4.2.1 Nodos de la red y su porcentaje de uso

A partir de los datos capturados con *Tcpdump* y con la ayuda de un *script* en *Python*, fue posible analizar los paquetes capturados y determinar la dirección IP origen para luego proceder a contar y sacar el porcentaje de paquetes provenientes de cada uno de los principales nodos de la red de Fundacite y determinar cuál de ellos tiene mayor consumo. El resultado fue registrado en la Tabla 4.1.

No se esperaba que el nodo OBS tuviese un 27,75% de consumo de red. El APM que corresponde al AP del área metropolitana tiene un porcentaje de uso de 33,18%, valor esperado ya que este AP presta servicio a una gran cantidad de usuarios.

Nodo	Paquetes	%
STC	4388796	8,14
PES	72	0,00013(S/U)*
MRN	1278745	2,37
PAG	2917194	5,41
OBS	14857603	27,57
VIG	2998824	5,56
NBO	5153350	9,56
APM	17881771	33,18
UVA	4327497	8,03
TUC	607	0,0011(S/U)*
Total Paquetes: 53894737		

* Sin suarios

Tabla 4.1: Porcentaje de consumo por nodo

Cuando se realizó la captura de los datos, los nodos de PES y TUC no tenían usuarios conectados, lo que explica su bajo porcentaje de uso. Los paquetes registrados puede deberse a paquetes de peticiones.

Con *Tcpdump* se capturaron 58.497.925 paquetes de los cuales 53.894.737 paquetes corresponden a paquetes cuya IP origen pertenece a los principales nodos de la red de Fundacite. Es decir, el 92,13% de los paquetes tienen IP origen en las subredes inalámbricas de Fundacite.

4.2.2 Paquetes por protocolo

El estudio de protocolos en la red se realizó a partir del tráfico capturado con *Tcpdump* y se filtró con *Tcpstat* para obtener, por cada hora de medición, la cantidad de paquetes TCP y UDP de capa transporte (capa 3), ICMP y ARP que pertenecen a la capa Internet (capa 2) del modelo TCP/IP. Los datos para cada uno de estos protocolos, fueron almacenados en archivos por separado y luego leídos con *Gnuplot* para realizar la gráfica del tráfico de red por hora.

En la Figura 4.1 se tiene, por cada hora de medición, la cantidad de paquetes por por protocolo. El eje *x* representa las horas de la semana, iniciando el día 31 de enero a las 9am y finalizando el sábado 4 de febrero a la 1pm. El eje *y*, en escala logarítmica, está representada la cantidad de paquetes transmitidos en cada hora de medición. Alrededor del 90% del tráfico corresponde a tráfico TCP de capa transporte y el tráfico UDP se encuentra por debajo de los cien mil paquetes. Para los protocolos ICMP y ARP, se tiene una cantidad cerca de los 10000 paquetes por protocolo.

Llama la atención la cantidad de tráfico ARP observado en la gráfica y este se puede deber a la forma como está actualmente configurada la red. (Explicado en el capítulo 3).

El tráfico de la red sigue un patrón, donde se tiene picos que representan los días de la semana en horario diurno, siendo mayor en las horas de la mañana y menor para las horas de la noche. Las caídas para las horas del medio día son muy leves.

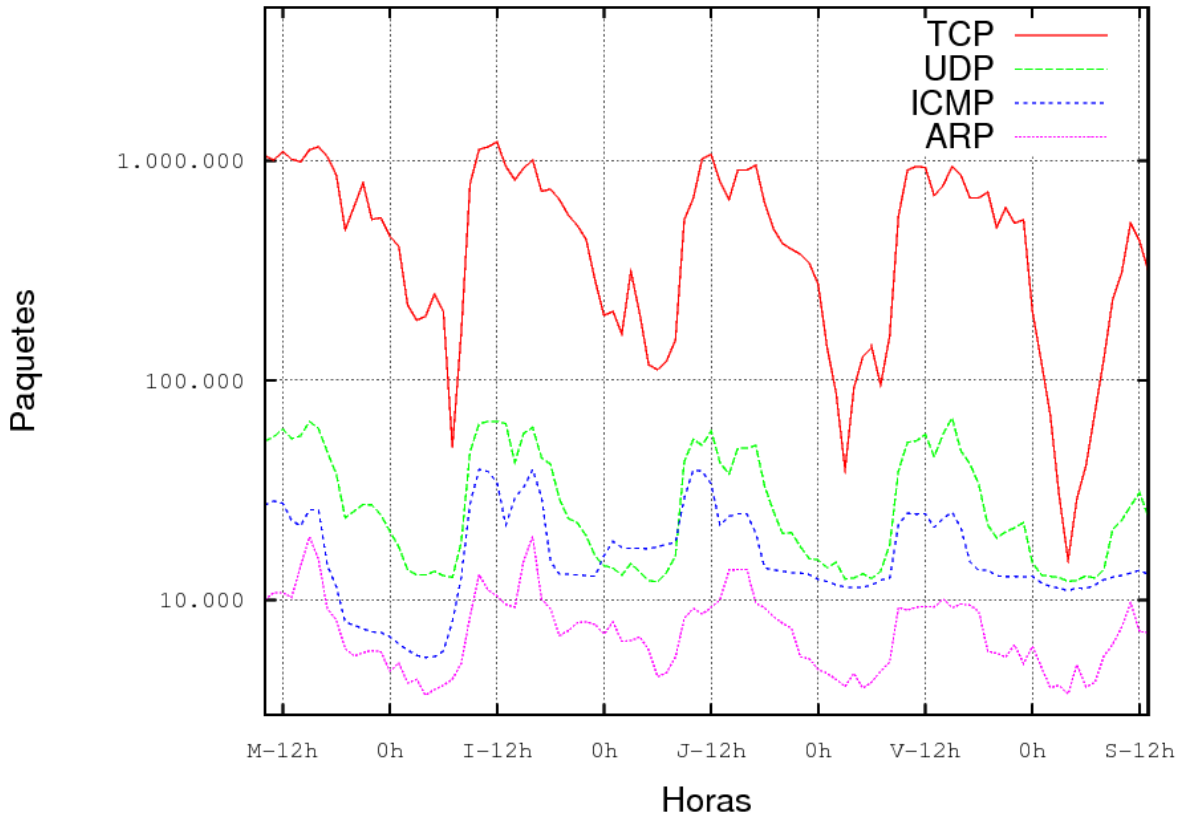

Figura 4.1: Tráfico de red por hora

En el tráfico de red se tiene 3 caídas importantes para el tráfico TCP; una alrededor de las 22 horas de medición lo que corresponde al día miércoles 01 de febrero a las 6am, la segunda caída se puede observar cerca de las 66 horas de medición que corresponde al día viernes 03 de febrero a las 2am y una última caída se aproxima a las 91 horas de medición que se estima sea del día sábado 04 de febrero a las 3am.

También se observa 4 picos que corresponden a horas de trabajo de los días martes, miércoles, jueves y viernes. Curiosamente se observa un pico para el día

sábado en la mañana a pesar de que se supone que las instituciones a las cuales se les presta el servicio, no laboran los fines de semana.

Respecto al tráfico ARP observado, se consideró necesario realizar un estudio más detallado en este punto para determinar cuáles nodos están generando tráfico ARP y hacia qué nodo.

Para esto, se filtró los paquetes ARP y se realizó un *script* en *Python* para realizar el conteo de paquetes ARP dirigidos hacia los principales nodos de la red. El resultado obtenido se puede observar en la Tabla 4.2.

Este resultado causó gran impresión ya que se tenía la sospecha de que las VLAN no eran reconocidas por los switches y por lo tanto, el tráfico ARP era visto por toda la red.

Nodo	Paquetes	%
ABA	5857	1,52
STC	0	0
PES	0	0
MRN	0	0
PAG	0	0
OBS	0	0
VIG	0	0
NBO	7594	1,97
APM	372789	96,52
UVA	0	0
TUC	0	0
Total Paquetes: 386240		

Tabla 4.2: Tráfico ARP entre los nodos

El *script* se ejecutó tanto para conocer por qué subred se estaba preguntando y quién estaba preguntado y se pudo determinar que los que preguntan son el nodo de NBO, el APM y el ABA de CANTV que se tiene en la sala de servidores de Fundacite.

El tráfico ARP de NBO se genera ya que la configuración que tiene este nodo es un enrutamiento sencillo con la puerta en enlace en FCT, es decir, el tráfico de NBO pasa por los elementos de la red sin ser filtrado.

La configuración que tiene el nodo del OBS permite que el *broadcast* sea filtrado por el MK-OBS de la Figura 3.3. Esta configuración la tienen los nodos principales, excepto NBO, y por lo tanto, el filtrado de paquetes funciona de manera similar evitando así, el tráfico ARP en la red.

El tráfico del APM no pertenece a ninguna VLAN y por lo tanto, no es filtrado por el *Mikrotik* de AGD. Esto trae como consecuencia que se tenga que preguntar en FCT dónde se encuentran los destinatarios de los paquetes generados por este APM generando así, el 96% del tráfico ARP observado en FCT.

La topología física del nodo de NBO plasmado en la Figura 3.4 muestra que el tráfico generado por los clientes de NBO pasa hacia el *Linksys* el cual tiene configurado su puerta de enlace (*Gateway*) en FCT, razón por la cual, el tráfico salta todos los elementos de red hasta FCT. Este enlace no pertenece a ninguna VLAN, es decir, está en modo bridge.

4.3 Consumo de ancho de banda

A continuación, se estudia el consumo de ancho de banda de la red. Los datos necesarios fueron obtenidos con *Tcpstat* desde los archivos capturados con *Tcpdump*.

4.3.1 Consumo de ancho de banda

En la Figura 4.2 se tiene en el eje *x*, las horas de medición. Las 0h representa las 12pm de cada día de medición y las 12h, a las 12m de cada día. En el eje *y*, el promedio de la velocidad de transferencia para cada una de esas horas.

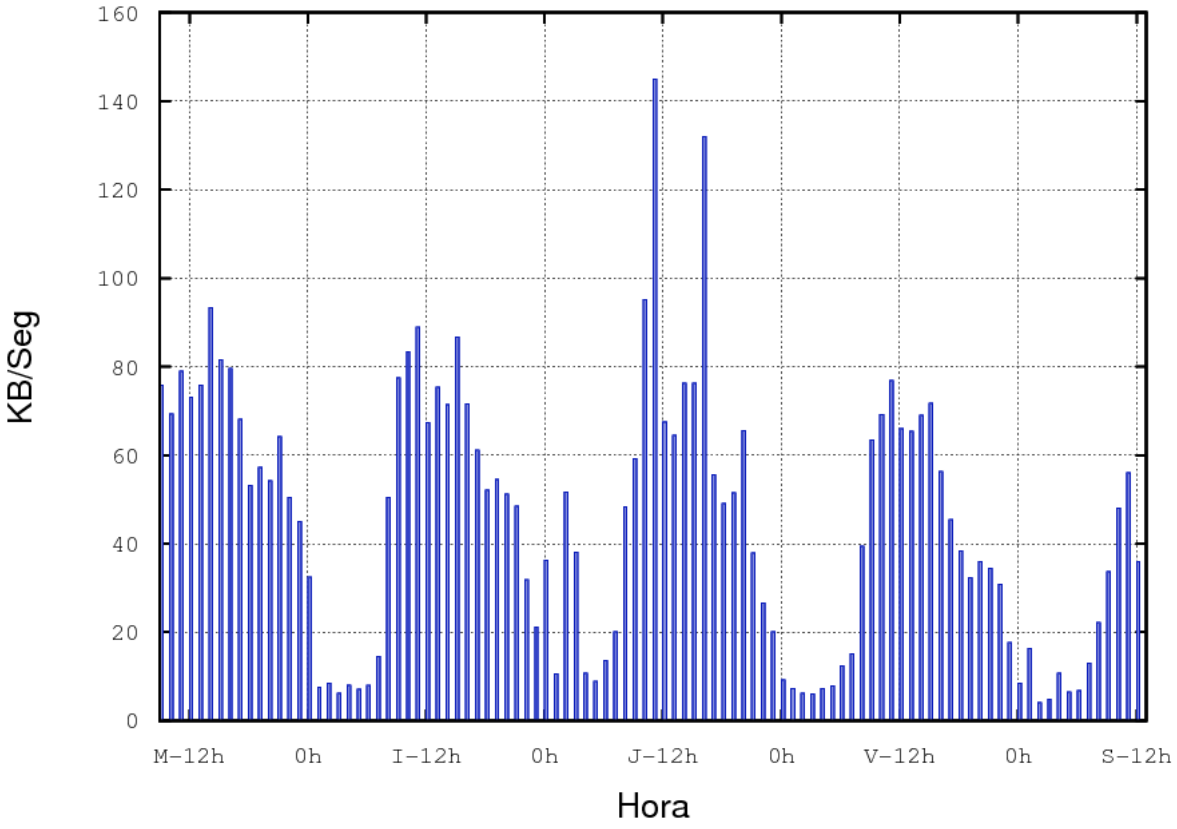

Figura 4.2: Consumo de ancho de banda durante 100 horas de medición

En la Figura 4.2 también se observan los 3 descensos que representan las horas de la noche de los días martes, jueves y viernes que es cuando se asume que no están laborando las instituciones a las cuales se les presta servicio. Llama la

atención que durante la media noche del día miércoles no cumple con el patrón presente en otros días.

Se tienen picos importantes que forman un patrón en la mayoría de los días en horas de trabajo entre las 9am y las 11am. En las barras que representan las 11am y 4pm día jueves 2 de febrero, muestra 2 picos que superan los 130 KB/Seg que llaman la atención. El consumo normal en el resto de la semana no superan los 100 KB/Seg.

Para las horas de la tarde se tiene importante tráfico hasta las 5pm y luego comienza a descender de forma progresiva hasta las 11pm ó 12pm.

Los picos representan las horas de trabajo y los descensos, a las horas de descanso de la noche. Las horas de descanso del medio día tienen un descenso suave entre las 12m y la 1pm.

Tomando los datos del día jueves, que es la que mayor discrepancia muestra respecto al resto de días de la semana, se realizó la gráfica correspondiente sólo al tráfico de ese día.

El resultado se puede observar el la Figura 4.3. Allí se representa, en el eje *x*, las horas del día jueves donde la hora 0 representa la media noche, es decir, la primera hora del día y la tabulación 10, representa la hora de las 10am. En el eje *y* se tiene el promedio de la velocidad de transferencia en kilobytes por segundo.

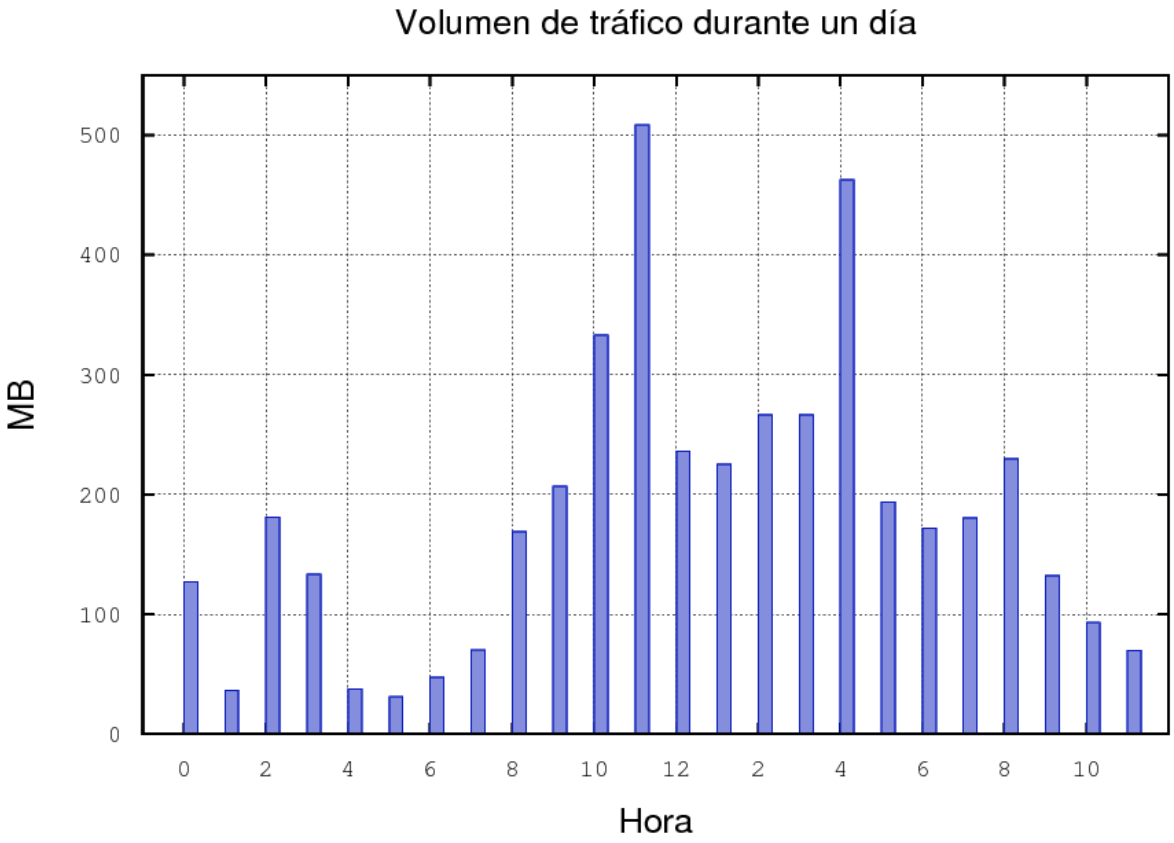

Figura 4.3: Consumo de ancho de banda durante un día

Desde las 0am hasta las 3am no se tiene un patrón claro. A partir de las 4am, el consumo comienza a ascender progresivamente hasta las 10am donde alcanza los 90 KB/Seg. Se tiene un pico brusco a las 11am y otro a las 4pm que superan los 130 KB/Seg. Después de las 4pm, el consumo comienza a descender teniendo un pequeño repunte a las 8pm.

4.4 Volumen de tráfico

El volumen de tráfico representa la cantidad total de bytes transmitidos por cada hora de medición.

Para obtener este volumen por hora, se realizó un pequeño *script* en *Python,* se totalizó los bytes transmitidos durante cada hora y luego realizó la conversión a MB por hora.

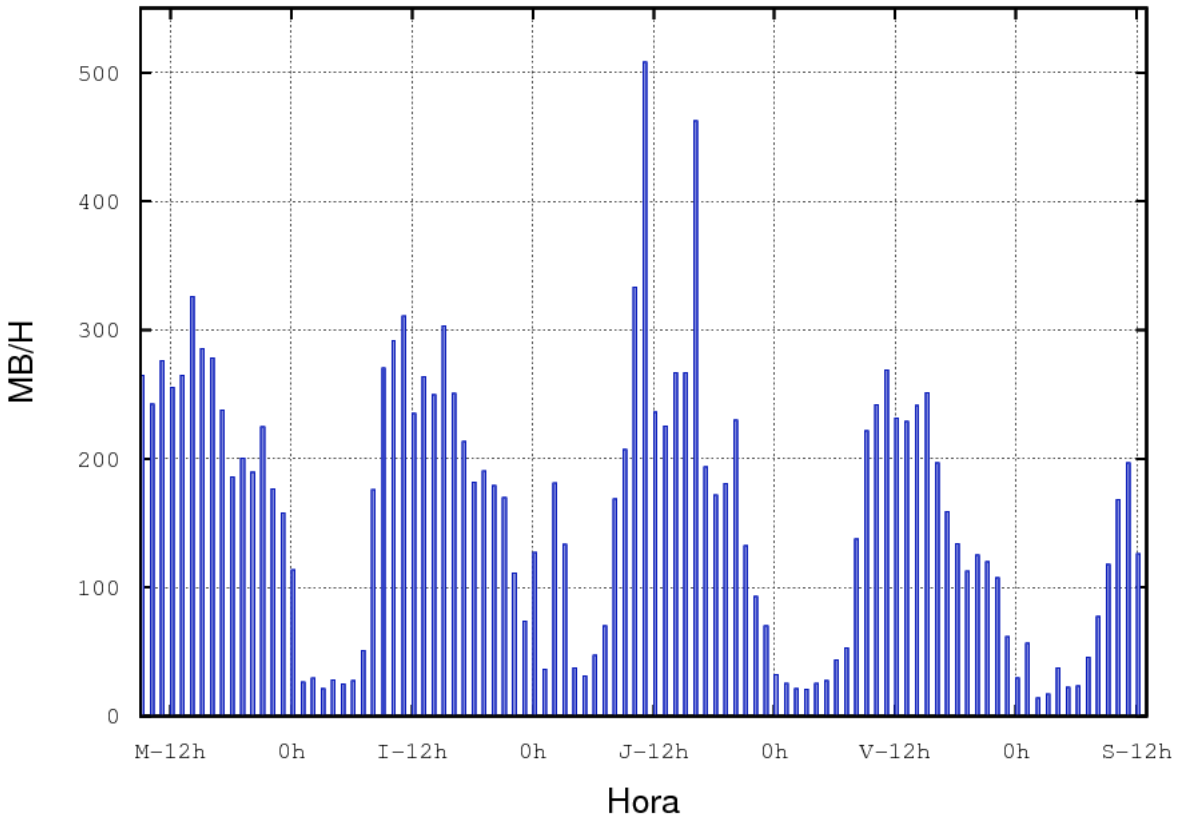

Figura 4.4: Volumen de tráfico durante 100 horas de medición

Otra forma de obtener el volumen de tráfico por hora, es haciendo uso de la aplicación *crl_flow* de la cual se hablará mas adelante.

El volumen de tráfico obtenido durante las 100 horas de medición se encuentra representada en la Figura 4.4, en ella se observa el patrón que sigue por el uso de la red.

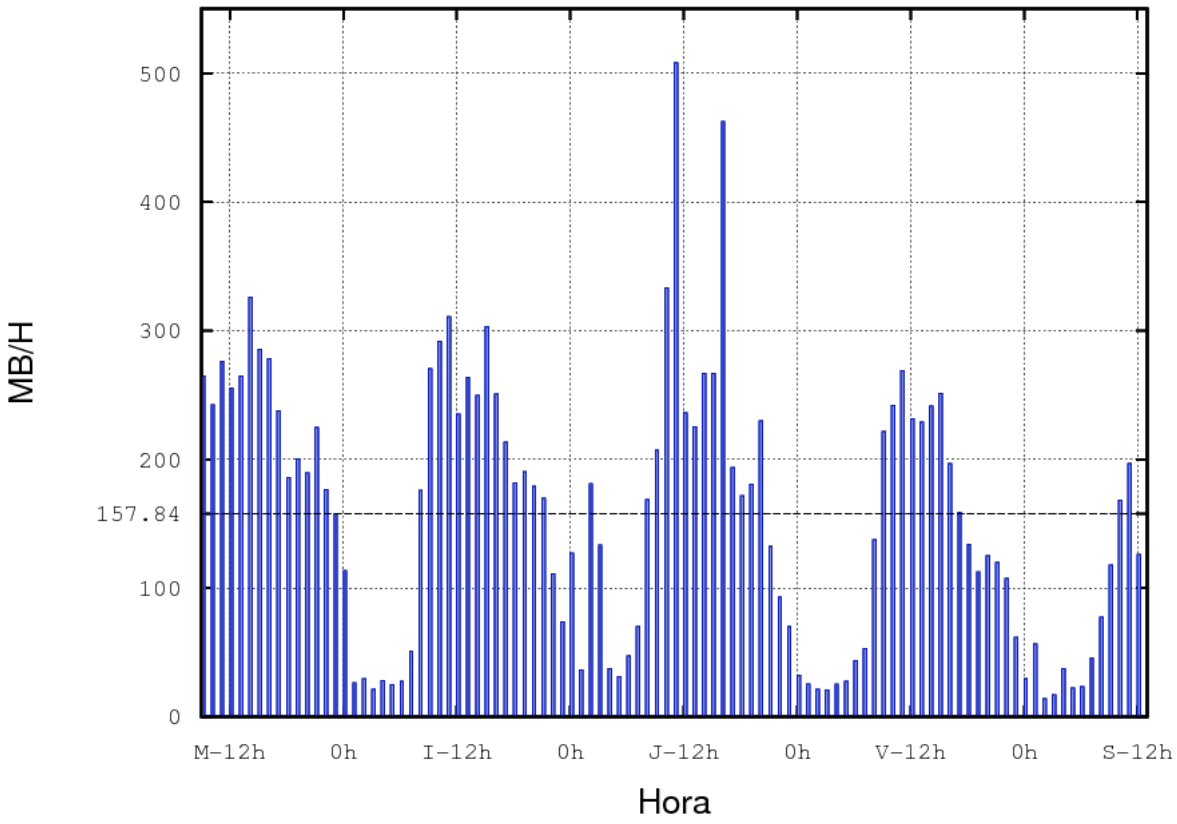

Figura 4.5: Media del volumen de tráfico durante 100 horas de medición

En el eje *x* se tiene las horas de medición por cada día de la semana al igual que la Figura 4.2. En el eje *y*, se representa el volumen de tráfico en megabytes por hora (MB/H).

Se tienen picos alrededor de los 250 MB por cada hora, con un descenso progresivo en horas de la tarde, manteniendo un tráfico bajo hasta cerca de las 6am.

El volumen de tráfico entre las 8am y las 8pm, está por encima de la mediana que es 157.84 MB/H tal y como se muestra en la Figura 4.5.

Para obtener la media, se usó el programa *R*, a nivel de línea de comando ya que tiene la capacitad de procesar un volumen de datos alto.

4.5 Escaneo de puertos

Para conocer las aplicaciones y servicios usados en la red bajo estudio, se analizaron los datos obtenidos en los archivos *pcap* correspondiente a las 100 horas de medición y se realizó un *script* en *Python* para realizar el conteo de los puertos más visitados, divididos en tres grupos: puertos bien conocidos, puertos registrados y puertos dinámicos.

Los puertos bien conocidos que van desde el 0 al 1023 son puertos reservados para servicios y aplicaciones. Los puertos registrados son usados por las aplicaciones de los usuarios y van desde el puerto 1024 hasta el 49151. Los puertos dinámicos son usados de forma aleatoria y comprende el grupo de puertos que van desde el 49152 al 65535.

Dentro del grupo de puertos bien conocidos, mostrados en la Tabla 4.3, destacan los puertos HTTP y protocolo seguro de transferencia de hipertexto (HTTPS), siendo estos los de mayor porcentaje de uso; 81,78 y 11,98 % respectivamente.

Puertos bien conocidos			
N	Puertos	Total paq / puerto	%
1	HTTP	36271735	81,78
2	HTTPS	5314829	11,98
3	Domain	1600733	3,61
4	NTP	686915	1,55
5	Microsoft-ds	161012	0,36
6	SSH	156747	0,35
7	SMTP	82725	0,19
8	IMAPS	30446	0,07
9	POP3s	16867	0,04
10	843	8205	0,02
	Subtotal	44330214	
	TOTAL	**44355287**	99,94

Tabla 4.3: Puertos bien conocidos

Puertos registrados			
N	Puertos	Total paq / puerto	%
1	1935	234653	2,97
2	36833	227675	2,88
3	6567	217292	2,75
4	43088	174243	2,20
5	12512	173762	2,20
6	43463	168138	2,13
7	5678	153466	1,94
8	2002	72656	0,92
9	8080	66463	0,84
10	8800	66274	0,84
	Subtotal	1554622	
	TOTAL	**7912060**	19,65

Tabla 4.4: Puertos registrados

N	Puertos	Total paq / puerto	%
1	63773	53295	1,51
2	60804	40003	1,14
3	56219	29289	0,83
4	63611	17589	0,50
5	57577	16256	0,46
6	50832	15181	0,43
7	56890	13484	0,38
8	51832	10306	0,29
9	56941	10064	0,29
10	56976	10036	0,29
	Subtotal	215503	
	TOTAL	**3521000**	6,12

Tabla 4.5: Puertos dinámicos

Porcentaje por grupos		
Puertos	Total paq / puerto	%
Bien conocidos	44355287	79,51
Registrados	7912060	14,18
Dinámicos	3521000	6,31

Tabla 4.6: Porcentaje por grupos

Los puertos registrados tienen un menor porcentaje de uso y su distribución entre los 10 más visitados, tabulados en la Tabla 4.4, no supera el 3%. Caso más acentuado para los puertos dinámicos de la Tabla 4.5, donde su distribución de uso es bastante uniforme y no mayor al 2%.

Del resultado anterior se obtiene un total de 55.788.347 paquetes escaneados lo que corresponde a un 100% del total de los paquetes. La Tabla 4.6 muestra que el 79,51% de los puertos usados, son puertos asignados a aplicaciones conocidas, el 14,18% son puertos registrados y el 6,31% son puertos dinámicos que comúnmente son usados en conexiones de red punto a punto (p2p).

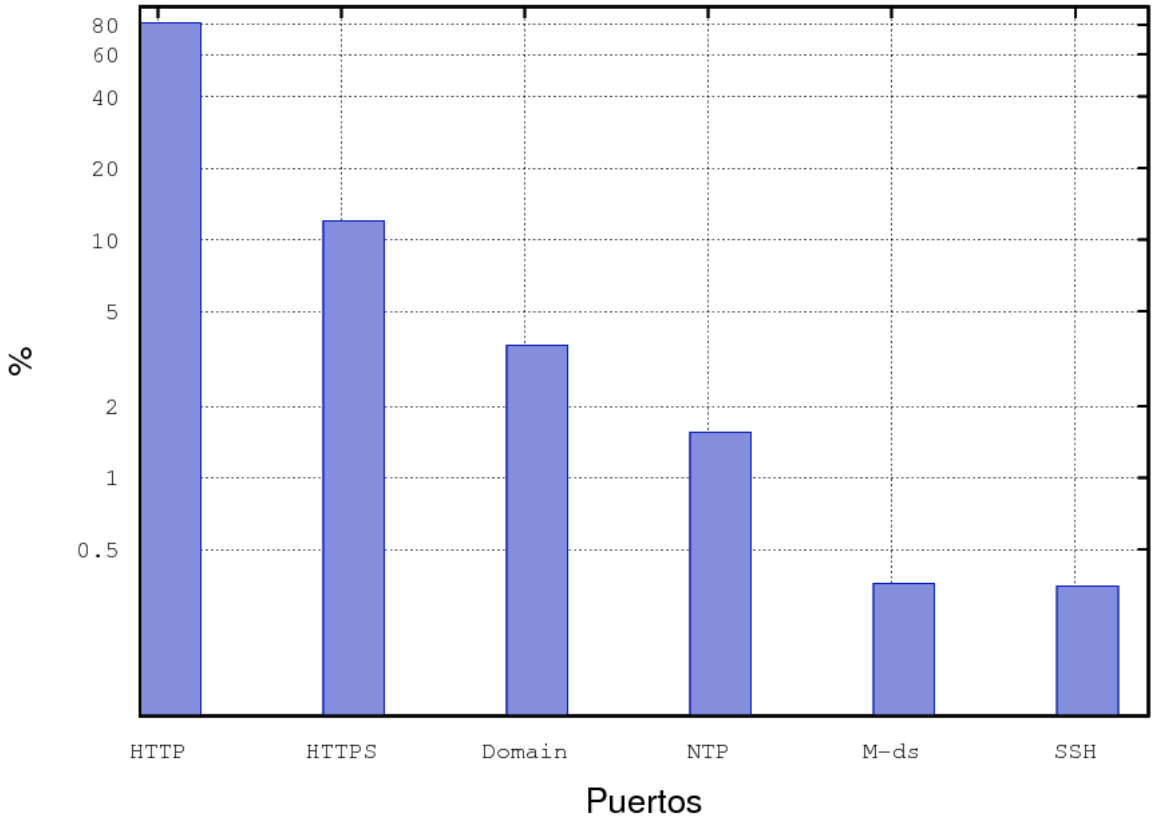

Figura 4.6: Puertos bien conocidos

De los resultados obtenidos se generan las gráficas con los puertos más usados por grada grupo y se ilustran en las Figuras 4.6; 4.7 y 4.8

El puerto más usado es el puerto 80 con un 81,78 % de uso y es el usado para tráfico HTTP. Le sigue el puerto 443 con un 11,98%, puerto usado por el protocolo HTTPS. El puerto 53 (DNS) con un 3,61%. Los 7 puertos restantes de los 10 más usados, tienen un bajo porcentaje de uso, el puerto 123 (NTP) con un 1,55% y los restantes con un porcentaje de uso inferior al 1%.

La escala para la gráfica de puertos registrados, Figura 4.7, está presentada hasta el 4% del 100% ya que el porcentaje del puerto más usado no superen éste valor.

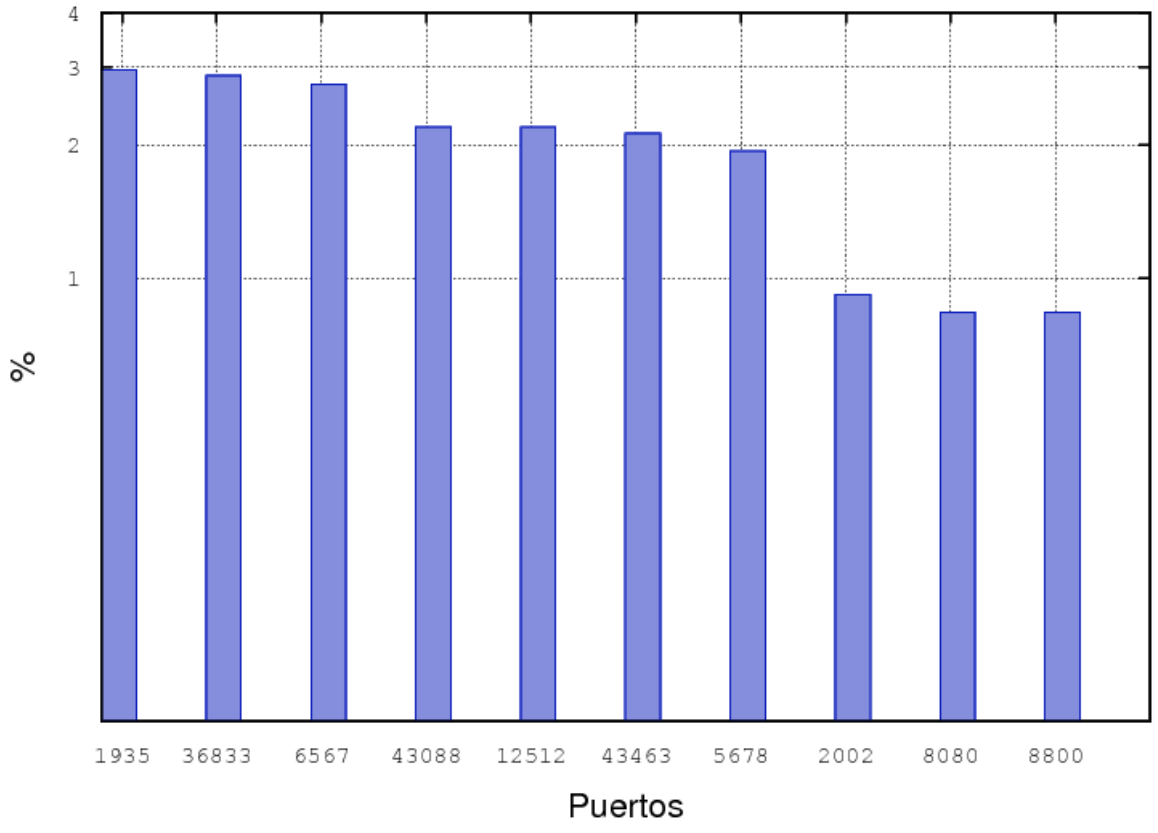

Figura 4.7: Puertos registrados

El porcentaje del puerto dinámico más usado no supera el 2%, por lo tanto, la escala en el eje *y* para la gráfica de la Figura 4.8 se tabula hasta el 2% para tener mayor legibilidad en los datos.

En la Figura 4.9 se tiene la distribución del porcentaje de uso por grupo de puertos, donde se puede observar que el 79,51% del tráfico viaja por puertos bien conocidos o puertos de servicio.

En análisis previos, se ha podido demostrar que el mayor porcentaje de tráfico corresponde al acceso a páginas HTTP y HTTPS que pertenecen a puertos bien conocidos.

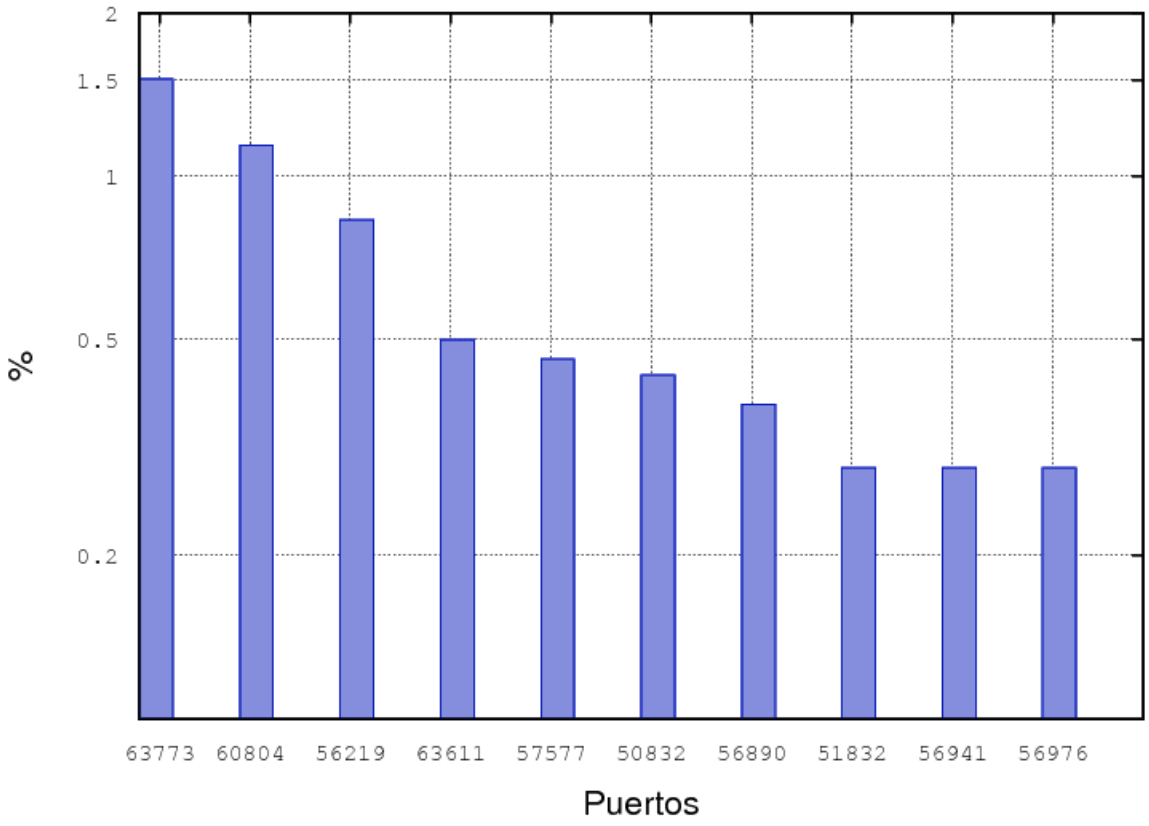

Figura 4.8: Puertos dinámicos

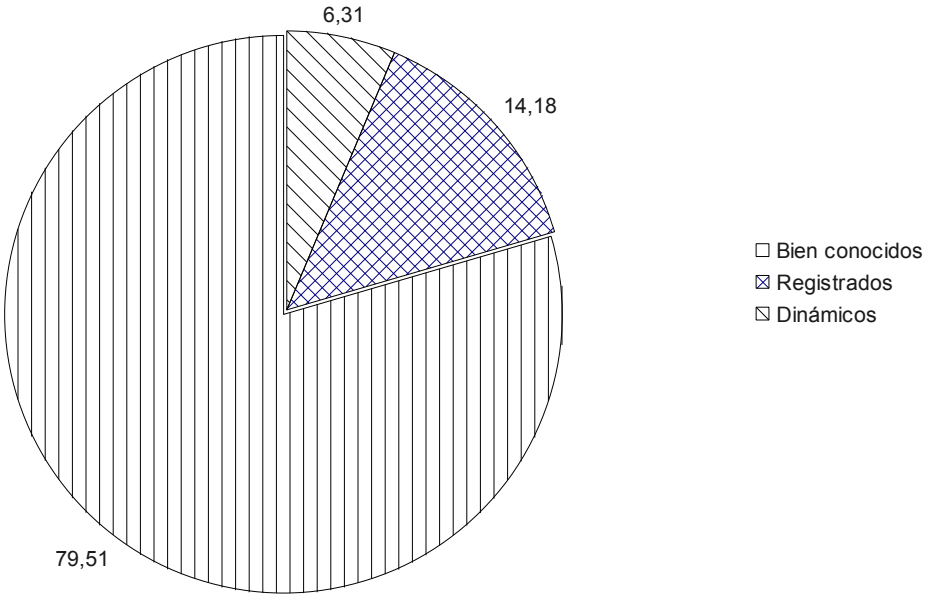

Figura 4.9: Grupos de puertos

4.6 Pares de IP origen-destino

Para el análisis de los pares de IP origen-destino, se consideró que un flujo corresponde a la conexión entre un par de IP origen destino y un par de puertos origen destino. El conteo total de la cantidad de paquetes, los bytes transmitidos y el total de flujos por cada par, se obtuvo haciendo uso de la aplicación *crl_flow* de la Herramienta *CoralReef*.

Con la aplicación *crl_flow* se obtiene archivos con extensión *t2* que contienen sólo la información requerida para los próximos análisis, disminuyendo considerablemente el espacio ocupado por los datos capturados (de 17 GB bajó a 362 MB).

Los datos obtenidos en *t2* son: IP origen, IP destino, puerto origen, puerto destino, cantidad de paquetes y de bytes enviados durante el flujo, total de flujos y tiempo de inicio y finalización del flujo.

4.6.1 Volumen de datos para los pares origen-destino

Las conexiones que ocurren más de una vez, son contadas a través de un *script* de *Python* para obtener el total de paquetes, bytes enviados y la cantidad total de flujos. El *script* considera que una dirección IP origen puede ser en otro momento, una dirección IP destino perteneciente a la misma conexión.

La cantidad de datos de subida entre pares de IP, se encuentra representada en la Figura 4.10. En el eje *x*, en escala logarítmica, se tiene el volumen de datos en bytes para 100 horas de medición y en el eje *y*, la frecuencia de aparición de los bytes por cada conexión entre los pares de IP.

La gráfica demuestra que un alto volumen de datos, entre los 100 y 10000 bytes, tienen una alta frecuencia de aparición y para volumen de datos mayores a los 10000 bytes, su frecuencia es baja lo que indica que el tamaño de los paquetes enviados por los usuarios, suele ser bajo.

La cantidad de flujos entre pares de IP origen-destino, tiene una frecuencia baja cuando se trata de flujos mayores a los 100 flujos. Esto puede ser observado en la Figura 4.11.

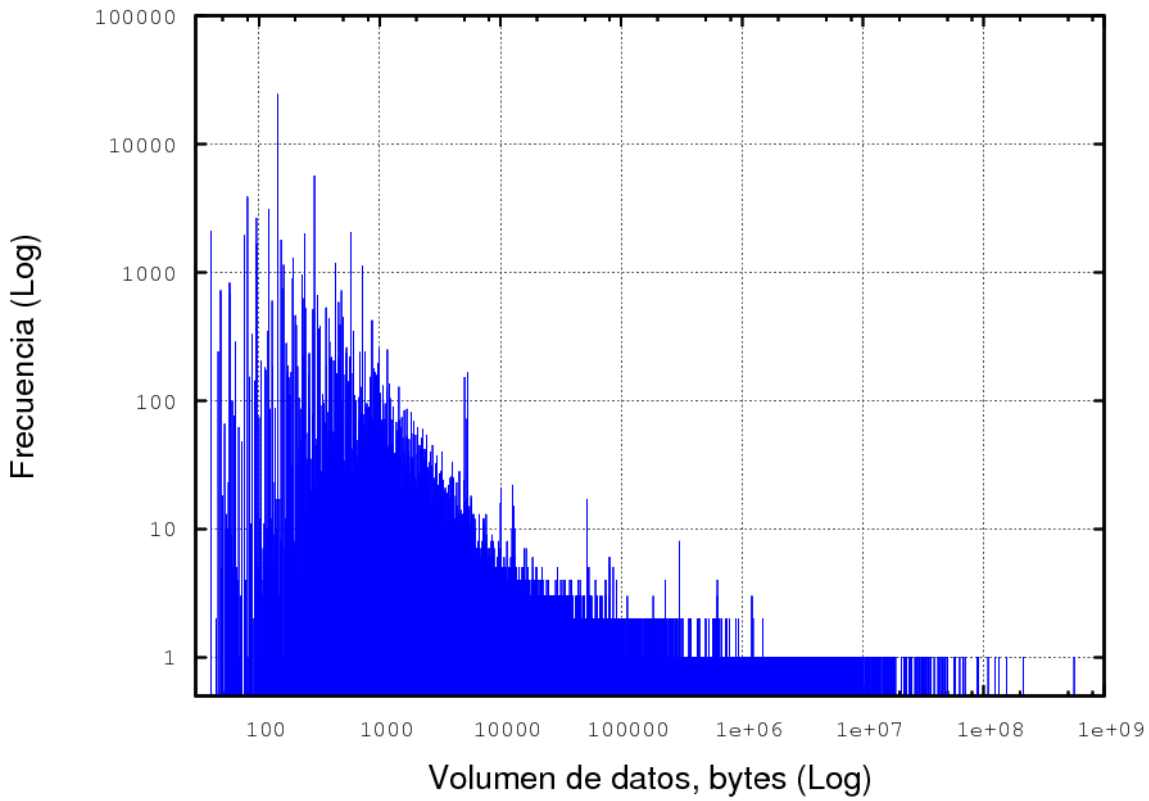

Figura 4.10: Histograma del volumen de datos entre pares Origen-Destino

En el eje *x* se tiene la cantidad de flujos por cada conexión entre pares de IP y en el eje *y*, la frecuencia para cada uno de los números de flujo. La gráfica demuestra que para una cantidad de 1000 flujos de entre pares de IP, suele ocurrir sólo 1 vez y que un flujo entre un par de IP, ocurre con una mayor frecuencia, es decir, una conexión entre un único par de IP ocurre alrededor de un millón de veces.

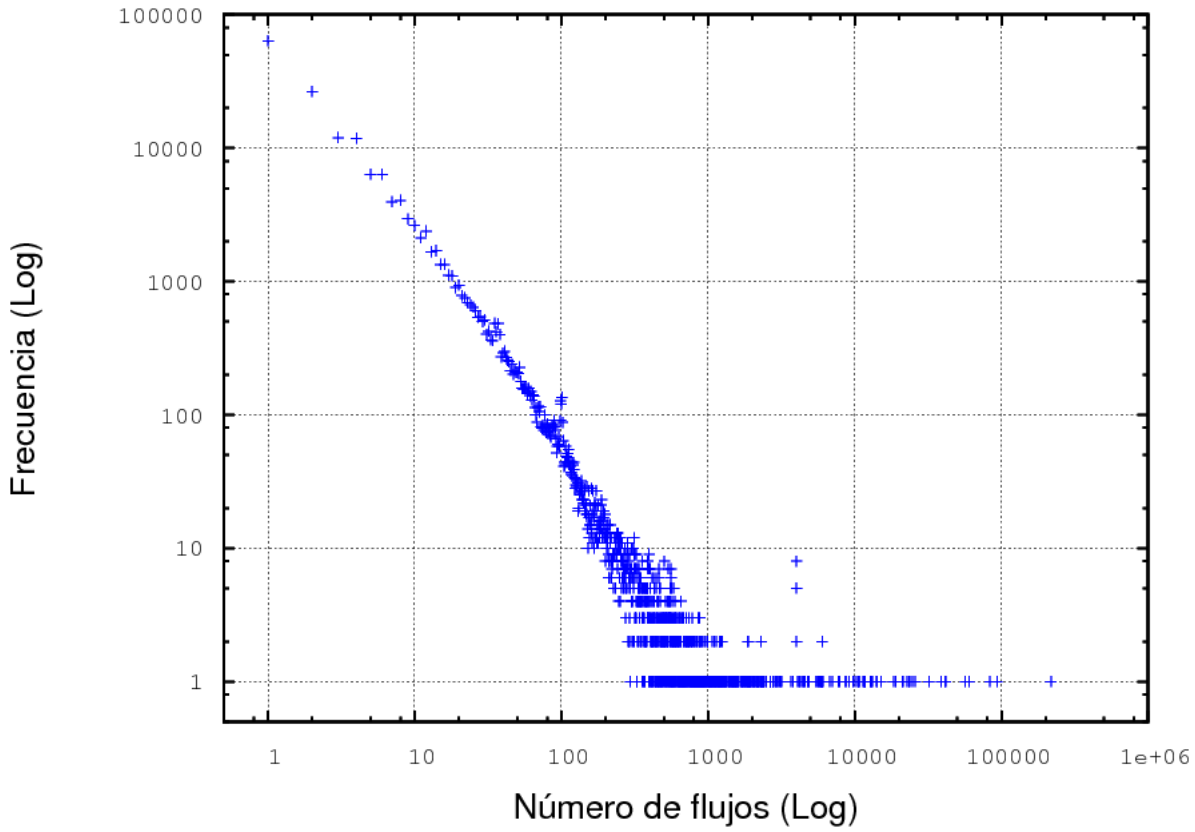

Figura 4.11: Pares Origen-Destino

La función de distribución acumulada (FDA) para el volumen de datos de la Figura 4.12, muestra una curva que asciende progresivamente entre los 100 y 10000 bytes, que es donde se tiene una alta frecuencia en la cantidad del volumen de datos de 10000 bytes. En este punto, se alcanza el 80% del volumen de los datos.

Se realizó un estudio estadístico con *R* para obtener las gráficas *boxplot*. Este tipo de gráfica muestra información resumida sobre la media, el valor mínimo, valor máximo y los cuartiles (Tabla 4.7).

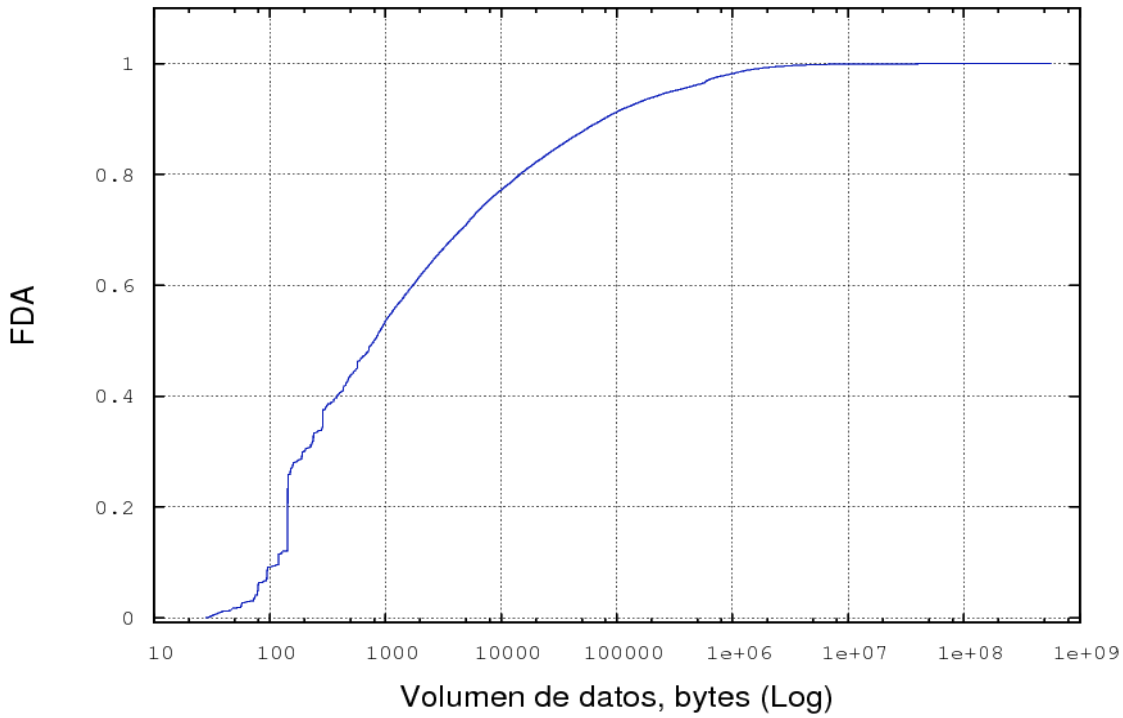

Figura 4.12: FDA del volumen de datos en bytes

Media	**Min.**	**Max.**	**Mediana** (Q2)	**Cuartiles**		
				Q1 25%	**Q2** 50%	**Q3** 75%
93123.69	28	562647260	800	144	800	7588

Tabla 4.7: Estudio estadístico del volumen de datos

La Figura 4.13 demuestra que el volumen de datos que circula en la red tienen un tamaño en bytes pequeño. El 25% del volumen, corresponde a un volumen por debajo de 144 bytes, el 50% es menor a 500 bytes y el 75% tiene un volumen de datos inferior a 7588 bytes. Se tiene un tamaño máximo que alcanza los 536 MB para un mensaje enviado por el usuario.

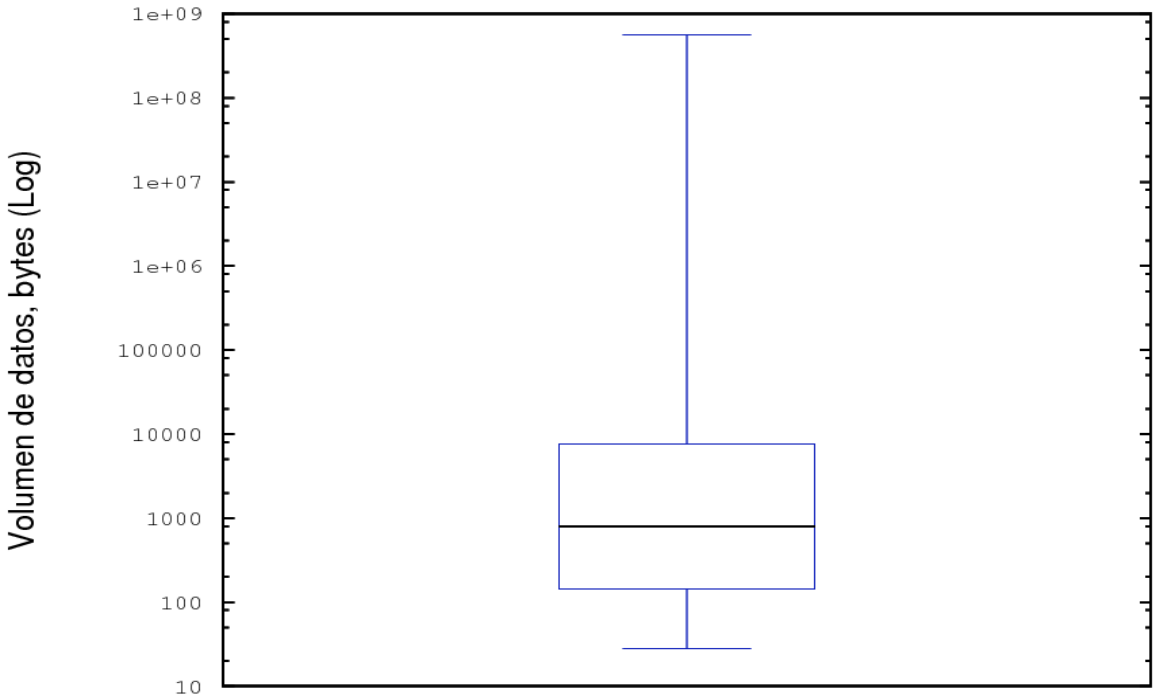

Figura 4.13: Boxplot del Volumen de datos

4.6.2 Distribución de la longitud del flujo (Por conexión)

Para el estudio de la longitud del flujo, se toma en cuenta el volumen de datos transmitidos por cada conexión entre un par de usuarios, es decir, usuarios individuales, sin tomar en cuenta el volumen total de datos para el total de conexiones realizadas entre ese par de IP.

Se realizó las gráficas de la misma forma que se realizaron para el volumen de datos entre pares de IP.

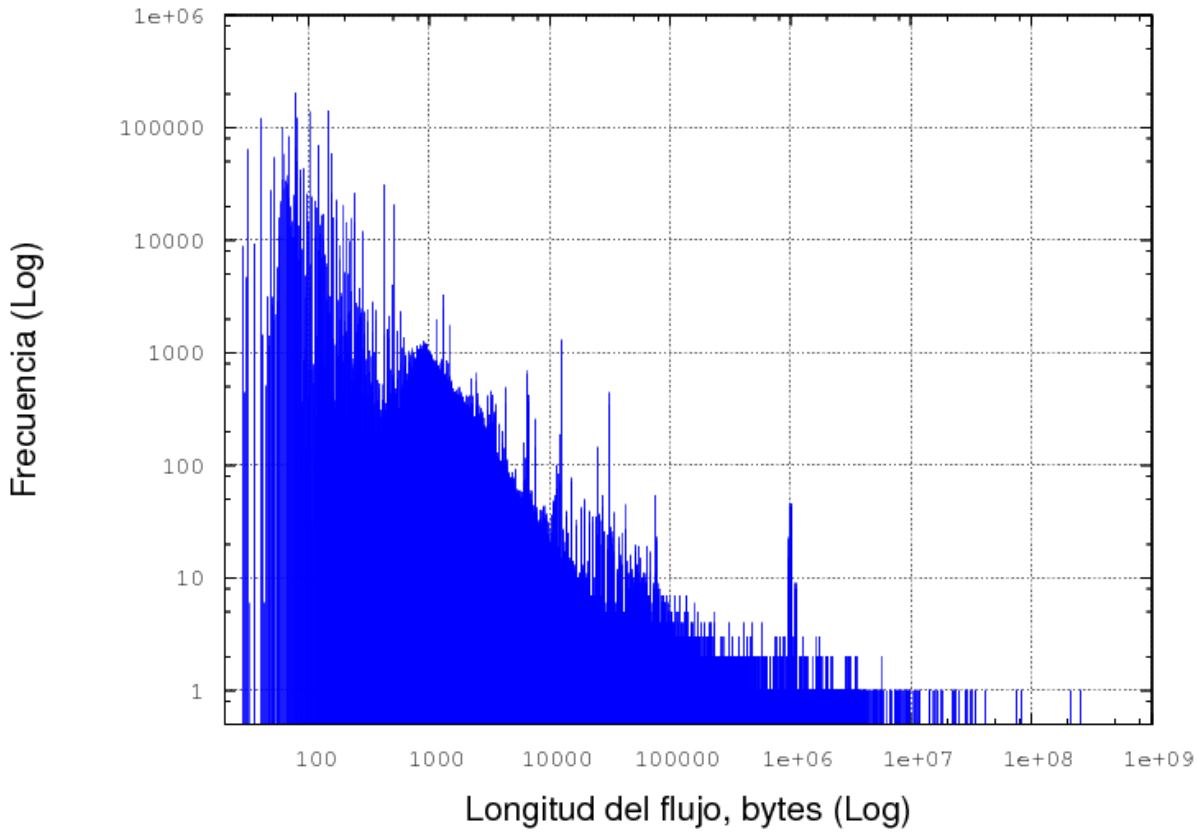

Figura 4.14: Flujo por conexión

En la Figura 4.14 se tiene la longitud del flujo por cada conexión. En el eje *x* está representada la longitud del flujo en bytes por cada conexión y en el eje *y*, la frecuencia de cada una de estas longitudes. Se puede observar que para una longitud del flujo menor a los 1000 bytes, tiene una alta frecuencia de ocurrencia demostrando nuevamente que el volumen de datos manejado por los usuarios es bajo.

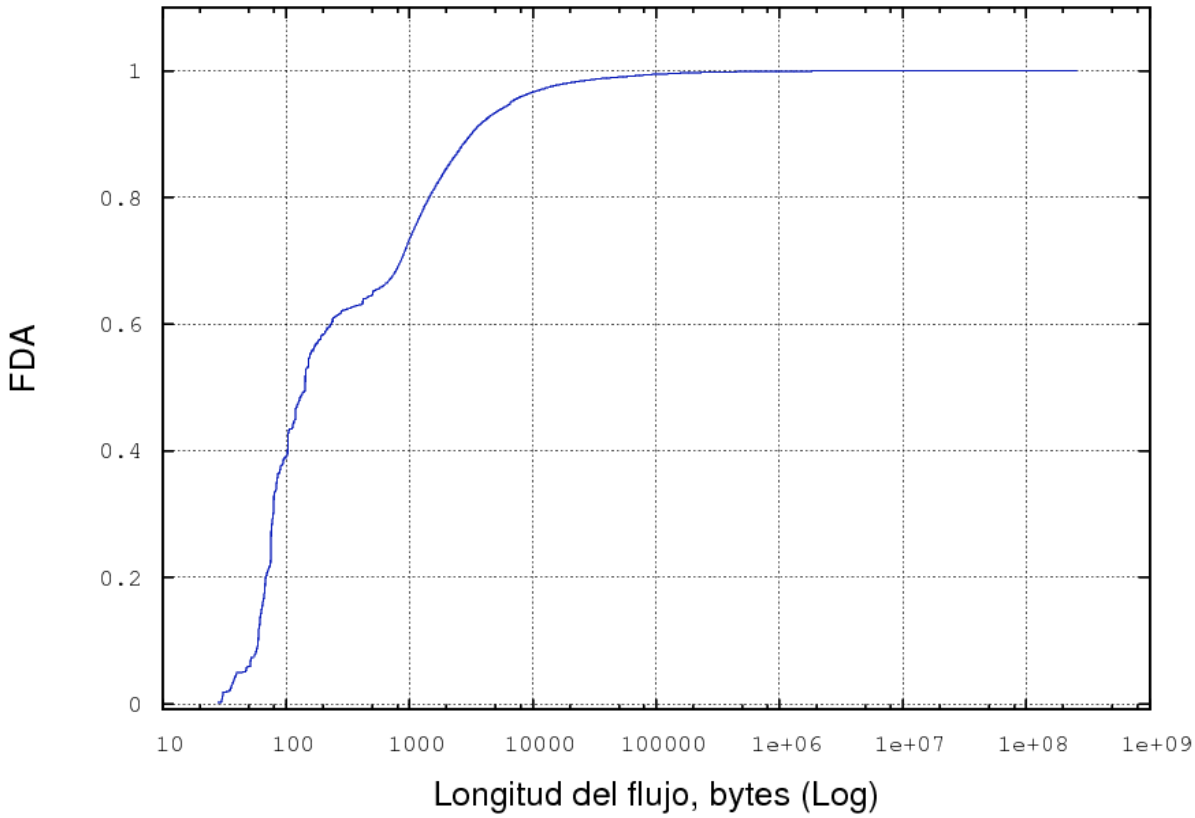

Figura 4.15: FDA de la distribución de la longitud de flujo

La FDA para la longitud del flujo muestra que el 80% del volumen de datos tiene un peso alrededor de los 1000 bytes tal como lo muestra la Figura 4.15.

El estudio estadístico arroja una media del volumen de datos de 144 bytes y un 75% del volumen, tiene un peso menor de aproximadamente 1089 bytes (Tabla 4.8).

Media	**Min.**	**Max.**	**Mediana** (Q2)	**Cuartiles**		
				Q1 25%	**Q2** 50%	**Q3** 75%
3951,714	28	257428864	144	76	144	1089

Tabla 4.8: Estudio estadístico de la longitud del flujo

Los datos estadísticos obtenidos fueron descargados en un archivo de texto para realizar la gráfica *boxplot* con la herramienta *Gnuplot*.

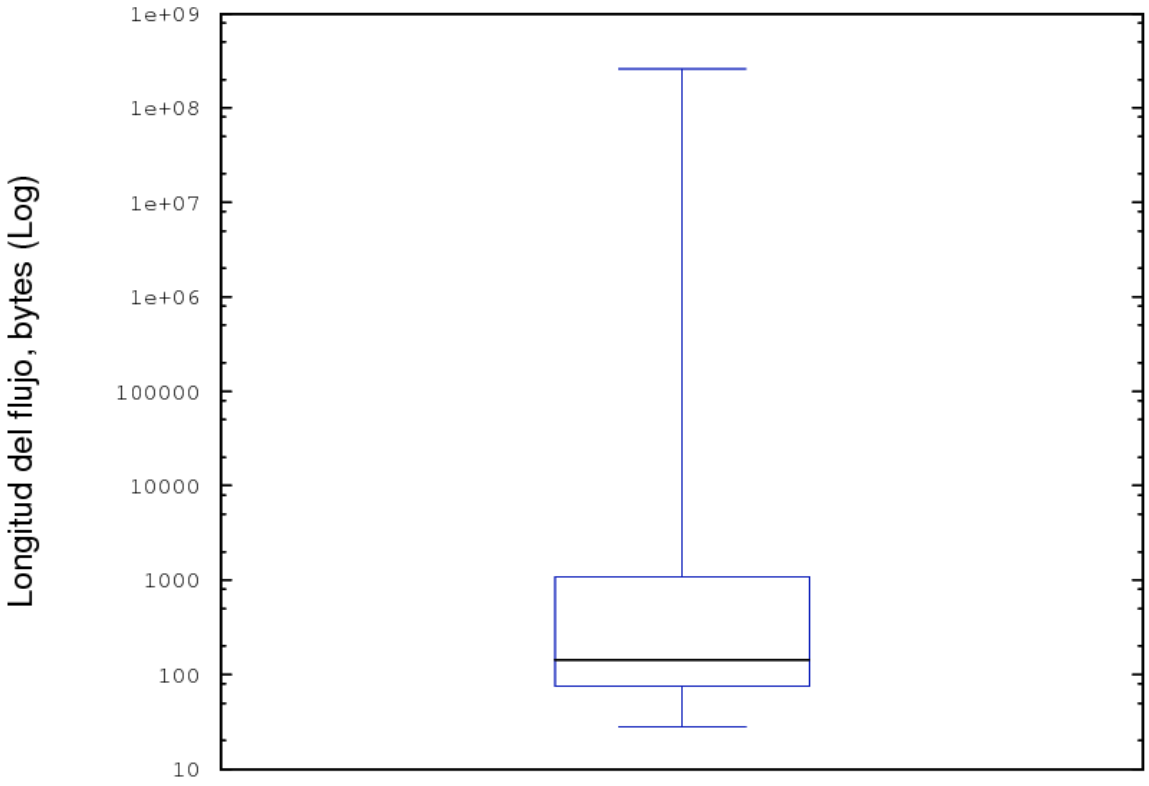

Figura 4.16: Boxplot de la longitud del flujo, bytes

En la Figura 4.16 se tienen que la longitud del flujo suele ser menor a los 1000 bytes por conexión.

En la Figura 4.13 donde se tiene la gráfica del volumen de datos para el total de conexiones entre cada par de IP, muestra que el 75% del volumen es menor a 10000 bytes.

Una vez obtenida la longitud del flujo en bytes, resulta sencillo realizar el estudio de la longitud del flujo en segundos para conocer cuánto tiempo se lleva el transmitir los datos entre cada uno de los pares de IP.

Para realizar este análisis, se usó nuevamente el archivo obtenido con *crl_flow*. Este archivo tiene el tiempo de inicio y final de la conexión. Al realizar la resta de los tiempos, se obtiene la duración del flujo por cada conexión. Muchos flujos tienen una duración de 0 segundos y fue necesario eliminarlos del estudio. También fue necesario truncar los decimales a 2 unidades para realizar el conteo de la frecuencia ya que de no hacerlo, era difícil obtener flujos con la misma duración en milésimas de segundo.

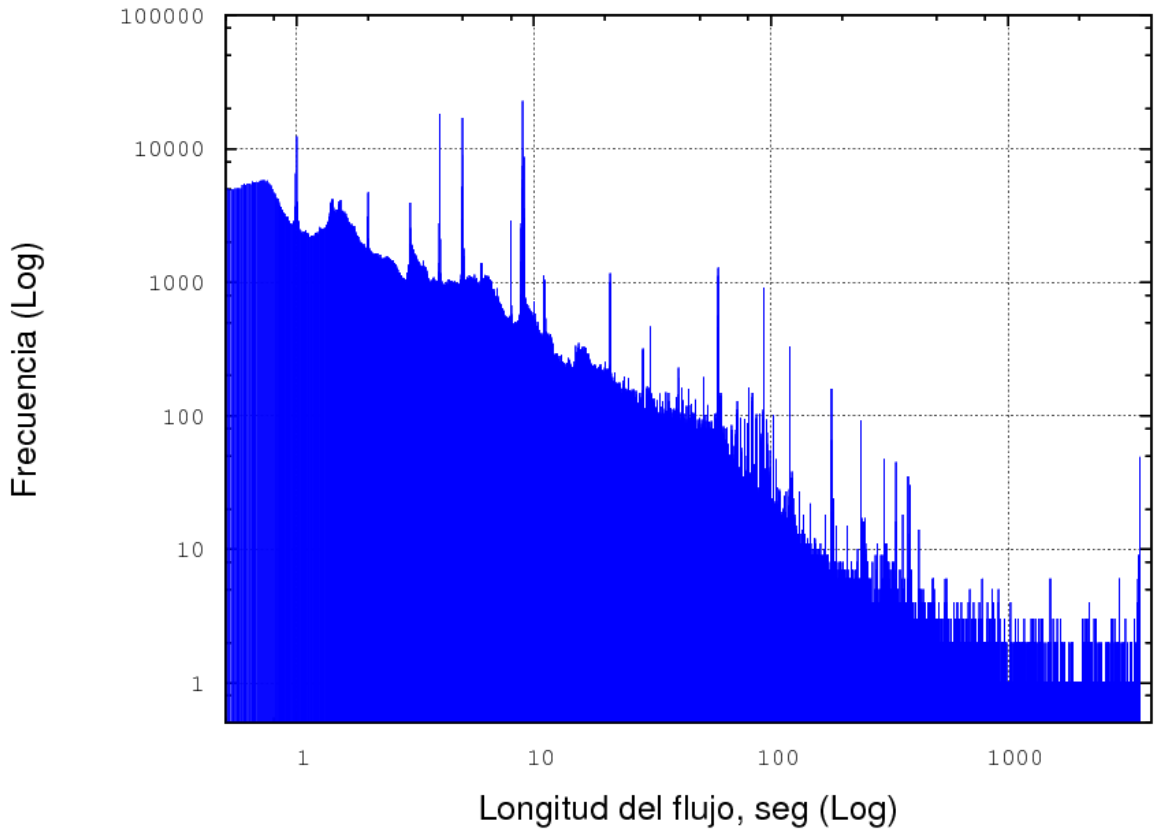

Figura 4.17: Longitud del tráfico por conexión

El resultado obtenido se puede ver en la Figura 4.17. La mayoría de los flujos tienen una duración menor a los 10 segundos y muy pocos, una duración superior a 1000 segundos.

En este punto se puede concluir que los usuarios realizan conexiones que tienen un bajo volumen de datos y un tiempo bajo de duración.

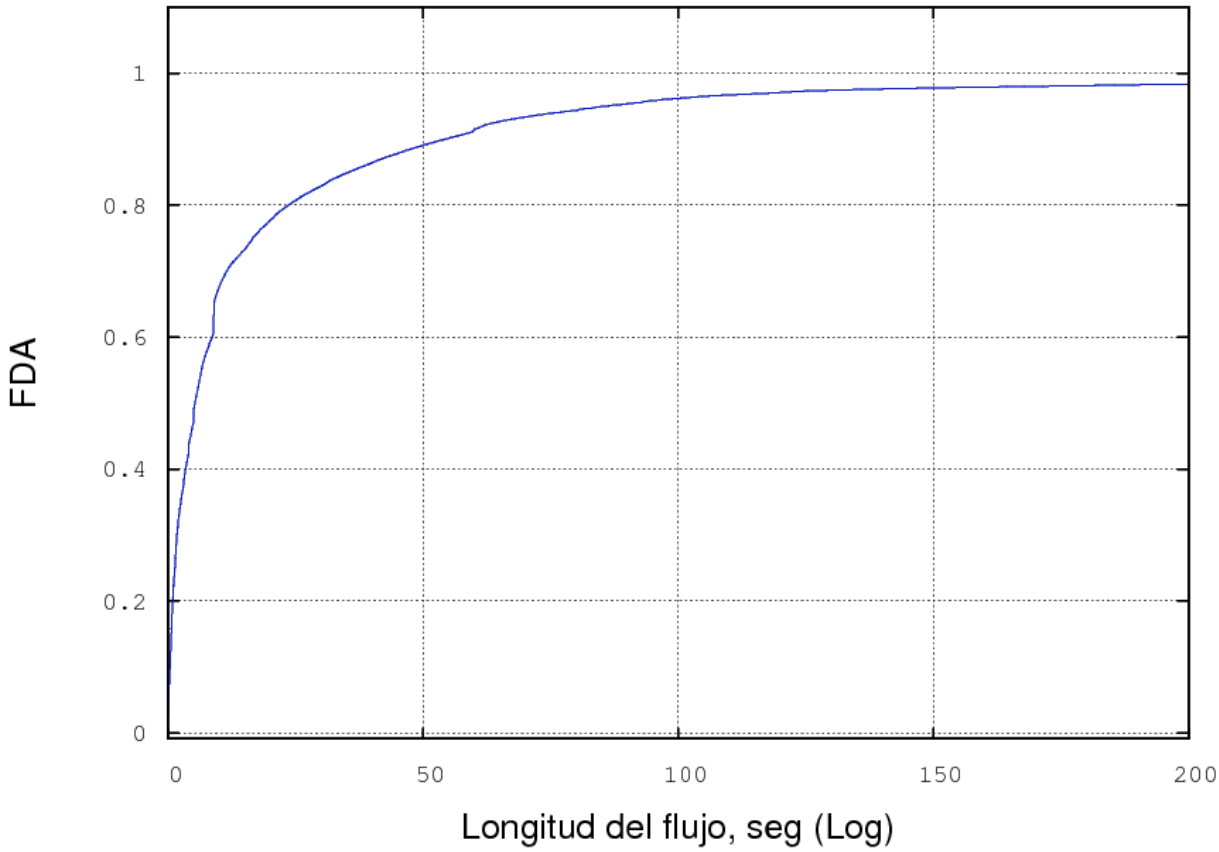

Figura 4.18: FDA de la longitud del tráfico por conexión

La FDA de la longitud del flujo en segundos representada en la Figura 4.18, tiene en su eje *x* la longitud del flujo en segundos y en el eje *y*, la función de distribución acumulada de la longitud.

El resultado del estudio estadístico de la longitud del flujo por conexión se puede observar en la Tabla 4.9.

Media	**Min.**	**Max.**	**Mediana** (Q2)	**Cuartiles**		
				Q1 25%	**Q2** 50%	**Q3** 75%
26,60409	0,01	3599,98	5,63	1,51	5,63	17,39

Tabla 4.9: Estudio estadístico de la longitud del flujo por conexión

La mediana de la longitud del flujo en segundos es de 5,63 segundos por conexión. Estos tiempos se graficaron en el *boxplot* de la Figura 4.19.

El 75% de las conexiones, tienen una duración menor a los 17 segundos y un promedio de 5 segundos de duración por conexión.

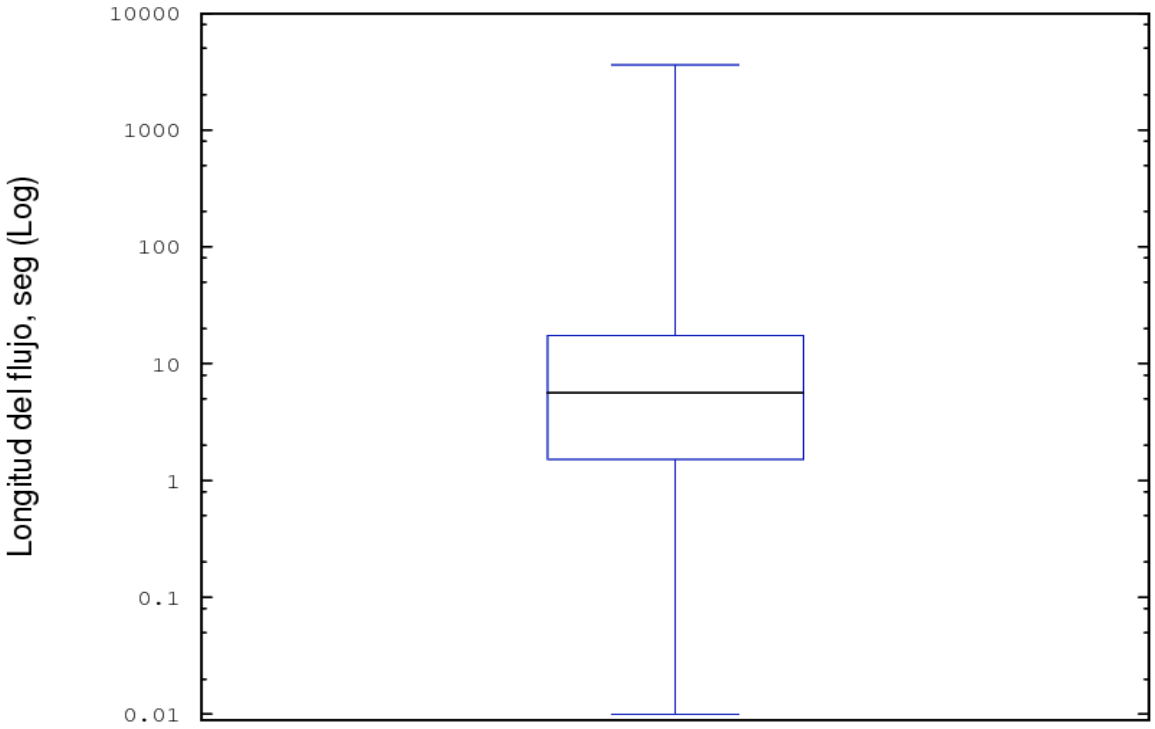

Figura 4.19: Boxplot de la longitud del flujo en seg.

4.6.3 Rendimiento del flujo

El rendimiento de un flujo se obtiene al dividir el tamaño del flujo en bytes, entre la duración del mismo. Al igual que para el estudio de la longitud del flujo, fue necesario tomar en cuenta sólo aquellos tiempos superiores a 0 segundos y tomar los resultados con sólo 2 decimales.

En la Figura 4.20 se tiene en el eje *x* el volumen de datos y en el eje *y*, la frecuencia del rendimiento para ese volumen de datos.

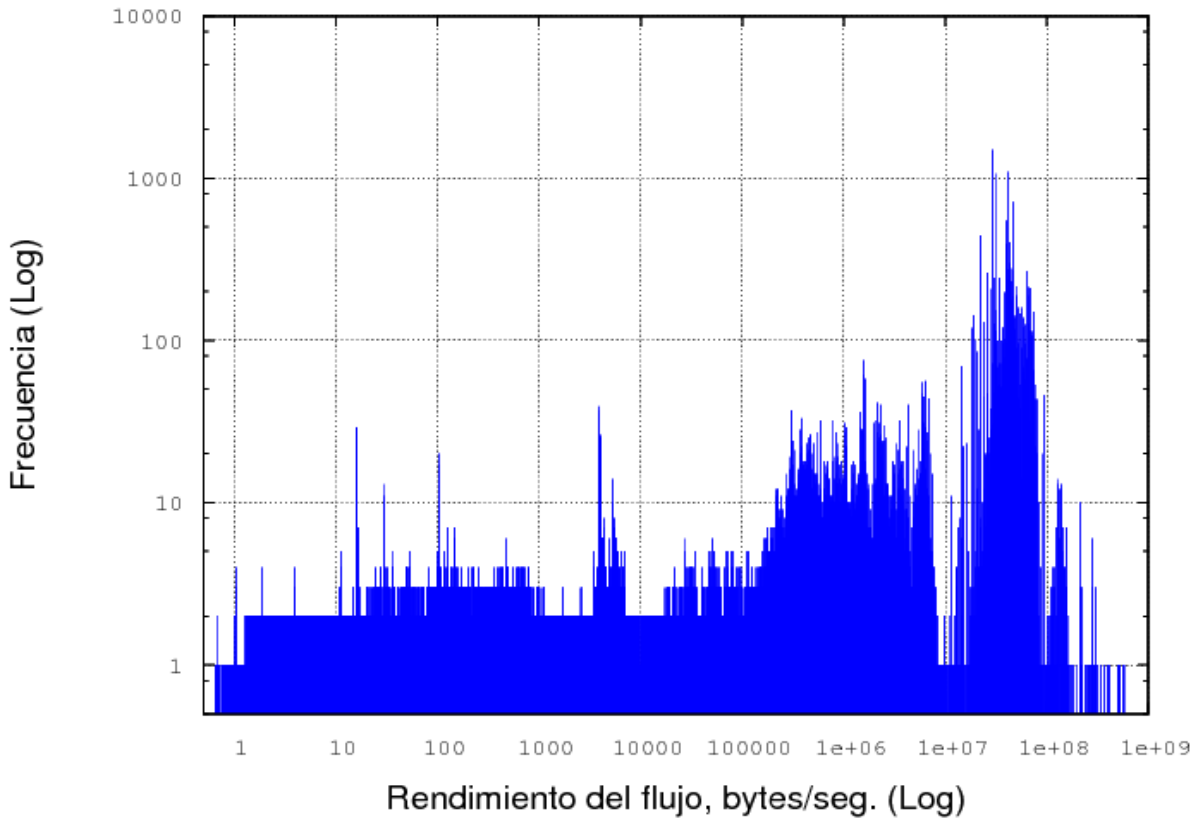

Figura 4.20: Rendimiento del flujo

Se intuye que el usuario experimenta una percepción de cambio brusco en la velocidad en la red. Al observar los datos se ve que la probabilidad de encontrar un rendimiento de 8 bps es igual a la probabilidad de encontrar un rendimiento de 800 Kbps.

Se observa que no se tiene un patrón claro de la frecuencia de aparición del rendimiento para el volumen de datos aunque pareciera ser que para volumen de datos altos, su rendimiento tiene mayor frecuencia.

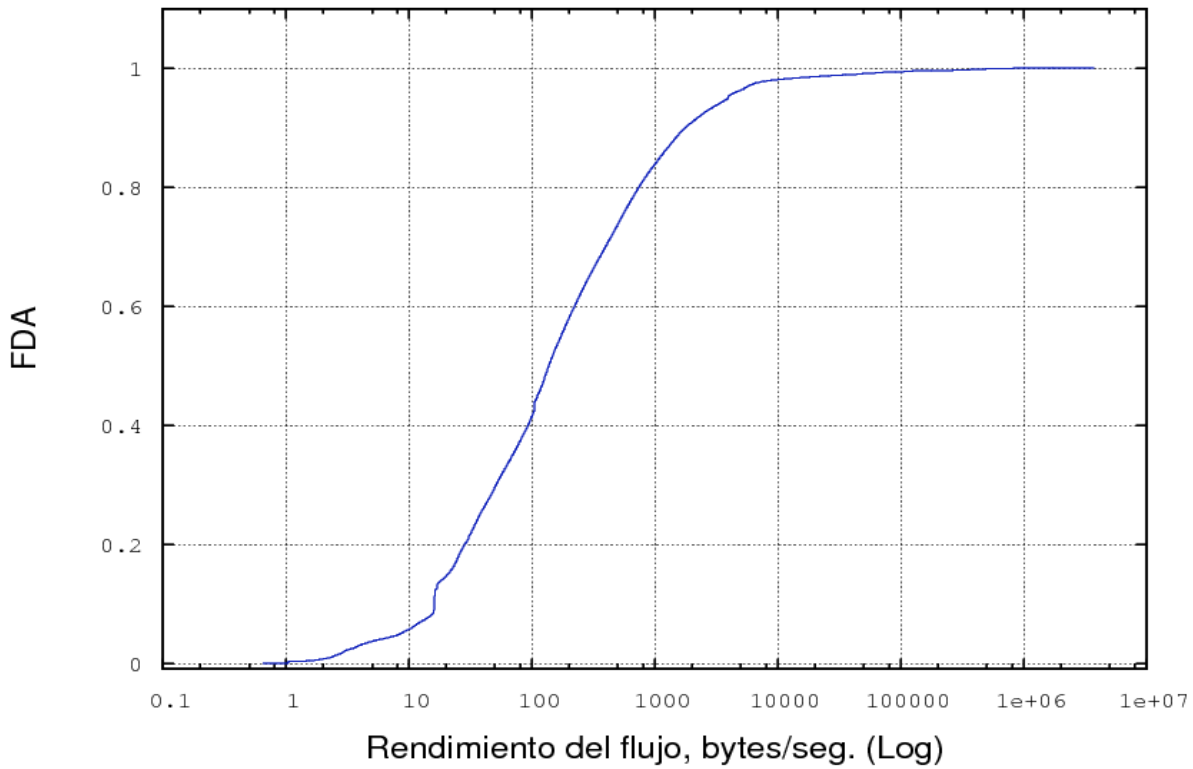

Figura 4.21: FDA del rendimiento del flujo

La Figura 4.21 de la FDA del rendimiento del flujo muestra que alrededor del 80% de los flujos tienen un rendimiento igual o menor a 1000 bytes/seg.

El resultado del estudio estadístico del rendimiento del flujo se encuentra en la Tabla 4.10.

Media	**Min.**	**Max.**	**Mediana** (Q2)	**Cuartiles**		
				Q1 25%	**Q2** 50%	**Q3** 75%
1542,048	0,65	1338000	135,02	37,14	135,02	520

Tabla 4.10: Estudio estadístico del rendimiento del flujo

Se tiene que el 75% del flujo de datos, tiene un rendimiento de 520 bytes/seg tal y como lo demuestra las Figuras 4.21 y 4.22.

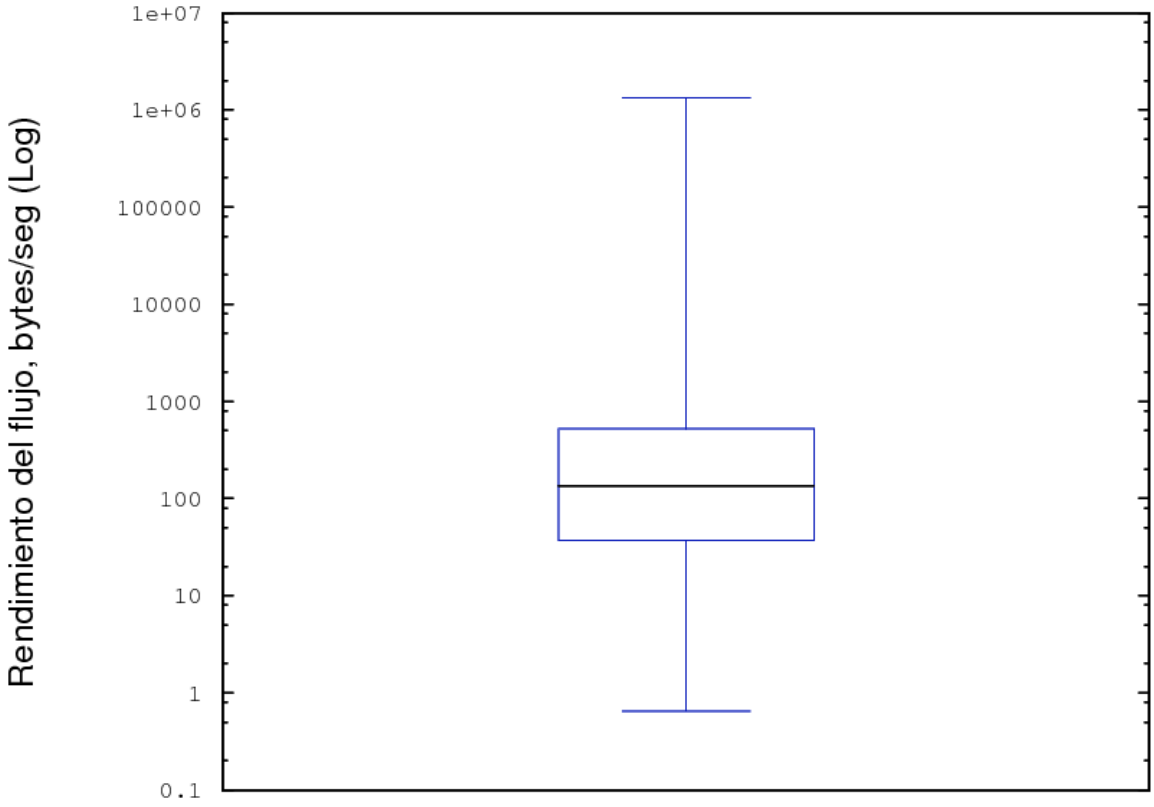

Figura 4.22: Boxplot del rendimiento del flujo

4.7 QoS

A través del estudio realizado, se pudo determinar que sigue existiendo tráfico ARP en el nodo de FCT y también se determinó que el origen de este tráfico corresponde a el nodo NBO y principalmente al APM (Tabla 4.2).

Este tráfico ARP puede deberse a problemas con las tablas cache ARP, algún gusano que esté causando daño o simplemente a la configuración que los equipos tienen actualmente.

Evaluando la configuración actual de los equipos pertenecientes a los nodos que causan problemas, se tiene que el nodo de NBO no pertenece a ninguna VLAN y su configuración es un enrutamiento sencillo con su puerta de enlace en FCT. Esta podría ser la razón del tráfico ARP de NBO visto en FCT.

Para eliminar este tráfico sería conveniente crear una VLAN para este nodo así como lo tienen los otros nodos de la red donde el equipo *Mikrotik* se encarga de filtrar los paquetes provenientes de los AP y de otros enlaces.

La configuración del APM en AGD, al igual que en NBO, no tiene el tráfico asignado a una VLAN. Este tráfico llega al CMM, representado en la Figura 3.3, y es replicado hacia el *Mikrotik*, switch, FCT y AGD causando el 96,52% del tráfico ARP observado en FCT. Para eliminar este tráfico, se puede crear una VLAN que contenga todo el tráfico generado por APM y dirigirlo hacia el MK-AGD para que realice el filtrado de paquetes.

Capítulo 5

Conclusiones y recomendaciones

5.1 Conclusiones

Después de realizar el análisis a la red de Fundacite Mérida, se ha podido determinar el perfil de tráfico de la red, sus necesidades y posibles soluciones para mejorar el consumo de ancho de banda.

Entre los resultados obtenidos se ha podido determinar que el mayor consumo de red corresponde a aplicaciones que usan el protocolo HTTP y HTTPS y que los paquetes transmitidos por los usuarios suelen ser de tamaño pequeño.

Otra de las características halladas en la red, es que los usuarios realizan conexiones hacia un destino que suele no repetirse con mucha frecuencia, es decir, un mismo usuario pocas veces repite la conexión hacia el mismo destino.

El estudio del perfil de tráfico también demuestra las horas de alto consumo de red se da entre las 10am y 12am y entre las 2pm y 4pm por lo que se puede tomar esto en cuenta para aplicar reglas de QoS que limiten las tasas de descarga dentro de estas horas de mayor consumo de red.

5.2 Recomendaciones

El estudio realizado abarca el tráfico hacia la Internet, es decir, el tráfico tanto de subida como de bajada. La velocidad del enlace no está discriminado entre subida y bajada, por lo que se recomienda separa el tráfico y realizar un estudio que permita conocer el volumen de tráfico en ambos sentidos y, de ser necesario, configurar los enlaces proporcionando mayor ancho de banda al tráfico de bajada.

Al analizar los resultados obtenidos, se determinó que existe una frecuencia alta en tráfico pequeño. Para determinar cuál es la razón, se propone realizar un estudio especial en este punto ya que esto podría estar afectando seriamente el consumo de ancho de banda.

El tráfico ARP generado por APM se podría solucionar configurando una VLAN para estos AP no sin antes realizar un estudio que permita determinar hasta qué punto se está pasando el tráfico.

Otra posible solución sería cambiar la topología física en la AGD para que el tráfico proveniente de los APM sean filtrados por el *Mikrotik* y no se envié paquetes ARP a FCT y posiblemente, hacia otros puntos de la red. Con esto se estaría mejorando la QoS en el enlace al disminuir el consumo de ancho de banda.

Para eliminar el tráfico ARP generado por NBO, se propone configurar una VLAN que enrute el tráfico en NBO o también configurar el enrutamiento para que la puerta de enlace esté en el siguiente salto y no en FCT.

Bibliografía

[1] Dye, M., Rufi, A. y McDonald, R. (2008). *Aspectos básicos de networking: Guía de estudio de CCNA Exploration.* Madrid: Pearson Educación C.A.

[2] Fundacite Mérida. Organización, organigrama. Recuperado el 7 de Mayo del 2011 de http://www.Fundacite-merida.gob.ve/drupal/?q=node/92

[3] García, A. y Widjaja, I. (2002). *Redes de comunicación: Conceptos fundamentales y arquitecturas básicas*. Madrid: McGRAW-HILL.

[4] Jiménez Gladys y Pazmiño Carlos (2009), Escuela Politécnica Nacional. Quito, Ecuador. “Análisis, implementación y evaluación de un prototipo *router* dual IPv4/IPv6 con soporte de QoS e IPsec sobre linux, usando AHP para la selección del hardware e IEEE 830 para la selección del software”

[5] Nechaev, B. (2009) S-38.3184 Assignment: From Traffic Measurements to Conclusions. Recuperado el 20 de enero del 2012 de http://www.hiit.fi/~nechaev/

[6] Quiroz Alberto (2011), Universidad Nacional Experimental de Táchira (UNET). “Actualización del esquema de enrutamiento y direccionamiento IP de

la red inalámbrica de Fundacite Mérida en la zona panamericana y Valle de Mocoties del Estado Mérida"

[7] Randall, J. y Charles, T. (1979). *Software Engineering*. New Jersey: Prentice Hall.

[8] WILAC. Topología de redes inalámbricas y estándar 802.11. Recuperado el 12 de Julio del 2011 de http://www.wilac.net/index_pdf.html

Anexos

A.1 Glosario

AP

Punto de acceso (AP). Dispositivo para crear una red y dar servicio de red inalámbrico a los clientes.

ARP

Protocolo de Resolución de Direcciones (ARP). Protocolo de capa Internet usado para obtener, a partir de la dirección lógica, la dirección física de una tarjeta de interfaz de red.

BH

BackHaul (BH). Equipo *Canopy* de *Motorola* para realizar enlaces punto a punto en redes a altas velocidades. Proporciona un ancho de banda de 20 Mbps y un alcance de hasta 58 Km.

Canopy

Productos de *Motorola* para redes inalámbricas punto a punto y multipunto.

CMM

Modulo de administración de clústeres (CMM). Caja de sincronismo para el suministro de energía. Está formado por una Antena de Posicionamiento Global

(GPS) y un switch no administrable, una fuente de alimentación a través de Ethernet (PoE) y conectores para los AP y los BH.

DMZ

Zona desmilitarizada o red perimetral (Demilitarized zone). Conectado a dos cortafuegos que enlazan, uno a la red interna y otro a la red externa.

Enlaces E1

Conexión de dos pares de cobre. 32 líneas E0 de 64 Kb cada una (2 Mbps ó 2048 Kb).

Frame Relay

Servicio de comunicación de datos a velocidades altas: 64kbps a 2Mbps.

HTTP

Protocolo de transferencia de hipertexto (HTTP). Protocolo de transferencia de hipertexto perteneciente a la capa aplicación.

HTTPS

Protocolo seguro de transferencia de hipertexto (HTTPS). Protocolo seguro de transferencia de hipertexto. Perteneciente a la capa aplicación y está basado en el protocolo HTTP y protocolos criptográficos para dar mayor seguridad en las conexiones.

Mikrotik

Equipos de comunicación inalámbrica como los routers (routerboards) y el sistema operativo *Mikrotik* RouterOS, vendidos por la compañía *MikrotikIs* LTD conocida como *Mikrotik*.

NAT

Traducción de dirección de red (NAT). Traductor para intercambiar paquetes entre redes con direcciones IP incompatibles. Mas comúnmente usado para acceder a la Internet a través de direcciones IP privadas.

P2P

Red punto a punto (P2P). Red de computadoras punto a punto que se comportan como clientes y como servidores a la vez, permitiendo la transferencia de archivos directa entre los usuarios interconectados.

Pair Gain

Convertidor de medios, convierte de serial a par de cobre. Multiplicador de pares de cobre que combina señales independientes en una sola para luego ser demultiplexada.

pfSense

Es una distribución de BSD (Berkeley Software Distribution) código abierto usada como firewall, router, NAT, entre otros.

QoS

Calidad de servicio (QoS). Conjunto de parámetros que sirven de medida para determinar la QoS de una red o la QoS ofrecida por un proveedor. Estos parámetros son: Disponibilidad, ancho de banda, pérdida de paquetes, retardo de ida y vuelta (RTT) y jitter.

SM

Módulo suscriptor (SM). Módulo suscriptor *Canopy* de *Motorola*, instalado en el cliente para escanear frecuencias disponibles y conectarse a un AP de *Motorola*.

TCP

Protocolo de control de transporte (TCP). Protocolo perteneciente a la capa transporte que garantiza la entrega de datos de extremo a extremo, sin errores y en el mismo orden en que fueron enviados.

UDP

Protocolo de datagramas de usuario (UDP). Protocolo mínimo de capa transporte no orientado a conexión que, a diferencia del TCP, no garantiza la entrega de los datos.

VLAN

Virtual LAN (VLAN). Es una red de área local virtual usada para segmentar las redes de una forma lógica y reducir el dominio de *broadcast*.

A.2 Instalación de aplicaciones

Las aplicaciones usadas para la realización del proyecto fueron herramientas y aplicaciones de uso libre y que funcionaban sobre la plataforma *GNU/Lunux* en la distribución de *Ubuntu 10.04*.

Para la realización de gráficos se usó la herramienta *Dia* y su instalación desde la línea de comando de *Ubuntu* se realizó de la siguiente forma:

$ sudo aptitude install dia

Una vez instalado, se puede acceder a la aplicación a través del menú de *Aplicaciones*.

Para la instalación de *Tcpdump* y *Tcpstat* se realizó:

$ sudo aptitude install tcpdump

$ sudo aptitude install tcpstat

Para la instalación de la herramienta *CoralReef* y *crl_flow* se realizó:

Se descargó la herramienta en http://www.caida.org/tools/measurement/coralreef/

Una vez descargada, se debe in a la carpeta *coralreef* y ejecutar los siguientes comandos:

$ ./configure

$ make

 # make install

Para ejecutar *crl_flow*, se debe copiar el ejecutable de la aplicación *crl_flow* en la carpeta donde se encuentran los archivos .pcap.

Awk es un lenguaje de programación que funciona en línea de comandos y que se usa para procesar y buscar patrones dentro de un texto. Para instalar mawk que es un intérprete de *awk* ejecutamos:

$ sudo aptitude install mawk

Para obtener el estudio estadístico se uso *R* y su instalación se realizó de la siguiente forma:

$ sudo aptitude install r-base

$ sudo aptitude install r-base-dev

$ sudo aptitude install r-recommended

Los gráficos fueron realizados con *Gnuplot* y su instalación se realizó con el siguiente comando:

$ sudo aptitude install gnuplot

A.3 Captura de datos

Para realizar la captura de datos con *Tcpdump* se configuró la computadora para que prendiera sola en caso de que se apagara de erróneamente. También se configuró c*rontab* que se encuentra dentro de /etc para que ejecutara el comando de

Tcpdump a una hora determinada.

 # tcpdump -n -i eth0 - G 3600 -w /home/fundacite/'fct_%Y-%m-%d_%H.pcap'

Donde:

-n: No resuelve nombres de las IP

-i eth0: Indica la interfaz de captura

- G 3600: La captura se almacenará en un archivo cada hora

- w: Realizar la operación de almacenar en el archivo indicado.

La cadena %Y-%m-%d_%H es sustituida por la fecha y hora del inicio de la hora de medición.

A.4 Comandos para el estudio del tráfico

Para obtener la cantidad de paquetes TCP, UDP, ICMP y ARP se debe ejecutar los siguientes comandos para cada archivo.

$ tcpstat -o "%T\n" -r fct_2012-01-31_09.pcap 3600 >> tcp.data

$ tcpstat -o "%U\n" -r fct_2012-01-31_09.pcap 3600 >> udp.data

$ tcpstat -o "%A\n" -r fct_2012-01-31_09.pcap 3600 >> arp.data

$ tcpstat -o "%C\n" -r fct_2012-01-31_09.pcap 3600 >> icmp.data

Para facilitar la tarea, se creo un *script* en *Python* para que ejecutara los comandos para cada uno de los 100 archivos obtenidos en la captura de tráfico.

El comando usado en cada uno de los archivos pcap para obtener el resumen de datos en extensión t2 fue el siguiente:

$ ./crl_flow -o fct_2012-01-31_09.t2 -Tf60 -Ci=0 -cl fct_2012-01-31_09.pcap

La información obtenida se muestra en el siguiente orden: IP origen, IP destino, protocolo, estados del flujo, puerto origen, puerto destino, cantidad de paquetes enviados en el flujo, cantidad de bytes enviados desde el origen hacia el destino, tiempo de inicio y fin del flujo.

Se ejecutó *awk* para obtener un archivo con sólo los datos requeridos para el análisis del perfil de tráfico y descartando los restantes.

Un ejemplo del comando usado es el siguiente:

*$ awk '/#/{next}{print $1,$2,$7,$8,$9}' *.t2 > flujoPar.dat*

Con este comando se extrae sólo las columnas que contiene las direcciones IP origen y destino, el total de paquetes, bytes transmitidos en cada flujo y el total de flujos en cada conexión

Para obtener los datos estadísticos con *R* del volumen de datos, por ejemplo, se realizó lo siguiente:

$ R

> volumen ← read.table(“volumen.dat”)

> mean (volumen)

> mediam (volumen [,1])

> p25 = quantile (volumen [,1], .25)

> p75 = quantile (volumen [,1], .75)

> min (volumen [,1])

> max (volumen [,1])

Para la realización de las gráficas con *Gnuplot* se generó pequeños *script* que ejecutara las líneas de comando necesarias para la realización de las gráficas.

Algunas de las líneas de comando necesarias serían:

set title 'Pares Origen-Destino'

set xlabel "Volumen de datos, bytes (Log)"

set ylabel "Frecuencia (Log)"

plot "volumenDatos.dat" w boxes lc rgb "blue" notitle

A.5 Script Python

En este punto se tiene uno de los *script* usados en el desarrollo de este proyecto.

El siguiente *script* fue usados para obtener la frecuencia de uso de los puertos.

```
import re
import os
from operator import itemgetter

archivos = os.popen('ls *.txt').read().strip().split('\n')
errores = []
puertos_conocidos = {}
puertos_registrados = {}
puertos_dinamicos = {}

for a in archivos:
```

```
      f = open(a,'r')
      lineas = f.readlines()
           patron  =  re.compile('.*?  IP  \d+?\.\d+?\.\d+?\.\d+?\.\d+?  >
(\d+?\.\d+?\.\d+?\.\d+?\.\d+?:).*')
          for i in range(len(lineas)):
          try:
              g = patron.match(lineas[i]).groups()
              puerto = g[0][:-1].split('.')[-1]
              if int(puerto) < 1024:
                  try:
                      puertos_conocidos[puerto]+=1
                  except KeyError:
                      puertos_conocidos[puerto]=1
              elif int(puerto) < 49152:
                  try:
                      puertos_registrados[puerto]+=1
                  except KeyError:
                      puertos_registrados[puerto]=1
         else:
                  try:
                      puertos_dinamicos[puerto]+=1
                  except KeyError:
                      puertos_dinamicos[puerto]=1
          except AttributeError:
              errores.append(i)

  # PUERTOS  BIEN CONOCIDOS
  items = puertos_conocidos.items()
  items.sort(key = itemgetter(1), reverse=True)
  print "Puertos conocidos: "
  total_conocidos = 0
  for i in range(len(items)):
      total_conocidos+=items[i][1]
      if i < 10:
          print items[i][0],items[i][1]

  print "TOTAL CONOCIDOS: %s" % total_conocidos

  # PUERTOS REGISTRADOS
  items = puertos_registrados.items()
  items.sort(key = itemgetter(1), reverse=True)
  print "Puertos registrados: "
  total_registrados = 0
  for i in range(len(items)):
      total_registrados+=items[i][1]
      if i < 10:
          print items[i][0],items[i][1]

  print "TOTAL REGISTRADOS: %s" % total_registrados

  # PUERTOS DINAMICOS O PRIVADOS
  items = puertos_dinamicos.items()
  items.sort(key = itemgetter(1), reverse=True)
```

```
print "Puertos dinamicos: "
total_dinamicos = 0
for i in range(len(items)):
    total_dinamicos+=items[i][1]
    if i < 10:
        print items[i][0],items[i][1]

print "TOTAL DINAMICOS: %s" % total_dinamicos
```

Parte de la salida obtenida:

Puertos conocidos:
Puerto Frecuencia
80 36271735
443 5314829
53 1600733
123 686915
445 161012
22 156747
25 82725
993 30446
995 16867
843 8205
TOTAL CONOCIDOS: 44355287

A partir de esta salida, se obtuvo el porcentaje de uso de los puertos para cada uno de los grupos.

A.6 Script Gnuplot

Un ejemplo de un *script* de *Gnuplot* es el que se generó para obtener la gráfica de la Figura 4.5 donde se tiene volumen de datos el promedio. Este *script* se muestra a continuación:

```
set grid
set output 'promedioVolumenSemMB.eps'
set encoding iso_8859_1
set terminal postscript color eps enhanced 20
```

```
set style fill solid 0.50
set style data histogram
set xrange [0: ]
set yrange [0:550]
set grid xtics
set xtics("M-12h" 3, "0h" 15, "I-12h" 27, "0h" 39, "J-12h" 51, "0h" 63,
"V-12h" 75, "0h" 87, "S-12h" 99) font "name{,14}"
set xlabel "Hora"
set grid ytics
set ytics("0" 0, "100" 100, "157.84" 157.84, "200" 200, "300" 300, "400"
400 , "500" 500, "600" 600) font "name{,14}"
set ylabel "MB/H"
plot "volumenSemMB.dat" using 2 lc rgb "#0b0b1dbb" notitle,\
     "promedioVolumenSemMB.data" w l lc rgb "#00000000" notitle
```