ANALISIS DE TRÁFICO EN EL ENLACE EXTERNO DE LA RED DE DATOS DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

ARMANDO GAMBOA GAMBOA
JORGE IVÁN VIDAL HERNÁNDEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2005

ANALISIS DE TRÁFICO EN EL ENLACE EXTERNO DE LA RED DE DATOS DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

ARMANDO GAMBOA GAMBOA
JORGE IVÁN VIDAL HERNÁNDEZ

Este proyecto es presentado como requisito para optar al título de Ingeniero Electrónico

Director
PHD. OSCAR GUALDRÓN GONZÁLEZ
Codirector
MI(c). LEYDI JOHANNA BARCO RINCÓN

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2005

AGRADECIMIENTOS

Los autores expresan su agradecimiento y reconocimiento a:

Nuestras familias por su apoyo incondicional.

Doctor Oscar Gualdrón González, director del proyecto y a la Ingeniera Leydi Johanna Barco codirectora del proyecto, por su orientación y colaboración.

Doctor Benjamín A. Pico Merchan y a la División de Servicios de Información, por su orientación, paciencia y confianza.

Ing. Jairo Augusto Cala, por su excelente disposición al prestarnos su colaboración.

Grupo de Investigación en Conectividad y Procesado de Señal.

La Especialización en Telecomunicaciones.

La Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones

La Universidad Industrial de Santander.

A Dios, a mis padres Jorge Elías y Ruby Marina por su paciencia, comprensión y apoyo incondicional, a mis hermanos Laura Lorena, Angélica Yaneth y Jorge Eliécer por su cariño, porque a pesar de la distancia siempre estuvieron a mi lado.

A mi preciosa ahijada Lili Marcela por inspirarme en momentos difíciles.

A Maruchita por su amor y paciencia en todo este tiempo.

Gracias a mis amigos a los que no nombro porque seria imperdonable olvidarme de alguno. Ellos me han enseñado cosas que no se aprenden en ningún aula. Quiero agradecerles todos los buenos momentos, pasados, presentes y futuros.

Y por supuesto a Goku.

Jorge Iván Vidal Hernández

A Dios

A mis Padres por su inmenso amor y apoyo incondicional.

A mi hermana Emilsen por sus palabras reconfortantes en los momentos difíciles.

A mis sobrinos Andrés, Silvia y Camilo, quienes con su inocencia me han enseñado a disfrutar más de la vida.

A todos esos grandes amigos, hermanos que la vida me ha permitido escoger y han estado conmigo en los momentos de alegría y tristeza.

A todos aquellos seres que de una u otra forma me han nutrido, dándome la fuerza necesaria para seguir en la búsqueda del fin principal de todo ser humano, EL SER PERSONA

Armando Gamboa G.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

TITULO
ANALISIS DE TRÁFICO EN EL ENLACE EXTERNO DE LA RED DE DATOS DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

AUTORES

ARMANDO GAMBOA GAMBOA
JORGE IVÁN VIDAL HERNÁNDEZ**

Palabras claves
Análisis, tráfico, enlaces, red, protocolos, paquetes

Descripción

El análisis del trafico le permite al administrador de red determinar el comportamiento, dinámica y tiempos de transición en una red de datos para poder llegar a un diagnostico sobre posibles fallas en la misma. El objetivo de este trabajo es determinar la distribución de protocolos y tamaños de paquetes en el enlace externo de la red de datos de la Universidad Industrial de Santander mediante la captura y el análisis de tráfico.

Para la realización de este proyecto se realizó un análisis del tráfico del enlace externo de la red por medio de una tarjeta de red Gigabit Ethernet conectada al switch central Cajun P880 en donde se configuró un Mirror Port; se utilizó un analizador de tráfico (Ethereal), que permitió obtener los parámetros necesarios haciendo registros de la información que viaja por la red. Estos registros son exportados a formato de texto y se procesan por medio de una aplicación desarrollada en MATLAB 7.0 con la cual se obtienen los parámetros de medición.

Entre los resultados más importantes se tiene que la mayor parte del ancho de banda del enlace esta siendo consumido por el tráfico lúdico (P2P), la utilización promedio del ancho de banda es del 65%.

* Trabajo de Grado.
** Facultad de Ingenierías Fisico-Mecánicas, Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones, Director Ph.D Oscar Gualdrón.

TITLE
TRAFFIC ANALYSIS ON THE OUTSIDE LINK OFTHE DATA NETWORK OF THE UNIVERSIDAD INDUSTRIAL DE SANTANDER *

AUTHORS

ARMANDO GAMBOA GAMBOA
JORGE IVÁN VIDAL HERNÁNDEZ**

Key words
Analysis, traffic, links, network, bandwidth

Abstract

Traffic analysis is a powerful tool that allows a network manager to determine the behavior, dynamics and transition times on a data network, those of which will be useful in a system diagnosis about possible flaws on the network. The objective of this project is to determine the protocol distribution and the size of the packages on the outside link of the data network of the Universidad Industrial de Santander, via the capture and the analysis of the traffic.

In this work, a traffic analysis of the outside link was made, using a Gigabit Ethernet card connected to the Cajun P880 central switch were a Port Mirror was configured. A traffic analyzer tool (Ethereal) help to obtain the necessary parameters via the recording of the data that travels on the net. Those registers were exported in text format and were processed by an application developed in MATLAB 7.0 in order to obtain the measurement parameters.

Among the most important results obtained was the fact that the most of the link bandwidth is occupied by peer to peer applications (P2P) which consumed about the 65% of the bandwidth.

* Work of Degree.
** Faculty of Physical-mechanical Engineerings, Electric, Electronic and Telecommunications School of Engineerings, Manager Ph.D Oscar Gualdrón.

INTRODUCCIÓN

En la actualidad, Internet se ha consolidado indiscutiblemente como la red telemática más extendida y utilizada a nivel mundial. Surgida a partir de una iniciativa del Departamento de Defensa de los Estados Unidos a finales del año 1960 y desarrollada durante sus primeras décadas de vida dentro del entorno académico proporcionado por las universidades y los centros de investigación en los últimos años ha supuesto una verdadera revolución en todos los ámbitos, no solo en el tecnológico.

El número de usuarios conectados y el ancho de banda demandado han crecido exponencialmente. Todo este crecimiento ha originado una producción de nuevos servicios y aplicaciones.

El tráfico que circula por las autopistas de la información de Internet es de naturaleza muy diversa. Es por tanto necesario conocer cómo es y cómo evoluciona, utilizando algún tipo captura y monitorización para poder realizar un dimensionamiento y mantenimiento adecuado de los recursos de red.

El análisis de tráfico se define como aquellos aspectos de red relacionados con las cuestiones de evaluación y optimización del rendimiento de las redes operacionales. El análisis de tráfico abarca la aplicación de la tecnología y los principios para la medición en una red de datos, las cuales permiten realizar mejoras del rendimiento de una red operacional, en cuanto a tráfico y niveles de recursos, siendo estos los principales objetivos del análisis de trafico de una red; esto se consigue dirigiéndose a los requerimientos del rendimiento orientado al tráfico, mientras se utilizan los recursos de la red económicamente y fiablemente.

El rendimiento de la red visto desde los usuarios de los servicios de la red es lo más importante; las características visibles a estos usuarios son las propiedades en vías de desarrollo de la red, las cuales son las características de la red viéndola como un todo.

La Universidad Industrial de Santander tiene una red de datos en permanente crecimiento, para garantizar a la comunidad universitaria unas condiciones básicas de acceso y generar un ambiente que favorezca el desarrollo investigativo, los avances académicos, no solo a nivel de la institución sino también para su entorno.

Permanecer aislado de los avances tecnológicos es limitar la capacidad creadora de la Universidad, la cual no debe ser espectadora sino protagonista de los procesos de cambio y desarrollo.

Este proyecto permitirá identificar acciones destinadas a mejorar aspectos como organización, control, administración y distribución de recursos en la red, así como agilizar labores de mejoramiento, mantenimiento y supervisión en la misma; esto se obtiene a través de registros y estadísticas finales.

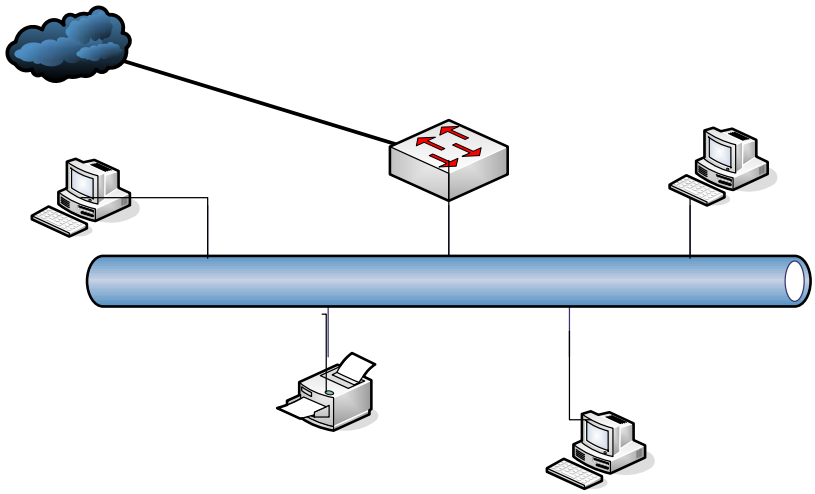
Finalmente con el proyecto también se pretende que una vez conocidas las demandas de los usuarios para los diferentes servicios/aplicaciones se planteen una serie de recomendaciones para el buen funcionamiento de la red.

1. INTRODUCCIÓN A LAS REDES DE DATOS DE ÁREA LOCAL – LAN

1.1 CONCEPTOS GENERALES

Una red LAN[1] es básicamente un medio de transmisión compartido y un conjunto de software y hardware que sirve de interfaz entre los dispositivos y el medio y al mismo tiempo regula el orden de acceso al mismo. El objetivo de estas redes es el de alcanzar altas velocidades de transmisión de datos para distancias relativamente cortas, además de conectar estaciones de trabajo, dispositivos periféricos, terminales y otros módulos que se encuentran en un solo edificio u otra área geográfica limitada. El diagrama general de una red de área local se muestra en la figura 1.

Figura 1. Diagrama general de una red LAN.



[1] Acrónimo de Local Area Network.

Al momento de implementar una red LAN, surgen distintos parámetros de diseño que afectarán las prestaciones finales de la misma. Uno de éstos es la elección del medio de transmisión, el cual puede ser un par trenzado, cable coaxial, fibra óptica o un medio inalámbrico. Otro problema es el control de acceso, ya que con un medio compartido se hace necesario implementar algún mecanismo para regular el acceso al mismo de forma eficiente y rápida; este control a su vez está relacionado con la topología que adopte la red, siendo las más usadas el anillo, la estrella y el bus.

Con base en lo anterior, se puede decir que los aspectos tecnológicos principales que determinan la naturaleza de una red LAN son:

- La topología.
- El medio de transmisión.
- La técnica de control de acceso al medio.

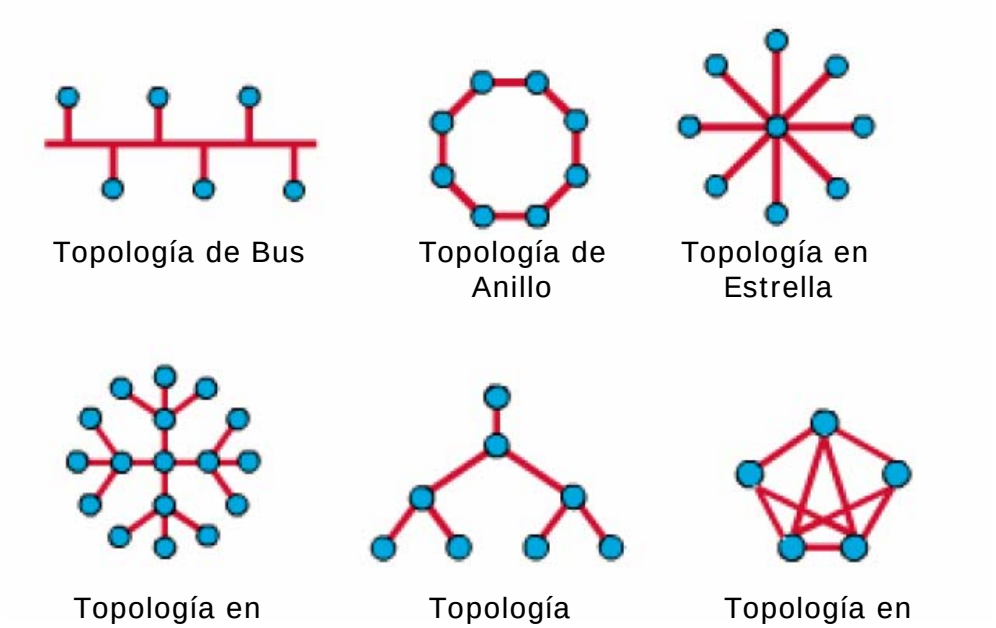
1.1.1 Topología.

La topología define la estructura de una red y se encuentra dividida en topología física, que es la disposición real de los cables (los medios) y la topología lógica, que define la forma en que los hosts[2] acceden a los medios.

Las topologías físicas que se utilizan comúnmente son las de bus, de anillo, en estrella, en estrella extendida, jerárquica y en malla. Estas topologías se indican en la figura 2 y se explican a continuación:

[2] Según el uso tradicional, se refiere al conjunto de máquinas dedicadas a ejecutar programas de usuario.

Figura 2. Topologías físicas.



- En la topología de Bus, todas las estaciones se encuentran directamente conectadas a través de interfaces físicas apropiadas conocidas como tomas de conexión, a un medio de transmisión lineal o bus.

- Para la topología de anillo, la red consta de un conjunto de repetidores unidos por enlaces punto a punto formando un lazo cerrado. Los enlaces son unidireccionales, es decir, los datos se transmiten solo en un sentido (horario o antihorario).

- En la topología en estrella, cada estación está directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, uno para transmisión y el otro para recepción. En general existen dos alternativas para el funcionamiento del nodo

central. Una es el funcionamiento en modo de difusión, en el que la transmisión de la trama por parte de una estación se transmite sobre todos los enlaces de salida del nodo central. En este caso aunque la disposición física es una estrella, funciona como un bus; una transmisión desde cualquier estación es recibida por el resto de las estaciones y solo puede transmitir una estación en un instante de tiempo dado.

La segunda aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino.

- La topología en estrella extendida se desarrolla a partir de la topología en estrella. Esta topología enlaza estrellas individuales, lo cual permite extender la longitud y el tamaño de la red.

- La topología jerárquica se desarrolla de forma similar a la topología en estrella extendida, pero en lugar de enlazar estrellas individuales, el sistema se enlaza con un computador que controla el tráfico de la red.

- La topología en malla se utiliza cuando no puede existir absolutamente ninguna interrupción en las comunicaciones. De modo que, como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Esto también se refleja en el diseño de la red mundial de datos, que tiene múltiples rutas hacia cualquier ubicación.

La topología lógica de una red, como se expresó anteriormente, se refiere a la forma en que los hosts se comunican a través del medio. Los dos

tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La topología de broadcast consiste simplemente en que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red; el primero que entra es el primero al que se sirve.

El segundo tipo es la transmisión de tokens. Esta transmisión controla el acceso a la red al transferir un token electrónico de forma secuencial a cada host. Cuando un host recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

1.1.2 Medios de transmisión.

Para la transmisión de información entre dispositivos a larga o corta distancia debe utilizarse un medio que asegure su correcta recepción en el destino.

Existen dos tipos de medios de transmisión de datos:

- **Medios guiados**, que incluyen a los cables metálicos (cobre, aluminio, etc.) y de fibra óptica. El cable se instala normalmente en el interior de los edificios o en conductos subterráneos. Los cables metálicos pueden presentar una estructura coaxial o de par trenzado, y el cobre es el material preferido como núcleo de los elementos de transmisión de las redes. El cable de fibra óptica se encuentra disponible en forma de hebras simples o múltiples de plástico o fibra de vidrio.

- **Medios no guiados**, se refieren a las técnicas de transmisión de señales a través del aire y del espacio entre transmisor y receptor (radioenlaces). La transmisión por infrarrojos y microondas cae dentro de esta categoría.

1.1.3 Control de acceso al medio[2]

Todas las redes locales consisten en una colección de dispositivos que deben compartir la capacidad de transmisión de la red. Para ello, se hace necesaria la existencia de algún método para controlar el acceso al medio de transmisión, con el objeto de evitar posibles conflictos o errores que podrían acaecerse. El protocolo de control de acceso al medio de transmisión es el factor que más caracteriza el funcionamiento de una red de área local; de el dependen los parámetros básicos del funcionamiento de la red como son el rendimiento, la confiabilidad y la gestión de la red. Dentro de los métodos de control más comunes encontramos los siguientes:

- Sondeo o Polling
- Pase de testigo (Token-Pass)
- Pase de testigo en bus (Token-Bus)
- Pase de testigo en anillo (Token-Ring)
- Acceso Múltiple con Detección de Portadora (CSMA)

1.2 TECNOLOGÍAS DE REDES LAN

Existen varias tecnologías de capa de enlace de datos disponibles para redes LAN, entre las que se encuentran Ethernet, Token Ring, Token Bus y FDDI principalmente. La mayoría de las redes recientemente instaladas utilizan Ethernet, debido a que dicha tecnología proporciona características superiores en cuanto a escalabilidad, administración,

confiabilidad y capacidad; además, es adaptable a las crecientes demandas de ancho de banda, precios bajos y calidad de servicio, aspectos que las demás tecnologías no han logrado desarrollar al mismo nivel.

Token Ring, Token Bus y FDDI también son utilizadas en redes LAN; sin embargo, éstas no han sido tan ampliamente desarrolladas debido a que son tecnologías más costosas, más susceptibles a problemas como ruido y retardos y más complejas de manejar y administrar que Ethernet. Por estas razones Ethernet ha sido aceptada en diversas áreas (industrial, comercial, científica, etc) como una de las mejores soluciones para implementación de redes LAN.

1.3 Estandar Ethernet

Ethernet es la capa física más popular de la tecnología LAN usada actualmente. La popularidad de Ethernet es debida a que permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría los usuarios de la informática actual. La norma de Ethernet fue definida por el Instituto para los Ingenieros Eléctricos y Electrónicos (IEEE) como el estándar IEEE802.3. Adhiriéndose a la norma de la IEEE, los equipos y protocolos de red pueden interoperar eficazmente.

Algunas de las principales características de Ethernet son el uso de tramas de longitud variable entre 64 y 1518 bytes y además una alta velocidad de transmisión (10 Mbps en su inicio hasta tasas de transmisión de Gbps en la actualidad); éstas y otras características han ubicado a Ethernet como la solución más masificada en la actualidad.

1.3.1. Estándares Ethernet[1]

A continuación se muestran las características de los estándares de Ethernet que se encuentran presentes en la red de datos de la Universidad Industrial de Santander. La notación con la que normalmente se designa cada uno se basa en la especificación XBaseY, cuya interpretación se aprecia en la tabla 1.

Tabla 1. Notación de estándares Ethernet

X	Este valor denota la velocidad de transmisión de datos, si X fuese 10, entonces se habla de 10 Megabits por segundo (Mbps).
Base	Esto indica que los datos se transmiten en banda base. Lo anterior significa que se usa o se envía la información tal y como se produce; es decir, no se modula en un ancho de banda específico, sino que se transmite en el ancho de banda en que llega originalmente. La razón detrás de esto es el hecho de que si se llegase a modular posiblemente se llegue a ocupar todo el ancho de banda disponible.
Y	Este número significa o denota la longitud de cada segmento. Si Y tiene un valor de 2, significa que la longitud máxima de cada segmento es de 200 metros.

10BASE-T. Este identificador significa que el sistema Ethernet opera a 10Mbps, en modo banda base, sobre dos pares de categoría 3 o superiores y el alambre es par trenzado.

100BASE-T. Este es un identificador para sistemas de entrada de 100Mbps, como lo son los sistemas *FastEthernet* de par trenzado y fibra óptica.

100BASE-TX. Es un identificador para sistemas 100BASE-TX y 100BASE- FX. El 100BASE-TX es una variedad de sistema *FastEthernet*, en modo banda base, sobre dos pares de alta calidad, utilizando cable par trenzado categoría 5 o superiores. 100BASE-TX tiene numerosas similitudes con el sistema 10BASE-T; ambos utilizan los mismos dos pares de cable UTP, el mismo conector RJ45 y la misma longitud máxima de segmento de 100m. El 100BASE-FX al igual que el anterior es un sistema de *FastEthernet* en modo banda base sobre un cable de fibra óptica que puede ser multimodo o monomodo. En la tabla 2 se ilustran algunas características de los sistemas 10BASE-T, 100BASE-T y 100BASE-X.

Tabla 2. Características Físicas Sistemas 10BASE-T, 100BASE-TX y 100BASE-FX

Parámetro	10BASE-T	100BASE-TX	100BASE-FX
Estandar IEEE	802,3	802,3u	802.3u
Codificaión	Manchester	4B/5B	4B/5B
Cableado requerido	UTP CAT. 3/4/5	UTP CAT. 5 ó STP	Fibra S.M. o M.M.
Frecuencia de la señal	20 MHz	125 MHz	125 MHz
Número de pares requerido	2	2	2
Distancia	100 m	100 m	150/412/2000 m
Capacidad Full Duplex	SI	SI	SI

1000BASE-X. Este es un identificador para sistemas Gigabit Ethernet, que incluye 1000BASE-SX, 1000BASE-LX y 1000BASE-CX. El 1000BASE-SX está definido para conexiones horizontales o *backbones* cortos. La **S** representa longitud de onda corta. Este sistema se usa solamente con fibra multimodo (MM). El 1000BASE-LX está definido para conexiones verticales o backbones largos. La **L** representa longitud de onda larga, 1000BASE-LX puede utilizar ambos, fibra monomodo (SM) o multimodo.

En la tabla 3 se ilustran algunas características de los sistemas 1000-BaseX.

Tabla 3. Características Físicas Sistemas 1000BASE-X

Parámetro	1000BASE-T	100BASE-SX	1000BASE-LX
Estandar IEEE	802.3ab	802.3z	802.3z
Codificaión	4D-PAM 5	8B/10B	8B/10B
Cableado requerido	UTP CAT. 5 ó superior	Fibra M.M.	Fibra S.M. y M.M.
Conector especificado	RJ45	S.C.(1)	S.C.
Número de pares requerido	4 pares	2 hilos	2 hilos
Distancia	100 m	220-550 m	5000m(SMF), 550m(MMF)
Capacidad Full Duplex	SI	SI	SI

1.3.2 Trama Ethernet.

El corazón del sistema Ethernet es la trama, la cual está compuesta por bits colocados en campos específicos. La descripción de la distribución de estos campos se muestra en la tabla 4.

Tabla 4. Trama Ethernet.

58 bits	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Preambulo	**Inicio de Delimitador de trama**	**Dirección Destino**	**Dirección Origen**	**Tipo**	**Datos**	**Secuencia de verificación de trama**

- Preámbulo: Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo inicio de Trama de la trama IEEE 802.3.

- Inicio de trama: Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.

- Direcciones destino y origen: Incluye las direcciones físicas (MAC)[3] únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección única, mientras que la de destino puede ser de unicast (trama enviada a una sola máquina), de multicast (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).

- Tipo (Ethernet): Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

- Longitud (IEEE 802.3): Indica la cantidad de bytes de datos que sigue este campo.

- Datos: Incluye los datos enviados en la trama. En la especificación IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama). Por su parte, las especificaciones Ethernet versión 2 no especifican ningún relleno, pero Ethernet espera por lo menos 46 bytes de datos.

[3] Acrónimo de Medium Access Control

- Secuencia de verificación de trama: Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

1.3.3 Protocolo CSMA-CD[2]

Ethernet es un medio compartido, por lo que hay reglas para enviar los paquetes para evitar conflictos y proteger la integridad de los datos. Los nodos en una red Ethernet envían paquetes cuando ellos determinan que la red no está en uso. Es posible que dos nodos en situaciones diferentes pudieran intentar enviar datos al mismo tiempo; cuando ambos nodos están transfiriendo un paquete al mismo tiempo a la red, se producirá una colisión.

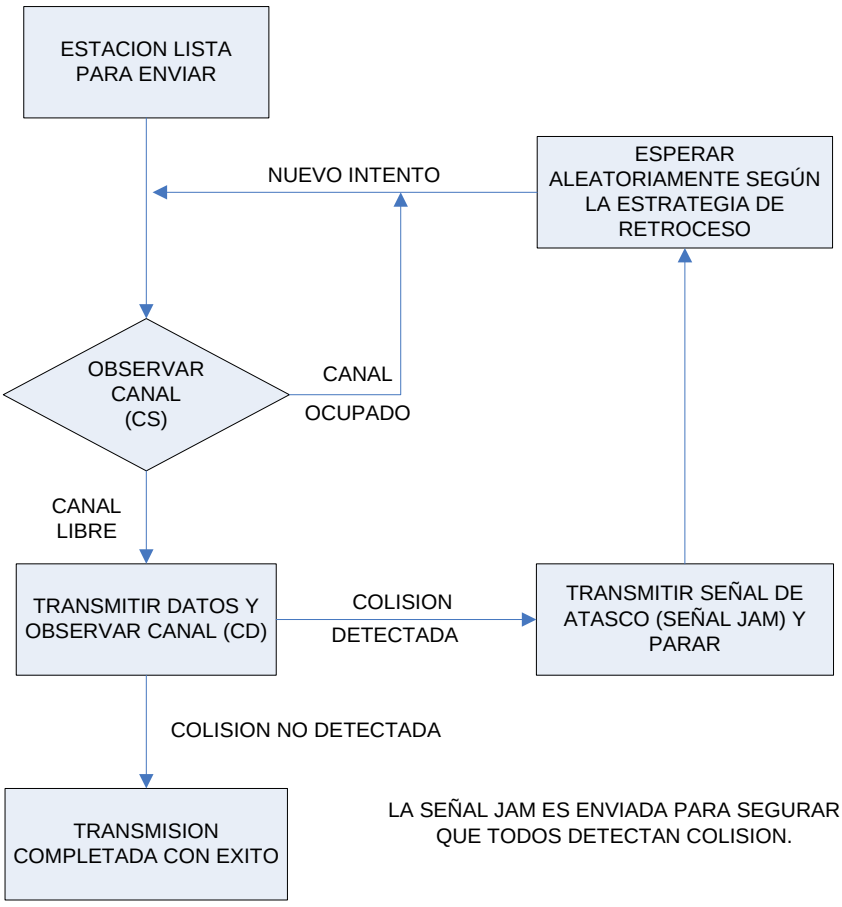
Minimizar colisiones es un elemento crucial en la planificación y funcionamiento de las redes, para esto es necesario utilizar un método de control de acceso al medio, el cuál está condicionado por la topología y estructura física que compone la red.

Ethernet busca un acceso equitativo para todas las estaciones que están ligadas al canal, para ello utiliza un protocolo de control de acceso al medio denominado **CSMA/CD** (Acceso Múltiple con Detección de Portadora y Detección de Colisión). Antes de la aparición de ésta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones; por ello apareció inicialmente la técnica CSMA que fue posteriormente refinada a la técnica CSMA/CD. En la figura 3 se describe su funcionamiento.

CSMA (*Carrier Sense Multiple Access*) significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir previamente escucha

el canal antes de realizar la emisión. Si el canal está ocupado espera un tiempo aleatorio y vuelve a escuchar. Cuando detecta libre el canal puede actuar de dos formas distintas: emitiendo de inmediato o esperando un tiempo aleatorio antes de emitir. Si emite con una probabilidad p, se dice que es un sistema CSMA p-persistente, mientras que si emite de inmediato se dice que es un sistema CSMA 1-persistente. Una vez comienza a emitir, no para hasta terminar de emitir la trama completa. Esto supone que se puede producir una colisión si dos estaciones intentan transmitir a la vez, de forma que las tramas emitidas por ambas serán incompresibles para las otras estaciones y la transmisión habrá sido infructuosa.

Figura 3. Funcionamiento del CSMA/CD



Finalmente CSMA/CD supone una mejora sobre CSMA, pues la estación se encuentra escuchando a la vez que emite, de forma que si detecta que se produce una colisión, detiene inmediatamente la transmisión.

La principal ventaja consiste entonces en la ganancia de tiempo, ya que no se continúa utilizando el medio para realizar una transmisión que resultará inútil, y que se podrá utilizar por otra estación para transmitir.

1.3.4 Ethernet dentro del modelo OSI-TCP/IP[4]

Es importante mencionar el modelo OSI debido a que se encuentra totalmente estandarizado, y aun cuando su estructura no se sigue rigurosamente, ha sido punto de partida fundamental en el desarrollo de *hardware* y *software* asociado a redes Ethernet. El sistema de comunicaciones del modelo OSI estructura el proceso en varias capas que interaccionan entre sí; una capa proporciona servicios a la capa superior siguiente y toma los servicios que le presta la precedente capa inferior. El modelo OSI como una referencia académica describe siete capas de funciones de red, como se muestra en la figura 4 y que se describen a continuación.

Figura 4. Modelo OSI.

APLICACIONES DE USUARIO	
Capa 7.	Aplicación
Capa 6.	Presentación
Capa 5.	Sesión
Capa 4.	Transporte
Capa 3.	Red
Capa 2.	Enlace de Datos
Capa 1.	Física
MEDIO DE TRANSMISIÓN	

[4] Acrónimo de Transport Control Protocol/Internet Protocol

- Capa física: se encarga del envío de bits al medio físico y de suministrar servicios a la siguiente capa. Para ello debe conocer las características mecánicas, eléctricas, funcionales y de procedimiento de las líneas.

- Capa de enlace de datos: esta capa debe encargarse de que el envío de datos se realice con seguridad a su destino y libre de errores. Cuando la conexión no es punto a punto, esta capa no puede asegurar su cometido y es la capa superior quien lo debe hacer.

- Capa de red: esta capa se encarga de enlazar con la red y de encaminar los datos hacia sus lugares o direcciones de destino. Para esto, se produce un diálogo con la red para establecer prioridades y encaminamientos. Ésta capa y las dos capas anteriores son las encargadas de todo el proceso externo al propio sistema y que están tanto en terminales como en enlaces o repetidores.

- Capa de transporte: esta capa se encarga de que los datos enviados y recibidos lleguen en orden, sin duplicar y sin errores. Puede ser servicio de transporte orientado a conexión (conmutación de circuitos o circuitos virtuales) o no orientado a conexión (datagramas).

- Capa de sesión: se encarga de proporcionar el diálogo entre aplicaciones finales para el uso eficiente de las comunicaciones. Puede agrupar datos de diversas aplicaciones para enviarlos juntos o incluso detener la comunicación y reestablecer el envío tras realizar algún tipo de actividad.

- Capa de presentación: esta capa se encarga de definir los formatos de los datos y si es necesario, procesarlos para su envío. Este proceso puede ser el de compresión o el de paso a algún sistema de codificación. En otras palabras, se encarga de la sintaxis.

- Capa de aplicación: esta capa acoge a todas las aplicaciones que requiere la red. Esta capa permite que varias aplicaciones compartan la red.

1.4 DISPOSITIVOS ASOCIADOS

Los dispositivos que se conectan de forma directa a un segmento de red se denominan hosts. Estos hosts incluyen computadores, tanto clientes y servidores, impresoras, escáners y varios otros dispositivos de usuario. Estos dispositivos suministran a los usuarios conexión a la red, por medio de la cual los usuarios comparten, crean y obtienen información. Los dispositivos host pueden existir sin una red, pero sin la red las capacidades de los hosts se ven sumamente limitadas.

1.4.1 Tarjeta de Interfaz de Red Ethernet

Las tarjetas de red actúan como interfaz entre un computador u otro dispositivo de red y el medio físico (cable UTP, coaxial, fibra, etc); estas dispositivos actúan como un filtro en la subcapa de control de acceso al medio; es decir, cada NIC[5] consta de un número único llamado dirección MAC o dirección de hardware que garantiza la autenticidad de los dispositivos dentro de un sistema de red y por medio de esta dirección es como se reconoce la información que va dirigida a un determinado equipo o dispositivo de red.

[5] Acrónimo de Network Interface Card.

La eficiencia de una interfaz de red depende del desempeño del sistema, del buffer de memoria del mismo y del software que interactúe con la interfaz, pero ninguno de ellos se encuentra definido en un estándar.

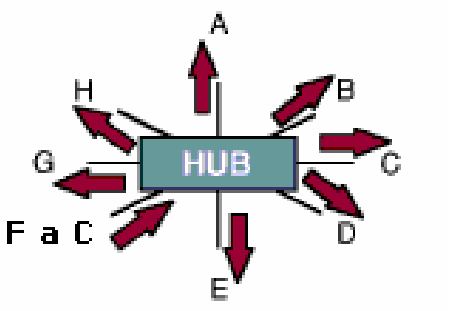
1.4.2 Hubs o Repetidores.

Los Hubs[1,3] o repetidores se emplean para conectar dos o más segmentos Ethernet. Cuando los segmentos exceden el máximo número de nodos o la longitud máxima, la calidad de las señales empieza a deteriorarse, por esto, se utilizan los repetidores que son los que proporcionan la amplificación y resincronización de las señales, necesarias para conectar los segmentos. Al dividir un segmento en dos o más subsegmentos, se facilita el crecimiento de la red.

Los hubs son usados para crear un punto de conexión central para los medios de cableado y aumentar la confiabilidad de la red. La confiabilidad de la red se ve aumentada al permitir que ante la eventualidad de un fallo en un cable, no se interrumpa el funcionamiento de la red.

Una de las desventajas del hub es que transmite *"Broadcast"* a todos los puertos que contenga, esto es, si el Hub contiene 8 puertos (ports), todas las computadoras que estén conectadas al hub, recibirán la misma información, y en ocasiones resulta innecesario y excesivo. En la figura 5 se ilustra el funcionamiento de un hub.

Figura 5. Funcionamiento del Hub.



Los hubs desempeñan funciones básicas que no varían para ninguno de los sistemas de 10, 100 y 1000 Mbps, entre las que se pueden nombrar las siguientes:

- Alertar sobre colisiones a todos los segmentos: cuando un hub detecta una colisión envía una señal *jam*, la cual asegurará que en los demás segmentos se detecte la colisión y se detengan las transmisiones.
- Restaurar la amplitud de la señal, reajustar el *timing* de la señal, restaurar la simetría de la señal y extensión del fragmento; es decir, toda señal menor a 96 bits que entra al hub será extendida hasta que al salir su tamaño sea igual a 96 bits, esto asegura que un fragmento de colisión corto sobrevivirá un viaje a través de una red de tamaño máximo y será reconocido y descartado por todas las estaciones.

Adicionalmente la mayoría de los hubs cuentan con leds que indican ciertos aspectos de la actividad de la red, tales como, segmentos que se encuentren transmitiendo o recibiendo datos, segmentos en los que ocurren colisiones y segmentos aislados por causa de una falla.

1.4.3 Switches o conmutadores.

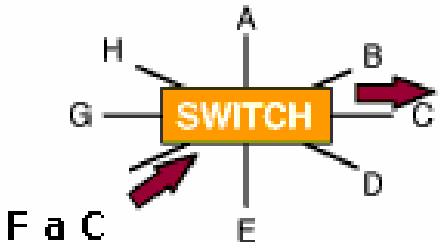
Los switches[1,2,3] son dispositivos que permiten construir sistemas Ethernet largos, enlazar segmentos Ethernet que operan a distintas velocidades y controlar el flujo y tráfico a través de un sistema. Los switches mejoran la confiabilidad de los sistemas Ethernet y pueden incrementar ampliamente el ancho de banda habilitado.

Los switches son diseñados de tal forma que su modo de operación sea transparente a las estaciones y/o equipos de trabajo en la red; es decir, que puedan enlazar segmentos de una red LAN sin necesidad de realizar

ningún cambio en las estaciones. Una de las mayores ventajas de la utilización de switches es que cada segmento de LAN enlazado opera como un dominio de colisión separado, entonces, es posible la conexión de segmentos Ethernet que funcionen con distintas velocidades y tecnologías. Otro punto a favor es el hecho de que los switches tienen la capacidad de soportar múltiples conversaciones entre los puertos.

La diferencia entre el hub y el switch, radica en el hecho de que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión en absoluto. Como los switches son capaces de tomar decisiones, hacen que la LAN sea mucho más eficiente. Los switches hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente. En la figura 6 se muestra su funcionamiento.

Figura 6. Funcionamiento del Switch.



1.5 PROTOCOLOS TCP / IP

Cuando se hace uso de una aplicación, se debe identificar el servicio al cual se quiere acceder. Esta identificación se realiza definiendo la dirección IP del host y su número de puerto TCP[6] (*socket*). Los números de puerto de TCP están en el intervalo 0 a 65535, de los cuáles de 0 a

[6] Transmisión Control Protocol. Protocolo orientado a conexión

1023 están asignados y se identifican como puertos bien conocidos y del 1024 a 65535 están disponibles para el usuario, los cuales se identifican como puertos de usuario. TCP cuenta con numerosos protocolos de aplicación. A continuación se especifican algunas características de los protocolos más importantes utilizados en la red objeto del estudio.

1.5.1 Protocolo de transferencia de archivos.

(FTP - *File Transfer Protocol*). Permite el envío y recepción de archivos de cualquier tipo, de o hacia un usuario. Cuando se desea el envío, se realiza una conexión TCP con el receptor y se le transmite información sobre el tipo y acciones del archivo, así como los usuarios que pueden acceder al mismo. Una vez realizado esto, se envía el archivo, al cabo de lo cual, se puede cortar la conexión.

1.5.2 Protocolo de transferencia de hipertexto.

(HTTP - *Hyper Text Transfer Protocol)*. HTTP es el protocolo de la red mundial de datos (www), usado en cada transacción. El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones para acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Al finalizar la transacción todos los datos se pierden. Por esto se popularizaron las *cookies*, que son pequeños archivos guardados en el propio computador que puede leer un

sitio web al establecer conexión con él, y de esta forma reconocer a un visitante que ya estuvo en ese sitio anteriormente.

1.5.3 Protocolo sencillo de transferencia de correo.

(SMTP - *Simple Mail Transfer Protocol*). Es un protocolo de servicio de correo electrónico, listas de correo, etc.; su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante TCP/IP.

1.5.4 Protocolo de mensajes de control de Internet.

(ICMP - *Internet Control Message Protocol*). Desempeña un papel fundamental como asistente de la red, cumple funciones de ayuda a los hosts con el enrutamiento IP y permite a los administradores de red comprobar el estado de los nodos de la red. Los mensajes ICMP se transmiten como datagramas IP, con una cabecera y con el campo de protocolo; todos los hosts y enrutadores deben ser capaces tanto de generar como de procesar los mensajes ICMP. Los mensajes más comunes son: Destino Inalcanzable, Plazo superado (*Time Exceeded*), Acallado de origen (*Source Quench*) y Redirigir (*Redirect*). Con la correcta utilización e interpretación de los mensajes ICMP se puede contribuir a que la operación de la red mejore.

1.5.5 P2P.

(Peer to Peer). A las técnicas clásicas de transferencias de archivos (como el FTP), se les ha añadido un conjunto de protocolos y aplicaciones *peer to peer*, también conocido como P2P, cuya difusión y utilización ha sido creciente en los últimos años. Con estos sistemas, los usuarios

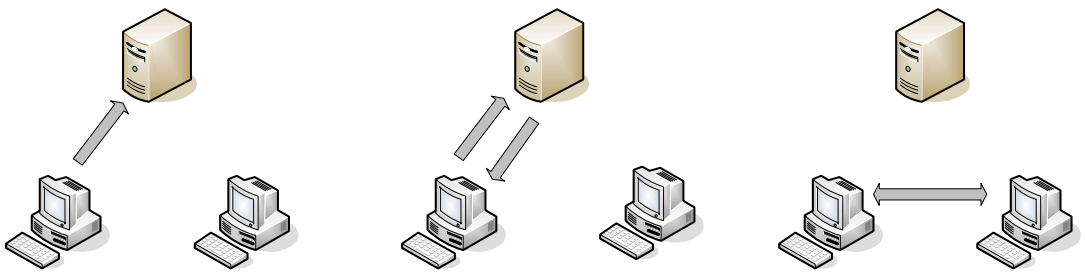
intercambian contenidos directamente, sin necesidad de servidores centrales que los almacenen.

Las primeras aplicaciones P2P surgieron para el intercambio de archivos MP3, hoy en día su uso se ha extendido a todo tipo de contenidos que los usuarios quieran compartir (video, imágenes, textos…). También incorporan muchas veces servicios añadidos, como la comunicación directa de usuarios mediante servicios de Chat.

En las aplicaciones P2P existen realmente dos protocolos, uno de ellos entre cliente y servidor para acciones de registro, búsqueda, etc, y otro cliente-cliente para el intercambio de archivos entre usuarios.

Existen dos tipos de aplicaciones P2P, en función de como se realice la funcionalidad del servidor. En los sistemas *centralizados*, los servidores son maquinas separadas de los clientes, que mantienen una visión global del conjunto de usuarios conectados y los archivos que comparte cada uno. En los sistemas *descentralizados*, los propios clientes actúan también como servidores y las búsquedas de archivos se propagan de unos a otros recursivamente. Generalmente las aplicaciones P2P utilizan un sistema centralizado. En la figura 7 se puede observar el funcionamiento de este sistema.

Figura 7. Funcionamiento de una aplicación P2P en un sistema centralizado.



2. DESCRIPCION DEL ANALISIS DE TRÁFICO EN EL ENLACE EXTERNO

Para analizar el comportamiento del tráfico en el enlace externo debe contarse con información general acerca del estado de la red de la Universidad Industrial de Santander. Además es necesario tener una serie de herramientas de monitoreo y administración, que permitan realizar un seguimiento sobre el flujo de datos.

2.1 DESCRIPCIÓN DE LA RED DE DATOS DE LA UIS

La descripción de la red, permite determinar los principales requerimientos y escenarios a implementar en la etapa de captura; el conocimiento de la red, facilitará la selección de los dispositivos y software que se utilizarán en esta etapa.

La información de mayor interés para este proyecto es la relacionada con la conexión a Internet, las direcciones IP de las diferentes subredes, y el Switch Central; del estado del resto de la red tan solo es necesaria una información básica.

Una correcta documentación de una red es muy difícil, debido a factores como el escaso personal con que se cuenta y el continuo crecimiento de las redes que se modifican casi a diario, haciendo difícil una descripción detallada de la misma, ya que cualquier generalización que se haga puede resultar obsoleta en poco tiempo.

La Universidad Industrial de Santander no es ajena a la situación anteriormente mencionada, por lo cual no tiene una documentación adecuada del estado de la red. La información con la que se cuenta se

basa en datos proporcionados por la persona encargada de la gestión de la red y en trabajos de pregrado y postgrado[7] realizados dentro del CPS[8].

2.1.1 Descripción general

Actualmente la Universidad Industrial de Santander cuenta con una red de datos de área local con topología en estrella y tecnología Giga y Fast Ethernet; el cableado que comunica el Switch Central y los Switches departamentales está hecho sobre fibra óptica multimodo. Para la concentración a nivel de cada segmento de red, se hace uso de 30 switches departamentales distribuidos a lo largo de los distintos segmentos de red.

En la actualidad (a Febrero de 2005), se cuenta con 79 subredes, las cuales han sido asignadas a ciertas dependencias y en algunos casos a edificios. Debido a que el número de subredes (segmentos lógicos) es superior al número de segmentos físicos (edificios), es bastante común que a un edificio se encuentren asociadas diferentes subredes. Este esquema de conexión es posible, gracias a la opción de configuración de VLANs que tienen los switches disponibles dentro de la red.

A continuación, en la tabla 5 se presentan las direcciones IP de las principales subredes de la Universidad Industrial de Santander.

Tabla 5. Direcciones IP de las principales subredes.

DIRECCIÓN IP	NOMBRE	DIRECCIÓN IP	NOMBRE
192.168.18.0	**Biblioteca**	**192.168.59.0**	**Admisiones**

[7] Guzmán C, Paola Fernanda. Análisis de la gestión de los dispositivos administrables en la red de datos institucional. Universidad Industrial de Santander, 2005. Tesis de Maestría.
[8] Grupo de Investigación en Conectividad y Procesado de Señal.

192.168.19.0	Servidores	192.168.61.0	LEA Salas 2-3-5
192.168.20.0	Ciencias Humanas	192.168.62.0	LEA Salas 4-6
192.168.21.0	Educación	192.168.65.0	Sistemas Lab JAV
192.168.22.0	LEA	192.168.71.0	Alta Tensión Lab Elect
192.168.23.0	Base datos	192.168.72.0	HIDR
192.168.24.0	Lab. Pesados	192.168.73.0	CITI
192.168.27.0	Lab. Livianos	192.168.74.0	BUCARICA CNBILING
192.168.28.0	Fisica1	192.168.75.0	Nodo PML Bucarica
192.168.29.0	Fisica2	192.168.76.0	Fundeuis
192.168.30.0	Salud Admón.	192.168.80.0	DSI
192.168.31.0	CICELPA,LIMN,INV,CEIAM	192.168.81.0	Planeación
192.168.32.0	Artes	192.168.84.0	Sistemas1
192.168.33.0	CAPRUIS	192.168.85.0	ICI,CEIC Civil Geomatica
192.168.34.0	Diseño Industrial	192.168.86.0	Civil Geomatica
192.168.35.0	Bienestar	192.168.87.0	Civil Geomatica 3
192.168.36.0	Luís A. Calvo	192.168.88.0	Petróleos CPIP
192.168.37.0	Ala Oriental E. Administración	192.168.89.0	Publicaciones
192.168.38.0	Ala Occidental E. Administración	192.168.92.0	Asesorias
192.168.39.0	IQUI	192.168.93.0	Incubadora de Empresas
192.168.40.0	Ing. Industrial	192.168.94.0	CIDLIS, GISEL
192.168.41.0	Postgrados	192.168.96.0	Teleuis
192.168.42.0	Planta Física	192.168.97.0	Recursos Humanos
192.168.43.0	Mecánica	192.168.99.0	SOCACAD

192.168.44.0	**Petróleos**	**192.168.100.0**	**ADMBAR**
192.168.45.0	**Alta Tensión**	**192.168.101.0**	**BARBOSA**
192.168.46.0	**Eléctrica**	**192.168.102.0**	**MALAGA**
192.168.47.0	**MORFOPAT**	**192.168.105.0**	**Fisioterapia 1**
192.168.48.0	**HURV**	**192.168.106.0**	**Nutrición**
192.168.49.0	**SALCONF**	**192.168.107.0**	**Instituto de Lenguas**
192.168.50.0	**INSED**		**Broadcast**
192.168.51.0	**FAVUIS**		**Spanning-tree-for-bridges_00**
192.168.54.0	**Bucarica**	**192.168.6.0**	**Rack1 Guatiguara**
192.168.58.0	**Financiero Tesoreria E. Administracion**		**OTROS**

2.2 SWITCH CENTRAL

El nodo principal de la red de la Universidad Industrial de Santander es el Switch-Router Cajun P880 marca Avaya de 16 slots, que también cuenta con 2 módulos con 10 puertos Fast Ethernet para cada uno, que conectan algunos edificios de la Universidad por medio de fibra óptica, como la Facultad de salud, la sede de Guatiguará y el enlace externo a Internet.

Otros 3 módulos cuentan con 4 puertos Gigabit Ethernet cada uno, de los cuales 10 están siendo utilizados y conectan otros edificios y/o subredes del campus con el Switch Central, principalmente aquellos de alta prioridad como lo son la Biblioteca Central, el Edificio de Administración y la subred donde se encuentran los principales servidores.

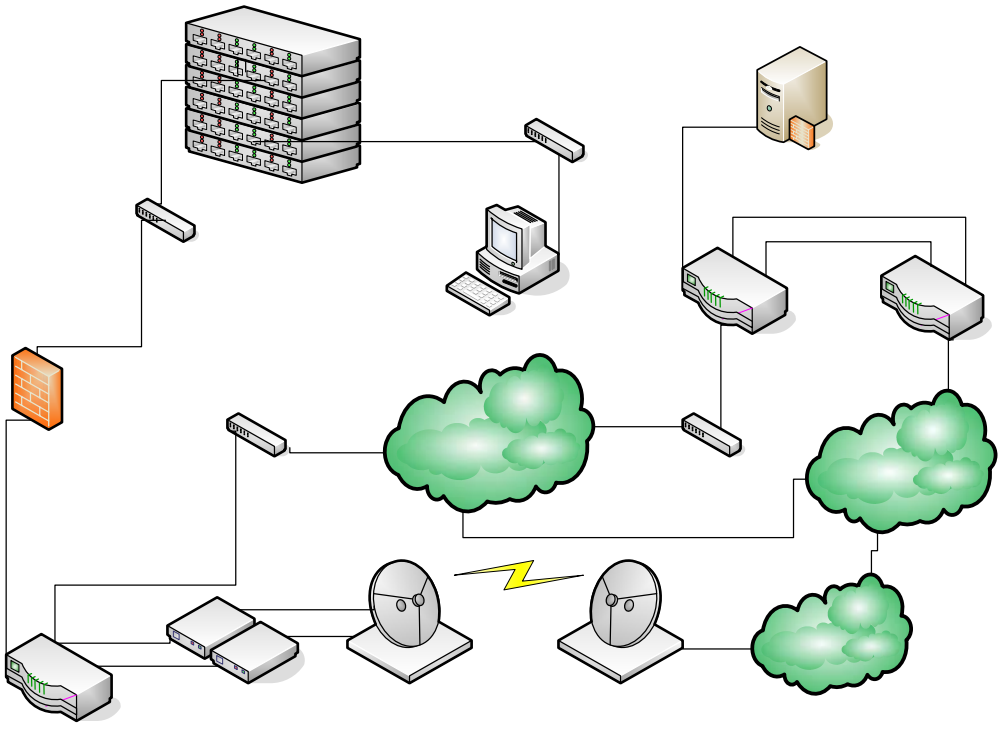
El puerto 8 del módulo 3 corresponde al puerto en el que se hace la conexión con los proveedores de Internet (ISPs). En la actualidad, la Universidad cuenta con dos enlaces WAN que interconectan la red con dos ISPs, estos proveedores de Internet son Telecom y ETB.

2.3 DESCRIPCIÓN DEL ENLACE DE CONEXIÓN A INTERNET

En los últimos meses el enlace de conexión a Internet ha tenido varios cambios relacionados con el aumento de ancho de banda y de proveedores del servicio. La Figura 8 permite ver el estado del enlace en el momento en que se realizó la captura de datos.

El ancho de banda contratado es de 10 Mbps de los cuales TELECOM proporciona 6Mbps por medio de fibra óptica monomodo y ETB proporciona 4Mbps por microondas terrestres.

Figura 8. Diagrama de conexión a Internet.



La información parte del puerto 8, módulo 3 del Switch Router Cajun P880, por medio de una fibra multimodo (100Mbps) hasta llegar a un convertidor de medios 100 Base FX (MM) a 100 Base TX; a través de un cable UTP se establece una conexión con el Firewall Cisco Pix 515, y luego éste es conectado por medio de un cable UTP, al enrutador BGP Cisco 3640 propiedad de la ETB y punto de unión entre los proveedores y la LAN UIS.

También se cuenta con un computador marca Dell, que se encuentra conectado a uno de los puertos del Switch Central por medio de un convertidor de medios 100 Base FX (MM) a 100 Base TX; este puerto se utiliza para hacer mirroring al puerto del enlace de Internet. Un puerto mirror (espejo), copia el tráfico de un puerto específico en otro puerto elegido por el administrador. Este mecanismo ayuda al seguimiento de posibles errores de red o transmisiones anormales de paquetes sin tener que interrumpir el flujo de datos a través de la red.

A partir del enrutador BGP Cisco 3640, la configuración de los equipos no es responsabilidad del administrador de red institucional. También es importante mencionar, que dentro de las instalaciones de Colombia Telecomunicaciones hay un Proxi Cisco Cache Engine y un enrutador Cisco 3620 propiedad de la UIS, para facilitar el sistema de conexión física del enlace.

2.4 MONITOREO DE TRÁFICO

El monitoreo del tráfico es un método utilizado para analizar el tráfico real de paquetes en la red y generar informes basados en este análisis. Aunque existen varios motivos para monitorear el tráfico de una red, los dos principales son el pronóstico de cambios futuros y el descubrimiento de cambios inesperados en el estado de la red. Los cambios inesperados

pueden incluir problemas tales como errores en un enrutador o un switch, o un error en el enlace de comunicaciones.

La falta de monitoreo en una red, implica que el administrador sólo podrá reaccionar a los problemas a medida que estos surjan, en lugar de preverlos para que no se presenten.

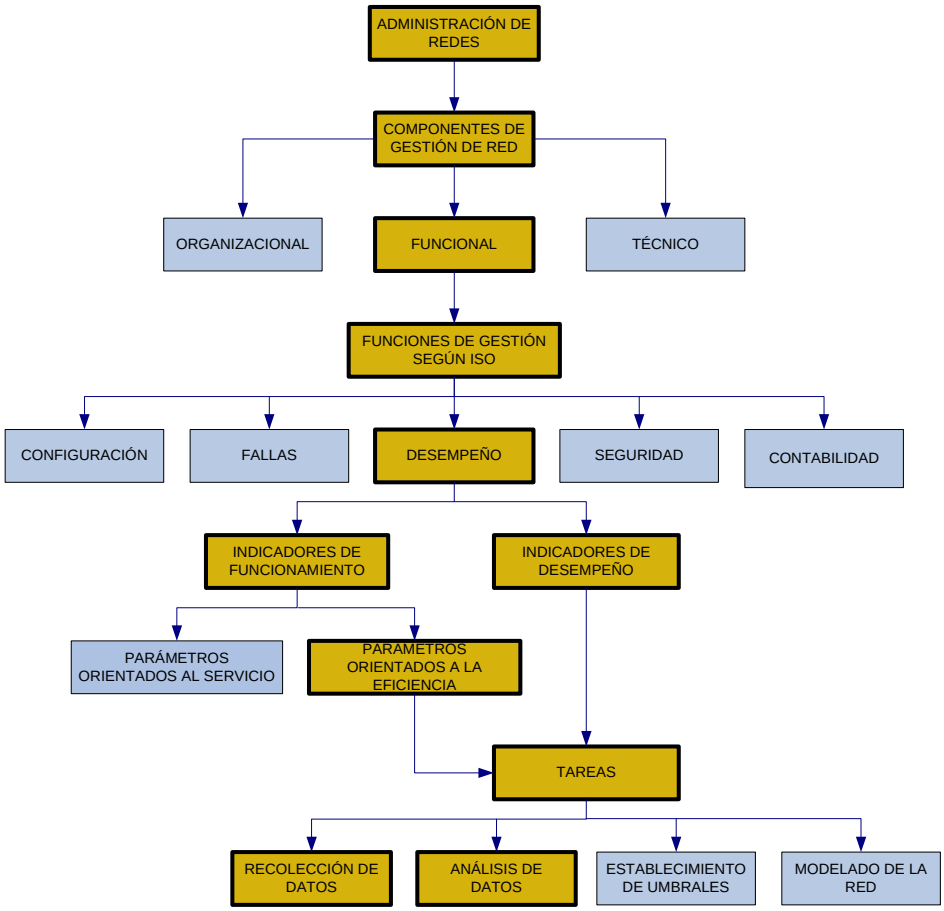
2.5 ANÁLISIS DE TRÁFICO

El análisis de tráfico se puede definir como el conjunto de mediciones relacionadas con la transmisión de paquetes en un segmento de la red de datos. Estos paquetes están originados por aplicaciones que corren sobre la red, los servicios que se prestan en ella o los protocolos que administran su funcionamiento.

La actividad de análisis de tráfico mide su cantidad, comportamiento, dinámica, tiempos de tránsito y otros factores que permiten efectuar el diagnóstico de problemas o niveles de actividad de la red. Para lograrlo, el profesional debe conocer el comportamiento de la red y sus protocolos, además de contar con un computador que tenga un software analizador de tráfico.

Esta disciplina es un área muy específica dentro de lo que se entiende como gestión de redes, específicamente en el sector de rendimiento. En la figura 9 se puede observar a qué parte del organigrama de la gestión de redes pertenece el análisis de tráfico.

Figura 9. Organigrama de la Administración de redes.



2.6 ESCENARIOS DE MEDICIÓN

Mediante estos escenarios de medición se presentan diferentes alternativas para realizar la captura del tráfico que circula por el enlace externo sin afectar el comportamiento de la red.

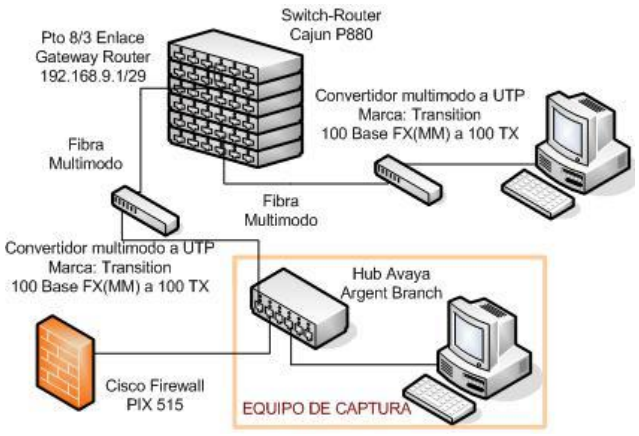
Gracias a la información previamente recopilada de la conexión a Internet, se pueden establecer dos posibles esquemas de captura. Estos hacen uso de los siguientes dispositivos:

- 1 Switch Central Avaya
- 1 Hub Avaya Argent Branch
- 1 Computador Optiplex GX marca DELL
- 1 Tarjeta de red Gibabit Ethernet de Fibra Óptica
- 1 Tarjeta de red Fast Ethernet

2.6.1 Primer escenario

Como se puede apreciar en la figura 10, para realizar la captura se conecta un hub entre el convertidor multimodo a UTP y el Cisco Firewall Pix 515; también es necesario conectar a uno de los puertos del hub un computador para almacenar los datos. El computador debe estar provisto de una tarjeta de red Fast Ethernet y un software de captura.

Figura 10. Primer escenario (Utilizando un Hub.)

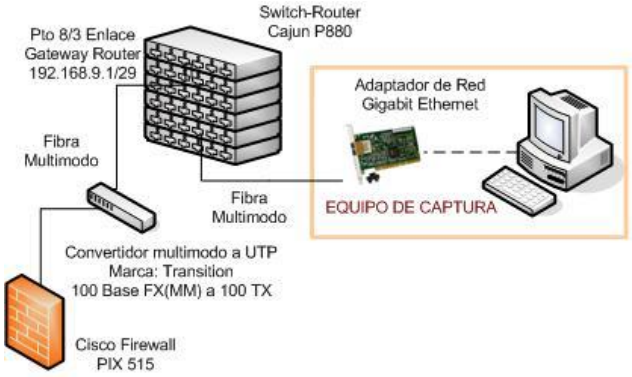


2.6.2 Segundo escenario

En este escenario como se observa en la figura 11, se utiliza una tarjeta de red Gibabit Ethernet de Fibra Óptica ubicada en el interior de un computador Dell (ver anexo B). La tarjeta se conecta a un puerto del

Switch Central por medio de un patch cord[9] de fibra óptica; luego se hace mirroring (puerto espejo) al puerto del enlace de Internet y se almacenan los datos en el computador.

Figura 11. Segundo escenario (Haciendo mirroring)



2.6.3 Selección del escenario

De los dos esquemas propuestos el más viable es el primero, puesto que no se necesita configurar el Switch Central, evitando de esta forma introducir alguna falla dentro del dispositivo. Al realizar esta implementación, el desempeño de la red cayó; esto puede ser debido a colisiones dentro del hub, por lo cual se optó por el segundo esquema.

En el segundo esquema se necesita hacer mirroring sobre el puerto del enlace de Internet, esto produce algunos inconvenientes debido a que el administrador de la red necesita también utilizar esta función sobre el mismo puerto y este soporta solo un mirroring a la vez. Para salvar esta situación se eligió hacer la captura en el equipo que estaba utilizando el administrador.

[9] Es una pieza de cobre o fibra, con conectores en cada uno de sus extremos utilizada para conectar diferentes dispositivos de red

La solución definitiva fue instalar la tarjeta de red Gigabit Ethernet de fibra óptica dentro del equipo del administrador; se eliminó el convertidor multimodo a UTP, y se conectó directamente la tarjeta al puerto del Switch Central por medio de un patch cord de fibra óptica (ver figura 11).

2.7 METODOLOGÍA DE CAPTURA DE TRÁFICO

Conocer el comportamiento del tráfico en una red, es de suma importancia para determinar cómo están siendo utilizados los recursos de ésta. A medida que la velocidad de las redes es superior, la carga de procesamiento de los paquetes aumenta. Cuando la velocidad de los enlaces es muy alta, la medida de tráfico llega a ser imposible si no se tiene un procesador muy rápido y que esté completamente dedicado a la medida de tráfico; por lo que es necesaria la utilización de diferentes métodos que permitan un mejor aprovechamiento de los recursos disponibles.

Para la captura y procesamiento de los datos es posible utilizar alguno de los siguientes métodos:

- Capturar y procesar sólo una parte de los datos. Para esto es necesario definir un intervalo de tiempo de captura. Este intervalo no es fácil de definir debido a que las redes son únicas, y no se puede evaluar una red basándose en los mismos criterios que se utilizaron para otra. Sin embargo, algunos autores recomiendan[4] unos intervalos de tiempo dependiendo de las características del tráfico que se deseen analizar.

- Capturar todos los datos y procesar sólo una parte de ellos. El principal problema de este método es que debido a la gran cantidad de datos la capacidad de almacenamiento es un factor crítico; en

cuanto al procesamiento de datos es necesaria la utilización de técnicas de muestreo que permiten seleccionar sólo una porción de los datos, posibilitando la utilización de un procesador más lento para ahorrar recursos.

- Capturar y procesar todos los datos es quizás la alternativa menos eficiente, por la gran cantidad de recursos que se consumen al tener que almacenar y procesar tantos datos. La ventaja que tiene es que el error presente en los resultados será menor, debido a que no se utilizan técnicas de muestreo o una selección errónea de intervalos de tiempo de captura.

2.7.1 Selección de la metodología de captura de tráfico

Un aspecto muy importante en la adecuada selección de la metodología para la captura y procesado de los datos, es contar con el apoyo y la experiencia del administrador de la red; pues sólo mediante ésta se puede conocer el comportamiento real y único de la red.

La experiencia del administrador permite identificar los días y rangos de tiempo durante los cuales se debe realizar la captura. Debido a que el lugar donde se realiza la captura es un punto crítico dentro de la red institucional, el tiempo permitido para realizar ésta debe ser el menor posible, para evitar que agentes externos afecten el desempeño de la red. También es importante mencionar que la red tiene un período de tiempo durante el día donde su correcto funcionamiento es primordial; este rango de tiempo es de 8 de la mañana a 8 de la noche.

En el campo de las redes una suposición equívoca puede llevar a grandes fracasos. Se deben elegir correctamente el intervalo en el que se hará el muestreo y la duración del estudio, para evitar errores relativos a la

utilización real de la red. Relacionado con lo anterior, es mejor no utilizar métodos donde se tenga que estimar ciertas variables sin tener unas bases sólidas para su formulación. Por ejemplo, si se desea dimensionar la red para condiciones de carga normal, pero se hace el muestreo durante un período pico, se tendrá una imagen distorsionada del tráfico y se tenderá a sobredimensionar la red.

En la literatura relacionada[4][9] con las metodologías donde no se hace una captura y/o procesamiento de todos los datos para evitar un excesivo consumo de recursos; se trabaja con enlaces de velocidades superiores a los 100 Mbps, trazas de varias semanas y durante las 24 horas. La Universidad Industrial de Santander cuenta con un enlace de 10 Mbps y el período de recolección de los datos que se eligió es tan solo de 5 días de los cuales solo se toman los datos de 12 horas de cada día; esto permitirá ver que aunque el consumo de recursos para la metodología donde se capturan y procesan todos los datos es alto, no es tan crítico y se puede manejar.

Teniendo en cuenta lo expuesto anteriormente, capturar y procesar la totalidad de los datos es un método que se ajusta a las características de la red institucional y da una mayor confiabilidad en los resultados obtenidos a partir de éste. Por esta razón, se decidió implementar el último método descrito.

2.8 HERRAMIENTAS DE MONITOREO BASADAS EN SOFTWARE - SNIFFERS

Las redes de datos son canales de comunicaciones compartidos, ya que simplemente es demasiado costoso poner un *switch* para cada par de computadores implicados en la comunicación. Compartir significa que los computadores pueden recibir la información que fue enviada a otras máquinas. Al proceso de capturar la información que pasa a la red se denomina *sniffing*.

El protocolo de Ethernet trabaja enviando la información del paquete a todos los *hosts* en el mismo circuito. La cabecera del paquete contiene la dirección apropiada de la máquina destino. Solamente la máquina con la dirección que va en la cabecera se supone que debe aceptar el paquete. Una máquina que está aceptando todos los paquetes, sin importar lo que ponga en la cabecera del paquete, se dice que esta en *modo promiscuo*.

Un sniffer de paquetes es un programa de “pinchado” (wiretap), que se instala en una red, por medio del cual se pueden ver todos los paquetes que circulan por ella.

Algunos usos típicos de estos programas son:

- Captura de passwords y logins que están en texto plano (sin encriptar) desde la red.
- Conversión de datos a un formato comprensible por el hombre.
- Análisis de errores para descubrir problemas en la red.
- Análisis de rendimiento para descubrir posibles cuellos de botella en la red.
- Detección de intrusos en la red (hackers/crackers potenciales).

Un Sniffer más que una herramienta de ataque, en manos de un administrador de red puede ser una valiosa arma para la auditoria de seguridad en la red. Puesto que el acceso a la red externa debe estar limitado a un único punto, un Sniffer puede ser la herramienta ideal para verificar como se está comportando la red.

2.9 SELECCIÓN DEL SNIFFER

Se realizaron pruebas preliminares usando *sniffers,* con el fin de observar y analizar su modo de operación, capacidad, ventajas y desventajas, para de esta manera seleccionar el más apropiado para las pruebas finales.

Todos los *sniffer*s analizados cuentan con características similares con respecto a su operación; se pueden instalar sobre un PC para lo cual es necesario especificar el *hardware* de red sobre el cual va a operar (*NIC*, *módem*, etc), trabajan en modo promiscuo, tienen interfaz gráfica, recolectan estadísticas de la red y en general determinan la cantidad de tráfico.

Se analizaron tres diferentes sniffers, teniendo en cuenta las siguientes características: modo promiscuo, exportación de capturas, resolución de protocolos, identificación de puertos origen y destino. En la tabla 6, se presentan las principales características de las herramientas comparadas.

Tabla 6. Características de los Sniffers.

PARAMETRO	ETHEREAL	ANALYZER	NETXRAY
Modo De Operación	Promiscuo	Promiscuo	Promiscuo
Exportación Datos	Si	Si	Si
Formato Exportación Capturas	Txt y csv	txt	csv
Filtros Protocolos	Si	Si	Si
Análisis Protocolos	Si (Extenso)	Si (Extenso)	Si (Limitado a configuración)
Presentación Capturas	Graficas y tablas	Gráficas y tablas	Gráficas y tablas
Seguimiento Sesión TCP	Si	No	No
Fácil Configuración	Si	Si	Si
Sistema Operativo	Windows, Linux	Windows, Linux	Windows

Teniendo en cuenta las características anteriores se decidió utilizar el **ETHEREAL version 0.10.7**, el cual trabaja bajo el sistema operativo Windows y cumple a cabalidad con todos los requisitos necesarios para el análisis de trafico.

2.10 Ethereal

Ethereal es un potente analizador de protocolos de redes, para máquinas Unix y Windows; permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco. Se destaca también por su impresionante soporte de más de 300 protocolos.

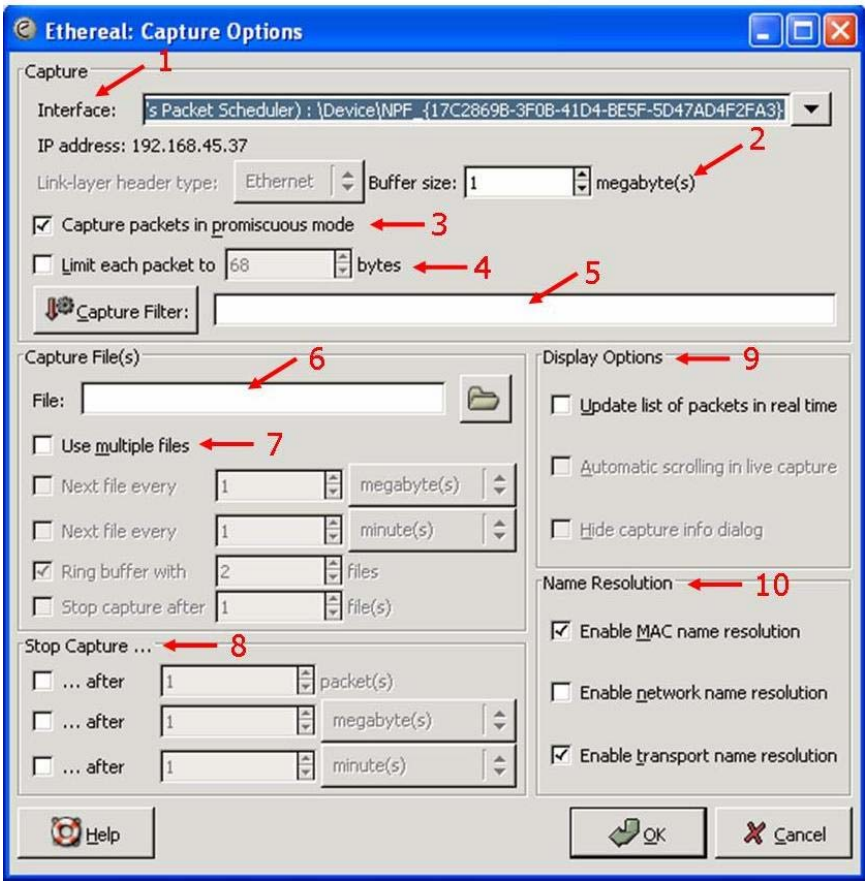
Algunas características destacables del Ethereal se describen a continuación:

- Captura los datos de paquetes en tiempo real de una interfaz de red.
- Muestra los paquetes con una información detallada de los protocolos.
- Abre y guarda los datos de paquetes capturados.
- Importa y exporta los datos de paquetes a muchos otros programas de captura.
- Posee diferentes filtros de paquetes.
- Proporciona estadísticas.

2.10.1 Configuración de captura en Ethereal

Para iniciar la captura de datos es necesario ir al menú *capture,* el cual despliega una ventana como la que se muestra en la figura 12.

Figura 12. Menú de captura del Ethereal.



Aquí se puede configurar una serie de parámetros o características dependiendo de las necesidades del usuario, como son las siguientes:

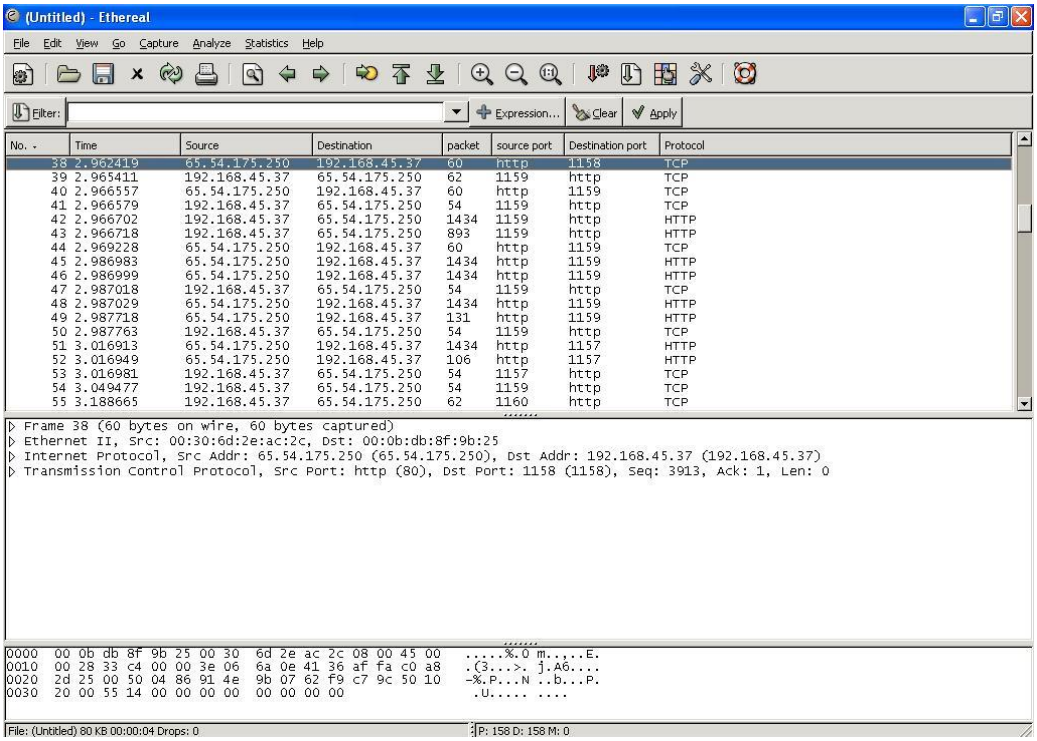
- Escoger la interfaz o medio de comunicación por el cual se va a realizar la captura. (1)
- Determinar el tamaño del buffer. (2)
- Captura en modo promiscuo o no. (3)
- Límite del tamaño del paquete. (4)
- Determinación de un filtro de captura. (5)
- Nombre y ubicación del archivo de captura. (6)

- Uso de archivos múltiples: si se escoge esta opción se tiene que definir el modo como se van a almacenar y determinar estos archivos; puede ser especificando su tamaño, intervalo de tiempo de captura y el número de archivos de captura requeridos. (7)
- Cuando no se usa la opción de archivos múltiples para detener la captura se tienen las opciones anteriores y también la del tamaño de la captura. (8)
- Opciones para visualización. (9)
- Resolución de nombres. (10)

2.10.2 Información de una captura mostrada por Ethereal

La primera columna que se observa en la figura 13, contiene el número de cada paquete transmitido en el transcurso de la captura; la segunda columna muestra el tiempo de captura, el cual se puede ver de distintas formas ya sea mostrando el tiempo del día, la fecha y el tiempo del día, los segundos desde que empieza la captura y segundos de los paquetes previos; la tercera columna muestra las estaciones fuente; la cuarta columna muestra las estaciones destino; la quinta columna muestra el tamaño en bytes de cada paquete; la sexta columna muestra el puerto fuente; la séptima columna muestra el puerto destino y la octava columna muestra el tipo de protocolo. Estos parámetros se pueden modificar conforme a la necesidad de cada usuario. En la figura 13 se muestra la información de una captura.

Figura 13. Captura mostrada por Ethereal.



3. CAPTURA Y PROCESADO DE DATOS

En este capítulo se presenta la captura y procesamiento de los datos del enlace externo, teniendo en cuenta los parámetros seleccionados en el capítulo anterior como son el escenario de medición, los intervalos de captura, la forma de usar y almacenar la información y la herramienta usada para la toma de los datos.

3.1 PRUEBAS PRELIMINARES UTILIZANDO EL SNIFFER

Teniendo la configuración del *sniffer* mencionada anteriormente, se realizaron pruebas preliminares en el enlace externo para determinar las condiciones más adecuadas en las cuáles se debían realizar las pruebas del estudio de tráfico.

Para estas primeras pruebas se realizó la conexión del computador donde se encuentra el sniffer, a un puerto mirror del switch central donde se ve reflejada la totalidad del tráfico del enlace externo. El puerto mirror es un puerto Gigabit Ethernet para lo cual fue necesario conectar una tarjeta de red Gigabit Ethernet de fibra óptica en el computador.

Con las pruebas preliminares se pudo detectar el tamaño en bytes de las muestras, teniendo aproximadamente un archivo de 100 Mbytes por cada minuto de captura, esto se redujo dramáticamente capturando sólo la cabecera de los paquetes, limitando en el sniffer cada paquete en 68 bytes, dando como resultado un archivo de muestra aproximadamente de 10 Mbytes por cada minuto de captura.

Por medio de estas pruebas, se pudo observar que algunos paquetes de protocolos conocidos P2P no eran resueltos; en la columna de protocolos se mostraba su protocolo de transporte el cual era TCP. Lo anterior, se

tendrá en cuenta al realizar el procesado de los datos ya que la carga útil es amplia.

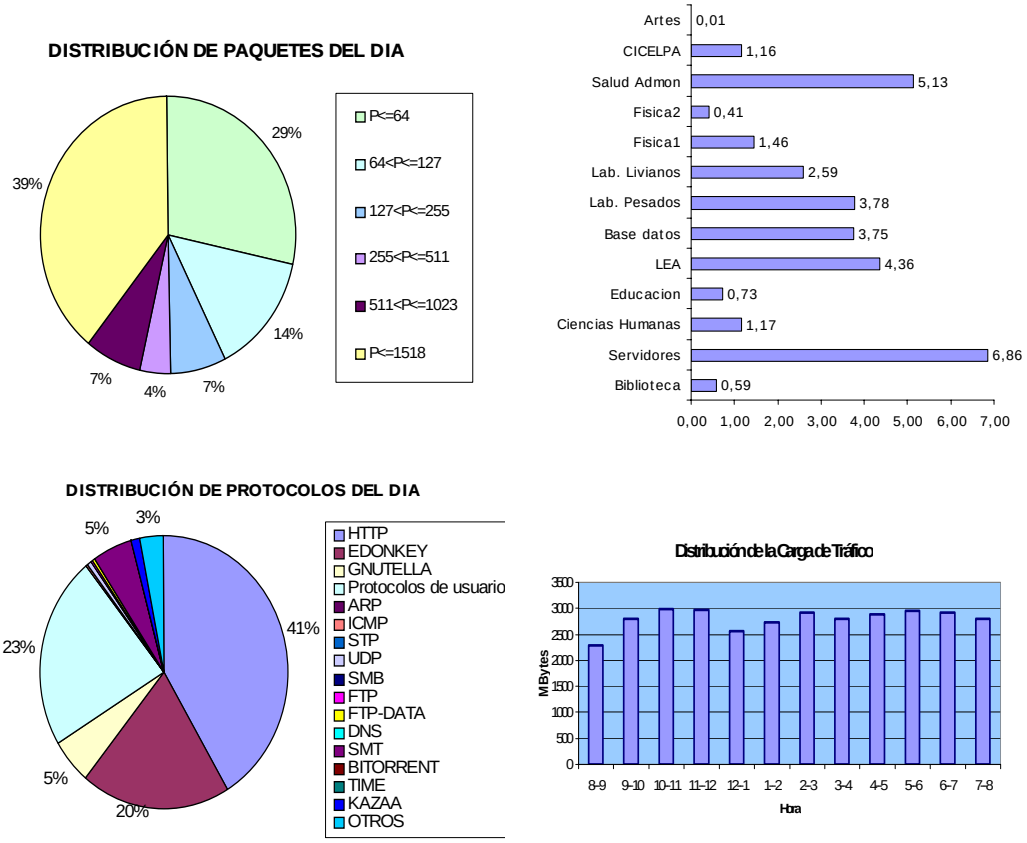
Otro aspecto que se verificó fue la forma en la que el *sniffer* permite exportar los datos. Los resultados de las sesiones de captura se exportaron en archivos tipo texto para luego evaluarlos y seleccionar información relevante requerida para el estudio de tráfico.

Estas pruebas se realizarón bajo condiciones de tráfico real generado en el enlace externo, lo cual permitió ajustar el tamaño del buffer y determinar el lapso de duración de cada captura.

Se determinó que la duración de cada captura sería de tres minutos. Ya que se trabajará durante 12 horas diarias (8 am a 8 pm), durante 5 días (lunes a viernes), se tendrá un total de 1200 muestras, cada una de aproximadamente 25 Mbytes.

Las últimas pruebas preliminares se realizaron para establecer la forma de organización y presentación de los resultados obtenidos en las sesiones de captura, de tal manera que resulte de fácil entendimiento. La presentación de resultados es principalmente en forma gráfica; para esto se utilizo el manejo de hojas de cálculo bajo la herramienta Microsoft Excel. Se muestra la distribución de tamaño de paquetes y distribución total de protocolos en forma de torta; consumo de las principales subredes y comportamiento del tráfico por horas en cada puerto en forma de barras (ver Figura 14).

Figura 14. Ejemplos de presentación de la información.



3.2 PRUEBAS FINALES

Estas pruebas son las que aportan la información más importante para el análisis de tráfico del enlace externo. Con estas pruebas se obtuvo una estimación del nivel de uso de la red y se identificó el comportamiento de ésta con respecto al flujo de tráfico circulante en el transcurso del día, durante el periodo de tiempo que se realizaron las sesiones de captura.

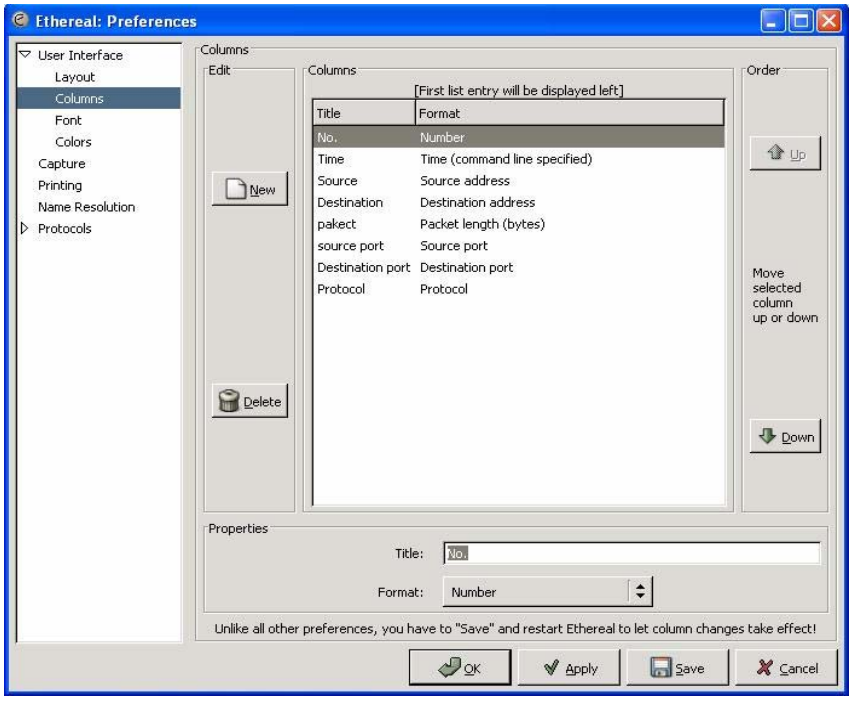
3.2.1 Configuración Final del Ethereal.

Primero es necesario identificar qué datos son relevantes para el análisis del tráfico, los cuales son:

- No: Numero del paquete
- Time: Tiempo al captura el paquete
- Source adress: Dirección fuente
- Destination adress: Dirección destino
- Packet length(bytes): Tamaño del paquete en bytes
- Source port: Puerto fuente
- Destination port: Puerto destino
- Protocol: Resolución del protocolo utilizado por el paquete.

Esta selección de campos se realiza en el menú *Edit – Preferences-Columns*. En la figura 15 se observa la selección.

Figura 15. Selección de campos.



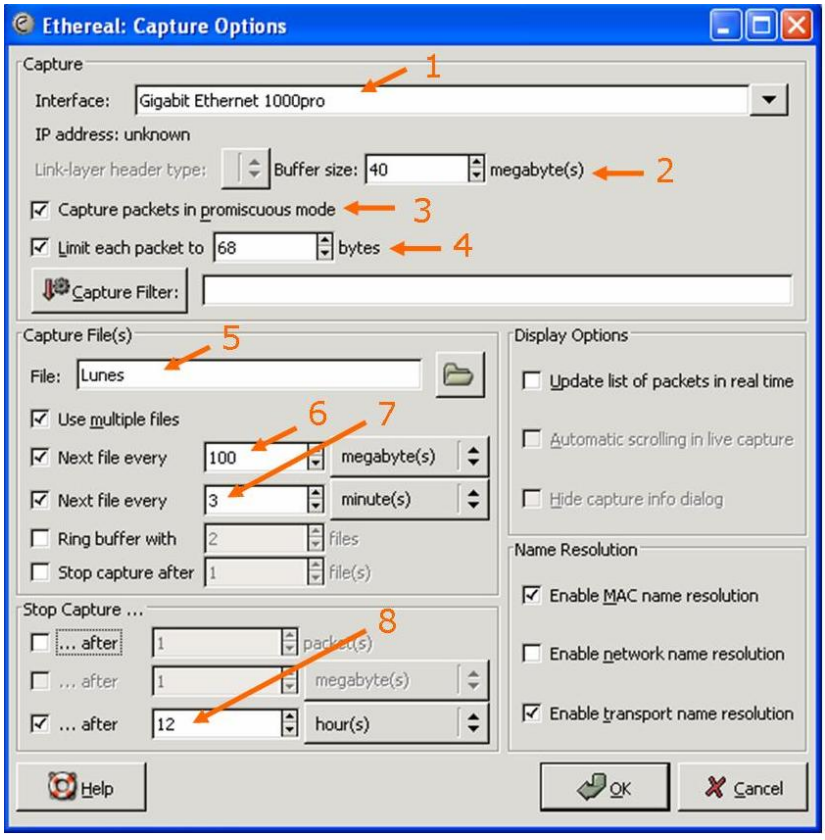
Como resultado se tienen los campos mostrados en la figura 16.

Figura 16. Campos de captura.

No.	Time	Source	Destination	packet	source port	Destination port	Protocol

El segundo paso consiste en configurar la captura. Las principales opciones que presenta Ethereal para realizar la captura se muestran en la figura 17 y se explican a continuación.

Figura 17. Configuración final de captura.



- Escoger la interfaz o medio de comunicación por el cual se va a realizar la captura. en este caso se escoge la tarjeta de Red Gigabit Ethernet. (1)
- Determinar el tamaño del buffer. Es necesario configurar el tamaño del buffer del *sniffer* según los requerimientos del flujo de datos. Realizando las pruebas preeliminares se determinó un buffer de 40 Mbytes, lo cual es suficiente para evitar desbordamientos. (2)
- Captura en modo promiscuo o no: cuando se envía una información por la red, las tarjetas dejan pasar todo el tráfico de la red que no les pertenece, es decir, todo tráfico que no tenga como destino el computador en el que está instalada. Sin embargo la tarjeta sabe que está pasando tráfico por el cable al que está conectada, por lo tanto, seleccionando este modo de operación se permite ver todo el tráfico que pasa por el cable, a este cambio se le conoce como modo promiscuo. (3)
- Límite del tamaño del paquete: una de las principales características de Ethereal es que limita el tamaño en bytes de cada paquete capturado, esto se hace indispensable ya que al realizar la captura en el enlace externo se tiene un gran volumen de tráfico. Con esta opción se restringe a la cabecera del paquete donde se encuentra la información necesaria, disminuyendo el tamaño del paquete en aproximadamente un 90%. (4)
- Nombre y ubicación del archivo de captura. Se especificó una ruta de almacenamiento y un nombre con el cual se van a identificar los archivos. (5)
- Con el intervalo de 3 minutos de captura se tendrá un archivo máximo de aproximadamente 35 Mbytes. (6)
- Uso de archivos múltiples: examinando las capturas preliminares realizadas en el enlace externo, se determinó un intervalo de 3 minutos de captura. Lo anterior debido a que si se tiene un mayor

tiempo de captura, pueden presentarse problemas de bloqueo en el sniffer, ya que no soporta capturas de un gran tamaño. En total se tendrían 20 muestras por hora de captura. (7)

- Se seleccionó un tiempo de captura de 12 horas al día, con esta opción se permite programar el tiempo de captura. (8)

3.2.2 Captura Final.

Las pruebas finales se realizaron desde el lunes 9 al viernes 13 del mes de mayo del presente año, teniendo una duración diaria de 12 horas.

Como se expresó anteriormente, estas pruebas finales condujeron a 1200 capturas en total. Cada captura tiene un promedio de 25 Mbytes de datos, por lo tanto, diariamente al terminar las pruebas, se hacía necesario respaldar los datos.

Estos archivos de captura estaban en el formato de ETHEREAL. Para poder analizar cada captura era necesario diseñar y programar una aplicación que permitiera analizar cada una de estas capturas y generara los datos relevantes para el análisis del tráfico del enlace externo. Se decidió utilizar la herramienta MATLAB 7.0 para realizar la operación de procesado.

Los parámetros que se escogieron para el análisis de tráfico fueron los siguientes:

- Distribución de paquetes.
- Distribución de protocolos de aplicación.
- Consumo de las subredes.
- Comportamiento del volumen de tráfico.

El análisis de la distribución del volumen de tráfico y la distribución del uso de protocolos son los elementos básicos para el análisis del tráfico en una red. La identificación del consumo de cada una de las subredes es útil para entender el flujo de tráfico y ayuda sustancialmente a caracterizar el comportamiento de la red, planear su desarrollo y expansión, verificar la calidad de los servicios de red, entre otros.

Analizar los tamaños de cada paquete y su distribución permite entender el estado de la red y su eficiencia.

Para poder usar la información capturada es necesario exportarla a un formato que sea compatible con la herramienta a utilizarse. Dentro de los formatos que dispone Ethereal para exportar los datos a otro formato están el texto plano, el post script y el xml.

Se realizó una exportación de cada archivo de captura a documento texto para su fácil manipulación en Matlab. Este archivo de texto debe tener la información necesaria para encontrar los parámetros seleccionados anteriormente; por lo tanto al exportar los datos a este formato, hay que tener en cuenta que se debe seleccionar únicamente la información que sea útil. Se obtiene un archivo de texto con la siguiente información de cada paquete:

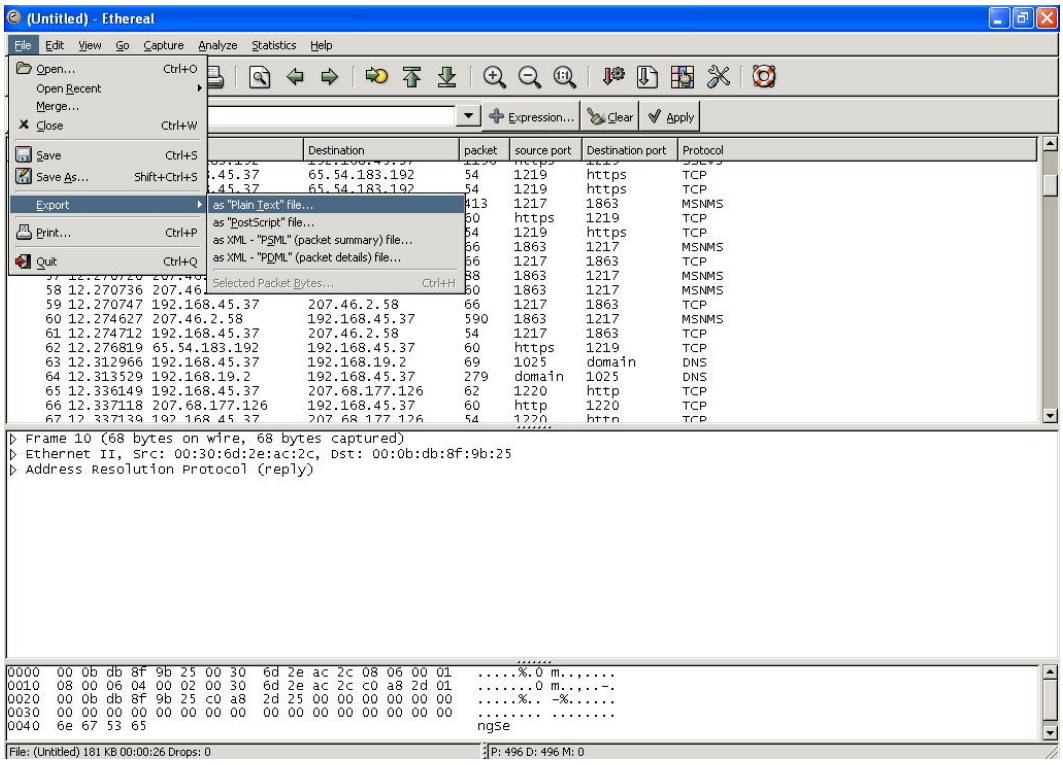
- Número
- Hora de captura
- Dirección fuente
- Dirección destino
- Longitud del paquete
- Puerto fuente
- Puerto destino
- Protocolo

Para realizar la exportación se llevaron a cabo los siguientes pasos:

- Primero. Ethereal permite la exportación a documento texto por una captura a la vez, por lo tanto es necesario realizar esta operación tantas veces como archivos de salida existan. Teniendo la configuración del Ethereal mencionada anteriormente, se carga el archivo de captura.

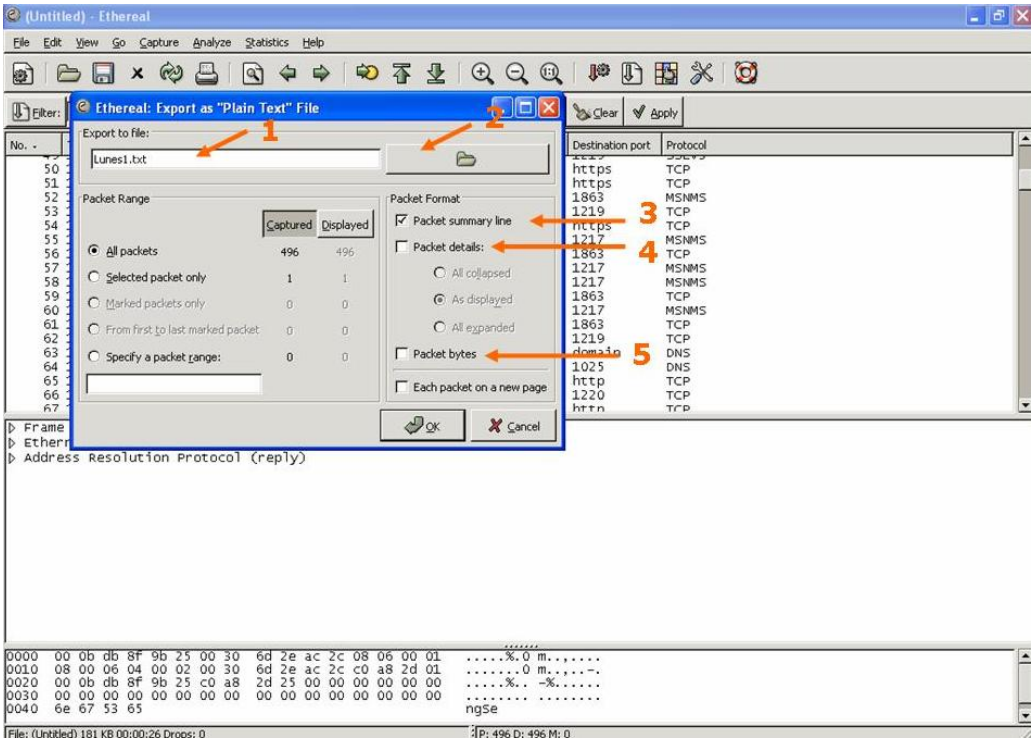
- Segundo. Para exportar los archivos de registro a archivos de texto se va al menú *File* y luego a la opción de Exportar como archivo de texto plano (as Plain Text file…) como se muestra en la figura 18.

Figura 18. Exportación de archivos de captura.



- Tercero. Para realizar la exportación de los datos se elige un nuevo nombre para el archivo con la extensión .txt (ver 1 en la fig 19), luego se escoge la ubicación del nuevo archivo (ver 2), por último se activa la opcion *Packet summary line* (ver 3) y se desactivan las opciones *Packet details* y *Packet bytes* (ver 4 y 5).

Figura 19. Exportación de capturas a texto plano.

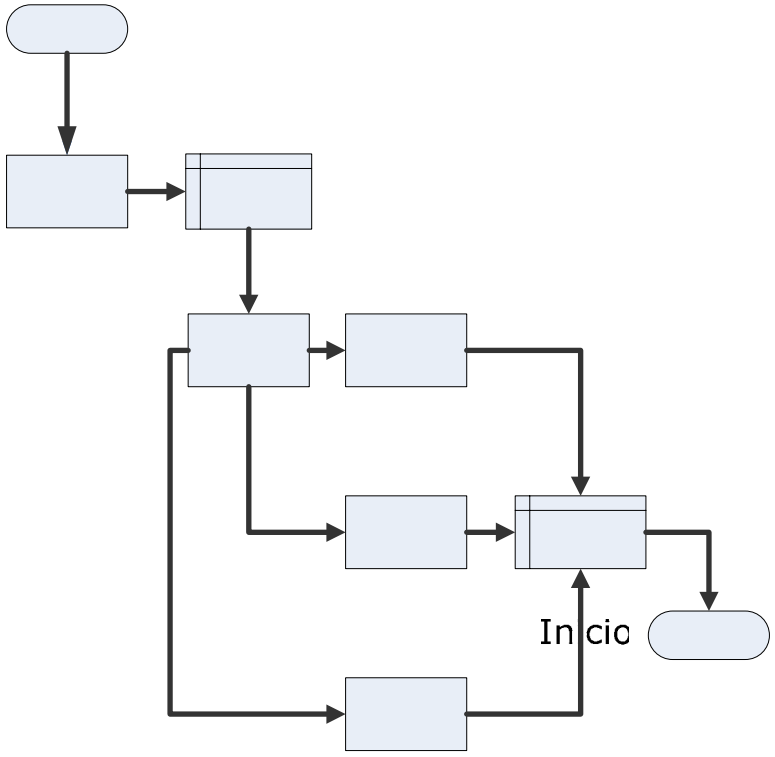


Como resultado, se tienen archivos de texto que contienen la información necesaria en una forma más fácil de procesar y de un tamaño más reducido.

3.3 PROCESAMIENTO DE LOS DATOS

El software realizado en Matlab comprende las siguientes etapas: (Figura 20)

Figura 20. Diagrama de bloques de la aplicación desarrollada.



Carga del archivo de captura. En esta etapa se importan los datos del archivo de captura en formato texto. Estos datos son organizados en una *matriz* que consta de 8 columnas y n filas, donde n es la cantidad de paquetes del archivo de captura.

Carga del archivo de captura

Matriz de datos

Filtrado de tráfico. En las pruebas finales se observó que existe una constante comunicación entre el computador y el switch central. Esta comunicación es despreciable, ya que no hace parte del tráfico real del

Filtrado de tráfico

enlace externo, por lo tanto se realizó un filtrado por medio del cual se eliminaron estos paquetes.

Distribución de Paquetes. En esta etapa se obtiene la distribución de paquetes entre unos rangos definidos, en este caso los rangos escogidos fueron:

P<=64	64<P<=127	127<P<=255	255<P<=511	511<P<=1023	P<=1518

Donde P es la longitud del paquete.

Distribución de Protocolos. Esta etapa arroja una distribución porcentual de los protocolos de aplicación. En las pruebas preliminares, se observó que muchos paquetes no tenían un protocolo de aplicación definido, por lo tanto se hizo un análisis más profundo revisando los puertos de origen y destino de cada paquete.

Muchos de estos paquetes pertenecían a protocolos p2p, por lo tanto se hicieron pruebas con varios programas que utilizan este protocolo, para definir los puertos que manejan. Algunos de estos programas con sus respectivos puertos[10][11], son:

- Kazaa: Puerto 1214.
- Bitorrent: Puertos 6881, 6882, 6883, 6884, 6885, 6886, 6887,6888, 6889.
- Gnutella: Puertos 6346, 6347, 6348.
- Emule, eDonkey: Puertos 4242, 5555, 3306, 2323, 6667, 7778, 4661-4672.

Consumo de Subredes. Este proceso permite identificar el consumo independiente de las subredes más importantes de la universidad.

Matriz de resultados. Esta matriz se realiza con base en la información adquirida en los procesos anteriores. Esta matriz de resultados es descargada en una hoja de cálculo de Excel, para, por medio de esta herramienta realizar gráficos de los parámetros seleccionados.

4. ANÁLISIS DE RESULTADOS OBTENIDOS.

En este capitulo se incluyen y comentan una selección del conjunto de gráficas que resultaron del análisis del tráfico del enlace externo. Se pretende que esta selección sea representativa de los distintos tipos de medidas realizadas, de acuerdo con lo expuesto en el capítulo precedente.

El apartado 4.1 se centra en medidas relativas a la distribución de la longitud de los paquetes IP, tratando de profundizar en las características intrínsecas del tráfico. El análisis del consumo de los principales protocolos se presenta en el apartado 4.2; en dicho apartado se trata de cuantificar el uso de recursos en la red mediante la diferenciación de servicios y perfiles de usuarios. En el apartado 4.3 se presenta el consumo general de las principales subredes de la universidad. Finalmente en el apartado 4.4 se recogen gráficas referentes a medidas de carga de tráfico.

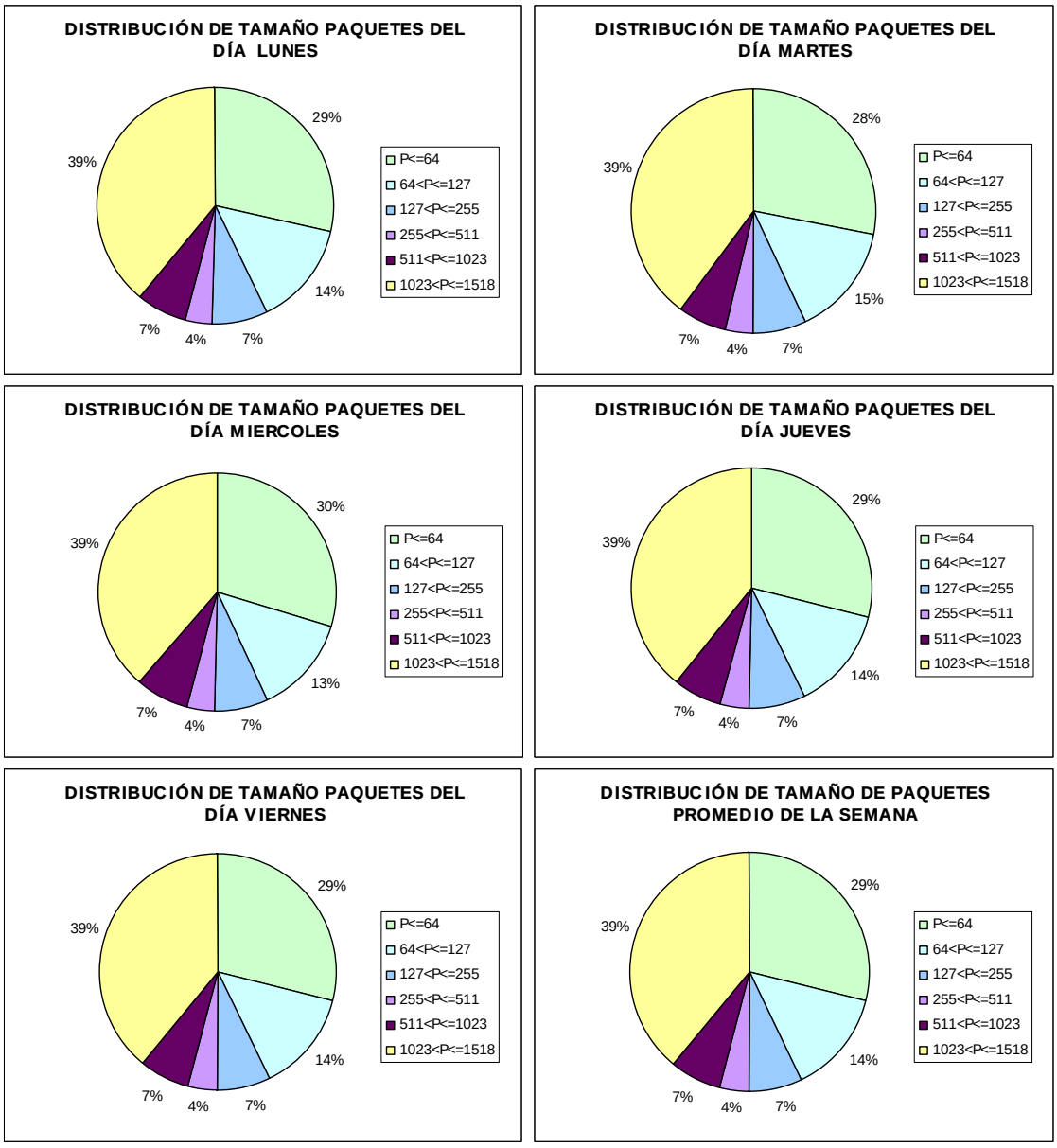
4.1 DISTRIBUCIÓN DE TAMAÑO DE PAQUETES

El tamaño de los paquetes generados afecta el desempeño de la red, dado que incide en aspectos tales como el retardo medio esperado (un paquete más grande tarda más tiempo en ser transmitido y liberar el medio), la probabilidad de error (un paquete de mayor longitud tiene mayor probabilidad de sufrir algún tipo de error), y el *throughput* de la red (un paquete muy pequeño contiene un *overhead* relativamente grande).

También se debe tener en cuenta que la utilización del ancho de banda se optimiza cuando aplicaciones y protocolos están configurados para enviar cantidades grandes de datos en un paquete, así se minimiza el número de paquetes para una transacción.

En la figura 21 se muestra la distribución de tamaño de paquetes en un tipo de gráfica circular. Los resultados se expresan de manera porcentual respecto del número total de paquetes capturados.

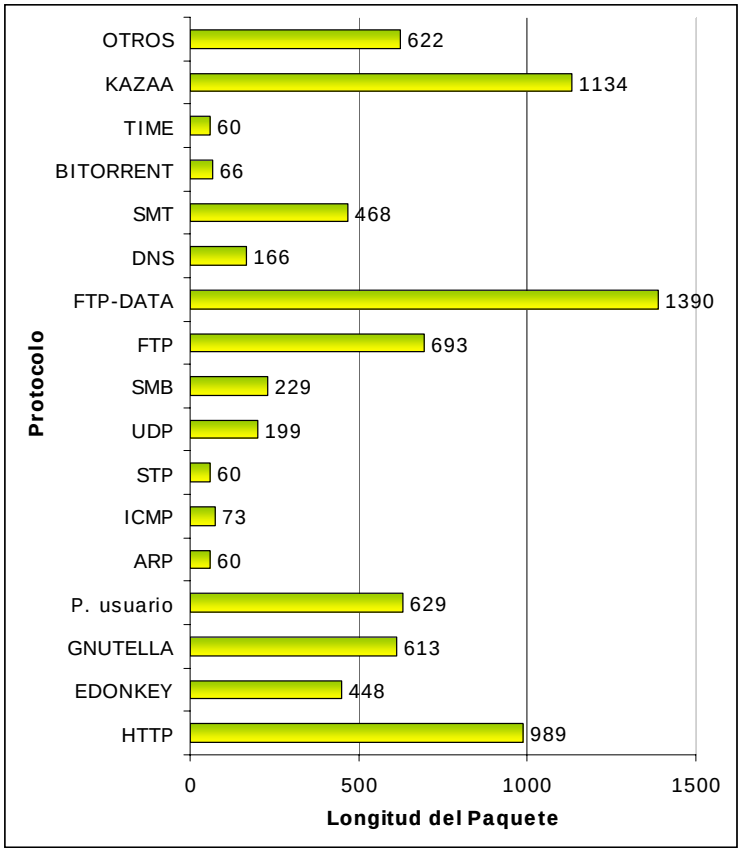
Figura 21. Distribución de tamaño de paquetes.



La distribución de tamaño de paquetes varía entre 54 y 1514 bytes. Se observa que la mayor parte del trafico del enlace se encuentra en el rango que varía de 1023 bytes a los 1518 bytes, seguido por el rango de 0 bytes a los 64 bytes; estos resultados son una constante en cada uno de los días analizados.

Se calculó el tamaño promedio del paquete para cada protocolo de aplicación para así determinar cual pertenece a los rangos con mayor porcentaje. Estos resultados se muestran en la figura 22.

Figura 22. Tamaño promedio de paquete para cada protocolo.



Los protocolos con mayor tamaño promedio de paquetes son: FTP-DATA, KAZAA y HTTP; los de menor son: ARP, ICMP, BITORRENT y TIME.

4.2 DISTRIBUCIÓN DE PROTOCOLOS DE APLICACIÓN

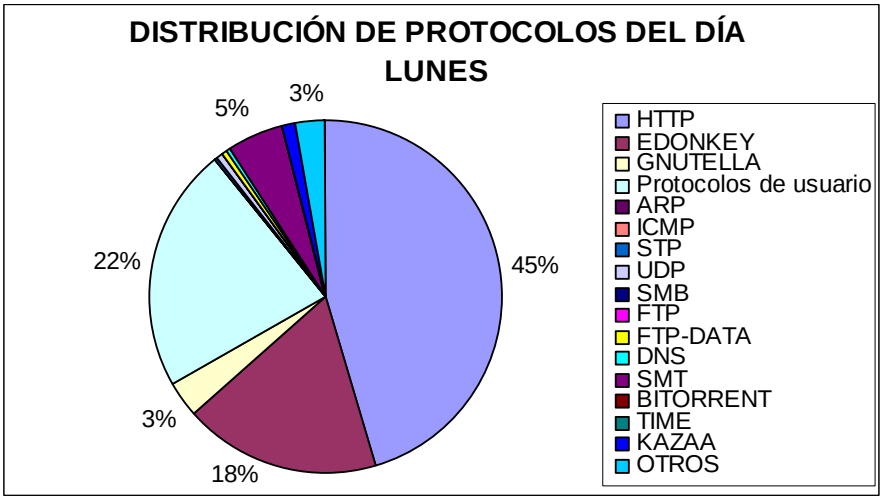
Este análisis permite conocer cuáles protocolos están presentes en el enlace externo, cuáles aplicaciones usan esos protocolos y cuál es la distribución de tamaño de paquetes que estas aplicaciones generan, con el fin de saber que servicios o aplicaciones consumen una porción importante de los recursos de la red.

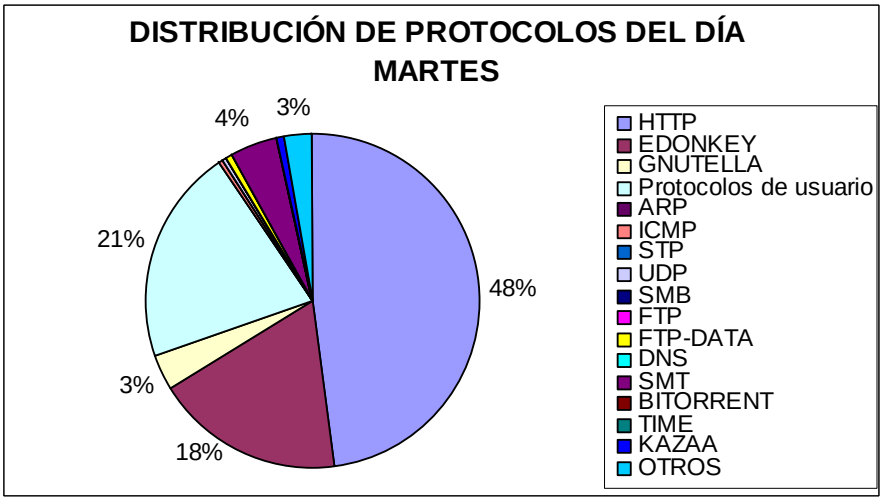
Esta distribución de protocolos es presentada en un tipo de gráfica circular (figura 23), mostrando sus porcentajes de utilización con respecto a su consumo en bytes. Se puede apreciar que HTTP es el protocolo de aplicación más utilizado, junto con EDONKEY y puertos de usuario.

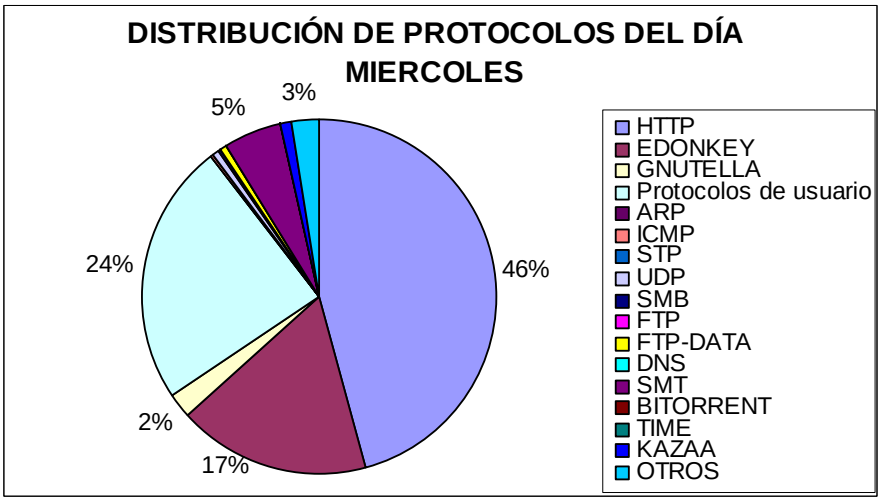
Es interesante hacer mención de la distribución del volumen de tráfico correspondiente a servicios que hemos llamado puertos de usuario, que en realidad corresponde a servicios no catalogados, es decir tráfico en el que se detectan puertos TCP no estándares (puertos entre 1024 a 65535).

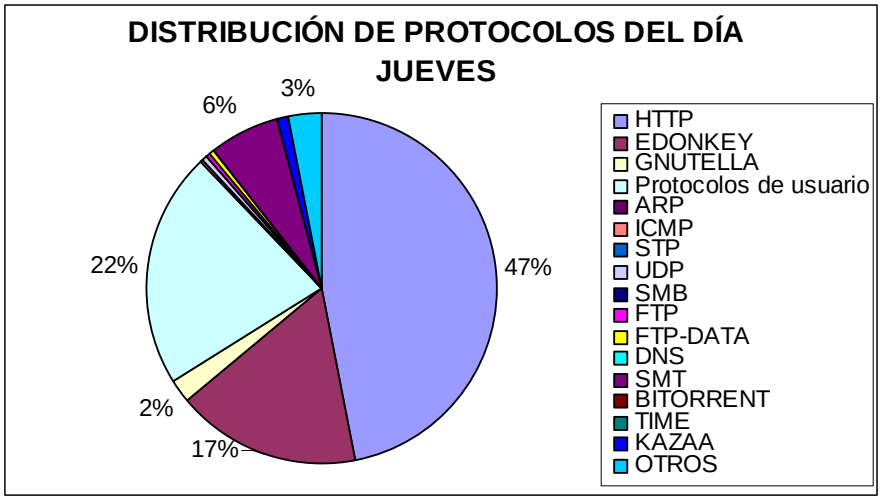
En conjunto los protocolos P2P identificados (EDONKEY, GNUTELLA, KAZAA Y BITORRENT) consumen un total del 22.3 % del tráfico del enlace. Cabe anotar que varias aplicaciones P2P no tienen un puerto de uso definido, por lo tanto no se pueden identificar (puertos de usuario).

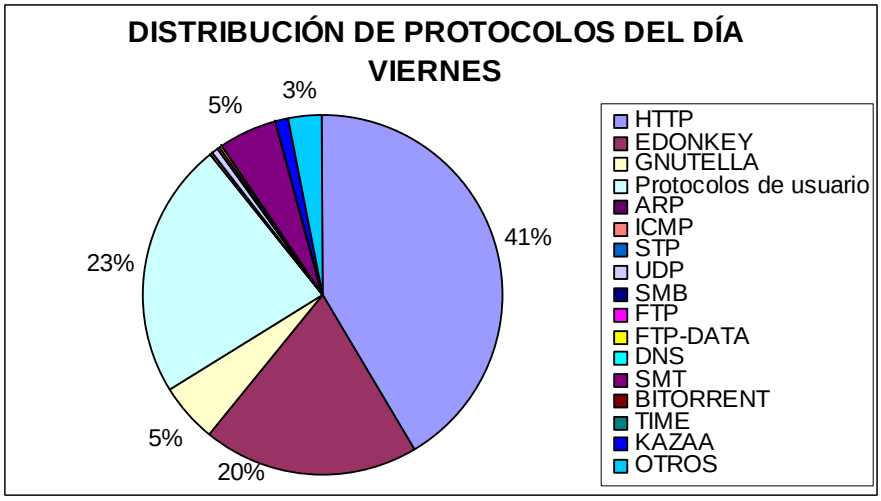
Figura 23. Distribución de Protocolos.

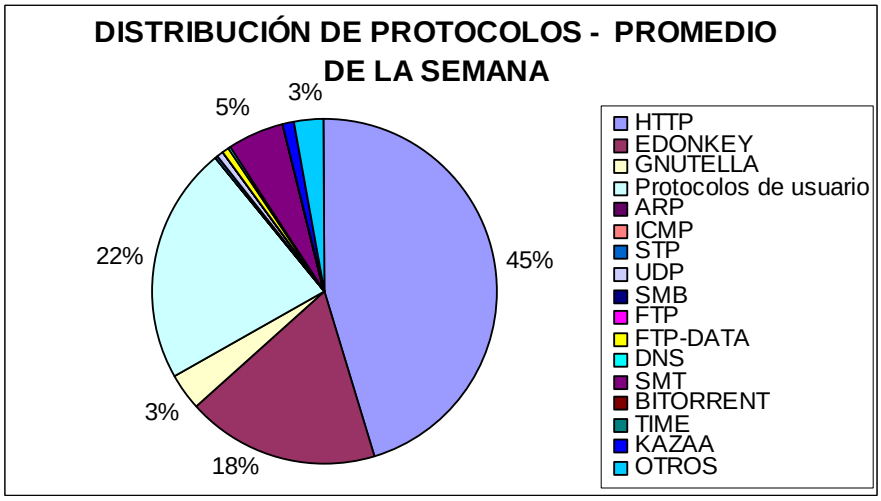







DISTRIBUCIÓN DE PROTOCOLOS DEL DÍA JUEVES
3%
6%
47%
22%
2%
17%
HTTP
EDONKEY
GNUTELLA
Protocolos de usuario
ARP
ICMP
STP
UDP
SMB
FTP
FTP-DATA
DNS
SMT
BITORRENT
TIME
KAZAA
OTROS


DISTRIBUCIÓN DE PROTOCOLOS DEL DÍA VIERNES
3%
5%
41%
23%
5%
20%
HTTP
EDONKEY
GNUTELLA
Protocolos de usuario
ARP
ICMP
STP
UDP
SMB
FTP
FTP-DATA
DNS
SMT
BITORRENT
TIME
KAZAA
OTROS


DISTRIBUCIÓN DE PROTOCOLOS - PROMEDIO DE LA SEMANA
3%
5%
45%
22%
3%
18%
HTTP
EDONKEY
GNUTELLA
Protocolos de usuario
ARP
ICMP
STP
UDP
SMB
FTP
FTP-DATA
DNS
SMT
BITORRENT
TIME
KAZAA
OTROS

4.3 CONSUMO DE LAS PRINCIPALES SUBREDES

Este análisis permite identificar el consumo de las principales subredes de la universidad. En la figura 24 se muestra la distribución porcentual del volumen de tráfico en bytes. Por motivos de claridad, sólo se han diferenciado algunas de las subredes más significativas.

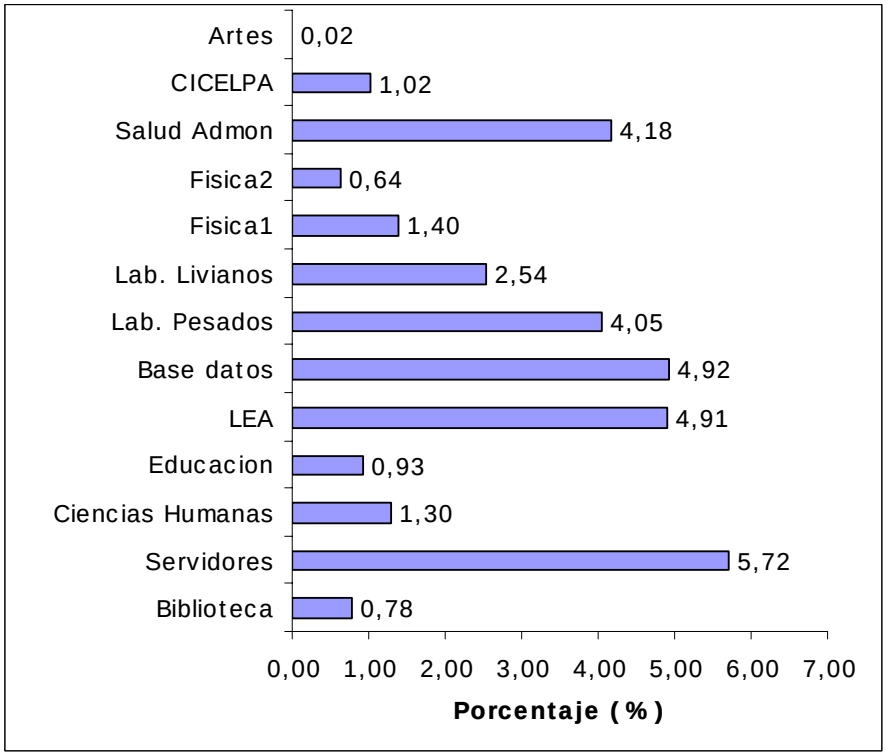
Las subredes que generan un mayor volumen de tráfico son:

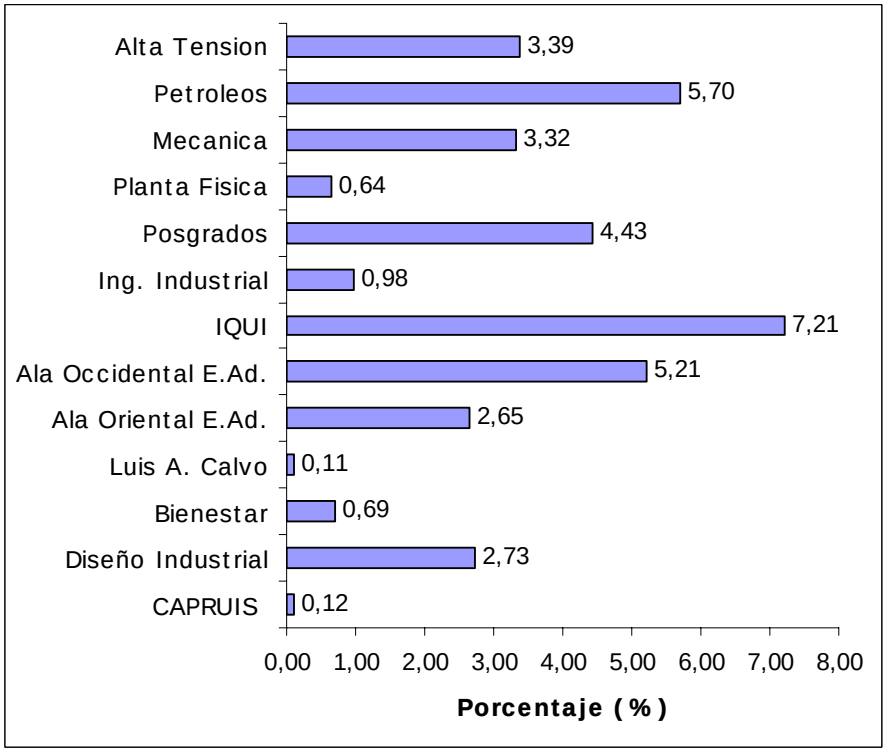
- Salud Administración. – 192.168.30.0
- Biblioteca base de datos – 192.168.23.0
- LEA – 192.168.22.0
- Servidores – 192.168.19.0
- Petróleos – 192.168.44.0
- Ing. Química – 192.168.39.0
- Ala occidental E. Administración – 192.168.38.0
- Civil Geomatica – 192.168.85.0
- Rack Guatiguara – 192.168.6.0
- Laboratorio Pesados – 192.168.24.0

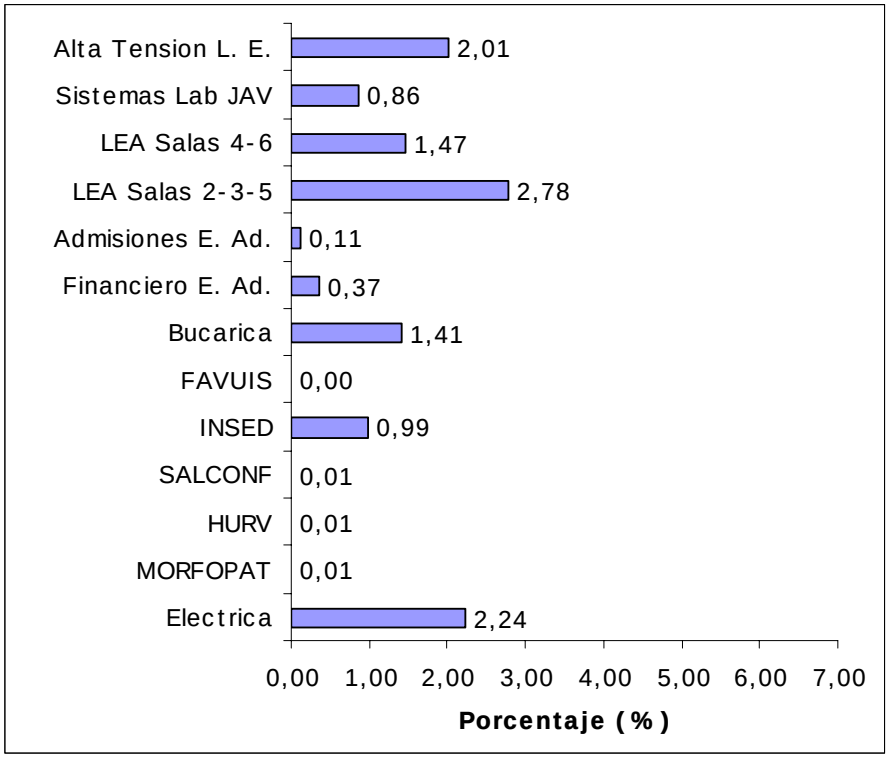
Estas 10 subredes representan el 52 % del consumo de tráfico del enlace externo. También se encuentran subredes que generan un volumen de tráfico despreciable, como las mencionadas a continuación:

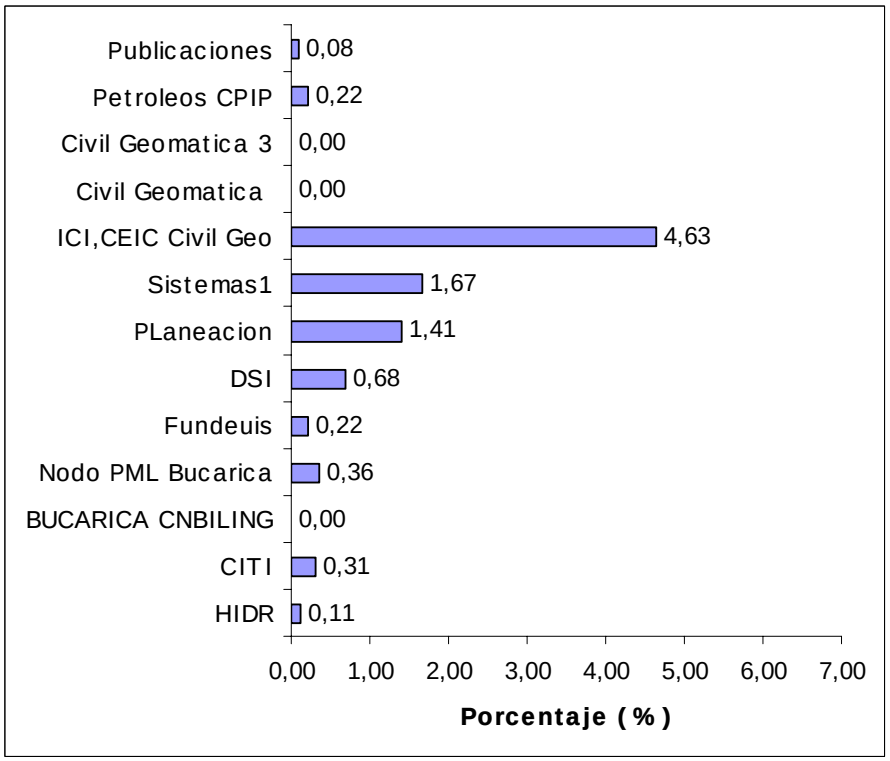
- Artes – 192.168.32.0
- Luís A. Calvo – 192.168.36.0
- Favuis – 192.168.51.0
- Sala Conferencias – 192.168.49.0
- HURV – 192.168.48.0
- MorfoPatología – 192.168.47.0
- Nutrición – 192.168.106.0
- Incubadora – 192.168.93.0

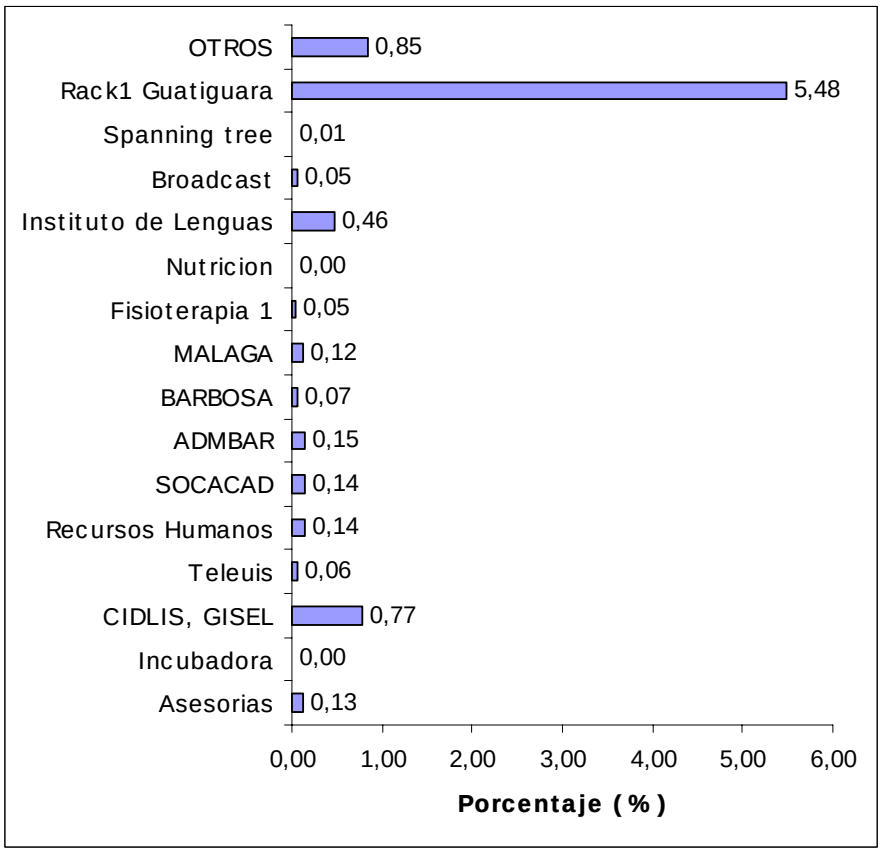
Figura 24. Volumen de tráfico de las principales subredes






Alta Tension L. E.
2,01
Sistemas Lab JAV
0,86
LEA Salas 4-6
1,47
LEA Salas 2-3-5
2,78
Admisiones E. Ad.
0,11
Financiero E. Ad.
0,37
Bucarica
1,41
FAVUIS
0,00
INSED
0,99
SALCONF
0,01
HURV
0,01
MORFOPAT
0,01
Electrica
2,24
0,00 1,00 2,00 3,00 4,00 5,00 6,00 7,00
Porcentaje (%)


Publicaciones
0,08
Petroleos CPIP
0,22
Civil Geomatica 3
0,00
Civil Geomatica
0,00
ICI,CEIC Civil Geo
4,63
Sistemas1
1,67
PLaneacion
1,41
DSI
0,68
Fundeuis
0,22
Nodo PML Bucarica
0,36
BUCARICA CNBILING
0,00
CITI
0,31
HIDR
0,11
0,00 1,00 2,00 3,00 4,00 5,00 6,00 7,00
Porcentaje (%)



4.4 DISTRIBUCIÓN DE LA CARGA DE TRÁFICO

La distribución de la carga de tráfico muestra el porcentaje medio de ocupación del ancho de banda utilizado durante el periodo de medida.

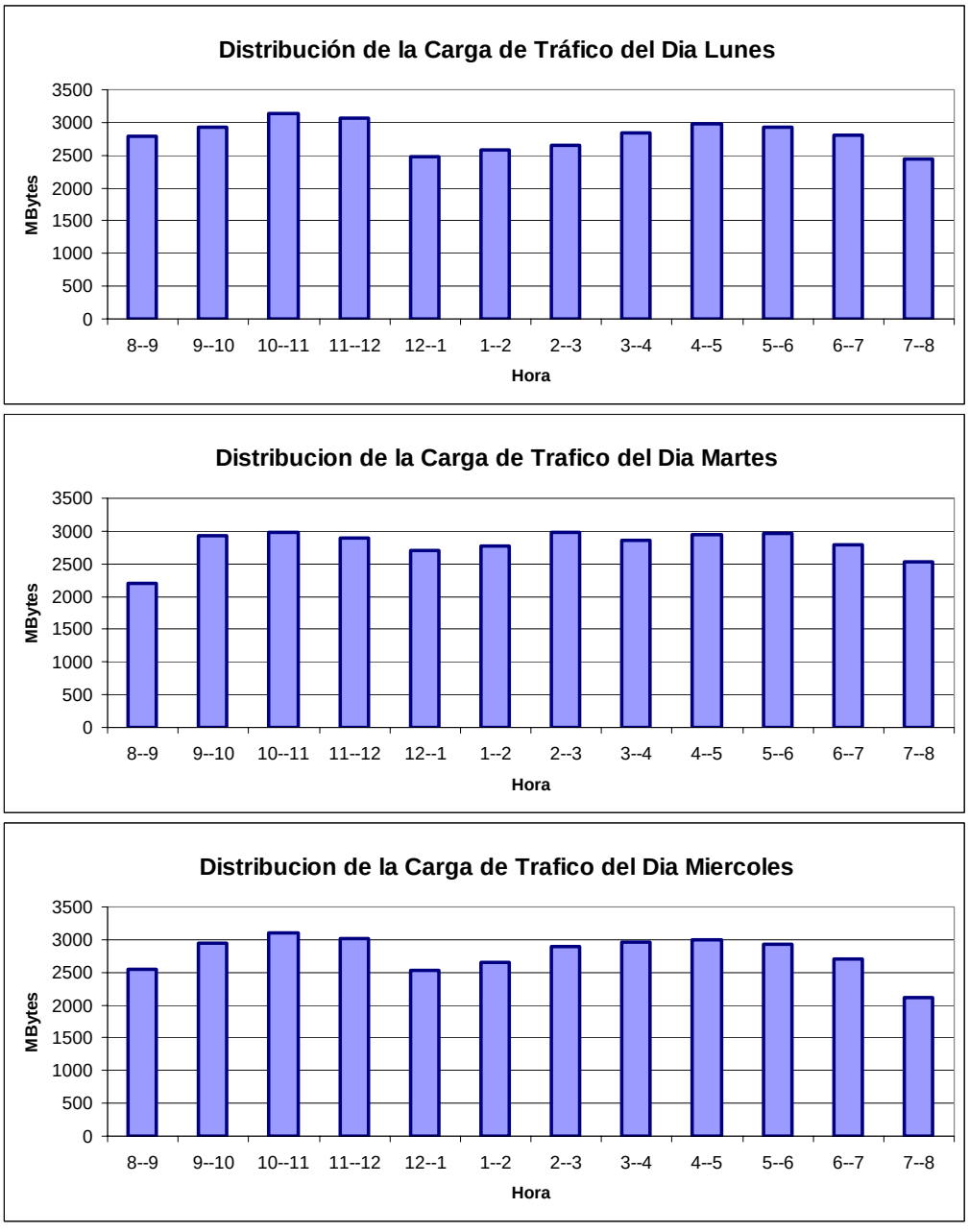
Uno de los principales motivos para realizar este análisis es detectar picos de actividad en el día, que luego se utilizan para precisar quien los genera.

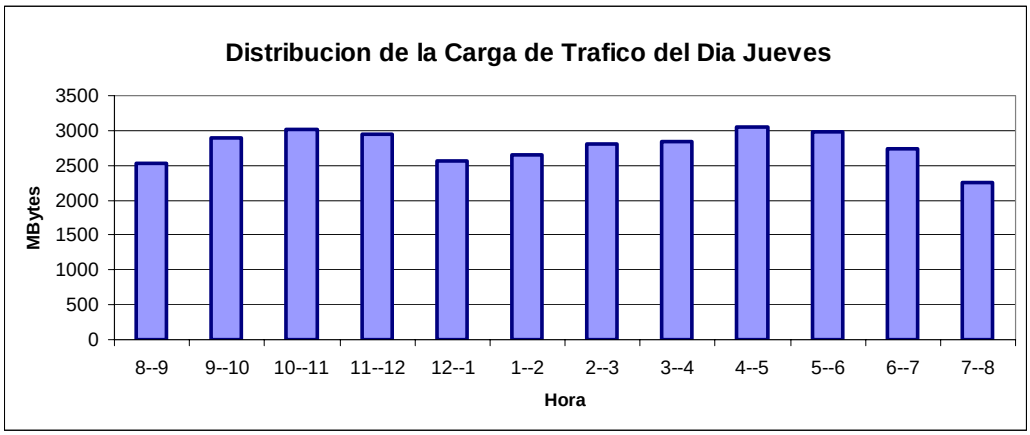
Cuando los picos son consistentemente altos, puede ser indicativo de que:

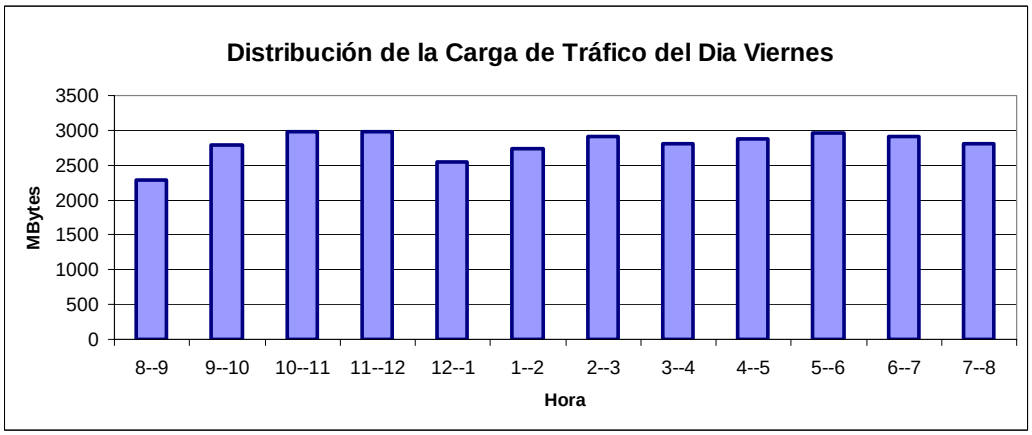
- El segmento o subred debe ser dividido
- Se está utilizando una aplicación exigente
- Hay procesos que deben ser trasladados a otro horario.

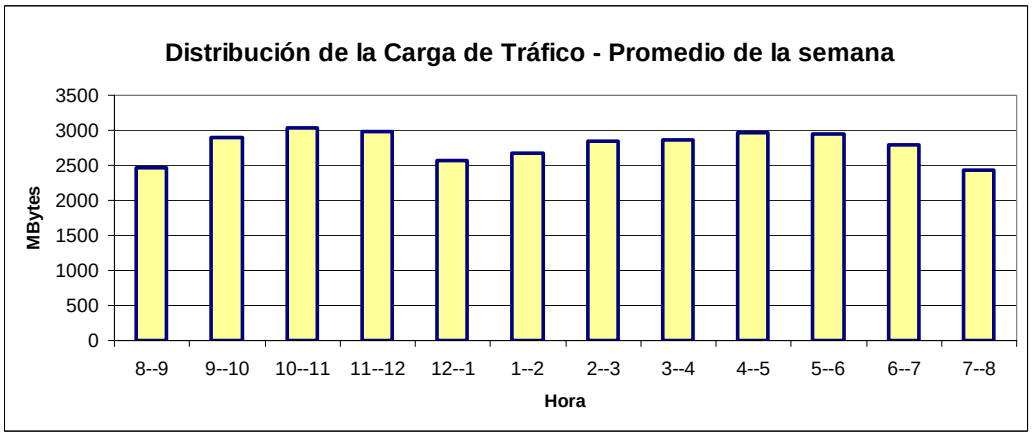
En la figura 25 se visualiza la distribución de la carga de tráfico en un gráfico de columnas en donde el eje ordenado representa el consumo de tráfico (Mbytes) y la abcisa representa el tiempo (horas).

Figura 25. Distribución de la carga de tráfico.




Distribucion de la Carga de Trafico del Dia Jueves
MBytes
3500
3000
2500
2000
1500
1000
500
0
8--9
9--10
10--11
11--12
12--1
1--2
2--3
3--4
4--5
5--6
6--7
7--8
Hora


Distribución de la Carga de Tráfico del Dia Viernes
MBytes
3500
3000
2500
2000
1500
1000
500
0
8--9
9--10
10--11
11--12
12--1
1--2
2--3
3--4
4--5
5--6
6--7
7--8
Hora


Distribución de la Carga de Tráfico - Promedio de la semana
MBytes
3500
3000
2500
2000
1500
1000
500
0
8--9
9--10
10--11
11--12
12--1
1--2
2--3
3--4
4--5
5--6
6--7
7--8
Hora

Se puede notar que existe cierta tendencia en el tráfico del enlace externo. En las primeras horas de la mañana se presenta un tráfico relativamente bajo, igual que en las horas del mediodía y finalizando el día. También se debe notar que existen picos en el consumo, hacia las 10:00 am y las 4:00 pm.

Se puede concluir que el comportamiento del tráfico se debe a los hábitos de los usuarios.

La carga de tráfico tiene una pendiente positiva debido a que a tempranas horas de la mañana, los usuarios encienden los equipos y hacen login, bajan aplicaciones y típicamente responden los mensajes de correo pendientes.

El periodo anterior al mediodía, cuando todos los usuarios están tratando de no dejar pendientes para la tarde, se incrementa el volumen de tráfico para luego decaer a las horas del medio día.

Se tiene un incremento hacia las 2:00 pm cuando los usuarios retornan a su jornada, este incremento se estabiliza hasta finalizar la tarde, para posteriormente mostrar un decaimiento, debido a que los usuarios dejan sus puestos de trabajo.

Con este análisis se obtiene un estimado del ancho de banda promedio utilizado en el enlace externo (ver tabla 7), este promedio es menor al ancho de banda real del enlace externo debido a la variabilidad del consumo de tráfico.

Tabla 7. Distribución de la carga de tráfico y ancho de banda promedio.

DÍA	CARGA	ANCHO DE BANDA (Promedio)
Lunes	33,610 GB	6,224 Mbps
Martes	33,515 GB	6,206 Mbps
Miércoles	33,367 GB	6,179 Mbps
Jueves	33,270 GB	6,161 Mbps
Viernes	33,596 GB	6,221 Mbps

La tabla anterior nos muestra que existe un aprovechamiento real cercano al 65 % en promedio. Cabe mencionar que el enlace externo en las horas pico se encuentra funcionando cerca a su capacidad total.

5. CONCLUSIONES

El trabajo que se describe en este proyecto, contribuye sustancialmente a la Universidad, identificando el estado real del enlace externo de la red de datos. Este proyecto contribuye a identificar acciones destinadas a mejorar aspectos como organización, control, administración y distribución de recursos en la red, así como agilizar labores de mejoramiento, mantenimiento y supervisión en la misma; esto se logra a través de registros y estadísticas finales.

Este material incluye información sobre el comportamiento del enlace externo a nivel lógico, estimando estadísticas del flujo de tráfico, de distribución de tamaño de paquetes, distribución de protocolos, consumo de las principales subredes y recomendaciones orientadas a mejorar el buen funcionamiento del enlace.

Para la selección de la metodología se realizó una serie de pruebas preliminares las cuales permitieron determinar el correcto escenario de medición, de tal forma que no afectara el desempeño del enlace.

Utilizando como base literatura técnica y trabajos realizados con anterioridad, se determinó capturar y procesar la totalidad de los datos. Aunque esta alternativa es menos eficiente, genera resultados confiables sin ningún margen de error.

Teniendo en cuenta características como modo de operación promiscuo, opción de exportación de datos, presentación de la información de las capturas, análisis de protocolos y tipo de software (*freeware*), se decidió utilizar como *sniffer* el software de monitoreo **Ethereal**; esta herramienta cumple a cabalidad los parámetros seleccionados para el análisis.

Se desarrolló una aplicación sobre Matlab 7.0, la cual permitió llevar a cabo la etapa de procesado de los datos. Se obtuvieron satisfactoriamente las variables requeridas para el análisis del tráfico. El código fuente se encuentra adjunto en el anexo A.

A partir del análisis de datos capturados en el enlace externo de la red de datos se llegó a las siguientes conclusiones:

- Se determinó en la distribución de tamaño de paquetes, que existe un alto porcentaje dentro del rango de 1023 bytes a 1518 bytes, seguido por el rango de 0 bytes a los 64 bytes.

  Existe un balance en la distribución de tamaño de paquetes. Este balance es de suma importancia teniendo en cuenta que si existiera un muy alto porcentaje de paquetes pequeños, indicaría que la eficiencia del enlace se ve afectada por frecuentes colisiones, tormentas de broadcast y un overhead relativamente grande. Un muy alto porcentaje de paquetes de gran tamaño incide en el retardo medio esperado ya que un paquete de gran tamaño tarda más tiempo en ser transmitido y liberar el medio, también presentan una gran probabilidad de error en la transmisión.

- De la distribución de protocolos se encontró que el mayor consumo de tráfico es debido al protocolo de aplicación HTTP, esto se debe a que este protocolo comúnmente es el más utilizado en la navegación de Internet.

  La segunda aplicación de mayor consumo se encuentra en las aplicaciones P2P.

Actualmente, el auge de las aplicaciones de intercambio de archivos entre iguales (P2P) lleva a que Internet se utilice cada vez más para transmitir contenidos de tipo lúdico. Esta transmisión llega a utilizar un porcentaje significativo del ancho de banda del enlace externo.

La creciente utilización de Internet con fines lúdicos puede acarrear problemas para los responsables de la red de datos, sobre todo cuando estas no están orientadas a la actividad lúdica, como es el caso de la red de datos de la Universidad. En primer lugar, consumen un excesivo ancho de banda, perjudicando a los usuarios que utilizan la red para los fines productivos para los que fue creada (académicos, investigación, etc.). En segundo lugar, muchas veces el intercambio de contenido es una actividad no reglamentada, debido a que esos contenidos se encuentran protegidos por derechos de autor.

- Las principales subredes que consumen el 52 % del ancho de banda del enlace son las que presentan un mayor porcentaje de uso. En estas 10 subredes se tiene aproximadamente 500 estaciones conectadas a la red de datos de la Universidad.

  La implementación de subredes en la Universidad cumple una buena labor en la agrupación de segmentos físicos permitiendo contención de tráfico y separación de dominios de colisión; lo cual contribuye al mejoramiento del desempeño de la red de datos.

- La carga de tráfico presenta un comportamiento similar en cada uno de los días que se evaluó. La utilización promedio del ancho de banda del enlace externo es de aproximadamente 65%; esto se

debe a que existe un menor consumo de recursos al empezar y al finalizar el día.

- Con el estudio del consumo de las principales subredes se identifico en cuales se deben enfocar mecanismos para mejorar el desempeño de la red. Algunas de estas subredes son: IQUI, petróleos y Laboratorio de pesados.

6. RECOMENDACIONES

- Al momento de realizar la captura de tráfico se debe tener un equipo dedicado exclusivamente al proceso de la toma de datos, ya que introducir tráfico puede generar unos resultados distorsionados del comportamiento real de la red.

- La elección del horario y días de captura deben reflejar el tráfico normal del enlace externo, para esto la Universidad debe estar en condiciones normales de funcionamiento.

- En posteriores estudios al enlace externo se debe tener en cuenta el incremento del ancho de banda para seleccionar una metodología de captura acertada.

- Se deben acoger mecanismos para regular el tráfico de protocolos P2P tales como:

    - Adoptar políticas para impedir la futura instalación de aplicaciones P2P en las estaciones de trabajo.
    - Hacer un filtrado identificando las cabeceras que caracterizan algunas de las principales aplicaciones P2P.
    - Identificar las estaciones que están consumiendo ancho de banda utilizando este protocolo, por medio del monitoreo de la red.

- Eliminando el tráfico generado por aplicaciones p2p se obtendría un mejor aprovechamiento del ancho de banda que dispone el enlace, optimizando el desempeño de la red; por lo cual se justifica la

adquisición de software y hardware que permita restringir tal tipo de aplicaciones.

- Con ayuda del código fuente utilizado en este proyecto, desarrollar un programa con fines educativos, con una interfaz de usuario, que permita una mejor comprensión de algunas variables que influyen en el desempeño de la red, tales como los presentes en este proyecto: distribución de protocolos, distribución de tamaño de paquetes, consumo de subredes, carga de tráfico; además se puede profundizar en variables como: saturación, picos de utilización, entre otros.

- Periódicamente se debe realizar un escaneo general de la red utilizando alguna herramienta de monitorización de red, con el fin de prever posibles errores y así mantener un buen desempeño de la red.

- Este proyecto contribuye significativamente a mejorar los servicios ofrecidos y administrados por la División de Servicios de Información, mediante el aporte de registros y estadísticas determinando una línea de base que sirve como punto de referencia para estudios y acciones futuras.

BIBLIOGRAFIA

[1]. SPURGEON, Charles. Ethernet. The Definitive Guide, United States of America, O'Reilly & Associates, 2000.

[2]. TANENBAUM, Andrew. Redes de computadoras, Tercera Edición, México, Prentice Hall Hispanoamericana, 1997.

[3]. BREYER, Robert y RILEY, Sean. Switched, Fast and Gigabit Ethernet, Third Edition, United States of America, MacMillan Technical Publishing, 1999.

[4]. OPPENHEIMER, Priscilla. Top-Down Network Design. A systems analysis approach to enterprise network design, Indiana, Cisco Press, 2001.

[5]. L. AGUILAR SINDES. Análisis de tráfico y diagnóstico en redes locales teoría y método, Aguilar & Asociados, Buenos Aires, 2002.

[6]. STALLINGS, William. Comunicaciones y redes de computadores, Quinta Edición, Madrid, Prentice Hall, 1998.

[7]. D. Awduche Movaz Networks, et al. Network Working Group Request for Comments: 3272 - Overview and Principles of Internet Traffic Engineering. Disponible en Internet: <http://www.ietf.org/rfc/rfc3272.txt >, Mayo de 2002.

[8]. Paola Fernanda Guzmán Castillo. ANÁLISIS DE LA GESTIÓN DE LOS DISPOSITIVOS ADMINISTRABLES EN LA RED DE DATOS INSTITUCIONAL. Universidad Industrial de Santander. Tesis de Maestría, 2005.

[9]. BUCHANAN Robert W., THE ART OF TESTING NETWORK SYSTEMS, Jhon Wiley & Sons, Inc. 1996.

[10]. IANA – Internet Assigned Numbers Authority. http://www.iana.org

[11]. J. Reynolds, J. Postel ISI. Request for Comments: 1700 - ASSIGNED NUMBERS. Disponible en Internet: http://www.rfc-editor.org/rfc/rfc1700.txt

ANEXO A. CODIGO FUENTE DE LA APLICACIÓN DESARROLLADA EN MATLAB 7.0

FINAL.m

```
clc
clear
vidi =input(' Que numero desea empezar la carga : ');
vidf =input(' Que numero desea finalizar la carga : ');
jk=0;
for w=vidi:vidf,
   cm=int2str(w);
   nom=['martes' cm '.txt']; %En este caso se analizan los del día martes.

[a,b,c,d,e,f,g,h,i] = textread(nom,'%n%s%s%s%n%s%s%s%s','headerlines',1);  %Este comando nos permite importar las capturas de documento texto y organizarla en una matriz.
long=length(a);
jk=jk+1; % contador de ciclos de carga

%filtro comunicación sniffer switch, debido a que existe un pequeño trafico de paquetes entre el switch y el sniffer , el cual no es relevante
swps=(strcmp(c,'192.168.5.188'));
swpd=(strcmp(d,'192.168.5.188'));
rwps=(strcmp(c,'192.168.9.2'));
rwpd=(strcmp(d,'192.168.9.2'));

psr=sum(swps.*rwpd);
prs=sum(rwps.*swpd);

pbsr=sum((swps.*rwpd).*e);
pbrs=sum((rwps.*swpd).*e);


max=long-(psr+prs); %Paquetes reales en la muestra
maxbytes=sum(e)-(pbsr+pbrs); %bytes reales en la muestra

tsr=(swps.*rwpd)+(rwps.*swpd);
ep=e+(tsr*2000);
pack=GOKU(ep); % esta función fue creada específicamente para obtener la distribución de tamaño de paquetes.
```

```
packe(jk,1)=w;
packe(jk,2)=max;
packe(jk,3)=pack(1);
packe(jk,4)=pack(2);
packe(jk,5)=pack(3);
packe(jk,6)=pack(4);
packe(jk,7)=pack(5);
packe(jk,8)=pack(6);


t=strcmp(h,'TCP');  %vector de protocolo TCP incluyendo r-s
tb=sum(e.*t);

%A continuación se obtiene la distribución de protocolos por bytes y numero de paquetes,
analizando los puertos utilizados por cada paquete.

   %Filtro HTTP
   h1=strcmp(f,'http');
   h2=strcmp(f,'8080');
   h3=strcmp(f,'https');
   h4=strcmp(g,'http');
   h5=strcmp(g,'8080');
   h6=strcmp(g,'https');

   realhttp1=sum(t.*h1);
   realhttp2=sum(t.*h2);
   realhttp3=sum(t.*h3);
   realhttp4=sum(t.*h4);
   realhttp5=sum(t.*h5);
   realhttp6=sum(t.*h6);

   httotal=realhttp1+realhttp2+realhttp3+realhttp4+realhttp5+realhttp6;

  %filtro HTTP por bytes
   hby1=sum(e.*h1.*t);
   hby2=sum(e.*h2.*t);
   hby3=sum(e.*h3.*t);
   hby4=sum(e.*h4.*t);
   hby5=sum(e.*h5.*t);
   hby6=sum(e.*h6.*t);

   httotalb=hby1+hby2+hby3+hby4+hby5+hby6;
```

```
%Filtro Gnutella
gnu1=strcmp(f,'6346');
gnu2=strcmp(f,'6347');
gnu3=strcmp(f,'6348');
realgnu1=sum(t.*gnu1);
realgnu2=sum(t.*gnu2);
realgnu3=sum(t.*gnu3);
htgnu=realgnu1+realgnu2+realgnu3;

%Filtro Gnutella por bytes
realgnu1b=sum(e.*t.*gnu1);
realgnu2b=sum(e.*t.*gnu2);
realgnu3b=sum(e.*t.*gnu3);
htgnub=realgnu1b+realgnu2b+realgnu3b;

%Filtro Edonkey
edo1=sum(t.*strcmp(f,'4242'));
edo2=sum(t.*strcmp(f,'5555'));
edo3=sum(t.*strcmp(f,'3306'));
edo4=sum(t.*strcmp(f,'2323'));
edo5=sum(t.*strcmp(f,'6667'));
edo6=sum(t.*strcmp(f,'7778'));
edo7=sum(t.*strcmp(g,'4242'));
edo8=sum(t.*strcmp(g,'5555'));
edo9=sum(t.*strcmp(g,'3306'));
edo10=sum(t.*strcmp(g,'2323'));
edo11=sum(t.*strcmp(g,'6667'));
edo12=sum(t.*strcmp(g,'7778'));


htedo=edo1+edo2+edo3+edo4+edo5+edo6+edo7+edo8+edo9+edo10+edo11+edo12;


ed1=sum(t.*strcmp(f,'4661'));
ed2=sum(t.*strcmp(f,'4662'));
ed3=sum(t.*strcmp(f,'4663'));
ed4=sum(t.*strcmp(f,'4664'));
ed5=sum(t.*strcmp(f,'4665'));
ed6=sum(t.*strcmp(f,'4666'));
ed7=sum(t.*strcmp(f,'4667'));
ed8=sum(t.*strcmp(f,'4668'));
```

```
ed9=sum(t.*strcmp(f,'4669'));
ed10=sum(t.*strcmp(f,'4670'));
ed11=sum(t.*strcmp(f,'4671'));
ed12=sum(t.*strcmp(f,'4672'));
ed13=sum(t.*strcmp(g,'4661'));
ed14=sum(t.*strcmp(g,'4662'));
ed15=sum(t.*strcmp(g,'4663'));
ed16=sum(t.*strcmp(g,'4664'));
ed17=sum(t.*strcmp(g,'4665'));
ed18=sum(t.*strcmp(g,'4666'));
ed19=sum(t.*strcmp(g,'4667'));
ed20=sum(t.*strcmp(g,'4668'));
ed21=sum(t.*strcmp(g,'4669'));
ed22=sum(t.*strcmp(g,'4670'));
ed23=sum(t.*strcmp(g,'4671'));
ed24=sum(t.*strcmp(g,'4672'));


hted=ed1+ed2+ed3+ed4+ed5+ed6+ed7+ed8+ed9+ed10+ed11+ed12+ed13+ed14+ed15+ed16+ed
17+ed18+ed19+ed20+ed21+ed22+ed23+ed24;

%Filtro Edonkey por bytes
edo1b=sum(e.*t.*strcmp(f,'4242'));
edo2b=sum(e.*t.*strcmp(f,'5555'));
edo3b=sum(e.*t.*strcmp(f,'3306'));
edo4b=sum(e.*t.*strcmp(f,'2323'));
edo5b=sum(e.*t.*strcmp(f,'6667'));
edo6b=sum(e.*t.*strcmp(f,'7778'));
edo7b=sum(e.*t.*strcmp(g,'4242'));
edo8b=sum(e.*t.*strcmp(g,'5555'));
edo9b=sum(e.*t.*strcmp(g,'3306'));
edo10b=sum(e.*t.*strcmp(g,'2323'));
edo11b=sum(e.*t.*strcmp(g,'6667'));
edo12b=sum(e.*t.*strcmp(g,'7778'));


htedob=edo1b+edo2b+edo3b+edo4b+edo5b+edo6b+edo7b+edo8b+edo9b+edo10b+edo11b+edo12
b;


ed1b=sum(e.*t.*strcmp(f,'4661'));
```

```
ed2b=sum(e.*t.*strcmp(f,'4662'));
ed3b=sum(e.*t.*strcmp(f,'4663'));
ed4b=sum(e.*t.*strcmp(f,'4664'));
ed5b=sum(e.*t.*strcmp(f,'4665'));
ed6b=sum(e.*t.*strcmp(f,'4666'));
ed7b=sum(e.*t.*strcmp(f,'4667'));
ed8b=sum(e.*t.*strcmp(f,'4668'));
ed9b=sum(e.*t.*strcmp(f,'4669'));
ed10b=sum(e.*t.*strcmp(f,'4670'));
ed11b=sum(e.*t.*strcmp(f,'4671'));
ed12b=sum(e.*t.*strcmp(f,'4672'));
ed13b=sum(e.*t.*strcmp(g,'4661'));
ed14b=sum(e.*t.*strcmp(g,'4662'));
ed15b=sum(e.*t.*strcmp(g,'4663'));
ed16b=sum(e.*t.*strcmp(g,'4664'));
ed17b=sum(e.*t.*strcmp(g,'4665'));
ed18b=sum(e.*t.*strcmp(g,'4666'));
ed19b=sum(e.*t.*strcmp(g,'4667'));
ed20b=sum(e.*t.*strcmp(g,'4668'));
ed21b=sum(e.*t.*strcmp(g,'4669'));
ed22b=sum(e.*t.*strcmp(g,'4670'));
ed23b=sum(e.*t.*strcmp(g,'4671'));
ed24b=sum(e.*t.*strcmp(g,'4672'));


htedb=ed1b+ed2b+ed3b+ed4b+ed5b+ed6b+ed7b+ed8b+ed9b+ed10b+ed11b+ed12b+ed13b+ed14
b+ed15b+ed16b+ed17b+ed18b+ed19b+ed20b+ed21b+ed22b+ed23b+ed24b;

%filtro smpt
smt1=sum(t.*strcmp(f,'smtp'));

%filtro smpt por bytes
smt1b=sum(e.*t.*strcmp(f,'smtp'));

%Filtro Bitorrent
bit1=sum(t.*strcmp(f,'6881'));
bit2=sum(t.*strcmp(f,'6882'));
bit3=sum(t.*strcmp(f,'6883'));
bit4=sum(t.*strcmp(f,'6884'));
bit5=sum(t.*strcmp(f,'6885'));
bit6=sum(t.*strcmp(f,'6886'));
bit7=sum(t.*strcmp(f,'6887'));
```

```
bit8=sum(t.*strcmp(f,'6888'));
bit9=sum(t.*strcmp(f,'6889'));

htbit=bit1+bit2+bit3+bit4+bit5+bit6+bit7+bit8+bit9;

%Filtro Bitorrent por bytes
bit1b=sum(e.*t.*strcmp(f,'6881'));
bit2b=sum(e.*t.*strcmp(f,'6882'));
bit3b=sum(e.*t.*strcmp(f,'6883'));
bit4b=sum(e.*t.*strcmp(f,'6884'));
bit5b=sum(e.*t.*strcmp(f,'6885'));
bit6b=sum(e.*t.*strcmp(f,'6886'));
bit7b=sum(e.*t.*strcmp(f,'6887'));
bit8b=sum(e.*t.*strcmp(f,'6888'));
bit9b=sum(e.*t.*strcmp(f,'6889'));

htbitb=bit1b+bit2b+bit3b+bit4b+bit5b+bit6b+bit7b+bit8b+bit9b;

%Filtro kazaa
kaz1=sum(t.*strcmp(f,'1214'));
kaz2=sum(t.*strcmp(g,'1214'));
realkaz=kaz1+kaz2;
%Filtro kazaa por bytes
kaz1b=sum(e.*t.*strcmp(f,'1214'));
kaz2b=sum(e.*t.*strcmp(g,'1214'));
realkazb=kaz1b+kaz2b;

dTCP=sum(t)-(psr+prs+httotal+htedo+hted+htgnu+smt1+htbit+realkaz); %·paquetes puertos de usuario(TCP)
dTCPb=tb-(pbsr+pbrs+httotalb+htedob+htedb+htgnub+smt1b+htbitb+realkazb); %·bytes puertos de usuario(TCP)

%Distribución total de protocolos por paquetes
dp(1,jk)=w;
dp(2,jk)=max;
dp(3,jk)=sum(strcmp(h,'HTTP'))+httotal;
dp(4,jk)=sum(strcmp(h,'eDonkey'))+htedo+hted;
dp(5,jk)=sum(strcmp(h,'Gnutella'))+htgnu;
dp(6,jk)=dTCP;
dp(7,jk)=sum(strcmp(f,'ARP'));
dp(8,jk)=sum(strcmp(f,'ICMP'));
dp(9,jk)=sum(strcmp(f,'STP'));
```

```
dp(10,jk)=sum(strcmp(h,'UDP'));
dp(11,jk)=sum(strcmp(h,'SMB'));
dp(12,jk)=sum(strcmp(h,'FTP'));
dp(13,jk)=sum(strcmp(h,'FTP-DATA'));
dp(14,jk)=sum(strcmp(h,'DNS'));
dp(15,jk)=htbit;
dp(16,jk)=smt1;
dp(17,jk)=sum(strcmp(h,'TIME'));
dp(18,jk)=realkaz;
dp(19,jk)=(max)-
(dp(3,jk)+dp(4,jk)+dp(5,jk)+dp(6,jk)+dp(7,jk)+dp(8,jk)+dp(9,jk)+dp(10,jk)+dp(11,jk)+dp(12,jk)+
dp(13,jk)+dp(14,jk)+dp(15,jk)+dp(16,jk)+dp(17,jk)+dp(18,jk));
```

%Distribución total de protocolos por bytes

```
dis(1,jk)=w;
dis(2,jk)=maxbytes;
dis(3,jk)=sum(e.*strcmp(h,'HTTP'))+httotalb;
dis(4,jk)=sum(e.*strcmp(h,'eDonkey'))+htedob+htedb;
dis(5,jk)=sum(e.*strcmp(h,'Gnutella'))+htgnub;
dis(6,jk)=dTCPb;
dis(7,jk)=sum(e.*strcmp(f,'ARP'));
dis(8,jk)=sum(e.*strcmp(f,'ICMP'));
dis(9,jk)=sum(e.*strcmp(f,'STP'));
dis(10,jk)=sum(e.*strcmp(h,'UDP'));
dis(11,jk)=sum(e.*strcmp(h,'SMB'));
dis(12,jk)=sum(e.*strcmp(h,'FTP'));
dis(13,jk)=sum(e.*strcmp(h,'FTP-DATA'));
dis(14,jk)=sum(e.*strcmp(h,'DNS'));
dis(15,jk)=htbitb;
dis(16,jk)=smt1b;
dis(17,jk)=sum(e.*strcmp(h,'TIME'));
dis(18,jk)=realkazb;
dis(19,jk)=(maxbytes)-
(dis(3,jk)+dis(4,jk)+dis(5,jk)+dis(6,jk)+dis(7,jk)+dis(8,jk)+dis(9,jk)+dis(10,jk)+dis(11,jk)+dis(12,j
k)+dis(13,jk)+dis(14,jk)+dis(15,jk)+dis(16,jk)+dis(17,jk)+dis(18,jk));
```

%Consumo de Subredes por bytes, tomando como referencia las direcciones que se tienen especificadas en la Universidad se realiza este análisis.

```
dsub=strrep(d,'192.168.','');
```
%se separa la ubicación de la dirección IP que nos permite analizar el consumo de las subredes.

```
esta(1,jk)=sum(e.*(strncmp(dsub,'18',2)));%192.168.18.0    (Biblioteca)
```

```
esta(2,jk)=sum(e.*(strncmp(dsub,'19',2)));%192.168.19.0  (Servidores)
esta(3,jk)=sum(e.*(strncmp(dsub,'20',2)));%192.168.20.0  (Ciencias Humanas)
esta(4,jk)=sum(e.*(strncmp(dsub,'21',2)));%192.168.21.0  (Educacion)
esta(5,jk)=sum(e.*(strncmp(dsub,'22',2)));%192.168.22.0  (LEA)
esta(6,jk)=sum(e.*(strncmp(dsub,'23',2)));%192.168.23.0  (Base datos)
esta(7,jk)=sum(e.*(strncmp(dsub,'24',2)));%192.168.24.0  (Lab. Pesados)
esta(8,jk)=sum(e.*(strncmp(dsub,'27',2)));%192.168.27.0  (Lab. Livianos)
esta(9,jk)=sum(e.*(strncmp(dsub,'28',2)));%192.168.28.0  (Fisica1)
esta(10,jk)=sum(e.*(strncmp(dsub,'29',2)));%192.168.29.0  (Fisica2)
esta(11,jk)=sum(e.*(strncmp(dsub,'30',2)));%192.168.30.0  (Salud Admon)
esta(12,jk)=sum(e.*(strncmp(dsub,'31',2)));%192.168.31.0  (CICELPA,LIMN,INV,CEIAM)
esta(13,jk)=sum(e.*(strncmp(dsub,'32',2)));%192.168.32.0  (Artes)
esta(14,jk)=sum(e.*(strncmp(dsub,'33',2)));%192.168.33.0  (CAPRUIS )
esta(15,jk)=sum(e.*(strncmp(dsub,'34',2)));%192.168.34.0  (Diseño Industrial)
esta(16,jk)=sum(e.*(strncmp(dsub,'35',2)));%192.168.35.0  (Bienestar)
esta(17,jk)=sum(e.*(strncmp(dsub,'36',2)));%192.168.36.0  (Luis A. Calvo)
esta(18,jk)=sum(e.*(strncmp(dsub,'37',2)));%192.168.37.0  (Ala Oriental) E. Administracion
esta(19,jk)=sum(e.*(strncmp(dsub,'38',2)));%192.168.38.0  (Ala Occidental) E. Administracion
esta(20,jk)=sum(e.*(strncmp(dsub,'39',2)));%192.168.39.0  (IQUI)
esta(21,jk)=sum(e.*(strncmp(dsub,'40',2)));%192.168.40.0  (Ing. Industrial)
esta(22,jk)=sum(e.*(strncmp(dsub,'41',2)));%192.168.41.0  (Posgrados)
esta(23,jk)=sum(e.*(strncmp(dsub,'42',2)));%192.168.42.0  (Planta Fisica)
esta(24,jk)=sum(e.*(strncmp(dsub,'43',2)));%192.168.43.0  (Mecanica)
esta(25,jk)=sum(e.*(strncmp(dsub,'44',2)));%192.168.44.0  (Petroleos)
esta(26,jk)=sum(e.*(strncmp(dsub,'45',2)));%192.168.45.0  (Alta Tension)
esta(27,jk)=sum(e.*(strncmp(dsub,'46',2)));%192.168.46.0  (Electrica)
esta(28,jk)=sum(e.*(strncmp(dsub,'47',2)));%192.168.47.0  (MORFOPAT)
esta(29,jk)=sum(e.*(strncmp(dsub,'48',2)));%192.168.48.0  (HURV)
esta(30,jk)=sum(e.*(strncmp(dsub,'49',2)));%192.168.49.0  (SALCONF)
esta(31,jk)=sum(e.*(strncmp(dsub,'50',2)));%192.168.50.0  (INSED)
esta(32,jk)=sum(e.*(strncmp(dsub,'51',2)));%192.168.51.0  (FAVUIS)
esta(33,jk)=sum(e.*(strncmp(dsub,'54',2)));%192.168.54.0  (Bucarica)
esta(34,jk)=sum(e.*(strncmp(dsub,'58',2)));%192.168.58.0  (Financiero  Tesoreria)  E.
Administracion
esta(35,jk)=sum(e.*(strncmp(dsub,'59',2)));%192.168.59.0  (Admisiones) E. Administracion
esta(36,jk)=sum(e.*(strncmp(dsub,'61',2)));%192.168.61.0  (LEA Salas 2-3-5)
esta(37,jk)=sum(e.*(strncmp(dsub,'62',2)));%192.168.62.0  (LEA Salas 4-6)
esta(38,jk)=sum(e.*(strncmp(dsub,'65',2)));%192.168.65.0  (Sistemas Lab JAV)
esta(39,jk)=sum(e.*(strncmp(dsub,'71',2)));%192.168.71.0  (Alta Tension Lab Elect)
esta(40,jk)=sum(e.*(strncmp(dsub,'72',2)));%192.168.72.0  (HIDR)
esta(41,jk)=sum(e.*(strncmp(dsub,'73',2)));%192.168.73.0  (CITI)
esta(42,jk)=sum(e.*(strncmp(dsub,'74',2)));%192.168.74.0  (BUCARICA CNBILING)
```

```
esta(43,jk)=sum(e.*(strncmp(dsub,'75',2)));%192.168.75.0  (Nodo PML Bucarica)
esta(44,jk)=sum(e.*(strncmp(dsub,'76',2)));%192.168.76.0  (Fundeuis)
esta(45,jk)=sum(e.*(strncmp(dsub,'80',2)));%192.168.80.0  (DSI)
esta(46,jk)=sum(e.*(strncmp(dsub,'81',2)));%192.168.81.0  (PLaneacion)
esta(47,jk)=sum(e.*(strncmp(dsub,'84',2)));%192.168.84.0  (Sistemas1)
esta(48,jk)=sum(e.*(strncmp(dsub,'85',2)));%192.168.85.0  (ICI,CEIC Civil Geomatica)
esta(49,jk)=sum(e.*(strncmp(dsub,'86',2)));%192.168.86.0  (Civil Geomatica )
esta(50,jk)=sum(e.*(strncmp(dsub,'87',2)));%192.168.87.0  (Civil Geomatica 3)
esta(51,jk)=sum(e.*(strncmp(dsub,'88',2)));%192.168.88.0  (Petroleos CPIP)
esta(52,jk)=sum(e.*(strncmp(dsub,'89',2)));%192.168.89.0  (Publicaciones)
esta(53,jk)=sum(e.*(strncmp(dsub,'92',2)));%192.168.92.0  (Asesorias)
esta(54,jk)=sum(e.*(strncmp(dsub,'93',2)));%192.168.93.0  (Incubadora de Empresas)
esta(55,jk)=sum(e.*(strncmp(dsub,'94',2)));%192.168.94.0  (CIDLIS, GISEL)
esta(56,jk)=sum(e.*(strncmp(dsub,'96',2)));%192.168.96.0  (Teleuis)
esta(57,jk)=sum(e.*(strncmp(dsub,'97',2)));%192.168.97.0  (Recursos Humanos)
esta(58,jk)=sum(e.*(strncmp(dsub,'99',2)));%192.168.99.0  (SOCACAD)
esta(59,jk)=sum(e.*(strncmp(dsub,'100',3)));%192.168.100.0    (ADMBAR)
esta(60,jk)=sum(e.*(strncmp(dsub,'101',3)));%192.168.101.0    (BARBOSA)
esta(61,jk)=sum(e.*(strncmp(dsub,'102',3)));%192.168.102.0    (MALAGA)
esta(62,jk)=sum(e.*(strncmp(dsub,'105',3)));%192.168.105.0    ( Fisioterapia 1)
esta(63,jk)=sum(e.*(strncmp(dsub,'106',3)));%192.168.106.0    (Nutricion)
esta(64,jk)=sum(e.*(strncmp(dsub,'107',3)));%192.168.107.0    (Instituto de Lenguas)
esta(65,jk)=sum(e.*(strcmp(dsub,'Broadcast')));%Broadcast
esta(66,jk)=sum(e.*(strcmp(dsub,'Spanning-tree-(for-bridges)_00')));%Spanning-tree-(for-
bridges)_00
esta(67,jk)=sum(e.*(strncmp(dsub,'6.',2)));%192.168.6.0      (Rack1 Guatiguara)

smby=sum(esta);
oesta=maxbytes-smby(jk);
esta(68,jk)=oesta;
```

%Consumo de Subredes por paquetes

```
estap(1,jk)=sum((strncmp(dsub,'18',2)));%192.168.18.0    (Biblioteca)
estap(2,jk)=sum((strncmp(dsub,'19',2)));%192.168.19.0    (Servidores)
estap(3,jk)=sum((strncmp(dsub,'20',2)));%192.168.20.0    (Ciencias Humanas)
estap(4,jk)=sum((strncmp(dsub,'21',2)));%192.168.21.0    (Educacion)
estap(5,jk)=sum((strncmp(dsub,'22',2)));%192.168.22.0    (LEA)
estap(6,jk)=sum((strncmp(dsub,'23',2)));%192.168.23.0    (Base datos)
estap(7,jk)=sum((strncmp(dsub,'24',2)));%192.168.24.0    (Lab. Pesados)
estap(8,jk)=sum((strncmp(dsub,'27',2)));%192.168.27.0    (Lab. Livianos)
estap(9,jk)=sum((strncmp(dsub,'28',2)));%192.168.28.0    (Fisica1)
estap(10,jk)=sum((strncmp(dsub,'29',2)));%192.168.29.0   (Fisica2)
```

```
estap(11,jk)=sum((strncmp(dsub,'30',2)));%192.168.30.0  (Salud Admon)
estap(12,jk)=sum((strncmp(dsub,'31',2)));%192.168.31.0  (CICELPA,LIMN,INV,CEIAM)
estap(13,jk)=sum((strncmp(dsub,'32',2)));%192.168.32.0  (Artes)
estap(14,jk)=sum((strncmp(dsub,'33',2)));%192.168.33.0  (CAPRUIS )
estap(15,jk)=sum((strncmp(dsub,'34',2)));%192.168.34.0  (Diseño Industrial)
estap(16,jk)=sum((strncmp(dsub,'35',2)));%192.168.35.0  (Bienestar)
estap(17,jk)=sum((strncmp(dsub,'36',2)));%192.168.36.0  (Luis A. Calvo)
estap(18,jk)=sum((strncmp(dsub,'37',2)));%192.168.37.0  (Ala Oriental) E. Administracion
estap(19,jk)=sum((strncmp(dsub,'38',2)));%192.168.38.0  (Ala Occidental) E. Administracion
estap(20,jk)=sum((strncmp(dsub,'39',2)));%192.168.39.0  (IQUI)
estap(21,jk)=sum((strncmp(dsub,'40',2)));%192.168.40.0  (Ing. Industrial)
estap(22,jk)=sum((strncmp(dsub,'41',2)));%192.168.41.0  (Posgrados)
estap(23,jk)=sum((strncmp(dsub,'42',2)));%192.168.42.0  (Planta Fisica)
estap(24,jk)=sum((strncmp(dsub,'43',2)));%192.168.43.0  (Mecanica)
estap(25,jk)=sum((strncmp(dsub,'44',2)));%192.168.44.0  (Petroleos)
estap(26,jk)=sum((strncmp(dsub,'45',2)));%192.168.45.0  (Alta Tension)
estap(27,jk)=sum((strncmp(dsub,'46',2)));%192.168.46.0  (Electrica)
estap(28,jk)=sum((strncmp(dsub,'47',2)));%192.168.47.0  (MORFOPAT)
estap(29,jk)=sum((strncmp(dsub,'48',2)));%192.168.48.0  (HURV)
estap(30,jk)=sum((strncmp(dsub,'49',2)));%192.168.49.0  (SALCONF)
estap(31,jk)=sum((strncmp(dsub,'50',2)));%192.168.50.0  (INSED)
estap(32,jk)=sum((strncmp(dsub,'51',2)));%192.168.51.0  (FAVUIS)
estap(33,jk)=sum((strncmp(dsub,'54',2)));%192.168.54.0  (Bucarica)
estap(34,jk)=sum((strncmp(dsub,'58',2)));%192.168.58.0  (Financiero Tesoreria) E. Administracion
estap(35,jk)=sum((strncmp(dsub,'59',2)));%192.168.59.0  (Admisiones) E. Administracion
estap(36,jk)=sum((strncmp(dsub,'61',2)));%192.168.61.0  (LEA Salas 2-3-5)
estap(37,jk)=sum((strncmp(dsub,'62',2)));%192.168.62.0  (LEA Salas 4-6)
estap(38,jk)=sum((strncmp(dsub,'65',2)));%192.168.65.0  (Sistemas Lab JAV)
estap(39,jk)=sum((strncmp(dsub,'71',2)));%192.168.71.0  (Alta Tension Lab Elect)
estap(40,jk)=sum((strncmp(dsub,'72',2)));%192.168.72.0  (HIDR)
estap(41,jk)=sum((strncmp(dsub,'73',2)));%192.168.73.0  (CITI)
estap(42,jk)=sum((strncmp(dsub,'74',2)));%192.168.74.0  (BUCARICA CNBILING)
estap(43,jk)=sum((strncmp(dsub,'75',2)));%192.168.75.0  (Nodo PML Bucarica)
estap(44,jk)=sum((strncmp(dsub,'76',2)));%192.168.76.0  (Fundeuis)
estap(45,jk)=sum((strncmp(dsub,'80',2)));%192.168.80.0  (DSI)
estap(46,jk)=sum((strncmp(dsub,'81',2)));%192.168.81.0  (PLaneacion)
estap(47,jk)=sum((strncmp(dsub,'84',2)));%192.168.84.0  (Sistemas1)
estap(48,jk)=sum((strncmp(dsub,'85',2)));%192.168.85.0  (ICI,CEIC Civil Geomatica)
estap(49,jk)=sum((strncmp(dsub,'86',2)));%192.168.86.0  (Civil Geomatica )
estap(50,jk)=sum((strncmp(dsub,'87',2)));%192.168.87.0  (Civil Geomatica 3)
estap(51,jk)=sum((strncmp(dsub,'88',2)));%192.168.88.0  (Petroleos CPIP)
estap(52,jk)=sum((strncmp(dsub,'89',2)));%192.168.89.0  (Publicaciones)
```

```
estap(53,jk)=sum((strncmp(dsub,'92',2)));%192.168.92.0   (Asesorias)
estap(54,jk)=sum((strncmp(dsub,'93',2)));%192.168.93.0   (Incubadora de Empresas)
estap(55,jk)=sum((strncmp(dsub,'94',2)));%192.168.94.0   (CIDLIS, GISEL)
estap(56,jk)=sum((strncmp(dsub,'96',2)));%192.168.96.0   (Teleuis)
estap(57,jk)=sum((strncmp(dsub,'97',2)));%192.168.97.0   (Recursos Humanos)
estap(58,jk)=sum((strncmp(dsub,'99',2)));%192.168.99.0   (SOCACAD)
estap(59,jk)=sum((strncmp(dsub,'100',3)));%192.168.100.0 (ADMBAR)
estap(60,jk)=sum((strncmp(dsub,'101',3)));%192.168.101.0 (BARBOSA)
estap(61,jk)=sum((strncmp(dsub,'102',3)));%192.168.102.0 (MALAGA)
estap(62,jk)=sum((strncmp(dsub,'105',3)));%192.168.105.0 (Fisioterapia 1)
estap(63,jk)=sum((strncmp(dsub,'106',3)));%192.168.106.0 (Nutricion)
estap(64,jk)=sum((strncmp(dsub,'107',3)));%192.168.107.0 (Instituto de Lenguas)
estap(65,jk)=sum((strcmp(dsub,'Broadcast')));%Broadcast
estap(66,jk)=sum((strcmp(dsub,'Spanning-tree-(for-bridges)_00')));%Spanning-tree-(for-
bridges)_00
estap(67,jk)=sum((strncmp(dsub,'6.',2)));%192.168.6.0    (Rack1 Guatiguara)
smpa=sum(estap);
oestap=max-smpa(jk);
estap(68,jk)=oestap;

end
```

GOKU.m **%Esta función fue creada para obtener la distribución de tamaño de paquetes, entre los rangos escogidos.**

```
function[packw] = GOKU(x)
packw(1)=0;
packw(2)=0;
packw(3)=0;
packw(4)=0;
packw(5)=0;
packw(6)=0;
max=length(x);
for i=1:max,

   if x(i)<=64
      packw(1)=packw(1)+1;
   else
     if x(i)<=127
      packw(2)=packw(2)+1;
      else
         if x(i)<=255
```

```
            packw(3)=packw(3)+1;
            else
               if x(i)<=511
               packw(4)=packw(4)+1;
               else
                  if x(i)<=1023
                  packw(5)=packw(5)+1;
                  else
                     if x(i)<=1518
                     packw(6)=packw(6)+1;
                     else
                     end
                  end
               end
            end
         end
      end
   end
end
```

ANEXO B. ESPECIFICACIONES DE LOS EQUIPOS UTILIZADOS

A continuación se listan las especificaciones y referencias de los equipos utilizados en la sala redes de la escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones de la Universidad Industrial de Santander para la puesta en marcha de las pruebas del proyecto.

1. SWITCH CAJUN P880

El switch central utilizado en la Universidad Industrial de Santander es un switch Cajun P880 marca Avaya, el cual cuenta con las siguientes características:

El ***switch Cajun P880 Routing*** es compatible con aplicaciones de voz, datos y video DayOne sin necesidad de costosas actualizaciones globales.

Admite hasta 768 puertos Ethernet 10/100, 128 puertos Gigabit Ethernet o 384 puertos 100Base-FX. Ofrece distintos tipos de tráfico con capacidad de reserva y restricción del ancho de banda, y compatibilidad con tráfico en tiempo real. Estas propiedades de Calidad de Servicio (QoS) son totalmente compatibles con los estándares del mercado. También ofrece una capacidad de enrutamiento de más de 1,5 millones de paquetes por segundo (pps) para cualquier módulo de medios de nivel 2 (únicamente) instalado.

Características destacables

- DayOne^{TM} Ready para aplicaciones de voz datos y video.
- Calidad de servicio (QoS) para evitar retrasos del tráfico vital.
- Capacidad de conmutación y enrutamiento de hasta 139 Gbps.

- Hasta 768 puertos 10/100 por cada switch.
- Hasta 128 puertos Gigabit.
- Hasta 384 puertos 100Base-FX.
- Tecnología Switch Architecture For Extreme Resiliency (SAFERTM) para eliminar todos los puntos vulnerables.

Sus especificaciones se encuentran en la tabla 1.

Tabla 1. Especificaciones del Switch Cajun P880.

	Modulos Serie 50	**Modulos Serie 80**
Panel posterior	**56 Gbps**	**139 Gbps**
Conmutación	**41 Gbps**	**106 Gbps**
Enrutamiento	**41 Gbps**	**106 Gbps**
No Máximo de puertos Gigabit	**60**	**128**
No Máximo de puertos 10/100 (Conectores Telco)	**720**	**768**
VLAN	**300**	**384**
Entrada de la Tabla de reenvío de direcciones	**1000**	**1000**
Entradas de la Tabla de reenvío de direcciones	**24.000**	**24.000**
Rutas	**16.000**	**16.000**
No Máximo de Flujos	**600.000**	**2.560.000**

Especificaciones físicas:

Suministro eléctrico:

- ✓ Tensión de entrada (CA): 100-120/200-240 VCA @ +6%, - 10%
- ✓ Frecuencia: 50-60 Hz

- ✓ Máxima corriente de entrada (por fuente de alimentación): 12,0 A @ 100-120 VAC 6,0 A @ 200-240 VA

Condiciones ambientales:

- ✓ Temperatura de funcionamiento: 0° a 40° C
- ✓ Temperatura de almacenamiento: -20° a 80°C
- ✓ Humedad relativa: 5% a 95% sin condensación

Dimensiones físicas:

- ✓ Ancho: 43,8 cm
- ✓ Diámetro: 45,72 cm
- ✓ Alto: 63.5cm

2. ADAPTADOR DE RED GIGABIT ETHERNET (Intel® PRO/1000 Server Adapter)

Figura 1. Adaptador de red gigabit ethernet (Intel® PRO/1000 Server Adapter)

Para la realización de la captura de datos se optó por la compra de una tarjeta de red Gigabit Ethernet con las siguientes especificaciones:

Compatibilidad de hardware:

- Puede trabajar con los siguientes tipos de slots:
  - ✓ Slot PCI bus master de 32-bit o 64-bit que opera a 33 o 64 MHz.
  - ✓ Slot PCI-X que opere a 66, 100 o 133 MHz.
- Mínimo 64MB de memoria del sistema.
- Todos los adaptadores Intel basados en fibra con conectores SC utilizan un láser de longitud de onda de 850 nm (1000Base-SX).
- Tipo de cable a usar y distancia operativa:
  - ✓ Fibra multimodo con 50 μm de diámetro de núcleo, su máxima longitud es de 550 metros.
  - ✓ Fibra multimodo con 62.5 μm de diámetro de núcleo, su máxima longitud es de 275 metros.
  - ✓ Conector de fibra óptica SC.
- Compatibilidad IEEE: 802.1p, 802.1Q, 802.3ac, 802.3ad, 802.3x, 802.3z, PCI v2.1.
- Drivers : Linux 2.2, 2.4; Windows XP, 2000, NT 4.0, Server 2003; Novell NetWare 6.x, 5.x, 4.2; UnixWare 7; Sun Solaris X86

Para objetivos de prueba y funcionamiento del adaptador de red se descargó un software de prueba de la pagina del fabricante del mismo, www.intel.com , cuyo nombre es Intel PROSet.

El software de diagnóstico Intel PROSet permite probar el adaptador para verificar si hay problemas con el hardware del adaptador, el cable o la conexión de red.

En la tabla 2 se muestran las especificaciones técnicas de la tarjeta de red Gigabit Ethernet.

Tabla 2. Especificaciones técnicas de la tarjeta de red Gigabit Ethernet.

Bus architecture:	**PCI**
Bus Connector:	**PCI 2.1** **32/64 bit** **(33 Mhz only)**
Transmission/ Connector	**SX Fiber Optic/ SC**
Cabling:	**50µm Multi-mode Fiber - 550m** **62.5µm Multi-mode Fiber - 275m**
Interrupt:	**INTA**
Available Speeds:	**1000 full-duplex only**
Standards Conformance:	**IEEE 802.1p** **IEEE 802.1Q** **IEEE 802.3ac** **IEEE 802.3ad** **IEEE 802.3x** **IEEE 802.3z** **PCI v2.1**
On-board memory:	**64KB**
H/W LEDs:	**TX Activity** **RX Activity** **Link** **Identity**

3. HUB AVAYA ARGENT BRANCH

Un hub es simplemente un aparato que repite las señales recibidas. Éste no sabe qué computadoras están conectadas a él, y tampoco hace ninguna clase de procesamiento de red basado en el computador origen o destino. Los Hubs son primordialmente usados como aparatos de bajo precio que permiten adherir más computadores a una red.

Pero, a medida que se incrementa el número de computadores, también se incrementa el tráfico innecesario en la red. Utilizar un hub para conectar una red no es muy seguro, ya que cualquier computador puede ser configurado para “escuchar” los mensajes que son transmitidos. Un hub no permite compartir automáticamente una conexión de Internet, aunque puede ser posible si se corre el software de Compartimiento de Conexión de Internet en un computador con conexión de alta velocidad.

Es preferible conectar la red con un switch en vez de Hub, especialmente desde que los Switches se han vuelto más baratos. Dentro de los equipos de red presentes en el laboratorio de la escuela se encuentran el HUB AVAYA ARGENT BRANCH cuyas características son:

- Posee 8 puertos LAN.
- Posee dos slots para módulos ISDN.
  Puede conectar 2 LANS – 10 MHz y otra de 100 MHz, estas LANS son independientes.
- El dispositivo interconecta las dos redes. Las dos LANS son 100 MHz 192.168.42.1 y 100 MHz 192.168.43.1 por defecto. La LAN conectada es determinada por la velocidad de la tarjeta de red del PC, no por el puerto físico del HUB al cual se conecte.
- Ofrece llamada en conferencia -63 usuarios en una conferencia simple, o 21 conferencias en grupos de tres personas.
- Soporta hasta 30 llamadas de datos simultáneas.
- Soporta el modulo de comprensión de voz VCM5/10/20.
- Soporta el modulo Modem2.
- Soporta VoIP.
- Permite realizar sondeos SNMP, los cuales son dirigidos a la dirección IP de 10 MHz.

Este un dispositivo plug and play por lo que no necesita ninguna configuración.

4. EQUIPOS DE CÓMPUTO

Los equipos de cómputo utilizados tienen las siguientes características:

Fabricante: Dell Computer corporation

Modelo: Dell Optiplex Gx 260

Procesador: Pentium 4 de 2.4 Ghz

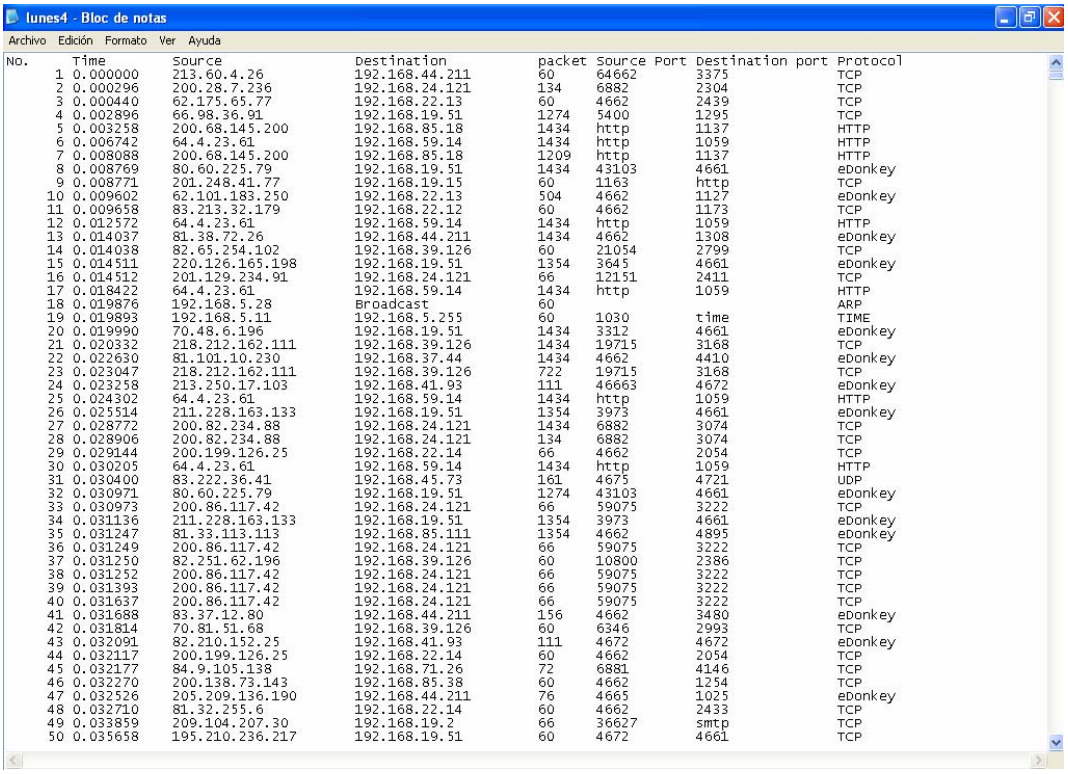
Memoria RAM: 512 MB

Disco duro: 30MB

Sistema operativo: Windows XP Professional

ANEXO C. EJEMPLO DE UNA CAPTURA EN FORMATO TEXTO

La imagen que se muestra a continuación muestra el resultado de las capturas exportadas a formato texto. No se adjunta la totalidad de archivos registrados por su gran cantidad y tamaño; en su lugar se presentan resultados consolidados en gráficas y tablas.



lunes4 - Bloc de notas

Archivo Edición Formato Ver Ayuda

No.	Time	Source	Destination	packet	Source Port	Destination port	Protocol
1	0.000000	213.60.4.26	192.168.44.211	60	64662	3375	TCP
2	0.000296	200.28.7.236	192.168.24.121	134	6882	2304	TCP
3	0.000440	62.175.65.77	192.168.22.13	60	4662	2439	TCP
4	0.002896	66.98.36.91	192.168.19.51	1274	5400	1295	TCP
5	0.003258	200.68.145.200	192.168.85.18	1434	http	1137	HTTP
6	0.006742	64.4.23.61	192.168.59.14	1434	http	1059	HTTP
7	0.008088	200.68.145.200	192.168.85.18	1209	http	1137	HTTP
8	0.008769	80.60.225.79	192.168.19.51	1434	43103	4661	eDonkey
9	0.008771	201.248.41.77	192.168.19.15	60	1163	http	TCP
10	0.009602	62.101.183.250	192.168.22.13	504	4662	1127	eDonkey
11	0.009658	83.213.32.179	192.168.22.12	60	4662	1173	TCP
12	0.012572	64.4.23.61	192.168.59.14	1434	http	1059	HTTP
13	0.014037	81.38.72.26	192.168.44.211	1434	4662	1308	eDonkey
14	0.014038	82.65.254.102	192.168.39.126	60	21054	2799	TCP
15	0.014511	220.126.165.198	192.168.19.51	1354	3645	4661	eDonkey
16	0.014512	201.129.234.91	192.168.24.121	66	12151	2411	TCP
17	0.018422	64.4.23.61	192.168.59.14	1434	http	1059	HTTP
18	0.019876	192.168.5.28	Broadcast	60			ARP
19	0.019893	192.168.5.11	192.168.5.255	60	1030	time	TIME
20	0.019990	70.48.6.196	192.168.19.51	1434	3312	4661	eDonkey
21	0.020332	218.212.162.111	192.168.39.126	1434	19715	3168	TCP
22	0.022630	81.101.10.230	192.168.37.44	1434	4662	4410	eDonkey
23	0.023047	218.212.162.111	192.168.39.126	722	19715	3168	TCP
24	0.023258	213.250.17.103	192.168.41.93	111	46663	4672	eDonkey
25	0.024302	64.4.23.61	192.168.59.14	1434	http	1059	HTTP
26	0.025514	211.228.163.133	192.168.19.51	1354	3973	4661	eDonkey
27	0.028772	200.82.234.88	192.168.24.121	1434	6882	3074	TCP
28	0.028906	200.82.234.88	192.168.24.121	134	6882	3074	TCP
29	0.029144	200.199.126.25	192.168.22.14	66	4662	2054	TCP
30	0.030205	64.4.23.61	192.168.59.14	1434	http	1059	HTTP
31	0.030400	83.222.36.41	192.168.45.73	161	4675	4721	UDP
32	0.030971	80.60.225.79	192.168.19.51	1274	43103	4661	eDonkey
33	0.030973	200.86.117.42	192.168.24.121	66	59075	3222	TCP
34	0.031136	211.228.163.133	192.168.19.51	1354	3973	4661	eDonkey
35	0.031247	81.33.113.113	192.168.85.111	1354	4662	4895	eDonkey
36	0.031249	200.86.117.42	192.168.24.121	66	59075	3222	TCP
37	0.031250	82.251.62.196	192.168.39.126	60	10800	2386	TCP
38	0.031252	200.86.117.42	192.168.24.121	66	59075	3222	TCP
39	0.031393	200.86.117.42	192.168.24.121	66	59075	3222	TCP
40	0.031637	200.86.117.42	192.168.24.121	66	59075	3222	TCP
41	0.031688	83.37.12.80	192.168.44.211	156	4662	3480	eDonkey
42	0.031814	70.81.51.68	192.168.39.126	60	6346	2993	TCP
43	0.032091	82.210.152.25	192.168.41.93	111	4672	4672	eDonkey
44	0.032117	200.199.126.25	192.168.22.14	60	4662	2054	TCP
45	0.032177	84.9.105.138	192.168.71.26	72	6881	4146	TCP
46	0.032270	200.138.73.143	192.168.85.38	60	4662	1254	TCP
47	0.032526	205.209.136.190	192.168.44.211	76	4665	1025	eDonkey
48	0.032710	81.32.255.6	192.168.22.14	60	4662	2433	TCP
49	0.033859	209.104.207.30	192.168.19.2	66	36627	smtp	TCP
50	0.035658	195.210.236.217	192.168.19.51	60	4672	4661	TCP