CARACTERIZACIÓN DEL TRÁFICO DEL BACKBONE DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

HÉCTOR ALFONSO ACEVEDO SILVA
RONALD MARTÍN VERGEL ZAPATA

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

CARACTERIZACIÓN DEL TRÁFICO DEL BACKBONE DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

HÉCTOR ALFONSO ACEVEDO SILVA
RONALD MARTÍN VERGEL ZAPATA

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 Gonzáles, director del proyecto y a la Ingeniera Leydi Johanna Barco codirectora del proyecto, por su orientación y colaboración.

La Especialización en Telecomunicaciones.

La Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones

La Universidad Industrial de Santander.

Este libro esta dedicado a mis padres Hermes y Carmenza que con su esfuerzo y empeño hicieron posible la realizacion de este proyecto, a mi familia, a mis compañeros, a los compañeros del grupo cps por su apoyo

Héctor Alfonso Acevedo Silva

A Dios, a mis padres, Martín y Ana Delina por su apoyo incondicional y paciencia, a mi hermano Carlos Fernando, a mi novia Leidy, a Zeus, y a todos mis compañeros del CPS.

Ronald Martín Vergel Zapata

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

TITULO
CARACTERIZACION DEL TRAFICO DEL BACKBONE DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER*

AUTORES

HÉCTOR ALFONSO ACEVEDO SILVA
RONALD MARTÍN VERGEL ZAPATA**

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

Descripción

El análisis del trafico es una actividad que permite al analizador 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 caracterizar el tráfico por puertos del switch central de la red de datos de la Universidad Industrial de Santander.

Para la realización de este proyecto se realizó un análisis del tráfico de los enlaces por medio de una tarjeta de red Gigabit Ethernet de fibra óptica conectada al switch central Cajun P880 en donde se configuró un Mirror Port; se utilizó un analizador de tráfico como el Ethereal, que permitió obtener los parámetros necesarios haciendo registros de la información que viaja por la red. A través de estos registros exportados a formato de texto plano se vincularon a una base de datos; por medio de la base de datos Microsoft Access se pueden obtener los parámetros de medición establecidos haciendo las consultas necesarias, una vez realizadas las consultas se obtuvieron los diferentes resultados de los parámetros.

Entre los resultados más importantes se tiene que la mayor parte del tráfico de datos esta siendo consumido para descargar archivos de música y video a través de programas P2P, el porcentaje de utilización del ancho de banda de los enlaces no supera el 0.35%; la metodología propuesta es viable ya que en poco tiempo se puede obtener una buena caracterización de los enlaces y además puede implementarse en una red en la que no se posean los medios económicos para adquirir un software especializado en análisis de tráfico.

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

TITLE
TRAFFIC CHARACTERIZATION OF THE BACKBONE OF THE UNIVERSIDAD INDUSTRIAL DE SANTANDER *

AUTHORS

HÉCTOR ALFONSO ACEVEDO SILVA
RONALD MARTÍN VERGEL ZAPATA * *

Key words
Analysis, traffic, links, network, bandwidth

Abstract

The traffic analysis is an activity that allows the network analyzer to determine the performance, dynamics and transition times in a data network to be able to arrive to a diagnose on possible flaws in the same one. The objective of this work is to characterize the traffic by ports of the central switch of the data network of the Universidad Industrial de Santander.

For the realization of this project it was carried out an traffic analysis of the links by means of a Gigabit Ethernet network card connected by optic fiber to the central switch Cajun P880 where a Mirror Port was configured; a traffic analyzer like the Ethereal that it allowed to obtain the necessary parameters making registrations of the information that flows for the network was used. Through these registrations exported to format of plane text they were linked to a database; by means of the Microsoft Access database the established measurement parameters can be obtained making the necessary consults, once carried out the consults the different results of the parameters were obtained.

Among the most important results one has that most of the data traffic is being consumed to download music and video files through P2P programs, the percentage of the bandwidth utilization of the links doesn't overcome 0.35%; the proposed methodology is viable since in little time one can obtain a good characterization of the links and it can also be implemented in a network in which the economic means are not possessed to acquire a specialized software in traffic analysis.

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

INTRODUCCIÓN

Desde el inicio de las redes de datos, tanto locales como la red mundial Internet, el tráfico de datos o información sobre éstas ha sido uno de los principales temas de estudio en su extenso y rápido desarrollo. En el afán del hombre de transmitir mayor cantidad de datos y a una velocidad más alta, se ha venido presentando un fenómeno que ha conllevado a que estas redes se saturen o se sobrecarguen provocando un efecto contrario al deseado por el hombre, este fenómeno comúnmente es llamado congestión.

Hoy en día las redes de datos demandan un alto número de servicios y recursos. Algunas poseen una infraestructura robusta que soporta las necesidades de los usuarios. Es necesario hacer un análisis del estado de la red de datos para determinar su capacidad real, ya que las aplicaciones demandan y consumen cada vez más recursos de la red, son más complejas e interactúan con mayor diversidad de componentes, tales como otros servidores, otros protocolos, etc.; hay más aplicaciones distribuidas y servicios instalados por usuarios y terceras partes, incluso por desconocimiento de los consumos de recursos que genera una aplicación por parte de los responsables de su desarrollo.

El ingreso de nuevos equipos a la red, la existencia de protocolos no necesarios, la mala configuración de equipos activos de red o la deficiencia de mantenimiento al cableado estructurado y las interfaces de red pueden causar la decadencia del desempeño de esta.

Es necesario hacer un análisis minucioso en la mayoría de redes para obtener cuales son las verdaderas causas de la congestión de tráfico representada en

una considerable disminución de la velocidad de transmisión de los datos y en los ya conocidos cuellos de botella.

La Universidad Industrial de Santander no es ajena a este fenómeno ya que su red local muchas veces se encuentra saturada, por lo cual se ha decidido hacer un estudio detallado del comportamiento de algunos puertos del switch router central de la red de datos institucional.

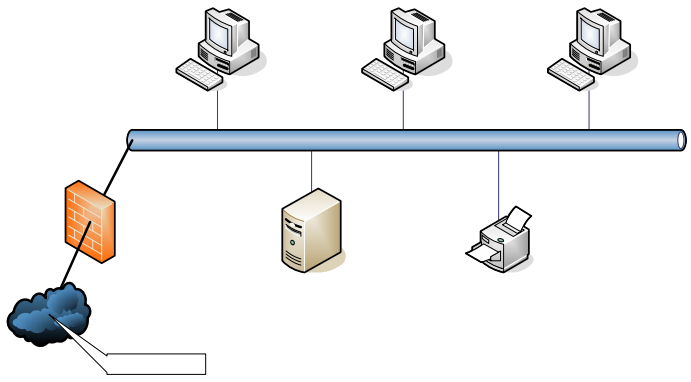
El estudio o análisis propuesto generará un conjunto de parámetros de tráfico de datos obtenido desde el backbone de la Universidad Industrial de Santander, ubicado en el switch central de la misma, para lo cual se realizarán una serie de registros sobre los puertos que presenten un mayor flujo de datos y por ende una mayor congestión.

1. FUNDAMENTOS SOBRE REDES DE DATOS DE ÁREA LOCAL – LAN

1.1 CONCEPTOS GENERALES

Podemos encontrar varias definiciones que resumen el concepto de una LAN (Local Area Network). Una primera idea de red de área local es la conexión de dos o más estaciones que se comunican entre si a través de un medio físico, tal como el cable UTP, fibra óptica, coaxial o cable de par trenzado. Estas estaciones comparten recursos, dispositivos periféricos y datos a una velocidad de transferencia alta. Normalmente, se localizan dentro de una zona limitada como puede ser una oficina, o un piso de un edificio. Son de fácil instalación y explotación. En la figura 1 se muestra un diagrama general de una red LAN.

Figura 1. Diagrama de una red LAN.



1.2 DESEMPEÑO DE UNA LAN

1.2.1 Estadísticas del desempeño de la Red. Para la evaluación del desempeño de un enlace de datos en una red de área local LAN, se usan las estadísticas de desempeño; para tal fin se hacen una serie de campañas de medición de varios parámetros, luego su tabulación y posteriormente su evaluación.

Entre los parámetros más representativos están los siguientes:

- Distribución de protocolos
- End Points
- Tráfico Multicast, Broadcast y Unicast
- Total bytes Transmitidos/Recibidos
- Total paquetes Transmitidos/Recibidos
- Medida de Ancho de Banda

• **Distribución de protocolos**. La distribución de protocolos permite identificar los protocolos de la capa de enlace de datos, capa de red, capa de transporte y capa de aplicación que están presentes en la red y cuantificar los recursos que consumen. Se tiene además una distribución porcentual de los protocolos presentes en la red. Estas medidas son generalmente dadas en paquetes o bytes.

• **End Points (Puntos finales).** Se refiere a la cantidad de datos enviados y recibidos por cada usuario del enlace de datos para cada protocolo usado como, IP, TCP, UDP, entre otros.

• **Tráfico Unicast, Multicast y Broadcast.** El tráfico Unicast se produce cuando un nodo envía paquetes a un único nodo receptor. El tráfico Multicast se produce cuando un nodo fuente sólo envía una copia de cada paquete sobre

un enlace a un grupo multicast de más de un participante (receptores) no necesariamente en la misma red. El tráfico Broadcast se produce cuando hay retransmisión múltiple.

- **Total bytes Transmitidos/Recibidos.** Como su nombre lo indica se refiere a la cantidad de bytes que se transmiten y se reciben en la toma de datos o campañas de medición.

- **Total paquetes Transmitidos/Recibidos.** Como su nombre lo indica se refiere a la cantidad de paquetes que se transmiten y se reciben en la toma de datos o campañas de medición.

- **Medida de Ancho de Banda.** El ancho de banda es la tasa máxima de datos que pueden ser transmitidos sobre una conexión de red.

1.2.2 Técnicas de medición para el desempeño de una Red. Existen muchas técnicas y herramientas software disponibles para medir el desempeño de una LAN cableada. Sin embargo, en cuanto a las mediciones en redes de área local se han implementado métodos que varían con cada tipo de red LAN a evaluar y aún no se cuenta con una metodología propuesta por una organización internacional, para tal fin.

La mayoría de los métodos empleados para las mediciones usan analizadores de tráfico que se caracterizan por permitir al analista de protocolos observar los parámetros más importantes de la red durante un tiempo determinado, tomar mediciones y efectuar registros con el fin de hacer su evaluación, para luego llegar a un diagnóstico. Normalmente dichas mediciones se repiten varias veces y luego se promedian para mejorar su aproximación. Algunas de éstas técnicas, se presentan a continuación.

- **Software especializado de medición.** En la actualidad existen diferentes herramientas software que permiten realizar mediciones sobre una red. La mayoría de herramientas permiten capturar los paquetes que se están transmitiendo por un enlace de datos y obtener características de interés. Entre las herramientas software disponible se encuentran los sniffers o analizadores de tráfico centralizados, los cuales analizan y monitorean el tráfico de tramas y datagramas de protocolos, su composición, errores, frecuencia, volúmenes, etc., como por ejemplo el Analyzer, el Ethereal y los monitores de red o analizadores distribuidos, aplicaciones que dialogan con sondas o agentes de medición que recopilan estadísticas diversas generalmente basadas en estándar SNMP[1] RMON para luego ser extraídas por un software de gestión y permiten monitorear más de un segmento a la vez, como el Solarwinds.

- **Soluciones basadas en hardware y software.** Los métodos que implementan soluciones basadas en hardware generalmente utilizan una sonda, un dispositivo que se coloca en un punto determinado de la red y recoge estadísticas de los dispositivos generalmente usando el estándar RMON, son analizadores distribuidos y pueden monitorear redes de área local LAN o redes de área extensa WAN. Consultan eventualmente los dispositivos (routers, switches y servidores) realizando polling (sondeo). La escala de tiempo en la que se llevan a cabo las mediciones es de largo plazo. En la tabla 1 se muestra las diferencias entre las soluciones basadas en hardware y software.

[1] SNMP es un protocolo de gestión de red, esto es, un conjunto de estructuras que permiten obtener los datos concretos del tráfico que se producen en la red, así como averiguar quién lo produce. La arquitectura de gestión SNMP representa todos lo recursos de red como objetos, cada objeto es una variable de datos que representa un aspecto del agente gestionado.

- **Herramientas.** El ámbito geográfico (WAN) plantea herramientas diferentes de las de uso local (LAN). En la tabla 2 se muestra el tipo de herramientas para monitoreo, análisis y corrección de redes LAN.

  - **Scanners de cable.** Miden y analizan las características de los enlaces físicos (distancias, crosstalk, atenuaciones inversiones de pares, cortocircuitos, etc.,) como por ejemplo el Fluke LanMeter.

  - **Analizadores de tráfico.** Analizan y monitorean el tráfico de tramas y datagramas de protocolos, su composición, errores, frecuencia, volúmenes, etc., como por ejemplo el Observer de Network Instruments.

  - **Consolas de SNMP + software de gestión de dispositivos.** Realizan un polling de los dispositivos, captando alarmas o alterando su estado, como por ejemplo el Managewise, eventualmente se enlazan con el software específico de gestión de dispositivos, tal como el Trascend de 3COM.

  - **Sondas**. Tanto de hardware como se software, son elementos que recopilan estadísticas diversas (generalmente basadas en estándar RMON) para luego ser extraída por un software de gestión. Tal es el caso del NetScout.

  - **Estadísticas.** Tomadas por los dispositivos (routers, switches y servidores), cada una de ellas tiene su aplicación específica y funcionan en conjunto para un correcto monitoreo ya sea correctivo como pro-activo.

Tabla 1. Diferencias entre las soluciones basadas en software y en hardware.

Factor	Software	Hardware/Software
Costo	Bajo	Alto
Capacidad de procesamiento	Depende de la interfaz de red utilizada	Alta
Facilidad de uso	Media a alta	Baja a media
Capacidad de distribución	Si	Si
Obsolescencia	Capacidad de fácil actualización	Debe reemplazar el hardware/firmware por obsolescencia
Capacidad de Trending	Limitada al disco	Limitada a la capacidad del equipo
Fallas	Susceptible a las fallas del SO subyacente	Baja
Contingencia	Puede ser reinstalado ante falla de hardware	Depende de la reparación de la unidad
Capacidad reporting de RMON/SNMP	Si	Si
Capacidad de medición en WAN	No	Si
Capacidad de mediciones de capa física	No	Si

Tabla 2. Tipo de herramientas para monitoreo, análisis y corrección de redes LAN.

HERRAMIENTAS PREVENTIVAS	HERRAMIENTAS DE DIAGNOSTICO	HERRAMIENTAS CORRECTIVAS
Consolas de SNMP Analizadores de trafico (trending y triggers)	Analizadores de trafico TDRs Sondas Consolas de SNMP	Rediseño físico / lógico Comandos de los sistemas operativos de dispositivos y servidores para reconfiguración

- **Analizadores de tráfico.** Permiten analizar el comportamiento de la red por segmento, lo que hace la cantidad de tráfico (bandwith) consumido, quién lo consume, cuáles errores lógicos o físicos hay en el tráfico, quién los genera,

cuáles tipos de protocolos hay en la red, qué porcentaje de cada uno, cuáles son los signos vitales de la red.

Permiten además realizar la captura de tráfico para saber que fluye en una conversación entre un cliente y un servidor.

Como ya mencionamos anteriormente ejemplos de estos equipos son el Observer de Network Instruments , el Sniffer de Network General, el Lan Analyzer de Novell , etc.

- **Concepto.** Un analizador de tráfico es una herramienta de software, hardware o mixta que permite al analista de protocolos tomar mediciones y efectuar capturas para su análisis posterior, a fin de llegar a un diagnóstico.

- **Tipos de analizadores de tráfico.**

    - Soluciones basadas en software solamente.
    - Soluciones basadas en hardware y software, generalmente de tipo propietaria y especializada.

Según su capacidad de toma de mediciones en más de un segmento se dividen en:

- Analizadores distribuidos, que dialogan con sondas o agentes de medición.
- Analizadores centralizados.

- **Funciones de un analizador de tráfico:** Básicamente, las funciones se agrupan en:

    - Captura y análisis experto post-captura, con capacidades de filtrado pre y post-captura.

- Mediciones interactivas.
- Mediciones de largo plazo (trendings).
- Alarmas y triggers.
- Descubrimiento de direcciones físicas y sus correspondientes direcciones lógicas.
- Generación de tráfico.

1.3 ANÁLISIS DE TRÁFICO

Una definición breve y clara del análisis de tráfico es la siguiente: Es el conjunto de mediciones relacionadas con la transmisión de paquetes en un segmento de la red de datos. Estos paquetes están originados por las aplicaciones que hacen uso de la red, los servicios que se prestan en ella o los protocolos que administran su funcionamiento.

Con el análisis de tráfico se mide cantidad, comportamiento, dinámica, tiempos de tránsito y otros factores que permiten efectuar el diagnóstico de problemas o niveles de actividad de la red. Para lograr estos objetivos, el profesional debe conocer el comportamiento de la red y sus protocolos, además de estar dotado de una estación que cuenta con un software especializado en análisis de tráfico (traffic analyzer). Son ejemplos de esta actividad la medición de ancho de banda utilizado (bandwith utilization), distribución de protocolos o captura y decodificación de paquetes (packet capture).

1.3.1 Mediciones para evaluar el desempeño de una Red. A continuación se presentan algunos de los trabajos más representativos desarrollados en torno al desempeño y medición de redes de datos de área local.

- **Uso del Internet en la Universidad Española. [1]** En este trabajo se realiza una exposición e interpretación de distintas medidas y análisis de

tráfico que han sido realizadas en la red académica RedIris. La red académica RedIris interconecta las universidades y centros de investigación españoles entre sí, así como con el resto de Internet. Entre los parámetros tomados se encuentran la carga de tráfico en los enlaces y se expresan en Gigabytes. Se calculan midiendo la información transferida en cada día laborable en intervalos de 10 a 15 minutos y evaluando la media a lo largo del periodo de medida. También presenta mediciones sobre el desempeño a lo largo de la franja horaria tomado para el total de los enlaces de RedIris a las comunidades autónomas, y caracterizan la naturaleza del tráfico IP que circula por uno de los enlaces de la red troncal de RedIris, con base en los servicios o protocolos de aplicación utilizados.

- **Analizador en tiempo real de calidad de servicio en redes IP, ORENETA. [2]** Trabaja registrando el tráfico de la red en dos puntos distintos mediante dos sondas. Las sondas capturan el tráfico en modo pasivo, minimizando la interferencia con el tráfico analizado. Esto permite el análisis de tráfico real aportando un valor añadido sobre las medidas de tráfico generado.

Los registros de tráfico son preprocesados en las sondas y enviadas a un analizador. Éste es el elemento que hace los cálculos de las medidas con los datos obtenidos de las sondas y ofrece la interacción con el usuario. El analizador desglosa las medidas obtenidas en flujos unidireccionales, lo que permite observar de forma clara los parámetros y comportamiento de cada uno de ellos. Esto a su vez permite la caracterización del tráfico. El control de las sondas se realiza desde el analizador. El sistema funciona según la arquitectura cliente/servidor, siendo el cliente el analizador y las sondas los servidores.

- **MIRA: Plataforma de monitorización y análisis de tráfico para redes IP. [3]** Es una herramienta avanzada que incorpora novedosas características,

como el análisis automático de contenidos (no únicamente cabeceras de protocolos), posibilidades de despliegue distribuido, detección de ataques de seguridad y soporte para IPv6, entre otras. Además, es versátil y soporta distintas tecnologías de subred, como Ethernet o ATM.

La arquitectura funcional de MIRA consta de varios módulos, que trabajan en cascada. Cada uno de los módulos a su vez se implementa en uno o varios procesos. Existen mecanismos de sincronización y control de flujo para la comunicación entre procesos. Los módulos que hacen parte de esta monitorización son: el módulo de captura, preprocesado, consolidación, clasificación y postprocesado.

1.4 GIGABIT ETHERNET

Es una tecnología de red que se desarrolla para satisfacer las necesidades del mercado, en particular soportar aplicaciones de redes que incluyen:

- Modelos de alta resolución en 3D.
- Videos en tiempo real.
- Servicios de publicaciones / ediciones digitales
- Internet/intranet

Gigabit Ethernet es confiable para cualquier usuario siendo completamente compatible con la base instalada de 10 y 100 Mbps con un costo inicial razonable y con poca necesidad de entrenamiento para los usuarios de Ethernet.

Desde 1970 Ethernet es la tecnología más representativa de las redes de trabajo. Ethernet fue establecido como una tecnología escalable, es decir, que podría ser actualizada o mejorada.

La rápida demanda de mayores velocidades de transmisión provocó la necesidad de aplicaciones troncales (backbone) con tasas de transmisión de 1 Gbps o superiores. En Junio de 1998, el IEEE aprobó el estándar Gigabit Ethernet desarrollado por el comité IEEE 802.3z. El nuevo estándar Gigabit Ethernet es compatible con las instalaciones Ethernet existentes, reteniendo el mismo método de acceso CSMA/CD y soportando modos de operaciones como Full-Duplex y Half-Duplex. Inicialmente, soportaría fibra mono-modo y multi-modo y cable coaxial short-haul.

Gigabit Ethernet ha sido desplegada para ser empleada como backbone en las redes existentes. Estas se pueden usar para agregar tráfico entre clientes y conjunto de servidores interconectando switches Fast Ethernet, los cuales pueden ser usados para interconectar estaciones de trabajo y servidores de aplicaciones de alto ancho de banda, tales como imágenes médicas, transmisiones de video en tiempo real, etc.

El estándar Gigabit Ethernet requiere el uso de láser en lugar de los tradicionales LEDs como fuentes de luz, ya que éstos no pueden ser modulados a velocidades de Gigabit por segundo.

1.4.1 Capa Física. La capa física de Gigabit Ethernet usa una mezcla entre las tecnologías Ethernet y la Especificación de Canales por Fibra ANSI X3T11. Gigabit Ethernet se apoya en 4 tipos de medios de comunicación físicos, los cuales son definidos en 802.3z (1000Base-X) y 802.3ab (1000Base-T)

- **1000Base-X.** En el estándar 1000Base-X la capa física es el canal de fibra. El canal de fibra es una tecnología de interconexión entre estaciones de trabajo, supercomputadoras, dispositivos de almacenamiento de información y periféricos, tiene una arquitectura de 4 capas.

Hay 3 tipos de medios de transmisión que son incluidos en el estándar 1000Base-X:

- 1000Base-SX: usa una fibra multi-modo, 850nm.
- 1000Base-LX: puede ser usada tanto mono-modo y multi-modo, 1300nm.
- 1000Base-CX: usa un cable par trenzado de cobre (STP).

En la tabla 3 se muestra una descripción de los distintos tipos de fibra existentes.

Tabla 3. Distancias de operabilidad de los distintos tipos de cable.

TIPO DE CABLE	DISTANCIA DE OPERACIÓN
Single-mode Fiber (9 micron)	3000 m usando 1300nm laser (LX)
Multi mode Fiber (62.5 micron)	300 m usando 850 nm laser (SX) 550 m usando 1300 nm laser (LX)
Multi mode Fiber (50 micron)	550 m usando 850 nm laser (SX) 550 m usando 1300 nm laser (LX)
Short-haul Copper	25 m

- **1000Base-T.** El estándar 1000Base-T de Gigabit Ethernet emplea como medio de transmisión un cable UTP, usando 4 pares de líneas de categoría 5 UTP.

1.4.2 Capa MAC. La capa MAC de Gigabit Ethernet usa el mismo protocolo de Ethernet, CSMA/CD. La máxima longitud del cable usado para interconectar las estaciones está limitada por el protocolo CSMA/CD.

1.5 TARJETA DE RED GIGABIT ETHERNET

Para la realización del registro de datos primero se tuvo que realizar una búsqueda y luego una selección de una tarjeta de red de fibra óptica Gigabit Ethernet con las debidas especificaciones técnicas requeridas, entre las cuales se tienen las siguientes:

- Tipo de fibra óptica: Multimodo SX
- Tipo de conector: SC
- Arquitectura de bus: PCI
- Velocidad de bus: Mínima de 32 MHz
- Compatibilidad: IEEE 802.3z
- Sistema operativo: Windows o Linux

Después de haber realizado una búsqueda y un análisis exhaustivo se seleccionó la tarjeta de red Gigabit Ehernet de fibra óptica **Intel® PRO/1000 Server Adapter**, la cual se ajusta a los requerimientos del proyecto, especificaciones técnicas necesarias y presupuesto. En el anexo B se muestra información detallada sobre la tarjeta.

En la tabla 4 se muestra un cuadro comparativo de las distintas tarjetas de red de fibra óptica Gigabit Ethernet que se encontraron.

Tabla 4. Tarjetas de Red Gigabit Ethernet de fibra óptica.

PRODUCTO	MEDIA	CONECTOR	BUS	DISTANCIA OPERATIVA	COMPATIBILIDAD IEEE	DRIVERS	PRECIO
3Com® Gigabit Fiber-SX Server NIC	1000BASE-SX	SC	32-/64-bit, 33/66 MHz PCI; 32-/64-bit, 33/66/100/133 MHz PCI-X	Con fibra multimodo de 850 nm hasta 500 m (1,40 ft) full duplex. 220 m con 2.5/125 µm con fibra multimodo de 62,5/125 µm y 500 m con fibra multimodo de 50/125 µm	802.3, 802.3u, 802.3x, 802.3z, 802.1Q, 802.3ad	Linux 2.2, 2.4; Windows XP, 2000, NT 4.0; Novell NetWare 6.x, 5.x, 4.2; UnixWare 7; OpenServer 5; Sun Solaris X86	$539.24(cdw) $321.00
3Com® Gigabit Fiber-SX Server NIC 710012 with Memory	1000BASE-SX-compliant multimode fiber	SC	PCI bus master 32/64-bit, 33/66 MHz with adaptive DMA	62.5/125 um up to 275 m (902 ft); 50/125 um up to 550 m (1,803 ft)	802.3z, 802.3u, 802.1Q	NetWare 4.1x/5; Windows 2000/NT 4.0	
Allied Telesyn 1000Mbps PCI Gigabit Ethernet adapter. 1000Base-SX SC	1000BASE-SX	SC x 1 or SC x 2 Half & full-duplex operation	64-bit PCI bus		Fully IEEE 802.3z compliant	Novell NetWare 4.1x, 5.x Windows NT 4.0, 2000, 98 SUN Solaris 2.5.1, 2.6, 7 Linux 2.0.x	
SysKonnect 1000Base-SX Gigabit Ethernet Adapter	1000BASE-SX	SC connector Half & full-duplex operation	PCI bus 64 bit/66MHz or 32 bit/33MHz Signalling voltage 3.3v and 5v compatible PCI Hot Plug (OS-dependent)		802.3ac, 802.3z, 802.3x, 802.1Q, 802.1P, 802.3ad, 802.3ab	Linux 2.2, 2.4; Windows XP, 2000, NT 4.0, Server 2003 98 SE and ME; Novell NetWare 6.x, 5.x, 4.2; Sun Solaris X86	$559.81(cdw) $375.00

Intel® PRO/1000 Server Adapter	**1000BASE-SX**	**SC**	**32-/64-bit, 33 MHz PCI**	**850nm MMF 50µ cable to 550 meters and 62.5µ to 275 meters.**	**802.1p, 802.1Q, 802.3ac, 802.3ad, 802.3x, 802.3z, PCI v2.1**	**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**	**$99.00**
Intel® PRO/1000F Server Adapter	1000BASE-SX	SC	32-/64-bit, 33/66 MHz PCI	850nm MMF 50µ cable to 550 meters and 62.5µ to 275 meters.	802.1p, 802.1Q, 802.3ac, 802.3ad, 802.3u, 802.3x, 802.3z, PCI v2.2	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	$265.75
Tigercard 9462-SX	1000BASE-SX	SC	bus PCI v2.1 de 32 y 64 bits		IEEE 802.3z 1000BASE-SX, IEEE 802.3x, IEEE 802.1Q, IEEE 802.1p	Novell Netware 3.12, 4.x, 5.x, Dos, OS/2, Win 95/98 y NT client Linux 2.0.35 y posteriores, Sco Unís Openserver 5.05A o posteriores	219,22e
TRENDnet's TEG-PCISXplus 32/64-bit Gigabit Ethernet Fiber Adapter	1000Base-SX	SC Type connector for 62.5/125µm or 50/125 µm multi-mode fiber optic cable	Support 32/64-Bit PCI Local Bus Master high-speed operation of rev. 2.1/2.2 specification	Network Media: 62.5/125um multi-mode fiber optic cable with SC type connector, 220 meters max. 50/125um multi-mode fiber optic cable with SC type connector, 550 meters max.	Supports IEEE 802.1q VLAN and IEEE 802.1p QoS	Microsoft Windows 98/Me/2000/NT4.0, Novell Netware Server 5.x, Linux 2.2, 2.4	$120.00

1.6 MIRRORING PORT

Esta función permite al swicht hacer un espejo de todas las transmisiones que se emitan por un puerto cualquiera, pudiendo así analizar todas las tramas entrantes o salientes por dicho puerto y visualizarlas en el puerto escogido para el port mirroring.

Para llevar a cabo el análisis de tráfico es necesario instalar la tarjeta de red Gigabit Ethernet en un PC y este a su vez ser conectado a un puerto del switch principal de la Universidad Industrial de Santander, este puerto recibirá el nombre de Mirror Port (Puerto espejo), ya que por medio de él se refleja el tráfico de datos del Source Port (Puerto fuente), debidamente seleccionado, para así analizar su comportamiento.

El switch P880 nos proporciona en su Web Agent la manera de configurar dicho Port Mirror, a continuación se muestra la información de los parámetros de configuración del Mirror Port.

1.6.1 Configuración fuente. Selecciona la configuración del puerto fuente. Proporciona un enlace a la página de configuración del Port Mirroring.

1.6.2 Puerto Fuente. Muestra el puerto bajo estudio. Se puede seleccionar un puerto fuente cualquiera.

1.6.3 Puerto Espejo. Muestra el puerto que transmite los datos reflejados. Este puerto puede estar sobre otro módulo en el switch. El puerto fuente y el puerto espejo deben ser diferentes puertos físicos.

1.6.4 Tipo de Muestreo. Muestra la velocidad o tipo de muestreo que se aplica al tráfico del puerto fuente. Se puede seleccionar muestreo periódico (periodic), siempre (always) o ninguno (none).

1.6.5 Cantidad de paquetes por segundo. Se debe seleccionar el máximo número de paquetes por segundo que son enviados al puerto espejo. Éste valor debe ser lo suficientemente alto para evitar pérdidas de paquetes en el mirroring.

2. SELECCIÓN DE LA HERRAMIENTA SOFTWARE

2.1 INSTALACIÓN DE LOS EQUIPOS DE MEDICIÓN

La instalación física de la tarjeta se realiza en un slot PCI de un PC, para luego seguir con la instalación de los drivers, descargados de la página Web del fabricante.

El manejo de la tarjeta de red es sencillo, sólo basta con conectar el patch cord a la tarjeta y al switch. La tarjeta posee un software de test que permite comprobar su correcto funcionamiento.

Se usaron varios switches para la realización de las pruebas de la tarjeta. Estos fueron el switch Cajun P333R y el switch Cajun P550. Para la conexión con el switch Cajun P333R sólo se tuvo que habilitar el puerto de fibra óptica y asignarle una dirección IP, con ello se constató la comunicación de la tarjeta con el switch y con otros PCs por medio de la red LAN de la Universidad.

Para la conexión con el switch Cajun P550, primero se hizo uso del setup por medio del puerto de consola, para allí habilitar los puertos de fibra que este posee.

Una vez habilitados estos puertos se procede a crear unas interfaces y asignarles una dirección IP para así poder comunicarse con ellos desde la tarjeta de red. Después de creada la interfaz se configura el Puerto Espejo (port mirror), terminada esta última etapa, se pueden llevar a cabo las pruebas necesarias que son la base del proyecto.

Para el desarrollo de la toma de datos se trasladó el PC al centro de cableado principal de la Universidad Industrial de Santander en donde se encuentra ubicado el switch central, switch Cajun P880.

La configuración de este switch es muy similar a la del switch Cajun P550. Debido a que las tarjetas para fibra SX del switch tenían todos sus puertos en uso, fue necesario desinstalar una de las tarjetas del P550 e instalarla en uno de los slots libres del P880, más exactamente en el slot 10. Al ya tener instalado la tarjeta en el switch y conectar el PC a este mediante la tarjeta de red se procedió a la configuración del Puerto Espejo.

2.2 CONSIDERACIONES GENERALES

Para la puesta en marcha de la metodología y la realización de la toma de datos descrita en el capítulo anterior, se realizaron una serie de campañas de medición que mostraron los valores de los parámetros propuestos gracias a las herramientas software seleccionadas.

Se optó por utilizar un analizador de tráfico ya que es de fácil manejo, fácil adquisición y su capacidad de procesamiento es muy buena.

2.3 HERRAMIENTA SOFTWARE

La herramienta software utilizada para la realización de las mediciones es el ETHEREAL v.0.10.7 que fue seleccionada dentro de una serie de herramientas de análisis de tráfico encontradas en Internet.

En la tabla 5 se muestran algunos de los programas encontrados en Internet con sus principales características.

Tabla 5. Cuadro comparativo se Software de Análisis de Tráfico.

PROGRAMA	Sistema Operativo	Comercial	Tipo paquete		Mediciones				
			TCP	UDP	Distribución de protocolos	Ancho de Banda	End Point	Tamaño de paquetes	Total bytes Transmitidos/Recibidos
Analyzer	Windows, Linux		X	X	X	X	X		X
Ethereal	Windows Linux		X	X	X	X	X	X	X
Solarwinds	Windows	X	X	X		X		X	X
Observer	Windows,	X	X	X	X	X	X	X	X
FlowScan	Linux		X	X	X	X	X	X	X

Después de examinar cada una de las características de cada uno de estos analizadores de tráfico se llegó a la determinación de usar el ETHEREAL v.0.10.7, mencionado anteriormente, el cual trabaja sobre el sistema operativo Windows, mide los parámetros necesarios para la caracterización del tráfico y también por ser de distribución libre.

2.3.1 Ethereal. Ethereal es un analizador de paquetes de red, es usado por los profesionales de red alrededor del mundo para localizar averías, desarrollo de análisis de software, protocolo y educación. Este analizador de paquetes de red captura los paquetes que fluyen por la red y los muestra de la manera más detallada posible, funciona sobre todas las plataformas computacionales como son Unix, Linux y Windows.

Algunas características destacables del Ethereal se describen a continuación:

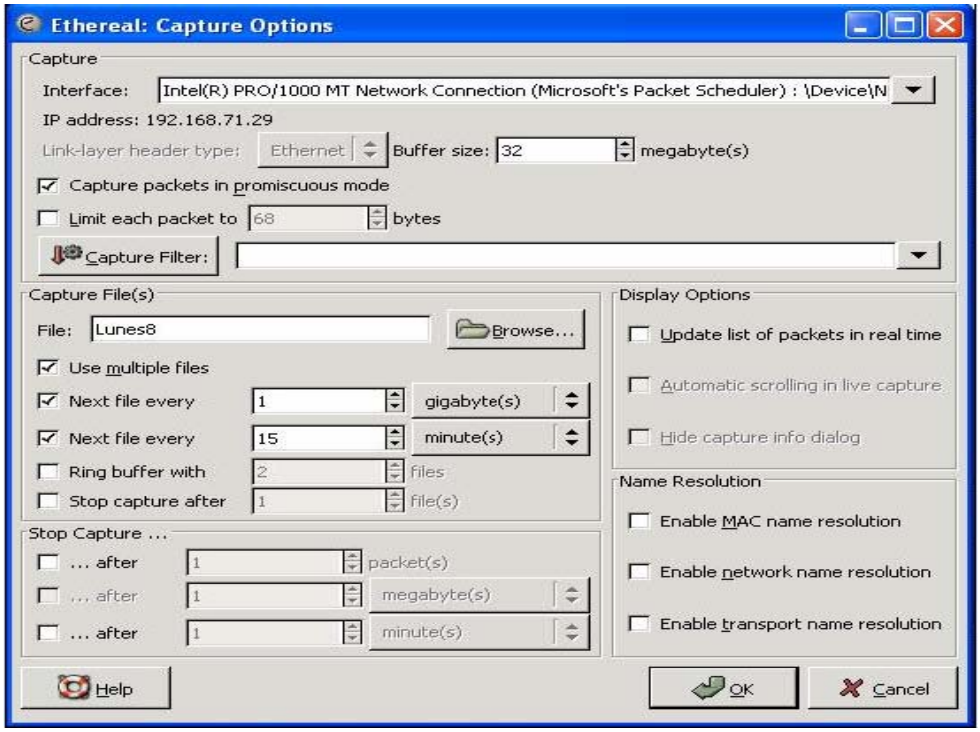
- Captura los datos de paquetes en tiempo real de una interfaz de red.

- 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.

Para iniciar la captura de datos se va al menú *capture* y este despliega una ventana mostrada en la figura 2. Aquí se puede configurar una serie de parámetros o características dependiendo de las necesidades del usuario, como son las siguientes:

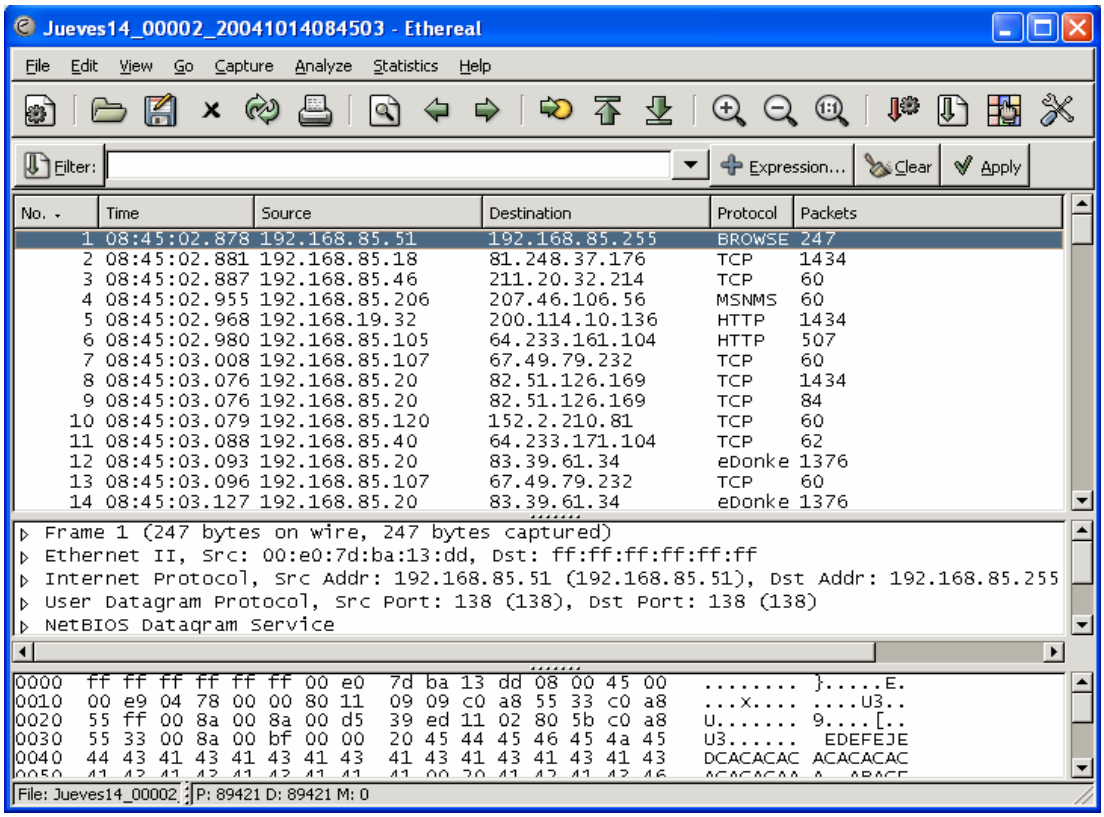
- Escoger la interfaz o medio de comunicación por el cual se va a realizar la captura, en este caso se escoge la tarjeta de Red Gigabit Ethernet.
- Determinar el tamaño del buffer.
- Captura en modo promiscuo o no.
- Límite del tamaño del paquete
- Determinación de un filtro de captura.
- Nombre y ubicación del archivo de captura.
- Uso de archivos múltiples, si se escoge esta opción se tiene que definir el modo como se van a almacenar y determinar estos archivos, pueden ser especificando su tamaño, intervalo de tiempo de captura y el número de archivos de captura que se requieran.
- Otras opciones para detener la captura son el número de paquetes capturados y el tiempo de captura.
- 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.
- Opciones para visualización.
- Resolución de nombres.

Figura 2. Opciones de captura del Ethereal.



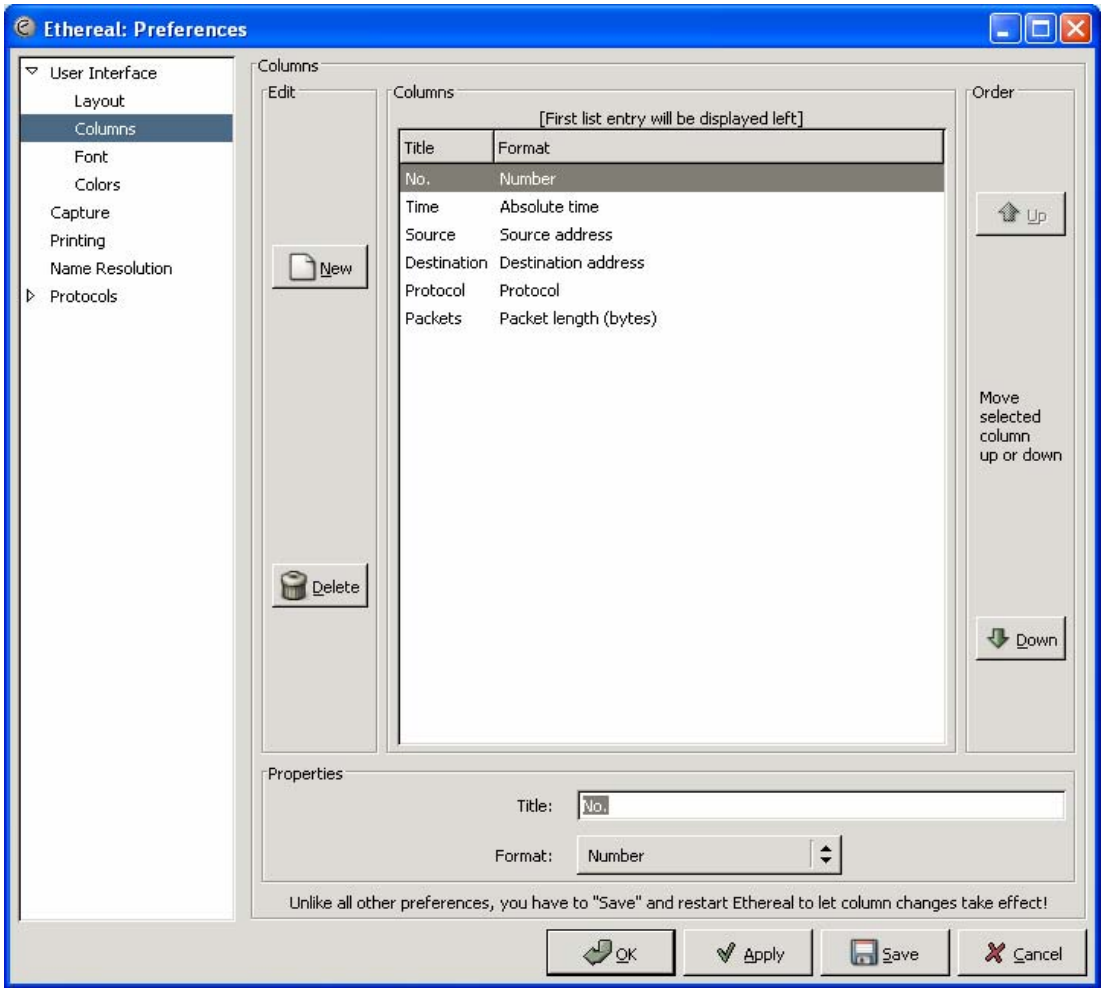
Como se puede observar en la figura 3, Ethereal muestra de una forma ordenada y detallada una serie de características o parámetros de las capturas hechas. Esta presentación de los parámetros puede modificarse en la opción de configuración del software según los requerimientos del usuario.

Figura 3. Información de una captura mostrada por Ethereal.



La primera columna que se observa contiene el número de cada paquete transmitido en el transcurso de la captura, la segunda columna muestra el tiempo de captura, pero este se puede ver de distintas formas; 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 tipo de protocolo y la sexta columna muestra el tamaño en bytes de cada paquete transmitido y recibido. Como se mencionó antes, estos parámetros se pueden modificar; por ejemplo, se puede observar información de cada paquete capturado, el puerto fuente y el puerto destino, así como la suma acumulativa de bytes. La ventana donde se pueden modificar estas columnas se pueden observar en la figura 4.

Figura 4. Opciones para modificar la información que se desea observar en las capturas.

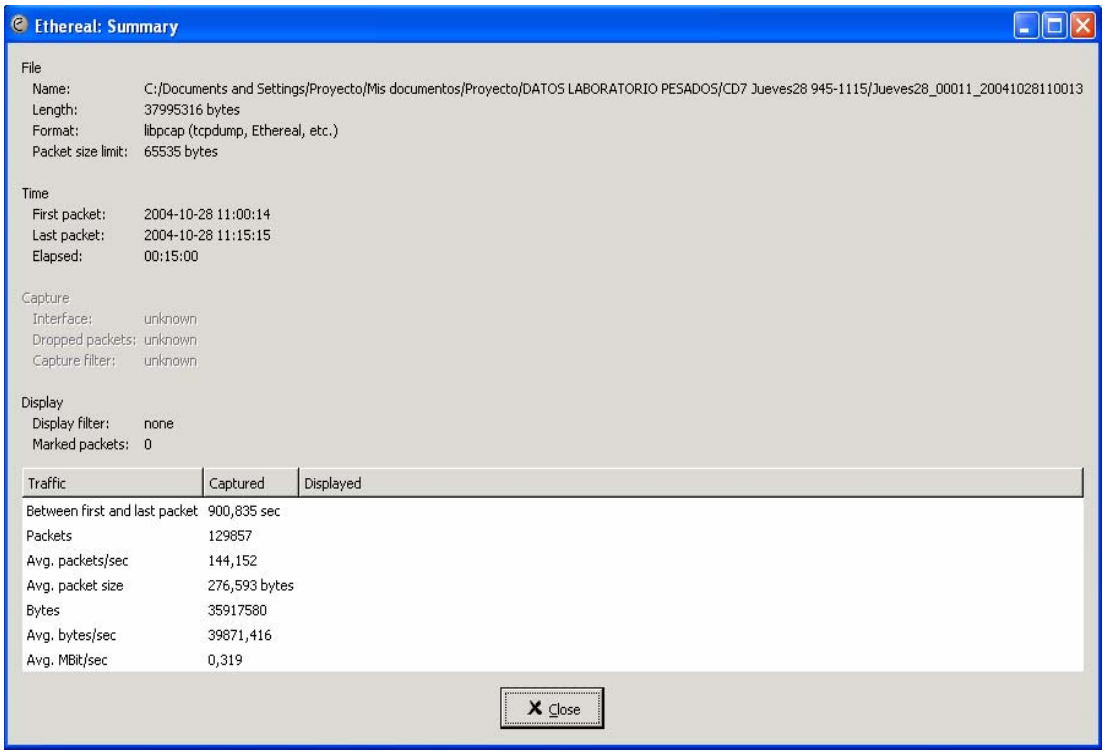


Después de realizado el registro se pueden visualizar las estadísticas, que son una característica muy importante del Ethereal. Entre estás estadísticas se tienen:

- Un resumen en donde se muestra el nombre del registro, el tamaño en bytes del archivo, el formato, el límite de tamaño de paquete, la fecha y tiempo de captura del primer paquete, la fecha y tiempo de captura del último paquete y el tiempo de duración del registro, promedio en bytes por segundo, promedio en megabits por segundo, promedio de tamaño

de paquete, promedio de paquetes por segundo, total de bytes y total de paquetes. Esto se puede visualizar en la figura 5.

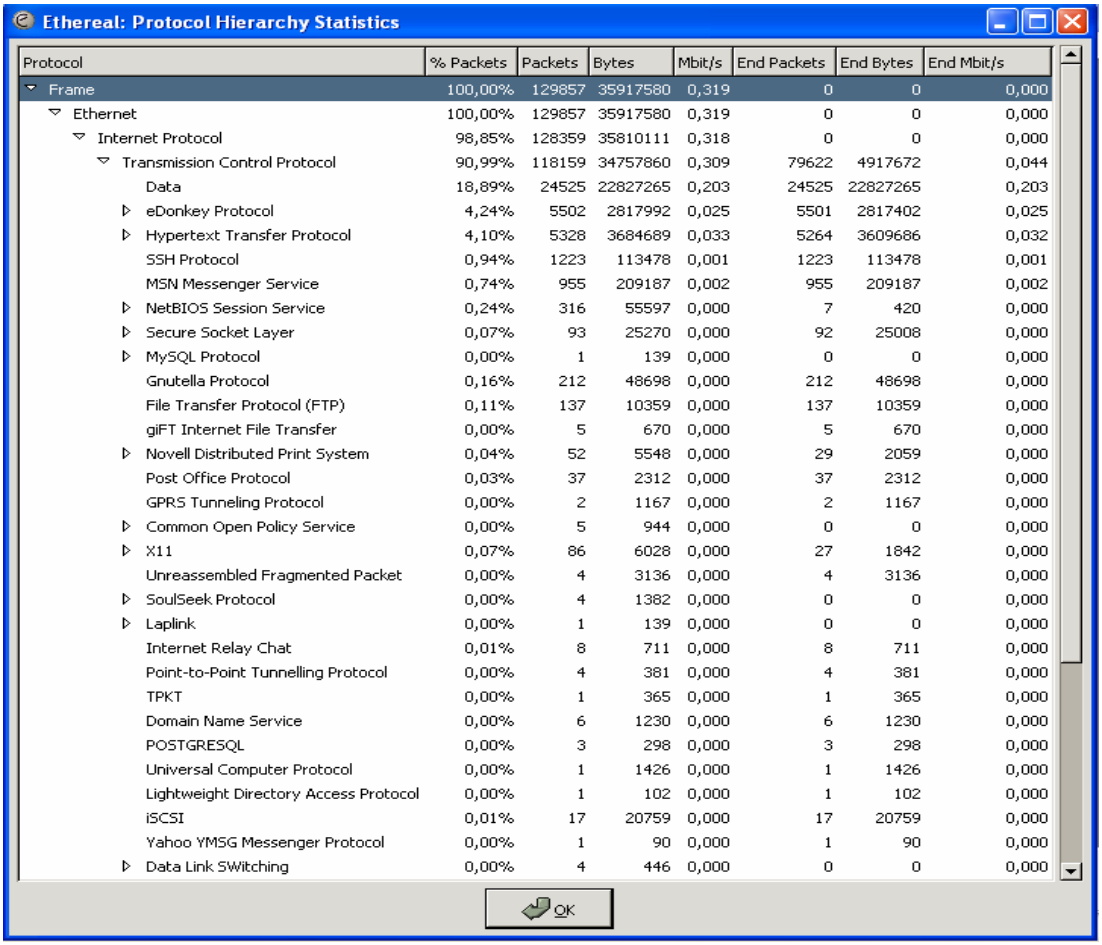
Figura 5. Resumen de la captura.



- Muestra una jerarquía de protocolos con los siguientes parámetros: porcentaje de paquetes, paquetes, bytes, megabits por segundo, mostrados en la figura 6.
- Muestra una ventana en donde se visualizan las conversaciones entre las fuentes y los destinos con su respectivo tamaño en paquetes y bytes, figura 7.
- Muestra una ventana en donde se visualizan los end points o estaciones finales con el respectivo tamaño de paquetes y bytes transmitidos y recibidos, figura 8.
- Ethereal también posee una herramienta que nos permite observar los datos capturados en una forma gráfica, en la cual se puede ajustar

parámetros en la eje de las *x*, como la escala de tiempo y resolución, y en el eje de las *y*, la unidad de medida, bytes o paquetes, y la escala de tiempo. También se pueden visualizar estas gráficas de tres formas diferentes: en línea, en impulsos o en histograma, figura 9.

Figura 6. Estadísticas de la jerarquía de protocolos.



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	129857	35917580	0,319	0	0	0,000
Ethernet	100,00%	129857	35917580	0,319	0	0	0,000
Internet Protocol	98,85%	128359	35810111	0,318	0	0	0,000
Transmission Control Protocol	90,99%	118159	34757860	0,309	79622	4917672	0,044
Data	18,89%	24525	22827265	0,203	24525	22827265	0,203
eDonkey Protocol	4,24%	5502	2817992	0,025	5501	2817402	0,025
Hypertext Transfer Protocol	4,10%	5328	3684689	0,033	5264	3609686	0,032
SSH Protocol	0,94%	1223	113478	0,001	1223	113478	0,001
MSN Messenger Service	0,74%	955	209187	0,002	955	209187	0,002
NetBIOS Session Service	0,24%	316	55597	0,000	7	420	0,000
Secure Socket Layer	0,07%	93	25270	0,000	92	25008	0,000
MySQL Protocol	0,00%	1	139	0,000	0	0	0,000
Gnutella Protocol	0,16%	212	48698	0,000	212	48698	0,000
File Transfer Protocol (FTP)	0,11%	137	10359	0,000	137	10359	0,000
giFT Internet File Transfer	0,00%	5	670	0,000	5	670	0,000
Novell Distributed Print System	0,04%	52	5548	0,000	29	2059	0,000
Post Office Protocol	0,03%	37	2312	0,000	37	2312	0,000
GPRS Tunneling Protocol	0,00%	2	1167	0,000	2	1167	0,000
Common Open Policy Service	0,00%	5	944	0,000	0	0	0,000
X11	0,07%	86	6028	0,000	27	1842	0,000
Unreassembled Fragmented Packet	0,00%	4	3136	0,000	4	3136	0,000
SoulSeek Protocol	0,00%	4	1382	0,000	0	0	0,000
Laplink	0,00%	1	139	0,000	0	0	0,000
Internet Relay Chat	0,01%	8	711	0,000	8	711	0,000
Point-to-Point Tunnelling Protocol	0,00%	4	381	0,000	4	381	0,000
TPKT	0,00%	1	365	0,000	1	365	0,000
Domain Name Service	0,00%	6	1230	0,000	6	1230	0,000
POSTGRESQL	0,00%	3	298	0,000	3	298	0,000
Universal Computer Protocol	0,00%	1	1426	0,000	1	1426	0,000
Lightweight Directory Access Protocol	0,00%	1	102	0,000	1	102	0,000
iSCSI	0,01%	17	20759	0,000	17	20759	0,000
Yahoo YMSG Messenger Protocol	0,00%	1	90	0,000	1	90	0,000
Data Link SWitching	0,00%	4	446	0,000	0	0	0,000

Figura 7. Conversaciones entre fuentes y destinos.

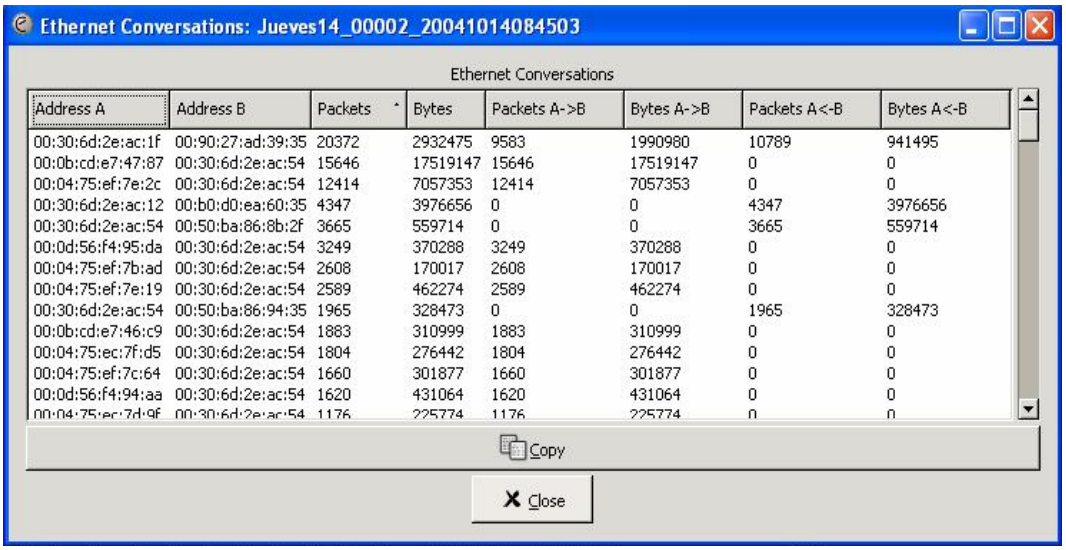
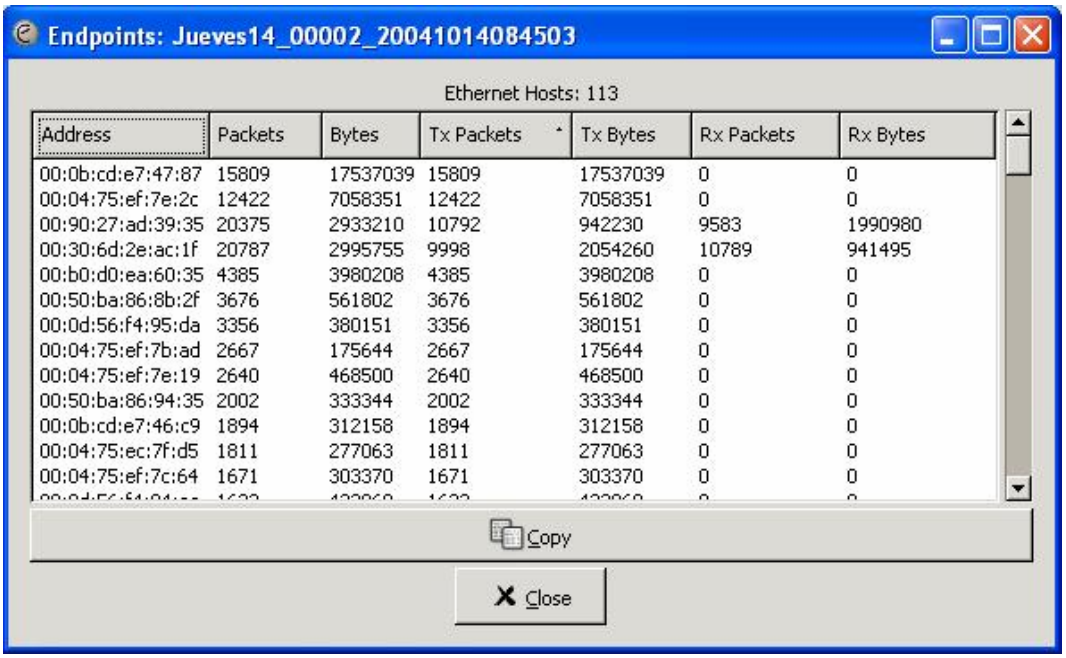
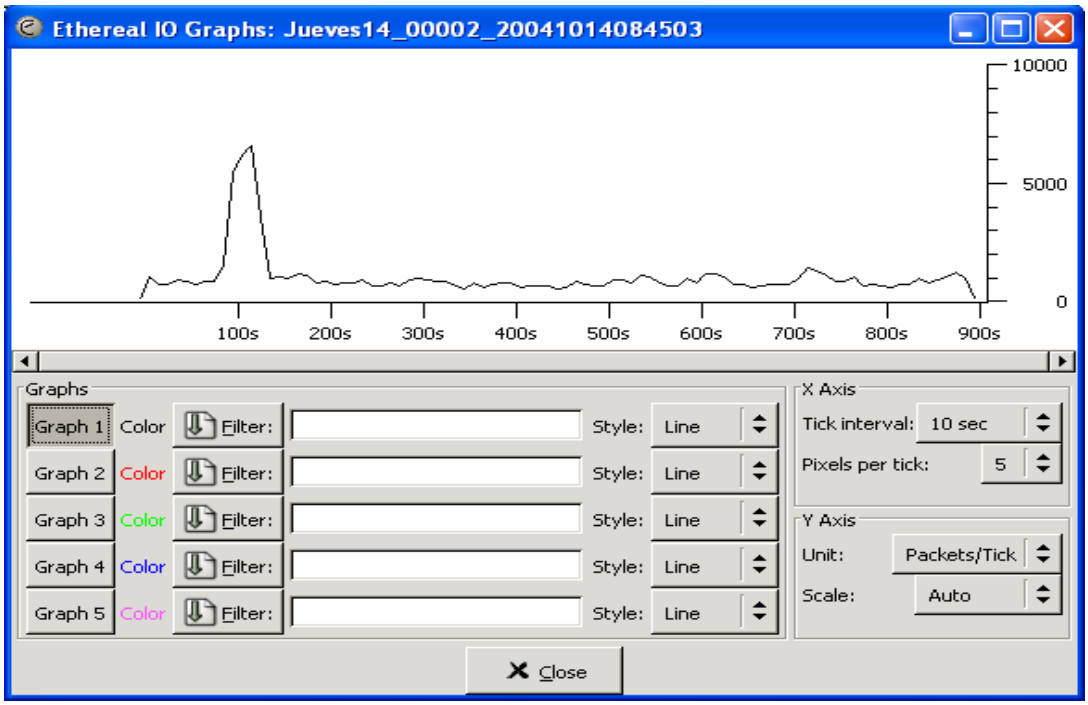


Figura 8. Puntos Finales (End Points).



Figuras 9. Interfaz gráfica.



Además Ethereal permite exportar los registros realizados a archivos de texto plano, para así poder ordenarla y analizarla con otras herramientas como bases de datos o software matemático.

2.4 PRUEBAS PRELIMINARES

Con el fin de probar la capacidad de la tarjeta y de llegar a la toma de datos, con los conceptos claros, y definida de la mejor manera la forma de hacer las campañas de medición, se realizaron una serie de pruebas preliminares en el laboratorio de redes de datos de la Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones.

2.4.1 Equipos de Prueba. Para la realización de estas pruebas preliminares y la toma de datos principal se cuenta con los siguientes equipos, pertenecientes

a la Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones de la Universidad Industrial de Santander.

- 1 Switch Cajun P880 de AVAYA [2]
- 1 Switch Cajun P333R de AVAYA
- 1 Switch Cajun P330 de AVAYA
- 1 Switch Cajun P550 de AVAYA
- 1 Tarjeta Gigabit Ethernet de Fibra Óptica de INTEL

En la figura 10 se muestra la tarjeta de red Gigabit Ethernet.

Figura 10. Tarjeta de Red Gigabit Ethernet de fibra óptica utilizada en la toma de datos.

Las especificaciones de la tarjeta se muestran en la Tabla 6.

[2] Las referencias completas de estos switches, de la tarjeta y demás equipos utilizados se especifican en el Anexo B, además de una descripción más detallada.

Tabla 6. Características de la Tarjeta utilizada.

Producto	Media	Conector	Compatibilidad IEEE
Intel® PRO/1000 Server Adapter	1000BASE-SX	SC connector	802.1p, 802.1Q, 802.3ac, 802.3ad, 802.3x, 802.3z, PCI v2.1

- Se utilizaron 4 equipos Optiplex GX 260 marca Dell como se referencia en el Anexo B. Sus características se especifican a continuación:

  - ✓ Procesador: Pentium 4 de 2.4 Ghz
  - ✓ Memoria RAM: 512 MB

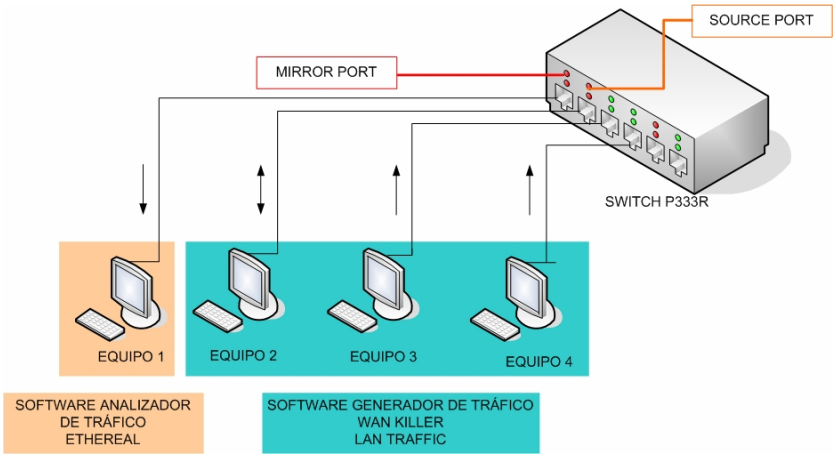
2.4.2 Procedimiento de las pruebas preliminares. Para estas pruebas preliminares se hizo uso de 4 equipos de cómputo, los cuales se nombraron de la siguiente manera para su configuración: Equipo Nº1, Equipo Nº2, Equipo Nº3 y Equipo Nº4.

El equipo Nº1 es donde están instalados los analizadores de tráfico, el equipo Nº2 es el equipo fuente y aquí se encuentra instalado un generador de tráfico, lo mismo que en los equipos Nº3 y Nº4. Se configuró el switch Cajun P333R de Avaya para que realizara un port mirror (puerto espejo, equipo Nº1) sobre un puerto fuente (equipo Nº2).

Por medio de dos herramientas generadoras de tráfico llamadas LanTraffic y Wankiller, esta última siendo una herramienta que posee uno de los analizadores de tráfico nombrados anteriormente, el SolarWinds, se dispuso a generar tráfico desde varios PCs hacia este puerto fuente. La función del port mirror era la de registrar por medio de los analizadores de tráfico seleccionados anteriormente todos los datos que entraran y salieran del puerto

fuente, para luego almacenarlos, clasificarlos y ordenarlos de una manera adecuada y así tener una visión clara de que está compuesto y cómo se comporta el tráfico de datos, para así poder plantear soluciones a posibles cuellos de botella. El esquema de esta prueba se aprecia en la figura 11.

Figura 11. Esquema de Pruebas Preliminares.



2.4.3 Escenarios. Para la prueba de la tarjeta Gigabit Ethernet se utilizó el Laboratorio de Redes de Datos, que cuenta con los equipos mencionados anteriormente menos el switch Cajun P880.

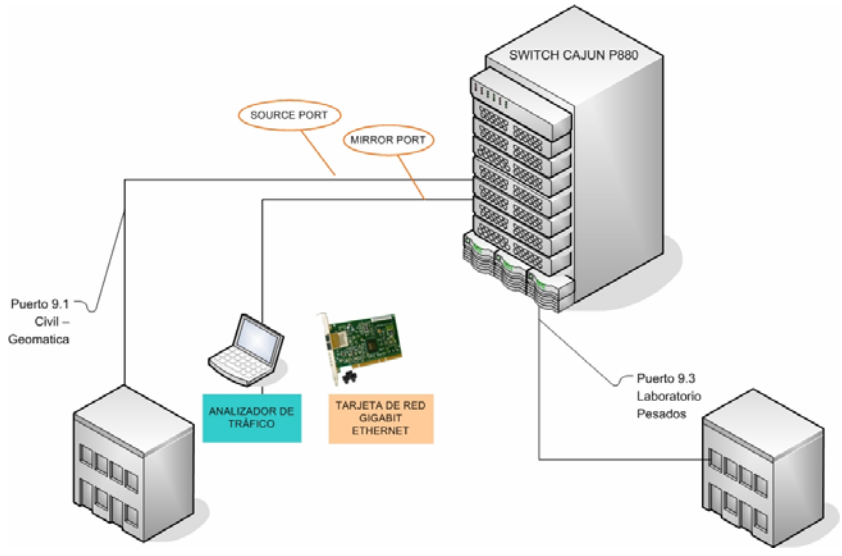
Para las campañas de medición se trasladó un PC, con la tarjeta Gigabit Ethernet debidamente instalada, al centro de cableado principal, lugar donde se encuentra ubicado el switch central de la Universidad Industrial de Santander.

Aquí también se realizaron unas pruebas preliminares ya que el flujo de datos es considerablemente mayor del que se podía generar en el Laboratorio de Redes, y esto con el fin de establecer el límite de la herramienta de software utilizada, Ethereal. La realización de estas pruebas y en general el desarrollo del proyecto se contó con la absoluta e importante colaboración de la división de servicios de información.

Estas pruebas duraron una semana y con ellas se llegó a conclusiones muy importantes como lo es la definición de los tiempos de captura de datos, los cuáles se habían establecido usando múltiples archivos cada quince minutos desde las 8:30am hasta las 6:00pm, esto debido a que los tamaños de los registros eran significativamente grandes, lo cual generaba un problema cuando se intentaban abrir estos archivos; ya que el PC se bloqueaba por la excesiva utilización de recursos de su sistema para ello.

También se definieron los puertos sobre los que se realizarán el registro de datos, los cuales son los puertos 9.1 y 9.3 correspondientes a CIVIL-GEOMÁTICA Y CIVIL- PESADOS[3] respectivamente. Estos se seleccionaron teniendo en cuenta el número de estaciones de trabajo presentes en ellos y consultando con el Ingeniero Benjamín Pico, administrador de la red de la universidad, quien por experiencia nos informó que puertos presentaban un tráfico de datos alto y medio. En la figura 12 se muestra el escenario de medición.

Figura 12. Escenario de medición.



[3] Estos puertos corresponden a estos edificios a la fecha de realización de los registros de datos.

3. METODOLOGÍA DE PROCESADO DE DATOS

En éste capítulo se expondrá la metodología propuesta para el registro y el procesamiento de los datos que se transmiten y se reciben de cualquier enlace del Backbone de la red de datos de la Universidad Industrial de Santander, la cual comprende los parámetros principales de medición, los intervalos de captura, la forma de usar y almacenar la información, la herramienta usada para la toma de los datos, los parámetros de registro, la herramienta usada para hacer la caracterización de los datos, y finalmente se muestran las consultas utilizadas para obtener los parámetros del tráfico.

3.1 ESCENARIOS DE MEDICIÓN

Con el objetivo de obtener resultados confiables y satisfactorios, es de rigor tener en cuenta los puertos a utilizar y el tiempo durante el cual se va a realizar la toma de datos. En el switch central de la universidad generalmente cada puerto corresponde a un edificio o parte de un edificio que conforman el campus. Se deben analizar los puertos que corresponden a los enlaces que forman parte del Backbone de la universidad para decidir en cuales de estos se realizan las campañas de medición. Esta información es útil para saber cuales puertos presentan un tráfico alto y cuales uno bajo. Para la metodología propuesta se establece que las medidas de los parámetros se deben hacer en los puertos que representen un tráfico de datos significativo.

Para realizar las campañas de medición se debe seleccionar un periodo de medida, durante el cual se van a tomar los datos, este puede ser durante el tiempo en el cual se llevan a cabo la mayor parte de las actividades

académicas y administrativas en la universidad, desde las 8:00 AM hasta las 6:00 PM, por lo tanto este será el periodo de medición. Es necesario evaluar el tráfico de cada puerto por separado, ya que la toma de datos se puede hacer solamente a un puerto a la vez.

Dado que la actividad académica tiene periodicidad semanal se sugiere realizar registros a lo largo de una semana para cada puerto, pues analizando estos datos se puede predecir con buena aproximación el comportamiento del tráfico de datos de la universidad.

Para poder observar el tráfico de datos del enlace y realizar el registro de estos, se configura un Puerto Espejo al puerto seleccionado de la siguiente manera:

- Primero que todo se debe verificar que haya disponibilidad de un puerto en el switch central Cajun P880 que sea compatible con la tarjeta de red Gibgabit Ethernet de fibra óptica, es decir, que posean las mismas características, como lo son el tipo de fibra óptica con el cual se conectará y el tipo de conector de ésta.
- Se conecta un PC al switch central Cajun P880 por medio de la tarjeta de red Gigabit Ethernet. Este PC debe contar con una buena capacidad de almacenamiento, ya que el tamaño de los archivos de registro es significativamente grande.
- Usando el setup del switch, se configura el Puerto Espejo (Mirror Port); esto se hace tomando como Puerto Fuente (Source Port), el puerto a analizar y como Mirror Port, el puerto por el cual se encuentra conectado el PC al switch.

Para que los datos tomados sean significativos y representen el comportamiento del tráfico en la universidad se necesita tener en cuenta las siguientes consideraciones:

- Es recomendable contar con una persona que esté presente durante la toma de datos para corregir posibles errores o desbordamientos en el equipo.
- También es recomendable no generar ningún tipo tráfico durante la toma de datos, dejar el equipo solo para recibir datos, ya que generación de tráfico desde éste alterará los resultados.
- Es necesario tener en cuenta que se deben realizar las tomas de datos en los días en que la universidad se encuentre en normalidad académica. No es recomendable realizar las capturas en días de anormalidad académica ya que el comportamiento del tráfico de datos no es el mismo, por no encontrarse la mayor parte de los estudiantes, personal administrativo y docente de la universidad, los cuales son los generadores de éste tráfico.

3.2 PARÁMETROS DE MEDICIÓN

Como se mencionó en el capítulo anterior[4] los parámetros para la evaluación de una red de datos de área local LAN, son variados y dependen de las necesidades o el interés del usuario. Entre éstos parámetros se consideran de manera primordial o básicos la distribución de protocolos, el tráfico que envían los host o estaciones finales, el tráfico multicast, broadcast, el total de bytes transmitidos y recibidos, la medida del ancho de banda y la distribución del tamaño de paquetes.

[4] Ver sección 1.2.1. Estadísticas del desempeño de la red.

3.3 INTERVALOS DE CAPTURA

Es importante tener en cuenta el intervalo de tiempo durante el cual se va a realizar el registro de datos; éste puede variar según se necesite. De acuerdo con estudios realizados[5], para obtener la distribución de protocolos y la carga total de tráfico en los enlaces, el registro de datos se debe realizar por intervalos de 10 a 15 minutos y obtener el valor medio de la carga a lo largo del periodo de medida. La longitud de este intervalo es importante para determinar si se producen o no variaciones considerables de la magnitud a medir e identificar cuales son los protocolos más utilizados en la red LAN de la Universidad.

Para la toma de datos, se sugiere realizar los registros en intervalos de 15 minutos a lo largo del periodo de medición establecido previamente, ya que ensayos realizados durante un intervalo de tiempo más grande, 30 minutos o 1 hora, generan archivos de gran tamaño que ocupan mucho espacio de almacenamiento en el equipo de medida, y que son difíciles de manejar por la herramienta Ethereal.

Hay que tener en cuenta que es necesario organizar los datos capturados de una forma que sean de fácil identificación uno del otro, ya que se van a obtener muchos de estos registros durante el periodo de medida. Ethereal permite obtener múltiples archivos de registro durante un tiempo prolongado de medición, como puede ser una mañana o una tarde, y organizarlas de forma que cada una sea identificable de las otras con nombre, fecha y hora. El nombre lo da el usuario y Ethereal añade automáticamente la fecha y la hora.

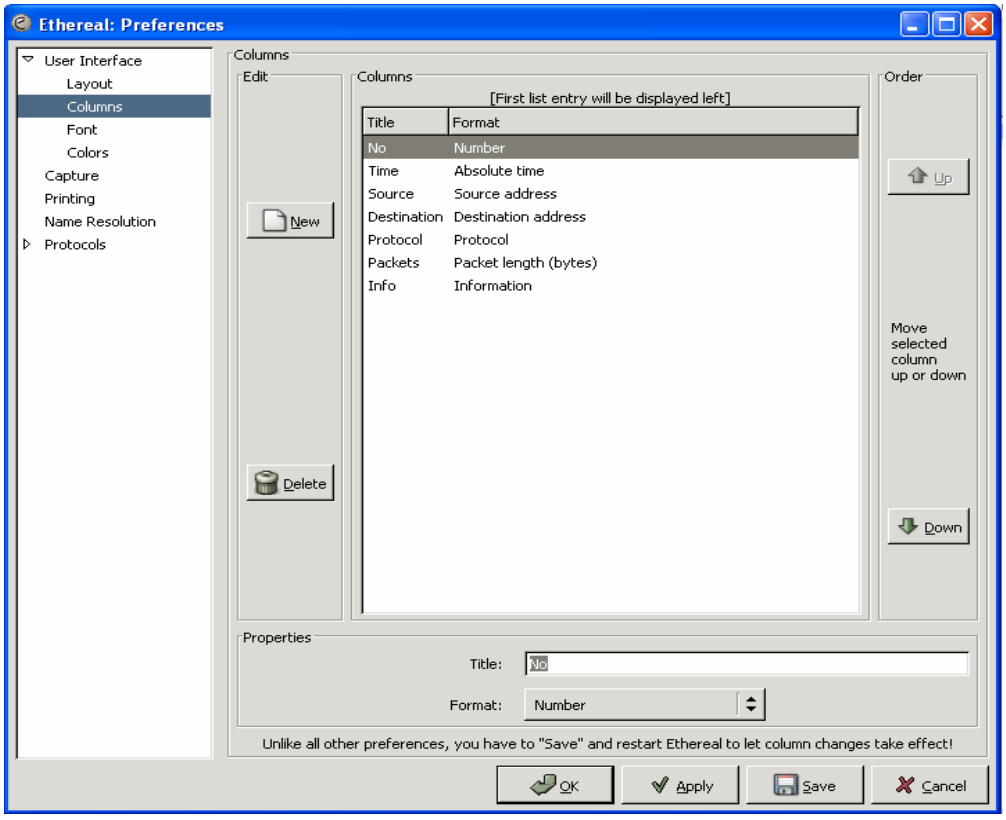
[5] Ver sección 1.3.1

3.4 PARÁMETROS DE CAPTURA

Antes de realizar la toma de datos es necesario seleccionar los parámetros de captura que nos den información útil del tráfico de datos.

Ethereal nos permite seleccionar las características que deseemos del tráfico de datos como el número del paquete, el tiempo en que se transmitieron los paquetes con fecha y hora, la dirección origen, la dirección destino entre otros. Estos parámetros se pueden seleccionar en la configuración del analizador de tráfico en la opción *Preferences* del menú *Edit* de la ventana principal de Ethereal, en donde se pueden escoger varios parámetros para observar diferentes características de las capturas, dependiendo de aquellas que sean de interés para el usuario. En la figura 13 se muestran estos parámetros.

Figura 13. Selección de los parámetros de captura en el analizador de tráfico.



Para la metodología propuesta, dentro de los parámetros de interés de los paquetes capturados que nos dan información útil están la dirección origen, la dirección destino, el protocolo usado y el tamaño de los paquetes en bytes, las demás características como direcciones hardware destino y origen u otra información sobre los paquetes que también es importante, no es necesaria para el desarrollo de estas capturas. Tampoco es necesario el contenido de los paquetes para obtener los parámetros de medición del tráfico.

Para el desarrollo de los registros de datos se deben utilizar los parámetros mostrados en la tabla 7, seleccionados en la configuración del Ethereal.

Tabla 7. Parámetros de información de captura.

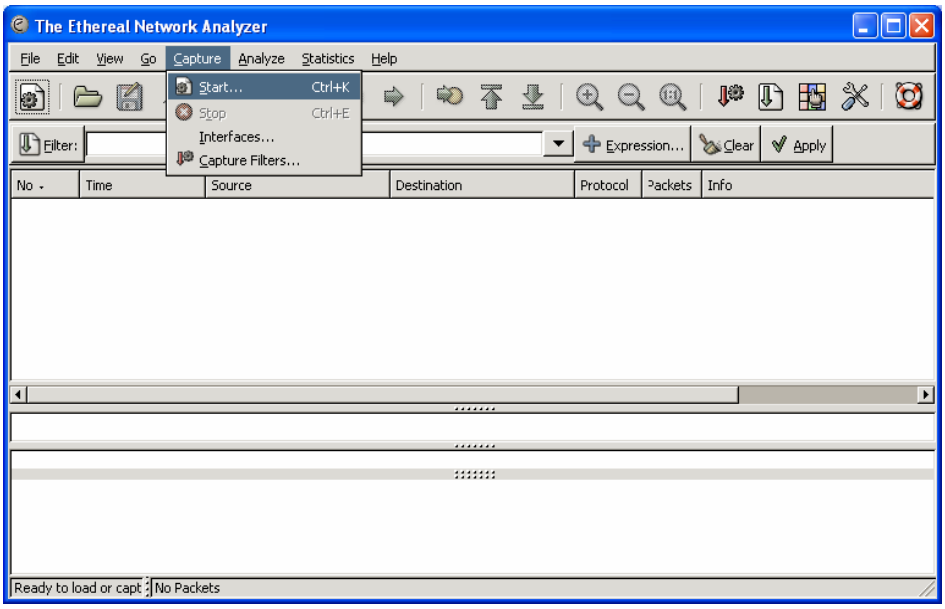
Name	No	Time	Source	Destination	Protocol	Bytes
Formato	Number	Absolute Time	Source Address	Destination Address	Protocol	Packet length bytes

Hay que tener en cuenta que las direcciones origen y destino de los paquetes capturados deben ser las direcciones IP de los equipos presentes en el enlace de datos y no las direcciones con resolución de nombres y dominios.

3.5 TOMA DE DATOS

Para iniciar las capturas se tiene que ir al menú *Capture* de la ventana principal de Ethereal como se muestra en la figura 14.

Figura 14. Inicio de Capturas



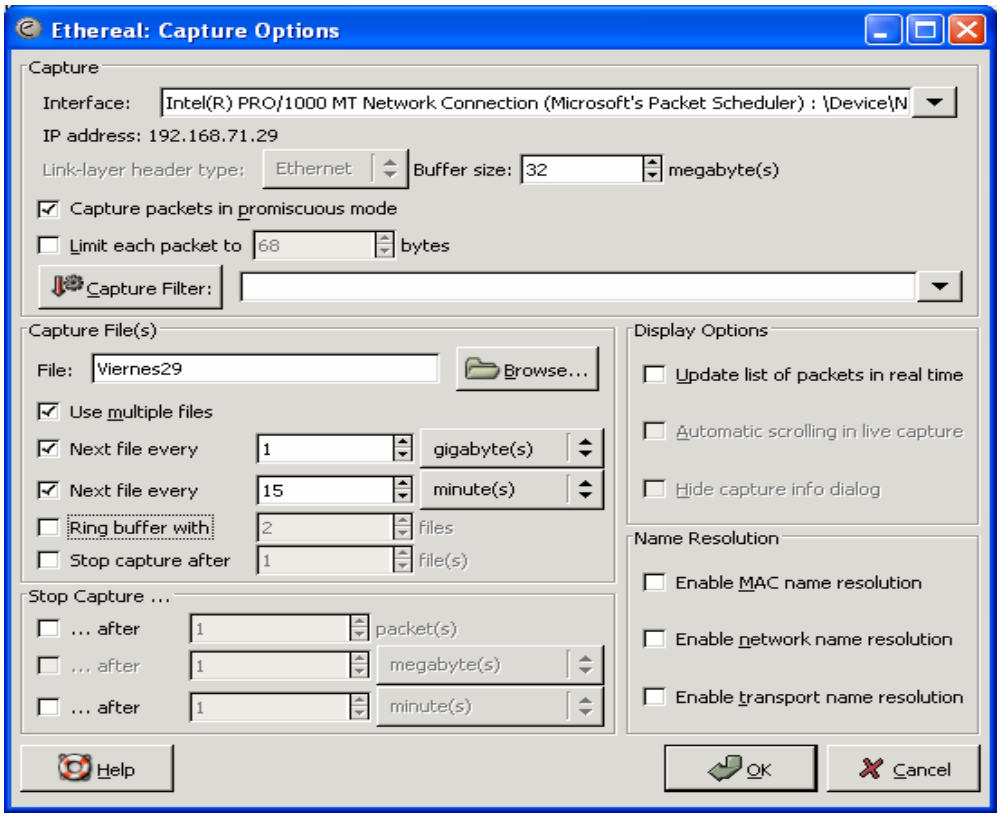
Luego para realizar la toma de datos de una forma en que se obtengan los resultados esperados se necesitan definir las opciones de captura. Estas opciones se describen a continuación:

- Se deben utilizar intervalos de captura de 15 minutos.
- Determinar un tamaño límite de archivo de 1 gigabyte por cada captura, para evitar un desbordamiento o bloqueo en el Ethereal y evitar que el intervalo de captura no se cumpla.
- Se debe deshabilitar la resolución de nombres y dominios de las direcciones.
- Se recomienda usar un buffer de 32 megabytes para evitar que la herramienta se desborde y no tome todos los datos presentes en el enlace y llegue a presentar errores.
- Se debe habilitar la opción de usar múltiples archivos para que la herramienta genere estos a medida que transcurre el periodo de medición establecido.

- Se debe especificar una ruta de almacenamiento y un nombre con el cual se van a identificar los archivos de registro, Ethereal le añade automáticamente la hora y la fecha para distinguirlos.
- Se debe seleccionar la interfaz por medio de la cual se va a realizar el registro, en este caso la tarjeta de red Gigabit Ethernet de fibra óptica que se instaló en el equipo.
- Los demás parámetros se recomienda no tenerlos en cuenta y no cambiarlos ya que para el fin que se persigue no tendrán ninguna funcionalidad. Estas opciones se muestran en la figura 15.

Una vez establecidas estas opciones se pueden iniciar las capturas de los datos teniendo en cuenta que estas solo se detendrán cuando el usuario lo desee o según se haya programado.

Figura 15. Configuración de las opciones de captura.



3.6 ALMACENAMIENTO DE LOS DATOS

Para poder utilizar la información capturada en las sesiones es necesario utilizar una base de datos que sea accesible. Esta base de datos debe poseer la capacidad de trabajar con una gran cantidad de información y realizar las consultas de los datos en un tiempo relativamente rápido. Para poder usar la información capturada es necesario exportarla a un formato que sea compatible con la base de datos a utilizarse. Dentro de los formatos que dispone la herramienta de captura para exportar los datos a otro formato están el texto plano, el post script y el xml.

El texto plano posee la ventaja de ser fácil de utilizar y manejar con cualquier base de datos, para los demás formatos no se cuenta con las licencias de las herramientas o bases de datos para manejarlos.

Al exportar los datos a otro formato hay que tener en cuenta que se debe seleccionar la información que sea útil. Durante el proceso de captura se obtiene la siguiente información sobre los paquetes:

- Las características o parámetros de captura que se seleccionaron.
- Detalles de los paquetes que dan información sobre las etiquetas.
- El contenido de los paquetes como tal.

De estos solo son útiles los parámetros seleccionados, sin los demás detalles ni el contenido de los mismos; esta información no es necesaria y ocupará un gran espacio de almacenamiento en el equipo.

Como el Ethereal solo permite ver un archivo de registro a la vez es necesario abrir y exportar estos, tantas veces como archivos se haya capturado.

Primero se abre el archivo de captura en Ethereal y para cerciorarse de que la información que se va a exportar es la adecuada y necesaria se debe verificar en el menú *View* de la ventana principal de Ethereal, que el Formato para mostrar el Tiempo sea el Tiempo de Día y que todas las opciones en Resolución de Nombres estén desactivadas como se muestra en las figuras 16 y 17, después de esto se selecciona la opción *Reload* y se procede a la exportación.

Figuras 16. Formato de Tiempo de Día

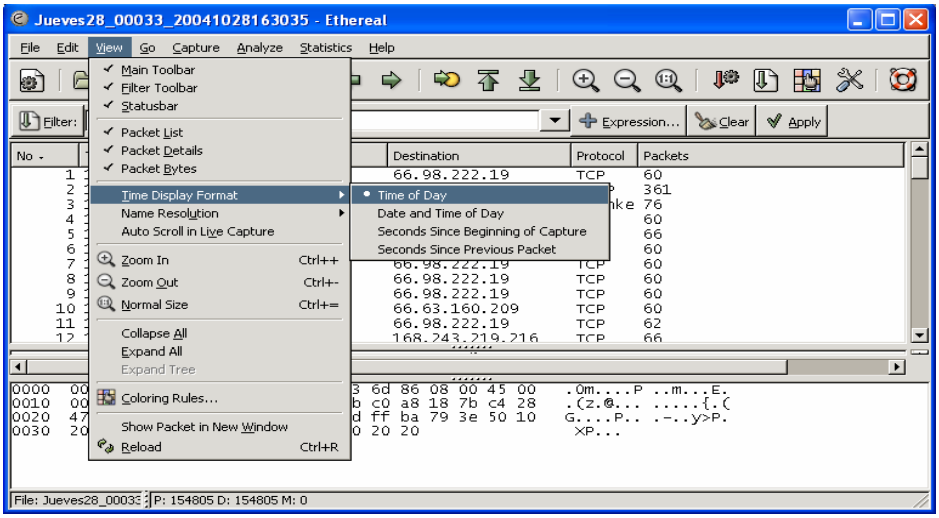
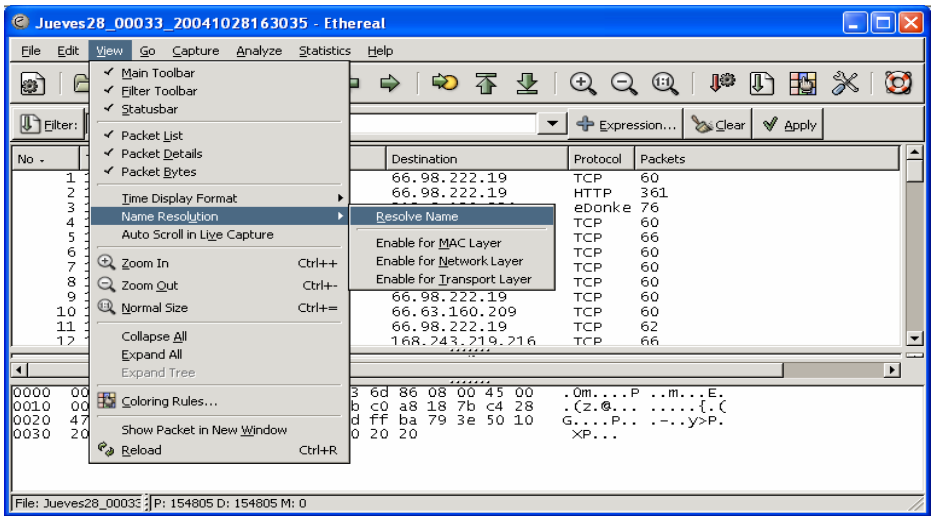
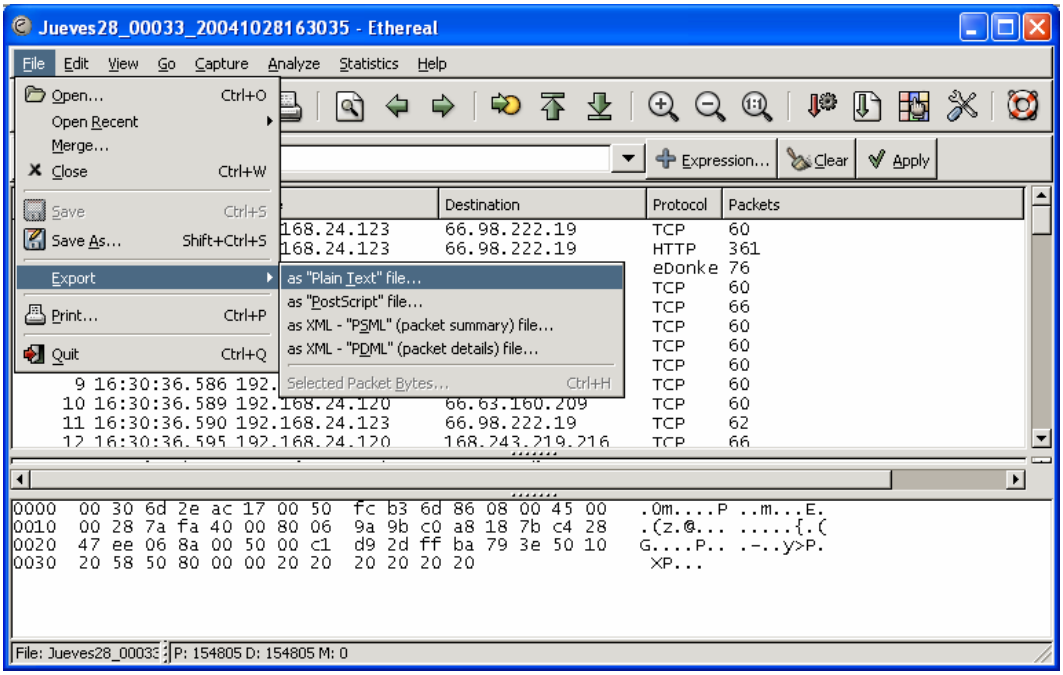


Figura 17. Resolución de Nombres.



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 como se muestra en la figura 18.

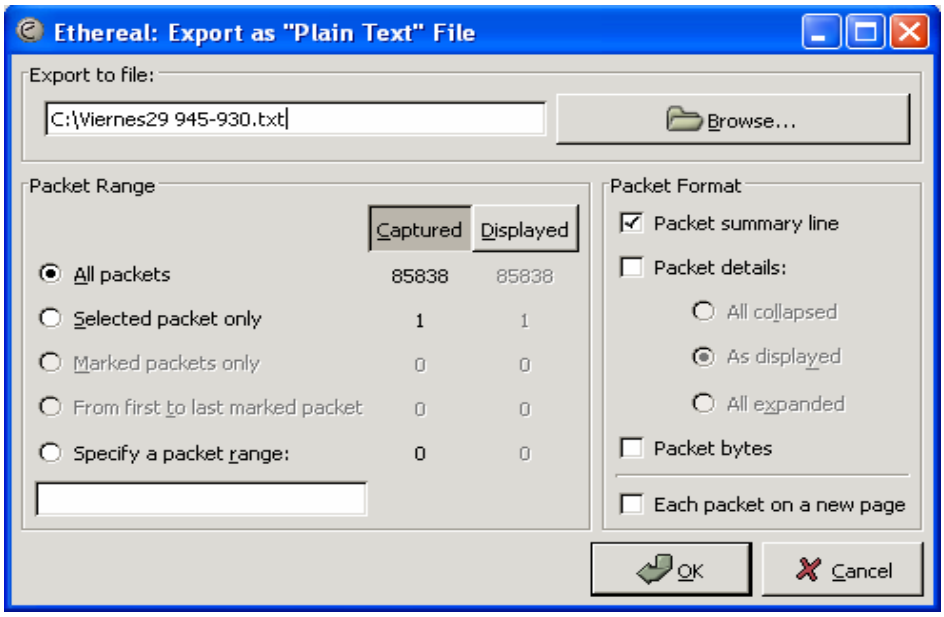
Figura 18. Exportación de archivos de captura.



Para exportar los datos necesarios sólo se debe utilizar la opción *Packet summary line* y desactivar las opciones *Packet details* y *Packet bytes*. Se debe especificar la ruta en donde se desean almacenar los archivos y su nombre. La figura 19 muestra como se deben exportan los datos al formato texto plano.

El resultado son archivos de texto que contienen la información necesaria en una forma más fácil de procesar y de un tamaño más reducido. Luego estos archivos de texto serán abiertos en la base de datos a utilizarse en donde se le aplicará un procedimiento para extraer los parámetros de medición establecidos.

Figura 19. Exportación de capturas a texto plano.



Cuando ya se tengan todos los archivos de texto es recomendable agruparlos en uno o varios archivos, ya sea por horas, por jornadas o por días, según se requiera. Para realizar esta tarea se puede recurrir a un software de unión de archivos de texto, como lo es el Simple File Joiner, de libre adquisición en Internet.

Se recomienda no intentar abrir con el block de notas estos archivos unidos, pues si son muy grandes seguramente se bloqueará el PC.

3.7 TABLAS Y CONSULTAS

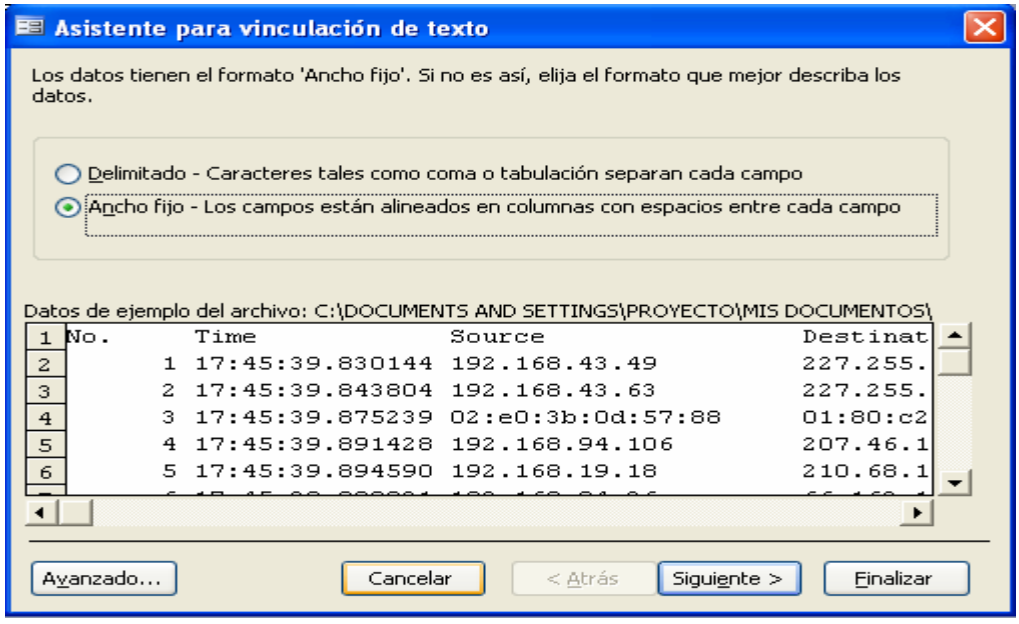
Para obtener los parámetros de medición se deben vincular los archivos de texto obtenidos por medio de una base de datos, en este caso Microsoft Access. De esta vinculación se generarán una o varias tablas según el usuario requiera, que contienen la información de las capturas, y con estas se

realizarán las consultas que mostrarán los parámetros de medición establecidos.

La vinculación de los archivos de texto se realiza de la siguiente manera:

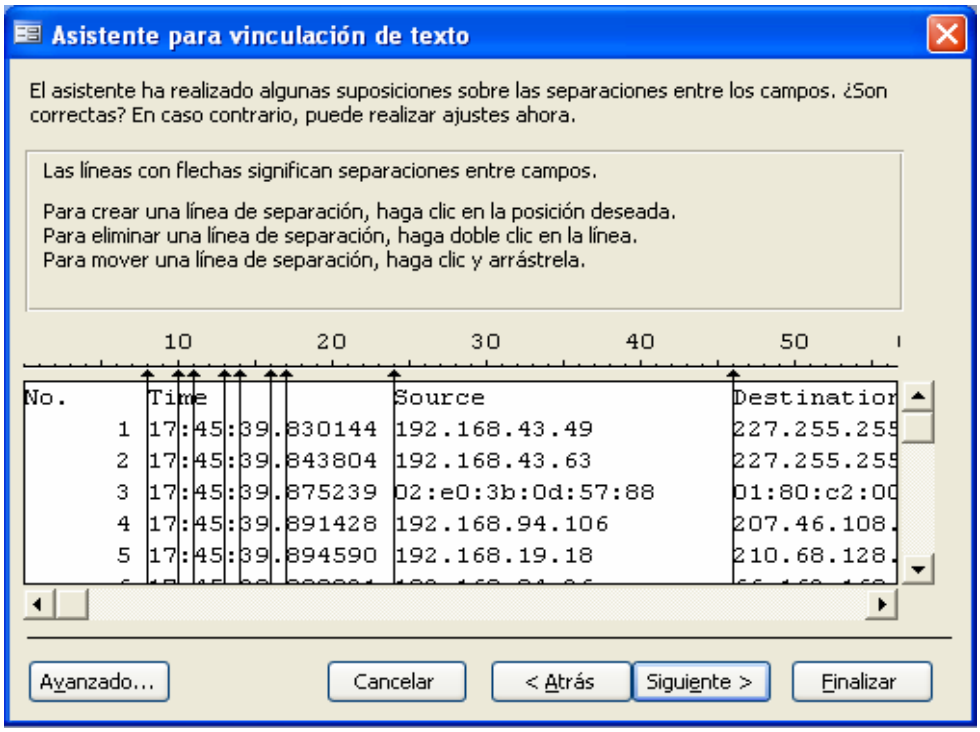
1. Se procede a abrir los archivos de texto con Microsoft Access mostrando el asistente para la vinculación de archivos de texto, figura 20.

Figura 20. Asistente para vinculación de texto.



2. Se siguen las instrucciones que nos muestra el asistente dejando este como se muestra en la figura 21. Esto se hace con el fin de crear una tabla en donde se encuentren separadas las horas, los minutos y los segundos para así poder graficar y hacer un análisis con la libertad de tiempo que se requiera. Se recomienda revisar con cautela todos los campos, ya que se pueden estar creando algunos innecesarios o lo contrario.

Figura 21. Definición de campos.



3. Se usa la opción Avanzado y se verifica que el tipo de dato de cada campo corresponda a lo que se requiera, es decir, los campos en los se necesite que se lean como número, el tipo de dato debe ser entero largo, en los demás el tipo de dato debe ser texto, como se especifica en la Figura 22. Una vez configuradas estas opciones se guardan y se continúa con el proceso.
4. En dado caso que se tengan más archivos de texto para vincular, se hace clic derecho como se muestra en la figura 23, se selecciona vincular tablas y se abre el archivo deseado. De nuevo se vuelve al menú Avanzado, se usa la opción Especificaciones, donde se encuentra almacenada la configuración establecida anteriormente, se acepta y se finaliza.

Figura 22. Especificaciones de vinculación.

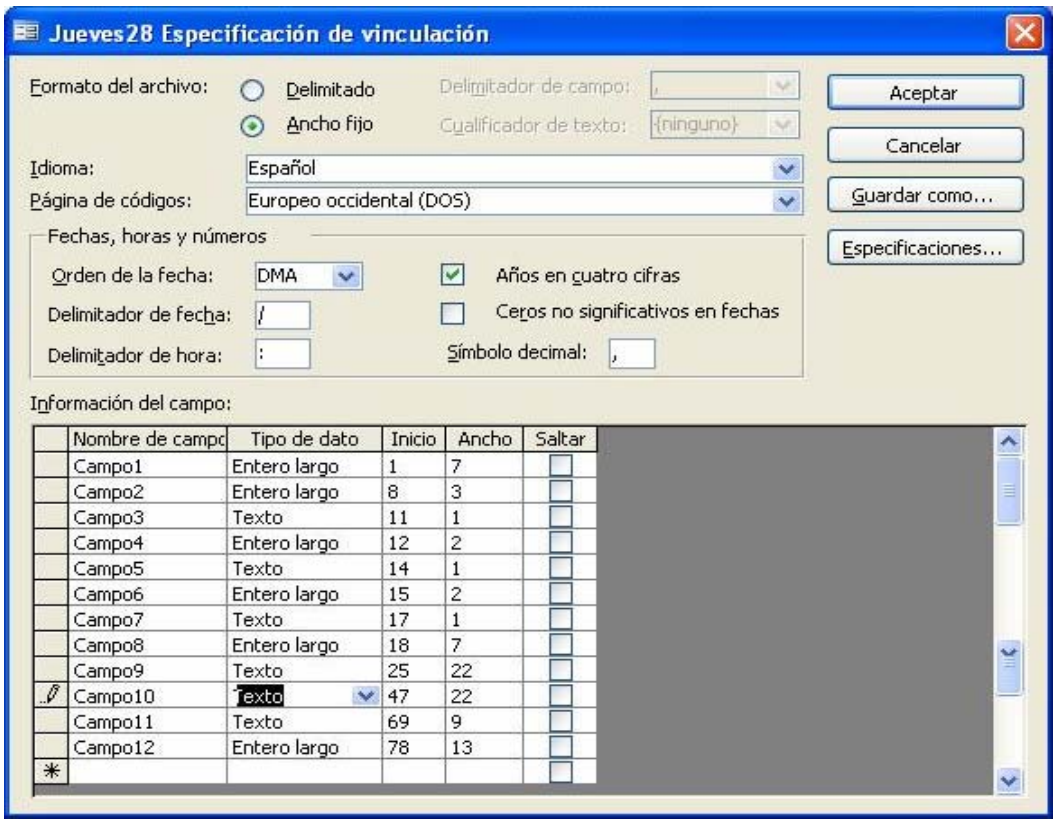
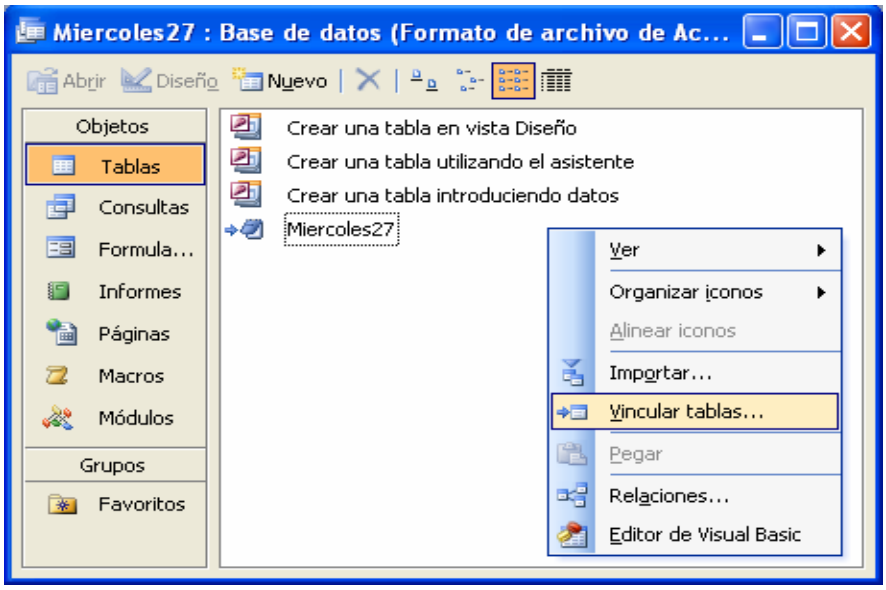
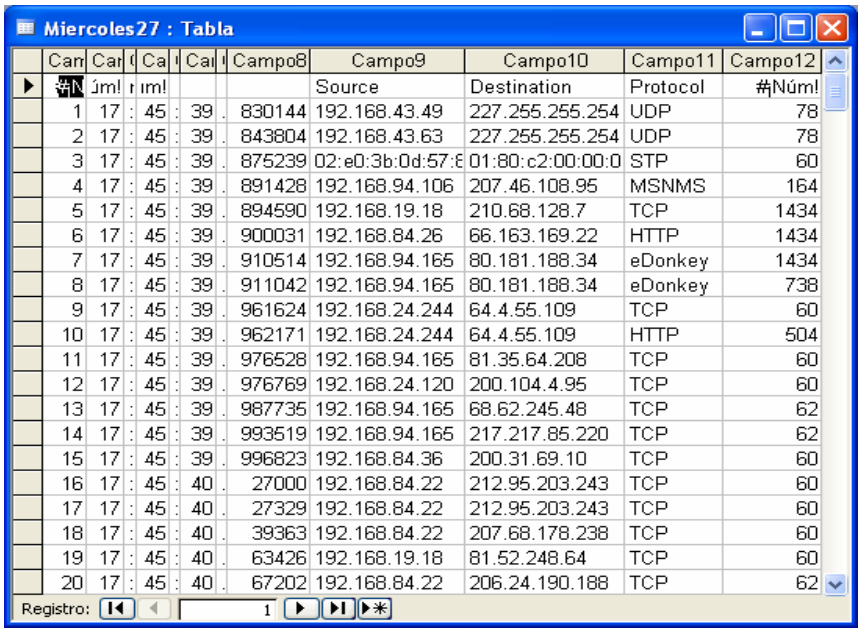


Figura 23. Vinculación de tablas.



En la figura 24 se muestra una tabla de datos, resultado de la vinculación de los archivos de texto.

Figura 24. Tabla de datos.



Miercoles27 : Tabla

Campo8	Campo9	Campo10	Campo11	Campo12
	Source	Destination	Protocol	#Núm!
830144	192.168.43.49	227.255.255.254	UDP	78
843804	192.168.43.63	227.255.255.254	UDP	78
875239	02:e0:3b:0d:57:8	01:80:c2:00:00:0	STP	60
891428	192.168.94.106	207.46.108.95	MSNMS	164
894590	192.168.19.18	210.68.128.7	TCP	1434
900031	192.168.84.26	66.163.169.22	HTTP	1434
910514	192.168.94.165	80.181.188.34	eDonkey	1434
911042	192.168.94.165	80.181.188.34	eDonkey	738
961624	192.168.24.244	64.4.55.109	TCP	60
962171	192.168.24.244	64.4.55.109	HTTP	504
976528	192.168.94.165	81.35.64.208	TCP	60
976769	192.168.24.120	200.104.4.95	TCP	60
987735	192.168.94.165	68.62.245.48	TCP	62
993519	192.168.94.165	217.217.85.220	TCP	62
996823	192.168.84.36	200.31.69.10	TCP	60
27000	192.168.84.22	212.95.203.243	TCP	60
27329	192.168.84.22	212.95.203.243	TCP	60
39363	192.168.84.22	207.68.178.238	TCP	60
63426	192.168.19.18	81.52.248.64	TCP	60
67202	192.168.84.22	206.24.190.188	TCP	62

Registro: 1

Los campos generados en la tabla a partir de la vinculación de los archivos de texto corresponden cada uno a la siguiente información, se mencionan los que representan información:

- ✓ Campo 1: Número de cada paquete transmitido o recibido.
- ✓ Campo 2: Hora.
- ✓ Campo 4: Minutos.
- ✓ Campo 6: Segundos.
- ✓ Campo 9: Dirección Origen.
- ✓ Campo 10: Dirección Destino.
- ✓ Campo 11: Protocolo
- ✓ Campo 12: Tamaño en bytes de cada paquete.

Una vez vinculado el archivo o todos los archivos de texto en la base de datos se pueden obtener los parámetros de medición deseados haciendo Consultas en Microsoft Access, estas consultas se realizan seleccionando uno o varios campos de las tablas vinculadas a la base de datos y seleccionando una opción para agrupar los datos, o también seleccionando un tipo de filtro.

En la tabla 8 se muestran las diferentes consultas realizadas con los campos y criterios de selección.

Tabla 8. Consultas realizadas.

CONSULTAS O PARÁMETROS DE MEDICIÓN	CAMPOS A UTILIZARSE	AGRUPAR POR	CRITERIOS DE SELECCIÓN
Distribución de protocolos	Campo 11 Campo 12	Agrupar por suma campo 12	
Carga de bytes	Campo 2 Campo 4 Campo 12	Agrupar por suma campo 12	
Orígenes y Destinos	Campo 9 Campo 10 Campo 12	Agrupar por suma campo 12	
Numero de paquetes	Campo 2 Campo 4 Campo 12	Agrupar por cuenta campo 12	
Distribución de tamaño de paquetes	Campo 12 Campo 12	Agrupar por suma campo 12	
Broadcast	Campo 9 Campo 10 Campo 12		Como "*.255.255" O Como "*ff" (campo 10)
Multicast	Campo 9 Campo 10 Campo 12		Como "*.255" Y Negado Como "*.255.255" (campo 10)

Estas consultas se muestran en detalle en el anexo C.

3.8 CRONOGRAMA DE ACTIVIDADES DE LA TOMA DE DATOS.

En la tabla 9 se presenta el cronograma de actividades que se llevó a cabo durante la toma de datos.

Como la realización de esta toma de datos se planeó para dos puertos, el tiempo que se determinó necesario para la caracterización de cada uno de estos fue de una semana.

Fue necesario hacer otras pruebas preliminares pero ya con el switch P880, estas pruebas preliminares tuvieron una duración de una semana.

Tabla 9. Cronograma de registros.

EDIFCIO CIVIL-GEOMÁTICA Puerto 9.1	LUNES	MARTES	MIERCOLES	JUEVES	VIERNES
HORA INICIO	8:30 am	8:30 am	8:30 am	8:30 am	8:30 am
HORA FIN	6:00 pm	6:00 pm	6:00 pm	6:00 pm	6:00 pm

EDIFCIO CIVIL- PESADOS Puerto 9.3	LUNES	MARTES	MIERCOLES	JUEVES	VIERNES
HORA INICIO	8:30 am	8:30 am	8:30 am	8:30 am	8:30 am
HORA FIN	6:00 pm	6:00 pm	6:00 pm	6:00 pm	6:00 pm

La fecha de inicio de la toma de datos en el puerto 9.1 que corresponde al edificio Civil-Geomática fue el día Jueves 14 de Octubre de 2004 y su fecha de finalización el día Lunes 25 de Octubre de 2004.

La fecha de inicio de la toma de datos en el puerto 9.3 que corresponde al edificio Civil-Pesados fue el día Martes 26 de Octubre de 2004 y su fecha de finalización el día Lunes 8 de Noviembre de 2004.

Como se puede notar este es un lapso de tiempo mayor a dos semanas, como era previsto. Esto se debe a la anormalidad académica presentada por la Universidad en estos días y también por la presencia de unos días festivos.

En el siguiente capítulo se muestran los resultados obtenidos con las campañas de medición.

4. RESULTADOS Y ANÁLISIS OBTENIDOS

En éste capítulo se muestran los diferentes parámetros utilizados para la caracterización del tráfico de los dos enlaces seleccionados del Backbone de la Universidad Industrial de Santander, los resultados obtenidos después de su posterior ordenamiento y su análisis correspondiente.

Como se mencionó en el capítulo anterior los datos serán analizados usando características de la base de datos Microsoft Access. Los parámetros se presentarán en el orden en que se definieron en el capítulo anterior.

4.1 DISTRIBUCIÓN DE PROTOCOLOS

La distribución de protocolos muestra la cantidad de protocolos usados en el tráfico de datos de la red institucional, en este caso en los puertos 9.1 y 9.3 correspondientes a Civil-Geomática y Civil-Pesados respectivamente. Esta distribución de protocolos es presentada en un tipo de gráfica circular mostrando sus porcentajes de utilización durante el día. Para una mejor visualización, se toman los protocolos más significativos presentes en las diferentes jornadas que se realizaron para la toma de datos y se muestran de una forma independiente; los demás protocolos que no representan un tráfico significativo de datos se agrupan en una sola categoría llamada otros, figuras 25 y 27.

4.1.1 Puerto 9.3 (Civil-Pesados). En el puerto 9.3 correspondiente a Civil-Pesados se puede observar que la distribución de protocolos durante la semana o periodo de medición es similar. Generalmente siempre hay 5 protocolos que son los que consumen el mayor ancho de banda del enlace, estos protocolos

son TCP, HTTP, SMB, eDonkey y Gnutella, el resto del ancho de banda lo consumen alrededor de unos 125 protocolos como SMTP, TDS, ARP, NBSS, UDP, MSNMS, entre otros. Estos protocolos consumen aproximadamente un 3% del ancho de banda del enlace, figura 25.

La mayor parte del ancho de banda en este puerto está siendo consumido por protocolos de la capa transporte y un porcentaje más pequeño está siendo consumido por protocolos de la capa de aplicación y la capa de red.

Como se puede observar hay un excesivo uso del protocolo de la capa transporte TCP, seguido por protocolos como eDonkey y Gnutella que son utilizados para descargas de archivos como música y video especialmente; a éste tipo de tráfico se le conoce como tráfico P2P (Peer to Peer), dando a entender que se está utilizando la mayoría del ancho de banda del Backbone de la Universidad solo para este tipo de consultas o descargas. Una de las desventajas de este tipo de tecnología es el consumo de ancho de banda de la red de una forma incontrolable produciendo cuellos de botella además del fomento de la piratería.

Podría asumirse que el tráfico TCP se debe a descargas comunes como documentos, páginas de Internet, material académico, etc., pero se sabe que programas P2P como Kazaa, iMesh, BitTorrent, eMule, etc., utilizan el protocolo TCP para transportar y compartir archivos. Para determinar las razones por las cuales se presenta este porcentaje elevado de TCP, se hizo un análisis en el cuál se encontró que el porcentaje de utilización del protocolo TCP debido a protocolos como Netbios-ssn, HTTP, FTP-DATA, Microsoft-ds, MSNMS, los cuales lo utilizan para su funcionamiento, es muy pequeño en comparación al tráfico total de éste, atribuyendo así que el tráfico restante se debe a programas de descarga de archivos o P2P, como se muestra en la figura 26.

Este análisis se realizó haciendo un muestreo aleatorio simple de cuatro muestras de la población total de cada día. Cada muestra corresponde a un registro de 15 minutos y la población total corresponde a los 38 registros obtenidos durante todo el día.

Para dar certeza de los resultados obtenidos se calculó el error muestral en el cual se tomo una probabilidad del 95% de confiabilidad, para una población finita. Éste valor de error obtenido es del 10.3%, dando confianza de los resultados obtenidos.

Con las muestras obtenidos se realizó un filtrado del tráfico generado por el protocolo TCP teniendo en cuenta el número de puerto origen y puerto destino de cada paquete, para lo cual se utilizó como criterio de selección, que los puertos que van del 1 al 1024 son los usados por los protocolos de aplicación más conocidos y que los puertos de usuario que van del 1024 al 65535 son los más usados por aplicaciones P2P.

Es normal que sea el protocolo HTTP el segundo en uso pues la consulta de páginas Web y la navegación en Internet ya hace parte de la actividad propia de buena parte de la comunidad universitaria.

Protocolos como SMB y NBSS que son de uso interno presentan un porcentaje de utilización de ancho de banda bajo comparándolos con los anteriores.

Figura 25. Distribución de protocolos, puerto 9.3. Los datos están porcentajes de utilización.

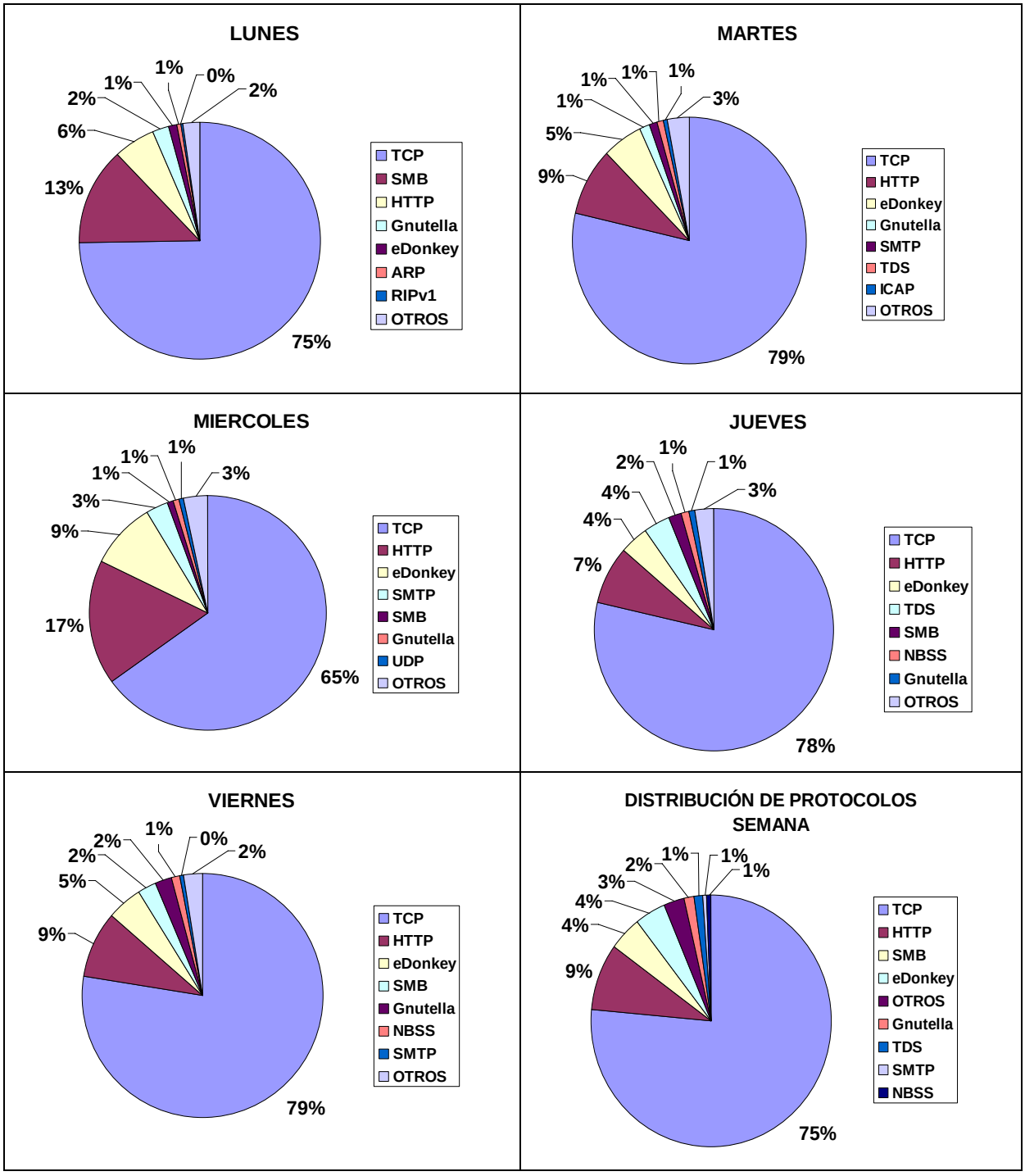
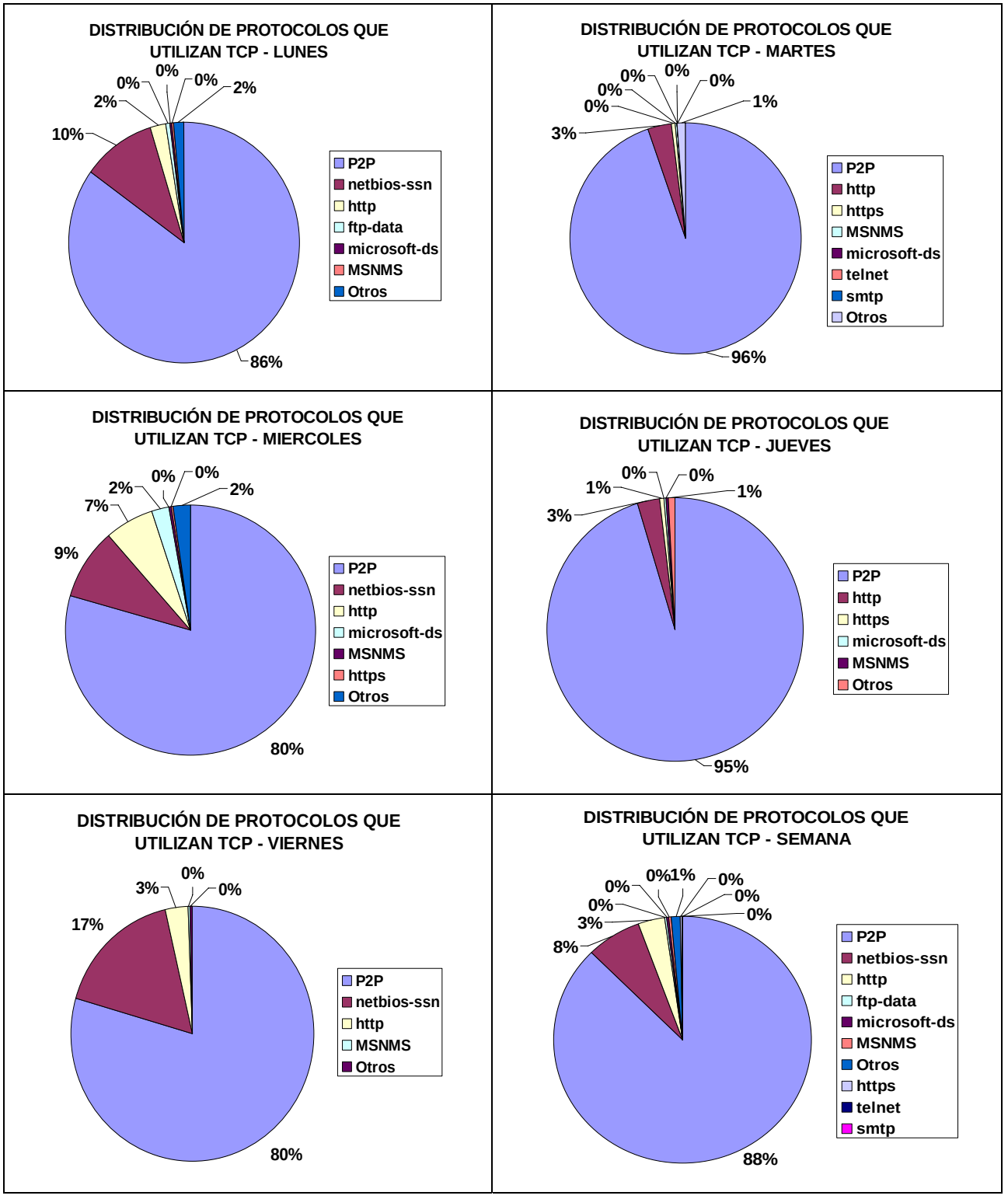


Figura 26. Distribución de protocolos que utilizan TCP, puerto 9.3. Los datos están porcentajes de utilización.



4.1.2 Puerto 9.1 (Civil-Geomática). Se encuentra que el comportamiento de los protocolos en el puerto 9.1 correspondiente a Civil-Geomática es similar durante todo el periodo de medición. Se observa que el porcentaje de los protocolos más significativos no varía mucho durante los diferentes días y estos son casi siempre los mismos.

Generalmente siempre hay cuatro o cinco protocolos que son los que consumen el mayor ancho de banda del enlace. Entre estos protocolos están TCP, HTTP, SMB, eDonkey y UDP, los cuales consumen cerca del 90% de éste. El resto del ancho de banda lo consumen unos 140 protocolos distintos entre los cuales se encuentran ARP, ICMP, DNS, STP, entre otros. Estos protocolos consumen aproximadamente un 2% del ancho de banda de este puerto. Esta misma característica se puede observar durante los diferentes días en que se realizó la toma de datos, figura 27.

Se puede observar que la mayor parte del ancho de banda está siendo consumido por protocolos de la capa de aplicación como eDonkey, HTTP, y SMB; un porcentaje también considerable está siendo consumido por protocolos de la capa de transporte como TCP y UDP, y un porcentaje más pequeño está siendo consumido por otros protocolos entre los cuales se encuentran protocolos de la capa de red como ARP, DNS, DHCP y SMTP entre otros.

Se observa que el ancho de banda es consumido en gran parte por aplicaciones que comparten archivos como música, video, documentos, textos, las cuales hacen uso de protocolos como eDonkey, TCP, y Gnutella, y un porcentaje también considerable está siendo consumido por los servicios de paginas Web, los cuales hacen uso de protocolos como HTTP.

Al igual que en el puerto 9.3 se hizo un análisis en el cuál se encontró que el porcentaje de utilización debido a protocolos como Netbios-ssn, HTTP,

Microsoft-ds, MSNMS, SMTP, que utilizan para su funcionamiento el protocolo de la capa de transporte TCP, es relativamente pequeño en comparación al tráfico total de éste, atribuyendo así el tráfico restante a programas de descarga de archivos o P2P. Esto se muestra en la figura 28.

Figura 27. Distribución de protocolos, puerto 9.1. Los datos están porcentajes de utilización.

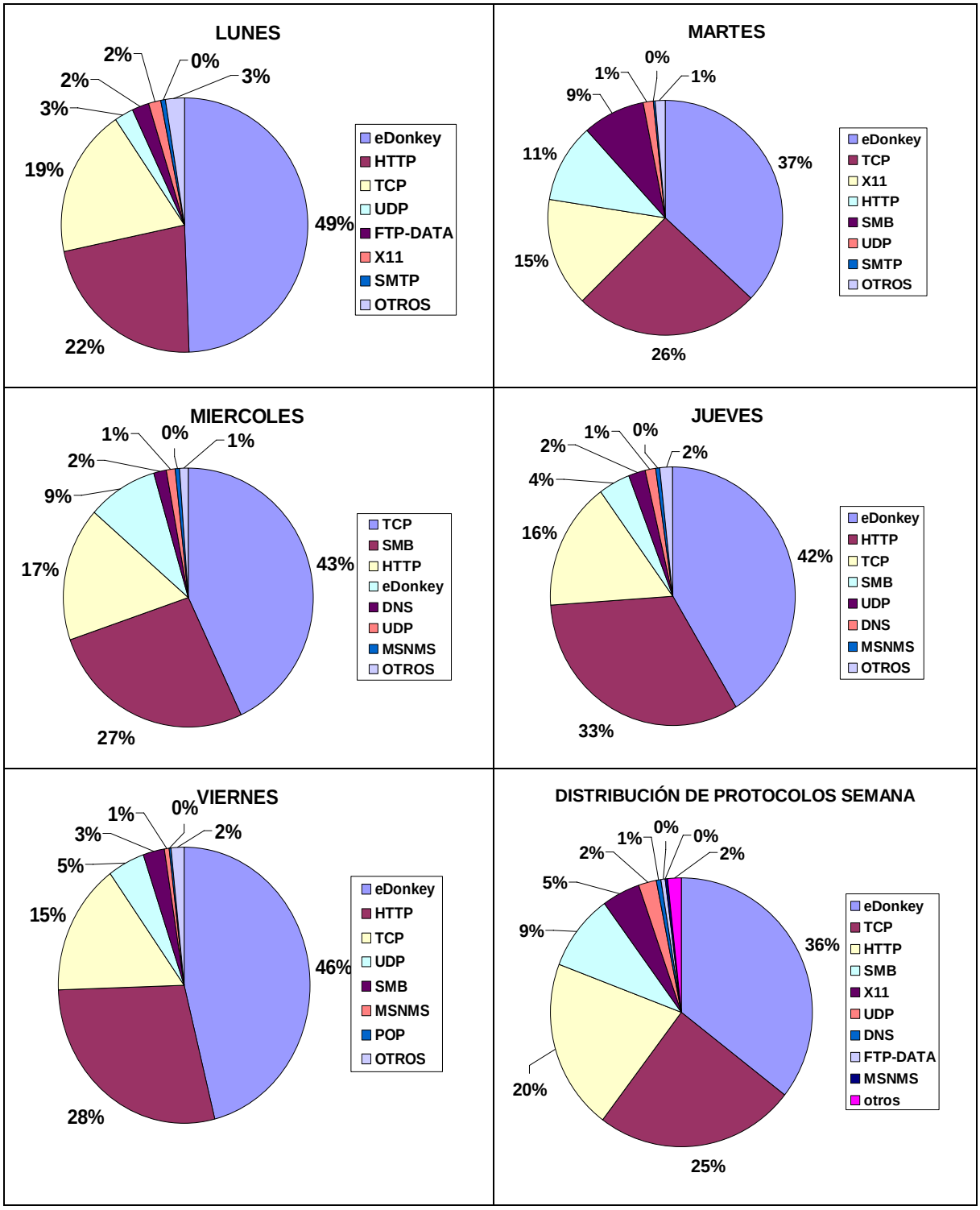
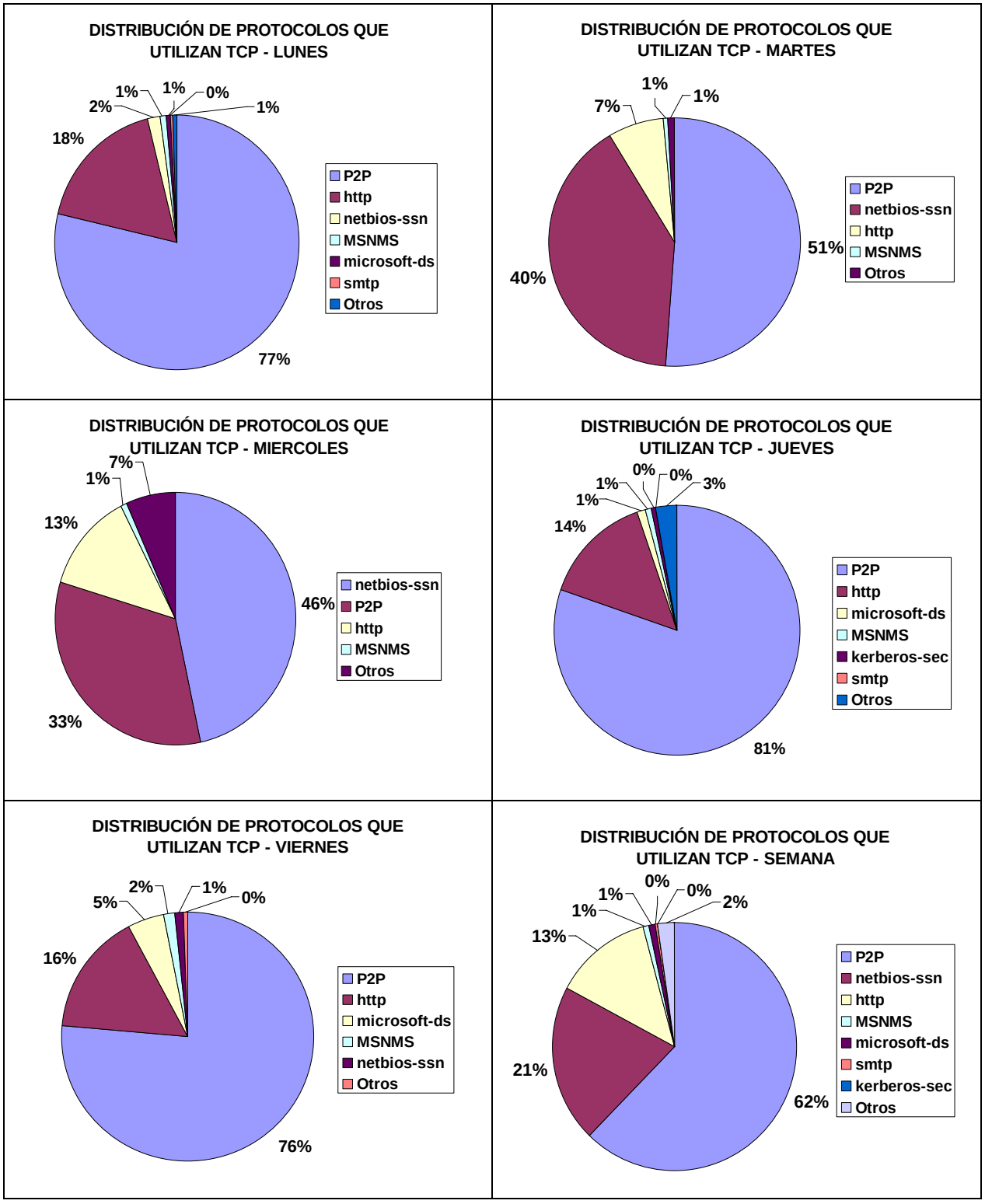


Figura 28. Distribución de protocolos que utilizan TCP, puerto 9.1. Los datos están porcentajes de utilización.



4.2 DISTRIBUCIÓN DE LA CARGA DE TRÁFICO

La distribución de la carga de tráfico muestra el ancho de banda utilizado durante el periodo de medida. Para una mejor visualización esta se presenta en un gráfico de columnas en donde el eje de las *y* representa el ancho de banda en Mbps cada 15 minutos y el eje de las *x* representa el tiempo.

4.2.1 Puerto 9.3 (Civil-Pesados). En el puerto 9.3 correspondiente a Civil-Pesados se observa que el comportamiento del tráfico es muy variable, pero con alguna similitud a lo largo de algunos días u horas.

Como se puede notar el día de mayor tráfico y consumo de ancho de banda es el Lunes, seguido del día Jueves, Viernes, Martes y por último con una considerable caída del tráfico el día Miércoles, pero esta conclusión solo es debida a la suma de la carga durante el día. También se debe tener en cuenta que se producen picos de gran tamaño a distintas horas del día y un promedio bajo y constante durante otros lapsos del día, como se puede notar comparando los días Martes y Jueves, este comportamiento se muestra en la figura 29.

Se puede concluir que el tráfico de carga es más pesado durante la jornada de la mañana, específicamente durante la primera mitad de la mañana, seguida por el tráfico del mediodía, y con el tráfico más bajo la segunda mitad de la mañana.

En la tabla 10 se muestra la carga de tráfico y el ancho de banda en el puerto 9.3.

Figura 29. Distribución de la carga de tráfico y porcentaje de utilización, puerto 9.3.

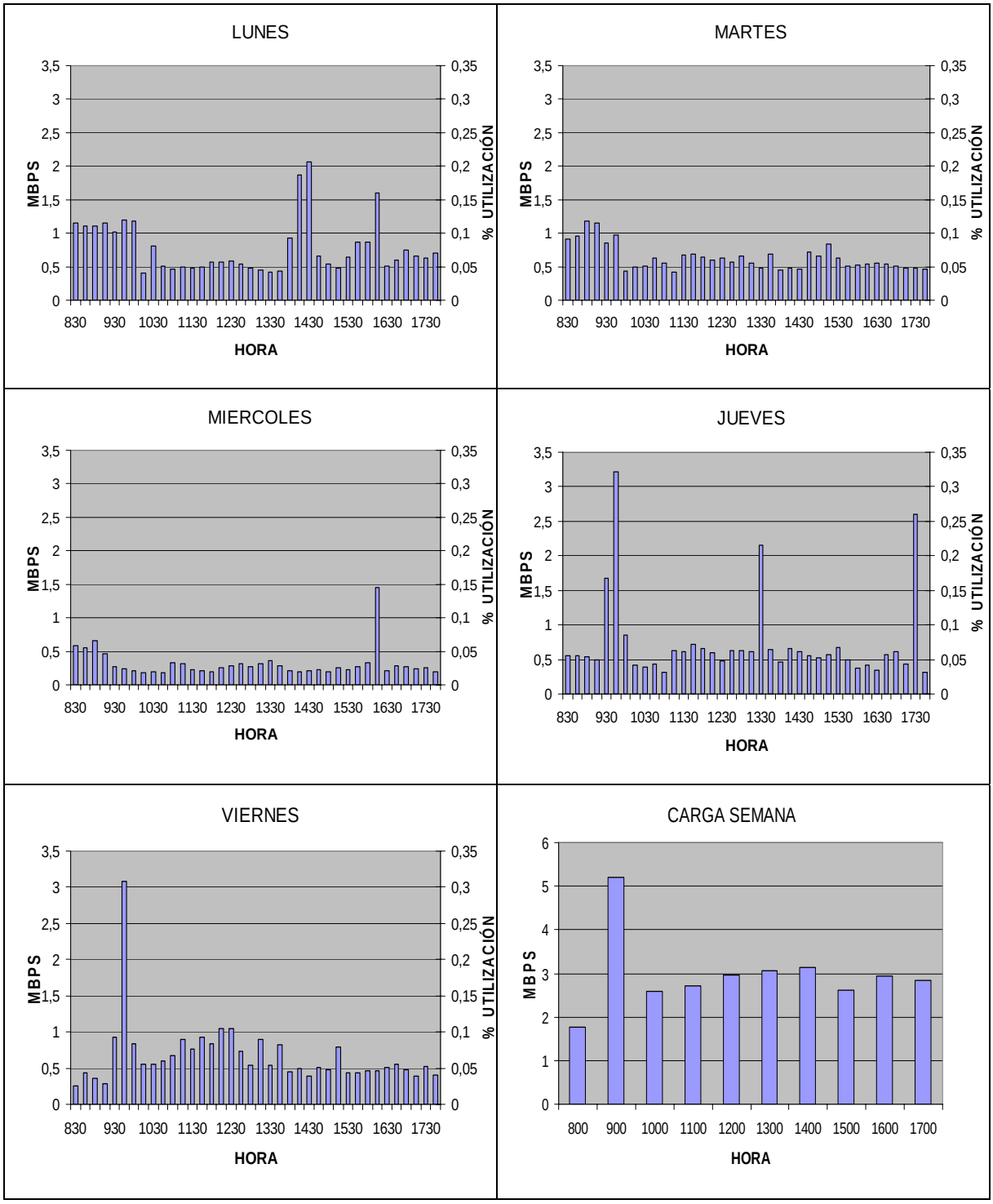


Tabla 10. Distribución de la carga de tráfico y ancho de banda, puerto 9.3.

DÍA	CARGA	ANCHO DE BANDA
Lunes	3.37 Gb	0.788 Mbps
Martes	2.71 Gb	0.633 Mbps
Miércoles	1.34 Gb	0.312 Mbps
Jueves	3.15 Gb	0.738 Mbps
Viernes	2.85 Gb	0.667 Mbps

Razones por las cuales se produce este tráfico particular existen muchas, debido a su variabilidad, pero con base en las observaciones anteriores sobre la distribución de protocolos y el uso de la red por parte de las personas se puede llegar a las siguientes interpretaciones:

- Una razón por la cual el tráfico de datos de la red institucional es más alto en la mañana es debido al inicio de la jornada laboral y académica de la comunidad UIS en general, por tanto se encienden las estaciones de trabajo, se llega a consultar el correo electrónico, leer las noticias, etc., generando un tráfico alto.
- El alto tráfico que se presenta al comienzo de la mañana tiene mucha relación con la tendencia de aumento presentada al finalizar la tarde, debido a una utilización excesiva de software P2P como se mencionó anteriormente. Se puede afirmar pero no de manera general, que estudiantes, personal administrativo y en general la comunidad UIS, utilizan estos programas para descargar música, videos, películas, software etc., aprovechando el fin de las clases o su jornada laboral para dejar los equipos de cómputo encendidos, descargando todo este tipo de material, lo que lleva a un aumento del ancho de banda utilizado al finalizar la tarde, en la noche y al inicio de la mañana del siguiente día.

- Se podría deducir que la razón por la cual el tráfico de la segunda mitad de la jornada de la mañana es el más bajo, es debido a que las estaciones de trabajo son utilizadas para labores académicas por tanto las personas que se encuentran haciendo este tipo de descargas cierran estos programas, para evitar ser detectados por el docente o los estudiantes que se encuentran en estas clases y también debido a que algunos o casi todos estos programas consumen recursos de la máquina, limitando así el uso de estas estaciones de trabajo.
- El mediodía es una parte del día en que por lo general la red de la Universidad no presenta un alto uso interno, ya que esta es una hora de descanso para la mayoría de la comunidad, pero que es aprovechada para navegación, consulta de correo y otras actividades propias del uso del Internet, presentando así un porcentaje de utilización medio.

4.2.2 Puerto 9.1 (Civil-Geomática). En este puerto se puede observar que el tráfico durante los días en que se realizó la toma de datos comienza con un tráfico relativamente bajo y crece a medida que se van realizando las actividades en la universidad; finalizando la mañana se presentan un tráfico alto. En el periodo comprendido entre los doce del mediodía y las dos de la tarde se observa una disminución considerable en el tráfico; esto se debe probablemente a la ausencia de estudiantes en la universidad durante este tiempo, pero después de esta hora el tráfico retoma un nivel alto. A medida que transcurre la tarde diminuye un poco debido al cese de actividades en la universidad. Este comportamiento se muestra en la figura 30.

Terminando la tarde se puede observar un incremento en el tráfico que no desciende como se esperaría; esto puede deberse a que algunos equipos en la universidad permanecen encendidos después de esta hora, lo cual genera tráfico durante la noche y la mañana siguiente.

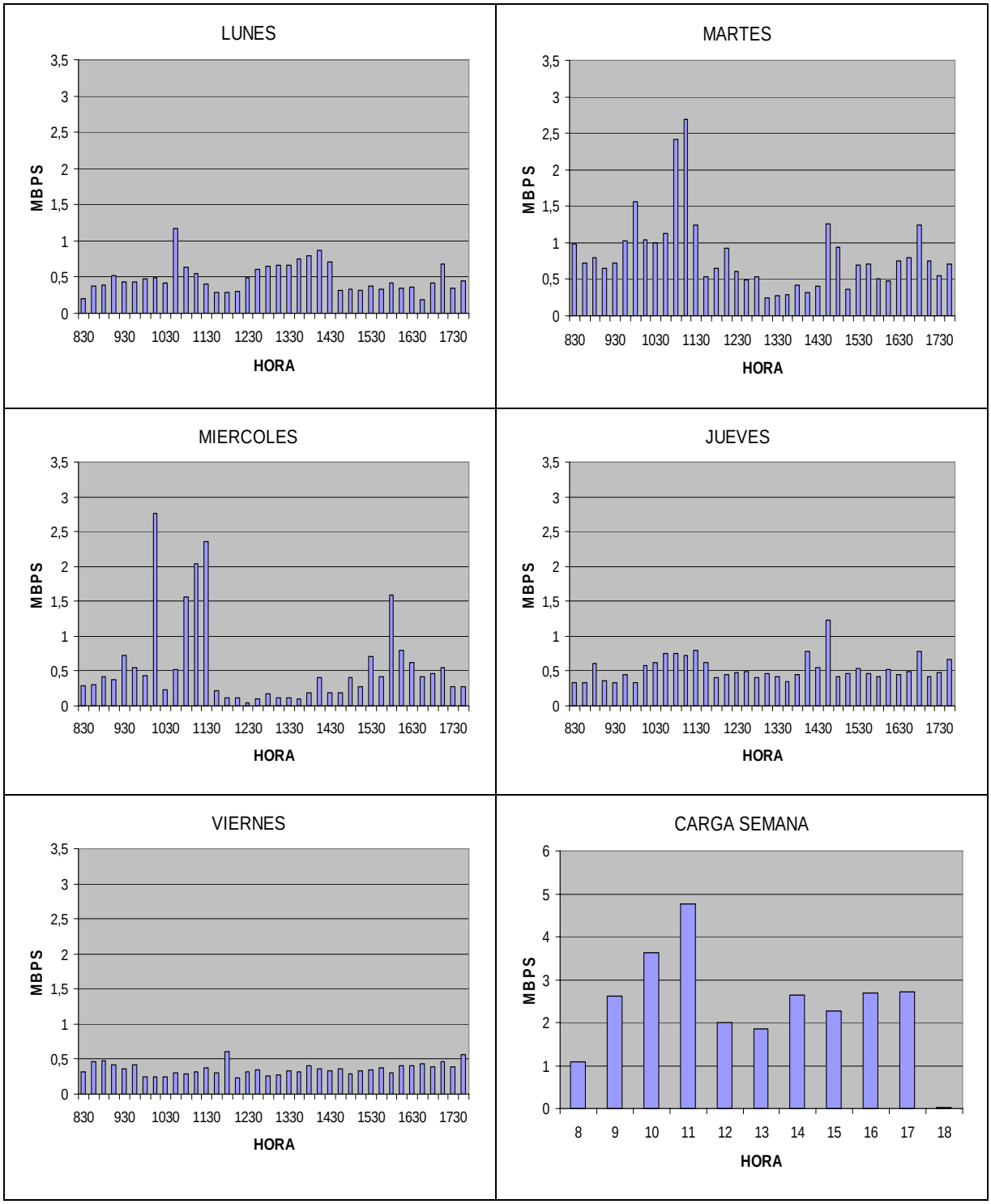
Durante el periodo de medida se puede observar que el tráfico en los días Lunes y Viernes es relativamente bajo, en los días Martes, Miércoles y Jueves es más alto; esto puede reflejar un patrón de clases y horarios de los estudiantes durante la semana. En la tabla 11 se muestra la carga de tráfico y ancho de banda durante el periodo de medida en el puerto 9.1.

Tabla 11. Distribución de la carga de tráfico y ancho de banda, puerto 9.1.

Día	CARGA	ANCHO DE BANDA
Lunes	2.078 Gb	0.486 Mbps
Martes	3.533 Gb	0.827 Mbps
Miércoles	2.411 Gb	0.564 Mbps
Jueves	2.27 Gb	0.530 Mbps
Viernes	1.53 Gb	0.359 Mbps

Los dos enlaces del backbone de la Universidad bajo estudio poseen un ancho de banda de 1Gbps. De acuerdo con la distribución de carga obtenida en estos dos enlaces durante el periodo de medida establecido, se determinó que estos presentan un porcentaje de utilización del 0.35% como máximo, por lo cual se concluye que este ancho de banda está siendo subutilizado.

Figura 30. Distribución de la carga de tráfico, puerto 9.1.



4.3 DISTRIBUCIÓN DEL NÚMERO DE PAQUETES

La distribución del número de paquetes se muestra de una manera similar a la distribución de la carga, en gráficos de columnas durante el periodo de medida.

4.3.1 Puerto 9.3 (Civil-Pesados). Como se puede observar en las gráficas el número de paquetes transmitidos y recibidos durante el día muestra una semejanza con la distribución de la carga, siendo la jornada de la mañana en la que más número de paquetes se transmiten y se reciben, también especialmente en la primera mitad de la mañana. Esto deja más en claro una de las anteriores afirmaciones, en las que se concluye que este tráfico alto es debido a transporte de paquetes por medio de programas P2P.

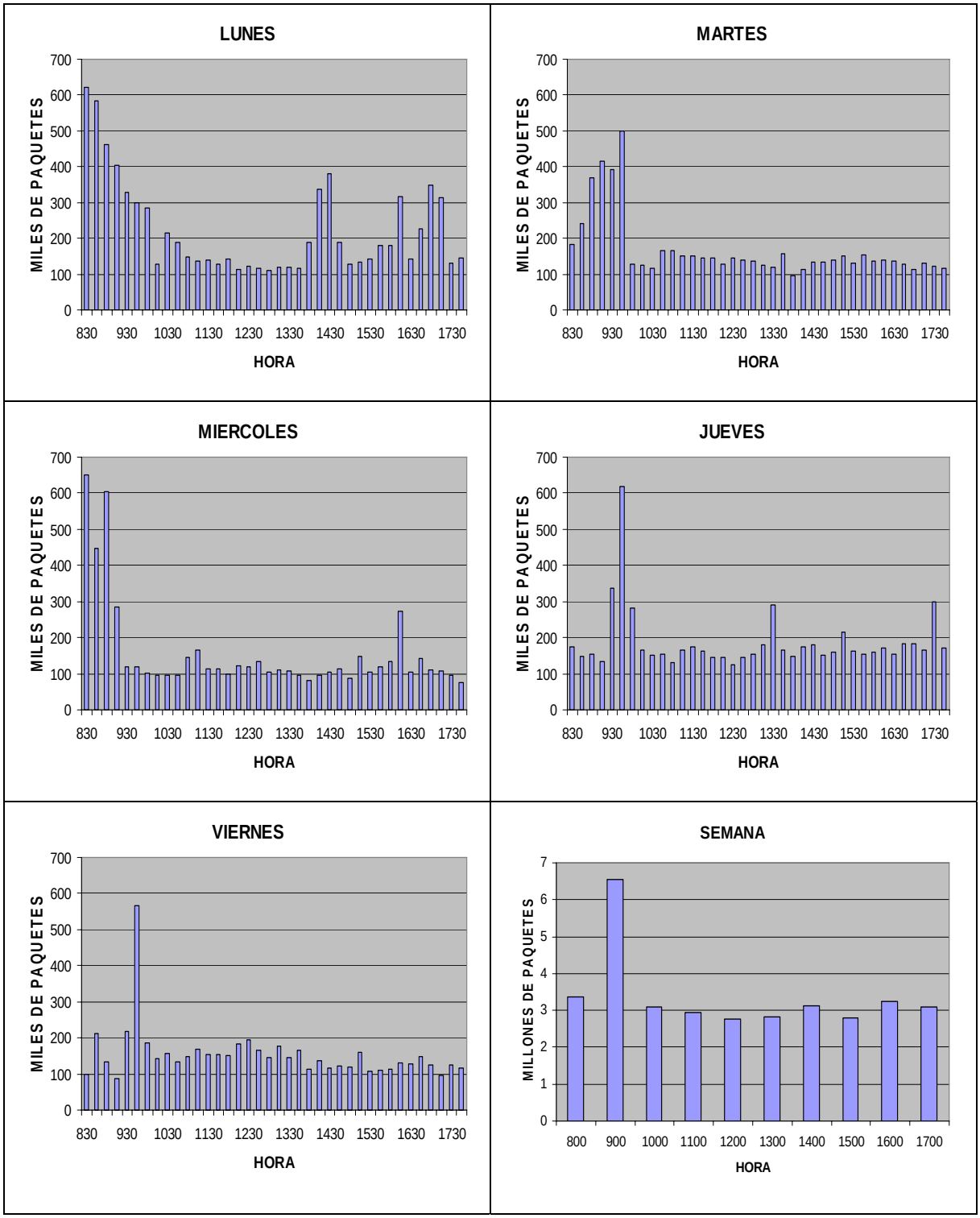
Cabe notar que la carga de tráfico y el número de paquetes no muestran un comportamiento exacto ya que como se observa gráficamente tienen algunas diferencias, debido a que el tamaño de los paquetes es muy variado, es decir, la carga de tráfico no es directamente proporcional al número de paquetes. La distribución del número de paquetes se muestra en la figura 31.

En la tabla 12 se muestra el número de paquetes por día.

Tabla 12. Distribución del número de paquetes, puerto 9.3.

DÍA	NÚMERO DE PAQUETES
Lunes	8 508 289
Martes	6 417 228
Miércoles	5 929 586
Jueves	7 131 539
Viernes	5 860 700

Figura 31. Distribución del número de paquetes, puerto 9.3.



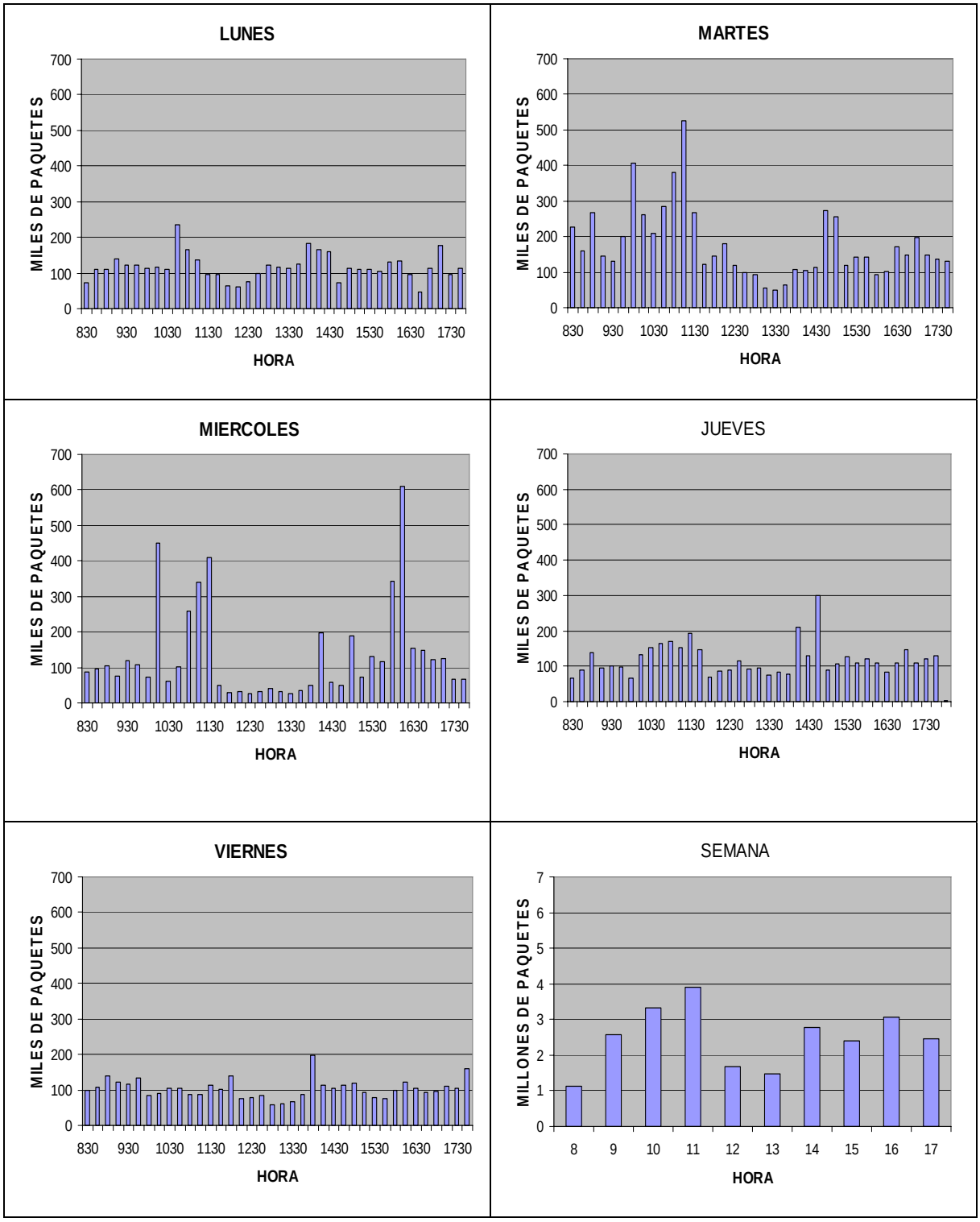
4.3.2 Puerto 9.1 (Civil-Geomática). La distribución de número de paquetes muestra la cantidad de paquetes transmitidos y recibidos durante el periodo de medida. Se puede observar que el número de paquetes a lo largo del periodo de medida varía mucho y en general es proporcional a la cantidad de bytes transmitidos y recibidos. Se observa que el día en que se transmitieron más paquetes es el martes, correspondiendo al día en que se transmitieron la mayor cantidad de bytes. En la figura 32 se observa la distribución de número de paquetes en cada día de la semana.

En la tabla 13 se muestra la distribución de número de paquetes durante los diferentes días de toma de datos.

Tabla 13. Distribución del número de paquetes, puerto 9.1.

DÍA	NÚMERO DE PAQUETES
Lunes	4 493 362
Martes	6 776 184
Miércoles	5 084 756
Jueves	4 558 871
Viernes	3 916 642

Figura 32. Distribución del número de paquetes, puerto 9.1.

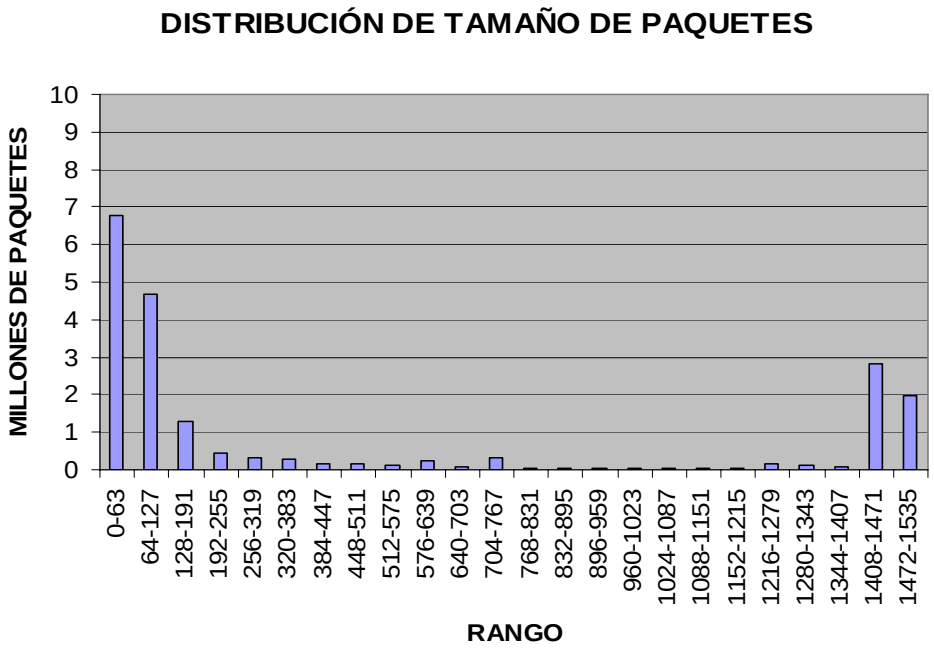


4.4 DISTRIBUCIÓN DEL TAMAÑO DE PAQUETES

La distribución del tamaño de paquetes se presenta en un gráfico de barras mostrando la cantidad de paquetes de cada rango de tamaño de paquetes presentado.

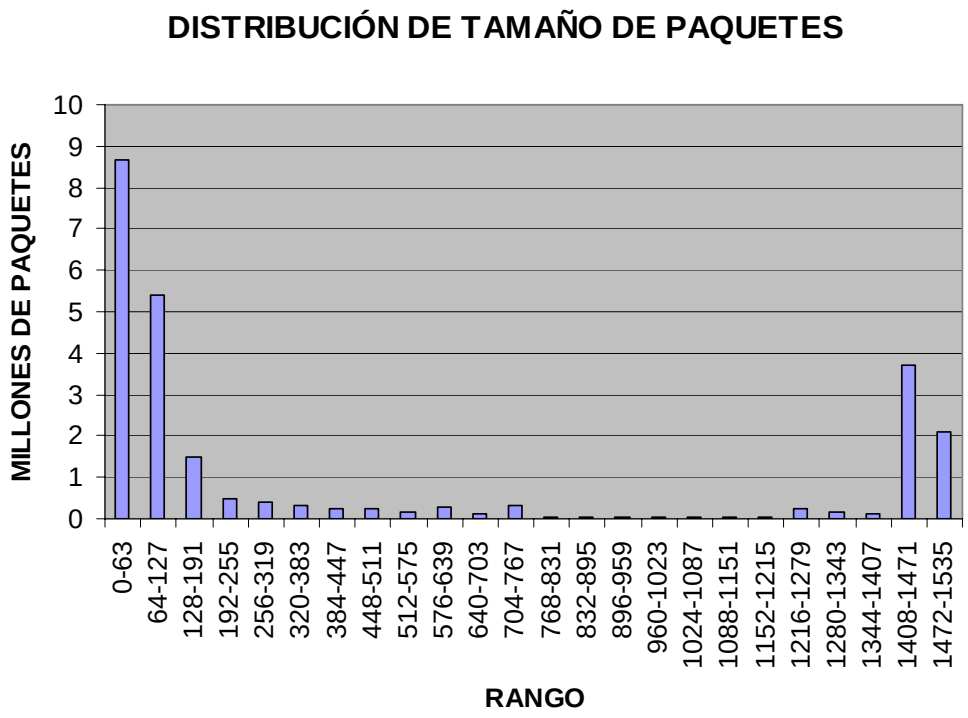
4.4.1 Puerto 9.3 (Civil-Pesados). La distribución del tamaño de paquetes muestra que el tamaño de los paquetes en los registros realizados varía entre 54 bytes y 1514 bytes, mostrando que la mayor cantidad de paquetes se encuentra en un rango que va de los 0 bytes a los 63 bytes, es decir que la mayoría de las aplicaciones que hacen uso de la red utilizan paquetes en éste rango. Otros rangos que presentan una cantidad considerable de paquetes son; el de 64 bytes a 127 bytes, el de 1408 bytes a 1471 bytes y el de 1427 bytes a 1535 bytes. Sin embargo se observa que el mayor tráfico es debido a paquetes de gran tamaño. La distribución del tamaño de paquetes se muestra en la figura 33.

Figura 33. Distribución del tamaño de paquetes, puerto 9.3.



4.4.2 Puerto 9.1 (Civil-Geomática). Se observa que el tráfico durante los días que se realizaron las pruebas está conformado por paquetes que varían en tamaño de los 60 bytes y 1500 bytes. Este parámetro sirve como observación del estado del tráfico de datos de la red de la universidad y sus diversos equipos. Se considera que los resultados obtenidos reflejan una condición adecuada para el tráfico de datos, ya que un tráfico con un tamaño de paquetes muy alto puede verse afectado por una disminución en el ancho de banda del enlace por retransmisiones o pérdidas. La mayor cantidad de paquetes está siendo transmitida en tamaños que van de 0 a 63 bytes y de 64 a 127 bytes, éste rango es usado por la gran mayoría de las aplicaciones que se encuentran en la red. Sin embargo la mayor parte del tráfico del enlace está contenido en el rango que varía de los 1408 bytes a los 1535 bytes, como se muestra en la figura 34.

Figura 34. Distribución de tamaño de paquetes, puerto 9.1.



4.5 DISTRIBUCIÓN DE TRÁFICO UNICAST, BROADCAST Y MULTICAST.

4.5.1 Puerto 9.3 (Civil-Pesados). En la tabla 14 se muestra el ancho de banda utilizado por el tráfico Unicast, Broadcast, Multicast y su respectivo porcentaje respecto a la carga total. Como es de notarse el tráfico Broadcast y Multicast es muy pequeño en comparación del tráfico Unicast, representando menos del 1%, mostrado en las figuras 35 y 36.

Se observa que durante el periodo de medida el tráfico Multicast siempre es mayor que el tráfico Broadcast superándolo casi siempre por el doble del tamaño a excepción del Lunes, en cual éste supera al tráfico Multicast por una pequeña cantidad.

El tráfico Broadcast está formado en su mayoría por el protocolo ARP con un 88%, seguido de IPX SAP con un 7%, BROWSER con un 2% y NBIPX y TIME cada uno con un 1%. Los demás protocolos que con forman el tráfico Broadcast como IPX RIP, NMPI, TFTP, DHCP, NBNS, TCP Y UDP, representan otro 1%.

El pequeño porcentaje presentado por el tráfico Broadcast es debido a que el tamaño de paquetes del protocolo ARP es uno de los más pequeños, 60 bytes, y como ya se mencionó este representa el 88% de este tráfico.

El tráfico Multicast esta formado por protocolos como RIPv1 con un 38%, BROWSER con un 23%, NBNS con un 20%, TIME con un 18% y otros protocolos que representan un 1% como son TCP, WHO, eDonkey, SMB, Portmap, NETLOGON, UDP y Gnutella.

El tráfico Multicast supera en tamaño al tráfico Broadcast debido a que el tamaño de paquetes de los protocolos que conforman el primero típicamente es superior a los del segundo.

Figura 35. Tráfico Multicast, Broadcast y Unicast, puerto 9.3.

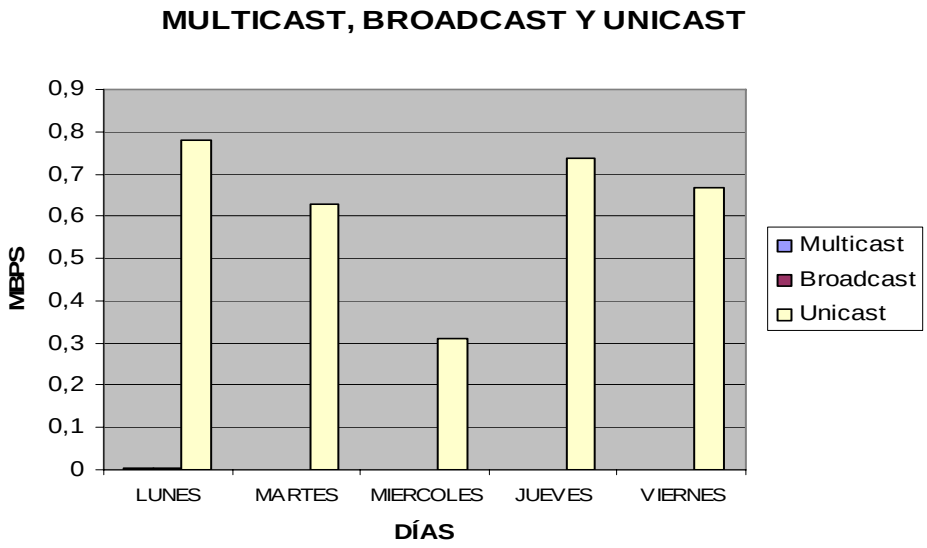


Figura 36. Tráfico Broadcast y Multicast, puerto 9.3

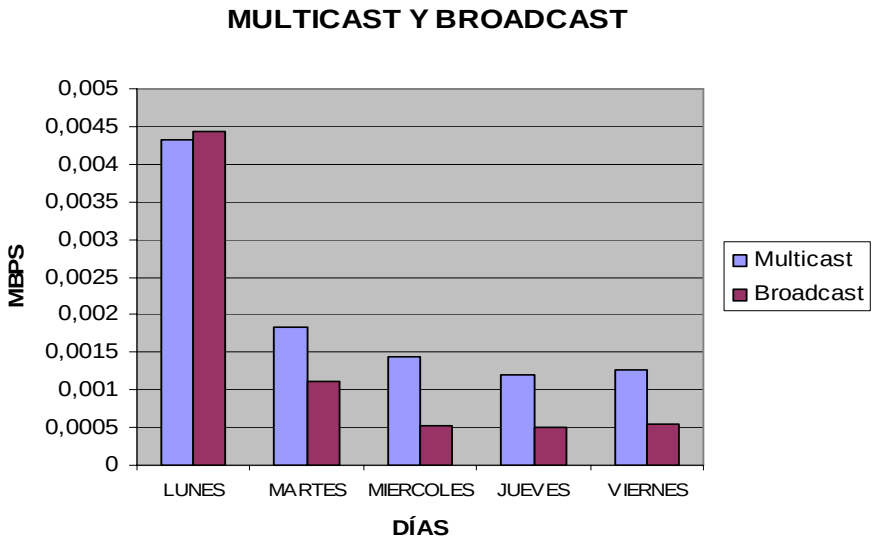


Tabla 14. Cantidad de tráfico Unicast, Broadcast y Multicast, puerto 9.3.

	Broadcast (Mbps)	Multicast (Mbps)	Unicast (Mbps)	% Broadcast	% Multicast	% Unicast
Lunes	0,0044246	0,0043162	0,7799284	0.56	0.547	98.891
Martes	0,0011163	0,0018347	0,6300249	0.17	0.29	99.533
Miércoles	0,0005145	0,001436	0,3105273	0.16	0.46	99.375
Jueves	0,0005002	0,0011964	0,7362188	0.067	0.16	99.77
Viernes	0,0005484	0,0012559	0,6656734	0.08	0.19	99.729

4.5.2 Puerto 9.1 (Civil-Geomática). La distribución de tráfico Multicast, Broadcast y Unicast ilustre el volumen en Mbps sobre el enlace, y el porcentaje de éste con respecto al tráfico total. Se ha evaluado este resultado para los diferentes días que comprenden la toma de datos.

Se puede observar que el porcentaje de tráfico Multicast es aproximadamente un 1% del tráfico total y se mantiene en este margen durante los diferentes días, mientras que el tráfico Broadcast es aproximadamente 0.5 por ciento del tráfico total, como se muestra en la tabla 15.

El porcentaje del tráfico Broadcast y Multicast no supera el 1% del tráfico total en los diferentes días. Se puede considerar un porcentaje aceptable si se tiene en cuenta que este tráfico es generado por los dispositivos de red encargados del enrutamiento de los paquetes como los switches y los servidores.

El tráfico Broadcast está compuesto principalmente de paquetes transmitidos usando protocolos como ARP, UDP, BROWSER, DHCP, NETLOGON y otros protocolos usados por algunos dispositivos de la red. El mayor porcentaje de este tráfico corresponde al protocolo ARP, cerca de un 94 %, y el resto a los

diferentes protocolos que hacen uso del trafico broadcast como IPX SAP, IPX RIP y TIME entre otros.

El tráfico Multicast está compuesto principalmente por protocolos que hacen uso de la difusión a un grupo de equipos como RIP, TIME, BROWSER , los cuales representan aproximadamente el 70% de este tráfico y el resto de este está formado por protocolos como TSP, NBNS, UPD, entre otros.

Tabla 15. Cantidad de tráfico Broadcast y Multicast, puerto 9.1.

	Broadcast (Mbps)	**Multicast (Mbps)**	**Unicast (Mbps)**	**% Broadcast**	**% Multicast**	**% Unicast**
Lunes	0,00130	0,00249	0,48516	0,266	0,510	99,2241
Martes	0,00039	0,00102	0,82524	0,047	0,124	99,8282
Miércoles	0,00039	0,00113	0,56261	0,070	0,201	99,7288
Jueves	0,00042	0,00116	0,52875	0,080	0,219	99,7006
Viernes	0,00043	0,00116	0,35701	0,123	0,324	99,5531

Se puede observar que el tráfico Multicast y Broadcast tienen un comportamiento similar durante los diferentes días en que se tomaron los datos. Se observa que el total de tráfico multicast es casi el doble del total del trafico broadcast durante los diferentes días, en las figuras 37 y 38 se muestra el tráfico Unicast, Multicast y Broadcast total diario transmitido durante los diferentes días.

Figura 37. Tráfico Unicast, Multicast y Broadcast puerto9.1

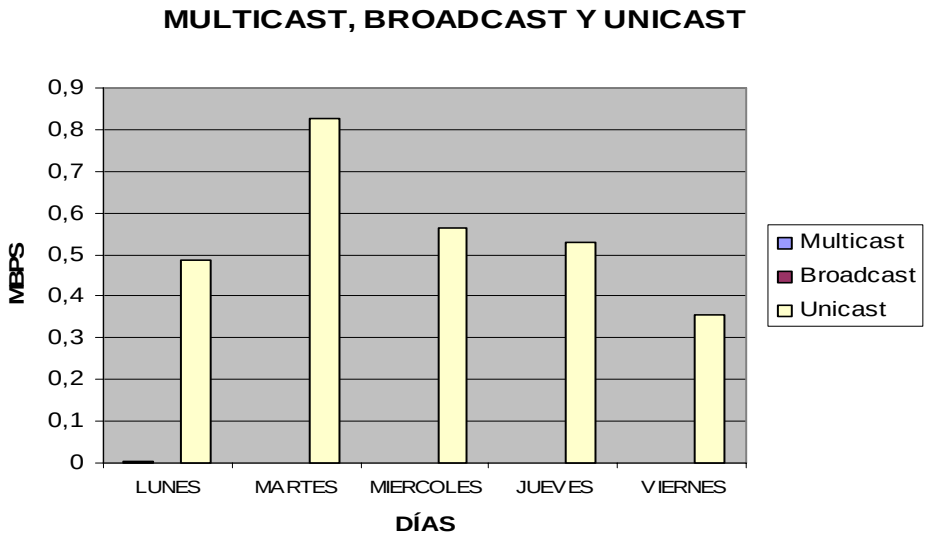
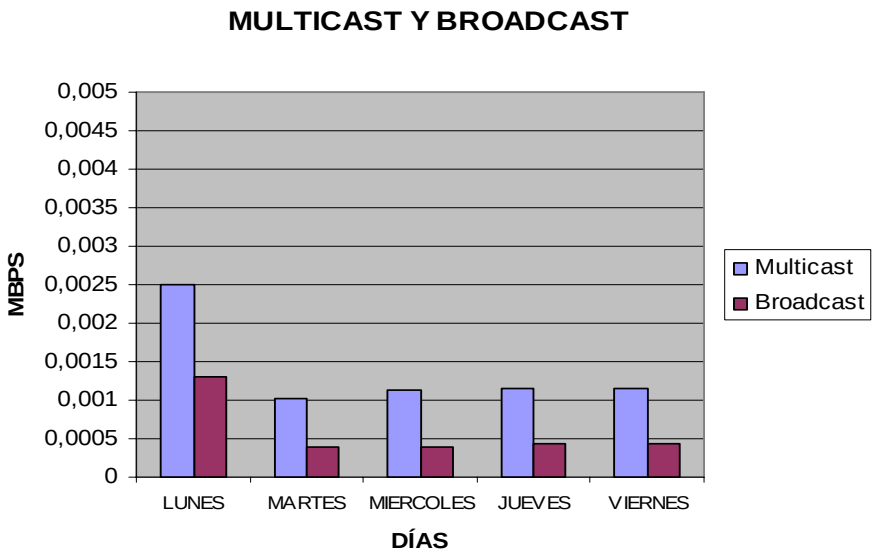


Figura 38. Tráfico Broadcast y Multicast, puerto 9.1.



4.6 DISTRIBUCIÓN DE ORÍGENES Y DESTINOS.

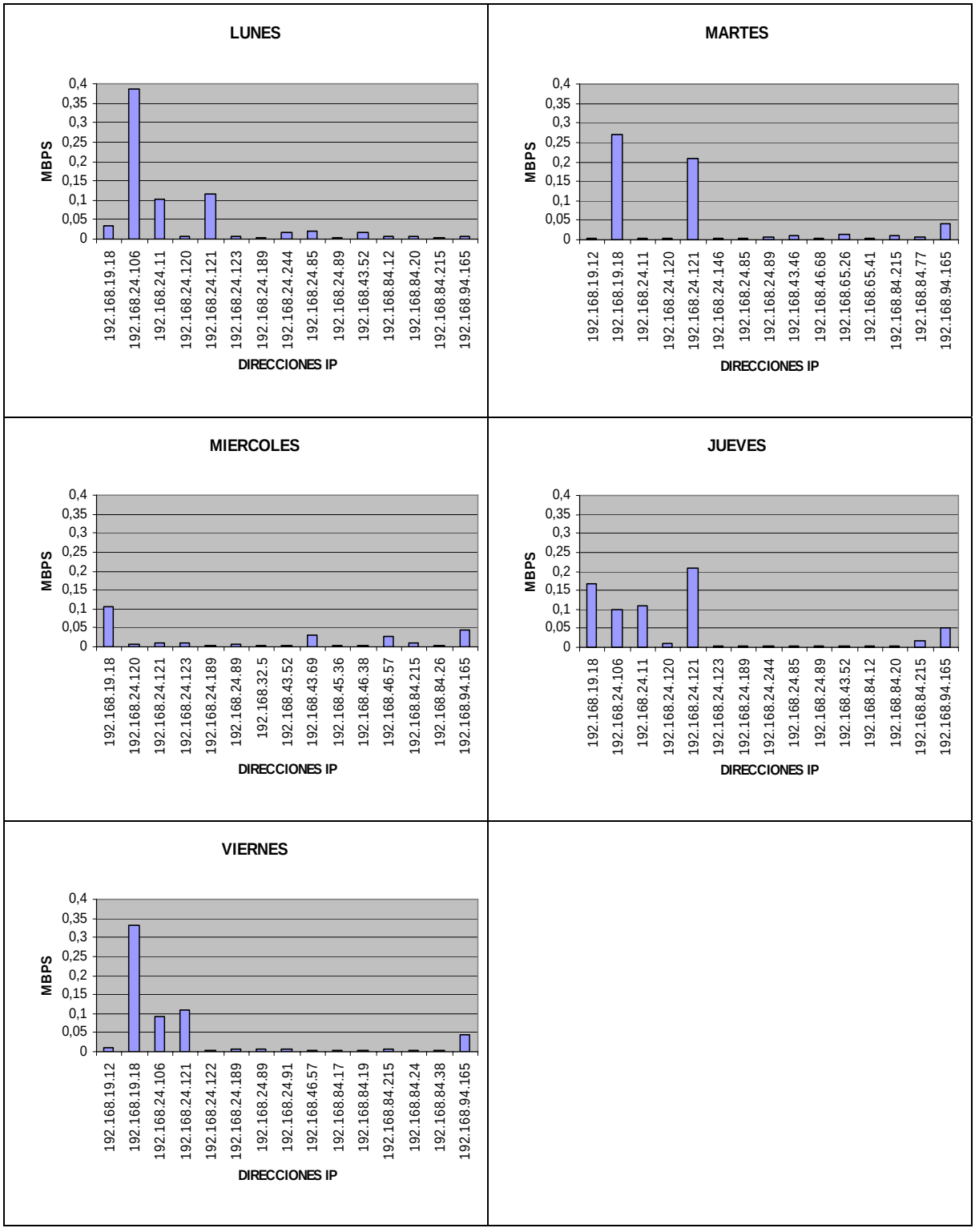
La distribución de orígenes y destinos muestra la cantidad de Mbps transmitidos durante todo el periodo de medida por cada estación presente en el enlace de datos.

4.6.1 Puerto 9.3 (Civil-Pesados). Se observa que la dirección que más tráfico genera y por ende más ancho de banda utiliza es la 192.168.19.18 que corresponde al servidor quetzal.uis.edu.co, quien sirve de Gateway para unos 50 equipos, también se encuentra otro servidor, el 192.168.19.12 cuyo nombre de dominio es cormoran.uis.edu.co, pero que presenta un tráfico bajo. También se determinó que en el puerto 9.3 correspondiente a Civil-Pesados existen 2 subredes. La subred con dirección IP 192.168.24.0 cuenta con 29 equipos o hosts y la subred con dirección 192.168.84.0 cuenta con 37 equipos o hosts.

Observando las gráficas de una manera general se puede establecer que los servidores mencionados anteriormente presentan un tráfico alto como es predecible, debido a los servicios de puerta de enlace instalados en ellos. Los hosts muestran un tráfico constante durante el periodo de medición, pero se tiene el caso de algunos de ellos en los que el tráfico que generan es demasiado grande presentando picos bastante elevados en comparación con los demás; tales hosts son el 192.168.24.121 y el 192.168.94.165, figura 39.

Haciendo un análisis de los protocolos que usaban estos hosts se llegó a la conclusión de que presentaban un exceso de uso de protocolos como el eDonkey en el host 192.168.94.165 y de TCP en el host 192.168.24.121 lo que nos indica el gran uso de programas P2P por parte de estos.

Figura 39. Distribución de Orígenes, puerto 9.3.



En la figura 40 se muestra la distribución de orígenes con los hosts que presentan un alto tráfico y los protocolos asociados con éste.

Figura 40. Distribución de Orígenes con protocolos, puerto 9.3.

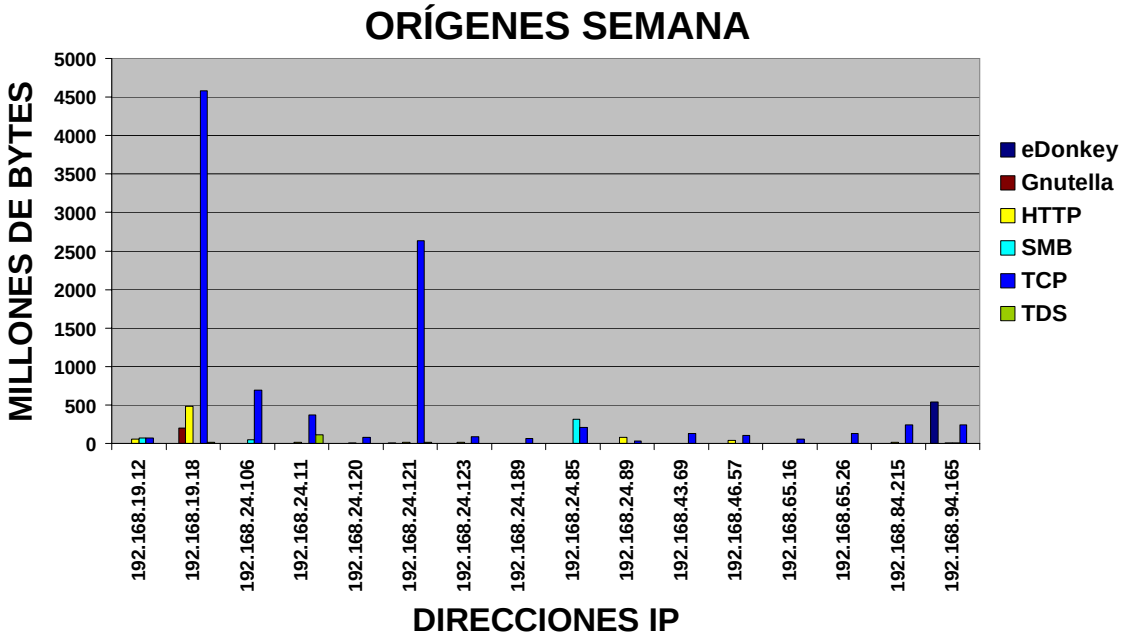
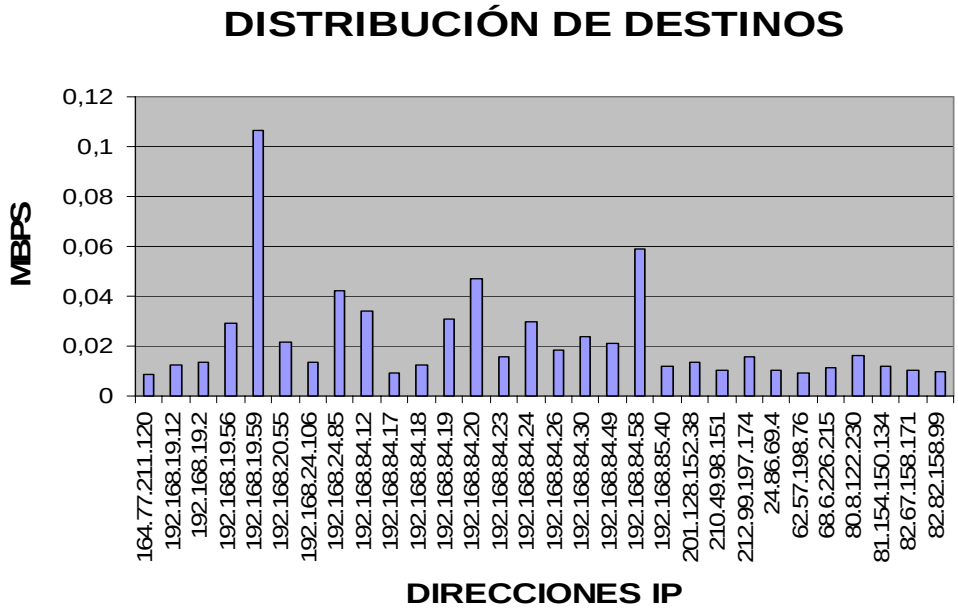


Figura 41. Distribución de Destinos durante la semana, puerto 9.3.



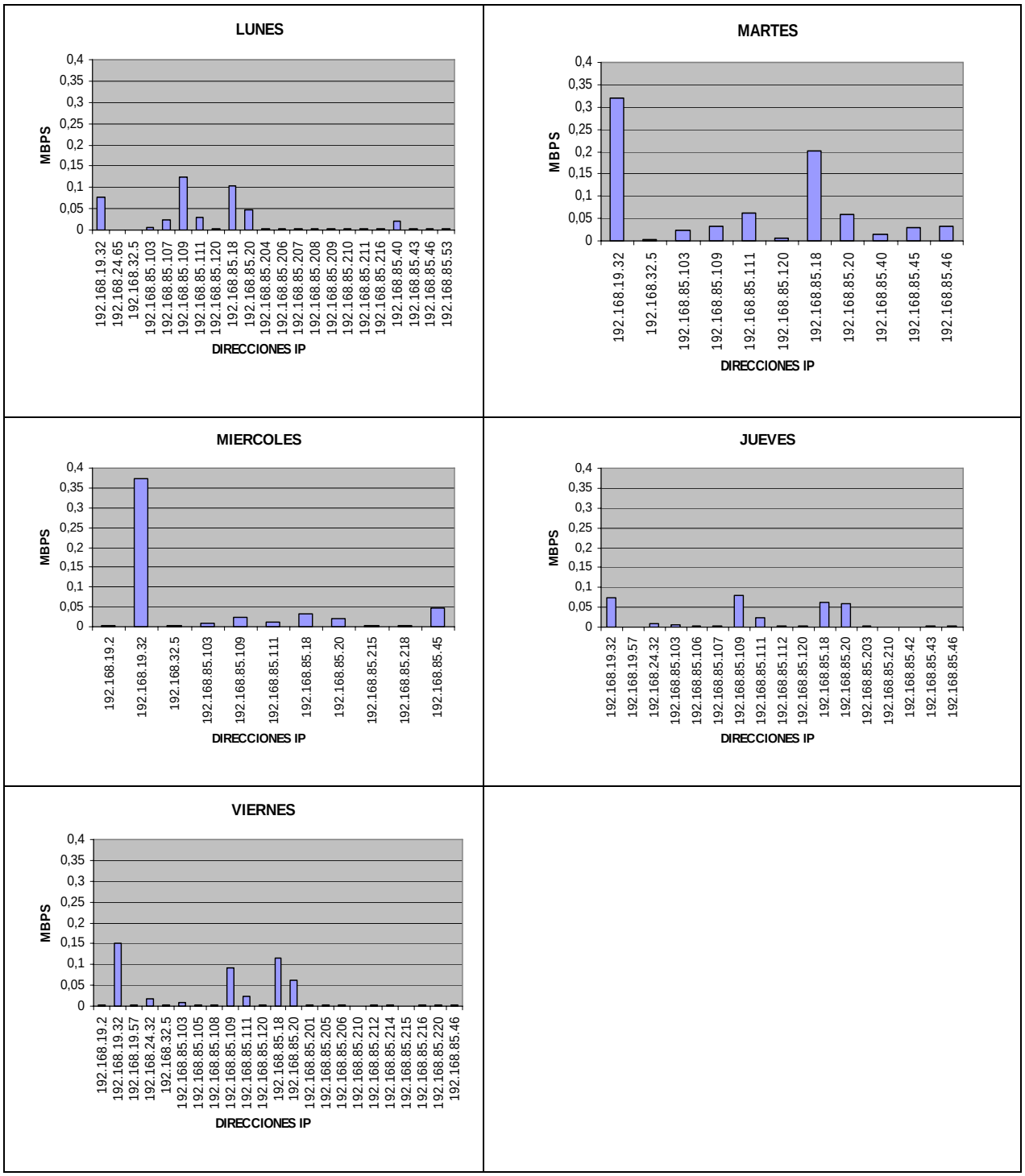
La distribución de destinos muestra que el tráfico de destino es muy amplio y por lo tanto es difícil visualizarlo por completo. Debido a esto se seleccionó una cantidad determinada de destinos que representaban un gran tráfico de datos.

Se encontró que las direcciones que representaban los destinos más frecuentados o con más tráfico son servidores y hosts que hacen parte del enlace de la Universidad, pero también se encontraron direcciones de los servicios de correo gratuito como Yahoo, Latinmail y Hotmail, así como direcciones de hosts o servidores que seguramente se consultan para descargas cualquier tipo de archivo. Esto se muestra en la figura 41.

4.6.2 Puerto 9.1 (Civil-Geomática). La distribución de orígenes y destinos muestra la cantidad de equipos presentes en el enlace que consumen la mayor cantidad del ancho de banda del enlace, en total se cuentan con algo más de 100 equipos conectados al puerto, los cuales están usando diferentes subredes, entre la cuales se destacan la 192.168.85.0 y la 192.168.24.0. En estas subredes se tienen 46 y 13 equipos respectivamente, El mayor ancho de banda lo utilizan 4 equipos, los cuales alcanzan a utilizar cerca del 80% del ancho de banda, estos equipos están conformados por hosts y servidores.

En la figura 42 se observa la cantidad de tráfico transmitido por las diferentes estaciones, mostrando las estaciones que consumen el mayor ancho de banda del enlace.

Figura 42. Distribución de Orígenes, puerto 9.1.



Se puede observar que el mayor tráfico que se presenta de consultas de páginas Web en este puerto pasa a través del servidor con dirección IP 192.168.19.32 el cual maneja casi en su totalidad el trafico de SMB, HTTP Y X11. Los equipos de este puerto que consumen un ancho de banda considerable usan servicios que manejan protocolos como eDonkey, TCP, UDP, MSNMS. Se observa que el mayor tráfico de protocolos como eDonkey, protocolo con un porcentaje alto de participación en este puerto, está presente en casi su totalidad en tres estaciones y los demás protocolos como TCP, UDP, DNS y MSNMS están siendo consumidos por las demás estaciones. Este comportamiento se observa durante los diferentes días que se realizó la toma de datos. En la figura 43 se observa el comportamiento de las direcciones orígenes con respecto a los protocolos más usados, mostrando las estaciones con el mayor porcentaje de tráfico en el puerto durante toda la semana.

Figura 43. Distribución de Orígenes con protocolos durante la semana, puerto 9.1.

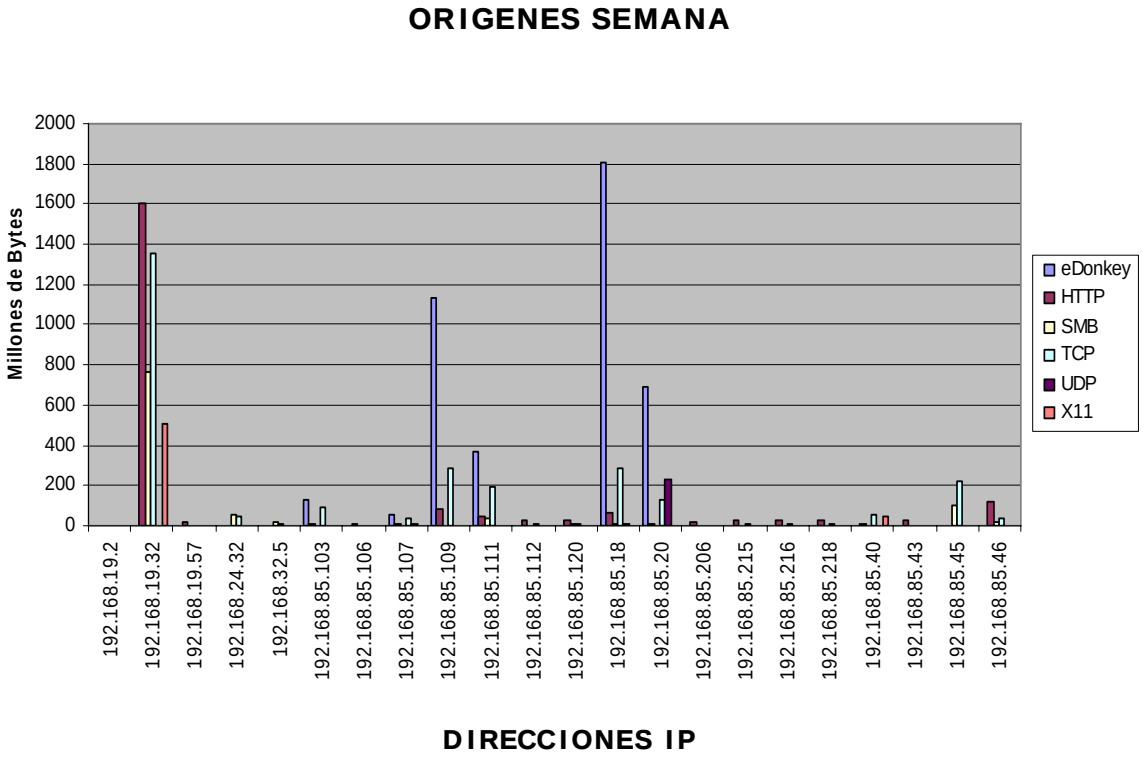
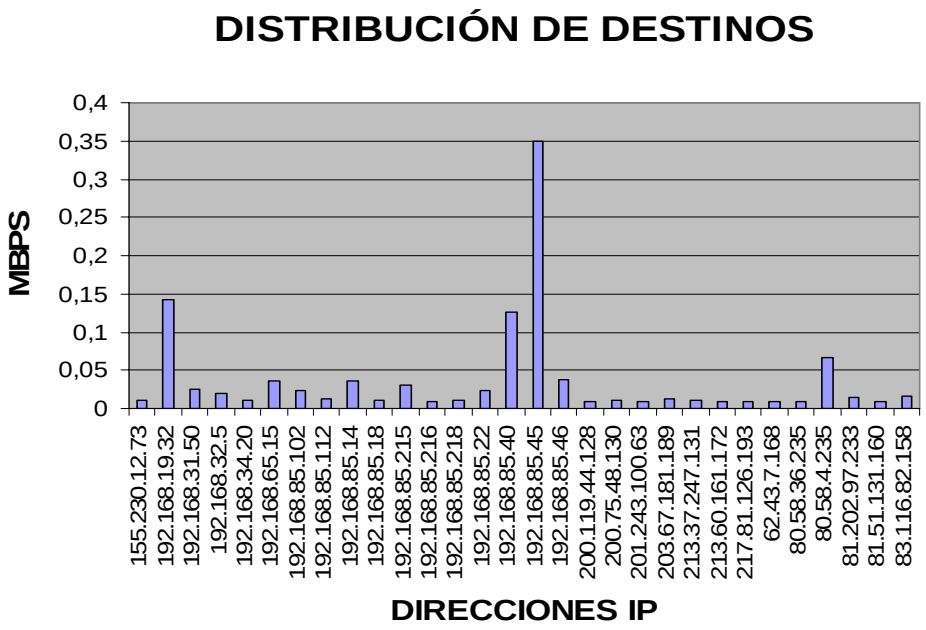


Figura 44. Distribución de Destinos durante la semana, puerto 9.1.



En la distribución de destinos se observa una gran cantidad de hosts que son destinos y por consiguiente se muestran los más significativas de ellas, entre estos destinos se encuentra que hay hosts que están dentro de la red institucional presentando un tráfico considerable. Además se encuentran hosts, servidores http que son parte de Internet y que son muy frecuentadas como por ejemplo los servidores de los servicios de correo gratuito como Yahoo, Latinmail y Hotmail. Se encuentran más de 90000 destinos, lo cual hace difícil la identificación de estos y su respectivo porcentaje de tráfico en la red. Algunos de estos destinos se muestran en la figura 44.

5. CONCLUSIONES

Este documento presenta una metodología para la caracterización del tráfico de datos de redes de área local LAN, basados en la captura del tráfico de datos que se presenta en dos puertos del backbone de la Universidad Industrial de Santander. La caracterización del tráfico se desarrolla con base en parámetros como la distribución de protocolos, la distribución de la carga de tráfico, la distribución del número de paquetes, la distribución del tamaño promedio de paquetes, el tráfico Broadcast y Multicast, la distribución de orígenes y destinos y el ancho de banda, los cuales nos proporcionan información detallada sobre el comportamiento y estado de las redes LAN.

Para la realización de los registros de datos se seleccionó, entre un conjunto de tarjetas de red Gigabit Ethernet de fibra óptica que cumplían con las especificaciones técnicas necesarias, la tarjeta de red Intel® PRO/1000 Server Adapter, ya que esta era una de las que mejor se ajustaba a las especificaciones técnicas y económicas del proyecto.

Para la implementación de la metodología se realizaron una serie de pruebas preliminares que sirvieron como base para poder determinar los puertos a caracterizar y realizar de la mejor manera la captura de los datos. Al implementar esta metodología se realizaron una serie de toma de datos sobre la red institucional siendo esto la base de este trabajo. Los resultados obtenidos de estas jornadas de medición se muestran de una manera clara y sencilla para poder observar el comportamiento de los diferentes parámetros que caracterizan el tráfico de una red LAN y así a su vez determinar la validez de esta metodología.

Con base en información sobre estudios realizados anteriormente y conceptos sobre redes de área local esta metodología se fundamenta en los principales parámetros que dejan ver el comportamiento de estas redes.

Se hace un énfasis en la distribución de la carga de tráfico y la distribución de protocolos ya que estos son los parámetros más significativos que nos proporcionan la mayor información para verificar el estado de la red.

De un conjunto de herramientas software disponibles para análisis de tráfico de datos se seleccionó Ethereal, ya que ésta proporcionaba la información necesaria para obtener los parámetros de tráfico definidos anteriormente y además es de libre distribución.

A partir de la toma de datos realizados en dos de los principales enlaces del backbone de la Universidad y la metodología propuesta para su ordenamiento, caracterización y análisis se llegó a las siguientes conclusiones:

- Se determinó que el tráfico de datos en los puertos seleccionados presenta una concentración alta de uso de protocolos como TCP, eDonkey, HTTP, SMB y Gnutella, consumiendo un gran ancho de banda, mientras protocolos como TDS, MSNMS, UDP, DNS, X11, NBSS presentan un consumo de ancho de banda muy bajo. A partir del uso excesivo de estos protocolos se puede determinar que se presenta un alto uso de programas P2P cuya finalidad es compartir y descargar archivos como música, videos, software, etc., el uso de estos programas produce un consumo incontrolable del ancho de banda y el fomento de la piratería.
- Se determinó que la carga de tráfico en el puerto 9.3 correspondiente a Civil-Pesados es ligeramente mayor que en el puerto 9.1 correspondiente a Civil-Geomatica, corroborando la información

suministrada por el administrador de la red institucional, en la que se establecía que el tráfico presentado por el puerto 9.3 era uno de los más pesados de la universidad.

- Se observa que la distribución de la carga de tráfico presenta un comportamiento diferente a lo largo del día en los dos puertos seleccionados del backbone, ya que en uno de estos se observa un comportamiento típico de las actividades de una institución y el otro un comportamiento atípico a este, pero estas conclusiones no son definitivas debido a que el tráfico de datos en la universidad y en cualquier red presenta alta variabilidad.
- La carga de tráfico de datos en la universidad puede verse afectada por múltiples factores como son el cese de actividades, la temporada de matrículas, fallas en los equipos de la red como switches y routers, entre otros. El tráfico en los enlaces puede variar por el simple hecho que las condiciones que se presentan durante un tiempo pueden ser diferentes en otro momento. Esto conlleva a concluir que la caracterización del tráfico de una red de datos debe hacerse en un periodo de tiempo en que se presente la mayor normalidad posible en su funcionamiento.
- Se concluyó que la distribución de tamaño de paquetes se mantiene en un rango determinado durante el periodo de medición, y se encuentra una similitud en el comportamiento de los dos puertos. Además se observa que el tráfico casi en su totalidad es enviado en paquetes cuyo tamaño varía entre los 60 y los 127 bytes y entre los 1408 y los 1535 bytes.
- El tráfico multicast y broadcast presenta un porcentaje muy pequeño en comparación con el tráfico unicast, representando este tráfico el 1 % de la carga total. El tráfico broadcast casi siempre es la mitad del tráfico multicast, debido a que el tráfico broadcast está conformado casi en su totalidad por el protocolo ARP el cual presenta uno de los tamaños de paquete más pequeños.

- En la distribución de orígenes y destinos se observa que el mayor ancho de banda es utilizado por 5 estaciones las cuales hacen un alto uso de programas P2P. Esta conclusión se obtiene a partir de un minucioso análisis de los protocolos que más utilizan estas estaciones, como lo son eDonkey, TCP y Gnutella, responsables de los llamados cuellos de botella.

Las herramientas utilizadas para el desarrollo de esta metodología como Ethereal y Microsoft Access presentaron un desempeño óptimo, ya que con ellas se pudieron realizar los registros y la organización de los datos de una manera relativamente rápida y sencilla. Esto demuestra que la metodología propuesta es viable ya que en poco tiempo se puede obtener una buena caracterización de los enlaces y además puede implementarse en una red en la que no se posean los medios económicos para adquirir un software especializado en análisis de tráfico.

La caracterización del tráfico de datos de una red LAN nos permite descubrir el comportamiento, anomalías, fallas, cuellos de botella, mala configuración de los equipos y recursos que están presentes en ella para así poder dar un diagnóstico y posibles soluciones a todos estos problemas y determinar su capacidad real.

6. RECOMENDACIONES

La caracterización y análisis de tráfico son estudios que cada día se hacen más frecuentes en las redes de datos debido a la necesidad de solucionar problemas en éstas provenientes del aumento de recursos y aplicaciones que demandan un mayor ancho de banda y generan congestiones de tráfico representados en cuellos de botella. Algunas recomendaciones para llevar acabo estos estudios de una manera más rápida y satisfactoria se presentan a continuación:

- Antes de realizar la toma de datos es indispensable consultar con el encargado de la red a caracterizarse, sobre la disponibilidad de un puerto en el switch central de esta red que posea las mismas especificaciones técnicas que la tarjeta de red a utilizarse para evitar pérdida de tiempo.
- Dependiendo del periodo de medición que se establezca, trabajar con el menor número de archivos de registro que se pueda, para simplificar o disminuir la tarea tediosa de exportar estos archivos a formato de Texto plano.
- Buscar una alternativa que permita hacer el registro de los datos de varios puertos a la vez, ya que esta metodología plantea la captura de datos de un solo puerto a la vez, para así reducir el tiempo que se necesita para realizar la toma de datos.
- Para evitar desbordamiento en el equipo por el tamaño de los archivos generados se podría limitar el registro a las cabeceras de los paquetes sin almacenar el contenido de estos para así poder realizar la toma de datos durante periodos de tiempo más largos.
- Es necesario tener en cuenta que se debe realizar las tomas de datos en los días en que la red a caracterizarse presente normalidad en su funcionamiento, para que esta caracterización represente el tráfico real.

REFERENCIAS

[1] ARTURO AZCORRA SALOÑA. "Uso del Internet en la universidad española". Univ. Carlos III de Madrid, II Congreso Internacional de la Lengua Valladolid, 16-19 Octubre de 2001. Tomado de http://cvc.cervantes.es/obref/congresos/valladolid/ponencias/nuevas_fronteras_del_espanol/3_la_universidad_e_internet/azcorra.pdf

[2] ABEL NAVARRO, JORDI DOMINGO. Analizador en tiempo real de calidad de servicio en redes IP. Centro de Comunicaciones Avanzadas de Banda Ancha – UPC, Diciembre 2003 - Enero 2004. Tomado de http://www.rediris.es/rediris/boletin/66-67/ponencia7.pdf

[3] FERMÍN GALÁN, RICARDO ROMERAL. MIRA: Plataforma de monitorización, Agora Systems, Área de Ingeniería Telemática, Universidad Carlos III de Madrid, oct-2003, tomado de http://greco.dit.upm.es/~abgarcia/publications/2003TELECOM.pdf

BIBLIOGRAFÍA

L. AGUILAR SINDES. Midiendo redes, Aguilar & Asociados, Buenos Aires, 2002.

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

ANDREW TANENBAUM, Redes de Computadoras, PEARSON, PRENTICE HALL, Tercera edición, 1997.

ILKA MILOUCHEVA, Traffic Measurement and Monitoring Roadmap, Next Generation Network Initiative, 2002

STALLING, William. COMUNICACIONES Y REDES DE COMPUTADORES, Sexta Edición, Pearson Educación S.A: 2000

M. ÁLVAREZ CAMPANA, A. AZCORRA, J. BERROCAL, J. DOMINGO PASCUAL, D. LARRABEITI, X. MARTÍNEZ, J. I. MORENO, J. R. PÉREZ Y J. SOLÉ PARETA. "CASTBA: Medidas de tráfico sobre la Red Académica Española de Banda Ancha", Telecom I+D, Madrid, Octubre1998.

P. J. LIZCANO, A. AZCORRA, J. SOLÉ PARETA Y J. DOMINGO PASCUAL. "MEHARI: A System for Analysing the Use of the Internet Services". Computer Networks and ISDN Systems. ISSN: 0169-7552 31 (10), Noviembre 1999.

"RedIRIS, red académica y de investigación nacional". Tomado el 10 de Septiembre de 2003 de
http://www.rediris.esG

ANEXO A. INSTALACIÓN DE LA TARJETA DE RED Y DESCRIPCIÓN DEL SOFTWARE DE ANÁLISIS DE TRÁFICO

En este anexo se mostrará la forma en como se realizó la instalación de la tarjeta de fibra óptica Gigabit Ethernet utilizada para la toma de datos y una clara descripción de la herramienta software utilizada.

INSTALACIÓN DE LA TARJETA DE FIBRA ÓPTICA GIGABIT ETHERNET

La tarjeta de red es de marca Intel. Se conecta a un slot PCI del PC y para su instalación y prueba se tiene que descargar de la página de Internet de su constructor, un software llamado Intel(R)PROSet Wired, el cual esta diseñado para trabajar en cualquier sistema operativo Windows.

La instalación de esta tarjeta se realizó de la siguiente forma: se conectó al PC por medio de uno de sus slots PCI, después se prosiguió a conectar los cables de red (patch cord), después de que la tarjeta está instalada físicamente se continuó con la instalación de los drivers.

Los drivers de esta tarjeta se descargan de la página de su constructor, www.intel.com, los cuales vienen con una serie de utilidades y plug-ins, después de la instalación del software se continúa con un test que contiene el mismo para como su nombre lo indica probar o testear la tarjeta y así comprobar su correcta instalación y posterior funcionamiento.

En las figuras 1 y 2 se pueden observar las ventanas que nos permiten realizar el test de la tarjeta de Red.

Figura 1. Ventana principal del software Intel(R) PROSet Wired.

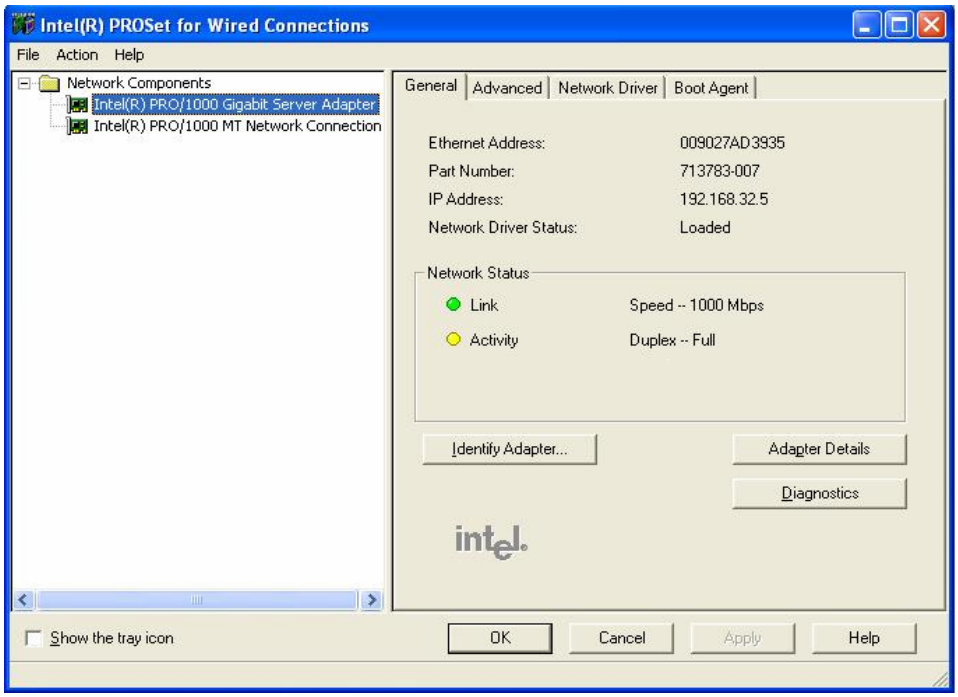
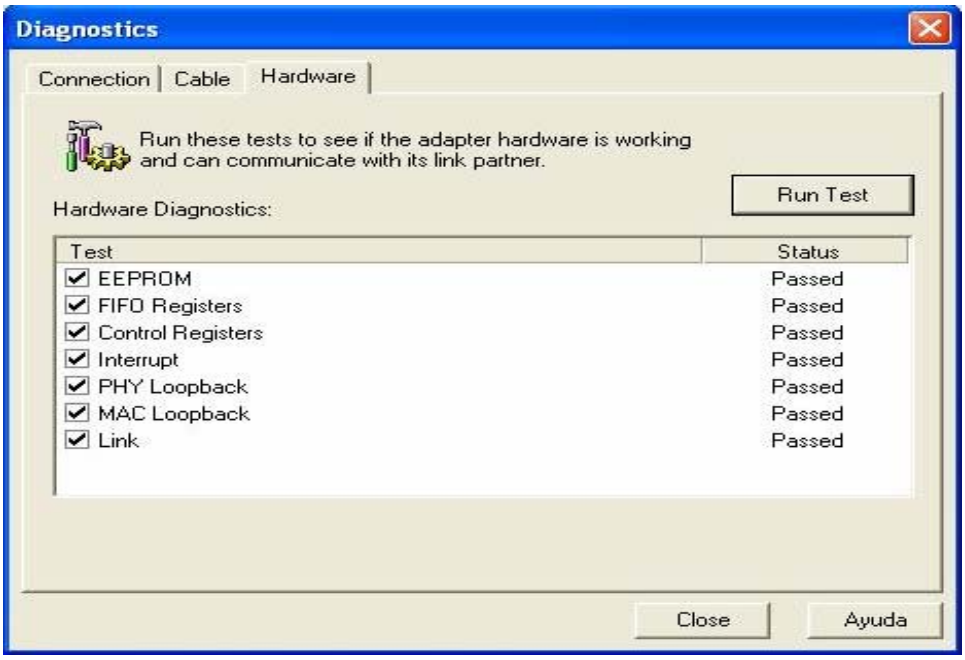


Figura 2. Ventana de diagnóstico



ETHEREAL

Ethereal es un analizador de protocolos de red. Le permite a usted observar interactivamente los datos de paquetes de una red en funcionamiento o los archivos de una captura previamente almacenada. El formato de captura original de Ethereal es el formato **libpcap**, el cual es también el formato usado por tcpdump y varias otras herramientas.

Ethereal puede leer e importar los formatos de archivo siguientes:

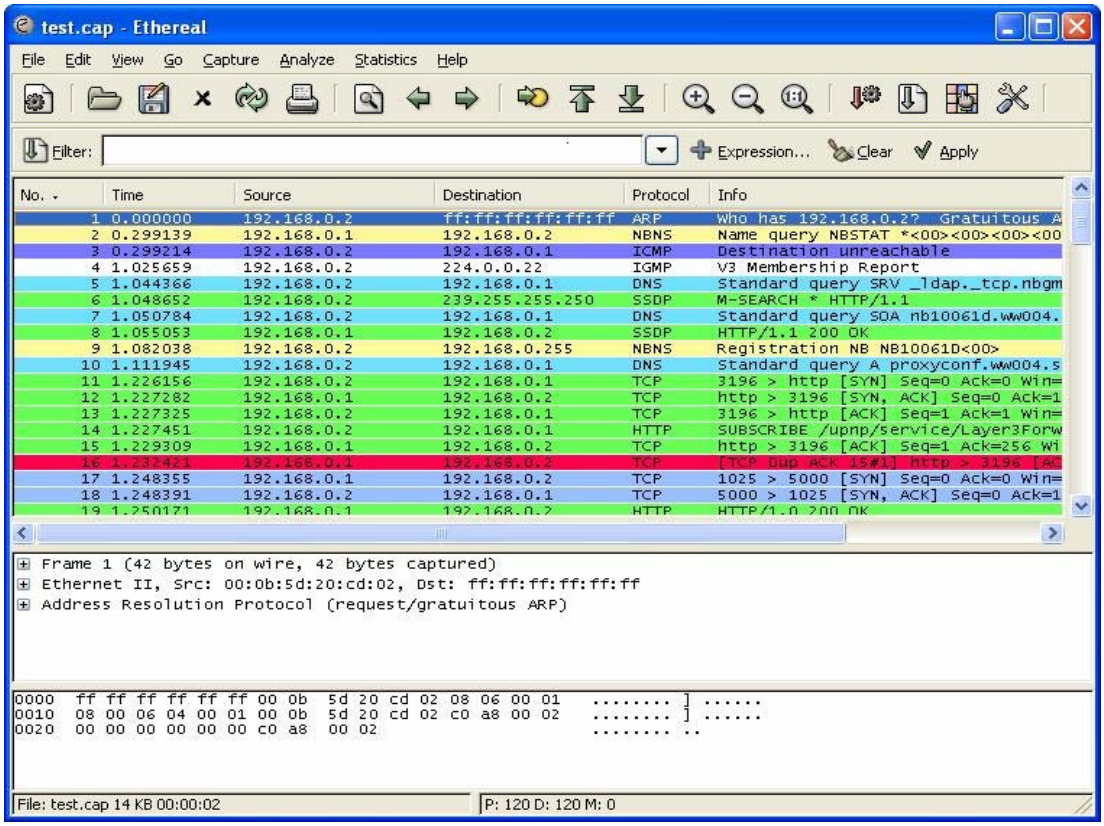
- Libpcap, tcpdump y varias otras herramientas que usan el formato de captura tcpdump.
- Snoop y atmsnoop.
- Capturas de Novell LANalyzer.
- Capturas de Microsoft Network Monitor.
- Capturas de Cinco Networks NetXRay.
- Capturas de Network Associates Windows-based Sniffer.
- Capturas de RADCOM's WAN/LAN analyzer.
- Capturas de Network Instruments Observer version 9.
- Capturas de Visual Networks' Visual UpTime traffic.
- Capturas de Endace Measurement Systems' ERF format.
- Capturas de AIX's iptrace.
- Capturas de Network General/Network Associates DOS-based Sniffer (compressed or uncompressed).
- Capturas de Endace Measurement Systems' ERF format.

No hay necesidad de decirle a Ethereal que tipo de archivo se está leyendo; el determina el tipo de archivo por si mismo, como también tiene la capacidad de leer cualquier tipo de archivos así se encuentren comprimidos.

Como otros analizadores de protocolos, Ethereal muestra en su ventana principal tres vistas de un paquete. Muestra una línea sumaria y describe

brevemente lo que es el paquete. El paquete detallado se muestra y le permite al usuario examinar los protocolos o los campos en los que este mismo se encuentra interesado, figura 3.

Figura 3. Ventana principal de Ethereal.



Además, Ethereal tiene unas características que lo hacen único. Este puede agrupar todos los paquetes en una conversación de TCP y puede mostrarle los datos ASCII en esa conversación. Los filtros que posee Ethereal son muy poderosos, y además el usuario tiene la facilidad de crear sus propios filtros de una manera fácil y rápida.

ANEXO B. ESPECIFICACIONES DE LOS EQUIPOS UTILIZADOS

A continuación se listan las especificaciones y referencias de los equipos utilizados en la red de área local de la Universidad Industrial de Santander para la caracterización del tráfico de esta.

1. 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 1 se muestran las especificaciones técnicas de la tarjeta de red Gigabit Ethernet.

Tabla 1. 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**

2. SWITCH CAJUN P880

El switch utilizado en la caracterización del tráfico de 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 vídeo 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™ Ready para aplicaciones de voz datos y video.
- Calidad de servicios (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 2.

Tabla 2. 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

3. SWITCH CAJUN P550

Se utilizó un switch Cajun P550 marca Lucent para realizar las pruebas del adaptador de red Gigabit Ethernet, sus características principales son las siguientes:

- Backplane capacity of 45.76 Gbps.
- Switching throughput capacity of 22.88 Gbps.
- Up to 33,000,000 pps Layer 2 switching.
- Up to 18,000,000 pps Layer 3 routing in the routing switch.
- Layer 2 and Multilayer (Layer2/Layer 3) modules.
- Fault tolerant fans, power, switch, links, management.
- Unique Lucent OpenTrunk VLAN interoperability.
- Class of Service/Quality of Service/RSVP support.

En la tabla 3 se muestran otras especificaciones del Switch Cajun P550.

Tabla 3. Lucent Cajun P550: KEY FEATURES.

Lucent Cajun P550: KEY FEATURES	
Switch software tested	1.0.17
Max. N° Gigabit Ethernet ports	24
10/100 support	20-port 10/100module replaces 4-port Gig. Mod.; 10/100ports
Integral 10/100 port for management	Yes
Configuration flexibility/modularity	7-slot chasis; 1 control slot; 6 slots for modules
1000Base LX Support	Yes
MAV address table capacity	24.000/switch
Gigabit Ethernet trunking or hot-stanby redundancy of Gig Enet links	Trunking up to 8 ports/groups; switchover in under one second
Auto-negotiation on Gigabit ports	No; off by default
Pause frame flow control	Obeys and issues on Gigabit ports
Port mirroring (roving/port monitor)	Yes
Type of VLANs supported	Port- and/or MAC-based
Spanning tree support per VLAN	Yes
Per-port broadcast/multicast control/thresholds	Planned
Priorization queues, Quality Of Service (QoS)	Maps 802.1p levels into 2 per-port queues
Filtering per port, user-definable	Yes; by MAC address; additional filtering with Layer 3
Layer 3 (routing) support	IP,IPX; requires different hardware modules
Fault tolerance redundancy	Power supply; load balancing
MAC-level security	Address locking
Windows/Web-based management interfaces, applications	Windows NT app. ($2,450); Web interface
Cost of switch, as tested (list price)	$57,650(L2 only)

4. SWITCH CAJUN P333R

Se utilizó un switch P333R para hacer pruebas del adaptador de red Gigabit Ethernet, sus características principales son las siguientes:

Specifications

Interfaces

24 x 10/100BASE-TX ports with RJ connectors

Expansion slot for X330 modules

Stacking slot

RS-232 for terminal setup/modem and PPP

Standards Supported

IEEE 802.3x	Flow control on all ports
IEEE 802.1Q/p	VLAN Tagging and priority compatible on all ports
IEEE 802.1D	Spanning Tree protocol
IEEE 802.3z	Gigabit Ethernet ports
IETF	MIB-II, Bridge MIB, RMON, SMON, IP Forward MIB
Routing:	RIP 1, RIP 2, OSPF, VRRP, ARP, ICMP and DHCP/BOOTP Relay

Physical Characteristics

Dimensions (h, w, d):	2U (3.5"/88 mm) x 19" (482.6 mm) x 17.7" (450 mm)

Environmental Conditions

Operating Temp:	23 to 122°F (–5 to 50°C)
Humidity:	5% to 95% non-condensing

Power Consumption

Power Entry (AC):	100-240 VAC, 2A, 50/60 Hz
Power Consumption:	150W max.

Agency Approval

EMC Emission:	US—FCC Part 15, Subpart B, Class A Europe—EN55022 class A and EN61000-3-2 Japan—VCCI-A
Immunity:	Approved according to EN55024 and EN61000-3-3
Safety:	UL for US approved according to UL1950 Std. C-UL (UL for Canada) approved according to C22.2 No.950 Std. CE for Europe approved according to EN 60950 Std
CLEI CODE	According to Telcordia (Bellcore) KS-22022 standard
NEBS Level 3	
AC version:	With optional brackets
DC version:	Certified

5. SWITCH CAJUN P330

Se utilizó un switch P330 para hacer pruebas del adaptador de red Gigabit Ethernet, sus características principales son las siguientes:

Specifications

Power Requirements

Output voltage:	5.5 V
Max. output current:	4 x 27A @ 5.5V
Max. output power:	4 x 150W @ 5.5V
Input voltage range	
AC:	100 to 240 VAC
DC:	-36 to -72 VDC
Input current	
AC:	7.76A @ 100 VAC 3.82A @ 200 VAC
DC:	20.4A @ 36 VDC 10A @ 72 VDC
Inrush current	
AC:	70A @ 100 VAC (max.) 150A @200 VAC (max.)
DC:	140A @48 VDC

Physical Characteristics

Dimensions (h,w,d):	2U (3.5"/88 mm) x 482.6 mm (19") x 450 mm (17.7")
Weight	
AC:	22 lbs (10 kg)
DC:	19.8 kbs (9 kg)

Overload Protection

All circuits are protected against overload and short circuits through shutdown of control circuits.

Reliability

Physical Durability:
Vibration and shock compliance with TR and NWT-000063 (NEBS) Par.4.4.1 and 4.4.2

MTBF

AC:	125,194 hours
DC:	166,443 hours

Environmental Conditions

Operating Temp:	-5 to 50°C (23 to 122°F) (ambient)
Rel. Humidity:	5% to 95%, non-condensing

Agency Approval

EMC Emission:	US – FCC Part 15, Subpart J, Class A Europe – EN55022 class A
Immunity:	Approved according to EN50082-1
Safety:	UL for US approved according to UL1950 Std. C-UL (UL for Canada) approved according to C22.2 No.950 Std. CE for Europe approved according to EN 60950 Std.

Ordering Information

Product	PEC Code	COM Code
Avaya P330 BUPS	4705-057	108563339
Avaya P330 DC BUPS	4705-144	108731563

6. EQUIPOS DE CÓMPUTO

Se utilizaron 9 equipos de cómputo para las pruebas, todos con las mismas características:

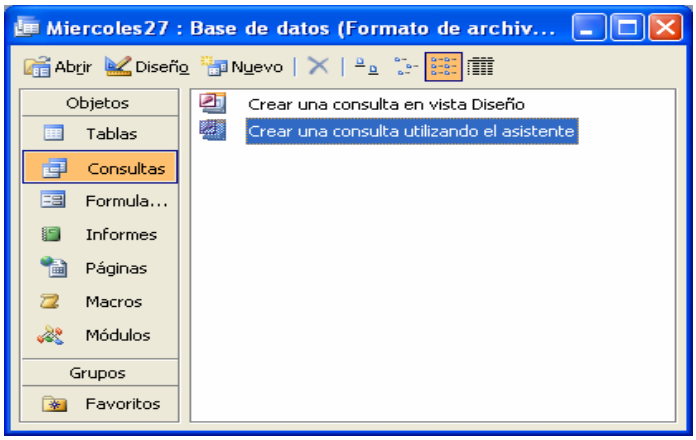
Fabricante: Dell Computer corporation
Modelo: Dell Optiplex Gx 260
Procesador: Pentium 4 de 2.4 Ghz
Memoria RAM: 512 MB
Disco duro: 30MB
Sistema operativo: Windows XP Professional

ANEXO C. BASE DE DATOS (CONSULTAS)

En este anexo se mostrará de forma detallada la manera de realizarse las Consultas y las Gráficas en Microsoft Access. Una vez vinculado el archivo o todos los archivos de texto en la base de datos se pueden obtener los parámetros de medición deseados haciendo consultas gráficas, estos procedimientos se realizan de la siguiente manera:

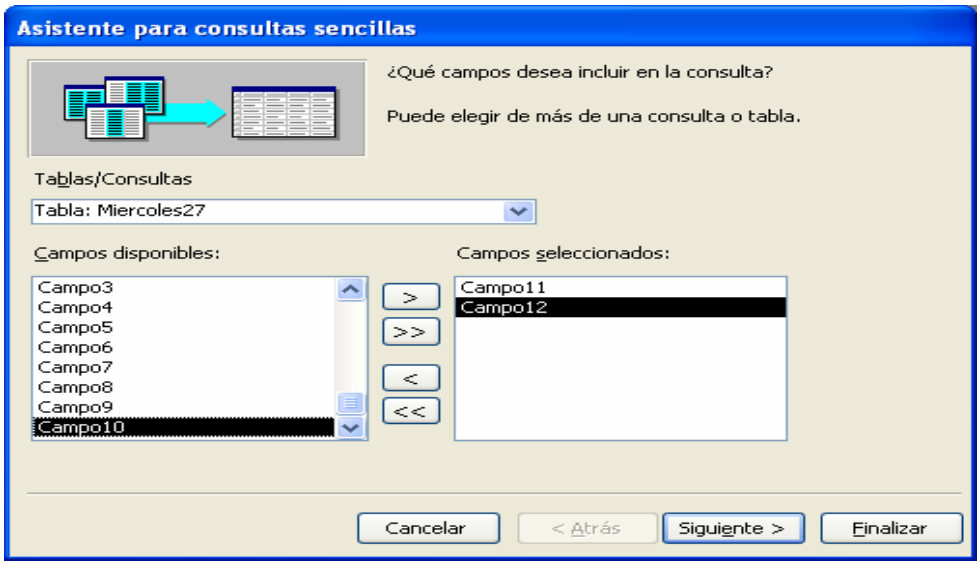
1. Se usa la opción Consultas y se selecciona Crear una consulta utilizando el asistente, en donde se mostrará el asistente para la creación de consultas, figura 1.

Figura 1. Creación de consultas.



2. Se selecciona la tabla a consultar y luego se seleccionan los campos necesarios según el tipo de parámetro deseado. En la figura 2 se muestran los campos seleccionados para obtener la distribución de protocolos, ya que como se puede observar en los archivos de texto y en las tablas los protocolos corresponden al campo 11 y el tamaño del paquete al campo 12.

Figura 2. Asistente para consultas.



3. Se continúa con el proceso, se escoge la opción Resumen y luego Opciones de resumen, como se muestra en la figura 3, en este cuadro se selecciona el valor de resumen que se desea calcular, en este caso se escoge la opción sumar ya que lo que se quiere calcular es la distribución de protocolos con su respectivo tamaño en bytes.
4. Se finaliza el proceso e inmediatamente se muestra la consulta deseada, figura 4.
5. Luego se procede a graficar los resultados de la consulta.

Figura 3. Opciones de resumen.

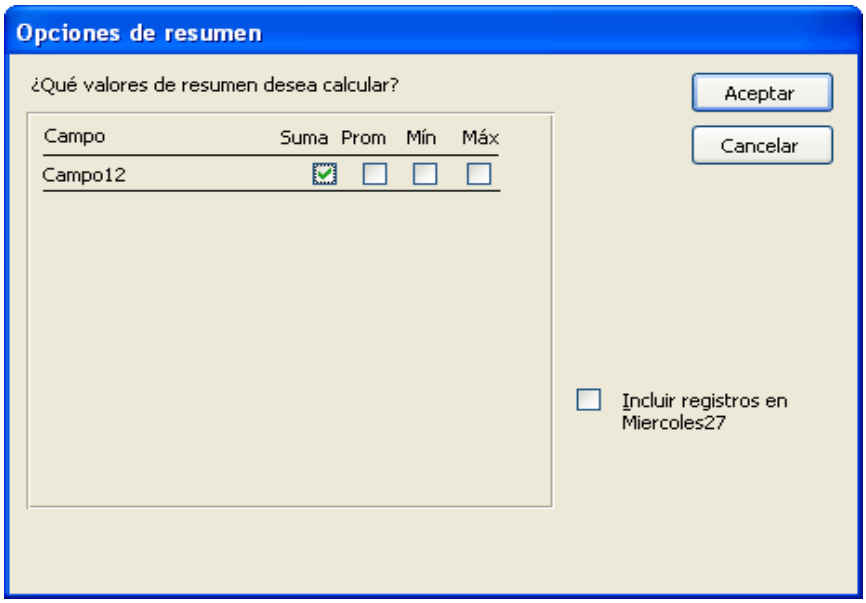
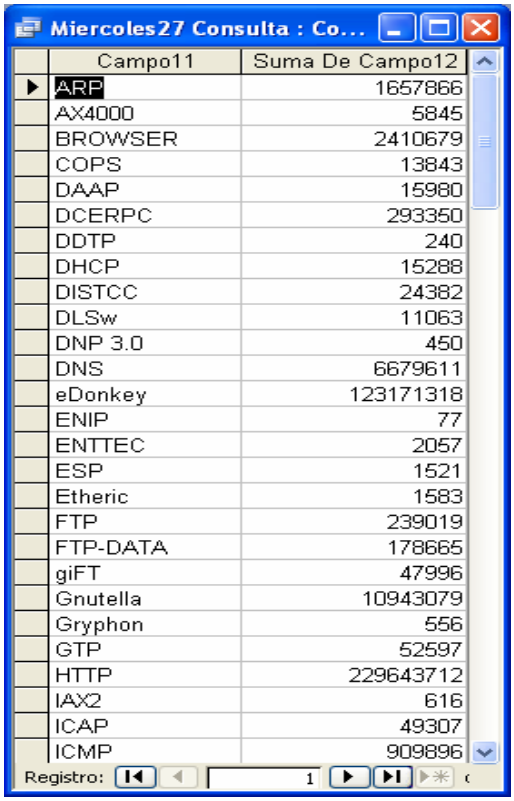
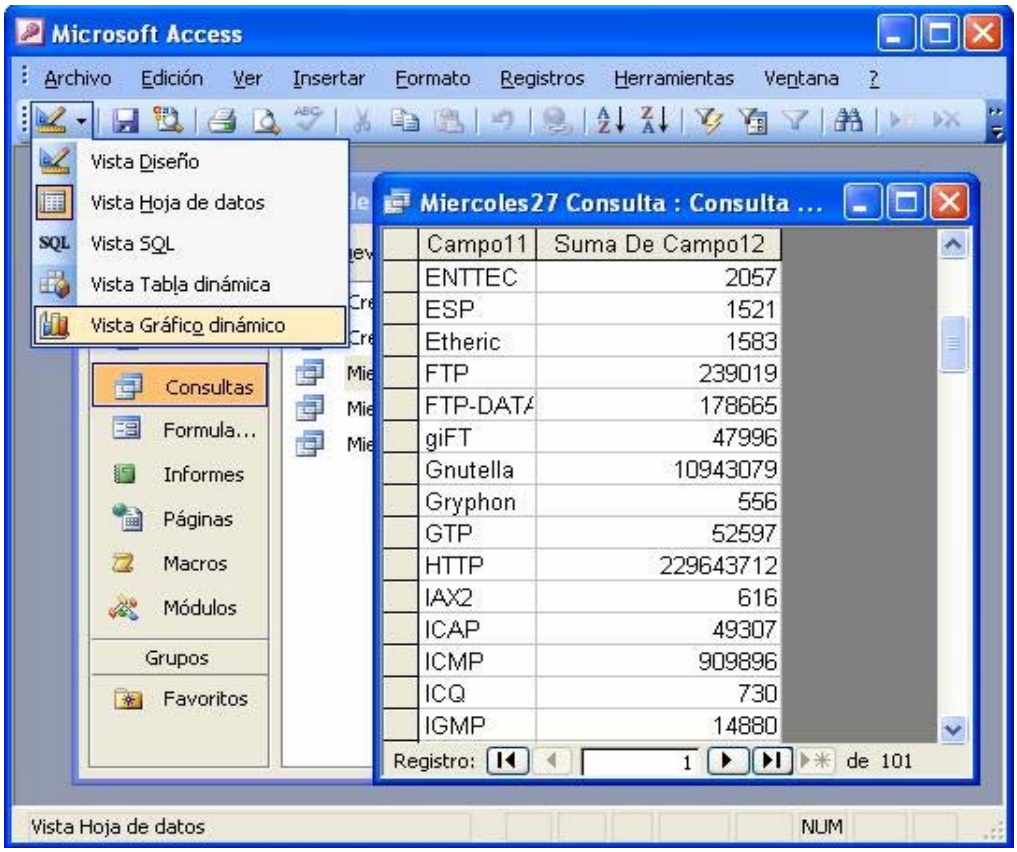


Figura 4. Consulta de Distribución de protocolos.



Para graficar los resultados de la consulta se va al menú Vista, como se muestra en la figura 5 y se selecciona Vista Gráfico dinámico.

Figura 5. Creación de Gráfica.



Aquí se muestran dos ventanas, una en donde se creará la gráfica, y la otra con los campos a graficarse. Para obtener la gráfica se deben arrastrar los campos hacia la otra ventana, teniendo en cuenta las variables. Después de tener esto se hace clic derecho a un lado de la gráfica y se selecciona Tipo de Gráfico, para la distribución de protocolos se seleccionó Tipo de Gráfico Circular, ya que con este se aprecian mejor los protocolos más importantes o más utilizados, figura 6. Para mejorar la visualización de los protocolos se hace

clic derecho encima del gráfico y se escoge a opción Propiedades y en ella se selecciona Filtrar y Agrupar. Figura 7.

Aquí se tiene la opción de mostrar todos los elementos, los más representativos o los menos representativos y el número de estos.

Habiendo seleccionado las opciones más adecuadas para lo que se requiera visualizar, podemos mediante el cursor, señalar dentro de la gráfica el campo que se desee y se desplegará una etiqueta en la cual se muestra el nombre del protocolo, su tamaño en bytes y su porcentaje con respecto a los demás. Figura 6.

Figura 6. Grafica Distribución de Protocolos.

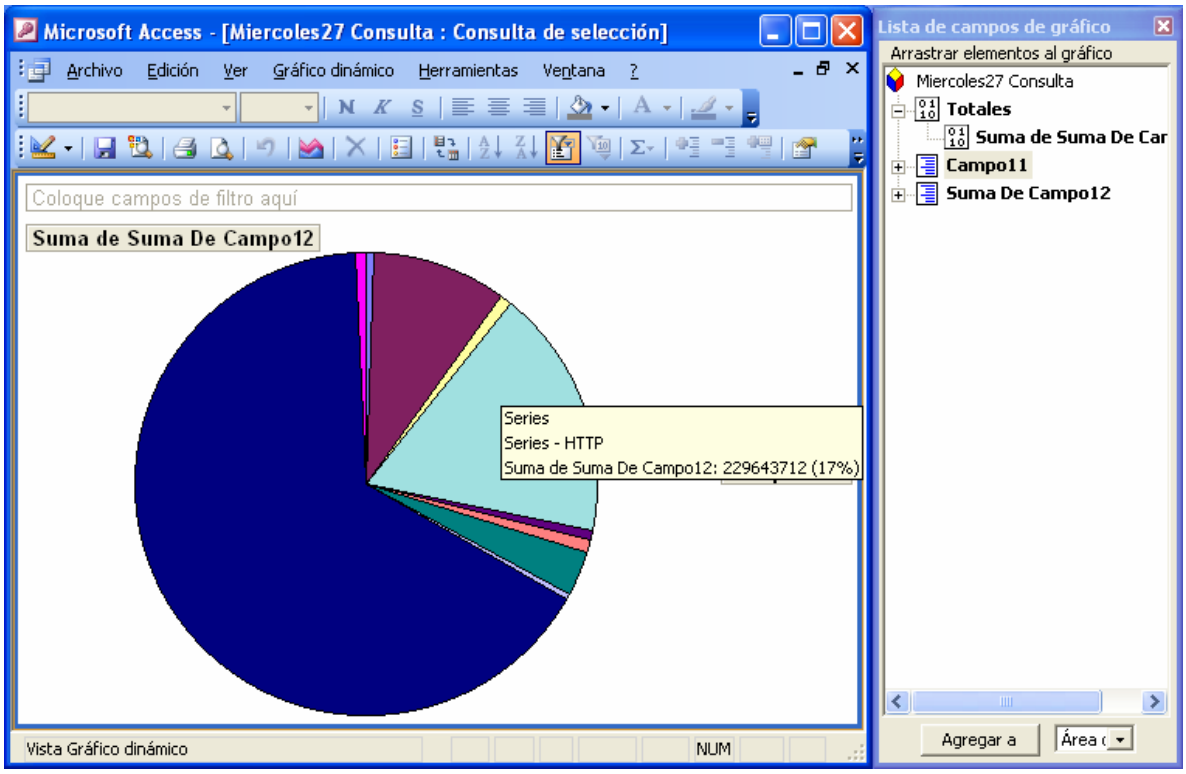
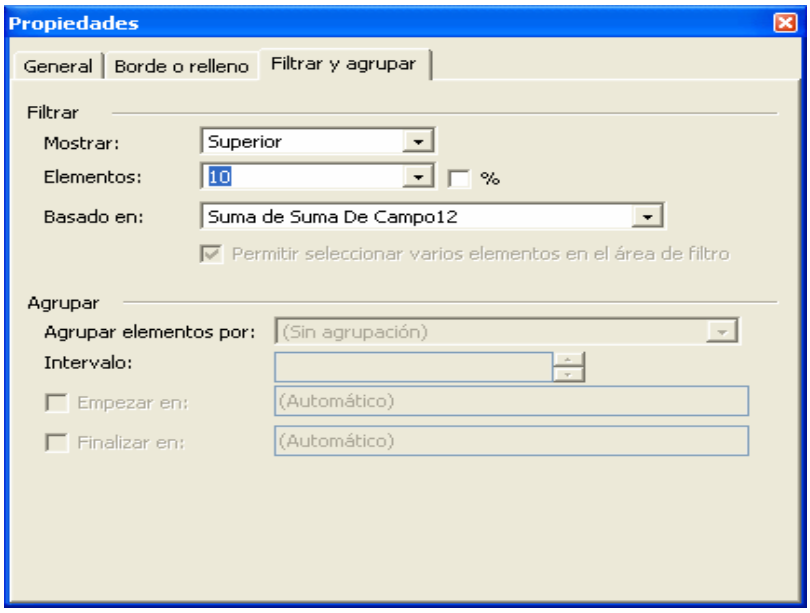


Figura 7. Propiedades de Gráfica.



Consulta de la Carga en bytes, distribuida a lo largo del periodo de medida y número de paquetes. Figuras 8, 9 y 10.

Figura 8. Asistente para consultas.

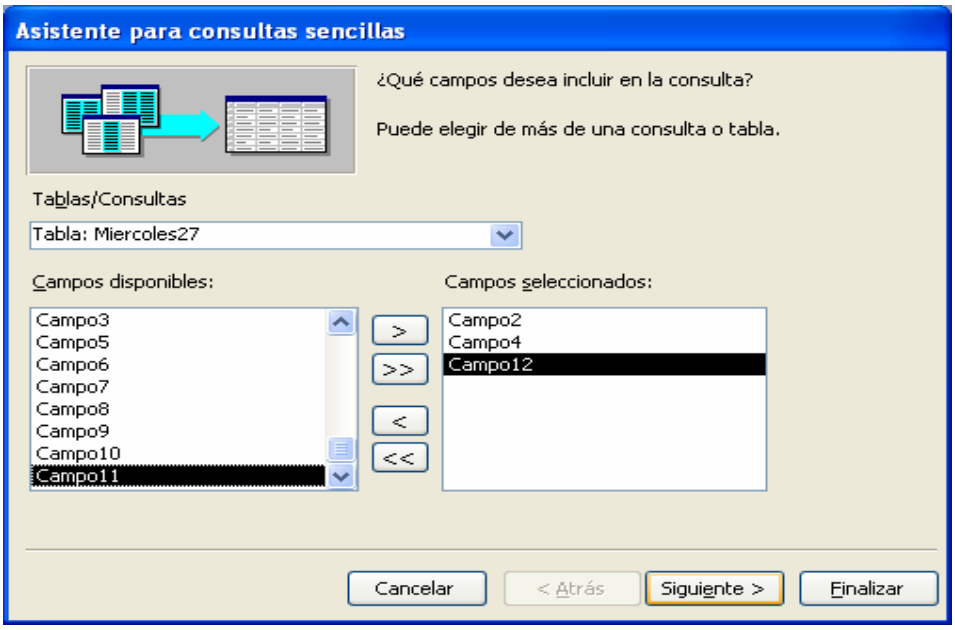


Figura 9. Opciones de resumen.

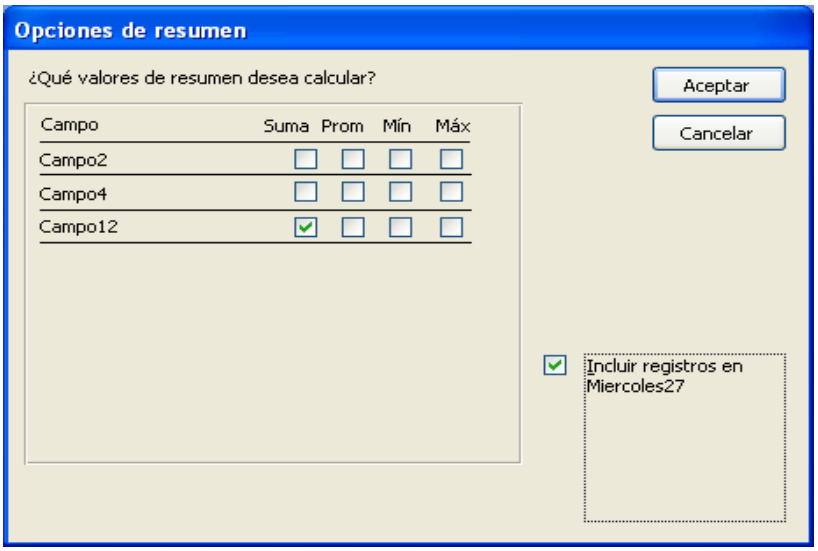


Figura 10. Consulta de la Carga en bytes, distribuida a lo largo del periodo de medida y número de paquetes.

Miercoles27 Consulta3 : C...

Car	Ca	Suma De Camp	Cuenta De Mier
8	30	3927210	36918
8	31	2718661	23909
8	32	2903567	17772
8	33	4216062	39576
8	34	4199894	43155
8	35	4160147	44485
8	36	4258912	42421
8	37	3035178	20990
8	38	5388625	66872
8	39	5504852	64500
8	40	5876814	67360
8	41	5696571	63815
8	42	4929453	44843
8	43	5182193	48888
8	44	3747841	23102
8	45	2340298	16921
8	46	3688478	34875
8	47	4157977	31637
8	48	3912433	23988
8	49	4191870	25949
8	50	3976324	27227

Registro: 1

Para graficar esta Consulta se repite el procedimiento anterior solo que en este caso se escoge como Tipo de Gráfico, Columna. Para una mejor visualización de la carga en bytes distribuida a lo largo del día, se hace clic derecho sobre el campo 4 en la gráfica, se escoge la opción Propiedades y en ella Filtrar y Agrupar.

En Filtrar se selecciona Mostrar Todos los elementos y en Agrupar se selecciona Agrupar elementos por Intervalo numérico, el Intervalo se escoge según el detalle que el usuario desee, así como se muestra en las figuras 11, 12 y 13.

Figura 11. Propiedades de Gráfico.

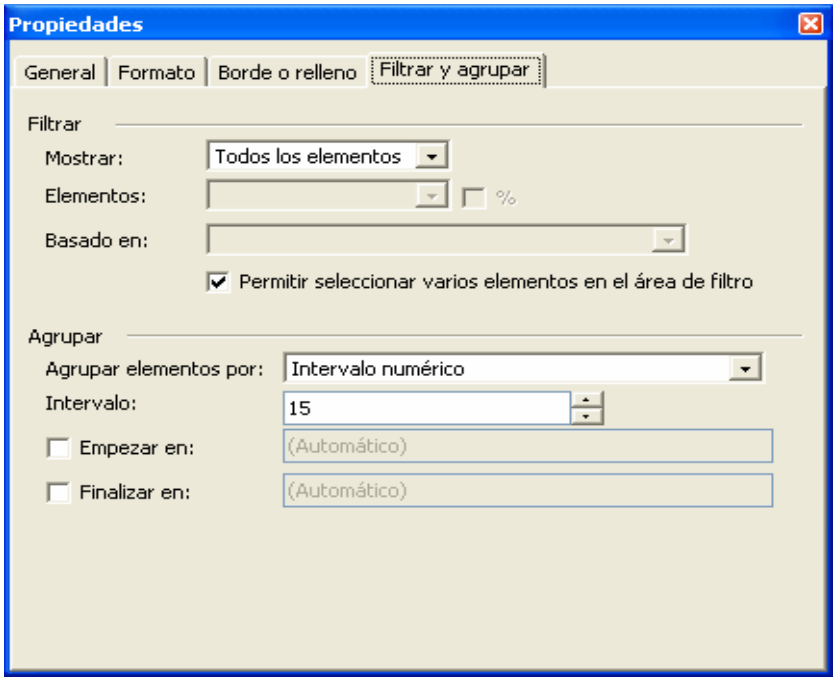


Figura 12. Gráfica Distribución de carga en bytes a lo largo del día.

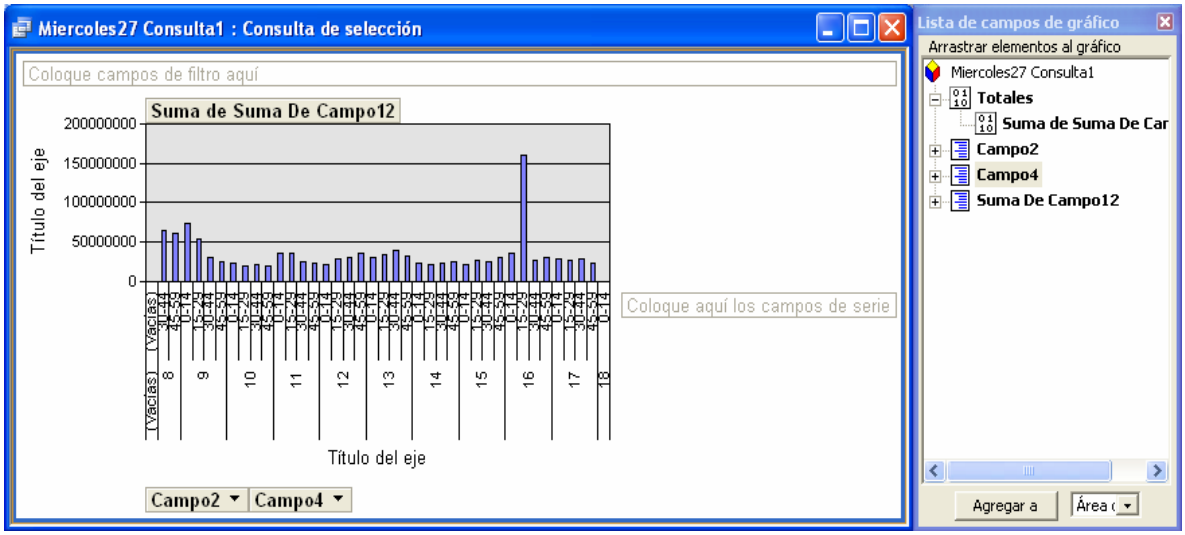
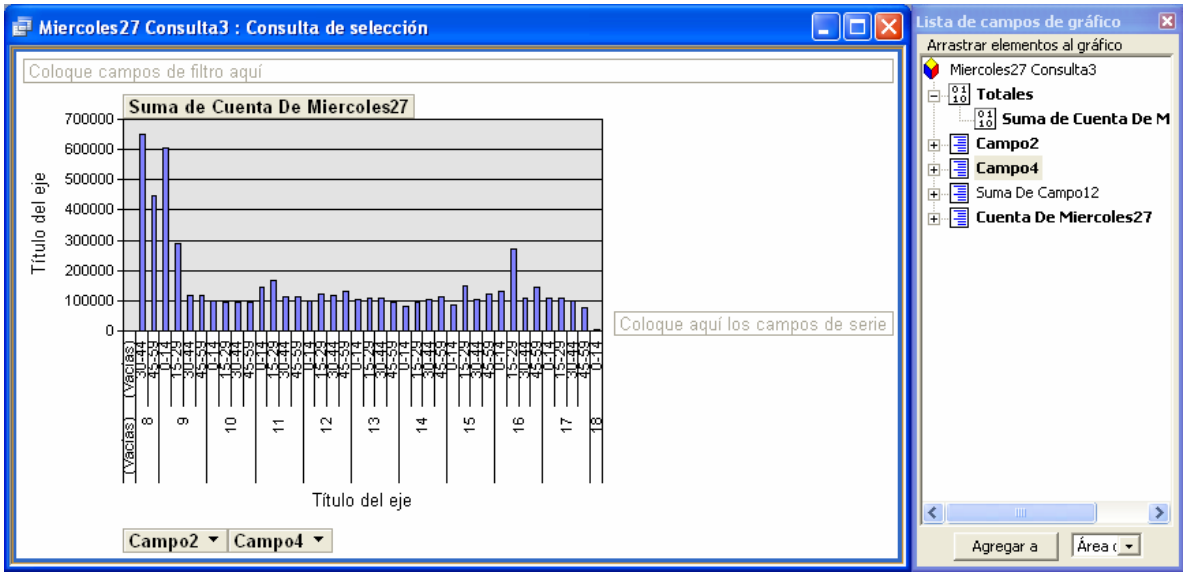


Figura 13. Número de paquetes.



Consulta de Orígenes y Destinos. Figuras 14, 15 y 16.

Figura 14. Asistente para consultas.

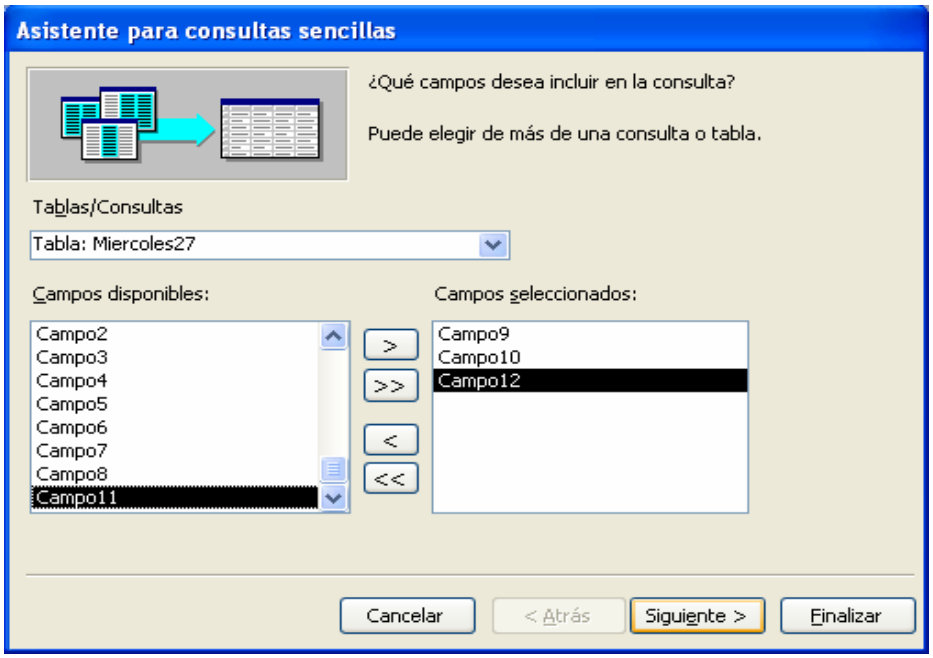


Figura 15. Opciones de resumen.

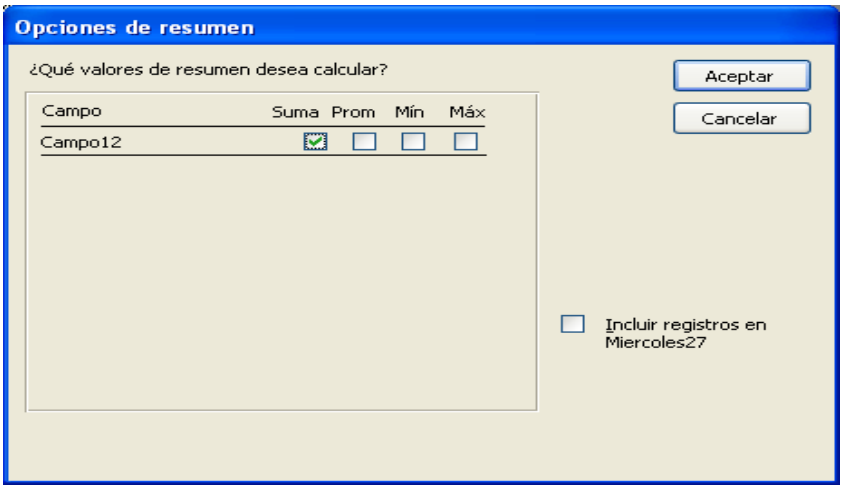
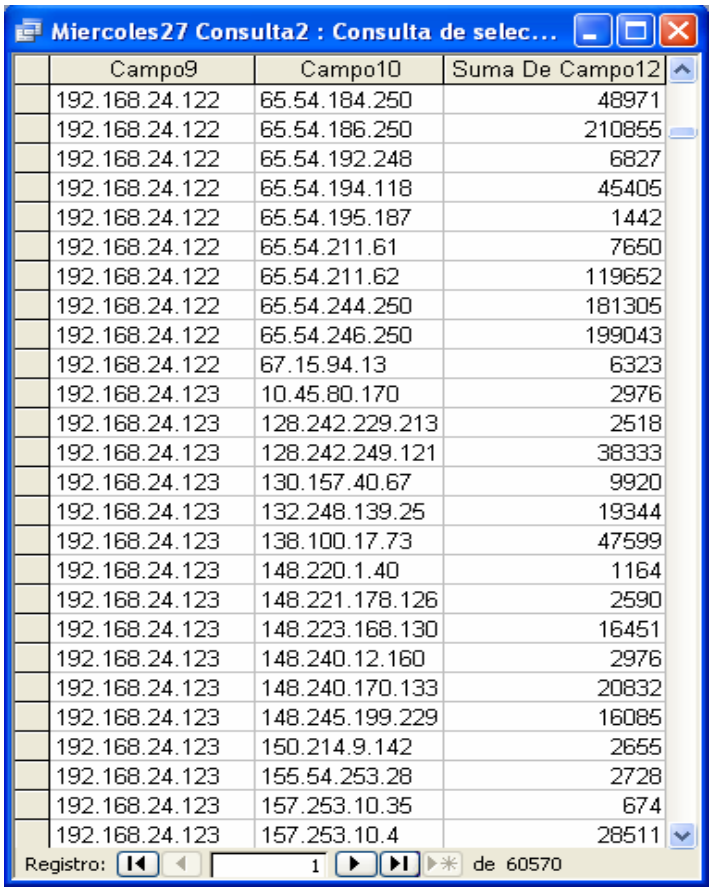


Figura 16. Consulta de Orígenes y Destinos.



Miercoles27 Consulta2 : Consulta de selec...

Campo9	Campo10	Suma De Campo12
192.168.24.122	65.54.184.250	48971
192.168.24.122	65.54.186.250	210855
192.168.24.122	65.54.192.248	6827
192.168.24.122	65.54.194.118	45405
192.168.24.122	65.54.195.187	1442
192.168.24.122	65.54.211.61	7650
192.168.24.122	65.54.211.62	119652
192.168.24.122	65.54.244.250	181305
192.168.24.122	65.54.246.250	199043
192.168.24.122	67.15.94.13	6323
192.168.24.123	10.45.80.170	2976
192.168.24.123	128.242.229.213	2518
192.168.24.123	128.242.249.121	38333
192.168.24.123	130.157.40.67	9920
192.168.24.123	132.248.139.25	19344
192.168.24.123	138.100.17.73	47599
192.168.24.123	148.220.1.40	1164
192.168.24.123	148.221.178.126	2590
192.168.24.123	148.223.168.130	16451
192.168.24.123	148.240.12.160	2976
192.168.24.123	148.240.170.133	20832
192.168.24.123	148.245.199.229	16085
192.168.24.123	150.214.9.142	2655
192.168.24.123	155.54.253.28	2728
192.168.24.123	157.253.10.35	674
192.168.24.123	157.253.10.4	28511

Registro: 1 de 60570

Consulta de tráfico Broadcast y Multicast.

Para realizar la consulta de Broadcast se debe crear una consulta en vista de Diseño y se deben llenar los campos como se muestra en la figura 17 y para realizar la consulta de Multicast se deben llenar los campos como se muestra en la figura 18.

Figura 17. Consulta Broadcast.

Figura 18. Consulta Multicast.

Consulta de Distribución de Tamaño de Paquete.

Para realizar la consulta de Distribución de Tamaño de Paquete se debe crear una consulta en vista de Diseño y se deben llenar los campos como se muestra en la figura 19.

Figura 19. Consulta de Distribución de tamaño de paquete.