ESCUELA POLITECNICA DEL EJÉRCITO

SEDE LATACUNGA

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

TEMA: ANLALISIS Y OPTIMIZACION DEL FLUJO DEL TRAFICO DE PROTOCOLOS Y APLICACIONES EN LA RED LAN DE LA ESCUELA POLITECNICA DEL EJERCITO SEDE LATACUNGA PARA EVALUAR LA CALIDAD DE SERVICIO EN BASE A LA METODOLOGIA (MIRA METODOLOGIA PARA LA INSPECCIONDE PTRAFICO EN REDES AVANZADAS)

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS E INFORMATICA

ELABORADO POR

SEGUNDO JAVIER CAYO MOLINA

DIRECTOR:

ING. FABIAN MONTALUISA

CODIRECTOR:

ING. RAUL CAJAS

LATACUNGA, FEBRERO DE 2007

CERTIFICADO

En nuestra calidad de Director y Codirector, certificamos en el siguiente trabajo fue realizado en su totalidad por el señor Segundo Javier Cayo Molina. Como requisito en su totalidad previo a la obtención del titulo de Ingeniero en Sistemas e Informática

_____	_____
Ing. Fabián Montaluisa	Ing. Raúl Cajas
DIRECTOR	CODIRECTOR

AGRADECIMIENTO

Mi agradecimiento especial a Dios todopoderoso, a la Virgen santísima a Jesús en la imagen del Divino Niño y Jesús del Gran Poder, por su protección sus bendición es por haberme dado la vida, unos excelentes padres y una linda familia, lo que ha permitido dar un gran paso en m i vida profesional.

Agradezco a la Escuela Politécnica del Ejercito Sede Latacunga, ya que me abrió sus puertas para poder formarme profesional e intelectualmente.

A la carrera de Ingeniería en Sistemas e Informática a sus profesores, por todos los conocimientos que me brindaron.
Agradezco al director de este proyecto al ingeniero Fabián Montaluisa por su apoyo, confianza y apertura para poder desarrollar el presente Proyecto en la unidad de Tecnologías de la Información y Comunicación, al codirector al ingeniero Raúl Cajas, por guiarme para culminar con éxito el proyecto.

Un profundo agradecimiento a las personas que trabajan en la Unidad de Tecnologías de Información y Comunicación, en especial a la Ingeniera Tatiana Mayorga por su apoyo sus conocimientos en todo momento que requería sin ningún egoísmo, gracias por todo.
Al ingeniero Patricio Espinel por su ayuda, sus consejos y principalmente por su amistad.

javier

DEDICATORIA

En la vida hay personas muy importantes que brindan su apoyo te extienden la mano en momentos difíciles, te escuchan te entienden por esto dedico este trabajo con todo el amor del mundo a mis padres que les admiro y les amo mucho, gracias por todo lo que han hecho por mi, por el apoyo que me han brindad tanto moral como económico, que Dios la Virgen Santísima les bendiga y les proteja siempre.

Dedico este trabajo a toda mi familia en especial a mis hermanos Jacqueline y Jorge Luis por su apoyo por estar siempre preocupados de que todo me salga bien.

A mi tío Fabián Molina y su familia por todo su apoyo, por su preocupación sus consejos, su amistad, buscando siempre el bienestar de mi familia gracias por todo.

Este trabajo va dedicado con todo mi amor a mi esposa Rosi y a mi hija Janine el amor de mi vida, gracias por todo el apoyo, pero sobre todo por la paciencia y comprensión.

Javier

ÍNDICE

CAPÍTULO I **Página**

CAPÍTULO II METODOLOGÍA MIRA (METODOLOGÍA PARA LA INSPECCIÓN DE TRÁFICO EN REDES AVANZADAS)

Página

CAPÍTULO III ANÁLISIS DEL FLUJO DE TRÁFICO DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA.

Página

CAPÍTULO IV OPTIMIZACIÓN DEL FLUJO DE TRÁFICO DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA

CAPITULO V CONCLUSIONES Y RECOMENDACIONES

Página

ÍNDICE DE FIGURAS

CAPITULO I **Página**

CAPITULO II **Página**

CAPITULO III **Página**

CAPITULO IV **Página**

CAPITULO I

1.1 INTRODUCCIÓN.

Las redes informáticas son sistemas que permite conectar ordenadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos, esto permite que la comunicación no sea muy complicada entre los diferentes usuarios que estén conectados a la red en la Institución que opte por tener una red informática.

Mediante el proceso de compartir información y recursos en una red, los usuarios de los diferentes sistemas informáticos de la organización a la que pertenecen podrán hacer un mejor uso de los mismos, mejorando de este modo el rendimiento global de la organización.

Para visualizar de mejor forma lo referente a las redes, vamos a citar varias de las ventajas que nos brinda la red que está instalada en una organización.

- Mayor facilidad en la comunicación entre usuarios.
- Reducción en el presupuesto para software.
- Posibilidad de organizar grupos de trabajo.
- Mejoras en la administración de los equipos y programas.
- Mejoras en la integridad de los datos.
- Mayor seguridad para acceder a la información.

1.1.1 SERVICIOS DE RED

Para obtener todas las ventajas que anteriormente se detalló del uso de una red, se deben tener instalados una serie de servicios de red, como son:

1.1.1.1 Acceso

Los servicios de acceso se encargan tanto de verificar la identidad del usuario (para asegurar que sólo pueda acceder a los recursos para los que tiene permiso) como de permitir la conexión de usuarios a la red desde lugares remotos.

1.1.1.2 Ficheros

El servicio de ficheros consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones.

1.1.1.3 Impresión

Permite compartir impresoras entre varios ordenadores de la red, lo cual vitará la necesidad de tener una impresora para cada equipo, con la consiguiente reducción en los costes. Las impresoras de red pueden ser conectadas a un servidor de impresión, que se encargará de gestionar la impresión de trabajos para los usuarios de la red, almacenando trabajos en espera (cola de impresión), asignando prioridades a los mismos, etc.

1.1.1.4 Información

Los servidores de información pueden almacenar bases de datos para su consulta por los usuarios de la red u otro tipo de información, como por ejemplo documentos de hipertexto, correo electrónico, antivirus, sistemas académicos.

1.1.1.5 Otros

En el campo de la comunicación entre usuarios existen una serie de servicios que se debe mencionar. El más antiguo y popular es el correo electrónico (e-mail) que permite la comunicación entre los usuarios a través de mensajes escritos. Los mensajes se enviarán y se recuperarán usando un equipo servidor de correo. Resulta mucho más barato, económico y fiable que el correo convencional.

1.1.2 EQUIPOS DE RED

1.1.2.1 Servidores

Un servidor es un ordenador que ejecuta un sistema operativo de red y ofrece servicios de red a las estaciones de trabajo. El servidor debe ser un sistema fiable con un procesador potente, con discos de alta capacidad y con gran cantidad de memoria RAM.

El software del sistema operativo del servidor de red se integra en un número importante de sistemas operativos conocidos, incluyendo Windows 2000 Server/Professional, Windows NT Server, Windows 95/98/ME y Apple Talk.

1.1.2.2 Estaciones de Trabajo

Cuando un ordenador se conecta a una red el primero se convierte en un nodo o estación de trabajo del servidor. Las estaciones de trabajo pueden ser ordenadores personales con el DOS, sistemas Macintosh de Apple o sistemas Windows.
Las estaciones de trabajo se conectan al servidor para solicitarle un servicio de la red, de acuerdo a los permisos que tenga la estación de trabajo.

DEFINICIÓN DE RED LAN

RED LAN

LAN es la abreviatura de Local Area Network (Red de Área Local). Una red de área local es la interconexión de varios ordenadores y periféricos para intercambiar recursos e información. En definitiva, permite que dos o más máquinas se comuniquen.

Una red de área local es un sistema de transmisión de datos que nos permite que la comunicación entre diferentes dispositivos de tratamientos de datos sea posible.

Los inicios experimentales de la red de área local se dan desde la década de los sesenta hasta la mitad de los setenta. Fueron importantes los trabajos realizados por Bell Telephone Laboratories en redes con topología en anillo, en Xerox Corporation donde se desarrolló la primera Ethernet.

La segunda etapa, data de los finales de los setenta. Coincide con el incremento de las prestaciones y con los primeros productos en el mercado. Empiezan a aparecer numerosas empresas con servicios de redes locales.

La última etapa se inicia a principios de los ochenta cuando el IEEE 802 empieza a influir en lo relacionado con las redes locales. Se afianzan las topologías en anillo y en bus. Prosperan los protocolos basados en CSMA/CD.

Todos los dispositivos pueden comunicarse con el resto aunque también pueden funcionar de forma independiente. Las velocidades de comunicación son elevadas estando en el orden de varios millones de bits por segundo dependiendo del tipo de red que se use. Dentro de una red de área local existen algunos ordenadores que sirven información, aplicaciones o recursos a

los demás. Estos ordenadores se les conocen con el nombre de servidores.

Los servidores pueden ser de dos tipos dedicados o no dedicados:

- **Dedicados**. Normalmente tienen un sistema operativo más potente que los demás y son usados por el administrador de la red.
- **No dedicados**. Pueden ser cualquier puesto de la red que además de ser usado por un usuario, facilita el uso de cierto recursos al resto de los equipos de la red, por ejemplo, comparte su impresora.

El creciente uso de las redes locales se debe al abaratamiento de sus componentes y a la generalización de sistemas operativos orientados a uso en red. Con esto se facilita las operaciones de compartir y usar recursos de los demás ordenadores y periféricos.

BENEFICIOS DE UNA RED DE ÁREA LOCAL

Bien planificada e implementada, una red local aumenta la productividad de los PC'S y periféricos implicados en ella. Si no se planifica y monta apropiadamente puede ser motivo de frustración y de pérdida de tiempo e información.

Algunas de las facilidades que nos abre el uso de una red local son:

- Compartir los recursos existentes como: impresoras, módems, escáner, etc.
- Uso de un mismo software desde distintos puestos de la red.
- Acceder a servicios de información internos (Intranet) y externos (Internet).
- Intercambiar archivos.
- Uso del correo electrónico.
- Permite conexiones remotas a los distintos recursos.
- Copias de seguridad centralizadas
-

En definitiva, hace posible una mejor distribución de la información que se disponga dentro de la Organización.

APLICACIONES EN UN CENTRO EDUCATIVO

La red de área local dentro de un centro educativo nos abre una serie de posibilidades muy interesantes e importantes para su uso como herramienta de apoyo en el aula. Algunas de ellas son:

- Compartir los recursos existentes en el centro educativo, desde las impresoras, escáner y las comunicaciones con el exterior, hasta el propio software instalado en los distintos equipos de la red.
- Correo electrónico tanto interno entre alumnos y profesores del mismo centro educativo, como a nivel de todo el mundo.
- Servidores de información internos tipo Web.

ADMINISTRADOR DE LA RED LAN

Es muy importante designar a un responsable técnico que sea quien planifica y mantiene operativa y confiable a la red de área local.

El administrador de la red de área local es una figura clave en el éxito de su funcionamiento. Él mantiene los archivos y recursos, así como previene consecuencias nefastas siguiendo los procedimientos de seguridad (antivirus, copias de seguridad, etc.). También decide los privilegios de cada uno de los usuarios o grupos de usuarios de la LAN restringiendo convenientemente el uso de sistemas vitales sólo al personal adecuado.

Algunas de las funciones de mantenimiento del administrador de la LAN son:

- Mantener operativa la Red LAN
- Decidir e implementar la política de seguridad en la red
- Privilegios de los usuarios
- Antivirus
- Copias de seguridad
- Búsqueda de mayores capacidades para el mejor funcionamiento de la Red LAN
- Investigar nuevas soluciones o sistemas que den apoyo a la Red LAN.
- Instalación de nuevos dispositivos y nuevos software para poner a disposición de los diferentes usuarios de la Red LAN.

Cada día se facilita más el trabajo del administrador con la aparición de nuevas utilidades y herramientas de automatización de las tareas más habituales. Muchas de estas tareas pueden ser programadas para que se ejecuten de forma automática. Es el caso de las copias de seguridad o de la distribución de un antivirus por los distintos equipos de la red.

1.3 CARACTERÍSTICAS DE LA RED LAN DE LA ESPEL

La Red LAN de la Escuela Politécnica del Ejército Sede Latacunga posee ciertas características muy importantes, las mismas que darán una pauta pasa desarrollar este trabajo de mejor forma.

1.3.1 Topología de Red

La topología de red se refiere a la forma en que están interconectados los distintos equipos (nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como por ejemplo un computador o una impresora.

La topología de red que se utiliza en la Escuela Politécnica del Ejército Sede Latacunga es la topología de estrella, está topología en redes LAN hace referencia que cada estación esta directamente conectada a un modo central , generalmente a través de dos enlaces punto a punto , uno para transmisión y otro para recepción.

Entre las ventajas de utilizar la topología estrella tenemos las siguientes:

- Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.

- Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida de uno hacia el otro debe pasar por el punto central.

- Si se rompe un cable sólo se pierde la conexión del nodo que lo interconectaba.

- Es más accesible detectar y de localizar un problema en la red.

En la Figura 1.1 se muestra de forma gráfica la topología estrella.

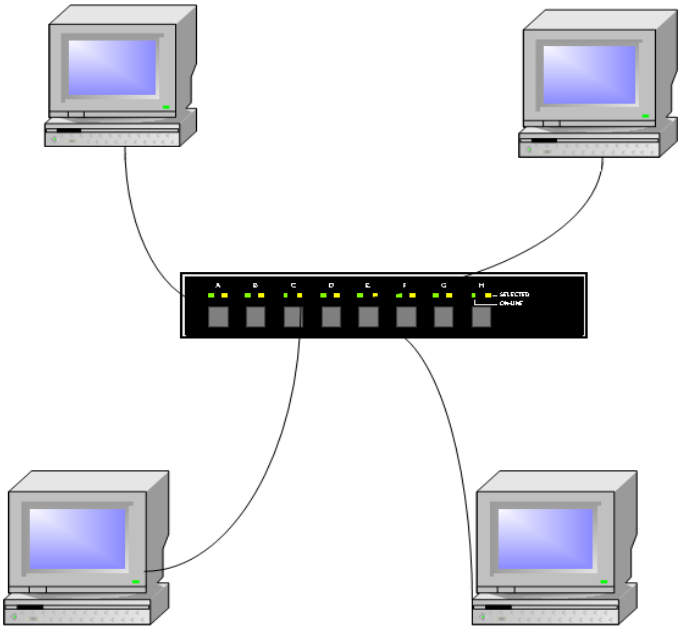


Figura 1.1. Topología Estrella.
Elaborado por: Segundo Javier Cayo Molina

1.3.2 CABLEADO ESTRUCTURADO

El cableado estructurado es una red de cables y conectores en número, calidad y flexibilidad de disposición suficientes que nos permita unir dos puntos cualesquiera dentro de un edificio para cualquier tipo de red sea voz, datos o imágenes.

El cableado nos brinda varios beneficios los mismos que se detallan a continuación.

- El cableado estructurado va a permitir trasmitir datos en la misma instalación, independientemente de los equipos y productos que se utilicen.

- Se facilita y agiliza mucho las labores de mantenimiento.
- Es fácilmente ampliable.
- El sistema es seguro tanto a nivel de datos como a nivel de seguridad personal.
- Un beneficio muy importante del cableado estructurado es que se encuentra regulado mediante estándares, lo que garantiza a los usuarios seguridad al momento de utilizar la red.

En la Escuela Politécnica del Ejército Sede Latacunga, existe el cableado estructurado para la comunicación entre las estaciones de trabajo y los switchs, para lo cuál se utiliza cable par trenzado UTP categoría 5 y 5e.

De igual forma como se habló anteriormente es necesario utilizar un estándar para realizar el cableado, el estándar que se utiliza EIA/TIA 568A. Este estándar fue desarrollado y aprobado por comités del Instituto Nacional Americano de Normas (ANSI), la Asociación de la Industria de Telecomunicaciones (TIA), y la Asociación de la Industria Electrónica, (EIA). l estándar establece criterios técnicos y de rendimiento para diversos componentes y configuraciones de sistemas.

El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán. La instalación de los sistemas de cableado durante el proceso de instalación y/o remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.

El estándar de colores que se utiliza para el cableado estructurado en la Escuela Politécnica del Ejército Sede Latacunga es el EIA/TIA 568B, la distribución de colores de dicho estándar podemos observar en la figura 1.2.

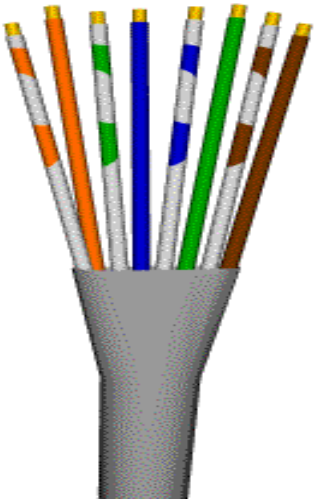


Figura 1.2. Distribución de colores del Estándar EIA/TIA 568B.
Fuente: www.paginasclick.com

También como parte muy importante y fundamental del cableado estructurado, se dispone de 2 enlaces de fibra óptica, los mismos que permite comunicarse desde el centro de datos 1 al centro de datos 2 y de igual forma desde el centro de datos 1 con la Facultad de Sistemas e Informática.

1.3.3 ELEMENTOS DE RED

Antes de empezar a mencionar los diferentes elementos de red debemos tomar en consideración que la Red LAN de la Escuela

Politécnica del Ejército Sede Latacunga se encuentra dividida en tres grupos muy importantes que son: La Red Administrativa, La Red Académica, La Red DMZ y la Red Académica de la Facultad de Sistemas e Informática.

La Red Administrativa está compuesta por la Unidad de Tecnologías de la Información y Comunicación, Unidad de Finanzas, Unidad de Marketing, Unidad de Talento Humano, Unidad de Bienestar Estudiantil, MED, Unidad de Logística, Centro de Producción, Unidad de Admisión y Registro y los diferentes departamentos de las Carreras que dispone la Escuela Politécnica del Ejercito Sede Latacunga.

La Red Académica está compuesta por los diferentes laboratorios que utilizan día a día los estudiantes de la Escuela Politécnica del Ejército Sede Latacunga, como son el laboratorio de Internet, la biblioteca virtual, la biblioteca, los laboratorios de Electrónica, Electromecánica, Inglés, también se incluye en esta red la sala de profesores de la Institución.

La Red DMZ es una red que se encuentra detrás del Firewall, es decir es una red pública, esta red es usada para servicios que precisan ser accedidos directamente desde Internet, en la Escuela Politécnica del Ejercito la red DMZ presta los servicios de Mail y Web.

La Red Académica de Sistemas esta compuesta por todos los laboratorios que existen en dicha facultad como son: Multimedia, Novell, Redes, Unix.

1.3.3.1 Estructura de los Centros de Datos

En la Escuela Politécnica del Ejército Sede Latacunga se dispone de 4 centros de datos, los mismos que están distribuidos de la siguiente forma:

1.3.3.1.1 Centro de Datos 1

El centro de datos 1 es el principal, aquí se encuentra la Unidad de Tecnologías de Información y Comunicación, en este centro de datos se encuentra el rack principal como podemos observar en la figura 1.3, en el cuál se encuentran los switchs, hubs y los diferentes dispositivos que permiten la correcta comunicación con los diferentes centros de datos que dispone la Escuela Politécnica del Ejército Sede Latacunga.

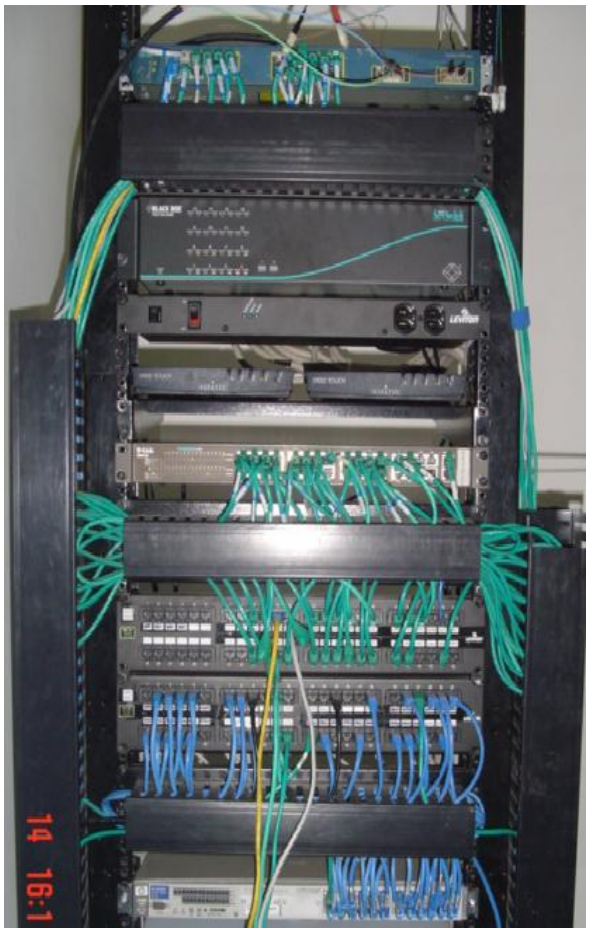


Figura 1.3. Rack Principal del Centro de Datos 1.
Elaborado por: Segundo Javier Cayo Molina

De la misma forma aquí se encuentran la sala de servidores, como podemos observar en la figura 1.4, los mismos que prestan los siguientes servicios:

ÁREA ADMINISTRATIVA

Servicios

- Servidor de Base de Datos

Sistema Operativo

- Windows 2000 Advanced Server en Español

Servicios

- Controlador Principal de Dominio
- Servidor de DHCP
- Servidor de Archivos

Sistema Operativo

- Windows 2003 Estándar Edition en Inglés

Marca

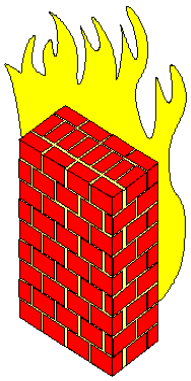
Servicios

- Servidor de Backup de Dominio
- Aplicaciones Web
- Antivirus

Sistema Operativo

- Windows 2003 Estándar Edition en Español

Marca



Servicios

- Firewall

Sistema Operativo

Linux Red Hat

Marca

Dell PowerEdge 2800

Servicios

- Respaldos

Sistema Operativo

- Windows Server 2003

Marca

ÁREA ACADÉMICA

Servicios

- Controlador Principal de Dominio
- DHCP
- Servidor de Aplicaciones

Sistema Operativo

- Windows 2003 Estándar Edition en Español

Marca

Servicios

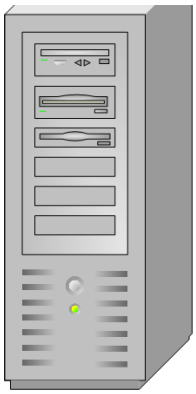
- WebAccess

Sistema Operativo

- Linux Red Hat 9.0

Marca

RED DMZ



Servicios

- Web

Sistema Operativo

- Linux Enterprise Server 4.0

Marca

Servicios

- Mail

Sistema Operativo

- Linux Red Hat 7.2

Marca

Figura 1.4. Sala de Servidores.
Elaborado por: Segundo Javier Cayo Molina

Para conocer de mejor forma como están conectados los servidores que dispone la Escuela Politécnica del Ejército Sede Latacunga vamos a observar el Anexo A.

1.3.3.1.2 Centro de Datos 8

El centro de datos 8 se encuentra ubicado junto al Centro de Producción, este centro de datos se enlaza con el centro de datos 1 mediante fibra óptica.

De este centro de datos se conectan las diferentes estaciones de trabajo que están en el centro de producción, también permite el enlace con el centro de datos 7.

Figura 1.5. Rack del Centro de Datos 8.
Elaborado por: Segundo Javier Cayo Molina

1.3.3.1.3 Centro de Datos de Servicios

El centro de datos de servicios se encuentra en la copiadora, este centro de datos para que se pueda enlazar con el centro de datos 1 debe realizar un puente con el centro de datos 4 que pertenece a los laboratorios de la Carrera de Ingeniería de Sistemas e Informática, este puente consiste en que desde el

centro de datos 1 se realiza un enlace mediante fibra óptica hasta el centro de datos 4 y luego se enlaza al centro de datos de servicios mediante cable UTP categoría 5e.

De este centro de datos se conectan los laboratorios de Idiomas, Laboratorio de Comunicaciones, Laboratorio de Instrumentación, Aula de Uso Múltiple y también para la oficina donde se encuentran las copiadoras de la Institución.

Hay que recalcar que este centro de datos, ya no estará a disposición en el lugar que se encuentra, ya que los directivos de la Escuela Politécnica del Ejército Sede Latacunga han visto conveniente realizar la construcción de un nuevo edificio en el lugar que se encuentra este centro de datos.

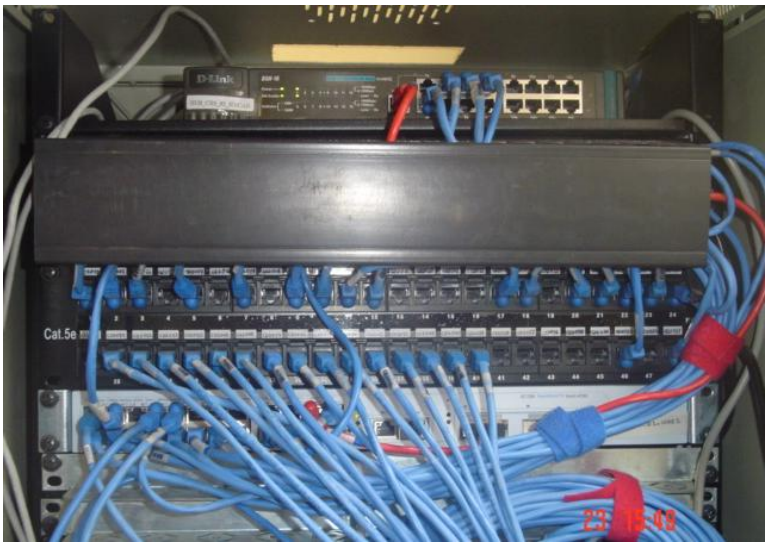


Figura 1.6. Rack del Centro de Datos de Servicios
Elaborado por: Segundo Javier Cayo Molina

1.3.3.1.4 CENTRO DE DATOS 7

El centro de datos 7 se encuentra en la biblioteca, para enlazarse con el centro de datos 1 tiene que realizarlo mediante cable par trenzado UTP categoría 5e al centro de datos 8.

Este centro de datos permite conectarse a la red a las diferentes estaciones de trabajo que se encuentran dentro de la biblioteca.

Figura 1.7. Rack del Centro de Datos 7.
Elaborado por: Segundo Javier Cayo Molina

1.3.3.1.5 Centro de Datos 4.

Este centro de datos se encuentra en jefatura de los laboratorios de la Carrera de Ingeniería de Sistemas e Informática, para enlazarse con el centro de datos 1 tiene que realizarlo mediante fibra óptica.

Este centro de datos permite conectarse a la red a los diferentes laboratorios que pertenecen a esta Facultad.

ÁREA ACADÉMICA DE LA FACULTAD DE SISTEMAS E INFORMÁTICA

Servicios

- Servidor de Backup de Dominio
- DHCP
- DNS
- Active Directory

Sistema Operativo

- Windows 2003 Estándar Edition en Español

Marca

Servicios

- Antivirus Kaspersky
- Estrategic
- SPS

Sistema Operativo

- Windows 2003 Estándar Edition en Español

Marca

Servidor Premio Pentium III

1.3.4 SOFTWARE DE RED

El software de red que se utiliza dentro la Escuela Politécnica del Ejército Sede Latacunga es el siguiente:

En la parte de la Red Administrativa se utiliza el siguiente software, los mismos que consumen los recursos de red:

- Antivirus Kaspersky
- Sistema Académico
- Base de Datos Sybase
- Sistema Financiero Olympo
- Base de Datos Oracle

También tenemos Múltiples Sistemas que se comparten desde carpetas para que los utilicen los usuarios que están autorizados.

- Rol de Pagos
- Sistema de La biblioteca Siabuc 8
- Sistema contable Olympo
- Sistema de Ingresos
- Sistema para análisis estadístico SPSS 13.0
- Record Académico Antiguo
- Sistema de Activos Fijos
- Sistemas de Ordenes de Pago
- Escolástico de Niños
- Sistema de Cursos
- Registro de Cursos

En la Red Académica en general el software que se utiliza es:

- Antivirus Kaspersky

En la Red Académica de la Facultad de Sistemas e Informática se utiliza el siguiente software:

- Antivirus Kaspersky
- Sistema de Análisis Estadístico SPSS 13.0
- Estrategic

También existe software que se va modificar como son:

- Sistema de Cursos
- Rol de Pagos

También existen los sistemas que están operativos vía web y son los siguientes:

- Strategic - Metodología de planificación estratégica
- Servicios Web del Portal de la Escuela Politécnica del Ejército Sede Latacunga
- Sistema de seguridades del sistema Web de la Escuela Politécnica del Ejército Sede Latacunga

1.4 CONCEPTO DE FLUJO DE TRÁFICO

Las redes de cómputo, se vuelven cada vez más complejas y la exigencia de una operación muy efectiva y correcta es cada vez más demandante. Las redes, cada vez mas, soportan aplicaciones y servicios estratégicos para las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor muy importante y de carácter pro-activo para evitar y dar solución a los

diferentes problemas que se presenten, y tener un correcto, eficaz servicio de red en la organización.

Es por esta razón que se ha visto que es muy necesario realizar el monitoreo de la red LAN de la Escuela Politécnica del Ejército Sede Latacunga, ya que después de realizar esto vamos a obtener varias ventajas que permitirán optimizar y mejorar el servicio de red que se ofrece en la actualidad. Por ende los usuarios de la red van estar satisfechos y se administrará de mejor forma los diferentes recursos de red.

1.5 ASPECTOS QUE INFLUYEN EN EL FLUJO DE TRÁFICO EN UNA RED LAN.

1.5.1 EL TAMAÑO FÍSICO DE LA RED.

El tamaño físico de la red hace referencia al número de puntos de red que se dispone en el sitio donde se ha implementado la red.

En la Escuela Politécnica del Ejército Sede Latacunga se dispone de 170 puntos de red aproximadamente, los mismos que se encuentra divididos entre las Áreas Administrativa, Académica, Académica de Sistemas, por ende van a permitir la comunicación entre las estaciones de trabajo, utilizar los diferentes servicios y recursos que dispone la red.

1.5.2 EL NÚMERO DE USUARIOS QUE ACCESAN A LA RED.

Al momento de monitorizar la red vamos a saber el número de usuarios que accesan en ese momento a la red, y en base a

eso vamos a poder analizar los diferentes protocolos y aplicaciones que utilizan cada uno de los clientes de la red LAN de la Escuela Politécnica del Ejército Sede Latacunga, por ende vamos a realizar el análisis respectivo que nos dará los resultados y así podremos optimizar el servicio de red en base a las soluciones que podamos brindar.

1.5.3 EL MEDIO FÍSICO DE COMUNICACIÓN.

Como ya se detalló anteriormente el medio físico de comunicación entre el rack principal y las diferentes estaciones de trabajo que dispone la Escuela Politécnica del Ejército Sede Latacunga es el cable par trenzado UTP categoría 5 y 5e.

Otro medio físico que dispone la Institución es la fibra óptica y se dispone de 2 enlaces, que permiten comunicarse entre los centros de datos.

1.5.4 LA VELOCIDAD Y LA TECNOLOGÍA DE LA RED.

La velocidad es muy importante en una red, ya que de esta depende la satisfacción de los clientes que se encuentran conectados a la red, es por eso que en la Escuela Politécnica del Ejército Sede Latacunga la velocidad de red es de 100 Mbps en la mayoría de las dependencias que se dispone.

Pero también hay que tomar en cuenta que existen equipos que trabajan a 10 Mbps pero son muy pocos, esto debido a que

los equipos tienen tarjetas de red que solo le permite trabajar a esa velocidad, pero poco a poco van ir desapareciendo ya la Unidad de Organización y Sistemas están adquiriendo equipos de última tecnología y contratando la certificación de cableado estructurado.

La tecnología que se utiliza es FastEthernet en las máquinas que trabajan a 100 Mbps y Ethernet en las máquinas que trabajan a 10 Mbps.

1.5.5 LOS PROTOCOLOS DE COMUNICACIÓN

Al momento de realizar el monitoreo de la red vamos a determinar los protocolos de comunicación que se utiliza en la Escuela Politécnica del Ejército Sede Latacunga, lo que permitirá que el análisis sea muy eficiente para determinar el estado de la red Lan.

CAPITULO II

METODOLOGÍA MIRA (METODOLOGÍA PARA LA INSPECCIÓN DE TRÁFICO EN REDES AVANZADAS).

2.1 INTRODUCCIÓN

Conocer el uso que se da a las redes es sumamente importante para el diseño y gestión de las mismas. El entorno de red actual, dominado por la arquitectura TCP/IP es muy dinámico y constantemente va creciendo. Aparecen nuevas aplicaciones día a día que no se restringen a los servicios básicos como web, correo electrónico o transferencia de ficheros, sino que traspasan al ámbito del comercio electrónico, los servicios multimedia, etc.

Los usuarios, a su vez, modifican sus hábitos (número y tipo de peticiones, duración de las sesiones) que ofrecen distintos niveles de calidad de servicio.

Esto ha supuesto un impacto importante en las redes de ámbito académico, a través de las cuales hoy en día se puede acceder a servicios no estrictamente académicos ni de investigación. Por consiguiente, las redes académicas deben adecuarse a políticas de uso aceptable, que impidan que dichas redes supongan una competencia desleal con las redes comerciales, es por eso que es muy necesario realizar la monitorización del tráfico que pasa por la red.

2.2 METODOLOGÍA MIRA

La Metodología MIRA **(Metodología para la Inspección de tráfico en Redes Avanzadas)** es fruto de la evolución de distintos proyectos orientados al análisis y caracterización de tráfico. En esta metodología se integran distintos métodos de análisis de tráfico, basados en parámetros derivados de las cabeceras de los paquetes a distintos niveles, así como parámetros derivados del análisis de contenidos. Se desarrollan nuevos mecanismos que nos permitirán analizar el comportamiento de las redes con topología compleja y preveer sus tendencias.

MIRA es una metodología 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, entre algunas de la utilidades que presta esta metodología. Además, es muy versátil

y soporta distintas tecnologías de red, entre las más importantes tenemos Ethernet.

2.3 ARQUITECTURA FUNCIONAL DE LA METODOLOGÍA MIRA

La arquitectura funcional de MIRA consta de varios módulos, que trabajan en cascada, como se aprecia en la Figura 2.1.
Cada uno de los módulos a su vez se implementa en uno o varios procesos. Como interfaz de comunicación entre procesos se utilizan ficheros, periódicamente escritos y leídos, con un formato predefinido.

Existen mecanismos de sincronización y control de flujo para la comunicación entre procesos.

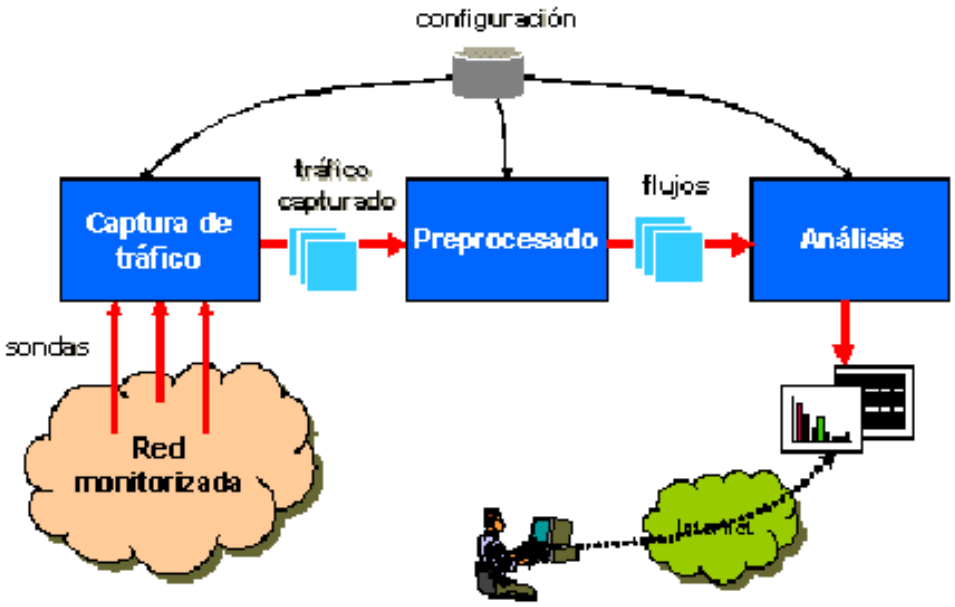


Figura 2.1. Arquitectura de la Metodología MIRA.

Fuente: www.dit.upm.es

Es de destacar el enfoque modular de la metodología, el cual, junto con la posibilidad de configurar cada uno de los módulos independientemente, la dota de una gran flexibilidad. A continuación se describen cada uno de los módulos y sus funcionalidades más destacadas.

2.3.1 MÓDULO DE CAPTURA

El objetivo de este módulo es realizar la captura de tráfico sobre la red que queremos monitorizar.

Para capturar el tráfico se lo realiza mediante el uso de un software de captura específicamente adaptado a la tecnología de enlace de la red monitorizada.

La captura de tráfico se realiza de forma no intrusiva, esto quiere decir que no haya pérdida de eficiencia para la red que se va monitorizar.
En la actualidad existe software que permite capturar tráfico en una red, lo cual muestra la aplicabilidad de MIRA tanto a redes de área extensa (WAN) como redes de área local (LAN). En el nivel de red, para IPV4.

El resultado de este módulo es un conjunto de ficheros con trazas del tráfico capturado que se proporcionan al módulo de preprocesado como entrada. Esto se lo realizará de acuerdo a los resultados que arroje la captura del tráfico en la red, es decir si las trazas de tráfico son las necesarias para un correcto análisis, el administrador optará por pasar al siguiente módulo que se detalla en la metodología.

Es recomendable realizar la captura de tráfico en horas en las cuales se trabaje en la mayoría de los puntos que se encuentran conectados a la red, ya que de esa forma se podrá obtener información más eficiente para el análisis de la red, de esta forma se podrá conocer los verdaderos problemas y la situación en la que se encuentra la red Lan. Si la carga de tráfico que cursa la red monitorizada es baja, es posible llegar a capturar todo el tráfico. En todo caso, los módulos de postprocesado de MIRA pueden realizar interpolaciones para extender las conclusiones obtenidas del análisis del tráfico capturado.

2.3.2 MÓDULO DE PREPROCESADO

El objetivo del preprocesado es reducir el volumen de datos de los paquetes capturados en el módulo anterior, es decir no se tomará en cuenta el tráfico innecesario, y se extraerá de los paquetes sólo lo que es más relevante como puede ser direcciones IP, puertos de transporte, en el caso de que el volumen del tráfico capturado sea muy elevado. El agotamiento del espacio de almacenamiento y la necesidad legal de preservar la confidencialidad de las comunicaciones obligan a

ello. Cada fichero de captura es procesado paquete a paquete, extrayendo los parámetros relevantes. El resto es eliminado. El preprocesado se realiza en cuatro etapas, como se muestra en la Figura 2.2.

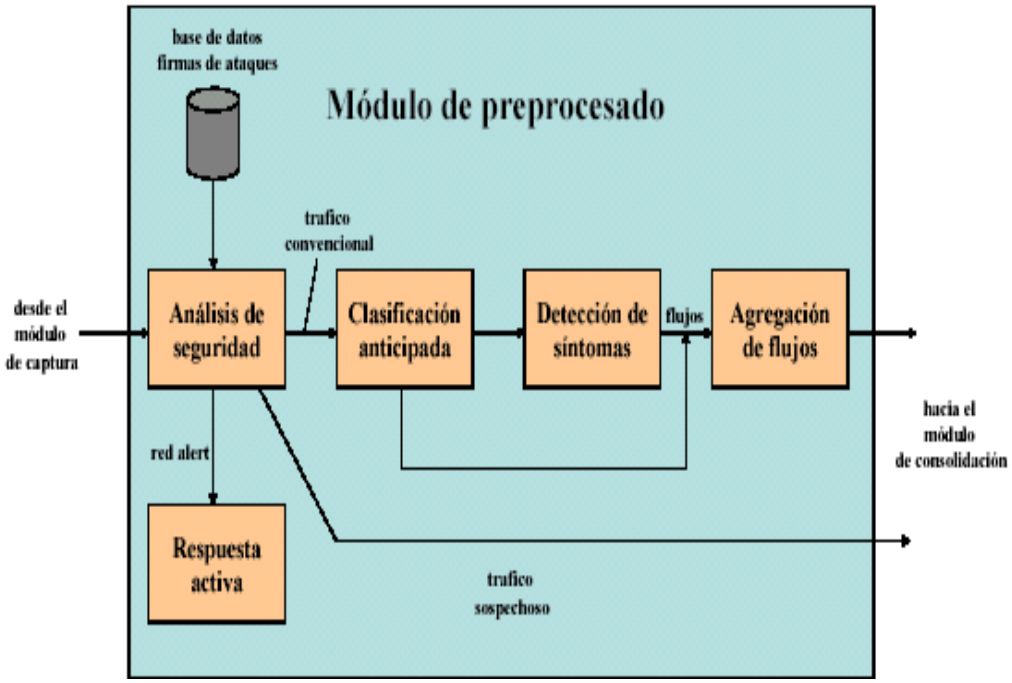


Figura 2.2. Estructura del Módulo de Preprocesado.
Fuente: www.dit.upm.es

Primera Etapa.- En la primera etapa se realiza un análisis de seguridad, que separa el tráfico capturado en dos categorías: convencional y sospechoso, esto permitirá que no se den incidentes de seguridad, lo cuál es muy beneficioso para la red que se va monitorizar.

- **Trafico Convencional.-** Se conoce como tráfico convencional, aquel tráfico de red que no representa peligro alguno al buen funcionamiento de nuestra red, es decir que los diferentes paquetes que circulan por toda la red cumplen el objetivo para el que fueron enviados desde una computadora hacia otra, por ejemplo para establecer la comunicación entre las estaciones de trabajo, la transferencia de archivos, entre otros. Es por eso que si el tráfico es convencional la red será rápida, eficaz y permitirá que los usuarios trabajen de mejor forma.

- **Tráfico Sospechoso.-** Se conoce como tráfico sospechoso, aquel tráfico de red que representa peligro a la red y por ende no permite un correcto funcionamiento, esto produce inconformidad en los diferentes usuarios de las estaciones de trabajo, un claro ejemplo de tráfico sospechoso es la presencia de intrusos, si se detecta presencia de un virus, etc. También se considera como tráfico sospechoso a los diferentes protocolos que son innecesarios para el funcionamiento de la red, estos protocolos se detectan al momento de monitorear la red con la ayuda de un analizador de red.

Segunda Etapa.- En esta etapa el tráfico convencional sufre un proceso de clasificación anticipada, cuyo objetivo es clasificar el tráfico directamente (basándose en direcciones IP y puertos TCP/UDP), evitando la búsqueda de patrones para parte del tráfico de red.

Tercera Etapa.- Posteriormente, se realiza una detección de síntomas mediante búsqueda de patrones en el contenido del paquete. Un síntoma es un indicio significativo en el paquete donde se ha detectado (por ejemplo, síntoma MUSICA, identificando la presencia de contenidos en el paquete relacionados con la música).

2.3.3 MÓDULO DE CONSOLIDACIÓN

Puesto que la metodología MIRA permite la utilización de un conjunto de sondas de captura-preprocesado trabajando concurrentemente, es necesario realizar la consolidación de los resultados parciales de todas ellas.

Además de realizar la consolidación, este módulo realiza también correlación de flujos bidireccionales (dos flujos unidireccionales se consideran correlacionados si existe una relación recíproca entre sus direcciones IP y puerto TCP/UDP origen y destino). La correlación aumenta la precisión del módulo de clasificación que viene a continuación, ya que en ocasiones los síntomas solo aparecen en una dirección.

2.3.4 MÓDULO DE CLASIFICACIÓN

Este módulo clasifica el tráfico (excepto aquel que ya lo haya sido durante el preprocesado) en categorías de uso definidas de antemano conforme a la política de uso aceptable del operador de la red monitorizada (por ejemplo, tráfico académico, comercial, lúdico e indeterminado).

La clasificación se da tomando en cuenta una ponderación de los síntomas presentes en el flujo, la ponderación es de acuerdo al tipo de tráfico que más afecta a la red que se monitorea, así como también la presencia de puertos TCP/UDP característicos. Así, por ejemplo, un flujo en el que haya 4 síntomas de tipo lúdico y 1 de tipo comercial puede ser clasificado como lúdico (mayoría).

2.3.5 MÓDULO DE POSTPROCESADO

Tras la clasificación, se pueden realizar distintos análisis sobre los resultados, que pueden ser desarrollados a modo de extensión de la metodología. El resultado de realizar el análisis y tratamiento de la información proporcionada por el preprocesado, es generar un conjunto de informes en la forma de gráficos, tablas, estadísticas, etc, esto va ser de mucha

utilidad para el usuario de la metodología, ya que es el punto de partida para empezar a realizar los correctivos en la red monitorizada, y así dar un eficaz servicio de red.

Por ejemplo, es posible mostrar la distribución (porcentajes) del tráfico clasificado durante un período de tiempo un día una semana o mes, por ejemplo, esto lo determinará la persona que va realizar el monitoreo de la red, de acuerdo a los resultados que se obtenga ya que en un día no todos los usuarios de la red van a utilizar los servicios de red y no se podrá saber cuál es el verdadero estado en el que se encuentra la red monitorizada.

2.3.6 ARQUITECTURA DISTRIBUIDA

La arquitectura modular de MIRA dota de una gran flexibilidad y escalabilidad a la metodología, permitiendo distribuir los distintos módulos (y los procesos de los que constan) en equipos físicos independientes.

Esta característica puede utilizarse para distribuir la carga de proceso en un conjunto de equipos físicos, para aumentar las tasas de captura (a base de replicar módulos de captura en un mismo punto) o para estudiar redes de gran cobertura. En este último caso, el modelo consiste en utilizar un conjunto de

sondas situadas en distintos puntos de la red, para que los resultados sean los que se requieren se debe situar las sondas en puntos que sean más críticos de la red que se va monitorear, al realizar esto los resultados se consolidan en un punto central para ofrecer un análisis homogéneo del tráfico cursado, tal y como se muestra en la Figura 2.3.

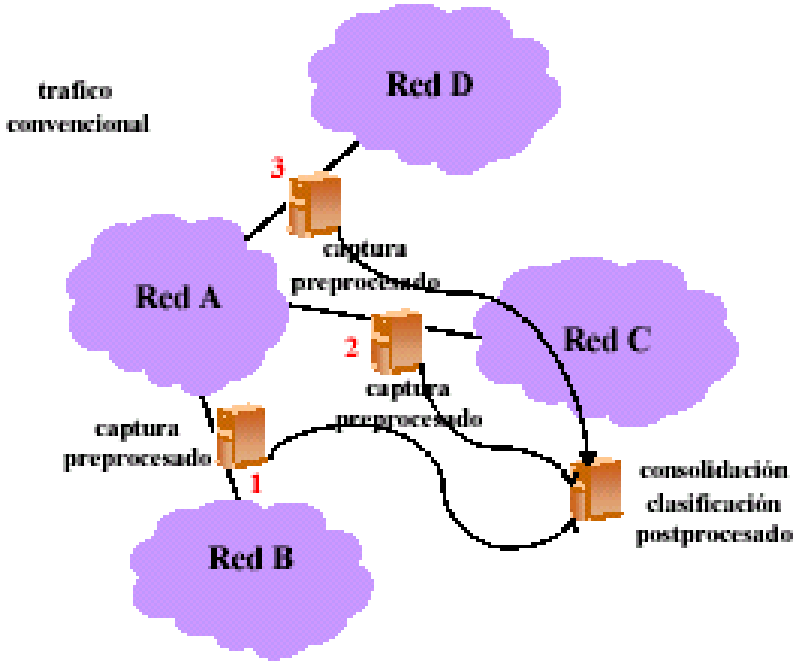


Figura 2.3. Despliegue Distribuido de la Metodología MIRA.
Fuente: www.dit.upm.es

2.4 CARACTERÍSTICAS AVANZADAS DE LA METODOLOGÍA MIRA

La metodología MIRA incorpora una serie de características novedosas, donde se encuentra la verdadera aportación en el campo

de lo que se refiere a la monitorización de redes, que vamos a describir a continuación.

2.4.1 ANÁLISIS DE CONTENIDOS

Si bien la metodología MIRA es capaz de realizar análisis convencionales basados en parámetros de la cabecera de los paquetes IP (como direcciones y puertos TCP/UDP) durante el postprocesado, resulta más interesante el análisis de contenidos de paquete que se realiza para extraer síntomas en los flujos de tráfico.

El registro de concurrencias de cada síntoma es utilizado por el módulo de clasificación para dar un veredicto sobre la categoría de tráfico a la que pertenece el flujo, basándose en ponderación de síntomas. Para ello es necesario asociar cada síntoma a una categoría de tráfico (por ejemplo puede ser, MUSICA, JUEGOS estos podrían ser lúdicos).

Básicamente la clasificación compara la cantidad de síntomas de cada tipo y decide (si la suma de los síntomas de tipo lúdico es mayor que las de tipo comercial, o el tipo de tráfico que este pasando por la red en ese instante).

La inspección de contenidos permite caracterizar de manera más fiable el tráfico que realmente está cursando la red, sin limitarse a estudiar los aspectos formales relacionados con la información que aparece en las cabeceras.

Para entender de mejor forma el análisis de contenidos tenemos un ejemplo, si se especifica que un paquete que se ha

capturado es MUSICA y este consta de dos patrones que son: “music” y “jazz”, o, dicho de otro modo, que si se detecta la palabra “music” o “jazz” en un contenido del paquete, el flujo al que pertenezca será marcado como MUSICA.

Otro ejemplo tenemos que si un flujo consta de tres paquetes, uno de ellos que contiene MUSICA, otro JUEGO y otro de MUSICA, la conclusión será que el flujo contiene 2 paquetes de MUSICA, y 1 paquete de JUEGO.

2.4.2 DETECCIÓN DE TRÁFICO LÚDICO

Debido a la creciente tendencia de utilizar Internet como una gran red de intercambio de información, la mayor parte de usuarios en la actualidad la utilizan con fines lúdicos, por ejemplo páginas de grupos musicales, consulta de resultados deportivos, páginas de juegos y todas aquellas páginas que utilizan gran parte del ancho de banda de la red monitorizada. Es por eso que surge la necesidad de desarrollar técnicas que permitan detectar este tipo de tráfico en la red monitorizada mediante la metodología MIRA. Estas transmisiones pueden llegar a utilizar un porcentaje significativo del ancho de banda en las redes de los operadores, lo cual justifica la utilización de plataformas como MIRA para medir y controlar su impacto, especialmente si la transmisión de tales contenidos va en contra de la política de uso aceptable de la red.

Por ejemplo, dentro de la metodología MIRA se han desarrollado técnicas especiales para la detección del tráfico

de contenidos MP3, uno de los formatos de codificación de audio comprimido más populares del momento en Internet.

Para detectar si un determinado flujo se corresponde con la transmisión de MP3, se utiliza el análisis de contenidos que realiza MIRA, definiendo una serie de patrones bajo el síntoma MP3. Podríamos basar esos patrones en las palabras claves que utilizan los protocolos de intercambio de ficheros P2P (eDonkey, KaZaA, Gnutella). No obstante, no es la mejor alternativa, ya que obliga a estudiar muchos sistemas distintos y además la utilización de estos protocolos es demasiado inestable como para basar los patrones en ellos.
Por tanto, resulta más adecuado realizar inspección de contenidos basada en el propio formato MP3. El audio está estructurado en tramas, con cabecera y carga útil, como podemos observar en la figura 2.4.

Precisamente el análisis de contenidos es la clave que ha permitido dotar a la plataforma de dos novedosas funcionalidades: la detección de contenidos de tipo lúdico como es el audio MP3 y la detección de incidentes de seguridad (ya sea en modo pasivo o con la posibilidad de respuestas activas en tiempo real).

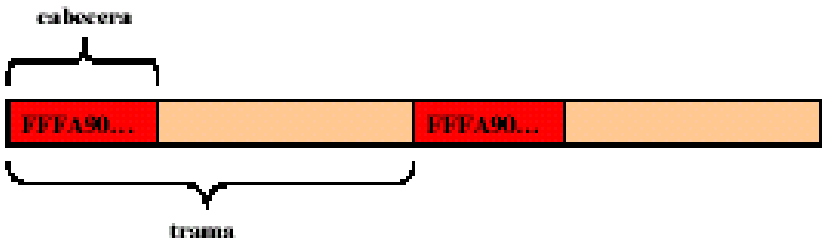


Figura 2.4 Estructura de una trama MP3

Fuente: www.dit.upm.es

2.4.3 DETECCIÓN DE ATAQUES DE SEGURIDAD

Para realizar el monitoreo de la red hay que tomar en cuenta que toda institución dispone de Internet y es un entorno potencialmente inseguro, donde existen amenazas de seguridad para los equipos que a ella se conectan.

Los ataques utilizan la red, generando un tráfico que en ocasiones puede ser detectado e identificado como peligroso.

MIRA incorpora funciones especializadas en la detección del tráfico sospechoso, involucrado en la realización de ataques o incidencias de seguridad de algún tipo las cuales se utilizan en la primera etapa del preprocesado para separar este tráfico sospechoso del tráfico convencional.

En la figura 2.2. que se mostró anteriormente, se incluyen todos los elementos de la arquitectura que intervienen en la provisión de las funciones de seguridad. Obsérvese que es necesario realizar este preprocesado al principio, ya que posteriores etapas eliminan el paquete capturado y con ello la posibilidad de detectar tráfico sospechoso.

El analizador encargado de realizar el análisis de seguridad en el tráfico capturado es un recubrimiento de la herramienta NIDS (Network Intrusión Detection System, Sistema de Detección de Intrusiones de Red) de libre distribución Snort. En muchos

aspectos, este analizador es similar al ya descrito analizador de contenidos de la metodología MIRA que se encarga de la búsqueda de patrones, pero hay dos diferencias fundamentales.

En primer lugar, realiza un análisis basado en estados que le permite detectar ataques que involucran un conjunto paquetes IP.

En segundo lugar, la detección de tráfico sospechoso está basada en firmas. Las firmas nos permiten diferenciar entre todo el tráfico generado por la redes y obtener un subconjunto de este lo suficientemente pequeño como para que sea tratable y lo suficientemente amplio como para poder detectar comportamientos anómalos de la red en tiempo real.

Aparte de estas acciones en tiempo real, el subsistema de seguridad proporciona como salida las trazas de tráfico sospechoso capturado, con lo que pueden ser analizadas con herramientas como Ethereal para investigar el ataque que se está realizando

2.4.4 ESTADÍSTICAS CONVENCIONALES

Como parte del trabajo que permite realizar la metodología MIRA se encuentra la implementación de funciones para la generación de estadísticas convencionales. La denominación convencionales obedece a

que son del tipo que se obtiene con analizadores de protocolos típicos, que se basan en la inspección de las cabeceras de los paquetes (a nivel IP y de transporte), a diferencia del punto fuerte de MIRA, que es la clasificación de tráfico a través de la inspección del contenido de dichos paquetes.

Las estadísticas convencionales se dividen en dos niveles como podemos observar en la figura 2.5.

Estadísticas a bajo nivel**.- Se conoce como estadísticas de bajo nivel, aquellas que muestran el tráfico de red cursado por cada puerto TCP y UDP.**

Estadísticas a alto nivel.- **Estas estadísticas son las que muestran el tráfico cursado por aplicaciones y por grupos de aplicaciones. Es necesario relacionar la información a bajo nivel con la información a alto nivel,**

para que las estadísticas sean muy eficientes.

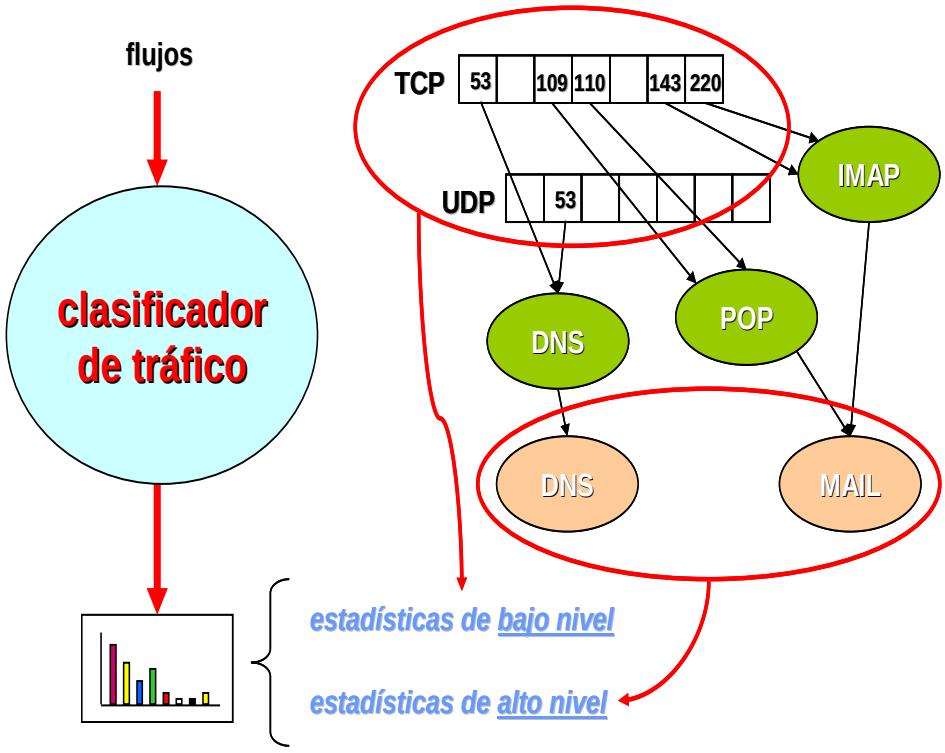


Figura 2.5 Módulo de las estadísticas convencionales.
Fuente: www.dit.upm.es

Por lo tanto, las estadísticas de alto nivel sirven para analizar el tráfico clasificado al momento de monitorear la red, mientras que las estadísticas de bajo nivel sirven para verificar la corrección de las anteriores (si por ejemplo

como resultado de un informe de bajo nivel un puerto no utilizado hasta entonces empieza a cursar gran volumen de tráfico, será necesario revisar la asociación de aplicaciones y grupos de aplicación, pues es probable que haya aparecido una nueva).

Es por eso que son muy importantes las estadísticas, ya que en base a estas se darán las conclusiones, y de esto dependerá los cambios que se deben implementar en la red monitorizada, para mejorar la calidad de servicio, en consecuencia los usuarios trabajaran de forma más eficaz.

CAPÍTULO III

ANÁLISIS DEL FLUJO DE TRÁFICO DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA.

3.1 INTRODUCCIÓN

En este capítulo se realizará el análisis del flujo de tráfico de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, para esto se tendrá como guía fundamental la metodología MIRA, aquí se aplicará cada uno de los módulos de la metodología que se detallaron en el capítulo anterior.

Al realizar el análisis del flujo de tráfico de la red Lan, vamos a conocer los paquetes que circulan por la red, al momento que utilizan las diferentes aplicaciones que dispone la Escuela Politécnica del Ejército Sede Latacunga, tanto en el área Administrativa como en el área Académica, al realizar el análisis del flujo de tráfico se determinará el porcentaje del ancho de banda que se consume y se determinará el estado en el que se encuentra la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, de este análisis se obtendrá varias conclusiones, las mismas que nos servirá para resolver problemas concretos o bien para optimizar la utilización de la red, mejorando la calidad y servicio que se presta actualmente en las diferentes dependencias de la Escuela Politécnica del Ejército Sede Latacunga, por ende esto beneficiará a todos los usuarios de la red.

Antes de iniciar con el análisis del flujo de tráfico de la red Lan debemos involucrarnos con lo que se refiere a los protocolos de red, esto nos ayudará a tener una idea clara de las diferentes reglas y procedimientos que se utilizan en una red para comunicarse entre las diferentes estaciones de trabajo y el servidor.

3.2 PROTOCOLOS DE RED

Protocolo de red es un conjunto de normas, reglas y procedimientos que regulan la comunicación (establecer, mantener y cancelar) entre los distintos componentes de una red.
Los protocolos gobiernan dos niveles de comunicaciones:

- **Los protocolos de alto nivel.-** Estos protocolos definen la forma en que se comunican las diferentes aplicaciones.

- **Los protocolos de bajo nivel.-** Estos protocolos son aquellos que controlan la f0orma en que las señales se transmiten por el cable o medio físico. Habitualmente utilizados en redes locales (Ethernet y Token Ring).

El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red (NIC) y salgan al cable de la red.

Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos se corresponden con los niveles del modelo OSI. Por ejemplo, el nivel de aplicación del protocolo TCP/IP se corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

3.2.1 CÓMO FUNCIONAN LOS PROTOCOLOS

La operación técnica en la que los datos son transmitidos a través de la red se puede dividir en dos pasos.
Cada paso incluye sus propias reglas y procedimientos.
Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y que sea el mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se tienen que llevar a cabo de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que llevar a cabo de abajo hacia arriba.

El equipo origen

Los protocolos en el equipo origen:

1.- Se dividen en secciones más pequeñas, denominadas paquetes.

2.- Se añade a los paquetes información sobre la dirección, de forma que el equipo de destino pueda determinar si los datos le pertenecen.

3.- Prepara los datos para transmitirlos a través de la NIC y enviarlos a través del cable de la red.

El equipo de destino

Los protocolos en el equipo de destino constan de la misma serie de pasos, pero en sentido inverso.

1.- Toma los paquetes de datos del cable y los introduce en el equipo a través de la NIC.

2.- Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.

Los equipos origen y destino necesitan realizar cada paso de la misma forma para que los datos tengan la misma estructura al momento que se recibe de la estación de trabajo que se envió.

A continuación se detalla los diferentes tipos de protocolos de red:

3.2.2 PROTOCOLOS DE APLICACIÓN

Los protocolos de aplicación trabajan en el nivel superior del modelo de referencia OSI y proporcionan interacción entre aplicaciones e intercambio de datos.

- **SMTP (Protocolo básico para la transferencia de correo).-** Un protocolo Internet para las transferencias de correo electrónico.

- **SNMP (Protocolo básico de gestión de red).-** Un protocolo de Internet para el control de redes y componentes.
- **Telnet.-** Un protocolo de Internet para la conexión a máquinas remotas y procesar los datos localmente.
- **SMBs (Bloques de mensajes del servidor) de Microsoft y clientes o redirectores.-** Un protocolo cliente/servidor de respuesta a peticiones.
- **NCP (Protocolo básico de NetWare) *y* clientes o redirectores.-** Un conjunto de protocolos de servicio.
- **AppleTalk *y* AppleShare.-** Conjunto de protocolos de red de Apple.
- **AFP (Protocolo de archivos AppleTalk).-** Protocolo de Apple para el acceso a archivos remotos.
- **DAP (Protocolo de acceso a datos).-** Un protocolo de DECnet para el acceso a archivos.

3.2.3 PROTOCOLOS DE TRANSPORTE

Los protocolos de transporte facilitan las sesiones de comunicación entre equipos y aseguran que los datos se pueden mover con seguridad entre equipos.

- **TCP.-** El protocolo de TCP/IP para la entrega garantizada de datos en forma de paquetes secuenciados.
- **SPX.-** Parte del conjunto de protocolos IPX/SPX de Novell para datos en forma de paquetes secuenciados.
- **NWLink.-** La implementación de Microsoft del protocolo IPX/SPX.

- **NetBEUI (Interfaz de usuario ampliada NetBIOS).-** Establece sesiones de comunicación entre equipos (NetBIOS) y proporciona los servicios de transporte de datos subyacentes (NetBEUI).
- **ATP (Protocolo de transacciones Apple Talk) y NBP (Protocolo de asignación de nombres).-** Protocolos de Apple de sesión de comunicación y de transporte de datos.

3.2.4 PROTOCOLOS DE RED

Los protocolos de red proporcionan lo que se denominan servicios de enlace. Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

- **IP.-** Internet Protocol es el protocolo principal de TCP/IP, es el encargado de la transmisión y enrutamiento de los paquetes de datos al equipo destino.
  Es un protocolo no fiable, esto quiere decir que no garantiza la recepción final en el equipo destinatario de la información. Para el control de los posibles errores dispone de un protocolo de aviso que es el ICMP.

  Cuando se transmite un paquete, este protocolo añade una cabecera al paquete, de forma que pueda enviarse a través de la red utilizando las tablas de encaminamiento dinámico. IP es un protocolo no orientado a la conexión y envía paquetes sin esperar la

señal de confirmación por parte del receptor. Además, IP es el responsable del empaquetado y división de los paquetes requeridos por los niveles físico y de enlace de datos del modelo OSI. Cada paquete IP está compuesto por una dirección de origen y una de destino, un identificador de protocolo, un checksum (un valor calculado) y un TTL (tiempo de vida, time to live*).* El TTL indica a cada uno de los routers de la red entre el origen y el destino cuánto tiempo le queda al paquete por estar en la red. Funciona como un contador o reloj de cuenta atrás. Cuando el paquete pasa por el router, éste reduce el valor en una unidad (un segundo) o el tiempo que llevaba esperando para ser entregado.

El ICMP.- Este protocolo es utilizado por los protocolos IP y superiores para enviar y recibir informes de estado sobre la información que se está transmitiendo. Los routers suelen utilizar ICMP para controlar el flujo, o velocidad, de datos entre ellos. Si el flujo de datos es demasiado rápido para un router, pide a los otros routers que reduzcan la velocidad de transmisión.

Los dos tipos básicos de mensajes ICMP son el de informar de errores y el de enviar preguntas.

- **IPX.-** El protocolo de Novell para el encaminamiento de paquetes.
- **NWLink.-** La implementación de Microsoft del protocolo IPX/SPX.
- **NetBEUI.-** Un protocolo de transporte que proporciona servicios de transporte de datos para sesiones y aplicaciones NetBIOS.
- **DDP (Protocolo de entrega de datagramas).-** Un protocolo de Apple Talk para el transporte de datos.

3.2.5 LOS PROTOCOLOS DE IEEE A NIVEL FÍSICO

- **802.3 (Ethernet)**.- Es una red lógica en bus que puede transmitir datos a 10 Mbps. Los datos se transmiten en la red a todos los equipos. Sólo los equipos que tenían que recibir los datos informan de la transmisión. El protocolo de acceso de múltiple con detección de portadora con detección de colisiones (CSMA/CD) regula el tráfico de la red permitiendo la transmisión sólo cuando la red esté despejada y no haya otro equipo transmitiendo.

- **802.4 (Token Bus)**.- Es una red en bus que utiliza un esquema de paso de testigo. Cada equipo recibe todos los datos, pero sólo los equipos en los que coincida la dirección responderán. Un testigo que viaja por la red determina quién es el equipo que tiene que informar.

- **802.5 (Token Ring)**. Es un anillo lógico que transmite a 4 ó a 16 Mbps. Aunque se le llama en anillo, está montada como una estrella ya que cada equipo está conectado a un hub. Realmente, el anillo está dentro del hub. Un token a través del anillo determina qué equipo puede enviar datos.

El IEEE definió estos protocolos para facilitar la comunicación en el subnivel de Control de acceso al medio (MAC).

Un controlador MAC está situado en el subnivel de Control de acceso al medio; este controlador de dispositivo es conocido como controlador de la NIC. Proporciona acceso a bajo nivel a los adaptadores de red para proporcionar soporte en la transmisión de datos y algunas funciones básicas de control del adaptador.

Un protocolo MAC determina qué equipo puede utilizar el cable de red cuando varios equipos intenten utilizarlo simultáneamente. CSMA/CD, el protocolo 802.3, permite a los equipos transmitir datos cuando no hay otro equipo transmitiendo. Si dos máquinas transmiten simultáneamente se produce una colisión. El protocolo detecta la colisión y detiene toda transmisión hasta que se libera el cable. Entonces, cada equipo puede volver a tratar de transmitir después de esperar un período de tiempo aleatorio.

3.2.6 PROTOCOLO TCP/IP

El Protocolo de control de transmisión/Protocolo Internet (TCP/IP) es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes). Además, TCP/IP proporciona un protocolo de red encaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad,

TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como interconexión de redes, la intercomunicación en una red que está formada por redes más pequeñas.

TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP. La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el encaminamiento y se suele utilizar como un protocolo de interconexión de redes.

Entre otros protocolos escritos específicamente para el conjunto TCP/IP se incluyen:

- **SMTP** (Protocolo básico de transferencia de correo). Correo electrónico.
- **FTP** (Protocolo de transferencia de archivos). Para la interconexión de archivos entre equipos que ejecutan TCP/IP.

Históricamente, TCP/IP ha tenido dos grandes inconvenientes: su tamaño y su velocidad. TCP/IP es una jerarquía de protocolos relativamente grandes que puede causar problemas en clientes basados en MS-DOS. En cambio, debido a los requerimientos del sistema (velocidad de procesador y memoria) que imponen los sistemas operativos con interfaz gráfica de usuario (GUI), como Windows NT o Windows 95 y 98, el tamaño no es un problema.

3.2.7 PROTOCOLO ARP

Antes de enviar un paquete IP a otro host se tiene que conocer la dirección hardware de la máquina receptora. El ARP determina la dirección hardware (dirección MAC) que corresponde a una dirección IP. Si ARP no contiene la dirección en su propia caché, envía una petición por toda la red solicitando la dirección. Todos los hosts de la red procesan la petición y si contienen un valor para esa dirección, lo devuelven al solicitante. A continuación se envía el paquete a su destino y se guarda la información de la nueva dirección en la caché del router.

Los mensajes ARP van a ser encapsulados directamente en una trama Ethernet. En el campo tipo de la cabecera de la trama Ethernet es necesario especificar que contiene un mensaje ARP. El emisor se debe encargar de poner el valor correspondiente y el receptor de mirar el contenido de ese campo. Como Ethernet asigna un único valor para los dos mensajes ARP, el receptor debe examinar el campo operación del mensaje ARP para determinar si es el mensaje recibido es una petición o una respuesta.

3.2.8 PROTOCOLO RARP

Un servidor RARP mantiene una base de datos de números de máquina en la forma de una tabla (o caché) ARP que está creada por el administrador del sistema. A diferencia de ARP, el protocolo RARP proporciona una dirección IP a una petición con dirección de hardware. Cuando el servidor RARP recibe una petición de un número IP desde un nodo de la red, responde comprobando su tabla de encaminamiento para el

número de máquina del nodo que realiza la petición y devuelve la dirección IP al nodo que realizó la petición.

3.2.9 PROTOCOLO UDP

El User Datagram Protocol, es un protocolo muy sencillo, no orientado a conexión, por lo que son los protocolos de nivel superior los que deben asegurarse de la recepción de los datos. Este protocolo es del tipo best-effort (máximo esfuerzo), porque hace lo que puede para transmitir los datagramas hacia la aplicación, pero no puede garantizar que la aplicación los reciba.

Tampoco utiliza mecanismos de detección de errores. Cuando se detecta un error en un datagrama, en lugar de entregarlo a la aplicación destino, se descarta. Cuando una aplicación envía datos a través de UDP, éstos llegan al otro extremo como una unidad. Por ejemplo, si una aplicación escribe 5 veces en el puerto UDP, la aplicación al otro extremo hará 5 lecturas del puerto UDP. Además, el tamaño de cada escritura será igual que el tamaño de las lecturas. El protocolo UDP es empleado principalmente en aplicaciones multimedia, para el envío de flujos de información sin un coste de conexión asociado.

3.2.10 PROTOCOLO DNS

El protocolo de Sistema de nombres de dominios "DNS Domain Name System". Se encuentra en el grupo de protocolos TCP-

IP, los protocolos de resolución de nombres por direcciones IP. Estos protocolos permiten a las aplicaciones tener acceso a los servicios de un computador a través del uso de un nombre. Para ello debe existir un mecanismo que permita la resolución y asociación de una dirección IP por un nombre. El mecanismo de asociación consiste en una base de datos donde se encuentran las asociaciones de una dirección IP con su nombre respectivo. Y el mecanismo de resolución consiste en identificar cual es la dirección IP asociada a un nombre. De esta manera los computadores de la red pueden ser accesados a través de un nombre en vez de su dirección IP.

El protocolo DNS trabaja en la capa de aplicación. Si el segmento a enviar es menor que 512 Bytes utiliza el protocolo UDP, de lo contrario utiliza el protocolo TCP. El número de puerto que utiliza el protocolo DNS para comunicarse con la capa de aplicación es el número 53.

El protocolo DNS está compuesto por dos programas uno llamado servidor de nombres de dominios y otro llamado resolvers. Los servidores de nombres de dominios contienen la base de datos de un segmento y dicha base de datos es accesada por los clientes a través de un programa conocido como resolvers. Los resolvers son rutinas utilizadas para tener acceso a la base de datos ubicada en los servidores de nombres de dominios con el fin de resolver la búsqueda de una dirección IP asociada a un nombre.

3.2.11 CDP (CISCO DISCOVERY PROTOCOL, 'PROTOCOLO DE DESCUBRIMIENTO DE CISCO')

CDP es un protocolo de red propietario de nivel 2 desarrollado por Cisco Systems que corre la mayoría de los equipos Cisco y se utiliza para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP. CDP también puede ser usado para realizar encaminamiento bajo demanda (ODR, On-Demand Routing), que es un método para incluir información de encaminamiento en anuncios CDP, de forma que los protocolos de encaminamiento dinámico no necesiten ser usados en redes simples.

Los dispositivos Cisco envían anuncios a la dirección de destino de multidifusión 01:00:0C:CC:CC:CC (que también es usada por otros protocolos propietarios de Cisco tales como VTP). Los anuncios CDP (si están soportados y configurados en el IOS) se envían por defecto cada 60 segundos en las interfaces que soportan cabeceras SNAP, incluyendo Ethernet, Frame Relay y ATM. Cada dispositivo Cisco que soporta CDP almacena la información recibida de otros dispositivos en una tabla que puede consultarse usando el comando show cdp neighbor. La información de la tabla CDP se refresca cada vez que se recibe un anuncio y la información de un dispositivo se descarta tras tres anuncios no recibidos por su parte (tras 180 segundos usando el intervalo de anuncio por defecto).

La información contenida en los anuncios CDP varía con el tipo de dispositivo y la versión del sistema operativo que corra. Dicha información incluye la versión del sistema operativo, el nombre de equipo, todas la direcciones de todos los protocolos configurados en el puerto al que se envía la trama CDP (por

ejemplo, la dirección IP), el identificador del puerto desde el que se envía el anuncio, el tipo y modelo de dispositivo, la configuración duplex/simplex, el dominio VTP, la VLAN nativa, el consumo energético (para dispositivos PoE) y demás información específica del dispositivo.

3.2.12 PROTOCOLO HTTP

En la red, la Web utiliza el protocolo HTTP o HyperText Transfer Protocol, el Protocolo de Transferencia de Hipertexto que permite el intercambio de información hipertextual de las páginas Web y que ha sido utilizado por los servidores World Wide Web desde su inicio en 1990. Es un protocolo que permite la transferencia de archivos y documentos en múltiples plataformas. Fue inventado para que los ordenadores se comunicaran mientras intercambiaban documentos, agregando conectividad e interfaces. Si un ordenador usa el protocolo HTTP y pide un archivo a otro ordenador, éste último sabrá, al recibirlo, si se trata de imagen, vídeo, texto, etc. Esta funcionalidad que se agregó a HTTP permite que Internet sea hipermedia a través de la Web. Bajo la interfaz de usuario, representada por los navegadores, se encuentran los protocolos.

3.2.13 PROTOCOLO STP

El Spanning Tree Protocol es un protocolo de capa 2 que gestiona enlaces redundantes, previniendo loops en aquellas redes que presentan configuración redundante. STP es transparente a las estaciones de usuario. Está basado en el algoritmo inventado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP, la original (DEC STP) y la estandarizada por el IEEE (IEEE 802.1D) ambas no son compatible entre si. Los loops ocurren cuando hay rutas alternativas entre hosts. Para establecer redundancia de la trayectoria, STP crea un árbol que atraviesa todos los switch en una red, forzando las trayectorias redundantes en un recurso seguro, o bloqueando, puertos si es necesario. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (éste previene los loops) pero establece los caminos redundantes como reserva si el camino inicial falla.

Si los costes de STP cambian, o si un segmento de la red en el STP llega a ser inalcanzable, el algoritmo del árbol que atraviesa configura de nuevo la topología del árbol que atraviesa y restablece el acoplamiento activando la trayectoria espera. Sin atravesar el árbol en lugar, es posible que ambas conexiones pueden ser simultáneamente vivas, que podrían dar lugar a un lazo sin fin del tráfico en el Lan.

Este algoritmo cambia una red física con forma de malla, en la que se pueden formar bucles, en una red lógica en árbol en la que no se puede producir ningún lazo. Los Bridges se comunican mediante Bridge Protocol Data Units (B.P.D.U's). El bridge con la prioridad más alta (el número más bajo de prioridad numérico) se constituye en la raíz. Este bridge raíz

establece el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Todos los demás caminos son bloqueados para propósitos de bridge. El árbol de expansión (Spanning tree) permanece activo hasta que ocurre un cambio en la topología. Esto sucede cuando se da cuenta de ello. El máximo de tiempo de duración del árbol de expansión es de cinco minutos.

3.2.14 PROTOCOLO NBNS

El tener un NBNS en la red puede ayudar enormemente. Para ver exactamente el por qué, vamos a dar una explicación a continuación.

Cuando un cliente arranca una sesión, envía un mensaje broadcast manifestando su deseo de registrar un nombre NetBIOS específico para el. Si nadie pone objeción al uso del nombre, el obtiene el nombre. Por otro lado, si otra máquina en la subred local está actualmente usando ese nombre, enviará un mensaje de respuesta al cliente solicitante indicando que ese nombre ya está siendo usado. Esto es conocido como defender el nombre del host. Este tipo de sistema es útil cuando un cliente se ha caído inesperadamente de la red -otro puede tomar su nombre-, pero se incurre en un importante aumento del tráfico de la red para algo tan simple como el registro de un nombre.

Con un NBNS, ocurre lo mismo, pero con la diferencia que la comunicación está confinada a la máquina solicitante y al servidor de nombres NBNS. No se produce un broadcast cuando una máquina desea registrar su nombre; el mensaje de

registro es simplemente enviado desde el cliente hacia el servidor NBNS, y el servidor NBNS responde si el nombre está o no libre. A esto se le denomina como comunicación punto-a-punto, y es beneficioso en redes con más de una subred. Esto se debe a que los routers suelen estar preconfigurados para bloquear los paquetes broadcast entrantes.

Los mismos principios se aplican a la resolución de nombres. Sin un servidor NBNS, la resolución de nombres NetBIOS se podría realizar mediante broadcast. Todos los paquetes se enviarían a cada ordenador de la red, con la esperanza que el ordenador afectado por la petición responda directamente a la máquina solicitante. El uso de un servidor NBNS y la comunicación punto-a-punto para este propósito cargan mucho menos la red que inundar la red con peticiones broadcast para cada petición de resolución de nombres que se produzca.

Se puede discutir que los paquetes broadcast no causan problemas significativos en las redes modernas y de gran ancho de banda compuestas por máquinas con CPUs muy rápidas, si sólo un grupo reducido de ordenadores están presentes en la red, o la demanda de ancho de banda es pequeña. Hay muchos casos en los que la anterior suposición es cierta; sin embargo, se aconseja no confiar en el broadcast tanto como se pueda. Esta es una regla a seguir en redes grandes y saturadas, y si se sigue este consejo a la hora de configurar redes pequeñas, estas podrán crecer sin problemas en el futuro.

3.3 ANÁLISIS DEL FLUJO DE TRÁFICO DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA.

Para realizar el análisis del flujo de tráfico de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, nos vamos a guiar en los diferentes módulos de la metodología MIRA.

Como primer punto para realizar el análisis del flujo de tráfico debemos tomar en cuenta lo que se especifica en el módulo de arquitectura distribuida de la metodología MIRA, que en el caso que la red sea grande, y para que los resultados sean los que se quiere obtener, se debe realizar el análisis del flujo de tráfico en los puntos más críticos de la red. Para el caso de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga vamos a realizar el análisis del flujo de tráfico en las áreas administrativa, académica.

3.3.1 ÁREA ADMINISTRATIVA

En el área administrativa el análisis de flujo de tráfico se realizará en determinados lapsos de tiempo, esto dependerá del número de estaciones de trabajo que haya en los diferentes departamentos que pertenecen a esta área y también dependerá de las actividades que realizan los diferentes usuarios de las estaciones de trabajo.

Si el departamento es grande, es decir tiene varias estaciones de trabajo, el tiempo de captura de los paquetes que circulan por la red será mayor, y la captura de dichos paquetes se lo realizará

en horas pico, es decir en horas que más se utilicen los servicios que presta la red.

De igual forma debemos tomar muy en cuenta los resultados que arrojen las capturas de tráfico, esto nos ayudará a determinar si es necesario seguir realizando más capturas, ya que si los resultados de las capturas que se realizan no varían, esto nos indicará que debemos continuar con el monitoreo en los demás departamentos del área administrativa.

Es necesario determinar que aplicaciones son las más utilizadas y en que momento del día, y del mes. Para esto nos ayudaremos de una encuesta a la persona encargada, o a los diferentes miembros de cada departamento, de esta forma se podrá realizar la captura del tráfico en el momento adecuado y por ende el trabajo será más eficiente, y arrojará resultados reales.

A continuación detallamos los diferentes departamentos que pertenecen al Área Administrativa y nos servirán para realizar el análisis del flujo de tráfico de red.

- Unidad de Tecnologías de Información y Comunicación.
- Unidad de Finanzas.
- Unidad de Marketing.
- Unidad de Talento Humano.
- Unidad de Bienestar Estudiantil.
- MED.
- Unidad de Logística.
- Centro de Producción.
- Unidad de Admisión y Registro.
- Departamento de Ciencias Exactas.
- Departamento de Lenguas.

- Departamento de Ciencias Administrativas, Económicas y Humanísticas.
- Departamento de Ciencias Eléctricas, Electrónicas y de la Computación.
- Departamento de Ciencias de la Energía y Mecánica Automotriz.
- Dirección.

3.3.1.1 Analizador de red Ethereal

Luego de haber establecido los puntos críticos de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, es necesario disponer de un software que nos permitirá realizar el análisis del flujo de tráfico de la red Lan.

Luego de haber analizado varias opciones de software que se encuentran disponibles en internet y tienen como objetivo el análisis de redes, se eligió como el más adecuado al software denominado Ethereal, el cuál es un analizador de red para Windows y Unix.

Este analizador de protocolos dispone de una interfaz gráfica capaz de reconocer muchos protocolos distintos. Permite revisar los paquetes de datos en una red activa como desde un archivo de captura previamente generado; es capaz de comprender diversos formatos de archivo propios de otros programas de captura.

A continuación se explicará el funcionamiento de Ethereal, en la figura 3.1 se muestra la interfaz de inicio, como

observaremos la interfaz es muy comprensible para el usuario, esto permitirá que el análisis que se va realizar sea muy eficaz.

La versión de Ethereal que se utilizará para realizar la captura de tráfico de los diferentes paquetes que circulan por la red Lan es la 0.99.0, esta versión se obtuvo del sitio Web de Ethereal (http://www.ethereal.com).

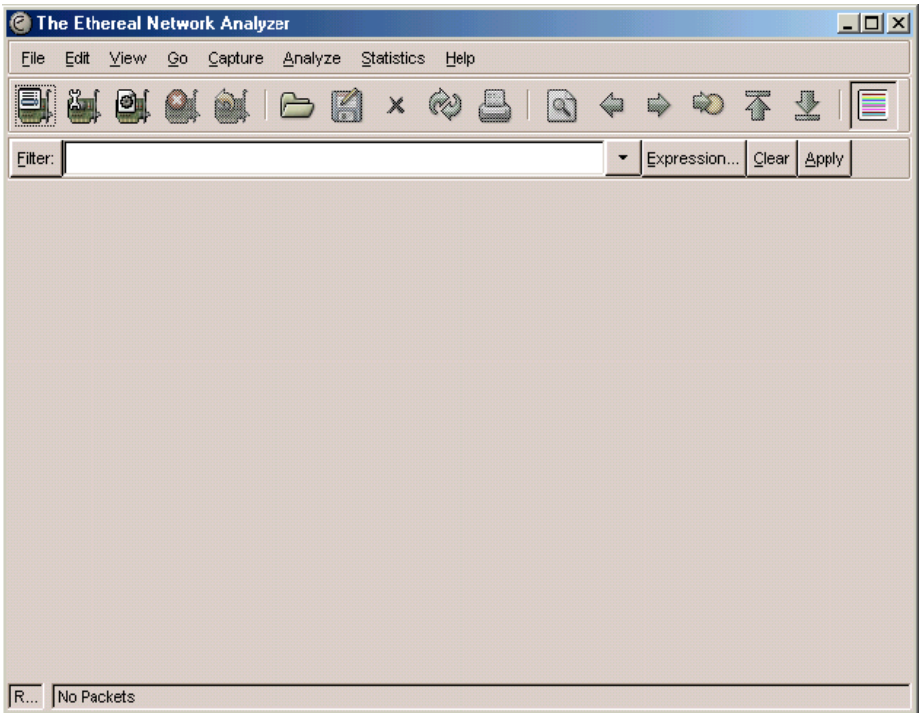


Figura 3.1. Interfaz de inicio de Ethereal.
Fuente: Ethereal.

Como todo software Ethereal dispone de una barra de herramientas la misma que nos permite realizar varias actividades, en el menú nos presenta las siguientes opciones File, Edit, View, Go, Capture, Analize, Statistics, Help. Esto lo podemos observar en la figura 3.2.

En File tenemos la opción de abrir un archivo de captura de tráfico que se encuentre almacenado en una determinada ubicación, también existe la opción Osen Recent, la misma que permite abrir una captura de tráfico recientemente, de igual forma se dispone de las opciones para guardar la captura de tráfico en la ubicación que haya sido seleccionada, también tenemos la opción para imprimir y salir del programa Ethereal. Esto lo podemos visualizar en la figura 3.2.

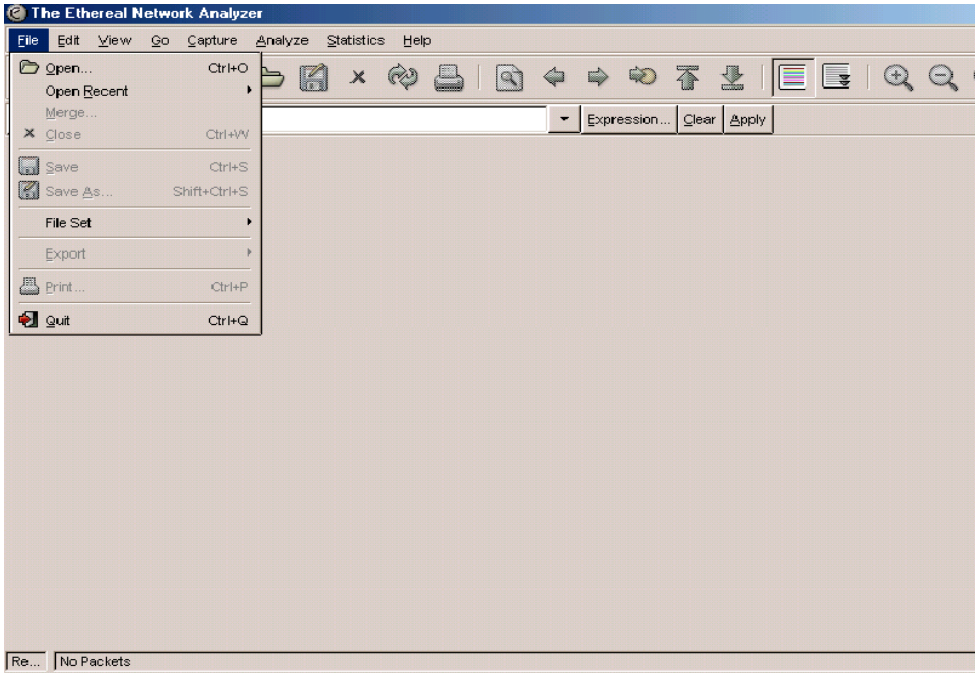


Figura 3.2. Opciones de File.

Fuente: Ethereal.

En el menú Edit tenemos las opciones principales que son: búsqueda de un paquete de la captura de tráfico que se realice, también la opción para seleccionar todos los paquetes de la captura. En la figura 3.3 podemos observar la opción Edit.

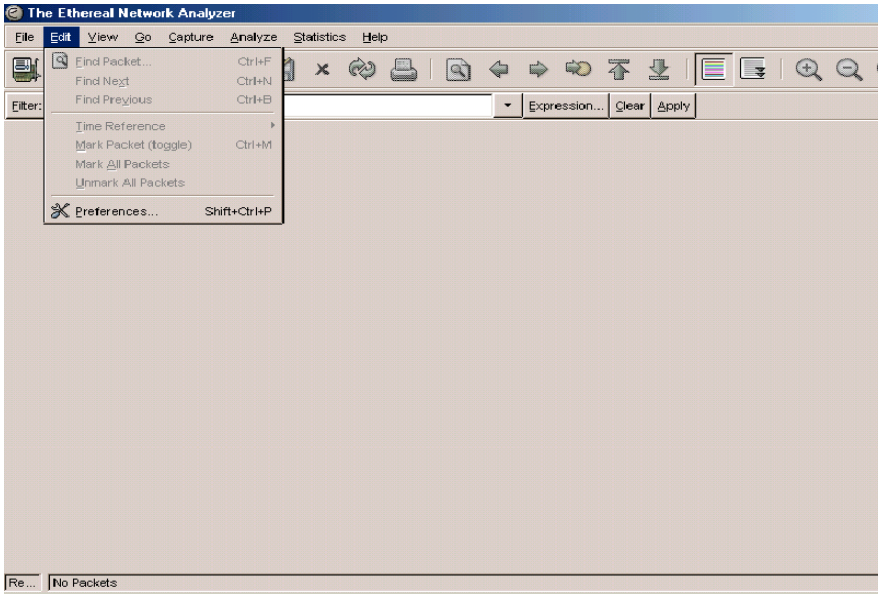


Figura 3.3. Opciones de Edit.

Fuente: Ethereal.

Ethereal en la opción View permite visualizar las diferentes barras de tarea que dispone como es la barra principal, la barra de filtros, la barra de estado, la lista de paquetes, detalle de cada uno de los paquetes que se ha capturado. En la figura 3.4 podemos observar la opción View de Ethereal.

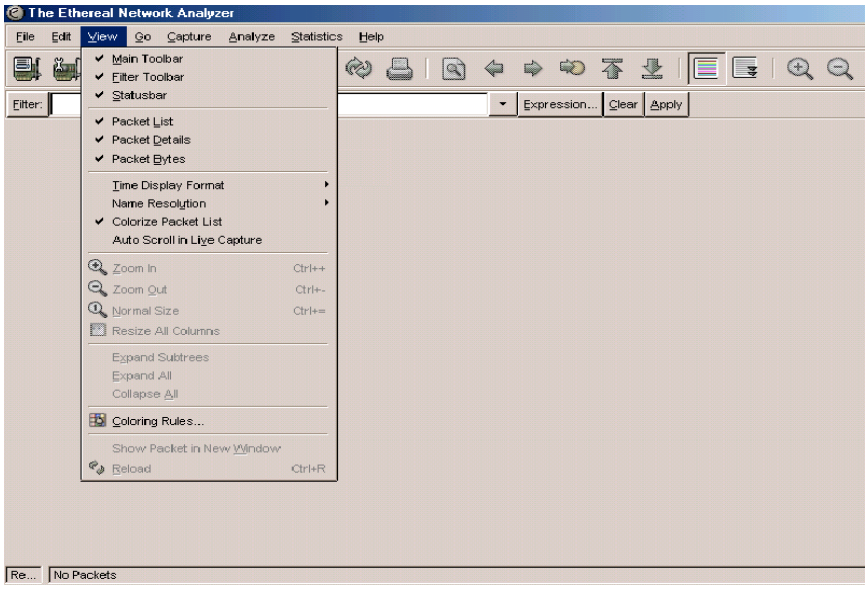


Figura 3.4. Opciones de View.

Fuente: Ethereal.

Una de las opciones más importantes que nos brinda Ethereal es Capture, en esta opción vamos a realizar la captura de tráfico de los diferentes paquetes que están circulando por la red. Al seleccionar la opción Capture nos despliega un menú en el cuál tenemos varias opciones como son: Interfaces, Options, Star, Stop, Restart, Capture Filtres, esto lo visualizamos de mejor forma en la figura 3.5.

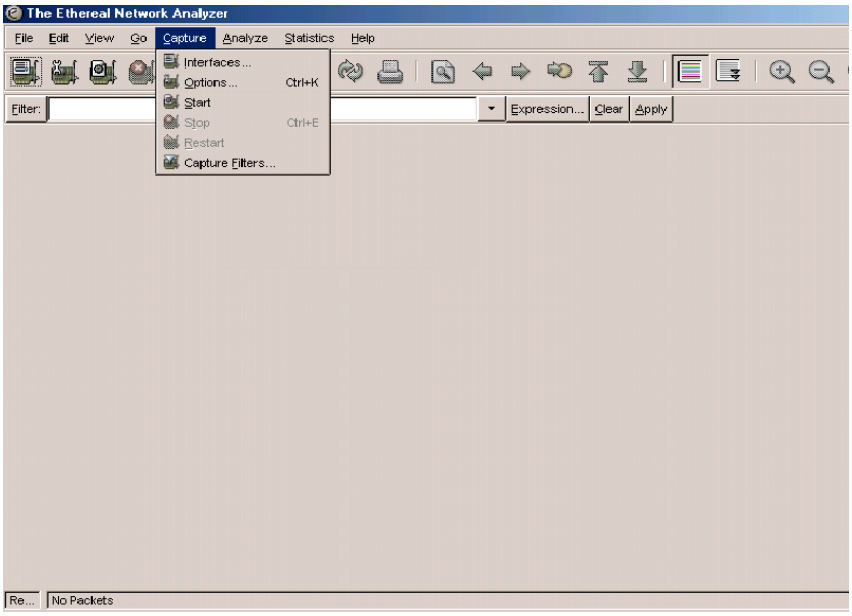


Figura 3.5. Opciones de Capture.

Fuente: Ethereal.

De las opciones que se muestran en la figura anterior una de las más importantes y que más se utilizará es Options, al seleccionarla nos presentará una ventana, la misma se puede observar en la figura 3.6, en esta ventana se puede elegir la interfaz de red con la que se va monitorear la red, es decir aquí aparece la tarjeta electrónica conocida como NIC, esta tarjeta tiene las siguientes funciones:

- Forma los paquetes de datos.
- Da acceso al cable, con la conversión eléctrica y ajuste de velocidad
- Es el transmisor y el receptor de la estación de trabajo
- Chequea las tramas para verificar errores
- Conversión Serie/Paralelo

- Identificación o dirección única en la red que permite saber cual es físicamente la terminal.

Luego de haber seleccionado la interfaz de monitoreo, también se puede seleccionar un protocolo específico para realizar la captura de tráfico por ejemplo puede ser TCP, UDP, HTTP, todo depende de lo que requiera el usuario. Estos protocolos se pueden seleccionar en la opción capture filter, antes de iniciar con el proceso de captura de tráfico podemos determinar una ubicación donde se guardará la captura de tráfico luego de finalizar el proceso, Ethereal permite elegir el tiempo que se va a monitorear la red, el tiempo de captura puede ser indefinido, todo depende del usuario, también permite que se detenga la captura de tráfico luego de haber capturado una determinada cantidad de paquetes. Después de haber elegido todas las opciones que se requiera para una mejor captura y según las necesidades del usuario podemos empezar pulsando el botón Start.

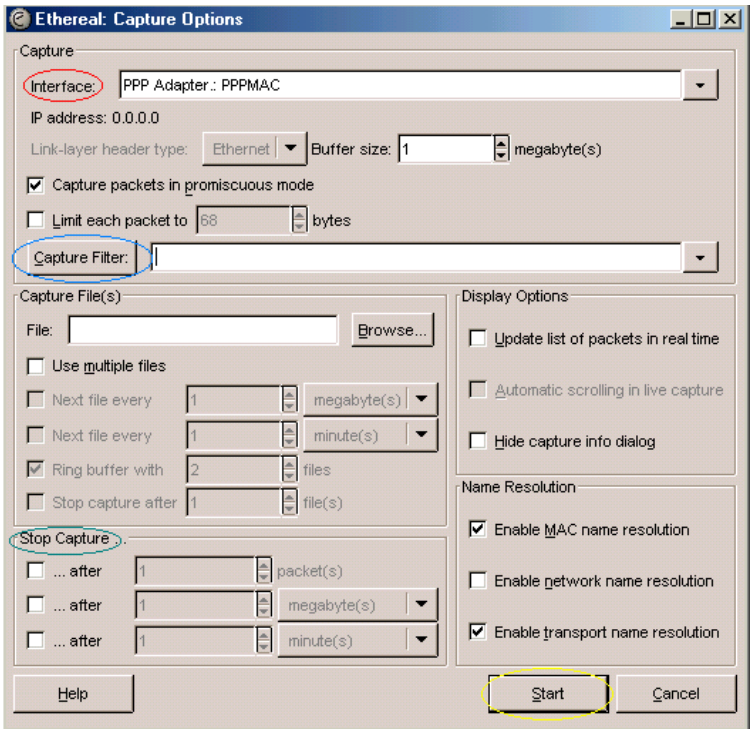


Figura 3.6. Capture Options.

Fuente: Ethereal.

En la figura 3.7 se podrá observar los diferentes paquetes que se han capturado en determinado tiempo, se muestra en diferentes colores, esto depende del tipo de paquete que ha sido capturado, por ejemplo podemos observar que los paquetes HTTP, TCP, son de color verde, los paquetes del protocolo ARP son de color celeste, y así todos los paquetes tienen un color específico para mayor comprensión de la persona que está encargada de realizar el monitoreo de la red. También tenemos una pequeña ventana en la parte inferior de la figura 3.7, en la cuál se muestra la información detallada de cada uno de los diferentes paquetes que han sido capturados.

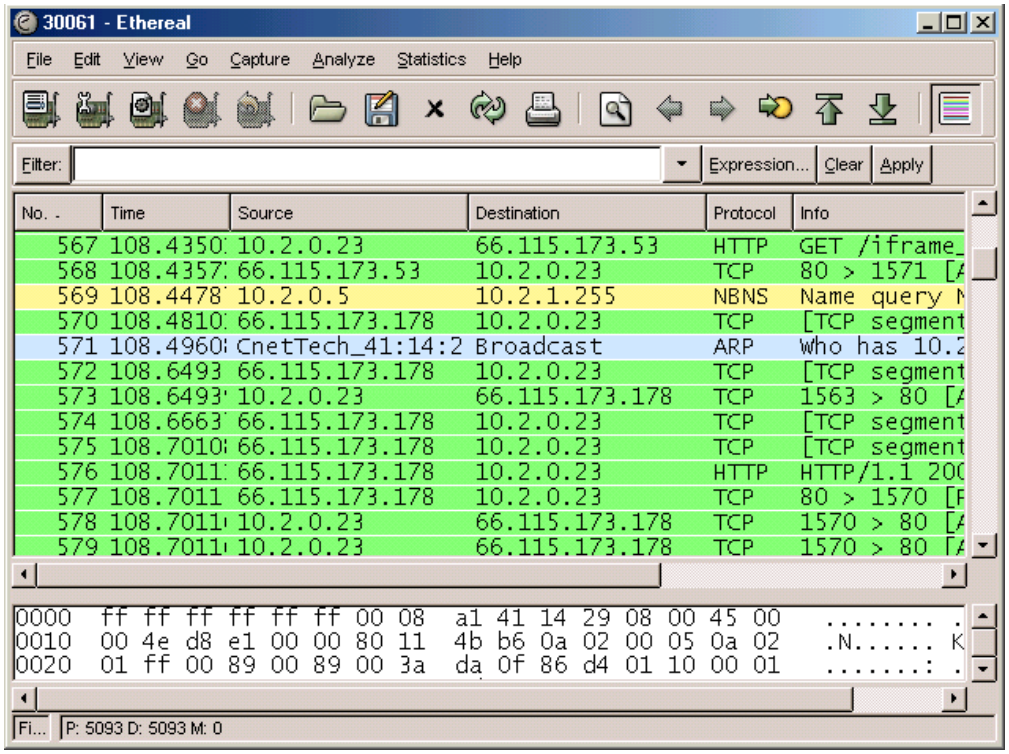


Figura 3.7. Interfaz de captura de Ethereal.

Fuente: Ethereal.

En el menú de Ethereal se dispone de la opción Analyze, esta permite filtrar determinados paquetes, para poder realizar el análisis solo de los paquetes que se han filtrado y determinar si existe alguna anomalía en la red.

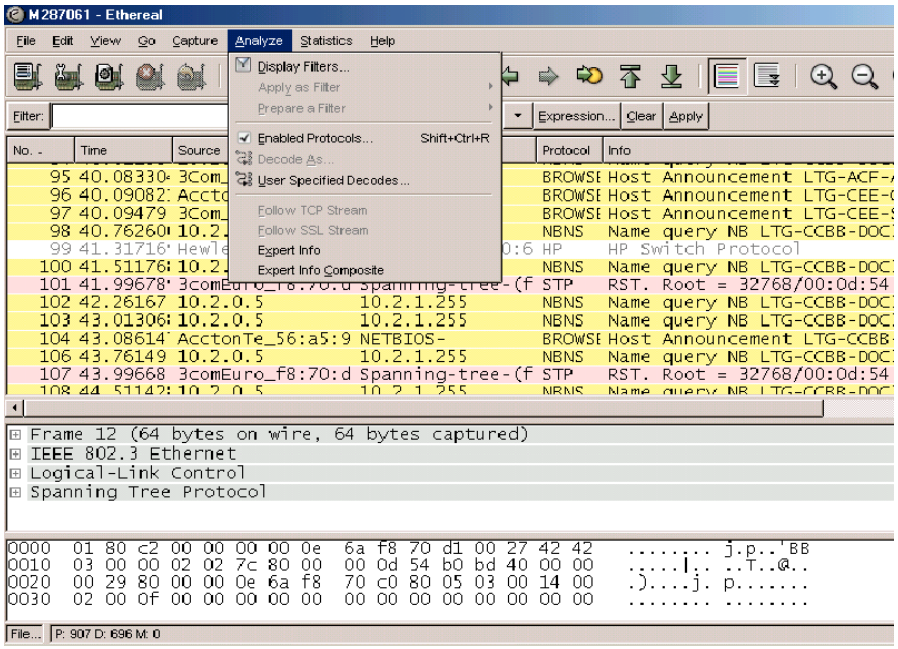


Figura 3.8. Analyze de Ethereal.

Fuente: Ethereal.

El módulo de estadísticas permite mostrar la información de las diferentes capturas de tráfico realizadas, sea en informes o en forma gráfica, una opción importante es Summary, esta opción genera un informa de forma general de la captura de tráfico realizada. Esto lo podemos observar en la Figura 3.9.

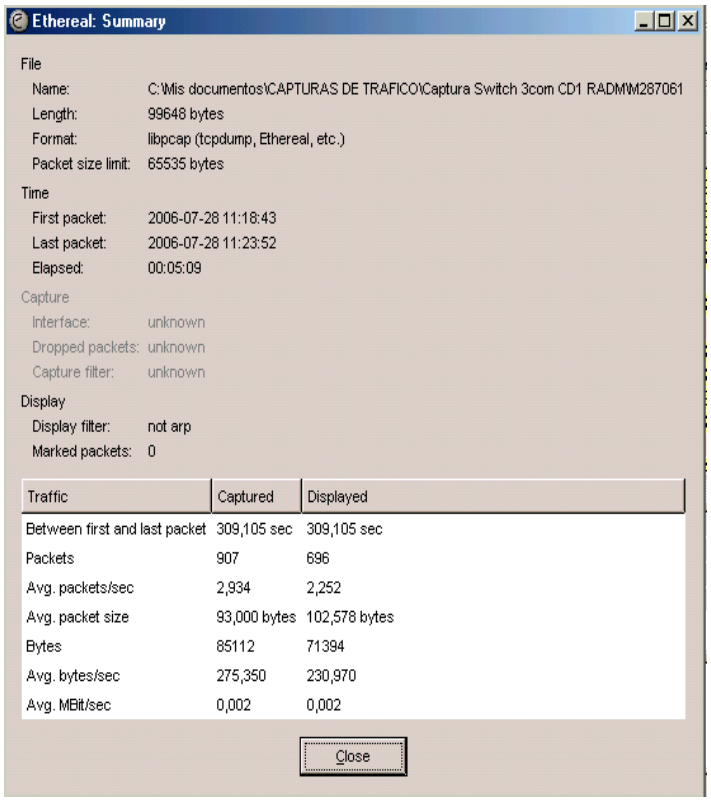


Figura 3.9. Summary de Ethereal.

Fuente: Ethereal.

Como se indicó anteriormente las estadísticas se muestran de forma gráfica, para esto en el menú de Statistics debemos escoger la opción de ¡O Graphs, aquí nos muestra los paquetes que se han capturado en diferentes tiempos, se puede observar en líneas de diferentes colores según los paquetes que se capturen, como podemos observar en la figura 3.10.

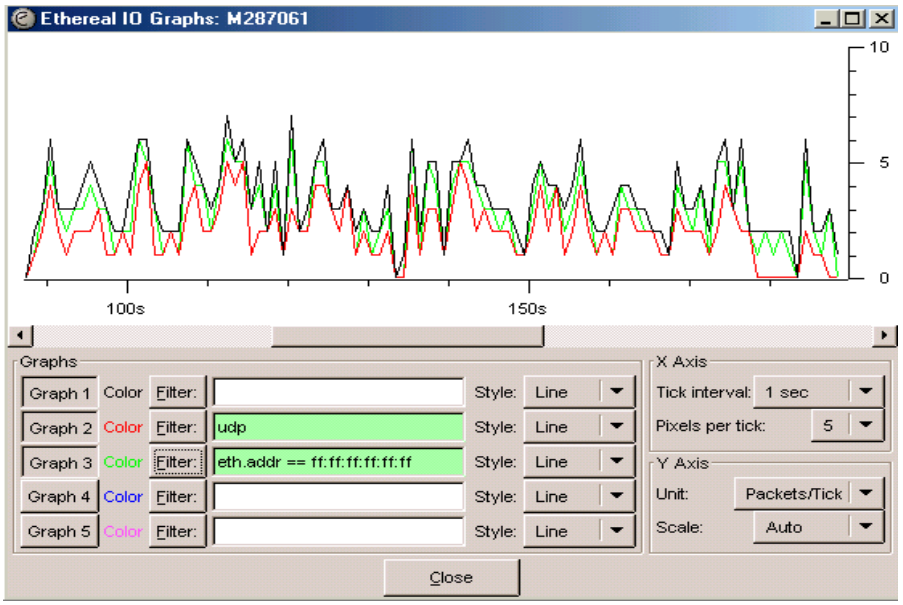


Figura 3.10. ¡ O Graphs de Ethereal.

Fuente: Ethereal.

Las estadísticas también nos permiten saber las máquinas que han generado más tráfico de ciertos paquetes, y el porcentaje del ancho de banda que ha utilizado. Ver la figura 3.11.

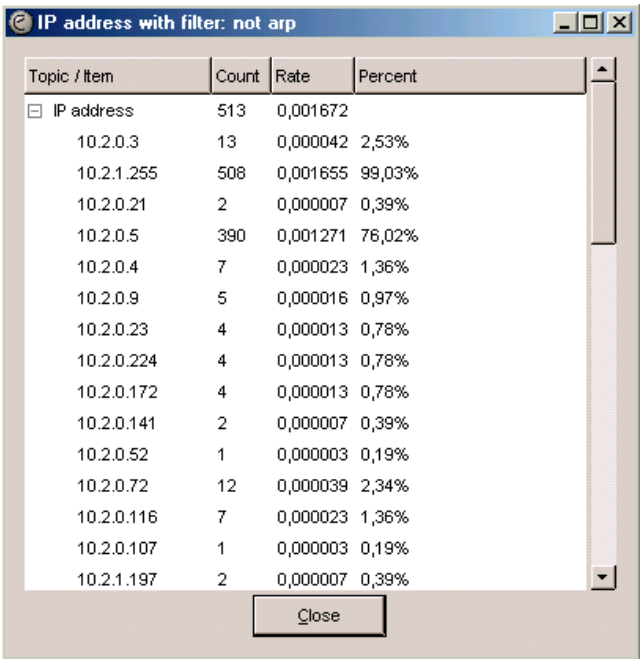


Figura 3.11. Estadísticas de direcciones IP de Ethereal.

Luego de haber conocido el funcionamiento de Ethereal podemos iniciar con el monitoreo de la Red Lan de la Escuela Politécnica del Ejército Sede Latacunga en todas las dependencias que se describió anteriormente, para esto vamos a guiarnos en la metodología Mira (METODOLOGÍA PARA LA INSPECCIÓN DE TRÁFICO EN REDES AVANZADAS).

3.3.2 ANÁLISIS DEL TRÁFICO EN EL SWITCH D-LINK-DES-1016 DE LA UNIDAD DE FINANZAS.

3.3.2.1 MÓDULO DE CAPTURA

El primer módulo de la metodología Mira es el de captura, en este módulo hemos realizado la captura de los paquetes que se genera desde la Unidad de Finanzas, este monitoreo se lo realizó en diferentes días y periodos de tiempo, las capturas de tráfico se las realizaron en base a una encuesta realizada a las personas que laboran en esta Unidad, las horas en que más actividades realizan, utilizando el servicio de red es en la mañana. En todas las estaciones de trabajo de esta dependencia manejan el software Olympo, y tienen acceso a determinadas páginas del Internet, el acceso a estas páginas es poco frecuente, generalmente se utiliza el internet para revisar el rol de pagos.

A continuación se detallará las capturas de tráfico que se realizaron en la Unidad de Finanzas.

3.3.2.1.1 Capturas de tráfico realizadas en el Switch SW-D-LINK-DES-1016 de la Unidad de Finanzas.

En la tabla 3.1 se describen las capturas de tráfico realizadas en el SW-D-LINK-DES-1016.

SW-D-LINK-DES-1016		
Nº DE CAPTURA	**FECHA**	**DETALLE**
1	26 de Julio de 2006	Realizado en la mañana
2	27 de Julio de 2006	Realizado en la tarde

Tabla 3.1. Captura de tráfico realizada en el SW-D-LINK-DES-1016.
Autor: Javier Cayo.

En el Anexo B se detallan las capturas de tráfico realizadas en el SW-D-LINK-DES-1016.

En el Anexo C se muestra de forma gráfica como se realizó la captura de tráfico.

3.3.2.2 MÓDULO DE PREPROCESADO.

En el módulo de preprocesado se eliminará el tráfico innecesario de la captura que se realizó.

Luego de haber realizado la captura de tráfico, se determina que las diferentes capturas de tráfico realizadas en los diferentes switches, circulan la misma clase de paquetes en toda la red. Por lo que no es necesario eliminar ninguno de los paquetes que están circulando por la red ya que todos nos van a servir para realizar un mejor análisis.

Como parte del módulo de preprocesado tenemos varias etapas, las que se detallarán a continuación:

3.3.2.2.1 Análisis de Seguridad

La primera etapa es el análisis de seguridad, en esta etapa se va a dividir el tráfico capturado en dos clases que son: tráfico convencional y tráfico sospechoso.

3.3.2.2.1.1 Tráfico Convencional

1. Entre el tráfico convencional tenemos los paquetes TCP/IP los mismos que como sabemos sirven para establecer la comunicación entre las diferentes estaciones de trabajo por ende no presentan peligro alguno para el correcto funcionamiento de la red, y no representan un consumo elevado del ancho de banda.

   Gracias al analizador de red Ethereal se ha determinado las aplicaciones que generan el tráfico TCP son las siguientes:

- El sistema Académico.
- El sistema Olympo que se utiliza todos los días por las personas que trabajan en la Unidad de Finanzas.
- Las páginas de Internet que se manejan diariamente.
- El Sistema de rol de pagos, utilizado el fin de mes.

De esta forma es como se maneja el protocolo TCP en la Unidad de Finanzas, es el que más se utiliza en las diferentes aplicaciones que se describieron anteriormente en la Unidad de Finazas.

2. También tenemos los paquetes HTTP, los mismos que se generan cuando los usuarios navegan en el Internet lo que permite la comunicación, transferencia de archivos de las páginas Web que utilizan los usuarios, de la misma forma este tipo de protocolos no representan peligro para el buen funcionamiento de la red, de acuerdo al análisis que se realizó mediante Ethereal no consumen mucho ancho de banda.

   Como se explicó anteriormente este tipo de tráfico lo generan las diferentes páginas Web que se manejan en la Institución.

3. Otro de los paquetes que pertenecen al tráfico convencional es el DNS el mismo que está en el grupo de TCP/IP y permite la resolución de nombres de direcciones al momento que se navega en el Internet, es por eso que este protocolo es muy común y necesario, no va a representar peligro alguno para la red.

Los protocolos anteriormente mencionados son los que pertenecen al tráfico convencional, dichos protocolos se han capturado en la Unidad de Finazas de la Escuela Politécnica del Ejército Sede Latacunga.

En las tablas que se presentarán a continuación, se muestra de forma detallada el número de paquetes, el ancho de banda que consumen, switch de la Unidad de Finanzas de la Escuela Politécnica del Ejército Sede Latacunga y pertenecen al tráfico convencional.

Tráfico Convencional				
Switch	**N° de Captura**	**Protocolo**	**N° de Paquetes**	**Ancho de Banda**
SW-D-LINK-DES-1016	1	HTTP	0	0
SW-D-LINK-DES-1016	2	HTTP	10	0.000001
SW-D-LINK-DES-1016	1	DNS	18	0.000001

SW-D-LINK-DES-1016	2	DNS	14	0.000001

Tabla 3.2. Resumen del tráfico convencional en el Switch LTG-SW-CD1-04- ACC.

Autor: Javier Cayo.

3.3.2.2.1.2 Tráfico Sospechoso

Como parte de la primera etapa del módulo de preprocesado tenemos también el tráfico sospechoso, este tipo de tráfico es el que puede ocasionar peligro, riesgo, esto no permitirá el buen funcionamiento de la red, estos paquetes los hemos escogido de las diferentes capturas que se ha realizado.

1. Entre el tráfico sospechoso tenemos que en todas las capturas de tráfico realizadas se detectó que se genera una gran cantidad de tráfico de broadcast como una de las principales novedades que se encontró en el switch. Los paquetes del tráfico de broadcast no ocupan mucho espacio del ancho de banda que dispone la Institución, pero genera inquietud ya que como se mencionó anteriormente es una cantidad considerable el tráfico de broadcast que se genera en la red.

Este tipo de tráfico lo generan todas las estaciones de trabajo que pertenecen a la Unidad de Finanzas, ya que al momento que quieren establecer comunicación con un servidor o con una computadora, mandan mensajes de tipo ARP que es el protocolo que permite que se resuelva la dirección de la máquina que se quiere localizar.

2. Otro de los protocolos que se encontró como parte del tráfico sospechoso es el NBNS, este protocolo se genera en gran cantidad , de ahí que de 5002 paquetes que se capturó 1872 son del protocolo NBNS, y no es común que este protocolo se genere en esa cantidad en la red, es por eso que se a puesto en el grupo del tráfico sospechoso.

   Este tipo de protocolo se genera a partir del servidor de antivirus, es así que al momento de realizar la captura de tráfico con el analizador Ethereal, tenemos como resultado que la dirección de origen es la que pertenece al servidor de antivirus y la dirección destino es una tipo broadcast.

   Se debe revisar el funcionamiento el antivirus, para determinar el porque se genera en gran cantidad el protocolo NBNS, de esta forma se podrá optimizar el ancho de banda de la red.

Los 2 protocolos que se describieron anteriormente son los que se generan en mayor cantidad en el switch, por ende se les va dar mayor prioridad para poder presentar la solución más adecuada en el próximo capítulo, lo que permitirá que la red funcione de mejor forma y no se desperdicie el ancho de banda, de esta forma estamos optimizando el ancho de banda que se dispone en la Escuela Politécnica del Ejército Sede Latacunga.

3. También entre el tráfico sospechoso de la red tenemos la presencia del protocolo STP, se genera de una forma considerable en todas las capturas de tráfico que se realizaron en las distintas áreas de la Institución.

4. También tenemos la presencia del protocolo Browser, este protocolo se genera en todas las capturas que se realizó. Podemos citar que como ejemplo se tomó una captura de tráfico y con la ayuda de Ethereal determinamos que de 3050 paquetes capturados 250 pertenecen al protocolo Browser, estas cantidades son una referencia de dicho protocolo.

   El protocolo Browser se genera cuando desde una computadora se manda a

imprimir un documento, este protocolo ayuda a buscar la ubicación de la impresora y de esta forma imprimir el documento que ha sido enviado.

En la tabla que se presentará a continuación, se muestra de forma detallada el número de paquetes, el ancho de banda que consumen, en el switch que se encuentra en la Unidad de Finanzas de la Escuela Politécnica del Ejército Sede Latacunga y pertenecen al tráfico sospechoso.

Tráfico Sospechoso				
Switch	**N° de Captura**	**Protocolo**	**N° de Paquetes**	**Ancho de Banda**
SW-D-LINK-DES-1016	1	Broadcast	2274	0.000001
SW-D-LINK-DES-1016	1	NBNS	4508	0.001000
SW-D-LINK-DES-1016	1	Browser	800	0.000001
SW-D-LINK-DES-1016	1	STP	1614	0.000001
SW-D-LINK-DES-1016	2	Broadcast	1259	0.000001
SW-D-LINK-DES-1016	2	NBNS	2193	0.001000
SW-D-LINK-DES-1016	2	Browser	354	0.000000
SW-D-LINK-DES-1016	2	STP	940	0.000001

Tabla 3.3. Resumen del Tráfico Sospechoso en el Switch LTG-SW-CD1-04-ACC.

Autor: Javier Cayo.

3.3.2.2.2 Etapa de Clasificación

En la segunda etapa del módulo de preprocesado el tráfico convencional que se detalló anteriormente, va ser clasificado en base a las direcciones IP de las máquinas que están conectadas al switch SW-D-LINK-DES-1016.

A continuación se detallará las direcciones IP de las diferentes estaciones de trabajo de la Unidad de Finanzas, son el resultado de haber realizado la captura de tráfico con el analizador de red Ethereal.

En las tablas que se detallarán a continuación se muestra la dirección IP de la máquina, el total de paquetes y el porcentaje del ancho de banda que consume cada paquete que pasa por la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

3.3.2.2.2.1 Switch SW-D-LINK-DES-1016

En las tablas 3.4 y 3.5 tenemos las direcciones de las máquinas que utilizan el protocolo TCP. Estas tablas se tomaron de las capturas de tráfico que se realizaron en el Switch SW-D-LINK-DES-1016, para referencia podemos ver en la tabla 3.1.

En esta tabla existen direcciones IP de las diferentes estaciones de trabajo que existen en la Unidad de Finanzas como también de los diferentes servidores que dispone la Institución. Como se observará los 1888 paquetes los que han circulado por la red, y que representan un 0.000593 del total del ancho de banda disponible.

Dirección IP	Total de Paquetes	Porcentaje Ancho de Banda
10.2.1.152	938	0.000295
10.2.0.5	726	0.000228
10.2.0.2	118	0.000037
10.2.0.9	99	0.000031
10.2.1.31	5	0.000002
10.2.0.3	1	0.000000
10.2.1.131	1	0.000000
TOTAL	**1888**	**0.000593**

Tabla 3.4. Direcciones IP del Protocolo TCP del Switch SW-D- LINK-DES-1016 de la captura de tráfico 1.
Fuente: Ethereal.

En la tabla 3.5 aparecen direcciones que no pertenecen a los grupos que existen en la Institución, estas son direcciones de las páginas de Internet que estaban abiertas al momento de realizar la captura de tráfico.

Se debe comprobar a que página de internet corresponde las direcciones que ha logrado identificar el analizador Ethereal, de esta

forma se podrá determinar si las páginas de internet son utilizadas para actividades relacionadas con el trabajo diario de los diferentes usuarios de la red.

Dirección IP	Total de Paquetes	Porcentaje Ancho de Banda
10.2.0.30	57	0.000036
200.52.65.80	27	0.000017
64.233.179.104	11	0.000007
216.23.176.100	10	0.000006
64.233.179.99	9	0.000006
10.2.0.5	7	0.000004
10.2.0.91	3	0.000002
10.2.0.51	3	0.000003
10.2.0.2	1	0.000001
10.2.0.61	1	0.000001
10.2.1.131	1	0.000001
TOTAL	130	0.000084

Tabla 3.5. Direcciones IP del Protocolo TCP del Switch SW-D-
LINK- DES-1016 de la captura de tráfico 2.
Fuente: Ethereal.

De la misma forma se debe clasificar las direcciones IP que utilizan el protocolo UDP, a continuación vamos a detallar en las tablas 3.6 y 3.7 las diferentes direcciones IP que usan dicho protocolo.

En la tabla 3.6 existen direcciones IP de las diferentes estaciones de trabajo que existen en la Unidad de Finanzas como también de los diferentes servidores que

dispone la Institución. Así también existen ciertas direcciones que pertenecen a páginas de Internet.

Dirección IP	Total de Paquetes	Porcentaje Ancho de Banda
10.2.1.255	4564	0.001412
10.2.0.5	3431	0.001062
169.254.255.255	597	0.000185
169.254.121.194	353	0.000109
169.254.211.46	221	0.000068
255.255.255.255	149	0.000046
10.2.0.3	148	0.000046
10.2.0.2	74	0.000023
10.2.0.9	73	0.000023
10.2.0.4	70	0.000022
10.2.0.101	55	0.000017
10.2.1.152	34	0.000011
10.2.0.194	31	0.000010
10.2.0.224	29	0.000009
10.2.0.83	27	0.000008
10.2.0.185	27	0.000008
10.2.1.154	26	0.000008
10.2.0.43	25	0.000008
10.2.0.41	25	0.000008
10.2.0.176	23	0.000007
10.2.0.23	23	0.000008
10.2.0.152	23	0.000007
10.2.1.181	23	0.000007
10.2.0.162	23	0.000007
10.2.1.91	22	0.000007
10.2.0.116	22	0.000007
10.2.1.101	22	0.000007
10.2.0.31	22	0.000007
10.2.0.93	21	0.000006
10.2.1.21	20	0.000006
10.2.0.64	20	0.000006
10.2.0.132	19	0.000006
10.2.0.106	19	0.000006
10.2.0.184	18	0.000006
10.2.0.63	16	0.000005
10.2.0.53	15	0.000005
10.2.0.51	15	0.000005
10.2.0.171	15	0.000005
10.2.0.91	13	0.000004
10.2.0.161	12	0.000004
10.2.0.111	10	0.000003
10.2.1.111	10	0.000003
10.2.1.183	10	0.000003

10.2.1.155	10	0.000003
10.2.1.151	10	0.000003
10.2.1.186	10	0.000003
10.2.1.153	10	0.000003
10.2.0.107	10	0.000003
10.2.0.186	9	0.000003
10.255.255.255	7	0.000002
10.2.0.181	6	0.000002
10.2.0.178	6	0.000002
10.2.0.61	6	0.000002
169.254.7.148	4	0.000001
192.188.58.163	4	0.000001
10.2.1.184	4	0.000001
TOTAL	10523	0.000326

Tabla 3.6. Direcciones IP del Protocolo UDP del Switch SW-D- LINK-DES-1016 de la captura de tráfico 1.

En la tabla 3.7 se muestran las direcciones IP que utilizan el protocolo UDP del SW-D-LINK-DES-1016.

Dirección IP	**Total de Paquetes**	**Porcentaje Ancho de Banda**
10.2.0.5	18866	0.001002
10.2.1.255	2532	0.001360
10.2.0.3	84	0.000045
10.2.0.30	44	0.000024
10.0.2.4	41	0.000022
10.2.0.9	40	0.000021
10.2.0.2	34	0.000018
10.2.0.141	30	0.000016
10.2.0.111	21	0.000011
10.2.0.224	18	0.000010
10.2.0.21	17	0.000009
10.2.0.83	16	0.000009
10.2.0.194	15	0.000008
10.2.0.185	15	0.000008
10.2.0.202	15	0.000008
10.2.0.72	14	0.000008
10.2.0.43	14	0.000008
10.2.0.93	14	0.000008
10.2.0.64	13	0.000007
10.2.0.176	13	0.000007
10.2.0.162	12	0.000006
10.2.1.111	12	0.000006
10.2.1.91	11	0.000006

10.2.0.132	11	0.000006
10.2.0.23	11	0.000006
10.2.0.172	11	0.000006
192.188.58.163	10	0.000005
10.2.1.61	9	0.000005
10.2.0.151	8	0.000004
10.2.0.41	8	0.000004
10.2.0.152	8	0.000004
10.2.0.116	7	0.000004
10.2.1.184	7	0.000004
10.2.0.171	7	0.000004
10.2.0.91	7	0.000004
10.2.1.184	6	0.000003
10.2.0.107	6	0.000003
10.2.0.186	6	0.000003
10.2.0.161	6	0.000003
10.2.1.154	6	0.000003
10.2.0.192	6	0.000003
10.2.0.94	6	0.000003
10.2.1.183	6	0.000003
10.2.1.151	6	0.000003
10.2.1.186	6	0.000003
255.255.255.255	6	0.000003
10.2.0.71	5	0.000003
10.2.1.153	5	0.000003
10.2.0.51	5	0.000003
10.2.0.31	5	0.000004
10.2.0.61	4	0.000002
10.255.255.255	4	0.000004
10.2.1.51	4	0.000004
1.2.1.181	4	0.000002
10.2.0.106	4	0.000002
10.2.1.31	4	0.000002
10.2.0.142	3	0.000002
10.2.1.197	2	0.000001
239.255.255.250	1	0.000001
TOTAL	**22111**	**0.002749**

Tabla 3.7. Direcciones IP del Protocolo UDP del Switch SW-D- LINK-DES-1016 de la captura de tráfico 2.

Fuente: Ethereal.

3.3.2.3 MÓDULO DE CONSOLIDACIÓN.

Para continuar con el desarrollo de la metodología Mira tenemos el módulo de consolidación, en este módulo vamos a consolidar los resultados parciales de las diferentes capturas de tráfico que se ha realizado en el Switch SW-D- LINK-DES-1016, de la Unidad de Finanzas, de esta forma se tendrá una idea de cómo ha sido el comportamiento de la red al momento de realizar las capturas de tráfico.

3.3.2.3.1 SWITCH SW-D-LINK-DES-1016

En la tabla 3.8 se muestra de una forma detallada las capturas de tráfico que se realizaron en la Unidad de Finanzas.

SW-D-LINK-DES-1016			
Nº DE CAPTURA	**FECHA**	**TIEMPO DE CAPTURA**	**NUMERO DE PAQUETES**
1	26 de Julio de 2006	55 Minutos	10861Paquetes
2	**27 de Julio de 2006**	**32 Minutos**	**5022 Paquetes**

Tabla 3.8. Detalle de las capturas de tráfico realizadas en el Switch SW-D-LINK-DES-1016.

Fuente: Ethereal.

3.3.2.4 MÓDULO DE CLASIFICACIÓN

En este módulo se clasificará el tráfico que se ha capturado en diferentes categorías.

A continuación vamos a detallar las categorías de tráfico que se ha logrado identificar en las diferentes capturas de tráfico que se realizaron.

- **Primera Categoría.-** La primera categoría que se ha identificado, es el traficó normal o convencional el mismo que ya se detalló en el módulo de preprocesado.

  Este tipo de tráfico es el que no representa peligro alguno para el buen desenvolvimiento de la red, este tipo de tráfico se genera en todas las estaciones de trabajo que dispone la Escuela Politécnica del Ejército Sede Latacunga.

  A continuación vamos a citar los protocolos que se han tomado en cuenta en el tráfico normal, tenemos al protocolo TCP, el protocolo UDP, el protocolo HTTP, el protocolo DNS.

- **Segunda Categoría.-** La segunda categoría que podemos identificar es el tráfico administrativo, el mismo que produce cada una de las estaciones de trabajo que pertenecen a la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga.

  Este tipo de tráfico lo generan las diferentes aplicaciones que se utilizan todos los días, en los diferentes departamentos de la Escuela Politécnica del Ejército Sede Latacunga, entre las aplicaciones tenemos:

  - Sistema Olympo
  - Antivirus Kaspersky
  - Sistema Académico

- **Tercera Categoría.-** Otra categoría que se ha identificado y se puede decir que es una de las más

importantes y nos da la idea principal para saber que problemas tiene nuestra red, es la del tráfico indeterminado, este tipo de tráfico se produce en gran cantidad en la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga, el tráfico indeterminado se ha logrado identificar en todas las capturas de tráfico que se han realizado en los diferentes departamentos de la Institución, y es lo que más inquietud produce ya que se generan varios protocolos no muy usuales para el correcto funcionamiento de la red, los protocolos que se encuentran en esta categoría son: el broadcast, NBNS, STP, BROWSER, estos protocolos ocupan el ancho de banda de la red, el espacio que utilizan no es muy considerable pero sería mejor que este tipo de tráfico de red no se de y de esta forma el espacio que estos protocolos utilizan sería distribuido de mejor forma entre las demás aplicaciones que necesitan el ancho de banda para un correcto y rápido funcionamiento.

3.3.2.5 MÓDULO DE POSTPROCESADO

Luego de haber realizado la clasificación podemos continuar con el módulo de postprocesado aquí se va realizar informes de forma general de los diferentes resultados que hemos conseguido luego de haber capturado el tráfico en la red.

Con la ayuda del analizador de red Ethereal se presenta los diferentes informes y gráficos del monitoreo de la red, de esta forma ya se puede dar un análisis del estado en el que se encuentra la red.

Para realizar este módulo, vamos a tomar como referencia las capturas de tráfico de red del módulo de consolidación.

3.3.2.5.1 ESTADÍSTICAS DEL SWITCH SW-D-LINK-DES-1016

En figura 3.12 se muestra de una forma general la cantidad de paquetes que circularon por la red, el tiempo, la fecha entre otras.

El punto más importante de esta estadística es saber cuanto es el consumo del ancho de banda, en la captura de tráfico que se ha realizado.

Para la figura 3.12 vamos a observar que el consumo es del 0.004% del total del ancho de banda.

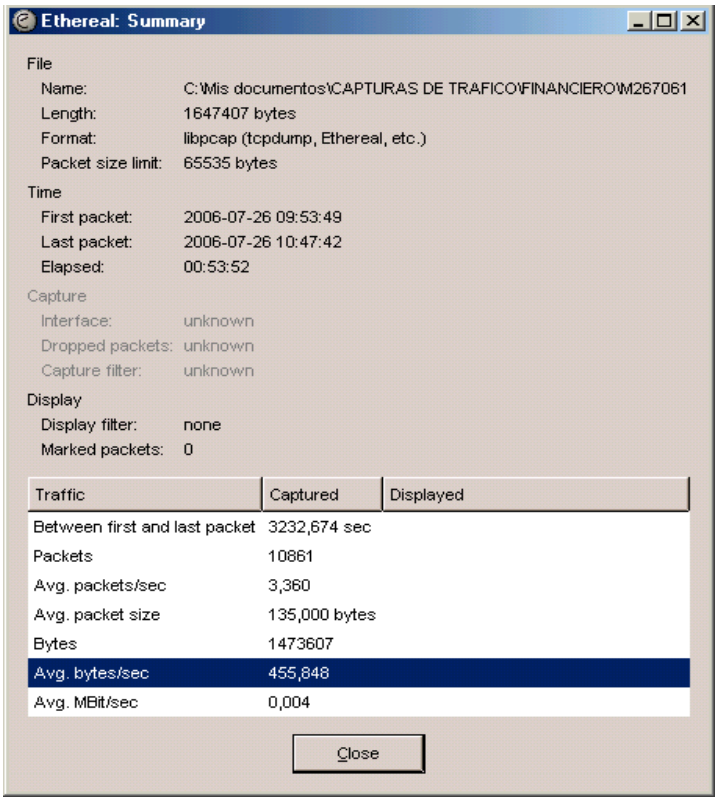


Figura 3.12. Resumen de la captura de tráfico realizada en el Switch SW-D-LINK-DES-1016.

Fuente: Ethereal.

En la figura 3.13 se muestra los diferentes paquetes que han circulado por la red Lan.

En este gráfico vamos a observar que los paquetes de TCP se distinguen con una línea de color negro, estos paquetes son generados por los usuarios que manejan los diferentes sistemas como puede ser el Olympo. De la misma forma este tipo de protocolos se generan cuando se navega en las páginas de internet.

Los paquetes UDP están con color rojo, este protocolo se genera constantemente.

El tráfico de Broadcast se encuentra identificado con color verde, este tipo de tráfico generan todas las estaciones de trabajo al momento que se quieran comunicar con una determinada estación de trabajo o también con un servidor.

Con color azul se encuentran los paquetes que pertenecen a NBNS, se genera cuando el servidor de antivirus no ha logrado encontrar a una determinada estación de trabajo, para poder ejecutar una tarea.

De color lila se encuentran los paquetes del protocolo STP, se genera automáticamente en todos los switches.

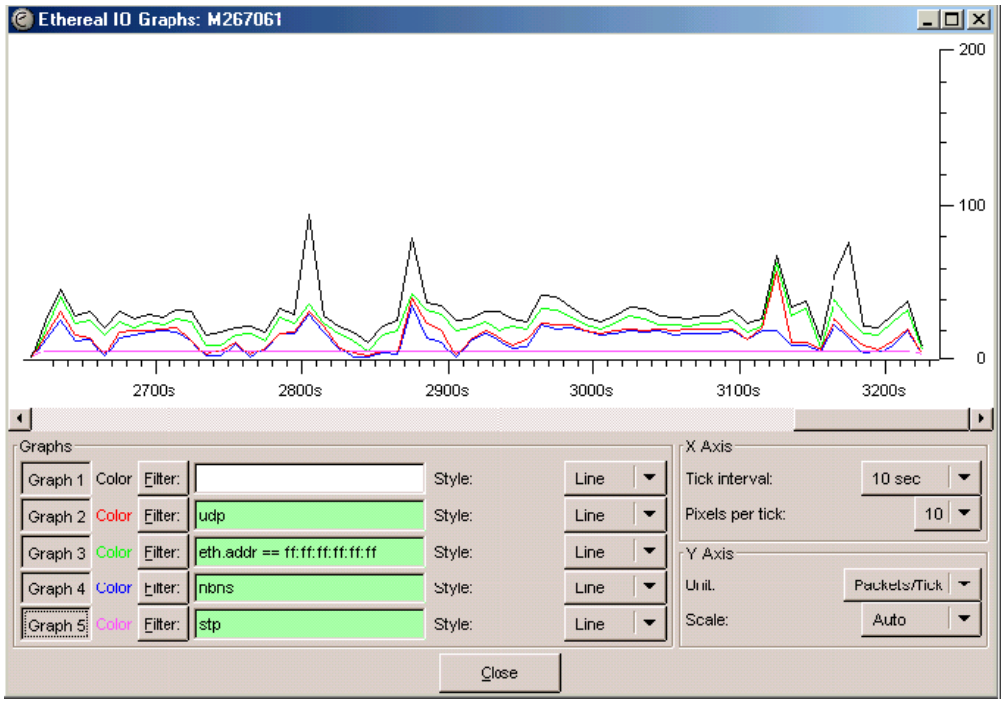


Figura 3.13. Gráfico de paquetes capturados en el Switch SW-D-LINK-DES-1016 de la captura de tráfico 1 de la tabla 3.1

Fuente: Ethereal.

Como podemos observar el tráfico de broadcast se genera en gran cantidad y en una forma constante, también hay gran cantidad paquetes que corresponden a NBNS y también se genera de forma constante los paquetes que pertenecen a STP.

En figura 3.14 se muestra el resumen de la captura de tráfico 2 de la tabla 3.8 realizada en el Switch Unidad de Finanzas.

En la figura se podrá observar que el consumo del ancho de banda es del 0.002% del total del ancho de banda, esto nos da una pauta para determinar que la red se encuentra e buen estado.

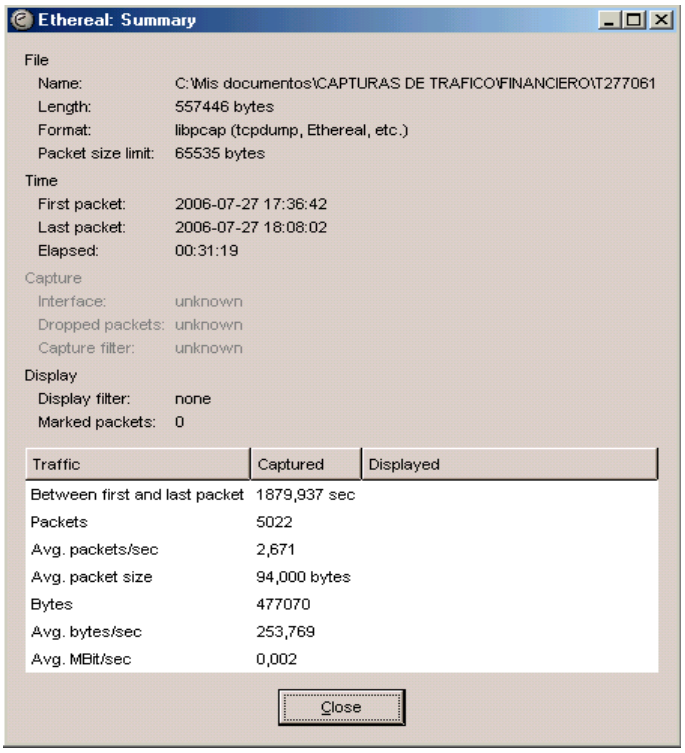


Figura 3.14. Resumen de captura de tráfico realizada en el Switch SW-D-LINK-DES-1016.

Fuente: Ethereal.

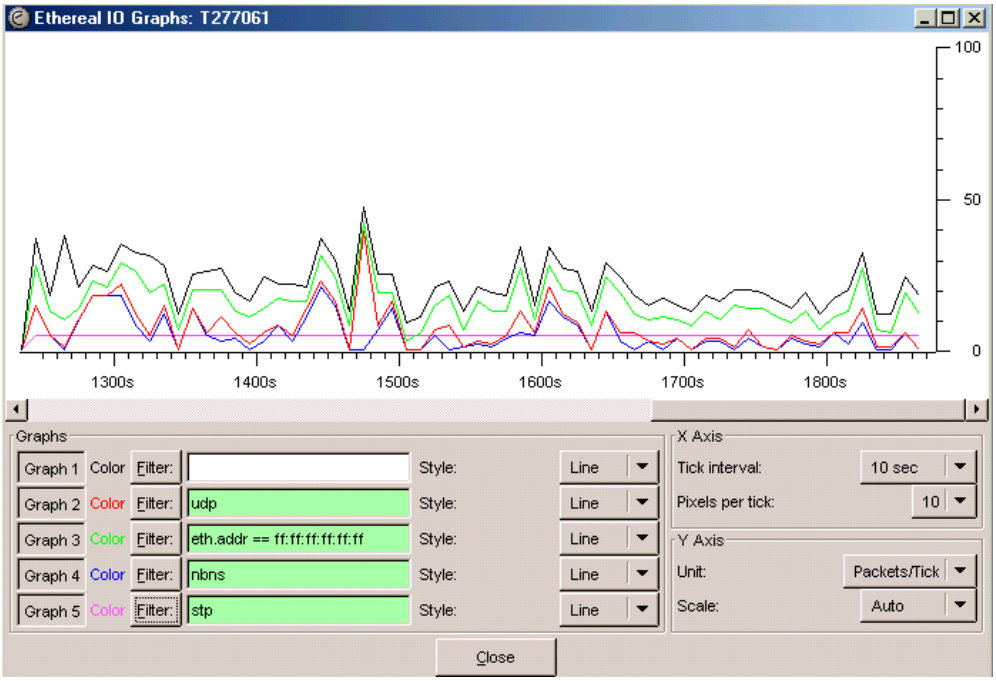


Figura 3.15. Gráfico de paquetes capturados en el Switch SW-D-LINK-DES-1016 de la captura de tráfico 2 de la tabla 3.1

Fuente: Ethereal.

De igual forma en la figura 3.15 podemos observar los diferentes protocolos que circulan en mayor cantidad por la red Lan.

En el gráfico se observa que los paquetes de TCP se distinguen con una línea de color negro, este tipo de tráfico es constante y se genera en gran cantidad, ya que en el departamento financiero se realizan varias

actividades diariamente, por parte de las personas que laboran en este departamento.

Los paquetes UDP están con color rojo, este protocolo se genera en gran cantidad, y es el principalmente utiliza el antivirus para realizar todas las tareas que tiene programado.

El tráfico de Broadcast se encuentra identificado con color verde, este tipo de tráfico es constante.
Con color azul se encuentran los paquetes que pertenecen a NBNS, este tipo de tráfico se genera porque en este departamento hay máquinas que no están sincronizadas con el servidor de antivirus, y esto hace que se de este tipo de tráfico.

De color lila se encuentran los paquetes del protocolo STP, este tipo de tráfico se da porque en el switch esta habilitada la opción de STP, y siempre se generará este protocolo.

3.3.3 ANÁLISIS DEL TRÁFICO EN EL SWITCH LTG-SW-CD8-01-COR DEL CENTRO DE PRODUCCIÓN.

3.3.3.1 MÓDULO DE CAPTURA

En este módulo hemos realizado la captura de los paquetes que se genera en el switch que se encuentra en el centro de producción, este monitoreo se lo realizó en diferentes días y periodos de tiempo

A continuación se detallará la captura de tráfico realizada en el switch LTG-SW-CD8-01-COR.

3.3.3.1.1 Capturas de tráfico realizadas en el Switch LTG-SW-CD8-01-COR.

En la tabla 3.9 se describen las capturas de tráfico realizadas en el Switch LTG-SW-CD8-01-COR.

LTG-SW-CD8-01-COR		
N° DE CAPTURA	**FECHA**	**DETALLE**
1	26 de Julio de 2006	Realizado en la mañana

Tabla 3.9. Captura de tráfico del SWITCH LTG-SW-CD8-01-COR.
Autor: Javier Cayo.

En el Anexo D se detalla cada uno de los diferentes paquetes que se capturaron en el Switch LTG-SW-CD8-01-COR.

En el Anexo E se muestra de forma gráfica para mayor comprensión, como se realizó la captura de tráfico en el Switch LTG-SW-CD8-01-COR.

3.3.3.2 MÓDULO DE PREPROCESADO.

En el módulo de preprocesado se eliminará el tráfico innecesario de la captura que se realizó.

Luego de haber realizado la captura de tráfico, se determina que las diferentes capturas de tráfico realizadas en switch, circulan la misma clase de paquetes en toda la red. Por lo que no es necesario eliminar ninguno de los paquetes que están circulando por la red ya que todos nos van a servir para realizar un mejor análisis.

Como parte del módulo de preprocesado tenemos varias etapas, las que se detallarán a continuación:

3.3.3.2.1 Análisis de Seguridad

La primera etapa es el análisis de seguridad, en esta etapa se va a dividir el tráfico capturado en dos clases que son: tráfico convencional y tráfico sospechoso.

3.3.3.2.1.1 Tráfico Convencional

1. Entre el tráfico convencional tenemos los paquetes TCP/IP los mismos que como sabemos sirven para establecer la comunicación entre las diferentes estaciones de trabajo por ende no presentan peligro alguno para el correcto funcionamiento de la

red, y no representan un consumo elevado del ancho de banda.

Gracias al analizador de red Ethereal se ha determinado las aplicaciones que generan el tráfico TCP son las siguientes:

- El sistema Olympo que utilizan las personas que laboran en las oficinas del Centro de Producción.
- Las páginas de Internet que se manejan diariamente.
- El Sistema Siabuc que se maneja en la bibilioteca.

De esta forma es como se maneja el protocolo TCP en la Unidad de Finanzas, es el que más se utiliza en las diferentes aplicaciones que se describieron anteriormente en switch del Centro de Producción.

2. También tenemos los paquetes HTTP, los mismos que se generan cuando los usuarios navegan en el Internet lo que permite la comunicación, transferencia de archivos de las páginas Web que utilizan los usuarios, de la misma forma este tipo de protocolos no representan peligro para el buen funcionamiento de la red, de acuerdo al

análisis que se realizó mediante Ethereal no consumen mucho ancho de banda.

Como se explicó anteriormente este tipo de tráfico lo generan las diferentes páginas Web que se manejan en la Institución.

3. Otro de los paquetes que pertenecen al tráfico convencional es el DNS el mismo que está en el grupo de TCP/IP y permite la resolución de nombres de direcciones al momento que se navega en el Internet, es por eso que este protocolo es muy común y necesario, no va a representar peligro alguno para la red.

   Los protocolos anteriormente mencionados son los que pertenecen al tráfico convencional, dichos protocolos se han capturado en el Switch que se encuentra en el Centro de Producción de la Escuela Politécnica del Ejército Sede Latacunga.

   En las tablas que se presentarán a continuación, se muestra de forma detallada el número de paquetes, el ancho de banda que consumen, en el switch LTG-SW-CD8-01-COR que se encuentra junto al Centro de Producción de la Escuela Politécnica del Ejército Sede Latacunga y pertenecen al tráfico convencional.

Tráfico Convencional				
Switch	**N° de Captura**	**Protocolo**	**N° de Paquetes**	**Ancho de Banda**
LTG-SW-CD8-01-COR	1	HTTP	105	0.000111
LTG-SW-CD8-01-COR	1	DNS	44	0.000011

Tabla 3.10. Resumen del tráfico convencional en el Switch LTG-SW-CD1-04-ACC.

Autor: Javier Cayo.

3.3.3.2.1.2 Tráfico Sospechoso

Como parte de la primera etapa del módulo de preprocesado tenemos también el tráfico sospechoso, este tipo de tráfico es el que puede ocasionar peligro, riesgo, esto no permitirá el buen funcionamiento de la red, estos paquetes los hemos escogido de las diferentes capturas que se ha realizado.

1. Entre el tráfico sospechoso tenemos que en todas las capturas de tráfico realizadas se detectó que se genera una gran cantidad de tráfico de broadcast como una de las principales novedades que se encontró en el switch. Los paquetes del tráfico de broadcast no ocupan mucho espacio del ancho de banda que dispone la Institución, pero

genera inquietud ya que como se mencionó anteriormente es una cantidad considerable el tráfico de broadcast que se genera en la red.

Este tipo de tráfico lo generan todas las estaciones de trabajo que pertenecen al Centro de Producción, ya que al momento que quieren establecer comunicación con un servidor o con una computadora, mandan mensajes de tipo ARP que es el protocolo que permite que se resuelva la dirección de la máquina que se quiere localizar.

2. Otro de los protocolos que se encontró como parte del tráfico sospechoso es el NBNS, este protocolo se genera en gran cantidad, de ahí que de 12511 paquetes que se capturó 4837 son del protocolo NBNS, y no es común que este protocolo se genere en esa cantidad en la red, es por eso que se a puesto en el grupo del tráfico sospechoso.

   Este tipo de protocolo se genera a partir del servidor de antivirus, es así que al momento de realizar la captura de tráfico con el analizador Ethereal, tenemos como resultado que la dirección de origen es la que pertenece al servidor de antivirus y la dirección destino es una tipo broadcast.

Se debe revisar el funcionamiento el antivirus, para determinar el porque se genera en gran cantidad el protocolo NBNS, de esta forma se podrá optimizar el ancho de banda de la red.

Los 2 protocolos que se describieron anteriormente son los que se generan en mayor cantidad en el switch, por ende se les va dar mayor prioridad para poder presentar la solución más adecuada en el próximo capítulo, lo que permitirá que la red funcione de mejor forma y no se desperdicie el ancho de banda, de esta forma estamos optimizando el ancho de banda que se dispone en la Escuela Politécnica del Ejército Sede Latacunga.

3. También entre el tráfico sospechoso de la red tenemos la presencia del protocolo STP, se genera de una forma considerable en todas las capturas de tráfico que se realizaron en las distintas áreas de la Institución.

4. También tenemos la presencia del protocolo Browser, este protocolo se genera en todas las capturas que se realizó. Podemos citar que como ejemplo se tomó una captura de tráfico y con la ayuda de Ethereal determinamos que de 3050 paquetes capturados 250 pertenecen al protocolo

Browser, estas cantidades son una referencia de dicho protocolo.

El protocolo Browser se genera cuando desde una computadora se manda a imprimir un documento, este protocolo ayuda a buscar la ubicación de la impresora y de esta forma imprimir el documento que ha sido enviado.

5. En este dispositivo se genera el protocolo CDP, ya que es un dispositivo Cisco.

En la tabla que se presentará a continuación, se muestra de forma detallada el número de paquetes, el ancho de banda que consumen, en el switch que se encuentra en la Unidad de Finanzas de la Escuela Politécnica del Ejército Sede Latacunga y pertenecen al tráfico sospechoso.

Tráfico Sospechoso				
Switch	**Nº de Captura**	**Protocolo**	**Nº de Paquetes**	**Ancho de Banda**
LTG-SW-CD8-01-COR	1	Broadcast	2209	0.000001
LTG-SW-CD8-01-COR	1	NBNS	4837	0.001000
LTG-SW-CD8-01-COR	1	Browser	725	0.000001
LTG-SW-CD8-01-COR	1	STP	1800	0.000001

Tabla 3.11. Resumen del Tráfico Sospechoso en el Switch LTG-SW-CD8-01-COR.

Fuente: Ethereal.

3.3.3.2.2 Etapa de Clasificación

En la segunda etapa del módulo de preprocesado el tráfico convencional que se detalló anteriormente, va ser clasificado en base a las direcciones IP de las máquinas que están conectadas al switch LTG-SW-CD8-01-COR.

A continuación se detallará las direcciones IP de las diferentes estaciones de trabajo del switch LTG-SW-CD8-01-COR, son el resultado de haber realizado la captura de tráfico con el analizador de red Ethereal.

En las tablas que se detallarán a continuación se muestra la dirección IP de la máquina, el total de paquetes y el porcentaje del ancho de banda que consume cada paquete que pasa por la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

3.3.3.2.2.1 SWITCH LTG-SW-CD8-01-COR

En la tabla 3.12 se muestra las direcciones IP del protocolo TCP, esta información se tomó de la captura de tráfico 1 de la tabla 3.9 que corresponde al Switch LTG-SW-CD8-01-COR.

En la tabla antes mencionada se muestra, que de un total de 12511 paquetes, 2007 pertenecen al protocolo TCP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.0.30	936	0.000268
10.2.0.5	808	0.000231
10.2.0.3	330	0.000094
10.2.1.153	320	0.000092
10.2.0.2	132	0.000038
207.46.248.112	119	0.000034
207.46.248.240	119	0.000034
64.235.53.203	81	0.000023
69.45.79.9	78	0.000022
207.46.250.101	66	0.000019
10.2.0.9	66	0.000019
207.46.208.105	59	0.000017
10.2.0.162	51	0.000015
10.2.0.152	44	0.000013
10.2.1.91	42	0.000012
10.2.0.91	41	0.000012
10.2.0.181	34	0.000010
10.2.0.178	34	0.000010
10.2.0.171	33	0.000009
10.2.0.21	30	0.000009
207.46.196.100	30	0.000009
10.2.0.184	29	0.000008
200.41.8.16	28	0.000008
10.2.0.176	27	0.000008
10.2.0.4	27	0.000008
10.2.0.106	27	0.000008
207.46.248.236	24	0.000007
10.2.0.93	24	0.000007
10.2.0.172	24	0.000007
207.46.196.121	22	0.000006
10.2.1.61	22	0.000006
10.2.1.154	22	0.000006
10.2.0.23	21	0.000006
10.2.0.116	21	0.000006
10.2.0.142	20	0.000006
10.2.0.61	18	0.000005
10.1.0.105	18	0.000005
10.2.1.181	15	0.000004
10.2.0.224	13	0.000004
10.2.0.186	13	0.000004
10.2.0.64	9	0.000003
10.2.0.31	9	0.000003

10.2.0.161	7	0.000002
10.2.0.83	7	0.000002
10.2.0.151	5	0.000001
10.2.1.111	5	0.000001
10.2.1.186	4	0.000001
169.254.9.229	4	0.000001
10.2.1.197	3	0.000001
10.2.0.41	2	0.000001
193.238.162.16	1	0.000000
10.2.0.194	1	0.000000
10.2.0.32	1	0.000000
TOTAL	**3940**	**0.001113**

Tabla 3.20. Direcciones IP del Protocolo TCP del Switch LTG-SW-CD8-01-COR de la captura de tráfico 1 de la tabla 3.9.

En la tabla 3.13 se muestra las direcciones IP del puerto UDP, se tomó de la captura de tráfico 1, de la tabla 3.9 que corresponde al Centro de Producción.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.1.255	5481	0.001525
10.2.0.5	4221	0.001174
10.2.0.3	151	0.000042
10.2.0.2	90	0.000025
10.2.0.9	88	0.000024
10.2.0.4	74	0.000021
10.2.0.30	73	0.000020
10.2.0.64	44	0.000012
10.2.0.132	34	0.000009
10.2.0.224	34	0.000009
10.2.0.23	34	0.000009
10.2.0.162	32	0.000009
10.2.0.184	31	0.000009
10.2.0.43	30	0.000008
192.188.58.163	29	0.000008
10.2.0.176	29	0.000008
10.2.0.101	29	0.000008
10.2.0.116	28	0.000008
10.2.0.21	27	0.000008
10.2.1.101	27	0.000008
10.2.0.151	27	0.000008
10.2.0.185	26	0.000007
10.2.0.172	25	0.000007
10.2.0.83	25	0.000007

10.2.0.93	24	0.000007
10.2.0.31	23	0.000006
10.2.1.91	23	0.000006
10.2.0.51	22	0.000006
10.2.1.197	22	0.000006
10.2.0.171	21	0.000006
10.2.1.196	20	0.000006
10.2.1.186	19	0.000005
255.255.255.255	19	0.000005
10.2.0.41	18	0.000005
10.2.0.152	18	0.000005
10.2.1.181	17	0.000005
10.2.1.154	14	0.000004
10.2.0.53	14	0.000004
10.2.0.106	13	0.000004
10.2.0.91	12	0.000003
10.2.1.151	12	0.000003
10.2.1.183	12	0.000003
10.2.1.111	12	0.000003
10.2.1.155	12	0.000003
10.2.0.63	12	0.000003
10.2.1.61	11	0.000003
10.2.0.61	7	0.000002
10.2.1.153	7	0.000002
10.2.0.181	6	0.000002
10.2.0.142	6	0.000002
10.2.0.186	5	0.000001
10.2.1.152	5	0.000001
200.105.255.2	5	0.000001
TOTAL	11106	0.003087

Tabla 3.12. Direcciones IP del Protocolo TCP del Switch LTG-SW-CD8-01-COR de la captura de tráfico 1, de la tabla 3.9.

Fuente: Ethereal.

3.3.3.3 MÓDULO DE CONSOLIDACIÓN.

El siguiente paso en la metodología Mira, tenemos al módulo de consolidación, en este módulo vamos a consolidar los resultados parciales de la captura de tráfico realizada en el Switch LTG-SW-CD8-01-COR.

3.3.3.3.1 SWITCH LTG-SW-CD8-01-COR

En la tabla 3.14 se muestra de una forma detallada la captura de tráfico que se realizó en el SWITCH LTG-SW-CD8-01-COR.

SWITCH LTG-SW-CD8-01-COR			
Nº DE CAPTURA	**FECHA**	**TIEMPO DE CAPTURA**	**NUMERO DE PAQUETES**
1	26 de Julio de 2006	60 Minutos	12511 Paquetes

Tabla 3.14. Detalle de la captura de tráfico realizada en el SWITCH LTG-SW-CD8-01-COR.

Fuente: Ethereal.

3.3.3.4 MÓDULO DE CLASIFICACIÓN

En este módulo se clasificará el tráfico que se ha capturado en diferentes categorías.

- **Primera Categoría.-** La primera categoría que se ha identificado, es el traficó normal o convencional el mismo que ya se detalló en el módulo de preprocesado.
  Este tipo de tráfico es el que no representa peligro alguno para el buen desenvolvimiento de la red, este tipo de tráfico se genera en todas las estaciones de trabajo se conectan al Switch LTG-SW-CD8-01-COR.

  A continuación vamos a citar los protocolos que se han tomado en cuenta en el tráfico normal, tenemos al protocolo TCP, el protocolo UDP, el protocolo HTTP, el protocolo DNS.

- **Segunda Categoría.-** La segunda categoría que podemos identificar es el tráfico administrativo, el mismo que produce cada una de las estaciones de trabajo que pertenecen a la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga.

  Este tipo de tráfico lo generan las diferentes aplicaciones que se utilizan todos los días, en los diferentes departamentos de la Escuela Politécnica del Ejército Sede Latacunga, entre las aplicaciones tenemos:

  - Sistema Olympo
  - Antivirus Kaspersky

- **Tercera Categoría.-** Otra categoría que se ha identificado y se puede decir que es una de las más importantes y nos da la idea principal para saber que problemas tiene nuestra red, es la del tráfico indeterminado, este tipo de tráfico se produce en gran cantidad en la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga, el tráfico indeterminado se ha logrado identificar en todas las capturas de tráfico que se han realizado en los diferentes departamentos de la Institución, y es lo que más inquietud produce ya que se generan varios protocolos no muy usuales para el correcto funcionamiento de la red, los protocolos que se encuentran en esta categoría son: el broadcast, NBNS, STP, BROWSER, estos protocolos ocupan el ancho de banda de la red, el espacio que utilizan no es muy considerable pero sería mejor que este tipo de tráfico de

red no se de y de esta forma el espacio que estos protocolos utilizan sería distribuido de mejor forma entre las demás aplicaciones que necesitan el ancho de banda para un correcto y rápido funcionamiento.

3.3.3.5 MÓDULO DE POSTPROCESADO

Luego de haber realizado la clasificación del tráfico podemos continuar con el módulo de postprocesado aquí se va realizar informes de forma general de los diferentes resultados que hemos conseguido luego de haber capturado el tráfico en el switch LTG-SW-CD8-01-COR.

Con la ayuda del analizador de red Ethereal se presenta los diferentes informes y gráficos del monitoreo de la red, de esta forma ya se puede dar un análisis del estado en el que se encuentra la red.

Para realizar este módulo, vamos a tomar como referencia las capturas de tráfico de red del módulo de consolidación.

3.3.5.1 Estadísticas del SWITCH LTG-SW-CD8-01-COR.

En figura 3.16 se muestra el resumen de la captura de tráfico realizada en el Switch LTG-SW-CD8-01-COR.

En esta figura se puede observar que el consumo del ancho de banda es del 0.004% del total del ancho de banda.

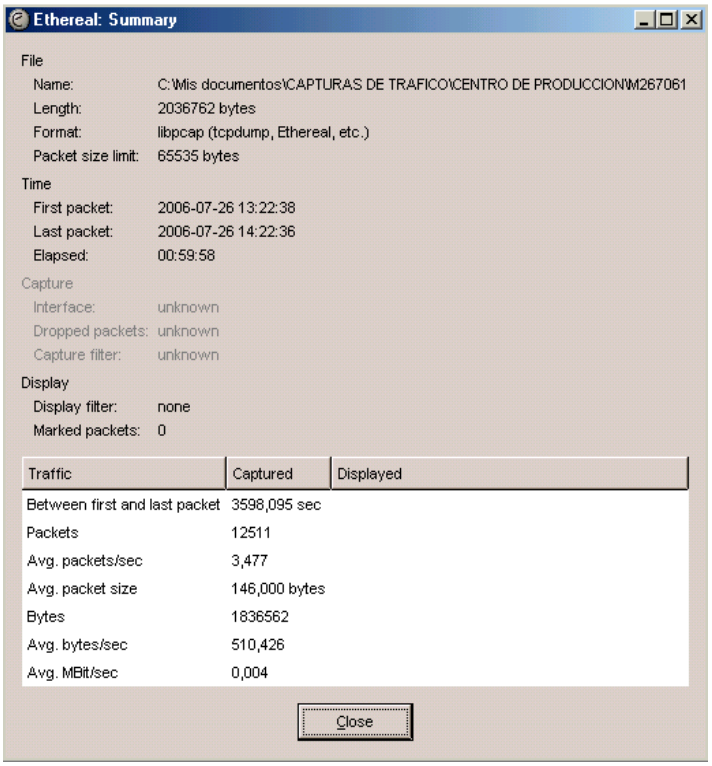


Figura 3.16. Resumen de los paquetes capturados en el Switch LTG-SW-CD8-01-COR.

Fuente: Ethereal.

En la Figura 3.17 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo, estos paquetes se los representa en líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico es constante, se genera en gran cantidad, este tipo de tráfico se da ya que, desde la biblioteca se realizan varias transacciones por lo que interactúan con la base de datos.

Este tipo de tráfico también lo generan desde las estaciones de trabajo que se encuentran en el centro de

producción, ya que en este centro utilizan diariamente el software Olympo.

Los paquetes UDP están con color rojo, se genera constantemente ya que es la base para que se genere el protocolo NBNS.

El tráfico de Broadcast se encuentra identificado con color verde, se genera en gran cantidad, ya que las estaciones de trabajo siempre están interactuando con los servidores o con las demás estaciones trabajo.

Con color azul se encuentran los paquetes que pertenecen a NBNS, este protocolo se genera porque existen estaciones de trabajo que no se están registradas en el servidor de antivirus o a su vez están con sistemas operativos Windows 95 0 98 por esta razón no es posible instalar el antivirus.

De color lila se encuentran los paquetes del protocolo STP, este protocolo es constante, ya que en los switches esta habilitada la opción del STP.

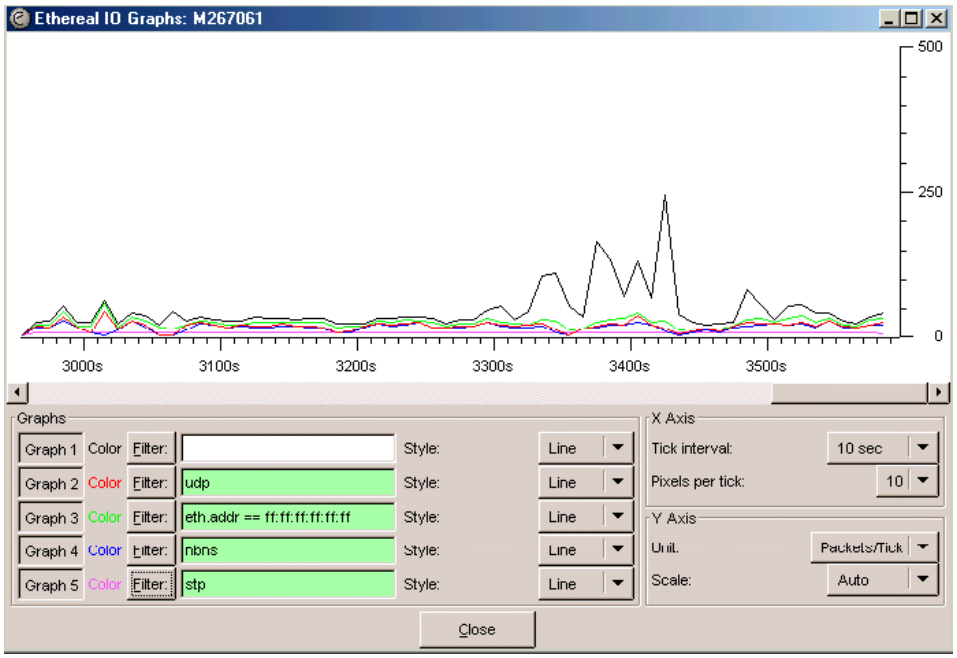


Figura 3.17 Gráfico de paquetes capturados en el Switch SW-D-LINK-DES-1016 de la captura de tráfico 1 de la tabla 3.14.

Fuente: Ethereal.

En este Switch no hay problemas de consideración, que afecten al buen funcionamiento de la red, ya que el consumo del ancho de banda no es elevado ya que a este switch están conectadas pocas computadoras.

3.3.4 ANÁLISIS DEL TRÁFICO EN EL SWITCH LTG-SW-CD2-01-COR.

3.3.4.1 MÓDULO DE CAPTURA

En este módulo hemos realizado las capturas de tráfico de los paquetes que se genera en el switch que se

encuentra en el centro de datos1, este monitoreo se lo realizó en diferentes días y periodos de tiempo

A continuación se detallará la captura de tráfico realizada en el switch LTG-SW-CD2-01-COR.

3.3.4.1.1 Capturas de tráfico realizadas en el Switch LTG-SW-CD2-01-COR.

En el rack principal se encuentra el switch LTG-SW-CD1-02-ACC, a este switch se encuentran conectados los siguientes grupos de trabajo:

- Departamento de Lenguas.
- Subdirección.
- Dirección.
- Unidad de Desarrollo Humano.
- Unidad de Marketing.

En la tabla 3.15 se detallan las capturas de tráfico que se realizaron en el switch LTG-SW-CD1-02-ACC.

LTG-SW-CD1-02-ACC

Nº DE CAPTURA	**FECHA**	**DETALLE**
1	25 de Julio de 2006	Realizado en la tarde
2	25 de Julio de 2006	Realizado en la tarde
3	25 de Julio de 2006	Realizado en la tarde
4	28 de Julio de 2006	Realizado en la mañana

Tabla 3.15. Captura de tráfico realizada en el Switch LTG-SW-CD1-02-ACC.

Autor: Javier Cayo.

En el Anexo F se detalla cada uno de los diferentes paquetes que se capturaron desde el switch LTG-SW-CD1-02-ACC.

En el Anexo G se muestra de forma gráfica para mayor comprensión, como se realizó la captura de tráfico en el switch LTG-SW-CD1-02-ACC.

3.3.4.2 MÓDULO DE PREPROCESADO.

En el módulo de preprocesado se eliminará el tráfico innecesario de la captura que se realizó.

Luego de haber realizado la captura de tráfico, se determina que las diferentes capturas de tráfico realizadas en switch LTG-SW-CD1-02-ACC, podemos decir que circulan la misma clase de paquetes en toda la red. Por lo que no es necesario eliminar ninguno de los paquetes que están circulando por la red ya que todos nos van a servir para realizar un mejor análisis.

Como parte del módulo de preprocesado tenemos varias etapas, las que se detallarán a continuación:

3.3.4.2.1 Análisis de Seguridad

La primera etapa es el análisis de seguridad, en esta etapa se va a dividir el tráfico capturado en dos clases que son: tráfico convencional y tráfico sospechoso.

3.3.4.2.1.1 Tráfico Convencional

1. Entre el tráfico convencional tenemos los paquetes TCP/IP los mismos que como sabemos sirven para establecer la comunicación entre las diferentes estaciones de trabajo por ende no presentan peligro alguno para el correcto funcionamiento de la red, y no representan un consumo elevado del ancho de banda.

   Gracias al analizador de red Ethereal se ha determinado las aplicaciones que generan el tráfico TCP son las siguientes:

   - Las páginas de Internet que se manejan diariamente.
   - Antivirus Kaspersky.

2. También tenemos los paquetes HTTP, los mismos que se generan cuando los usuarios navegan en el Internet lo que permite la comunicación, transferencia de archivos de las páginas Web que utilizan los usuarios, de

la misma forma este tipo de protocolos no representan peligro para el buen funcionamiento de la red, de acuerdo al análisis que se realizó mediante Ethereal no consumen mucho ancho de banda.

Como se explicó anteriormente este tipo de tráfico lo generan las diferentes páginas Web que se manejan en la Institución.

3. Otro de los paquetes que pertenecen al tráfico convencional es el DNS el mismo que está en el grupo de TCP/IP y permite la resolución de nombres de direcciones al momento que se navega en el Internet, es por eso que este protocolo es muy común y necesario, no va a representar peligro alguno para la red.

Los protocolos anteriormente mencionados son los que pertenecen al tráfico convencional, dichos protocolos se han capturado en el Switch LTG-SW-CD1-02-ACC de la Escuela Politécnica del Ejército Sede Latacunga.

En las tablas que se presentarán a continuación, se muestra de forma detallada el número de paquetes, el ancho de banda que consumen, en el switch LTG-SW-CD1-02-ACC que se encuentra junto al Centro de

datos 1 pertenecientes al tráfico convencional.

Tráfico Convencional				
Switch	**Nº de Captura**	**Protocolo**	**Nº de Paquetes**	**Ancho de Banda**
LTG-SW-CD1-02-ACC	1	HTTP	29	0.000001
LTG-SW-CD1-02-ACC	1	DNS	162	0.000111
LTG-SW-CD1-02-ACC	2	HTTP	0	0.000000
LTG-SW-CD1-02-ACC	2	DNS	0	0.000000
LTG-SW-CD1-02-ACC	3	HTTP	0	0.000000
LTG-SW-CD1-02-ACC	3	DNS	0	0.000000

Tabla 3.16. Resumen del tráfico convencional en el Switch LTG-SW-CD1-02-ACC.

Autor: Javier Cayo.

3.3.4.2.1.2 Tráfico Sospechoso

Como parte de la primera etapa del módulo de preprocesado tenemos también el tráfico sospechoso, este tipo de tráfico es el que puede ocasionar peligro, riesgo, por lo que no permitirá el buen funcionamiento de la red, estos paquetes los hemos escogido de las diferentes capturas que se ha realizado.

1. Entre el tráfico sospechoso tenemos que en todas las capturas de tráfico realizadas se detectó en gran cantidad el tráfico de broadcast.

Los paquetes del tráfico de broadcast no ocupan mucho espacio del ancho de banda que dispone la Institución, pero genera inquietud ya que como se mencionó anteriormente es una cantidad considerable el tráfico de broadcast que se genera en la red.

Este tipo de tráfico lo generan todas las estaciones de trabajo que pertenecen al Switch LTG-SW-CD1-02-ACC, ya que al momento que quieren establecer comunicación con un servidor o con una computadora, mandan mensajes de tipo ARP que es el protocolo que permite que se resuelva la dirección de la máquina que se quiere localizar.

2. Otro de los protocolos que se encontró como parte del tráfico sospechoso es el NBNS, este protocolo se genera en gran cantidad, de ahí que de 5366 paquetes que se capturó 2476 son del protocolo NBNS, y no es común que este protocolo se genere en esa cantidad en la red, es por eso que se a puesto en el grupo del tráfico sospechoso.

   Este tipo de protocolo se genera a partir del servidor de antivirus, es así que al momento de realizar la captura de tráfico con el analizador Ethereal, tenemos como resultado que la dirección de origen es la

que pertenece al servidor de antivirus y la dirección destino es una tipo broadcast.

Se debe revisar el funcionamiento el antivirus, para determinar el porque se genera en gran cantidad el protocolo NBNS, de esta forma se podrá optimizar el ancho de banda de la red.

Los 2 protocolos que se describieron anteriormente son los que se generan en mayor cantidad en el switch, por ende se les va dar mayor prioridad para poder presentar la solución más adecuada en el próximo capítulo, lo que permitirá que la red funcione de mejor forma y no se desperdicie el ancho de banda, de esta forma estamos optimizando el ancho de banda que se dispone en la Escuela Politécnica del Ejército Sede Latacunga.

3. También entre el tráfico sospechoso de la red tenemos la presencia del protocolo STP, se genera de una forma considerable en todas las capturas de tráfico que se realizaron en las distintas áreas de la Institución.
4. También tenemos la presencia del protocolo Browser, este protocolo se genera en todas las capturas que se realizó.

El protocolo Browser se genera cuando desde una computadora se manda a imprimir un documento, este protocolo ayuda a buscar la ubicación de la impresora y de esta forma imprimir el documento que ha sido enviado.

Tráfico Sospechoso				
Switch	**Nº de Captura**	**Protocolo**	**Nº de Paquetes**	**Ancho de Banda**
LTG-SW-CD1-02-ACC	1	Broadcast	1020	0.000001
LTG-SW-CD1-02-ACC	1	NBNS	2476	0.001000
LTG-SW-CD1-02-ACC	1	Browser	355	0.000000
LTG-SW-CD1-02-ACC	1	STP	788	0.000001
LTG-SW-CD1-02-ACC	2	Broadcast	431	0.000000
LTG-SW-CD1-02-ACC	2	NBNS	569	0.000100
LTG-SW-CD1-02-ACC	2	Browser	83	0.000000
LTG-SW-CD1-02-ACC	2	STP	263	0.000000
LTG-SW-CD1-02-ACC	3	Broadcast	211	0.000000
LTG-SW-CD1-02-ACC	3	NBNS	459	0.000100
LTG-SW-CD1-02-ACC	3	Browser	59	0.000000
LTG-SW-CD1-02-ACC	3	STP	155	0.000000

Tabla 3.17. Resumen del Tráfico Sospechoso en el Switch LTG-SW-CD1-04-ACC.

Autor: Javier Cayo.

3.3.4.2.2 Etapa de Clasificación

En la segunda etapa del módulo de preprocesado el tráfico convencional que se detalló anteriormente, va ser clasificado en base a las direcciones IP de las máquinas que están conectadas al switch LTG-SW-CD1-02-ACC.

A continuación se detallará las direcciones IP de las diferentes estaciones de trabajo del switch LTG-SW-CD1-02-ACC, son el resultado de haber realizado la captura de tráfico con el analizador de red Ethereal.

En las tablas que se detallarán a continuación se muestra la dirección IP de la máquina, el total de paquetes y el porcentaje del ancho de banda que consume cada paquete que pasa por la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

3.3.4.2.2.1 SWITCH LTG-SW-CD1-02-ACC

A continuación se detallará las diferentes direcciones IP de los equipos que usan el Protocolo TCP y el protocolo UDP, los datos son tomados de la captura de tráfico 2 de la tabla 3.15 correspondiente al Switch LTG-SW-CD1-02-ACC.

En la tabla 3.18 se puede observar las direcciones IP de las máquinas que utilizan el protocolo TCP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.0.30	288	0.000184
10.2.0.5	131	0.000084
64.233.179.104	117	0.000075
10.2.2.4	99	0.000063
10.2.0.172	36	0.000023
10.2.0.91	18	0.000012
10.2.0.9	10	0.000006
161.114.198.119	9	0.000006
10.2.0.106	8	0.000005
10.2.0.184	6	0.000004
10.2.0.116	6	0.000004
10.2.0.107	4	0.000003
TOTAL	**732**	**0.000469**

Tabla 3.18. Direcciones IP del Protocolo TCP del Switch LTG-SW-CD1-02-ACC de la captura de tráfico 2 de la tabla 3.15.

Fuente: Ethereal.

En la tabla 3.19 se detallan las direcciones IP de las máquinas que utilizan el protocolo UDP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.1.255	2193	0.001392
10.2.0.5	1638	0.001040
169.254.255.255	609	0.000389
169.254.7.148	443	0.000281
10.2.0.30	178	0.000113
169.254.211.46	166	0.000105
192.188.58.163	157	0.000100
10.2.0.3	69	0.000044
255.255.255.255	55	0.000035
10.2.0.9	37	0.000023
10.2.0.4	33	0.000021
10.2.0.2	33	0.000021
10.2.0.224	33	0.000021
10.2.1.197	17	0.000011
10.2.0.21	15	0.000010

10.2.0.43	14	0.000009
10.2.1.186	14	0.000009
10.2.0.116	14	0.000009
10.2.0.31	13	0.000008
10.2.0.184	13	0.000008
10.2.0.64	12	0.000008
10.2.0.202	12	0.000008
10.2.0.162	11	0.000007
10.2.0.172	11	0.000007
10.2.1.91	11	0.000007
10.2.0.23	11	0.000007
10.2.0.24	11	0.000007
10.2.0.151	10	0.000006
10.2.0.83	10	0.000006
10.2.0.52	9	0.000006
10.2.0.152	8	0.000005
10.2.1.155	7	0.000004
10.2.0.94	7	0.000004
10.2.0.32	7	0.000004
10.2.1.173	7	0.000004
10.2.1.121	7	0.000004
10.2.0.185	7	0.000004
10.2.0.132	7	0.000004
10.2.0.154	7	0.000004
10.2.0.171	7	0.000004
10.2.0.186	7	0.000004
10.2.0.181	7	0.000004
10.2.1.181	6	0.000004
10.2.0.71	4	0.000003
10.2.0.107	4	0.000003
10.2.1.51	4	0.000003
10.255.255.255	4	0.000003
10.2.0.51	4	0.000003
10.2.0.106	4	0.000003
10.2.0.41	4	0.000003
200.105.225.2	4	0.000003
10.2.1.61	3	0.000002
10.2.1.31	3	0.000002
10.2.0.142	2	0.000001
10.2.0.61	2	0.000001
10.2.1.152	2	0.000001
10.2.0.178	2	0.000001
10.2.0.183	1	0.000001
239.255.255.250	1	0.000001
TOTAL	**5991**	**0.003805**

Tabla 3.19. Direcciones IP del Protocolo UDP del Switch LTG-SW-CD1-02-ACC de la captura de tráfico 2 de la tabla 3.15.

Fuente: Ethereal.

En las siguientes tablas se detallan las direcciones IP de las máquinas que utilizan el protocolo TCP y el protocolo UDP, los datos son tomados de la captura de tráfico 3 de la tabla 3.15 correspondiente al Switch LTG-SW-CD1-02-ACC.

En la tabla 3.20 se puede observar las direcciones IP de las máquinas que utilizan el protocolo TCP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.0.5	85	0.000173
10.2.0.30	78	0.000158
10.2.2.4	23	0.000047
10.2.0.41	17	0.000035
10.2.0.31	8	0.000016
10.2.0.181	6	0.000012
169.254.9.229	4	0.000008
10.2.0.51	3	0.000006
10.2.0.2	2	0.000004
10.2.1.197	1	0.000002
10.2.1.181	1	0.000002
TOTAL	**228**	**0.000463**

Tabla 3.20. Direcciones IP del Protocolo TCP del Switch LTG-SW-CD1-02-ACC de la captura de tráfico 3 de la tabla 3.15.

Fuente: Ethereal.

En la tabla 3.21 se muestra las direcciones IP de las máquinas que utilizan el protocolo UDP de la captura de tráfico 3 de la tabla 3.15.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.0.5	423	0.000803
10.2.1.255	557	0.001058
255.255.255.255	12	0.000023
10.2.0.131	1	0.000002
10.2.0.9	8	0.000015
10.2.0.186	4	0.000008
169.254.7.148	34	0.000065
169.254.211.46	41	0.000078
169.254.255.255	75	0.000142
10.2.0.21	4	0.000008
10.2.0.71	1	0.000002
10.2.0.224	6	0.000011
10.2.0.4	17	0.000032
10.2.0.184	6	0.000011
10.2.0.31	3	0.000006
10.2.0.30	5	0.000009
10.2.0.107	1	0.000002
10.2.0.151	4	0.000008
10.2.0.3	23	0.000044
10.2.0.24	5	0.000009
10.2.0.162	3	0.000006
10.2.0.116	3	0.000006
10.2.1.91	1	0.000002
10.2.0.43	3	0.000006
10.2.0.2	4	0.000008
10.2.0.172	1	0.000002
10.2.0.52	1	0.000002
10.2.0.152	9	0.000017
10.2.0.106	1	0.000002
10.2.0.23	4	0.000008
10.2.1.155	1	0.000002
10.2.0.64	3	0.000006
10.2.1.51	1	0.000002
10.255.255.255	1	0.000002
10.2.0.91	1	0.000002
10.2.0.202	1	0.000002
10.2.1.31	1	0.000002
10.2.0.32	1	0.000002
10.2.1.186	2	0.000004
10.2.1.151	1	0.000002
10.2.1.173	1	0.000001
10.2.0.83	3	0.000006
10.2.0.171	1	0.000002
10.2.0.93	1	0.000002
10.2.1.154	1	0.000002
TOTAL	**1286**	**0.002446**

Tabla 3.21. Direcciones IP del Protocolo UDP del Switch LTG-SW-CD1-02-ACC de la captura de tráfico 3 de la tabla 3.15.

Fuente: Ethereal.

3.3.4.3 MÓDULO DE CONSOLIDACIÓN.

El siguiente paso en la metodología Mira, tenemos al módulo de consolidación, en este módulo vamos a consolidar los resultados parciales de la captura de tráfico realizada en el Switch LTG-SW-CD1-02-ACC.

3.3.4.3.1 SWITCH LTG-SW-CD1-02-ACC

En la tabla 3.22 se muestra de una forma detallada las capturas de tráfico que se realizaron en el Switch LTG-SW-CD1-02-ACC.

LTG-SW-CD1-02-ACC			
N° DE CAPTURA	**FECHA**	**TIEMPO DE CAPTURA**	**NUMERO DE PAQUETES**
1	25 de Julio de 2006	27 Minutos	5366 Paquetes
2	25 de Julio de 2006	10 Minutos	1528 Paquetes
3	25 de Julio de 2006	13 Minutos	2173 Paquetes
4	28 de Julio de 2006	10 Minutos	1012 Paquetes

Tabla 3.22. Detalle de las capturas de tráfico realizadas en el Switch LTG-SW-CD1-02- ACC.

Fuente: Ethereal.

3.3.4.4 MÓDULO DE CLASIFICACIÓN

En este módulo se clasificará el tráfico que se ha capturado en diferentes categorías.

- **Primera Categoría.-** La primera categoría que se ha identificado, es el traficó normal o convencional el mismo que ya se detalló en el módulo de preprocesado.

  Este tipo de tráfico es el que no representa peligro alguno para el buen desenvolvimiento de la red, este tipo de tráfico se genera en todas las estaciones de trabajo se conectan al Switch LTG-SW-CD1-02-ACC.

  A continuación vamos a citar los protocolos que se han tomado en cuenta en el tráfico normal, tenemos al protocolo TCP, el protocolo UDP, el protocolo HTTP, el protocolo DNS.

- **Segunda Categoría.-** La segunda categoría que podemos identificar es el tráfico administrativo, el mismo que produce cada una de las estaciones de trabajo que pertenecen a la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga.

  Este tipo de tráfico lo generan las diferentes aplicaciones que se utilizan todos los días, en los diferentes departamentos de la Escuela Politécnica del Ejército Sede Latacunga, entre las aplicaciones tenemos:

  - Sistema Olympo
  - Antivirus Kaspersky

- **Tercera Categoría.-** Otra categoría que se ha identificado y se puede decir que es una de las más importantes y nos da la idea principal para saber que problemas tiene nuestra red, es la del tráfico indeterminado, este tipo de tráfico se produce en gran cantidad en la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga, el tráfico indeterminado se ha logrado identificar en todas las capturas de tráfico que se han realizado en los diferentes departamentos de la Institución, y es lo que más inquietud produce ya que se generan varios protocolos no muy usuales para el correcto funcionamiento de la red, los protocolos que se encuentran en esta categoría son: el broadcast, NBNS, STP, BROWSER, estos protocolos ocupan el ancho de banda de la red, el espacio que utilizan no es muy considerable pero sería mejor que este tipo de tráfico de red no se de y de esta forma el espacio que estos protocolos utilizan sería distribuido de mejor forma entre las demás aplicaciones que necesitan el ancho de banda para un correcto y rápido funcionamiento.

3.3.4.5 MÓDULO DE POSTPROCESADO

Luego de haber realizado la clasificación del tráfico podemos continuar con el módulo de postprocesado aquí se va realizar informes de forma general de los diferentes resultados que hemos conseguido luego de haber capturado el tráfico en el switch LTG-SW-CD1-02-ACC.

Con la ayuda del analizador de red Ethereal se presenta los diferentes informes y gráficos del monitoreo de la red, de esta forma ya se puede dar un análisis del estado en el que se encuentra la red.

Para realizar este módulo, vamos a tomar como referencia las capturas de tráfico de red del módulo de consolidación.

3.3.4.5.1 Estadísticas del Switch LTG-SW-CD1-02-ACC.

En figura 3.18 se muestra el resumen de la captura de tráfico 1 de la tabla 3.22 realizada en el switch LTG-SW-CD1-02-ACC.

E consumo del ancho de banda en este switch es del 0.003% del total del ancho de banda.

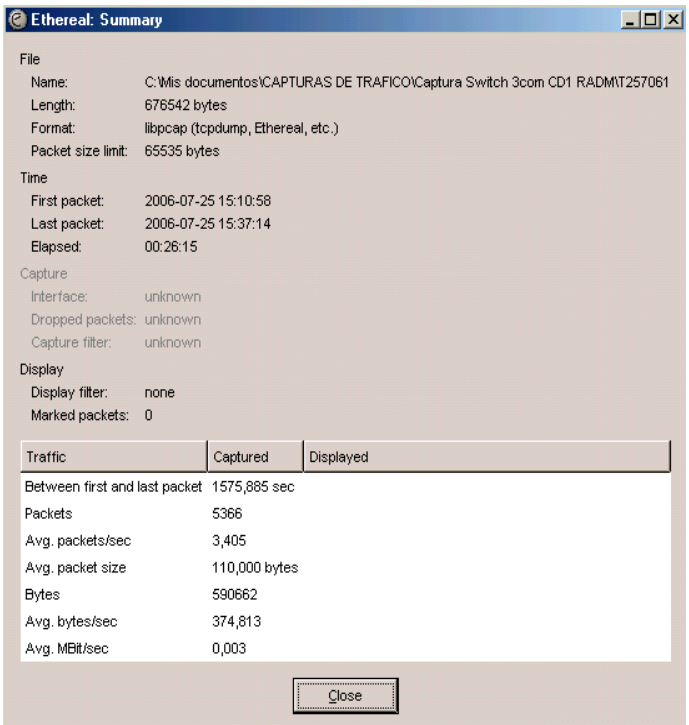


Figura 3.18. Resumen de los paquetes capturados en el Switch LTG-SW-CD1-02-ACC.

Fuente: Ethereal

En la Figura 3.19 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo.
Los protocolos se los representa con líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico es constante y se genera en gran cantidad, ya que diariamente se realizan diferentes actividades en las estaciones de trabajo, están interactuando con las bases de datos, el uso de internet, la actualización del antivirus.

Los paquetes UDP están con color rojo, se genera en gran cantidad ya que este protocolo es el que ayuda a que se ejecuten las diferentes tareas entre el servidor de antivirus y las diferentes estaciones de trabajo.

El tráfico de Broadcast se encuentra identificado con color verde, este protocolo se genera en gran cantidad, ya que las estaciones de trabajo siempre están interactuando con los servidores o con las demás estaciones de trabajo, es por eso que se genera el tráfico de broadcast.

Con color azul se encuentran los paquetes que pertenecen a NBNS, este tipo de protocolo lo genera el antivirus.

De color lila se encuentran los paquetes del protocolo STP, se puede ver que este tipo de tráfico pasa en una forma constante durante toda la captura de tráfico es por eso que se puede ver una línea continua.

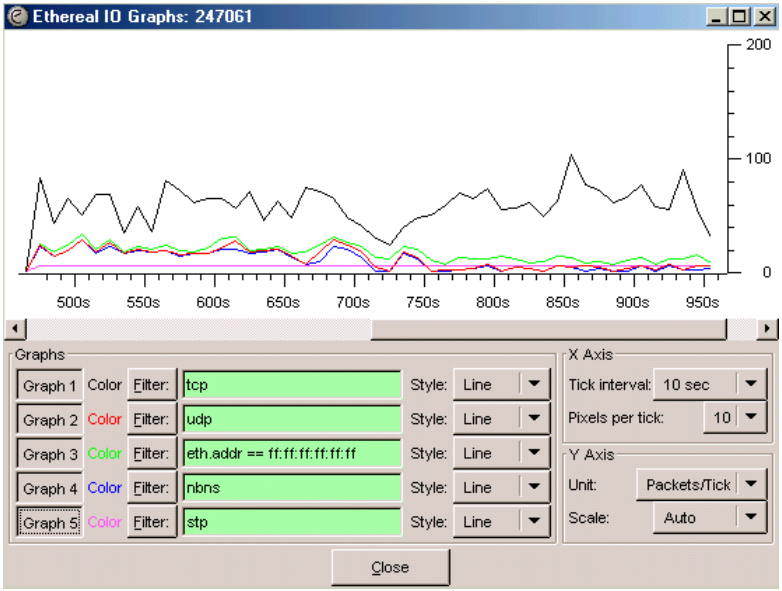


Figura 3.19. Gráfico de paquetes capturados en el Switch LTG-SW-CD1-02-ACC
de la captura de tráfico 1 de la tabla 3.22.

En figura 3.20 se muestra el resumen de la captura de tráfico 2 de la tabla 3.22 realizada en el switch LTG-SW-CD1-02-ACC.

En este caso el consumo del ancho de banda es del 0.002% del total del ancho de banda que dispone la Institución.

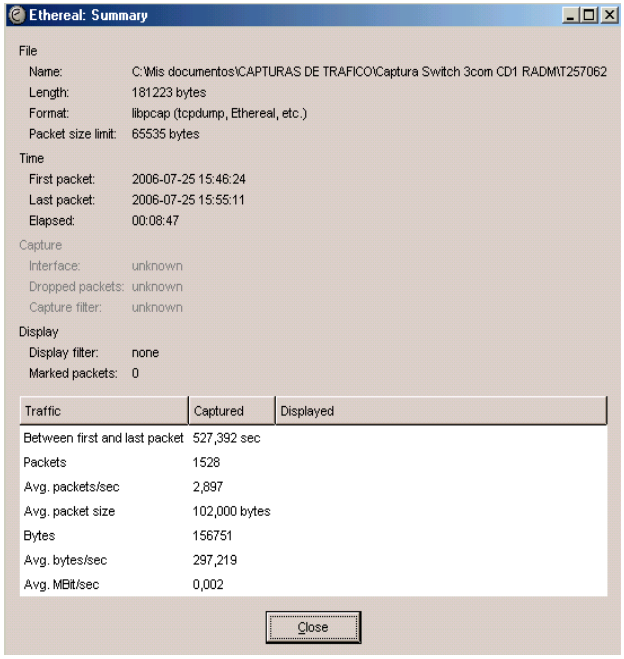


Figura 3.20. Resumen de los paquetes capturados en el Switch LTG-SW-CD1-02.

Fuente: Ethereal.

En la Figura 3.21 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo.

Los protocolos se los representa en líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico es constante y se genera en gran cantidad, ya que diariamente se realizan diferentes actividades en las estaciones de trabajo, están interactuando con las bases de datos, el uso de internet, la actualización del antivirus.

Los paquetes UDP están con color rojo, se genera en gran cantidad ya que este protocolo es el que ayuda a que se ejecuten las diferentes tareas entre el servidor de antivirus y las estaciones de trabajo.

El tráfico de Broadcast se encuentra identificado con color verde, este tráfico se genera ya que las estaciones de trabajo siempre están interactuando con los servidores o con las demás estaciones de trabajo, es por eso que se genera el tráfico de broadcast.

Con color azul se encuentran los paquetes que pertenecen a NBNS, este tipo de protocolo lo genera el antivirus.

De color lila se encuentran los paquetes del protocolo STP, se puede ver que este tipo de tráfico pasa en una forma constante durante toda la captura de tráfico es por eso que se puede ver una línea continua.

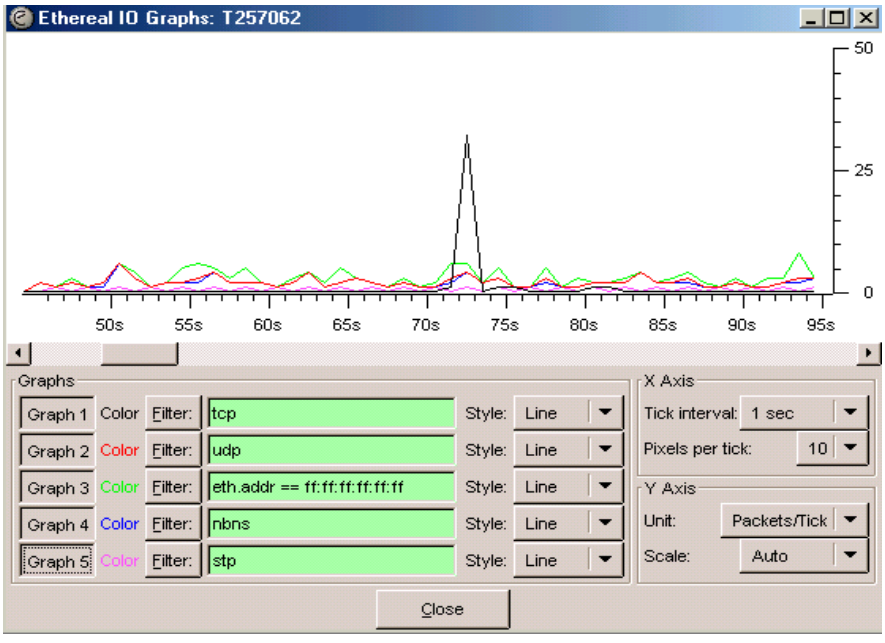


Figura 3.21. Gráfico de paquetes capturados en el Switch LTG-SW-CD1-02-ACC
de la captura de tráfico 2 de la tabla 3.22.

Fuente: Ethereal.

3.3.5 ANÁLISIS DEL TRÁFICO EN EL SWITCH LTG-SW-CD1-04-ACC.

3.3.5.1 MÓDULO DE CAPTURA

En este módulo hemos realizado la captura de los paquetes que se genera en el switch que se encuentra en el centro de producción, este monitoreo se lo realizó en diferentes días y periodos de tiempo

A continuación se detallará la captura de tráfico realizada en el switch LTG-SW-CD1-04-ACC.

3.3.5.1.1 Capturas de tráfico realizadas en el Switch LTG-SW-CD1-04-ACC.

En el centro de datos 1 está el switch LTG-SW-CD1-04-ACC, a este switch se encuentran conectados los siguientes puntos:

- Unidad de Admisión Y Registro.

- Departamento de Ciencias Económicas, Administrativas y Humanísticas.
- Subdirección de Investigación y Docencia.
- Departamento de Ciencias de la Energía y Mecánica Automotriz.
- Departamento de Ciencias Eléctricas, Electrónicas y de la Computación.

En la tabla 3.5 se detallan las capturas de tráfico que se realizaron en el switch LTG-SW-CD1-04-ACC.

LTG-SW-CD1-04-ACC		
N° DE CAPTURA	**FECHA**	**DETALLE**
1	24 de Julio de 2006	Realizado en la tarde
2	25 de Julio de 2006	Realizado en la mañana
3	25 de Julio de 2006	Realizado en la mañana

Tabla 3.23. Captura de tráfico realizadas en el Switch LTG-SW-CD1-04-ACC.

Autor: Javier Cayo.

En el Anexo H se detalla cada uno de los diferentes paquetes que se capturaron desde el switch LTG-SW-CD1-04-ACC.

En el Anexo I se muestra de forma gráfica para mayor comprensión, como se realizó la captura de tráfico en el switch LTG-SW-CD1-04-ACC.

3.3.5.2 MÓDULO DE PREPROCESADO.

En el módulo de preprocesado se eliminará el tráfico innecesario de la captura que se realizó.

Luego de haber realizado la captura de tráfico, se determina que las diferentes capturas de tráfico realizadas en switch LTG-SW-CD1-04-ACC, podemos decir que circulan la misma clase de paquetes en toda la red. Por lo que no es necesario eliminar ninguno de los paquetes que están circulando por la red ya que todos nos van a servir para realizar un mejor análisis.

Como parte del módulo de preprocesado tenemos varias etapas, las que se detallarán a continuación:

3.3.5.2.1 Análisis de Seguridad

La primera etapa es el análisis de seguridad, en esta etapa se va a dividir el tráfico capturado en dos clases que son: tráfico convencional y tráfico sospechoso.

3.3.5.2.1.1 Tráfico Convencional

1. Entre el tráfico convencional tenemos los paquetes TCP/IP los mismos que como sabemos sirven para establecer la comunicación entre las diferentes estaciones de trabajo por ende no presentan peligro alguno para el correcto funcionamiento de la red, y no representan un consumo elevado del ancho de banda.

   Gracias al analizador de red Ethereal se ha determinado las aplicaciones que generan el tráfico TCP son las siguientes:

   - Las páginas de Internet que se manejan diariamente.
   - El sistema Académico.
   - Antivirus Kaspersky.

2. También tenemos los paquetes HTTP, los mismos que se generan cuando los usuarios navegan en el Internet lo que permite la comunicación, transferencia de archivos de las páginas Web que utilizan los usuarios, de la misma forma este tipo de protocolos no representan peligro para el buen funcionamiento de la red, de acuerdo al análisis que se realizó mediante Ethereal no consumen mucho ancho de banda.

Como se explicó anteriormente este tipo de tráfico lo generan las diferentes páginas Web que se manejan en la Institución.

3. Otro de los paquetes que pertenecen al tráfico convencional es el DNS el mismo que está en el grupo de TCP/IP y permite la resolución de nombres de direcciones al momento que se navega en el Internet, es por eso que este protocolo es muy común y necesario, no va a representar peligro alguno para la red.

Los protocolos anteriormente mencionados son los que pertenecen al tráfico convencional, dichos protocolos se han capturado en el Switch LTG-SW-CD1-04-ACC de la Escuela Politécnica del Ejército Sede Latacunga.

En las tablas que se presentarán a continuación, se muestra de forma detallada el número de paquetes, el ancho de banda que consumen, en el switch LTG-SW-CD1-04-ACC que se encuentra junto al Centro de datos 1 pertenecientes al tráfico convencional.

Tráfico Convencional				
Switch	**N° de Captura**	**Protocolo**	**N° de Paquetes**	**Ancho de Banda**
LTG-SW-CD1-04-ACC	1	HTTP	693	0.003000
LTG-SW-CD1-04-ACC	1	DNS	9	0.000000
LTG-SW-CD1-04-ACC	2	HTTP	30	0.001000
LTG-SW-CD1-04-ACC	2	DNS	5	0.000000
LTG-SW-CD1-04-ACC	3	HTTP	0	0.000000
LTG-SW-CD1-04-ACC	3	DNS	0	0.000000

Tabla 3.24. Resumen del tráfico convencional en el Switch LTG-SW-CD1-04-ACC.

Autor: Javier Cayo.

3.3.5.2.1.2 Tráfico Sospechoso

Como parte de la primera etapa del módulo de preprocesado tenemos también el tráfico sospechoso, este tipo de tráfico es el que puede ocasionar peligro, riesgo, por lo que no permitirá el buen funcionamiento de la red, estos paquetes los hemos escogido de las diferentes capturas que se ha realizado.

1. Entre el tráfico sospechoso tenemos que en todas las capturas de tráfico realizadas se detectó en gran cantidad el tráfico de broadcast.

Los paquetes del tráfico de broadcast no ocupan mucho espacio del ancho de banda que dispone la Institución, pero genera inquietud ya que como se mencionó anteriormente es una cantidad considerable el tráfico de broadcast que se genera en la red.

Este tipo de tráfico lo generan todas las estaciones de trabajo que pertenecen al Switch LTG-SW-CD1-04-ACC, ya que al momento que quieren establecer comunicación con un servidor o con una computadora, mandan mensajes de tipo ARP que es el protocolo que permite que se resuelva la dirección de la máquina que se quiere localizar.

2. Otro de los protocolos que se encontró como parte del tráfico sospechoso es el NBNS, este protocolo se genera en gran cantidad, lo genera desde todas las estaciones de trabajo que están conectadas al switch.

   Este tipo de protocolo se genera a partir del servidor de antivirus, es así que al momento de realizar la captura de tráfico con el analizador Ethereal, tenemos como resultado que la dirección de origen es la que pertenece al servidor de antivirus y la dirección destino es una tipo broadcast.

Se debe revisar el funcionamiento el antivirus, para determinar el porque se genera en gran cantidad el protocolo NBNS, de esta forma se podrá optimizar el ancho de banda de la red.

Los 2 protocolos que se describieron anteriormente son los que se generan en mayor cantidad en el switch, por ende se les va dar mayor prioridad para poder presentar la solución más adecuada en el próximo capítulo, lo que permitirá que la red funcione de mejor forma y no se desperdicie el ancho de banda, de esta forma estamos optimizando el ancho de banda que se dispone en la Escuela Politécnica del Ejército Sede Latacunga.

3. También entre el tráfico sospechoso de la red tenemos la presencia del protocolo STP, se genera de una forma considerable en todas las capturas de tráfico que se realizaron en las distintas áreas de la Institución.

4. También tenemos la presencia del protocolo Browser, este protocolo se genera en todas las capturas que se realizó.

   El protocolo Browser se genera cuando desde una computadora se manda a imprimir un documento, este protocolo

ayuda a buscar la ubicación de la impresora y de esta forma imprimir el documento que ha sido enviado.

Tráfico Sospechoso				
Switch	**N° de Captura**	**Protocolo**	**N° de Paquetes**	**Ancho de Banda**
LTG-SW-CD1-04-ACC	1	Broadcast	589	0.000010
LTG-SW-CD1-04-ACC	1	NBNS	1279	0.000101
LTG-SW-CD1-04-ACC	1	Browser	92	0.000000
LTG-SW-CD1-04-ACC	1	STP	500	0.000001
LTG-SW-CD1-04-ACC	2	Broadcast	1219	0.000010
LTG-SW-CD1-04-ACC	2	NBNS	1872	0.001000
LTG-SW-CD1-04-ACC	2	Browser	346	0.000000
LTG-SW-CD1-04-ACC	2	STP	839	0.000001
LTG-SW-CD1-04-ACC	3	Broadcast	549	0.000001
LTG-SW-CD1-04-ACC	3	NBNS	1488	0.001000
LTG-SW-CD1-04-ACC	3	Browser	242	0.000000
LTG-SW-CD1-04-ACC	3	STP	518	0.000001

Tabla 3.25. Resumen de Tráfico Sospechoso en el Switch LTG-SW-CD1-04-ACC.

Autor: Javier Cayo.

3.3.5.2.2 Etapa de Clasificación

En la segunda etapa del módulo de preprocesado el tráfico convencional que se detalló anteriormente, va ser clasificado en base a las direcciones IP de las máquinas que están conectadas al switch LTG-SW-CD1-04-ACC.

A continuación se detallará las direcciones IP de las diferentes estaciones de trabajo del switch LTG-SW-CD1-04-ACC, son el resultado de haber realizado la captura de tráfico con el analizador de red Ethereal.

En las tablas que se detallarán a continuación se muestra la dirección IP de la máquina, el total de paquetes y el porcentaje del ancho de banda que consume cada paquete que pasa por la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

3.3.5.2.5 SWITCH LTG-SW-CD1-04-ACC

A continuación se detallará las diferentes direcciones IP de las máquinas que utilizan el protocolo TCP y el protocolo UDP, los datos son tomados de la captura de tráfico 2 de la tabla 3.23 correspondiente al Switch LTG-SW-CD1-04-ACC.

En la tabla 3.26 se puede observar las direcciones IP de las máquinas que utilizan el protocolo TCP.

Dirección IP	*Total de Paquetes*	*Porcentaje Ancho de Banda*
10.2.0.30	536	0.000425
69.45.79.8	405	0.000321
10.2.0.5	132	0.000105
10.2.0.61	5	0.000004
169.254.9.229	4	0.000003
TOTAL	**1082**	**0.000858**

Tabla 3.26. Direcciones IP del Protocolo TCP del Switch LTG-SW-CD1-04-ACC de la captura de tráfico 2 de la tabla 3.23.

Fuente: Ethereal.

La tabla 3.27 muestra las direcciones IP de las máquinas que utilizan el protocolo UDP.

Dirección IP	*Total de Paquetes*	*Porcentaje Ancho de Banda*
10.2.1.255	1980	0.001183
10.2.0.5	1459	0.000872
169.254.255.255	191	0.000114
169.254.211.46	122	0.000073
169.254.7.148	69	0.000041
10.2.0.3	63	0.000038
255.255.255.255	52	0.000031
10.2.0.9	38	0.000023
10.2.0.4	34	0.000020
10.2.0.2	31	0.000019
10.2.0.185	31	0.000019
10.2.0.30	24	0.000014
10.2.1.91	16	0.000010
10.2.0.23	15	0.000009
10.2.0.162	14	0.000008
10.2.0.21	13	0.000008
10.2.0.64	12	0.000007
10.2.0.186	11	0.000007
10.2.0.172	11	0.000007
10.2.0.91	11	0.000007
10.2.0.31	11	0.000007
10.2.0.43	11	0.000007
10.2.0.183	11	0.000007
10.2.0.132	10	0.000006
10.2.0.171	10	0.000006

10.2.0.116	10	0.000006
10.2.0.184	10	0.000006
10.2.0.83	10	0.000006
10.2.0.176	9	0.000005
10.2.0.106	8	0.000005
10.2.1.173	8	0.000005
10.2.0.181	8	0.000005
10.2.0.152	7	0.000004
10.2.0.63	6	0.000004
10.2.1.154	6	0.000004
10.2.0.224	6	0.000004
10.2.0.51	5	0.000003
10.2.1.153	5	0.000003
10.2.1.186	5	0.000003
10.2.1.151	5	0.000003
10.2.1.111	5	0.000003
10.2.1.155	5	0.000003
10.2.0.61	4	0.000002
10.2.1.51	4	0.000002
10.255.255.255	4	0.000002
10.2.0.107	4	0.000002
10.2.1.181	3	0.000002
10.2.0.142	3	0.000002
10.2.1.61	3	0.000002
10.2.0.161	3	0.000002
10.2.1.152	3	0.000002
10.2.0.41	3	0.000002
10.2.1.197	3	0.000002
TOTAL	4445	0.002637

Tabla 3.27. Direcciones IP del Protocolo UDP del Switch LTG-SW-CD1-04-ACC de la captura de tráfico 2 de la tabla 3.23.

Fuente: Ethereal.

En las siguientes tablas se detallarán las diferentes direcciones IP de las máquinas que utilizan el protocolo TCP y el protocolo UDP, los datos son tomados de la captura de tráfico 3 de la tabla 3.28 correspondiente al Switch LTG-SW-CD1-04-ACC.

En la tabla 3.32 se puede observar las direcciones IP de las máquinas que utilizan el protocolo TCP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.0.5	110	0.000114
10.2.0.30	84	0.000087
10.2.1.154	19	0.000020
10.2.1.61	7	0.000007
TOTAL	220	0.000228

Tabla 3.28. Direcciones IP del Protocolo TCP del Switch LTG-SW-CD1-04-ACC de la captura de tráfico 3 de la tabla 3.23.

Fuente: Ethereal.

En la tabla 3.29 se muestra las direcciones IP de las máquinas que utilizan el protocolo UDP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.1.255	1669	0.001616
10.2.0.5	1321	0.001279
169.254.255.255	47	0.000045
10.2.0.3	43	0.000042
255.255.255.255	25	0.000024
169.254.211.46	25	0.000024
10.2.0.4	24	0.000023
10.2.0.9	23	0.000022
169.254.7.148	22	0.000021
10.2.0.2	20	0.000019
10.2.0.30	12	0.000012
10.2.0.23	11	0.000011
10.2.0.64	10	0.000010
10.2.1.91	9	0.000009
10.2.0.21	9	0.000009
10.2.0.141	9	0.000009

10.2.0.151	9	0.000009
10.2.0.184	8	0.000008
10.2.0.83	8	0.000008
10.2.0.171	8	0.000008
10.2.0.132	7	0.000007
10.2.0.185	7	0.000007
10.2.0.116	7	0.000007
10.2.0.162	7	0.000007
10.2.0.224	7	0.000007
10.2.0.176	7	0.000007
10.2.0.43	7	0.000007
10.2.0.183	7	0.000007
10.2.0.152	6	0.000006
10.2.0.172	6	0.000006
10.2.0.106	6	0.000006
10.2.0.91	6	0.000006
10.2.0.31	6	0.000006
10.2.0.51	4	0.000004
10.2.1.61	4	0.000004
10.2.0.41	4	0.000004
10.2.0.161	4	0.000004
10.2.1.197	4	0.000004
10.2.0.178	4	0.000004
10.2.0.107	4	0.000004
10.2.1.186	3	0.000003
10.2.0.32	3	0.000003
10.2.1.155	3	0.000003
10.2.1.151	3	0.000003
10.2.1.173	3	0.000003
10.2.1.111	3	0.000003
10.2.0.63	3	0.000003
10.2.1.51	3	0.000003
10.255.255.255	3	0.000003
10.2.1.153	3	0.000003
10.2.0.142	2	0.000002
10.2.0.61	2	0.000002
10.2.1.152	2	0.000002
10.2.1.154	2	0.000002
10.2.0.186	2	0.000002
TOTAL	3472	0.003368

Tabla 3.29. Direcciones IP del Protocolo UDP del Switch LTG-SW-CD1-04-ACC de la captura de tráfico 2 de la tabla 3.23.

Fuente: Ethereal.

3.3.5.3 MÓDULO DE CONSOLIDACIÓN.

El siguiente paso en la metodología Mira, tenemos al módulo de consolidación, en este módulo vamos a consolidar los resultados parciales de la captura de tráfico realizada en el Switch LTG-SW-CD1-04-ACC.

3.3.5.3.1 SWITCH LTG-SW-CD1-04-ACC

En la tabla 3.30 se muestra de una forma detallada las capturas de tráfico que se realizaron en el Switch LTG-SW-CD1-04-ACC.

LTG-SW-CD1-04-ACC			
N° DE CAPTURA	**FECHA**	**TIEMPO DE CAPTURA**	**NUMERO DE PAQUETES**
1	24 de Julio de 2006	17 Minutos	8642 Paquetes
2	25 de Julio de 2006	29 Minutos	5002 Paquetes
3	25 de Julio de 2006	18 Minutos	3003 Paquetes

Tabla 3.30. Detalle de las capturas de tráfico realizadas en el Switch LTG-SW-CD1-04-ACC.
Fuente: Ethereal.

3.3.5.4 MÓDULO DE POSTPROCESADO

Luego de haber realizado la clasificación podemos continuar con el módulo de postprocesado aquí se va realizar informes de forma general de los diferentes resultados que hemos conseguido luego de haber capturado el tráfico en la red.

Con la ayuda del analizador de red Ethereal se presenta los diferentes informes y gráficos del monitoreo de la red, de esta forma ya se puede dar un análisis del estado en el que se encuentra la red.

Para realizar este módulo, vamos a tomar como referencia las capturas de tráfico de red del módulo de consolidación.

3.3.5.4.1 Estadísticas del Switch LTG-SW-CD1-04-ACC.

En figura 3.22 se muestra el resumen de la captura de tráfico 1 de la tabla 3.30 realizada en el Switch LTG-SW-CD1-04-ACC.

En la figura 3.22 podemos observar que el consumo del ancho de banda representa el 0.006%.

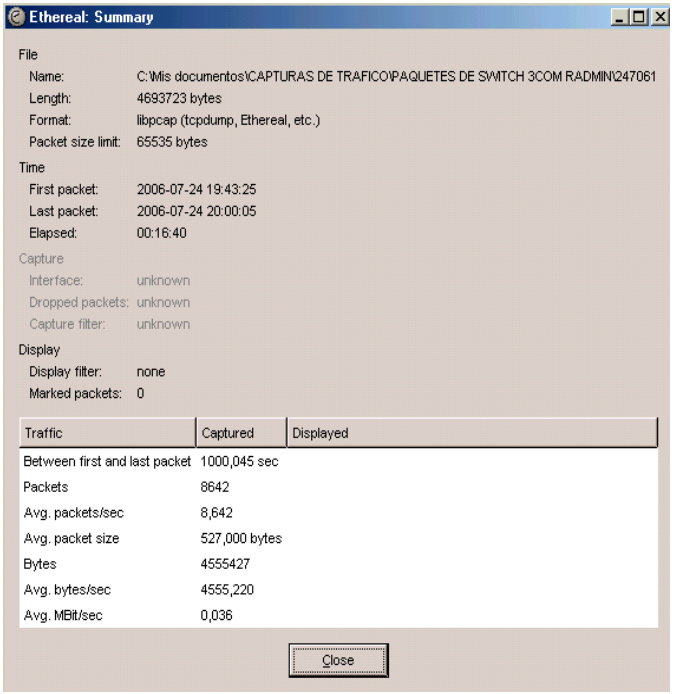


Figura 3.22. Resumen de los paquetes capturados en el Switch LTG-SW-CD1-04-ACC.

Fuente: Ethereal.

En la Figura 3.23 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo.
Los protocolos se los representa en líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico es constante, básicamente se genera porque los usuarios que están conectados al switch navegan en el internet.

Los paquetes UDP están con color rojo, se genera en gran cantidad ya que este protocolo es el que ayuda a que se ejecuten las diferentes tareas entre el servidor de antivirus y las estaciones de trabajo.

El tráfico de Broadcast se encuentra identificado con color verde, este tráfico se genera ya que las estaciones de trabajo siempre están interactuando con los servidores o con las demás estaciones de trabajo, es por eso que se genera el tráfico de broadcast.

Con color azul se encuentran los paquetes que pertenecen a NBNS, este protocolo lo genera el antivirus cuando el servidor no logra realizar una tarea en una estación de trabajo.

De color lila se encuentran los paquetes del protocolo STP, este tipo de tráfico pasa en una forma constante durante toda la captura de tráfico, ya que

en los switches 3Com que dispone la Institución tienen habilitada la opción del STP.

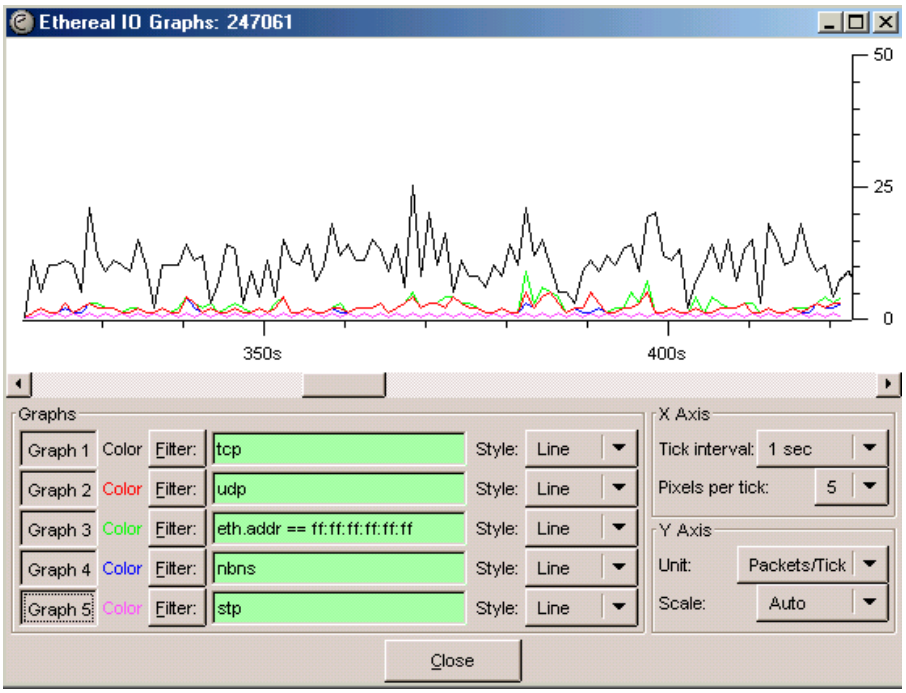


Figura 3.24. Gráfico de los paquetes capturados en el Switch LTG-SW-CD1-04-ACC de la captura de tráfico 1 de la tabla 3.30.
Fuente: Ethereal.

En figura 3.25 se muestra el resumen de la captura de tráfico 2 de la tabla 3.30 realizada en el Switch 3Com 4228G.

En la figura se puede observar que de los 5002 paquetes que se han capturado en 28 minutos, consumen un 0.003% del total del ancho de banda que dispone la Institución.

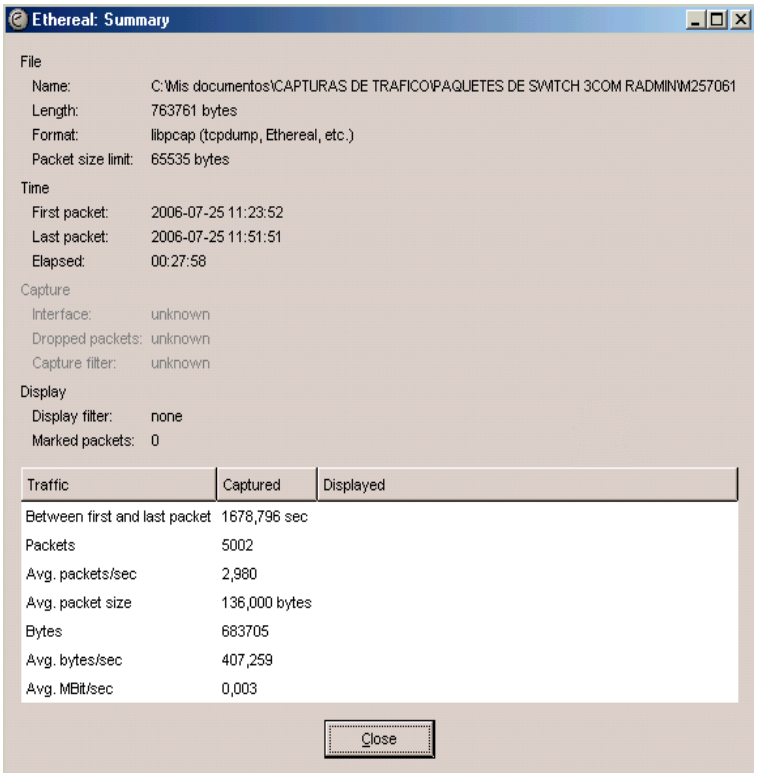


Figura 3.25. Resumen de los paquetes capturados en el Switch LTG-SW-CD1-04-ACC.

Fuente: Ethereal.

En la Figura 3.25 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo.

Los protocolos se los representa en líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico es constante y se genera básicamente porque los usuarios que están conectados al switch navegan en el internet, otra de las razones es porque el antivirus se está actualizando y permite que se genere este tipo de tráfico.

Los paquetes UDP están con color rojo, este protocolo se genera en gran cantidad, ya que ayuda principalmente al servidor de antivirus a realizar las tareas que han sido programadas en las diferentes estaciones de trabajo.
El tráfico de Broadcast se encuentra identificado con color verde, este tráfico se genera ya que las estaciones de trabajo siempre están interactuando con los servidores o con las demás estaciones de trabajo, es por eso que se genera el tráfico de broadcast.

Con color azul se encuentran los paquetes que pertenecen a NBNS, este tipo de tráfico lo genera el antivirus, ya que momento de que el servidor manda a ejecutar una determinada tarea y la estación de trabajo no esta lista, o no la encuentra el servidor siempre estará enviando este tipo de tráfico hasta que se cumpla la tarea.

De color lila se encuentran los paquetes del protocolo STP, este tipo de tráfico pasa en una forma constante durante toda la captura de tráfico, ya que

en los switches 3Com que dispone la Institución tienen habilitada la opción del STP.

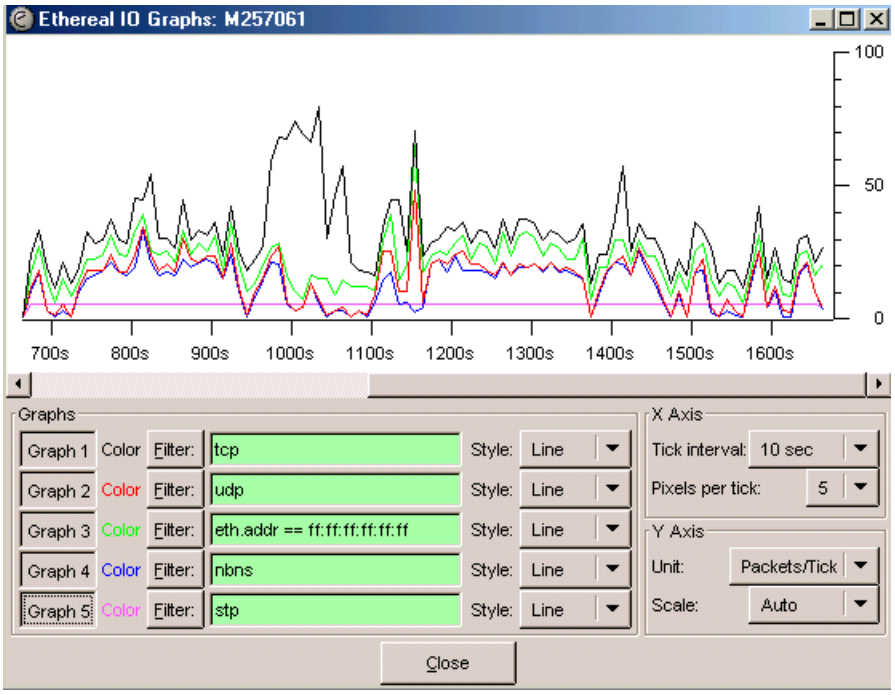


Figura 3.26. Gráfico de los paquetes capturados en el Switch LTG-SW-CD1-04-ACC de la captura de tráfico 2 de la tabla 3.30.

Fuente: Ethereal.

3.3.6 ANÁLISIS DEL TRÁFICO EN EL SWITCH LTG-SW-CD5-01-ACC.

3.3.6.1 MÓDULO DE CAPTURA

En este módulo hemos realizado las capturas de tráfico de los paquetes que se genera en el switch que se encuentra en el centro de datos1, este monitoreo se lo realizó en diferentes días y periodos de tiempo

A continuación se detallará la captura de tráfico realizada en el switch LTG-SW-CD1-05-ACC.

3.3.6.1.1 CAPTURAS DE TRÁFICO REALIZADAS EN EL SWITCH LTG-SW-CD1-05-ACC

Las capturas de tráfico se realizaron desde el Rack principal que se encuentra en el Centro de Datos 1, el switch LTG-SW-CD1-05-ACC, a este switch conectan los siguientes grupos:

- Unidad de Tecnologías de la Información y Comunicación.

En la tabla 3.31 se muestra las capturas de tráfico que se realizaron en el switch LTG-SW-CD1-05-ACC**.**

LTG-SW-CD1-05-ACC		
N° DE CAPTURA	**FECHA**	**DETALLE**
1	24 de Julio de 2006	Realizado en la mañana
2	24 de Julio de 2006	Realizado en la tarde
3	25 de Julio de 2006	Realizado en la tarde
4	25 de Julio de 2006	Realizado en la tarde
5	27 de Julio de 2006	Realizado en la tarde

Tabla 3.31. Captura de tráfico del Switch LTG-SW-CD1-05-ACC.
Autor: Javier Cayo.

En el Anexo J se detalla cada una de las capturas de tráfico que se realizaron desde el switch LTG-SW-CD1-05-ACC.

En el Anexo K se muestra de forma gráfica para mayor comprensión, como se realizó la captura de tráfico en el switch LTG-SW-CD1-05-ACC.

3.3.6.2 MÓDULO DE PREPROCESADO.

En el módulo de preprocesado se eliminará el tráfico innecesario de la captura que se realizó.

Luego de haber realizado la captura de tráfico, se determina que las diferentes capturas de tráfico realizadas en switch LTG-SW-CD1-05-ACC, podemos decir que circulan la misma clase de paquetes en toda la red. Por lo que no es necesario eliminar ninguno de los paquetes que están circulando por la red ya que todos nos van a servir para realizar un mejor análisis.

Como parte del módulo de preprocesado tenemos varias etapas, las que se detallarán a continuación:

3.3.4.2.1 Análisis de Seguridad

La primera etapa es el análisis de seguridad, en esta etapa se va a dividir el tráfico capturado en dos clases que son: tráfico convencional y tráfico sospechoso.

3.3.4.2.1.1 Tráfico Convencional

1. Entre el tráfico convencional tenemos los paquetes TCP/IP los mismos que como sabemos sirven para establecer la comunicación entre las diferentes estaciones de trabajo por ende no presentan peligro alguno para el correcto funcionamiento de la red, y no presentan peligro al buen funcionamiento de la red.

   Gracias al analizador de red Ethereal se ha determinado las aplicaciones que generan el tráfico TCP son las siguientes:

   - Las páginas de Internet que se manejan diariamente.
   - Antivirus Kaspersky.
   - Sistema Olympo.
   - Web Access.
   - Página Web de la ESPEL
   - Página Web de la ESPE Matríz.

2. También tenemos los paquetes HTTP, los mismos que se generan cuando los usuarios navegan en el Internet lo que permite la comunicación, transferencia de archivos de las páginas Web que utilizan los usuarios de la Unidad de Tecnologías de la Información y Comunicación, de la misma forma este tipo

de protocolos no representan peligro para el buen funcionamiento de la red, de acuerdo al análisis que se realizó mediante Ethereal no consumen mucho ancho de banda.

Como se explicó anteriormente este tipo de tráfico lo generan las diferentes páginas Web que se manejan en la Institución.

3. Otro de los paquetes que pertenecen al tráfico convencional es el DNS el mismo que está en el grupo de TCP/IP y permite la resolución de nombres de direcciones al momento que se navega en el Internet, es por eso que este protocolo es muy común y necesario, no va a representar peligro alguno para la red.

   Los protocolos anteriormente mencionados son los que pertenecen al tráfico convencional, dichos protocolos se han capturado en el Switch LTG-SW-CD1-05-ACC de la Escuela Politécnica del Ejército Sede Latacunga.

   En las tablas que se presentarán a continuación, se muestra de forma detallada el número de paquetes, el ancho de banda que consumen, en el switch LTG-SW-CD1-05-ACC que se encuentra en el Centro de datos 1 pertenecientes al tráfico convencional.

Tráfico Convencional				
Switch	**Nº de Captura**	**Protocolo**	**Nº de Paquetes**	**Ancho de Banda**
LTG-SW-CD1-05-ACC	1	HTTP	675	0.002000
LTG-SW-CD1-05-ACC	1	DNS	41	0.000011
LTG-SW-CD1-05-ACC	2	HTTP	422	0.003000
LTG-SW-CD1-05-ACC	2	DNS	14	0.000001
LTG-SW-CD1-05-ACC	3	HTTP	603	0.001000
LTG-SW-CD1-05-ACC	3	DNS	56	0.000011

Tabla 3.32. Resumen del tráfico convencional en el Switch LTG-SW-CD1-04-ACC.

Autor: Javier Cayo

3.3.4.2.1.2 Tráfico Sospechoso

Como parte de la primera etapa del módulo de preprocesado tenemos también el tráfico sospechoso, este tipo de tráfico es el que puede ocasionar peligro, riesgo, por lo que no permitirá el buen funcionamiento de la red, estos paquetes los hemos escogido de las diferentes capturas que se ha realizado.

1. Entre el tráfico sospechoso tenemos que en todas las capturas de tráfico realizadas se

detectó como en las demás capturas de tráfico gran cantidad el tráfico de broadcast.

Los paquetes del tráfico de broadcast no ocupan mucho espacio del ancho de banda que dispone la Institución, pero genera inquietud ya que como se mencionó anteriormente es una cantidad considerable el tráfico de broadcast que se genera en la red.

Este tipo de tráfico lo generan todas las estaciones de trabajo que pertenecen al Switch LTG-SW-CD1-05-ACC, ya que al momento que quieren establecer comunicación con un servidor o con una computadora, mandan mensajes de tipo ARP que es el protocolo que permite que se resuelva la dirección de la máquina que se quiere localizar.

2. Otro de los protocolos que se encontró como parte del tráfico sospechoso es el NBNS, este protocolo se genera en gran cantidad, este tipo de tráfico es uno de los que más se genera en la red, es por esa razón que se le a puesto en el grupo del tráfico sospechoso.

   Este tipo de protocolo se genera a partir del servidor de antivirus, es así que al momento de realizar la captura de tráfico con el analizador Ethereal, tenemos como

resultado que la dirección de origen es la que pertenece al servidor de antivirus y la dirección destino es una tipo broadcast.

Se debe revisar el funcionamiento el antivirus, para determinar el porque se genera en gran cantidad el protocolo NBNS, de esta forma se podrá optimizar el ancho de banda de la red.

Los 2 protocolos que se describieron anteriormente son los que se generan en mayor cantidad en el switch, por ende se les va dar mayor prioridad para poder presentar la solución más adecuada en el próximo capítulo, lo que permitirá que la red funcione de mejor forma y no se desperdicie el ancho de banda, de esta forma estamos optimizando el ancho de banda que se dispone en la Escuela Politécnica del Ejército Sede Latacunga.

3. También entre el tráfico sospechoso de la red tenemos la presencia del protocolo STP, se genera de una forma considerable en todas las capturas de tráfico que se realizaron en las distintas áreas de la Institución.

4. También tenemos la presencia del protocolo Browser, este protocolo se genera en todas las capturas que se realizó.

El protocolo Browser se genera cuando desde una computadora se manda a imprimir un documento, este protocolo ayuda a buscar la ubicación de la impresora y de esta forma imprimir el documento que ha sido enviado.

Tráfico Sospechoso				
Switch	**N° de Captura**	**Protocolo**	**N° de Paquetes**	**Ancho de Banda**
LTG-SW-CD1-05-ACC	1	Broadcast	892	0.000001
LTG-SW-CD1-05-ACC	1	NBNS	1917	0.001000
LTG-SW-CD1-05-ACC	1	Browser	291	0.000000
LTG-SW-CD1-05-ACC	1	STP	712	0.000001
LTG-SW-CD1-05-ACC	2	Broadcast	360	0.000000
LTG-SW-CD1-05-ACC	2	NBNS	788	0.001000
LTG-SW-CD1-05-ACC	2	Browser	57	0.000000
LTG-SW-CD1-05-ACC	2	STP	310	0.000000
LTG-SW-CD1-05-ACC	3	Broadcast	1539	0.000001
LTG-SW-CD1-05-ACC	3	NBNS	1257	0.001000
LTG-SW-CD1-05-ACC	3	Browser	466	0.000000
LTG-SW-CD1-05-ACC	3	STP	1423	0.000000

Tabla 3.33. Resumen del Tráfico Sospechoso en el Switch LTG-SW-CD1-04- ACC.

Autor: Javier Cayo.

3.3.6.2.2 Etapa de Clasificación

En la segunda etapa del módulo de preprocesado el tráfico convencional que se detalló anteriormente, va ser clasificado en base a las direcciones IP de las máquinas que están conectadas al switch LTG-SW-CD1-05-ACC.

A continuación se detallará las direcciones IP de las diferentes estaciones de trabajo del switch LTG-SW-CD1-05-ACC, son el resultado de haber realizado la captura de tráfico con el analizador de red Ethereal.

En las tablas que se detallarán a continuación se muestra la dirección IP de la máquina, el total de paquetes y el porcentaje del ancho de banda que consume cada paquete que pasa por la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

3.3.6.2.3 SWITCH LTG-SW-CD1-05-ACC

En la tabla 3.34 se muestra las direcciones IP de los equipos que utilizan del protocolo TCP, esta información se tomó de la captura de tráfico 1, de la tabla 3.31 que corresponde al switch LTG-SW-CD1-05-ACC.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.0.30	5160	0.003630
69.45.79.7	2384	0.001677
206.24.233.62	1230	0.000865
208.172.128.253	808	0.000568
208.172.44.62	337	0.000237

193.134.194.11	146	0.000103
64.233.179.99	98	0.000069
200.42.136.212	54	0.000038
10.2.0.93	34	0.000024
10.2.1.91	34	0.000024
200.52.65.80	32	0.000023
38.118.213.4	31	0.000022
64.8.121.121	31	0.000022
10.2.0.5	24	0.000017
10.2.0.91	18	0.000013
64.233.179.104	9	0.000006
10.2.0.2	8	0.000006
10.2.0.51	8	0.000006
10.2.0.131	5	0.000004
10.2.1.31	1	0.000001
TOTAL	**10452**	**0.007355**

Tabla 3.34. Direcciones IP del Protocolo TCP del switch LTG-SW-CD1-05-ACC de la captura de tráfico 1 de la tabla 3.31.

Fuente: Ethereal.

En la tabla 3.35 se puede observar las direcciones IP de los equipos que utilizan el protocolo UDP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.1.255	2058	0.001447
10.2.0.5	1443	0.001015
169.254.255.255	143	0.000101
169.254.211.46	91	0.000064
10.2.0.30	78	0.000055
10.2.0.3	58	0.000041
169.254.7.148	52	0.000037
255.255.255.255	44	0.000031
10.2.0.63	43	0.000030
10.2.0.83	41	0.000029
10.2.0.194	38	0.000027
192.188.58.163	35	0.000025
10.2.0.2	31	0.000022
10.2.0.9	29	0.000020
10.2.0.4	28	0.000020

10.2.0.101	23	0.000016
10.2.0.106	16	0.000011
10.2.0.202	16	0.000011
10.2.0.21	15	0.000011
10.2.1.181	14	0.000010
10.2.0.141	12	0.000008
10.2.0.171	11	0.000008
10.2.0.93	10	0.000007
10.2.0.162	10	0.000007
10.2.0.172	9	0.000006
10.2.0.24	9	0.000006
10.2.0.176	8	0.000006
10.2.0.116	8	0.000006
10.2.0.185	8	0.000006
10.2.0.111	8	0.000006
10.2.0.72	7	0.000005
10.2.0.132	7	0.000005
10.2.0.64	7	0.000005
10.2.0.94	7	0.000005
10.2.1.184	7	0.000005
10.2.1.173	7	0.000005
10.2.1.111	7	0.000005
10.2.0.186	7	0.000005
10.2.0.23	6	0.000004
10.2.0.43	6	0.000004
10.2.1.91	6	0.000004
10.2.0.151	6	0.000004
10.2.0.152	5	0.000004
10.2.0.53	5	0.000004
10.2.0.131	5	0.000004
200.105.225.2	4	0.000003
10.2.2.51	3	0.000002
10.255.255.255	3	0.000002
10.2.0.51	3	0.000002
10.2.0.91	3	0.000002
10.2.0.41	3	0.000002
10.2.0.178	3	0.000002
10.2.0.142	3	0.000002
10.2.1.151	3	0.000002
10.2.1.61	1	0.000001
TOTAL	4515	0.003178

Tabla 3.36. Direcciones IP del Protocolo UDP del switch LTG-SW-CD1-05-ACC de la captura de tráfico 1 de la tabla 3.31.

Fuente: Ethereal.

En la tabla 3.37 se muestra las direcciones IP de los equipos que utilizan el protocolo TCP, esta información se tomó de la captura de tráfico 2, de la tabla 3.31 que corresponde al switch LTG-SW-CD1-05-ACC.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.0.30	4069	0.006561
69.45.79.7	3293	0.005309
69.45.79.6	757	0.001221
198.65.115.109	19	0.000031
TOTAL	**8138**	**0.013122**

Tabla 3.37. Direcciones IP del Protocolo TCP del switch LTG-SW-CD1-05-ACC de la captura de tráfico 2 de la tabla 3.31.

Fuente: Ethereal.

En la tabla 3.38 se puede observar las direcciones IP de las máquinas que utilizan el protocolo UDP.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.1.255	801	0.001296
10.2.0.5	649	0.001046
169.254.255.255	38	0.000061
10.2.0.3	23	0.000037
169.254.211.46	20	0.000032
10.2.0.2	19	0.000031
169.254.7.148	18	0.000029
10.2.0.30	15	0.000024
10.2.0.9	13	0.000021
192.188.58.163	12	0.000019
10.2.0.4	11	0.000018
10.2.0.183	10	0.000016

10.2.0.83	10	0.000016
255.255.255.255	10	0.000016
10.2.0.172	6	0.000010
10.2.0.151	6	0.000010
10.2.1.184	5	0.000008
10.2.0.185	4	0.000006
10.2.0.23	4	0.000006
10.2.1.91	4	0.000006
10.2.0.21	4	0.000006
10.2.0.93	4	0.000006
10.2.0.176	4	0.000006
10.2.0.162	4	0.000006
10.2.1.173	3	0.000005
10.2.0.202	3	0.000005
10.2.0.132	3	0.000005
10.2.0.91	2	0.000003
200.105.225.2	2	0.000003
10.2.0.161	1	0.000002
10.2.0.41	1	0.000002
10.2.0.107	1	0.000002
10.2.0.106	1	0.000002
10.2.0.71	1	0.000002
10.2.0.72	1	0.000002
TOTAL	**1716**	**0.002771**

Tabla 3.38. Direcciones IP del Protocolo UDP del switch LTG-SW-CD1-05-ACC de la captura de tráfico 2 de la tabla 3.31.

Fuente: Ethereal.

3.3.6.3 MÓDULO DE CONSOLIDACIÓN.

El siguiente paso en la metodología Mira, tenemos al módulo de consolidación, en este módulo vamos a consolidar los resultados parciales de la captura de tráfico realizada en el Switch LTG-SW-CD1-05-ACC.

LTG-SW-CD1-05-ACC			
N° DE CAPTURA	**FECHA**	**TIEMPO DE CAPTURA**	**NUMERO DE PAQUETES**

1	24 de Julio de 2006	25 Minutos	9296 Paquetes
2	24 de Julio de 2006	15 Minutos	5652 Paquetes
3	25 de Julio de 2006	50 Minutos	12224 Paquetes
4	25 de Julio de 2006	24 Minutos	3328 Paquetes
5	27 de Julio de 2006	25 Minutos	3215 Paquetes

Tabla 3.39. Detalle de las capturas de tráfico realizadas en el Switch LTG-SW-CD1-05-ACC.

Fuente: Ethereal.

3.3.6.4 MÓDULO DE CLASIFICACIÓN

En este módulo se clasificará el tráfico que se ha capturado en diferentes categorías.

- **Primera Categoría.-** La primera categoría que se ha identificado, es el traficó normal o convencional el mismo que ya se detalló en el módulo de preprocesado.

  Este tipo de tráfico es el que no representa peligro alguno para el buen desenvolvimiento de la red, este tipo de tráfico se genera en todas las estaciones de trabajo se conectan al Switch LTG-SW-CD1-05-ACC.

  A continuación vamos a citar los protocolos que se han tomado en cuenta en el tráfico normal, tenemos al protocolo TCP, el protocolo UDP, el protocolo HTTP, el protocolo DNS.

- **Segunda Categoría.-** La segunda categoría que podemos identificar es el tráfico administrativo, el mismo que produce cada una de las estaciones de trabajo que pertenecen a la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga.

Este tipo de tráfico lo generan las diferentes aplicaciones que se utilizan todos los días, en los diferentes departamentos de la Escuela Politécnica del Ejército Sede Latacunga, entre las aplicaciones tenemos:

- Sistema Olympo.
- Antivirus Kaspersky.
- Sistema Académico.
- Sistema Académico de Idiomas.
- Web Access.

- **Tercera Categoría.-** Otra categoría que se ha identificado y se puede decir que es una de las más importantes y nos da la idea principal para saber que problemas tiene nuestra red, es la del tráfico indeterminado, este tipo de tráfico se produce en gran cantidad en la red Administrativa de la Escuela Politécnica del Ejército Sede Latacunga, el tráfico indeterminado se ha logrado identificar en todas las capturas de tráfico que se han realizado en la Unidad de Tecnologías de la Información y Comunicación, y es lo que más inquietud produce ya que se generan varios protocolos no muy usuales para el correcto funcionamiento de la red, los protocolos que se encuentran en esta categoría son: el broadcast, NBNS, STP, BROWSER, estos protocolos ocupan el ancho de banda de la red, el espacio que utilizan no es muy considerable pero sería mejor que este tipo de tráfico de red no se de y de esta forma el espacio que estos protocolos utilizan sería distribuido de mejor forma entre

las demás aplicaciones que necesitan el ancho de banda para un correcto y rápido funcionamiento.

3.3.6.5 MÓDULO DE POSTPROCESADO

En el módulo de postprocesado se va realizar informes de forma general y gráfica de los diferentes resultados que hemos conseguido luego de haber capturado el tráfico en el switch LTG-SW-CD1-05-ACC.

Con la ayuda del analizador de red Ethereal se presenta los diferentes informes y gráficos del monitoreo de la red, de esta forma ya se puede dar un análisis del estado en el que se encuentra la red.

Para realizar este módulo, vamos a tomar como referencia las capturas de tráfico de red del módulo de consolidación.

3.3.6.5.1 Estadísticas del SWITCH LTG-SW-CD1-05-ACC

En figura 3.27 se muestra el resumen de la captura de tráfico 1 de la tabla 3.39 realizada en el switch LTG-SW-CD1-05-ACC.

En la figura se muestra el consumo del ancho de banda, para este caso es de 0.022%, del total de ancho de banda.

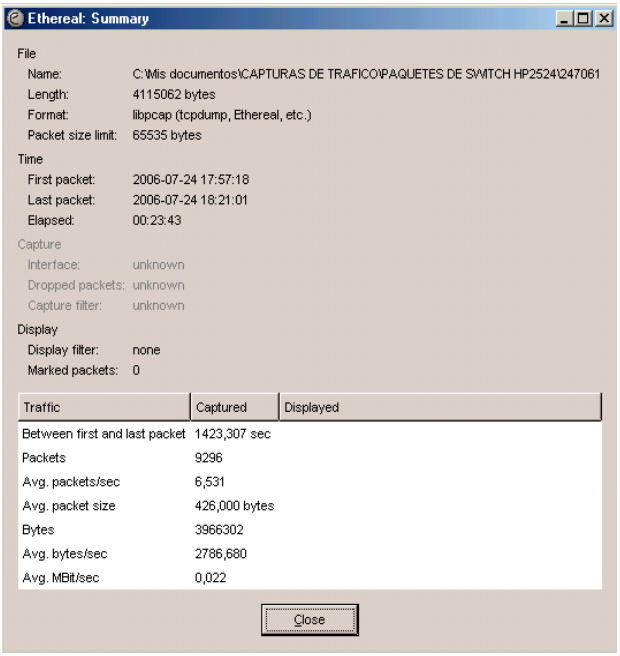


Figura 3.27. Resumen de los paquetes capturados en el SWITCH LTG-SW-CD1-05-ACC.

Fuente: Ethereal.

En la Figura 3.28 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo.

Los protocolos se los representa en líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico se genera en gran cantidad, ya que diariamente se realizan actividades en los diferentes sistemas que dispone la Institución, de igual forma se generan porque las diferentes estaciones de trabajo navegan en el internet.

Los paquetes UDP están con color rojo, se genera en gran cantidad, ya que el servidor de antivirus utiliza este

protocolo parar trasmitir los datos a las diferentes estaciones de trabajo.

El tráfico de Broadcast se encuentra identificado con color verde, como en todos los dispositivos este tipo de tráfico lo generan las diferentes estaciones de trabajo, ya que al momento de que una estación de trabajo quiere localizar a otra estación de trabajo envía un mensaje y se ve en toda la red, es por eso que se genera el broadcast.

Con color azul se encuentran los paquetes que pertenecen a NBNS, se genera porque el servidor de antivirus, manda a buscar a las computadoras que se encuentran registradas, pero no tienen instalado el antivirus.

De color lila se encuentran los paquetes del protocolo STP, se genera en todos los switches, este protocolo se genera cada 2 segundos.

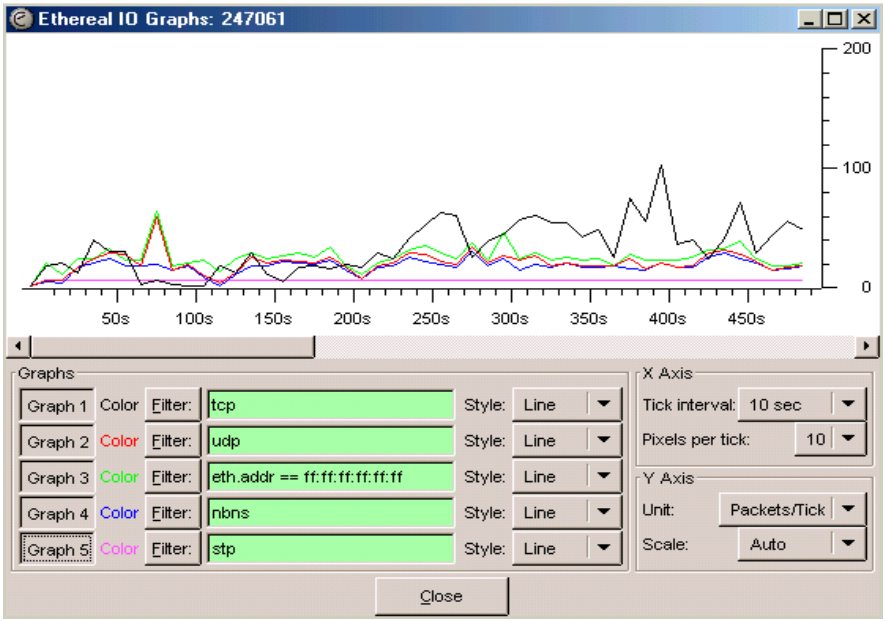
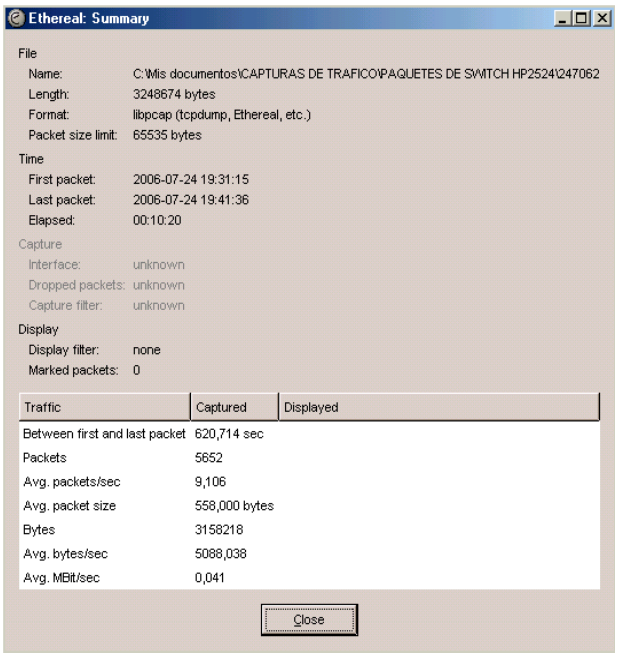


Figura 3.28 Gráfico de paquetes capturados en el Switch LTG-SW-CD1-05-ACC
de la captura de tráfico 1 de la tabla 3.3.
Fuente: Ethereal.

En figura 3.29 se muestra el resumen de la captura de tráfico 2 de la tabla 3.39 realizada en el Switch LTG-SW-CD1-05-ACC.



En la Figura 3.30 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo.
Los protocolos se los representa en líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico se genera en gran cantidad, ya que diariamente se realizan actividades en los diferentes sistemas que dispone la Institución, de igual

forma se generan porque las diferentes estaciones de trabajo navegan en el internet.

Los paquetes UDP están con color rojo, se genera en gran cantidad.

El tráfico de Broadcast se encuentra identificado con color verde, como en todos los dispositivos este tipo de tráfico lo generan las diferentes estaciones de trabajo, ya que al momento de que una estación de trabajo quiere localizar a otra estación de trabajo envía un mensaje y se ve en toda la red, es por eso que se genera el broadcast.

Con color azul se encuentran los paquetes que pertenecen a NBNS, se genera porque el servidor de antivirus, manda a buscar a las computadoras que se encuentran registradas, pero no tienen instalado el antivirus.

De color lila se encuentran los paquetes del protocolo STP, se genera en todos los switches, este protocolo se genera cada 2 segundos.

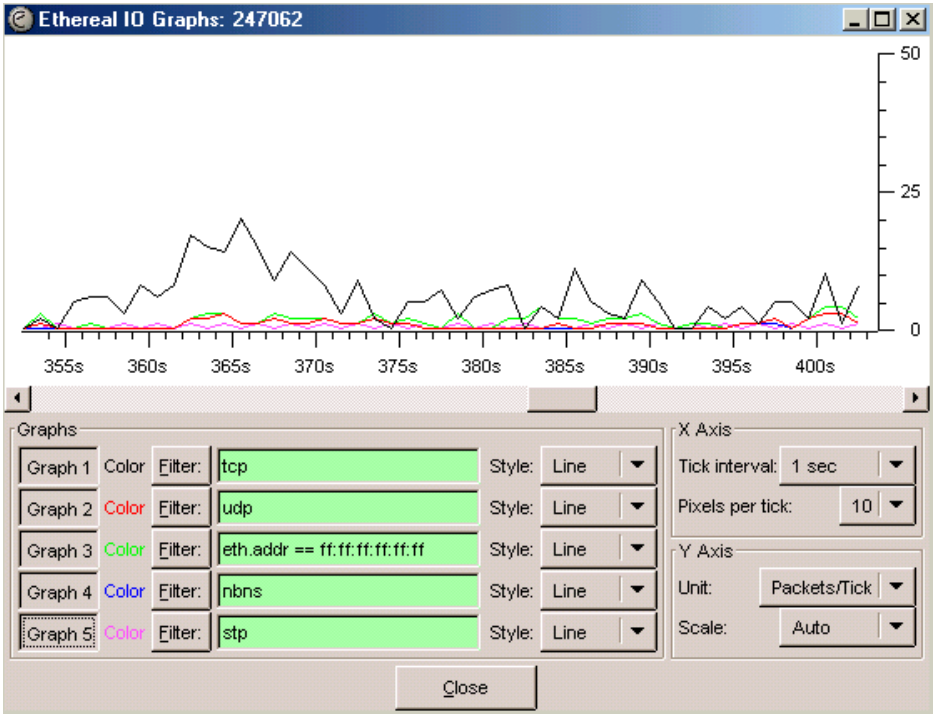
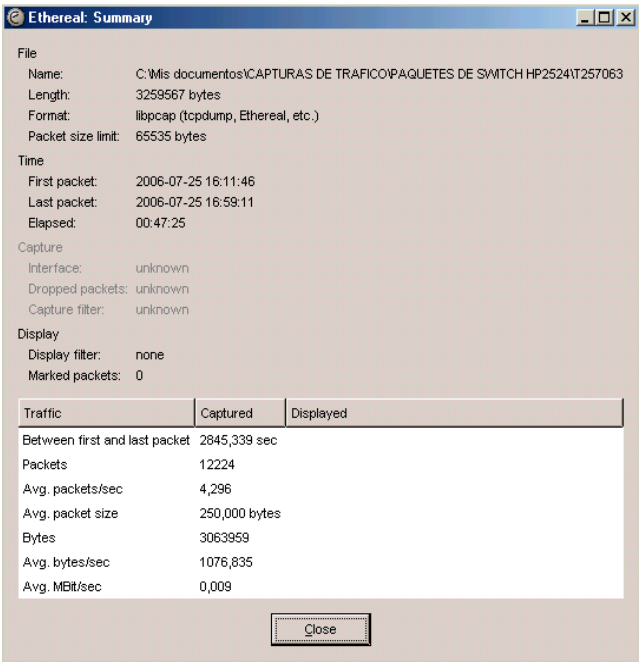


Figura 3.30. Gráfico de paquetes capturados en el Switch LTG-SW-CD1-05-ACC
de la captura de tráfico 2 de la tabla 3.39.

En figura 3.31 se muestra el resumen de la captura de tráfico 3 de la tabla 3.39 realizada en el Switch LTG-SW-CD1-05-ACC.



En la Figura 3.32 podemos observar gráficamente como circulan los diferentes paquetes por la red en determinados lapsos de tiempo.
Los protocolos se los representa en líneas de diferentes colores.

Se observa que los paquetes de TCP están con una línea de color negro, este tipo de tráfico se genera en gran cantidad, ya que diariamente se realizan actividades en los diferentes sistemas que dispone la Institución, de igual forma se generan porque las diferentes estaciones de trabajo navegan en el internet.

Los paquetes UDP están con color rojo, se genera en gran cantidad.

El tráfico de Broadcast se encuentra identificado con color verde, este tipo de tráfico lo generan las diferentes estaciones de trabajo, ya que al momento de que una estación de trabajo quiere localizar a otra estación de

trabajo envía un mensaje y se ve en toda la red, es por eso que se genera el broadcast.

Con color azul se encuentran los paquetes que pertenecen a NBNS, se genera porque el servidor de antivirus, manda a buscar a las computadoras que se encuentran registradas, pero no tienen instalado el antivirus.

De color lila se encuentran los paquetes del protocolo STP, se genera en todos los switches, este protocolo se genera cada 2 segundos.

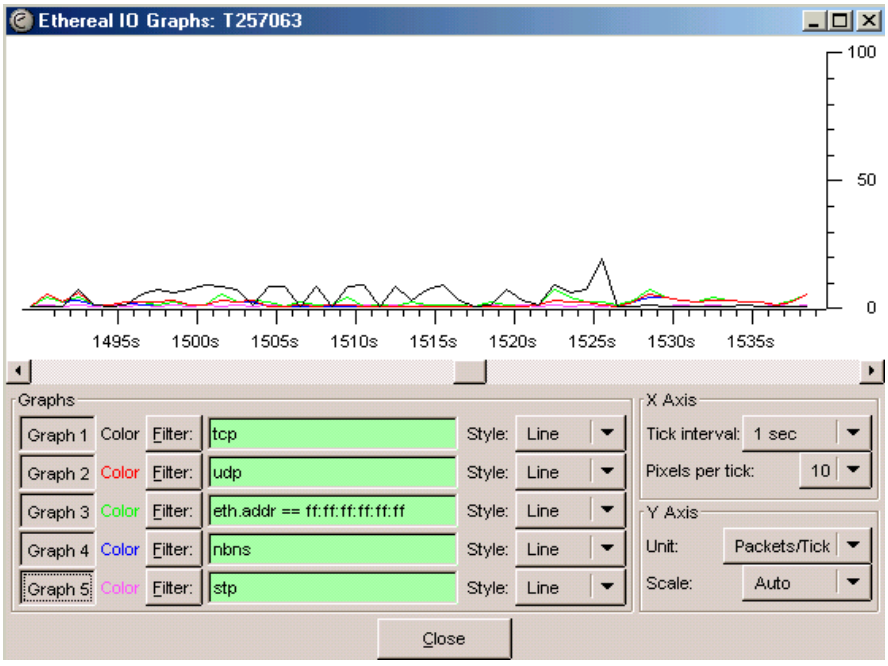


Figura 3.32. Gráfico de paquetes capturados en el Switch LTG-SW-CD1-05-ACC

de la captura de tráfico 2 de la tabla 3.39.

Fuente: Ethereal.

3.3.7 CONCLUSIONES LUEGO DE HABER FINALIZADO EL ANÁLISIS DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA EN EL ÁREA ADMINISTRATIVA.

Luego de haber realizado el análisis de flujo de tráfico de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga en el Área Administrativa, se ha llegado a obtener varias conclusiones del estado en el que se encuentra la red Lan.

1. La principal novedad que se pudo obtener es que en todas las capturas de tráfico que se realizaron en los diferentes departamentos de la Institución, la presencia en gran cantidad de tráfico de Broadcast, este tipo de tráfico lo generan todas las estaciones de trabajo que existen en la Escuela Politécnica del Ejército Sede Latacunga. Como ya se explicó anteriormente el tráfico de broadcast no consume gran cantidad del ancho de banda que dispone la Institución, pero con el pasar del tiempo puede ocasionar serios problemas y mermar el buen desempeño de la red.

2. Otra de las conclusiones que existe en el Área Administrativa es la presencia en gran cantidad del protocolo NBNS, este tipo de tráfico lo genera el servidor de Antivirus Kaspersky que dispone la Institución, no consume mucho ancho de banda pero causa molestia y

esta consumiendo recursos de la red que podrían servir para las aplicaciones que necesitan más el ancho de banda.

3. El protocolo STP es otra de las novedades que se encuentran en el Área Administrativa, este protocolo se genera en todas las capturas de tráfico que se realizaron, se presenta de una forma considerable, se debe realizar el estudio necesario, para llegar a determinar si es norma este tipo de tráfico o si ocasiona riesgo al buen desenvolvimiento de la red.

4. El protocolo CDP se genera en algunas capturas de tráfico que se realizó, ya que este protocolo aparece solo en los equipos de marca Cisco.

Estas son las principales conclusiones que se obtuvieron luego de realizar el análisis del flujo de tráfico de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga realizado en el Área Administrativa.

Todas las conclusiones a las que se han llegado, nos permite determinar que la Red Lan de la Escuela Politécnica del Ejército Sede Latacunga en el Área Administrativa se encuentra en buen estado, ya que como se ha determinado en todo el proceso de análisis, en la mayor parte de capturas de tráfico que se realizaron, los protocolos que se capturaron con la ayuda del analizador Ethereal, no representan peligro al buen funcionamiento de la red Lan.

Como se explicó existen ciertos protocolos que no son muy usuales en la red, para lo cuál se va tomar las medidas más

apropiadas para determinar si representan peligro al desempeño de la red Lan.

A nivel general se debe buscar el mecanismo apropiado para poder solucionar la presencia del tráfico de broadcast, ya que en las capturas de tráfico que se han realizado siempre ha estado presente el mencionado tráfico, por el momento no es algo que pueda ocasionar problemas para el buen desempeño de la red, pero hay que tratar de dar solución, ya que en algún momento la red puede perder eficiencia por la presencia del tráfico de broadcast.

Otro de los problemas que se detectaron en la red, como ya se mencionó anteriormente es la presencia del protocolo NBNS, este protocolo se logró identificar que lo genera el antivirus, es por eso que se va realizar los estudios necesarios para poder solucionar este problema, y de esta se obtenga un óptimo rendimiento tanto en la red como en el antivirus.

Todas las novedades que se encontraron, por el momento no afectan al buen desempeño de la red, los protocolos que se detallaron consumen recursos de red, que pueden ser utilizados de mejor forma por otras aplicaciones.

3.4 ANÁLISIS DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA EN EL ÁREA ACADÉMICA.

A continuación detallamos los diferentes departamentos que pertenecen al Área Académica y nos servirán para realizar el análisis del flujo de tráfico de red.

- Laboratorios de Internet
- Sala de Profesores
- Biblioteca

Como ya se explicó anteriormente, es necesario realizar el análisis de flujo de tráfico de la red Lan en el Área Académica de la Escuela Politécnica del Ejército Sede Latacunga, este análisis permitirá saber el estado en el que se encuentra la red.

Para realizar el análisis del flujo de tráfico de la red Lan en el Área Académica se utilizará como guía fundamental la metodología MIRA, esto ayudará a que los resultados sean eficaces.

3.4.1 MÓDULO DE CAPTURA EN EL HUB LTG-HB-CD7-01-ACC.

Como sabemos el primer módulo de la metodología Mira es el de captura, en este módulo se ha realizado la captura de los paquetes que circulan por el Hub LTG-HB-CD7-01-ACC, el monitoreo se lo realizó en diferentes días y periodos de tiempo.

En el Área Académica los usuarios de la red son los estudiantes de las diferentes carreras que dispone la Escuela Politécnica del Ejército Sede Latacunga, en esta área los estudiantes utilizan el

internet durante todo el día desde la 7:30 hasta las 21:30 y durante los días de clases, es decir de lunes a viernes.

A continuación se detallará todas las capturas de tráfico que se realizaron en las diferentes áreas que pertenecen a la red Académica.

3.4.1.1 HUB LTG-HB-CD7-01-ACC.

En la tabla 3.40 se describen las capturas de tráfico realizadas en el Hub LTG-HB-CD7-01-ACC, el mismo que se encuentra en el centro de datos 7 y presta el servicio a las máquinas que se encuentran en la biblioteca y usan los estudiantes para acceder al servicio de internet.

En el Anexo L se muestra de forma gráfica como se realizó la captura de tráfico en la Biblioteca.

LTG-HB-CD7-01-ACC		
N° DE CAPTURA	**FECHA**	**DETALLE**
1	4 de Julio de 2006	Realizado en la mañana
2	4 de Julio de 2006	Realizado en la tarde
3	4 de Julio de 2006	Realizado en la tarde

Tabla 3.40. Capturas de tráfico realizadas en el Hub LTG-HB-CD7-01ACC.

Fuente: Ethereal.

3.4.2 MÓDULO DE PREPROCESADO

En el módulo de preprocesado se eliminará el tráfico innecesario de las capturas de tráfico que se realizó.
En el Área Académica no es necesario eliminar ningún paquete que está circulando por la red ya que todos estos nos van a servir para realizar un mejor análisis.
Como parte del módulo de preprocesado tenemos varias etapas, las que se detallarán a continuación:

3.4.2.1 ANÁLISIS DE SEGURIDAD

La primera etapa es el análisis de seguridad, en esta etapa se va dividir el tráfico capturado en dos clases que son: tráfico convencional y tráfico sospechoso.

3.4.2.1.1 TRÁFICO CONVENCIONAL

En el Área Académica el tráfico convencional se encuentra en su mayoría, ya que existe gran cantidad de paquetes tales como:

1. TCP/IP los mismos que, permiten establecer la comunicación entre las diferentes estaciones de trabajo por ende no representan peligro alguno para la red.

2. También tenemos en gran cantidad los paquetes HTTP, los mismos que se generan porque todos los usuarios están navegando en el Internet y permite la comunicación, transferencia de archivos de

las páginas Web que utilizan los usuarios, de la misma forma este tipo de protocolo no representan peligro para el buen funcionamiento de la red, de acuerdo al análisis que se realizó mediante Ethereal no consumen mucho ancho de banda.

3. Otro de los paquetes que pertenecen al tráfico convencional es el DNS el mismo que está en el grupo de TCP/IP y permite la resolución de nombres de direcciones al momento que se navega en el Internet, es por eso que este protocolo es muy común y necesario, no va a representar peligro alguno para la red.

3.4.2.1.2 TRÁFICO SOSPECHOSO

Los paquetes que se ha escogido de las diferentes capturas de tráfico que se han realizado en el Área Académica y que pertenecen al tráfico sospechoso son los siguientes:

1. El tráfico de broadcast se genera pero en muy poca cantidad es así que de 10046 paquetes, 125 pertenecen a broadcast, en una captura de tráfico que se realizó en la biblioteca.

2. En las capturas de tráfico que se realizaron aparece el protocolo SSL, este protocolo se genera en muy poca cantidad.

   Este tipo de protocolo se genera porque existen páginas en internet que se abren en el modo seguro es por eso que se genera el SSL.

3. El protocolo Browser aparece en muy poca cantidad en las capturas de tráfico realizadas en el Área Académica.

   El protocolo Browser no se genera en gran cantidad, ya que los estudiantes no tienen recursos compartidos entre las diferentes estaciones de trabajo.

3.4.2.2 ETAPA DE CLASIFICACIÓN

En la segunda etapa del módulo de preprocesado el tráfico convencional que se detalló anteriormente, va ser clasificado en base a las direcciones IP de las máquinas que están conectadas a la red.

A continuación se detallará las direcciones IP de las diferentes estaciones de trabajo del Área Académica, son el resultado de haber realizado la captura de tráfico con el analizador de red Ethereal.

En las tablas que se detallarán a continuación se muestra la dirección IP de la máquina, el total de paquetes y el porcentaje del ancho de banda que consume cada paquete que pasa por la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

3.4.2.2.1 HUB LTG-HB-CD7-01-ACC

En las tablas 3.41 y 3.42 tenemos las direcciones de las máquinas que utilizan el protocolo TCP y UDP respectivamente. Estas tablas se tomaron de las capturas de tráfico 1 de la tabla 3.40 que se realizó en el Hub LTG-HB-CD7-01-ACC.

En las tablas que se presentarán a continuación, se muestran las direcciones IP de las diferentes computadoras que pertenecen al Área Académica y que están en la biblioteca, también se pueden observar direcciones IP de las diferentes páginas de internet que ingresan los estudiantes.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.2.97	17917	0.029872
10.2.2.4	11098	0.018475
216.57.203.33	10919	0.018177
10.2.2.100	7060	0.011753
10.2.2.110	6000	0.009988
10.2.2.109	5397	0.008985
10.2.2.106	4289	0.007140
10.2.2.99	3835	0.006384
10.2.2.98	3817	0.006354
10.2.2.108	2999	0.004992
10.2.2.101	2575	0.004287

10.2.2.102	1898	0.003160
216.32.170.134	1535	0.002555
192.188.58.167	997	0.001660
64.14.123.137	944	0.001571
200.74.221.163	865	0.001440
66.151.4.170	826	0.001375
200.53.64.230	808	0.001345
217.12.10.250	496	0.000826
64.76.233.104	465	0.000774
194.116.241.54	448	0.000746
216.109.124.98	438	0.000729
72.246.50.14	400	0.000666
66.98.158.92	387	0.000644
207.46.11.124	384	0.000639
64.154.81.197	311	0.000518
205.234.199.80	266	0.000443
72.246.50.23	246	0.000410
195.78.228.202	241	0.000401
10.1.0.105	240	0.000400
64.233.179.99	207	0.000345
69.45.79.6	159	0.000256
66.142.228.136	156	0.000260
69.45.79.16	147	0.000245
64.233.187.104	144	0.000746
198.64.137.197	130	0.000216
207.46.216.60	113	0.000188
64.56.205.38	103	0.000171
207.46.216.60	103	0.000171
216.155.194.207	72	0.000120
201.212.1.210	72	0.000120
72.14.219.99	70	0.000117
64.86.142.80	65	0.000108
216.155.200.155	64	0.000107
194.116.241.4	61	0.000102
69.45.79.17	55	0.000092
194.116.241.67	50	0.000083
200.57.147.3	50	0.000083
68.142.213.132	48	0.000080
216.234.246.153	48	0.000080
216.109.127.125	47	0.000078
64.14.123.135	36	0.000060
64.86.142.50	26	0.000043
194.116.240.62	24	0.000040
62.26.220.5	23	0.000038
194.116.241.9	23	0.000038
204.10.108.162	22	0.000037
194.116.241.7	21	0.000035
216.239.51.99	20	0.000033
64.233.179.104	15	0.000025
62.26.220.2	13	0.000022
83.243.23.25	10	0.000017
71.255.213.12	6	0.000010

72.138.85.236	6	0.000010
24.53.174.190	6	0.000010
70.45.64.41	6	0.000010
12.44.66.57	3	0.000005
69.45.79.9	3	0.000005
68.114.71.103	3	0.000005
24.238.95.217	3	0.000005
84.194.220.94	3	0.000005
67.161.146.144	3	0.000005
24.209.9.155	3	0.000005
200.56.237.148	2	0.000003
TOTAL	90360	0.156908

Tabla 3.41. Direcciones IP del Protocolo TCP de la captura de tráfico de la tabla 3.40 del Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.2.4	833	0.001387
10.2.3.255	602	0.001002
200.105.225.2	390	0.000649
10.2.2.97	198	0.000330
10.2.2.110	149	0.000248
10.2.2.109	130	0.000216
10.2.2.98	119	0.000198
10.2.2.100	104	0.000173
200.31.6.34	96	0.000160
10.2.2.106	43	0.000072
192.188.58.163	42	0.000070
10.2.2.99	41	0.000068
10.2.4.4	22	0.000037
10.2.2.107	20	0.000033
10.2.2.101	19	0.000032
10.2.2.108	18	0.000030
10.2.2.95	12	0.000020
10.2.2.102	7	0.000012
10.2.2.173	3	0.000005
10.2.2.96	3	0.000005
10.2.2.104	2	0.000003
10.2.2.103	2	0.000003
234.5.6.7	2	0.000003
10.2.2.94	1	0.000002
10.2.2.105	1	0.000002
10.2.2.174	1	0.000002
10.2.4.7	1	0.000002

TOTAL	2865	0.004772

Tabla 3.42. Direcciones IP del Protocolo UDP de la captura de tráfico 1 de la tabla 3.40 del Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

En las tablas 3.43 y 3.44 tenemos las direcciones de las máquinas que utilizan el protocolo TCP y UDP respectivamente. Estas tablas se tomaron de la captura de tráfico 2 de la tabla 3.40 que se realizó en el Hub LTG-HB-CD7-01-ACC.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.2.103	2784	0.004729
69.45.79.16	864	0.001468
69.45.79.9	592	0.001006
69.16.208.58	569	0.000967
216.252.98.209	191	0.000324
69.45.79.6	119	0.000202
64.233.179.104	107	0.000182
69.45.79.8	90	0.000153
192.188.58.167	71	0.000121
69.45.79.17	58	0.000099
68.142.213.132	47	0.000080
10.1.0.105	38	0.000065
10.2.2.4	29	0.000049
64.233.179.99	9	0.000015
TOTAL	5568	0.009460

Tabla 3.43. Direcciones IP del Protocolo TCP de la captura de tráfico 2 de la tabla 3.40 del Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.2.4	603	0.001009
10.2.3.255	445	0.000744
10.2.2.103	238	0.000398
200.105.225.2	14	0.000023
192.188.58.163	9	0.000015
200.31.6.34	8	0.000013
10.2.2.105	8	0.000013
10.2.2.55	4	0.000007
10.2.2.91	4	0.000007
10.2.2.110	3	0.000005
10.2.2.107	3	0.000005
10.2.2.100	2	0.000003
10.2.2.191	1	0.000002
10.2.2.99	1	0.000002
10.2.2.47	1	0.000002
TOTAL	1358	0.002288

Tabla 3.44. Direcciones IP del Protocolo UDP de la captura de tráfico 2 de la tabla 3.39 del Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

3.4.3 MÓDULO DE CONSOLIDACIÓN

Para continuar con el desarrollo de la metodología Mira tenemos el módulo de consolidación, en este módulo se consolida los resultados parciales de las diferentes capturas de tráfico que se ha realizado en toda el Área Académica de la Escuela Politécnica del Ejército Sede Latacunga, y exponer los diferentes resultados que nos han dado al momento de realizar las capturas de tráfico de la red Lan.

3.4.3.1 HUB LTG-HB-CD7-01-ACC

En la tabla 3.45 se muestra de una forma detallada las capturas de tráfico que se realizaron en el Hub LTG-HB-CD7-01-ACC.

LTG-HB-CD7-01-ACC			
N° DE CAPTURA	**FECHA**	**TIEMPO DE CAPTURA**	**NUMERO DE PAQUETES**
1	4 de Julio de 2006	15 Minutos	59394 Paquetes
2	4 de Julio de 2006	15 Minutos	3899 Paquetes
3	6 de Julio de 2006	10 Minutos	10046 Paquetes

Tabla 3.45. Detalle de las capturas de tráfico realizadas en el Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

3.4.4 MÓDULO DE CLASIFICACIÓN

En este módulo se clasificará el tráfico que se ha capturado en diferentes categorías.

A continuación se detallará las categorías de tráfico que se ha logrado identificar en las diferentes capturas de tráfico que se realizaron.

1. **Primera categoría**.- Esta categoría que se ha identificado, es el traficó normal o convencional el mismo que ya se detalló en el módulo de preprocesado.

   Este tipo de tráfico es el que no representa peligro alguno para el buen desenvolvimiento de la red, este tipo de tráfico

se genera en todas las estaciones de trabajo que dispone la Escuela Politécnica del Ejército Sede Latacunga.

A continuación vamos a citar los protocolos que se han tomado en cuenta en el tráfico normal, tenemos al protocolo TCP, el protocolo UDP, el protocolo HTTP, el protocolo DNS.

2. **Segunda Categoría**.- Esta categoría representa al tráfico académico, este tipo de tráfico se genera en cada una de las estaciones de trabajo que utilizan los estudiantes del Área Académica de la Escuela Politécnica del Ejército Sede Latacunga.

   Luego de haber realizado las diferentes capturas de tráfico, se logró identificar el tráfico académico, el mismo que como se dijo anteriormente lo generan día a día los estudiantes, entre el tráfico tenemos:

   - Cuando un estudiante ingresa al internet debe utilizar el sistema de control Web Access, al realizar este proceso genera tráfico.

   - Cuando el estudiante ingresa al portal de la Institución para consultar sus notas, evaluar a los docentes, estas actividades son las que generan el tráfico administrativo.

   - Navegar en el internet genera tráfico a cada momento durante todo el día en el Área Académica.

3. **Tercera categoría**.- Esta categoría representa al tráfico indeterminado, este tipo de tráfico no se genera en gran cantidad en el Área Académica de la Escuela Politécnica del Ejército Sede Latacunga, el tráfico indeterminado se ha logrado identificar en todas las capturas de tráfico que se han realizado, los protocolos que se encuentran en esta categoría son: el broadcast, NBNS, STP, CDP, BROWSER, estos protocolos ocupan el ancho de banda de la red, el espacio que utilizan no es muy considerable pero sería mejor que este tipo de tráfico de red no se de y de esta forma el espacio que estos protocolos utilizan sería distribuido de mejor forma entre las demás aplicaciones que necesitan el ancho de banda para un correcto y rápido funcionamiento.

3.4.5 MÓDULO DE POSTPROCESADO

En el módulo de postprocesado se realizará informes de forma general de los diferentes resultados que hemos conseguido luego de haber capturado el tráfico en la red.

Con la ayuda del analizador de red Ethereal se presenta los diferentes gráficos del monitoreo de la red, de esta forma ya se puede dar un análisis del estado en el que se encuentra la red.

Para realizar este módulo, vamos a tomar como referencia las capturas de tráfico de red del módulo de consolidación.

3.4.5.1 Hub LTG-HB-CD7-01-ACC

En figura 3.33 se muestra el resumen de la captura de tráfico 1 de la tabla 3.45 realizada en el Hub LTG-HB-CD7-01-ACC.

En la figura se puede ver que el consumo total del ancho de banda es de 0.42%, en este caso el valor ha subido en comparación al Área Administrativa, ya que el uso de internet hace que se generen más paquetes en la red.

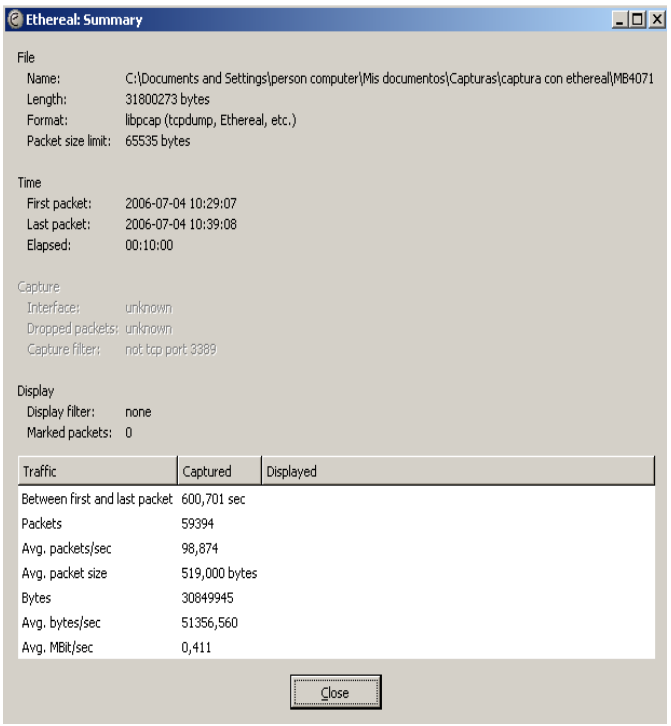


Figura 3.33. Resumen de los paquetes capturados en el Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

En la figura 3.34 se muestra de forma gráfica los paquetes que se capturaron en el Hub LTG-HB-CD7-01-ACC, este gráfico representa a la captura de tráfico 1 de la tabla 3.45.

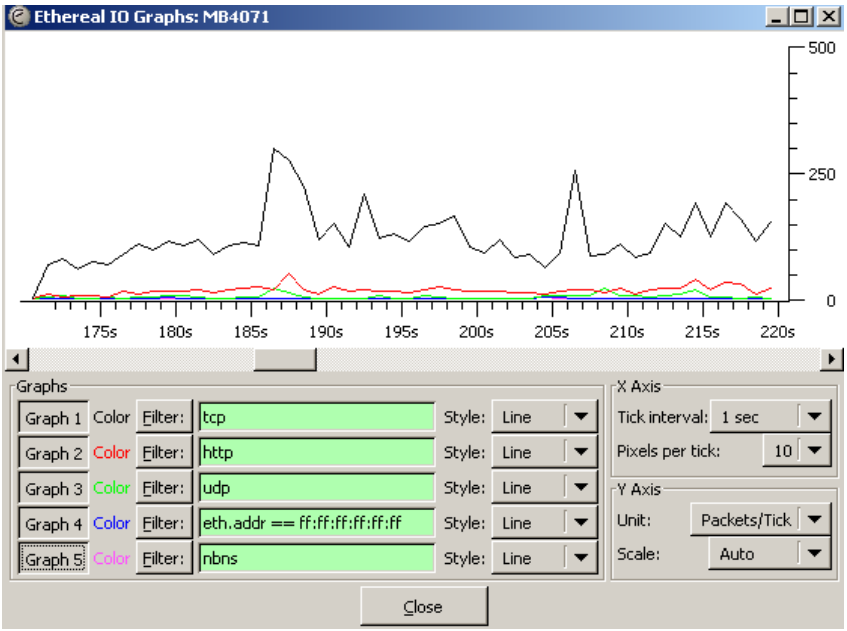


Figura 3.34. Gráfico de los paquetes capturados en el Hub LTG-HB-CD7-01-ACC de la captura de tráfico 1 de la tabla 3.45.

Fuente: Ethereal.

La línea de color negro muestra los paquetes del protocolo TCP como se observa este protocolo se genera en gran cantidad y durante todo el periodo de la captura de tráfico que se realiza, este protocolo se genera ya que los estudiantes a cada momento están navegando en el internet y esa es la principal razón que se genera este tipo de tráfico.

El protocolo HTTP se muestra con una línea de color rojo se puede ver que se genera de forma constante durante toda la captura de tráfico y como era de esperar, luego del TCP el protocolo HTTP es el que se genera en más cantidad, ya que los estudiantes acceden al servicio de internet que presta la Escuela Politécnica del Ejército Sede Latacunga.

De color verde tenemos al protocolo UDP como se puede observa se genera pero en muy poca cantidad.

De color Azul tenemos el tráfico de broadcast en este caso no existe gran cantidad de este tipo de tráfico.

La línea de color lila representa al protocolo NBNS como observamos casi no se genera este tipo de protocolo, este tipo de tráfico lo genera el antivirus.

En figura 3.35 se muestra el resumen de la captura de tráfico 2 de la tabla 3.45 realizada en el Hub LTG-HB-CD7-01-ACC.
En la figura muestra que existe un consumo del 0.08% del total del ancho de banda.

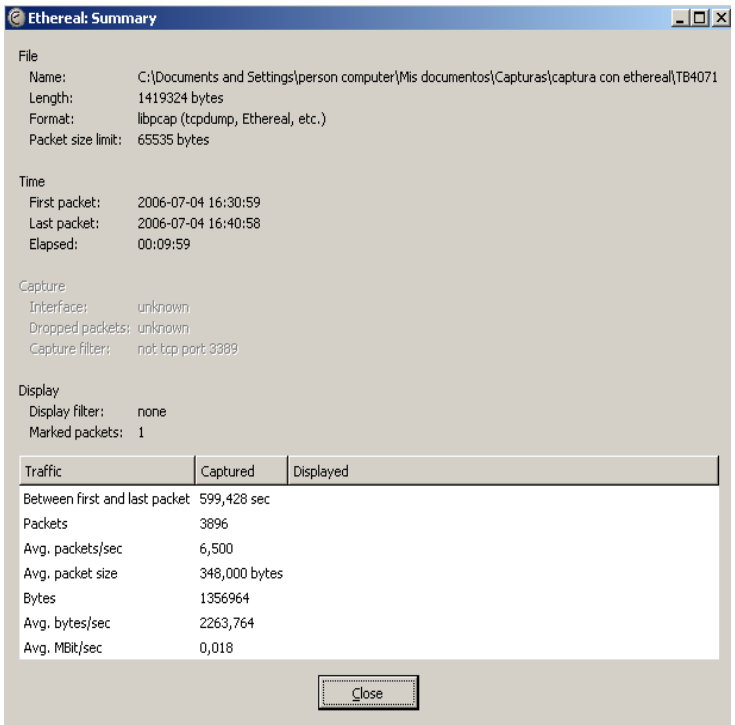


Figura 3.35. Resumen de los paquetes capturados en el Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

En figura 3.36 se muestra de forma gráfica los paquetes que se capturaron en la biblioteca, este gráfico representa a la captura de tráfico 2 de la tabla 3.45.

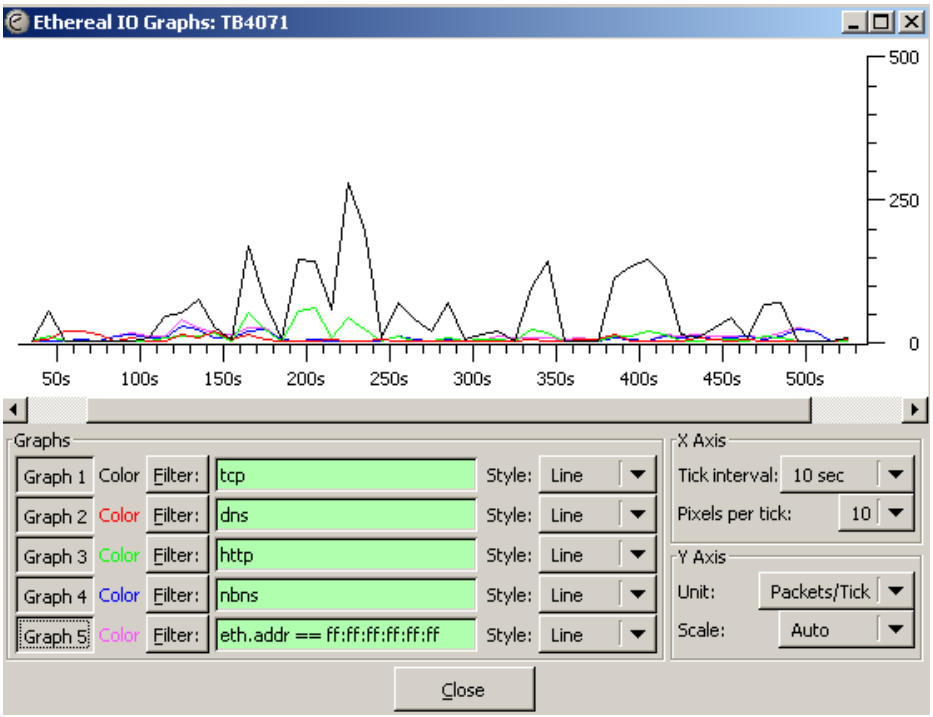


Figura 3.36. Gráfico de los paquetes capturados en el Hub LTG-HB-CD7-01-ACC de la captura de tráfico 1 de la tabla 3.49.

Fuente: Ethereal.

La línea de color negro muestra los paquetes del protocolo TCP como se observa este protocolo se genera en gran cantidad y durante todo el periodo de la captura de tráfico que se realiza, este tipo de tráfico va ser el que predomina siempre ya que los

estudiantes están navegando en el internet, esta es la principal razón que se genere este tipo de tráfico. Otra de las razones que se genera el TCP es porque el antivirus se actualiza diariamente.

El protocolo DNS se muestra con una línea de color rojo se puede ver que se genera de forma constante durante toda la captura de tráfico.

De color verde tenemos al protocolo HTTP como se puede observar que luego del protocolo TCP es el que se genera en más cantidad, la razón es porque los estudiantes utilizan a cada momento el internet.

De color Azul tenemos el protocolo NBNS, en este caso existe una cantidad considerable de este protocolo, como ya se explicó este tipo de tráfico lo genera el antivirus.

La línea de color lila representa el tráfico de broadcast como observamos, este tipo de tráfico no se genera en gran cantidad, ya que las computadoras del Área Académica no interactúan con los servidores.

3.5.1 MÓDULO DE CAPTURA EN EL HUB LTG-HB-CD1-ACC

Como se ha indicado el primer módulo de la metodología Mira es el de captura, en este módulo se ha realizado la captura de los paquetes que circulan por el Hub LTG-HB-CD1-01-ACC, el monitoreo se lo realizó en diferentes días y periodos de tiempo.

En el Área Académica los usuarios de la red son los estudiantes de las diferentes carreras que dispone la Escuela Politécnica del

Ejército Sede Latacunga, en esta área los estudiantes utilizan el internet durante todo el día desde la 7:30 hasta las 21:30 y durante los días de clases, es decir de lunes a viernes.

A continuación se detallará todas las capturas de tráfico que se realizaron en las diferentes áreas que pertenecen a la red Académica.

3.5.1.1 HUB LTG-HB-CD1-01-ACC.

En la tabla 3.46 se describen las capturas de tráfico realizadas en el Hub LTG-HB-CD1-O1-ACC, el mismo que se encuentra en el centro de datos 1 y da servicio a las máquinas que se encuentran en el laboratorio de internet.

LTG-HB-CD1-O1-ACC		
N° DE CAPTURA	**FECHA**	**DETALLE**
1	5 de Julio de 2006	Realizado en la mañana
2	5 de Julio de 2006	Realizado en la mañana
3	5 de Julio de 2006	Realizado en la tarde

Tabla 3.46. Capturas de tráfico realizadas en el Hub LTG-HB-CD1-01-ACC.
Fuente: Ethereal.

3.5.2 MÓDULO DE PREPROCESADO

En el módulo de preprocesado se eliminará el tráfico innecesario de las capturas de tráfico que se realizó.

En el Área Académica no es necesario eliminar ningún paquete que está circulando por la red ya que todos estos nos van a servir para realizar un mejor análisis.
Como parte del módulo de preprocesado tenemos varias etapas, las que se detallarán a continuación:

3.5.2.1 Análisis de Seguridad.

3.5.2.1.1 Tráfico Convencional

En el Área Académica el tráfico convencional se encuentra en su mayoría, ya que existe gran cantidad de paquetes tales como:

1. TCP/IP los mismos que, permiten establecer la comunicación entre las diferentes estaciones de trabajo por ende no representan peligro alguno para la red.

2. También tenemos en gran cantidad los paquetes HTTP, los mismos que se generan porque todos los usuarios están navegando en el Internet y permite la comunicación, transferencia de archivos de las páginas Web que utilizan los usuarios, de la misma forma este tipo de protocolo no representan peligro para el buen funcionamiento de la red, de acuerdo al análisis que se realizó mediante Ethereal no consumen mucho ancho de banda.

3. Otro de los paquetes que pertenecen al tráfico convencional es el DNS el mismo que está en el

grupo de TCP/IP y permite la resolución de nombres de direcciones al momento que se navega en el Internet, es por eso que este protocolo es muy común y necesario, no va a representar peligro alguno para la red.

3.5.2.1.2 Tráfico Sospechoso

Los paquetes que se ha escogido de las diferentes capturas de tráfico que se han realizado en el Área Académica y que pertenecen al tráfico sospechoso son los siguientes:

1. El tráfico de broadcast se genera pero en muy poca cantidad es así que de 16066 paquetes, 97 pertenecen a broadcast, en una captura de tráfico que se realizó en la biblioteca.

2. En las capturas de tráfico que se realizaron aparece el protocolo SSL, este protocolo se genera en muy poca cantidad.
   Este tipo de protocolo se genera porque existen páginas en internet que se abren en el modo seguro es por eso que se genera el SSL.

3. El protocolo Browser aparece en muy poca cantidad en las capturas de tráfico realizadas en el Área Académica.

El protocolo Browser no se genera en gran cantidad, ya que los estudiantes no tienen recursos compartidos entre las diferentes estaciones de trabajo.

3.5.2.2 Etapa de Clasificación

En la segunda etapa del módulo de preprocesado el tráfico convencional que se detalló anteriormente, va ser clasificado en base a las direcciones IP de las máquinas que están conectadas a la red.

A continuación se detallará las direcciones IP de las diferentes estaciones de trabajo del Área Académica, son el resultado de haber realizado la captura de tráfico con el analizador de red Ethereal.

En las tablas que se detallarán a continuación se muestra la dirección IP de la máquina, el total de paquetes y el porcentaje del ancho de banda que consume cada paquete que pasa por la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

3.5.2.2.1 HUB LTG-HB-CD1-01-ACC

En las tablas 3.47 y 3.48 tenemos las direcciones IP de las máquinas que utilizan el protocolo TCP y UDP respectivamente. Estas tablas se tomaron de

la captura de tráfico 1 de la tabla 3.46 que se realizó en el Hub LTG-HB-CD1-01-ACC.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.2.4	4798	0.015965
10.2.2.110	4048	0.013469
10.2.2.96	3763	0.012521
205.188.226.51	3748	0.012471
209.172.57.71	2553	0.0084495
10.2.2.108	1872	0.006229
10.2.2.101	1345	0.004475
10.2.2.102	1030	0.003427
10.2.2.106	982	0.003267
80.24.6.24	787	0.002619
10.2.2.98	666	0.002216
10.2.2.99	663	0.002206
10.2.2.97	540	0.001797
10.2.2.100	535	0.001780
208.19.69.132	278	0.000925
216.239.209.173	221	0.000735
64.233.187.99	114	0.000379
207.138.234.72	85	0.000283
216.239.209.172	81	0.000270
10.1.0.105	75	0.000250
10.2.2.109	58	0.000193
130.94.72.77	54	0.000180
217.76.143.127	54	0.000180
80.67.86.55	50	0.000166
62.37.237.71	50	0.000166
216.74.132.12	48	0.000160
69.20.14.179	38	0.000126
216.109.112.136	38	0.000126
64.74.197.108	36	0.000120
64.233.179.104	29	0.000096
216.139.221.122	26	0.000087
217.12.4.96	20	0.000067
72.37.157.36	20	0.000067
195.167.168.51	16	0.000053
212.59.195.194	13	0.000043
209.73.177.115	12	0.000040
207.138.234.74	10	0.000033
72.14.219.104	9	0.000030
207.138.234.66	8	0.000027
217.76.142.28	8	0.000027
201.219.15.18	6	0.000020
204.2.240.9	4	0.000013
66.24.194.27	3	0.000010

24.53.174.190	3	0.000010
24.19.62.191	3	0.000010
209.249.170.10	3	0.000010
198.78.183.215	3	0.000010
70.45.64.41	3	0.000010
66.214.240.60	3	0.000010
24.184.177.179	3	0.000010
24.31.116.141	3	0.000010
71.232.6.171	1	0.000003
68.125.99.90	1	0.000003
TOTAL	28836	0.952590

Tabla 3.48. Direcciones IP del Protocolo TCP de la captura de tráfico 1 de la tabla 3.46 del Hub LTG-HB-CD1-01-ACC.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.2.4	144	0.000503
10.2.3.255	90	0.000314
10.2.2.108	84	0.000294
200.105.225.2	81	0.000283
10.2.2.106	26	0.000091
10.2.2.101	19	0.000066
10.2.2.96	17	0.000059
200.31.6.34	14	0.000049
10.2.2.110	12	0.000042
10.2.2.98	8	0.000028
TOTAL	495	0.001827

Tabla 3.48. Direcciones IP del Protocolo UDP de la captura de tráfico 2 de la tabla 3.46 del Hub LTG-HB-CD1-01-ACC.

Fuente: Ethereal.

En las tablas 3.49 y 3.50 tenemos las direcciones IP de las máquinas que utilizan el protocolo TCP y UDP respectivamente. Estas tablas se tomaron de la captura de tráfico 2 de la tabla 3.41 que se realizó en el Hub LTG-HB-CD1-01-ACC.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
69.45.79.15	2711	0.000188
10.2.2.4	2709	0.014986
10.2.2.108	1935	0.010704
10.2.2.102	1868	0.010333
10.2.2.98	1750	0.009681
10.2.2.99	1186	0.006551
10.2.2.109	1164	0.006439
10.2.2.110	1074	0.005941
10.21.2.100	989	0.005471
209.85.33.83	863	0.004774
69.28.159.180	581	0.003214
192.188.58.167	546	0.003031
213.171.218.49	518	0.002865
10.2.2.101	471	0.002605
102.2.106	464	0.002567
204.11.109.61	191	0.001057
10.1.0.105	149	0.000824
64.14.123.137	145	0.000802
64.233.179.104	132	0.000730
69.45.79.9	129	0.000714
80.38.213.254	127	0.000703
62.37.237.71	95	0.000526
65.54.179.248	57	0.000315
68.142.228.136	56	0.000310
150.244.8.55	56	0.000310
70.84.143.160	50	0.000277
68.142.225.170	47	0.000260
216.109.117.223	46	0.000254
217.15.42.28	42	0.000232
130.94.72.77	40	0.000221
213.244.183.216	35	0.000194
200.80.42.134	34	0.000188
207.44.134.37	33	0.000183
62.37.236.163	24	0.000133
64.14.123.140	23	0.000127
66.35.214.30	23	0.000127
216.117.166.96	18	0.000100
64.233.179.99	15	0.000083
69.45.79.8	8	0.000044
203.84.209.211	6	0.000033
63.99.244.79	3	0.000017
84.194.220.94	3	0.000017
66.158.226.157	3	0.000017
64.247.65.225	3	0.000017
208.42.174.133	3	0.000017
67.50.91.145	3	0.000017
75.3.185.224	3	0.000017
70.228.174.25	3	0.000017

71.235.189.22	3	0.000017
200.56.172.87	3	0.000017
140.192.178.139	1	0.000006
147.26.236.209	1	0.000006
209.185.12.47	1	0.000006
TOTAL	20461	0.098386

Tabla 3.49. Direcciones IP del Protocolo TCP de la captura de tráfico 2 de la tabla 3.46 del Hub LTG-HB-CD1-01-ACC.

Dirección IP	***Total de Paquetes***	***Porcentaje Ancho de Banda***
10.2.2.4	323	0.001797
10.2.3.255	287	0.001597
200.105.225.2	112	0.000623
10.2.2.102	85	0.000473
10.2.2.108	26	0.0000145
200.31.6.34	23	0.000128
10.2.2.99	23	0.000128
10.2.2.106	18	0.000100
192.188.58.163	14	0.000078
10.2.2.107	12	0.000067
10.2.2.98	12	0.000067
10.2.2.110	10	0.000056
10.2.2.101	7	0.000039
10.2.2.97	5	0.000028
10.2.2.100	3	0.000017
10.2.2.44	1	0.000006
10.2.2.43	1	0.000006
10.2.2.105	1	0.000006
TOTAL	964	0.052365

Tabla 3.50. Direcciones IP del Protocolo TCP de la captura de tráfico 2 de la tabla 3.46 del Hub LTG-HB-CD1-01-ACC.

Fuente: Ethereal.

3.5.3 MÓDULO DE CONSOLIDACIÓN

Para continuar con el desarrollo de la metodología Mira tenemos el módulo de consolidación, en este módulo se consolida los resultados parciales de las diferentes capturas de tráfico que se ha realizado en toda el Área Académica de la Escuela Politécnica del Ejército Sede Latacunga, y exponer los diferentes resultados que nos han dado al momento de realizar las capturas de tráfico de la red Lan.

3.5.3.1 HUB LTG-HB-CD1-01-ACC

En la tabla 3.51 se muestra de una forma detallada las capturas de tráfico que se realizaron en el Hub LTG-HB-CD1-01-ACC.

LTG-HB-CD1-01-ACC			
N° DE CAPTURA	**FECHA**	**TIEMPO DE CAPTURA**	**NUMERO DE PAQUETES**
1	5 de Julio de 2006	15 Minutos	16066
2	6 de Julio de 2006	10 Minutos	12695
3	**6 de Julio de 2006**	**11 Minutos**	**895**

Tabla 3.51. Detalle de las capturas de tráfico realizadas en el Hub LTG-HB-CD7-01-ACC.

Fuente: Ethereal.

3.5.4 MÓDULO DE CLASIFICACIÓN

En este módulo se clasificará el tráfico que se ha capturado en diferentes categorías.

A continuación se detallará las categorías de tráfico que se ha logrado identificar en las diferentes capturas de tráfico que se realizaron.

1. **Primera categoría**.- Esta categoría que se ha identificado, es el traficó normal o convencional el mismo que ya se detalló en el módulo de preprocesado.

   Este tipo de tráfico es el que no representa peligro alguno para el buen desenvolvimiento de la red, este tipo de tráfico se genera en todas las estaciones de trabajo que dispone la Escuela Politécnica del Ejército Sede Latacunga.

   A continuación vamos a citar los protocolos que se han tomado en cuenta en el tráfico normal, tenemos al protocolo TCP, el protocolo UDP, el protocolo HTTP, el protocolo DNS.

2. **Segunda Categoría**.- Esta categoría representa al tráfico académico, este tipo de tráfico se genera en cada una de las estaciones de trabajo que utilizan los estudiantes del Área Académica de la Escuela Politécnica del Ejército Sede Latacunga.

   Luego de haber realizado las diferentes capturas de tráfico, se logró identificar el tráfico académico, el mismo que como se dijo anteriormente lo generan día a día los estudiantes, entre el tráfico tenemos:

   - Cuando un estudiante ingresa al internet debe utilizar el sistema de control Web Access, al realizar este proceso genera tráfico.

   - Cuando el estudiante ingresa al portal de la Institución para consultar sus notas, evaluar a los docentes, estas actividades son las que generan el tráfico administrativo.

- Navegar en el internet genera tráfico a cada momento durante todo el día en el Área Académica.

3. **Tercera categoría**.- Esta categoría representa al tráfico indeterminado, este tipo de tráfico no se genera en gran cantidad en el Área Académica de la Escuela Politécnica del Ejército Sede Latacunga, el tráfico indeterminado se ha logrado identificar en todas las capturas de tráfico que se han realizado, los protocolos que se encuentran en esta categoría son: el broadcast, NBNS, STP, CDP, BROWSER, estos protocolos ocupan el ancho de banda de la red, el espacio que utilizan no es muy considerable pero sería mejor que este tipo de tráfico de red no se de y de esta forma el espacio que estos protocolos utilizan sería distribuido de mejor forma entre las demás aplicaciones que necesitan el ancho de banda para un correcto y rápido funcionamiento.

3.5.5 MÓDULO DE POSTPROCESADO

En el módulo de postprocesado se realizará informes de forma general de los diferentes resultados que hemos conseguido luego de haber capturado el tráfico en la red.

Con la ayuda del analizador de red Ethereal se presenta los diferentes gráficos del monitoreo de la red, de esta forma ya se puede dar un análisis del estado en el que se encuentra la red.

Para realizar este módulo, vamos a tomar como referencia las capturas de tráfico de red del módulo de consolidación.

3.5.5.1 HUB LTG-HB-CD1-01-ACC

En figura 3.37 se muestra el resumen de la captura de tráfico 1 de la tabla 3.51 realizada en el Hub LTG-HB-CD1-01-ACC.

En este caso el consumo del ancho de banda representa 0.177% del total de ancho de banda disponible. En el Área Académica el consumo es más elevado ya que los estudiantes utilizan el internet diariamente.

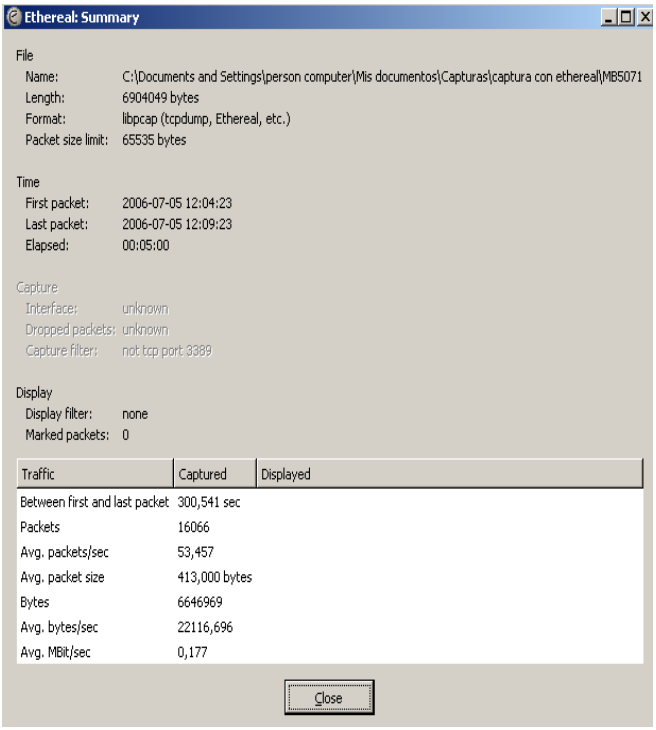


Figura 3.37. Resumen de los paquetes capturados en el Hub LTG-HB-CD1-01-ACC.

Fuente: Ethereal.

En la figura 3.38 se muestra de forma gráfica los paquetes que se capturaron en el Hub LTG-HB-CD1-01-ACC, este gráfico representa a la captura de tráfico 1 de la tabla 3.51.

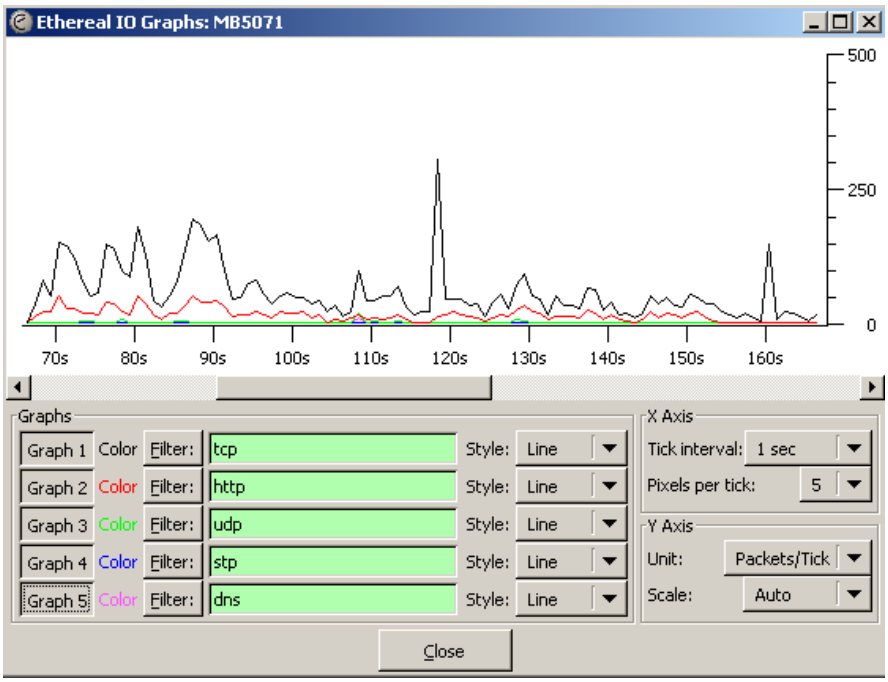


Figura 3.38. Gráfico de los paquetes capturados en el Hub LTG-HB-CD1-01-ACC de la captura de tráfico 1 de la tabla 3.51.

Fuente: Ethereal.

La línea de color negro muestra los paquetes del protocolo TCP como se observa este protocolo se genera en gran cantidad y durante todo el periodo de la captura de tráfico que se realiza, este tipo de tráfico es el que se generará siempre y en gran

cantidad, ya que los estudiantes están navegando en el internet, esta es la principal razón que se genere este tipo de tráfico. Otra de las razones que se genera el TCP es porque el antivirus se actualiza diariamente.

.

De color rojo tenemos al protocolo HTTP como se puede observar que luego del protocolo TCP es el que se genera en más cantidad, al igual que protocolo TCP, el HTTP es el que siempre estará presente, ya que permite que usuario pueda navegar en las diferentes páginas que existen en el internet.

El protocolo UDP se muestra con una línea de color verde se puede ver que se genera de forma constante durante toda la captura de tráfico.

De color Azul tenemos el protocolo STP, en este caso existe una cantidad considerable de este protocolo, ya que pocas computadoras que se están ubicadas en la biblioteca están conectadas al switch 3Com, y de esta forma se genera el STP.

La línea de color lila representa el protocolo DNS como observamos casi no se genera este tipo protocolo.

En figura 3.39 se muestra el resumen de la captura de tráfico 2 de la tabla 3.51 realizada en el Hub LTG-HB-CD1-01-ACC.

El consumo del ancho de banda en este Hub representa el 0.258, como se explicó esto se debe a que los estudiantes trabajan constantemente en el internet.

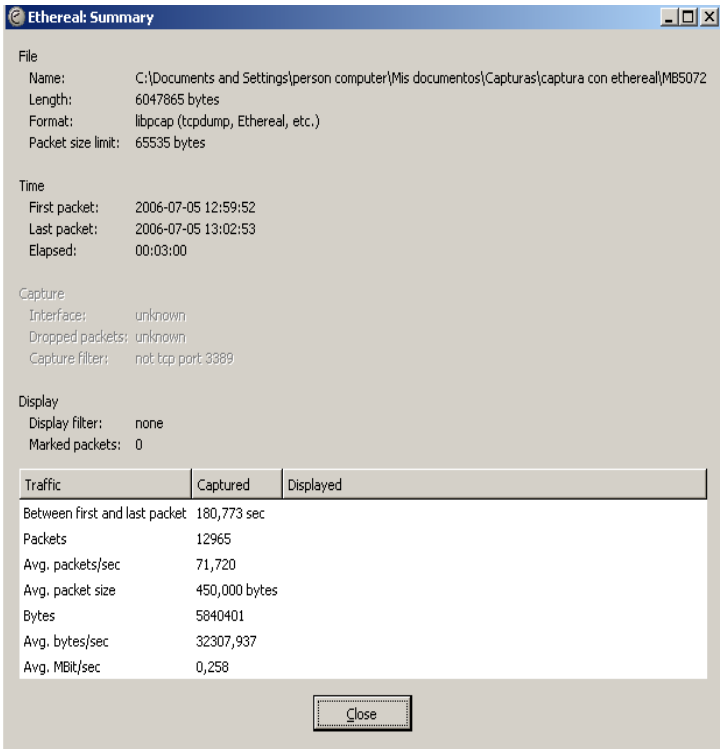


Figura 3.39. Resumen de los paquetes capturados en el Hub LTG-HB-CD1-01-ACC.

Fuente: Ethereal.

En la figura 3.40 se muestra de forma gráfica los paquetes que se capturaron en el Hub LTG-HB-CD1-01-ACC, este gráfico representa a la captura de tráfico 2 de la tabla 3.51.

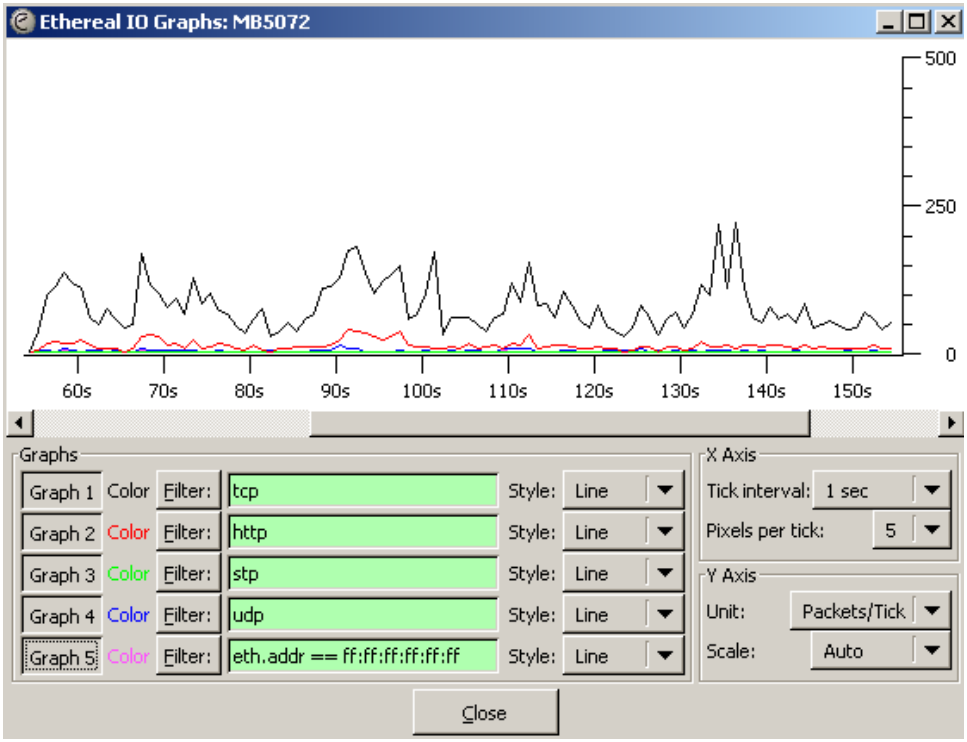


Figura 3.40. Gráfico de los paquetes capturados en el Hub LTG-HB-CD1-01-ACC de la captura de tráfico 2 de la tabla 3.50.

Fuente: Ethereal.

La línea de color negro representa a los paquetes del protocolo TCP como se observa este protocolo se genera en gran cantidad y durante todo el periodo de la captura de tráfico que se realiza, este tipo de tráfico va ser el que predomina siempre ya que los estudiantes están navegando en el internet, esta es la principal razón que se genere este tipo de tráfico. Otra de las razones que se genera el TCP es porque el antivirus se actualiza diariamente.

De color rojo tenemos al protocolo HTTP como se puede observar que luego del protocolo TCP es el que se genera en más cantidad, de igual forma este tipo de tráfico lo generan todas las computadoras que están conectadas al internet.

De color verde se encuentra identificado el protocolo STP, se genera en poca cantidad, por motivo de que hay pocas computadoras conectadas a un switch 3Com en la biblioteca.

De color Azul tenemos el protocolo UDP, en este caso existe una cantidad considerable de este protocolo.

La línea de color lila representa el tráfico de broadcast como observamos se presenta en muy poca cantidad este tipo de protocolo, ya que las computadoras no se conectan con frecuencia a los servidores que dispone la Institución.

En los Hub que se ha realizado el análisis no existe mayor novedad, ya que el consumo del ancho de banda no es muy elevado, como se explicó en las figuras existe más tráfico que en el Área Administrativa, debido a que los estudiantes navegan todo el día en el internet, lo que hace que se genere gran cantidad de paquetes.

3.6 CONCLUSIONES LUEGO DE HABER FINALIZADO EL ANÁLISIS DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA EN EL ÁREA ACADÉMICA.

Luego de haber finalizado con eL análisis de flujo de tráfico de la red Lan en el Área Académica de la Escuela Politécnica del Ejército Sede Latacunga, se puede determinar que en esta área no existe novedades de consideración, ya que como era de esperar en esta área los protocolos más utilizados son el TCP,

HTTP, ya que los estudiantes acceden diariamente al servicio de internet que presta la Institución, los protocolos que anteriormente se mencionaron son los que predominan en este tipo de red.

La principal novedad que se puede determinar luego de haber realizado el análisis del flujo de tráfico en el Área Académica, es referente a los hubs que se encuentran tanto en el centro de datos 1 como en el centro de datos 7, estos dispositivos no se pueden administrar, simplemente permiten la conexión de equipos entre sí y nada más.
Es por esa razón que se debe reemplazar los hubs por switches, de esta forma se podrá administrar de mejor forma los equipos que se conecten al switch.

Otro de las novedades que se encontraron e el Área Académica es la presencia del protocolo NBNS, se presenta en una cantidad considerable, como ya se mencionó en el Área Administrativa, este protocolo lo genera el antivirus Kaspersky, es por eso que se realizará los cambios necesarios para optimizar el servicio de red y al mismo tiempo del antivirus.

En base a la solución de los problemas que se den en el Área Administrativa se implementará cambios en el Área Académica para el correcto funcionamiento de la red Lan.

CAPÍTULO IV

OPTIMIZACIÓN DEL FLUJO DE TRÁFICO DE LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA

4.1 INTRODUCCIÓN

En este capítulo se realizará la optimización del flujo de tráfico de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, esto permitirá que si es del caso se realice varios cambios, para que la red funcione de mejor forma, se ahorren recursos, y de esta forma se beneficiará a todos los usuarios de la red.

La optimización consiste en dar solución a los diferentes problemas, novedades que se identificaron en el capítulo anterior.

En base a las recomendaciones que se van a dar a continuación se podrá realizar la optimización del flujo de tráfico.

4.2 RECOMENDACIONES PARA OPTIMIZAR EL TRÁFICO EN LA RED LAN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA.

Las recomendaciones que se darán a continuación son una parte fundamental para que se pueda realizar los correctivos necesarios en la red Lan de la Escuela Politécnica del Ejército Sede Latacunga.

1. Luego de haber realizado el Análisis del Flujo de Tráfico en la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, la principal novedad que se identificó, es que en todas las capturas de tráfico realizadas en el Área Administrativa se genera una gran cantidad de tráfico de broadcast, para solucionar este problema se debe realizar los estudios necesarios para ver si existe la posibilidad de disminuir la presencia de este tipo de tráfico, siempre y cuando no afecte el normal funcionamiento de las diferentes aplicaciones que se manejan en la Institución, o de alguna forma tratar de controlar para que la red Lan funcione de mejor forma y se optimicen sus recursos.

2. Verificar el funcionamiento del protocolo STP, ya que en todas las capturas de tráfico realizadas, el protocolo antes mencionado esta siempre presente y en gran cantidad, y de esta forma determinar si es normal o no este tipo de tráfico, de esta forma no se desperdicie los recursos de red.

3. Realizar los estudios necesarios para ver si existe la posibilidad de mejorar el funcionamiento del antivirus, ya que al realizar el monitoreo se detectó que, cuando el servidor de antivirus manda a ejecutar una tarea en una estación de trabajo y si la misma está apagada o no está en red, el servidor de antivirus esta enviando paquetes constantemente a la estación de trabajo, esta tarea la

realiza el servidor hasta detectar que la computadora esté lista, y por ende siempre esta generando tráfico y se desperdicia los recursos de red.

4. Se recomienda dotar de computadoras de última generación a todos los usuarios que no disponen de este tipo de computadoras, ya que en algunos casos no es que la red sea lenta, sino las características de las computadoras hace que la información que solicitan tarde en mostrarse al usuario.

4.3 IMPLANTACIÓN DE LAS RECOMENDACIONES

4.3.1 Implantación de la primera recomendación.

Como ya se explicó, en todo el análisis del flujo de tráfico de la red Lan que se realizó, la presencia en gran cantidad del tráfico de broadcast, ha sido la principal novedad, para lo cuál se ha realizado los estudios necesarios para tratar de reducir este tipo de tráfico y de esta forma no se consuman los recursos de red de forma innecesaria.

Se ha realizado los estudios necesarios para optimizar el tráfico de broadcast y se ha determinado que es conveniente realizarlo en la capa 3 del modelo OSI, es decir en la capa de red.

A dicha capa pertenecen los dispositivos que permiten la comunicación entre las diferentes estaciones de trabajo como son los switchs, y es en estos dispositivos que existe la posibilidad de

controlar el tráfico de broadcast que se genera en la red Lan de la Institución.

Para lo cuál como se detalló en capítulos anteriores la Escuela Politécnica del Ejército Sede Latacunga dispone de varios centros de datos en los que se encuentra varios switchs y en los que se realizará las respectivas configuraciones para optimizar el tráfico de broadcast, y evitar que en algún momento baje el rendimiento de la red a causa del tráfico antes mencionado.

Hay que acotar que antes de implementar el control de tráfico de broadcast, se realizaron varias pruebas, de esta forma se determinó que funciona de forma correcta la opción broadcastStormCont. Para realizar las pruebas mencionadas se utilizó valores de 10, 30, 50, 100 pps, esto quiere decir paquetes por segundo.

Luego de haber realizado las pruebas se procedió configurar los diferentes switches que dispone la Escuela Politécnica del Ejército Sede Latacunga.

4.3.1.1 Implantación de la primera recomendación en el Centro de Datos 1.

Para este centro de datos, se va optimizar el tráfico de broadcast en el switch Cisco 3559 que realiza la función COR y este switch es el principal de toda la red.

Luego pasaremos a los switches que permiten la función de acceso es decir en los Switchs 3Com 4228G, la configuración que se va determinar para estos equipos se muestran en la siguiente tabla:

CENTRO DE DATOS 1		
NOMBRE DEL EQUIPO	**SWITCH**	**# DE PUERTOS**
LTG-SW-CD1-01-COR	CISCO 3550	24
LTG-SW-CD1-02-ACC	3Com 4228G	24
LTG-SW-CD1-03-ACC	3Com 4228G	24
LTG-SW-CD1-04-ACC	3Com 4228G	48
LTG-SW-CD1-05-ACC	HP Procurve	24
LTG-HB-CD1-01-ACC	DSH-32 DLINK	32

Tabla 4.1 Información referente a los Switch y Hub del Centro de Datos 1

4.3.1.1.1 Pasos para implantar el Storm-Control Broadcast en el Switch Cisco 3560G del Centro de Datos 1.

Para configurar el control del tráfico de broadcast en el switch Cisco 3560G se debe seguir los siguientes pasos:

- Debemos ingresar a la configuración principal del Switch, el administrador de este dispositivo deberá ingresar el login y password correspondiente al equipo.

- En la configuración debemos ingresar Configure Terminal.

Luego ingresamos la interfaz, es decir el número de puerto que se va a controlar el tráfico de broadcast, para el caso del switch Cisco 3560G se configurará varios puertos, los mismos que garantizaran un correcto funcionamiento en la red.

- Luego se debe ingresar el comando storm-control broadcast level 10, esto quiere decir que para el tráfico de broadcast se asigna el 10% del total del ancho de banda, esto hará que la red no pierda eficiencia ya que hemos asignado un espacio para el tráfico que puede ocasionar problema en algún momento. En la figura 4.1 podemos observar los pasos que se describieron anteriormente.

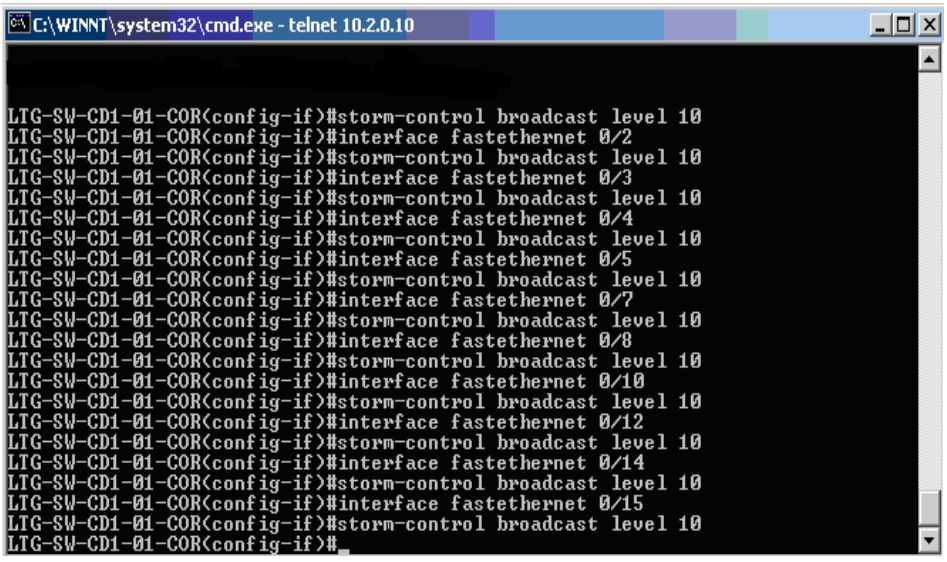


Figura 4.1. Configuración del store-control broadcast en el switch LTG-SW-CD1-01-COR.

- Para verificar si los pasos que hemos realizado se han ejecutado correctamente debemos ingresar el comando show interfaces mas el número de puerto que deseamos verificar. Esto podemos ver de mejor forma en la figura 4.2.

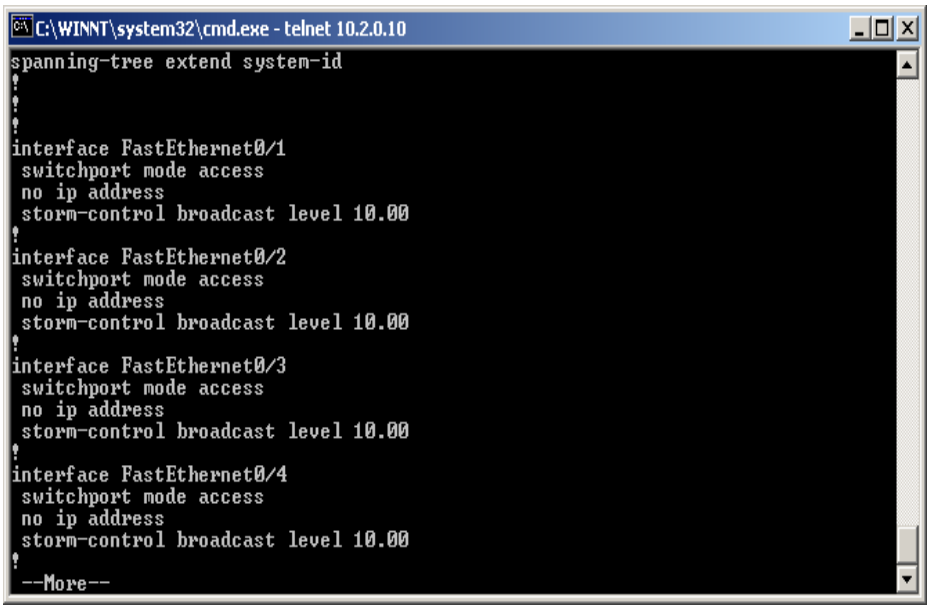


Figura 4.2. Configuración del store-control broadcast en el switch LTG-SW-CD1-01-COR.

4.3.1.1.2 Pasos para implantar el BroadcastStormCont en los Switches 3Com 4228G del Centro de Datos 1.

En los switches 3Com se aplicará los siguientes pasos para configurar el control del tráfico de broadcast:

- Debemos ingresar a la configuración principal del Switch, el administrador de estos dispositivos deberá ingresar el login y password correspondiente al

equipo, luego de eso nos aparecerá una ventana como la que observaremos en la figura 4.3.

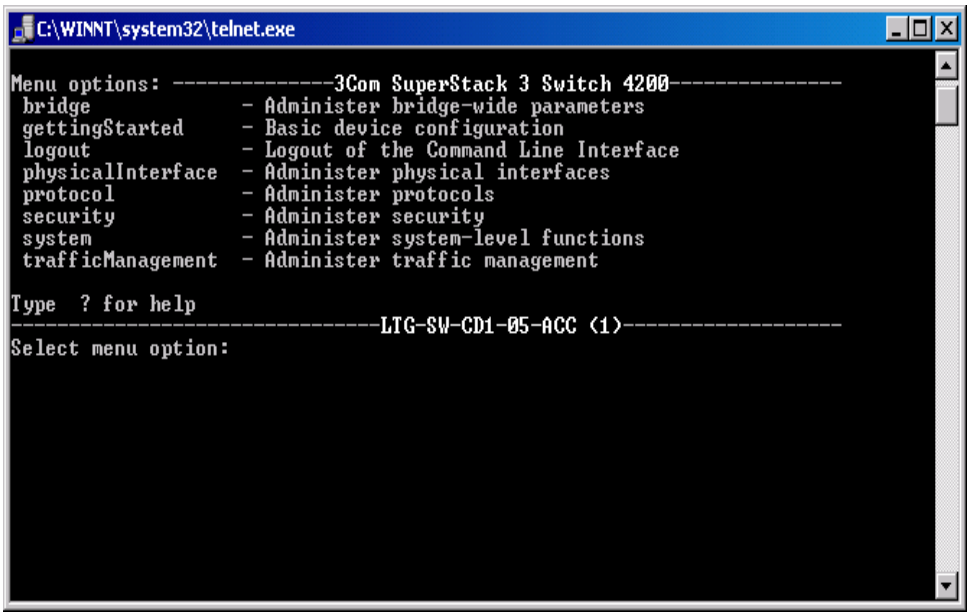


Figura 4.3 Menú de configuración del Switch 3Com.

- Luego de esto se debe seleccionar la opción Bridge y nos aparecerá un menú como el que podemos observar en la figura 4.4.

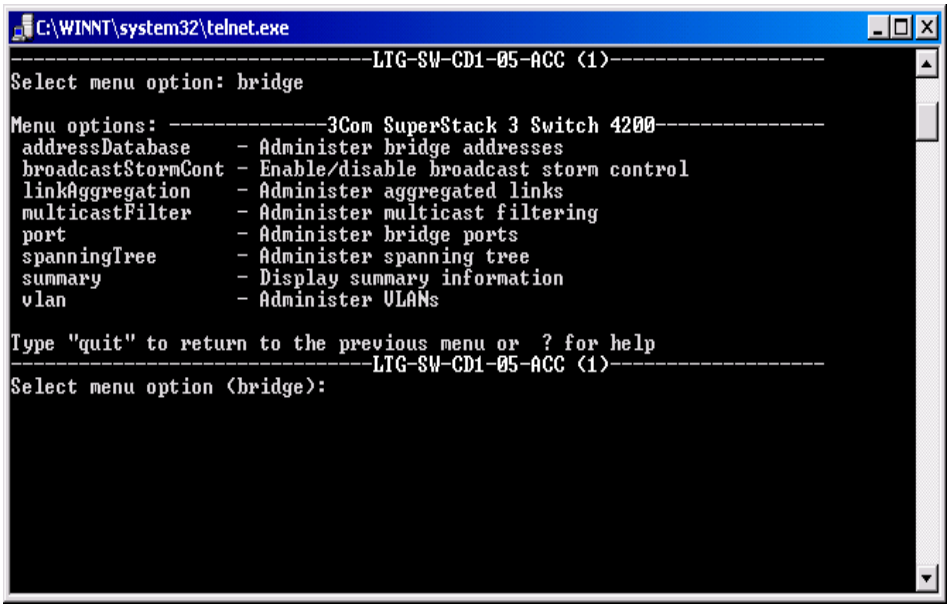


Figura 4.4 Menú de la opción Bridge.

- Seleccionamos la opción BroadcastStormCont, y va aparecer un menú como podemos observar en la figura 4.5.

- Nos pedirá que ingresemos un nuevo valor en el que debe seleccionar enable, esta opción permite que se habilite el BroadcastStormCont.

- Luego nos pide ingresar un valor que está entre 0 y 200000, este valor esta dado en pps, que quiere decir paquetes por segundo, aquí se ingresará para todos los switchs 3Com el valor de 1000 pps, es decir el Switch permitirá que solo pasen 1000 paquetes de broadcast por segundo, este valor se asignado tomando en cuenta que los paquetes de broadcast tienen un tamaño entre 60 y 106 Bytes, y al realizar esta configuración del BroadcastStomCont se va ahorrar los recursos de la red, y no permitirá que el tráfico de broadcast ocupe más del 0.106 % aproximadamente del ancho de banda que dispone la Institución en el supuesto caso que en algún

momento se llegue a ocupar los 1000 paquetes por segundo que se asignado.

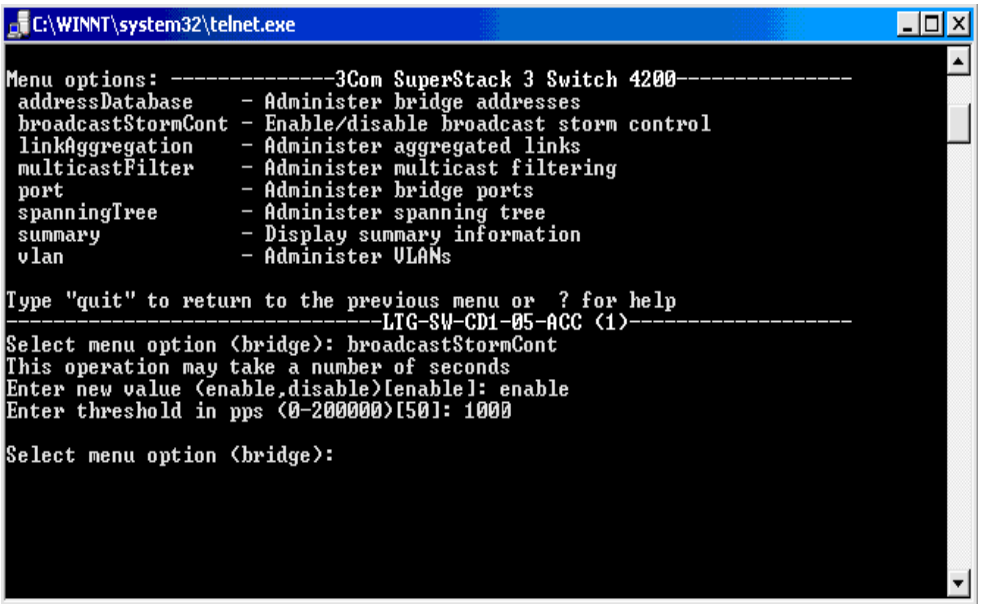


Figura 4.5 Configuración de la opción BroadcastStormCont.

4.3.1.2 Implantación de la primera recomendación en el Centro de Datos 4.

En el centro de datos 4 ubicado en los laboratorios de la facultad de Sistemas e Informática, se encuentra el switch Cisco 3560G el mismo que realiza la función de COR, a este switch se le configuró para que el tráfico de broadcast no supere el 10% del ancho de banda disponible en la Institución.

CENTRO DE DATOS 4		
NOMBRE DEL EQUIPO	**SWITCH**	**# DE PUERTOS**

LTG-SW-CD4-01-COR	Cisco 3560G	24

Tabla 4.2 Información referente al switch del Centro de Datos 4

Para realizar la configuración de este switch se ha tomado referencia de todos los pasos realizados en el Switch del Centro de datos 1. En las páginas 210, 211.

4.3.1.3 Implantación de la primera recomendación en el Centro de Datos 7.

En el centro de datos 7 ubicado en la biblioteca, se encuentra el switch 3Com 4228G el mismo que realiza la función de COR.

CENTRO DE DATOS 7		
NOMBRE DEL EQUIPO	**SWITCH**	**# DE PUERTOS**
LTG-SW-CD7-01-COR	3Com 4228G	24
LTG-HB-CD7-01-ACC	DSH-16 DLINK	16

Tabla 4.3 Información referente a los switch del Centro de Datos 7

En el switch 3Com 4228G se aplicará los pasos que se realizaron en switch 3Com de las páginas 212, 213, 214.

En el hub no es posible realizar ningún cambio ya que este dispositivo no es administrable, y simplemente permite comunicarse a varios equipos a la red.

4.3.1.4 Implantación de la primera recomendación en el Centro de Datos 8.

En el centro de datos 8 ubicado junto al Centro de Producción, se encuentra el switch Cisco 3560G el mismo que realiza la función de COR.

Como en los anteriores switch, en este no se encuentra configurado el control de tráfico de broadcast, es así que se muestra la información del switch en la tabla 4.4

CENTRO DE DATOS 8		
NOMBRE DEL EQUIPO	**SWITCH**	**# DE PUERTOS**
LTG-SW-CD8-01-COR	Cisco 3560G	24

Tabla 4.4 Información referente al switch del Centro de Datos 8.

Para configurar el control de tráfico de broadcast en este switch se realizaron todos los pasos que se indican en las páginas 211, 212.

4.3.1.5 Implantación de la primera recomendación en el Centro de Datos de Servicios.

En el centro de datos de servicios que presta servicios a los laboratorios de Electrónica, se encuentra un switch 3Com

4228G y un Hub DLINK los que realizan la función de COR y acceso respectivamente.

Como en los anteriores switch, en este no se encuentra configurado el BroadcastStormCont.

CENTRO DE DATOS DE SERVICIOS		
NOMBRE DEL EQUIPO	**SWITCH**	**# DE PUERTOS**
LTG-SW-CDS-01-COR	3Com 4228G	24
LTG-HB-CDS-01-ACC	DSH-16 DLINK	36

Tabla 4.5 Información referente al switch y hub del Centro de Datos de Servicios

En el switch 3Com 4228G se aplicará todos los pasos que se ha señalado en las páginas 212, 213, 214.

En la tabla 4.6 se muestra la información de los switches en los que se aplicó la configuración para controlar el tráfico de broadcast, en los diferentes centros de datos de la Escuela Politécnica del Ejército Sede Latacunga.

4.3.1.6 Resultados luego de haber implementado el control del tráfico de broadcast en los switches de los Centros de Datos.

Luego de haber configurado la opción para controlar el tráfico de broadcast, se ha realizado las capturas de tráfico para verificar si se cumple la condición que se habilitó en todos los switchs de los diferentes centros de datos de la Escuela Politécnica del Ejército Sede Latacunga.

Gráficamente se va mostrar como circulaban los paquetes antes de que se habilite la opción BroadcastStormCont, y de la misma forma luego de que se habilitó dicha opción.

En la figura 4.6 se muestra como circulaban los diferentes paquetes por la red, antes de que se realice el control de broadcast, la captura de tráfico realizada en el Switch LTG-SW-CD1-02-ACC, del centro de datos 1.

La línea de color rojo es la que representa el tráfico de broadcast, es evidente que en momentos de la captura había flujos de tráfico de broadcast que llegaban hasta los 90 paquetes por segundo. Como podemos observar en la figura 4.6.

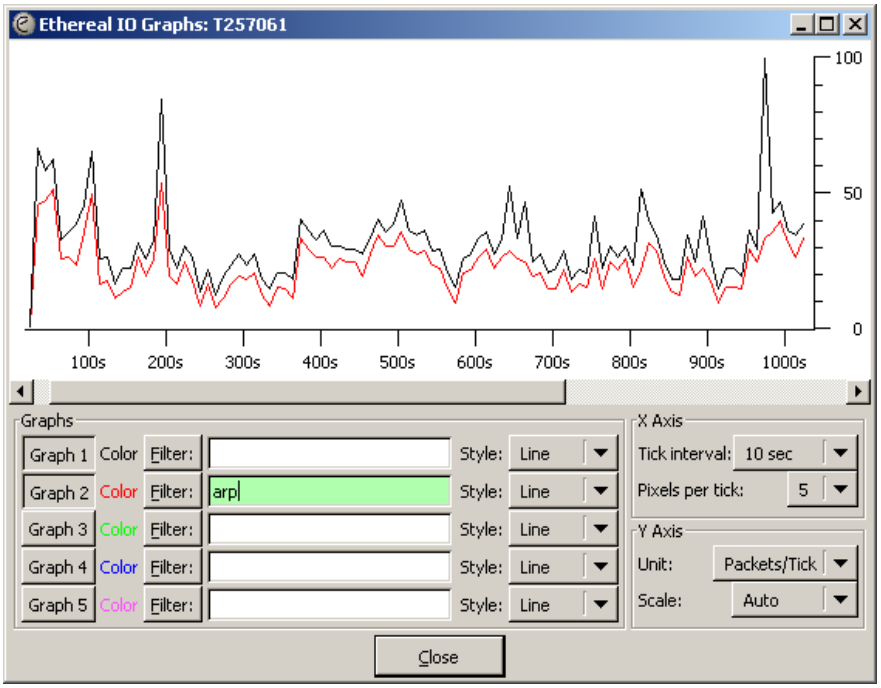


Figura 4.6 Gráfico de la captura de tráfico en el Switch LTG-SW-CD1-02-ACC, antes de implementar la opción BroadcastStormCont.

Fuente: Ethereal.

Luego de haber habilitado la opción BroadcastStormCont en el Switch LTG-SW-CD1-02-ACC, no se podrá ver un cambio importante, ya que como se explicó el valor de control es de 1000 paquetes por segundo, y en las capturas de tráfico que se ha realizado el promedio ha sido hasta 80 paquetes por segundo. Es por esa razón que la gráfica es idéntica a la de la figura 4.6.

En el centro de producción se realizó la captura de tráfico respectiva antes de que se implemente el control de tráfico de broadcast, y los niveles de este tipo de tráfico estaban en un promedio de 30, 40 paquetes por segundo, como podemos observar en la figura 4.7. La línea de color rojo representa al tráfico de broadcast.

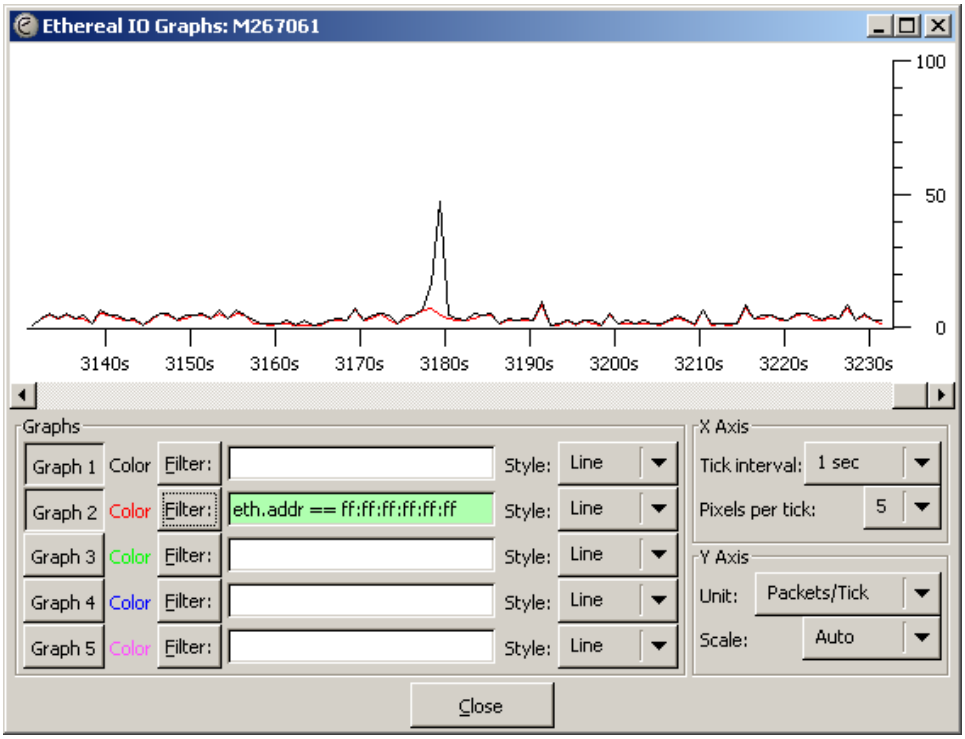


Figura 4.7 Gráfico de la captura de tráfico en el Switch LTG-SW-CD8-01-COR, antes de implementar la opción BroadcastStormCont.

Fuente: Ethereal.

Luego de haber implementado el control de tráfico de broadcast el resultado es el mismo ya que como se explicó el valor que hemos configurado es 1000 paquetes por segundo, y el promedio que existe en las capturas de tráfico es de 30, 40 paquetes por segundo. En la figura 4.8 se puede observar que no existen cambios en lo referente al tráfico de broadcast.

Con el control de tráfico de broadcast se mejora el funcionamiento de la red, ya que estamos administrando de mejor este tipo de tráfico, porque es necesario en la red para una comunicación correcta entre las computadoras que se encuentra conectadas a la

red, así como es necesario el broadcast, también puede causar serios problemas, y no permitir el correcto funcionamiento de la red.

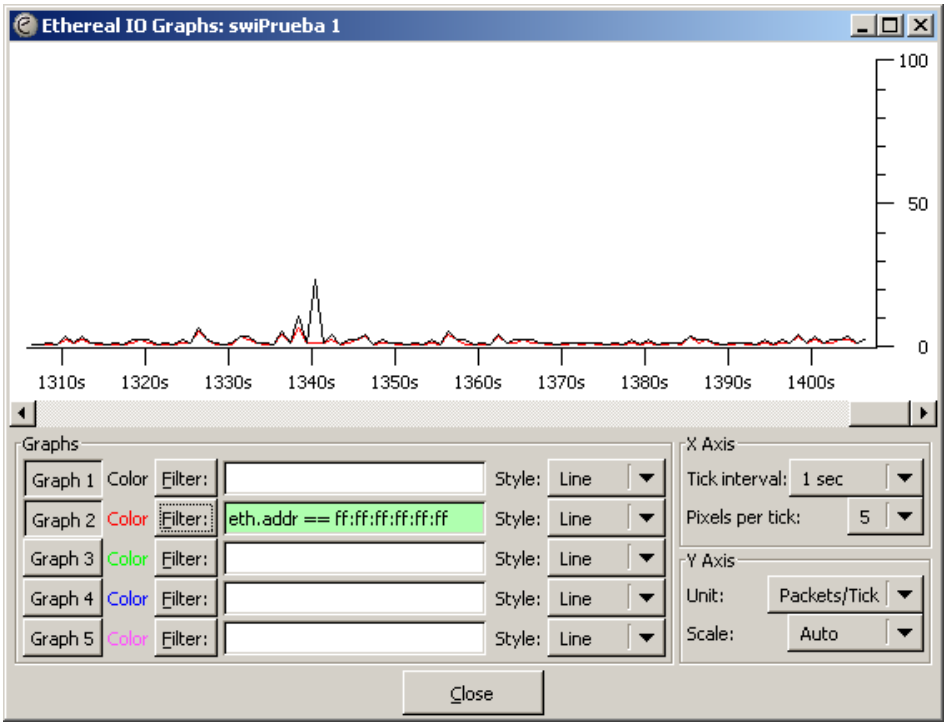


Figura 4.8 Gráfico de la captura de tráfico en el Switch LTG-SW-CD8-01-COR, luego de haber implementado la opción BroadcastStormCont.

Fuente: Ethereal.

Luego de que se ha realizado las respectivas configuraciones en los diferentes switches que dispone la Escuela Politécnica del Ejército Sede Latacunga, para controlar el tráfico de broadcast, se debe mencionar que como se explica previamente, todas las configuraciones realizadas son simplemente para controlar el tráfico de broadcast, y no es para eliminarlo, ya que como se dijo este tipo de tráfico es muy necesario para el buen desenvolvimiento de la red, pero se debe

controlarlo para que con el tiempo no se produzca las denominadas tormentas de broadcast, lo que quitaría la eficiencia de la red.

Implantación de la segunda recomendación.

Durante la fase del análisis del flujo de tráfico de la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, se produjo otra novedad, la presencia en gran cantidad del protocolo STP, esto hizo que se realice el estudio necesario para saber el funcionamiento de dicho protocolo.

Como ya se explicó en el capítulo anterior el Spanning Tree Protocol fue creado para superar automáticamente el problema de caminos múltiples entre los segmentos. Con todos los puentes en la red ejecutando STP, creando un camino redundante, negociarán y sólo uno de ellos se usará para transferir el tráfico. Si el puente activo falla, un puente libre empezará a transferir el tráfico en su lugar. De este modo, se puede emplear un puente redundante para proteger segmentos de la red críticos.

Cuando existe más de un camino de puente entre los segmentos LAN, el STP definirá un puente activo y el resto se pondrá en modo ocioso. El puente activo continúa enviando mensajes STP a la red de puentes STP para indicar que todavía está vivo. Si el puente activo falla, el STP reconfigurará la red automáticamente y activará un puente redundante previamente ocioso para asegurar que los datos continúan fluyendo.

Cada switch en una LAN que usa STP envía un mensaje especial llamado unidades de datos del protocolo puente (Bridge Protocol Data Unit, BPDU) desde todos sus puertos para que los otros switches sepan de su existencia y elijan un puente raíz para la red, Los switches intercambian información (BPDU) cada dos segundos si se detecta alguna anormalidad en algún puerto STP cambiara de estado algún puerto automáticamente utilizando algún camino redundante sin que se pierda conectividad en la red.

En la figura 4.9 podemos observar que mediante Ethereal se determina que en se generan los mensajes BPDU.

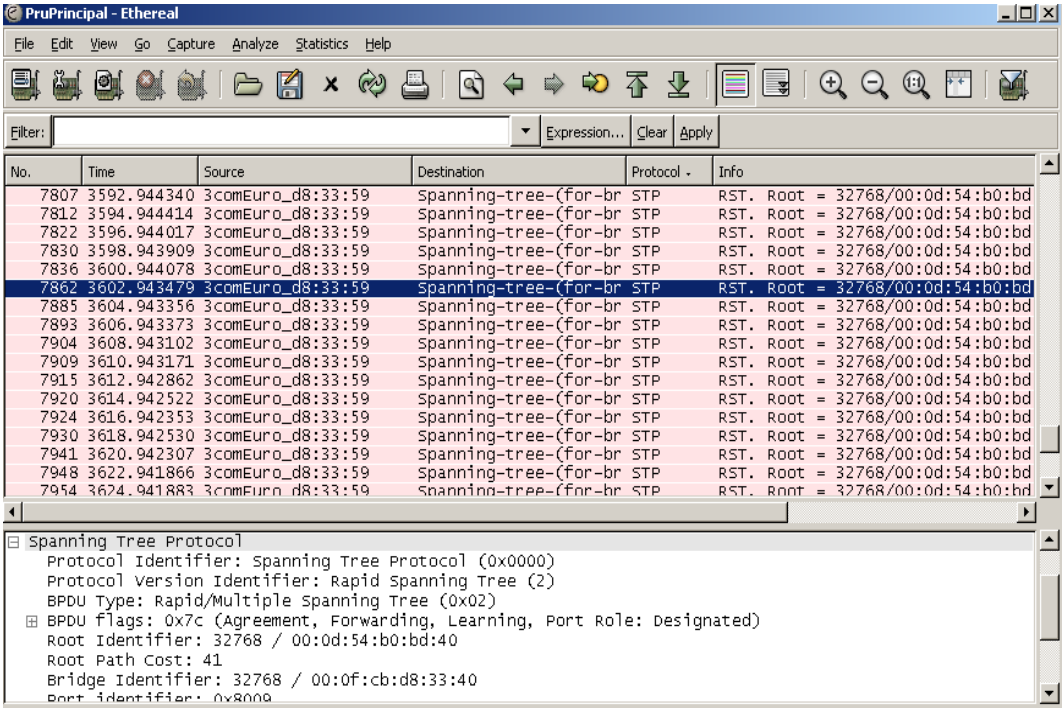


Figura 4.9. Mensajes BPDU del STP.

Fuente: Ethereal.

Cada puerto de un switch que usa protocolo STP se encuentra en uno de los cinco que enumeramos a continuación:

- Bloquear
- Escuchar
- Aprender
- Enviar
- Desactivar

El puerto pasa por estos cinco estados de la forma siguiente:

- De la inicialización al bloqueo
- De bloqueo a escucha o desactivado
- De o escucha a aprendizaje desactivado
- De aprendizaje a envío o desactivado
- De envío a desactivado

En la figura 4.10 podemos observar como fluye el tráfico del protocolo STP, como ya se explicó se genera cada 2 segundos.

Con línea de color rojo se representa al protocolo STP podemos ver que fluye de forma constante, esto ocurre en todas las capturas de tráfico que se han realizado en los diferentes switchs de la Escuela Politécnica del Ejército Sede Latacunga. Ya que luego de conocer el funcionamiento del protocolo STP, podemos determinar que dicho protocolo debe estar siempre habilitado en los diferentes switchs ya que con esto se evitará que se generen caminos redundantes, lo que hará que rápidamente pierda eficiencia la red.

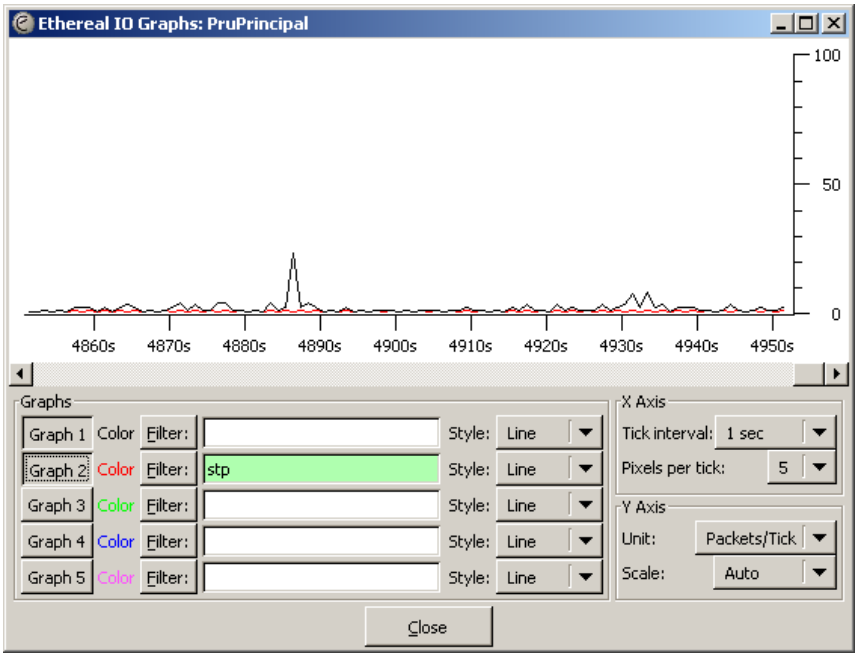


Figura 4.10 Gráfico que representa como fluye en la red el protocolo STP.

4.3.3.- Implantación de la tercera recomendación.

Para optimizar los recursos de red hemos visto que es conveniente realizar ciertos cambios en la configuración del servidor de antivirus, ya que como se ha determinado en el capítulo anterior el antivirus está generando paquetes innecesarios, por ende consumen recursos que podrían servir para otras aplicaciones de la red.

A continuación vamos a seguir los siguientes pasos para configurar el servidor de Antivirus, de esta forma se optimizará el servicio de red.

- Debemos ingresar al Kaspersky Administration Kit que se encuentra en Menu Inicio → Programas.

En la figura 4.11 se muestra donde se debe ingresar para obtener la información del antivirus.

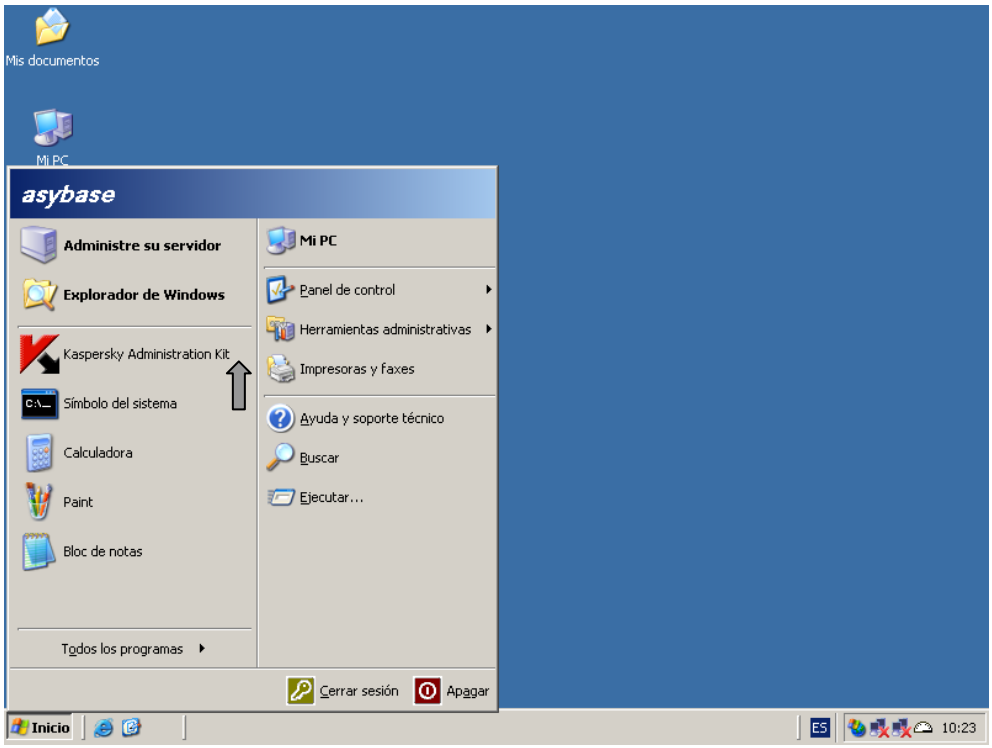


Figura 4.11. Ingreso al Kaspersky Administration Kit.

- Al momento que ingresamos a dicha opción nos aparecerá una pantalla como la que se muestra en la figura 4.12.

Figura 4.12. Interfaz gráfica del Kaspersky Administration Kit.

- Luego damos clic derecho en la opción Administration Server y elegimos la opción propiedades. Esto lo podemos visualizar en la figura 4.13.

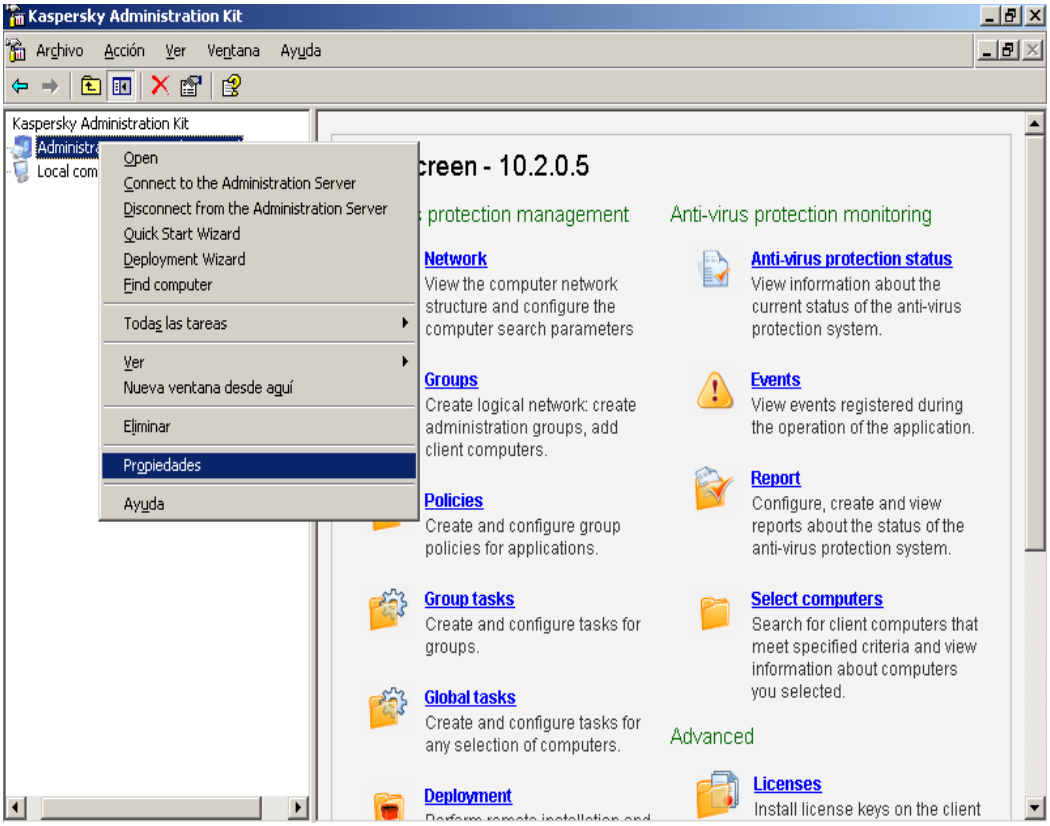


Figura 4.13 Interfaz gráfica del Kaspersky Administration Kit.

- Luego de haber dado clic en propiedades nos aparecerá una ventana, la misma que podemos visualizar en la figura 4.14. En esta ventana tenemos varias viñetas, debemos seleccionar Setting.

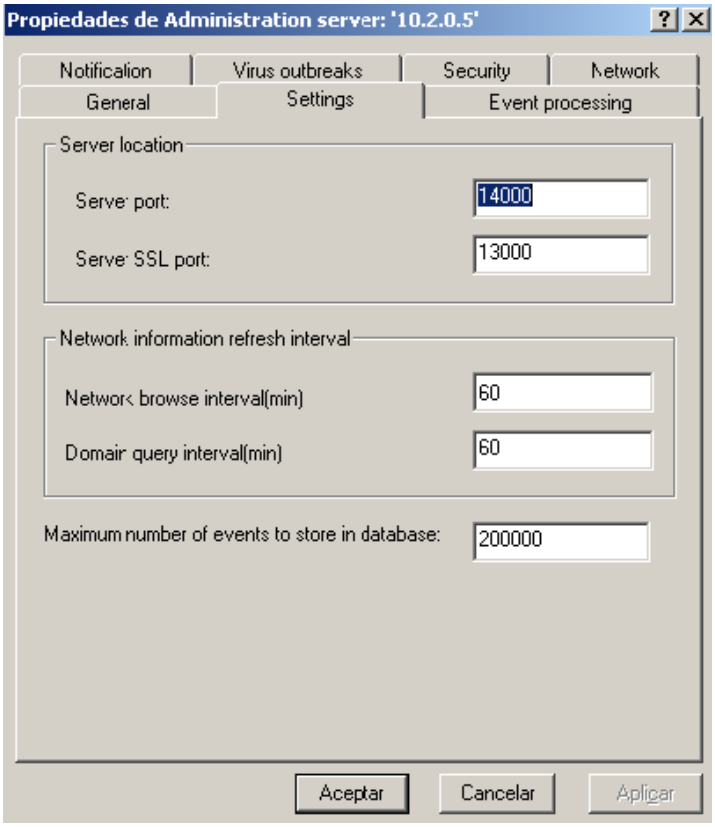


Figura 4.14 Ventana de propiedades del Kaspersky Administration Kit.

En esta ventana debemos asignar los siguientes valores:

1. En la opción Network Information refresh interval.

   - Network browser interval (min)

   60

2. El valor de esta opción viene por defecto en 60, es por eso que no se lo ah modificado.

   - Domain query interval (min)

   60

3. El valor de 60 lo hemos dado para que el antivirus busque computadoras en los dominios que tiene el servidor de antivirus en un intervalo de 1 hora, de esta forma se podrá mejorar el funcionamiento del antivirus, ya que antes esta opción se la realizaba cada 5 minutos.

- Maximum number of events to store in database | 200000 |

Esta opción permite que se guarde 200000 eventos en la base de datos que dispone el antivirus, un evento es cuando el antivirus detecta un virus, esta información forma parte de los 200000 eventos que se ha mencionado.

Adicionalmente debemos habilitar ciertos valores en la opción task, ingresamos al Kaspersky Administration Kit.

En lado izquierdo de la pantalla nos presenta varias opciones en la que nos aparece Tasks, la que se encuentra señalada en la figura 4.15. Al dar un clic en la opción Tasks nos aparece una ventana en la que muestra todas las tareas que manda a ejecutar el antivirus en las estaciones de trabajo que dispone la Institución.

- Damos un clic derecho en la opción Update Workstation que se encuentra en la parte derecha de la figura 4.15.

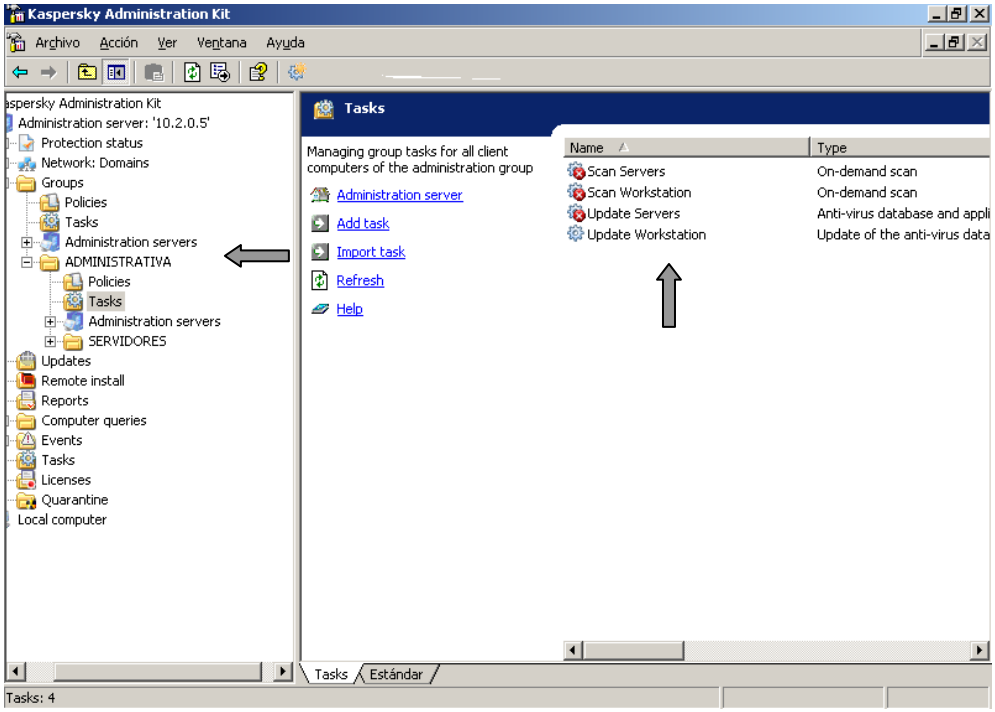


Figura 4.15. Ventana principal de la opción Tasks.

- Nos aparecerá una ventana, como la que podemos visualizar en la figura 4.16.

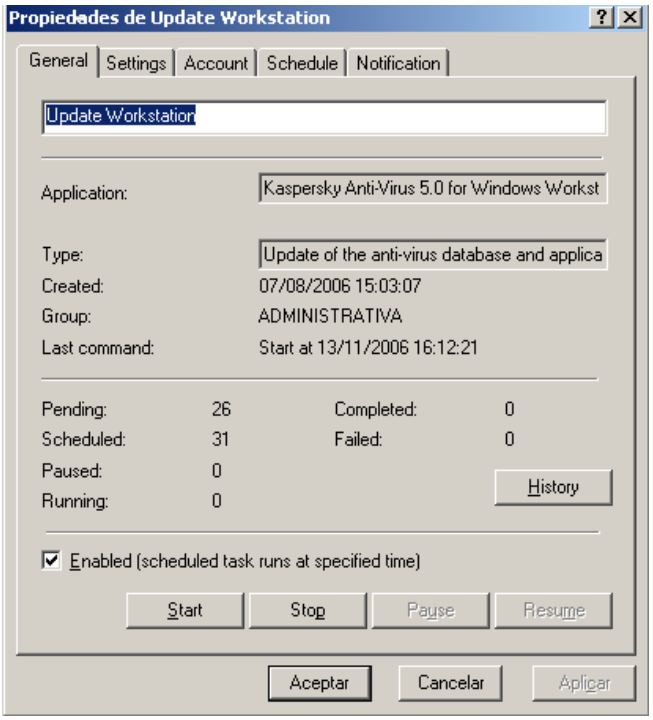


Figura 4.16. Ventana de propiedades de la opción Tasks.

- Se debe seleccionar la Viñeta Schedule, en esta opción se despliega la información y las configuraciones de los momentos en que la tarea se va ejecutar en las diferentes estaciones de trabajo. En la figura 4.17 se puede ver la ventana de la viñeta Schedule.

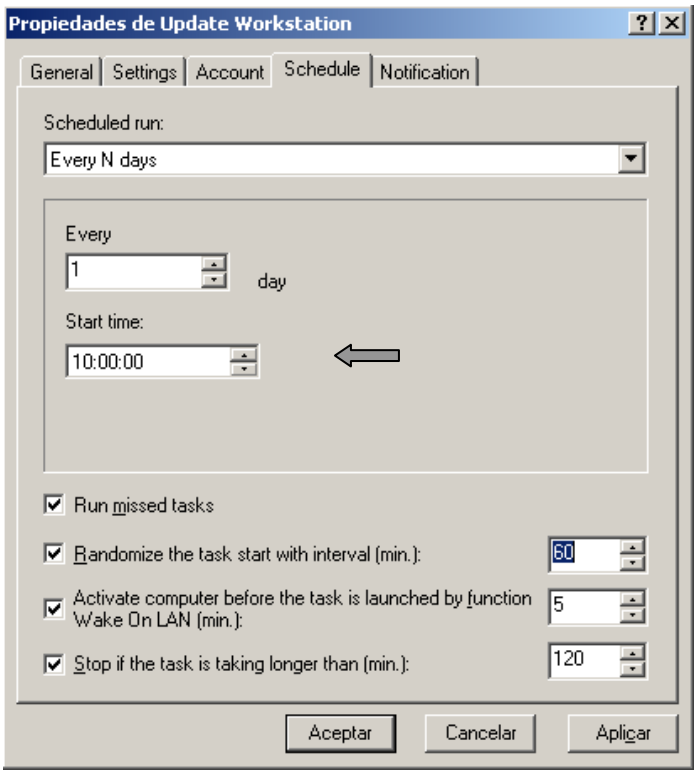


Figura 4.17. Ventana de propiedades de la opción Tasks.

- Por defecto están habilitadas las opciones Run missed tasks y Randomize the task star witch interval (min) con el valor de 60.

- Se ha visto que es necesario habilitar la opción Activate computer befote the task is lauched by function Wake On L[5]n) con esta opción se condiciona a que si la estación en la que se va a realizar

la tarea no está prendida 5 minutos antes de que se ejecute la tarea, no se ejecutará la tarea.

- También se debe configurar la opción Stop if the task is taking longer than (r 120 al momento de que se ingresa el valor de 120 minutos, se dice que si la tarea que se ejecuta se pasa los 120 minutos se de va detener y queda para ejecutarse el siguiente día, ya que esta tarea se realiza todos los días a las 10 am, esto lo podemos visualizar en la figura 4.17.

  Adicional a los pasos que se detallaron, al administrador del antivirus debe tomar en cuenta ciertas recomendaciones, lo cuál permitirá un funcionamiento óptimo del antivirus, y al mismo tiempo obtener un mejor funcionamiento de la red.

  El administrador del antivirus debe revisar constantemente que estén habilitadas en el servidor de antivirus únicamente las computadoras que se encuentran conectadas a la red, ya que si alguna computadora no esta trabajando en el entorno de red y el servidor envía a realizar una tarea, nunca va poder encontrarle a dicha computadora para realizar la tarea que ha sido ejecutada, y se generará tráfico innecesario, lo cuál conlleva a que la red pierda eficiencia porque se están desperdiciando los recursos que pueden ser utilizados por otras aplicaciones que se encuentran en la red.

  En el servidor de antivirus se encuentran varios dominios como son Académico, Biblioteca, Clase ESPE, MSHOME, WORKGOUP, los mismos que se pueden observar en la figura 4.18.

  En estos dominios se encuentra las computadoras que al momento de realizar una tarea el servidor ejecuta una búsqueda, las encuentran pero no se encuentran sincronizadas con el servidor, esto puede ser

por varias razones como por ejemplo que en la computadora no se encuentra instalado el antivirus, la computadora tiene el sistema operativo Windows 95 o Windows 98, ya que en estos sistemas no es posible instalar el antivirus Kaspersky, cuando pasa esto las computadoras que detectó el servidor se ponen de un color gris, como lo podemos observar en la figura 4.18.

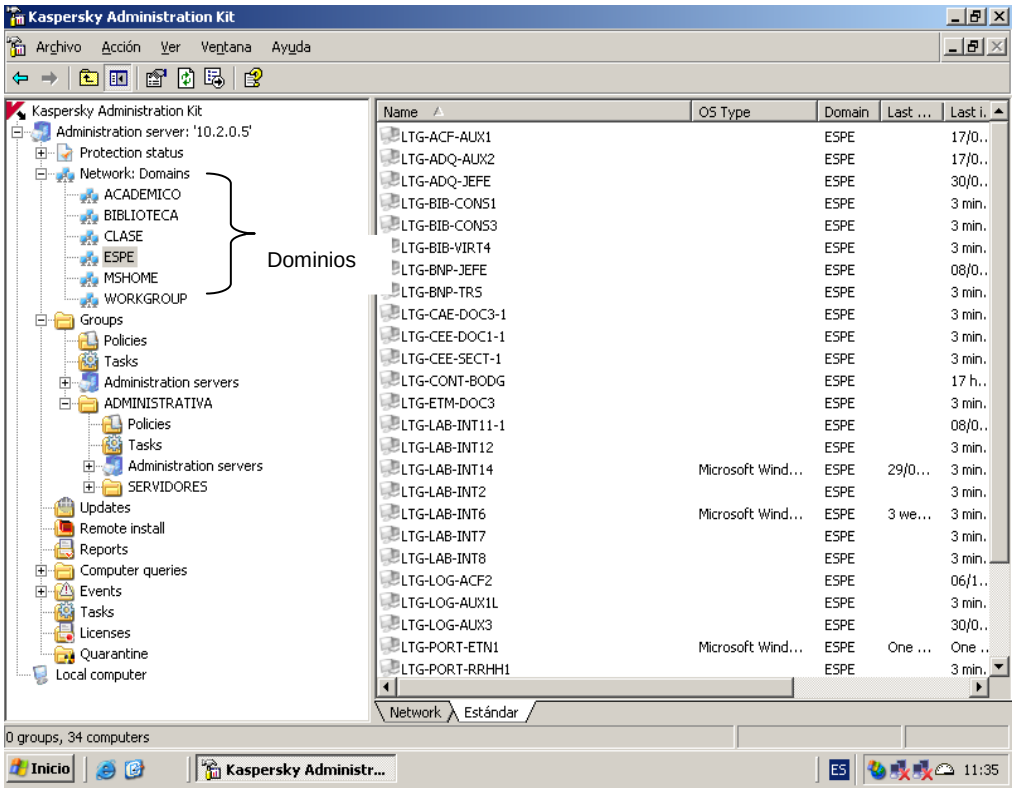


Figura 4.18. Dominios del Kaspersky Administration Kit.

En la figura 4.18, todas las computadoras que se ven de color gris se encontraron en el dominio ESPE, estas computadoras estaban con nombres que no tenían nada que ver con el Área Administrativa, es por eso que se procedió a borrarlas, ya que estás computadoras eran las que originaban el tráfico del protocolo NBNS, esto lo podemos visualizar en la figura 4.19.

Adicional a esto, se debe mencionar que se encontró varias computadoras que ya no existen en la red, pero que en algún momento el servidor de antivirus las detectó, y es por eso que está constantemente buscando.

Para complementar lo anterior, en el DHCP se procedió a eliminar las diferentes computadoras que se encontraban registradas con nombres anteriores que no tienen nada que ver con la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, es decir que una computadora se encontraba registrada con 2 nombres.

De esta forma se logró que se eliminen las computadoras que buscaba el servidor de antivirus, y que estaba generando el tráfico innecesario en la red.

4.3.3.1 Resultados de las capturas de tráfico en el Área Administrativa antes de implantar los cambios en el servidor de antivirus Kaspersky.

Como se explicó durante el análisis, que se generaba gran cantidad de tráfico del protocolo NBNS, es así que de una captura de tráfico realizada en el switch LTG-SW-CD1-01-COR, de un total de 10697 paquetes, 2150 pertenecían al mencionado protocolo, lo cuál hacía que se desperdicien los recursos de red.

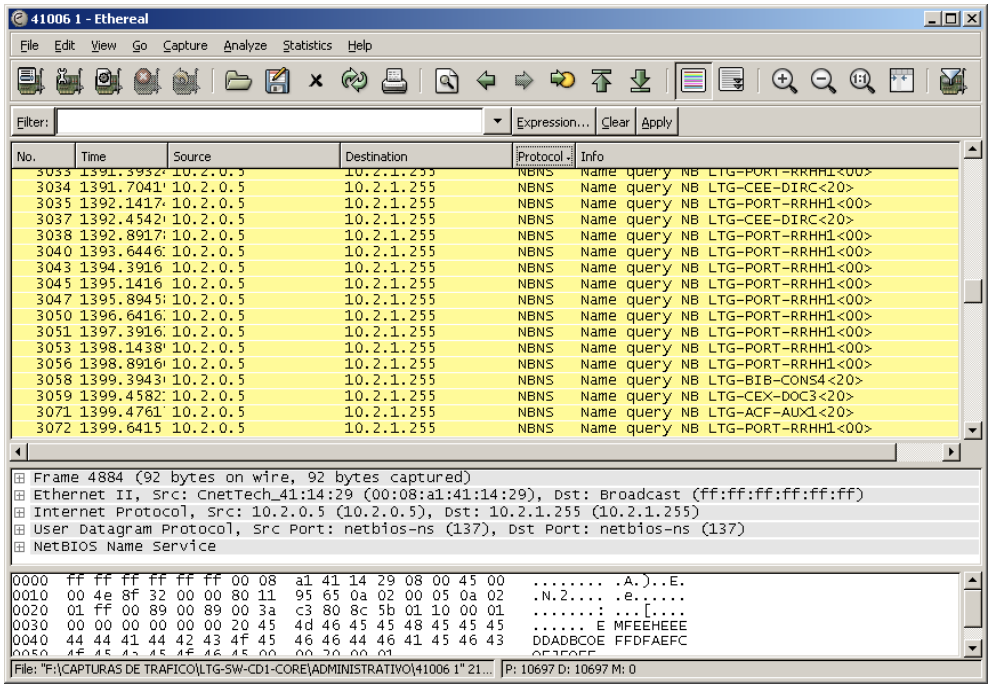


Figura 4.19. Captura de tráfico realizada en el Switch LTG-SW-CD1-01-COR, antes de realizar los correctivos en el servidor de antivirus Kaspersky.

Como ya se explicó anteriormente en el dominio ESPE se encontró varias computadoras que debían estar en el grupo Administrativa, por lo que se procedió a cambiarlas, para que cuando el servidor de antivirus ejecuta una tarea que esta programada, no exista problema alguno y si las computadoras se encuentran listas se ejecutará las respectivas tareas.

Adicional a esto, se debe tomar en cuenta que existen computadoras que ya no existen en la red, pero que en algún momento el servidor de antivirus las detectó, y es por eso que está constantemente buscando, para esto se debe comprobar que en realidad ya no existen las computadoras y proceder a eliminarlas en el servidor de antivirus, de esta forma se está optimiza el antivirus y la red, ya que el servidor no volverá a buscar a las computadoras, lo cuál hará que no se genere tráfico innecesario.

Para mostrar de mejor forma donde deben estar las computadoras al momento que el antivirus ejecute las tareas correspondientes, y de esta forma no generen problema alguno al buen desenvolvimiento de la red podemos observar la figura 4.20.

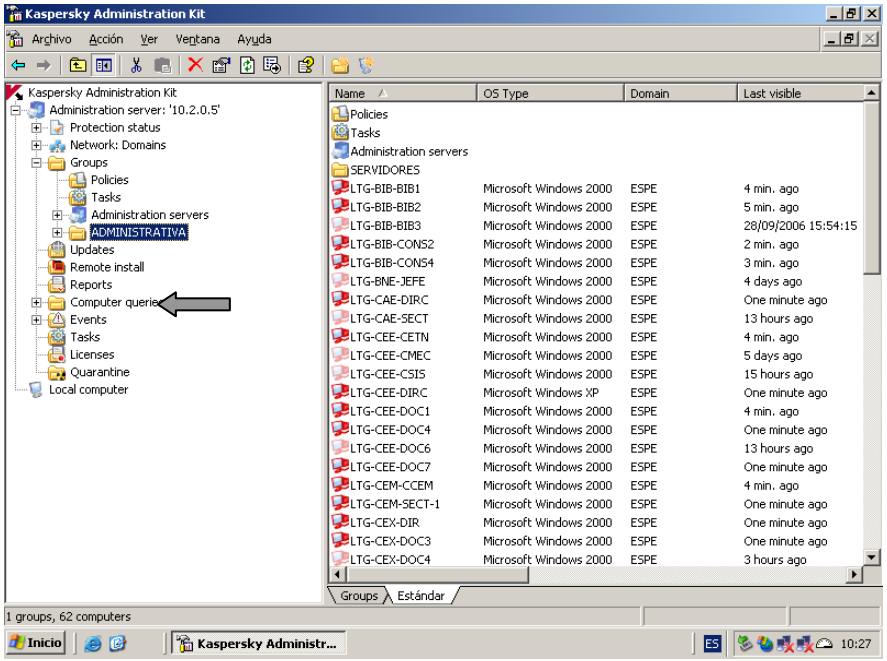


Figura 4.20. Área Administrativa donde se ejecutan las tareas del Antivirus.

4.3.3.2 Resultados de las capturas de tráfico en el Área Administrativa después de implantar los cambios en el servidor de antivirus Kaspersky.

Luego de que se realizaron los cambios, se capturó el tráfico y se obtuvo los resultados esperados, se disminuyo casi en su totalidad la presencia del protocolo NBNS, es así que en un 98% se elimino este tráfico innecesario, el 2% restante corresponde a las computadoras que están con sistema operativo Windows 95 y 98, es por esa razón que existe en poca cantidad el protocolo NBNS. En la figura 4.21 se puede observar lo antes mencionado.

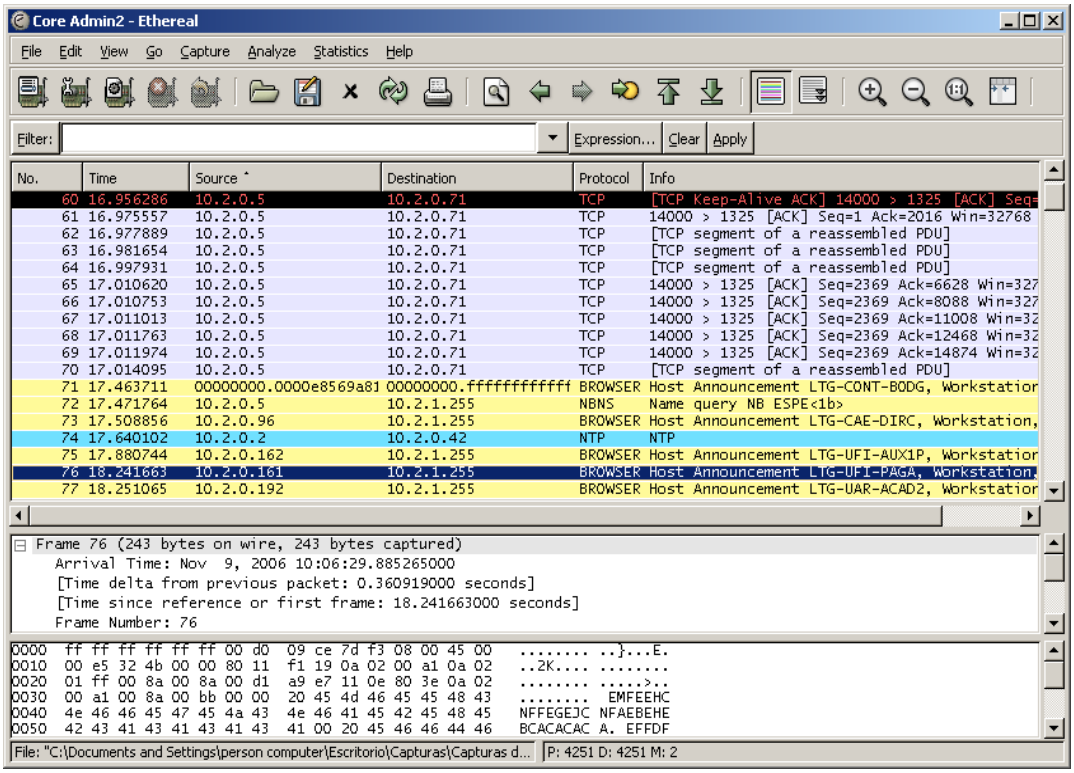


Figura 4.21. Captura de tráfico realizada en el Switch LTG-SW-CD1-01-COR, luego de realizar los correctivos en el servidor de antivirus Kaspersky.

Fuente: Ethereal.

4.3.3.3 Resultados de las capturas de tráfico en el Área Académica antes de implantar los cambios en el servidor de antivirus Kaspersky.

En la figura 4.22, se muestra como circulaba el tráfico antes de que se realice las implementaciones necesarias, para obtener un correcto funcionamiento del antivirus y se optimice el servicio de red.

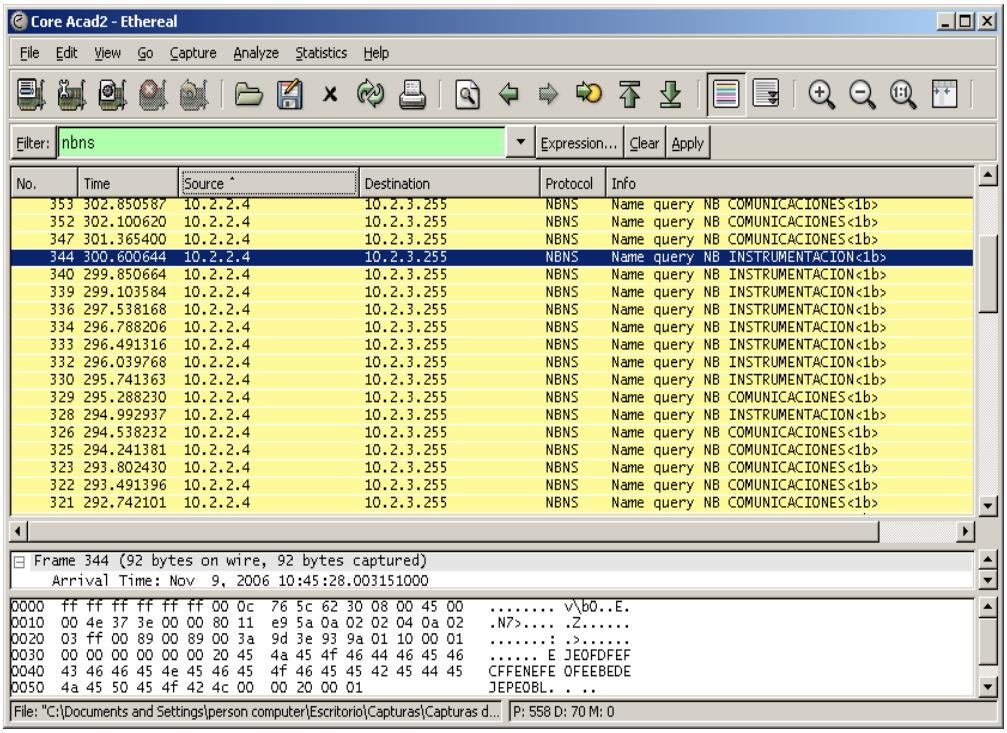


Figura 4.22. Captura de tráfico realizada en el Área Académica, antes de realizar los correctivos en el servidor de antivirus Kaspersky.

Fuente: Ethereal.

Hay tomar en consideración que todos los cambios que se realizaron en el Área Administrativa para el buen funcionamiento del antivirus y por ende optimizar la red, se han ejecutado de igual forma el Área Académica paso a paso todo lo que se mencionó anteriormente.

4.3.3.4 Resultados de las capturas de tráfico en el Área Académica después de implantar los cambios en el servidor de antivirus Kaspersky.

Luego de que se realizaron los diferentes cambios, que se describieron anteriormente, se logró eliminar la gran cantidad de tráfico del protocolo NBNS, esto ayuda a que se optimice el ancho de banda de la red.

Para visualizar de mejor forma lo descrito anteriormente podemos observar la figura 4.23.

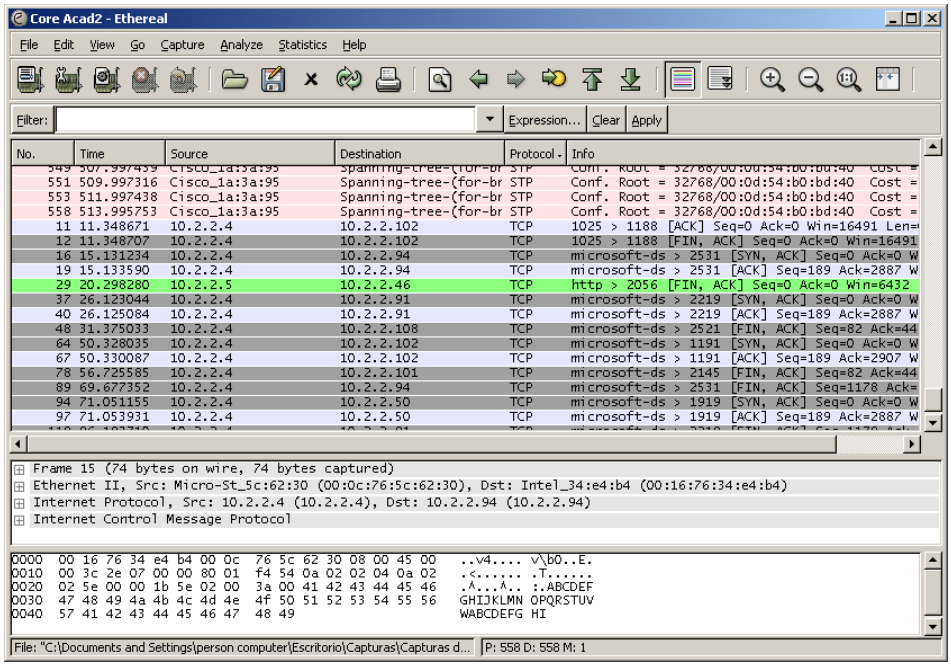


Figura 4.23. Captura de tráfico realizada en el Área Académica, después de realizar los correctivos en el servidor de antivirus Kaspersky.

Fuente: Ethereal.

4.3.4 Implantación de la cuarta recomendación.

La cuarta recomendación debe ser implantada por las personas encargadas de dotar las computadoras a la Escuela Politécnica del Ejército Sede Latacunga.

Conjuntamente con las personas que trabajan en el Unidad de Tecnologías de la información y Comunicación, deben ver las mejores características para poder realizar los tramites

necesarios para adquirir nuevas computadoras para todos los usuarios que no disponen de dichos equipos.

4.3.5 Conclusiones luego de haber implantado las recomendaciones para optimizar el servicio de red.

Luego de haber realizado todos los correctivos, tanto en el Área Administrativa como en el Área Académica, en general se obtuvo buenos resultados.

Referente al tráfico de broadcast, como se explicó, no se puede eliminar ya que es muy necesario para el buen funcionamiento de la red. Lo que se realizó es administrar los switches de los diferentes centros de datos de la Escuela Politécnica del Ejército Sede Latacunga, de esta forma se logró reservar un espacio para el broadcast del total del ancho de banda.
Para los switches 3Com se utilizó la opción BroadcastStormCont, y para los switches Cisco el strom-control Broadcast. Todos estos cambios se visualizan en la tabla 4.6.

Principalmente lo que se ha logrado es el ahorro de los recursos de red, es así que anteriormente el protocolo NBNS en una captura de tráfico de un total de 5005 paquetes, 1890 pertenecían al protocolo NBNS, por lo que ocupaban el 0.001% del total del ancho de banda. Luego de que se realizó los cambios en el servidor de antivirus, que era desde donde se generaba este tráfico, se logró reducir casi en su totalidad, es así que en una captura de tráfico realizada de un total de 4538 paquetes capturados 163 pertenecen al NBNS.
De esta forma hemos optimizado el servicio de red, reduciendo el tráfico innecesario.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1.- CONCLUSIONES

1. Como conclusión principal luego de haber finalizado el presente trabajo de investigación tenemos que la red Lan de la Escuela Politécnica del Ejército Sede Latacunga, en forma general se encuentra en buen estado, ya que luego de haber realizado el respectivo análisis, no se encontró novedades que en realidad afecten el buen desempeño de la red.

2. Realizar el monitoreo de la red Lan ha sido de mucha importancia, ya que se ha llegado a determinar los diferentes paquetes que circulan diariamente por la red y se ha determinado que aplicaciones son las que generan dichos paquetes, lo que nos ha permitido determinar con exactitud donde se generan los problemas.

3. El uso de una metodología en nuestro caso la Metodología MIRA, ha sido de mucha ayuda para realizar el Análisis de Flujo de Tráfico de una forma ordenada, de esta forma se obtuvieron resultados reales y precisos, lo que nos permitió determinar los problemas que existía en la red, y por ende se dio pautas para solucionar dichos problemas.
4. Luego de haber finalizado con el Análisis de Flujo de Tráfico de la Red Lan, se determinó que había gran cantidad de tráfico de

broadcast, lo que nos llevó a realizar estudios sobre este tipo de tráfico, y se determinó que este tipo de tráfico es útil para la red, ya que gracias al broadcast se pueden comunicar las diferentes estaciones de trabajo que se encuentran en un entorno de red, pero hay veces que se producen las llamadas tormentas de broadcast lo que originarían ineficiencia en la red, para esto se han realizado configuraciones en los diferentes switch que dispone la Escuela Politécnica del Ejército Sede Latacunga, lo que permitirá controlar el tráfico de broadcast si alguna vez llegara a ocurrir un problema mayor.

5. El servidor de antivirus provocaba que se generen paquetes innecesarios que circulaban en la red, lo cuál hacia que se consuman los recursos que podían ser utilizados de mejor forma por otras aplicaciones, para solucionar dicho inconveniente, se realizaron ciertos cambios en la configuración del servidor, lo que permitió que se mejore el funcionamiento del antivirus y por ende de la red.

6. Las diferentes aplicaciones que dispone la Escuela Politécnica del Ejército Sede Latacunga que trabajan en red, no generan problemas al buen desenvolvimiento de la red, ya que se realizó análisis que nos permitió llegar a esta conclusión.

7. La implementación de las VLAN’s en un proyecto anterior, ayudado a que se distribuyan de mejor forma las diferentes estaciones de trabajo en los puertos físicos de un switch, lo cuál permite que la estación de trabajo tenga una ruta determinada para llegar a su destino.

5.2.- RECOMENDACIONES

1. Luego de realizar el presente trabajo de investigación se recomienda que, el administrador de la red LAN debe realizar por lo menos 1 vez a la semana, un monitoreo de las diferentes actividades que se realizan en la red, de esta forma se podrá determinar si se esta generando alguna novedad, y de acuerdo a esto dar solución para tener un óptimo funcionamiento de la red.

2. Se recomienda la adquisición del Software Ethereal, ya que para realizar este trabajo de investigación se ha utilizado dicho software y los resultados que se obtuvieron han sido los esperados, a pesar que la versión que se utilizó era de distribución gratuita.

3. Se recomienda también al administrador del antivirus, realizar un chequeo continuo al servidor, siguiendo las pautas que se han establecido en este trabajo, de esta forma se obtendrá un funcionamiento óptimo tanto del antivirus como de la red.

4. Es necesario dotar de computadoras de última generación, a todas las personas que laboran en la institución, ya que como se explicó anteriormente hay veces que surgen problemas en las computadoras que son muy antiguas y el problema no está no precisamente en la red.

5. Se debe reemplazar los hubs que se encuentran en los centros de datos por switches, ya que los hubs no se pueden administrar y simplemente sirven para conectar diferentes estaciones de trabajo.

5.3.- GLOSARIO DE TÉRMINOS

Ancho de Banda

El ancho de banda es la cantidad de información que puede fluir a través de una conexión de red en un período de tiempo.

Broadcast

Broadcast es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Capa de Enlace

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Capa de red

La capa de red debe hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sea necesario, para hacer llegar los datos al destino.

Dirección IP

Dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz, dentro de una red que utilice el protocolo IP.

Ethereal

Ethereal es una herramienta muy útil para analizar las comunicaciones, tanto a nivel de conexión como a nivel del tráfico que se intercambia. Proporciona información muy útil a la hora de entender los protocolos, pudiendo incluso detallar con mucha precisión algunos protocolos que reconoce, como el de DNS, TCP, UDP, HTTP, y muchos otros más.

Fast Ethernet

Fast Ethernet es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps. En su momento el prefijo fast se le agregó para diferenciarlas de la Ethernet regular de 10 Mbps. Fast Ethernet no es hoy por hoy la más rápida de las versiones de Ethernet.

Flujo de Tráfico

El Flujo de Tráfico es como están circulando los diferentes paquetes que pasan por la red.

Gigabit Ethernet

Gigabit Ethernet, también conocida como GigE, es una ampliación del estándar Ethernet, que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet.

Hub

Hub o concentrador es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs están dejando de ser utilizados, debido al gran nivel de colisiones y tráfico de red que propician.

Paquetes

Paquete es cada uno de los bloques en que se divide, en el nivel de Red, la información a enviar. Los paquetes pueden estar formados por una cabecera, una parte de datos y una cola. En la cabecera estarán los campos que pueda necesitar el protocolo de nivel de red, en la cola, si la hubiere, se ubica normalmente algún mecanismo de comprobación de errores.

Protocolo de Comunicación

Protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de mensajes durante la comunicación entre las entidades que forman parte de una red.

Red Lan

LAN es la abreviatura de Local Area Network (Red de Área Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, iInstituciónes educativas, fábricas, para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

STP

El Spanning Tree Protocol es un protocolo de red de la capa 2 del modelo OSI, gestiona enlaces redundantes previniendo bucles infinitos de repetición de datos en redes que presenten configuración redundante.

Switch

Un switch o conmutador, es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 del modelo OSI. Un switch interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

TCP

El Protocolo de Control de Transmisión, garantiza que los datos sean entregados en su destino sin errores y en el mismo orden en que se transmitieron.

UDP

User Datagram Protocol es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

5.4 BIBLIOGRAFÍA

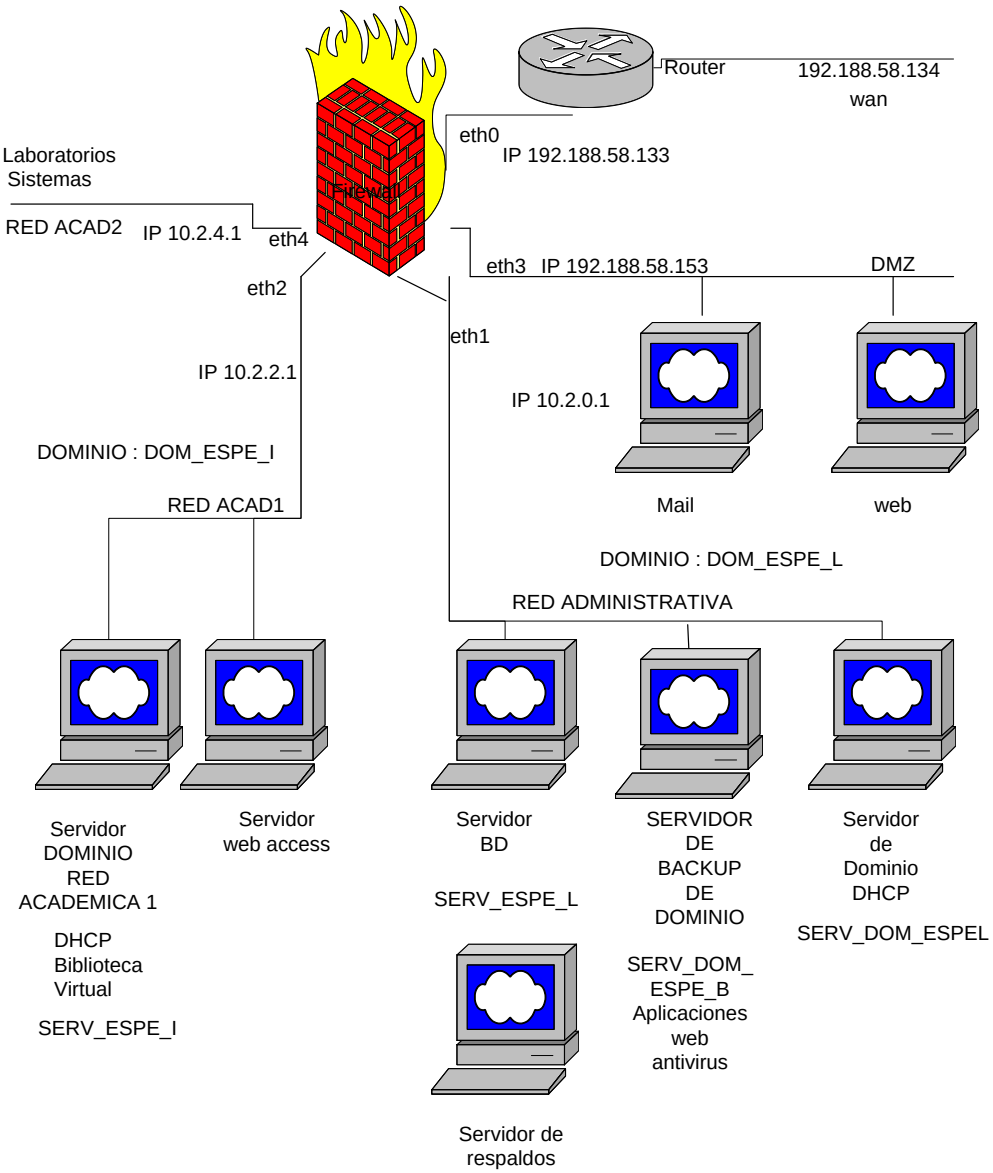
- Fundamentos de Redes, Bruce A. Hallberg, 2003

5.5 WEBGRAFÍA

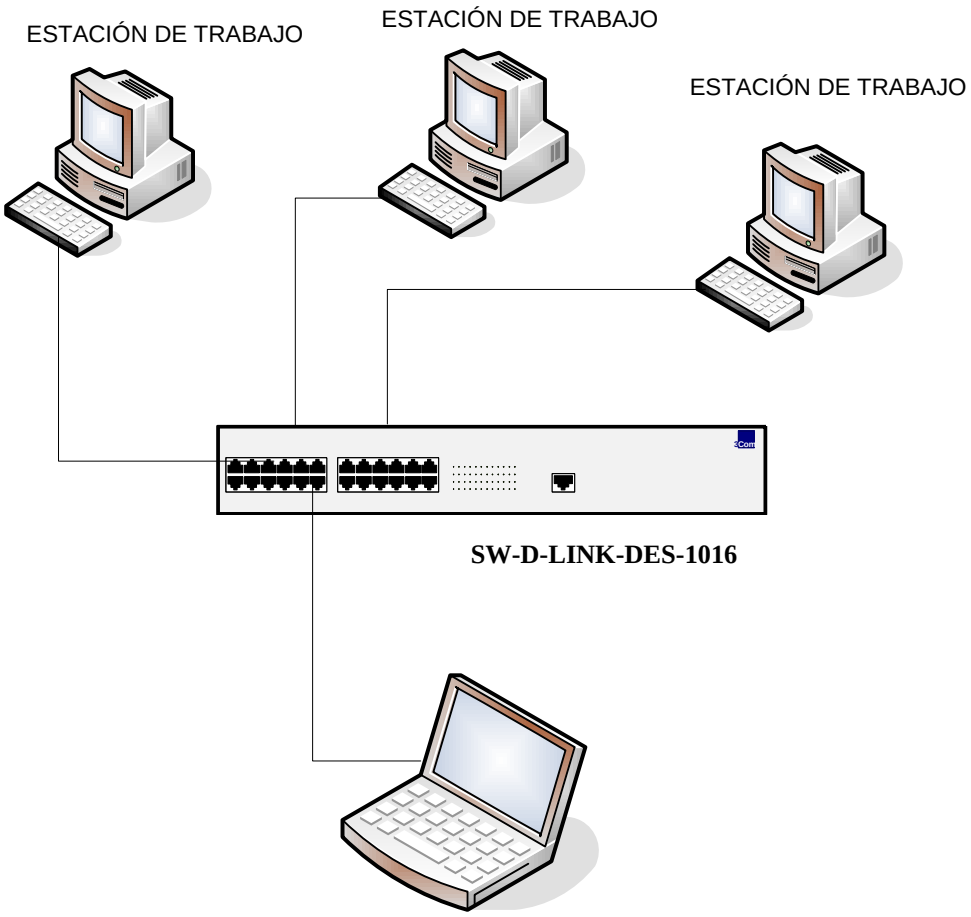
- http://www.google.com
- http://www.abcdatos.com/redlan.html
- http://www.3com.com
- http://www.ethereal.com
- http://www.archivospc.com/programas/categorias/Análisisdetrafico.php
- http://neo.lcc.uma.es/evirtual/cdd/tutorial/sesion/Especif.html

- http://www.monografias.com/redesdedatos.html
- http://fferrer.dsic.upv.es/cursos/Integracion/html/ch04s02.html
- http://www.netjernetworks.com/hardware/consultoria.html
- http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a008031ff7e.html
- http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a00801f0a3d.html
- http://www.trucoswindows.net
- http://www.insecure.org/nmap/
- http://www.rincondelvago.com
- http://es.wikipedia.org/wiki/Imagen:Bandwidth_blue.png
- http://es.wikipedia.org/wiki/User_Datagram_Protocol
- http://es.wikipedia.org/wiki/Spanning_Tree
- http://www.rediris.es
- http://www.kaspersky.com
- http://www.cs.virginia.edu/redesdebroadcast.html
- http://www.saulo.net

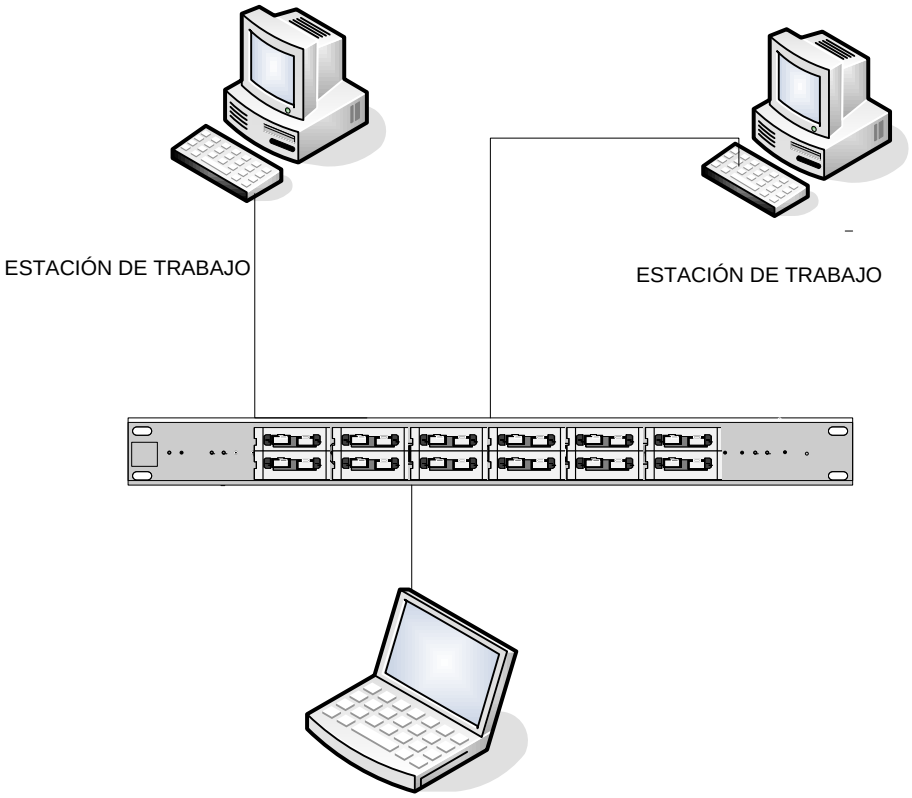
ANEXOS


Router
192.188.58.134
wan
eth0
IP 192.188.58.133
Laboratorios
Sistemas
RED ACAD2
IP 10.2.4.1
eth4
Firewall
eth3
IP 192.188.58.153
DMZ
eth2
eth1
IP 10.2.2.1
IP 10.2.0.1
DOMINIO : DOM_ESPE_I
RED ACAD1
Mail
web
DOMINIO : DOM_ESPE_L
RED ADMINISTRATIVA
Servidor
DOMINIO
RED
ACADEMICA 1
DHCP
Biblioteca
Virtual
SERV_ESPE_I
Servidor
web access
Servidor
BD
SERV_ESPE_L
SERVIDOR
DE
BACKUP
DE
DOMINIO
SERV_DOM_
ESPE_B
Aplicaciones
web
antivirus
Servidor
de
Dominio
DHCP
SERV_DOM_ESPEL
Servidor de
respaldos

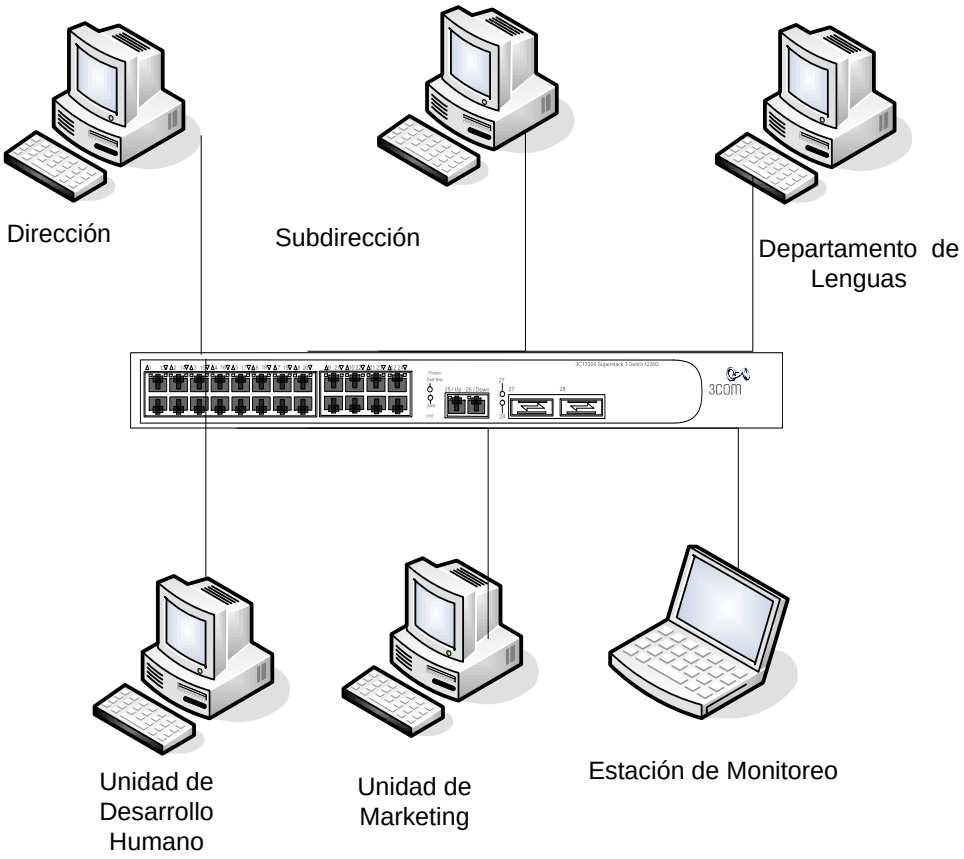
ESQUEMA GRÁFICO DE LA CAPTURA DE TRÁFICO REALIZADA EN EL SWITCH SW-D-LINK-DES-1016



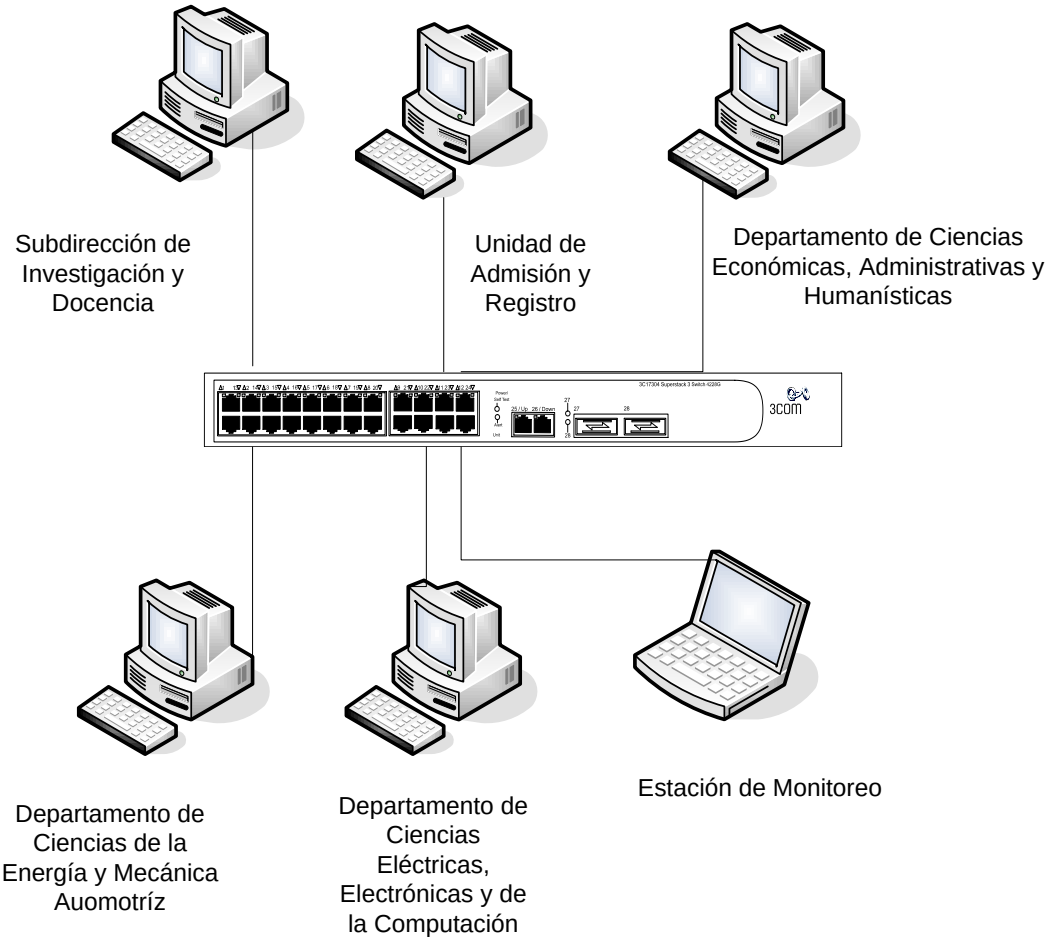
ESQUEMA GRÁFICO DE LA CAPTURA DE TRÁFICO REALIZADA EN EL SWITCH LTG-SW-CD8-01-COR



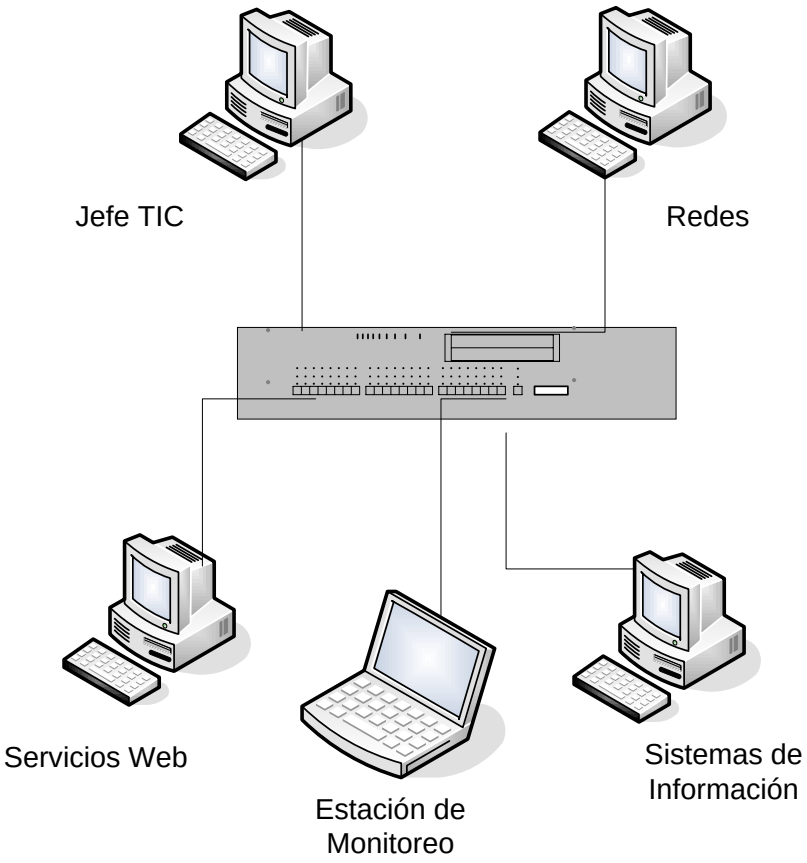
ESQUEMA GRÁFICO DE LA CAPTURA DE TRÁFICO REALIZADA EN EL SWITCH 3COM LTG-SW-CD1-02-ACC



ESQUEMA GRÁFICO DE LA CAPTURA DE TRÁFICO REALIZADA EN EL SWITCH 3COM LTG-SW-CD1-04-ACC



ESQUEMA GRÁFICO DE LA CAPTURA DE TRÁFICO REALIZADA EN EL SWITCH HP 2524 PROCURVE LTG-SW-CD1-05-ACC



ESQUEMA GRÁFICO DE LA CAPTURA DE TRÁFICO REALIZADA EN EL HUB LTG-HB-CD7-01-ACC