ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACIÓN

ANALIZADOR DE TRÁFICO DE RED

TESINA DE SEMINARIO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

INGENIERÍA EN TELEMÁTICA

AUTORES

BARAHONA DELGADO ERICKA MARTHA

GELLIBERT LÓPEZ PAOLA FERNANDA

AÑO

2011

AGRADECIMIENTO

A nuestro director Ing. Ignacio Marín García
que nos guió en el proceso para
culminar nuestra tesis.

Al Ing. Carlos Desiderio por ayudarnos
con el acceso a una red real para
realizar las capturas requeridas.

A Washington y Mauro por su ayuda
incondicional, su apoyo fue
fundamental para el desarrollo
de nuestra tesis.

DEDICATORIA

A Dios, a mis padres, a mi abuela y a mi novio que siempre han estado junto a mí apoyándome incondicionalmente, para ellos este trabajo.

Ericka Barahona Delgado

A Dios, a mis queridos padres, a mi hermana por su ayuda incondicional y apoyo, a mi esposo por su paciencia y amor, a mi querido Franklincito ya que por él, pude regresar a cumplir mis sueños, y en especialmente a Mí por no darme por vencida en seguir adelante cuando todos me decían lo contrario.

Paola Gellibert López

TRIBUNAL DE SUSTENTACIÓN

_____	_____
Ing. Ignacio Marín García	Ing. Vanessa Cedeño
Profesor del Seminario de Graduación	Profesora Delegada del Decano

DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesina de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral

_____

Ericka Martha Barahona Delgado

_____

Paola Fernanda Gellibert López

RESUMEN

El proyecto a realizar consiste en dos partes, la primera es el diseño e implementación de un analizador de tráfico de redes, capaz de proporcionar capturas en tiempo real de la información que atraviesa una red de área local. La captura de datos puede ser almacenada en un archivo y visualizada a manera de distintos protocolos de acceso a la red, internet, transporte y aplicaciones, realiza además análisis estadísticos de los protocolos de uso más comunes en una red LAN como POP3, HTTP, FTP, SSH, IP y FTP, además realiza el filtrado de paquetes de acuerdo a las necesidades de cada usuario. Para la implementación del proyecto se utilizó lenguaje de programación JAVA mediante el entorno Netbeans, así como el uso de ciertas librerías como Jpcap y Winpcap.

La segunda parte es un análisis comparativo con tres analizadores de tráfico de redes: un analizador licenciado llamado Observer, un analizador no licenciado, Wireshark y el analizador ErPa. El objetivo principal es determinar que analizador tiene más funcionalidades y cuál de ellos nos da más información sobre la red. Este análisis comparativo se lo realizará en una red con datos reales de una mediana empresa, donde se va a determinar cuál de los analizadores de red tiene mejor rendimiento en las mismas condiciones de captura.

INDICE GENERAL

CAPITULO 3

DISEÑO E IMPLEMENTACIÓN DEL ANALIZADOR DE RED ERPA

CAPITULO 4

DISEÑO EXPERIMENTAL DE LOS ANALIZADORES DE RED

CAPITULO 5

ANALISIS DE RESULTADO DEL DISEÑO EXPERIMENTAL DE LOS ANALIZADORES DE RED

GLOSARIO

802.11: Tipo de estándar IEEE que define el uso de capas física y de enlace de datos del modelo OSI.

Apple Talk: Es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes.

Browser: Browser o navegador web es un programa que permite ver la información que contiene una página web

Checksum: Una suma de verificación o checksum es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corruptos.

Conexión de última milla: La última milla es la conexión entre el usuario final y la estación central que provee el servicio de Internet.

Conmutador: Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI.

Cuellos de botella: Cuando la capacidad de procesamiento de un dispositivo es mayor que la capacidad del bus al que se encuentra conectado el dispositivo.

Desktop: Computadora de escritorio u ordenador de mesa, es una computadora personal que es diseñada para ser usada en una ubicación estable.

Enrutador: Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI.

Ethernet: Ethernet es un estándar de redes de computadoras de área local con acceso al medio.

Frame: También conocido como trama o paquete de datos usados en el nivel de enlace de datos del modelo OSI.

H.248: Megaco o H.248 define el mecanismo necesario de llamada para permitir a un controlador Media Gateway el control de puertas de enlace para soporte de llamadas de voz/fax entre redes RTC-IP o IP-IP.

Java: Es un lenguaje de programación orientado a objetos, desarrollado por Sun Microsystems.

Kerberos: Es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura.

Logger: Es un es un tipo de software o un dispositivo hardware específico que se encarga de registrar información.

MP3: Es un formato de compresión de audio digital patentado que usa un algoritmo con pérdida para conseguir un menor tamaño de archivo.

Multicast: Es el envío de la información en una red a múltiples destinos simultáneamente.

NetBIOS: Network Basic Input/Output System, es una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

Netbook: Es una categoría de ordenador portátil de bajo costo y generalmente reducidas dimensiones, lo cual aporta una mayor movilidad y autonomía.

NetFlow: Es un Protocolo de red desarrollado por Cisco Systems para la recopilación de información de tráfico IP.

OSI: El modelo de interconexión de sistemas abiertos, también llamado es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización. (ISO)

Paquete de datos: Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas.

PDA: Personal Digital Assistant, es una computadora de mano originalmente diseñado como agenda electrónica.

Protocolos: Un protocolo es una regla que controla la comunicación en su forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación.

Sniffer: Significa analizador de paquetes, es un programa de captura de las tramas de una red de computadoras.

Software Libre: Es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, modificado y redistribuido libremente

Software: Comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Subnetting: Es una colección de direcciones IP que permiten definir el numero de redes y de host que se desean utilizar en una subred determinada

Tabla de enrutamiento: Es un documento electrónico que almacena las rutas a los diferentes nodos en una red informática.

Topología Bus: Se caracteriza por tener un único canal de comunicaciones denominado bus, troncal o backbone al cual se conectan los diferentes dispositivos.

Traffic-vis: Traffic-vis proceso demonio que monitoriza el tráfico TCP/IP y convierte esta información en gráficos en ASCII, HTML o Postscript.

Trama: Es una unidad de envío de datos en el nivel de enlace de datos.

Virus: Programa informático que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

ABREVIATURAS

ACK: Acknowledgement, Acuse de Recibo

AIM: AOL Instant Messenger

ARP: Address Resolution Protocol, Protocolo de Resolución de Direcciones

ASCII: American Standard Code for Information Interchange, Código Estadounidense Estándar para el Intercambio de Información

BOOTP: Bootstrap Protocol, Protocolo de Arranque

CIFS: Common Internet File System

DHCP: Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host

DNS: Domain Name System, Sistema de Nombres de Dominio

DoS: Denegation of Service**,** Denegación de Servicio

FCIP: Fibre Channel over IP, Canal de Fibra sobre IP

FTP: File Transfer Protocol, Protocolo de transferencia de archivos

GPL: General Public License, Licencia General Pública

GRE: Generic Routing Encapsulation, Encapsulación Genérica de Enrutamiento

HTML: HyperText Markup Language, Lenguaje de Marcado de Hipertexto.

HTTP: Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto

HTTPS: Hyper Text Transfer Protocol Secure, Protocolo Seguro de Transferencia de Hipertexto

ICMP: Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet

ICQ: I seek you, en castellano te busco, cliente de mensajería instantanea

IDE: Integrated Development Environment, Entorno de Desarrollo Integrado.

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos

IGMP: Internet Group Management Protocol

IMAP: Internet Message Access Protocol, Protocolo de red de acceso a mensajes electrónicos

IPv4: Internet Protocol version 4, Protocolo de Internet versión 4

IPv6: Internet Protocol version 6, protocolo de Internet versión 6

ITU: International Telecommunication Union, Unión Internacional de Telecomunicaciones

LBT-TCP: Load-Based Teaming - Transmission Control Protocol

LLMNR: Link Local Multicast Name Resolution

MAC: Media Access Control, Control de acceso al medio

MSN: MicroSoft Network

MSRPC: Microsoft Remote Procedure Call

NIC: Network Interface Card, Adaptador de red

NTP: Network Time Protocol, Protocolo de Tiempo de red

POP3: Post Office Protocol version 3, Protocolo de la Oficina de Correo

RAM: Random-Access Memory, Memoria de Acceso Aleatorio

RARP: Reverse Address Resolution Protocol, Protocolo de Resolución Reversa de Direcciones

RTP: Real Time Protocol, Protocolo de Tiempo Real

SAP: Session Announcement Protocol, protocol de Aviso de Sesión

SMB: Server Message Protocol, Protocolo de Mensajes del Servidor

SMPP: Short Message Peer-to-Peer**,** Mensaje Corto de Puerto a Puerto

JRE: Java Runtime Environment,

LAN: Local Area Network, Red de Área Local

SMTP: Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo

SSDPV1: Simple Service Discovery Protocol version 1. Protocolo Simple de Descubrimiento de Servicios

SSH: Secure Shell, Intérprete de Órdenes Seguras

SSL: **Secure** Sockets Layer, Protocolo de Capa de Protección Segura

TCP: Transmission Control Protocol, Protocolo de Control de Transmisión

TELNET: Telecommunication Network, Red de Telecomunicaciones

TLS: Transport Layer Security, Seguridad de la Capa de Transporte

UDP: User Datagram Protocol, Protocolo de Datagrama del Usuario

UML: Unified Modeling Language, Lenguaje Unificado de Modelado

WAN: Wide Area Network, Red de Área Extensa

WLAN: Wireless Local Area Network, Red de Área Local Inalámbrica

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Con el paso del tiempo las comunicaciones han ido evolucionando, recordando que las primeras comunicaciones eran mediante cables y poco a poco fueron mejorando, llegando cada vez más lejos y abarcando más usuarios. Con todo esto se llegó a la necesidad de mejorar estos medios de transmisión de una manera muy rápida, hasta lo que en la actualidad tenemos.

Con el tiempo la tecnología se ha vuelto parte de nuestras vidas, por ejemplo el internet y las conexiones de alta velocidad se encuentran disponibles para todas las personas que tengan un dispositivo de comunicación tales como un computador, PDA o celulares.

Internet ha impulsado el fenómeno de la globalización y ha dado lugar al nacimiento de una nueva era, caracterizada por el uso de la red para las comunicaciones, negociaciones, transacciones y trabajos remotos los cuales dan un mayor valor y agilita las actividades de las empresas. Una de las ventajas más significativas del internet y la alta velocidad de las comunicaciones actuales, es que no es necesario estar físicamente en el sitio, ya que mediante una conexión a internet podemos acceder a cualquier lugar remoto y estar conectados, resolviendo problemas en tiempo real.

Con el paso de los años el acceso a las redes crece con más usuarios y estos a su vez, tienen más requerimientos tanto para cargar o descargar información, haciendo que cada día exista más tráfico. Debido a este gran incremento de usuarios se deben adoptar soluciones relacionadas con las redes ya que estas sufren frecuentemente de congestionamientos y colapsos importantes.

En la red circula mucha información y a veces estas redes se saturan debido al congestionamiento, esto se produce porque en las redes circula tráfico que hasta hace poco no era habitual como descarga de videos, audio, mensajería, o multimedia en general. Incluso considerando una red LAN pequeña de una empresa también puede sufrir saturación de tráfico, debido a que la mayor parte del tiempo los usuarios están enviando requerimientos tales como, mails, navegando en la web o descargando multimedia esto nos trae como consecuencia que la red presente problemas de lentitud, virus o intrusos hacia información valiosa de la empresa.

Varios de estos problemas de red se pueden resolver con el uso de algunas herramientas como los analizadores de tráfico, que observe que tipo de información circula con mayor frecuencia por la red, el tiempo, de donde proviene en tráfico (envío-destino) y así poder tomar las medidas correctivas para el manejo adecuado del tráfico de la red LAN de una empresa, universidad y escuelas [1], [2].

CAPITULO I

GENERALIDADES

Como habíamos indicado anteriormente el crecimiento constante de las redes de comunicaciones estimula la búsqueda de nuevas herramientas, con el fin de mantener el estado de estas redes en óptimas condiciones. Nuestro objetivo es crear una herramienta de monitoreo y análisis básico capaz de indicarnos mediante gráficos estadísticos y filtrado los paquetes la información que atraviesa una red LAN.

1.1 Antecedentes

Durante la materia de graduación “Seguridad en Redes” aprendimos muchas cosas sobre la red informática, el avance, la evolución,

seguridades y sus debilidades, metodologías de análisis de seguridad como análisis de puertos, análisis de tráfico, análisis de protocolos, análisis estadísticos, además de ver cómo en muy poco tiempo, las redes informáticas crecieron en tamaño y en importancia. Aprendimos que la tecnología siempre está variando de una manera muy rápida, que el acceso a internet está cada vez más globalizado, y como también están en crecimiento la creación de aplicaciones, como redes sociales, chats y videos [2].

Con todos los cambios que existen y los que están por venir en el mundo de las redes, cada vez se exige soluciones de seguridad perfectamente integradas, más transparentes y más flexibles.

Si la seguridad de la red se encuentra afectada ya sea esta una LAN, WLAN, WAN, etc., podría tener consecuencias graves, como la pérdida de privacidad, el robo de información e incluso, responsabilidad legal. Para que esta situación constituya un desafío aun mayor, los tipos de amenazas potenciales a la seguridad de la red se encuentran siempre en evolución [2].

Por eso existe la necesidad de un software que analice el tráfico de red, que observe que acontece por la red en un determinado momento y que permita analizar mediante gráficos estadísticos, que tramas y protocolos se encuentren con más frecuencia pasando por nuestra red

y que solución tomar mediante este análisis que lo realiza el software Analizador de Red.

1.2 Planteamiento del problema

A través de las redes informáticas, pasan millones de paquetes de información los que muchas veces son ignorados por el usuario, trayendo así complicaciones en nuestra red como por ejemplo lentitud, problemas de virus, intrusos, o acceso a información no autorizada. Es por eso que se plantea como una posible solución, la implementación de analizadores de tráfico de redes donde se pueda visualizar en detalle los protocolos utilizados en nuestra red, para así detectar posibles inconvenientes.

En esta materia de graduación cuyo tema es sobre “Seguridad en Redes” el proyecto a realizar se basa en el análisis, creación y pruebas de un analizador de tráfico de red llamado comúnmente sniffer de red.

Un analizador de tráfico de red es un programa de para monitorear y analizar el tráfico en una red de computadoras, detectando cuellos de botellas y problemas que existan en ella. Esta sería una definición de su uso legal, puesto que también podemos utilizarlo para interceptar las comunicaciones de los programas de conversación como MSN, AIM,

ICQ, e incluso filtrar tráfico HTTP, POP3, SMTP, ver claves, mensajes y demás [3].

1.3 Justificación

Como proyecto de materia de graduación Seguridad en Redes, tenemos como objetivo principal desarrollar una herramienta gráfica orientada principalmente a fines educativos. La aplicación debe capturar y analizar el tráfico de una red determinada, realizando capturas en tiempo real y control estadístico de protocolos, con esta información capturada podemos indicar al usuario que está sucediendo en su red, y que protocolos serian los más comunes, clasificados por aplicación, ayudándonos a comprender que se esconde detrás de cada uno de ellos.

No se descarta el uso de esta aplicación en el ámbito empresarial para la detección de intrusos, monitoreo y análisis del tráfico en una red de computadoras detectando cuellos de botella, virus y problemas que existan en ella.

1.4 Objetivos del proyecto

Los objetivos generales y específicos del presente proyecto, se detallan a continuación.

1.4.1 Objetivos Generales

El objetivo principal de este proyecto es realizar un software que analice el tráfico de red, que pueda generar estadísticas de lo que pasa en una red, que permita filtrar los paquetes por medio de sus protocolos, puertos de orígenes, direcciones MAC etc.

Realizar todo este análisis con la finalidad de brindar seguridad a una red ya sea esta de una empresa o una red en una casa, y así establecer que sucede por dicha red y tomar las respectivas correcciones, seguridades o permisos.

Con esta herramienta se puede mejorar la seguridad de la red de una empresa o lugar donde se instale el analizador de red. También tenemos como objetivo realizar una comparativa entre varios analizadores de red licenciados y no licenciados con respecto al analizador de tráfico de red creado.

1.4.2. Objetivos Específicos

Los objetivos específicos del presente trabajo son:

- Aplicar los diversos conceptos de seguridad en redes al momento de diseñar el analizador.
- Analizar el tráfico proveniente de una red de datos y notar cuales son los protocolos de uso más comunes en una red.
- Diseñar diversos tipos de consulta de los datos de la red, así como un ente gráfico donde se pueda visualizar la información.
- Aplicar los conceptos de los protocolos de red al momento de filtrar la información.
- Comparar las capturas del tráfico de una red con tres diferentes analizadores de tráfico de red existentes en el mercado.

CAPITULO II

MARCO TÉORICO

Definiremos el concepto de analizador de tráfico de redes, su funcionamiento y su importancia en el ámbito laboral y empresarial, definiremos además el alcance del analizador de redes ErPa y los protocolos que esta aplicación puede procesar. En el mercado actual tenemos diferentes tipos de analizadores de tráfico de red, de los cuales hemos seleccionado los más usados para proporcionar una pequeña descripción de los mismos.

2.1 Descripción General

A diferencia de los circuitos tradicionales telefónicos, las redes de computadoras son canales de comunicaciones compartidos que pueden

recibir información proveniente de diversos dispositivos. Esta información muchas veces puede ser de contenido confidencial o puede ser dañina para nuestra red de computadoras, de allí nace la necesidad de crear un programa que en adelante denominaremos, analizador de redes o analizador de tráfico de red, el cual se trata de un software que analiza toda la información transmitida en tiempo real, a través de una red [4].

Existen muchos tipos de analizadores de tráfico de red en el mercado, los cuales varían de una funcionalidad a otra, pero todos tienen en común el analizar las redes para ver qué está pasando en ellas. Algunos de estos programas analizadores de redes están hechos en base a software libre y otros remunerados. Muchos de los analizadores de tráfico de red que se pueden descargar de Internet son gratis, pero no tiene todas las funcionalidades incluidas, si se requiere del software completo hay que pagar por la totalidad del analizador de red.

Como objetivo de trabajo de esta tesis proponemos investigar todas las funcionalidades y características que los analizadores de redes tengan tanto en el ámbito laboral como estudiantil. En el ámbito laboral puesto que se envían paquetes con información importante, que podrían comprometer la integridad de una empresa y en el ámbito estudiantil para recalcar la importancia y el funcionamiento de una herramienta tan importante como esta.

2.2 Concepto de analizador de tráfico de red

Su definición en informática, es un programa especializado de monitoreo y análisis, que captura tramas o paquetes de una red de datos.

Es un software informático que puede interceptar y registrar tráfico de paquetes pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el husmeador captura cada unidad de datos del protocolo y puede decodificar y analizar su contenido, de acuerdo a la especificación del programa [5].

Su uso varía desde la detección de un cuello de botella en una red hasta el análisis de fallas en las redes, aunque también es habitual su uso para fines maliciosos, como robo de contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de chat, obtener datos personales entre otros [5].

La cantidad de tramas que puede obtener un Analizador de tráfico de red depende de la topología de red, del diseño del analizador, así como el medio de transmisión. Para poner en funcionamiento este tipo de software, la persona debe tener conocimientos básicos sobre estructuras de redes y las tramas de datos.

2.3 Funcionamiento General de un Analizador de Tráfico de Red

Para explicar el funcionamiento de un analizador de tráfico de red es necesario tener presente varios conceptos. Una red de datos, está formada por varias computadoras conectadas entre sí por un medio cableado o inalámbrico, que a su vez están conectados a otros dispositivos como conmutadores y estos a su vez a otros dispositivos llamados enrutadores, el cual se encarga de escoger rutas y dirigir los paquetes de información hacia la computadora destino como podemos ver en la figura 2.1 [6].

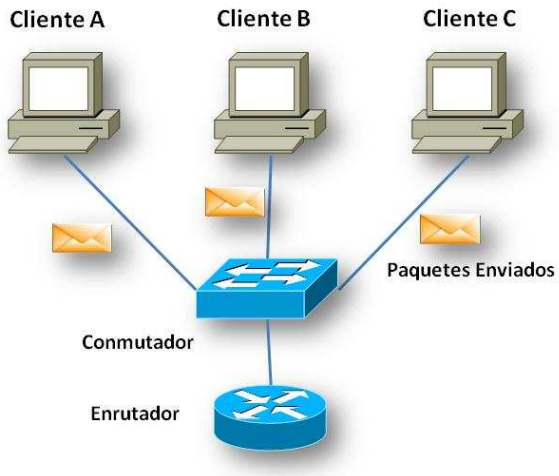


Figura 2.1 Conexión de una red LAN

Es muy común en las redes LAN, con una topología tipo bus que un analizador de tráfico de red pueda operar en dicha red, ya que todas las computadoras están conectadas a un mismo medio compartido, donde

todo el tráfico es transmitido y recibido por todas las máquinas que pertenecen a esa red local, es decir comparten un medio común.

Otro medio donde los analizadores de tráfico de red pueden desenvolverse tranquilamente es en la máquina de la víctima, pero para este caso es necesario tener acceso a la maquina víctima, donde se instala el programa y el fin de hacer esto es encontrar información de otros usuarios y tener acceso a otros dispositivos, que normalmente se accede desde la máquina víctima.

Los analizadores de tráfico de red funciona por una simple razón, existen protocolos que son de acceso remoto y las máquinas transmiten las claves de acceso remoto en forma de texto plano por esta razón es que se captura la información que se transmite por la red, ya que nos da la información correcta para tener acceso a alguna maquina determinada [7].

Como ejemplo de cómo procede la captura en la figura 2.2, tenemos una máquina que transmite un dato, lo hace a través del cable compartido, en el cual están conectadas todas las maquinas, las maquinas que están conectadas tienen la misma posibilidad de ver los datos que en ese momento se están transmitiendo, pero eso no sucede ya que cada tarjeta de red que tienen las maquina conectadas, solo reciben o capturan los paquetes de datos que van dirigidos hacia ellos,

y todos los otros datos que se transmiten son ignorados, por ese motivo cuando se va a comenzar a capturar los datos se activa la tarjeta en modo promiscuo [7].

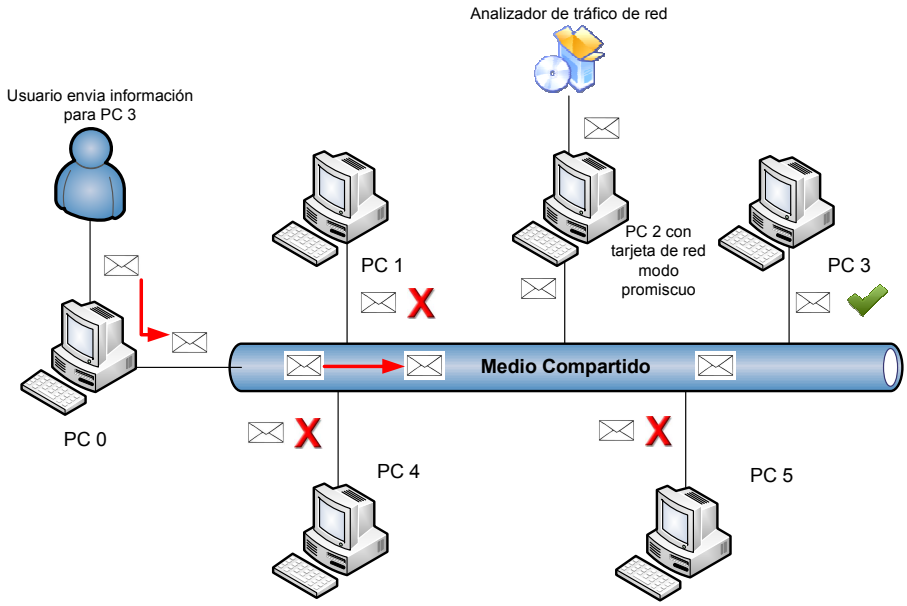


Figura 2.2 Funcionamiento general de un analizador de redes

Así es como un analizador de tráfico de red trabaja accediendo a los datos que pasan por una tarjeta de red, sea esta inalámbrica o Ethernet. Una vez que se accede a los datos, lo que realiza el analizador de tráfico de red es filtrar todos los paquetes, los examina y mira las peticiones de los puertos según los filtrados del usuario como TCP, UDP, POP3, etc.

2.4 Analizadores de tráfico de red existente en el mercado

Por su importancia tenemos los siguientes tipos de Analizadores de tráfico de red:

TCPDUMP Permite monitorizar tráfico de red en tiempo real. Los filtros que se pueden crear para mostrar tan sólo la información que nos interesa, hacen de TCPDUMP una herramienta muy potente para el análisis de tráfico en redes de comunicaciones [8].

Darkstat Realiza la estadística de direcciones que se generan en la comunicación entre hosts, el tráfico que se produce, y los diferentes números de puerto usados por los diversos protocolos. Adicionalmente, el programa obtiene un breve resumen y gráficos por períodos de tiempo de los paquetes analizados desde que se empieza a ejecutar el programa [9].

***Traffic* –VIS** Proceso demonio que monitoriza el tráfico TCP/IP y convierte esta información en gráficos en ASCII, HTML o PostScript. Traffic-vis también permite analizar el tráfico entre hosts para determinar qué hosts han comunicado y el volumen de su intercambio [10].

SNORT Es un Sistema de detección de intrusiones basado en red. Implementa un motor de detección de ataques y barrido de puertos que

permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos o aprovechar alguna vulnerabilidad, análisis de protocolos, etc., conocidos, todo esto en tiempo real [11].

NWATCH Se puede entender como un analizador de puertos pasivo, que está solamente interesado en tráfico IP y organiza los resultados como un explorador de puertos. Para la seguridad de la red NWatch es un complemento excelente al barrido de puertos regular de sus redes. Por defecto, NWatch permanece activo indefinidamente hasta que recibe un aviso. Durante ese tiempo mira el interfaz por defecto, siguiendo cada combinación del IP host/port que descubre [12].

ETHEREAL Ethereal que ahora se llama Wireshark, es un potente analizador libre de protocolos de redes, funciona bajo Unix, Mac OS X y Windows. Nos permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco, puede leer más de 20 tipos de formato distintos. Destaca también por su impresionante soporte de más de 300 protocolos [13].

ETTERCAP Es un sniffer, interceptor o logger para redes LAN con switch, que soporta la disección activa y pasiva de muchos protocolos, incluso cifrados e incluye muchas características para el análisis de la red y del host anfitrión. Inyecta caracteres en una conexión establecida

emulando comandos o respuestas mientras la conexión está activa. Intercepta tráfico remoto mediante un túnel GRE: Si la conexión se establece mediante un túnel GRE con un router, puede interceptarla y crear un ataque tipo Man in the Middle [14].

KISME Es un analizador de tráfico de red específico a Linux para redes inalámbricas. Específicamente, es un detector de la red 802.11 en capa 2, un sistema sin hilos para la detección de la intrusión. Funciona correctamente con dos principales tipos de tarjetas inalámbricas. Kismet identifica redes de modo pasivo, recogiendo paquetes y detecta redes nombradas estándares, redes ocultas e infiere la presencia de redes vía tráfico de los datos [15].

2.5 Requerimientos de la Aplicación

Se requiere una aplicación que sea capaz de analizar, filtrar, separar y contabilizar la cantidad de paquetes de las diferentes capas de los protocolos. Se pretende analizar esta información accediendo de manera promiscua a la NIC de un ordenador y analizar el tráfico que proviene de una red en un determinado tiempo, para mostrar una estadística de la cantidad de paquetes que existen en dicha red en cierto tiempo, esto con la finalidad de poder desglosar y examinar el tipo de información que pasa por esta red para evitar problemas como

cuellos de botella, filtrado de información fuera de la empresa entre otros.

2.6 Tráfico Capturado por la Aplicación

En este proyecto de materia de graduación que es un analizador de tráfico el objetivo principal es de capturar tráfico de una red, donde tráfico lo entendemos en este caso, como todo paquete de datos, protocolos TCP/IP que circulen por nuestra red, y que vamos a capturar para posteriormente analizar.

Los protocolos que vamos a capturar en el analizador de red ERPA, los hemos subdividido mediante capas y se muestran en la siguiente tabla.

Capas Analizadas por ERPA	Protocolos a capturar
Capa Aplicación:	SSH Telnet FTP HTTP POP3 SMTP
Capa de Transporte:	TCP
Capa de Acceso a la red:	Información del paquete Trama de los paquetes Ethernet

Tabla 2.1 Resumen protocolos capturados por ErPa

CAPÍTULO 3

DISEÑO E IMPLEMENTACIÓN DEL ANALIZADOR DE RED ERPA

Para realizar el diseño del analizador de red ErPa utilizamos herramientas de desarrollo de software orientado a objetos como es el diagrama UML, descripciones de casos de uso, así como el diagrama de clases para describir la estructura de nuestro sistema. En la implementación del proyecto nos encontramos con algunas limitantes que serán descritas en subcapítulos posteriores.

3.1 Diseño del analizador de tráfico de red ErPa

Como parte del proceso de diseño a continuación mostramos el esquema del diagrama UML en la figura 3.1, usado para el analizador de redes ErPa.

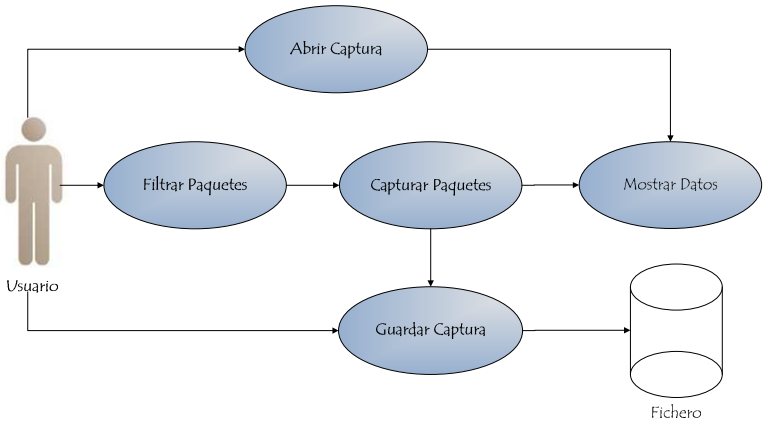


Figura 3.1 Diagrama UML del analizador ErPa

Como podemos observar en la figura 3.1 el usuario tiene la opción de establecer un filtro antes de capturar los paquetes, así como abrir una captura anterior para luego mostrar los datos en el formato establecido. A continuación detallamos cada uno de los casos de uso que pueden existir al utilizar el analizador ErPa.

Filtrar Paquetes: Permite crear filtros para la captura de paquetes. El actor es el usuario conectado a una red. Deben existir precondiciones tales como que el usuario debe estar conectado a la red y el usuario debe haber seleccionado la tarjeta de red. En el flujo normal el actor selecciona Captura y luego Empezar de la barra de menú, luego el

actor pulsa sobre el cuadro Filtro e introduce el tipo de Filtro que desea para iniciar la captura en el formato preestablecido. Como flujo alternativo tenemos que el sistema comprueba la sintaxis del tipo de filtro devolviendo un error en caso de ser incorrecta. La pos condiciones es que el usuario puede empezar con la captura de paquetes.

Capturar Paquetes: Permite capturar paquetes que se encuentran en una tarjeta de red. El actor es el usuario conectado a una red. Deben existir precondiciones tales como que el usuario debe estar conectado a la red y debe haber seleccionado la tarjeta de red. En el flujo normal del diagrama el actor selecciona Captura y luego Empezar de la barra de menú, luego se pueden visualizar paquetes enteros, solo encabezados o seleccionar el tamaño máximo de la captura, después el actor presiona OK y los paquetes obtenidos se van mostrando en la pantalla de acuerdo a las opciones de visualización del usuario. Como flujo alternativo el sistema comprueba la validez del tamaño máximo de la captura, regresando un mensaje de error en caso de encontrarse errónea. Cuando termine la captura de acuerdo al tamaño máximo definido o si el usuario detuvo la captura antes, los datos se pueden visualizar en pantalla o grabarla en un fichero para posterior análisis.

Mostrar Datos: Permite mostrar en pantalla los paquetes capturados. El actor es el usuario conectado a una red. Para mostrar los datos el fichero de captura debe existir y los datos de una captura están almacenados en el búfer de captura. En el flujo normal el actor abre un fichero de captura y obtiene los datos en el búfer de captura, después el actor podrá visualizar por pantalla una lista en detalle mediante celdas de los paquetes capturados. En el flujo alternativo el sistema comprueba si el fichero es válido para poder cargarlo, caso contrario muestra un mensaje de error. Después como pos condiciones el usuario puede visualizar y analizar los paquetes capturados en la pantalla pudiendo cambiar las opciones de visualización en el menú Ver, además de realizar gráficos estadísticos acumulativos y continuos de los paquetes mostrados en pantalla.

Abrir Captura: Permite al usuario abrir una captura almacenada en fichero, como actor tenemos al usuario conectado a la red. Como precondición el fichero de captura debe existir. En el flujo normal**,** el actor pulsa Archivo luego Abrir, y busca el fichero para poder cargarlo al programa, luego el actor puede visualizar el contenido de los paquetes en forma de celda. En el flujo alternativo, el sistema comprueba la validez del fichero cargado devolviendo un mensaje de error cuando no

se pueda abrir. Como pos condiciones tenemos que el usuario recupera una sesión de captura anterior y la puede visualizar en pantalla.

Guardar Captura: Permite guardar una sesión de captura de paquetes dentro de un fichero. El actor es el usuario conectado a la red. Como precondiciones tenemos que el usuario debe haber terminado la captura debido a los paquetes máximos o bien parar la captura y que los paquetes estén almacenados en el búfer de captura. En el flujo normal el actor se dirige a la barra de menús en Archivo, luego Guardar, después el actor escoge el nombre la captura, donde será almacenado el fichero y pulsa en Guardar. Como flujo alternativo el programa presenta un mensaje de error en caso de encontrarse algún problema al guardar el fichero. Como pos condiciones tenemos que el fichero ha sido almacenado para su previo análisis y visualización.

3.2 Implementación del analizador de tráfico de red ErPa

Para implementar el analizador de tráfico de red ErPa, se decidió trabajar en la plataforma JAVA conjuntamente con Netbeans. Para el desarrollo del analizador de tráfico de red, se requirió el uso de la librería JPCAP, ya que esta librería nos permite desde JAVA enviar paquetes IP para poder hacer las capturas en la red, la información más detallada de la librería se encuentra en el anexo D. También se utilizó

Winpcap que es un controlador que extiende el sistema operativo para proveer acceso de red a bajo nivel, esta biblioteca es indispensable para el correcto funcionamiento de algunos programas como por ejemplo Wireshark; Snort [16]. Utilizamos JpcapDumper, que es una aplicación que captura paquetes gráficos, la cual nos ayudó para realizar nuestro analizador de red ErPa y poder capturar los paquetes que necesitábamos capturar como por ejemplo POP3, FTP, SMTP, SHH, TELNET y HTTP. Captura longitud del paquete, puerto origen y puerto destino, con el protocolo POP3, SHH, TELNET, FTP captura usuarios y contraseñas, y se muestra graficas de pastel para ver que paquetes son los que más circulan en la red.

Otro requerimiento de ErPa analizador de tráfico de red, fue que el sistema operativo donde se iba a ejecutar el proyecto debe ser sistema operativo Windows XP de 32 bits, para poder utilizar Winpcap se necesita como mínimo un procesador de 166 MHz, con un mínimo de memoria RAM de 32 MB, con un espacio libre en disco duro de 25 MB. Al comenzar la programación utilizamos un computador con Windows 7 de 64 bits, con un procesador Core i5, con memoria RAM de 4 GB, y disco duro de 500 GB, y al momento de instalar Winpcap se producía un mensaje de error. Este se debió a que Winpcap solo funciona en sistemas operativos que trabajen en 32 bits.

3.3 Presentación de los datos

Los datos que son capturados por el analizador de tráfico de red ErPa se muestran en forma de tabla, es decir que a cada línea de la tabla le corresponde un arreglo, con todos los datos básicos que contiene un paquete capturado por el analizador de tráfico de red. También se puede desplazar verticalmente por la tabla y observar en cada línea el contenido del paquete, este puede ser IP destino, IP fuente, numero de puerto, servicio, MAC, etc.

El campo donde se encuentran los datos del paquete se presenta en forma de área de texto, marcado en color azul como se puede ver en la figura 3.2 y los campos del paquete se presentan del lado izquierdo en forma de árbol es decir en diferentes niveles, en donde cada nodo es representado por un nivel.

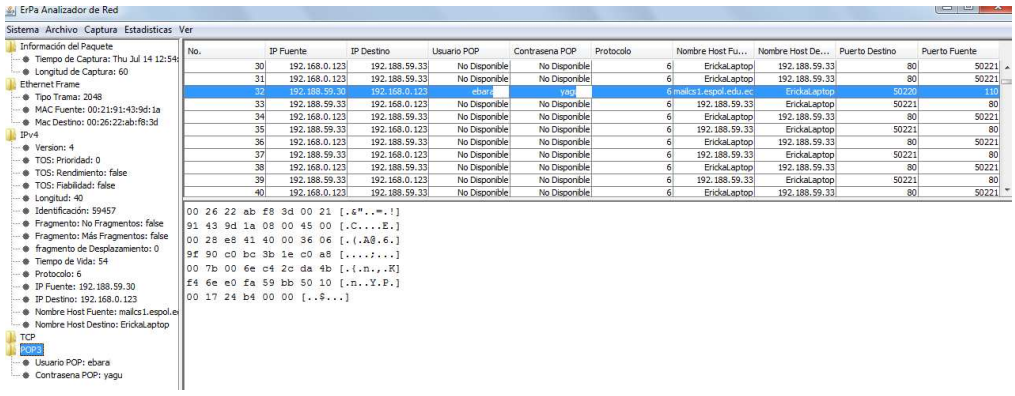


Figura 3.2 Presentación de los datos

El Analizador de Tráfico de Red ErPa cuenta con funciones de captura en tiempo real, captura los paquetes por medio de archivos y se puede visualizar el contenido de los paquetes.

CAPÍTULO 4

DISEÑO EXPERIMENTAL DE LOS ANALIZADORES DE RED

Para la realización de este capítulo nos basamos en el análisis y monitoreo de las redes de hoy en día, proponemos un breve análisis de los diferentes analizadores que se utilizan en la comparación, exponemos las ventajas y desventajas de usar un analizador de red licenciado y no licenciado, detallamos las características de los equipos utilizados para la captura, mostramos una breve descripción de la red de la empresa en la cual se realizaron las capturas, y también la ubicación de los dispositivos para realizar la captura.

4.1 Objetivos de la comparación entre analizadores de red licenciados y no licenciados

- Determinar cuál de los analizadores de tráfico de red es más completo y más fácil de usar.
- Determinar cuál de los analizadores de tráfico de red captura más detalladamente los paquetes.
- Observar cuál de los analizadores captura más paquetes en un tiempo determinado.
- Observar y determinar cuál es el punto en donde se debe colocar el analizador de tráfico de red, para poder solucionar los posibles errores que tenga la red analizar.
- Determinar si el punto en donde colocamos el analizador de red fue el correcto para el análisis de la red y cuál fue el resultado de dicha captura.

4.2 El análisis y monitoreo de las redes hoy en día

Las redes de cómputo de las organizaciones en la actualidad, se vuelven cada vez más complejas y las exigencias de las operaciones es cada vez más demandante. Las redes están soportando cada vez más exigencias en cuanto a aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha

convertido en una labor cada vez más importante y de carácter proactivo para evitar problemas.

Anteriormente, cuando no se disponía de las herramientas como software analizadores, era necesario contratar a una empresa especializada para realizar el análisis y monitoreo del tráfico de la red, con un costo muy elevado. Las herramientas que se ofrecen hoy en día, le permiten, al administrador de red, realizar el análisis del tráfico de red por cuenta propia, y manejar un sistema experto que ayude a la interpretación de los resultados obtenidos y facilitándole el análisis de la red [17].

4.3 Analizador de red Wireshark

Wireshark es un analizador de tráfico de red, antes conocido como Ethereal, pertenece a la categoría de software libre y es ampliamente utilizado en el ámbito de las redes, realiza el análisis y soluciona problemas en redes de comunicaciones, entre otras características Wireshark observa el comportamiento de los protocolos en una red, y también es utilizado como una herramienta didáctica para educación. Wireshark además cuenta con todas las características estándar que pueda tener un analizador de protocolos.

La funcionalidad que provee Wireshark es similar a la del analizador tcpdump, pero añade una interfaz gráfica amigable con muchas

opciones de organización y filtrado de la información que se captura o se requiere capturar, además permite ver todo el tráfico que pasa a través de una red aunque es mayormente utilizada en redes Ethernet puede llegar a ser compatible con otro tipo de redes, se puede también establecer la configuración en modo promiscuo que ya se explicó capítulos anteriores.

Wireshark permite examinar datos de una red en tiempo real o de un archivo de alguna captura anterior. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un lenguaje completo para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP [21].

4.4 Analizador de Red Observer

Observer es un completo analizador de tráfico de red y protocolos, se ubica en la categoría de analizadores licenciado, entre sus características tenemos que puede ser utilizado tanto para redes alámbricas como inalámbricas, captura, analiza y descifra 500 protocolos. Es un software desarrollado por Network Instruments y tiene varias versiones con diferentes cualidades, Observer Estándar, Observer Expert, Observer Suite, Enterprise Observer, comprenden la

gama de analizadores que se pueden utilizar según las exigencias de la red. En la comparación de esta tesis, vamos a utilizar Observer Trial que es una versión de muestra con una licencia de 15 días para ser utilizada.

Con el analizador de tráfico Observer, el administrador de la red tiene una visión más clara del tráfico de la red LAN, facilitando la toma de decisiones sobre la administración de esta red.

El analizador Observer ofrece varios modos de análisis para ayudar a aislar problemas específicos de la red y concentrarse en una solución más óptima para la misma [19].

4.5 Ventajas y desventajas entre un analizador de red en código libre

Una de las principales o tal vez la más importante ventaja, es la parte económica, ya que esto permite que las pequeñas y medianas empresas tengan acceso a soluciones de bajo costo que pueden ayudar y mejorar el manejo de la red de la empresa. Unos de los analizadores de tráfico de red más usados en código libre es el Wireshark, es el analizador más reconocido en el mercado por administradores de redes, de pequeñas y grandes empresas. Wireshark

realiza un análisis de la trama de los protocolos proporcionando información muy valiosa y completa de la red.

Las ventajas de usar Wireshark son: las capturas que se realizan, son en vivo es decir en tiempo real, captura el tráfico de muchos medios diferentes, admite el formato estándar de archivos tcpdump, Wireshark se provee bajo la licencia GPL, puede trabajar tanto en modo promiscuo como en modo no promiscuo, el software es compatible con más de 480 protocolos, es capaz de capturar datos de la red o leer datos almacenados en un archivo (de una captura previa), su código se basa en la librería pcap, tiene capacidades de filtrado muy extensas, una súper ventaja es que puede leer archivos de captura de más de 20 plataformas o Sistemas Operativos, puede volver a reconstruir de sesiones TCP, y se puede ejecutar en más de 20 plataformas o Sistemas Operativos [21]

Wireshark puede realizar captura de varias horas seguidas incluso de días, la desventajas que tiene Wireshark es en el momento de levantar una captura hecha con anterioridad y comenzar a analizarla dependiendo el tamaño de la captura esta puede dar un error “OUT of Memory” Esto significa que Wireshark se queda sin memoria para levantar toda la información antes capturada y actualmente no hay ninguna solución para este problema.

Las desventajas de usar Wireshark es que no tiene un sistema de detección de intrusos, es decir no avisa a nadie cuando alguien se encuentra en la red y realiza cosas extrañas o modifica cosas en la red

En este análisis de comparación vamos a usar Wireshark como analizador de tráfico de red como software libre versus Observer Analizador de tráfico de red como software licenciado.

4.6 Diseño experimental del análisis de comparación

Para realizar el análisis y comparación entre los analizadores de tráfico de red, utilizamos tres computadores portátiles con diferentes características, las cuales de ahora en adelante se llamaran equipo A, equipo B y equipo C. Las características de los equipos se describen en la tabla 4.1.

Tipo	Tipo de Dispositivo
Equipo A	Toshiba Satellite A505 con procesador I5, Sistema Operativo Windows 7, 4 GB de RAM, y 500GB de disco duro.
Equipo B	HP Pavilon dvd600 AMD Turiom(tm) 64 Mobile con 1.61GHz, 1.93 GB de RAM, 80 GB de disco duro, Sistema Operativo Win XP Profesional, Versión 2003 y Service Pack 3.
Equipo C	HP Pavilon dvd600 AMD Turiom(tm) 64 Mobile Technology MK-36, con 2.0 GHz, 1.50 GB de RAM, 80 GB de disco duro, Sistema Operativo Windows 7 Home Premium Profesional de 32 bits, Versión 2003 y Service Pack 3

Tabla 4.1 Dispositivos y analizadores a usar

La captura se la realizo durante tres días, con tres equipos diferentes y cada uno con el mismo analizador de red. La distribución de la captura del tráfico fue la siguiente:

El primer día los tres equipos capturaron el tráfico con el analizador de red Observer, esta captura se realizó en el día A.

El segundo día de captura los tres equipos estuvieron con el analizador de red Wireshark, esta captura se realizó en el día B.

El tercer día de captura los tres equipos se mantuvieron con el analizador de red ErPa, esta captura se realizó en día C.

Los intervalos de tiempo para la captura del tráfico de red fueron tres, el primer intervalo de media hora, el segundo intervalo de una hora, y el tercer intervalo de cuatro horas. Se puede observar la tabla 4.2 cómo se realizo la distribución de los equipos.

HORAS	OBSERVER DÍA A	WIRESHARK DÍA B	ErPa DÍA C
8:30 – 9:30	Equipo A	Equipo A	Equipo A
9:30 – 10:30	Equipo B	Equipo B	Equipo B
17:00 – 21:00	Equipo C	Equipo C	Equipo C

Tabla 4.2 Distribución de los Equipos con los Analizadores

4.7 Estructura de red de la empresa

La red donde se realizó la captura es una empresa que posee 75 usuarios en el área administrativa, consta de una red mediana con un router principal y otros elementos de red los cuales se muestran en la figura 4.1.

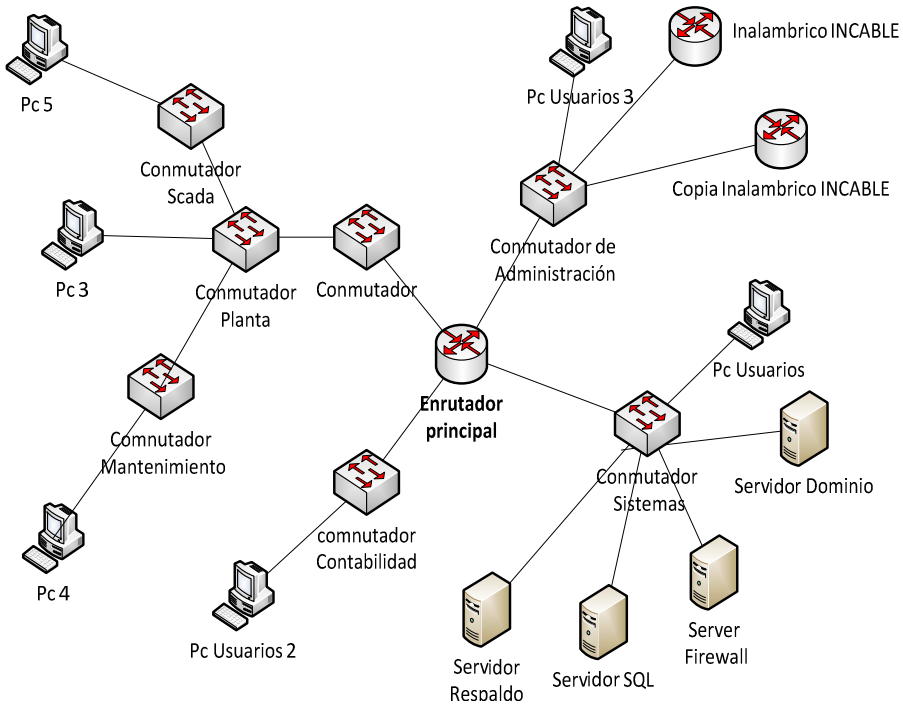


Figura4.1 Gráfico de la Red Empresa X

Para realizar las capturas en la red de la empresa X, nos ubicamos en el departamento de sistemas y nos conectamos en un punto de red, que está conectado directamente al router principal. Para hacer la captura del tráfico utilizamos un switch D-link para conectar los equipos a la red

y comenzar a capturar el mismo tráfico pero con diferentes equipos y diferentes analizadores de red. A continuación la figura 4.2 nos muestra la ubicación de los Equipos A, B, C.

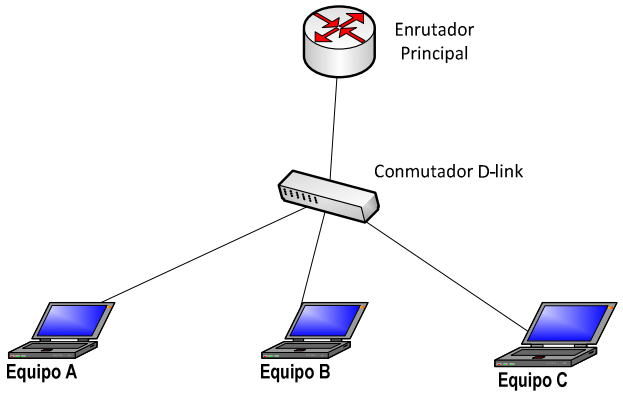


Figura 4.2 Distribución de los equipos para realizar la captura

CAPÍTULO 5

ANALISIS DE RESULTADO DEL DISEÑO EXPERIMENTAL DE LOS ANALIZADORES DE RED

Análisis y comparación del tráfico de red, se lo realiza con tres analizadores de red diferentes uno licenciado, no licenciado y el analizador realizado en esta tesis, el propósito es capturar el tráfico de red, de la empresa X, en un lapso de tres días, con tres intervalos de tiempo de captura y además con tres computadoras de diferentes características.

5.1 Análisis de captura del tráfico de red por media hora

La captura del tráfico de red de la empresa se realizó con tres analizadores de tráfico de red Observer, Wireshark, y ErPa. La primera muestra se tomó el día A (martes) con el analizador de red Observer, la segunda muestra se tomó el día B (miércoles) con el analizador de red Wireshark y la tercera muestra se tomó el día C (jueves) con el analizador de red ErPa en un intervalo de tiempo de 30 minutos.

Como se puede observar el tráfico capturado en el día A (martes) por el equipo A fue de 15826 paquetes, en el equipo B fue de 19614 paquetes, y en el equipo C 14000 paquetes. Existe una diferencia de 3788 paquetes capturados entre el equipo A y B, entre el equipo B y C la diferencia es de 5614 paquetes y entre A y C es de 1826 paquetes capturados.

Observer	Intervalo de tiempo	Paquetes Capturados
Equipo A	08:30 – 9:00	15826
Equipo B	08:30 – 9:00	19614
Equipo C	08:30 – 9:00	14000

Tabla 5.1 Cantidad de paquetes capturados en media hora en el día A

Con el analizador de red Wireshark se realizó la captura el día B (miércoles) el tráfico capturado por el equipo A fue de 45475 paquetes, en el equipo B el tráfico capturado fue de 28562 paquetes, y en el equipo

C fue de 24382 paquetes del trafico capturado, en el mismo intervalo de tiempo que la muestra obtenida el día A (martes).

Wireshark	Intervalo de tiempo	Paquetes Capturados
Equipo A	08:30 – 9:00	45475
Equipo B	08:30 – 9:00	28562
Equipo C	08:30 – 9:00	24382

Tabla 5.2 Cantidad de paquetes capturados en media hora en el día B

Con el analizado de red ErPa se realizó la captura del tráfico de red el día C (jueves), en la cual en los tres equipos se capturo 1000 paquetes, el analizador de trafico ErPa solo captura hasta 10000 paquetes en tiempo es más o menos entres 15 a 30 minutos de captura.

ErPa	Intervalo de tiempo	Paquetes Capturados
Equipo A	08:30 – 9:00	10000
Equipo B	08:30 – 9:00	10000
Equipo C	08:30 – 9:00	10000

Tabla 5.3 Cantidad de paquetes capturados en media hora en el día C

5.2 Análisis de captura del tráfico de red por una hora

Para realizar el análisis de la captura del tráfico de red en el primer día A (martes), el intervalo de tiempo fue de hora, con el analizador Observer, en el equipo A se capturo 24450 paquetes, en el equipo B se capturo 34294 paquetes, y en el equipo C se capturo 30828.paquetes

La diferencia entre las capturas del equipo A y B fue de 9844 paquetes, entre el equipo B y C fue de 3466 paquetes, entre el equipo A y C fue de 6378 paquetes.

Observer	Intervalo de tiempo	Paquetes Capturados
Equipo A	10:00 – 11:00	24450
Equipo B	10:00 – 11:00	34294
Equipo C	10:00 – 11:00	30828

Tabla 5.4 Cantidad de paquetes capturados por una hora en el día A

Con el analizador de red Wireshark se realizó la captura en el día B (miércoles), con el equipo A se capturo 51672 paquetes, con el equipo B se capturo 45225 paquetes, con el equipo C se capturo 40249 paquetes.

La diferencia entre las capturas de los equipos A y B es de 6447 paquetes, es decir el equipo A capturo 6891 paquetes más que el equipo B.

La diferencia entre los equipos B Y C fue de 4976 paquetes, se puede observar que el equipo B capturo 4976 paquetes más que el equipo C.

La diferencia entre los equipos A y C fue de11423 paquetes, el equipo A capturo 11423 más paquetes que el equipo C.

Wireshark	Intervalo de tiempo	Paquetes Capturados
Equipo A	10:00 – 11:00	51672
Equipo B	10:00 – 11:00	45225
Equipo C	10:00 – 11:00	40249

Tabla 5.5 Cantidad de paquetes capturados por una hora en el día B

El siguiente período de capturas de una hora se realizó con el analizador de trafico ErPa, se capturo 10000 paquetes, esta captura se la realiza entre 15 y 30 minutos es decir que nuestro analizador de red lo máximo que captura es hasta 10000 paquetes.

ErPa	Intervalo de tiempo	Paquetes Capturados
Equipo A	10:00 – 11:00	10000
Equipo B	10:00 – 11:00	10000
Equipo C	10:00 – 11:00	10000

Tabla 5.6 Cantidad de paquetes capturados por una hora en el día C

5.3. Comparativa de las capturas realizadas

En la tabla 5.7 podemos observar los diferentes valores obtenidos en las capturas pero también podemos decir que, cada muestra fue capturada en diferentes días, los paquetes capturados por el Observer fueron capturados el primer día en este caso sería el día A (martes).

El día siguiente fue el día B, en el mismo intervalo de tiempo podemos observar que en este día, se capturo más tráfico que el día A, este incremento de captura se podría decir que el día B había más

requerimientos por parte de los usuarios. En pocos términos el tráfico del día anterior no es el mismo del tráfico del día siguiente aunque se lo tome en el mismo intervalo de tiempo.

	Observer	Wireshark	ErPa
8:30 - 09:00	**Paquetes Capturados**	**Paquetes Capturados**	**Paquetes Capturados**
Equipo A	15826	45475	10000
Equipo B	19614	28562	10000
Equipo C	14000	24382	10000

Tabla 5.7 Comparativa de paquetes capturados en 30 minutos

En esta misma muestra podemos observar que con el analizador Observer se capturo más paquetes en el equipo B, en el día A, pero en el día B el equipo que más capturo fue equipo A. también tenemos en cuenta que el tráfico es diferente en ambas nuestras.

Lo mismo se puede observar en la muestra tomada por una hora en la cual se realizó así mismo la captura, como se puede observar en la tabla 5.8. En donde, el equipo B con el analizador Observer capturo 30828 paquetes, en el día A, pero con el analizador Wireshark el equipo que más captura hizo fue el equipo A.

	Observer	Wireshark	ErPa
10:00 - 11:00	**Paquetes Capturados**	**Paquetes Capturados**	**Paquetes Capturados**
Equipo A	24450	51672	10000
Equipo B	34294	45225	10000
Equipo C	30828	40249	10000

Tabla 5.8 Comparativa de paquetes capturados en una hora

5.4 Protocolos capturados por Observer

Cuando se Captura tráfico con el analizador Observer, tiene una ventaja que no tienen los otros analizadores como Wireshark, una de las principales facilidades es el análisis de la red con los datos capturados nos nuestra la captura por tipo de protocolos esto se puedo observar en la tabla 5.9 y en la tabla 5.10.

Protocolos	Equipo A 15826	Equipo B 19614	Equipo C 1400
IP	6341	9871	2026
ARP	3844	4054	9968
IPV6	2259	2026	455
IPX	942	600	988
OTHER	469	588	0
Apple talk	168	213	512
NetBIOS	15	20	47

Tabla 5.9 Protocolos capturados por Observer en media hora

Protocolos	Equipo A 242450	Equipo B 34294	Equipo C 30828
IP	10231	14871	14927
ARP	6389	10751	6706
IPV6	1917	1497	3251
IPX	965	994	970
OTHER	950	0	955
Apple talk	345	534	348
NetBIOS	31	47	32

Tabla 5.10 Protocolos capturados por Observer en una hora

5.5 Protocolos capturados por Wireshark

Con Wireshark el análisis del tráfico es más elaborado de realizar pero menos complicado que en los otros analizadores, ya que para ver los tipos de protocolos que se han capturado debemos pasar un filtro e indicar que protocolo queremos que se muestren, para poder saber cuántas veces se requirió el mismo protocolo. A continuación las tablas de los protocolos capturados en la muestra de media hora y una hora.

Wireshark Datos	Equipo A 45475	Equipo B 28563	Equipo C 24382
IP	39656	13134	16440
ARP	3465	5240	4354
IPv4	0	0	0
IPv6	1108	5927	2162
IPX	527	538	581
AppleTalk	186	225	218
NetBIOS	19	22	19

Tabla 5.11 Protocolos capturados por Wireshark en media hora

Wireshark Datos	Equipo A 51672	Equipo B 45225	Equipo C 40249
IP	23155	22126	22287
ARP	9730	8197	8041
IPv4	0	0	0
IPv6	10478	7651	6502
IPX	1118	1048	2037
AppleTalk	438	378	357
NetBIOS	40	33	34

Tabla 5.12 Protocolos capturados por Wireshark por una hora

5.6 Protocolos capturados con ErPa

El analizador ErPa realiza las capturas hasta 10000 paquetes, este valor es capturado entre 10 y 15 minutos según el tráfico de red que se esté transmitiendo. De la misma forma que se realizó la captura con el analizador Observer y Wireshark, se utilizó tres equipos con diferentes características. Para cumplir con el diagrama de capturas se dejó a ErPa capturando por el intervalo de treinta minutos y una hora, aunque sabemos que la captura máxima es de 10000 paquetes, dejamos que capture e esos dos intervalos y es a continuación se muestran tablas que contienen los tipos y cantidad de protocolos capturados con el analizador licenciado ErPa.

En la tabla 5.13 observamos el tráfico capturado por media hora, de los protocolos que puede capturar ErPa. El equipo A capturo más paquetes ARP que los otros dos equipos, el equipo C capturo más paquetes IPv4 que los otros dos equipos. Y el equipo B capturo más protocolos IPv6 que los otros dos equipos.

Protocolos de Capa de Red			
ErPa Datos	**Equipo A 10000**	**Equipo B 10000**	**Equipo C 10000**
ARP	1830	3357	374
IPv4	5491	5560	9006
IPv6	2115	965	488
Otros	564	118	132

Tabla 5.13 Protocolos capturados de la capa de Red por media hora

Los protocolos de la capa de transporte que fueron capturados se muestran en la tabla 5.14 observamos que el equipo C capturo más paquetes TCP, el equipo A capturo más paquetes UDP y ICMP.

Protocolos de Capa de Transporte			
ErPa Datos	**Equipo A 10000**	**Equipo B 10000**	**Equipo C 10000**
TCP	9	0	7869
UDP	6979	6367	1498
ICMP	173	0	18
Otros	2839	3633	615

Tabla 5.14 Protocolos capturados de la capa de Transporte por media hora

Los protocolos capturados en la capa de aplicación son los que se muestran en la tabla 5.15. Esto se debe que en el momento de analizar el tráfico de red en el punto donde estábamos era muy cerca al enrutador.

Protocolos de Capa de Aplicación			
ErPa Datos	**Equipo A 10000**	**Equipo B 10000**	**Equipo C 10000**
HTTP	0	0	0
FTP	0	0	0
TELNET	0	0	0
SSH	0	0	0
Pop3	0	0	0
Otros	991	1000	213

Tabla 5.15 Protocolos capturados de la capa de aplicación por media hora

Luego dejamos que el analizador de red este capturando por una hora aun sabemos que el máximo de captura es de 10000 lo dejamos correr para ver qué pasaba y que capturaba. Los resultados fueron los siguientes el equipo B capturo más protocolos ARP con un total de 3343, con el protocolo IPv4 y IPv6 el equipo que más capturo fue el equipo C.

Protocolos de Capa de Red			
ErPa Datos	Equipo A 10000	Equipo B 10000	Equipo C 10000
ARP	1851	3343	1804
IPv4	5299	5147	5441
IPv6	2170	817	2232
Otros	680	693	523

Figura 5.16 Protocolos capturados de la capa de Red una hora

En la capa de transporte el equipo que realizo más capturas con el protocolo TCP fue el equipo A, con el protocolo UDP y ICMP el equipo que más capturas realizo fue el equipo C.

Protocolos de Capa de Transporte			
ErPa Datos	Equipo A 10000	Equipo B 10000	Equipo C 10000
TCP	626	0	134
UDP	6517	5820	7016
ICMP	50	0	121
Otros	2807	4180	2729

Figura 5.17 Protocolos capturados de la capa de transporte una hora

En la capa de Aplicación se observa que el único protocolo capturado es SMTP en el equipo A con el valor de 480, como se ve en la tabla de los paquetes capturados.

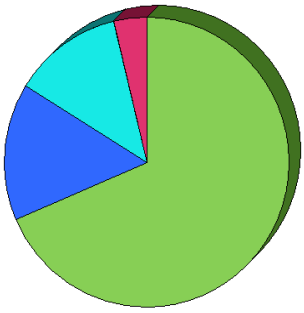
Protocolos de Capa de Aplicación			
ErPa Datos	Equipo A 10000	Equipo B 10000	Equipo C 10000
HTTP	0	0	0
FTP	0	0	0
TELNET	0	0	0
SSH	0	0	0
Pop3	0	0	0
SMTP	480	0	0
Otros	9520	10000	10000

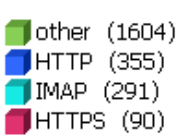
Figura 5.18 Protocolos capturados de la capa de aplicación una hora

5.7 Gráficos de pastel de los protocolos Capturados

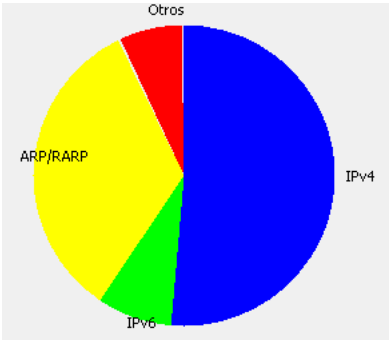
En los tres analizadores de trafico de red tienen manera de representar gráficamente los paquetes capturados, en el analizador Observer tiene una manera más detallada de como mostrar los datos por protocolos, en el analizador ErPa también pose graficas de los protocolos capturados pero de una manera más sencilla y los muestra por capas, capa de red, capa de transporte, capa de aplicación como se muestra en la figura 5.1. En cambio el analizador de tráfico de red Wireshark no tiene en sus funcionalidades gráficos de pie, los gráficos son de manera lineal y no son fáciles de interpretar la información que tienen.

Protocolo IP Capturados Observer





Varios Protocolos Capturados ErPa



	IPv4	IPv6	ARP/RARP	Otros
# Del Paquete	5147	817	3343	693
% Del Paquete	26	4	17	3
Total del Ta...	727646	154892	187728	59062
% Del Tam.	64	13	16	5

Figura 5.1 Gráficas pastel de los protocolos capturados por los analizadores

CONCLUSIONES

En los apartados siguientes se procede a mencionar las conclusiones y recomendaciones de la realización del presente proyecto de aplicación.

1. Se realizó con éxito la programación del analizador de tráfico de red ErPa, el cual puede generar graficas estadísticas acumulativas y continuas de los protocolos capturados de las siguientes capas: capa de enlace de datos, capa de red, capa de transporte, capa de aplicación.

2. ErPa es un analizador que puede ser usado por los estudiantes para entender el comportamiento de una red, ya que es sencillo en su estructura, sencillo al momento de realizar la captura, sencillo y agradable de interpretar el trafico que captura, ya que muestra cantidades exactas y las graficas de fácil entendimiento y comprensión.

3. ErPa cumple con las características principales de cualquier analizador tráfico de red sencillo, captura protocolos como Telnet, POP3, SHH, FTP, HTTP, SMTP, TCP y UDP. Que son los más comunes en la red.
4. Se observó que el tráfico de red capturado durante todo el proceso siempre se mantuvo, ya que los tres equipos estaban conectados a un

mismo punto mediante un conmutador D-Link a un punto directo del enrutador principal.

5. Se concluyó que para elegir el tipo de analizador de red debemos determinar el problema que tenemos, saber con cuanto detalle y cuán completo necesitamos el análisis y por supuesto instalar el analizador en el segmento de red que creemos tiene alguna falencia.

RECOMENDACIONES

1. Al momento de realizar la captura es preferible observar detenidamente la red y ver cuál es el punto correcto para analizar el comportamiento del tráfico en dicha red.

2. Todo tipo de red ya sea esta pequeña, mediana o grande, se recomienda que cada cierto tiempo analice su red, con un analizador de tráfico, debido a los posibles problemas que pudieran tener como por ejemplo IP duplicadas, el internet lento o detectar intrusiones en la red.

3. Para realizar una captura con un analizador de red cualquiera, el lugar preciso es en un conmutador, haciendo un espejo del puerto para luego capturar los paquetes con el analizador de redes.

ANEXO A

PROTOCOLO TCP/IP

El modelo TCP/IP se basa en la descripción de protocolos de red, en el cual se describe un conjunto de reglas de diseño e implementación de protocolos específicos para que un dispositivo pueda conectarse a una red.

El modelo TCP/IP y sus protocolos son administrados por la Internet Engineering Task Force (IETF) [22]

Como podemos observar en la figura el modelo se compone de 4 etapas jerarquizadas:

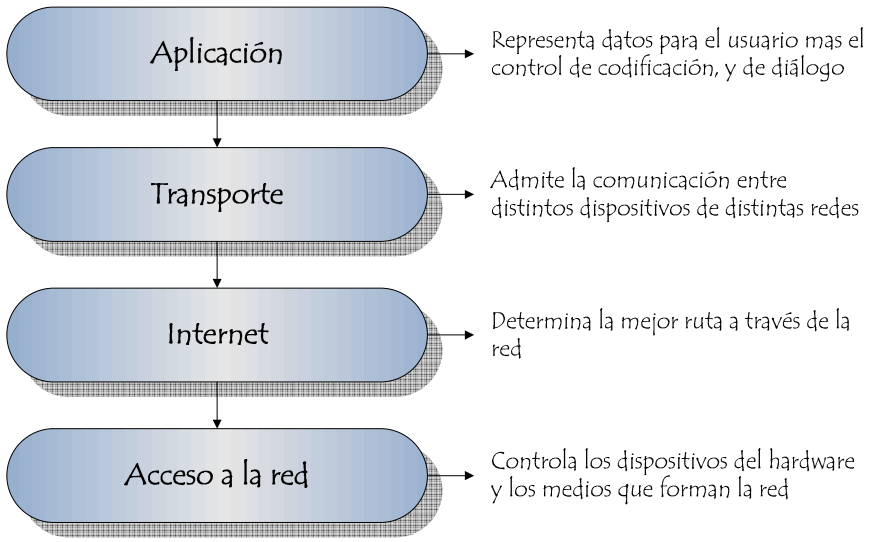


Figura A.1 Esquema de modelo TCP/IP

Capa de acceso a la red

También denominada acceso al medio, se encarga de transmitir la información por el medio y determinar cuál será el medio físico usado para

distribuir la información. Esta capa consta de una interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red especifica.

Ethernet es la interfaz LAN predominante en uso hoy en día [1].

Capa de Internet

Esta capa maneja la forma de comunicación entre una red y otra, se encarga de identificar el enrutamiento de paquetes entre una o más redes. Este nivel se encarga del direccionamiento lógico y determinación de ruta hasta el host final [22].

Entre los protocolos más importantes de la capa de Internet tenemos: Protocolo IP, Protocolo ARP, Protocolo ICMP, Protocolo RARP, Protocolo RARP.

Protocolo IP: Protocolo no orientado a conexión, usado en host de origen y destino. Este protocolo posee un servicio de envío no fiable, es decir tratara de enviar lo mejor posible un paquete sin garantizar nada sobre su recepción ya que el único mecanismo de seguridad que posee es un cheksum.El protocolo de internet IPv4 e IPv6 son los protocolos más usados [23].

Protocolo ARP: Adress Resolution Protocol, es el responsable de encontrar la dirección MAC que corresponde a una dirección IP. El proceso se realiza cuando se envía un paquete ARP a la broadcast MAC que tiene la dirección IP que se quiere encontrar, y así espera que una maquina responda con un ARP reply para terminar el proceso. El *protocolo RARP* realiza la operación inversa a la descrita anteriormente [23].

Protocolo ICMP: Internet Protocol Message Protocol, se utiliza para enviar mensajes de error, o notificaciones sobre si un host no está disponible o no puede ser alcanzado. Este protocolo puede ser verificado utilizando comandos ping y traceroute donde se envían mensajes de petición, visto a través de un analizador de redes [23.]

Capa de Transporte

Es la capa encargada del transporte de los datos que se encuentran en cada paquete del host origen hasta el host destino, independientemente de la red física que se esté usando para la transmisión. La capa de transporte posee dos protocolos el protocolo TCP y el UDP.

Protocolo TCP: Protocolo de control de transmisión, se utiliza para crear conexiones entre redes de computadoras en la cual se está garantizando que los datos serán entregados a su destinatario sin errores y en el mismo orden

que fueron transmitidos, además se tiene un mecanismo de distinción para las aplicaciones mediante los números de puertos TCP.

TCP provee de soporte a muchas aplicaciones tales como HTTP, SMTP, FTP, SSH [24].

Protocolo UDP: Este protocolo se basa en el intercambio de datagramas, permitiendo su envío sin que haya establecido previamente una conexión, ya que el datagrama contiene un direccionamiento en su cabecera. No posee mecanismos de confirmación ni de control, es decir no se puede tener la certeza de que los paquetes hayan llegado correctamente a su destino.

Se usan principalmente con otros protocolos como DHCP, BOOTP, DNS, así como para transmisión de multimedia en tiempo real, además poseen números de puertos así como en el TCP [24].

Capa de aplicación

La capa de aplicación del modelo TCP/IP incluye detalles de representación, codificación y control de diálogo. Esta capa se comunica con las demás mediante protocolos de la capa inferior es decir mediante TCP o UDP.

Existen varias aplicaciones en esta capa pero las más utilizadas radican en servicios de red o aplicaciones para que el usuario tenga interacción con un sistema operativo.

El usuario normalmente no interactúa directamente con la capa de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad que esta encierra. [22]

Entre los más comunes tenemos:

Protocolo FTP: Protocolo de transferencia de archivos, utilizado ampliamente para transferencia de información entre sistemas conectados a una red TCP, basado en una arquitectura cliente-servidor. Este protocolo utiliza normalmente el puerto de red 20 y el 21 [1].

Protocolo HTTP: HyperText Transfer Protocol por sus siglas en ingles, este protocolo define la sintaxis y los elementos de software de la arquitectura web para poder comunicarse entre un cliente y un servidor y permite las descargas de páginas web. Los navegadores son los encargados de interpretar los comandos para tener como resultado la pagina web que solicito el usuario [25].

Protocolo POP: Post Office Protocol, su función es almacenar el correo electrónico en un servidor remoto, un servidor POP. Existen 3 versiones de este protocolo el ultimo POP3 está diseñado únicamente para recibir correo y permite descargar el correo electrónico mientras se tiene conexión a internet para posteriormente revisarlo inclusive cuando se está desconectados [25].

La siguiente tabla resume los comandos de POP3 usados en ERPA:

Comando	**Función**
USER *usuario*	Identifica al usuario ante el servidor POP
PASS *contraseña*	Envía la contraseña al servidor POP

Tabla A.1: Comandos y funciones protocolo POP3

Protocolo SMTP: Simple Mail Transport Protocol, también se basa en el esquema cliente-servidor donde un los usuarios se comunican con los servidores en un protocolo basado en líneas de texto ASCII.

El formato del mensaje, encabezado y cuerpo está descrito en la RFC 822. Las versiones actualizadas son las RFC 2821 y RFC 2822 [25].

Comando	**Función**
HELO host	Identifica al host en SMTP
EHLO host	Identifica al host en ESMTP (SMTP ampliado)
MAIL FROM: dirección	Identifica en el sobre al remitente
RCPT TO: dirección	Identifica en el sobre al destinatario (puede haber varios)

Tabla A.2: Comandos y funciones protocolo SMTP

Protocolo SSH: Secure Shell, intérprete de órdenes seguras, sirve para acceder a hosts de manera remota a través de una red, además nos permite copiar datos, gestionar claves, y pasar datos de otras aplicaciones por medio de una red insegura, pero tunelizada mediante SSH.

La conexión se realiza con el comando:

ssh <nombre_servidor_ssh>

En la primera conexión se realiza un intercambio de claves encriptadas sobre el cual se pide la confirmación al usuario.

Protocolo TELNET: El programa telnet permite al usuario acceder a una maquina remota pero sin entorno grafico, es útil para arreglar fallos a distancia sin necesidad de estar físicamente cerca de la maquina a la que se quiere acceder.

Cabe recalcar que el uso de TELNET puede ser visualizado sin ningún problema por un analizador de paquetes ya que las contraseñas y también los usuarios se envían en un canal de datos no cifrado. [25]

Para iniciar una sesión TELNET se lo realiza de la siguiente manera en algún intérprete de comandos de otro ordenador:

telnet <nombre-máquina> <número-puerto>

ANEXO B

DIAGRAMA DE CLASES Y FORMATO DE LOS PAQUETES UTILIZADOS

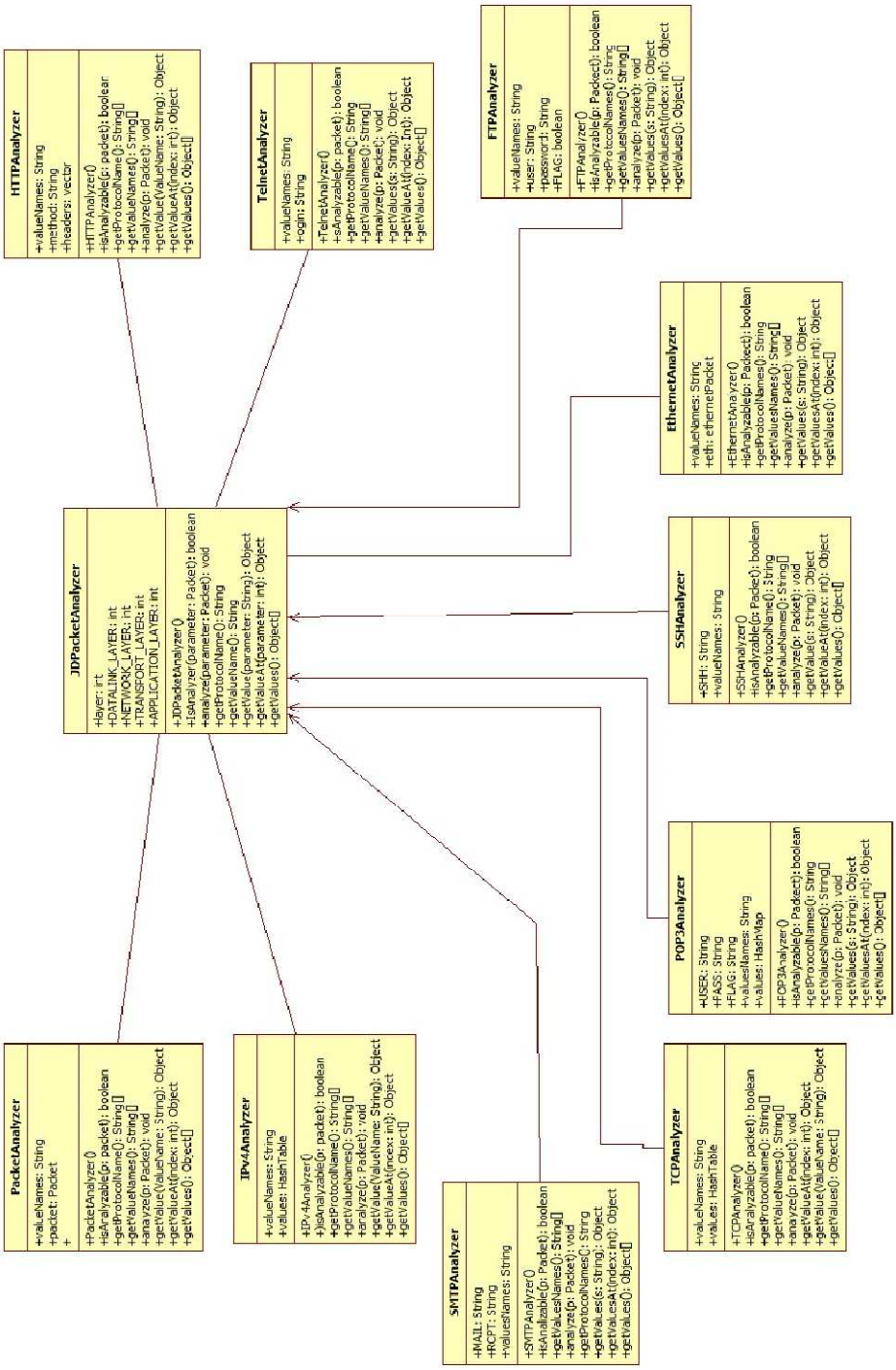
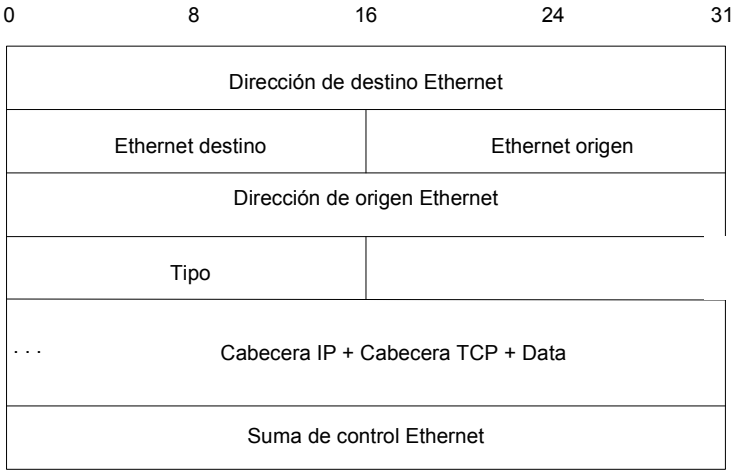
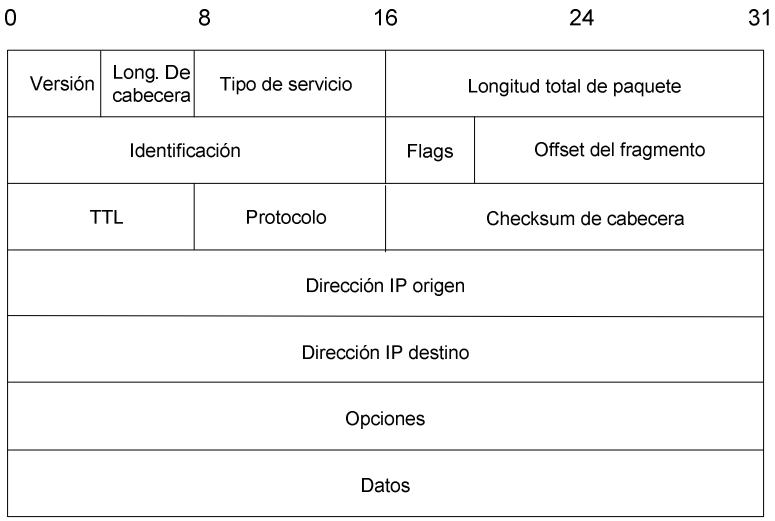


Figura B.1 Diagrama de clases de analizador ErPA

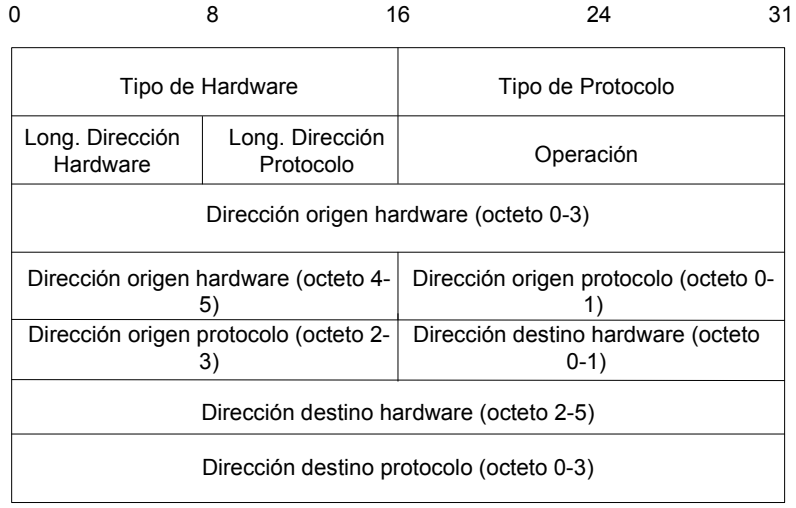
Formato del paquete Ethernet



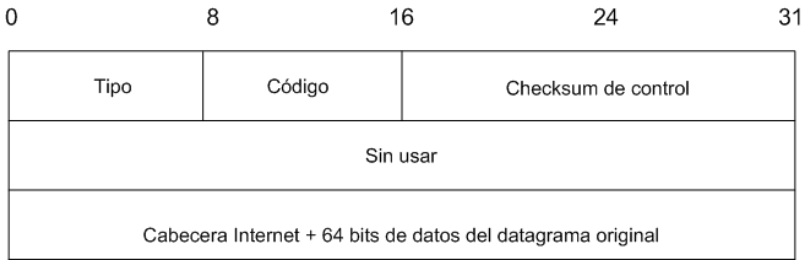
Formato del paquete IP



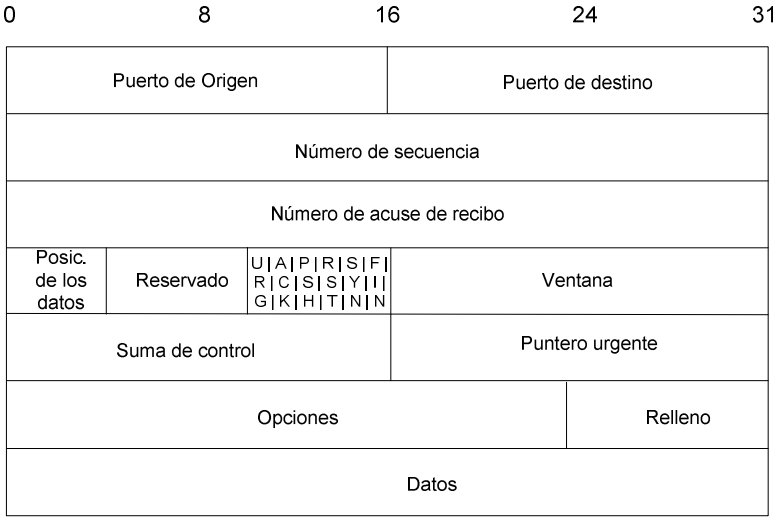
Formato de paquetes ARP/RARP



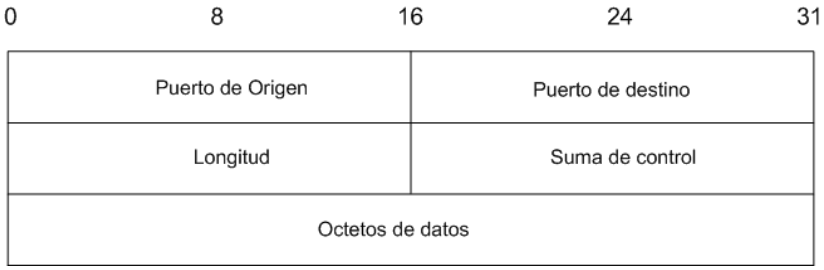
Formato de paquete ICMP



Formato de paquete TCP



Formato de paquete UDP



ANEXO C

HERRAMIENTAS DE DISEÑO E IMPLEMENTACIÓN

Entorno de Desarrollo Integrado

Un entorno de desarrollo integrado o también denominado IDE por sus siglas en inglés es un programa informático compuesto por un conjunto de herramientas de programación en donde puede dedicarse solo a un lenguaje de programación o bien a varios de ellos, en nuestro caso utilizamos lenguaje JAVA.

El IDE es un entorno de programación el cual consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráficas. [27]

Netbeans

Netbeans es un proyecto de código abierto con una comunidad de muchos usuarios y de constante crecimiento. La empresa Sun Microsystems fundó el proyecto de código abierto Netbeans en junio del año 2000.

Actualmente hay disponibles dos productos Netbeans IDE, Netbeans Plataform, amos productos son de código abierto y gratuito para uso tanto comercial como no comercial. [2]

En nuestro proyecto de Materia de Graduación usamos la plataforma NetBeans IDE en conjunto con el lenguaje de programación JAVA, para

desarrollar nuestro analizador de red cuyo nombre es ‘ERPA’, por las iniciales de nuestros nombres.

Netbeans IDE

Es un entorno de desarrollo, una herramienta para que los programadores puedan escribir, compilar, depurar y ejecutar programas. Está escrito en lenguaje Java, pero puede trabajar en cualquier otro lenguaje de programación. Existen además muchos módulos para extender el Netbeans IDE. Cabe recalcar que Netbeans IDE es un producto libre y gratuito sin restricciones de uso [2]

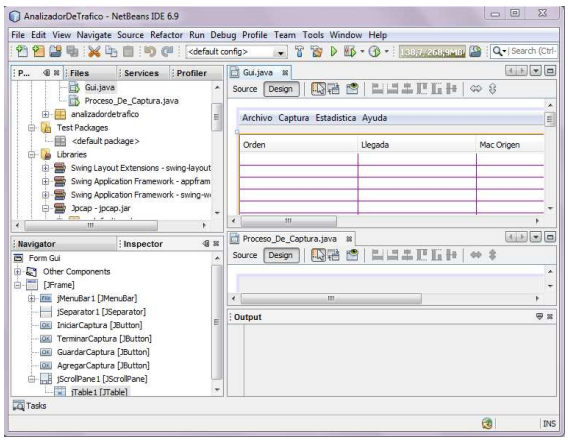


Figura C.1 Entorno gráfico de Netbeans IDE

Liberia JPCAP

Jpcap es una librería de código abierto para capturar y enviar paquetes de red en aplicaciones Java. Esta librería proporciona funciones como:

- Captura de paquetes en vivo.
- Guardar los paquetes capturados en un archivo para ser interpretados sin conexión a la red.
- Identificación de los tipos de paquetes y generación de objetos Java como por ejemplo Ethernet, IPv4, ARP/RARP, TCP, UDP.
- Filtrado de paquetes de acuerdo a las reglas especificadas por el usuario antes del envió a la aplicación.
- Envió de paquetes en bruto a la red.

Jpcap se basa en otras librerías como libpcap y winpcap, ha sido probado en diferentes sistemas operativos como Microsoft Windows (98/2000/XP/Vista), Linux (Fedora, Ubuntu), Mac OS X, Solaris.

Esta librería puede utilizarse para desarrollar muchas aplicaciones de red como por ejemplo:

- Analizadores de red y protocolo
- Monitores de red
- Logs de trafico
- Generadores de trafico
- Sistema de detección de intrusos en la red.
- Escáner de redes.
- Herramienta de seguridad.

Para nuestro proyecto utilizamos las funcionalidades de la librería Jpcap, como:

Obtener la lista de interfaces de redes mediante el método JpcapCaptor,getDeviceList() el cual devuelve una matriz de objetos NetworkInterface donde se muestra información sobre la interfaz de red correspondiente, como nombre, direcciones IP y MAC.

Abrir la interfaz de red, una vez elegida la lista de interfaces de red se elige la captura de paquetes de esa interfaz de red mediante el métodos JpcapCaptor.openDevice() mediante el cual se puede elegir la forma de realizar la captura en modo promiscuo, tiempo de espera entre capturas, número máximo de bytes a capturar.

Capturar los paquetes de la interface de red, una vez abierta la interfaz de red en el modo deseado se obtienen los paquetes por el método JpcapCaptor por medio de devolución de llamada o capturando paquetes de uno a uno.

Definir filtros para captura, se pueden también establecer filtros para que Jpcap no capture cierto tipos de paquetes como ICMP, POP3, etc

Guardar y leer una captura mediante los métodos JpcapWriter.openDumpFile() y JpcapCaptor.openFile(), los cuales permiten

grabar en vivo los paquetes para luego ser analizados sin estar conectados a la red [28].

Winpcap

WinPcap es una librería de código abierto para el análisis de red y captura de paquetes para las plataformas Win32.

El propósito de WinPcap es dar este tipo de acceso a las aplicaciones Win32; y proporciona facilidades para:

- Capturar paquetes en bruto.
- Filtrar los paquetes de acuerdo a las reglas especificadas por el usuario
- Transmitir paquetes a la red
- Recopilar información estadística sobre el tráfico de red. [16]

Winpcap en nuestro proyecto sirve además para la monitorización del tráfico de red, es necesaria esta librería para el funcionamiento de ERPA.

El que Winpcap sea un programa con la categoría software freeware hace que esta librería sea ampliamente utilizada en aplicaciones comerciales con compatibilidad de múltiples sistemas operativos.

El usuario final solo requiere instalar un ejecutable para que el programa quede en el sistema operativo y poder usarlo con demás aplicaciones.

Figura C.2 Ejecutable de la instalación Winpcap

ANEXO D

MANUAL DEL USUARIO

Requerimientos Mínimos

Para la ejecución del analizador de redes ErPa hemos utilizado una máquina Intel ® Pentium ® 4, procesador de 2.80 GHz, 1Gb de memoria RAM, con sistema operativo Microsoft Windows XP Profesional, versión 2002, Service Pack3.

Además necesitamos tener instaladas las librerías Winpcap, Jpcap, y JRE 6 de las cuales hablamos en el Anexo D.

ErPa ha sido probado en sistema operativo Windows XP SP3/Windows 7 32 bits y debe ser ejecutado con permisos de administrador, junto con JRE 6 o superior.

Instalación

Cuando las librerías mencionadas ya estén instaladas, procedemos a abrir la aplicación que se encuentra en una carpeta comprimida la cual se va a distribuir, dentro de esta carpeta se encuentra una aplicación tipo .jar con el nombre ErPa Analizador de Red, el cual se hace doble clic y la aplicación comienza a correr.

Una vez ejecutado el programa se visualizará la pantalla principal del analizador de tráfico de red ErPa, el cual posee un entorno, donde el usuario puede interactuar con un menú contextual y sus opciones se resumen en la tabla E.1.

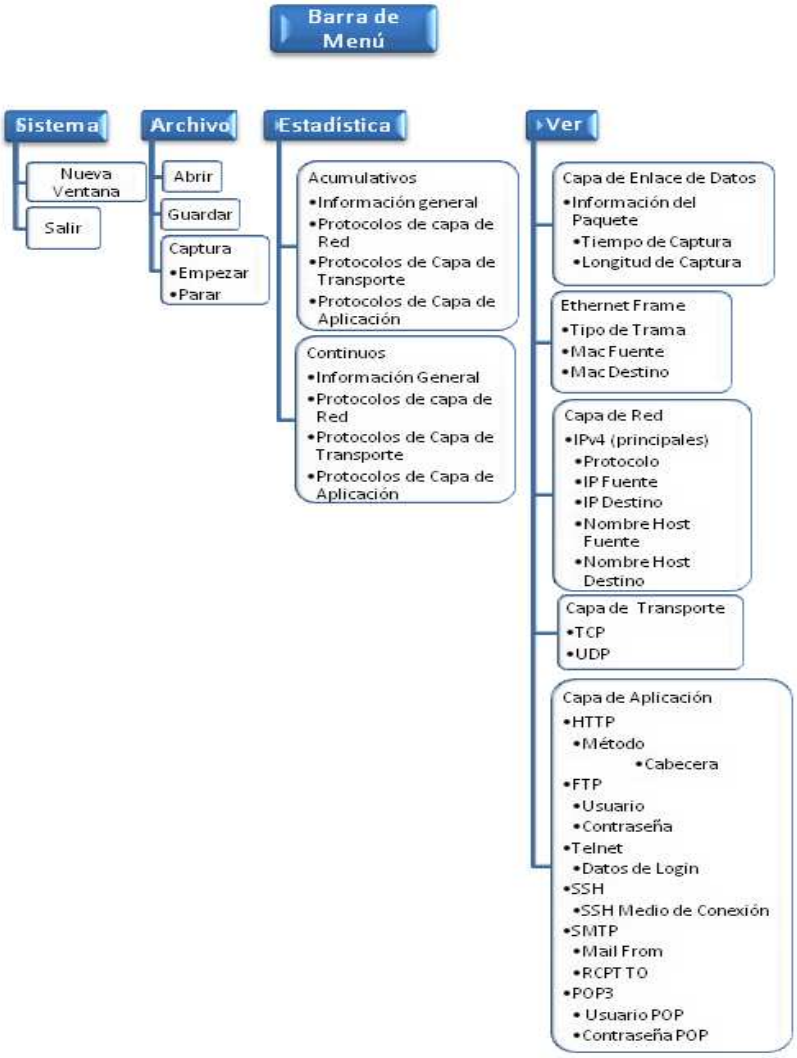


Tabla D.1. Barra de Menú del Analizador ErPa

Iniciar una nueva Captura

Para Iniciar la captura con el analizador de trafico de red ErPa, activamos la opción del menú “Capturar > Empezar”, como se muestra en la gráfica D.1

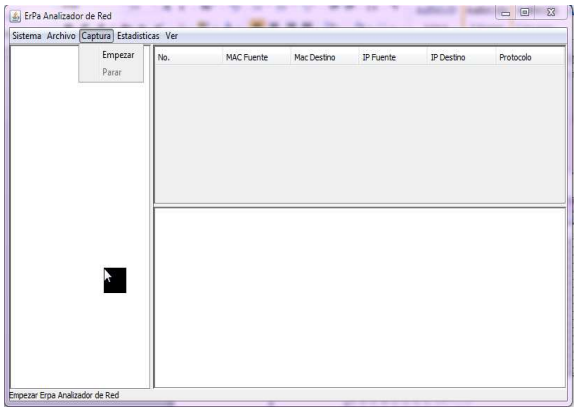


Figura D.1 Imagen de la ventana principal

Después de haber hecho clic en “Empezar” se despliega una nueva ventana en la cual se escoge el dispositivo de captura y demás opciones. En dispositivos se escoge la tarjeta de red que deseamos escanear ya que se puede tener más de una en el computador y entre las opciones de captura se pueden filtrar los paquetes por protocolo específico como por ejemplo que solo capture el protocolo POP3.

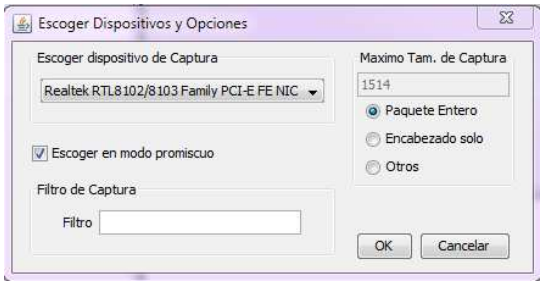


Figura D.2 Pantalla para escoger dispositivos y Opciones de Captura

También se procede a seleccionar la opción de modo promiscuo que se trató en el capítulo 2 en este documento. Se selecciona el tamaño máximo de longitud del paquete, en la cual se puede escoger de tres opciones, Paquete Entero, Encabezado Solo, y Otros como se puede observar en la figura 5.2. La longitud del paquete se puede variar entre 68 y 1514 bytes, se hace clic en “OK” y se comienza con la captura.

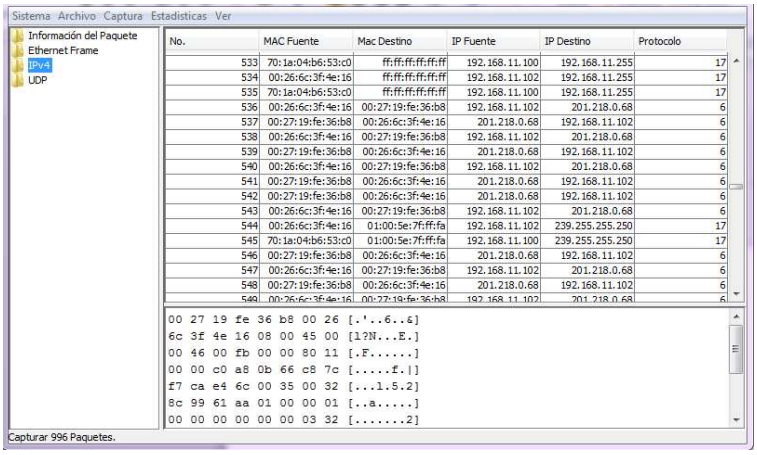


Figura D.3 Entorno gráfico de la captura

Guardar una Captura

Para guardar la captura en un fichero en el analizador de trafico de red ErPa, primero se debe realizar una captura, después se activa la opción del menú “Archivo > Guardar”.

Luego de esto aparece una ventana de diálogo donde se puede escoger la ubicación y el nombre del fichero a guardar.

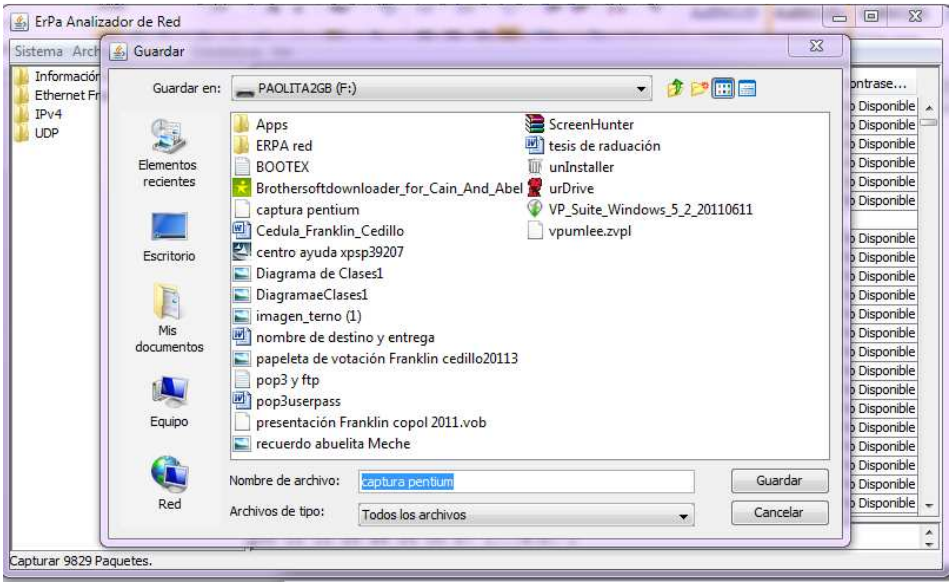


Figura D.4 Ventana para guardar captura

Abrir una Captura Previa

Para poder abrir una captura ya grabada, se activa la opción del menú “Archivo > Abrir”, luego aparece una ventana de diálogo, donde se puede escoger el fichero que queremos cargar en el analizador de tráfico de red ErPa.

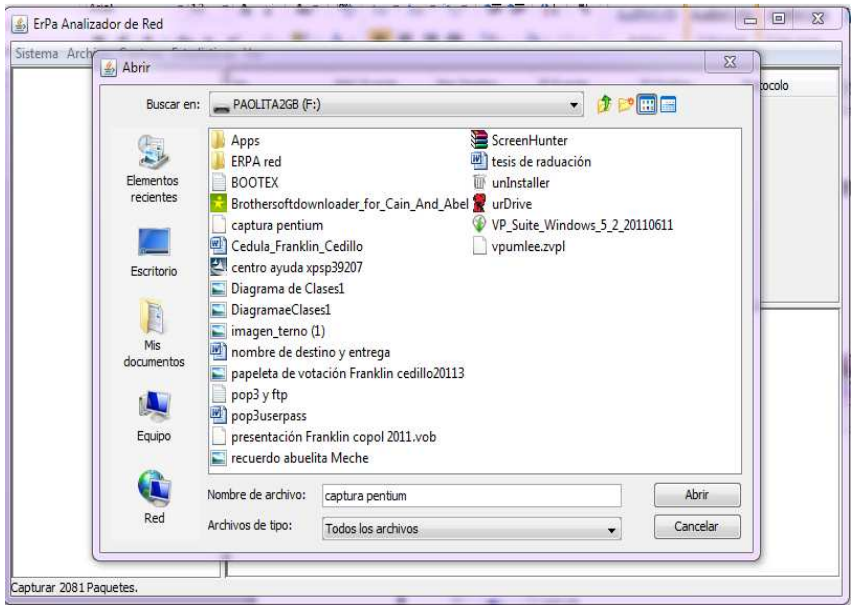


Figura D.5 Ventana mostrada para abrir una captura

Si el fichero no puede ser abierto por la aplicación se visualiza un mensaje de error en forma de ventana donde se informa al usuario que no puede abrir la captura hecha con anterioridad y muestra el siguiente mensaje "No se puede Abrir el Archivo <nombre del archivo>".

Figura D.6 Mensaje error al abrir el fichero

Mostrar Cuadros Estadísticos

Para mostrar las estadísticas de las diferentes capturas que realiza ErPa, nos dirigimos al menú “Estadísticas” en el cual tiene dos opciones de como mostrar los datos, estas pueden ser de forma acumulativa y de forma continua. Las gráficas estadísticas generadas nos ayudan a entender el comportamiento de la red y a conocer de una manera más precisa que protocolo, es más usado en la red por los usuarios y así poder mejorar el rendimiento de la red realizando los correctivos necesarios.

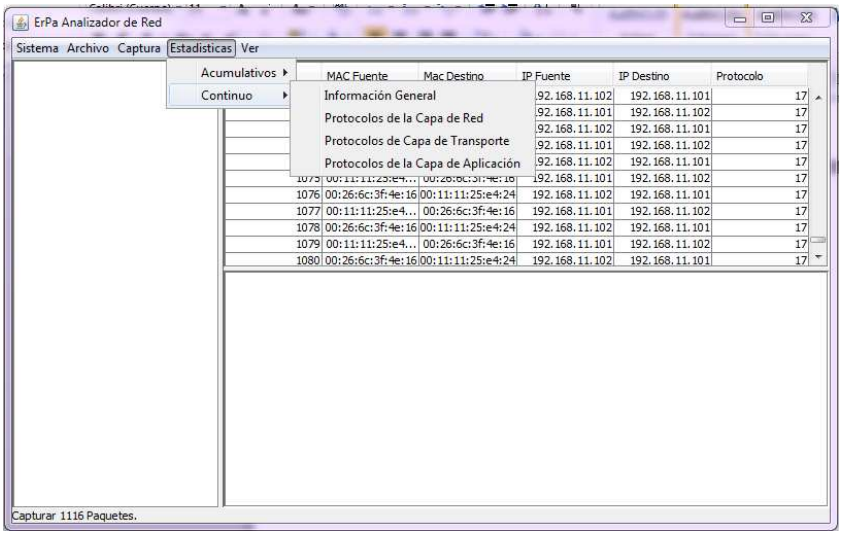


Figura D.7 Imagen del menú Estadísticas

En ambas opciones se encuentra información general, protocolos de capa de red, protocolos de capa de transporte, protocolos de capa de aplicación. La diferencia radica en la manera de como son presentados los datos.

En la opción “Información general” se muestra la cantidad de paquetes, la suma total de la longitud de los paquetes y la longitud media de los paquetes capturados.

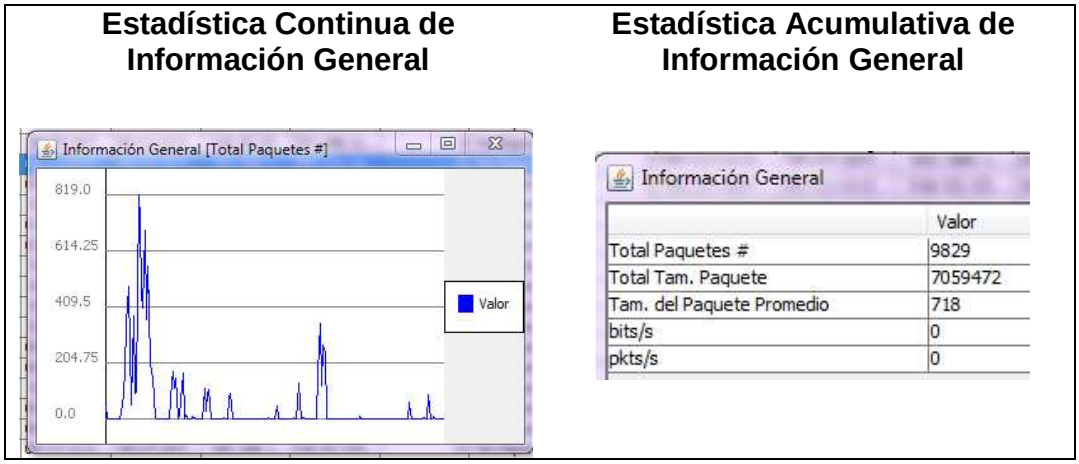
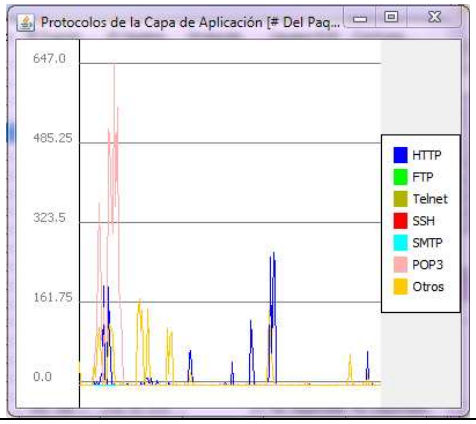


Figura D.8 Ventanas de Información General de ErPa

En la opción “Capa de aplicación” se visualiza una gráfica con la cantidad y porcentaje de los protocolos en este nivel. Con esta gráfica podemos darnos cuenta que tipo de protocolo es más concurrido por el usuario de la red y realizar el respectivo análisis.

Los protocolos que captura ErPa, en capa de aplicación son: POP3, SMTP, Telnet, FTP, HTTP, SSH y los demás protocolos existentes los reconoce como otros.

Estadística Continua de los protocolos de la capa de aplicación.



Estadística Acumulativa de los protocolos de la capa de aplicación.

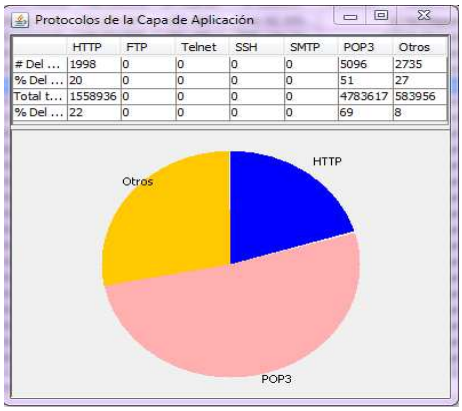


Figura D.9 Ventana de la capa de aplicación

Mostrar forma de presentación de los datos capturados

Para poder visualizar el contenido de los paquetes en el analizador de trafico ErPa nos dirigimos a la opción del menú “VER” allí aparecerán las capas de todos los protocolos para que el usuario pueda escoger que tipo de capa de red desea que se muestre para su debido análisis.

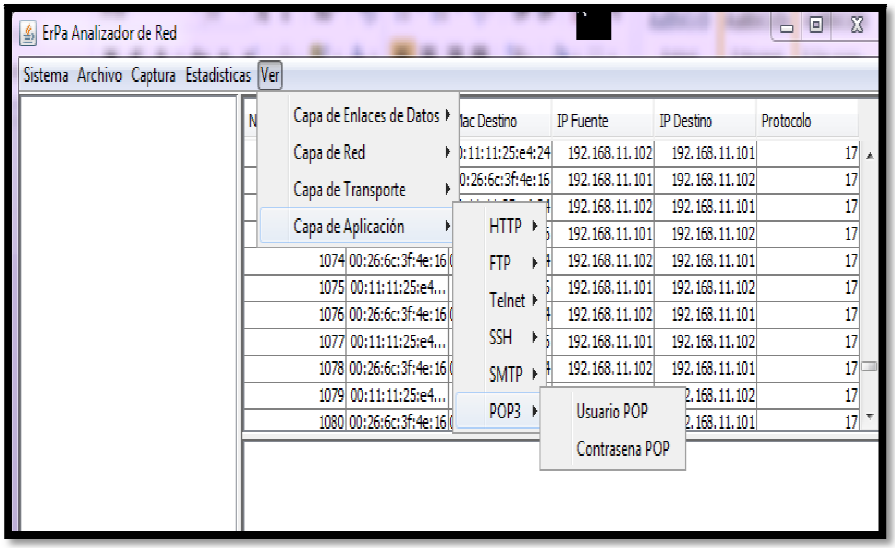


Figura D.10 Barra de la opción del Menú Ver

ANEXO E

CAPTURA DE RED POR MÁS TRES HORAS

Captura del tráfico de red la empresa por un intervalo de 3 horas

Esta captura se realizó por tres horas con cuarenta minutos, en el equipo A con el analizador observer el día A, lo que se capturo fue 95160 paquetes, protocolo IP 45675, son los protocolos más capturados en esta muestra.

Captura desde las 15:40 hasta 19:30

Observer	Equipo A
IP	45675
La ARP	18259
IPv6	6168
IPX	3533
Apple Talk	1338
NetBIOS	123
Otros	

Tabla E.1 Protocolos Capturados por Observer

Observer	Tamaño de Captura
Equipo A	**95160**

Tabla E.2 Tamaño captura Observer en equipo A

Con el equipo B se tomó una muestra seis horas de Captura, en día A, con el software Observer, se capturo 125060 paquetes capturados y el protocolo con más capturas fue el IP con 57649

Captura 15:41 hasta 21:38

Observer	Equipo B
IP	57946
ARP	23184

IPv6	7300
IPX	5455
Apple Talk	2043
NetBIOS	186
Otros	7508

Tabla E.3 Protocolos Capturados por Observer en equipo B

Observer	**Tamaño de Captura**
Equipo B	**125060**

Tabla E.4 Protocolos Capturados por Observer en equipo B

Con el analizador de red Wireshark se Capturo el día B con el equipo B la cantidad de 141877 paquetes, el protocolo más Capturado fue IP con 76051, observar tabla

Captura 17:05 hasta 08:14

Wireshark	**Equipo B**
IP	76051
ARP	22630
IPv6	6685
IPX	14180
Apple Talk	5193
NetBIOS	478
Otros	16660

Tabla E.5 Protocolos Capturados por Wireshark en equipo B

Observer	**Tamaño de Captura**
Equipo B	**141877**

Tabla E.6 Protocolos Capturados por Wireshark en equipo B

BIBLIOGRAFÍA

[1] Cisco Networking Academy <CCNA Exploration 4.0: Aspectos Básicos del Networking> 2007-2008; Última Revisión: Mayo 2011

[2] Cisco Networking Academy <CCNA Exploration 4.0: WAN > 2007-2008; Última Revisión: Abril 2011

[3] Análisis de patrones de tráfico de red; Mayo 2011, Cruz Edmanuel, Díaz; < http://www.slideshare.net/chichoAnitec/sniffer-7740876>; Última Revisión: Julio 2011

[4] Ingeniería Social; 20 febrero 2010; Escobar Iris, López María;< http://es.scribd.com/doc/52565118/Ingenieria-Social>; Última Revisión: Junio 2011

[5] Wikipedia: Categoría redes informáticas; Junio 2011; Analizador de paquetes; <http://es.wikipedia.org/wiki/Sniffer>; >; Última Revisión: Junio 2011

[6] El blog de Xosef; 23 Septiembre del 2009 Criterio del funcionamiento de un sniffer**;** < http://xosef.obolog.com/criterio-funcionamiento-sniffer-cain-abel-344139>; >; Última Revisión: Mayo 2011

[7] Aprendaredes.com; 2010-2011; Artículo de redes – Networking; < http://www.aprendaredes.com/dev/articulos/aprende-a-mirar-dentro-de-la-red-con-un-sniffer.htm>; Última Revisión: Mayo 2011

[8] Wikipedia Categoría Redes Informáticas; 23 Junio 2010; Tipos de Sniffer TCPDUMP;
< http://es.wikipedia.org/wiki/Tipos_de_Sniffer>; Última Revisión: Junio 2011

[9] Wikipedia categoría: Redes|Sniffers; 30 marzo 2010; Darkstat;
< http://es.wikipedia.org/wiki/Darkstat >; Última Revisión: Junio 2011

[10] OverBlog Mirelucx; 9 marzo 2009; Sniffer – El Blog de Luz; < http://mirelucx.over-blog.com/article-28809768.html>; Última Revisión: Junio 2011

[11] Wikipedia categoría: Redes|Sniffers; 20 abril 2011; Snort - Wikipedia;
< http://es.wikipedia.org/wiki/Snort>; Última Revisión: Junio 2011

[12] Noticias Darkub; 19 mayo 2008; Tipos de Sniffers;
< http://darkub.wordpress.com/2008/05/19/tipos-de-sniffer/>; Última Revisión: Junio 2011

[13] Insecure.org; Enero 2010; Las 75 Herramientas de Seguridad Más Usadas; < http://insecure.org/tools/tools-es.html>; Última Revisión: Junio 2011

[14] El hacker.net; 24 Mayo 2010; Introducción al ETTERCAP;

<http://foro.elhacker.net/wireless_en_linux/introduccion_al_ettercap_obtener_contrasenas_etc-t294519.0.html>; Última Revisión: Junio 2011

[15] WebAyunate; 23 Agosto 2010; El oscuro arte del sniffing; Facundo de la Cruz; < http://www.webayunate.com/sniffing-facundo-de-la-cruz/>**;** Última Revisión: Abril 2011

[16] WinPcap; 2010; support and documentation <http://www.winpcap.org>; Última Revisión: Junio 2011

[17] Especialistas en integración de nuevas tecnologías; 2006; El análisis y monitoreo de las redes hoy en día;
< http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html>; Última Revisión: Mayo 2011

[18] Wikipedia categoría: Redes|Sniffers; 14 junio 2011; Wireshark - Wikipedia; <http://es.wikipedia.org/wiki/Wireshark >; Última Revisión: Junio 2011

[19] TSD; Total Service Desk; Observer; < http://www.tsd.com.mx/observer.htm>; Última Revisión: Mayo 2011

[20] Gurú de la Informática; Wireshark analizador de protocolos; < khttp://vtroger.blogspot.com/2007/02/wireshark-analizador-de-protocolos.html >; Última Revisión: Mayo 2011

[21] Wireshark; Stephenfisher; 12 de junio del 2011; knownBugs/OUTOFMemory; < http://wiki.wireshark.org/KnownBugs/OutOfMemory>; Última Revisión: Mayo 2011

[22] Wikipedia Categoría Redes Informáticas | Protocolos; 15 de junio del 2011; Modelo TCP/IP; <http://es.wikipedia.org/wiki/Modelo_TCP/IP>; Última Revisión: Marzo 2011

[23] Wikipedia Categoría Protocolos de Internet | Protocolos de nivel de red; 12 de abril del 2011;
<http://es.wikipedia.org/wiki/Categor%C3%ADa:Protocolos_de_nivel_de_red>; Última Revisión: Marzo 2011

[24] Categoría Protocolos de internet | Protocolos de nivel de transporte; <http://es.wikipedia.org/wiki/Categor%C3%ADa:Protocolos_de_nivel_de_transporte >;Última revisión: Marzo 2011

[25] Redes de Datos, Instructivo Laboratorio 1; Curso 20100 Montevideo-Uruguay; <http://iie.fing.edu.uy/cursos>; Última Revisión: Marzo 2011

[26] Categoría; Entorno de desarrollo integrado; 2009-2011; < http://es.wikipedia.org/wiki/Entorno_de_desarrollo_integrado>; Última Revisión: Marzo 2011

[27] Netbeans.org, Portal del IDE Java de Código Abierto; Netbeans; 2011; < http://netbeans.org/index_es.html>; Última revisión: Marzo 2011

[28] Jpcap Tutorial; Autor: Keita Fujii; 2007; http://netresearch.ics.uci.edu/kfujii/Jpcap/doc/tutorial/; Última revisión: Marzo 2011