UNIVERSIDAD DEL AZUAY
FACULTAD DE CIENCIAS DE LA ADMINISTRACION
ESCUELA DE INGENIERIA DE SISTEMAS

TESIS PREVIA A LA
OBTENSIÓN DEL TÍTULO DE
INGENIERO DE SISTEMAS

TEMA

"ANÁLISIS E INTERPRETACIÓN DE PAQUETES IP QUE CIRCULAN POR UNA RED ETHERNET"

AUTOR: HERNAN QUITO B. - hernanquito@hotmail.com

DIRECTOR: ING. FERNANDO BALAREZO

CUENCA – ECUADOR

2004

Dedicatoria.

A Elsa mi paciente esposa, que por mucho tiempo ha soportado los inconvenientes de tener un universitario en casa, y me apoya en mis más tenaces proyectos e ideales

A mis pequeños niños, que con esfuerzo han comenzado y están por comenzar su vida de preparación

A mis padres, que apostaron por mi y me inculcaron valores que hoy guían mi vida.

Agradecimientos

A todos los profesores de la universidad del Azuay que me han brindado más que solo sus conocimientos.

A los profesores de la Universidad de Buenos Aires, que con mucha dedicación y empeño me enseñaron que se puede llegar muy lejos

A los miembros del programa de postgrado de la Universidad de Buenos Aires y a todos quienes hicieron posible que el mismo se llevara a cabo con éxito.

Y finalmente, pero no menos importante a mis amigos por haberme brindado su amistad, y apoyarme continuamente con sus experiencias y conocimientos.

Responsabilidad

Los criterios vertidos en el desarrollo de esta labor investigativa son de exclusiva responsabilidad del autor

CONTENIDO

Pág.

INTRODUCCION **1**

1. FUNDAMENTOS TEORICOS **3**

1.1 Redes de computadoras **3**

1.1.1 Generalidades: 3
1.1.2 Redes Ethernet 4
1.2 Protocolos **5**

1.2.1 Introducción 5
1.2.2 Arquitectura TCP/IP 5
1.2.3 Protocolo IP (Internet Protocol) 7
1.2.3.1 Introducción 7
1.2.3.2 La cabecera IP 8
1.2.4 TCP (Transmission Control Protocol) 8
1.2.4.1 Características 8
1.2.4.2 Estructura de TCP 9
Conclusiones del capítulo 1. 9
2. HERRAMIENTAS DEL ADMINISTRADOR DE LA RED **10**

2.1 Herramientas de diagnóstico de conectividad **10**

2.1.1 Introducción 10
2.1.2 Ping 11
2.1.3 Nslookup 11
2.1.4 Dig 11
2.1.5 Tracert 11
2.1.6 Netstat 12
2.1.7 Ifconfig 12
2.1.8 Mensajes De Error frecuentes 12
2.2 Herramientas de captura y Análisis de datos **13**

2.2.1 Introducción 13
2.2.2 Analizadores de protocolos o Sniffers 14
2.2.2.1 Tcpdump 14
2.2.2.2 Monitor de red de Windows 15
2.2.2.3 Ethereal 15
2.2.2.4 Distinct Network Monitor 16
2.2.2.5 Optiview protocol expert 16
Conclusiones del capítulo 2. 17
3 PLANIFICACIÓN, DISEÑO, SELECCIÓN DE ESCENARIOS Y PRUEBAS DE LOS TRABAJOS PRÁCTICOS **18**

3.1 Introducción 18
3.2 Trabajo Práctico 1 - PING 20
3.3 Trabajo Práctico 2 - TRACERT 22
3.4 Trabajo Práctico 3 - NSLOOKUP 24
3.5 Trabajo Práctico 4 - DIG 26
3.6 Trabajo Práctico 5 – email 28
3.7 Trabajo Práctico 6 - WEB 30
Conclusiones del capítulo 3: 31
4 MONTAJE DE LA RED **33**

4.1 Introducción **33**

4.2 Instalación de Linux. **34**

4.3 Instalación del servidor Proxy **35**

4.4 Configuración de los clientes de Internet **35**

4.5 Instalando las herramientas de captura **36**

Conclusiones del capítulo 4: 37

5 CAPTURA Y ANALISIS DE LOS DATOS 38

5.1 Introducción **38**

5.2 Desarrollo del Trabajo Práctico 1 - PING **39**

5.3 Desarrollo del Trabajo Práctico 2 - TRACERT **48**

5.4 Desarrollo del Trabajo Práctico 3 - NSLOOKUP **55**

5.5 Desarrollo del Trabajo Práctico 4 - DIG **64**

5.6 Desarrollo del Trabajo Práctico 5 - email **69**

5.7 Desarrollo del Trabajo Práctico 6 - WEB **80**

Conclusiones del capitulo 5: 90

CONCLUSIONES GENERALES 91

RECOMENDACIONES 92

BIBLIOGRAFÍA 93

ANEXOS 95

GLOSARIO DE TÉRMINOS 96

APROBACIÓN Y DISEÑO DE TESIS 101

RESUMEN EJECUTIVO

Tema de la Monografía:

ANÁLISIS E INTERPRETACIÓN DE PAQUETES IP QUE CIRCULAN POR UNA RED ETHERNET

Autor: Hernán Quito (hernanquito@hotmail.com)

Esta monografía consiste en definir procedimientos y condiciones enfocadas a introducirnos al tema del análisis de tráfico IP sobre redes Ethernet; para que ello resulte posible, se desarrolla una introducción teórica del funcionamiento de la arquitectura TCP/IP, se identifican además algunas de las herramientas necesarias para desencadenar tráfico en la red y también herramientas que permiten capturar dicho tráfico y efectuar un análisis sobre estos datos capturados.

Basándose en informes y recomendaciones de docentes de la materia Redes de comunicaciones dictada en la Universidad de Buenos Aires, se diseñan hojas de trabajo con escenarios que simulan condiciones a las que una red de computadoras normal podría estar sometida, considerando que se debe iniciar con capturas de tráfico sencillo para que la comprensión sobre el tema de análisis se desarrolle de lo simple hacia lo complejo.

Esta monografía también abarca la instalación y configuración de una red con múltiples sistemas operativos (Windows y Linux), conectados a Internet, de tal manera que las pruebas diseñadas puedan ser realizadas a cabalidad.

Para el análisis del tráfico propiamente dicho se utiliza un Analizador de protocolos que nos permite ver la información de un modo fácil de asociar con los conceptos teóricos, haciendo un estudio también con analizadores más avanzados que permiten la visualización gráfica y resumida de los datos capturados.

INTRODUCCION

Actualmente la comunicación es esencial para todas las personas, por esta razón, el permanecer conectados compartiendo información ya sea en forma interna, en el caso de las redes LAN o externa, comúnmente dada por el uso del Internet, se ha vuelto lo más normal; y cuando se trata de manejo de datos, el que éstos estén disponibles y a una velocidad razonable, es extremadamente importante. Todo esto conlleva a que sea necesario que se conozcan y se usen herramientas para poder diagnosticar el funcionamiento de la red o la falla, de tal manera que se pueda implementar una solución rápidamente y con conocimiento de causa.

Es en este marco en el que se desarrolla el presente tema de análisis de tráfico de paquetes que contienen datagramas IP, que tiene por finalidad servir de referencia para que quienes lo lean puedan realizar pruebas que permitan clarificar la teoría sobre el funcionamiento de la comunicación en las redes de computadoras y junto con el uso de las herramientas aquí descritas, pueda además incrementar sus habilidades de diagnóstico y solución de ser el caso, en problemas de las redes antes mencionadas; por tal razón empezaremos el primer capítulo con una breve introducción hacia las redes de computadoras, continuando con la explicación del protocolo IP, que actualmente va de la mano con el protocolo TCP.

En el segundo capítulo se tratará el tema de las herramientas de diagnóstico de conectividad que se encuentran disponibles en algunos sistemas operativos, asimismo se

trata el tema de las herramientas que se usan para capturar la información que fluye por la red y por supuesto las que permiten realizar el análisis.

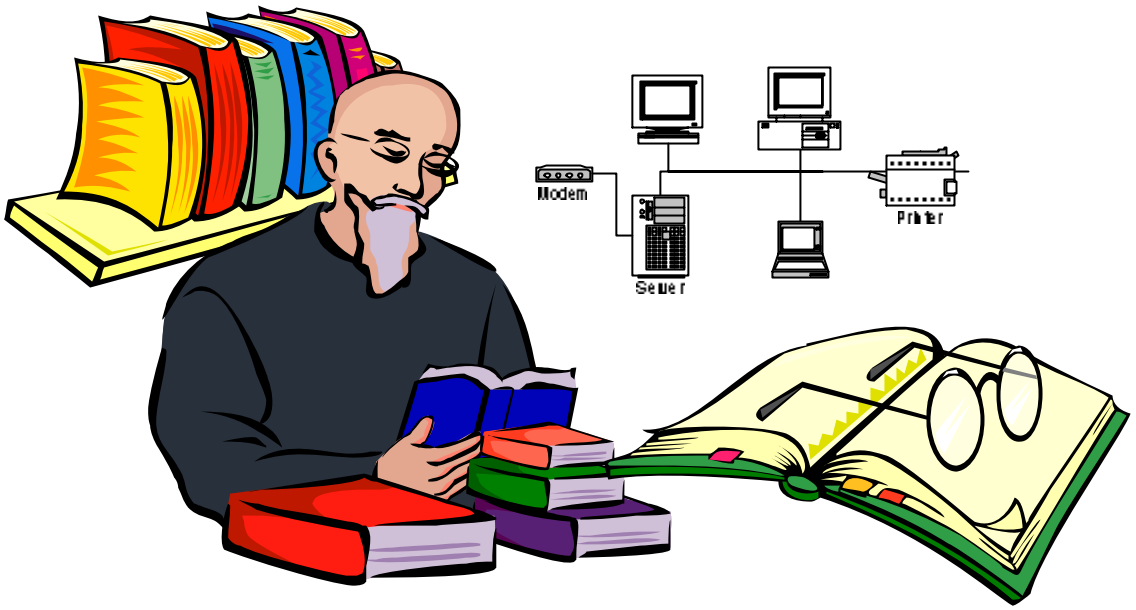
En el tercer capítulo se abordará el diseño y planificación necesarios para realizar los trabajos prácticos, materia de nuestro estudio. Es pues aquí en donde se delinean las situaciones más didácticas que se podrían presentar, para que se pueda de una manera sencilla introducir al tema del análisis de datos. Cabe anotar que se utilizó como modelo inicial para realizar este capítulo, las recomendaciones y estructuras de informes explicadas por los Ing. Marcelo Utard e Ing. Pablo Ronco, docentes de la Universidad de Buenos Aires en Argentina, que propusieron y apoyaron el desarrollo del presente tema.

En el capítulo cuarto se hace un seguimiento a la instalación de servicios necesarios en los sistemas operativos que se usan como base de nuestras pruebas, pues al ser pruebas controladas, es necesario que sepamos cómo y que transportamos por la red, para poder relacionar con la información que se captura.

El capitulo final se centra en la captura de la datos en la red, la interpretación y el análisis que permitirá obtener información muy valiosa, y que cumplirá con la misión de clarificar el funcionamiento de la comunicación en las redes de una manera visual, a la luz de los conceptos teóricos.

CAPITULO 1

FUNDAMENTOS TEÓRICOS



1.1 REDES DE COMPUTADORAS

1.1.1 Generalidades:

Cuando el uso de las computadoras se expandió por el mundo empresarial, se vio la necesidad de unir varios terminales para poder trabajar sobre una información común, esto inicialmente se lo realizaba mediante el uso de un mainframe y terminales tontos conectados a tal poderoso computador abarcando una área reducida.

Stalling sostiene que se produce un cambio drástico en las tecnologías cuando se unieron los campos de las computadoras y los de los sistemas de comunicaciones. "El objetivo principal de un sistema de comunicaciones es intercambiar información entre dos entidades" (Stallings:2000, 4). Esto produce un avance impresionante en la estructura de las redes actuales, que ya no se limitan en cuanto a la distancia entre terminales, pudiendo ahora estar incluso en diversos continentes sin mayor problema.

En la figura 1, se ejemplifica la comunicación entre una estación de trabajo y un servidor de archivos ubicado en una localidad remota a través de la red telefónica pública, como lo que comúnmente ocurre en nuestro medio con la conexión a Internet

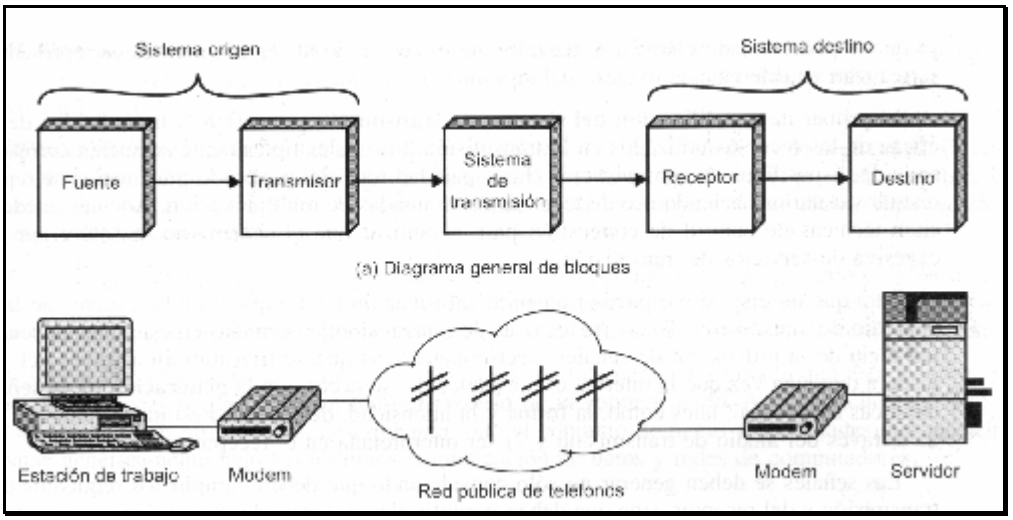


Figura 1. Modelo simple de comunicaciones.

1.1.2 Redes Ethernet.

Las redes locales *Ethernet* son posiblemente la tecnología que domina en tiempos de Internet. Este tipo de redes se destacar por su alto nivel de rendimiento y bajo costo. Son sus características la utilización de cable coaxial para la transmisión, una velocidad de 10Mbit/seg. (ahora con cableado UTP a 100 Mps en Fast Ethernet y 1 Gbps en Giga Ethernet) y CSMA/CD como técnica de acceso.

Ethernet es un medio en el que todos los ordenadores pueden acceder a cada uno de los paquetes que se envían, aunque un ordenador sólo tendrá que prestar atención a aquellos que van dirigidos a él mismo. Es ésta característica la posteriormente veremos nos sirve de gran ayuda para realizar nuestras capturas.

También es popular por la facilidad de conectar equipos localizados a distancias de más de 100 metros sin incurrir en costos elevados. "Cada versión de ethernet tiene una máxima longitud de cable permitido. Para permitir redes de mayor extensión, se pueden conectar múltiples cables por medio de repetidores " (Tanenbaum, 2003, 274).

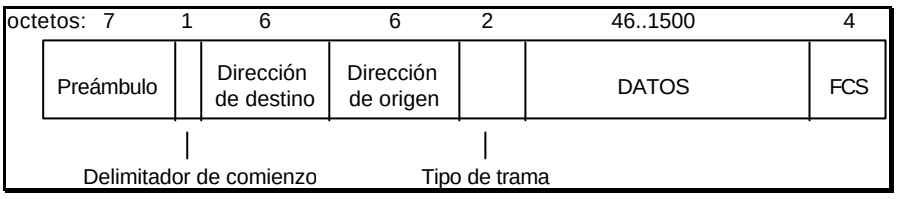


Figura 2. Formato de la trama ethernet

La organización de los datos en una trama ethernet[1] se puede ver en la figura 2.

1.2 Protocolos

1.2.1 Introducción.

Stallings describe a una arquitectura de protocolos como una estructura de capas de hardware y software que facilita el intercambio de datos entre sistemas, y proporciona aplicaciones distribuidas como por ejemplo el correo electrónico y la transferencia de archivos.
En cada capa de la arquitectura se implementa cada uno o varios protocolos. Cada protocolo proporciona un conjunto de reglas que regulan el intercambio de datos entre los sistemas.
Las tareas típicas que realiza un protocolo son entre otras: encapsulamiento, segmentación, ensamblado, control de la conexión, transmisión ordenada, control de flujo, control de errores, direccionamiento y multiplexación.

La arquitectura que más se usa es la familia de protocolos TCP/IP (Stallings: 2000, 30), y es por este hecho que vamos a ver los principales protocolos relacionados a TCP/IP.

1.2.2 Arquitectura TCP/IP

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto.

Una red TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetes, cada paquete comienza con una cabecera que contiene información de control.

Cuando se envía un archivo por la red TCP/IP, su contenido se envía utilizando una serie de paquetes diferentes. El Internet protocol (IP), un protocolo de la capa de red, permite a las aplicaciones ejecutarse transparentemente sobre redes interconectadas.

[1] Para detalles, se puede consultar el libro de Stallings. Comunicaciones y redes de Computadoras. P. 442

La arquitectura de Internet esta basada en capas. Esto hace mas fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura como se puede ver en la figura Nº 3.

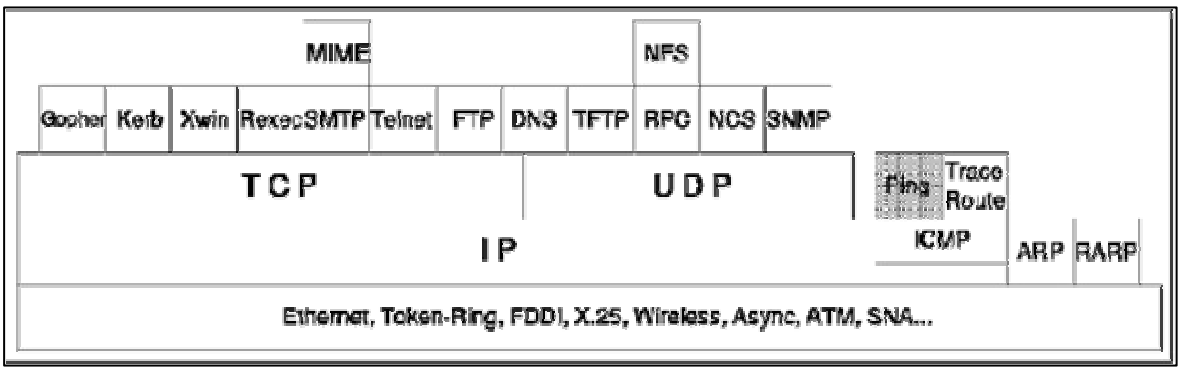


Figura 3. Arquitectura de los protocolos TCP/IP

El funcionamiento de la comunicación se lo puede resumir como:

Supóngase que un proceso asociado a al puerto 1 en el computador A, desea enviar un mensaje a otro proceso, asociado al puerto 2 del computador B. El proceso en A pasa el mensaje al TCP con la instrucción de enviarlo al puerto 2 del computador B. El TCP pasa el mensaje al IP con instrucciones que lo envíe al computador B. Obsérvese que no es necesario comunicarle a IP la identidad del puerto destino. Todo lo que necesita saber es que los datos van dirigidos al computador B. A continuación , IP pasa el mensaje a la capa de acceso a la red (por ejemplo a la lógica ethernet) con el mandato expreso de enviarlo al dispositivo de encaminamiento X (el primer salto en el camino a B).
Para controlar esta operación se debe transmitir información de control junto con los datos del usuario, como así se sugiere en la figura 4 Supongamos que el proceso emisor genera un bloque de datos y lo pasa al TCP. El TCP puede que divida este bloque en fragmentos más pequeños para hacerlos mas manejables. A cada uno de estos fragmentos le añade información de control, denominada cabecera TCP, formando un segmento TCP. La información de control la utilizará la entidad par TCP en el computador B. Entre otros, en la cabecera se incluyen los siguientes campos:

- ***Puerto destino**: cuando la entidad TCP en B recibe el segmento, debe conocer a quién se le deben entregar los datos.*
- ***Número de secuencia:** TCP numera secuencialmente los segmentos que envía a un puerto destino dado, para que si llegan desordenados, la entidad TCP en B pueda reordenarlos.*
- ***Suma de comprobación:** la entidad emisora TCP incluye un código calculado e función del resto del segmento. La entidad receptora TCP realiza el mismo cálculo y compara el resultado con el código recibido. Si se observa alguna discrepancia, implicará que ha habido un error en la transmisión.*

A continuación, TCP pasa cada segmento IP con instrucciones para que los transmita a B. Estos segmentos se transmitirán a través de una o más subredes y serán retransmitidos en uno o más dispositivos de encaminamiento intermedios. Esta operación también requiere del uso de información de control. Así el IP añade una cabecera de información de control a cada segmento para formar un datagrama IP. En la cabecera IP, además de otros campos se incluirá la dirección del computador destino.

Finalmente cada datagrama IP se pasa a la capa de acceso a la red para que se envíe a través de la primera subred. La capa de acceso a la red añade su propia cabecera , creando un paquete o trama. El paquete se transmite a través de la red al dispositivo de encaminamiento J. La cabecera del paquete contiene la información que la red necesita para transferir los datos.
En el dispositivo de encaminamiento J se elimina la cabecera del paquete y se examina la cabecera IP. El módulo IP del dispositivo de encaminamiento direcciona el paquete a través de la red 2 hacia B basándose en la dirección destino que contenga la cabecera IP. Para hacer esto, se le añade al datagrama una cabecera de acceso a la red.
Cuando se reciben los datos en B, ocurre el proceso inverso. En cada capa se elimina la cabecera correspondiente y el resto se pasa a la capa inmediatamente superior, hasta que los datos de usuario alcancen el proceso destino (Stallings: 2000, 54-55).

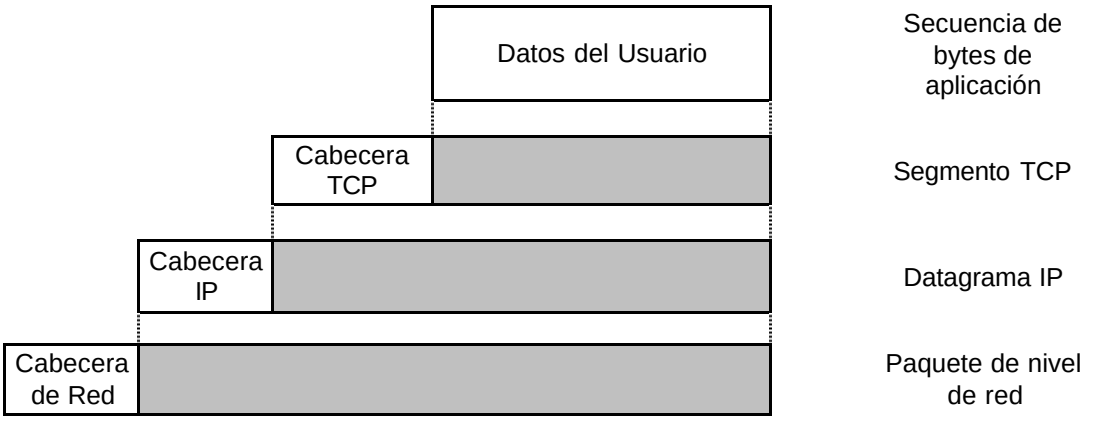


Figura 4 Unidades de datos de protocolo en la arquitectura TCP (Stalling: 2000, 53)

1.2.3 Protocolo IP (Internet Protocol)

1.2.3.1 Introducción

El protocolo IP es parte integral de la arquitectura TCP/IP. Cada dato TCP, UDP, ICMP, e IGMP se transmiten como datagramas IP

IP es un protocolo no confiable, pues no hay garantía de que el datagrama IP llegue exitosamente a su destino. IP provee el servicio denominado de mejor esfuerzo . Cualquier requerimiento de fiabilidad debe ser proporcionado por niveles superiores como por ejemplo TCP.

IP también en un protocolo no orientado a la conexión, lo que significa que no mantiene ningún registro de los datagramas sucesivos, sino que cada datagrama es manejado de manera independiente (Stevens: 1994, cap. 3.1).

1.2.3.2 La cabecera IP

La Figura 5 muestra el formato de un datagrama IP. El tamaño normal de una cabecera IP es de 20 bytes, sin contar con las opciones, si las hubiere.

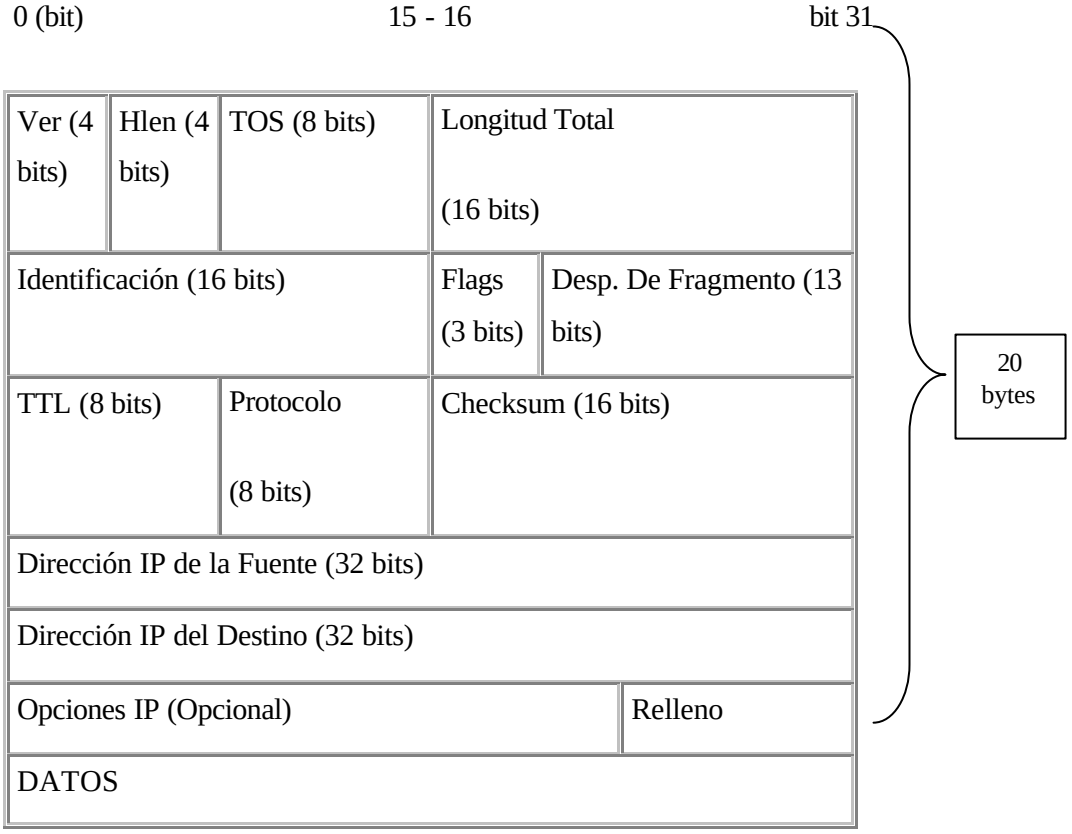


Figura 5. Datagrama IP, con sus campos en la cabecera.

1.2.4 TCP (Transmission Control Protocol)

1.2.4.1 Características

El protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece que sea continuo. TCP proporciona un circuito virtual el cual es llamado una conexión. Los programas que utilizan el TCP tienen un servicio de conexión entre los programas llamados y los que llaman, además cuentan con capacidades de chequeo de errores, control de flujo y capacidad de interrupción.

El TCP recuerda el estado de cada conexión por medio del TCB. Cuando se abre una conexión, se efectúa una entrada única en el TCB. Un nombre de conexión se le asigna al

usuario para activar los comandos de la conexión. Cuando se cierra una conexión se elimina su entrada del TCB.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. (PROTOCOLS: 2003)

1.2.4.2 Estructura de TCP

Figura 6. Estructura de una datagrama TCP

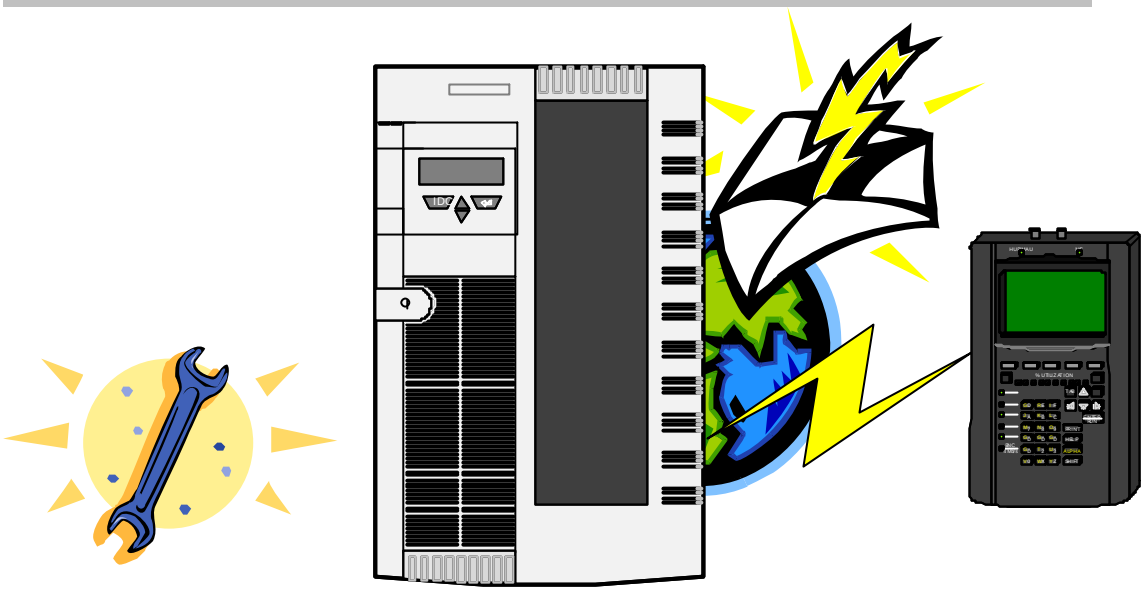
Conclusiones del capítulo 1.

Con el desarrollo de este capítulo se pudo dar un pequeño recuento a modo general sobre los principal de las redes y los protocolos, para poder enmarcarnos en lo que debemos conocer antes de tratar de comprender los datos que capturemos.

No se ha hecho una explicación prolongada del tema puesto que esta información se puede obtener fácilmente en libros de redes como el de Tanembaum, Stallings u otros; estas obras se detallan en la bibliografía para que sean consultadas en el caso de ser necesarias Otra fuente de información rápida es actualmente las páginas web, que asimismo en la bibliografía se detallan.

CAPITULO 2

HERRAMIENTAS DEL ADMINISTRADOR DE RED



2.1 HERRAMIENTAS DE DIAGNÓSTICO DE CONECTIVIDAD

2.1.1 Introducción

Cuando una red está funcionando correctamente al estar recién instalada, es seguro que de a poco con el uso que se le de a la misma y por programas que se hayan agregado mas otros factores varios, se presenten problemas de velocidad, de fallas de servicios, Caídas de enlaces, etc. Es en ese momento que quien administra la red debe usar todas las herramientas posibles para determinar con rapidez el origen del problema y solucionarlo.

Existen algunas herramientas fundamentales que nos van a ayudar en el caso tratado en el párrafo anterior, en esta sección explicaremos su funcionamiento y posteriormente las usaremos en el desarrollo de las prácticas.

2.1.2 Ping

El ping es la más sencilla de todas las aplicaciones TCP/IP, envía uno o más datagramas a un host de destino determinado solicitando una respuesta y mide el tiempo que tarda en retornarla.

Tradicionalmente, si se podía hacer un ping a un host, otras aplicaciones como Telnet o FTP podían comunicarse con ese host. Con el advenimiento de las medidas de seguridad en Internet, particularmente los cortafuegos(firewalls), que controlan el acceso a redes a través del protocolo de aplicación y/o el número de puerto, esto ha dejado de ser estrictamente cierto. Aún así, la primera prueba para comprobar si es posible alcanzar un host sigue siendo intentar hacerle un ping.

El ping es útil para verificar instalaciones TCP/IP (Stevens: 1994, cap. 7).

2.1.3 Nslookup

Nslookup es un programa que realiza consultas a servidores de nombres de Dominio de Internet y funciona de dos modos: el interactivo y el no interactivo. El modo interactivo permite al usuario consultar servidores de nombres solicitando información de varios host y dominios o imprimir la lista de los host en los dominios. El modo no interactivo es usado para listar solo el nombre y la información requerida del host o dominio. (Linux: 2003)

2.1.4 Dig

La herramienta Dig (**d**omain **i**nformation **g**roper) es muy flexible para interrogar servidores DNS, este realiza búsquedas DNS y muestra las respuestas enviadas por el o los servidores de nombres que fueron consultados. La mayoría de administradores DNS usan Dig para detectar problemas de DNS debido a su flexibilidad, claridad y facilidad de uso. Otras herramientas de búsqueda suelen ser menos flexibles que dig.

Además de consultar los servidores específicos, dig tratará de llegar a cada uno de los servidores nombrados en el archivo /etc/resolv.conf. (Linux: 2003)

2.1.5 Tracert

El programa tracert es útil cuando se usa para la depuración. Nos permite determinar la ruta que siguen los datagramas IP para llegar de un host a otro.

El tracert usa como medio de acción mensajes ICMP.

El proceso inicia cuando se envía un datagrama IP con un tiempo de vida (TTL) de 1 al host de destino. El primer router que vea el datagrama decrementará el TTL a 0, y lo

descartará, además devolverá un mensaje ICMP de Tiempo excedido (Time Exceeded) y por supuesto en el campo dirección IP origen colocará su dirección. De este modo se identifica el primer router del camino. Este proceso se repite sucesivamente incrementando TTL en 1 cada vez, de este modo arma la ruta identificando la serie de routers que se encuentran en el camino hasta llegar al host de destino (Stevens: 1994, cap. 8).

2.1.6 Netstat

Muestra información sobre la tabla de ruteo, las interfaces y los sockets activos. El propósito es mostrar el estatus de la red. Simbólicamente despliega el contenido de varias estructuras de datos para conexiones activas, relacionadas con la red. Se puede especificar el parámetro Interval para estar desplegando continuamente la información del tráfico en las interfaces de red configuradas.

2.1.7 Ifconfig

Si bien es básicamente una herramienta de configuración, puede utilizarse también como herramienta de diagnóstico, para detectar errores en la dirección IP, mascara de subred o dirección de broadcast (Linux: 2003).

2.1.8 Mensajes De Error frecuentes

Existen unos errores que podrían catalogarse como típicos y de fácil solución aunque los mensajes emitidos por las herramientas de diagnóstico puedan parecer intimidantes; el reconocer tales mensajes será de mucha ayuda, por lo que a pesar de haberlos descrito en secciones previas, por la utilidad se hará un resumen sobre ellas en esta sección.

Connection refused by peer: Este mensaje indica que aunque hay comunicación con el equipo remoto no se puede establecer una conexión porque el equipo la rechazó. Esto sucede cuando no hay un servicio escuchando en el puerto TCP indicado o se trata de una medida de seguridad y no se permite la conexión remota.

Network unreachable: Este mensaje nos avisa que el sistema local no tiene una ruta que conduzca a la red de la máquina remota. Esto se da por errores en la configuración de la tabla de ruteo, o porque hayan caído algunos vínculos de comunicación que lo conecta a nuestra red.

No answer from host: Se da cuando el sistema remoto no contesta las peticiones de nuestro host. Esto se da cuando la red del equipo es alcanzada, pero el equipo está apagado o desconectado de dicha red..

Unknown host: Se produce este mensaje cuando el nombre de host utilizado por el usuario no pudo resolverse; es decir, no pudo obtenerse su dirección IP. Puede ser indicativo de un error en el acceso al servidor de nombres o que simplemente no exista tal nombre.

2.2 HERRAMIENTAS DE CAPTURA Y ANÁLISIS DE DATOS

2.2.1 Introducción

Para poder conocer lo que sucede en una red y poder diagnosticar con más precisión el origen de los errores son necesarias herramientas que permitan en primera instancia ver los datos que circulan por una red, esto podría plantear situaciones de conflicto en cuanto a la privacidad de la información, pero desde el punto de vista técnico es totalmente recomendable el poder verificar la información; se debería en el caso de información delicada usar métodos de cifrado que protejan, pues en el caso del administrador de la red, eso no tendría mayor aporte a la solución de problemas, salvo en el caso que se debiera a exceso de ancho de banda ocupado. Al margen de estas consideraciones, es necesario llevar registro del rendimiento de la red, cuidar que no se esté dando un uso inapropiado a recursos que no están destinados a ello, y sobre todo, detectar tráfico no esperado y cualquier intrusión en nuestra red. Considerando que físicamente las conexiones no permiten conocer si están cargadas de tráfico y de que tipo, es necesario valernos de herramientas que en muchos casos ya incluye el sistema operativo como parte integral de su distribución, es el caso de tcpdump en Linux, que inclusive incluye el analizador ethereal.

En los sistemas operativos Windows también contamos con analizadores de tráfico como el monitor de red, que sirven como preámbulo al uso de analizadores más avanzados, los cuales vamos a describir en esta sección.

Resumiendo, con un correcto trabajo de monitorización de la información que circula por la red podemos hacer diagnósticos de problemas con más precisión, analizar la eficiencia del sistema, identificar posibles problemas de seguridad y problemas de uso adecuado

2.2.2 Analizadores de protocolos o Sniffers

Los analizadores de protocolos, también son conocidos como sniffers y funcionan gracias a que pueden configurar el interfaz de red de acuerdo a sus requerimientos:

"De forma predeterminada, las estaciones de trabajo escuchan y responden solamente a los paquetes que van dirigidos a ellas. Sin embargo, es posible modelar el software que lanza la interfaz de red de una estación de trabajo en algo llamado promiscuo. Tendiendo en cuenta esto, la estación de trabajo puede monitorizar y capturar todo el tráfico de la red y los paquetes que pasen por ella, independientemente del destino que tengan." (Anónimo: 2003, 203)

Los sniffer usados por personas no autorizadas son muy riesgosas debido a que:

- Pueden capturar contraseñas
- Pueden capturar información confidencial o patentada
- Pueden utilizarse para romper la seguridad en los entornos de red u obtener acceso por la fuerza

Una forma de verificar si hay un sniffer funcionando es en Linux, utilizar el comando *ifconfig* descrito en la sección anterior, que nos indica los detalles de las interfaces de red disponibles, y expone "RUNNING PROMISC" en el detalle en el caso de que esté funcionando en modo promiscuo.

2.2.2.1 Tcpdump

"Tcpdump es una herramienta de supervisión de red que descarga cabeceras de paquetes de una interfaz de red específica." (Anónimo: 2003, 641)

La herramienta tcpdump se encuentra por defecto en cualquier distribución del sistema operativo Linux o se puede incluir en cualquier sistema UNIX. Permite la captura de paquetes que circulen por la red a la que pertenece el ordenador en el que se ejecute. Un requerimiento indispensable para su empleo, es su ejecución con privilegios de superusuario, Por último, cabe indicar que esta herramienta se maneja desde la consola y que carece de interfaz gráfico, aunque su archivo de captura puede ser analizado con otras herramientas más amigables.

2.2.2.2 Monitor de red de Windows

El Monitor de red de Windows es una herramienta muy útil para detectar y solucionar problemas en redes de área local. Se puede por ejemplo notar que algún cliente hace cantidades exorbitantes de solicitudes de algún servicio, o uso de la red, identificar problemas de conexiones entre el cliente y el servidor, como también se podría identificar usuarios no autorizados. Se puede pues identificar patrones de tráfico y problemas de red.
Algunas de las funciones que permite realizar son: Capturar tráfico directamente desde la red, generar reportes con las tramas capturadas, guardar los datos en un archivo de captura y también mostrar en tiempo real las estadísticas de las tramas capturadas cumpliendo criterios de filtros si es que se requiere

2.2.2.3 Ethereal

"Ethereal es un analizador de protocolos de red, es un sniffer de paquetes que soporta ARP/RAP, DHCP, DNS, Ethernet, ICMP, IP/TCP/UDP, OSPF y otros protocolos " (Anónimo: 2003, 619)

"La GUI de ethereal permite analizar fácilmente los datos del snniffer, bien desde una captura en tiempo real, bien desde archivos de capturas *tcpdump* previamente generados" (Anónimo: 2003, 223).

Este programa analizador de protocolos está catalogado quizá como el mejor programa de código abierto para captura de paquetes; tiene versiones para Windows y unix, por esto se lo ha usado como analizador principal en este trabajo..

Este programa consta de 3 paneles horizontales en donde se puede ver la información capturada. El panel superior muestra la lista de cada paquete capturado, además muestra un resumen del paquete. Seleccionando el paquete de la lista se puede ver el detalle en las otras pantallas.

La pantalla del medio brinda una vista en modo de árbol, en donde a cada paquete se puede expandir de modo que se vea cada campo que compone el paquete. El panel inferior muestra los datos en hexadecimal y en ASCII, y señala los bytes que componen el campo

seleccionado en la ventana del medio. Además puede realizar filtrado de información cuando se trata de mucha información y en la parte inferior derecha se muestran mensajes de lo que se esta capturando o el campo que estamos consultando.

2.2.2.4 Distinct Network Monitor

Este es un analizador de paquetes IP para las redes de computadores, que traduce la negociación compleja de protocolos al lenguaje natural, señalando los errores. Además incorpora una aplicación para captar una selección variada de estadísticas sobre el tráfico en cualquier segmento de red de interés y ofrece una presentación figura de éstas estadísticas.

Las estadísticas indicarán el tráfico generado entre todas las direcciones IP locales además de los paquetes de difusión y de difusión múltiple. Los datos están presentados al nivel de la aplicación. Por ejemplo, si se hace clic en una dirección IP, se podrá ver la distribución de paquetes en cada protocolo

Características principales

Permite monitorear el tráfico de red al lenguaje natural y ofrece una traducción detallada de cada protocolo.

El Network Monitor guarda la historia de cada conexión a la red lo que lo permite dar sentido a cada Paquete en una cadena. Esto simplifica la detección de errores y permite entender la causa de un problema.

Se pueden importar archivos creados por productos similares.

Se puede realizar análisis remoto de paquetes a través de sus Agentes y además reúne estadísticas relativas al tráfico detectado por el sistema con el que funciona (Distinct: 2003)

2.2.2.5 Optiview protocol expert

El analizador de redes Protocol Expert es un conjunto integrado de software y hardware que provee control y visibilidad de datos que circula a través de la empresa, permite hacer captura y análisis de paquetes dentro de una red WAN, LAN o inalámbrica.

Protocol Expert funciona bajo Windows y analiza paquetes capturados con herramientas hardware apropiadas para ello y del mismo fabricante, aunque puede también analizar el tráfico capturando directamente desde la tarjeta de red. Tiene un ayudante que

ayuda a detectar el problema y realiza sugerencias para corregir el problema. Tiene un nivel de decodificación de 7 capas lo que permite analizar con mucha profundidad los paquetes capturados.(FlukeNetworks: 2000)

Conclusiones del capítulo 2.

Se ha podido verificar que existen muchas herramientas para comprobar la conectividad entre redes, las cuales son un recurso inicial para dar soporte a tales sistemas y sin duda alguna, todos deberíamos conocer su uso.

La forma como los analizadores hacen su trabajo es configurando a la interfaz de red en modo promiscuo, en el que lee todos los datos sin importar si son o no dirigidos a ése equipo.

Los analizadores de protocolos o sniffer son de gran utilidad, pero así mismo pueden ser muy peligros si son usados por personal no autorizado o ajeno, así que hay que tener en cuenta este detalle y hacer las revisiones necesarias para asegurarse de no tener complicaciones posteriores.

DISEÑO DE LOS TRABAJOS PRACTICOS

3 PLANIFICACIÓN, DISEÑO, SELECCIÓN DE ESCENARIOS Y PRUEBAS DE LOS TRABAJOS PRÁCTICOS

3.1 Introducción

En este capítulo de realizará la planificación de los trabajos prácticos que se llevaran a cabo, la finalidad es crear los distintos escenarios en los cuales se va a realizar la captura de paquetes. Esto es muy importante ya que de acuerdo al caso, se podrán ver distintos Intercambios protocolares que serán analizados con bastante detalle de tal manera que resulte su observación muy didáctica, es así que los primeros análisis tratan del uso de herramientas como ping, que hace una tarea sencilla sobre redes TCP/IP, usando el protocolo IP y los mensajes ICMP nos servirá de base para los siguientes análisis, que tomando como base los análisis anteriores, no se centrará ya en considerar a fondo los datos que de ellos se pueda obtener, a excepción de casos en que difieren o tienen una funcionalidad que aún no haya sido analizada.

Se ha tomado en cuenta para el diseño también la aplicabilidad de los análisis, es así que siendo lo más común el uso de redes ethernet se ha concentrado en ellas, y más aún considerando que actualmente son muy populares las implementaciones enlazadas a Internet o por Internet. Así pues el presente trabajo se ha realizado bajo estas consideraciones que corresponden a una realidad actual.

La organización del presente capítulo esta dividida en las tareas de Planificación, diseño y selección de escenarios, diseño de las pruebas y maquetas gráficas, agrupadas para cada Trabajo práctico y sintetizadas en hojas de trabajo que serán directamente utilizadas como base para iniciar el trabajo de captura y análisis.

Para el diseño de los informes se utilizó como modelo inicial, las recomendaciones y estructuras de informes explicadas por los Ing. Marcelo Utard e Ing. Pablo Ronco, docentes de la Universidad de Buenos Aires en Argentina, que propusieron y apoyaron el desarrollo del presente tema; además esta modalidad de hojas de trabajo nace al apreciar personalmente su conveniencia, pues he tenido la oportunidad de usar modalidades similares en varias prácticas de laboratorio que realicé durante mi preparación anterior como tecnólogo en Electrónica; también se ha recogido comentarios y sugerencias de compañeros de varias prácticas de laboratorios realizadas en la Universidad de Buenos Aires durante el curso de Telecomunicaciones.

Los diseños de las maquetas gráficas y escenarios se ha elaborado a partir de un listado de comandos importantes como ping, tracert, dig, nslookup y un listado de protocolos como http y smtp, que han sido propuestos por los docentes antes mencionados; comandos y protocolos que permitirán estudiar la información capturada desde un nivel de complejidad mínimo hasta un nivel mucho mayor al final; Adicionalmente para el diseño final fue muy importante la circunstancia dada por la necesidad de realizar las pruebas sin que se tenga que usar más equipamiento que del que se pueda disponer en una pequeña oficina como en la que se realizaron las tomas de datos; se consideró incluso la posibilidad de que grupos de estudiantes pudiesen efectuar tales pruebas sin mayores complicaciones en sus casas, uniendo en red sus computadoras y teniendo una conexión a Internet mediante un modem, lo cual hoy en día es muy común.

3.2 Trabajo Práctico 1 - PING

Tema:

Análisis de tramas portadoras de comandos PING

Objetivo:

El objetivo de este trabajo práctico es realizar una captura de paquetes generados con el comando *Ping* para verificar conectividad entre hosts. Se pretende iniciar el trabajo práctico con el uso escenarios que gradualmente se incrementarán en complejidad para observar otros mensajes protocolares, así que se deberá verificar la operación del protocolo ARP, reconocer la estructura de las tramas Ethernet y de los datagramas IP, así como inspeccionar los mensajes ICMP que se intercambien los equipos.

Maqueta:

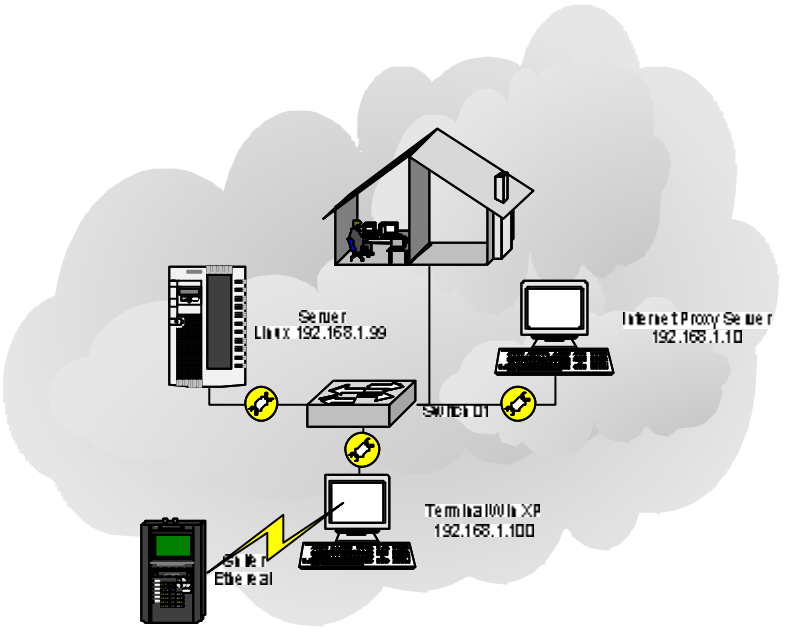


Figura 7. Maqueta para TP 1

Escenario:

1. Se desea conocer si hay conectividad entre dos equipos localizados en una LAN, dentro de un segmento de red ethernet común.

Lista de Tareas a realizar

1.1. Obtener datos de la configuración de la red con el comando *ipconfig:*

1) Dirección IP _____
2) Máscara de subred _____
3) Puerta de enlace predeterminada _____
4) Clase de red _____
5) Dirección de red _____
6) Dirección de broadcast _____
7) Rango de direcciones de host _____

1.2. [ ] ejecución de comando *"arp -a"*

1.3. [ ] Inicio de captura del programa ethereal

1.4. [ ] ejecución de comando *"ping 192.168.1.10"*

1) Cuantos mensajes ICMP se produjeron_____
2) Ha recibido el destino los mensajes ICMP_____
3) Tiempo de vida_____
4) Tiempos de ida y vuelta: min_____máx._____media_____

1.5. [ ] ejecución de comando *"arp -a"*

1.6. [ ] Finalizar la captura y salvar el archivo capturado como "*Captura_p1_e1.txt*"

3.3 Trabajo Práctico 2 - TRACERT

Tema:

Análisis de tramas generadas a partir del comando TRACERT

Objetivo:

El objetivo de este trabajo práctico es realizar una captura de paquetes generados con el comando *Tracert* para conocer la ruta que los paquetes recorren, reconociendo los diferentes mensajes de control y mecanismos que usa este comando.

Maqueta:

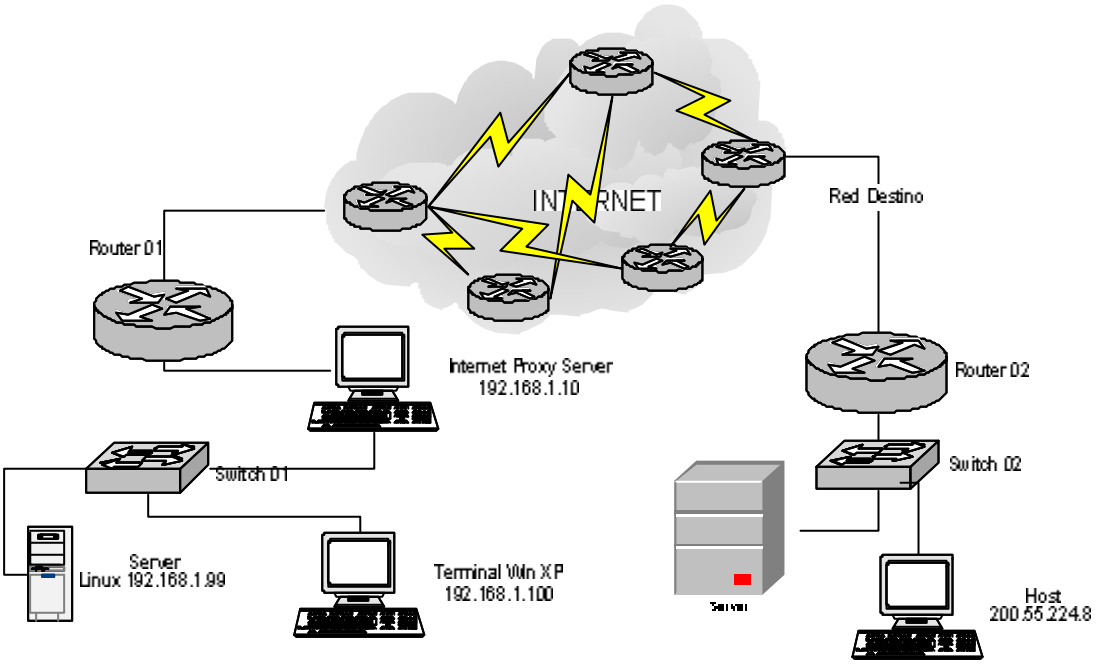


Figura 8. Maqueta para TP 2

Escenario:

2. Se necesita conocer la ruta que une a mi equipo con un equipo localizado fuera de mi red; red que está enlazada a internet mediante un servidor proxy.

Lista de Tareas a realizar

2.1 Obtener datos de la configuración de la red con el comando *ipconfig:*

1) Dirección IP _____
2) Máscara de subred _____
3) Puerta de enlace predeterminada _____
4) Clase de red _____
5) Dirección de red _____
6) Dirección de broadcast _____
7) Rango de direcciones de host _____

2.2 [ ] Inicio de captura del programa ethereal

2.3 [ ] ejecución de comando *"tracert 200.55.224.8"*

2.4 [ ] Finalizar la captura y salvar el archivo capturado como "*Captura_p2.txt*"

3.4 Trabajo Práctico 3 - NSLOOKUP

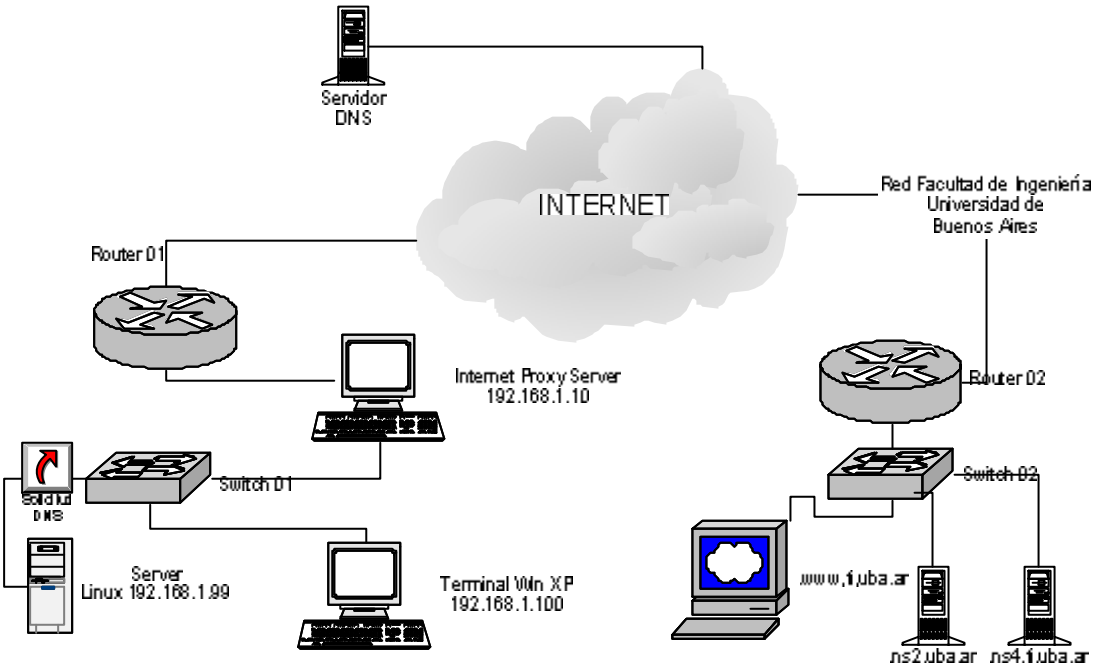
Tema:

Análisis de tramas generadas a partir del comando *nslookup*

Objetivo:

El objetivo de este trabajo práctico es realizar una captura de paquetes generados con el comando de consulta de servidores de dominio de Internet *nslookup* para conocer los datos intercambiados al resolver los nombres y dominios e identificar los diferentes campos y el significado de sus valores.

Maqueta:



conocer los servidores de domino de Internet que resuelven los nombres de las Universidades de Buenos Aires y también de la UDA

Lista de Tareas a realizar

3.1 Obtener datos de la configuración de la red con el comando *ifconfig:*

1) Dirección IP _____
2) Máscara de subred _____
3) Puerta de enlace predeterminada _____
4) Clase de red _____
5) Dirección de red _____
6) Dirección de broadcast _____
7) Rango de direcciones de host _____

3.2 [ ] Inicio de captura del programa ethereal

3.3 [ ] ejecución de comando *nslookup www.fi.uba.ar y nslookup www.uazuay.edu.ec*

3.4 [ ] Finalizar la captura y salvar el archivo capturado como "*Captura_p3.txt*"

3.5 Trabajo Práctico 4 - DIG

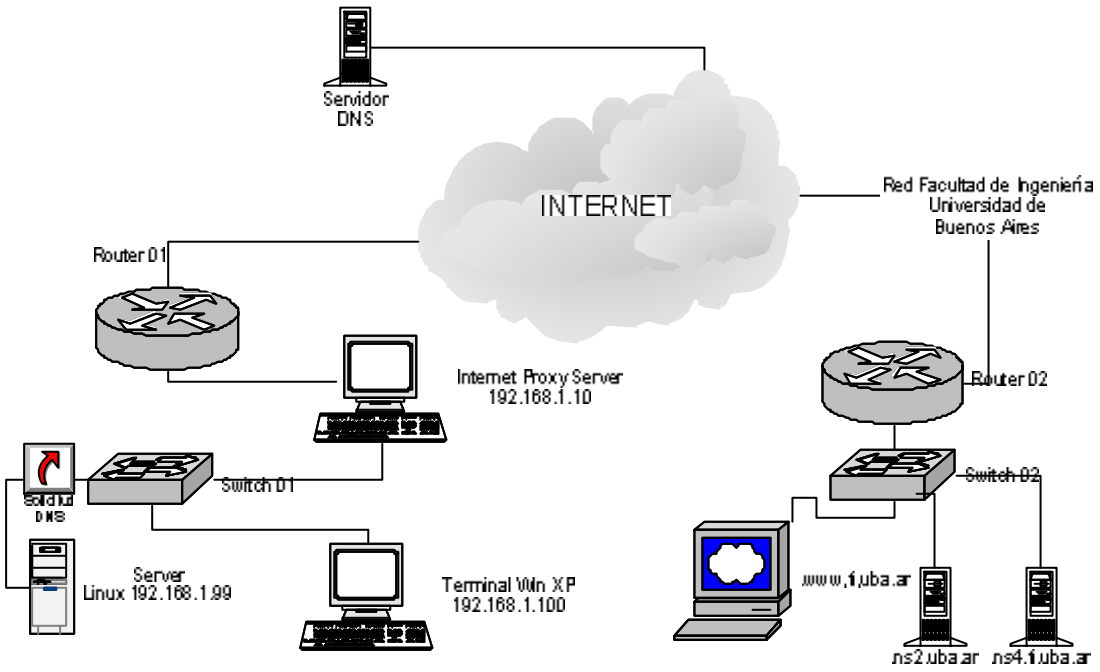
Tema:

Análisis de tramas generadas a partir del comando "*dig*"

Objetivo:

El objetivo de este trabajo práctico es realizar una captura de paquetes generados con el comando de consulta de servidores de dominio de Internet *dig* para conocer los datos intercambiados al resolver los nombres, además para conocer el modo de funcionamiento de esta utilidad y los servicios protocolares que utiliza.

Maqueta:



Universidades de Buenos Aires y también de la UDA tratando de conectarse con todos los servidores que tengamos registrados en nuestro sistema

Lista de Tareas a realizar

4.1 Obtener datos de la configuración de la red con el comando *ifconfig:*

1) Dirección IP _____
2) Máscara de subred _____
3) Puerta de enlace predeterminada _____
4) Clase de red _____
5) Dirección de red _____
6) Dirección de broadcast _____
7) Rango de direcciones de host _____

4.2 [ ] Inicio de captura del programa ethereal

4.3 [ ] ejecución de comando *dig www.fi.uba.ar y dig www.uazuay.edu.ec*

4.4 [ ] Finalizar la captura y salvar el archivo capturado como "*Captura_p4.txt*"

3.6 Trabajo Práctico 5 – email

Tema:

Análisis de tramas generadas a partir de una consulta de correo electrónico

Objetivo:

El objetivo de este trabajo práctico es realizar una captura de paquetes generados con el envío y recepción de mensajes de correo electrónico almacenados en un computador del ISP a fin de conocer el modo de funcionamiento del protocolo TCP e ICMP, además identificar los campos más importantes y el significado de sus valores y corroborar con la teoría el modo de establecer una conexión.

Maqueta:

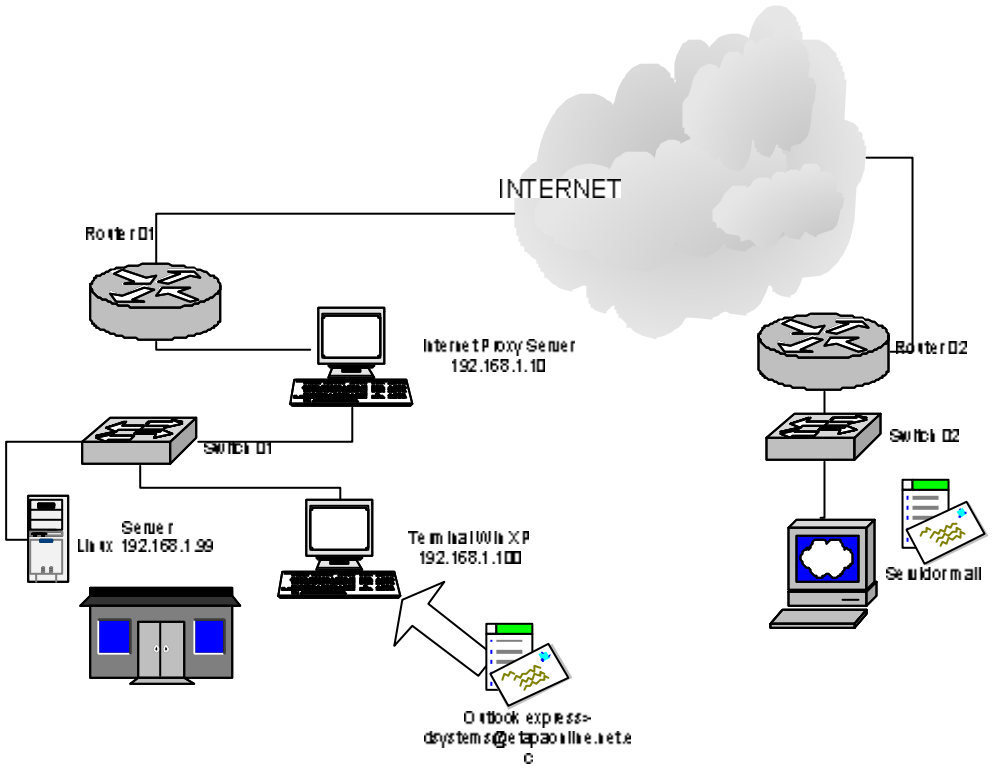


Figura 11 Maqueta para TP 5

Escenario:

5. Se tiene una red con un equipo windows Xp y cliente de correo electrónico Outlook express, que accede a Internet y a los servicios de correo a través de una red ethernet y un servidor proxy Internet.

Lista de Tareas a realizar

5.1 Obtener datos de la configuración de la red con el comando *ipconfig:*

1) Dirección IP _____
2) Máscara de subred _____
3) Puerta de enlace predeterminada _____
4) Clase de red _____
5) Dirección de red _____
6) Dirección de broadcast _____
7) Rango de direcciones de host _____

5.2 [ ] Inicio de captura del programa ethereal

5.3 [ ] envío de un mensaje de corrreo electrónico a la dirección *dsystems@etapaonline.net.ec*

5.4 [ ] Consultar la existencia de mensajes de corrreo electrónico en la cuenta ***dsystems*** del servidor ISP Etapaonline

5.5 [ ] Finalizar la captura y salvar el archivo capturado como "*Captura_p5.txt*"

3.7 Trabajo Práctico 6 - WEB

Tema:

Análisis de tramas generadas a partir de la carga de una página web

Objetivo:

El objetivo de este trabajo práctico es realizar una captura de paquetes generados con el la solicitud de una página web a través del navegador de internet, para luego analizar con la herramientas de análisis de tráfico y sacar figuras estadísticas.

Maqueta:

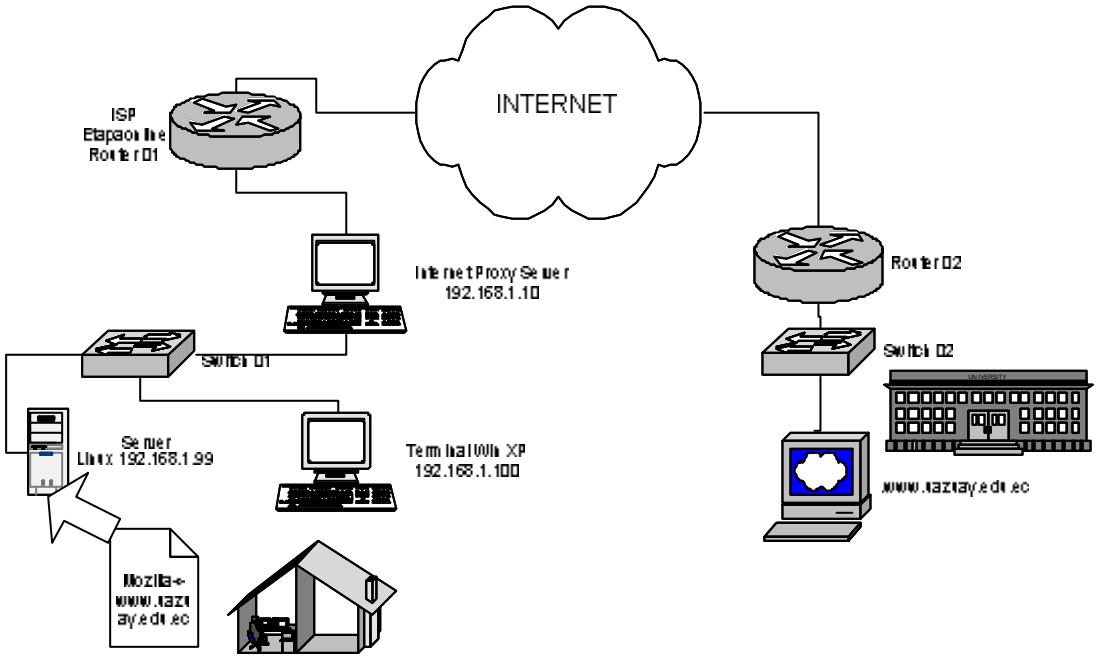


Figura 12. Maqueta para TP 6

Escenario:

6. Se tiene una red con un equipo Linux, que se conecta a Internet a través de una red Ethernet y un servidor proxy, y utilizando el navegador Mozilla se realiza un pedido de carga de la página web principal de la Universidad del Azuay.

Lista de Tareas a realizar

6.1 Obtener datos de la configuración de la red con el comando *ifconfig:*

1) Dirección IP _____
2) Máscara de subred _____
3) Puerta de enlace predeterminada _____
4) Clase de red _____
5) Dirección de red _____
6) Dirección de broadcast _____
7) Rango de direcciones de host _____

6.2 [ ] Inicio de captura del programa ethereal

6.3 [ ] solicitud de la página www.uazuay.edu.ec en el navegador de Internet

6.4 [ ] Finalizar la captura y salvar el archivo capturado como "*Captura_p6.txt*"

Conclusiones del capítulo 3:

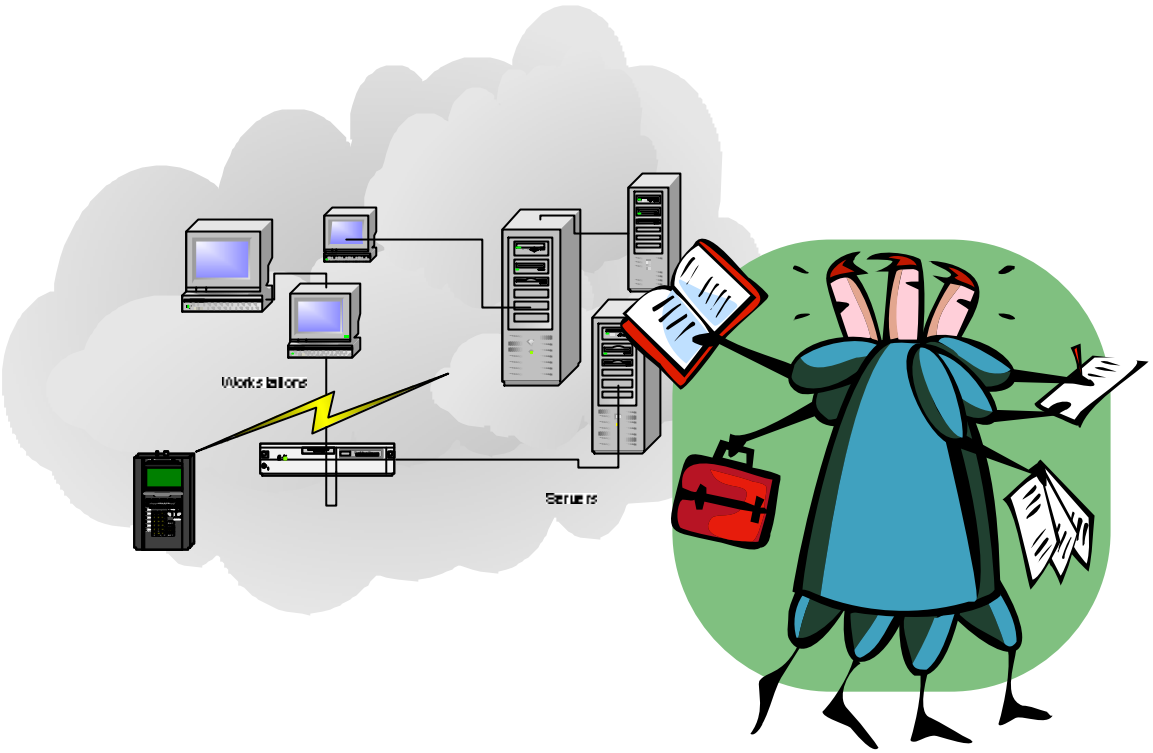
Luego de haber elaborador estas hojas de trabajo, se pudo ver que es una forma didáctica que permite un mejor aprovechamiento del tiempo en los laboratorios ya que el procedimiento de toma de la información está claramente definido, con lo cual se ahorra tiempo, usando tal ahorro para profundizar sobre aspectos mismos de la interpretación y análisis que son de mayor complejidad.

El diseño final obtenido de las maquetas gráficas puede usar tanto las instalaciones de laboratorios de la universidad, en cuyo caso se daría la captura de datos de forma directa, puesto que ya cuenta con la conexión a Internet, o puede utilizar la conexión de Internet que provee por ejemplo Etapa, en cuyo caso se recurre al uso de un servidor Proxy, para que haya el tráfico por la red ethernet y se lo pueda capturar.

Con la experiencia del diseño actual, nacieron interrogantes sobre análisis con más tipos de tráfico protocolar, como es el caso de transferencia de archivos con ftp, sesiones remotas con telnet, comunicacioes de chat y voz con el Messenger, o conexiones de video conferencia entre otros, que siguiendo con el esquema usado de estas hojas de trabajo, y con más tiempo, seguro se podrán realizar y brindarán un aporte importante a la práctica y conocimiento de quien las realice.

CAPITULO 4

EL ESCENARIO DE PRUEBAS



4 MONTAJE DE LA RED

4.1 Introducción

Para realizar los trabajos prácticos y las pruebas es necesario contar con una red instalada, por lo que se ha procedido a instalarla aprovechando los equipos de la empresa Sistemas Digitales[2].

El diseño de los trabajos prácticos requieren que haya un equipo con Linux funcionando, puesto que es necesario utilizar algunas herramientas que son provistas o funcionan en ese sistema operativo. Para poder utilizar los analizadores de tráfico es necesario que hayan equipos con Windows dentro de la red, aunque también la información capturada con tcpdump puede ser pasada a equipos con este sistema operativo, sin embargo

[2] Sistemas Digitales, empresa proveedora de equipamiento y asesoría informática. Dirigida por el autor de la presente obra.

debido a que se trata de probar en escenarios diversos y de acuerdo a las tendencias actuales, utilizamos una red con equipos tanto con Windows como con Linux.

Otro requisito de la red es que tenga conexión a Internet, esto es requerido porque se necesitan hacer pruebas con capturas de tráfico Web y de correo electrónico, a más de ser una forma de hacer las pruebas con host remotos y con el sistema de resolución de nombres DNS.

4.2 Instalación de Linux.

Para estas pruebas de ha procedido a instalar el sistema operativo Linux Red Hat versión 9.0. Se ha optado por instalar Linux debido a que es un sistema que además de ser de uso gratuito, tiene muchas herramientas importantes además su uso está extendiéndose con mucha rapidez y soporta sin muchas complicaciones enlaces con sistemas Windows.

Un inconveniente es que no soporta a la mayoría de módems (IBM, 2000, 12) que se encuentran en el mercado[3], es por eso que la conexión a Internet se ha realizado mediante un equipo distinto.

La instalación se la ha efectuado seleccionando todas las herramientas de red y los servicios necesarios, se ha elegido usar una tarjeta de interfaz de red Intel de 100 Mbps, a la cual se asignó la dirección 192.168.1.99, dirección dentro del grupo de direcciones reservadas para el uso público, de tal manera que no tengamos inconvenientes al conectarnos a Internet; además se configuró la máscara de red como 255.255.255.0, estableciéndose como una dirección de clase C.

Posteriormente se configuró como dirección de puerta predeterminada a la 192.168.1.10, que corresponde al servidor proxy mediante el cual nos enlazaremos a Internet y a las redes remotas con las cuales haremos las pruebas de conectividad y demás planificadas en este trabajo.

Además se ha procedido a colocar las direcciones de los hosts con los cuales mantendremos comunicación.

[3] En: http://www.o2.net/~gromitkc/winmodem.html se puede encontrar un listado de los modem compatibles con Linux

Un siguiente paso para que funcione las solicitudes de resolución de nombres de Internet ha sido el configurar los servicios de DNS, se seleccionó inicialmente una dirección de servidor DNS recomendado por el software proxy, pero al tener tiempos de resolución excesivamente largos o incluso sin recibir respuesta, se procedió a hacer una captura de datos en el equipo que se encontraba conectado directamente al Internet, y al realizar la consulta se pudo observar que el número de DNS que utilizaba el ISP para darnos el servicio, que fue el 200.55.224.68, valor que después de colocado funciono muy bien.

El enlace físico requirió de un cableado UTP y un switch formando una red ethernet.

4.3 Instalación del servidor Proxy

Para proveer el servicio de Internet a la red se procedió a instalar la versión 5.2.2 del Wingate. Se escogió este servidor porque es uno de los más utilizados por los servicios que brinda como servidor de Web, mail, noticias, etc. Además que brinda facilidad en la configuración.

La versión 5.2.2 fue descargada directamente desde la página Web (wingate, 2003) en Internet y se configuró de acuerdo al manual online que presenta.

La instalación se la realizó en un equipo con el sistema operativo Windows 98, conectado a la red ethernet de pruebas mediante un adaptador de red 3COM a la que se asignó la dirección 192.168.1.10, dirección que estaba libre para no interferir con otros equipos de la red aparte de ser también una dirección reservada de uso público.

Posteriormente se procedió a configurar la conexión a Internet que usará el Wingate para brindar el servicio, para lo cual se habilitó la conexión mediante EtapaOnline, especificando que use el nombre de usuario *dsystems*, reintente 3 veces el establecimiento de la conexión y espere a que hayan 5 minutos de inactividad antes que se desconecte automáticamente la conexión.

4.4 Configuración de los clientes de Internet.

Para configurar el cliente Windows xp de dirección 192.168.1.100 se procedió en el caso de Internet, a deshabilitar la conexión por modem y a habilitar el servicio de proxy con la dirección del equipo en el que se ejecuta wingate que es 192.168.1.10, esto en las

propiedades de la conexión a internet (Menú herramientas, opciones de Internet, conexiones, configuración de LAN)

Para que las pruebas de conexión con servidores DNS funcionen correctamente, se ha procedido a configurar la interfaz de red adicionando los valores 200.55.224.68 para el servidor DNS principal y 131.107.1.7 para el servidor DNS secundario, valores que como se vio en la instalación y configuración de linux fueron obtenidos gracias a la captura del tráfico de la interfaz serie (módem) durante consultas de resolución de nombres al establecer una conexión con una página web y en el caso del servidor DNS secundario, tomando el dato de la sugerencia de la ayuda del servidor proxy Wingate.

Después de terminadas estas configuraciones se procedió a realizar las pruebas de conectividad internas y con host de la Universidad del Azuay y de la Universidad de Buenos Aires, comprobándose el correcto funcionamiento. En el siguiente gráfico se diagrama cmo quedó conformada la estructura final de la red.

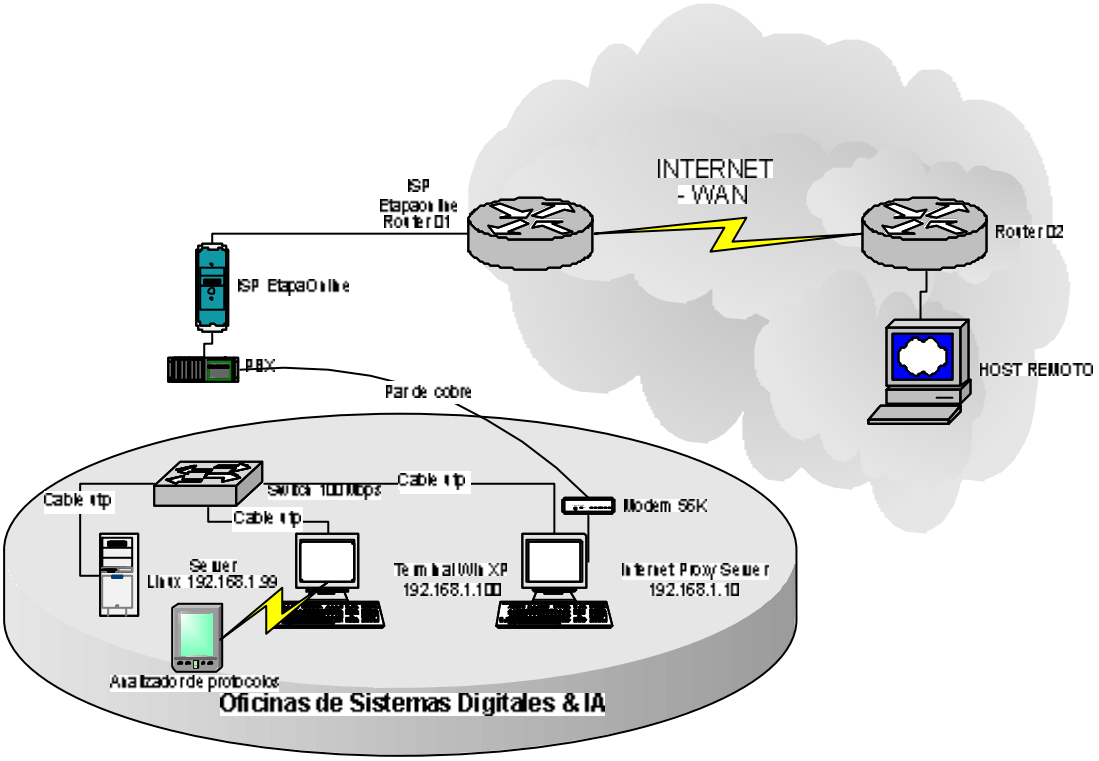


Figura 13. Red de pruebas finalizada

4.5 Instalando las herramientas de captura

Un paso final para proceder a la realización de los trabajos prácticos fue la instalación de los programas analizadores de tráfico, en este caso se utilizó el Ethereal, obtenido desde la

página Web www.ethereal.com. Este analizador necesita además del programa WinPcap_3_01_a.exe para que pueda funcionar, el cual fue descargado de la misma página.

Se instaló también el programa Optiview Protocol expert, con el que se pretendía hacer el ultimo trabajo práctico aprovechando a sus resultados gráficos que proporciona una manera resumida de ver la información, pero no fue utilizado en vista de la imposibilidad de analizar tramas capturadas con el tcpdump ni el ethereal. El programa fue descargado de www.flukenetworks.com.

En analizador que finalmente se utilizó en la práctica fue el *Network Monitor* de *Distinct*, el cual se lo obtuvo de www.distinct.com, analizador que si lee capturas de tcpdump y ethereal previo un proceso de conversión con el que el programa cuenta.

Conclusiones del capítulo 4:

El armado de la red, fue una tarea de complejidad media, ya que fue necesario buscar métodos de interconexión de redes, solucionar el problema de conectar linux a Internet, sin embargo luego de realizado el trabajo, no parece tan difícil y se logró el objetivo de armar el escenario necesario para cada uno de los casos, con la utilización de pocos recursos materiales.

La configuración de la red actual ciertamente aseguraba el funcionamiento del correo electrónico y del servicio web, pero no era tan seguro que los comandos como dig, tracert y otros funcionasen fuera de la red local, puesto que los IPS pueden permitir únicamente determinados servicios, sin embargo al realizar las pruebas se pudo comprobar con regocijo que todos los comandos daban el resultado esperado, como si se tratase de una red normal enlazada por medio de un router a la red principal del ISP, con lo cual las prácticas ya podían ser realizadas con todos sus requerimientos de comandos y servicios.

CAPITULO 5

IDENTIFICACIÓN DE LOS RESULTADOS

5 CAPTURA Y ANALISIS DE LOS DATOS

5.1 Introducción

Para el desarrollo de este capítulo tan importante, se procedió a realizar la captura de la información mediante el uso del analizador de protocolos ethereal, para luego llenar las hojas de trabajo con la información requerida y a continuación elaborar el informe en el cual se analiza las principales características de las tramas capturadas. Esto se hace a la luz de lo que la teoría indica, de tal manera que se pueda ir clarificando tanto los conceptos teóricos como los campos que se observan en las tramas capturadas.

Se desarrolla en orden cada trabajo práctico con su respectivo informe, que incluye los comentarios y conclusiones que de cada uno de los trabajos prácticos se extrae.

Se trata de un procedimiento de investigación experimental, pues usamos como variable el programa que vamos a ejecutar, de tal manera que según el comando ejecutado, observaremos los diferentes protocolos que actúan, de acuerdo a los servicios que requiera.

5.2 Desarrollo del Trabajo Práctico 1 - PING

Realizado por:

Hernán Quito

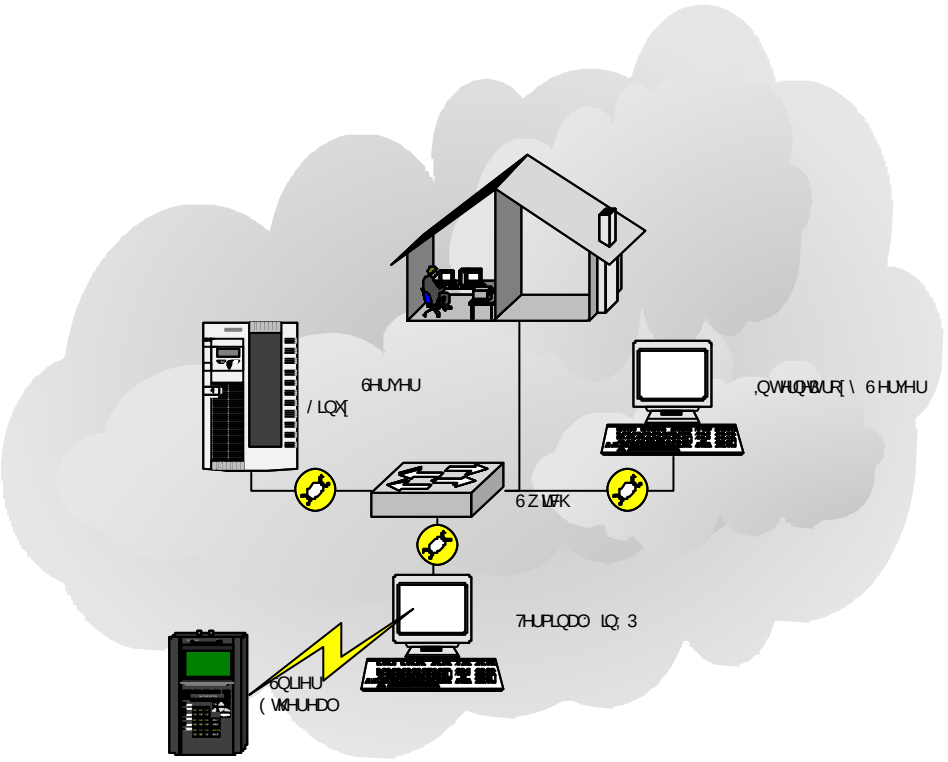
Tema:

Análisis de tramas portadoras de comandos PING

Objetivo:

El objetivo de este trabajo práctico es realizar una captura de paquetes generados con el comando *Ping* para verificar conectividad entre hosts. Se pretende iniciar el trabajo práctico con el uso escenarios que gradualmente se incrementarán en complejidad para observar otros mensajes protocolares, así que se deberá verificar la operación del protocolo ARP, reconocer la estructura de las tramas Ethernet y de los datagramas IP, así como inspeccionar los mensajes ICMP que se intercambien los equipos.

Maqueta:

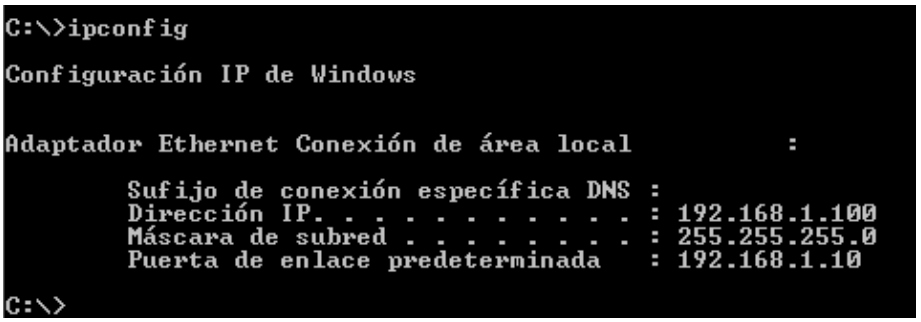


Escenario:

1. Se desea conocer si hay conectividad entre dos equipos localizados en una LAN, dentro de un segmento de red ethernet común.

Lista de Tareas a realizar

1.7. Obtener datos de la configuración de la red con el comando *ipconfig:*



1) Dirección IP __192.618.1.100_____
2) Máscara de subred _____255.255.255.0_____
3) Puerta de enlace predeterminada _192.168.1.10
4) Clase de red _____C_____
5) Dirección de red _____192.168.1.0_____
6) Dirección de broadcast ____192.168.1.255_____
7) Rango de direcciones de host ____.1 a .254_____

1.8. [ ] ejecución de comando *"arp -a"*

1.9. [ ] Inicio de captura del programa ethereal

1.10. [ ] ejecución de comando *"ping 192.168.1.10"*

```
C:\Documents and Settings\Hernan>ping 192.168.1.10

Haciendo ping a 192.168.1.10 con 32 bytes de datos:

Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Hernan>_
```

1) Cuantos mensajes ICMP se produjeron_____8_____
2) Ha recibido el destino los mensajes ICMP_____si_____
3) Tiempo de vida_____128_____
4) Tiempos de ida y vuelta:
   min__0____máx.__0____media__0___

1.11. [ ] ejecución de comando *"arp -a"*

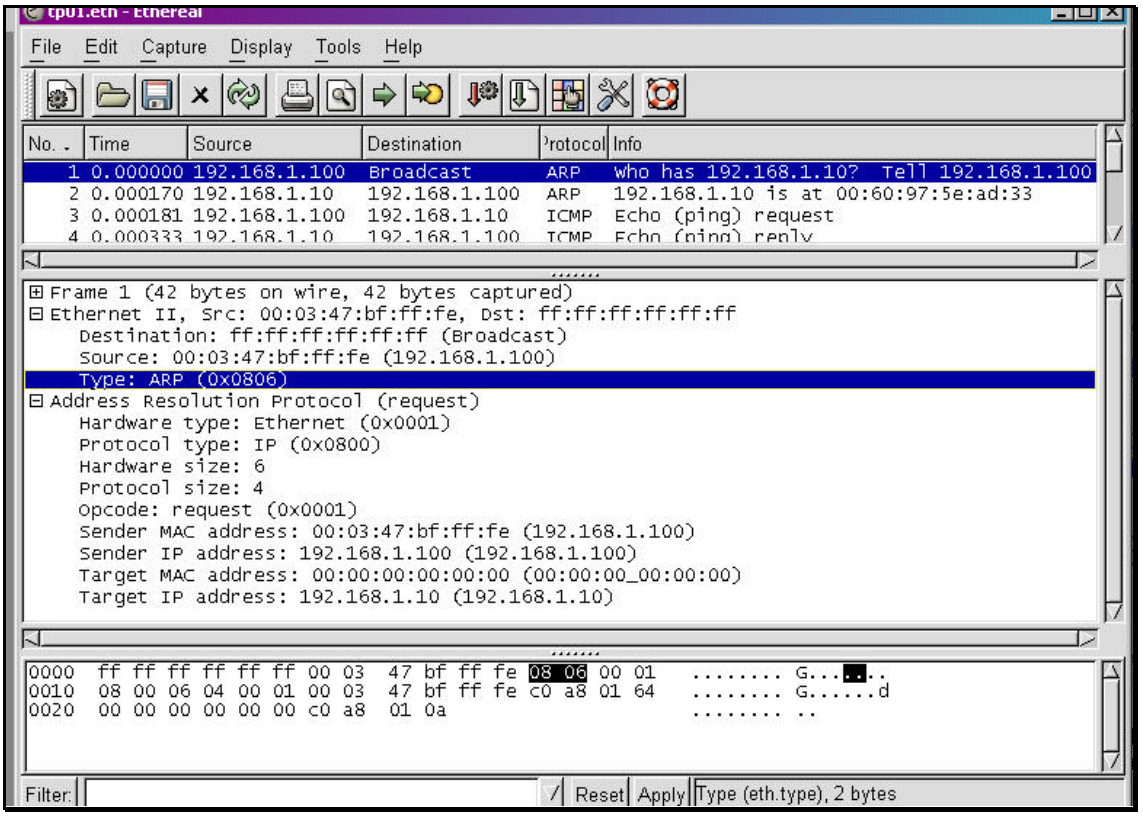
1.12. [ ] Finalizar la captura y salvar el archivo capturado como *"Captura_p1_e1.txt"*

Análisis TP 1:

Parte 1: Resolución de Direcciones MAC

Directamente mediante el uso de las herramientas básicas se ha podido verificar la existencia de conectividad entre los dos equipos de la red.
El comando *ipconfig* nos ha dado la información de nuestro equipo.
Con el primer comando *arp –a* podemos verificar que la tabla de direcciones MAC en nuestro equipo está vacía

Cuando se ejecuta el comando *ping*, según dice la teoría, se produce una solicitud broadcast para conocer la dirección MAC de la dirección solicitada como primer paso. Esto se puede comprobar analizando la trama capturada como se ve a continuación:

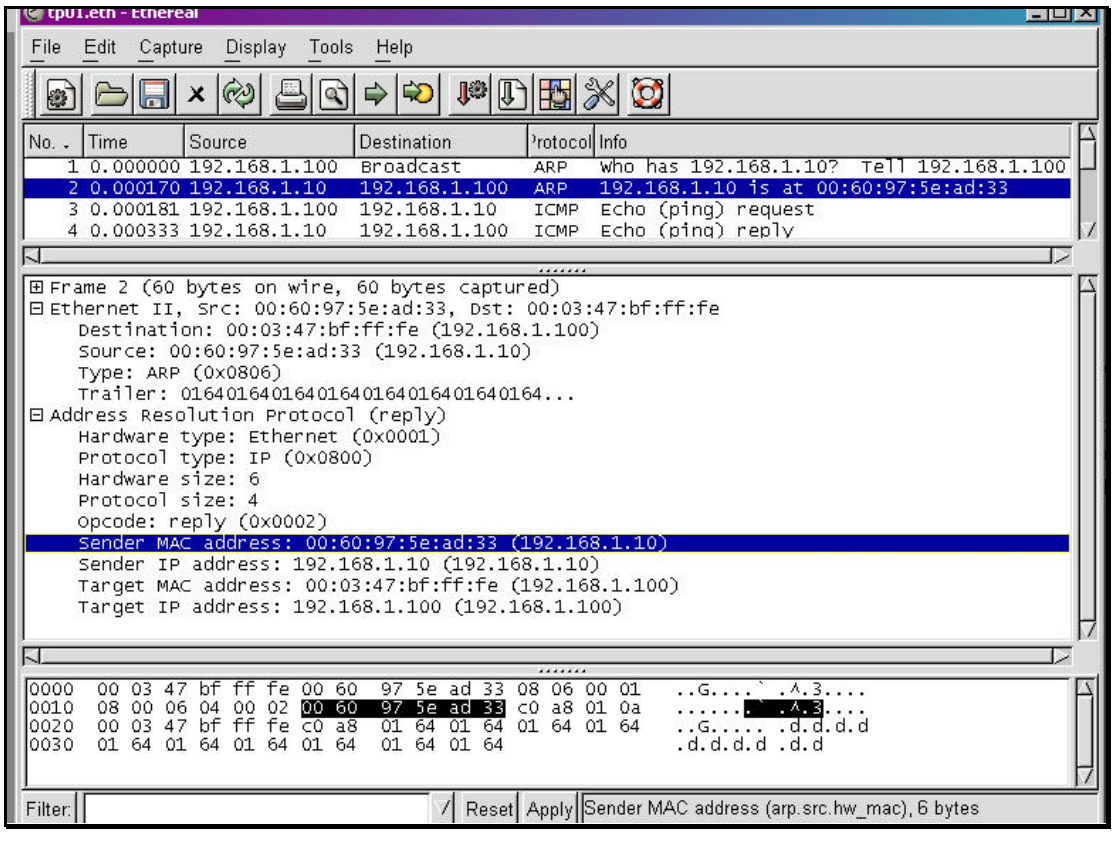


La trama número 1 costa de 42 bytes y se puede verificar en la ventana superior que el origen de la trama es nuestro equipo con destino a todos los equipos de la red usando el protocolo ARP para serolver la dirección MAC. En esta ventana resumen se puede observar que se plantea la pregunta quién tiene la dirección MAC para la dirección IP 192.168.1.10, pregunta realizada por el equipo 192.168.1.100.

En la segunda ventana, se detallan los datos capturados en función de cómo están estructurados, así la trama completa es de 42 bytes, sobre una red ethernet II, se puede ver el detalle de la dirección origen y destino expresado en el número MAC del dispositivo de red, nótese que el campo destino de la trama ethernet, en su sección destino (*Destination*) tiene un valor de ff:ff:ff:ff:ff:ff, valor que indica que se trata de un mensaje para todos los equipos del segmento de red. También se observa el tipo de protocolo, que en este caso es ARP como está resaltado en la imagen.

El protocolo ARP del que esta compuesto la trama se detalla también, allí podemos observar algo importante que es el tipo de protocolo usado, que es IP. El otro campo que nos interesa verificar en este caso es la dirección MAC del destino, así como su dirección IP, mientras que el destino se ve que es broadcast al tener todos los 8 bits a 0, lo que significa ninguna MAC definida, pero si tiene el dato de la dirección IP, pues es conocida al ser la invocada explícitamente por el comando ping.

La tercera ventana muestra en la parte izquierda los mismos datos pero en formato hexadecimal, y la selección resaltada corresponde al campo que se ha seleccionado en la ventana intermedia, mientras que a la derecha podemos verlo en formato ASCII.

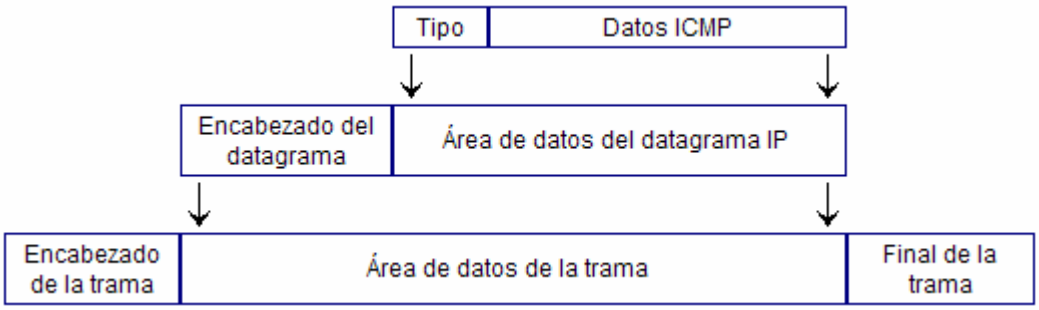


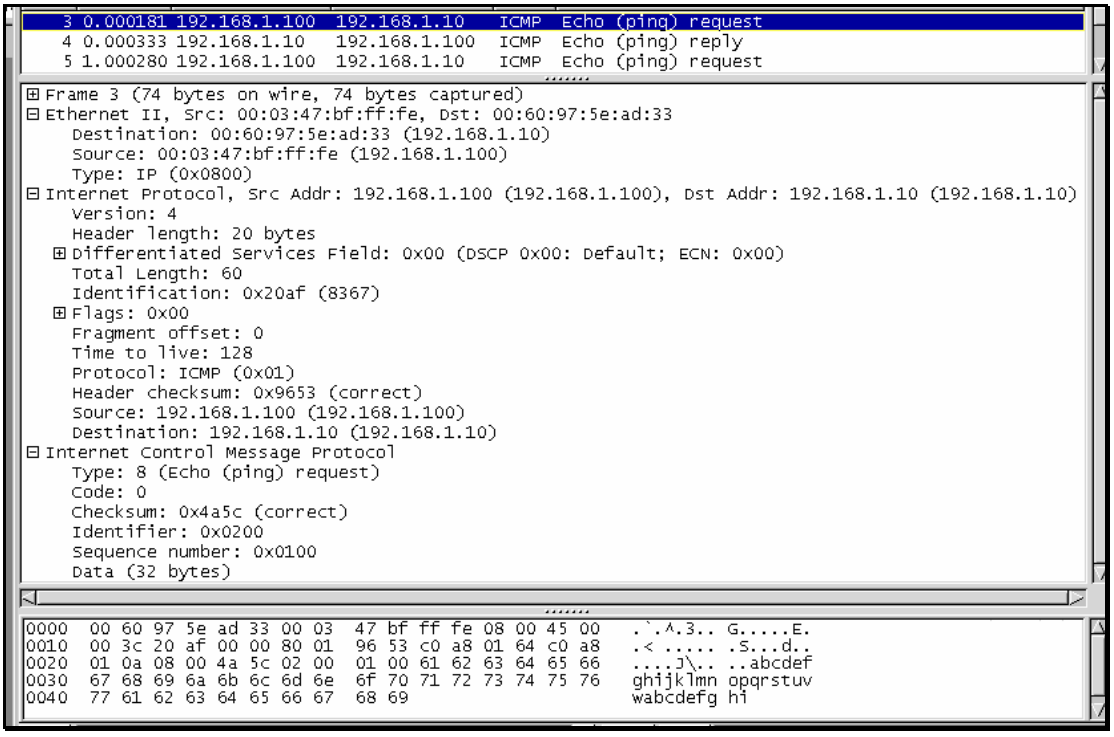
La segunda trama es la respuesta del destino con su dirección MAC, como se puede ver en la figura anterior en la línea resaltada, y dice que 192.168.1.10 está en la MAC 00:60:97:5e:ad:33.

En el detalle del protocolo ARP se determina que se trata de una respuesta (reply) y se nota que la información para poder transmitir está completa, lo cual aparece desde la línea resaltada, es decir tenemos las direcciones IP de las máquinas que necesitan comunicarse, también se tienen las direcciones MAC, para que ethernet pueda enviar la información.

Parte 2: Envío

Es en la tercera trama en la que se produce el envío de información útil, en nuestro caso por ser un comando ping, la información tiene el protocolo ICMP, que es para mensajes de control. Para poder comparar, se grafica la composición de las tramas:





El resumen nos dice que se trata de un mensaje echo request, el detalle ethernet nos informa las direcciones MAC origen y destino, necesarias para que el mensaje llegue y que el destinatario nos pueda contestar a nuestra MAC, además especifica que transporta un protocolo IP (*type IP*). Es importante notar que el tamaño de la trama capturada es de 74 bytes, los cuales están formados por 14 bytes de cabecera ethernet (6 bytes de dirección origen, 6 de destino y 2 de tipo) y los 60 restantes son de la trama IP, como comprobaremos posteriormente. Vemos aquí que la teoría es precisa.

A continuación repetimos la figura de la cabecera IP para poder verificar la concordancia de la teoría.

<table>
<tr><td>Ver (4 bits)</td><td>Hlen (4 bits)</td><td>TOS (8 bits)</td><td colspan="2">Longitud Total

(16 bits)</td></tr>
<tr><td colspan="3">Identificación (16 bits)</td><td>Flags
(3 bits)</td><td>Desp. De Fragmento (13 bits)</td></tr>
<tr><td>TTL (8 bits)</td><td colspan="2">Protocolo

(8 bits)</td><td colspan="2">Checksum (16 bits)</td></tr>
<tr><td colspan="5">Dirección IP de la Fuente (32 bits)</td></tr>
<tr><td colspan="5">Dirección IP del Destino (32 bits)</td></tr>
<tr><td colspan="4">Opciones IP (Opcional)</td><td>Relleno</td></tr>
<tr><td colspan="5">DATOS</td></tr>
</table>

El detalle del protocolo IP nos indica:

La versión de IP, que es la 4

La longitud de la cabecera (*Header length*), que es la estándar de 20 bytes

El campo Tipo de Servicio (*Type of service TOS*) tiene el valor 00, que significa no minimizar el retardo, no maximizar el throughput, no maximizar la fiabilidad, no minimizar el costo monetario; valores que como hemos visto en la teoría son típicos del protocolo ICMP de pregunta o error.

A continuación vemos el campo Longitud total (*total length*) que es de 60 bytes

El campo identificación es el 8367

Las banderas (*flags*) están establecida con los valores 00, que significa no establecido el bit de no fragmentar (*don´t fragment*), y al no tratarse de tramas que han sido fragmentadas, tampoco está activo el bit de más fragmentos (*more fragments*)

El campo desplazamiento de fragmento (*fragment offset*) indica 0 ya que no se ha fragmentado el mensaje

Tiempo de vida (*Time to Live*) está con el valor de 128, es decir que es el valor establecido por el comando ping para este mensaje.

El campo protocolo indica que se trata del protocolo ICMP al tener el valor de 01

El campo chequeo de error (*checksum*) muestra que se ha realizado la comprobación correctamente

La dirección IP origen que es 192.168.1.100

La dirección IP destino que es 192.168.1.10

La información que lleva el protocolo ICMP es la siguiente:

Tipo de mensaje es el 8, que significa un *echo request*

El código es 0, no significa nada debido al tipo de mensaje, en otros casos nos indicará detalles de errores

La suma de comprobación está correcta

El identificador es 0x0200

El número de secuencia es 0x0100

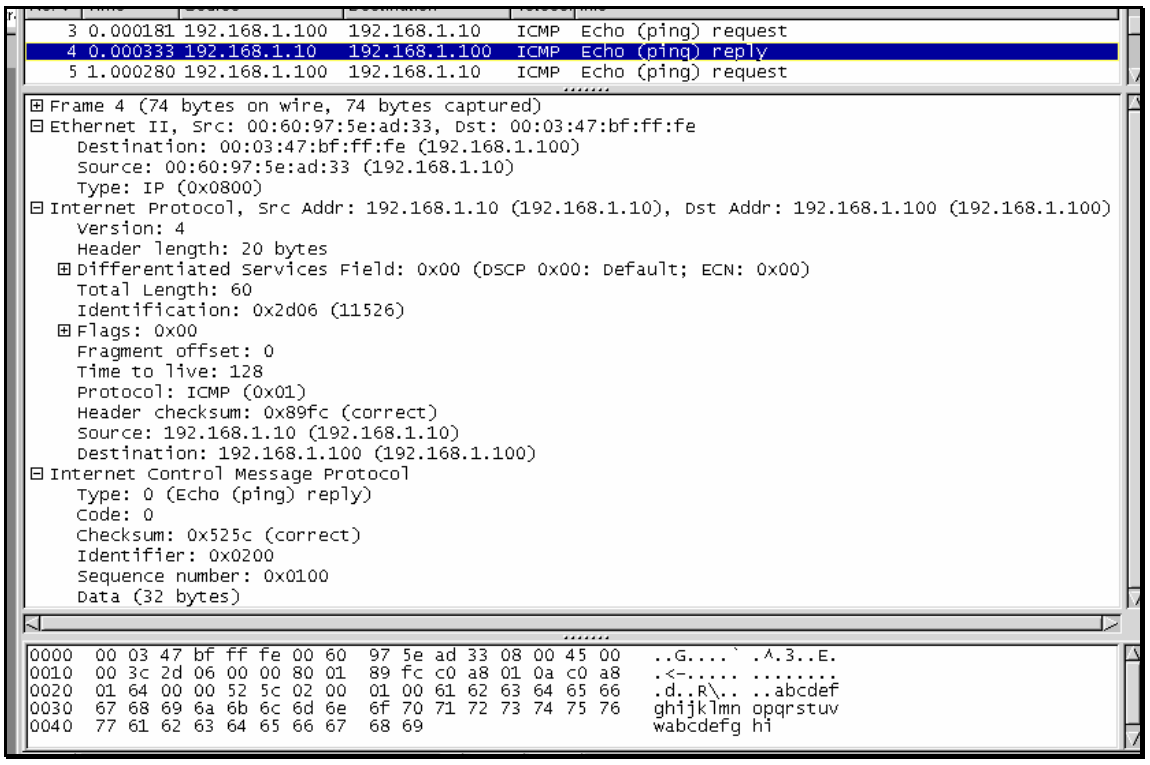
Y los datos son 32 bytes

Mediante estos datos podemos obtener detalles de errores, en este caso al tratarse de un echo request, no hay mucha información.

Parte 3: Recepción de la información

En la cuarta trama se puede ver la respuesta a la petición por parte del comando ping

Aquí se puede observar que el número de identificación del protocolo IP es un número muy distinto al del datagrama anterior, y es que cada host coloca su número; se comprobó también que los números son secuenciales verificando los datagramas enviados por el mismo host.



Asimismo el protocolo ICMP lleva en su cabecera el tipo 0, que es el que corresponde a la respuesta a un pedido de *echo request*, es decir se trata de un mensaje tipo *echo reply*

El campo identificador es el mismo para el grupo de mensajes producidos por ping para poder determinar que se trata de la misma prueba.

También se comprueba que el número de secuencia corresponde a la del datagrama recibido (el anterior), así cada par de datagramas tienen el mismo número de secuencia, que los identifica como respuesta a la solicitud requerida.

Conclusiones del TP1:

En este primer caso se ha podido verificar la teoría con la práctica, y comprender el funcionamiento del comando ping, así como también del protocolo ARP.

El proceso de toma de información fue sencillo, pues se trata de únicamente cambiar mensajes entre dos computadoras conectadas directamente sin necesidad de encaminador alguno. Este comienzo ha sido bueno puesto que se ha logrado analizar desde la capa más inferior y con menos datos, lo cual ha sido comprensible.

El uso de una guía de procedimientos u hoja de trabajo ha sido muy útil, ya que siguiendo las instrucciones, permitió desarrollar el trabajo rápidamente.