UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA

UNIDAD ENSENADA

"USO DE HERRAMIENTAS DE LIBRE DISTRIBUCIÓN EN APOYO A LA GESTIÓN DE REDES DE DATOS Y TELECOMUNICACIONES DEL DEPARTAMENTO DE INFORMACIÓN ACADEMICA, CAMPUS ENSENADA"

T E S I S

Que para cubrir parcialmente los requisitos necesarios para obtener el grado de MAESTRÍA EN INGENIERÍA presenta:

JESÚS VELÁZQUEZ PADILLA

Ensenada Baja California, México. ***Agosto del 2004***

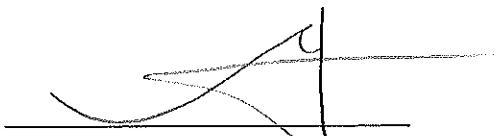
TESIS PRESENTADA POR

ING. JESÚS VELÁZQUEZ PADILLA

Y APROBADA POR EL SIGUIENTE COMITÉ:

MC Juan de Dios Sánchez López
Director del Comité

MC Oscar Ricardo Osorio Cayetano
Sinodal del Comité



MI Juan Pablo Torres Herrera
Sinodal del Comité

Agosto del 2004

DEDICATORIA

A MI ESPOSA E HIJOS POR EL AMOR, CARIÑO Y PACIENCIA QUE SIEMPRE HAN MOSTRADO, GRACIAS.

A MIS PADRES POR SI GUIANZA Y GRAN EJEMPLO,

A MIS HERMANOS POR SU CARIÑO,

A MIS COMPAÑEROS DE TRABAJO POR SU APOYO Y COMPAÑERISMO Y DE FORMA MUY PARTICULAR A MEMO Y A HUGO.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

I INTRODUCCIÓN

1.1. ANTECEDENTES

En agosto de 1991 se inaugura el Centro de Cómputo Universitario Unidad Ensenada (CECUUE) conocido originalmente como *CEPRODET (Centro de Productividad y Desarrollo Tecnológico)* El proyecto original proponía la creación de un centro capaz de cubrir las necesidades de cómputo de la Universidad Autónoma de Baja California (UABC) campus Ensenada, y que además aportara productos y servicios informáticos a la comunidad.

Este proyecto partió de aportaciones hechas por las diferentes escuelas de la unidad. Equipos de cómputo y personal se integraron al departamento de informática, punto de partida del proyecto. También se hicieron compras y donaciones de computadoras de distintas plataformas, dando así inicio a lo que ahora se conoce como l*as redes de cómputo y telecomunicaciones del CECUUE,* y recientemente conocido como el Departamento de Información Académica (DIA).

Antes de abordar la situación actual de las redes de cómputo y de telecomunicaciones del DIA empezaremos por mencionar algunos de los aspectos originales de las mismas.

- Equipos personales con sistema operativo Novell en una topología tipo ducto
- Terminales, servidores e impresoras tipo HP-UNIX
- Estaciones de trabajo y servidores APOLLO
- Área de graficación que incluía: impresoras láser, impacto, *scanner*, *plotters*, etc.
- Aulas equipadas para trabajo en grupo o de forma individual.
- Enlace vía satélite de [1]64kbps utilizado para telefonía y transmisión de datos.

[1] Canal digital de transmisión medido en bits por segundo (bps)

Adicionalmente se contaba con ocho personas de planta además de becarios y alumnos de servicio social.

Después de varios años el proyecto del centro de cómputo cobro forma, se adquirió más equipo, se contrato más personal y se ofrecieron nuevos servicios. Un aspecto importante en la historia de las redes del DIA fue la instalación de un troncal para comunicar las escuelas y facultades. Dicho troncal, en sus inicios, constaba de cable coaxial pero posteriormente fue reemplazado por un robusto enlace de fibra óptica.

A momento de escribir este documento, el DIA cuenta con siete aulas equipadas: cinco para clases y dos más para trabajo individual. Dentro del mismo se dispone de un poco mas 300 equipos de computo compatibles y distribuidos a lo largo sus instalaciones, oficinas, salas equipadas, [2]*site*, etc. Se actualizo las plataformas de cómputo tanto en hardware como software quedando de la siguiente manera:

- Servidores Web, correo, archivos, nombres, etc. con sistema operativo LINUX
- Computadoras personales como clientes con sistema operativo Windows XP
- Mini computadoras *HP-LINUX* con terminales y equipo personal emulando ambiente *Unix*
- Mini computadoras y estaciones de trabajo *SUN*

En cuanto conectividad se adquirió el siguiente equipo:

- [3]*Switch* y [4]*routers* Cabletron SSR-2000 y SSE-8000
- *Switch* Enterasys y Netgear

[2] Área designada para concentrar cableado y dispositivos redes de datos y telecomunicaciones
[3] Dispositivo conectividad de alta eficiencia utilizado para comunicar dispositivos de red

También se mejoro la comunicación del campus adquiriendo e instalando los siguientes enlaces:

- Un [5]canal E1 para Internet
- Fibra Óptica de varios pares al CICESE para enlace privado y conexión a Internet 2
- Enlace de radiofrecuencia a 2.4Ghz a 11 Mbps a Extensión Universitaria y Escuela de idiomas de la UABC.
- Un canal E1 al campus Mexicali para transmisión de voz, datos y video

1.2. JUSTIFICACIÓN

Las actividades académicas, administrativas y de investigación del campus Ensenada dependen en gran manera de una conectividad de datos confiable tanto interna como externa. Por ello es importante garantizar el acceso a la información supervisando en todo tiempo una operación correcta de los dispositivos responsables del tráfico. Existen aplicaciones que permiten un monitoreo automático y grafico de dichos dispositivos, lo cual permite conocer la situación actual y tendencias de los mismos

Un punto importante en las actividades académicas diarias del campus, son las aulas y áreas equipadas del DIA, pues estas exigen un acceso confiable a la red. Una gran cantidad de usuarios asisten a estos sitios y lo hacen en un horario bastante amplio de tal manera que una falla de conectividad resulta muy negativa. Causando tiempo muertos para los usuarios y en algunos casos hasta perdidas de información dañando así la imagen del DIA. Los servicios que se afectan son el almacenamiento de información, acceso a impresoras, Internet e Internet 2, etc.

---

[4] Dispositivo de conectividad para comunicar redes de datos
[5] Enlace digital de datos equivalente a 2.044Mbps

Debido a lo diverso de las redes del DIA y lo amplio de sus dimensiones se hace necesario la utilización aplicaciones o herramientas de apoyo al monitoreo de los dispositivos de conectividad. El uso de estas herramientas permite, entre otras cosas, tener acceso de forma automática a información estadística general y detallada de los mismos.

Los dispositivos de conectividad principales del DIA (switches, routers y servidores) soportan el uso de herramientas basadas en el protocolo de gestión SNMP (*del ingles, Simple Network Managment Protocol*). Mediante dicho protocolo el administrador utiliza algunas herramientas basadas en este protocolo para realizar de forma más rápida y automática tareas como lo es la administración del dispositivo, su configuración y monitoreo de interfaces de red.

1.3. SUPUESTO

Es posible mantener operando de forma correcta las redes de cómputo y telecomunicaciones del DIA mediante el uso de herramientas de monitoreo que apoyen en las tareas de:

- Análisis y medición de tráfico
- Medición y monitoreo de enlaces de conectividad interna y externa
- Detección de abusos en los enlaces
- Detección de actividades sospechosas en las redes y
- Optimización y planeación de la red

1.5. OBJETIVO GENERAL

Implementar diferentes herramientas de gestión que contribuyan a una eficiente administración del entorno de red de computadoras del DIA, realizando las pruebas en "tiempo real" para verificar el cumplimiento de recomendaciones para la utilización de las redes del campus.

1.6. OBJETIVOS ESPECÍFICOS

- Buscar, instalar, y configurar aplicaciones de apoyo en las tareas monitoreo de tráfico de redes, que cumplan con la característica de libre distribución.
- Integración de las aplicaciones y generación de reportes en ambiente Web

II GESTIÓN DE REDES

2.1. INTRODUCCIÓN

La supervisión y control de los diferentes dispositivos de la red así como su continua actualización son tareas muy importantes del personal de redes. Dentro de sus funciones esta detectar y corregir problemas de comunicación a la brevedad posible. Estas actividades son muy importantes para el administrador y a la vez difíciles si se trata de redes amplias y heterogéneas, es decir, redes de plataformas distintas.

En un esfuerzo por aplicar una administración efectiva en la redes de datos y comunicaciones, se estableció la Gestión de Redes que entre otras cosas permitan automatizar las funciones de monitoreo, control y configuración remota. Casi todos los dispositivos de la red ofrecen información acerca de su estado de operación. Esta información es almacenada en bases de datos especiales llamadas *MIB* (*del ingles, Managment Información Base*). La información almacenada varia dependiendo del dispositivo que se trate, por ejemplo paquetes perdidos por un enrutador, su memoria disponible e utilizada, utilización de alguna interfase, etc. Los datos obtenidos de la base de datos son utilizados para determinar el comportamiento estadístico así como también otra valiosa información.

La gestión de redes se apoya en el protocolo de comunicación SNMP (*del Ingles, Simple Network Managment Protocol*) que permiten acceso a las bases de datos de los dispositivos. El modelo *cliente-servidor* (ver anexo) es utilizado de manera que una computadora *central* corriendo la aplicación funge como *servidor* solicitando información de la base de datos almacenada en *los clientes* (computadoras o dispositivos de red). Los clientes entregan información al servidor según sea el esquema de recuperación previamente establecido.

Para el intercambio de información entre el cliente y el servidor se utilizan los protocolos de transporte común: ***TCP*** (*del ingles, Transport Control Protocol*) y ***UDP*** (*del ingles User Data Protocol*). Sin embargo, la tarea de gobernar este intercambio de información recae sobre el protocolo simple *SNMP*.

2.2. DEFINICIÓN

La ISO (*del ingles, Internacional Standard Organization*) define la gestión de redes como:

"Conjunto de elementos que controlan y supervisan los recursos de manera que la comunicación tenga lugar sobre la red"

Con lo anterior se entiende que la gestión de redes son todos aquellos aspectos necesarios para la planificación, organización y el control de los elementos de red, de manera tal que se garanticen los servicios de las mismas.

2.3. ÁREAS FUNCIONALES

Son cinco las áreas funcionales de la gestión de redes:

Gestión de contabilidad: Es el registro de parámetros de utilización de los servicios de la red. Por ejemplo: espacio en disco, tiempo maquina, impresiones entre otros servicios. Mediante esta gestión es posible disponer de información que muestre la utilización de los servicios por parte de los usuarios con fines tarifarios.

Gestión de Prestaciones: Muestra mediante el análisis de datos tomados de la red la forma en la que la que esta se comporta. Se analizan por igual dispositivos y enlaces a fin de observar su desempeño buscando ofrecer calidad de servicio. Enlaces, servidores y recursos compartidos son ejemplos de elementos de red susceptibles a este análisis tratando de evitar en ellos problemas tales como cuellos de botella.

Gestión de Fallas: Se refiere al uso de aplicaciones que permiten la detección, el aislamiento y la corrección de fallas presentes en los diferentes dispositivos de red.

Gestión de Configuración: Tiene que ver con la configuración de los elementos de la red y se divide de la siguiente manera:

- Configuración Activa. Modifica los parámetros de operación de los dispositivos según se necesite.
- Configuración Pasiva: Utiliza aplicaciones que automatizan el monitoreo en tiempo real de los dispositivos de red.

Gestión de Seguridad: Defensa de los sistemas contra ataques internos y exteriores.

- Seguridad de la información en tránsito.
- Detección de fallos en la seguridad.

2.4. IMPORTANCIA DE LA GESTIÓN DE REDES

La gestión de redes viene a satisfacer aspectos técnicos y funcionales necesarios para la administración efectiva de la red:

Aspectos técnicos:

- Administración de entornos heterogéneos desde una misma plataforma
- Administración de elementos de interconexión
- Interfaces con grandes sistemas
- Interfaz gráfica amigable
- Evolución según las necesidades de los usuarios

Aspectos funcionales:

- Garantizar la disponibilidad de los servicios
- Administración de prestaciones a los usuarios
- Tiempos de respuesta a fallas mas cortos
- Segmentación y clasificación de los problemas para facilitar su solución
- Simplificación de procesos de modificación y configuración
- Apoyo a la toma de decisiones

2.5. ASPECTO HUMANO DE LA GESTIÓN DE REDES

Una gestión de redes eficiente debe contar con dos aspectos importantes: un recurso humano capaz y una colección de aplicaciones de apoyo en la gestión. Ambas partes son esenciales al momento de atender una falla en la red. Por ello, quienes tengan a su cargo la responsabilidad de la red deben conocer en su totalidad la red que administran a decir: topología, dispositivos, Sistemas Operativos, etc. Además, de un conjunto de herramientas de hardware y software necesarios para esta función.

2.6. EVOLUCIÓN DE LA GESTIÓN DE REDES

Tradicionalmente la gestión de redes ha contado con aplicaciones para garantizar su desempeño, pero solamente del tipo *propietarias*, en donde la gestión es solo posible para equipos de la misma compañía o plataforma. Sin embargo, en la actualidad la mayoría del equipo que se fábrica se hace apegado al estándar de gestión SNMP. Para el caso de dispositivos que no son compatibles con el estándar, existen actualización de [6]firmware o [7]hardware.

[6] Programa almacenado en circuiteria

La gestión es una actividad que se ha venido formalizando gracias a los esfuerzos de algunos grupos de trabajo, los cuales durante la década de los noventa desarrollaron diversas iniciativas con el objetivo de ofrecer los primeros borradores de lo que serían las recomendaciones y estándares.

2.7. ESTANDARIZACIÓN DE GESTIÓN DE REDES

Entre los organismos que han intervenido para la estandarización de la gestión de redes se pueden mencionar dos grupos principales: Los grandes operadores de redes de telecomunicaciones y aquellos que solo gestionan redes de computadoras (Figura 1).

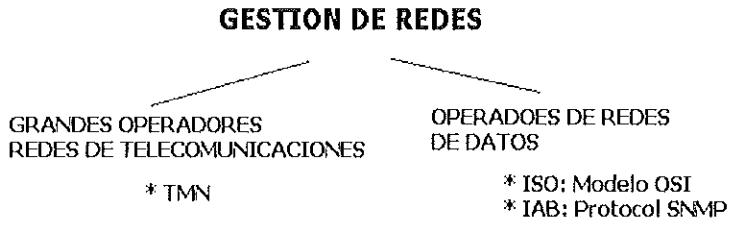


Figura 1. Organismos participantes en la estandarización de la gestión de redes

7

[7] Circuiteria disponible regularmente en forma de módulos

III PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED (SNMP)

3.1. INTRODUCCIÓN

En 1988, el comité de actividades de Internet determino la estrategia de gestión para TCP/IP (del ingles, Transport Control Protocol / Internet Protocol) que significo el nacimiento de dos esfuerzos paralelos: una solución a corto plazo, SNMP, y la solución a largo plazo, CMOT (*del ingles, Common Management Information Protocol*).

La solución CMOT pretendía implantar los estándares del modelo de gestión de OSI (*del ingles, Open System Interconection*) en el entorno Internet (TCP/IP). Sin embargo, esta solución enfrento problemas derivados de la demora en la aparición de especificaciones y la ausencia de implementaciones prácticas. Como consecuencia de ello, esta iniciativa fue paralizada en 1992. En cuanto a la solución SNMP aparece como una extensión del protocolo de gestión de red para *gateways* SGMP (*del Ingles, Simple Gateway Monitoring Protocol*), convirtiéndose en 1989 en el estándar reconocido por Internet. SNMP es un protocolo a nivel de aplicación que ofrece servicios de gestión para observar, controlar y administrar las instalaciones de la red. Debido a su flexibilidad y extensibilidad se ha convertido en el estándar de facto para la gestión de redes

3.2. FUNCIONES DEL PROTOCOLO SNMP

- supervisión del rendimiento de la red y su estado.
- Control de parámetros de operación.
- Obtención de información de fallos
- Análisis de fallas

3.3. ARQUITECTURA SNMP

Se basa en una relación cliente-servidor donde se establece un dialogo entre el gestor y un agente con la finalidad de intercambiar información (figura 2). El gestor es un programa instalado en una estación de gestión y el agente es una *inteligencia* alojada en el dispositivo a gestionar. El intercambio de información entre ambas entidades, se da en forma de preguntas y respuestas que corresponden a tipos particulares de paquetes (trap, get, set, etc.) enviados hacia puertos específicos (161 y 162).

En caso de que existan perdidas de paquetes, el protocolo incluye un mecanismo de reenvió para los mismos.

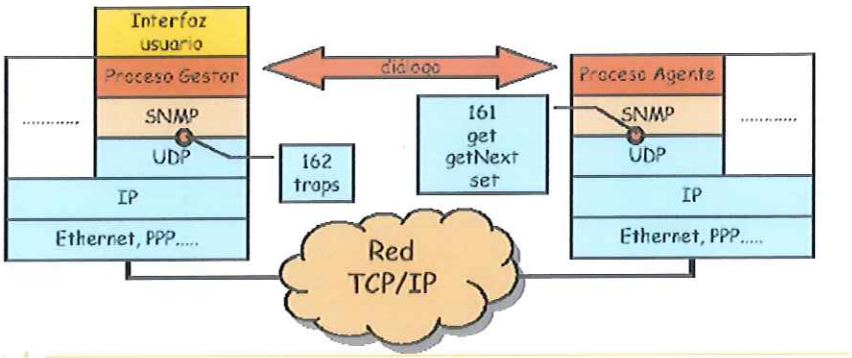


Figura 2. Arquitectura del protocolo SNMP

3.4. FUNCIONAMIENTO.

Este protocolo surge como una herramienta que simplifica la gestión de red sin importar la plataforma de operación de los dispositivos. Opera bajo la arquitectura de Cliente-Servidor, donde por un lado el cliente es una computadora conocida como *estación de gestión* y por el otro el servidor es una "inteligencia" llamada *agente* que reside en algún dispositivo de la red. Esta basado en el envió de paquetes tipo [8]UDP por lo que no se considera un servicio orientado a conexión.

[8] UDP Por sus siglas en Ingles *Unit Data Protocol* se refiere a la unidad mínima de transferencia posible

Cada dispositivo gestionado cuenta con un agente, cuya función es recabar información, y una base de datos o MIB. El *cliente* por su parte, es un software instalado en la estación de gestión, que interactúa con los agentes solicitándoles la información almacenada en sus bases de datos para efectos de análisis estadístico, de control y de configuración.

La comunicación entre ambos se realiza mediante el intercambio de paquetes de información del tipo UDP en ambas direcciones (figura 2).

SNMP opera en la capa de aplicación (capa siete del modelo OSI) y de igual modo tiene equivalencia con las capas del modelo TCP/IP. (ver anexo)

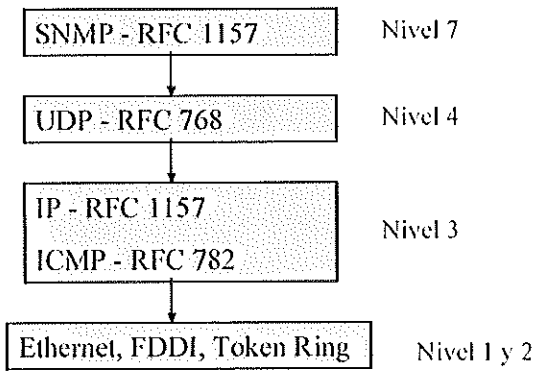


Figura 3. SNMP y la pila de protocolos OSI

La identificación de dispositivos se realiza mediante direcciones IP, que si bien, este tipo de direccionamiento resulta útil por la popularidad que tiene también es cierto que presenta problemas de comunicación en la presencia de problemas de enrutamiento IP.

3.5. ELEMENTOS DEL MODELO DE GESTIÓN SNMP

El modelo de gestión incorpora los siguientes elementos:

3.5.1. AGENTE.

Equipamiento lógico alojado en un dispositivo sensible a gestión. Recoge, almacena y reporta datos del dispositivo gestionado.

3.5.2. GESTOR.

Equipamiento lógico alojado en la estación de gestión de la red. Tiene la capacidad de preguntar a los agentes utilizando diferentes mandos SNMP.

3.5.3. OBJETO GESTIONADO.

Es algún elemento ubicado en el dispositivo gestionado del cual se puede conocer información. Por ejemplo: interfaces disponibles, las sesiones establecidas, entre varios más. Cada elemento a su vez pueden tener variables.

3.5.4. MIB (*del ingles, MANAGEMENT INFORMATION BASE*)

La Base de datos que contiene información acerca de los objetos gestionados. La MIB es utilizada por el agente para reportar al gestor acerca de estado que guardan los dispositivo.

3.5.5. SMI (*del ingles, STRUCTURE OF MANAGEMENT INFORMATION*)

Conjunto de reglas que definen las características de los objetos de la red y como obtiene los protocolos de gestión información de ellos.

3.5.6. SINTAXIS ASN.1. (*del Ingles, ABSTRACT SYNTAX NOTATION*)

Es un lenguaje que permite a diferentes tipos de computadoras compartir información independiente de la arquitectura de las mismas. Es utilizado por SNMP para describir los objetos gestionados y sus variables

3.5.7. INSTRUCCIONES SNMP

En SNMP incorpora cinco mandos u operaciones básicas:

- TRAP
- GETRequest
- GETNEXTRequest
- GETRESPONSE
- SETRequest

Estos mandos son paquetes que se intercambian entre el gestor y el agente de la forma que se muestra en la figura 4.

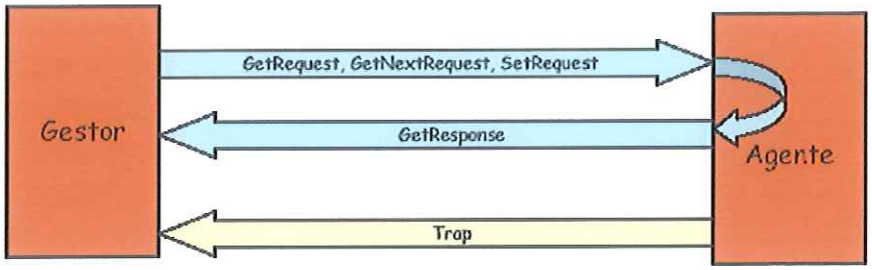


Figura 4. Interacción Gestor-Agente para el intercambio de información

3.5.7.1. TRAP

Es un paquete que *no solicitado* y es enviado por el agente de algún dispositivo a una o varias estaciones de gestión (previamente registradas). La idea del mando Trap es notificar a la estación de gestion la ocurrencia de algún evento considerado importante. Existen seis subtipos de paquetes tipo Trap enviados mediante el protocolo SNMP y recibido en el puerto 161.

3.5.7.2. GETRequest

Solicita los valores actuales almacenados por el agente en la base de datos del dispositivo

3.5.7.3. GETNEXTRequest

Solicita los subsecuentes valores almacenados en la base de datos del dispositivo y que se encuentran en forma de tabla.

3.5.7.4. GETRESPONSE

Paquete enviado por el agente conteniendo la respuesta a solicitudes de SET, GET o GETNEXT

3.5.7.5. SETRequest

Modifica valores en la base de datos del objeto gestionado

3.6. TRAMA SNMP

Los mandos se encapsulan en tramas tipo UDP según se muestra en la figura 5. La trama incluye la versión del protocolo SNMP (utilizado para crear la trama), comunidad a que pertenece la trama e información correspondiente al tipo de mando utilizado. Todas las tramas SNMP son recibidas por la estación de gestión el puerto 161 a excepción las tramas tipo TRAP que son recibidas en el puerto 162.

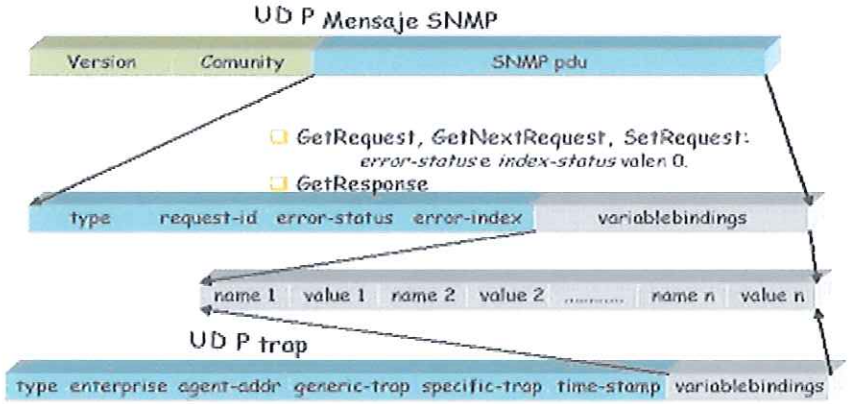


Figura 5. Formato de una trama UDP del tipo SNMP

3.7. COMUNIDAD

Cada trama contiene un campo llamado comunidad utilizado como un método no muy seguro de validar el acceso a la información de los objetos gestionados. Existen dos tipos de comunidades de ***escritura y lectura***. La comunidad de lectura concede derechos de solo lectura en la información de los objetos gestionados. Mientras que la comunidad de escritura permite tanto la lectura como la escritura en la base de datos. Estas comunidades o claves pueden y deben ser configurados por el administrador, ya que de fábrica incluyen valores predeterminados: *Public* y *Private* para lectura y escritura respectivamente. Es común y nada recomendable que los dispositivos conserven estos valores de comunidad una vez instalados en la red, lo que presenta un riesgo en la seguridad ya que cualquiera puede obtener acceso a información privilegiada del dispositivo.

3.8. ACTUALIZACIONES DEL PROTOCOLO SNMP

3.8.1. SNMPv2

En 1993 surge una segunda versión del protocolo SNMP. Se incorporan ventajas sobre la versión anterior como nuevos mensajes de error (tabla 1), además de:

- Transmisión más eficiente de información
- Mecanismo de seguridad: cifrado y autentificación
- Comunicación entre estaciones de gestión

Tabla 1. Mensajes de error agregados en Snmpv2

Operación	Descripción
ColdStart	Reinicio inesperado debido a alguna tipo de falla
WarmStart	Reinicio en caliente normalmente programado
LinkDown	Falla en alguno de los enlaces del sistema
LinkUp	Enlace establecido
EgpNeighborLoss	Falla de enlace con un vecino EGP
AuntentificationFailure	Se recibió mensaje SNMP con comunidad incorrecta

3.8.2. SNMPv3

Presenta las siguientes características:

- Mayor complejidad
- Mejoras en la seguridad
- Arquitectura modular

3.9. SEGURIDAD

Como una medida de seguridad SNMP valida el acceso a la información de la MIB por medio de comunidades. Como se menciono anteriormente, la comunidad de *Public* permite al administrador consultar el estado de los dispositivos. Mientras que *Private* permite alterar la configuración de los dispositivos (asignar valores nuevos a las variables). Este esquema presenta serios problemas de seguridad debido a que cualquier persona con acceso a la red y con un analizador de paquetes puede conocer la comunidad y alterar los parámetros importantes en la red. Conocer la comunidad es fácil dado que las tramas SNMP viajan por la red sin ninguna técnica de seguridad en el caso de SNMP primera versión.

En versiones posteriores a la primera se implemento:

- ✓ Privacidad de los datos, (la información no es visible para usuarios extraños al sistema)
- ✓ Autenticación: evita alterar la configuración de los dispositivos gestionados
- ✓ Control de acceso: restricción de ciertas variables a ciertos usuarios que pueden ocasionar fallas en la red.

IV HERRAMIENTAS DE APOYO A LA GESTIÓN

4. INTRODUCCIÓN

En este capitulo se describirán herramientas utilizadas en el DIA para apoyo en la gestión de redes y telecomunicaciones. Se incluye el procedimiento de instalación de las mismas, así como la forma de utilización y los beneficios obtenidos.

4.1. ETHEREAL

[9]Ethereal es un analizador de paquetes de libre distribución disponible tanto para ambientes Linux como Windows. Esta herramienta configura la interfase de red para capturar paquetes del medio de transmisión de manera que se pueda conocer mediante ellos información importante de la red. La captura se hace en dos modalidades: Modo *normal* donde solo se capturan paquetes dirigidos a la misma estación; y M*odo promiscuo* aceptando cualquier paquete sin importar su destino. Una nota importante es que en ambos modos los paquetes capturados corresponden solo al *segmento de red* al que pertenece el equipo. Esto hace que Ethereal se instale en segmentos que por lo regular correspondan a puntos de entrada y salida de tráfico o bien en segmentos donde se tiene algun interés particular.

Ethereal permite la captura los paquetes por instantes de tiempo (lo que en algunos casos genera cantidades grandes paquetes!) o bien especificando el numero de paquetes a capturar. Después de la captura, los paquetes son desplegados por una interfase gráfica (figura 1) y pueden ser almacenados en archivos en caso de ser necesario.

Al igual que Ethereal existen otros analizadores de paquetes con los cuales se guarda compatibilidad. Algunos ejemplos de esos analizadores son: Microsoft Network Monitor, Sniffer Pro y LanAnalizer.

4.1.1. APOYO EN SEGURIDAD

Cuando un usuario envía información por la red esta puede ser vista por otras personas. Esto se debe a que en algunos casos el contenido viaja en texto plano, es decir, sin ningún mecanismo de seguridad.

Por ejemplo, el programa de acceso remoto *Telnet* no aplica seguridad en su transmisión de datos lo que hace posible conocer sin mucho problema información importante como el *login* y *password* de algún usuario. Ethereal como cualquier otro analizador de paquetes, permite conocer el contenido de los paquetes por lo que se convierte en una herramienta útil de seguridad al momento de rastrear algún acceso indebido

4.1.2. ANÁLISIS DE TRÁFICO.

Cada paquete capturado ofrece información importante para el análisis de la red. Por esta razón se despliega en una interfase grafica. Los paquetes capturados son ordenados según su origen, destino, contenido o cualquier otro campo del paquete. Gracias a su interfase grafica Ethereal permite conocer los tipos de servicios más utilizados en base a los protocolos que generan los paquetes. Además también se puede conocer equipos con tráfico excesivo (algún posible abuso del recurso), problema de configuración o inclusive la presencia de algún tipo de virus o ataque. Lo anterior ha resultado de utilidad para mantener las políticas de calidad en los servicios del DIA, pues ubica acertadamente algún usuario o dispositivo que este ocasionando este tipo de situaciones.

[9] Desarrollado por Combs, G. et al. Se encuentra disponible en http://ethereal.zing.org/

4.1.3. INTERFASE GRAFICA

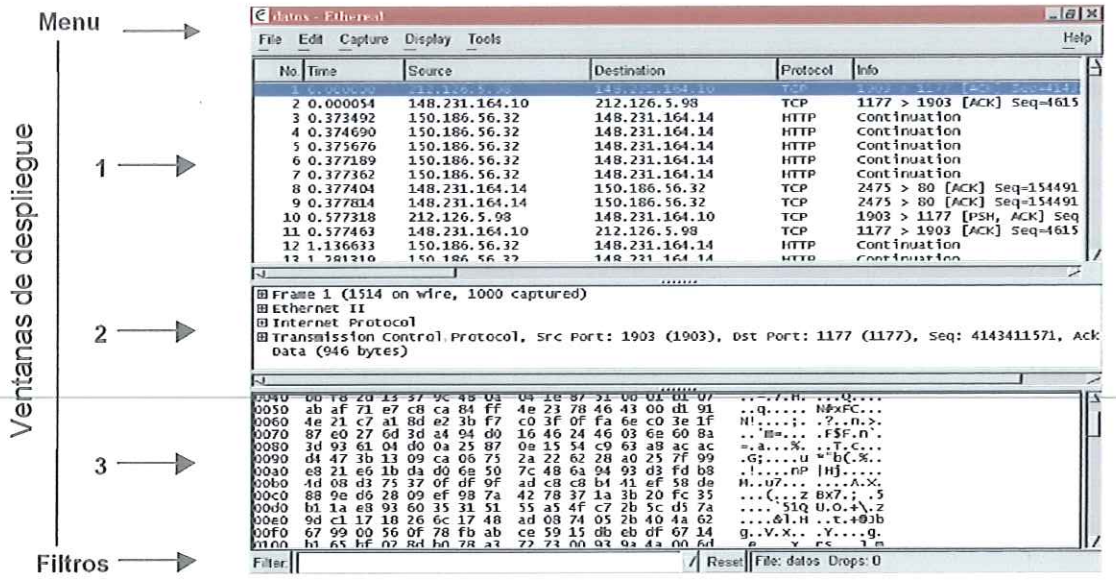


Figura 6. Interfase gráfica mostrando sus distintas secciones.

4.1.3.1. ELEMENTOS DE LA INTERFASE GRAFICA

- Menú
- Ventana de despliegue (dividida en tres segmentos)
- Barra de filtros de captura

4.1.3.1.1. MENÚ

Permite acceder a los funciones de la aplicación mediante el teclado o Mouse.

4.1.3.1.2. VENTANA DE DESPLIEGUE

La interfase grafica de Ethereal se divide en tres secciones principales o segmentos (figura 6). La información contenida en los paquetes se muestra a través de esos segmentos. Cada uno de los tres segmentos, muestra diferentes perspectivas de la información. Por ejemplo, el primer

segmento da una apreciación general de la captura mostrando todos los paquetes, el segundo particulariza a un solo paquete clasificando su contenido por los distintos protocolos que intervienen en su creación y el último segmento muestra a detalle el contenido del paquete seleccionado en el primer segmento. A continuación se ofrecen mas información de dichos segmentos:

PRIMER SEGMENTO Muestra de forma general la lista completa paquetes capturados. La cantidad de paquetes variará dependiendo del modo de captura hecha (*por tiempo o número de paquetes*). Como puede observarse en la figura seis este segmento esta formado por seis columnas, cada una correspondiente a un campo del paquete (Tabla 2.). Una vez hecha una captura los paquetes quedaran sorteados según el orden en que fueron capturados, pero después pueden ser reordenados por cualquiera de sus campos. Ordenar los paquetes por campos es útil al momento querer conocer la cantidad de paquetes con un mismo origen, destino, protocolo, etc.

También es posible quitar o poner más columnas según se requiera.

Tabla 2. Campos de un paquete y su descripción

Columna	Contenido
No	Indica la secuencia en que fue capturado cada paquete
Time	Tiempo de captura relativo al primer paquete captado
Source	Dirección IP numérica o de nombre del equipo propietario del paquete
Destination	Dirección IP numérica o de nombre del equipo destino el paquete
Protocol	Se refiere al protocolo que propietario del paquete, por ejemplo: IP, TCP, HTTP, etc.
Info	Descripción del contenido del paquete por ejemplo: indicadores de secuencia, De tipo de paquete

SEGUNDO SEGMENTO Aquí se muestra específicamente encabezados y campos utilizados por un paquete para transportarse por la red y que son agregados por los diferentes protocolos que intervienen. Se puede expandir la lista para ver los campos de cada encabezado y conocer a detalle los valores contenidos en los campos.

TERCER SEGMENTO Permite observar a detalle la información del paquete tanto en formato hexadecimal como ASCII. (Fig. 6)

4.1.3.1.3. BARRA DE FILTROS

Cuando la captura de paquetes es grande se hace necesaria la utilización de filtros. Un filtro es una expresión que despliega solo aquellos paquetes que cumplen con el criterio establecido en el mismo. En la figura 7c se muestra la barra donde se escriben los filtros. Más de adelante se detalla el uso de filtros

4.1.3.1.4. MENÚ DE CAPTURA

A continuación se describen las opciones disponibles en el menú de captura (figura 7)

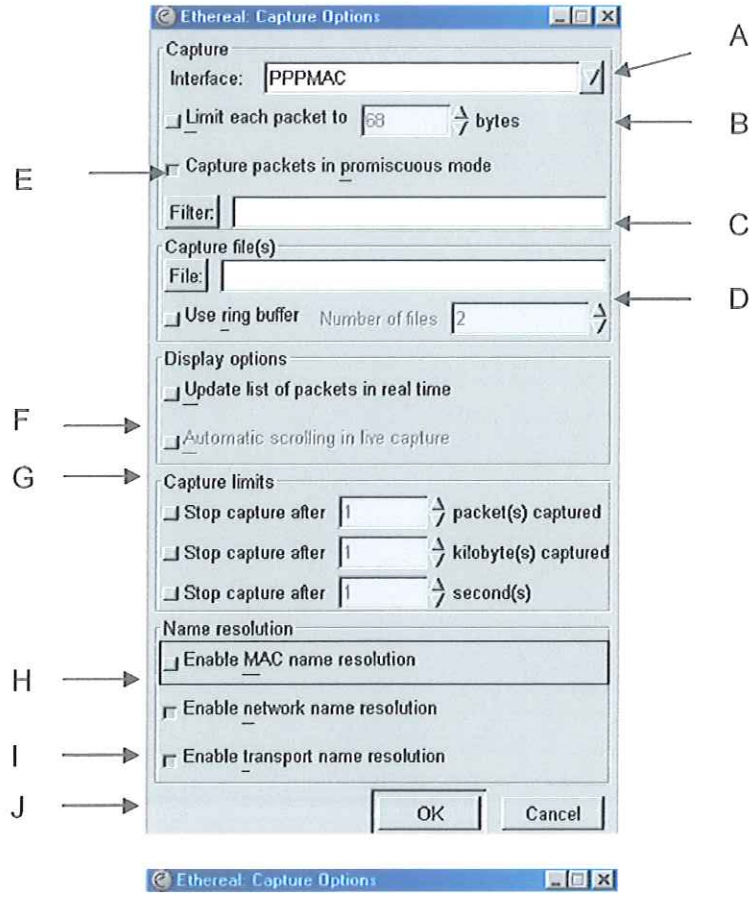


Figura 7. Menú de captura de paquetes.

A) Selecciona la interfase de red a utilizar en la captura (*un dispositivo puede tener mas de una interfase*)

B) Especifica la longitud máxima de bytes que serán capturados por paquete

C) Campo para especificar el filtro de captura. Se puede crear un filtro nuevo o inclusive seleccionar alguno de los grabados previamente.

D) Recupera alguna captura grabada en archivo previamente.

E) Activa la interfase de red en *modo promiscuo* para la captura de paquetes

F) Habilita el deslizamiento de paquetes en pantalla conforme estos van siendo capturados

G) Resuelve direcciones MAC cuando es seleccionado

H) Resuelve direcciones IP a su equivalente en el DNS

I) Resuelve nombre de transporte

4.1.4. MANEJO DE FILTROS

La cantidad de paquetes obtenidos durante una captura suele ser grande, más si se hace en puntos donde el trafico sea abundante (en algunos casos se capturan miles por segundo). Sín embargo, nuestro interés puede estar solo en algún tipo de paquete. Por ejemplo a su dirección origen o destino, protocolo o puerto de origen, etc. Para discriminar los paquetes que nos interesen de aquellos que no, utilizamos los *filtros*. Un filtro es una expresión que compara el contenido de un campo (de los mostrados en la figura 6) con valores conocidos.

Los filtros especifican criterios apoyados en operandos tales como: igual que, menor igual, mayor que, etc. Cuando se aplica un filtro la interfase grafica, esta sólo presentará aquellos paquetes que cumplan con el criterio establecido por el mismo.

Existen dos tipos de filtros: aquellos que se aplican durante una captura (en "vivo") y los que se utilizan para visualizar paquetes de capturas previas.

4.1.5. DEFINICIÓN DE FILTRO DE CAPTURA

Como ya se ha mencionado anteriormente, una captura puede contener una cantidad de paquetes grande. Esto resulta un problema si solo se tiene interés en algún tipo de paquetes en particular. Para evitar esto, Ethereal utiliza filtros que discriminan los paquetes en los que no tenemos interés. Un filtro es una expresión que utiliza una sintaxis semejante a la utilizada por *tcp dump* de Unix de la siguiente manera:

[not] expresión [and | or [not] expresión ...]

Donde ***expresión*** puede ser cualquier de las posibilidades mostradas en la tabla 3.

Tabla 3. Expresiones más utilizadas en filtro de captura

Expresión	Explicación y ejemplos
[src | dst] host < host >	Captura los paquetes dirigidos o provenientes del dispositivo señalado como *host* (nombre o dirección IP). Ejemplos ***src host 192.168.192.6*** Captura los paquetes cuyo origen sea el dispositivo de red 192.168.192.6 ***dst host faro.ens.uabc.mx*** Captura los paquetes cuyo destino sea el dispositivo de red 192.168.192.10 ***host 192.168.186.42*** Captura paquetes que provengan o vayan dirigidos al dispositivo 192.168.192.6
ether [src | dst] host < host >	Captura los paquetes dirigidos o provenientes del dispositivo señalado como *host* (dirección MAC). Ejemplos: ***Ether dst host 00:c0:f0:54:d8:a3*** Captura el trafico destinado a la dirección MAC 00:c0:f0:54:d8:a3 ***Ether src host 00:e0:63:a1:72:6f*** Captura el trafico dirigido a la dirección MAC 00:e0:63:a1:72:6f
Gateway host <host>	Captura el trafico que utilice al dispositivo *host* (nombre o dirección IP) como gateway
[tcp | udp] [src | dst] port < port>	Captura el trafico dirigido a un puerto especificado en ***port*** (puede ser paquetes UDP o TCP) Ejemplos: ***tcp dst port 443*** Capta los paquetes TCP cuyo destino sea el puerto 443 ***udp port 1863*** Capta los paquetes UDP cuyo destino sea el puerto 1863

4.1.6. DEFINICIÓN DE FILTRO DE DESPLIEGUE

Una vez capturados los paquetes, estos pueden ser almacenados como archivos para algún análisis posterior. Dependiendo de la cantidad de paquetes puede ser necesario usar algún *filtro de despliegue*. Estos filtros a diferencia de los filtros de captura, separan sus componentes por puntos (observe los incisos a y b) y utilizan la lista de operandos mostrados en la tabla 4. Se definen en la parte inferior de la interfase grafica (figura 6)

Tabla 4. Operandos utilizados en filtros

OPERANDO	SIMBOLOGÍA	
Igual	= =	Eq
Diferente	! =	Ne
Mayor que	>	Gt
Menor que	<	Lt
Mayor igual	> =	Ge
Menor igual	< =	Le

Ejemplos de filtros de despliegue:

a) ip.src == 192.168.45.6

Lista en pantalla únicamente los paquetes cuya dirección numérica IP origen sean igual a 192.168.45.6

b) ip.dst == www.hotmail.com

Lista en pantalla los paquetes cuya dirección de *nombre* origen sean igual www.hotmail.com

c) ip.addr = = 129.111.0.0/16

Despliega aquellos paquetes que pertenezcan una red clase B con dominio 129.111

También se puede seleccionar paquetes comparando el contenido de sus campos con algún valor del tipo indicado en la Tabla 5.

Tabla 5. Tipos de valores utilizados para los filtros

Entero sin signo (16, 24 y 32 bits)
Entero con signo (16, 24 y 32 bits)
Boleano
Dirección Ethernet (6 bytes)
Byte String (de n bytes)
IPv4 Direcciones
IPv6 Direcciones
IPX Numero de red
Numero de punto flotante de doble precisión

Utilizando los operadores lógicos de la tabla 6.

Tabla 6. Valores boleanos

Operador	Descripcion	Caracter
and	AND Lógico	&&
or	OR Lógico	||
xor	XOR Lógico	^^
not	NOT Logico	!
[...]	Operador de subcadena	

Un entero puede ser expresado en bases octal, decimal o hexadecimal por ejemplo:

e) Frame.pkt_len > 10

Lista en pantalla los paquetes con una longitud mayor a 10 decimal

d) Frame.pkt_len > 0xa (Hexadecimal)

Lista en pantalla los paquetes cuya dirección longitud sea mayor a 0xa hexadecimal

4.1.7. IMPLEMENTACIÓN

Esta herramienta se Instalo en una distribución de Linux Mandrake 8.2 en un equipo con dos tarjetas de red: una para administración remota y la otra para captura de paquetes. Físicamente el equipo se ubico en el segmento de salida, justo antes del FireWall (figura 8) para captar todos los paquetes entrantes y salientes de la red del campus.

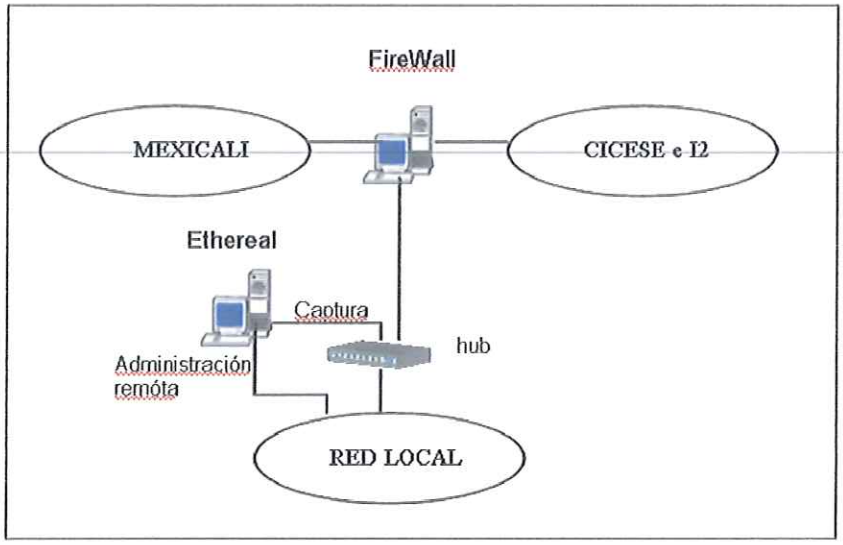


Figura 8. Ubicación física de Ethereal en el DIA

4.1.8. CONCLUSIONES

El uso de esta herramienta en las redes de datos y telecomunicaciones del DIA permitió ubicar con mayor facilidad los equipos que presentaban alguno de los siguientes problemas:

Trafico Excesivo

Antes de utilizar Ethereal, no era posible identificar los equipos causantes de tráfico excesivo. Si bien, las graficas de MRTG indicaban el sitio (escuela, facultad, sala, etc) o interfase a la cual pertenecía dicho dispositivo, no había forma de conocer su dirección IP y el tipo de trafico que este generaba. En algunas ocasiones inclusive por no tener la información exacta del dispositivo se llego a cancelar el acceso a subredes (o escuelas, inclusive) de manera temporal hasta que el responsable del área identificara y corrigiera el problema.

Detección de Virus

Algunos virus utilizan puertos de comunicación para infectar a otros equipos en la red. Ethereal apoya la tarea de protección mediante el uso de filtros que identifiquen paquetes sospechosos. Por ejemplo es el virus Blaster (W32.Blaster.T.Worm) que utiliza el puerto de comunicación 135. Este virus se contagia enviando paquetes al puerto 135 de todos los equipos conectados en red. Hasta que logra infectar aquellos que sean vulnerables al mismo. Para este ejemplo basta usar un filtro de captura sencillo como: ***tcp port 135*** para conocer la lista de equipos que envían paquetes a este puerto y con ello, detectar equipos posiblemente infectados.

Trafico Improductivo

Aprovechando las cualidades propias de las redes de comunicación algunos usuarios comparten información en la red (música, documentos, software, etc.). Esto es normal excepto aquellos casos en que se comparte material no académico. Algunas aplicaciones que permiten realizar esta actividad son Kazaa, Emule, Mies, etc. las cuales pueden decrementar en gran manera el recurso de comunicación.

Mediante el uso de filtro de captura y un análisis sencillo es posible identificar con Ethereal este tipo de tráfico. Estas aplicaciones se caracterizan por generar una gran cantidad de paquetes, dirigidos a diferentes usuarios, la mayoría de ellos conectados en conexiones tipo *dial-up* y utilizar puertos conocidos. Esto ha permitido detectar este tipo de actividad y reportarla según corresponda.

Si bien, Ethereal permite conocer en tiempo real el contenido y la cantidad de paquetes enviados por algún dispositivo, no da información estadística actual o pasada, ni cuanto recurso esta siendo realmente consumido por el mismo.

4.2. MRTG (MULTI ROUTER TRAFFIC GRAPHER)

4.2.1. INTRODUCCIÓN

Para la realización de las tareas cotidianas en la vida universitaria del campus, se cuentan con diferentes enlaces de comunicaciones. En ellos se transporta información importante que requiere de una conectividad confiable. Lo anterior exige conocer en todo momento (presente o pasado), el estado de operación que los enlaces, a fin mantener los niveles de calidad adecuados en las mismas.

MRTG brinda la posibilidad de conocer de forma estadística y grafica el estado de los enlaces de comunicación para identificar situaciones de problema que requieran atención inmediata.

4.2.2. DEFINICIÓN

Es una aplicación de monitoreo grafico que se distribuye gratuitamente y por lo mismo muy utilizada en ambientes de Linux. Aunque también comienza a ser utilizado en plataformas como Windows. Aunque su mayor presencia se encuentra en plataformas tales como:

-Linux 1.2.x, 2.0.x, 2.2.x, 2.4.x (Intel, Alpha, Sparc y PowerPC)
- Linux MIPS, Linux S/390
- SunOS 4.1.3
- Solaris 2.4, 2.5, 2.5.1, 2.6, 7, 8
- AIX 4.1.4, 4.2.0.0, 4.3.2
- HPUX 9,10,11
- etc.

Su éxito se basa en ser un software de libre distribución con una interfase grafica amigable basada en Web, la cual permite el monitoreo grafico y estadístico de cualquier variable dentro de la MIB. Estas características han ayudado a que MRTG adquiera popularidad entre los administradores de red.

4.2.3. FUNCIONAMIENTO

Esta aplicación fue escrita originalmente en PERL, y se basa en el protocolo SNMP para recolectar los datos del tráfico de algún dispositivo. El dispositivo que será monitoreado se *configura* previamente para que responda a los requerimientos de información del MRTG (interfaces, ancho de banda, etc.) bajo las normas de seguridad del protocolo SNMP (figura 9)

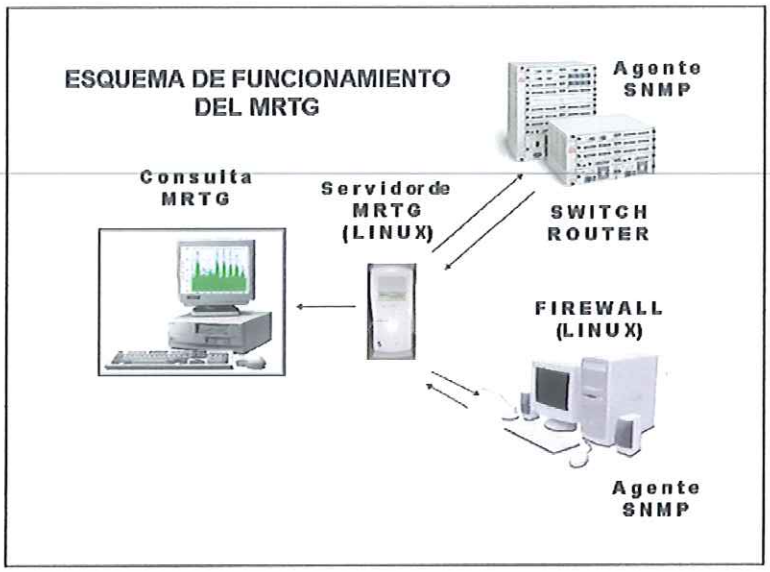


Figura 9. Esquema de funcionamiento del MRTG en los principales dispositivos del DIA

La información recolectada es mostrada casi en tiempo real mediante gráficas de tipo *gif* integradas a páginas Web (figura 10). Se observa en ellas el tráfico entrante (color verde) y el tráfico de salida (color azul). En las mismas se muestra el tráfico registrado durante los siguientes periodos:

- Diario
- Últimos siete días
- Cuatro últimas semanas
- Últimos doce meses

Para poder realizar las graficas MRTG concentra en un archivo los datos obtenidos de la red. El cual es consolidado automáticamente evitando así que crezca con el tiempo.

Los datos se almacenan con una antigüedad de hasta dos años.

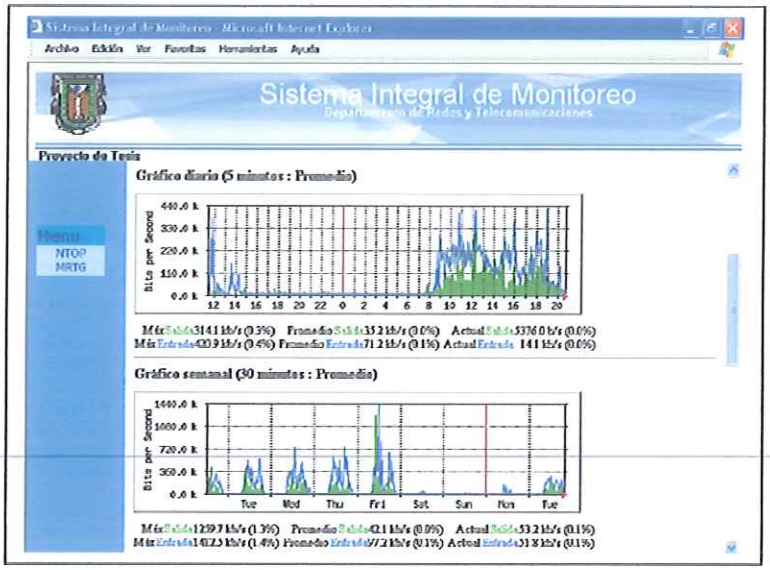


Figura 10. Graficas creadas con MRTG

MRTG es una herramienta versátil que permite conocer cualquier otra variable almacenada en la MIB del dispositivo (además del trafico). Por ejemplo el número de usuarios conectados a nuestros sistemas por mencionar algo.

4.2.4. HISTORIA

En 1994 Tobías Oetiker, el autor de la idea original, era usuario de una red donde se limitaba la comunicación a solo una canal de 64kb. Esta conectividad tan reducida hacia necesario conocer la manera en como se utilizaba el canal. Fue así como diseño un programa que generaba graficas en ambiente Web donde se mostraba de forma continua la utilización del mismo.

.

Con el tiempo apareció MRTG-1.0 escrito en Perl y liberado en la primavera de 1995. Tiempo después Tobías utilizando algunas ideas aportadas por *Dave Rand* cambio el código a lenguaje C haciendo más eficiente la aplicación obteniendo así lo que ahora conocemos como MRTG-2.

4.2.5. INSTALACIÓN Y COMPILACIÓN EN EL SERVIDOR

Para la instalación y funcionamiento de MRTG se requiere hacer lo siguiente:

- Compilar zlib, libpng y gd
- Compilar, y configurar MRTG
- Instalar y configurar agentes SNMP en los dispositivos a monitorear
- Crear archivos de configuración para cada dispositivo a monitorear

COMPILACIÓN DE LIBRERÍAS

Para instalar esta aplicación es necesario compilar las librerías utilizadas por MRTG. Algunas pudieran ya estar instaladas en la en el sistema operativo de Linux utilizado.

Paso 1. Crear un directorio para la compilación:

```
mkdir -p /usr/local/src
cd /usr/local/src
```

Paso 2. Instalar las librerías [10]zlib

```
gunzip -c zlib-*.tar.gz | tar xf -
rm zlib-*.tar.gz
mv zlib-* zlib
cd zlib
./configure
make
```

Paso 3. Instalar y comparar librerías [11]libpng:

```
gunzip -c libpng-*.tar.gz |tar xf -
rm libpng-*.tar.gz
mv libpng-* libpng
cd libpng
make -f scripts/makefile.std CC=gcc ZLIBLIB=../zlib
ZLIBINC=../zlib
rm *.so.* *.so
cd ..
```

[10] Disponible en http://www.libpng.org/pub/png/src/libpng-1.0.15.tar.gz

[11] Disponible en http://www.libpng.org/pub/png/src/libpng-1.0.15.tar.gz

Paso 4. Instalar y compilar la librería [12]gd:

```
gunzip -c gd-*.tar.gz |tar xf -
rm gd-*.tar.gz
mv gd-* gd
cd gd
```

El carácter \ indica continuidad de una misma instrucción.

```
make INCLUDEDIRS="-I. -I../zlib -I../libpng" \
     LIBDIRS="-L../zlib -L. -L../libpng" \
     LIBS="-lgd -lpng -lz -lm" \
     cd ..
```

COMPILAR Y CONFIGURAR MRTG

```
cd /usr/local/src
gunzip -c mrtg-2.10.11.tar.gz | tar xvf -
cd mrtg-2.10.11
```

Si todas las librerías han sido instaladas correctamente entonces:

```
./configure --prefix=/usr/local/mrtg-2
```

De lo contrario pudiera ser necesario agregar las siguientes trayectorias:

```
 ./configure --prefix=/usr/local/mrtg-2        \
             --with-gd=/usr/local/src/gd       \
             --with-z=/usr/local/src/zlib      \
             --with-png=/usr/local/src/libpng
make
make install
```

Siguiendo estos pasos la aplicación se instalada en */usr/local/mrtg-2*

[12] Disponible en http://www.boutell.com/gd/http/gd-1.8.4.tar.gz

ARCHIVO DE CONFIGURACIÓN PARA MONITOREÓ DE UN DISPOSITIVO

La siguiente línea configure el MRTG para monitorear un dispositivo de red. Se crea un archivo llamado mrtg.cfg en la trayectoria */home/mrtg/cfg* con las variables que se desea monitorear. La instrucción cfgmaker se encuentra dentro del subdirectorio *bin*:

```
cfgmaker --global 'WorkDir: /home/httpd/mrtg'  \
         --global 'Options[_]: bits,growright' \
         --output /home/mrtg/cfg/mrtg.cfg    \
          community@router.abc.xyz
```

La siguiente línea solicita la información al dispositivo *router.abc.xyz* utilizando la comunidad *community* y se crean las graficas de monitoreo especificadas en el archivo mrtg.cfg. Las graficas se depositan en la trayectoria */home/httpd/mrtg*

```
/usr/local/mrtg-2/bin/mrtg /home/mrtg/cfg/mrtg.cfg
```

La siguiente instrucción ejecuta el mrtg (línea anterior) de forma automática cada 5 minutos utilizando *crontab -e*

```
*/5 * * * *  <mrtg-bin>/mrtg <path to mrtg-cfg>/mrtg.cfg \
                --logging /var/log/mrtg.log
```

4.2.6. INSTALACIÓN EN EL CLIENTE

4.2.6.1. LINUX

En el caso del DIA se opto por instalar UCD-SNMP como agente SNMP. Los autores son de la "*University of California, the University of California at Davis*", y el "*Electrical Engineering department at the University of California at Davis*" y es completamente compatible con el estándar Snmpv1.

Esta distribución contiene algunas herramientas de gestión que permiten, desde la línea de comandos, enviar peticiones a dispositivos que ejecuten agentes SNMP. También contiene un programa agente SNMP, diseñado para ejecutarse sobre Linux, que ofrece a gestores ejecutándose en la red (o en el propio sistema), información sobre el estado de los interfaces, tablas de enrutamiento, instante de inicio (uptime), información de contacto, etc.

Para que MRTG pueda interactuar con el cliente es necesario instalar en este último las siguientes distribuciones:

Libsnmp0-4.2.3-5mdk
ucd-snmp-4.2.3-5mdk

De la siguiente manera y orden:

rpm –ivh libsnmp0-4.2.3-5mdk.rpm
rpm –ivh ucd-snmp-4.2.3-5mdk.rpm

Una vez instalado se procede a la configuración en el archivo snmpd.conf de la siguiente manera:

vi /etc/snmp/snmpd.conf

El archivo contiene las reglas de control de acceso al agente, establece quién puede conectarse, permisos de lectura, escritura, que ramas puedes ver, etc.

En el siguiente ejemplo de configuración, sólo será posible acceder al agente SNMP desde el equipo con dirección ip de 192.168.0.1 y exclusivamente para lectura utilizando la palabra ***secreto*** como comunidad:

com2sec *mi_red 192.168.0.1* ***secreto***
group *grupo_mi_red* v1 *mi_red*
group *grupo_mi_red* v2c *mi_red*
group *grupo_mi_red* usm *mi_red*

La siguiente línea establece permisos de lectura y escritura

access *grupo_mi_red* "" any noauth exact all none none

En la línea siguiente se proporciona información de Contacto del Sistema

syslocation *Depto de Redes*
syscontact *Administrador del sistema*

Una vez instalado y configurado se procede a iniciar el servicio:

/etc/rc.d/init.d/snmpd start

Y de esta manera queda listo el agente para ser consultado por el gestor MRTG.

4.2.6.2. SWITCH ENRUTADOR SSR-2000

Los dispositivos ssr2000 y ssr8000 requieren de dos líneas para ser configurados de manera que puedan ser gestionados por el MRTG. Estas las líneas se muestran continuación:

snmp set community *secreto* privilege read-write
snmp set target *192.168.0.1* community *secreto* status enable

Al igual que en el ejemplo anterior, en esta primera línea se le da el valor de *secreto* a la comunidad que incluye derechos de lectura y escritura. La segunda línea restringe la gestión a solo un IP: 192.168.0.1 por lo que peticiones de otras direcciones serán ignoradas. Las líneas se agregan a la lista de comandos de operación que los dispositivos y son guardadas ahí para ejecutarse en el siguiente encendido del sistema.

4.2.7. CONCLUSIÓN

MRTG es una excelente herramienta para conocer el comportamiento estadísticos de los enlaces de comunicación. Su fácil configuración y lo portabilidad de sus datos (formato Web) en combinación con el hecho de ser un software de distribución gratuita hace de esta aplicación la mejor opción para los administradores de red.

En el caso particular del DIA esta aplicación se ha venido utilizando por mucho tiempo lo que ha permitido la detección oportunidad y corrección de problemas en los enlaces de

comunicación. Algunos de los problemas resueltos con la utilización de este aplicación han sido:

- Abusos de utilización en los enlaces
- Equipos con problemas de configuración o con problemas de virus informático
- Problemas de seguridad (ataques internos y externos)
- Verificación de entrega de ancho de banda por del IPS
- Etc.

Si bien MRTG contiene todas las ventajas arriba señaladas no ofrece información específica acerca de algún dispositivo que este presentando problemas. Por esta razón se usa de forma complementaria con Ethereal mencionado anteriormente.

4.3. NTOP

4.3.1. INTRODUCCIÓN

En forma cotidiana una gran cantidad de tráfico circula por las redes de datos y telecomunicaciones del campus. Lo anterior hace que se tenga una variedad enorme datos circulando por la red, haciéndose necesario mecanismos que permitan conocer aspectos importantes, como lo son el origen, destino y tipo de información. Conocer estos aspectos del tráfico le permite al departamento de redes ubicar situaciones que pudieran comprometer el desempeño y seguridad de las redes.

Envió de paquetes en ráfaga o en forma continua, acceso a ciertos puertos considerados de peligro, son algunos ejemplos de actividades que no deben pasar desapercibidas.

Una buena alternativa para detectar esta y otras actividades sospechosas es el uso del analizador de protocolos Ethereal. Sin embargo, esta aplicación no ofrece una perspectiva global ni estadística del comportamiento del tráfico la red. MRTG por su parte, ofrece datos estadísticos e historial de utilización, pero se enfoca mas hacia los que son equipos conectividad, tales como *switches*, enrutadores, servidores, etc.

Ninguna de las aplicaciones anteriores permite conocer en forma precisa y directa el ancho de banda consumido por los equipos, sesiones establecidas ni los puertos utilizados por las mismas. Información importante para quienes se encargan de administrar una red.

Es en este contexto que se opta por la instalación de [13]NTOP como un complemento a las dos herramientas vistas anteriormente. Esta aplicación es del tipo *Open Source* desarrollada en 1997 en la Universidad de Pisa por Luca Deri. Fue desarrollada con el fin encontrar aquellos dispositivos de red que presentaban mayor actividad dentro de las redes de la universidad.

Los reportes que esta aplicación genera son en formato *html* y se enfoca básicamente en las siguientes funciones:

- Medición Tráfico
- Monitoreo trafico
- Optimización y planeación de la red
- Seguridad.

4.3.2. ESTADÍSTICA DE TRÁFICO

Todas las actividades de tráfico presentes en el medio son registradas en las bases de datos. Lo anterior permite identificar el tráfico de una subred o equipo especifico. Toda información capturada es asociada de acuerdo al par *transmisor-receptor* lo que facilita determinar la actividad relevante entre equipos. La información registrada puede ser consultada por *dispositivo* y en forma *global.* A continuación se muestran los datos y su descripción, tanto para tráfico por global.

4.3.2.1. ESTADÍSTICAS POR DISPOSITIVO

Para cada dispositivo esta disponible la información mostrada en la tabla 7.

Tabla 7. Datos estadísticos por equipo

Datos enviados/recibidos	**Es el total de paquetes enviados y recibidos clasificados al protocolo de red utilizado (IP, IPX, AppleTalk, etc) y protocolo IP (FTP, http, NFS, etc).**
Ancho de Banda Utilizado	**Permite conocer la utilización de ancho de banda actual, promedio y máxima.**
Trafico Multicast	**Cantidad de tráfico enviado o recibido del tipo multicast**
Historial de sesiones TCP	**Registro de las sesiones establecidas y aceptadas así como sus respectivas estadísticas de trafico**
Trafico UDP	**Total de trafico UDP clasificado por puerto**
Servicios TCP/UDP utilizados	**Lista de servicios basados en IP disponibles y abiertos con la lista de los últimos cinco equipos que los utilizaron**
Distribución del tráfico	**Se clasifica al tráfico en local-remoto, remoto-local**
Distribución Trafico IP	**Muestra una distribución relativa del trafico UDP vs TCP**

[13] Aplicación basada en paginas WEB desarrollada para monitoreo de trafico en la Universidad de Pisa en 1997 realizada por Deri, L., Suin, S and Carbone, R. disponible en http://www.ntop.org/

4.3.2.2. ESTADÍSTICAS GLOBALES.

En cuanto a estadísticas globales es posible conocer los siguientes datos mostrados en la tabla 8.

Tabla 8. Datos estadísticos globales

Distribución de tráfico.	Trafico local (subred), local vs remoto (fuera de la red local especificada), remoto vs local.
Distribución por paquetes.	Total de paquetes clasificados por tamaño de paquete, tipo transmisión unicast, multicast y broadcast, trafico IP vs no IP.
Utilización de Ancho de Banda	Actual, promedio y máximo
Utilización y distribución por protocolo	Distribución del trafico observado de acuerdo a al protocolo utilizado y al par transmisor-receptor (local vs remote).
Matriz de tráfico local y subred	Monitoreo del tráfico entre pares en una subred
Flujos de red	Estadísticas de flujo predefinidos por el usuario

4.3.3. USO DE PLUG-INS

Una característica importante que presenta este aplicación es que permite la adición de [14]plug-ins. Con ellos es posible obtener mayor detalle acerca de protocolos no presentes en la distribución estándar de este software. Por ejemplo NFS y NetBios en donde los plug-ins pueden obtener estadísticas acerca del equipo donde están ejecutándose, tales como lista de [15]sockets habilitados, datos enviados y recibidos, y lista de pares conectados para cada unos de los procesos actuales.

4.3.4. MONITOREO DE TRÁFICO

En ocasiones y sin que sea del conocimiento del responsable de la red, circulan por esta tráfico no deseado. La condición ideal desde luego, es que solo este presente aquellos paquetes de información útiles. Algunas razones que originan lo anterior son una inadecuada configuración de dispositivos de red, interfaces, dispositivos de enrutamiento, sistemas operativos entre otras cosas.

---

[14] Plug-ins: Pequeño programa de software que conectado a una aplicación mayor da nuevas funciones

Este programa permite identificar fácilmente los casos en que algún equipo de red no cumple con las políticas de utilización de ancho de banda o cuando este excede los umbrales previamente establecidos para el mismo. Es posible con NTOP detectar la presencia de algunos de los siguientes problemas:

- Uso direcciones IP duplicadas
- Identificación de equipo operando en modo "promiscuo"
- Errores de configuración en aplicaciones de software (analizando datos del protocolo)
- Equipos utilizando protocolos innecesarios
- Identificación de enrutadores innecesarios configurados por error
- Excesiva utilización del ancho de banda

4.3.5. OPTIMIZACIÓN Y PLANEACIÓN DE LA RED

La presencia de tráfico inútil en la red deteriora el desempeño de la misma (errores en enrutadores, utilización de protocolos innecesarios, uso inapropiado del ancho de banda, etc.) Con las opciones que presenta NTOP es posible detectar los elementos de red que producen esta condición, aplicar la solución conveniente y de esa forma mantener la red operando de manera optima.

De forma paralela, NTOP permite también detectar nuevos requerimientos de ancho de banda en áreas que se sirven de la red. Lo que llevará, ya sea a promover el uso mas adecuado del recurso de conectividad o la gestión de mayor ancho de banda según sea el caso.

[15] Socket: identificador de un servicio particular sobre un nodo particular en la red

4.3.6. APOYO EN SEGURIDAD DE CÓMPUTO

Gracias a la información recabada por NTOP es posible identificar la presencia de un ataque en la red. Así como también detectar la presencia de hoyos de seguridad, tarjetas de red en operando en modo promiscuo, rastreo de puertos. .

4.3.6.1. RASTREO DE PUERTOS.

Consiste en el envió de paquetes a diferentes puertos buscando cual de ellos están vulnerables a un ataque. Existen dos tipos de rastreo: Clásico y Lento. Para evitar lo anterior Ntop conserva una lista de los últimos tres equipos que han enviado información a un mismo puerto cuyo numero sea menor de 1024.

4.3.6.2. SPOOFING.

Se trata de un equipo que asegura tener la dirección de otro equipo con la finalidad de robar la información de este último mediante la captura de paquetes ARP. Ntop detecta esta actividad con el plug-in arpWatch que tiene incluido.

4.3.6.3. ESPIONAJE.

Lo realizan equipos operando en modo promiscuo. Son detectados por NTOP gracias a que este ejecuta la aplicación Neped. Esta aplicación que envía paquetes ARP periódicamente y las maquinas en modo promiscuo responde a estos paquetes con lo que son detectadas.

4.3.6.4. CABALLOS TROYANOS.

Su presencia es detectada gracias a que NTOP revisa periódicamente aquellos puertos en donde operan generando una advertencia al administrador en caso de ser utilizados.

4.3.6.5. DENIAL OF SERVICE.

El equipo atacante envía una serie de paquetes tipo *SYN* hacia el equipo victima con la finalidad de abrir en este ultimo el numero máximo de conexiones *TCP*. Se puede crear en NTOP una regla que detecte esta situación y genere una alarma.

4.3.6.6. NETWORK DISCOVERY.

Se incluyen en NTOP dos plug-in que detectan automáticamente actividades tipo ARP y ICMP

4.3.7 ALARMAS

Dada una condición que sugiera un ataque a la red o durante algún problema de configuración, NTOP puede ser programado para generar una alarma y efectuar alguna acción conducente (solo en algunos casos). Las alarmas pueden ser de las siguientes formas:

- E-mail
- Un paquete trap de SNMP
- Mensaje tipo SMS

4.3.8. R E G L A S

Son expresiones en lenguaje sencillo con sintaxis propia que expresan cosas que detectar. Las reglas son almacenadas en un archivo específico de donde son cargadas a memoria y verificada su consistencia. Las reglas son almacenadas en memoria durante la inicialización de la aplicación Todos los paquetes son comparados buscando que alguno de ellos cumpla con alguna o algunas reglas.

4.3.8.1 SINTAXIS:

Protocolo etiqueta parámetros

Protocolo Puede ser TCP UDP e ICMP

Etiqueta identificador único de la regla

Parámetros Varían dependiendo del protocolo

4.3.8.2. ETIQUETA.

Cualquier cadena que tenga los siguientes caracteres validos: a-z, A-Z, 0-9

4.3.8.3. PARÁMETROS.

Tabla 9. Parámetros aplicables a la sintaxis

Protocolo	Argumentos
TCP	[revert] <saddr>/<sport> <daddr>/<dport> [flags <flags>] [<pktDiscr>] [<pktSize>] action <action>
UDP	[revert] <saddr>/<sport> <daddr>/<dport> [<pktDiscr>] [<pktSize>] action <action>
ICMP	*<icmp-type>* [revert] <saddr>/<sport> [<pktDiscr>] [<pktSize>] action <action>

Tabla 10. Opciones disponibles para los parámetros

Donde:	Opciones
<icmp-type>	ICMP_ECHOREPLY | ICMP_ECHO | ICMP_UNREACH | ICMP_REDIRECT | ICMP_ROUTERADVERT | ICMP_TIMXCEED | ICMP_PARAMPROB | ICMP_MASKREPLY | ICMP_MASKREQ | ICMP_INFO_REQUEST | ICMP_INFO_REPLY | ICMP_TIMESTAMP | ICMP_TIMESTAMPREPLY | ICMP_SOURCE_QUENCH
<saddr> <daddr>	[!] any | gateway | broadcast | multicast | dsn | remote | local | anyremote | anylocal
<dport> <sport>	any | useport | servicePort
servicePort	named | ftp | telenet ...
PktDiscr	Contains <string> | type fragment
PktSize	Pktsize <comparison> <pktLen> <pktLen> | pktcount <comparison> <seconds>

Comparison	> | < | =
String	a-z A-Z 0-9
PktLen	0..65535
Action	Mark [expires <seconds>] | alarm <seconds>] | <clear>
<clear>	Clears <etiqueta> [all]
Seconds	0..65535

4.3.9 INSTALACIÓN Y COMPILACIÓN

```
1. cd ntop
2. ./configure
3. make
4. make install
```

4.3.10 CONCLUSIÓN

A diferencia de MRTG esta herramienta si permite ubicar de forma directa algún dispositivo que pudiera ocasionar al problemas. Además de brindar también información completa de la cantidad de enlace utilizado por algún dispositivo, en que se utiliza y los dispositivos con los que se ha establecido comunicación. Aspectos importantes en la detección de situación de riesgo tales como detección de intrusos, ataques a puertos o servicios y abusos del recurso de comunicación.

Sin embargo, esta aplicación no conserva archivos estadísticos de la información del tráfico como lo hace MRTG por lo que ambas herramientas resultan ser complementarias de acuerdo a la experiencia obtenida en el DIA.

V SIM: SISTEMA INTEGRAL DE MONITOREO

5.1. DESCRIPCIÓN

SIM (Sistema Integral de Monitoreo) es una página electrónica (figura 11) diseñada para integrar en un solo sitio Web el acceso a la información generada por MRTG y NTOP, herramientas mencionadas en los capítulos anteriores

Figura 11. Pagina del Sistema Integral de Monitoreo

Esta pagina se encuentra hospedada en unos de los servidores del campus. En la figura 12 se muestra la interaccion que guarda esta con los servidores de NTOP, MRTG y los clientes.

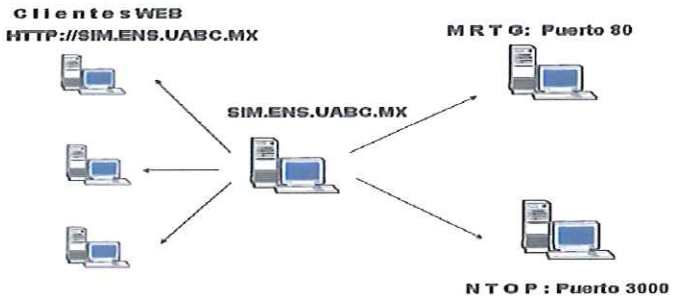


Figura 12. Pagina del Sistema Integral de Monitoreo

Los clientes Web mostrados a la izquierda de la figura 12, solicitan acceso a la página sim.ens.uabc.mx alojada en un servidor dentro de sitio de comunicaciones. A su vez, este servidor solicita información a cualquiera de los otros dos servidores (por el puerto correspondiente), donde se hospedan MRTG o NTOP según sea la eleccion del usuario. Esta página integra ambas herramientas para facilitar su consulta.

Una mejora a esta página, seria agregarle una base de datos y acceso restringido. En la base de datos se registraría equipos, su ubicación y responsables de los mismos agregando información de cómo contactarlos (teléfonos y correos electrónicos) para en caso de algún incidente notificar a quien corresponda. Registrando cualquier incidente y quien fue notificado para su consulta posterior en pantalla o impresa.

ANEXOS

A PARADIGMA CLIENTE-SERVIDOR

Es la interacción entre dos aplicaciones donde una de ellas espera pasivamente a que la otra inicia una comunicación. La aplicación que inicia la comunicación se conoce como *cliente* y la que espera se le llama *Servidor*. Algunas características generales de esta relación son las siguientes:

La aplicación cliente:

- Programa de aplicación que adquiere la identidad de cliente temporalmente cuando se necesita acceso remoto, pero también realiza computo local.
- Se ejecuta localmente en la computadora del usuario.
- Inicia el contacto de con el servidor
- Puede acceder a varios servicios, según se necesite, pero contacta activamente con un servicio remoto a la vez

- No requiere de hardware especial ni de un sistema operativo complicado

La aplicación servidor:

- Es un programa privilegiado de propósito específico.
- Se inicia automáticamente al arranque del sistema y continua ejecutándose en varias sesiones.
- Espera pasivamente el contacto de los clientes remotos
- Acepta el contactó de varios clientes, pero solo ofrece un solo servicio.
- Necesita un hardware poderoso y un sistema operativo complicado.

B MODELO TCP/IP

Modelo de referencia que define un conjunto de protocolos de comunicación de redes, agrupados en capas funcionales que establecen estándares de intercambio de información entre computadoras a diferentes niveles operativos. Para cada uno de dichos niveles se define uno o más protocolos interactuando entre pares (peer-to-peer), es decir, un protocolo de algún nivel dialoga con el protocolo del mismo nivel en la computadora remota.

Las metas principales de este modelo son:

- Independencia de tecnología de conexión a bajo nivel y de la arquitectura de la computadora.
- Conectividad Universal a través de la red.
- Reconocimientos de extremo a extremo.
- Protocolos de Aplicación Estandarizados.

Sus características:

- Protocolos de no conexión en el nivel de red.
- Conmutación de paquetes entre nodos.
- Protocolos de transporte con funciones de seguridad.

C CAPAS DEL MODELO TCP/IP

Como se puede apreciar en la figura 10 este modelo presenta cinco capas funcionales, siendo notorio su parecido con el Modelo OSI de referencia.

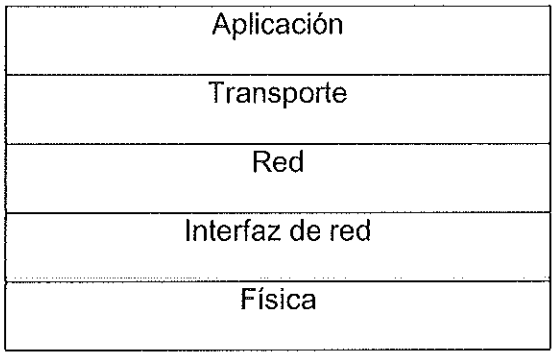


Figura 13. Las cinco capas del modelo de referencia TCP/IP

CAPA FÍSICA.

A este primer nivel se especifica el hardware básico de la red que incluye la interfaz física y el medio de transmisión. Emite al medio físico los flujos de bit y recibe los que de él provienen. Consiste en los manejadores de los dispositivos que se conectan al medio de transmisión.

CAPA DE INTERFAZ DE RED.

Esta capa contiene un grupo de protocolos que especifican la organización y transmisión de los datos en tramas

CAPA DE INTERRED.

Contiene los protocolos que indican el formato de los paquetes, el ruteo de los mismos y forma evitar la congestión. Controla la comunicación entre un equipo y otro, decide qué rutas deben seguir los paquetes de información para alcanzar su destino. Conforma los paquetes IP que será enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación.

CAPA DE TRANSPORTE

En este nivel existe un conjunto de protocolos que establecen mecanismos para la entrega de información dentro de la red (secuencia y control de flujo). Por ejemplo TCP, protocolo primario de este modelo y orientado a conexión que permite una entrega segura de paquetes. Otro caso es UDP, que a diferencia de TCP no establece conexión por lo que la entrega de paquetes no es segura. Este protocolo, se utiliza en esquemas de comunicación basados en la arquitectura cliente-servidor y aplicaciones donde la prontitud esta por encima de seguridad de la entrega. Coordina a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota, esto lo hace añadiendo identificadores de cada una de las aplicaciones. Realiza además una verificación por suma, para asegurar que la información no sufrió alteraciones durante su transmisión.

CAPA DE APLICACIÓN.

Aquí se abarcan los protocolos de alto nivel, tales como FTP, TELNET, SMTP, etc.

D TCP/IP y OSI

Ambos modelos utilizan protocolos independientes además de una integración en forma de capas funcionales. TCP/IP marca una diferencia al contener solo cinco capas, dos menos que el modelo OSI. Por su parte, el modelo OSI en su capa de red, permite dos esquemas de comunicación: orientada a conexión y sin conexión mientras que en la capa de transporte solo se limita a comunicación a orientada a conexión.

Por su parte, TCP/IP en la capa de red admite únicamente comunicación no orientada a conexión pero apoya ambos esquemas en la capa de transporte.

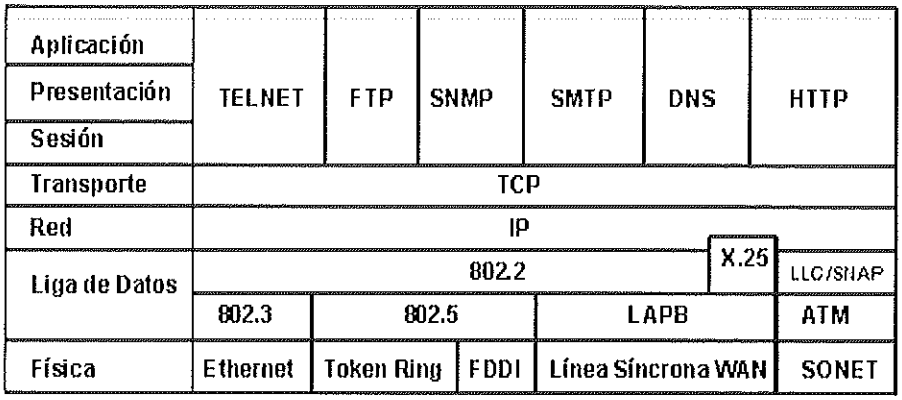


Figura 14. Modelo de referencia OSI (izquierda) mostrando los protocolos su equivalencia con los protocolos del modelo TCP/IP (derecha)

E PROTOCOLO DE DATAGRAMA DE USUARIO UDP

Protocolo para comunicación en redes que permite el intercambio de información entre dos o mas computadoras (a nivel de aplicación) sin necesidad de establecer una conexión. Mediante este protocolo los equipos de cómputo involucrados en la comunicación envían y reciben datos en forma de datagramas sin que exista ninguna garantía de entrega o retransmisión de los mismos.

TABLA DE PUERTOS UDP

Para le entrega correcta de datagramas UDP es conveniente saber a priori a que numero de puerto se enviara el datagrama. Es por ello que cada computadora tiene asignado *un número de puerto* por donde pueda realizar la entrega de datagramas UDP de algún determinado servicio.

Este tipo de paquetes pueden ser transmitidos en dos variantes: *punto a punto* con lo cual solo dos computadoras se comunican, y *punto a multipunto* donde un equipo actúa como servidor y de otros equipos llamados clientes.

FORMATO DE LOS DATAGRAMAS UDP

Los datagramas UDP están formados por los campos que se muestran en la figura 5. Observe como los dos primeros campos corresponden a los números de puertos origen y destino respectivamente. El campo de puerto origen es opcional debiendo asignarle un valor de cero en caso de no utilizarse. En el campo longitud se especifica la medida en bytes del datagrama incluyendo la cabecera y los datos del usuario. Se agrega también un campo de cheksum que permite la verificación de la información transmitida

BIBLIOGRAFÍA

D.Mauro, K. Schmidt, Julio 2001. ***Essential SNMP***, O'Reilly

A.Barba, Septiembre 1999. ***Gestión de red***, Ediciones UPC

William Stallings.. 1993. ***SNMP, SNMPv2 and CMIP. The Practical Guide to Network Management Standards*** , Addison Wesley

Williams Stallings. 1996. ***SNMP, SNMPv2, and RMON Practical Network Management.***

Addison-Wesley Publishing Company, Inc. Second edition.

William Stallings 1998. ***SNMP, SNMPv2, SNMPv3 and RMON 1 and 2,*** Addison Wesley.

Marshal T. Rose, Keith McCloghrie. 1995. ***How To Manage Your Network Using SNMP.*** Prentice Hall.

Douglas E. Comer, 1995. ***Internetworking with TCP/IP. Vol. 1: Principles, Protocols and Architecture,***. Tercera edición, Prentice Hall.

Black Uyless, 1996. ***Computer Networks, Andrew S. Tanenbaum.*** Tercera edición, Prentice Hall.

Feit Sidnie.1995. ***SNMP A guide to network management.*** Mc Graw Hill.

Woodcock, Joanne 2000. Microsoft Diccionario de informática e Internet. McGraw Hill

REFERENCIAS DE PÁGINAS WEB

Pagina oficial de MRTG en idioma Ingles:

[http://www.mrtg.org]

Pagina oficial de MRTG en idioma Español:

[http://people.ee.ethz.ch/~oetiker/webtools/mrtg/es_es/]

Tutorial para monitoreo de variables utilizando SNMP y MRTG:

[http://net-snmp.sourceforge.net/tutorial/mrtg/]

Guía de Instalación de MRTG en Linux

[http://people.ee.ethz.ch/~oetiker/webtools/mrtg/unix-guide.html]

Manual de implementación de MRTG

[http://www.enterastream.com/whitepapers/mrtg/mrtg-manual.html]

Guía de utilización de Ethereal:

[http://www.linuxjournal.com/article.php?sid=6842]

Información General acerca de Ethereal

[http://www.gnu.org/directory/All_Packages_in_Directory/ethereal.html]

Pagina Oficial en Ingles de Ethereal:

[http://www.ethereal.com/]

Diseño de filtros de captura para Ethereal:

[http://home.insight.rr.com/procana/]