UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERIA EN COMPUTACIÓN

HERRAMIENTAS DE MONITOREO DE RED, CASO PRACTICO: IMPLEMENTACION Y CONFIGURACION EN EL CC DE LA UNIVERSIDAD DON BOSCO Y ACADEMIA CISCO.

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE INGENIERO

EN CIENCIAS DE LA COMPUTACIÓN

PRESENTADO POR:

HUGO ALBERTO ORELLANA GUEVARA

MARVIN ALEXIS PEÑA PLEITEZ

AMILCAR ALEXANDER RIVAS MORALES

ASESOR:

ING. RIGOBERTO IRAHETA

SOYAPANGO **OCTUBRE 2002**

UNIVERSIDAD DON BOSCO

RECTOR

ING. FEDERICO MIGUEL HUGUET RIVERA

SECRETARIO

LIC. MARIO OLMOS

VICERRECTOR ACADÉMICO

LIC. VICTOR BERMÚDEZ

DECANO DE LA FACULTAD DE INGENIERÍA

ING. CARLOS BRAN

ASESOR

ING. RIGOBERTO IRAHETA

JURADOR EVALUADOR

ING. KARIM HEREDIA

ING. ERICK FLORES

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN

JURADO EVALUADOR

TEMA:

HERRAMIENTAS DE MONITOREO DE RED: CASO PRACTICO IMPLEMENTACIÓN Y CONFIGURACIÓN EN EL CENTRO DE COMPUTO DE LA UNIVERSIDAD DON BOSCO Y ACADEMIA CISCO.

ING. KARIM HEREDIA
JURADO

ING. ERICK FLORES
JURADO

ING. RIGOBERTO IRAHETA
ASESOR

INDICE

INTRODUCCIÓN

A medida que la masificación de las computadoras se ha ido desarrollando, las edes de computadoras han adquirido gran importancia a nivel mundial. Las redes nformáticas son ahora muy importantes para las comunicaciones (Internet), la educación, a industria, etc.

Con todas las ventajas y beneficios de lo anterior, existen, sin embargo varios roblemas propios del funcionamiento de las redes, como son: la administración, la revención de fallas y la corrección oportuna de las mismas, el monitoreo de trafico, la listribución de la carga, etc.

Muchos de estos problemas son resueltos según las percepciones y la experiencia istórica de la red en particular . Obviamente es necesario utilizar herramientas que ermitan al administrador de red detectar problemas, cuantificarlos y solucionarlos

Un sistema de monitoreo de redes es un instrumento que entrega información elevante sobre la red en la cual esta instalada. Esta información incluye disponibilidad de ervicios, reportes, intrusividad, análisis de protocolos, desempeño de la red, entre otros; además es de vital importancia para conocer el comportamiento de la red, permitiendo sí diagnosticar fallas de manera oportuna, tomar decisiones en base a eventos reales y ontrolar el desempeño de la red.

Este estudio pretende proveer de información y herramientas orientados a la onitoreo, detección y corrección de fallas en la red del Centro de Computo de La niversidad Don Bosco y los laboratorios del programa de redes de la Academia Cisco.

Los resultados esperados una vez se concluya este estudio y la implementación de s herramientas de monitoreo de red son entre otros, la generación de un documento que ueda ser utilizado como referencia y bibliografía de apoyo por los estudiantes de signaturas de redes de área local, redes de área amplia y protocolos de comunicación.

CAPÍTULO I. DESCRIPCIÓN DEL PROBLEMA

1.1 OBJETIVO GENERAL

Implementar un sistema de monitoreo y diagnóstico de fallas de red que sirva como recurso auxiliar en el proceso enseñanza – aprendizaje en la academia cisco y en las asignaturas que impliquen el estudio de redes de la Universidad Don Bosco, además de proveer una herramienta de monitoreo de red al Centro de Computo de la Universidad Don Bosco.

1.2 OBJETIVOS ESPECÍFICOS

1. Proporcionar al instructor y al estudiante una herramienta de monitoreo de red que sirva como recurso didáctico en el área de resolución de problemas de red.

2. Realizar un estudio y comparación entre diversas herramientas de monitoreo de red de dominio público.

3. Realizar la configuración, depuración y adaptación de las herramientas seleccionadas para su posterior implementación dentro de las entidades que se verán beneficiadas

4. Proveer al centro de cómputo de la Universidad Don Bosco una herramienta que facilite la tarea de resolución de problemas de la red.

1.3 PLANTEAMIENTO DEL PROBLEMA

En la actualidad el Centro de Cómputo de la Universidad Don Bosco no cuenta con herramientas para la administración y monitoreo de redes LAN, por esto, existe la necesidad de implementar herramientas que garanticen el buen funcionamiento y rendimiento de la misma. Además, la Academia Regional de Redes Cisco de La Universidad Don Bosco carece de una herramienta para el análisis y el monitoreo de red, la cual, es de gran utilidad en el proceso de enseñanza-aprendizaje de las prácticas de laboratorio. En adición a esto, las asignaturas cuyo contenido incluye el estudio de redes no poseen herramientas de laboratorio que ayuden al estudiante a comprender el comportamiento de éstas.

1.4 PROYECCION SOCIAL.

A corto plazo, el desarrollo de este proyecto se considera importante para el sector educativo de la Universidad Don Bosco y la Academia Cisco, ya que permite contar con herramientas de apoyo en el proceso de transmisión de conocimientos en el área de redes informáticas.

Además, se verán beneficiados el personal técnico del centro de computo de la Universidad Don Bosco, al proporcionarles un sistema de monitoreo y diagnóstico de fallas de redes que le permita optimizar el funcionamiento de la misma.

A largo plazo, se podrían beneficiar otras academias locales del programa de redes cisco, al implementar las soluciones propuestas en este proyecto.

1.5 SITUACIÓN ACTUAL

En vista que existen dos entidades dentro de la Universidad Don Bosco que se verán beneficiadas con la implementación de este proyecto: Centro de Cómputo y

Academia de Redes Cisco, a continuación se describe la situación actual de cada una de ellas.

En lo que se refiere a la situación actual del centro de computo, éste cuenta con 117 computadoras, siendo su topología física una estrella extendida utilizando una tecnología Ethernet. Además, el centro de computo brinda todos los servicios relacionados con Internet a la Universidad Don Bosco y al Centro de Investigación y Transferencia de Tecnología (CITT).

Aunque el desempeño óptimo de la red y la disponibilidad de los servicios son de vital importancia; no existen herramientas de monitoreo de red que permitan conocer el estado en la que ésta se encuentra en un momento determinado.

Usualmente, es el usuario el primero en darse cuenta cuando ocurre algún problema en la red, la determinación del origen de éste problema toma un tiempo considerable, ya que los procedimientos que se siguen actualmente no siempre ayudan a resolver el problema de una manera efectiva.

Tampoco existen bitácoras o reportes del los sucesos que han ocurrido en la red en un período determinado, con el fin de determinar un comportamiento de la misma.

En cuanto a la Academia de Redes Cisco, este es un programa que incluye un currículo de cuatro módulos distribuidos en 5 semanas cada uno de ellos, y consiste en lecciones multimedia y ejercicios de laboratorio. Las lecciones teóricas fueron diseñadas para aprender mediante la lectura y el uso de medios visuales. En los ejercicios de laboratorio los estudiantes se desenvuelven en un ambiente real de redes de información que les permite poner en práctica los conocimientos aprendidos mediante la teoría.

El equipo con el que cuentan estos laboratorios incluye 5 enrutadores Cisco 2500, 2 switch de Lan Catalyst 1900, software y diversas herramientas de utilidad en el trabajo con las redes (Patch panel, analizador de cables, tenaza engarzadora, tester, etc.).

El software utilizado actualmente se ha enfocado al análisis de protocolos de red, cubriendo así practicas del semestre uno del programa de esta academia. Sin embargo, por los altos costos de estos productos se están utilizando versiones de prueba, las cuales no brindan toda la funcionalidad del mismo o tienen un periodo de funcionamiento limitado.

Por otra parte, el contenido capitular de administración de redes de los semestres tres y cuatro no cuentan con un software adecuado para sus respectivas prácticas de laboratorio, quedando estas únicamente a nivel teórico.

1.6 ALCANCES

1. Monitoreo de los recursos de red del centro de cómputo, por parte de las personas encargadas de brindar soporte a ésta.

2. La implementación de las herramientas se realizará sobre plataforma Linux.

3. La arquitectura de red con la que se trabajará será Ethernet.

4. La herramienta será utilizada como material didáctico dentro de la metodología que aplique el instructor.

5. Como parte del proyecto se incluirán guías de laboratorios prácticos para los estudiantes de la Universidad Don Bosco. Las asignaturas que se cubrirán son: Protocolos de comunicación, Redes de área local(LAN), Redes de área

amplia (WAN) y Comunicación de datos. Se elaborará como mínimo una guía por asignatura.

6. Elaborar un documento de referencia que proporcione la información necesaria en caso de consultas de parte de los usuarios.

1.7 LIMITACIONES.

1. La implementación tomara como base únicamente herramientas existentes de dominio público.

2. Este proyecto cubrirá únicamente las siguientes áreas del monitoreo de redes:

a) Monitoreo de servicios de red:

- SMTP, POP3, http, DNS, PING, FTP, TELNET

b) Monitoreo de recursos de red:

- Carga de procesador, uso de disco, procesos en ejecución
- Identificación de dispositivos: dirección IP, dirección MAC, sistema operativo, nombre NetBios, Servicios disponibles.

c) Notificación de eventos a contactos:

- Notificación a contactos vía correo electrónico, cuando ocurran problemas en los servicios o recursos de red, así como cuando estos sean resueltos.

d) Monitoreo de tráfico:

- Uso de ancho de banda de la red.
- Distribución de trafico de red.

- Distribución del uso de protocolos de la red : TCP, UDP, ICMP, IP, IPX, ARP, DecNet, AppleTalk, Netbios, DNS, Telnet, FTP, SNMP.
- Distribución de paquetes por nodo.

e) Detección de problemas de red.

- Direcciones IP duplicadas.
- Identificación de equipos que utilizan protocolos innecesarios.
- Ancho de banda utilizado por un equipo determinado

f) Detección de violaciones de seguridad

- Detección de equipos en modo promiscuo.
- Detección de ataques de análisis de puertos.

3. Los resultados esperados dependerán en gran medida del uso adecuado que se le de a la(s) herramienta(s) implementadas.

CAPÍTULO II. MARCO TEÓRICO

2.1 CONCEPTOS GENERALES SOBRE REDES.

En los últimos años, las redes de computadoras han crecido dramáticamente en complejidad, rango geográfico y posibilidades de ubicación. Ésta breve sección introductoria tiene como objetivo proveer un contexto elemental sobre el estado actual de las redes informáticas.

Actualmente, grandes cantidades de datos atraviesan la red mundial de computadoras haciendo así posible una tecnología moderna de comunicaciones. A pesar de su relativa complejidad, las redes modernas son robustas y confiables.

Las redes modernas son marcadamente heterogéneas. Computadoras personales compatibles con IBM trabajan al lado de computadoras Macintosh; plataformas de DOS y Windows comparten datos con sistemas UNIX y con sistemas operativos propietarios; redes Ethernet y Token Ring se comunican con redes FDDI y ATM; y por si esto fuera poco, la comunicación sucede en una enorme mezcla de medio físicos. Un simple paquete de red puede pasar por medio de fibra óptica, cable coaxial, o par trenzado, etc., hasta ser enviado por medio de un satélite para que en su destino sea recibido por otra mezcla de computadoras, sistemas operativos y cables.

Otra característica de las redes modernas es la modularidad o el "diseño modular" del hardware y software para redes.

Hubo una época en la cual los desarrolladores producían ambientes de red que usaban software propietario, corriendo sobre hardware propietario, usando un solo tipo de cable. Esas redes "simples" fueron atractivas para muchos consumidores quienes requerían soluciones simples listas "al salir de la caja" ; Sin

embargo, los requerimientos de una entidad difícilmente pueden ser cubiertos por un sistema propietario solamente.

Por ejemplo, si los consumidores de un producto "X" deciden conectarse a la red de sus proveedores para consultar datos o compartir recursos de red, solamente encontrarían que la red de sus proveedores es simplemente incompatible con sus propios productos.

Una primera aproximación hacia la modularidad se hizo difícil en esa época. Pero a comienzos de los 80's, en lugar de decidir "cual red comprar", los consumidores encontraron por si mismos alternativas separadas para tarjetas de red, sistemas de cableado, dispositivos de interconexión, sistemas operativos de red, y aplicaciones para sus sistemas de red.

El incremento de la modularidad en el software para redes ha tenido un profundo y especial impacto. Esto es particularmente aparente en el "escritorio", en donde los protocolos de red pueden ser mezclados y complementados para suplir las necesidades del usuario, hasta el punto de que los administradores de estos sistemas, mezclan sistemas operativos de red (NOS, Network Operating Systems) para proveer la combinación de servicios requerida por la entidad en general, en lugar de buscar todos los beneficios en un producto simple.

Es necesario mencionar que el enfoque modular es sólo posible cuando se establecen acuerdos sobre standards adecuados. Nadie puede predecir exactamente que será lo que un usuario desee enviar por medio de la red, ni puede saberse a ciencia cierta que nos traerá una nueva generación de desarrollos tecnológicos. La única manera para que un desarrollador este seguro de que su producto trabajará con los componentes de una red, es adhiriéndose rigurosamente a standards reconocidos.

Cada fabricante de hardware debe conocer exactamente que se puede esperar como entrada a su parte del sistema, y lo que puede generar su parte del sistema como salida. Así también los desarrolladores de software deben apegarse a especificaciones similares.

El modelo de red OSI, que se tratará más adelante, ha tenido una influencia extrema en esta visión, permitiendo una clara y lógica delineación de las responsabilidades entre los componentes de una red. Al nivel de un "escritorio", la especificación ODI de Novell por ejemplo, era hasta hace un tiempo inimaginable: múltiples protocolos de red ejecutándose simultánea y silenciosamente sobre la misma plataforma de hardware. En este caso, solo la adopción de standards lo hizo posible.

Para concluir ésta breve introducción sobre el crecimiento de las redes en general, y particularmente de Internet, ha sido motivo de un significativo cambio en el nivel de conocimientos sobre las redes de computadoras. Este "elevado" conocimiento sobre las redes, ha sido también alimentado por la rápida expansión de las redes en los hechos de la vida cotidiana.

2.1.1 CONCEPTOS Y TERMINOLOGIA

Una red es un sistema de dispositivos de computadora interconectados entre sí para proveer acceso compartido y económico a una gran diversidad de servicios. La tarea de administrar el acceso a los servicios compartidos la realiza un tipo de software especializado conocido como "Sistema Operativo de Red" (NOS, Network Operating System). Actualmente, existen muchos NOS disponibles en el mercado, de los cuales algunos han destacado mas que otros y han logrado obtener un lugar privilegiado entre los usuarios.

- **EL MODELO CLIENTE / SERVIDOR**

El modelo Cliente / Servidor es un término que significa básicamente lo siguiente: es un sistema de computación en el cual la necesidad de procesamiento para completar una tarea particular es dividida entre una computadora centralizada llamada "SERVIDOR", y estaciones de trabajo individuales llamadas "CLIENTES". Estos dos elementos están conectados (por cables, medios infrarrojos, ondas de radio, o microondas) para lograr comunicación entre ellos.

Aunque estos dos elementos pueden ser computadoras muy parecidas en su arquitectura básica, las partes cliente y servidor regularmente presentan ciertas diferencias en cuanto a las configuraciones de hardware y software.

Esto depende de las funciones primarias de cada elemento, las cuales pueden ser vistas de la siguiente manera: el "cliente" hace peticiones a servicios ubicados en el "servidor" y el "servidor" por su parte, responde y provee de dichos servicios. Algunos ejemplos sencillos de operaciones cliente / servidor se mencionan a continuación:

- Una computadora ejecutando MS-DOS, hace la petición de un archivo almacenado en un servidor de archivos Netware.
- Una aplicación de Windows, requiriendo datos desde una computadora ejecutando Lotus Notes.
- Una computadora ejecutando OS/2, conectada a un mainframe de IBM, recibiendo información actualizada al minuto, sobre precios de productos
- Una PC ejecutando Windows XP, conectada a un Cisco Access Server para tener acceso a Internet

En cada caso, es claro cual sistema es el cliente y cual es el servidor. Es claro también, que la computadora que actúa como servidor provee un servicio que es esencial para que el cliente termine una determinada tarea.

Esta misma situación se reproduce "n" veces, ya que a un servidor pueden conectarse desde unas cuantas, hasta cientos de clientes al mismo tiempo, otra razón por la cual las características de software y hardware son superiores en el lado servidor.

Hay que hacer una diferenciación entre los sistemas centralizados en los cuales la parte importante del procesamiento ocurre en el servidor; mientras que en los sistemas distribuidos, el servidor hace una parte y el cliente hace otra, siendo las dos esenciales.

- **REDES PUNTO-A-PUNTO**

Mientras que las redes "cliente/servidor" se distinguen por lo diferente y especializado de las funciones de cada elemento, las redes punto-a-punto son justamente lo contrario. En estas redes, generalmente, ambas partes actúan simultáneamente como cliente y como servidor. Los recursos de cualquiera de las computadoras, pueden ser compartidos con cualquier otra computadora. Por ejemplo con Windows 98, los niveles de velocidad y confiabilidad de la red pueden ser aceptables hasta un número aproximado de 25 computadoras. Cuando se sobrepasa este número, debería dedicarse una de estas máquinas (con ciertas mejoras de hardware) como un pequeño servidor, pudiendo manejarse hasta 100 clientes sobre la red.

Cuando las redes sobrepasan este punto, es conveniente considerar la migración hacia una arquitectura completa de cliente / servidor.
Sin lugar a dudas la ventaja primaria de una red punto-a-punto es el bajo costo, pues prácticamente basta con las tarjetas de red, el cableado y dispositivos de concentración (opcionalmente).

Teniendo bien definidos los roles de los clientes y los servidores en una red, podemos pasar a considerar la red en sí misma. Una red esta compuesta por los medios de enlace entre las computadoras, y por los datos que se conducen entre los dispositivos.

Es recomendable manejar cierto vocabulario y conocimientos introductorios sobre los componentes y el funcionamiento de las redes computacionales. Algunos de estos conceptos son expuestos a continuación.

2.1.2 PROTOCOLOS

En cualquier discusión sobre tecnologías y métodos de comunicaciones de red, surgirá el término "*protocolo de red*". Un protocolo no es nada más que un conjunto de reglas y especificaciones que gobiernan la forma en que dos entidades se comunican. Por ejemplo, en las sociedades humanas, los lenguajes son protocolos formulados para permitir que una persona comprenda a otra, y por tanto, un uso impropio del lenguaje tiene como resultado una mala comprensión, o la ausencia total de cualquier comprensión.

Pues las computadoras también tienen definidos ciertos protocolos que especifican la manera correcta en que deben comunicarse entre ellas. Cuando cualquier dispositivo de hardware o un programa de software violentan estas reglas, no tiene lugar una comunicación correcta con las otras partes que sí están siguiendo dichas reglas.

Además los mensajes generados por una máquina de una manera no acorde a los protocolos aceptados, probablemente no sean aceptados por otras computadoras, sino que serán considerados como "ruido" e ignorados.

Debido a que la comunicación entre computadoras ocurre en varios niveles, es conveniente distinguir entre tipos diferentes de protocolos. El modelo OSI, es una construcción que está diseñada para ilustrar los siete niveles básicos de comunicaciones de red. Dicho modelo se cubrirá con más detalle posteriormente.

Para nuestro caso, NCP (Netware Core Protocol), TCP / IP y Ethernet, son técnicamente considerados protocolos, pero en diferentes niveles de comunicación. Una rápida vista a cada protocolo, puede hacer que estas distinciones sean mas claras.

El protocolo Ethernet funciona en la capa de transmisión o enlace de datos, proporcionando las reglas básicas para que las señales transmitidas a través de los medios de red sean formateadas de manera que representen datos. Los protocolos que funcionan en las capas antes mencionadas, se consideran dependientes unos de otros.

El protocolo TCP / IP (Transport Control Protocol / Internet Protocol) es un conjunto de reglas y standards, algunas veces llamados *suite de protocolos*, y que trabaja en las capas de red, transporte y sesión del modelo OSI. Dichas reglas controlan como los datos son enviados a través de la red por medio del "camino" correcto hasta llegar a su destino; también controla como son manejados los errores en la comunicación, y como son establecidas, mantenidas y terminadas las conexiones lógicas entre los nodos.

Y por último el NCP (Netware Core Protocol) es un conjunto de reglas que rige como las aplicaciones y los sistemas de computadoras se comunican en las capas de presentación y aplicación, por ejemplo: operaciones de procesamiento de datos tales como crear, leer, escribir y eliminar archivos, enviar trabajos de impresión, y conectarse / desconectarse de un servidor.
Otros protocolos de este tipo son el NFS (Network Filing System), y el AppleShare / AppleTalk.

2.1.3 TOPOLOGÍAS DE RED

Una topología es un patrón o forma de distribución de cómo el cable es usado para interconectar los diferentes componentes de una red. El concepto de topología está íntimamente ligado a la capa de enlace de datos del modelo OSI. Para elegir la topología adecuada hay que considerar aspectos tales como: la atenuación inherente al medio, la velocidad de la señal y la longitud de segmentos de cable.

Topología de Bus. Existen varias categorías generales de topologías físicas para una LAN, las cuales se diferencian por la forma en que el cable va de una estación a otra. La más simple de todas, y la primera y verdadera topología de LAN, es la topología de bus, la cual, consiste en un cable simple con los extremos libres de conexión (usando terminadores), y al cual las computadoras están conectadas. Esta topología es usada generalmente con cable coaxial.
Tal como en los circuitos conectados en serie, la topología de bus es susceptible a rupturas en cualquier punto del cableado dejando sin servicio a las demás estaciones.

Topología de Estrella. La posteriormente desarrollada topología de estrella, ha llegado a ser la más popular en las redes modernas, eliminando así el efecto de "guía de luces de Navidad" de la topología de bus. En esta topología, cada máquina conectada a la red tiene su propia conexión dedicada hacia un concentrador (hub).

Un hub es un dispositivo instalado en una localización central, que distribuye la señal a las estaciones conectadas. Tanto servidores como estaciones de trabajo pueden ser conectadas a un hub, y si ocurriera una falla en un cable en particular, solamente la computadora conectada a dicho cable sería afectada, continuando las demás con una operación normal. La topología de estrella es usada regularmente con cable de par trenzado (STP o UTP), tanto en redes Ethernet como en Token-ring.

Topología de Anillo. Esencialmente, una topología de bus en la cual los dos extremos están conectados forman una topología de anillo.
En este punto debemos hacer una consideración: una topología *física* difiere de una topología *lógica*. Por ejemplo el popular tipo de red Token-ring es actualmente construida usando una topología de estrella. Entonces podemos decir que la topología lógica describe como las señales recorren la red, y la física es como se distribuye el cableado. En el caso de la red Token-ring, se utilizan hubs especiales para crear un camino de datos en el cual las señales pasan de una computadora a otra, hasta llegar a la estación que originó la transmisión.

Topología de Malla. Este es otro tipo de distribución de cable que casi nunca se utiliza. En esta topología cada computadora tiene una conexión dedicada con cada una de las otras computadoras en la red. Uno de los problemas de esta topología se da en la capa de enlace de datos del modelo OSI, ya que no se podría transmitir señales en medios compartidos sin generar interferencia.
Este problema se puede solucionar evitando compartir el medio de transmisión, pero esto genera costos excesivos para la formación de la red. Por ejemplo para una red de 10 nodos serían necesarias 100 tarjetas de red y 100 secciones de cable; y aún resolviendo lo anterior, sería casi imposible encontrar computadoras que pudieran alojar 10 tarjetas de red cada una.

2.1.4 STANDARDS DE TRANSMISIÓN DE DATOS

Varios standards de transmisión de datos son usados comúnmente en la actualidad. En el presente estudio no se estudiarán exhaustivamente, pero los conocimientos en esta área son siempre necesarios para la mejor comprensión del estado actual de las redes de computadoras.

En cualquier protocolo de enlace de datos, una cantidad de datos determinada es "empaquetada" en un marco o paquete, el cual contiene información acerca de la dirección, enrutamiento, control y otra información adicional necesaria para que las

otras estaciones en la red puedan reconocer los datos relevantes para ellas, y además sepan que hacer con los datos que son recibidos.

ETHERNET.

Este standard fue desarrollado originalmente por Digital Equipment, Intel y Xerox, a finales de los años 70's. Desde entonces Ethernet ha sido adoptado como un standard internacional y ha llegado a ser el protocolo a nivel de enlace de datos predominante en nuestros días.

Ethernet trabaja originalmente a una razón de transferencia de 10 Mbps, y usa un método de control de acceso llamado Carrier Sense Multiple Access / Collision Detection (CSMA / CD).

En lugar de pasar un token (ficha) de estación a estación para permitir el acceso a transmisiones en la red, a cualquier estación Ethernet se le permite transmitir un paquete en cualquier momento, mientras la red no se encuentre ocupada por transmisiones de otras estaciones.

Cuando dos o más estaciones comienzan una transmisión al mismo tiempo una colisión ocurre. Las estaciones involucradas usualmente detectan la colisión e interrumpen la transmisión. Después de un período aleatorio de tiempo (algunos milisegundos nada mas) cada una de las estaciones intentan transmitir nuevamente, luego por supuesto de verificar que la línea está disponible. Un pequeño número de colisiones y otros errores son normales en una red Ethernet.

Debido a que es imposible determinar con precisión cual nodo será el siguiente en transmitir, e igualmente imposible garantizar que la transmisión sea exitosa, una red Ethernet es llamada una *red probabilística*. Debido a lo anterior, el aumento del tráfico en una red Ethernet causará un aumento en el número de

colisiones y errores, y por tanto la probabilidad de un paquete de ser transmitido exitosamente disminuirá. Para evitar problemas de saturación debe tenerse muy en cuenta la longitud de los segmentos, así como el número de nodos en la red, estos últimos factores dependen de los tipos de cable usados para construir la red.

Cuando se refiere a los variados standards de cableado para redes Ethernet, los términos tales como 10Base2 son frecuentemente usados. En estos términos, el primer número (10), se refiere a la razón de transferencia en megabits por segundo (Mbps). La palabra después del primer número (Base), indica un ancho de banda para la transmisión, y el último número se refiere a la longitud en unidades de 100 metros, a las que un segmento de cable está limitado. Las formas más comunes de Ethernet son 10Base5, 10Base2 y 10BaseT (para twisted pair), y son conocidas también como Thick Ethernet, Thin Ethernet, y UTP, respectivamente.

Actualmente se conocen también las variedades 100BaseT y 100BaseTX, que como podría suponerse sostienen razones de transferencia de 100 Mbps. Ethernet puede ser usado en redes ejecutando prácticamente cualquier sistema de operativo de red (NOS), y protocolos de transporte disponibles actualmente, incluyendo NetWare, Windows NT, LAN Server, VINES, y muchas de las variedades de UNIX.

TOKEN RING.

Token Ring fue desarrollado a mediados de los 80's por IBM, y aceptado como un standard industrial poco después. Las estaciones en una red token ring tienen acceso a la red solamente cuando están en posesión de un "token", el cual es un paquete especial, el cual es pasado de una estación a la siguiente. Como se mencionó anteriormente una red token ring puede usar una topología de estrella, donde los cables de cada estación están conectados a un punto central de acceso llamado Multistation Access Unit (MSAU). Este MSAU es el dispositivo que realiza

las operaciones de anillo en la red, permitiendo a las estaciones solamente transmitir paquetes a la siguiente, y recibir paquetes de la anterior en el anillo.

La razón de transferencia original de las redes Token Ring fue de 4 Mbps. Hoy en día la mayoría presentan una razón de 16 Mbps. En una red Token Ring puede determinarse precisamente que estación será la siguiente en transmitir, y el acceso para estas transmisiones está prácticamente garantizado mientras no ocurran errores de hardware; debido a esto las redes token ring son llamadas *redes determinísticas*, todo lo contrario de una red Ethernet.

En estas redes tampoco se espera la ocurrencia de colisiones, y si estas ocurren entonces son responsabilidad del administrador de la red.
Las reglas que gobiernan el diseño de una red token ring son mucho más complicadas que en una red Ethernet. En sus principios por ejemplo el cableado era propietario y distribuido solamente por IBM, pero en la actualidad puede usarse tanto STP como UTP para estas redes. Como punto adicional, podemos mencionar que debido a que las tarjetas de red para token ring necesitan cierta "inteligencia" adicional, esto vuelve a este tipo de redes considerablemente mas caras que las redes Ethernet.

FDDI.

Fiber Distributed Data Interface, es una topología de alta velocidad y tolerante a fallas, que soporta transmisiones a velocidades de 100 Mbps sobre una red con un tamaño hasta 100 Km. La máxima distancia entre nodos es de 2 Km. Otra de las ventajas de este tipo de red, es que cuando suceden rupturas en el sistema de cableado, es posible todavía la comunicación con las estaciones colocadas entre las rupturas.

2.1.5 DISPOSITIVOS IMPORTANTES DE INTERNETWORKING

Repetidores (Repeaters)

Estos son usados para interconectar segmentos de red en LAN's de gran tamaño. Estos dispositivos hacen justamente lo que su nombre indica: repetir cada señal recibida en uno de sus puertos hacia sus demás puertos. Debido a esto, los repetidores no solamente repiten los datos correctos, sino también las colisiones y los errores. Los repetidores trabajan en la capa física del modelo OSI, y no poseen capacidades de filtrado de tráfico, o conversión de paquetes. Otra observación es que los repetidores deben ser utilizados entre segmentos idénticos o muy similares de red. Lograr la interconexión de dos o más redes diferentes requiere de un dispositivo que trabaje en una capa más alta del modelo OSI.

Puentes (Bridges)

Los puentes trabajan en la capa de enlace de datos del modelo OSI. Primariamente los puentes requerían de tablas de direcciones que debían ser entradas a mano, pero en nuestros días, la mayoría son puentes que "aprenden".

La técnica más usada para la conexión de redes Ethernet es la conocida como *conexión transparente*, la cual funciona así: El puente monitorea el tráfico en todos sus puertos y guarda las direcciones de nodo de las estaciones conectadas a la red en una tabla en memoria. Cuando se recibe un paquete en un puerto, destinado a un nodo en un puerto diferente, el paquete se pasa a dicho puerto para que llegue a su destino. Si se recibe un paquete para un nodo desconocido, se envía el paquete a todos los puertos y se espera por una respuesta. Cuando esta es recibida en un puerto cualquiera, se añade la dirección del nodo a la tabla para dicho puerto, y además se pasa la respuesta al que inició la transmisión originalmente. De esta

forma, un puente puede "aprender" cuales estaciones están conectadas a cada puerto, y como llegar hasta ellas.

Los puentes pueden trabajar con casi cualquier protocolo, debido a que solamente requiere de las direcciones de nodo para la fuente y el destino del paquete. Por lo tanto los puentes pueden ser utilizados para conectar redes no similares.

Enrutadores (routers)

Los enrutadores operan en la capa de red del modelo OSI. Cada red individual en un entorno enrutado es identificada por una sóla dirección de red. Un enrutador inicialmente necesita las direcciones de las redes a las que está directamente conectado. Los enrutadores también pueden aprender acerca de redes distantes y el mejor camino hacia ellas, esto desde otros enrutadores.

Cuando un enrutador recibe un paquete que contiene una dirección de red diferente a la de origen, retransmite la dirección al puerto correcto hasta que este alcanza su destino. Los enrutadores no necesitan conocer las direcciones de los nodos individuales, sino solo las direcciones de las redes conectadas a él.

Además los enrutadores pueden "aprender" múltiples caminos hacia otras redes, y a saber a cuantos "saltos" de distancia está dicha red. Los enrutadores consiguen información acerca de sus redes conocidas por medio de un protocolo llamado Router Information Protocol (RIP), usualmente cada 30 segundos.

Hay que hacer la aclaración de que no todos los protocolos pueden ser enrutados, ya que muchos de ellos no incluyen la información necesaria sobre la dirección de red. Por ejemplo TCP/IP e IPX son protocolos que pueden ser procesados por las interfaces de un enrutador. En cambio NetBEUI usado por Microsoft e IBM no pueden pasar por un enrutador necesitan ser procesados por un

puente. Algunos enrutadores tienen la capacidad de realizar los procesos de un puente para los protocolos que no tienen la información de direcciones necesaria y son llamados *brouters* (bridge / routers).

Otra forma de manejar los protocolos que no pasan por un enrutador, es usando la técnica llamada *tunneling*.

Esta técnica encapsula cada paquete entero de un protocolo, como la porción de datos, dentro de un "sobre" de otro protocolo que si contenga la información de direcciones de red. Cuando el "sobre" llega a la red destino, es "abierto" y el protocolo original del paquete es restaurado.

Interruptores (switches)

Una nueva tecnología diseñada para satisfacer la demanda de ancho de banda en redes Ethernet es la llamada *switching*. Los switches Ethernet son realmente puentes (bridges) extremadamente rápidos y con muchos puertos. Solamente unas cuantas estaciones son conectadas a cada puerto, y la conexión del servidor principal es usualmente un link de alta velocidad, tales como full-duplex 10BaseT, FDDI, o 100BaseT(X). De esta forma, el ancho de banda completo de 10 Mbps de Ethernet puede ser dedicado a unas pocas estaciones en un dominio de colisiones más simple, y la conexión de alta velocidad en el server no obliga a ningún cambio de hardware o software en las estaciones.

2.1.6 EL MODELO OSI

El llamado Modelo de Referencia OSI es el producto de dos proyectos de desarrollo independientes tanto de la ISO (International Standards Organization), y el International Telegraph and Telephone Consultative Commitee, comenzando a finales de los años 70's.

Dos documentos separados fueron producidos, cada uno definiendo un modelo de comunicaciones de red de siete capas, pero en 1983 fueron combinados y eventualmente publicados como el standard ISO 7498. Su nombre completo es "The Basic Reference Model for Open Systems Interconnection", y de ahí las siglas OSI.

Uno de los problemas más grandes al estudiar el modelo OSI y su papel preponderante en las comunicaciones de red es la nomenclatura o terminología usada para describir los elementos de cada capa. Por ejemplo, los "marcos" son generados en la capa de enlace de datos; los "datagramas" en la capa de red; y los "mensajes" en la capa de aplicación.

De la forma más simple, las comunicaciones de red pueden ser reducidas a "peticiones" (requests) y "respuestas" (replies). La unidad fundamental de datos transmitidos sobre una red es el "paquete" (packet).

A continuación se describen de manera breve cada una de las capas de este modelo:

- **LA CAPA FÍSICA:**

La capa física del modelo, se refiere al medio por el cual los bits son transmitidos desde un host origen hacia otro destino. La conexión entre dos estaciones de red se logra por medio de algún tipo de medio conductor como por ejemplo: fibra óptica, cable UTP, cable coaxial, señales de radio, microondas, láser, infrarrojos, etc.

Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física.

- **LA CAPA DE ENLACE DE DATOS:**

Esta capa funciona como una interface entre los medios físicos y los protocolos y capas más altas, es responsable de empaquetar los datos binarios provenientes de niveles más altos, en paquetes discretos que puedan ser enviados por la capa física. En esta capa los paquetes transmitidos contienen la información de direccionamiento básico (direccionamiento físico) para que puedan ser correctamente llevados hacia su destino.

Esta capa también controla el acceso a los recursos de red. Esto es importantísimo teniendo en cuenta que en una red típica pueden existir docenas de estaciones tratando de usar estos recursos al mismo tiempo. Si todas estas estaciones transmitieran sus paquetes al mismo tiempo, el resultado sería caótico. Los protocolos que funcionan en esta capa, proveen además otros servicios tales como chequeo y corrección de errores, y control del flujo de paquetes.

Tal como la capa física, la capa de enlace de datos no es la responsable de llevar el paquete a su destino último. Solamente le concierne como mover el paquete hacia la próxima estación consecutiva en la red; y los elementos más complicados de este "viaje" son manejados por las capas más altas en el modelo OSI.

Otro aspecto de esta capa es el control de errores, el cual es un método de verificar que un paquete llegue a su destino tal como fue transmitido.

Este control se realiza haciendo uso de CRC (Cyclic redundancy check) de la siguiente forma: un algoritmo matemático es aplicado al contenido del paquete y el resultado es incluido en el paquete, usualmente cerca del final del mismo. Una vez que se ha enviado, el mismo algoritmo es aplicado por el receptor y los resultados son comparados con los guardados en el paquete. Si estos coinciden, es un indicativo de una transmisión correcta. Si existen discrepancias el paquete es desechado.

En algunos casos existen mecanismos para indicar al transmisor ésta situación y que el paquete debe ser reenviado, mientras que en otros, esta función es dejada a capas más altas.

- **LA CAPA DE RED:**

La capa de red es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Puede decirse que esta capa es la línea que divide los tipos de comunicación que ocurren en una red, ya que esta es la única capa a la que concierne la completa transmisión de paquetes desde la fuente hasta su destino. Las funciones provistas por las capas anteriores se pueden ver como "locales" ya que están diseñadas solamente para mover los paquetes hacia la próxima estación en la red. La tarea primaria de la capa de red es proveer la funcionalidad de enrutamiento necesaria para que los paquetes puedan ser enviados al mismo segmento de red, a una red adyacente, o a una red a miles de kilómetros de distancia. Algunas de las funciones que competen a la capa de red son:

- La división del flujo de datos binarios en paquetes discretos de una especificada longitud
- La detección de errores
- La corrección de errores a través de la retransmisión de paquetes "malos"
- El control del flujo de datos

Podría pensarse que estas mismas funciones son de las que se hablaba en la capa de enlace de datos, y en realidad lo son. La diferencia radica en que éstas funciones en ésta capa son provistas para la transmisión completa desde el transmisor al receptor, y no solo al nodo adyacente.

- **LA CAPA DE TRANSPORTE:**

La función primaria de esta capa, es proveer de los servicios esenciales no provistos por la capa de red. Si la funcionalidad de la capa de red disminuye, esto causa que la complejidad de la capa de transporte aumente. Entonces la tarea de la capa de transporte es proveer funciones que son necesarias para elevar la *calidad del servicio de red*, a un nivel aceptable para las comunicaciones. Algunos de los criterios para evaluar esta calidad de servicio son:

- Costos de las comunicaciones
- Ancho de banda disponible para la comunicación
- Recuperación de errores señalados por la capa de red
- Recuperación de pérdida de paquetes
- Reordenamiento de paquetes que llegan fuera de secuencia
- Detección de errores no encontrados en capas más bajas

- **LA CAPA DE SESIÓN:**

Como su nombre lo indica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que llevan a cabo una comunicación. Presta servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos.

Algunos de los protocolos (no servicios) reales que funcionan en la capa de sesión frecuentemente entrelazan dicha capa con las dos superiores (presentación y aplicación) son los siguientes:

- NetBIOS. Interface de sesión y protocolo, desarrollado por IBM, que también provee servicios referidos a las capas de transporte, presentación y aplicación.
- NetBEUI (NetBIOS Extended User Interface). Una extensión del NetBIOS 1usada por Microsoft en sus productos de redes, tales como Windows NT y LAN Manager.
- ADSP (AppleTalk Data Stream Protocol). Es la parte de la suite de protocolos AppleTalk responsable por establecer conexiones confiables entre nodos.
- PAP (Printer Access Protocol). Provee acceso a impresores Postscript en redes AppleTalk.

- **LA CAPA DE PRESENTACIÓN:**

La capa de presentación provee solamente un servicio de gran importancia: Desarrollar la "traducción" de diferentes tipos de sistemas de sintaxis.

En otras palabras, una petición originada en la capa de aplicación necesariamente utiliza la sintaxis nativa de la aplicación que genera la petición. La aplicación destino ubicada en el otro extremo del sistema, puede utilizar una sintaxis completamente diferente o diferente formato de codificación de bits. Por ejemplo, una conexión entre una PC y un mainframe puede requerir conversión desde el sistema de codificación EBCDIC al sistema ASCII. Para que esta traducción ocurra, la capa de presentación es responsable en ambos extremos del sistema de convertir la sintaxis nativa de cada aplicación (*sintaxis abstracta*), a una sintaxis común (*sintaxis de transferencia*), que sea conveniente para la transmisión a través de los medios de red.

- **LA CAPA DE APLICACIÓN:**

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. La aplicación puede ser un

procesador de texto tratando de recuperar un archivo en un volumen de un servidor de archivos. También podría ser una aplicación que solamente existe con el propósito de proveer una interface hacia un recurso de la red, tales como un protocolo ejecutable como son Telnet o FTP.

En cualquiera de los casos y en muchos otros, incluyendo el correo electrónico (e-mail), acceso a bases de datos y administración de archivos y redes, la capa de aplicación del modelo provee las herramientas necesarias para acceder a aquellos recursos de red disponibles. En pocas palabras, esta capa es una ventana entre aplicaciones funcionando en sistemas remotos.

2.2 LA SUITE DE PROTOCOLOS TCP/IP

TCP/IP es un conjunto de protocolos (suite) de comunicación de datos. Estos protocolos permiten transmitir la información de una máquina a otra, la entrega de correo electrónico y noticias, e incluso el uso de capacidades de sesiones remotas.

El nombre de TCP / IP se refiere a dos nombres principales: Protocolo de Control de Transmisión y Protocolo de Internet. Aunque hay muchos otros protocolos que ofrecen servicios que operan sobre TCP/IP, estos son los más comunes.

2.2.1 COMPONENTES DE TCP / IP

Para comprender los roles de los componentes de la familia de protocolos TCP/IP, es muy útil conocer que se puede hacer sobre una red TCP/IP. Así una vez que las aplicaciones son comprendidas, se hace posible de forma más sencilla comprender los protocolos. La lista siguiente no es una lista exhaustiva, pero menciona las aplicaciones primarias que provee TCP/IP.

- **TELNET**

El programa Telnet (telecommunications network) ha sido diseñado para proveer capacidades de acceso remoto (llamado también terminal virtual) a través de la red. En otras palabras, un usuario en la máquina A, debe ser capaz de acceder a la máquina B, donde quiera que se encuentre con respecto a la red, y no importa que tan alejado se encuentre, debe percibir la sensación de encontrarse frente a la máquina B. El servicio Telnet es provisto a través de uno de los puertos "bien conocidos" de TCP, el cual es el puerto 23. El término Telnet se usa para referirse tanto al programa, como al protocolo que se usan para proveer dicho servicio.

Telnet fue desarrollado debido a la necesidad existente de poder acceder a los recursos de otra máquina (incluyendo unidades de disco y los programas guardados en ellas), por medio de dispositivos tales como módems, puertos seriales dedicados, o tarjetas de red.

En una primera vista Telnet puede parecer sencillo, hasta que se piensa en la amplia diversidad de terminales y computadoras, cada una con sus propios códigos de control y características.

Otro problema, lo representaba el hecho de que cuando conectamos directamente dos máquinas, la máquina anfitriona (servidor) debe manejar la "traducción" de los códigos de la terminal (cliente), lo cual impone una carga extra al CPU del servidor. Ahora imaginemos una situación en la cual estuvieran conectadas varias computadoras (o hubieran varias sesiones) a un servidor. Entonces el servidor debería manejar la traducción completa para cada terminal, lo cual podría ocasionar que las capacidades del CPU fueran consumidas casi en su totalidad por esta función.

Telnet entonces, resuelve este problema, mediante el hecho de "anexar" las características de los tipos diferentes de terminal dentro del protocolo. Cuando dos computadoras se comunican usando Telnet, Telnet por si mismo puede determinar y

ajustar las características de comunicación de la terminal durante la fase de conexión. Cuando una conexión es establecida, ambos extremos de la misma, aceptan un método común para intercambiar información, eliminando así un buen porcentaje de la carga del CPU del servidor.

Usualmente, Telnet involucra un proceso en el cual el servidor acepta peticiones (requests) entrantes de una sesión Telnet. En sistemas UNIX, este proceso es llamado "telnetd". En Windows NT y otros sistemas operativos para PC's, un programa "Servidor de Telnet" es lo común.

El cliente (quien hace la "llamada") ejecuta un programa, generalmente llamado Telnet, que intenta conectarse al servidor especificado. Uno de estos programas utilizado en ambiente Unix es el "rlogin".

El protocolo Telnet usa el concepto de *terminal de red virtual*, o NVT (network virtual terminal), que define a ambos extremos de la conexión Telnet. Cada extremo en dicha conexión (cada NVT) posee un teclado y un impresor lógicos. El impresor lógico puede desplegar caracteres, y el teclado lógico puede generar caracteres. El impresor lógico es usualmente la pantalla, y el teclado lógico es el mismo teclado físico que utiliza el usuario. Estos términos (teclado e impresor lógicos) también son usados en FTP y SMTP.

Para iniciar una sesión Telnet, debe proveerse ya sea el nombre o la dirección IP de la máquina con la que deseamos conectarnos. El nombre puede ser utilizado solamente en sistemas donde puede convertirse dicho nombre en su respectiva dirección IP, por medio de un DNS.

- **FTP**

El protocolo de transferencia de archivos, usualmente conocido como FTP, es una utilidad para administrar archivos entre máquinas sin la necesidad de establecer una sesión Telnet. FTP permite transferir archivos hacia y desde la maquina destino,

administrar directorios, y acceder al correo electrónico. En realidad FTP no está diseñado para permitir la ejecución de programas, pero en algunas ocasiones puede ser absolutamente necesario, además de transferir archivos.

FTP usa dos "canales" o puertos de TCP. El puerto 20 de TCP es el canal de datos, y el puerto 21 es el canal de comandos o de control. En este sentido FTP es un tanto diferente de las demás aplicaciones basadas en TCP / IP, no solo por el uso de los dos canales o puertos, que permiten la transferencia simultanea de datos y comandos, sino también porque transfiere todos los archivos en primer plano (foreground), en lugar de hacerlo en segundo plano (background). En otras palabras, FTP no usa spools o colas, sino que le permite al usuario ver el proceso de transferencia en tiempo real.

En jerga propia de FTP, los dos canales que existen entre las dos máquinas son llamados *protocol interpreter* o PI (interprete de protocolo), y *data transfer process* o DTP (proceso de transferencia de datos). El PI transfiere instrucciones entre las dos implementaciones utilizando el puerto 21, y el DTP transfiere datos en el puerto 20.

Así como con el caso de Telnet, que usa un programa "servidor" que se ejecuta continuamente y un programa separado ejecutado en el lado cliente, también FTP, por lo menos en los sistemas Unix, tiene programas similares llamados ftpd, para el servidor, y ftp para el cliente.

Para iniciar una sesión FTP, se realiza de forma parecida a una sesión Telnet, usando la dirección IP de la máquina a la que el usuario desea conectarse.

- **SMTP**

Simple Mail Transfer Protocol (SMTP), es usado para transferir correo electrónico. SMTP es completamente transparente al usuario. Detrás de bambalinas, SMTP se conecta a computadoras remotas y transfiere los mensajes de correo de forma muy similar a las transferencias usando FTP. Los usuarios finales casi nunca se preocupan del funcionamiento del SMTP, y solo algunos administradores de sistemas de redes deben tratar con él. SMTP es un protocolo (servicio) bastante libre de problemas, y es muy ampliamente usado.

- **DNS**

Un nombre simbólico es una cadena de caracteres usada para identificar una máquina específicamente. Un nombre simbólico puede ser simple, o tan complicado como se decida.

Cuando se envía información a máquinas remotas por medio de Internet, las direcciones IP deben ser usadas. En lugar de pedirle a un usuario que memorice la dirección como tal de una determinada computadora, es común utilizar un nombre simbólico. Después de todo, un nombre es mucho más fácil de memorizar que una dirección de Internet de 32 bits.

Una de las posibles soluciones al problema de conocer cada computadora por su "nombre" en lugar de su dirección, es configurar un archivo o servicio (como él /etc/hosts, en Unix), donde están registrados todos los nombres y sus correspondientes direcciones IP.

Esto funciona en redes pequeñas, con un número bien definido o poco cambiante de estaciones. Pero cuando tratamos con una red como Internet, es hasta cierto punto imposible disponer de un archivo que contenga todos los posibles nombres simbólicos y sus correspondientes direcciones.

Y aunque esto pudiera ser posible, el mundo de Internet cambia a pasos tan apresurados que no existiría forma de mantener dicho archivo actualizado, por lo menos de manera diaria para que la lista fuera confiable.

La solución a este problema se encontró en ofrecer un método de administrar las tablas de búsqueda o "resolución" más allá del NIC, permitiendo realizar esta tarea a cada red de manera autónoma. Este sistema es el Domain Name Service (DNS), el cual es llamado algunas veces Internet Directory Service, pero este nombre no es reconocido ampliamente.

- **SNMP**

Simple Network Management Protocol (SNMP) provee mensajes de estado y reporte de problemas en un entorno de red, esto hacia un administrador del sistema. SNMP utiliza UDP (User Datagram Protocol) como un mecanismo de transporte.

- **NFS**

Network File System (NFS), es un conjunto de protocolos y servicios desarrollado por Sun Microsystems, que permite a las computadoras en una red, accesar a los directorios de otras de manera transparente. Sistemas NFS son comunes en entornos corporativos, especialmente en aquellos que usan estaciones de trabajo UNIX.

- **TFTP**

Trivial File Transfer Protocol (TFTP) es un protocolo simple, no sofisticado de transferencia de archivos con ciertas deficiencias de seguridad. Este protocolo, usa UDP como transporte. TFTP realiza la misma tarea que FTP, pero usa un protocolo de transporte diferente.

- **TCP**

Transmission Control Protocol (TCP), es un protocolo de comunicaciones que permite transmisiones confiables de datos. Es el responsable de ensamblar los datos pasados por aplicaciones de capas más altas (Modelo OSI) en paquetes standard, y además asegurar que los datos son transferidos correctamente.

- **UDP**

Para efectos de comparación es bueno dar un breve vistazo a este protocolo (UDP). Anteriormente mencionamos que TCP es un protocolo basado en conexiones, mientras que UDP es un protocolo no orientado o no basado en conexiones, usado por los servicios TFTP y RPC, como ejemplo.

Por no estar basado en conexiones, no es un protocolo 100% confiable, ya que no existen una indicación de que el mensaje enviado fue recibido correctamente. Los protocolos no orientados a las conexiones no ofrecen capacidades de recuperación de errores. Por tanto UDP es mucho más simple que TCP. Su interfaz con IP (y otros protocolos) no tiene mecanismos de control de flujo y recuperación de errores, funciona simplemente como un "enviador" y "receptor" de datagramas.

También como otra consecuencia del tipo de protocolo que es UDP, su encabezado de protocolo es mucho más simple.

- **IP**

El protocolo de Internet (IP) es uno de los protocolos primarios en el modelo OSI, y como ya sabemos, parte integral de TCP / IP. Aunque su nombre lo sugiere, su uso no está restringido solo al mundo de Internet. Es verdad que todas las máquinas en Internet pueden usar y comprender este protocolo, pero IP también puede ser usado en redes dedicadas que no tienen relación alguna con Internet. IP define un protocolo, no una conexión específicamente. De hecho, IP es una buena elección para cualquier red que necesite un protocolo eficiente para comunicaciones

máquina a máquina, y en este campo enfrenta cierta competencia de protocolos tales como IPX de Novell Netware.

¿Cuáles son las funciones de IP?

Sus principales atribuciones son el direccionamiento de datagramas de información entre computadoras, y además administrar la fragmentación de dichos datagramas. Esta fragmentación se refiere al hecho de que los datos pueden ser "rotos" o separados en porciones pequeñas para efectos de transmisión, y luego ser reensamblados en otra localización.

A este proceso completo se le llama "fragmentación y reensamblado". IP provee un tamaño máximo de paquete de 65,535 bytes, lo cual está muy por encima de lo que pueden manejar la mayoría de redes, y de ahí la necesidad de la fragmentación. IP entonces tiene la capacidad de dividir automáticamente un datagrama de información en datagramas más pequeños si es necesario.

Cuando el primer datagrama de un mensaje largo que ha sido dividido en fragmentos llega a su destino, un "temporizador de reensamblaje" es iniciado por la máquina que lo recibe. Si todas las piezas del datagrama completo no son recibidas antes de que el temporizador llegue a su valor máximo predeterminado, todos los datagramas que si habían sido recibidos son descartados.

Además la máquina que recibe los fragmentos conoce el orden en el cual las piezas deben ser reensambladas ya que esta información se encuentra en un campo del encabezado IP. Una consecuencia de este proceso, es que un mensaje fragmentado tiene menores probabilidades de llegar que un mensaje sin fragmentación, lo cual hace que la mayoría de aplicaciones traten de evitar la fragmentación siempre que sea posible.

IP es un protocolo no orientado a la conexión, lo que significa que no le interesa ni se preocupa acerca de los nodos por los que el datagrama pasa a través de su camino, o en que máquinas comienza y termina el datagrama.

Cuando se habla de encabezados, hay un término común el cual es la encapsulación, y que se refiere al hecho de añadir "algo" al inicio (y algunas veces al final) de los datos, tal como una cápsula encierra una sustancia medicinal. El encabezado y la "cola" añadidos brindan detalles sobre los datos encerrados.

- **ICMP**

Internet Control Message Protocol (ICMP) es el responsable de la revisión y generación de mensajes sobre el estado de los dispositivos en una red. También puede ser usado para informar a otros dispositivos de fallas en máquinas específicas. ICMP e IP regularmente trabajan juntos.

2.3 GNU (LICENCIA PÚBLICA GENERAL)

Las licencias que cubren la mayor parte del software están diseñadas para quitarle al usuario la libertad de compartirlo y modificarlo. Por el contrario, la Licencia Pública General de GNU pretende garantizar la libertad de compartir y modificar software libre, para asegurar que el software es libre para todos los usuarios. Esta Licencia Pública General se aplica a la mayor parte del software del la Free Software Foundation y a cualquier otro programa si sus autores se comprometen a utilizarla.

Cuando se habla de software libre, se refiere a libertad, no a precio. Las Licencias Públicas Generales están diseñadas para asegurar que se tenga la libertad de distribuir copias de software libre (y cobrar por ese servicio si se quiere), de que se reciba el código fuente o que pueda conseguirse si se quiere, de que se pueda modificar el software o usar fragmentos de él en nuevos programas libres, y de que se de a conocer que pueden hacerse todas estas cosas.

Para proteger los derechos de un autor se necesitan de algunas restricciones las cuales prohíban a cualquiera negarle al autor éstos derechos o pedirle que renuncie a ellos. Estas restricciones se traducen en ciertas obligaciones que le afectan si distribuye copias del software, o si lo modifica.

Por ejemplo, si se distribuye copias de uno de estos programas, sea gratuitamente, o a cambio de una contraprestación, es necesario dar a los receptores todos los derechos que tiene. Debe asegurarse de que ellos también reciben, o pueden conseguir, el código fuente. Y debe mostrarse estas condiciones de forma que conozcan sus derechos.

También, para la protección de cada autor, no se proporciona ninguna garantía para el software libre. Si el software se modifica por cualquiera y éste a su vez lo distribuye, los receptores deben saber que lo que tienen no es el original, de forma que cualquier problema introducido por otros no afecte a la reputación de los autores originales.

Por último, cualquier programa libre está constantemente amenazado por patentes sobre el software. GNU evita el peligro de que los redistribuidores de un programa libre obtengan patentes por su cuenta, convirtiendo de facto el programa en propietario. Para evitar esto, GNU ha dejado muy en claro que cualquier patente debe ser pedida para el uso libre de cualquiera, o no ser pedida.

Los términos exactos y las condiciones para la copia, distribución y modificación se exponen a continuación.

Términos y condiciones para la copia, distribución y modificación[1]

1. Esta Licencia se aplica a cualquier programa u otro tipo de trabajo que contenga una nota colocada por el tenedor del copyright diciendo que puede ser distribuido bajo los términos de esta Licencia Pública General. En adelante, «Programa» se referirá a cualquier programa o trabajo que cumpla esa condición y «trabajo basado en el Programa» se referirá bien al Programa o a cualquier trabajo derivado de él según la ley de copyright. Esto es, un

trabajo que contenga el programa o una porción de él, bien en forma literal o con modificaciones y/o traducido en otro lenguaje. Por lo tanto, la traducción está incluida sin limitaciones en el término «modificación». Cada concesionario (licenciatario) será denominado «usted».

Cualquier otra actividad que no sea la copia, distribución o modificación no está cubierta por esta Licencia, está fuera de su ámbito. El acto de ejecutar el Programa no está restringido, y los resultados del Programa están cubiertos únicamente si sus contenidos constituyen un trabajo basado en el Programa, independientemente de haberlo producido mediante la ejecución del programa. El que esto se cumpla, depende de lo que haga el programa.

2. Usted puede copiar y distribuir copias literales del código fuente del Programa, según lo has recibido, en cualquier medio, supuesto que de forma adecuada y bien visible publique en cada copia un anuncio de copyright adecuado y un repudio de garantía, mantenga intactos todos los anuncios que se refieran a esta Licencia y a la ausencia de garantía, y proporcione a cualquier otro receptor del programa una copia de esta Licencia junto con el Programa.

   Puede cobrar un precio por el acto físico de transferir una copia, y puede, según su libre albedrío, ofrecer garantía a cambio de unos honorarios.

3. Puede modificar su copia o copias del Programa o de cualquier porción de él, formando de esta manera un trabajo basado en el Programa, y copiar y distribuir esa modificación o trabajo bajo los términos del apartado 1, antedicho, supuesto que además cumpla las siguientes condiciones:
   a. Debe hacer que los ficheros modificados lleven anuncios prominentes indicando que los ha cambiado y la fecha de cualquier cambio.
   b. Debe hacer que cualquier trabajo que distribuya o publique y que en todo o en parte contenga o sea derivado del Programa o de cualquier parte de él sea licenciada como un todo, sin carga alguna, a todas las terceras partes y bajo los términos de esta Licencia.

c. Si el programa modificado lee normalmente órdenes interactivamente cuando es ejecutado, debe hacer que, cuando comience su ejecución para ese uso interactivo de la forma más habitual, muestre o escriba un mensaje que incluya un anuncio de copyright y un anuncio de que no se ofrece ninguna garantía (o por el contrario que sí se ofrece garantía) y que los usuarios pueden redistribuir el programa bajo estas condiciones, e indicando al usuario cómo ver una copia de esta licencia. (Excepción: si el propio programa es interactivo pero normalmente no muestra ese anuncio, no se requiere que su trabajo basado en el Programa muestre ningún anuncio).

Estos requisitos se aplican al trabajo modificado como un todo. Si partes identificables de ese trabajo no son derivadas del Programa, y pueden, razonablemente, ser consideradas trabajos independientes y separados por ellos mismos, entonces esta Licencia y sus términos no se aplican a esas partes cuando sean distribuidas como trabajos separados. Pero cuando distribuya esas mismas secciones como partes de un todo que es un trabajo basado en el Programa, la distribución del todo debe ser según los términos de esta licencia, cuyos permisos para otros licenciatarios se extienden al todo completo, y por lo tanto a todas y cada una de sus partes, con independencia de quién la escribió.

Por lo tanto, no es la intención de este apartado reclamar derechos o desafiar sus derechos sobre trabajos escritos totalmente por usted mismo. El intento es ejercer el derecho a controlar la distribución de trabajos derivados o colectivos basados en el Programa.

Además, el simple hecho de reunir un trabajo no basado en el Programa con el Programa (o con un trabajo basado en el Programa) en un volumen de almacenamiento o en un medio de distribución no hace que dicho trabajo entre dentro del ámbito cubierto por esta Licencia.

4. Puede copiar y distribuir el Programa (o un trabajo basado en él, según se especifica en el apartado 2, como código objeto o en formato ejecutable según los términos de los apartados 1 y 2, supuesto que además cumpla una de las siguientes condiciones:
    a. Acompañarlo con el código fuente completo correspondiente, en formato electrónico, que debe ser distribuido según se especifica en los apartados 1 y 2 de esta Licencia en un medio habitualmente utilizado para el intercambio de programas, o
    b. Acompañarlo con una oferta por escrito, válida durante al menos tres años, de proporcionar a cualquier tercera parte una copia completa en formato electrónico del código fuente correspondiente, a un coste no mayor que el de realizar físicamente la distribución del fuente, que será distribuido bajo las condiciones descritas en los apartados 1 y 2 anteriores, en un medio habitualmente utilizado para el intercambio de programas, o
    c. Acompañarlo con la información que recibiste ofreciendo distribuir el código fuente correspondiente. (Esta opción se permite sólo para distribución no comercial y sólo si usted recibió el programa como código objeto o en formato ejecutable con tal oferta, de acuerdo con el apartado b anterior).

Por código fuente de un trabajo se entiende la forma preferida del trabajo cuando se le hacen modificaciones. Para un trabajo ejecutable, se entiende por código fuente completo todo el código fuente para todos los módulos que contiene, más cualquier fichero asociado de definición de interfaces, más los guiones utilizados para controlar la compilación e instalación del ejecutable. Como excepción especial el código fuente distribuido no necesita incluir nada que sea distribuido normalmente (bien como fuente, bien en forma binaria) con los componentes principales (compilador, kernel y similares) del sistema operativo en el cual funciona el ejecutable, a no ser que el propio componente acompañe al ejecutable.

Si la distribución del ejecutable o del código objeto se hace mediante la oferta acceso para copiarlo de un cierto lugar, entonces se considera la oferta de acceso para copiar el código fuente del mismo lugar como distribución del código fuente, incluso aunque terceras partes no estén forzadas a copiar el fuente junto con el código objeto.

5. No puede copiar, modificar, sublicenciar o distribuir el Programa excepto como prevé expresamente esta Licencia. Cualquier intento de copiar, modificar sublicenciar o distribuir el Programa de otra forma es inválida, y hará que cesen automáticamente los derechos que te proporciona esta Licencia. En cualquier caso, las partes que hayan recibido copias o derechos de usted bajo esta Licencia no cesarán en sus derechos mientras esas partes continúen cumpliéndola.
6. No está obligado a aceptar esta licencia, ya que no la ha firmado. Sin embargo, no hay hada más que le proporcione permiso para modificar o distribuir el Programa o sus trabajos derivados. Estas acciones están prohibidas por la ley si no acepta esta Licencia. Por lo tanto, si modifica o distribuye el Programa (o cualquier trabajo basado en el Programa), está indicando que acepta esta Licencia para poder hacerlo, y todos sus términos y condiciones para copiar, distribuir o modificar el Programa o trabajos basados en él.
7. Cada vez que redistribuya el Programa (o cualquier trabajo basado en el Programa), el receptor recibe automáticamente una licencia del licenciatario original para copiar, distribuir o modificar el Programa, de forma sujeta a estos términos y condiciones. No puede imponer al receptor ninguna restricción más sobre el ejercicio de los derechos aquí garantizados. No es usted responsable de hacer cumplir esta licencia por terceras partes.
8. Si como consecuencia de una resolución judicial o de una alegación de infracción de patente o por cualquier otra razón (no limitada a asuntos relacionados con patentes) se le imponen condiciones (ya sea por mandato judicial, por acuerdo o por cualquier otra causa) que contradigan las condiciones de esta Licencia, ello no le exime de cumplir las condiciones de

esta Licencia. Si no puede realizar distribuciones de forma que se satisfagan simultáneamente sus obligaciones bajo esta licencia y cualquier otra obligación pertinente entonces, como consecuencia, no puede distribuir el Programa de ninguna forma. Por ejemplo, si una patente no permite la redistribución libre de derechos de autor del Programa por parte de todos aquellos que reciban copias directa o indirectamente a través de usted, entonces la única forma en que podría satisfacer tanto esa condición como esta Licencia sería evitar completamente la distribución del Programa.

Si cualquier porción de este apartado se considera inválida o imposible de cumplir bajo cualquier circunstancia particular ha de cumplirse el resto y la sección por entero ha de cumplirse en cualquier otra circunstancia.

No es el propósito de este apartado inducirle a infringir ninguna reivindicación de patente ni de ningún otro derecho de propiedad o impugnar la validez de ninguna de dichas reivindicaciones. Este apartado tiene el único propósito de proteger la integridad del sistema de distribución de software libre, que se realiza mediante prácticas de licencia pública. Mucha gente ha hecho contribuciones generosas a la gran variedad de software distribuido mediante ese sistema con la confianza de que el sistema se aplicará consistentemente. Será el autor/donante quien decida si quiere distribuir software mediante cualquier otro sistema y una licencia no puede imponer esa elección.

Este apartado pretende dejar completamente claro lo que se cree que es una consecuencia del resto de esta Licencia.

9. Si la distribución y/o uso de el Programa está restringida en ciertos países, bien por patentes o por interfaces bajo copyright, el tenedor del copyright que coloca este Programa bajo esta Licencia puede añadir una limitación explícita de distribución geográfica excluyendo esos países, de forma que la distribución se permita sólo en o entre los países no excluidos de esta manera. En ese caso, esta Licencia incorporará la limitación como si estuviese escrita en el cuerpo de esta Licencia.

10. La Free Software Foundation puede publicar versiones revisadas y/o nuevas de la Licencia Pública General de tiempo en tiempo. Dichas nuevas versiones serán similares en espíritu a la presente versión, pero pueden ser diferentes en detalles para considerar nuevos problemas o situaciones.

    Cada versión recibe un número de versión que la distingue de otras. Si el Programa especifica un número de versión de esta Licencia que se refiere a ella y a «cualquier versión posterior», tienes la opción de seguir los términos y condiciones, bien de esa versión, bien de cualquier versión posterior publicada por la Free Software Foundation. Si el Programa no especifica un número de versión de esta Licencia, puedes escoger cualquier versión publicada por la Free Software Foundation.

11. Si quiere incorporar partes del Programa en otros programas libres cuyas condiciones de distribución son diferentes, escribe al autor para pedirle permiso. Si el software tiene copyright de la Free Software Foundation, escribe a la Free Software Foundation: algunas veces hacemos excepciones en estos casos. Nuestra decisión estará guiada por el doble objetivo de de preservar la libertad de todos los derivados de nuestro software libre y promover el que se comparta y reutilice el software en general.

AUSENCIA DE GARANTÍA

12. Como el programa se licencia libre de cargas, no se ofrece ninguna garantía sobre el programa, en todas las extensiones permitidas por la legislación aplicable. Excepto cuando se indique de otra forma por escrito, los tenedores del copyright y/u otras partes proporcionan el programa «tal cual», sin garantía de ninguna clase, bien expresa o implícita, con inclusión, pero sin limitación a las garantías mercantiles implícitas o a la conveniencia para un propósito particular. Cualquier riesgo referente a la calidad y prestaciones del programa es asumido por usted. Si se probase que el Programa es defectuoso, asume el coste de cualquier servicio, reparación o corrección.

13. En ningún caso, salvo que lo requiera la legislación aplicable o haya sido acordado por escrito, ningún tenedor del copyright ni ninguna otra parte que modifique y/o redistribuya el Programa según se permite en esta Licencia será responsable ante usted por daños, incluyendo cualquier daño general, especial, incidental o resultante producido por el uso o la imposibilidad de uso del Programa (con inclusión, pero sin limitación a la pérdida de datos o a la generación incorrecta de datos o a pérdidas sufridas por usted o por terceras partes o a un fallo del Programa al funcionar en combinación con cualquier otro programa), incluso si dicho tenedor u otra parte ha sido advertido de la posibilidad de dichos daños.

FIN DE TÉRMINOS Y CONDICIONES

[1]Tomado de las leyes para el software de distribución libre. www.gnu.org

CAPÍTULO III. ADMINISTRACIÓN DE REDES

3.1 EN QUE CONSISTE LA ADMINISTRACIÓN DE RED.

Es de gran importancia visualizar lo que es una red. Una red es un conjunto de dispositivos que interactúan entre sí para proporcionar comunicación. Cuando un administrador de red analiza una red, su responsabilidad es verla como un todo y no como partes individuales. En otras palabras, cada dispositivo en una red afecta a otros dispositivos y a la red como un todo.

Los recursos usados en redes de computadoras tienen que ser continuamente "vigilados" y cualquier comportamiento desfavorable lleva al deterioro del funcionamiento de un recurso, recursos o la red en su totalidad y por lo tanto debe ser corregido. Esto es más una acción preventiva que una reactiva. Los recursos tienen que ser controlados. Esto significa que se debe permitir controlar cómo los recursos se comportan a fin de que su función se realice apropiadamente. Cuando los recursos tienen que ser monitoreados y controlados, existe un factor necesario: coordinación. Si no hay coordinación, la situación es del tipo de contienda general y surge el caos.

Existen dos modelos de administración de redes, dependiendo del ambiente computacional: una LAN (Red de Área Local) es un típico ambiente distribuido, la administración de un ambiente de LAN puede ser hecho con una administración peer-to-peer (igual a igual), también conocida como administración de redes distribuida, en el cual gran parte de la administración corre por cuenta del usuario.

El otro modelo es el administración jerárquica, o centralizada. En este modelo a administración es realizada por un solo punto, conocido como administrador. Pueden haber casos en donde exista un administrador que controle el

funcionamiento de varios administradores y se lo conoce como administrador del administrador (MOM, Manager of Manager).

Los objetivos de la Administración de Redes, son los siguientes:

- **Alta disponibilidad de la red:** proveyendo eficiencia operacional, reduciendo los "downtime" de la red y del sistema y proveyendo tiempos de respuesta aceptables. Los problemas de la red deben ser rápidamente detectados y corregidos.
- **Reducción de costos operacionales de red:** este es uno de los motivos primarios detrás de la administración de redes. Como las tecnologías cambian rápidamente, es deseable la administración de sistemas heterogéneos y múltiples protocolos.
- **Reducción de cuellos de botella en la red:** dependiendo de cada caso en particular, puede ser deseable un monitor centralizado para administración y en otros casos esta tarea debe ser distribuida.
- **Incrementar flexibilidad de operación e Integración:** las tecnologías de redes están cambiando a velocidades mayores que los cambios de requerimientos y necesidades. Cuando se usa una nueva aplicación, los protocolos usados en redes deberán cambiar también. Debe ser posible absorber nueva tecnología con un costo mínimo y adicionar nuevo equipamiento sin mucha dificultad. Además, debe permitir lograr una fácil migración de un software de administración de redes a otra versión.
- **Alta eficiencia:** se debe incrementar la eficiencia en detrimento de otros objetivos de la administración pero dependerá de otros factores tales como utilización, costo operacional, costo de migración y flexibilidad.
- **Facilidad de uso:** las interfaces de usuario son críticas para el éxito de un producto. El uso de aplicaciones de administración de redes no debe incrementar la curva de aprendizaje.
- **Seguridad:** existen casos en donde la seguridad es un aspecto a tener en cuenta tales como información de contaduría, información gerencial, etc.

Responsabilidades de un administrador de red.

La tarea de administración de red esta compuesta por varias responsabilidades, una de las cuales es el **estudio de los costos**. Esto quiere decir que el encargado debe considerar los siguientes elementos: costo del diseño e implementación, costo del mantenimiento, actualización y monitoreo de la red.

Entre otros costos que un administrador de red debe tomar en cuenta se encuentran: la expansión de la red con el tiempo, la capacitación del personal técnico y los usuarios, reparaciones y reemplazo de dispositivos y el software a utilizar. El administrador de red debe estar capacitado para analizar las tendencias de crecimiento de la empresa para de esta forma proyectar el costo del crecimiento en la red. Un administrador de red debe examinar el nuevo software y hardware para determinar si la empresa necesitará implementarlo y cuándo, así como las necesidades de capacitación del personal para brindar soporte a estas nuevas tecnologías.

Otra de las principales responsabilidades de un administrador de redes es la de **documentar** en caso de errores, una efectiva administración va acompañada de una completa documentación de los errores. Dicha documentación se utiliza para reunir la información necesaria para identificar un problema en la red, y también ofrece una manera para hacer un seguimiento del progreso y eventual solución del problema. Entre los aspectos por lo que se justifica la documentación de los errores se encuentran: la contratación de nuevo personal, adquisición de nuevos dispositivos y el brindar capacitación adicional y además, brinda soluciones para problemas recurrentes que ya han sido resueltos anteriormente.

Debe recalcarse que un administrador de red debe tener a la mano:

- Registro histórico de fallas y soluciones: llevar un historial documentado sobre los errores que se han presentado en los equipos y las soluciones que se

implementaron, esto permitirá reducir el tiempo de recuperación, además de prever situaciones de riesgo.

- Bitácora de respaldos: registro documental sobre el estado de los respaldos, su tipo, equipo al que pertenecen y ubicación.
- Bitácora de control de cambios, de parches aplicados al sistema operativo y a los programas.
- Directorio telefónico: datos sobre los domicilios y teléfonos de proveedores, responsables técnicos, programadores y usuarios de las aplicaciones.
- Acuerdos sobre el nivel de servicio comprometido de las aplicaciones.
- Diagramas eléctricos y de conexiones de red.
- Discos y cintas con el software original de los sistemas operativos y aplicaciones.
- Manuales de operación, encendido y apagado de los equipos de cómputo y telecomunicación.

Diseñar un plan de contingencia no es sencillo; sin embargo, un documento de este tipo permitirá que una situación de desastre no se convierta en una pesadilla.

La administración puede significar diferentes cosas para diferentes personas. En algunos casos involucra a un administrador solitario, que monitorea la actividad de la red con un analizador de protocolos obsoleto o que no brinda las capacidades necesarias para efectuar dicha tarea. En otros casos, la administración de la red implica el uso de un producto de alta calidad con capacidades para el reconocimiento de dispositivos de red, generación de gráficos en tiempo real de la topología de la red, analizador del trafico de paquetes en la red, monitoreo de servicios de la red, notificación de errores, entre otras características. En general, la administración de red es una tarea en la que se emplea una variedad de herramientas, aplicaciones y

dispositivos para asistir en sus tareas a las personas encargadas de la administración y el monitoreo de las redes.

La administración de redes abarca un amplio número de situaciones. En general, se suelen tratar con muchos datos estadísticos e información sobre el estado de distintas partes de la red, y se realizan las acciones necesarias para ocuparse de fallos y otros cambios. La técnica más primitiva para la monitorización de una red es hacer "pinging" a los hosts críticos; el "pinging" se basa en un mensaje de "echo" (eco), que es un tipo de mensaje o que produce una réplica inmediata cuando llega al destino. La mayoría de las implementaciones TCP/IP incluyen un programa (generalmente, llamado "ping") que envía un echo a un host en concreto. Si se recibe una réplica, se concluye que el host se encuentra activo, y que la red que los conecta funciona; en caso contrario, se concluye que hay algún error. Mediante "pinging" a un razonable número de ciertos hosts, se puede normalmente conocer qué ocurre en la red. Si los ping a todos los hosts de una red no dan respuesta, es lógico concluir que la conexión a dicha red, o la propia red, no funciona. Si sólo uno de los hosts no da respuesta, pero los demás de la misma red responden, es razonable concluir que dicho host no funciona.

Además del comando "ping" , existen otras herramientas de software que están disponibles para que el administrador de red pueda resolver los problemas de conectividad de la red.

Las herramientas del sistema operativo pueden ayudar en el diagnóstico de fallas de las redes de área local. Entre estos comandos se incluyen: Tracert (Taceroute), Telnet, Netstat, ARP, e Ipconfig (WinIPcfg). La descripción de cada uno de estos comandos será desarrollado ampliamente en el capitulo VI.

Ésta es una forma muy ineficiente y primitiva de monitorear la red. Otro aspecto de este tipo de monitoreo es que sólo determina si en algún lugar entre la estación de control y el dispositivo objetivo hay una ruptura de las comunicaciones.

El problema puede ser un router, switch o segmento de red defectuoso, o que el host esté desactivado. La prueba de ping sólo indica que la conexión está desactivada, pero no indica dónde lo está.

El monitoreo del tráfico es un método mucho más sofisticado de monitoreo de la red. Analiza el tráfico real de paquetes en la red y genera informes basados en el tráfico de la red. Estos programas no sólo detectan el equipo defectuoso sino que también determinan si un componente se encuentra sobrecargado o mal configurado. Esto se puede resolver mediante el uso de agentes en los segmentos remotos de red. Equipos como los switches y los routers tienen la capacidad de generar y transmitir estadísticas de tráfico como parte de su sistema operativo.

Los datos se reúnen y organizan en una ubicación central para que sean útiles para el administrador de red. Esto es posible a través del protocolo de administración de red simple (SNMP).

El protocolo de administración de red simple (SNMP) es un protocolo de la capa de aplicación del modelo OSI, que facilita el intercambio de información de administración entre dispositivos de red. Este protocolo es parte de la suite TCP/IP.

SNMP permite a los administradores de la red administrar el desempeño de esta, identificar y resolver problemas y la planeación del crecimiento de la red en el futuro. SNMP será desarrollado ampliamente en el capitulo V.

3.2 MODELO DE ADMINISTRACIÓN DE LA RED DE LA ISO.

La Organización Internacional de Estandarización o ISO por sus siglas en inglés, divide la administración de la red en cinco áreas conceptuales, las cuales se definen dentro del Modelo de Referencia para Interconexión de Sistemas Abiertos Open Systems Interconnection Reference Model, OSI-RM). Estas cinco áreas son descritas a continuación:

Administración del Desempeño:

El objetivo de la administración del desempeño es mantener una eficiencia y un desempeño máximo de las variables de la red, que incluye la recopilación de estadísticas y el mantenimiento de registros. Las variables de desempeño que podrían ser incluidas son el rendimiento de la red, tiempos de respuesta al usuario y la utilización de la red.

La administración del desempeño involucra tres pasos principales. El primero, el desempeño de los datos son recopilados en variables de interés para los administradores de red. Segundo, los datos almacenados son analizados para determinar los niveles normales de desempeño óptimos (baseline). Finalmente, establecer los limites máximos de desempeño para cada una de las variables de forma tal, que cuando se sobrepasen estos limites se indica que existe un problema en la red, el cual requiere ser atendido.

Las entidades encargadas de la administración, continuamente se encuentran monitoreando las variables de desempeño. Cuando un limite es excedido, una alerta es generada y es enviada al sistema de administración de red, esto constituye el establecimiento de un sistema reactivo. Sin embargo, la administración del desempeño también permite métodos proactivos: Por ejemplo, un simulador de red puede ser usado para proyectar el crecimiento futuro de la red y como este crecimiento afectaría las medidas de desempeño.

Administración de la Configuración:

El objetivo de la administración de la configuración es monitorear los dispositivos de la red y la información de la configuración del sistema. La información incluye elementos de hardware y software los cuales pueden ser rastreados y administrados.

Cada dispositivo dentro de la red posee una variedad de información asociada a él. Una estación de trabajo, por ejemplo, puede poseer la siguiente información:

- Sistema Operativo, Versión 3.2
- Interface Ethernet, Versión 5.4
- Protocolo TCP/IP, Versión 2.0
- Software NetWare, Versión 4.1
- Controlador de comunicación serial, Versión 1.1
- Software SNMP, Versión 3.1

Los subsistemas de administración de la configuración almacenan esta información en una base de datos para un facial acceso. Cuando ocurre un problema, esta base de datos puede ser consultada para ayudar a resolver el problema.

Administración de la Contabilidad:

El objetivo de la administración de la contabilidad es medir la utilización de la red, de tal manera que el uso individual o grupal de la red pueda ser regulado apropiadamente. El control minimiza los problemas de la red (debido a que los recursos de la red pueden ser distribuidos basado en la capacidad de los recursos) y además maximiza la imparcialidad del acceso a la red para todos los usuarios.

Administración de fallas:

La meta de la administración de fallas es detectar, almacenar en registro, notificar a usuarios y en medida de lo posible reparar automáticamente los problemas que se presentan en la red para que ésta desempeñe su labor efectivamente. Debido a que las fallas de red pueden provocar que la red quede fuera de servicio por un tiempo indeterminado o que la red trabaje a un nivel por debajo de su desempeño óptimo, la administración de fallas es quizá el elemento de mayor implementación del modelo ISO para administración de redes.

La administración de fallas detecta los síntomas del problema, luego lo asila y posteriormente corrige dicho problema. Finalmente la detección y solución del problema es almacenado en un registro.

Administración de la Seguridad:

El objetivo de la administración de la seguridad es controlar el acceso a los recursos compartidos de la red de acuerdo a políticas locales de tal manera que la red no sea saboteada (sea o no intencionalmente) y que la información confidencial sea protegida contra el acceso no autorizado. Un sistema de administración de seguridad , por ejemplo, puede monitorear el acceso de los usuarios sobre los recursos de red y puede rechazar el acceso a estos cuando tratan de ingresar con códigos de acceso inapropiados.

Los sistemas de administración de la seguridad dividen los recursos disponibles en la red en áreas autorizadas y no autorizadas. Para algunos usuarios, el acceso a cualquier recurso de red es inapropiado, en la mayoría de los casos debido a que estos usuarios son ajenos a la compañía. Para otros usuarios de red (internos), el acceso a la información que es generada desde un departamento especifico puede también ser inaccesible. El acceso a los archivos del Departamento de Recursos Humanos, por ejemplo, no debe ser accesado para los usuarios que no tienen ninguna relación con dicho departamento.

Los sistemas de administración de seguridad desarrollan varias funciones. Ellos identifican los recursos de red y tienen la capacidad de registrar los intentos por parte de usuarios no autorizados sobre diversos recursos.

3.3 SEGURIDAD DE RED

Cuando se habla de seguridad de red se deben de tomar en cuenta dos factores de gran importancia: Proteger la red contra el acceso no autorizado y la habilidad para la recuperación de datos ante eventos catastróficos.

Protección de red contra accesos no autorizados.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a cualquier persona ajena a la organización.

Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no autorizado de usuarios a los recursos propios de la red privada y protegerse contra la exportación privada de información. Todavía, aun si una organización no esta conectada a Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger de sobremanera la información confidencial.

Estas políticas incluyen lo que está permitido y lo que no está permitido en la red. También deben incluir cuáles son las consecuencias por violar las políticas para el usuario. Otros aspectos de las políticas para el usuario incluyen cuál es la longitud mínima que deben tener los identificadores de usuario y la contraseña y las normas para el contenido de las contraseñas.

Para proteger el acceso a los recursos de red, a cada cuenta de usuario debe asociársele una contraseña. Determinar quien será el que tendrá el control sobre la contraseña. Un administrador puede decidir asignar el mismo las contraseñas a los usuarios y prevenir que los usuarios lo cambien o también puede preferir que sea el usuario el que establezca su propia contraseña. Es recomendable que sea el usuario el que controle su contraseña.

El administrador de la red tiene como objetivo crear una red lo más funcional y segura que sea posible para la empresa.

Recuperación de datos.

La recuperación de datos, que constituye la segunda parte de la seguridad de red, tiene como objetivo proteger los datos ante pérdidas accidentales de la información. Existen varios métodos para evitar la pérdida de datos. Tres de los métodos más comunes para la protección y recuperación de datos son la copia de seguridad en cinta, la técnica de configuración de discos con tolerancia a fallas y el uso de sistemas de alimentación ininterrumpida (UPS) para evitar que el equipo deje de funcionar cuando se producen interrupciones de la energía eléctrica. A continuación se describen los primeros dos métodos de forma general.

Copias de Seguridad en Cinta.

La copia de seguridad en cinta es el proceso de duplicación de todos los datos almacenados en una cinta magnética. La capacidad de la unidad de cinta será un factor determinante en el tipo de copia de seguridad que se realizará en la red. Existen cinco tipos de copias de seguridad que se pueden realizar:

- Copia de seguridad normal
- Copia de seguridad incremental
- Copia de seguridad diferencial
- Copia de seguridad copia
- Copia de seguridad diaria

Configuración de discos con tolerancia a fallas.

Otro método para la protección de datos es a través de dispositivos de almacenamiento con tolerancia a fallas o comúnmente conocido como RAID. Este tipo de conjunto redundante de dispositivos es categorizado por los niveles 0-5 de RAID (Matrices Redundantes de Discos Económicos).

La idea básica del RAID es combinar varios discos pequeños y económicos en una matriz que proporcione un rendimiento mayor que el de un disco grande y

costoso. Además, la computadora ve esta matriz de discos como si fuese una sola unidad lógica de almacenamiento, o un solo disco.

Uno de los conceptos fundamentales del RAID es el «entrelazado», una forma de combinar el espacio de varios discos en un sólo disco lógico para el sistema operativo. El entrelazado se efectúa partiendo el espacio total de cada disco en pequeños «bloques». Estos bloques pueden tener tamaños tan pequeños como 4k, o tan grandes como varios mega-bytes (aunque las pruebas demuestran que 32k o 64k suele ser un valor óptimo). Los bloques se entrelazan entonces entre los discos que forman el RAID para crear una banda. Por ejemplo, los bloques 1 de cada disco duro pueden formar una banda, los segundos otra, etc... De esta forma, el tamaño total del disco lógico es la suma de los tamaños de todos los discos del RAID.

Hay dos métodos posibles para hacer un RAID: por hardware o por software.

RAID por hardware

Los sistemas de RAID basados en soluciones hardware manejan el subsistema RAID independientemente del sistema operativo, al que le presentan un solo disco por matriz.

Un ejemplo de RAID por hardware podría ser uno que se conectase a una controladora SCSI y presentase las matrices de discos como un solo disco SCSI. Una caja externa contiene el controlador que proporciona toda la «inteligencia» de manejo del RAID que se encuentra en el subsistema externo de disco. El subsistema completo se conecta al ordenador principal a través de un controlador SCSI que es visto por el ordenador como un solo disco.

RAID por software

Los RAID por software implementan los diferentes niveles de RAID en el código de dispositivo de bloque del núcleo. También proporcionan la solución más barata: No solamente porque prescinden de costosas controladoras de disco o chasis de intercambio en caliente, además los RAID por software funcionan tanto con

discos IDE más baratos como con SCSI. Con los rápidos procesadores actuales, un RAID por software ofrece un rendimiento excelente comparado con uno por hardware.

3.4 DESEMPEÑO DE LA RED

El desempeño de una red es una medición de la rápidez y la confiabilidad de la misma. La red parece volverse cada ves más lenta. Algunas veces esto puede pasar durante un periodo corto de tiempo y en ocasiones la degradación ocurre por días o semanas. La primera pregunta a responder es : ¿desempeñó la red alguna vez su trabajo de una manera óptima? Si no conoce la respuesta, entonces el administrador debe empezar por revisar las fases de planeación e instalación de la red y responderse las siguientes preguntas:

- ¿Si la red se desempeño de una manera efectiva alguna vez, cuanto ha cambiado desde entonces?
- ¿Se han adicionado nuevas aplicaciones o dispositivos?
- ¿Está algún usuario ejecutando juegos que corren a través de la red?
- ¿Ha crecido el número de usuarios en la red?

La respuesta a estas preguntas lleva a la conclusión de que para saber si la red actualmente esta funcionando de una manera defectuosa, se debe contar con una medición con la que se pueda comparar el desempeño en diferentes espacios de tiempo, es de suponerse que la primera medición debe de realizarse cuando la red acababa de montarse, esta medición es conocida como *nivel básico.*

Para establecer un nivel básico, se puede utilizar una herramienta para monitoreo de red, este tipo de herramientas registran varios tipos de datos del desempeño de la red, incluyendo el porcentaje de uso de la red y el tráfico de broadcast. Al establecer una medición del nivel básico cuando el sistema de red se ubica en los niveles de desempeño normal óptimos, el administrador de red cuenta con un valor de comparación que se puede utilizar para determinar el buen estado de a red.

3.5 ADMINISTRACION DEL SERVIDOR.

En general, existen dos modelos de redes que los administradores deben conocer. Estos dos modelos son las redes peer to peer (de igual a igual) y cliente-servidor.

Una *red de peer to peer* permite conectar un grupo de computadoras a fin de que compartan recursos, sin tener que utilizar a uno de los equipos como servidor de archivos (File Server). Al eliminar el servidor, se reduce el monto de la inversión en infraestructura. Asimismo, el mantenimiento administrativo no resulta demasiado caro, ya que se trata de un sistema que posee un grado de complejidad menor. Ante la ausencia de un servidor que proporcione los servicios y recursos, las computadoras que conforman la red son las que permiten que otras máquinas utilicen sus archivos o periféricos.

¿Qué recursos pueden compartirse en una plataforma peer-to-peer?

Una impresora, espacio en disco, un archivo o una unidad de CD-ROM. Windows 95/98, el ambiente operativo que está instalado en prácticamente todas de las PC del mundo, ofrece la funcionalidad necesaria para instrumentar una red peer-to-peer. Por lo tanto, no hace falta gastar dinero en un sistema operativo de red. La instalación de una red así se limita a conectar todos los equipos, otorgarles una identificación única (dentro de la plataforma de conectividad) y establecer privilegios y accesos a los recursos.

En una *red cliente-servidor*, cuando el servidor no funciona, los usuarios no tienen acceso a los recursos que el dispositivo controlador proporciona. Sin embargo, a cambio de esta "desventaja", un servidor permite que más usuarios consigan acceso simultáneo a una mayor cantidad de archivos. Además, el uso masivo de recursos (documentos o impresoras) no reduce el desempeño de los equipos, como sucede con las computadoras que están en una red peer-to-peer.

Una estructura basada en estaciones de trabajo sin servidor resulta más barata y fácil de mantener. Sin embargo, cuando el número de nodos crece, la complejidad de su administración aumenta. En tal caso, y en términos de eficiencia y desempeño, se justifica la utilización de un servidor.

Para gestionar las cuentas de usuario, los privilegios sobre los recursos y los servicios, así como el sistema de respaldo, se requiere de la figura de un administrador de la red.

Un servidor de archivos ofrece otras ventajas: un sistema más eficiente para la seguridad de la información, el control de privilegios y de los recursos que se comparten, orden en el acceso a recursos basados en un servidor (como son Base de datos y correo electrónico).

El modelo más apropiado para una empresa depende de la necesidad de acceso a servicios de correo electrónico, bases de datos, el tipo de aplicaciones y el tamaño de la red en número de nodos, entre otros aspectos.

3.6 RESOLUCIÓN DE PROBLEMAS DE RED.

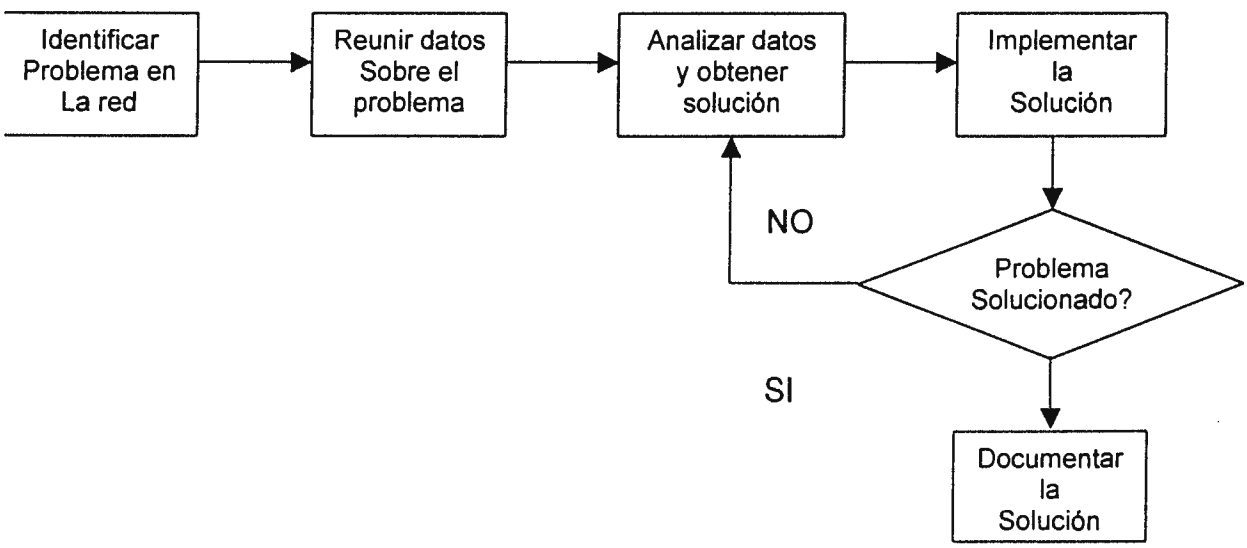
Definitivamente un administrador de red no está exento de problemas, aunque la red se monitoree constantemente, el equipo parezca el mejor y los usuarios muy capacitados, las cosas pueden no siempre salir bien. La capacidad de un buen administrador se demuestra a través de su habilidad para analizar, diagnosticar las fallas y corregir los problemas de la red que pueden hacer que la actividad de toda una compañía se paralice. Existen algunas técnicas las cuales facilitan al administrador de red la tarea de diagnosticar y corregir fallas. Una de estas técnicas es la descrita en la sección de responsabilidades del administrador de red: *la documentación de errores*, ésta puede representar la mejor manera de diagnosticar un problema. La documentación de errores describe las soluciones que ya se han probado y cual fue el efecto que causó sobre dicho problema. Esto es de gran

importancia para el personal técnico encargado ya que provee una guía en la cual puede reducirse el tiempo de solución de problemas, además, la documentación de errores puede representar un punto de consulta para problemas similares.

Es de gran utilidad para el administrador de red seguir un esquema sistemático que le ayude a la resolución de problemas, para ello se recomienda seguir los siguientes pasos:

1. Identificar el problema de la red.
2. Reunir los datos necesarios acerca del problema.
3. Analizar los datos para obtener una solución posible para el problema.
4. Implementar la solución obtenida del paso anterior en la red para tratar de corregir la falla.
5. Si no se solucionó el problema, buscar otra solución.
6. Retornar al paso 3.
7. Documentar la solución implementada.

Gráficamente, podemos representar el esquema de solución de la siguiente manera:



CAPÍTULO IV. MONITOREO DE RED.

4.1 MONITOREO Y CONTROL

Las redes y los sistemas de procesamiento distribuido tienen una importancia crítica en los sistemas de gobierno, empresariales, medicina, educación y otras organizaciones. Las organizaciones, mientras mas grandes son tienden a tener sistemas más complejos soportando más aplicaciones y más usuarios. A medida que estas redes crecen en escala, dos factores comienzan a evidenciarse:

- La red, sus recursos asociados y las aplicaciones distribuidas comienzan a volverse indispensables en la organización.
- Muchos dispositivos pueden fallar, inutilizando la red o una porción de ella, o la carga sobre la red puede ir degradando el desempeño hasta niveles inaceptables.

En respuesta a estas necesidades surgen aplicaciones estándar que permiten administrar las redes, cubriendo servicios, protocolos y bases de información de gestión.

4.2 ¿POR QUÉ ES NECESARIO MONITOREAR UNA RED?

Como se discutió en el capítulo de administración de redes, existen varias razones por las que hay que "vigilar" una red, pero los dos motivos principales son: la predicción de los cambios para el crecimiento en el futuro y la detección de sucesos no esperados en el estado de la red, como por ejemplo: fallas de dispositivos de red, inaccesibilidad de servicios (Correo Electrónico, Internet, bases de datos, etc). Si no se posee un plan de monitoreo de red, la persona encargada de administrarla sólo es capaz de reaccionar a los problemas a medida que éstos se den, en lugar de prevenirlos.

Uno de los métodos básicos usados por los administradores de una red se da diariamente en el momento en que los usuarios comienzan a conectarse a dicha red; en este momento se verifica si las conexiones funcionan correctamente; de lo contrario, será necesario contactar al administrador para que éste se encargue de resolver el problema.

Existen programas de operación sencilla que permiten que el administrador ingrese una grupo de direcciones IP asignadas a computadores específicos, se ejecuta el comando "ping" a estas direcciones de forma periódica, si se detecta un problema de conexión, el programa advierte al administrador que existe un problema de conexión. Una desventaja de este tipo de monitoreo es que el comando "ping" solamente me indica que determinado host tiene problemas de conectividad a la red, sin embargo no monitorea otro tipo de aplicaciones o servicios que pudieran estarse ejecutando en dicho host como por ejemplo Servicios de Correo Electrónico, WEB, FTP, DNS, Telnet, etc.

En conclusión el uso de "ping" es una forma ineficiente de monitoreo de red, sin embargo es preferible realizar éste tipo de pruebas en lugar de no hacer absolutamente nada.

El monitoreo del tráfico es un método más eficiente de monitoreo de la red. Analiza el tráfico de paquetes en la red y crea informes basados en el tráfico generado en la misma. Los programas como: HP Open View, Tivoli, What´s Up y el Network Analyzer de Fluke son ejemplos de este tipo de programas. Este tipo de programas de monitoreo de red no sólo detectan el equipo defectuoso; sino que también determinan si un componente se encuentra sobrecargado o mal configurado.

4.3 DEFINICIÓN DE MONITOR DE RED.

Un Monitor de Red es un instrumento que entrega datos de algún tipo (numérico, visual, auditivo) de un proceso o fenómeno. De aquí que el termino puede ser utilizado para monitores de computadoras o de vigilancia, hasta monitores de incendio y de intrusos (alarmas). El último caso, además de ser un monitor normal, entrega un dato específico cuando alguna variable ha sobrepasado algún umbral o situación prefijada.

Un Monitor de Redes de Computadores es un instrumento que entrega datos acerca de la red en la cual esta conectado, para extraer de ella información de tipo estadístico, evolución de parámetros de funcionamiento, histogramas, tráfico por cada enlace, estado de los servicios, etc. Esta información es mostrada en forma de gráficos que hacen más fácil su interpretación.

Las funciones básicas que debe tener un monitor de red son:

- Poder extraer estadísticas globales de tráfico, número de errores, bytes transmitidos y recibidos, etc.
- Poder extraer estadísticas para cada terminal de la red y los errores que provoca.
- Proporcionar estadísticas en tiempo real y estadísticas históricas (carga máxima y medida por intervalos de tiempo).
- Determinar qué ancho de banda se está utilizando en cada momento.
- Determinar protocolos innecesarios instalados en estaciones de trabajo, impresoras y servidores.
- Determinar el porcentaje de uso de los diferentes protocolos que se utilizan en la red.
- Proveer de una interfaz basada en web para el monitoreo.
- Permitir la notificación de alarmas a contactos.
- Proporcionar reportes consolidados dinámicamente.

- Mostrar la carga de tráfico en enlaces WAN

4.4 CLASIFICACIÓN DE MONITORES DE RED.

Los monitores de red se pueden clasificar según los criterios de Objetivo, Reporte, Intrusividad, Operación y Protocolos que miden.

Objetivo

- **Monitor de Estados (variables).**

El objetivo es el de "avisar" situaciones de emergencia como "caídas" de equipos o el sobrepaso de un umbral de alguna variable fijada por el administrador. Por ejemplo: la NO-RESPUESTA de un enrutador o la superación del umbral de 40% en el porcentaje de colisiones. Para ello generalmente se ocupa el estándar SNMP (Simple Network Management Protocol) que como su nombre lo indica esta orientado a monitorear y configurar el equipamiento físico de una red(Puentes, Switches, Enrutadores, concentradores y estaciones de trabajo). Cabe mencionar que el SNMP no solo sirve para monitorear y/o configurar variables de los equipamientos de la red física; sino también para mostrar el tráfico histórico en forma gráfica acerca de lo que se ha "traficado" por los equipos que forman la red.

- **Monitor de Tráfico.**

El objetivo es registrar el tráfico de las redes, ya sea con fines estadísticos o de detección de congestión. Este tipo de monitor también puede tener "alarmas" y por ende, enviar una señal al administrador cuando una variable monitoreada halla excedido un umbral prefijado (considerado como alarmante).

Reporte

- **Histórico.**

Éste tipo de monitor entrega informes o resúmenes de la actividad histórica de la red, ya sea por: hora, día, semana o mes. La actividad mencionada puede corresponder a tráfico, alarmas ocurridas, etc. El reporte generalmente consiste en archivos de tipo texto, dado que éste puede ser ingresado a otro programa para transformarlo a gráficos. Los últimos monitores de éste tipo entregan sus reportes en formato HTML (WWW) y generan automáticamente los gráficos usando programas propios o del sistema. Un monitor histórico debe entregar la mayor cantidad de información posible, ya sea en forma de texto o de gráfico, ya que la información entregada puede ser ingresada en una base de datos.

- **Tiempo real.**

Un monitor de este tipo entrega datos de ocurrencia reciente, desde 1 segundo hasta 10 minutos, con el objetivo de detectar y corregir los problemas cuanto antes. En algunos casos, como en las "alarmas" de umbrales, las variables son de tiempo corto y por lo tanto son inmediatamente avisadas. En otros casos, si la variable tiene un tiempo de "ejecución" como la transmisión de un paquete, se debe esperar la transmisión completa antes de poder tomar acciones. Por estas razones, un monitor de tiempo real no solo abarca los monitores "instantáneos"; sino también a los que deben monitorear variables que requieren de un tiempo determinado de ejecución.

Intrusividad

- **Intrusivo.**

Es aquel monitor que interviene en el proceso o fenómeno a monitorear, vale decir, actúa como agente activo. En este caso, el monitor afecta la medición, haciéndola no confiable o no representativa del proceso. Por ejemplo un monitor de tráfico local se considera intrusivo si ocupa la red para hacer mediciones. Sin embargo, si un monitor ocupa la red para obtener datos, no significa que su medición sea intrusiva, ya que esto depende del proceso que desee medir. Por ejemplo: si el monitor debe medir el tráfico que es cursado por un enrutador y consulta a éste último por esa información (usando la red local), su medición no es intrusiva.

- **No intrusivo.**

Un monitor es no intrusivo si no interviene en el proceso o fenómeno a monitorear, vale decir, si actúa como agente pasivo. Por ejemplo: un monitor de tráfico local no es intrusivo si no utiliza la red para medir su tráfico local.

Operación

Esta clasificación se refiere a la operación del monitor, en cuanto a dónde despliega sus datos y dónde es configurado por un administrador.

- **Local.**

Si la operación del monitor es local, entonces significa que muestra los datos en el mismo lugar de donde los obtiene. En el caso de una alarma de una casa, la alarma es configurada por el dueño en la casa misma y la alarma suena en la

misma en caso de la entrada de un intruso. En el caso de un monitor de tráfico, esto significa que los datos se despliegan en el mismo computador que obtiene los datos.

- **Remota**

La operación de este tipo de monitores se realiza en forma remota. En el caso de la alarma de casas, la operación se realiza desde una empresa dedicada, en caso de la entrada de un intruso, la alarma avisa en las dependencias de la empresa y no en la casa en cuestión. En el caso de un monitor de tráfico, esto significa que los datos son desplegados en otro computador distinto al que obtiene los datos. Lo anterior requiere ocupar la red para comunicar estos 2 computadores, por lo que dependiendo del tipo de medición, será también clasificado como intrusivo o no intrusivo.

Protocolos

Esta clasificación permite destacar los tipos de protocolos de redes con que el monitor puede trabajar.
La clasificación contempla mencionar la compatibilidad con los siguientes protocolos de red:

- Ethernet
- TCP/IP.
- IPX, estándar para redes Novell
- Netbeui (NETbios); estándar para redes Microsoft.

CAPÍTULO V. PROTOCOLO DE ADMINISTRACIÓN SIMPLE DE RED (SNMP)

5.1 ANTECEDENTES.

El organismo que administra y regula la red Internet encargó en 1987 a un grupo técnico (que se encarga de encontrar soluciones a los problemas técnicos que plantea el funcionamiento de la red), una solución de administración integrada para dicha red.

En la primera etapa de ARPANET se comprendió que cuando había problemas con la red, la única forma de identificar el problema era ejecutando comandos muy simples como el ping, el cual, no brinda suficiente información para resolver rápidamente dichos problemas. En el año de 1990, este grupo técnico propuso como solución utilizar un único protocolo capaz de ser entendido por todos los dispositivos de la red Internet. Surge un nuevo estándar llamado: SNMP (Protocolo Simple de Gestión de Red, Simple Network Management Protocol), definido en el RFC 1157. Este protocolo muestra una manera de administrar y supervisar las redes informáticas para identificar y resolver problemas, así como para planear su crecimiento. Se encuentra implementado en la capa de aplicación y pertenece al grupo de protocolos de TCP/IP.

Este protocolo ha sido muy aceptado desde entonces y la mayoría de los fabricantes lo implementan en sus equipos con protocolos TCP/IP.

El SNMP, se diseñó para permitir que sistemas heterogéneos y equivalentes se comunicaran entre sí, generasen informes y permitiesen modificaciones de sus configuraciones sobre una red TCP/IP. Por ejemplo, un dispositivo SNMP (como un router Cisco) se puede monitorear/configurar desde un cliente SNMP, y se pueden escribir con sencillez scripts, para alertar si los paquetes suben por encima de un límite. Por desgracia, SNMP no incluye seguridad. El SNMPv1 se propuso originalmente en el RFC 1157 (Mayo de 1990) y la sección 8 (Consideraciones de Seguridad) dice: "En esta memoria no se discuten asuntos de seguridad". Al parecer

eso lo resume todo. En 1992/1993, salió el SNMPv2, y contenía consideraciones de seguridad, sin embargo éstas se eliminaron más tarde cuando demostraron ser totalmente rompibles. De modo que se concluye con un SNMPv2 sin seguridad.

Hasta el momento existen tres versiones del protocolo: SNMPv1 (versión 1), SNMPv2 (versión 2) y SNMPv3 (versión 3). Las tres son muy parecidas, solo que SNMPv2 tiene algunas mejoras sobre la primera versión, y de la misma forma SNMPv3 tiene ciertas ventajas sobre la segunda versión.

5.2 COMPONENTES.

SNMP es un protocolo que permite que la administración transmita datos estadísticos a través de la red a una estación de administración central. SNMP es un componente de la Arquitectura de Administración de Red. La Arquitectura de Administración de Red se compone de cuatro componentes principales (fig. 5.1):

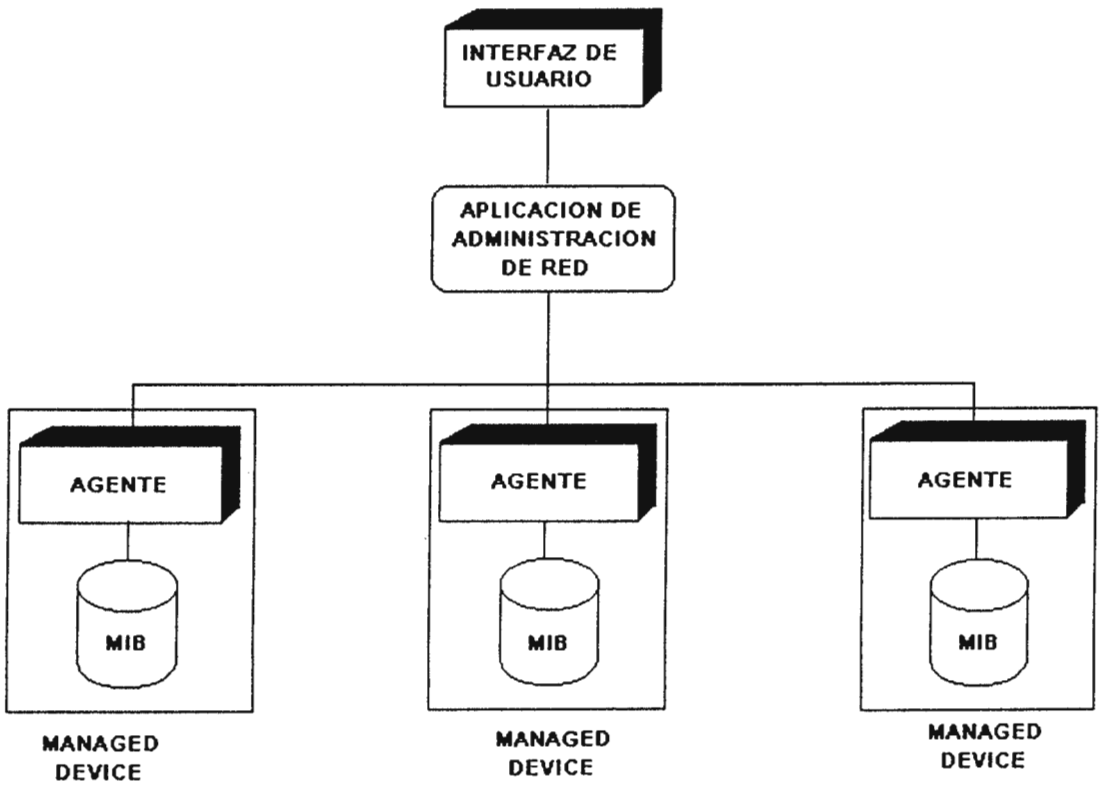


Fig. 5-1. Arquitectura de Administración de Red

1. Estación de administración:

La estación de administración es la interfaz del administrador de red al sistema de red. Posee los programas para manipular los datos y controlar la red. La estación de administración también mantiene una base de datos de información de administración (MIB) extraída de los dispositivos bajo su administración.

2. Agente de administración:

El agente de administración es el componente incluido en los dispositivos que se deben administrar. Puentes, routers, hubs y switches pueden contener agentes SNMP que les permitan ser controlados por la estación de administración. El agente de administración responde a la estación de administración de dos maneras. En primer lugar, mediante sondeo, la estación de administración requiere datos desde el agente y el agente responde con los datos solicitados. La captura es un método de recopilación de datos diseñado para reducir el tráfico en la red y el procesamiento en los dispositivos que se controlan. En lugar de que la estación de administración haga un sondeo a los agentes a intervalos específicos continuamente, se establecen umbrales (límites superiores o inferiores) en el dispositivo administrado. Si se supera este umbral en el dispositivo, el dispositivo administrado envía un mensaje de alerta a la estación de administración. Esto elimina la necesidad de realizar sondeos continuos de todos los dispositivos administrados en la red. La captura es muy ventajosa en las redes que incluyen una gran cantidad de dispositivos que necesitan administrarse. Reduce la cantidad de tráfico SNMP en la red para proporcionar mayor ancho de banda para la transferencia de datos.

3. Base de información de administración:

La base de información de administración tiene una estructura de base de datos y reside en cada dispositivo administrado. La base de datos contiene una serie de objetos, que son datos sobre recursos reunidos en el dispositivo administrado. Algunas de las categorías en el MIB incluyen datos de interfaz de puerto, datos de TCP y datos de ICMP.

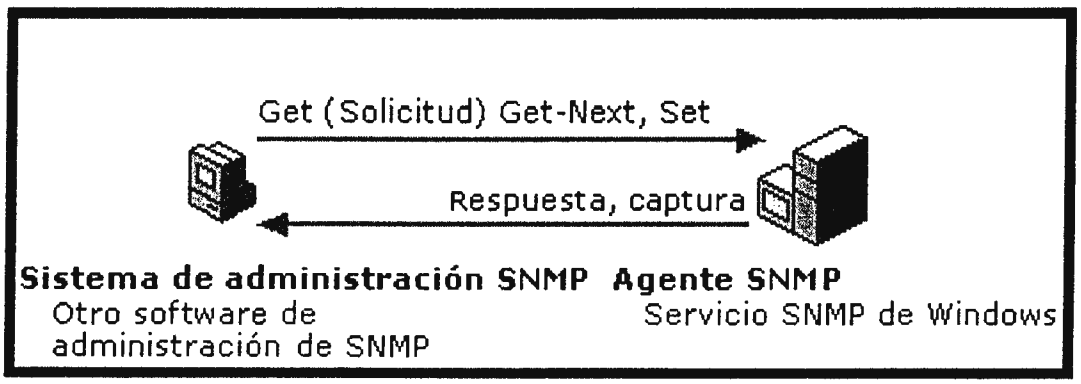
4. Protocolo de administración de red:

El protocolo de administración de red utilizado es SNMP. SNMP es un protocolo de capa de aplicación diseñado para comunicar datos entre la consola de administración y el agente de administración. Tiene tres capacidades clave. La capacidad para **OBTENER**, que implica que la consola de administración recupera datos del agente, **COLOCAR**, que implica que la consola de administración establece los valores de los objetos en el agente, y **CAPTURAR**, que implica que el agente notifica a la consola de administración acerca de los sucesos de importancia.

En el momento en que se desarrolló SNMP, se diseñó para ser un sistema a corto plazo que eventualmente se reemplazaría. Pero tal como ocurre con TCP/IP, se ha transformado en uno de los estándares principales en las configuraciones de administración de Internet-redes internas.

5.3 OPERATIVIDAD.

La operación de SNMP requiere dos componentes:



Jn sistema de administración SNMP.

El sistema de administración, también denominado consola de administración, ;nvía peticiones de actualización e información a un agente SNMP. Cualquier equipo ¡ue ejecute software de administración SNMP es un sistema de administración

SNMP. No es necesario que la aplicación del software de administración se ejecute en el mismo host que el agente SNMP.

El sistema de administración SNMP pide información de un equipo administrado, denominado agente SNMP, como la cantidad de espacio disponible en el disco duro o el número de sesiones activas. El sistema de administración también puede iniciar un cambio en la configuración de un agente. No obstante, esto no es muy común, ya que la mayoría de los clientes únicamente tienen acceso de sólo lectura.

Un agente SNMP.

El agente SNMP responde a las peticiones de información del sistema de administración. Cualquier equipo que ejecute el software del agente SNMP es un agente SNMP. El Servicio SNMP puede configurarse para determinar qué estadísticas se están supervisando y qué sistemas de administración están autorizados a pedir información.

En general, los agentes no originan mensajes sino que sólo los responden. Un mensaje de captura es la única comunicación SNMP iniciada por el agente. Una captura es un suceso que desencadena una alarma en un agente, como la reinicialización de un sistema o un acceso no válido, que mejora la seguridad.

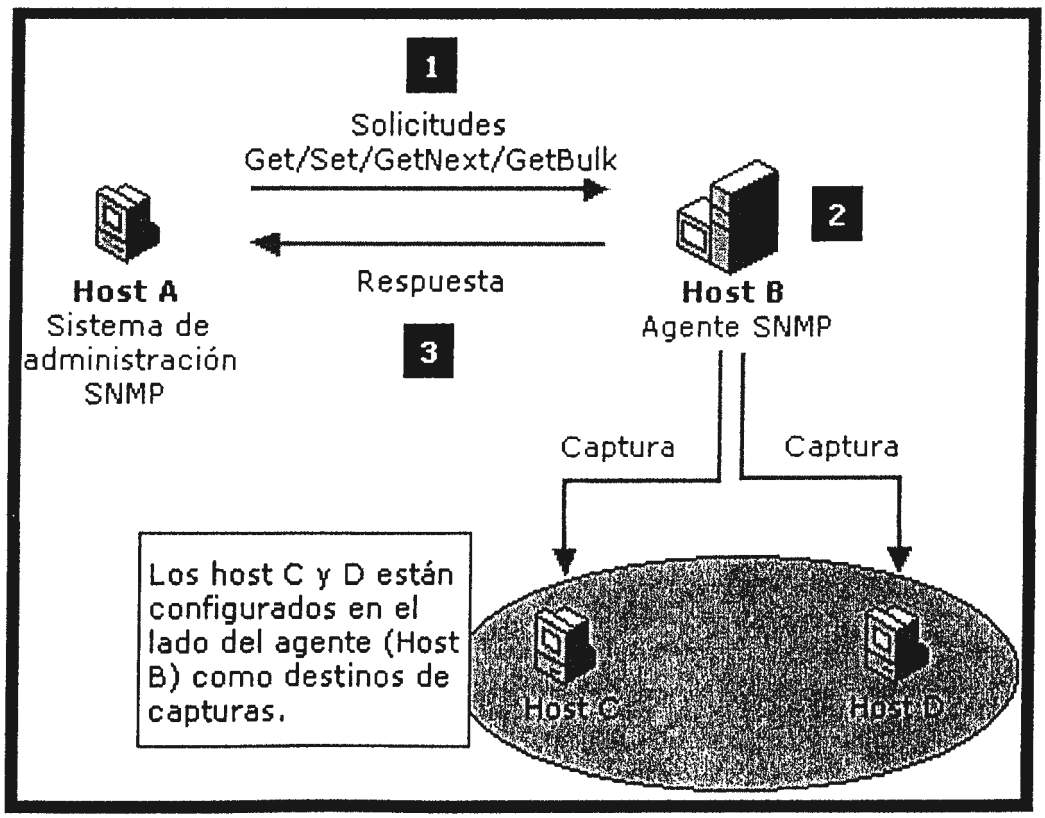
Los agentes y hosts de administración pertenecen a una comunidad SNMP, que es un conjunto de hosts agrupados con fines administrativos. La definición de comunidades proporciona seguridad, ya que sólo permite que se comuniquen sistemas de administración y agentes de la misma comunidad.

Tanto los agentes como los sistemas de administración utilizan mensajes de SNMP para inspeccionar y comunicar información del host. Los mensajes de SNMP se envían mediante el Protocolo de datagramas de usuarios (UDP). El Protocolo Internet (IP) se utiliza para enrutar mensajes entre el sistema de administración y el host.

La información que pide el sistema de administración se encuentra en una base de datos de información de administración (MIB) La base de datos MIB contiene varios tipos de información acerca de un equipo conectado a la red, como la versión del software de red que se ejecuta en ese equipo y el espacio disponible en el disco duro.

El ejemplo siguiente ilustra cómo responde un agente SNMP a una petición de información del sistema de administración:

1. El sistema de administración (Host A), envía un datagrama de SNMP al agente (Host B) con el nombre de host del agente y la dirección IP o IPX.
2. El agente SNMP recibe el datagrama y comprueba el nombre de comunidad al que pertenece el sistema de administración. Si es un nombre de comunidad válido, el agente recupera los datos solicitados del subagente SNMP adecuado. Si el nombre de comunidad no es correcto, el agente envía una captura de "error de autenticación" a los destinos de captura (hosts C y D).
3. El agente SNMP devuelve el datagrama al sistema de administración con la información pedida.



Mensajes de SNMP.

Cuando los programas de administración del protocolo simple de administración de redes (SNMP) envían peticiones a un dispositivo de red, el software del agente de ese dispositivo recibe las peticiones y recupera la información de las MIB, a continuación el agente vuelve a enviar la información pedida al programa de administración SNMP que realizó dicha petición. Para realizar estas tareas, el agente utiliza los mensajes siguientes:

Mensajes de SNMP	Descripción
Get	Mensaje básico de petición de SNMP. Enviado por un sistema de administración SNMP, pide información acerca de una única entrada de la base de datos MIB de un agente SNMP. Por ejemplo, la cantidad de espacio libre en el disco.
Get-next	Tipo ampliado de mensaje de petición que puede utilizarse para examinar el árbol entero de objetos de administración. Cuando se procesa una petición Get-next para un objeto determinado, el agente devuelve la identidad y el valor del objeto que sigue lógicamente al objeto de la petición. La petición Get-next resulta útil en el caso de tablas dinámicas, como una tabla interna de enrutado IP.
Set	Si está permitido el acceso de escritura, este mensaje puede utilizarse para enviar y asignar un valor de MIB actualizado al agente.
Getbulk	Pide que el tamaño de los datos transferidos por el agente del host sea lo más grande posible, dentro de las limitaciones dadas de tamaño de mensaje. Esto reduce al mínimo el número de intercambios de protocolo necesarios para recuperar una cantidad importante de información de administración. El tamaño máximo del mensaje no debe ser superior a la unidad de transmisión máxima (MTU) de la ruta de acceso, el tamaño de trama máximo permitido para una única trama de la red, ya que se puede producir una fragmentación.

Trap	Un mensaje no solicitado enviado por un agente SNMP a un sistema de administración SNMP cuando el agente detecta que se ha producido un tipo determinado de suceso localmente en el host administrado. La consola de administración SNMP que recibe un mensaje de captura se conoce como destino de captura. Por ejemplo, puede enviarse un mensaje de captura sobre un suceso de reinicio del sistema.

CAPÍTULO VI. UTILIDADES Y HERRAMIENTAS COMUNES.

Este capítulo provee una revisión detallada de los comandos y utilitarios disponibles en los sistemas operativos Linux y Windows.
Aunque nuestro estudio está basado específicamente en la plataforma Linux, hemos considerado conveniente hacer una revisión de los comandos disponibles en Windows.

6.1 DIAGNÓSTICO DE FALLAS DE RED.

Las fallas en la red son caracterizadas por ciertos síntomas. Éstos síntomas pueden ser generales (por ejemplo cuando un cliente no puede acceder a un servidor específico), o pueden ser específicos (cuando no existe una ruta en la tabla de enrutamiento).

Los siguientes pasos corresponden a un proceso detallado del diagnóstico de fallas de red.

Paso I:
Cuando se analiza un problema debe ser clara la definición del mismo. Para analizar ɔropiamente el problema deben identificarse claramente los síntomas y las causas ɥue las originan. Por ejemplo, un host no puede estar respondiendo a las solicitudes ɗe los clientes de red (síntoma). Las posibles causas del problema anterior pueden ɜer: una mala configuración del host en la red, problemas en la tarjeta de red o ɔroblemas de ruteo.

Paso II:
Recolectar toda la información relacionada con el problema. Se deben realizar ɔreguntas del problema a los usuarios afectados. Se debe además, recolectar ɲformación a través de monitores de red, analizadores de protocolos, chequeo de ɔanel de control de equipos de comunicación.

Paso III: Descartar posibles causas de problemas en base a la información obtenida en el paso anterior. Dependiendo de los datos obtenidos, por ejemplo, puede descartarse el hardware como posible causa del problema.

En la siguiente sección se profundizará en herramientas que nos permiten recolectar información para el diagnóstico de fallas de red.

6.2 HERRAMIENTAS DE DIAGNÓSTICO NATIVAS DEL NOS (NETWORK OPERATING SYSTEM).

Ésta sección provee un análisis detallado de los comandos y utilidades disponibles en los sistemas operativos más comunes.

PING

Sistemas Operativos:

 **Unix, Linux**

 **Windows 9x, NT, 2000, XP**

Descripción general

El comando ping provee dos servicios básicos: primeramente, puede ser usado para determinar si existe un nivel básico de conectividad entre uno o más sistemas. Éste comando puede ser utilizado si un dispositivo remoto en la red es alcanzable por el sistema local, es la herramienta más ampliamente utilizada para depurar problemas de conectividad.

Segundo, puede proveer estadísticas rudimentarias del rendimiento de la red, ping puede ser utilizado para determinar problemas de red relacionados con tráfico. El termino ping es derivado de la frase **packet internet groper.**

La herramienta ping puede utilizarse en dos formas: especificando un nombre de host ó dirección IP valida, ó utilizando opciones de línea de comando con un nombre de host ó dirección IP valida.

Determinando la disponibilidad en la red de dispositivos.

Ping puede ser utilizado para determinar la disponibilidad de cualquier dispositivo TCP/IP; aunque éste no tenga específicamente un sistema operativo. Por ejemplo, para determinar si el host Xeroxdoc es alcanzable podemos utilizar la línea de comando mostrado en la siguiente figura.

```
C:\>ping xeroxdoc

Haciendo ping a xeroxdoc [10.0.0.3] con 32 bytes de datos:

Respuesta desde 10.0.0.3: bytes=32 tiempo<1m TTL=255
Respuesta desde 10.0.0.3: bytes=32 tiempo<1m TTL=255
Respuesta desde 10.0.0.3: bytes=32 tiempo<1m TTL=255
Respuesta desde 10.0.0.3: bytes=32 tiempo<1m TTL=255

Estadísticas de ping para 10.0.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

En este caso ping no muestra ninguna perdida de paquetes con el dispositivo Xeroxdoc, el cual como se podrá imaginar es un impresor XeroxDoc Láser jet, Con lo anterior podemos asegurar que desde el punto de vista IP, Xeroxdoc esta vivo visible en la red) y operando normalmente.

Nótese que al decir que el dispositivo esta vivo no se esta garantizando que otros servicios de red como FTP ó TELNET estén disponibles. Ping es utilizado exclusivamente para determinar conectividad básica.

En este ejemplo el comando es ejecutado desde Windows, en el caso de Linux ping no finaliza hasta que se presiona `control+c`.

Si Xeroxdoc no estuviese disponible, mostrará el siguiente resultado

```
C:\>ping xeroxdoc

Haciendo ping a xeroxdoc [10.0.0.3] con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 10.0.0.3:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

Determinado el rendimiento de la red.

El comando ping puede ser utilizado para medir el tiempo requerido para transmitir un mensaje a un destino remoto y el tiempo requerido para obtener una respuesta.

Ping utiliza una solicitud ICMP cada segundo hacia el destino que se le ha especificado y reporta cada respuesta a esta solicitud ICMP. Un ejemplo de este reporte es el siguiente:

```
[root@mafia1 /]# ping mafia1
PING mafia1.mafia.net (10.0.0.1) from 10.0.0.1 : 56(84) bytes of data.
64 bytes from mafia1.mafia.net (10.0.0.1): icmp_seq=0 ttl=255 time=419 usec
64 bytes from mafia1.mafia.net (10.0.0.1): icmp_seq=1 ttl=255 time=373 usec
64 bytes from mafia1.mafia.net (10.0.0.1): icmp_seq=2 ttl=255 time=341 usec

--- mafia1.mafia.net ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.341/0.377/0.419/0.039 ms
[root@mafia1 /]#
```

Éste reporte nos proporciona el tamaño del paquete, el hostname ó la dirección IP del dispositivo destino, un número de secuencia, el valor del tiempo de ida y vuelta y un resumen estadístico. El valor del tiempo muestra el tiempo de ida y vuelta en micro segundos de cada respuesta recibida. Al final del reporte se muestran los cálculos de mínimo, promedio y máximo de todos los valores de los tiempos de ida y vuelta.

Generalmente en una red LAN la perdida de paquetes es rara y si ésta ocurre puede indicar un problema en la red o en el dispositivo al que se esta haciendo ping. Sin embargo, en redes bastante grandes o Internet, la perdida de paquetes puede considerarse normal. Por ejemplo el sitio de Internet mostrado abajo muestra una cierta cantidad de perdida de paquetes lo cual puede considerarse normal:

```
Ping -c 10 www.cdb.edu.sv
Ping www.cdb.edu.sv (168.243.3.2) : 56 data bytes
64 bytes from 168.243.3.2: icmp_seq=7  ttl=224  time=240.1 ms
64 bytes from 168.243.3.2: icmp_seq=7  ttl=224  time=240.1 ms
64 bytes from 168.243.3.2: icmp_seq=7  ttl=224  time=240.1 ms

--- www.cdb.edu.sv ping statistics
10 packets transmitted,   3 packets   received, 70% packet loss
round-trip min/avg/max = 240.1 /240.1 /240.1 ms
```

El ejemplo anterior indica que hay un 70% de perdidas de los paquetes enviados a www.cdb.edu.sv. En otras palabras de los 10 paquetes que enviamos, solo recibimos respuesta a tres de ellos, 7 de 10 representa el 70% de paquetes perdidos. Una posible causa es que algún router en la ruta hacia www.cdb.edu.sv este muy ocupado o sobrecargado con tráfico. Como resultado, algunas de nuestras solicitudes ICMP son descartadas al no poder llegar a su destino final (www.cdb.du.sv).

Opciones Misceláneas de Ping.

La opción **–R** para linux y **–r recuento** para Windows (donde recuento es un número entre 1 y 9, probado en Windows 2000 y XP) habilita el registro de la ruta por el cual se pasa para llegar al destino. Como resultado, se obtiene una lista de routers que son utilizados para llegar al destino final.

```
[root@mafia1 /root]# ping -c 5 -R 10.0.0.2
PING 10.0.0.2 (10.0.0.2) from 10.0.0.1 : 56(124) bytes of data.
64 bytes from hugo.mafia.net (10.0.0.2): icmp_seq=0 ttl=128 time=844 usec
NOP
RR:     mafia1.mafia.net (10.0.0.1)
        hugo.mafia.net (10.0.0.2)
        mafia1.mafia.net (10.0.0.1)

64 bytes from hugo.mafia.net (10.0.0.2): icmp_seq=1 ttl=128 time=922 usec
NOP     (same route)
64 bytes from hugo.mafia.net (10.0.0.2): icmp_seq=2 ttl=128 time=799 usec
NOP     (same route)
64 bytes from hugo.mafia.net (10.0.0.2): icmp_seq=3 ttl=128 time=931 usec
NOP     (same route)
64 bytes from hugo.mafia.net (10.0.0.2): icmp_seq=4 ttl=128 time=828 usec
NOP     (same route)

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.799/0.864/0.931/0.064 ms
[root@mafia1 /root]#
```

Existe una opción de ping disponible únicamente en UNIX que permite inundar la red con solicitudes ICMP aproximadamente 100 veces por segundo o tan rápido como el dispositivo destino pueda procesarlo.

La opción **–f** puede ser peligrosa dado que es capaz de consumir un porcentaje significativo del ancho de banda de la red y puede hacer que un dispositivo prácticamente desaparezca de la red debido a que este esta demasiado ocupado respondiendo las solicitudes de ping.

No es recomendable que se use esta opción en un ambiente de producción ya que con toda seguridad impactara las operaciones del uso de la red.

```
root@mafia1 /]# ping -c 2000 -f -v 10.0.0.1
PING 10.0.0.1 (10.0.0.1) from 10.0.0.1 : 56(84) bytes of data.
Warning: no SO_RCVTIMEO support, falling back to poll

--- 10.0.0.1 ping statistics ---
2000 packets transmitted, 2000 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.119/0.256/0.795/0.072 ms
root@mafia1 /]# _
```

¿Por qué utilizar el modo de inundación de la red de ping?, simple, para producir trafico en la red y ver que pasa. Esto puede ser muy útil para los

administradores de red, más que todo para determinar el comportamiento de dispositivos de red como routers o hubs en un ambiente de trafico real y para poner a prueba los monitores de red.

Por razones de seguridad esta opción solo puede ejecutarse teniendo los privilegios de root, un usuario convencional no podrá hacer uso de esta opción como lo muestra el siguiente ejemplo:

```
[hugo@mafia1 hugo]$ ping -f mafia1
ping: Operaci?n no permitida
[hugo@mafia1 hugo]$ _
```

PATHPING

Sistemas Operativos:

- **Windows 2000, XP**

Descripción general

Proporciona información acerca de la latencia de red y las pérdidas de red en saltos intermedios entre un origen y un destino. Pathping envía múltiples mensajes de solicitud de eco a cada enrutador entre un origen y un destino en un período de tiempo y calcula los resultados en función de los paquetes devueltos desde cada enrutador. Puesto que el comando pathping muestra el nivel de pérdidas de paquetes en un vínculo o enrutador específico, se puede determinar qué enrutadores o vínculos están causando problemas en la red. El comando pathping realiza la función equivalente al comando tracert para identificar los enrutadores que se encuentran en la ruta o camino para llegar a un destino específico. Hace ping periódicamente a todos los enrutadores durante un período de tiempo especificado y calcula estadísticas en función del número que devuelve cada uno. Cuando se usa sin parámetros pathping muestra ayuda sobre su uso.

Sintaxis:

pathping [-n] [-h saltosMáximos] [-g listaHost] [-p período] [-q NumConsultas] [-w tiempoDeEspera] [-T] [-R] [nombreDestino]

Parámetros:

-n

Impide que pathping intente resolver las direcciones IP de los enrutadores intermedios en sus nombres. Así se puede acelerar la presentación de los resultados de pathping.

-h *saltosMáximos*

Especifica el número máximo de saltos en la ruta para buscar el destino. El valor predeterminado es 30 saltos.

-g *listaHost*

Especifica que los mensajes de solicitud de eco utilizarán la opción Ruta de origen no estricta en el encabezado IP con el conjunto de destinos intermedios especificados en ListaHost. Con el enrutado de origen no estricto, los sucesivos destinos intermedios se pueden separar por uno o más enrutadores. El número máximo de direcciones o nombres que se pueden incluir en la lista es 9. ListaHost es una serie de direcciones IP (en notación decimal con puntos), separadas por espacios.

-p *período*

Especifica el número de milisegundos que se esperará entre pings consecutivos. El valor predeterminado es 250 milisegundos (1/4 de segundo).

-q *numConsultas*

Especifica el número de mensajes de solicitud de eco enviados a cada enrutador de la ruta. El valor predeterminado es 100 consultas.

-w *tiempoDeEspera*

Especifica el número de milisegundos que se esperará por cada respuesta. El valor predeterminado es 3.000 milisegundos (3 segundos).

-T

Adjunta una etiqueta de prioridad de capa 2 (por ejemplo, 802.1p) a los mensajes de solicitud de eco que envía a cada uno de los dispositivos de red de la ruta. Esto contribuye a identificar los dispositivos de red que no tienen configurada una prioridad de capa 2. Este modificador se utiliza para comprobar la conectividad de Calidad de servicio (QoS).

-R

Comprueba si cada uno de los dispositivos de red de la ruta es compatible con el protocolo RSVP (Protocolo de reserva de recursos), que permite que el equipo host reserve una determinada cantidad de ancho de banda para un flujo de datos. Este modificador se utiliza para comprobar la conectividad de Calidad de servicio (QoS).

NombreDestino

Especifica el destino, identificado por la dirección IP o el nombre de host.

?

Muestra Ayuda en el símbolo del sistema.

Comentarios Adicionales:

- Los parámetros de PATHPING distinguen entre mayúsculas y minúsculas.
- Para evitar congestiones en la red, se debe hacer ping en intervalos suficientemente espaciados.
- Cuando se utiliza el parámetro -p, los pings se envían individualmente a cada salto intermedio. Por lo tanto, el intervalo entre dos pings enviados al mismo salto es el período, multiplicado el número de saltos.

- Cuando se utiliza el parámetro -w, se pueden enviar múltiples pings en paralelo. Por ello, el tiempo especificado en el parámetro *tiempoDeEspera* no está limitado por el período de tiempo especificado en el parámetro período que se esperará entre pings.

- Utilizar el parámetro -T

  Al habilitar una prioridad de capa 2 en el equipo host, es posible enviar paquetes con una etiqueta de prioridad de capa 2, algo que puede ser utilizado por dispositivos de capa 2 para asignar una prioridad al paquete. Los dispositivos antiguos que no reconocen la prioridad de capa 2 descartarán estos paquetes, ya que parecen erróneos. Este parámetro ayuda a identificar los equipos de la red que están descartando estos paquetes.

- Utilizar el parámetro -R

  Se envía un mensaje de reserva RSVP para una sesión inexistente a cada dispositivo de red de la ruta. Si el dispositivo no está configurado para aceptar RSVP, devolverá un mensaje ICMP (Protocolo de control de mensajes Internet) de acceso imposible. Si el dispositivo admite RSVP, devuelve un mensaje de error de reserva de RSVP. Es posible que algunos dispositivos no devuelvan ninguno de estos mensajes. Si sucede esto, se muestra un mensaje de tiempo de espera superado.

- Este comando sólo está disponible si el Protocolo Internet (TCP/IP) está instalado como un componente en las propiedades de un adaptador de red, en conexiones de red.

Ejemplos:

El ejemplo siguiente muestra el resultado del comando PATHPING:

```
C:\>pathping www.cdb.edu.sv
```

```
Traza a master.cdb.edu.sv[168.243.3.10] sobre caminos de 30 saltos como
máximo:
  0  DC13 [10.17.56.93]
  1  10.17.56.1
  2  200.30.131.161
  3  200.13.174.65
  4  200.13.161.145
  5  168.243.249.30
  6  168.243.246.210
  7  168.243.250.246
  8  168.243.253.237
  9  168.243.254.129
 10  master.cdb.edu.sv [168.243.3.10]

Procesamiento de estadísticas durante 250 segundos...
            Origen hasta aquí   Este Nodo/Vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                                  DC13 [10.17.56.93]
                                    0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%       0/ 100 =  0%  10.17.56.1
                                    0/ 100 =  0%   |
  2    0ms     0/ 100 =  0%       0/ 100 =  0%  200.30.131.161
                                    1/ 100 =  1%   |
  3  388ms     7/ 100 =  7%       6/ 100 =  6%  200.13.174.65
                                    0/ 100 =  0%   |
  4  949ms     4/ 100 =  4%       3/ 100 =  3%  200.13.161.145
                                    0/ 100 =  0%   |
  5 1534ms    24/ 100 = 24%      23/ 100 = 23%  168.243.249.30
                                    0/ 100 =  0%   |
  6 1176ms     4/ 100 =  4%       3/ 100 =  3%  168.243.246.210
                                    0/ 100 =  0%   |
  7 1525ms    19/ 100 = 19%      18/ 100 = 18%  168.243.250.246
                                    0/ 100 =  0%   |
  8 1168ms     3/ 100 =  3%       2/ 100 =  2%  168.243.253.237
                                    0/ 100 =  0%   |
  9 1206ms     1/ 100 =  1%       0/ 100 =  0%  168.243.254.129
                                    4/ 100 =  4%   |
```

```
 10 1209ms     5/ 100 =  5%     0/ 100 =  0%  master.cdb.edu.sv
[168.243.3.10]

Traza completa.
C:\>
```

Cuando se ejecuta pathping, los primeros resultados muestran la ruta. Es la misma ruta de acceso que muestra el comando tracert. A continuación, se muestra un mensaje de ocupado durante un tiempo aproximado de 250 segundos (el tiempo varía en función del número de saltos). Durante este tiempo, se recopila información procedente de todos los enrutadores enumerados anteriormente, así como de los vínculos que se encuentran entre dichos enrutadores. Cuando finaliza este período, aparecen los resultados de la prueba.

PING6

Sistemas Operativos:

- **Windows 2000, XP**

Descripción general

Ping6 se utiliza para hacer ping a una dirección IP versión 6 [1] , por ser una tecnología que esta aún en desarrollo no se profundizará mucho en esta utilidad, pero es conveniente saber que Windows 2000 y XP ya incluyen IP versión 6 aunque no recomendado para un ambiente de producción.

Sintaxis:

Ping6 *Dirección_IPversión6*

Ejemplo:

```
C:\>ping6 fe80::201:2ff:fe64:df4

Haciendo ping fe80::201:2ff:fe64:df4
de fe80::201:2ff:fe64:df4%4 con 32 bytes de datos:

Respuesta desde fe80::201:2ff:fe64:df4%4: bytes=32 tiempo<1m
Respuesta desde fe80::201:2ff:fe64:df4%4: bytes=32 tiempo<1m
Respuesta desde fe80::201:2ff:fe64:df4%4: bytes=32 tiempo<1m
Respuesta desde fe80::201:2ff:fe64:df4%4: bytes=32 tiempo<1m

Estadísticas de ping para fe80::201:2ff:fe64:df4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

IP versión puede ser instalado en sistemas Windows 2000/XP utilizando la herramienta **ipv6 install:**

```
C:\>ipv6 install
Instalando...
Con éxito.
```

TRACERT (traceroute en plataformas Unix).

Sistemas Operativos:

Unix, Linux

Windows 9x, NT, 2000, XP

Descripción general

Este comando envía mensajes ICMP (portando datagramas UDP) de solicitud de eco con diferentes valores de TLL (tiempos de vida), indicándonos con ellos los diferentes routers y host (generalmente servidores o proxys) que atraviesa el paquete hasta llegar al host destino. Si en el camino el paquete se queda parado podremos averiguar en qué punto (router) se ha producido el fallo, una característica que el comando ping no puede realizar.

La sintaxis general de lo orden es:

C:>tracert www.servidor.com (tracert aaa.bbb.ccc.ddd).

Ejemplo: Trazar la ruta hacia el host www.laprensa.com.sv

```
C:\>tracert www.laprensa.com.sv

Traza a la dirección laprensa.com.sv [216.155.111.253]
sobre un máximo de 30 saltos:

  1     2 ms     3 ms     2 ms  router.cdb.edu.sv [168.243.3.1]
  2   348 ms   376 ms   188 ms  168.243.254.130
  3   612 ms   640 ms   479 ms  168.243.254.186
  4   232 ms   410 ms   603 ms  168.243.254.46
  5   476 ms   522 ms   623 ms  168.243.246.209
  6   731 ms   503 ms   538 ms  if-4-1-2-0.bb1.miami.teleglobe.net [207.45.205.1
41]
  7   582 ms   744 ms   645 ms  if-9-0.core1.miami.teleglobe.net [207.45.210.41]

  8   423 ms   691 ms   690 ms  if-9-0.core1.Chicago3.Teleglobe.net [64.86.81.17
0]
  9   736 ms   906 ms   872 ms  POS5-0.BR5.CHI2.ALTER.NET [204.255.169.17]
 10   553 ms   554 ms   752 ms  152.63.68.198
 11   370 ms   404 ms   483 ms  152.63.67.105
 12   861 ms   739 ms   887 ms  0.so-6-0-0.TL1.ATL1.ALTER.NET [146.188.136.157]
 13   830 ms   758 ms   667 ms  152.63.86.86
 14   657 ms     *      639 ms  152.63.84.205
 15   762 ms   880 ms   772 ms  acceleration-gw.customer.alter.net [65.195.233.6
]
 16     *        *      760 ms  laprensa.com.sv [216.155.111.253]

Traza completa.
```

NETSTAT

Sistemas Operativos:

 **Unix, Linux**

 **Windows 9x, NT, 2000, XP**

Descripción general

El comando netstat proporciona información sobre el estado actual de las conexiones de red, información de ruteo, los puertos en los que el equipo esta escuchando (aceptando conexiones), estadísticas de ethernet y otros datos importantes relacionados con las redes.

```
[root@mafia1 /root]# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 mafia1.mafia.net:www    mafia1.mafia.net:1189   TIME_WAIT
tcp        0      1 mafia1.mafia.net:1186   hugo.mafia.net:www      SYN_SENT
tcp        0    126 mafia1.mafia.net:telnet hugo.mafia.net:3054     ESTABLISHED
tcp        0      0 mafia1.mafia.net:ftp    hugo.mafia.net:3049     ESTABLISHED
tcp        0      0 mafia1.mafia.net:telnet hugo.mafia.net:3012     ESTABLISHED
[root@mafia1 /root]# _
```

Para mostrar las conexiones establecidas en los sistemas Windows utilice el comando **netstat** con la opción **–o** como se muestra en la figura:

```
C:\>netstat -o

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado           PID
  TCP    s6x1j1:3054            mafia1.mafia.net:telnet  ESTABLISHED     3644
  TCP    s6x1j1:3055            mafia1.mafia.net:ftp   ESTABLISHED     2576
  TCP    s6x1j1:3057            mafia1.mafia.net:ftp   ESTABLISHED     984
  TCP    s6x1j1:3001            hugo.mafia.net:3055    ESTABLISHED     984
```

Ambos comandos despliegan la actividad de los sockets TCP. Cada conexión incluye información concerniente a las direcciones locales y remotas, los cuales son mostrados en el formato:

```
Host: Puerto
```

Para cada conexión se muestra el estado de la misma, la tabla 6.2 lista los estados posibles de netstat.

Tabla 6.2 Estados TCP mostrados con netstat

Estado	Descripción
ESTABLISHED	La conexión es operacional
LISTEN	Un servicio o aplicación esta esperando por una conexión de un cliente.
SYN_SENT	El sistema local quiere abrir una conexión remota
SYN_RCVD	El sistema remoto quiere abrir una conexión.

FIN_WAIT_1	El sistema local esta en proceso de cerrar una conexión.
FIN_WAIT_2	El sistema local esta en proceso de cerrar una conexión.
CLOSE_WAIT	El sistema remoto quiere cerrar una conexión.
LAST_ACK	Paso final de CLOSE_WAIT
TIMED_WAIT	Paso final de FIN_WAIT_1 o FIN_WAIT_2
UNKNOW	El estado del socket es desconocido.

Cualquier conexión con el estado LISTEN esta esperando por conexiones entrantes las cuales usualmente son conocidas como recursos basados en servidor. Cuando un servicio esta esperando por solicitudes de la red, esta libre para ser accesado por cualquier dirección remota. Esta es la razón por la que 0.0.0.0 es listado bajo el campo de dirección remota.

```
C:\>netstat -a

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    s6x1j1:ftp             0.0.0.0:0              LISTENING
  TCP    s6x1j1:http            0.0.0.0:0              LISTENING
  TCP    s6x1j1:epmap           0.0.0.0:0              LISTENING
  TCP    s6x1j1:https           0.0.0.0:0              LISTENING
```

Analizando los resultados de netstat, el administrador puede fácilmente darse cuenta de servicios que no deberían estar corriendo. En el ejemplo anterior el servicio `ftp` representa un riesgo de seguridad para un servidor de aplicaciones, por lo tanto es recomendable deshabilitar tal servicio.

NBTSTAT

Sistemas Operativos:

 **Unix, Linux**

 **Windows 9x, NT, 2000, XP**

Descripción general

Muestra estadísticas del protocolo y conexiones TCP/IP actuales utilizando NBT (NetBIOS sobre TCP/IP). NBTStat es una herramienta que resulta de utilidad para solucionar problemas con la resolución de nombres llevada a cabo por NetBIOS.

Parámetros:

NBTStat -n

muestra los nombres que fueron registrados de forma local en el sistema por aplicaciones, tales como el servidor y el redirector.

NBTStat -c

muestra la caché de nombres NetBIOS, que contiene las traslaciones nombre-dirección para otras computadoras.

NBTStat –R

Purga la caché de nombres y la carga de nuevo desde el fichero LMHOSTS.

NBTStat -a <nombre>

Realiza un comando de estado del adaptador NetBIOS contra la computadora especificada por nombre. El comando de estado de adaptador devuelve la tabla de

nombres NetBIOS para esa computadora además de la dirección MAC de la tarjeta adaptadora.

NBTStat -S

Lista las sesiones NetBIOS en curso y sus estados, incluyendo estadísticas.

TCPDUMP

Sistemas Operativos:

 **Unix, Linux**

Descripción general

El comando TCPDUMP es un monitor de tráfico de propósito general que puede capturar y mostrar el contenido de los paquetes que viajan en la red.

Este comando puede ser utilizado como un **analizador de protocolos**, proporcionando una de las mejores formas de investigar problemas de comunicación y/o conectividad entre sistemas y dispositivos de red.

Generalmente los problemas de red pueden deberse a configuraciones incorrectas en los equipos o fallas en el hardware de comunicación, en ambos casos identificar la causa del problema puede ser complejo. La complejidad aumenta cuando el problema es a nivel de protocolos.

TCPDUMP posee un mecanismo de filtrado que le permite buscar aquellos paquetes que cumplan con cierto criterio de búsqueda.

Este comando posee dos modos de captura de paquetes: **promiscuo** y **no-promiscuo**. En el modo promiscuo, todo paquete que viaja por la red es

capturado, no importando si el paquete tenía por destino el equipo en el que se esta corriendo TCPDUMP. Debido a que ethernet es una red broadcast, cada frame transmitido puede ser visto por cualquier interface conectada a la red. Cualquier dispositivo puede leer cada frame transmitido siempre y cuando este dispositivo este configurado para hacerlo. Cuando un dispositivo o interface lee cada frame que viaja por la red, se dice que esta en `modo promiscuo`. En la práctica el modo promiscuo es utilizado en ocasiones en las que es necesario hacer un análisis de protocolos en la red. Por esta razón en los sistemas Unix únicamente el usuario root puede habilitar el modo promiscuo en una interface.

En el modo `no-promiscuo`, solo se pueden leer los paquetes que tienen por destino el equipo local. En condiciones normales toda interface esta en modo no-promiscuo.

Cuando TCPDUMP es invocado sin ninguna opción, este comenzara a capturar frames desde la red local y comenzara a mostrar su contenido. Debido a que la salida de TCPDUMP puede mostrar cantidades significativas de datos (lo cual puede ser in-leíble), es recomendable utilizar la opción **(–q)** para reducir la cantidad de información mostrada.

El formato de la salida incluye un marca de tiempo, host de origen y destino (o direcciones IP), el protocolo de red, algunas banderas, información adicional del protocolo y un resumen.

En el siguiente ejemplo, `hugo`(el host origen)y `mafia1`(el host destino) tienen una sesión telnet establecida. Lo anterior lo podemos asegurar observando que el puerto destino es telnet.

```
[root@mafia1 /root]# tcpdump -q
Kernel filter, protocol ALL, datagram packet socket
tcpdump: listening on all devices
00:05:50.204166 eth0 < hugo.mafia.net.1035 > mafia1.mafia.net.telnet: tcp 0 (DF)
00:05:50.204561 eth0 > mafia1.mafia.net.telnet > hugo.mafia.net.1035: tcp 88 (DF
) [tos 0x10]
00:05:50.294751 eth0 < hugo.mafia.net > mafia1.mafia.net: icmp: echo request
00:05:50.295074 eth0 > mafia1.mafia.net > hugo.mafia.net: icmp: echo reply
00:05:50.404478 eth0 < hugo.mafia.net.1035 > mafia1.mafia.net.telnet: tcp 0 (DF)
00:05:50.404809 eth0 > mafia1.mafia.net.telnet > hugo.mafia.net.1035: tcp 331 (D
F) [tos 0x10]
00:05:50.604754 eth0 < hugo.mafia.net.1035 > mafia1.mafia.net.telnet: tcp 0 (DF)
00:05:50.605158 eth0 > mafia1.mafia.net.telnet > hugo.mafia.net.1035: tcp 178 (D
F) [tos 0x10]

8 packets received by filter
```

Por default **TCPDUMP** captura paquetes hasta que el usuario interrumpa el programa presionando ctrl + c (control + z). En el ejemplo anterior el host **hugo,** también ha hecho una solicitud de ping al host **mafia1**, y este ha respondido a la solicitud. El símbolo **>** indica la dirección de la comunicación.

TELNET

Sistemas Operativos:

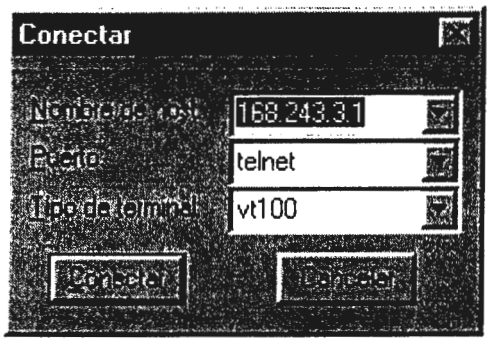
 **Unix, Linux**

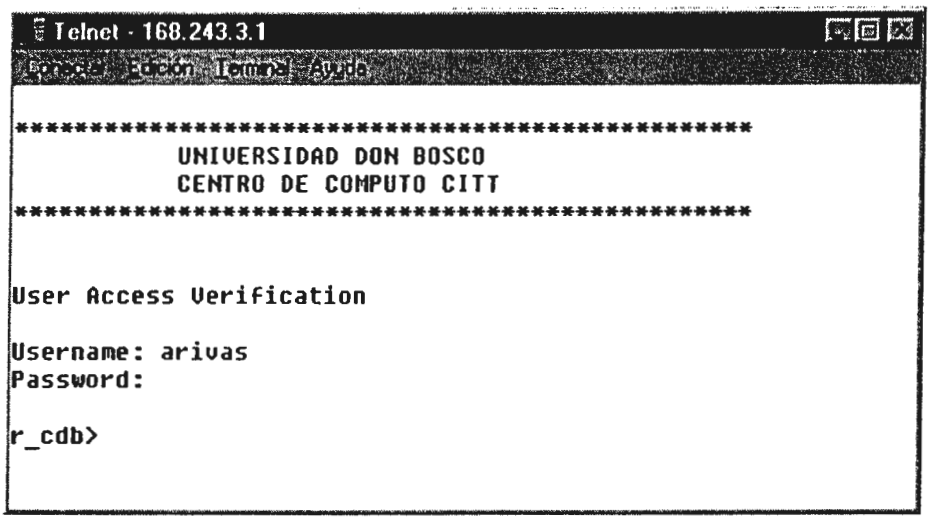
 **Windows 9x, NT, 2000, XP**

Descripción General

El software de emulación de terminal (Telnet) tiene la capacidad de acceder de forma remota a otro computador. Le permite conectarse a un host de Internet y ejecutar comandos. Se considera al cliente de Telnet como una máquina local y al servidor de Telnet como un host remoto. Para realizar una conexión desde un cliente Telnet, debe seleccionar una opción de conexión. Un cuadro de diálogo indica que se debe colocar un "Nombre de host" y un "Tipo de terminal". El nombre de host es la

dirección IP (DNS) del computador remoto con el que desea conectarse, y el tipo de terminal describe el tipo de emulación de terminal que desea que el computador ejecute.





La operación Telnet no utiliza en absoluto la capacidad de procesamiento de a PC transmisora, sino que transmite las pulsaciones del teclado al host remoto y envía el resultado de pantalla nuevamente al monitor local. El procesamiento y almacenamiento se producen en su totalidad en el computador remoto.

El computador host remoto ejecuta los comandos y transmite los resultados nuevamente al computador cliente local. Este proceso completo se vuelve a repetir, enviando comandos y recibiendo resultados hasta que el cliente local haya

completado la tarea que necesita realizar. Una vez que la tarea está finalizada, el cliente termina la sesión.

6.3 HERRAMIENTAS DE RED PROPIAS DE SISTEMAS OPERATIVOS UNIX.

ARPWATCH

Sistemas Operativos:

 **Unix, Linux**

Descripción General

ARPWATCH es una herramienta utilizada para comprobar la correspondencia entre pares de direcciones IP y direcciones MAC. En caso de que un cambio en un par se produzca (esto es, se escuche en el interfaz de red del sistema), ARPWatch envía un correo electrónico al administrador, notificando el suceso. También sirve para notificar la existencia de estaciones nuevas o la retransmisión de estaciones que llevaban mucho tiempo apagadas. De esta forma, es útil para notificar posibles ataques como IP Spoofing.

El spoofing es una técnica que consiste en engañar a un computador haciéndole creer que esta dialogando con un host cualquiera, cuando en realidad lo está haciendo con nosotros. Esto puede que no parezca una amenaza, ya que normalmente la autenticación se hace mediante password, por lo que aunque en nuestra conexión con un servidor suplantemos la identidad de otro host, tendremos que conocer la clave de acceso para hacer uso de un servicio dado.

El problema aparece cuando algunos de nuestros hosts establecen una relación de confianza : entonces, si alguien es capaz de engañarles diciendo que es uno del grupo, esto podría causar estragos en la seguridad de nuestra red.

ETHEREAL

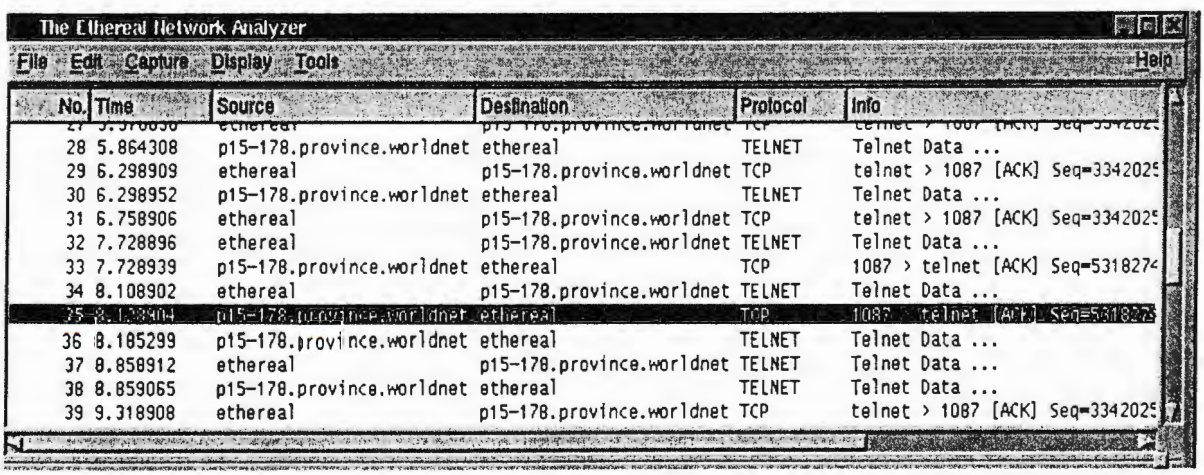
Sistemas Operativos:

Unix, Linux

Descripción General

Es un sniffer para Linux (y UNIX en general) que utiliza GUI y que ofrece algunos servicios interesantes. Uno de ellos es que la GUI de Ethereal permite examinar fácilmente los datos del sniffer, bien desde una captura en tiempo real o bien desde archivos de capturas tcpdump previamente generados. Todo ello, unido al continuo filtro para obtener una mejor exploracion, así como la compatibilidad con SNMP y la capacidad para realizar capturas sobre Ethernet, FDDI, PPP y Token Ring estándar, hace que Ethereal sea una buena opción.

La imagen que se presenta a continuación muestra a la herramienta Ethereal en el proceso de captura. Como se puede ver, es posible inspeccionar los datos capturados en detalle mientras la captura sigue en proceso.



FPING

Sistemas Operativos:

 **Unix, Linux**

Descripción General

Fping es una variación de ping, éste escanea un conjunto de servidores, así evita la espera que puede producir la llamada a un servidor que no este disponible. Es posible poner una red entera, creando un archivo con todas las IPs que se desean hacer en el fping y se le pasa el parámetro -f [Nombre de Archivo] y listo, el prueba todas las conexiones. Ejemplo:

```
[Monitor]>fping -f listaips -t

168.243.3.5 is alive
168.243.3.6 is alive
168.243.3.115 is alive
168.243.3.25 is alive
168.243.3.52 is unreachable
168.243.3.45 is unreachable
168.243.3.221 is unreachable
```

NMAP

Sistemas Operativos:

 **Unix, Linux**

Descripción General

Nmap es un software diseñado para permitir a los administradores de sistemas el monitoreo de redes, para determinar que servidores se encuentran activos y que servicios ofrecen. Nmap soporta un gran número de técnicas de

escaneo tales como: UDP, TCP Conect() (simplemente tratar de abrir una conexión como es habitual), TCP Syn (escaneos SYN semi-abiertos), ICMP.

Entre otras características nmap presenta la capacidad para la detección remota del sistema operativo de un host, detección de servidores inactivos por medio de pings paralelos, detección de filtrado de puertos, entre otras. A continuación se presenta un ejemplo en el cual se realiza un escaneo de puertos en un host. Posteriormente en el capítulo VII, se realizará un estudio más profundo de este software.

```
[root@monitor bin]# nmap -sT 168.243.3.4

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on data.cdb.edu.sv (168.243.3.4):
(The 1540 ports scanned but not shown below are in state: closed)
Port       State       Service
42/tcp     open        nameserver
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        listen
1026/tcp   open        nterm
8080/tcp   open        http-proxy


Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
[root@monitor bin]#
```

IFCONFIG

Sistemas Operativos:

- **Unix, Linux**

Descripción general

El comando ifconfig es la abreviación para **interface configuration** (configuración de la interface). Este comando es normalmente utilizado para configurar interfaces de red de área local en la mayoría de sistemas operativos unix. También puede ser usado para cambiar los parámetros de la interface después que el equipo ha sido iniciado.

Ifconfig permite el uso de un gran número de opciones. La tabla 6.3 lista las opciones más importantes.

Tabla 6.3 opciones de ifconfig.

-a	Muestra todas las interfaces del equipo
promisc -promisc	Habilita el modo promiscuo (que la tarjeta sea capaz de escuchar todo el trafico de la red) en la interface. La opción –promisc deshabilita el modo promiscuo.
Up	Permite habilitar la interface.
Down	Permite deshabilitar la interface.
Netmask	Configura la IP de la mascara de red. El argumento puede ser especificado en formato decimal (255.0.0.0) o hexadecimal (oxff00000)
broadcast	Configura la dirección IP broadcast. El argumento puede ser expresado de la misma forma que netmask.
Address	Configura la dirección IP de la interface. Esta dirección debe ser única.

Como listar las interfaces de red disponibles.

Para listar todas las interfaces del sistema, utilice el comando **ifconfig –a**.

La opción –a le indica a **IFCONFIG** que debe mostrar todas las interfaces instaladas en el sistema así como su actual configuración ó estado operacional.

```
[root@mafia1 /root]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 48:54:E8:29:8C:BC
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:644 errors:0 dropped:0 overruns:0 frame:0
          TX packets:556 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:11 Base address:0x1220

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:1320 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1320 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

[root@mafia1 /root]# _
```

En el ejemplo mostrado arriba indica que hay dos interfaces definidas. La primera, **eth0**, representa la interfaz física de 10Mps para una tarjeta NE2000.
La segunda, `lo`, es la interface `loopback`, usada para comunicaciones internas y diagnósticos. La dirección loopback puede ser usada para determinar si TCP/IP esta operando correctamente localmente, para ello es recomendable **hacer ping** a la dirección localhost ó 127.0.0.1 para determinar si se tiene respuestas validas.
Para cada interface, ifconfig –a muestra la siguiente información:

`Link encap`	Especifica el protocolo de encapsulamiento que la interfaz utilizará para transmitir. Estos generalmente pueden ser Ethernet, loopback local y protocolo punto a punto.
`HWaddr`	Representa la dirección MAC de la interface.
`Inet addr`	La dirección IP asignada a la interface.
`Bcast`	La dirección de Broadcast asignada a la interface.
`Mask`	Mascara de Red.
`Parámetros operacionales`	Estos parámetros son **`UP`**, **`BROADCAST`**, **`RUNNING`**, **`PROMISC`** y **`MULTICAST`**. Estos parámetros muestran el modo y el estado actual de la interface.
`Contadores estadísticos`	Representan los contadores estadísticos, estos son **`RX`** (paquetes recibidos), **`TX`** (paquetes transmitidos) y **`collisions`** (número de colisiones)

Interrupción y dirección I/O	Interrupt muestra el número de la interrupción utilizado físicamente por la interface. Base address muestra la dirección de memoria utilizada por la interfaz. Nótese que no todas las interfaces muestran estos dos datos. La interface loopback no muestra estos datos debido a que no utiliza ningún dispositivo de hardware.

Controlando el estado administrativo de las interfaces.

Con IFCONFIG es posible deshabilitar una interface activa o activar una interfaz deshabilitada mientras el sistema operativo esta corriendo. Esto es equivalente a desconectar el cable de red de la tarjeta de red.
Cuando una interface es deshabilitada, esta es considerada como **deshabilitada administrativamente**.

Para deshabilitar una interface utilice el comando **ifconfig eth0 down**.
Donde eth0 puede variar dependiendo si el equipo tiene más de una tarjeta de red instalada (eth1, eth2, etc).
Si vemos el estado de la interface que previamente deshabilitamos con **ifconfig eth0 down** se nos mostrara lo siguiente:

```
[root@mafia1 /root]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 48:54:E8:29:8C:BC
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:644 errors:0 dropped:0 overruns:0 frame:0
          TX packets:556 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:11 Base address:0x1220

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:1320 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1320 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

[root@mafia1 /root]# _
```

Nótese que ahora las palabras **UP** y **RUNNING** no aparecen, lo que indica que la interfaz ha sido deshabilitada y no esta disponible.
Para habilitar o activar esta interfaz, simplemente utilizamos la opción **UP** de ifconfig:

```
[root@mafia1 /root] ifconfig eth0 up
```

Modificando los parámetros de la interfaz.

En Linux existen varios métodos para modificar los parámetros de una interfaz de red. El primero de ellos es utilizando el comando **IFCONFIG**, con el cual los cambios se efectúan inmediatamente sin necesidad de reiniciar el equipo.
El segundo es modificar los archivos de sistema, con lo cual el cambio se hace permanente. El tercero es utilizando **LINUXCONF**.

Si se modifica los parámetros de la interfaz de red utilizando **IFCONFIG**, estos cambios se perderán la próxima vez que se reinicie el equipo.

Supongamos que necesitamos cambiar la dirección IP de nuestro servidor inux, la dirección antigua es 10.0.0.1 y la nueva dirección debe ser 10.0.0.6, en este caso en particular la mascara de red y la dirección broadcast se mantienen igual.
El siguiente comando hará el cambio requerido y tomara efecto inmediatamente:

```
[root@mafia1 /root] ifconfig eth0 10.0.0.6
```

Ahora supongamos que es necesario mover por unas cuantos horas nuestro servidor a una red completamente diferente, digamos que la nueva configuración de a interfaz de red en esa red debe ser:

Dirección IP	128.197.10.1
Mascara de red	255.255.0.0
Dirección broadcast	128.197.255.255

Para ello podemos utilizar las siguientes opciones de ifconfig

```
[root@mafia1 /root]# ifconfig eth0 128.197.10.1 netmask 255.255.0.0
broadcast 128.197.255.255
```

Interfaces Lógicas.

El comando **Ifconfig** permite configurar interfaces lógicas ó virtuales. Estas interfaces se comportan como interfaces físicas y pueden ser utilizadas para asignar diferentes direcciones IP al mismo equipo.

Para configurar interfaces virtuales, es necesario combinar la interface física con un número de referencia de la interfaz lógica, separados por dos puntos (:).
Por ejemplo para configurar la primera interface logia para eth0, se debe utilizar ifconfig con las siguientes opciones:

```
[root@mafia1 /root] # ifconfig eth0:1 100.0.0.3 netmask
255.0.0.0 broadcast 10.255.255.255
```

Nótese que la pseudo-interface, eth0:1 contiene la misma MAC (48:54:E8:29:8C:BC) y la misma interrupción (11) que la interfaz real.

```
[root@mafia1 /root]# ifconfig eth0:1 10.0.0.3 netmask 255.0.0.0 broadcast 10.25
5.255.255
[root@mafia1 /root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 48:54:E8:29:8C:BC
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:208 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:11 Base address:0x1220

eth0:1    Link encap:Ethernet  HWaddr 48:54:E8:29:8C:BC
          inet addr:10.0.0.3  Bcast:10.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:11 Base address:0x1220

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

Para remover una interface lógica, utilice la opción down:

```
[root@mafia1 /root]# ifconfig eth0:1 down
```

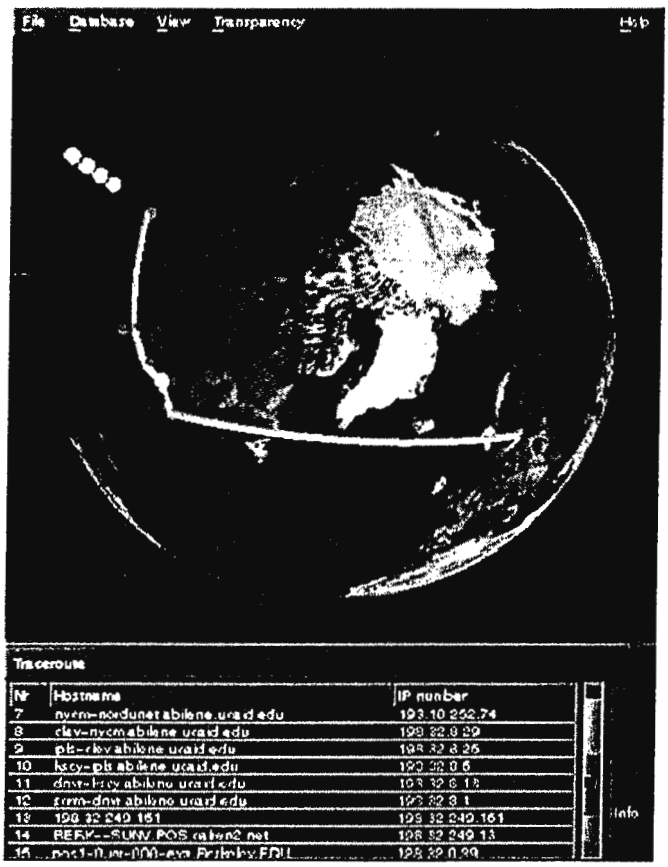
XTRACEROUTE

Sistemas Operativos:

Unix, Linux

Descripción General

XTRACEROUTE es una versión gráfica del programa traceroute, el cual traza la ruta que los paquetes IP siguen para llegar hasta su destino final.
Esta versión muestra un globo terráqueo y dibuja líneas de color amarillo entre los sitios por los que se pasa. Es posible hacer zoom, rotarlo y moverse alrededor de él.



CAPÍTULO VII. IMPLEMENTACIÓN DE HERRAMIENTAS DE MONITOREO Y DIAGNÓSTICO DE FALLAS DE RED.

7.1 ESTUDIO INDIVIDUAL DE LAS HERRAMIENTAS DE MONITOREO.

Como se describió en el capitulo IV (Monitoreo de Red), un Monitor de Redes de Computadores es un instrumento que entrega datos acerca de la red en la cual está conectado para extraer de ella información de tipo estadístico, evolución de parámetros de funcionamiento, histogramas, tráfico por cada enlace, estado de los servicios, etc. Ésta información es mostrada en forma de gráficos que hacen más fácil su interpretación.

Además, en el capitulo IV se definió la clasificación de los monitores de red, según su funcionamiento. Para hacer un breve recuento, los monitores de red se pueden clasificar según los criterios de: ***Objetivo, Reporte, Intrusividad, Operación y Protocolos que miden.***
Dentro de los monitores de objetivo existen dos clasificaciones: *Estado y Tráfico.*
Los monitores de reporte se clasifican en: *Histórico y Tiempo Real.*
La clasificación de los monitores de Operación son: *Local y Remota.*

A continuación se analizarán 10 monitores de red existentes, los 10 monitores son herramientas de dominio público, los cuales se encuentran disponibles de manera gratuita en Internet.

De estos monitores se incluye una descripción general, principales características, el proceso de instalación, configuración de los archivos correspondientes, captura de pantallas de su ejecución dentro de una red real (Red del Centro de Cómputo de la Universidad Don Bosco – 168.243.3.0), la clasificación (según la clasificación de monitores realizada en el capítulo IV), además sus ventajas y desventajas comparativas. Posteriormente se entregará un cuadro comparativo consolidado entre ellos.

Es de tomar muy en cuenta que la conclusión de este capítulo es de vital importancia para el presente estudio de tesis, ya que de la evaluación de estas herramientas surgirán las que se incorporarán a la interfaz de monitoreo de red para la Universidad Don Bosco.

Cheops-ng (cheops next generation) Version 0.1.5

Cheops-ng es una herramienta de administración de red para mapear y monitorear la red. Posee una funcionalidad de descubrimiento automático de red y de hosts, así como también la capacidad de detectar el sistema operativo que se ejecuta en la estación de trabajo monitoreada.

Cheops-ng es capaz de examinar las estaciones de trabajo para observar que servicios se ejecutan en ellas. Para algunos servicios, cheops-ng actualmente es capaz de ver que programa se encuentra ejecutándose para un servicio determinado y la versión del programa, por ejemplo puede detectar para un servicio http que se esté ejecutando a través del programa Internet Information Server 4.0 (IIS 4.0).
Las características principales que presenta cheops-ng son:

1. Son utilizados paquetes simples de ICMP "ping", para el descubrimiento inicial de la red y de los host que se encuentran activos dentro de dicha red.
2. Transferencias de nombre de dominio son utilizados para listar los host que pertenecen a un dominio o un rango de IP´s.
3. La detección del sistema operativo que se ejecuta en un host es realizada por medio de paquetes TCP. Para éste propósito también es utilizando el escaneo de puertos a través de nmap.
4. El mapeo es hecho utilizando paquetes UDP (u opcionalmente ICMP) con pequeños valores de time-to-live (traceroute y mtr, respectivamente).
5. El proceso de detección de servicios lo hace por medio del método conocido como "banner grabbing", el cual consiste en un análisis de puertos realizado por el programa nmap.

Instalación de cheops-ng Ver 0.1.5.

Instalación.

1. Copie el paquete cheops-ng-0.1.5.tar al directorio /usr/local.
2. Descomprima el paquete : tar –xvf cheops-ng-0.1.5
3. Cambie al directorio /usr/local/cheops-ng-0.1.5
4. Ejecute el comando ./configure
5. Ejecute el comando gmake
6. Ejecute el comando gmake install
7. Inicie una sesión gráfica de Linux : startx

Ejecución.

Ejecutar con el usuario root (realizarlo en la interfaz grafica de Linux. GUI):

1. cheops-agent *(Este comando ejecuta el agente para el monitoreo de la red)*

2. cheops-ng *(Ejecuta el programa y la consola de administración)*

Al ejecutar la línea de comando *cheops-ng,* se obtiene la ventana que se muestra en la Figura 7-1, en esta ventana se debe introducir la dirección *IP* que corresponde al host agente que se encarga del monitoreo de la red:

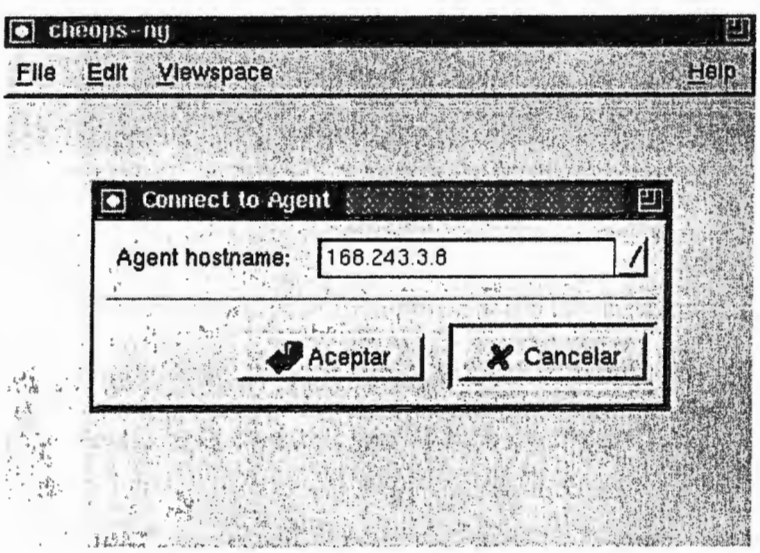


Fig. 7-1. Ip del host que será el agente de monitoreo

A continuación(Fig. 7-2) , se define el rango de direcciones *IP* de los hosts que se desean monitorear, para el ejemplo se monitorea la red 168.243.3.0 en el rango de 168.243.3.1 hasta 168.243.3.9:

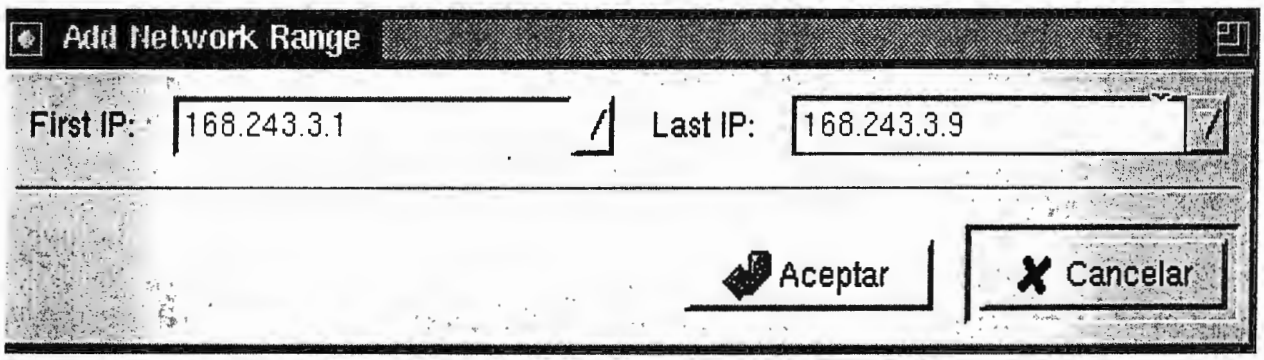


Fig. 7-2. Rango de direcciones IP que serán monitoreadas.

La Figura 7-3 muestra los host que fueron descubiertos en el rango definido, por el agente cheops-ng.

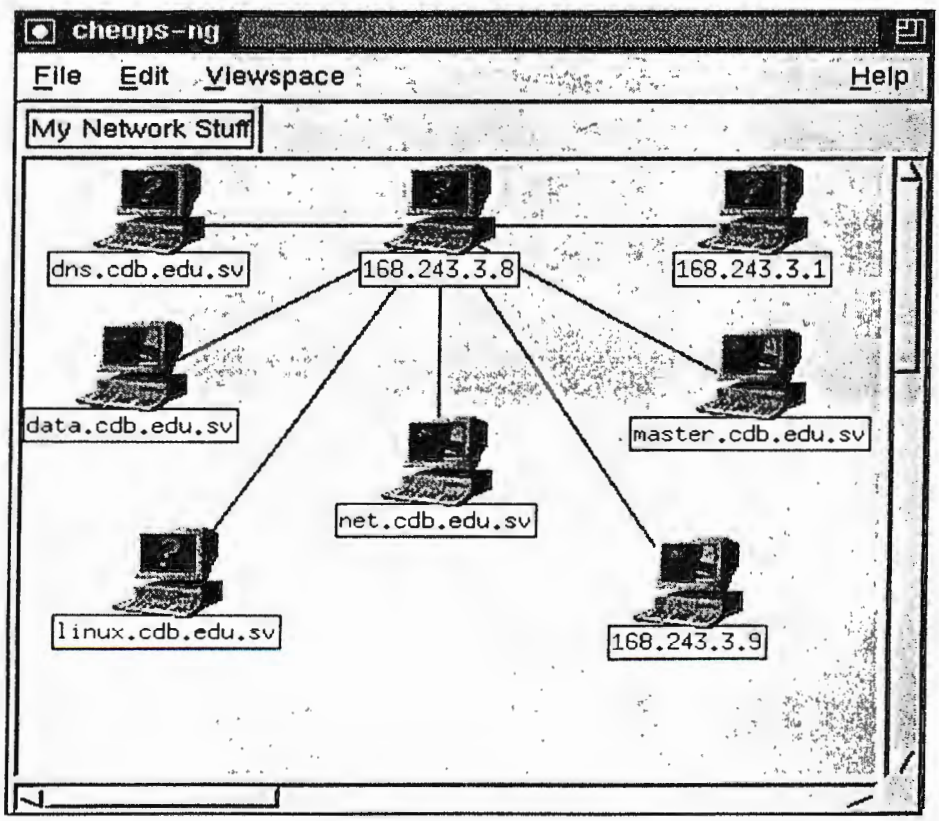


Fig. 7-3. Host descubiertos por el agente que opera Cheops-ng

Vista de los servicios que se están ejecutándose en los host descubiertos, figura 7-4:

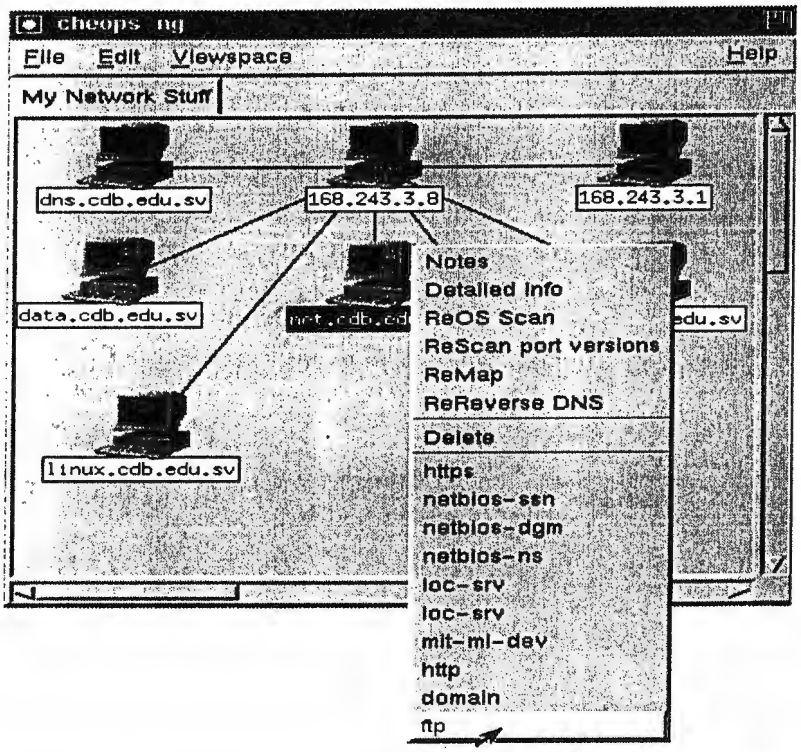


Fig. 7-4 Lista de servicios que se ejecutan en el host "net.cdb.edu.sv".

La Figura 7-5 muestra el resumen del sistema operativo, Nombre DNS, dirección IP, y los servicios que se ejecutan en un host específico. Para el ejemplo: data.cdb.edu.sv.

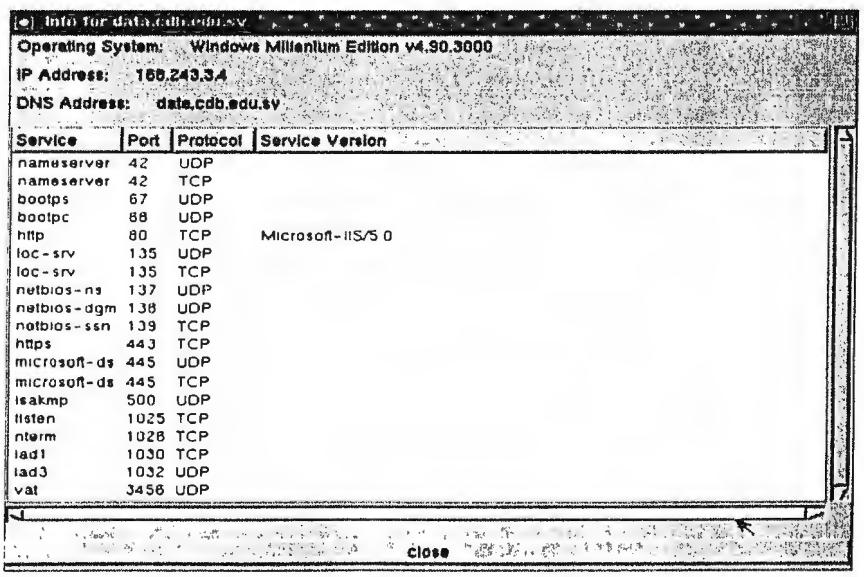


Fig. 7-5 Información referente al host data.cdb.edu.sv.

A partir de la clasificación de monitores de red, es posible clasificar al monitor cheops-ng según:

- **Objetivo:** Principalmente es un monitor de estado de variables, ya que no entrega reportes del tráfico en la red.
- **Reporte:** Histórico.
- **Intrusividad:** se considera intrusivo, ya que usa la red para obtener las variables.
- **Operación:** Local.
- **Protocolos:** básicamente la pila de protocolos TCP/IP.

Las ventajas y desventajas del cheops next generation se presentan en seguida:

Ventajas:

- Posee una plataforma de trabajo muy simple para la administración, donde entrega información de estado de los servicios.
- Realiza monitoreo de Servicios básicos de una red.
- La instalación no es complicada.

Desventajas:

- Es claramente un monitor de estado de servicios, por lo que no está destinado a medir en tiempo real ninguna clase de tráfico.
- A pesar que se menciona en la descripción de sus características, la capacidad para detectar el sistema operativo del host, esto es una tarea que no realiza a la perfección.
- Para obtener datos es necesario estar pendiente de la computadora donde se encuentra instalado, debido a que no posee las capacidades de administración y visualización remota.

Cheops Ver. 0.59.

Es una herramienta útil para detectar el sistema operativo de un host y manejar un gran número de hosts rápidamente. El Cheops construye una imagen de un dominio, o bloque IP, que está ejecutando cada host y así sucesivamente. Es extremadamente útil para preparar un escaneo inicial, pues se pueden localizar elementos interesantes (Impresoras, routers, etc) con rápidez. Cheops provee al administrador de red una buena herramienta para localizar, accesar, diagnosticar y administrar recursos de red.

Al igual que su sucesor cheops-ng, Posee una funcionalidad de descubrimiento automático de red y de hosts, así como también la capacidad de detectar el sistema operativo que se ejecuta en la estación de trabajo monitoreada.

Las características principales que presenta cheops son:

1. Son utilizados paquetes simples de ICMP "ping", para el descubrimiento inicial de la red y de los host que se encuentran activos dentro de dicha red.

2. Transferencia de nombres de dominio son utilizados para listar los host de un dominio o rango de IP´s.

3. El descubrimiento del sistema operativo que se ejecuta en un host es realizado gracias al programa de monitoreo "queso".

4. El mapeo es hecho utilizando paquetes UDP (u opcionalmente ICMP) con pequeños valores de time-to-live (traceroute y mtr, respectivamente).

Instalación de cheops Ver 0.59

1. Copie el paquete cheops-0.59.tar al directorio /usr/local/
2. Descomprima el paquete: tar –xvf cheops-0.59
3. Cambie al directorio /usr/local/cheops-0.59/
4. Ejecute el comando ./configure
5. Ejecute el comando make
6. Ejecute el comando make install
7. Inicie una sesión gráfica de Linux : startx

Ejecución.

Ejecutar con el usuario root (realizarlo en la interfaz grafica de Linux. GUI):

1. Abrir una termial de emulación.

2. Comando: cheops ó ./cheops *(Ejecutan el programa y la consola de administración).*

Al ejecutar la línea de comando anterior, cheops inicia haciendo la pregunta si se desea que automáticamente se descubran los host de la red o si se hará esta tarea de manera manual(Ver Fig 7-6).

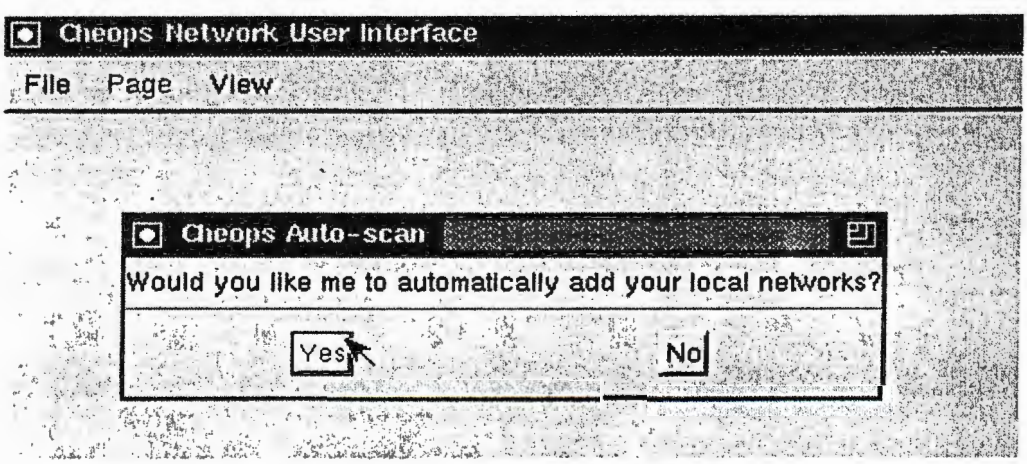


Fig. 7-6. Ventana de elección de modo de descubrimiento automático

A continuación la gráfica 7-7 muestra el mapa de hosts que fueron descubiertos por cheops en la red 168.243.3.0 (Red Centro de Cómputo UDB).

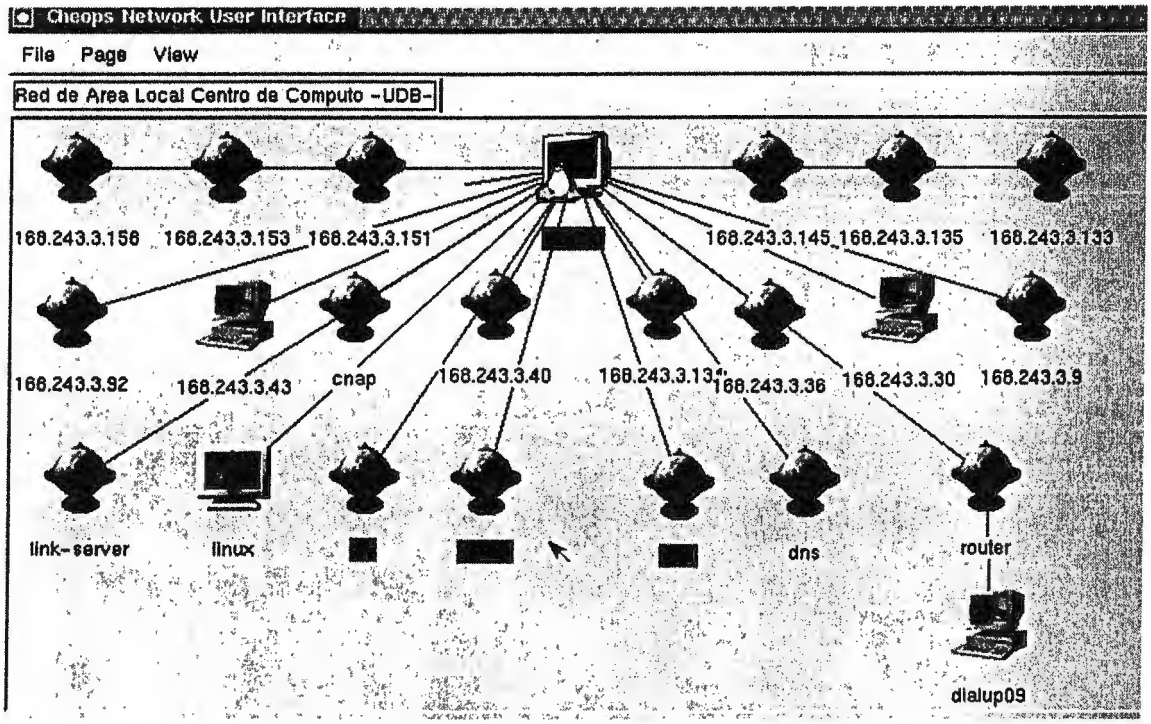


Fig. 7-7. Host descubiertos por Cheops en la red 168.243.3.0

Con el fin de monitorear los servicios de un host específico, la figura 7-8 muestra los servicios que serán "vigilados" en el host net.cdb.edu.sv.

En el ejemplo se establece el monitoreo para los servicios: FTP y Web Server. De tal forma que si alguno de estos falla, cheops reportará dicho error.

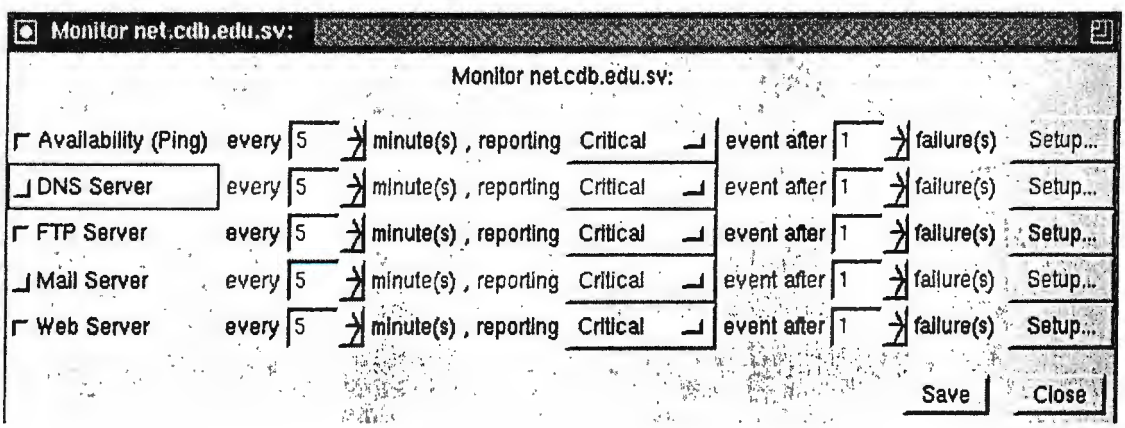


Fig 7-8. Servicios a monitorear en un host específico

En la gráfica 7-9 se muestra la detección de un error en los servicios que se monitorean en el host net.cdb.edu.sv, véase que el host con problemas se señala con un distintivo de color rojo.

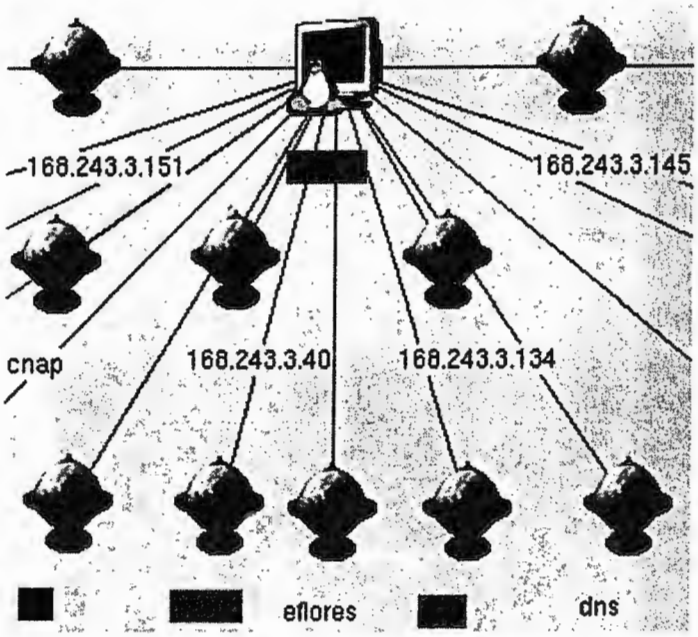


Fig. 7-9. Detección de una falla en el host "net"

A continuación la gráfica 7-10 muestra el "*event log*" para el suceso detectado por cheops en el host net.cdb.edu.sv, obsérvese que se reporta un error de nivel crítico para el servicio FTP que debiese estar ejecutándose en dicho host.

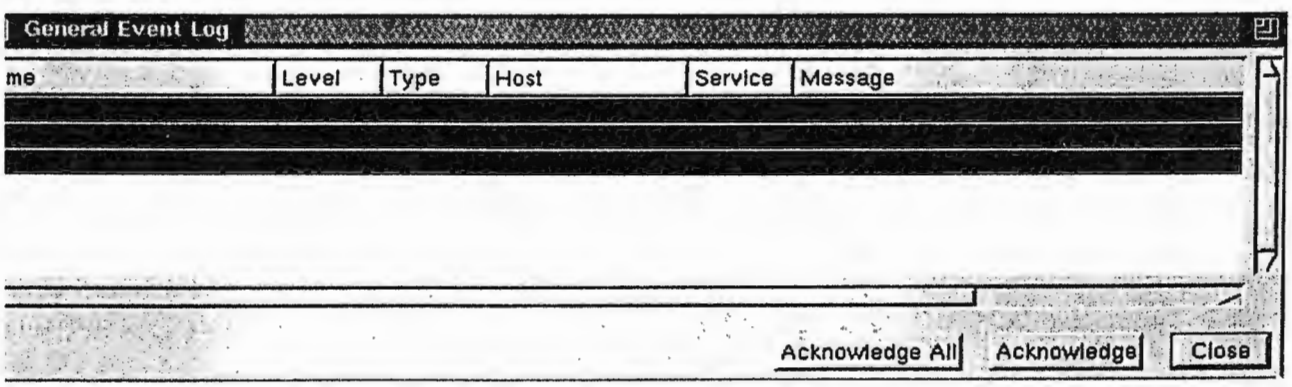


Fig. 7-10. Descripción del error suscitado en el host

A partir de la clasificación de monitores de red, es posible clasificar al monitor cheops según:

- **Objetivo:** Principalmente es un monitor de estado de variables, ya que no entrega reportes del tráfico en la red.
- **Reporte:** Histórico en su mayoría, En el caso de alarmas y caídas de servicio son realizadas en tiempo real.
- **Intrusividad:** se considera intrusivo, ya que usa la red para obtener las variables.
- **Operación:** Local.
- **Protocolos:** básicamente la pila de protocolos TCP/IP.

Ventajas: Similarmente a su homólogo Cheops Next Generation.

- Posee una plataforma de trabajo muy simple para la administración, donde entrega información de estado de los servicios.
- Realiza monitoreo de Servicios básicos de una red.
- La instalación no es complicada, no necesita de configuración adicional.

Desventajas:

- Es claramente un monitor de estado de servicios, por lo que no está destinado a medir en tiempo real ninguna clase de tráfico.
- No permite la administración y visualización remota.

Sintaxis: nmap [Tipos(s)de escaneo] [Opciones] <servidor o red #1 ... [#N]>

Escaneo de puertos.

El escaneo de puertos es una técnica para descubrir canales de comunicación aprovechables en un servidor, mediante las herramientas apropiadas es posible realizar un análisis y posterior reporte de los puertos abiertos del sistema objetivo. Esta técnica consiste en realizar un *scan* o barrido de un host o grupo de ellos de manera de obtener un listado con sus puertos abiertos, muchas veces esta información es crucial al momento de diagnosticar la seguridad de un host ya que sabiendo los puertos que atiende es posible determinar los ataques a los que esta expuesto. El origen de esta técnica se remonta antes de la aparición de Internet y del uso masivo de computadoras, se usaba esta técnica para descubrir números telefónicos no incluidos en guía, detrás de los cuales se encontraba a la escucha computadoras, probando sistemáticamente números bien al azar o de forma secuencial, uno de los sistemas mas famosos en su época fue Toneloc que usaba el modem para discar en busca de una computadora que contestara desde el otro lado de la línea.

Con la aparición de Internet llegaron también los ataques a los servidores, esta vez lo que se escanea son los puertos abiertos del host.

Nmap es un software diseñado para permitir a los administradores de sistemas el monitoreo de redes, determinar que servidores se encuentran activos y que servicios ofrecen. Nmap soporta un gran número de técnicas de escaneo tales como: UDP, TCP Conect() (simplemente tratar de abrir una conexión como es habitual), TCP Syn (escaneos SYN semi-abiertos), ICMP. Entre otras características nmap presenta la capacidad para la detección remota del sistema operativo de un host, detección de servidores inactivos por medio de pings paralelos, detección de filtrado de puertos, entre otras.

Compilación e Instalación de NMAP.

Una vez que se obtiene el paquete de http://www.insecure.org/ se debe descomprimir, para ello se usa el programa *tar* de la siguiente manera:

```
[root@intruder]/install # tar -xvfz  nmap-2.54.tgz
map-2.12/
nmap-2.12/nmap.c
nmap-2.12/targets.c
nmap-2.12/tcpip.c
nmap-2.12/error.c
nmap-2.12/utils.c
...continua...
```

Con ésto se obtiene un directorio llamado nmap-2.54 dentro del cual se encuentra el código fuente en C y la documentación del programa.

La compilación de este programa es sencilla y no debe representar mayores problemas, se describen a continuación los pasos necesarios:

1. Ingresar al directorio nmap-2.54 o el que corresponda segun la versión del programa.

2. Ejecutar el script de configuración *configure* no olvidar especificar la ruta mediante el símbolo "*./* ", de manera que quede *./configure*, con este script se verifica la existencias de las librerías necesarias y se crearan los archivos *config-status*, *Makefile* y *config.h* necesarios para la generación de los ejecutables.

3. Mediante la utilidad *make* se procede a la compilación en si, primero se compila la librería libpcap y luego el programa nmap.

4. Finalmente se procede a la instalación del ejecutable y de sus librerías y páginas del manual en línea de Linux con *make install,* con esto se obtiene el

archivo nmap en el directorio */usr/local/bin*, no olvidar que este directorio debe estar en el path para que su contenido pueda ser invocado desde cualquier lugar, si así no fuere, bien puede cambiar de lugar el programa o agregar el directorio a la variable de entorno PATH.

OPCIONES.

En general, pueden combinarse aquellas opciones que tengan sentido en conjunto. Algunas de ellas son específicas para ciertos modos de escaneo. A continuación se presentan las opciones más representativas.

Tipos de Escaneo

-sT → Escaneo TCP connect(): Es la forma más básica de escaneo TCP. La llamada de sistema connect() proporcionada por el sistema operativo se usa para establecer una conexión con todos los puertos de la computadora(Fig.7-11).

```
[root@monitor bin]# nmap -sT 168.243.3.4

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on data.cdb.edu.sv (168.243.3.4):
(The 1540 ports scanned but not shown below are in state: closed)
Port       State       Service
42/tcp     open        nameserver
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        listen
1026/tcp   open        nterm
8080/tcp   open        http-proxy

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
[root@monitor bin]#
```

Fig. 7-11. Scaneo de puertos por nmap.

-sP → Escaneo ping: A veces únicamente se necesita saber que servidores en una red se encuentran activos. Nmap puede hacer esto enviando peticiones de respuesta ICMP a cada dirección IP de la red que se especifica(Fig. 7-12).

```
[root@monitor bin]# nmap -sP 168.243.3.30

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host  (168.243.3.30) appears to be up.

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
[root@monitor bin]#
```

Fig. 7-12. prueba ping por medio de nmap.

-sO → Escaneo de Protocolo IP: Esta opción es para determinar que protocolos IP son soportados por el host(Fig. 7-13).

```
[root@monitor bin]# nmap -sO 168.243.3.4

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting protocols on data.cdb.edu.sv (168.243.3.4):
(The 251 protocols scanned but not shown below are in state: closed)
Protocol    State       Name
1           open        icmp
2           open        igmp
6           open        tcp
17          open        udp


Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
[root@monitor bin]#
```

Fig. 7-13. Lista de protocolos IP ejecutándose.

-O → Esta opción activa la detección remota del sistema operativo por medio de TCP/IP.

```
[root@monitor bin]# nmap -O 168.243.3.8

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on monitor.cdb.edu.sv (168.243.3.8):
(The 1530 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
5901/tcp   open        vnc-1
6001/tcp   open        X11:1
6666/tcp   open        irc-serv

Remote operating system guess: Linux 2.1.19 - 2.2.17
Uptime 0.380 days (since Sun Dec 30 10:27:44 2001)

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

Fig. 7-14. Detección remota del sistema operativo.

A partir de la clasificación de monitores de red, es posible clasificar Nmap según:

- **Objetivo:** Monitor de estado, presenta estado de variables como Servicios y puertos disponibles en los hosts monitoreados.
- **Reporte:** Tiempo real, provee el reporte en modo texto, a cerca de los puertos disponibles en un determinado host.
- **Intrusividad:** No intrusivo.
- **Operación:** Local.
- **Protocolos:** Protocolos TCP/IP.

Ventajas:

- Representa una herramienta efectiva contra los ataques a los servidores.
- Es capaz de monitorear hosts que no pertenecen a la red a la que está adicionado el monitor de red.

Etherape Ver 0.8.2

Etherape es un monitor de red gráfico creado para sistemas operativos UNÍX. Despliega gráficamente la actividad de la red, donde el tráfico generado por cada protocolo se identifica con un color específico. Etherape soporta Ethernet, FDDI, Token Ring, ISDN, PPP y SLIP.

Entre las características más destacables de etherape se encuentran:

- El tráfico de red es desplegado gráficamente. El nodo que genera mayor tráfico ilumina mayormente la zona gráfica que representa la red, con el color del protocolo que utilice.
- El tráfico puede ser capturado en tiempo real desde interfaces: ethernet, FDDI, PPP y SLIP
- Los siguientes tipos de frames y paquetes son soportados en la versión actual de etherape: ETH_II, 802.2, 803.3, IP, Ipv6, ARP, X25L3, REVARP, ATALK, AARP, IPX, VINES, TRAIN, LOOP, VLAN, ICMP, IGMP, GGP, IPIP, TCP, EGP, PUP, UDP, IDP, TP, IPV6, ROUTING, RSVP, GRE, ESP, AH, ICMPV6, EON, VINES, EIGRP, OSPF, ENCAP, PIM, IPCOMP, VRRP; La mayoría de servicios TCP y UDP, TELNET, FTP, HTTP, POP3, NNTP, NETBIOS, IRC, DOMAIN, SNMP, etc.
- El despliegue de los datos pueden ser depurados utilizando un filtro de red.

Instalación de Etherape Ver 0.8.2

Dentro el directorio en que se encuentran los archivos de instalación del programa etherape:

1. Copie el paquete etherape-0.8.2 al directorio /usr/local/
2. Descomprima el paquete: tar –xvf etherape-0.8.2
3. Ejecute el comando ./configure
4. Ejecute el comando make
5. Ejecute make check

6. Ejecute make install
7. Ejecutar con el usuario con derechos root (realizarlo en la interfaz grafica de Linux. GUI):
    1. Abrir una emulación de terminal.
    2. Ejecutar: etherape

La gráfica 7-15, presenta la interfaz etherape, la pantalla fue capturada desde la ejecución de etherape dentro de la red 168.243.3.0

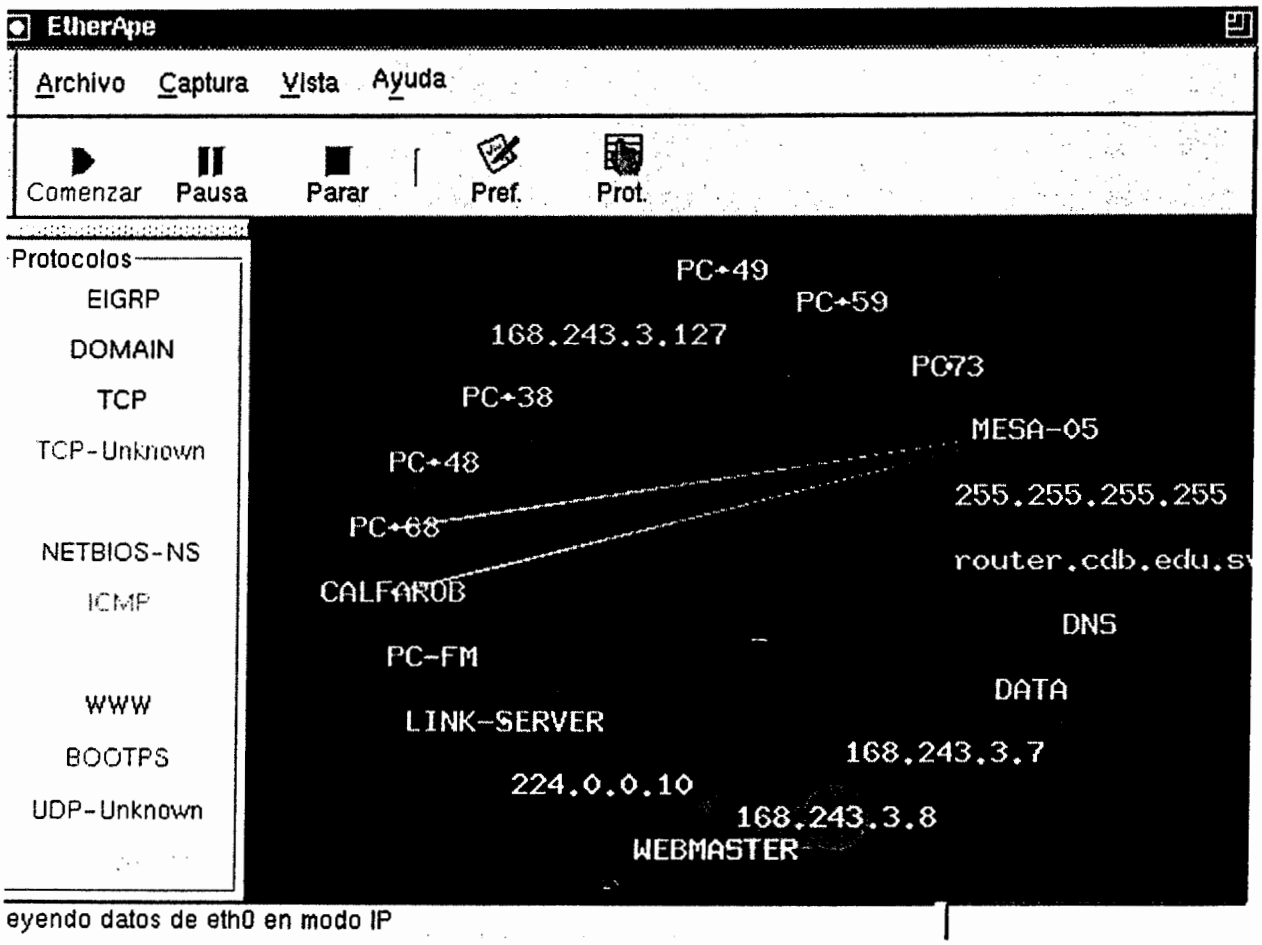


Fig. 7-15. Interfaz Etherape, ejecutándose en la red 168.243.3.0

La figura anterior muestra el tráfico y los enlaces que existen dentro de la red 168.243.3.0 y cada color representa a un protocolo en particular. Los protocolos en tráfico se muestran en la parte izquierda de la imagen, en este ejemplo se

destacan protocolos y servicios como: TCP, EIGRP, TELNET, ICMP, BOOTP, WWW, UDP, NETBIOS, entre otros.

Además, es posible obtener un resumen través de la ventana de protocolos, para el ejemplo en cuestión se presenta:

EtherApe: Protocolos

Columnas

Protocolo	Tráfico Instant.	Tráfico Acumul.	Última vez	Paquetes
TCP-Unknown	197,958 Kbps	12,555 Mbytes	hace 0"	24728
TCP	3,062 Kbps	435,033 Kbytes	hace 0"	7679
SMB	2,132 Kbps	136,896 Kbytes	hace 2"	601
NETBIOS-NS	1,207 Kbps	111,656 Kbytes	hace 2"	1191
EIGRP	375 bps	32,145 Kbytes	hace 1"	422
BOOTPS	0 bps	17,766 Kbytes	hace 4"	56
DOMAIN	0 bps	68,329 Kbytes	hace 39"	595
WWW	0 bps	17,570 Kbytes	hace 39"	274
HYLAFAX	0 bps	626 bytes	hace 4'35"	7
UDP-Unknown	0 bps	65 bytes	hace 2'27"	1
ICMP	0 bps	21,792 Kbytes	hace 2'16"	371
NETBIOS-SSN	0 bps	16,131 Kbytes	hace 2'16"	257
TELNET	0 bps	17,652 Kbytes	hace 3'27"	268
AIM	0 bps	66 bytes	15:34	1
AUTH	0 bps	8,406 Kbytes	hace 3'27"	112
CHARGEN	0 bps	768 bytes	hace 4'39"	12

Fig. 7-16. Trafico de protocolos, detectado por Etherape.

Las diferentes columnas representan: el protocolo, la cantidad de tráfico en tiempo real que está siendo generado por el protocolo (Kb), la cantidad de tráfico (Mb) acumulado por protocolo, hace cuantos minutos se genero el último tráfico y por último la cantidad de paquetes en transferencia.

Para redes voluminosas (más de 50 hosts) la interfaz gráfica de etherape puede representar un verdadero caos para el administrador de la red ya que se vuelve casi una tarea imposible determinar que host genera determinado tráfico, por ejemplo la figura 7-17 que se presenta a continuación (datos obtenidos de la red 168.243.3.0 – Centro de cómputo UDB):

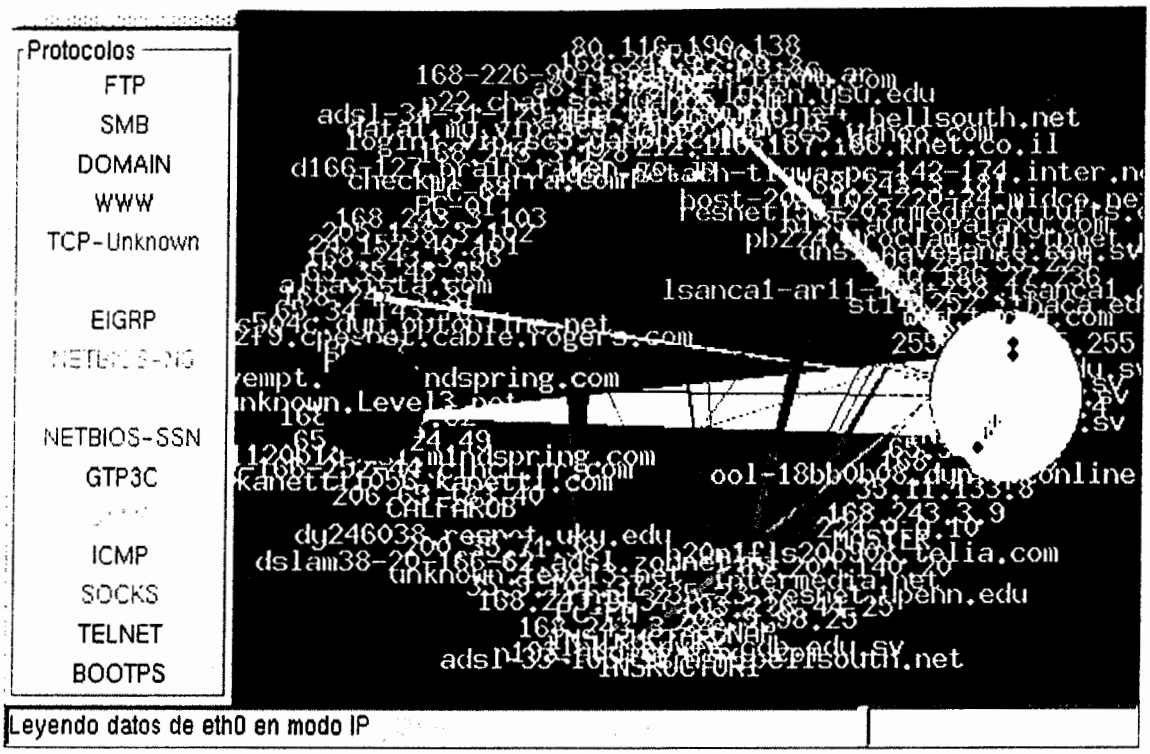


Fig. 7-17. Análisis de red de más de 50 host, un verdadero caos para analizar.

Definitivamente, este tipo de interfaz gráfica no resulta una herrmienta efectiva para la administración y monitoreo de una red.

A partir de la clasificación de monitores de red, es posible clasificar Nmap según:

- **Objetivo:** Monitor de tráfico (o conexiones), dado que al aumentar el tráfico de una conexión, el grosor de la línea aumenta.
- **Reporte:** Tiempo real.
- **Intrusividad:** No intrusivo.
- **Operación:** Local.
- **Protocolos:** Ethernet Versión II e IEEE 802.3. Protocolos TCP/IP.

Ventajas:

- Muestra las conexiones Ethernet punto a punto.
- Se puede capturar la pantalla para posterior análisis.

Desventajas:

- El tráfico se ve en forma cualitativa y no cuantitativa.
- El tráfico mostrado sólo corresponde al tráfico de la subred en la cual está conectado este monitor.
- No realiza registro de información o reportes históricos en forma automática.

Npulse Ver 0.54

Npulse es un monitor de red con una interfaz web, diseñado para sistemas operativos Linux y Unix. Es capaz de monitorear rápidamente decenas, centenas e inclusive miles de host, sitios o dispositivos a la vez en múltiples puertos.
Npulse está escrito en lenguaje Perl y viene acompañado de su propio servidor web. Además, en lugar de re-inventar código, Npulse utiliza algunos productos de distribución libre (código abierto GPL) como por ejemplo: nmap, Perl, OpenSSL, Java Telnet App y Net::SSLeay y Mail::Mailer

Instalación de npulse ver 0.54

Previamente a la instalación de npulse debe asegurarse que se cumple con el **software requerido** para su ejecución:

1. Linux/Unix Versión 2.1 ó superiores.
2. Perl Versión 5.004 ó inferiores.
3. Nmap Versión 2.51 ó inferiores.

Opcionalmente npulse puede hacer uso de:

1. OpenSSL Versión 0.9.6 ó superiores
2. Net::SSLeay Versión 1.0.4 ó superiores.
3. Mail::Mailer Versión 1.21 ó superiores.

Instrucciones para la instalación:

1. Como usuario root ejecutar el archivo de instalación: ./setup.sh
2. Seguir las instrucciones y contestar a las interrogantes que se le presentan.
   2.1 Directorio de instalación: [/usr/local/npulse]
   2.2 Directorio del archivo de configuración: [/usr/local/npulse/etc]
   2.3 Directorio para el archivo log [/usr/local/npulse/log]
   2.4 Directorio de datos [/usr/local/npulse/data]
   2.5 Se chequean si existen los software: traceroute y nmap`
   2.6 Operara en modo Seguro (SSL)? Por default [no].
   2.7 Npulse esta construido en Perl, se debe proveer la ruta completa donde se encuentra el interprete de Perl (Versión 5). [/usr/local/bin/perl]
   2.8 Npulse es capaz de monitorear automáticamente la red en un intervalo especificado, la opción por defecto es un intervalo de 20 minutos.
   2.9 Npulse permite administración vía Telnet. Habilitar soporte telnet? [SI].
   2.10 Puerto que se habilitara para npulse con la interfaz Web: 5500
   2.11 Digitar el password de administrador para npulse.
   2.12 Confirmar la contraseña
   2.13 Nombre del Web Server o su dirección IP: 168.243.3.8 (Para el caso)
   2.14 Finalización de instalación de archivos.

Ejecución del servicio npulse.

Para iniciar el servicio npulse se debe ingresar como usuario root al directorio **/etc/Npulse** y ejecutar el comando **./start**

Durante el proceso de instalación una de las interrogantes fue el puerto donde se ejecutaría el programa para el caso de este ejemplo se escogió el puerto 5500, el servidor web en el que se esta ejecutando es por lo tanto: http://168.243.3.28:5500/

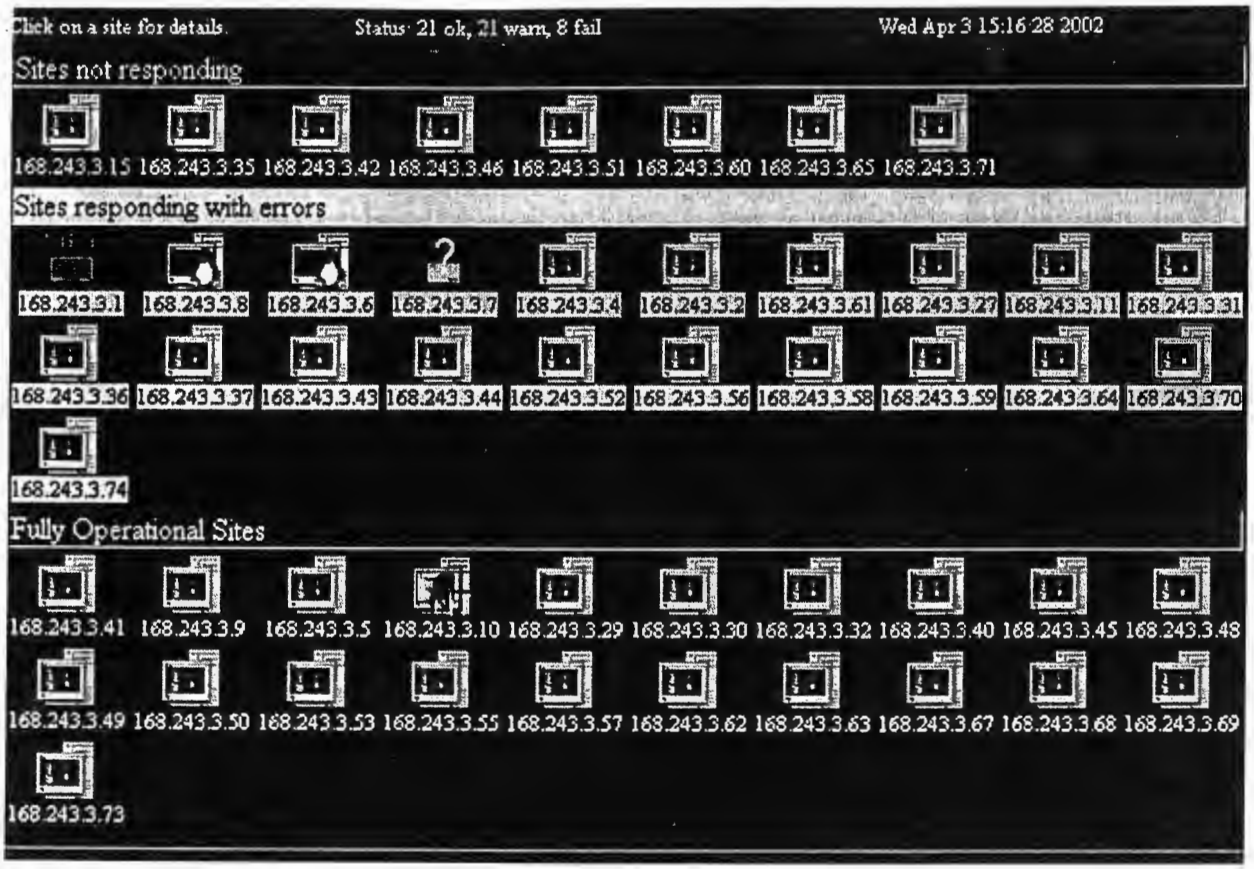


Fig. 7-18. Status de host en la red, definiendo su estado de acuerdo a colores.

La figura 7-18 muestra el estatus de los host que forman la red, estan divididos en tres grupos: los host que no responden en ninguno de sus servicios (se presentan en color rojo), los host que responden pero con algunos errores (representados por el color amarillo) y los host operando completamente sin problemas (representados por el color verde).

Nótese la capacidad de npulse para detectar el sistema operativo que se ejecuta en el host.

La grafica 7-19 muestra el estado de los servicios que se están ejecutando en cada host. Los servicios que son monitoreados npulse son: Telnet, FTP, SMTP, HTTP, finger, PPP, MySql, NetBios, tacacs, ping, POP3, entre otros.

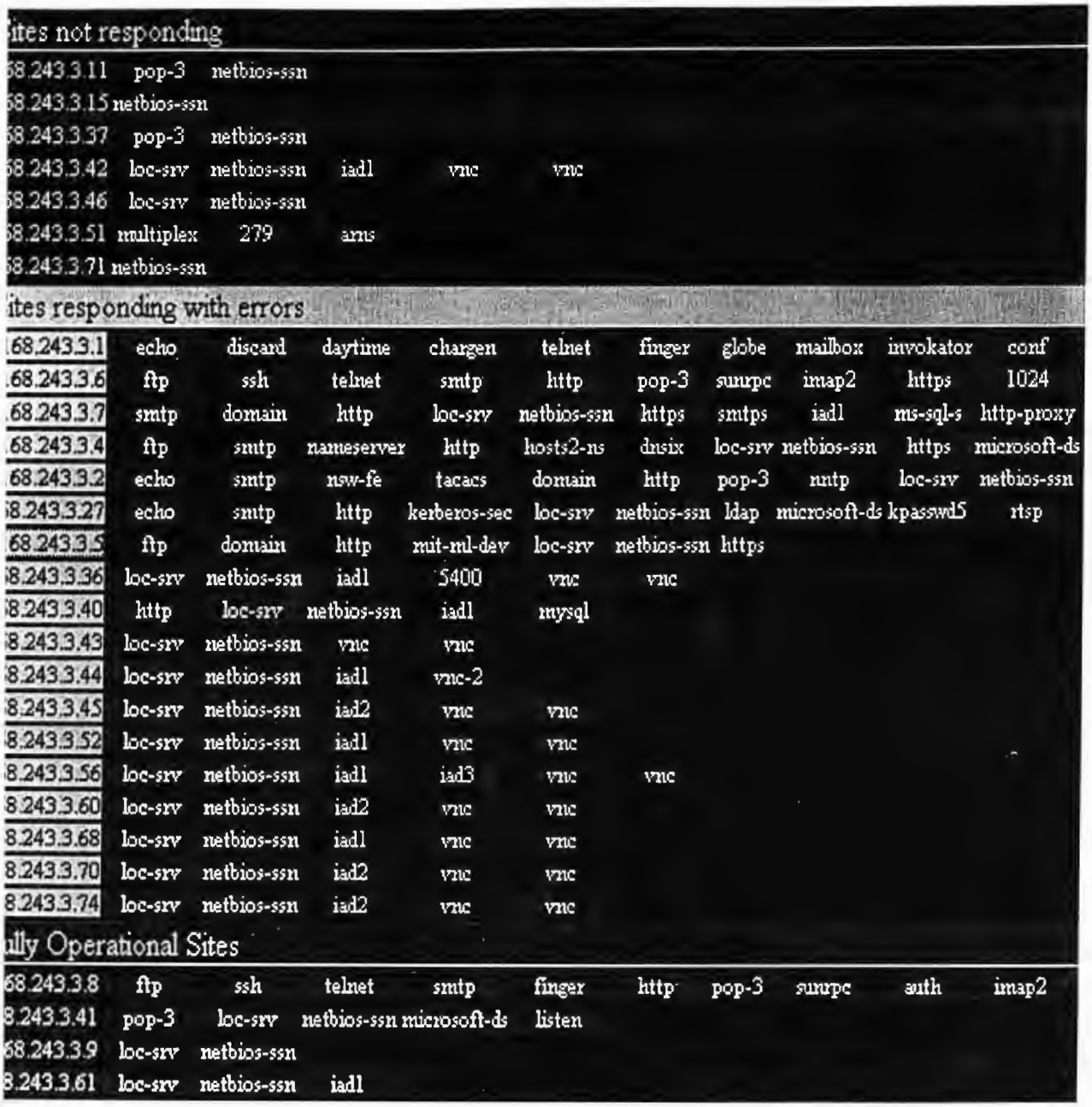


Fig. 7-19. Estado de los servicios en los hosts.

Npulse da la opción de ver el resumen de un host en particular, la figura 7-20 muestra en detalle lo que ocurre en el host 168.243.3.5 (net.cdb.edu.sv):

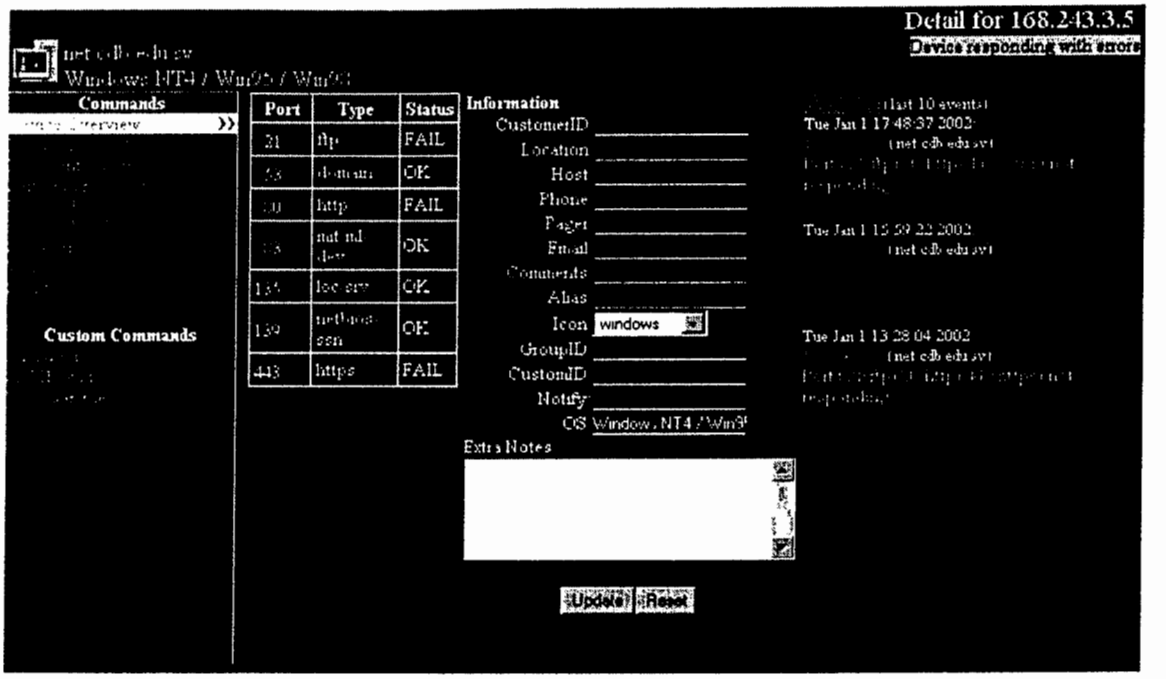


Fig. 7-20. Detalle del estado de los servicios e información general de un host.

Para el host 168.243.3.5, npulse informa que los servicios FTP y http experimentan fallas.

Además npulse es capaz de generar reportes históricos de manera gráfica del comportamiento de los hosts en la red, véase la figura 7-21:

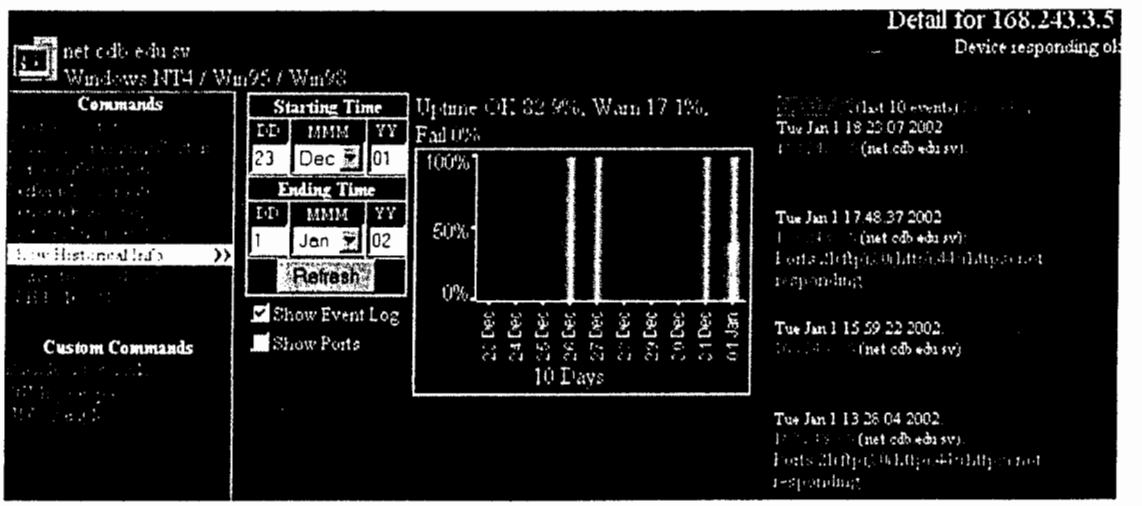


Fig. 7-21. Reporte histórico del comportamiento de un host específico

A partir de la clasificación de monitores de red, es posible clasificar Npulse según:

- **Objetivo:** Es un monitor de estado de variables, ya que no entrega reportes del tráfico en la red.
- **Reporte:** Tiempo Real Cuando ocurre un evento en los servicios monitoreados
- **Intrusividad:** se considera intrusivo, ya que usa la red para obtener las variables.
- **Operación:** Remota, es posible administrarlo y accesarla a través de un browser.
- **Protocolos:** Protocolos TCP/IP.

Ventajas:

- Capacidad para monitorear rápidamente cientos de servidores.
- Descubrimiento dinámico de la red en la cual está conectado.
- Interfaz web para el monitoreo remoto.
- Provee variados reportes sobre el estado de las variables monitoreadas.
- Incluye un reporte del comportamiento histórico de los hosts.

Desventajas:

- Funcionamiento inestable.

BCNU Versión 1.22 (Monitoreo Basado en Web)

Es una herramienta de administración de red, la cual, entrega información del estatus de los servicios que se ejecutan en los hosts. Este monitor usa un browser web para desplegar información acerca de los host de forma tabular. Con iconos de color muestra el estatus de los hosts en la red y los servicios que corren (ftp, http, telnet, smtp).

BCNU es capaz de administrar la red desde un sistema central UNÍX y monitorear los hosts a través de agentes los cuales se encargan de monitorear y entregar la información al servidor bcnu para que este lo despliegue en el browser.

Instalación.

1. Descomprimir el paquete, se sugiere hacerlo en la ruta /usr/local. Se creará una carpeta llamada bcnu donde se almacenaran los archivos de instalación y configuración del bcnu.
2. Cambiar al directorio /usr/local/bcnu
3. Ejecutar: ./Setup
4. Contestar a las interrogantes realizadas (se recomienda aceptar las opciones por defecto).
   4.1 Tipo de sistema en que se ejecutará *bcnu* será: [linux]
   4.2 El nombre de host maestro será: [monitor.cdb.edu.sv] (en este caso)
   4.3 El puerto en que se ejecutará *bcnu:* [6666]
   4.4 Se desea instalar un ejemplo de archivo de configuración para linux? [Si]
   4.5 Proveer la dirección de correo para la notificación en caso de alertas: [root@monitor.cdb.edu.sv] (para este caso).
   4.6 Copiando archivos de instalación y iniciando el servicio.

El servicio bcnu se ejecutará automáticamente cada vez que inicie el sistema operativo linux.

Para realizar una ejecución manual del servicio bcnu, es necesario ingresar a la ruta ***/usr/local/bcnu/etc/*** y ejecutar el comando ***./bcnud_server start***

Ahora que el servicio bcnu esta ejecutándose es necesario realizar la configuración del archivo **bcnunet,** el cual contiene la lista de los hosts que se desean monitorear dentro de la red y que servicios se vigilarán

El archivo **bcnunet** se encuentra en la ruta /usr/local/bcnu/etc. El siguiente es un ejemplo de configuración de este archivo, se configuró para la red del centro de cómputo de la Universidad Don Bosco, se han adicionado 6 hosts NT y dos hosts Linux.

```
# critical managed systems
 RETRIES=5
 SEVERITY=9
 ########################################
 BCNUHOSTTYPE=3       # NT
net      http     ftp
data     http     ftp
dns      http
master   http     ftp      telnet
fmorales         http     smtp
webmaster        ftp      http
 ########################################
 BCNUHOSTTYPE=1       # Unix
 linux     http  ftp   smtp   telnet
monitor   http        smtp
```

Para la revisión del estado de los servicios, es posible realizarlo accesando al servidor bcnu a través de una sesión web en un cualquier cliente.
La dirección para acceder es **http://host.dominio:6666/www/platforms.htm**
Para el ejemplo que se presenta a continuación:
http://monitor.cdb.edu.sv:6666/www/platforms.htm

Se presentan imágenes que explican de forma detallada la operación básica de este monitor. La figura 7-22 muestra el monitoreo realizado por bcnu, de acuerdo

a la configuración realizada sobre el archivo **bcnunet.** Muestra que están siendo monitoreados 8 host, de los cuales 6 son sistemas operativos NT y 2 sistemas Linux.

Los iconos con vivos verdes son los que ejecutan los servicios sin problema, los iconos con figuras rojas denotan problemas en determinados servicios. Al hacer clic sobre uno de estos iconos, se obtiene información más detallada.

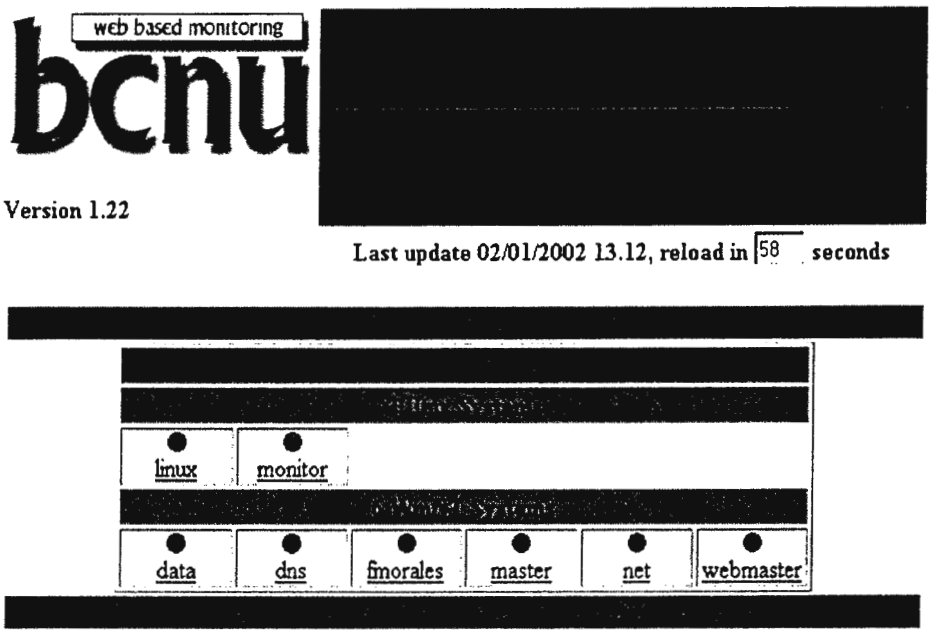


Fig. 7-22. Monitoreo sobre los host definidos en el archivo de configuración

De acuerdo a la información mostrada, los host *linux* y *net* no tienen ningún problema en sus servicios, mientras que los host restantes (*data, dns, fmorales, master y webmaster*), presentan problemas en su funcionamiento. Para obtener más detalles acerca de lo que está sucediendo en el host *dns*, se realiza un enlace y se obtiene el siguiente reporte:

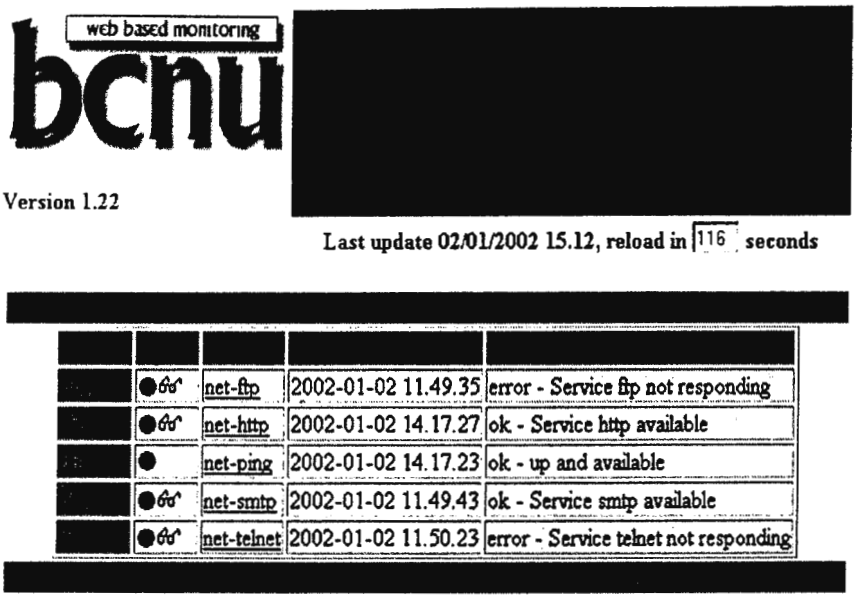


Fig. 7-23. Detalle del estado de servicios en el host "dns".

El reporte anterior indica problemas en el host *dns*, relacionado con los servicios telnet y ftp. Mientras que los servicios smtp, http se ejecutan satisfactoriamente.

A partir de la clasificación de monitores de red, es posible clasificar Npulse según:

- **Objetivo:** Es un monitor de estado de variables, ya que no entrega reportes del tráfico en la red.
- **Reporte:** Tiempo Real Cuando ocurre un evento en los servicios monitoreados
- **Intrusividad:** se considera intrusivo, ya que usa la red para obtener las variables.
- **Operación:** Remota, es posible administrarlo y accesarla a través de un browser.
- **Protocolos:** TCP/IP.

Ventajas:

- Interfaz web para el monitoreo remoto.
- El archivo de configuración no es complicado.

Desventajas:

- No posee Descubrimiento dinámico de la red en la cual está conectado.
- Interfaz de usuario poco seria.
- No ofrece reportes variados.

SAINT (Security Administrator's Integrated Network Tool)

Saint es una herramienta integrada para la administración de la seguridad en una red. Realiza un análisis de los host que pertenecen a la red para buscar vulnerabilidades en ellos y luego reporta los resultados en diferentes formatos a través de una interfaz web.

Saint puede hacer uso de software adicional como por ejemplo: *nmap,* si nmap está presente en el sistema, Saint lo utiliza para identificar el sistema operativo que se ejecuta en la estación, lo cual en algunos casos puede ayudar a determinar si un servicio es o no vulnerable.

Requerimientos para ejecutar Saint:

Antes de comenzar con el proceso de instalación de Saint, es necesario asegurarse que se cuenta con lo siguiente:

- Un sistema operativo Unix (Linux, Solaris, AIX, etc.).
- Perl 5.004 o superior (La versión más actualizada a la fecha es la 5.6.0 y puede ser obtenida desde **http://www.perl.com**).

- Un navegador Web (Mosaic, Lynx, Netscape, Cimera, etc.). Saint está diseñado para correr en modo grafico desde un navegador web aunque este también puede ejecutarse en modo texto, aunque su interfaz no es nada vistosa.
- Una computadora con suficiente recurso si se está planeando monitorear un gran número de hosts, ya que Saint esta diseñado para explotar al máximo los recursos del sistema.

Las siguientes utilidades son recomendadas para que estén instaladas en el sistema que ejecutará Saint, aunque este puede funcionar sin ellas:

- **nmap.** Utilizado para ayudar a identificar el tipo de sistema operativo que se ejecuta en el host y que además ayuda a Saint para buscar vulnerabilidades especificas de un sistema operativo. Se puede obtener la última versión de nmap e http://www.insecure.org/nmap

- **Utilidades Samba.** Usado para determinar los nombres Netbios y los recursos compartidos que existan en sistemas operativos Windows. Puede obtenerse en ftp://ftp.samba.org/pub/samba

Instalación de Saint.

1. Puede obtener Saint en la dirección http://www.saintcorporation.com/saint/
2. Descomprimir el paquete

   gunzip –c saint-3.5.8.tar.gz

   tar –xvf saint-3.5.8.tar
3. Ejecutar "./configure" .
4. Ejecutar "make" para compilar Saint.
5. Ejecutar "make install" para instalar la pagina man, para futuras ayudas.
6. Ejecutar Saint. Con la línea de comando "./saint"

Al ejecutar el comando en el punto 6, automáticamente se abrirá una sesión en el browser con la pagina web que se muestra en la figura 7-24.

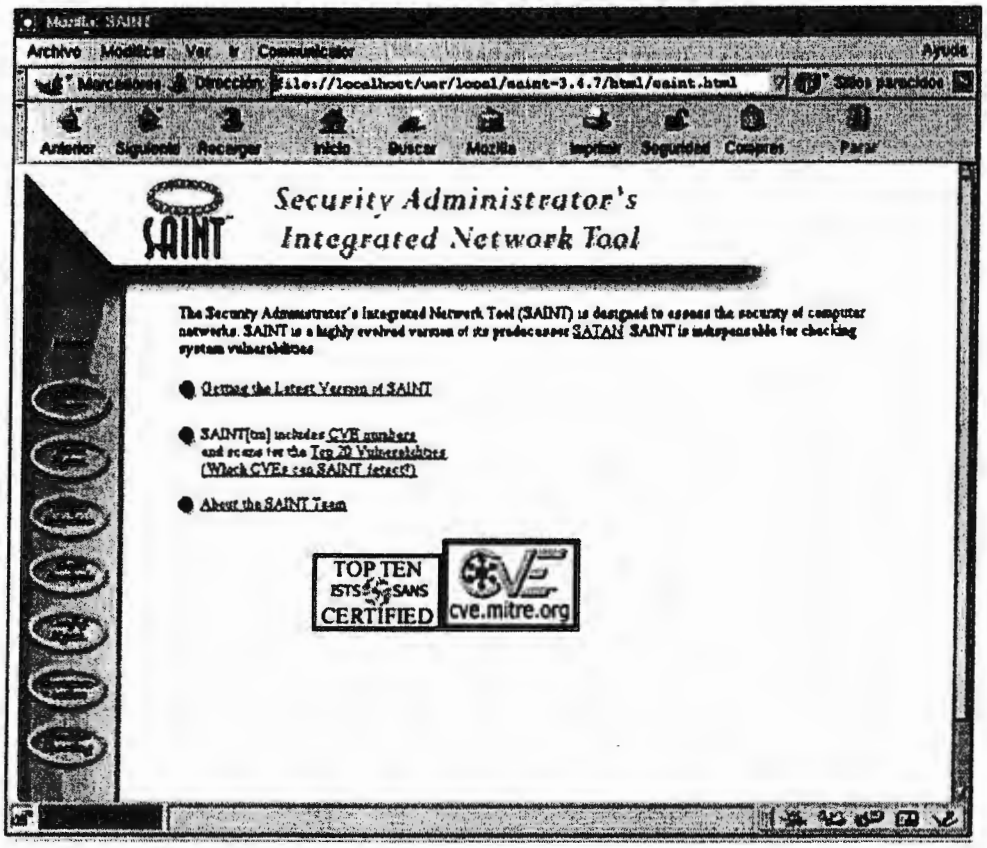


Fig. 7-24. Página inicial de SAINT.

En la figura 7-24, se muestra las opciones del menú principal de SAINT, entre estas opciones se destacan: administración de datos, selección de objetivos, análisis de datos y administración de la configuración, además de contar con secciones de documentación y de resolución de problemas.

El primer paso a realizar es construir el archivo de configuración, (administración de la configuración). La figura 7-25 muestra un ejemplo de archivo de configuración para SAINT.

Scanning levels and timeouts

What directory should I store the data in?

saint-data SAINT data directory

What probe level should I use?

- Light
- Normal
- Heavy
- Heavy+
- Top 20 (scans specifically for SANS Top 20 Internet Security Vulnerabilities)
- Custom: custom (Set up custom scan)

How many passwords should I guess against each account? (Values greater than 2 will lock out accounts on some systems. 0 disables password guessing.)

2 Password Guesses

What timeout values should I use?

150 Slow

120 Medium

Fig. 7-25. Modo de configuración de SAINT desde interfaz web.

Which of the above timeout values should I use for each SAINT check?

- Slow
- Medium
- Fast

What timeout values should I use for TCP and UDP port scans? (This value should be increased on slower networks to ensure that services are not missed.)

60 TCP Port Scan Timeout

60 UDP Port Scan Timeout

What is the maximum number of threads that can run concurrently? (Higher values result in faster scans but require much more memory. To disable multitasking, set this variable to 1.)

5 Maximum Threads

What signal should I send to kill a tool process when it times out?

9 Kill signal

How far out from the original target should I probe? (Under no circumstances should this be higher than "2" unless you're POSITIVE you know what you're doing!)

0 Maximal proximity

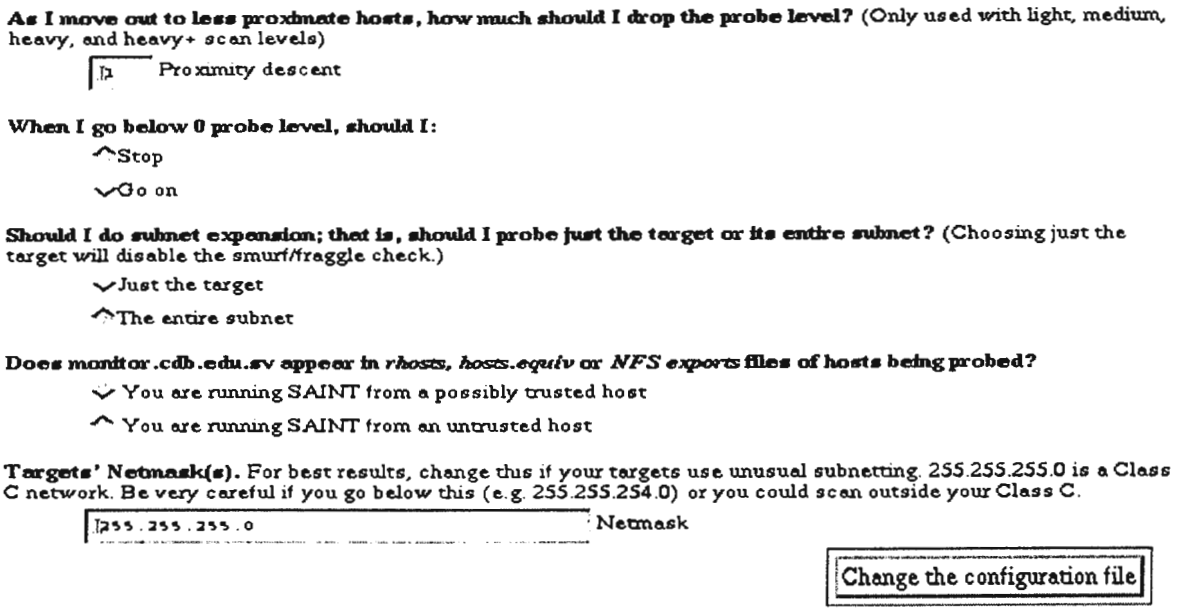


Fig. 7-25. Modo de configuración de SAINT desde interfaz web.

Una vez realizada la configuración, el siguiente paso es comenzar con el descubrimiento de la red, esto es posible desde la opción "selección de objetivo" o "target selection" la imagen 7-26 muestra la forma de hacerlo:

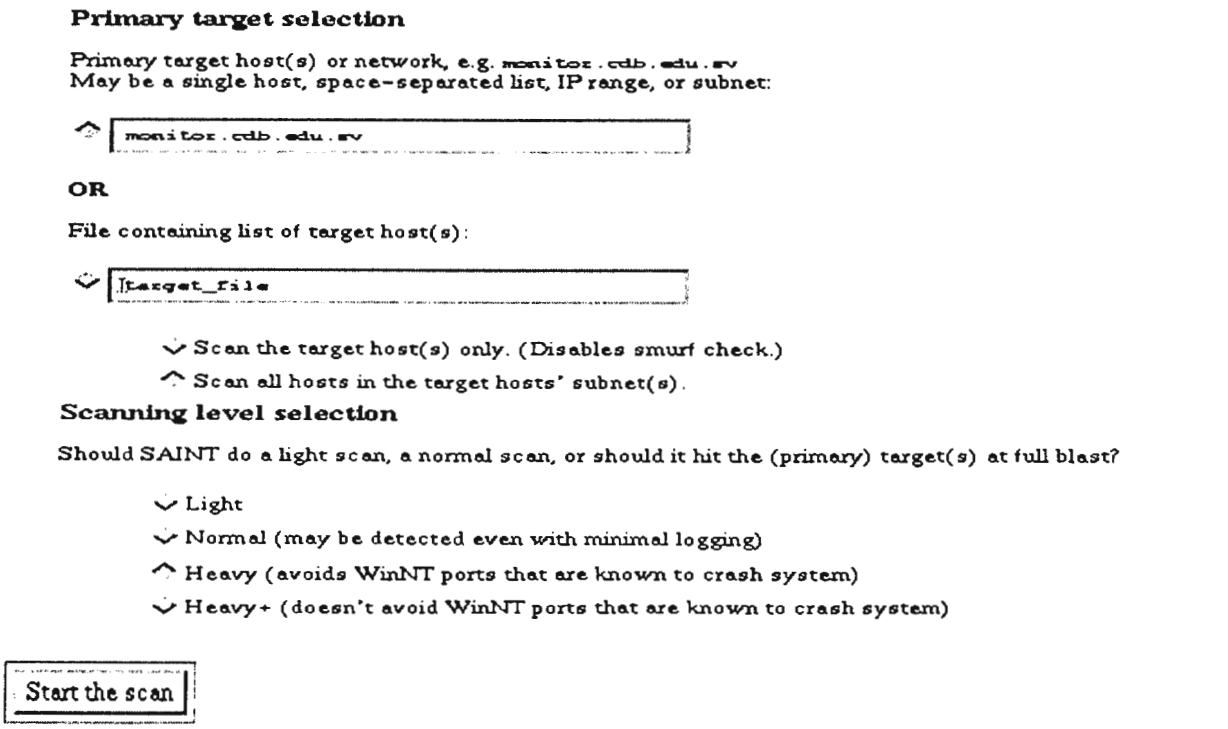


Fig. 7-26. Interfaz de configuración para el descubrimiento de la red.

Probablemente este procedimiento de escaneo de red tarde algunos minutos, no se debe de detener el proceso para que éste descubra todos los host y sus posibles vulnerabilidades. Una vez terminado el escaneo de la red es posible empezar a realizar el análisis de los datos y los host que fueron descubiertos por SAINT, en el proceso anterior.

Menú de SAINT para el análisis de datos (Data Analysis).

La interfaz principal de Saint, con la que es posible acceder a los diferentes reportes se muestra en la figura 7-27:

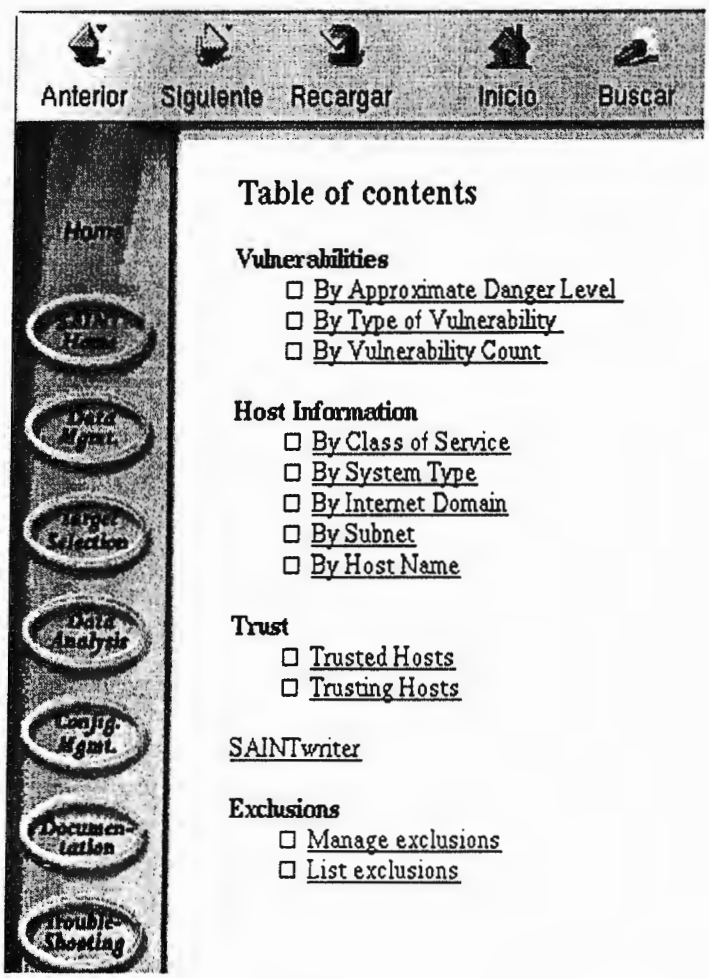


Fig. 7-27. Reportes para el análisis de los datos

Como se ve en la figura 7-27 Saint es capaz de dar varios tipos de reportes:

- Vulnerabilidades:
  - Por nivel de peligrosidad (Críticos, preocupantes y problemas potenciales).
  - Por tipo de vulnerabilidad.
  - Recuento de vulnerabilidades por host.

- Información de servicios en Host.
  - Por clase de servicio (DNS, FTP, IMAP, POP, SMB, SNMP, TELNET, WWW, etc.)
  - Por tipo de sistema operativo (Linux, Windows, Solaris, otros).
  - Por dominio de Internet.
  - Por subred.
  - Por nombre de host (a través de búsqueda).

Véase la figura 7-28, muestra el reporte por tipo de sistema operativo, detecta el numero de estaciones de trabajo que ejecutan Linux y las que poseen sistemas operativos Windows (NT, 2000, etc.)

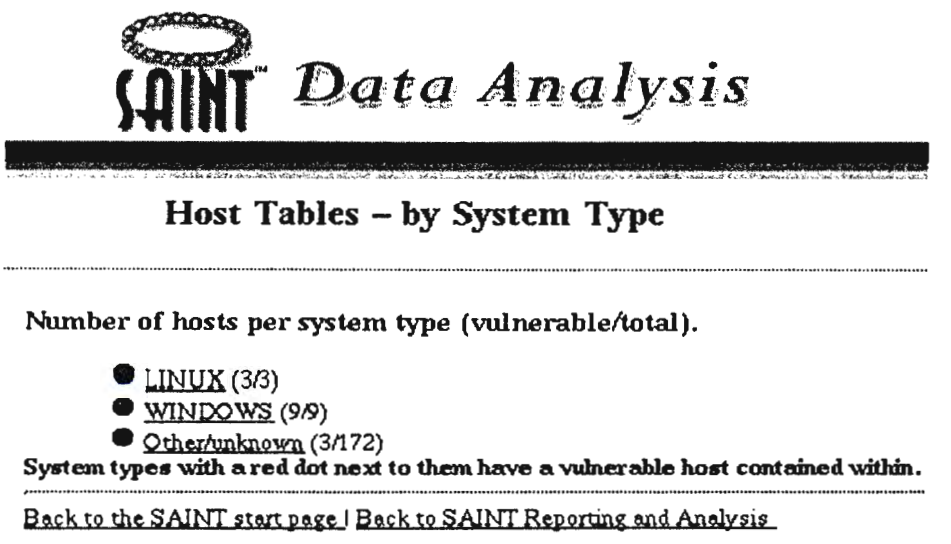


Fig. 7-28. Análisis de datos por tipo de sistema operativo

La figura 7-29 muestra el reporte sobre la estación de trabajo *cnap.cdb.edu.sv,* provee información como: sistema operativo, nombre Netbios, subred a la que pertenece, servicios de red que se ejecutan (DNS, ftp, WWW, SMTP). Además provee información a cerca de posibles vulnerabilidades que podrían dar lugar a un ataque por parte de hackers.

Results – cnap.cdb.edu.sv

General host information:

- Host type: Windows 2000
- Netbios Name: CNAP
- Subnet 168.243.3
- Scanning level: heavy
- Last scan: Mon May 13 19:02:36 2002

Network Services:

- DNS server
- SMB server
- SNMP server
- WWW server
- WWW (non-standard port 1029) server
- WWW (non-standard port 593) server
- WWW (non-standard port 9900) server
- 38 other services (show all services)

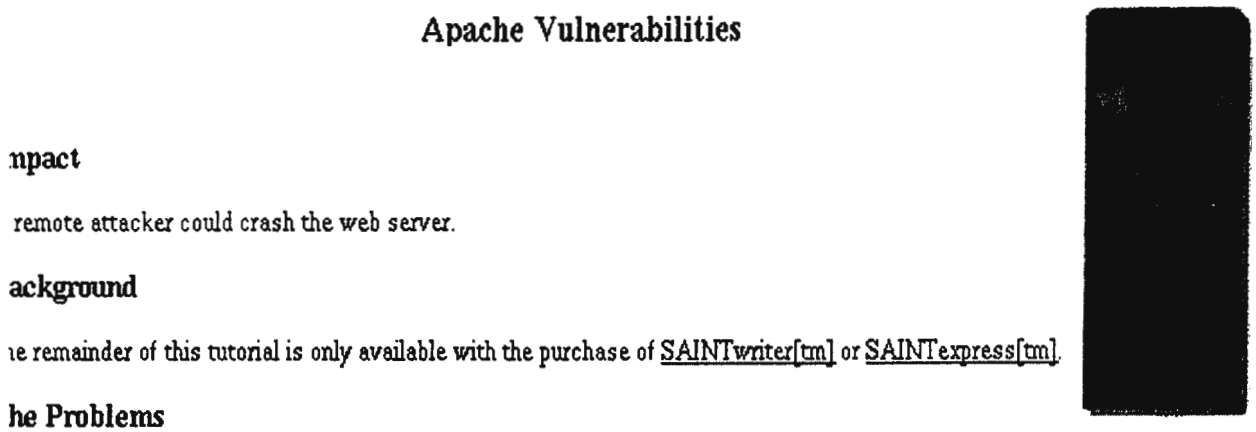
Vulnerability information: (Red: 1 Brown: 5)

- Possible vulnerability in ntpd (CVE 2001-0414) Ignore
- Denial of service in Apache . Ignore
- Is your Windows patched for DoS? Ignore
- Possible vulnerability in LDAP over SSL Ignore
- 

guessable read community string Ignore
- Is your LDAP secure? Ignore

Fig. 7-29. Análisis realizado sobre un Host en particular dentro de una red

La figura 7-30 muestra la vulnerabilidad detectada en el host *cnap.cdb.edu.sv* en el servidor web Apache en el que se advierte la posibilidad de un ataque remoto.



Apache Vulnerabilities

npact

remote attacker could crash the web server.

ackground

ıe remainder of this tutorial is only available with the purchase of SAINTwriter[tm] or SAINTexpress[tm].

he Problems

esolutions

/here can I read more about this?

Fig. 7-30. Vulnerabilidad detectada con peligro de ataque.

Las vulnerabilidades se pueden clasificar como críticas y se representan con una alerta roja, preocupantes con alerta amarilla y problemas potenciales , representados con una alerta de color café.

A partir de la clasificación de monitores de red, es posible clasificar SAINT según:

- **Objetivo:** Es un monitor de estado de variables, ya que no entrega reportes del tráfico en la red.
- **Reporte:** Tiempo Real Cuando ocurre un evento en los servicios monitoreados
- **Intrusividad:** se considera intrusivo, ya que usa la red para obtener las variables.
- **Operación:** Remota, es posible administrarlo y accesarla a través de un browser.

- **Protocolos:** TCP/IP.

Ventajas:

- Interfaz web para el monitoreo remoto.
- El archivo de configuración no es complicado de realizarlo, además posee una interfaz web para hacerlo.
- Provee información de vulnerabilidad en los sistemas, con el fin de evitar ataques a la red de parte de hackers.
- Descubrimiento dinámico de la red
- Ofrece una buena cantidad de reportes

Desventajas:

- La versión disponible gratuitamente no ofrece todas las capacidades, es necesario adquirir el software para sacar provecho de ellas.
- La estación de trabajo debe ser de gran capacidad ya que SAINT hecha mano de una gran cantidad de recursos.

MRTG (Multi Router Traffic Grapher)

El Graficador de Tráfico Multi Enrutador (Multi Router Traffic Grapher, MRTG) es una herramienta para monitorear la carga de tráfico en los enlaces de una red. El MRTG genera páginas HTML las cuales contienen gráficos GIF que proveen un representación visual EN VIVO de este tráfico.

PRINCIPALES CARACTERÍSTICAS:

- **Portable**

  El MRTG trabaja sobre la mayoría de las plataformas UNIX y sobre Windows NT.

- **Perl**

  El MRTG está escrito en Perl y viene con el código fuente completo.

- **SNMP Portable**

  El MRTG usa una implementación de SNMP altamente portable escrita completamente en Perl. No es necesario instalar ningún paquete de SNMP externo.

- **Soporte para SNMPv2c**

  El MRTG puede leer los nuevos contadores de 64bit de SNMPv2. No más enredos de contadores.

- **Confiable Identificación de Interfaces**

  Las interfaces de los enrutadores pueden ser identificadas por su dirección IP, Descripción y dirección Ethernet además del número de interfaz normal.

- **Bitácoras (logs) de tamaño constante**

  Las bitácoras del MRTG NO crecen. Gracias al uso de un algoritmo único de consolidación de datos.

- **Configuración Automática**

  El MRTG viene con un conjunto de herramientas de configuración las cuales hacen la configuración muy simple.

- **Gráficos libres de GIF**

  Los gráficos son generados directamente en formato PNG, usando la biblioteca GD.

- **Personabilidad**

  La apariencia de las páginas web producidas por el MRTG son altamente configurables.

El MRTG consiste en un programa en Perl que usa SNMP para leer los contadores de tráfico de los enrutadores y de un rápido programa en C el cual archiva los datos de tráfico y crea imágenes que representan el tráfico en la conexión de red monitoreada. Esos gráficos se insertan en páginas web que pueden ser vistas desde cualquier browser.

Además de una vista diaria detallada, el MRTG crea también representaciones visuales para el tráfico de los últimos siete días, las cuatro últimas semanas y los últimos doce meses. Esto es posible pues el MRTG mantiene un archivo de todos los datos que ha obtenido del enrutador. Este archivo es consolidado automáticamente, así que no crece con el tiempo, pero contiene todos los datos relevantes del tráfico de los últimos dos años. Todo esto se realiza de una manera eficiente. Por lo tanto, es posible monitorear 200 o más enlaces de red desde cualquier máquina con sistema operativo Linux.

El MRTG no está limitado al monitoreo de tráfico, es posible monitorear cualquier variable SNMP que se elija. Puede hasta usar un programa externo para recolectar datos que serán monitoreados por el MRTG. Organizaciones están usando el MRTG para monitorear cosas como Carga del Sistema, Inicio de Sesiones(logins), disponibilidad de módems y más.

PREPARACIÓN PREVIA A LA INSTALACIÓN:

A fin de compilar y usar el MRTG es necesario un compilador de C y una copia de perl instalado en la máquina. En la mayoría de los casos esto está ya disponible. De no ser este el caso, aquí hay algunos puntos para iniciar antes de dar un recorrido detallado por proceso de compilación completo.

GCC

El compilador de C de GNU, GCC, viene preinstalado en la mayoría de los sistemas operativos Linux. Para los derivados comerciales debe descargarse y compilarlo primero. Si no se tiene un compilador de GCC puede obtenerse en la dirección: http://gcc.gnu.org/

Perl

Amplias partes del sistema MRTG están escritas en el lenguaje Perl. Se debe asegurar que se tiene una copia reciente de Perl en la computadora. Al menos la versión 5.005 se requiere para que el MRTG trabaje bien. Se puede conseguir la última verisión de Perl en : http://www.perl.com/

El MRTG genera gráficos de tráfico en formato PNG. Para estar habilitado para hacer esto se necesitan bibliotecas de terceros. Cuando se compilen estas bibliotecas se deben compilar como bibliotecas estáticas no compartidas. Habrá mucho menos problema por delante si se hace así. Se debe hacer notar sin embargo, que varios Unix gratuitos tienen todas la bibliotecas requeridas ya instaladas. Así que no es necesario instalar otra copia. Para comprobarlo, es mejor saltar todas las instrucciones acerca de bibliotecas de abajo e ir directamente a la compilación del MRTG.

gd

Ésta es una biblioteca básica de dibujo de gráficos. Todas las versiones después de la versión 1.3 únicamente crea imágenes PNG. Esto es debido a que PNG es más eficiente y de patente libre. el MRTG puede trabajar con versiones viejas y nuevas de la biblioteca GD. Es posible obtener una copia reciente de GD de: http://www.boutell.com/gd/

libpng

Es requerida por gd para producir los gráficos PNG. Es posible obtenerla en http://www.libpng.org/pub/png/

zlib

Finalmente se necesita libpng para comprimir los gráficos que se crean. Obtener una copia desde:
http://www.info-zip.org/pub/infozip/zlib/

Y de último pero no de menor importancia se necesita también el MRTG por sí mismo. En caso que aún no se haya conseguido, puede encontrarse una copia en: http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/pub

COMPILACIÓN DE BIBLIOTECAS

En ésta sección se darán instrucciones de cómo compilar varias bibliotecas para la compilación del MRTG. Estas bibliotecas pueden estar ya instaladas si se tiene un sistema **BSD* o *Linux*. El programa **wget** usado más abajo es un simple descargador de web.

Primero se crea un directorio para la compilación. Note que esto puede ya existir en el sistema.

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

Si no se tiene zlib instalado:

```
wget http://ftp.info-zip.org/pub/infozip/zlib/zlib.tar.gz
gunzip -c zlib.tar.gz | tar xf -
mv zlib-?.?.?/ zlib
cd zlib
./configure
make
cd ..
```

Si no se tiene libpng instalado

```
wget http://www.libpng.org/pub/png/src/libpng-1.0.8.tar.gz
gunzip -c libpng-1.0.8.tar.gz |tar xf -
mv libpng-1.0.8 libpng
cd libpng
make -f scripts/makefile.std CC=gcc ZLIBLIB=../zlib ZLIBINC=../zlib
rm *.so.* *.so
cd ..
```

Y ahora, compilar gd

```
wget http://www.boutell.com/gd/http/gd-1.8.3.tar.gz
gunzip -c gd-1.8.3.tar.gz |tar xf -
mv gd-1.8.3 gd
cd gd
```

El caracter "\" al final de una línea significa que todo el siguiente material debería ser escrito en un única línea.

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

COMPILACIÓN DEL MRTG

Ahora todo está listo para la compilación del MRTG

```
cd /usr/local
gunzip -c mrtg-2.9.0pre31.tar.gz | tar xvf -
cd mrtg-2.9.0pre31
```

Si todas las bibliotecas han sido preinstaladas en el sistema es posible configurar el mrtg haciendo un simple: ./configure

De otro modo se debería tener algunas pistas acerca de dónde encontrar las librerías requeridas para compilar mrtg.

```
./configure --with-gd=/usr/local/src/gd      \
        --with-z=/usr/local/src/zlib     \
        --with-png=/usr/local/src/libpng
```

Configure estará seguro que el entorno se ajusta para construir el MRTG. Si él encuentra algún problema lo hará saber y dirá además qué hacer al respecto. Si todo está bien, se terminará con un Makefile personalizado para el sistema. Ahora escribir: make

Esto construirá un binario y editará todas las rutas de perl en los scripts. Todo el software requerido por el MRTG está ahora en el directorio *run*.

Puede borrarse en forma segura las bibliotecas que se compilaron arriba. Pero como sugerencia, se podrían mantener disponibles cuando se compile la próxima versión de MRTG.

CONFIGURACIÓN

El siguiente paso es configurar el MRTG para monitorear un dispositivo de red. Esto se hace al crear un archivo *mrtg.cfg* el cual define lo que se quiere monitorear. Por suerte no es necesario introducirse de lleno en empezar a escribir su propio archivo de configuración Junto con el MRTG hay una copia de **cfgmaker**. Este es un script que se puede apuntar a un enrutador y él creará un archivo de configuración de MRTG. El script lo encontrará en el directorio *run*.

CORRIENDO EL MRTG

Una vez que se ha creado el archivo de configuración, se puede intentar lo siguiente:

/usr/local/mrtg-2.9.0pre31/bin/mrtg /home/httpd/mrtg/mrtg.cfg

Esto hará una solicitud al enrutador y también creará el primer gráfico de tráfico y página de MRTG. Cuando se corre el MRTG por primera vez habrá una serie de quejas acerca de archivos log perdidos. Esto es normal para las dos primeras veces que se corre el MRTG.

Ejecutar el MRTG a mano no es lo ideal. Así que, se debe automatizar el proceso de corrida del MRTG en intervalos regulares (esto significa 5 minutos por defecto).

Se puede ya sea agregar el MRTG al crontab con una línea como esta:

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * \
    <mrtg-bin>/mrtg <path to mrtg-cfg>/mrtg.cfg
```

o si usted vive en la Tierra de Linux, la línea puede lucir como esta si usted está usando crontab -e

*/5 * * * * <mrtg-bin>/mrtg <path to mrtg-cfg>/mrtg.cfg

o como esta si usted usa */etc/crontab*

*/5 * * * * mrtg-user <mrtg-bin>/mrtg <path to mrtg-cfg>/mrtg.cfg

Usted puede también correr el MRTG como un demonio al agregar la línea RunAsDaemon: Yes al archivo de configuración del MRTG y creando un script de inicio en la secuencia de arranque de su sistema. Desafortunadamente, agregar un script de inicio difiere ampliamente entre los diferentes sistemas unix. Los modernos normalmente tienen un directorio llamado */etc/inid.d*, */etc/rc.d/init.d* donde usted pone scripts que inician el proceso que usted quiere correr cuando el sistema arranca. Además debe crear un enlace simbólico en */etc/rc3.d* o */etc/rc.d/rc?.d* llamado *S65mrtg* (este es sólo un nombre para muestra...es importante que empieza con S seguido de un número de dos dígitos.) Si no está seguro de esto, asegúrese de consultar la documentación de su sistema para que esté seguro que está bien.

Un script **mínimo** para poner en *init.d* podría lucir como este:

#! /bin/sh

cd /usr/local/mrtg-2.9.0pre31/bin

./mrtg /home/httpd/mrtg/mrtg.cfg

Note que esto sólo trabajará con **RunAsDaemon: Yes** en su archivo de configuración.

Accesando al MRTG vía web.

Una vez se ha instalado MRTG correctamente, es posible realizar el análisis a través de la interfaz web (véase figura 7-31), para este caso analizaremos la nterfaz ethernet del router de la Universidad Don Bosco y la Interfaz Serial0 del nismo equipo.

Para la interfaz Ethernet: **http://168.243.3.28/mrtg/168.243.3.1_1.html**

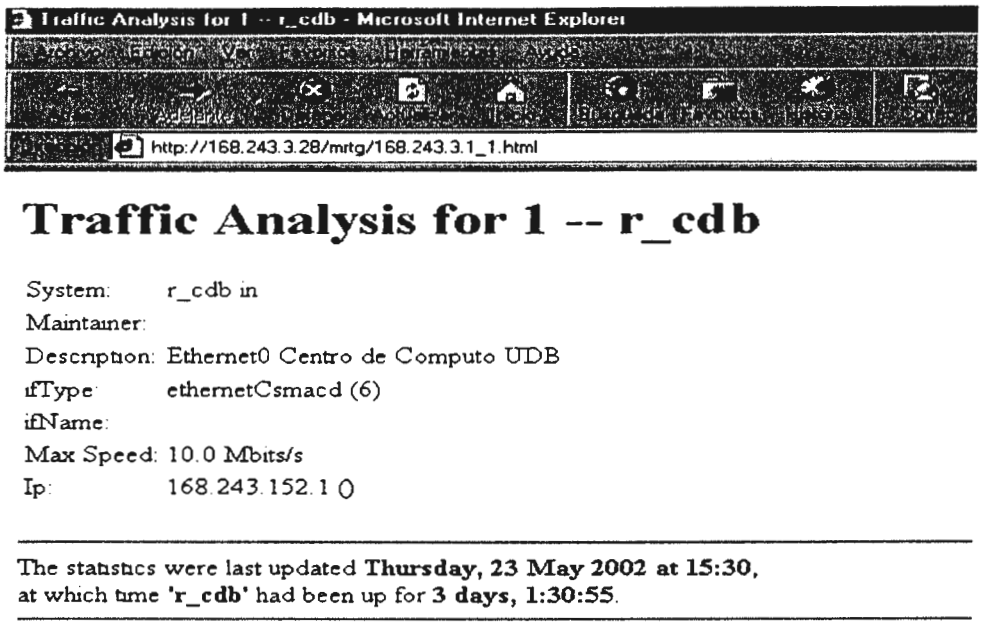


Fig. 7-31. Reporte descriptivo de la interfaz Ethernet del router de la UDB

La figura 7-31 muestra datos relevantes sobre la interfaz ethernet del enrutador, como los son su descripción, el tipo de interfaz (en este caso ethernet CSMA/CD), velocidad máxima y la dirección IP. La fecha de la última actualización de los datos y la fecha desde que la interfaz se encuentra "arriba".

La figura 7-32 muestra la actividad diaria del router en la interfaz Ethernet (en promedio, en un período de 5 minutos):

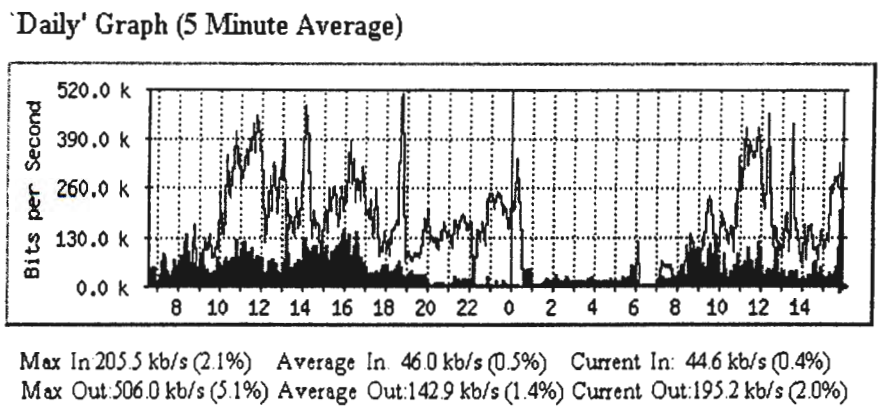


Fig. 7-32 Actividad de los últimos 5 minutos en la interfaz Ethernet.

Entre otros datos, se encuentra representado con color verde el tráfico de entrada: máximo, promedio y actual. El trafico de Salida se encuentra representado con color azul el tráfico de salida: máximo, promedio y actual.

Además, provee graficas semanales, mensuales y anuales (fig. 7-33, 7-34 y 7-35, respectivamente), del tráfico entrante y saliente, se muestran a continuación ejemplos de estas gráficas tomadas de la interfaz del router de la universidad Don Bosco:

Tráfico Semanal en Ethernet:

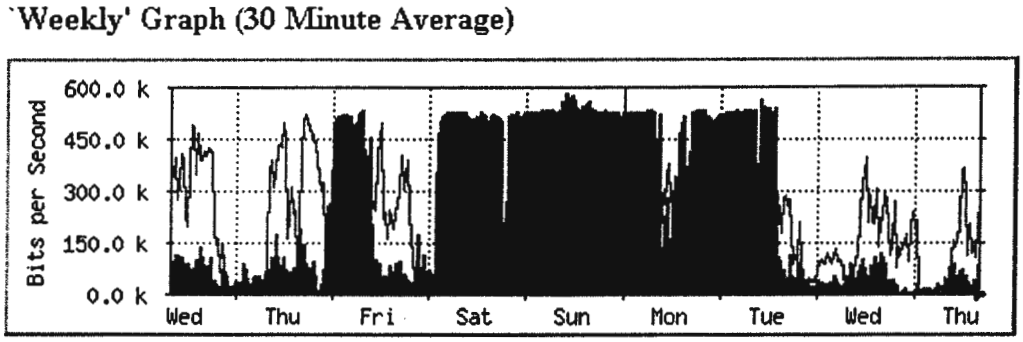


Fig. 7-33 Actividad semanal en la interfaz Ethernet.

Tráfico Mensual en Ethernet:

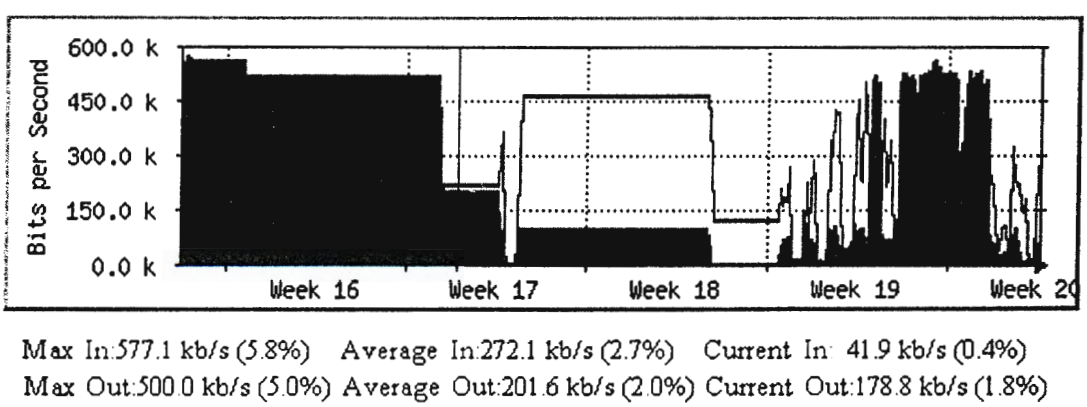


Fig. 7-34 Actividad mensual en la interfaz Ethernet.

Tráfico Anual en Ethernet:

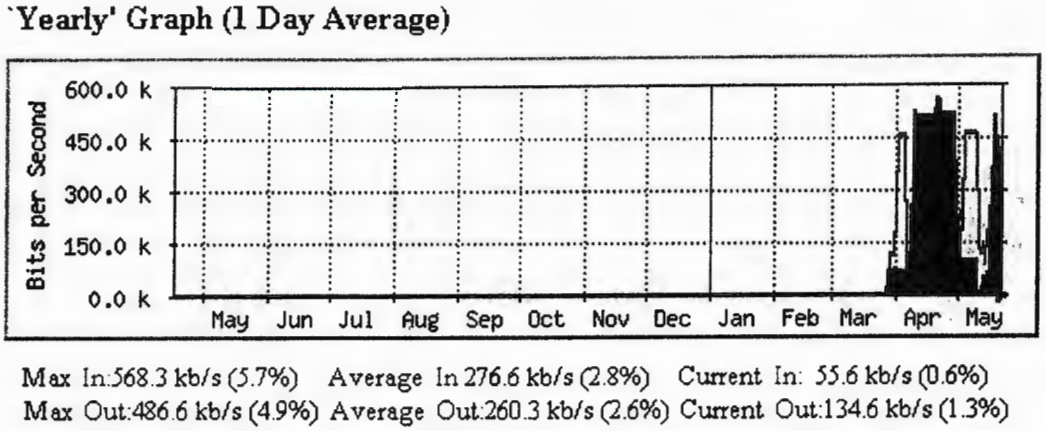


Fig. 7-35 Actividad anual en la interfaz Ethernet.

Las gráficas expuestas anteriormente son generadas también para la interfaz Serial0 del router, a continuación se muestra el análisis para la Serial0:

Para la interfaz Serial0: **http://168.243.3.28/mrtg/168.243.3.1_2.html**

Traffic Analysis for 2 -- r_cdb

System: r_cdb in
Maintainer:
Description: Serial0 cdb.edu/soyapango
ifType: propPointToPointSerial (22)
ifName:
Max Speed: 512.0 kbits/s
Ip: 168.243.254.129 ()

The statistics were last updated **Thursday, 23 May 2002 at 16:18,** at which time **'r_cdb'** had been up for **3 days, 2:18:55**.

Fig. 7-36. Reporte descriptivo de la interfaz Serial 0 del router de la UDB

Es posible percibir en la grafica 7-36 datos como: Descripción de la serial, tipo de enlace wan (PPP, para el caso), el ancho de banda (512 Kbps), y la fecha desde que está "Up" o "arriba". Como en el caso de la interfaz ethernet, MRTG despliega gráficas semanales, mensuales y anuales del tráfico entrante y saliente. A manera de ejemplo se muestra el reporte semanal del tráfico en la Serial0:

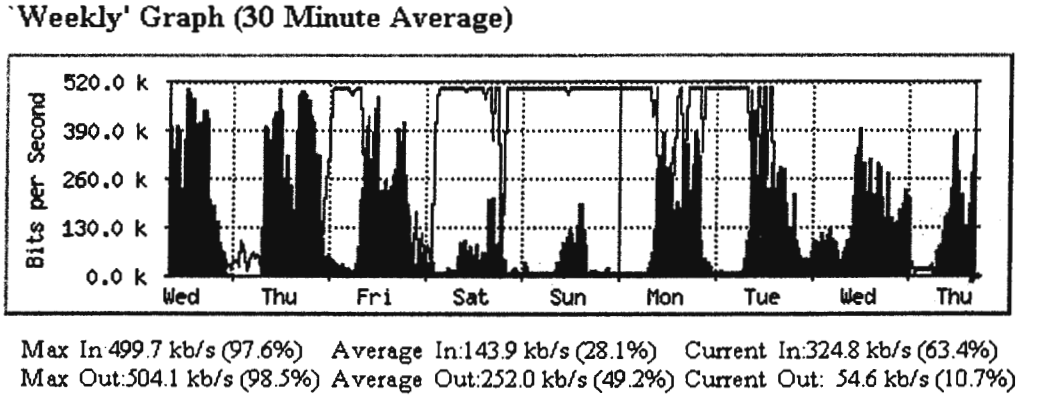


Fig. 7-37 Actividad semanal en la interfaz Serial 0 del router de la UDB.

A partir de la clasificación de monitores de red, es posible clasificar MRTG según:

- **Objetivo:** Monitor de tráfico.
- **Reporte:** Real e Histórico (5 minutos, diario, semanal, mensual y anual).
- **Intrusividad:** No intrusivo.
- **Operación:** remota, puede ser accesado por medio de web.
- **Protocolos:**

Ventajas:

- Realiza registro de información o reportes históricos en forma automática
- Monitorea la carga de tráfico en los enlaces de redes.

NTOP, muestra el uso en tiempo real de la red. Éste, **automáticamente** despliega una lista de hosts que se encuentran actualmente dentro de una red y reporta información concerniente al tráfico IP generado por cada host. El tráfico es ordenado de acuerdo al host y los respectivos protocolos. Entre los protocolos que ntop analiza se incluyen:

- TCP/UDP/ICMP
- (R)ARP
- IPX
- DLC
- Decnet
- AppleTalk
- Netbios
- TCP/UDP
    - FTP
    - HTTP
    - DNS
    - Telnet
    - SMTP/POP/IMAP
    - SNMP
    - NFS
    - X11

Ntop es una herramienta para la medición de tráfico y el monitoreo de redes, que es gratuita, simple y portátil, inicialmente fue concebida por Luca Deri y Stefano Suin, para afrontar problemas de desempeño en la red del campus de la Universidad de Pisa, Italia.

La versión actual de ntop, provee de una interfaz basada en web para el análisis de los datos. Ntop se enfoca en los siguientes puntos:

- Medición del tráfico.
- Monitoreo de tráfico.
- Planeamiento y optimización de red.

Funciones de NTOP

- ***Medición del trafico.***

Consiste en medir el tráfico relevante de la red que es generado por los hosts. Ntop rastrea el uso de la red, generando una serie de estadísticas por cada host. La información que se necesita es recolectada por el servidor que ejecuta ntop, simplemente observando el tráfico que pasa por la red. Todos los paquetes en la red son capturados y asociados con un par de transmisión / recepción. De esta forma es posible rastrear toda la actividad de tráfico generada por un host en particular.

La siguiente tabla muestra la información registrada por ntop para cada host conectado a la red:

Datos Enviados / Recibidos	El tráfico total (volumen y paquetes) generado o recibido por un host. Clasificado de acuerdo al protocolo de red (IP, IPX, Apple Talk, etc.) y al protocolo IP (FTP, http, NFS, etc.)
Uso de Ancho de Banda	Uso de ancho de banda actual, promedio y máximo
Multicast IP	Cantidad total de trafico multicast generado o recibido por el host.
Historia de Sesiones TCP	Sesiones TCP actualmente activas, establecidas y aceptadas por el host.
Tráfico UDP	Cantidad total de trafico UDP ordenado por puerto.
TCP/UDP Servicios Utilizados	Lista de servicios basados en IP (Ejemplo: puertos abiertos y activos)
Distribución de Tráfico	Tráfico local, trafico local a remoto, remoto a local.
Distribución de Tráfico IP	Tráfico UDP vs. TCP, distribución de protocolos IP de acuerdo al nombre de host.

Ntop también reporta estadísticas de tráfico global, que incluye:

Distribución de Tráfico	Tráfico local, local vs. remoto, remoto vs. local
Distribución de Paquetes	Numero total de paquetes ordenados por tamaño, unicast vs. broadcast vs. multicast e Tráfico IP vs. Tráfico No-IP
Uso de Ancho de Banda	Uso de ancho de banda actual, promedio y máximo.
Distribución y Uso de Protocolos	Distribución del tráfico observado.
Matriz de Tráfico de la Red Local	Monitorea el trafico entre cada par de host en la red local

- ***Monitoreo de Tráfico***

El monitoreo de tráfico es la habilidad para identificar aquellas situaciones donde el tráfico de red no cumple con políticas específicas o cuando este sobrepasa algunos límites definidos. En general, los administradores de red especifican políticas que son aplicadas para analizar el comportamiento de los elementos administrados en una red. A pesar de todo, es posible que algunos host no obedezcan con las políticas definidas. Causas típicas de mal comportamiento están relacionados con configuraciones erróneas del sistema operativo, interfaces de red, aplicaciones de software, entre otros.

Ntop provee soporte para detectar algunos problemas de configuración de la red, entre estos están:

- Uso de direcciones IP duplicadas.
- Identificación de host en modo promiscuo.
- Configuración errónea de aplicaciones de software, analizando datos de tráfico de protocolos.

- Uso erróneo de protocolos: identificación de host que utilizan protocolos innecesarios.
- Uso excesivo del ancho de banda de la red.

- ***Planeación y Optimización de la Red.***

Las configuraciones no optimas de hosts pueden influenciar negativamente en el desempeño de una red. Ntop permite al administrador identificar los orígenes del uso improductivo del ancho de banda, especialmente por el uso de protocolos innecesarios. Indirectamente, a través de la distribución del tráfico es posible revisar políticas para la red con el fin de usar sabiamente el ancho de banda.

PROCESO DE INSTALACIÓN DE NTOP 2.0 BETA 3

1. Es necesario obtener algunos paquetes o librerías que tienen el carácter de obligatorios para la ejecución de ntop:

- gdbm ; puede obtenerse en **http://www.gnu.org/**

- libpcap ; puede obtenerse en **http://www.tcpdump.org/**

2. Compilar las librerías de gráficas

- cd gdchart0.94c/
- ./configure
- cd gd-1.8.3/libpng-1.0.8
- cp scripts/makefile.[tipo sistema operativo] Makefile
- make
- cd ../../zlib-1.1.3/
- ./configure
- make
- cd ..

3. Compilar ntop

- cd ntop
- ./configure
- make

4. Ejecución de ntop

- ntop -d -w 3000

Presentación de Pantallas de ntop

En esta sección se mostrarán algunas pantallas capturadas del ambiente de trabajo de ntop, en ellas se muestran algunas capacidades de ntop:

A continuación en la gráfica 7-38, se muestra información general a cerca del host llamado "master " capturado de una pantalla real de ntop, en la red del centro de cómputo de la Universidad Don Bosco:

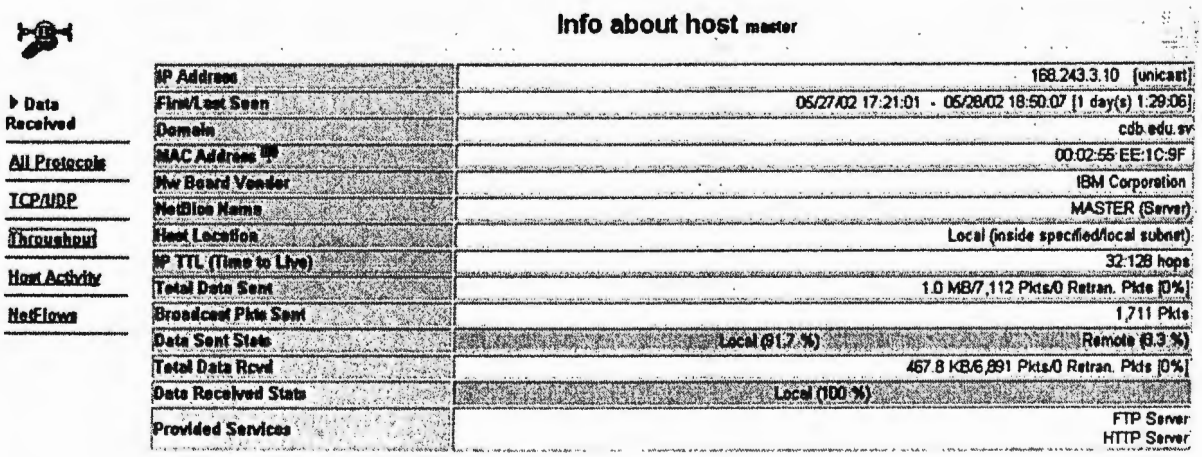


Fig. 7-38. Información obtenida de un host determinado en la red.

En la figura 7-38 se muestra información como dirección IP del host, dominio al que pertenece, dirección física de la tarjeta de red (MAC address) , fabricante de la tarjeta de red, total de datos enviados, total de datos recibidos, servicios activos en el host.

También es posible obtener información sobre el tráfico enviado y recibido por el host analizado en las diferentes horas del día. Para eso véase la figura 7-39

Data Received

All Protocols

TCP/UDP

Throughput

Host Activity

NetFlows

Host Traffic Stats

Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
Midnight - 1AM	37.3 KB	3.5 %	16.3 KB	3.5 %
1AM - 2AM	37.4 KB	3.6 %	16.3 KB	3.5 %
2AM - 3AM	37.0 KB	3.5 %	16.3 KB	3.5 %
3AM - 4AM	37.4 KB	3.6 %	16.3 KB	3.5 %
4AM - 5AM	37.7 KB	3.6 %	16.3 KB	3.5 %
5AM - 6AM	37.2 KB	3.5 %	16.3 KB	3.5 %
6AM - 7AM	37.5 KB	3.6 %	16.3 KB	3.5 %
7AM - 8AM	37.5 KB	3.6 %	16.2 KB	3.5 %
8AM - 9AM	42.9 KB	4.1 %	21.4 KB	4.6 %
9AM - 10AM	42.4 KB	4.0 %	21.1 KB	4.5 %
10AM - 11AM	43.1 KB	4.1 %	21.2 KB	4.5 %
11AM - Noon	42.9 KB	4.1 %	21.2 KB	4.5 %
Noon - 1PM	42.9 KB	4.1 %	21.1 KB	4.5 %
1PM - 2PM	47.1 KB	4.5 %	21.1 KB	4.5 %
2PM - 3PM	45.8 KB	4.4 %	21.1 KB	4.5 %

Fig. 7-39. Trafico enviado y recibido por un host, durante las horas del día.

La figura 7-40, muestra la estadísticas de datos recibidos por los hosts, a través del uso de diversos protocolos en la red:

Network Traffic: Data Received

Host	Domain	Received		TCP	UDP	ICMP	DLC	IPX	Decnet	IP/ ARP	AppleTalk	OSPF	NetBios	IGMP
data		32.9 KB	57.1 %	32.8 KB	0	0	0	0	0	28	0	0	0	0
monitor		16.2 KB	28.1 %	12.4 KB	3.7 KB	0	0	0	0	50	0	0	0	0
dns		2.6 KB	4.5 %	0	2.6 KB	0	0	0	0	56	0	0	0	0
224.0.0.10		1.4 KB	2.4 %	0	0	0	0	0	0	0	0	0	0	0
Cisco CDP/VTP		606	1.0 %	0	0	0	0	0	0	0	0	0	0	0
NetBios		396	0.7 %	0	0	0	0	0	0	0	0	0	0	0
router		262	0.4 %	0	262	0	0	0	0	0	0	0	396	0

Network Traffic: Data Received

Host	Domain	Received		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	SNMP	NEWS	NFS	X11
data		268.7 KB	56.4 %	296	9.6 KB	0	0	0	0	0	0	0	0
monitor		103.6 KB	21.7 %	1.6 KB	4.1 KB	20.7 KB	230	0	527	0	0	0	0
dns		16.3 KB	3.4 %	0	361	15.5 KB	0	0	0	0	0	0	0
224.0.0.10		15.4 KB	3.2 %	0	0	0	0	0	0	0	0	0	0
router		4.9 KB	1.0 %	0	0	0	0	0	0	0	0	0	0
linux		3.2 KB	0.7 %	487	421	0	260	0	487	0	0	0	0
net		958	0.2 %	469	361	0	0	0	0	0	0	0	0
master		874	0.2 %	415	361	0	0	0	0	0	0	0	0

Fig. 7-40. Datos recibidos por los host en una red.

La figura 7-41 muestra el host con el que la computadora inspeccionada tuvo su último contacto

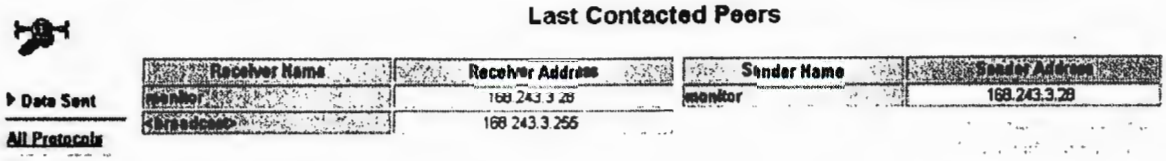


Fig. 7-41. Host con el que se tuvo el ultimo contacto.

La figura 7-42 muestra la Distribución del uso de protocolos por el host *master*, representado por gráficos de pastel:

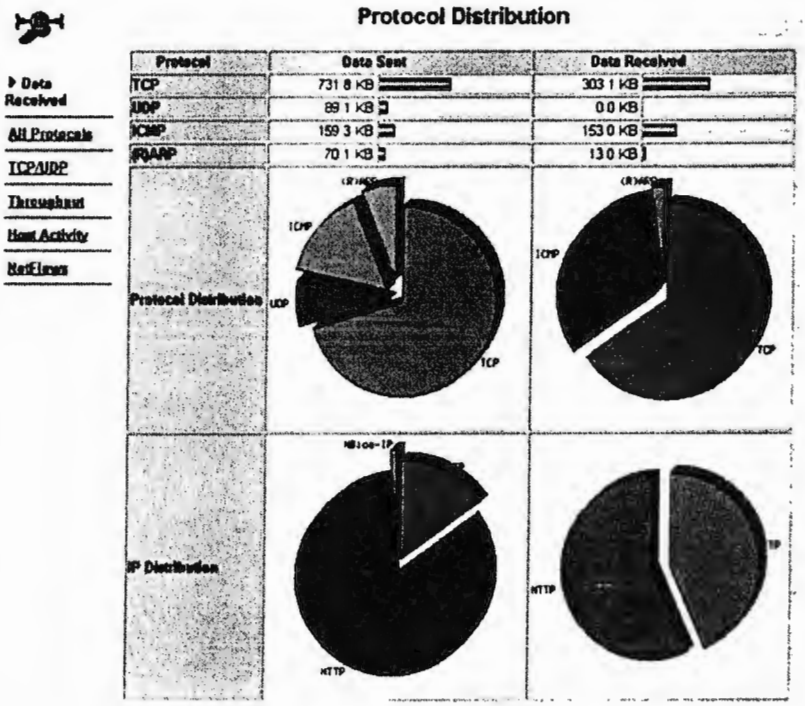


Fig. 7-42. Distribución de protocolos usados por un Host

Además de analizar host de manera individual, ntop también reporta estadísticas de tráfico global. Como se muestra en la figura 7-43, ntop genera un gráfico de barras sobre la Distribución global de protocolos que se usan en la red, por ejemplo: TCP, UDP, ICMP, IPX, Netbios, RARP, IGMP, entre otros.

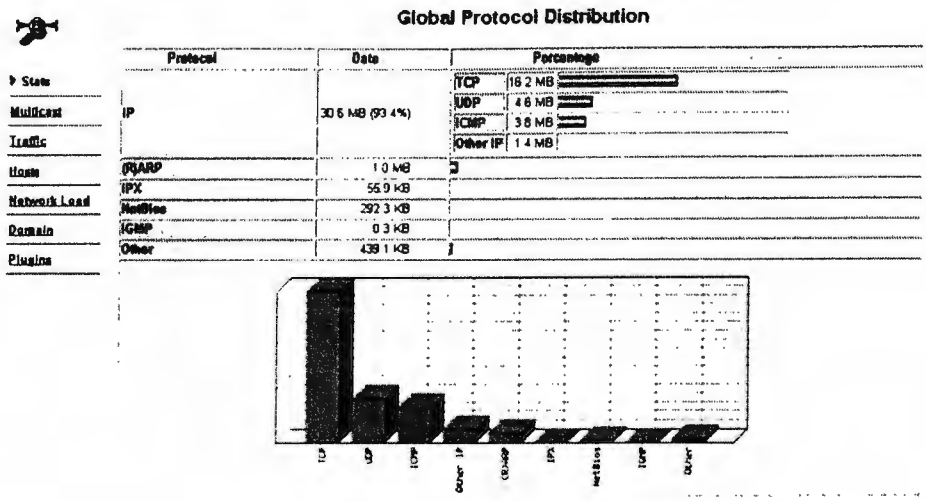


Fig. 7-43. Distribución del uso de protocolos en la red.

Puede hacerse un análisis del trafico de protocolos TCP/UDP en la red (Fig. 7-44): FTP, HTTP, DNS, TELNET, MAIL y NFS

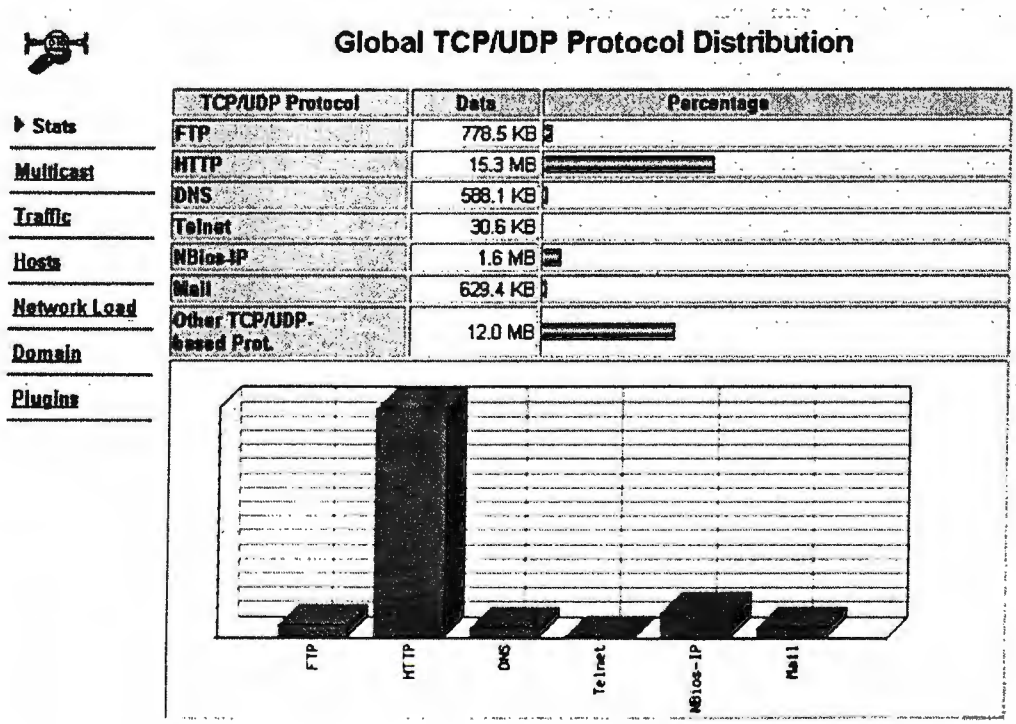


Fig. 7-44. Distribución del uso de protocolos TCP/UDP en la red.

Si se desea conocer la distribución de trafico: multicast, unicast y broadcast ntpo también da esa posibilidad, véase figura 7-45:

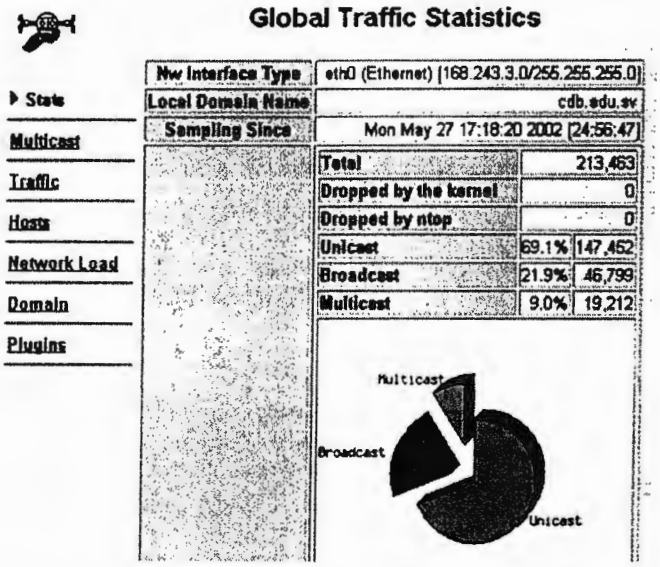


Fig. 7-45. Distribución de trafico Broadcast, Multicast y Unicast

Es posible conocer estadísticas de paquetes que atraviesan la red por ejemplo: el mayor paquete en bytes, paquete más pequeño y el tamaño promedio. (Fig. 7-46).

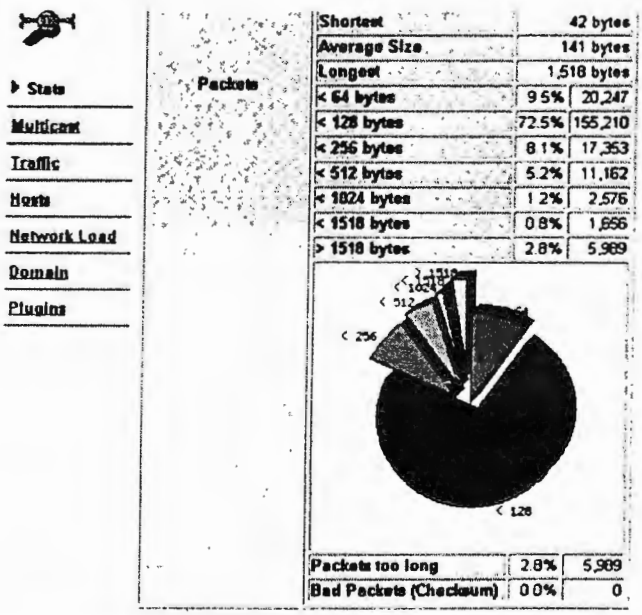


Fig. 7-46. Estadísticas de paquetes que atraviesan la red

Si el análisis de la red incluye conocer el trafico IP y el tráfico que no es IP, ntop genera la gráfica de pastel que se ve en la figura 7-47:

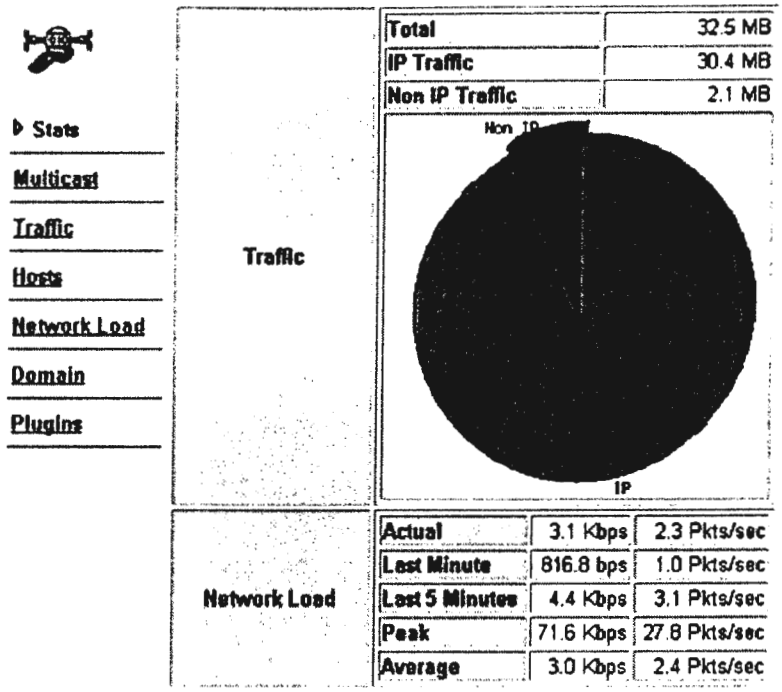


Fig. 7-47. Tráfico IP y No IP que fluye en la red.

Si se desea obtener un reporte a cerca del uso de la red, véase la figura 7-48, en ella se muestra la carga de la red en la última hora (también es posible obtenerlo por 24 horas y por mes).

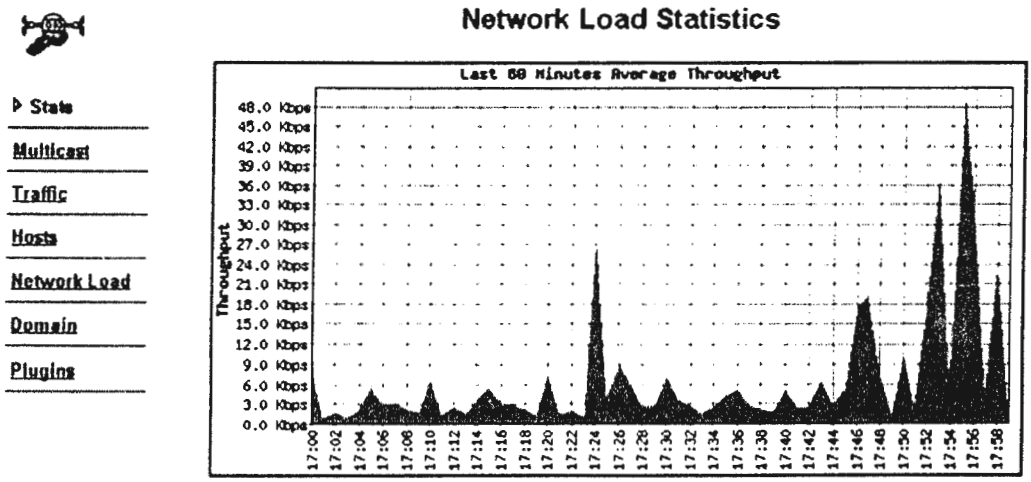


Fig. 7-48. Carga de la red, en los últimos 60 minutos

También es posible obtener un reporte del uso de trafico completamente local, ver figura 7-49:

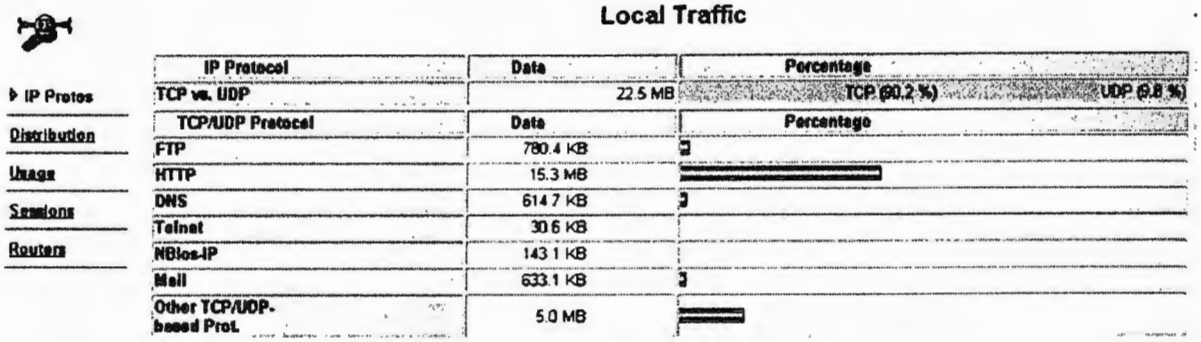


Fig. 7-49. Trafico Local.

Se presentan a continuación la figura 7-50 en la que se presenta estadísticas de tráfico local a remoto y de remoto a local:

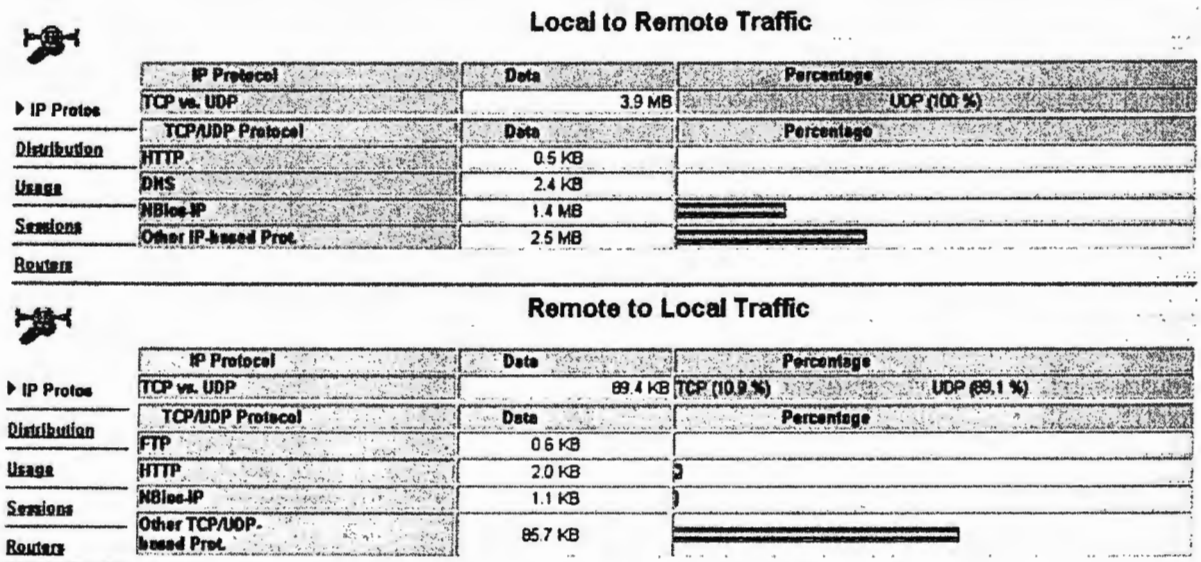


Fig. 7-50. Tráfico de Local a Remoto y de Remoto a Local

A partir de la clasificación de monitores de red, es posible clasificar NTOP según:

- **Objetivo:** Es un monitor de estado de variables y un monitor de tráfico a la vez.
- **Reporte:** Tiempo Real Cuando ocurre un evento en los servicios monitoreados
- **Intrusividad:** Se considera no intrusivo.
- **Operación:** Remota, es posible administrarlo y accesarla a través de un browser.
- **Protocolos:** TCP/IP, IPX, Apple Talk, Decnet, ARP, otros.

Ventajas:

- Interfaz web para el monitoreo remoto.
- Descubrimiento dinámico de la red
- Ofrece una gran cantidad de reportes
- Permite al administrador identificar los orígenes del uso improductivo del ancho de banda, especialmente por el uso de protocolos innecesarios.

Netsaint Versión 0.0.7

Netsaint es un sistema de monitoreo de red. Este se encarga de monitorear ıost y servicios (alertando cuando alguno de ellos provoca un error), sin embargo ɜsta aplicación no desempeña análisis de trafico ni monitoreo de paquetes.

Netsaint fue diseñado originalmente para correr bajo el sistema operativo ⌊inux, aunque debería trabajar bajo otros sistemas basados en sistema Unix ambién.

Algunas de las principales características de Netsaint son:

- Monitoreo de Servicios de Red (SMTP, POP3, HTTP, NNTP, PING)
- Monitoreo de recursos de host (carga del microprocesador, uso de disco, etc).
- Notificación a contactos vía correo electrónico, cuando ocurran problemas en host o servicio.
- Creación de archivos log de manera automática.
- Interfaz web para ver el estatus actual de la red, notificación de problemas, historial, archivos log, etc.

Que NO es Netsaint;

- Un administrador de SNMP.
- Una herramienta de seguridad ante vulnerabilidades.

Netsaint técnicamente no es una herramienta de seguridad, aunque había sido clasificada de esta manera por muchos profesionales de la seguridad en redes. Pero, por que se había tomado como una herramienta de seguridad? Bien, fue debido a los beneficios en pro de los usuarios no-técnicos (gerentes, abogados, etc.), la razón de que NetSaint pude ser considerada como una aplicación de relativa seguridad es por el hecho que ésta ayuda a garantizar la seguridad de nuestro trabajo y da "tranquilidad de espíritu".

Requerimientos del Sistema

El único requerimiento para la ejecución de NetSaint es una computadora corriendo Linux (o una variante de Unix) y un compilador de C. Además de tener configurado el protocolo TCP/IP.

No se requiere el uso de los CGI´s que están incluidos con el paquete de distribución de NetSaint. Sin embargo, si se decide usarlos, se necesitará el siguiente software instalado en la computadora:

1. Un web server (de preferencia Apache)
2. La librería gd.

Proceso de Instalación de Netsaint 0.07

A) Desempacando el paquete de distribución Netsaint.

1. Obtener el paquete en la dirección: http://www.netsaint.org/download/.
2. Para extraer el paquete de distribución de Netsaint, debe de escribirse los siguientes dos comandos:

gunzip netsaint-0.0.7.tar.gz

tar -xf netsaint-0.0.7.tar

Si se ha obtenido el paquete de Netsaint en formato ZIP, debe usarse la línea de comando:

unzip netsaint-0.0.7.zip

Cuando se hallan finalizados estos comandos, es necesario buscar el directorio netsaint-0.0.7 que ha sido creado en el actual directorio.

B) Compilando los programas.

1. Crear un directorio base:

mkdir /usr/local/netsaint

2. Ejecutar el archivos de configuración para inicializar las variables y crear el archivo Makefile:

./configure --prefix=prefix --with-cgiurl=cgiurl --with-htmurl=htmurl --with-netsaint-user=someuser --with-netsaint-grp=somegroup

- Reemplazar *prefix* por el directorio que se creo en el paso anterior (*/usr/local/netsaint*)
- Reemplazar *cgiurl* con la *URL* que se usará para acceder a los **CGIs** (por default es */cgi-bin/netsaint*). NO adicionar un slash (/) al final del *URL*.

- Reemplazar *htmurl* con la *URL* que se utilizara para acceder a la interfaz web HTML de Netsaint (por default es */netsaint/*)
- Reemplazar *someuser* con el nombre de un usuario en el sistema, el cual estará autorizado para establecer permisos en los archivos instalados (por default el usuario es *netsaint*)
- Reemplazar *somegroup* con el nombre de un grupo que este en el sistema el cual estará autorizado para establecer permisos en los archivos instalados (por default el grupo es *netsaint*)

Nota Importante: el argumento *--prefix* del script de configuración es de gran importancia, ya que en este se determina el directorio en el cual se realizará toda la instalación. Si no se le provee de este argumento el script de configuración tomara por defecto el directorio /usr/local/netsaint como el destino de la instalación. Debe asegurarse que este directorio existe antes de empezar con el proceso de instalación.

3. Compilar NetSaint y los CGI´s con el siguiente comando:

```
make all
```

4. Instalar los binarios y los archivos HTML (documentación y la página web principal) con el siguiente comando

```
make install
```

5. Creación e instalación de ejemplos de archivos de configuración.

Los archivos **main**, **host**, **resource**, y **CGI** son archivos de configuración que se crean automáticamente en la raíz del directorio de distribución del paquete, cuando se ejecuta el script de configuración.

Es posible instalar los archivos de configuración ejemplo con el siguiente comando:

```
make install-config
```

6. Instalación del init script .

Si se desea, es posible también instalar el ejemplo del script init en /etc/rc.d/init.d/netsaint con el siguiente comando:

make install-init

Estructura de directorios y localización de archivos

Cambiar al directorio de instalación del Netsaint con el siguiente comando:

cd /usr/local/netsaint

Dentro de este directorio se podrán observar cinco diferentes subdirectorios. Una breve descripción del contenido de estos se presenta en la siguiente tabla:

Sub-Directorio	Contenido
bin/	Núcleo del programa NetSaint
etc/	Archivos de configuración **Main**, **host**, **resource**, y **CGI** (netsaint.cfg, hosts.cfg, resource.cfg, y nscgi.cfg respectivamente)
sbin/	**CGIs**
Share/	Archivos HTML (Para interfaz Web y la documentación en línea)
var/	Directorio vacío para los archivos **log**

Instalación de la interfaz web de NetSaint.

En las instrucciones que siguen a continuación se asume que en la computadora que se está instalando NetSaint, se está ejecutando el Servidor Web Apache.

Si se esta utilizando otro servidor web, se deben de hacer los cambios donde sea apropiado.

Configuración de Alias para los archivos HTML y los CGI´s

Con el fin de hacer accesible los archivos HTML y CGI´s desde la vía web, es necesario editar la configuración de el servidor web Apache de la siguiente manera:

Adicionar una línea en el archivo **httpd.conf** (que está en el directorio **/etc/httpd/conf**), de la siguiente manera

Alias /netsaint/ /usr/local/netsaint/share/

Esto permitirá usar una URL como http://my_host/netsaint/ para ver la interfaz web y la documentación. El alias puede ser el mismo valor que se introdujo en el momento de crear el archivo Makefile en el argumento -- with-htmurl (por default es /netsaint/).

Será necesario crear un alias para los CGI´s de NetSaint también. La instalación por default espera encontrarlo dentro de http://my_host/cgi-bin/netsaint/. Aunque esto puede ser cambiado usando la opción --with-cgiurl en el script de configuración. Es necesario adicionar una en el archivo httpd.conf la línea que sigue a continuación:

ScriptAlias /cgi-bin/netsaint/ /usr/local/netsaint/sbin/

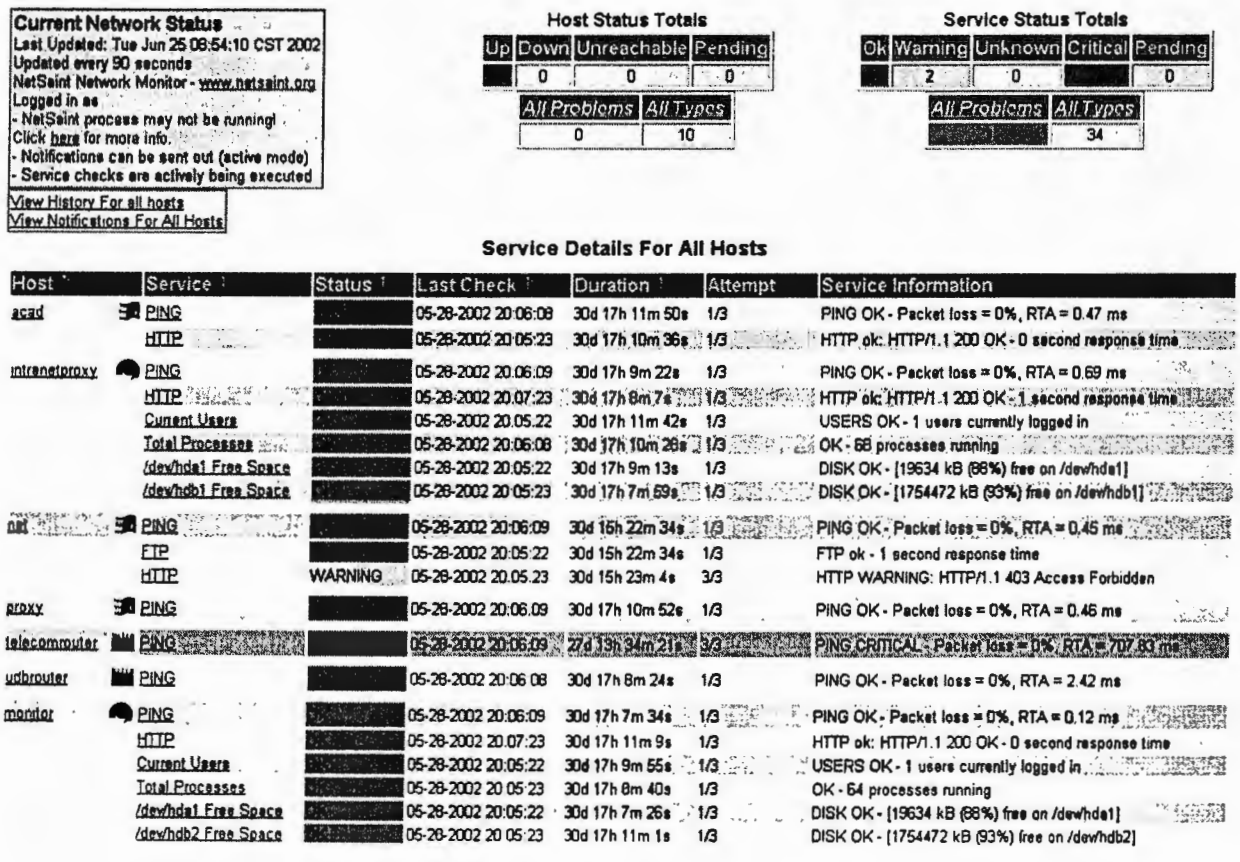
Nota: Una vez se ha editado el archivo de configuración de Apache, es necesario reiniciar el servidor web, con el siguiente comando:
/etc/rc.d/INIT.d/httpd restart

Una vez se ha terminado de instalar y configurar la interfaz web de Netsaint es posible verificar el estado de los host vía web. El formato de la dirección URL será http://hostname/netsaint/. **Para nuestro** caso: **http://monitor.cdb.edu.sv/netsaint/**

Presentación de Pantallas de Netsaint.

A continuación se mostrarán algunas pantallas capturadas del ambiente de trabajo de Netsaint

A, continuación en la gráfica 7-51, se muestra información detallada del estado de los servicios para todos los hosts monitoreados de la red. Netsaint verifica el estado de servicios como PING, http, FTP. Además para host en los que se ejecuta Linux, se monitorean variables como: carga de procesador y espacio libre de disco duro.



Current Network Status
Last Updated: Tue Jun 25 08:54:10 CST 2002
Updated every 90 seconds
NetSaint Network Monitor - www.netsaint.org
Logged in as
- NetSaint process may not be running!
Click here for more info.
- Notifications can be sent out (active mode)
- Service checks are actively being executed

View History For all hosts
View Notifications For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
	0	0	0

All Problems	All Types
0	10

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
	2	0		0

All Problems	All Types
	34

Service Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Service Information
acad	PING		05-26-2002 20:06:08	30d 17h 11m 50s	1/3	PING OK - Packet loss = 0%, RTA = 0.47 ms
	HTTP		05-26-2002 20:05:23	30d 17h 10m 36s	1/3	HTTP ok: HTTP/1.1 200 OK - 0 second response time
intranetproxy	PING		05-26-2002 20:06:09	30d 17h 9m 22s	1/3	PING OK - Packet loss = 0%, RTA = 0.69 ms
	HTTP		05-26-2002 20:07:23	30d 17h 8m 7s	1/3	HTTP ok: HTTP/1.1 200 OK - 1 second response time
	Current Users		05-26-2002 20:05:22	30d 17h 11m 42s	1/3	USERS OK - 1 users currently logged in
	Total Processes		05-26-2002 20:06:08	30d 17h 10m 26s	1/3	OK - 68 processes running
	/dev/hda1 Free Space		05-26-2002 20:05:22	30d 17h 9m 13s	1/3	DISK OK - [19634 kB (88%) free on /dev/hda1]
	/dev/hdb1 Free Space		05-26-2002 20:05:23	30d 17h 7m 59s	1/3	DISK OK - [1754472 kB (93%) free on /dev/hdb1]
net	PING		05-26-2002 20:06:09	30d 15h 22m 34s	1/3	PING OK - Packet loss = 0%, RTA = 0.45 ms
	FTP		05-26-2002 20:05:22	30d 15h 22m 34s	1/3	FTP ok - 1 second response time
	HTTP	WARNING	05-26-2002 20:05:23	30d 15h 23m 4s	3/3	HTTP WARNING: HTTP/1.1 403 Access Forbidden
proxy	PING		05-26-2002 20:06:09	30d 17h 10m 52s	1/3	PING OK - Packet loss = 0%, RTA = 0.46 ms
telecommuter	PING		05-26-2002 20:06:09	27d 19h 34m 21s	3/3	PING CRITICAL - Packet loss = 0%, RTA = 707.83 ms
utbrouter	PING		05-26-2002 20:06:08	30d 17h 8m 24s	1/3	PING OK - Packet loss = 0%, RTA = 2.42 ms
monitor	PING		05-26-2002 20:06:09	30d 17h 7m 34s	1/3	PING OK - Packet loss = 0%, RTA = 0.12 ms
	HTTP		05-26-2002 20:07:23	30d 17h 11m 9s	1/3	HTTP ok: HTTP/1.1 200 OK - 0 second response time
	Current Users		05-26-2002 20:05:22	30d 17h 9m 55s	1/3	USERS OK - 1 users currently logged in
	Total Processes		05-26-2002 20:05:23	30d 17h 8m 40s	1/3	OK - 64 processes running
	/dev/hda1 Free Space		05-26-2002 20:05:22	30d 17h 7m 26s	1/3	DISK OK - [19634 kB (88%) free on /dev/hda1]
	/dev/hdb2 Free Space		05-26-2002 20:05:23	30d 17h 11m 1s	1/3	DISK OK - [1754472 kB (93%) free on /dev/hdb2]

Fig. 7-51. Estado de servicios de red para todos los hosts.

Es posible verificar el estado de un host en particular, por ejemplo, la figura 7-52 muestra información del host DNS.

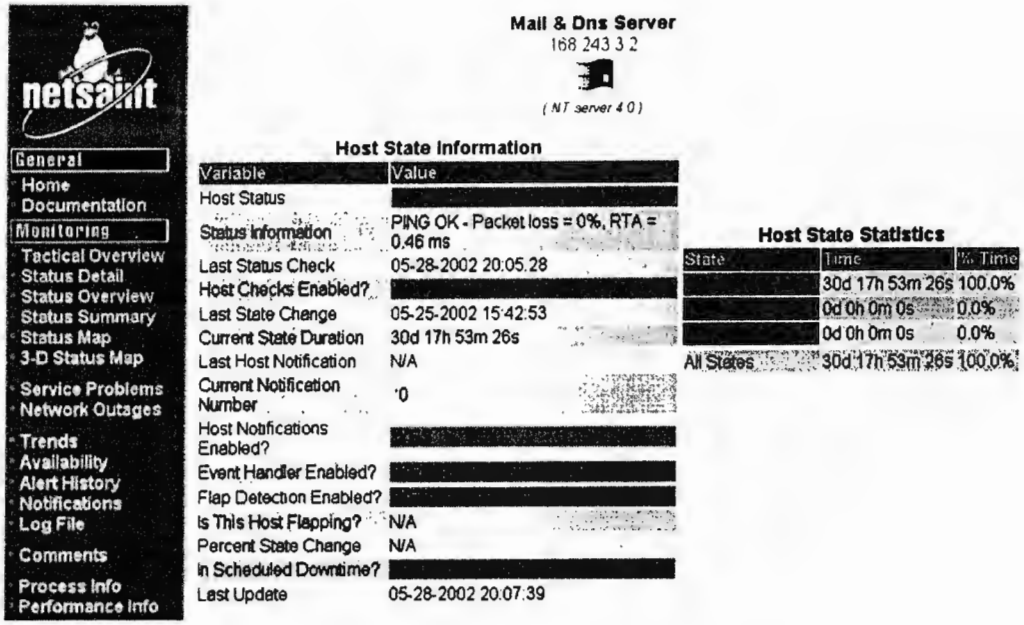


Fig. 7-52. Información de un host en particular.

Si desea saber información sobre un servicio en particular, por ejemplo PING en un dispositivo la figura 7-53 muestra esta capacidad:

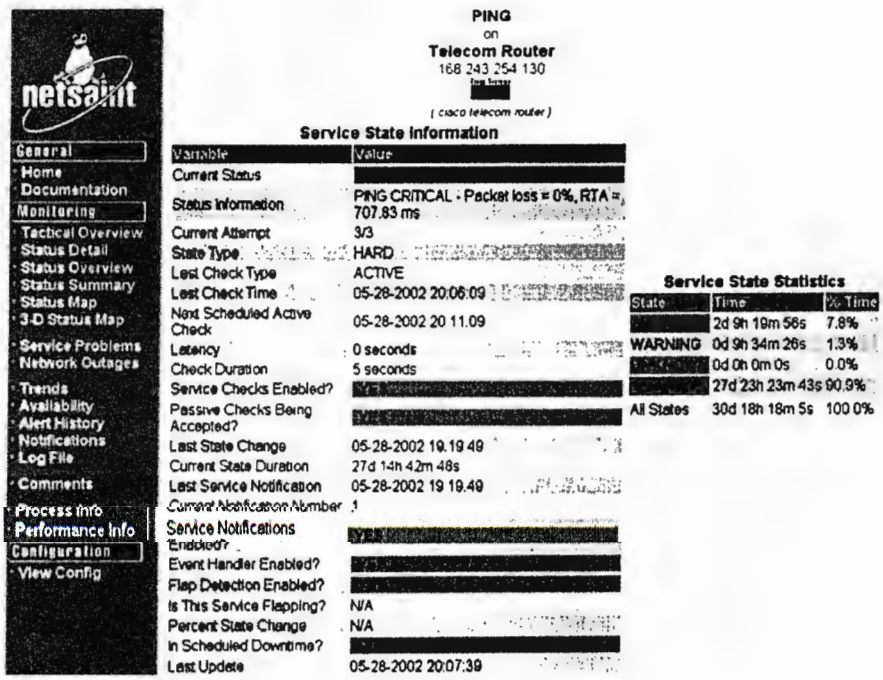


Fig. 7-53. Estado de conectividad (ping) en el host "Telecom Router"

La figura 7-54, muestra de manera gráfica la disponibilidad (Up, Down, Unrechable e Indeterminate), de un host dentro de la red.

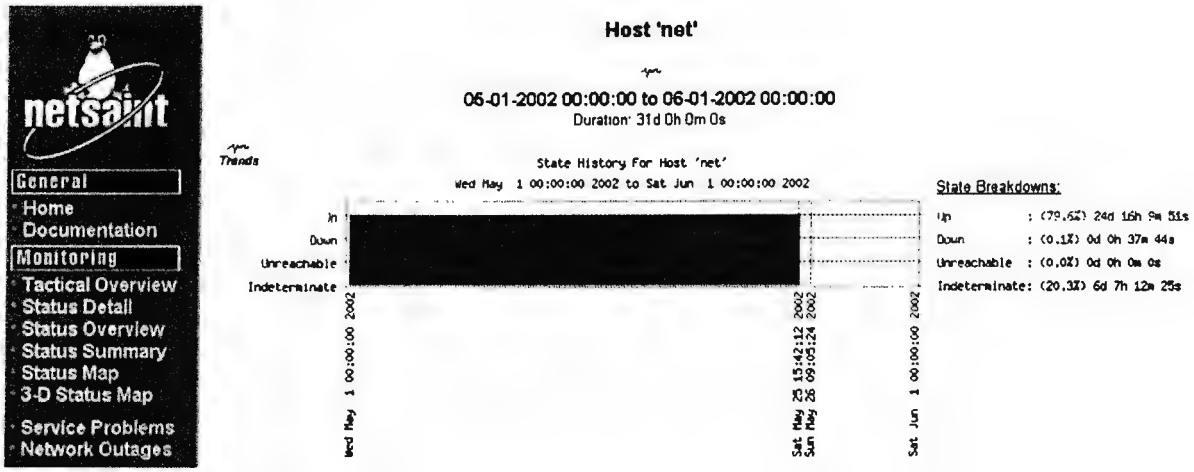


Fig. 7-54. Disponibilidad de un host de manera gráfica.

En la figura 7-55 se muestra un resumen de estatus de todos los sistemas monitoreados por Netsaint, nótese que los host se agrupan de acuerdo al tipo de sistema operativo y por tipo de equipo (routers). Además da información de los hosts sin problema, las advertencias o warning y los problemas críticos.

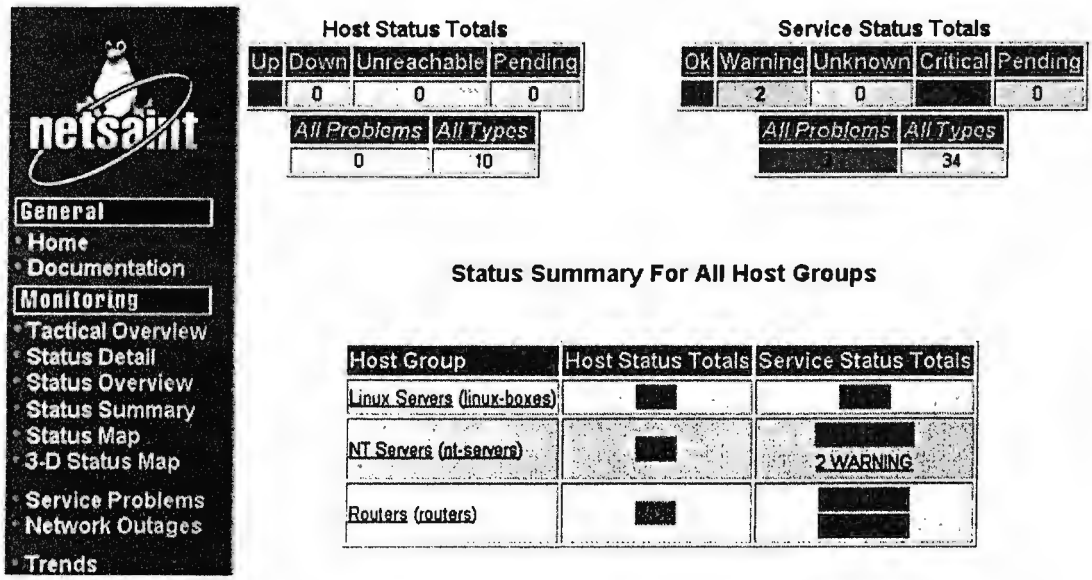


Fig. 7-55. Resumen del estatus para todo los host monitoreados.

Es posible obtener un reporte de los problema que hay en la red, la figura 7-56 muestra esta característica. Incluso Netsaint da una señal audible cuando ocurre un problema dentro de la red.

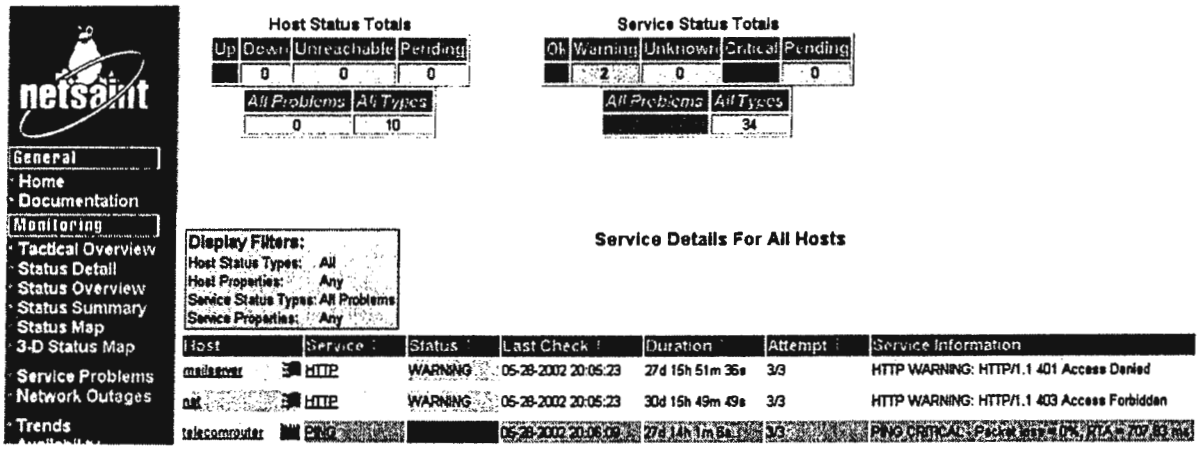


Fig. 7-56. Problemas ocurridos con los servicios de los hosts monitoreados.

Netsaint tiene la capacidad de generar un reporte histórico de los eventos que se han dado en la red. La figura 7-57 muestra un ejemplo de este tipo de reporte.

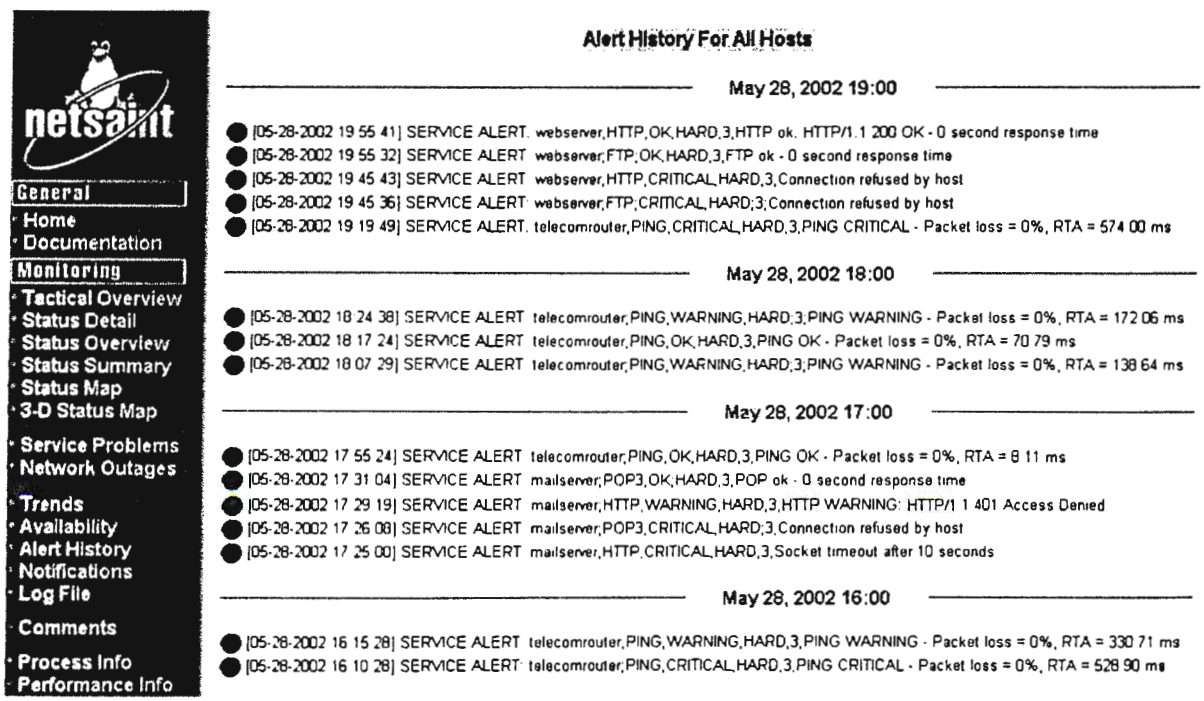


Fig. 7-57. Historial de alertas ocurridas en la red.

Como se dijo en una de las características, netsaint tiene la capacidad de notificar vía correo electrónico, la figura 7-58 muestra las notificaciones enviadas ante un problema en la red.

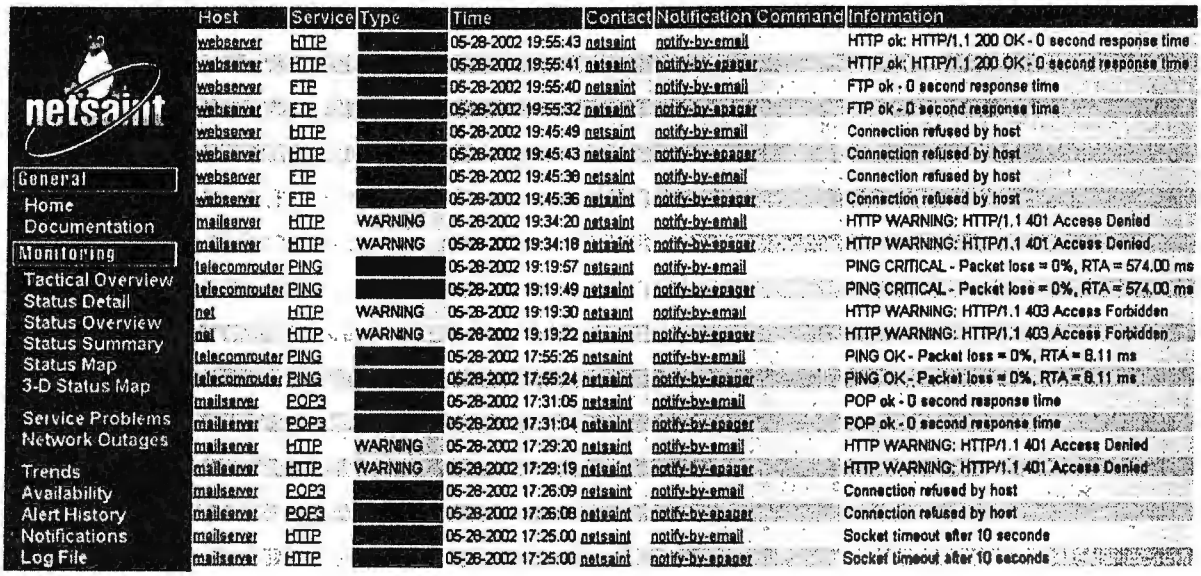


Fig. 7-58. Notificaciones a contactos a causa de eventos en la red

A partir de la clasificación de monitores de red, es posible clasificar SAINT según:

- **Objetivo:** Es un monitor de estado de variables, ya que no entrega reportes del tráfico en la red.
- **Reporte:** Tiempo Real Cuando ocurre un evento en los servicios monitoreados
- **Intrusividad:** se considera intrusivo, ya que usa la red para obtener las variables.
- **Operación:** Remota, es posible administrarlo y accesarla a través de un browser.
- **Protocolos:** TCP/IP.

/entajas:

- Interfaz web para el monitoreo remoto.
- Ofrece una gran cantidad de reportes

- Proporciona avisos audibles cuando se produce una falla dentro de la red.
- Notificación de errores vía correo electrónico, sobre sucesos en la red.
- Mantiene un historial de los sucesos en la red.

Desventajas

- Es necesario introducir manualmente los host en el archivo de configuración.

7.2 Comparación entre los monitores de red estudiados

La presente sección es crucial en la investigación realizada, ya que de ésta surgirán las herramientas que formarán parte de la interfaz final de este proyecto. Se realizará una comparación de las 10 herramientas configuradas.

Según lo descrito en el capitulo IV, Monitoreo de Red, las funciones básicas que debe tener un monitor de red son:

1. Poder extraer estadísticas globales de tráfico, bytes transmitidos y recibidos, etc.

2. Detectar dificultades en los servicios de red (SMTP, POP3, HTTP, NNTP, PING).

3. Poder extraer estadísticas para cada terminal de la red.

4. Proporcionar estadísticas en tiempo real y estadísticas históricas (carga máxima y medida por intervalos de tiempo).

5. Determinar qué ancho de banda se está utilizando en cada momento.

6. Determinar protocolos innecesarios instalados en estaciones de trabajo, impresoras y servidores.

7. Determinar el porcentaje de uso de los diferentes protocolos que se utilizan en la red.

8. Interfaz basada en web para el monitoreo.

9. Notificación de alarmas a contactos.

10. Herramientas para la generación de reportes.

11. Carga de tráfico en enlaces WAN.

Estos criterios son los que se tomarán en cuenta para tomar la decisión de que herramientas de las diez configuradas serán las que integren la Herramienta de Monitoreo de Red propuesto en ésta investigación. En el siguiente cuadro se muestra una comparación entre los monitores de red estudiados, con el propósito de caracterizar y poder concluir en que casos es conveniente ocupar uno o una combinación de ellos.

Anteriormente se definieron un total de once criterios de evaluación para aceptar o rechazar las herramientas sometidas a evaluación, esos 11 criterios representan el 100% de calificación, de esta forma se establecerá la siguiente convención para obtener la calificación de cada herramienta evaluada:

$$\text{Puntuación de criterios cumplidos(\%)} = \frac{\#\ \text{de criterios cumplidos}}{\text{Total de criterios evaluados}} * 100$$

De la formula definida anteriormente se procede a obtener el porcentaje de cumplimiento de criterios en cada una de las herramientas evaluadas, los resultados se presentan en la siguiente tabla:

NOMBRE DE LA HERRAMIENTA	CALCULO DE PUNTUACION	PUNTUACIÓN DE CRITERIOS CUMPLIDOS(%)
CHEOPS	(1 / 11) * 100 = 0.0909	9.09 %
CHEOPS-NG	(1 / 11) * 100 = 0.0909	9.09 %
NMAP	(1 / 11) * 100 = 0.0909	9.09 %
ETHERAPE	(1 / 11) * 100 = 0.0909	9.09 %
NPULSE	(3 / 11) * 100 = 0.2727	27.27%
BCNU	(2 / 11) * 100 = 0.1818	18.18%
SAINT	(2 / 11) * 100 = 0.1818	18.18%
MRTG	(5 / 11) * 100 = 0.4545	45.45%
NTOP	(7 / 11) * 100 = 0.6363	63.63%
NETSAINT	(5 / 11) * 100 = 0.4545	45.45%

De la tabla anterior se puede observar que el porcentaje más alto lo obtiene la herramienta NTOP con un porcentaje del 63.63% seguido de las herramientas NETSAINT y MRTG ambas con 45.45%.

TABLA DE CRITERIOS CUMPLIDOS POR CADA HERRAMIENTA DE MONITOREO

	Cheops	Cheops-ng	Nmap	Etherape	Npulse	BCNU	Saint	MRTG	Ntop	NetSaint
1. Estadísticas Globales de Tráfico, Bytes Tx y Rx				√				√	√	
2. Monitoreo de Servicios de Red.	√	√	√		√	√	√			√
3. Estadísticas para cada terminal de la red.									√	
4. Estadísticas en tiempo real y estadísticas históricas					√			√	√	√
5. Determinar ancho de banda que se utiliza.								√	√	
6. Protocolos innecesarios en estaciones de trabajo.									√	
7. Determinar el porcentaje de uso de los protocolos.									√	
8. Notificación de alarmas a contactos										√
9. Interfaz web, para monitoreo remoto.					√	√	√	√	√	√
10. Herramientas de reporte										√
11. Carga de tráfico en enlaces WAN.								√		
Criterios cumplidos	1	1	1	1	3	2	2	**5**	**7**	**5**

CUADRO COMPARATIVO ENTRE MONITORES DE RED.

	Monitor de Red	Puntuación de criterios cumplidos (%)	Ventajas	Desventajas
1	Cepos www.cheops.org	9.09%	Administración simple, monitoreo servicios de red, instalación simple.	No permite administración remota, dificultad para reconocer sistema operativo.
2	Cheops-ng www.cheops.org	9.09%	Administración simple, monitoreo servicios de red, instalación simple.	No permite administración remota, dificultad para reconocer sistema operativo.
3	Nmap www.nmap.org	9.09%	Permite determinar que puertos tiene abiertos un equipo de comunicación, permite detectar el sistema operativo remoto.	
4	Etherape www.etherape.net	9.09%	Muestra el trafico de red en forma gráfica, identifica una gran cantidad de protocolos, trafico en tiempo real	Tráfico en forma cualitativa no cuantitativa, no posee reporte histórico, dificil de interpretar con muchos nodos en la red.
5	Npulse www.npulse.net	27.27%	Descubrimiento dinámico de host, posee interfaz web, provee reportes históricos.	Funcionamiento inestable.
6	BCNU www.bcnu.org	18.18%	Sencillo de configurar, posee interfaz web para el monitoreo remoto.	Intrefaz web poco seria, no ofrece reportes, no posee descubrimiento de la red.
7	Saint	18.18%	Detecta vulnerabilidades de los equipos, detección automática de host, identificación de sistema operativo y servicios.	No es totalmente gratuito, necesita de una buena cantidad de recursos para su operación.
8	MRTG www.mrtg.org	45.45%	Monitoreo y grafica el tráfico de red de dispositivos que utilizan SNMP, sencillo de instalar y configurar, provee interfaz web.	
9	Ntop www.ntop.org	63.63%	Muestra el uso de la red en tiempo real, descubrimiento dinámico de host, identifica gran cantidad de protocolos, muestra estadísticas por hosts, provee interfaz web.	Su instalación requiere la preinstalación de varias librerias gráficas.
10	NetSaint www.netsaint.org	45.45%	Interfaz web para el monitoreo remoto, ofrece gran cantidad de reportes, excelente sistema de notificación a contactos sobre caidas, altamente estable.	

De los cuadros anteriores concluimos lo siguiente:

1. No existe un monitor de red que realice todas las funciones deseadas, sino que para una finalidad específica, existe un monitor de red adecuado.

2. En base a los criterios cumplidos se muestran los monitores de red con mayor puntaje, indicando el área donde son mejor aprovechados:

   Ntop: Cumplió con 7 de los criterios evaluados, se recomienda para la medición de variables de tráfico en una red de área local, como ancho de banda, paquetes enviados/recibidos, porcentaje de uso de protocolos por nodo y en general.

   Netsaint: Cumplió con 5 de los criterios evaluados, su especialidad es mostrar la disponibilidad de hosts y los servicios que se ejecutan en este.

   MRTG: Cumplió con 5 criterios, siendo el único de los monitores evaluados que permite medir la carga de trafico de los enlaces de redes WAN.

3. Una utilización en paralelo de los monitores que obtuvieron mayor puntaje de criterios permitirá obtener la información necesaria que ayude al diagnóstico de fallas de red.

CAPITULO VIII. IMPLEMENTACION DE HERRAMIENTAS DE MONITOREO Y DIAGNOSTICO DE FALLAS DE RED

En la actualidad el uso de redes de área local genera gran cantidad de información, por lo cual dificulta la tarea de administrar la red. Por lo tanto, es necesaria una o varias herramientas que sean capaces de prevenir y ayudar a resolver problemas en la red para tener una mejor eficiencia en su utilización.

Con objeto de asistir la administración de la red, este manual presenta una descripción general de la interfaz web de monitoreo remoto de la Universidad Don Bosco, la cual, servirá al usuario final como una guía operativa en la que pueda realizar o verificar aspectos relacionados con la administración y monitoreo de las redes informáticas, tales como: *Análisis de trafico, Estadísticas de la red, Utilización de la red, Disponibilidad de Servicios, Porcentaje de uso de Protocolos en la red, Consumo de Ancho de Banda, Generador de Reportes Consolidados, etc,* todo esto a través de una interfaz amigable(vía web), simplificando la iteración con el usuario que haga uso de la misma.

El contenido de la interfaz web para monitoreo remoto de la Universidad Don Bosco fue diseñada con el objeto de poder analizar y Administrar las diferentes redes implantadas en la Universidad Don Bosco, para poder tomar una decisión a la solución de los problemas que se generen en las mismas. Esta interfaz no debe de presentar un costo adicional, la intención de la misma es el ahorro económico, ya que esta basada en software de dominio publico bajo licencia GNU y recursos tecnológicos con que la Universidad cuenta(software para desarrollar paginas web, Apache Web Server, Red Hat Linux (o cualquier variante de Unix), hardware en general, configuraciones de red, etc.). De esta forma se utilizaran los propios recursos de la Universidad Don Bosco y se emplearán diferentes herramientas de monitoreo de dominio publico para analizar y administrar las redes involucradas, de esta forma el diagnostico le corresponderá al administrador de la red(usuario). Por ultimo, se debe tomar en cuenta que por ser un ambiente web, el usuario podrá

profundizar en el análisis de la información presentada, esto a base de los hipervínculos contenidos en la interfaz, logrando de ésta forma ir de lo general a lo detallado.

8.1 Monitores de red implementados

Como se determinó en el capitulo VII sobre la implementación de herramientas de monitoreo y diagnostico de fallas de red, se han implementado aquellas con el mayor número de criterios cumplidos.

Los monitores de red incluidos en la solución son los siguientes:

Ntop

El cual se utilizara para la obtención de estadísticas de trafico de la red monitoreada.

NetSaint

Su objetivo es monitorear la disponibilidad de los *hosts* y los servicios que se ejecutan dichos *hosts*.

MRTG

Se utilizara para medir la carga de trafica en el enlace a Internet del Centro de Computo de la UDB.

Los detalles de instalación, configuración y forma de iniciar todos los monitores anteriores se exponen en los respectivos manuales de administración los cuales puede encontrar en el anexo "A".

8.2 Forma de Ingreso y Salida.

La forma de poder ingresar o acceder a la pagina web principal del monitoreo remoto de la Universidad Don Bosco es a través de un navegador de Internet , el cual es un programa para poder cargar paginas web con hipertexto y enlaces a nivel de hipervínculos.

De lo anterior se definen los siguientes requerimientos mínimos para poder acceder a la pagina principal de la interfaz, dichos requerimientos son:

- Computadora configurada para acceder a la red(cualquiera de las redes implementadas en la Universidad.(centro de computo – cisco, administración CITT, administración UDB, departamento de ortopedia) .
- Poseer instalado un navegador de Internet en la computadora tales como el *Internet Explorer, Nestcape Navigator, Mosaic,* etc.

Cumpliendo con los requerimientos arriba mencionados se procede a digitar en el navegador de Internet la siguiente dirección web: www.cdb.edu.sv/monitor , como forma de ingreso a la interfaz, la cual presentará la pantalla principal de la misma, dicha pantalla se muestra en la figura A.

Con respecto a la forma de salir de la interfaz web, esta se realiza de la misma forma que se cierra una pagina web cualquiera: dando clic con el ratón en el botón superior derecho de la barra de titulo en la ventana(denotada como X) o por medio de a combinación de teclas <<ALT>>+ <<F4>>.

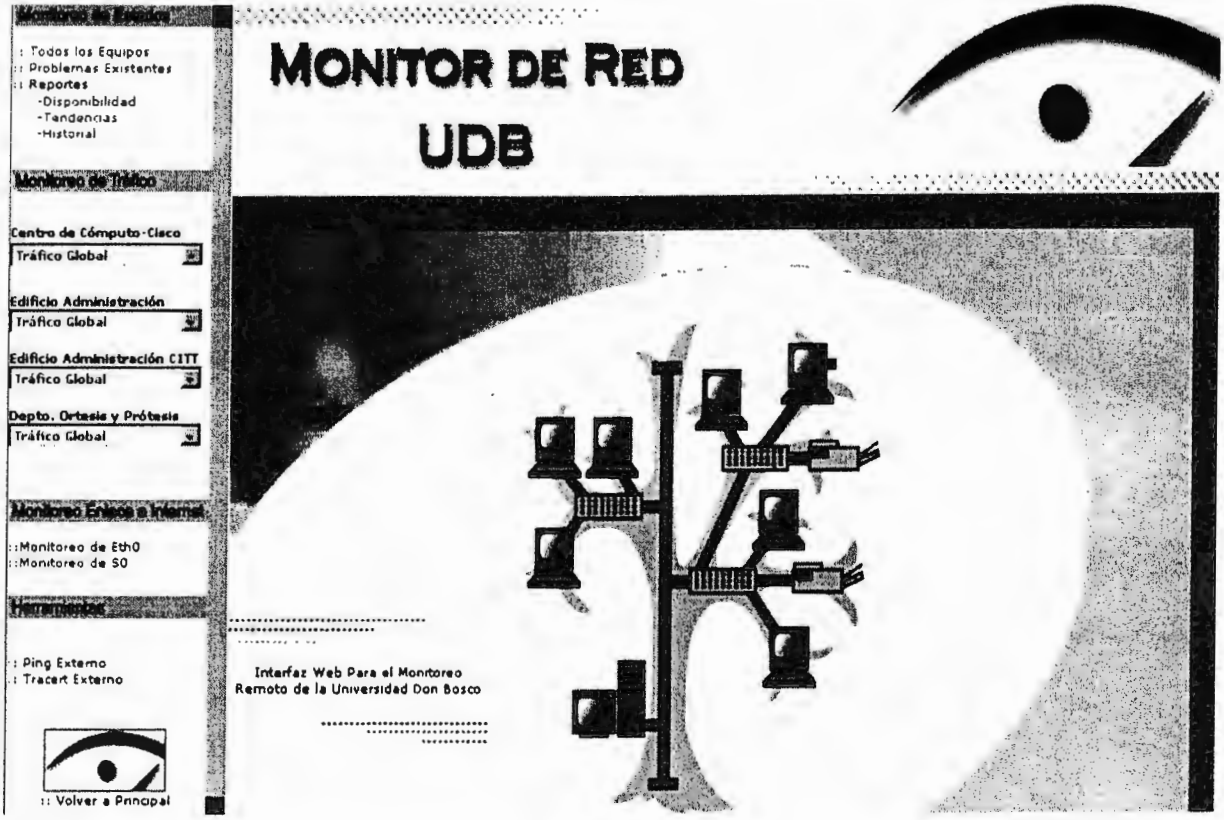


Figura A. Pantalla Principal de la Interfaz Web de la Universidad Don Bosco.

3.3 Diagrama Jerárquico de la Interfaz Web.

La interfaz web posee una serie de opciones, las cuales realizan una función especifica para poder mostrar la información detallada de lo que se desea monitorear. El árbol de opciones se presenta o desglosa en la figura B.

La función que realizan dichas opciones de la interfaz se presentaran en el apartado numero cuatro de éste manual de usuario.

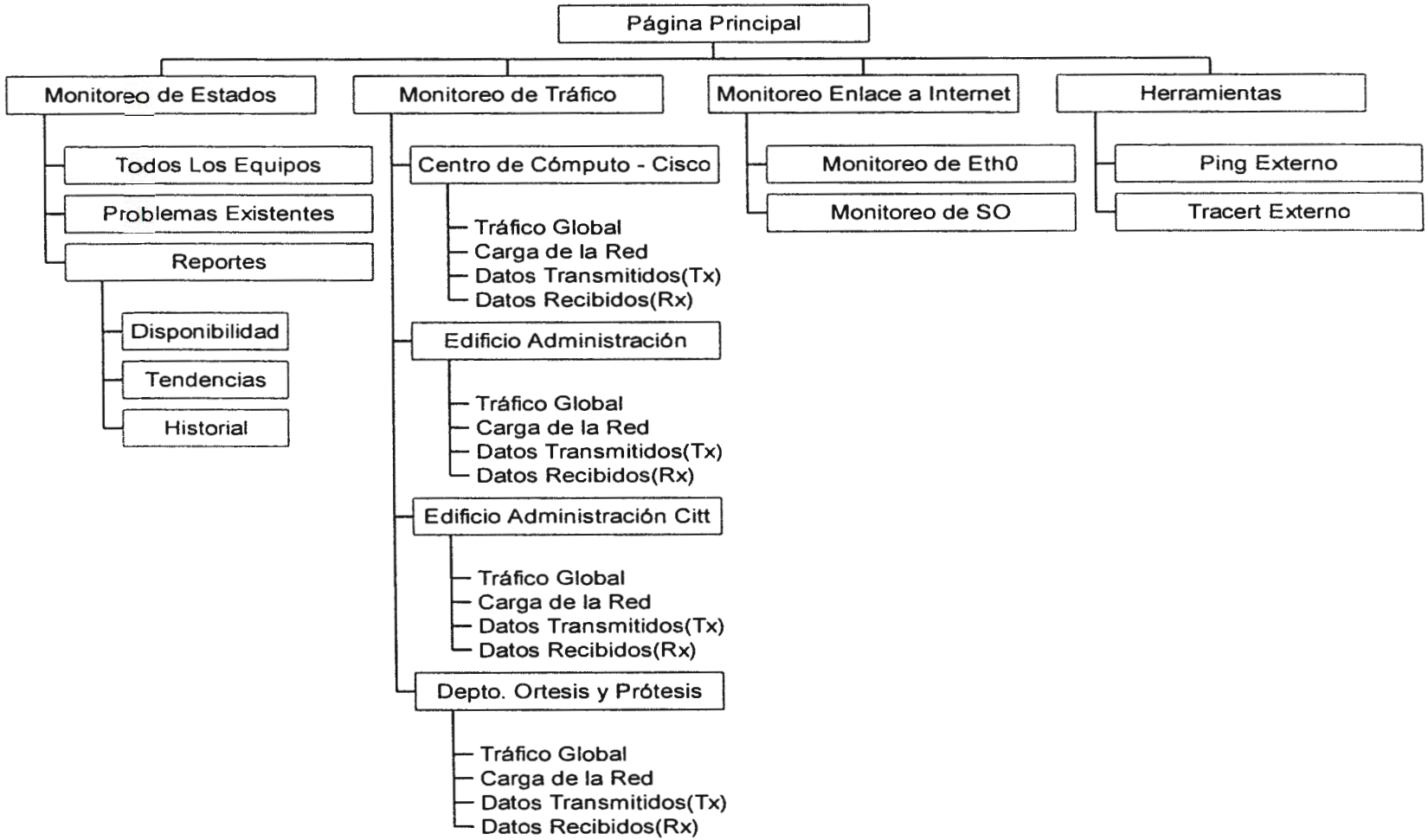


Figura B. Diagrama Jerárquico de la Interfaz Web (árbol de Opciones).

8.4 Descripción de las Opciones de la Interfaz.

Como se presentó en la Figura B., la interfaz web de monitoreo remoto esta compuesta por una serie de opciones, las cuales realizan una función específica en la red o redes monitoreadas. A continuación se presenta una descripción general de cada una de las opciones que se detallan en la pagina principal de la interfaz web.

1. Monitoreo de Estados.

El objetivo es el de "avisar" situaciones de emergencia como "caídas" de equipos o el sobrepaso de un umbral de alguna variable fijada por el administrador.

1.1 Todos los Equipos.

Se muestra un resumen de estatus de todos los sistemas monitoreados por dicha opción, nótese que los *host* se agrupan de acuerdo al tipo de sistema operativo y por tipo de equipo *(routers)*. Además da información de los *hosts* sin problema, las advertencias o *warning* y los problemas críticos(Ver figura C).

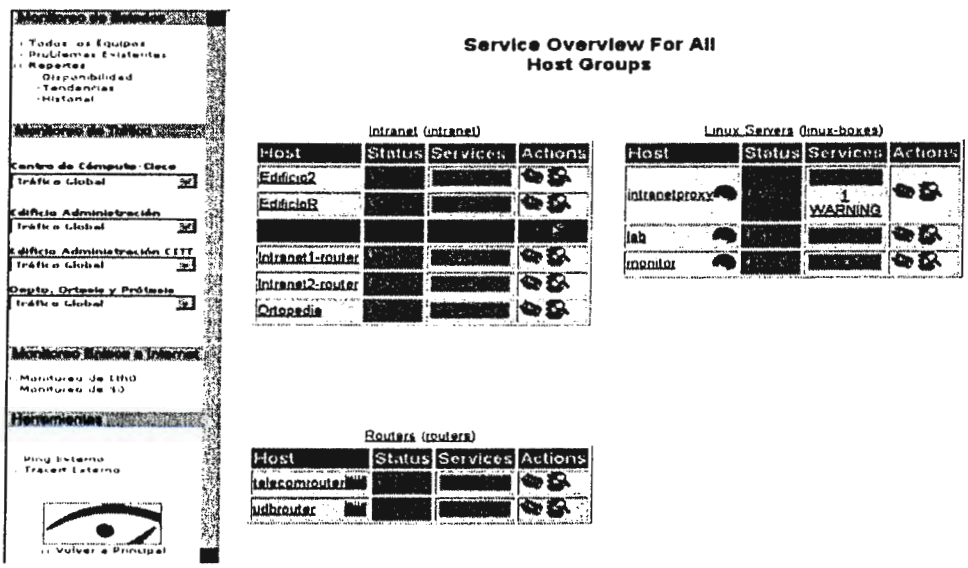


Figura C. Resumen del estatus para todo los host monitoreados.

1.2 Problemas Existentes.

Al hacer clic sobre ésta opción, Es posible obtener un reporte de los problema que hay en la red, la Figura D muestra esta característica. Incluso dicha opción da una señal audible cuando ocurre un problema dentro de la red.

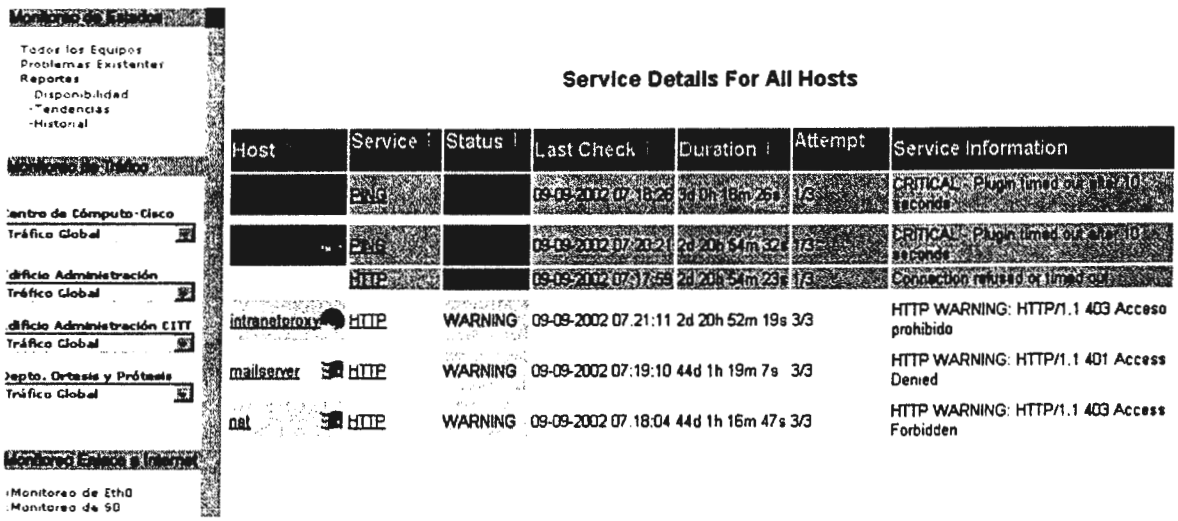


Figura D. Problemas ocurridos con los servicios de los *hosts* monitoreados.

1.3 Reportes.

Existen una clasificación de tres tipos de reportes:

1.3.1 Disponibilidad.

Éste tipo de reporte tiene como función presentar el detalle de la disponibilidad de un grupo de *host*, un *host* especifico o los diferentes servicios que se ejecutan en la red, esto en base a un rango de fechas.

Al dar clic sobre la opción "Disponibilidad" como paso 1 aparecen tres tipos de reportes de disponibilidad, de los cuales hay que elegir uno de ellos para generar

al mismo(ver Figura. E), al seleccionar el tipo de reporte se da clic en el botón "Continue to Step 2"(continuar con el paso 2).

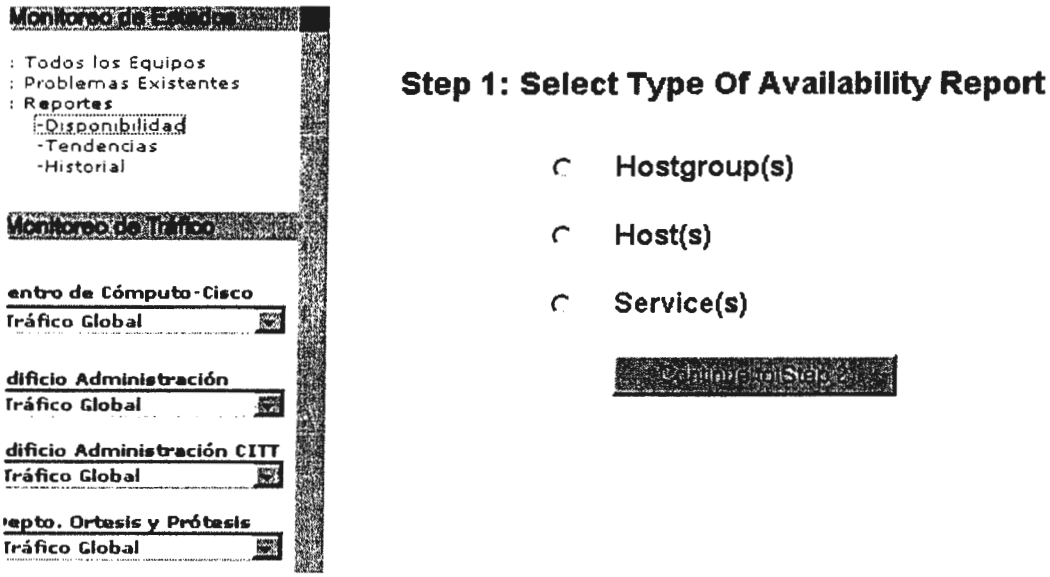


Figura E. Selección del tipo de Reporte de Disponibilidad.

Supongamos que se eligió la opción número dos *(Host(S))* en el paso 1, en el paso 2 me pedirá que seleccione el *host* a analizar(ver figura F).

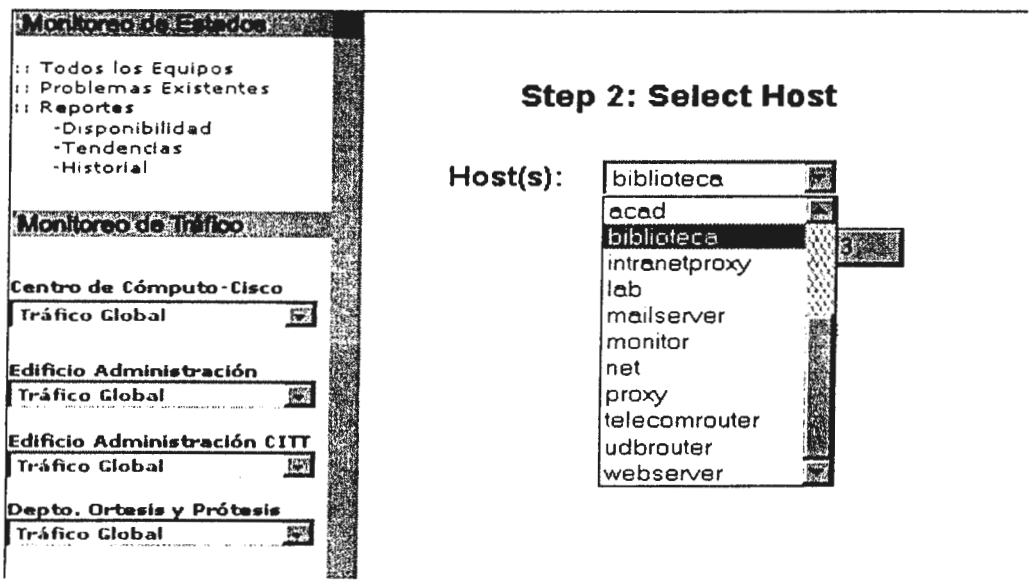


Figura F. Seleccionando el *Host* a analizar su disponibilidad(paso 2).

Luego de haber seleccionado el *host*, se procede a establecer el rango de fechas del reporte(paso 3) tal como se muestra en la figura G. Para dicho ejemplo se establece un rango de fechas del 01/09/2002 al 11/09/2002.

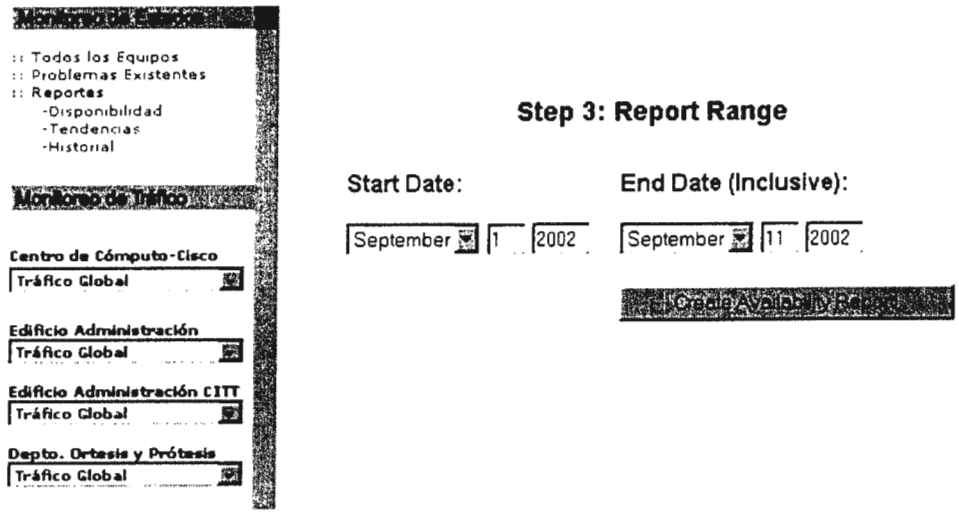


Figura G. Estableciendo el Rango de Fechas para el Reporte.

Por último, como paso 4, se presenta el reporte de disponibilidad(*Up, Down, Unrechable e Indeterminate*) para el *host* elegido o seleccionado en el paso 2(biblioteca). Dicha información se presenta en la Figura H.

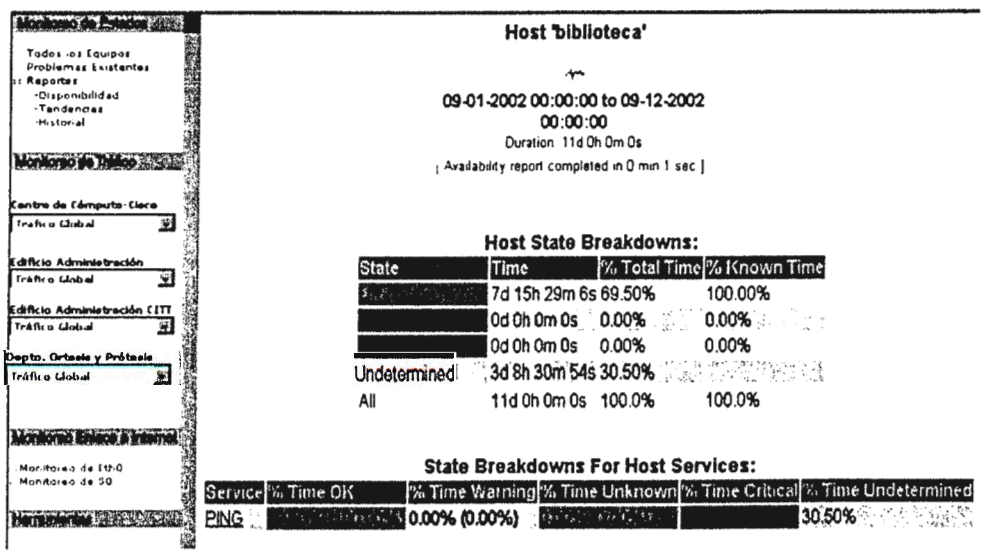


Figura H. Disponibilidad del *Host* Biblioteca.

1.3.2 Tendencias.

Al seleccionar esta opción en el grupo de reportes se debe de definir como paso 1 el tipo de reporte (*Host* o Servicio), tal como se muestra en la figura I.

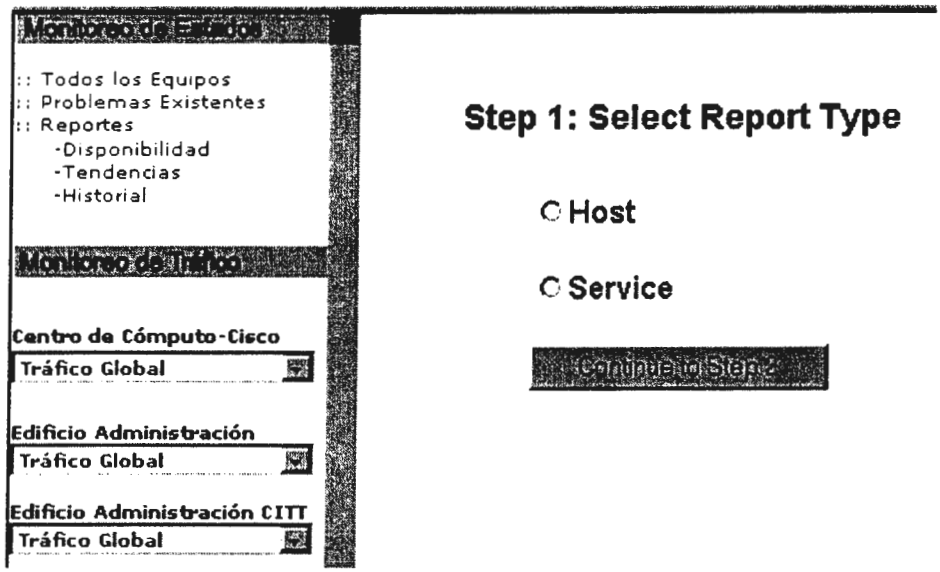


Figura I. Seleccionando el tipo de reporte *(Host o Service).*

Luego en el paso 2 se selecciona el *host* al cual se analizará su tendencia, tal como se muestra en la figura J.

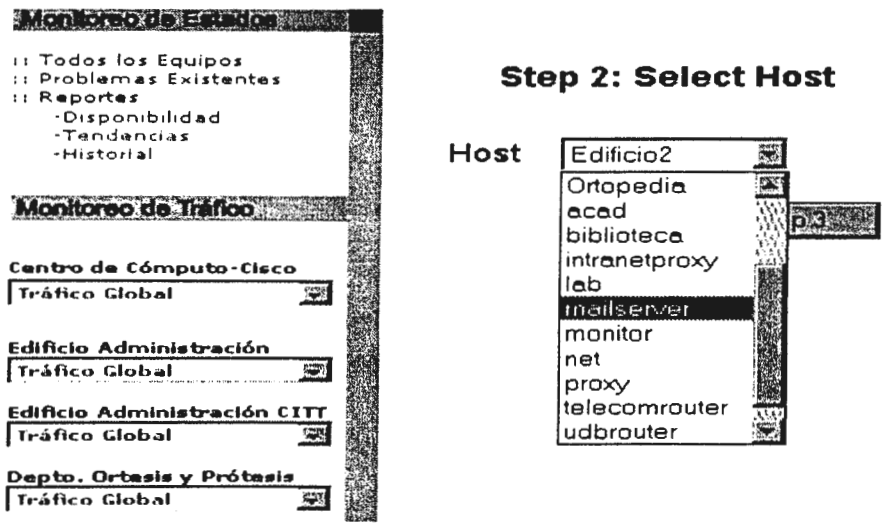


Figura J. Seleccionando el *Host.*

Suponiendo que en el paso 2 elegimos el "mailserver" como *host*, en el paso tres hay que definir el rango del reporte y otras opciones de presentación de la información generada en dicho reporte(ver Figura K.)

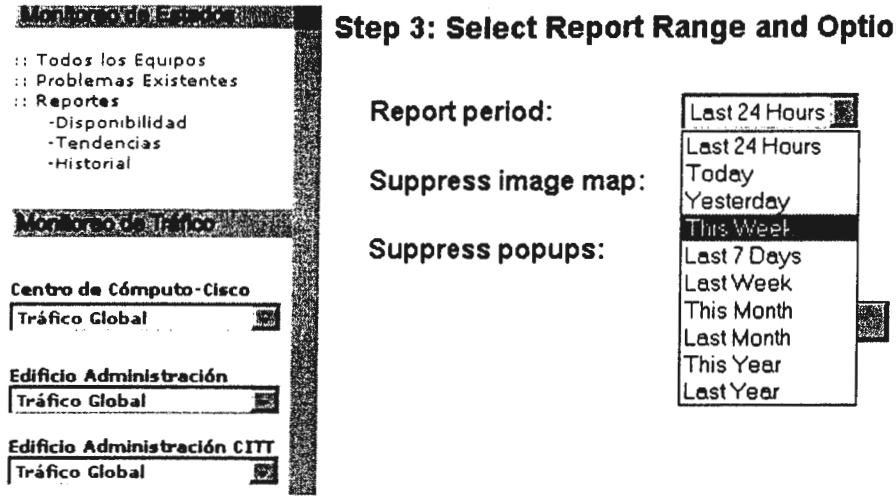


Figura K. Seleccionando el rango del reporte.

Por ultimo se presenta la tendencia del *host* "mailserver" para esta semana*(this week)* , el resultado del reporte se presentaría tal como aparece en la figura L.

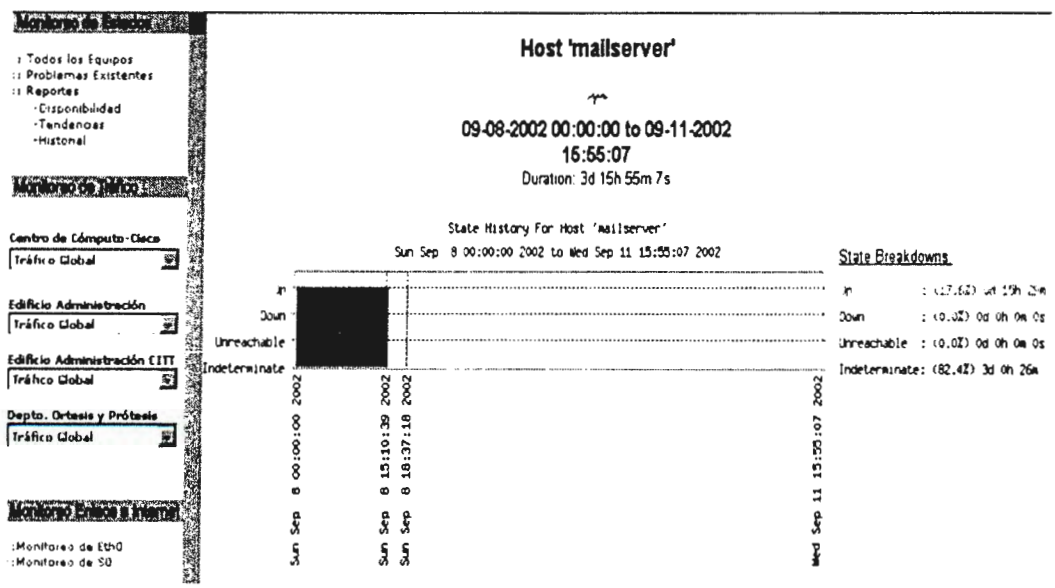


Figura L. Resultado del Reporte de Tendencias del *Host* "Mailserver" en el rango de una semana.

1.3.3 Historial.

Ésta opción posee la capacidad de generar un reporte histórico de los eventos que se han dado en la red. La figura M muestra un ejemplo de este tipo de reporte.

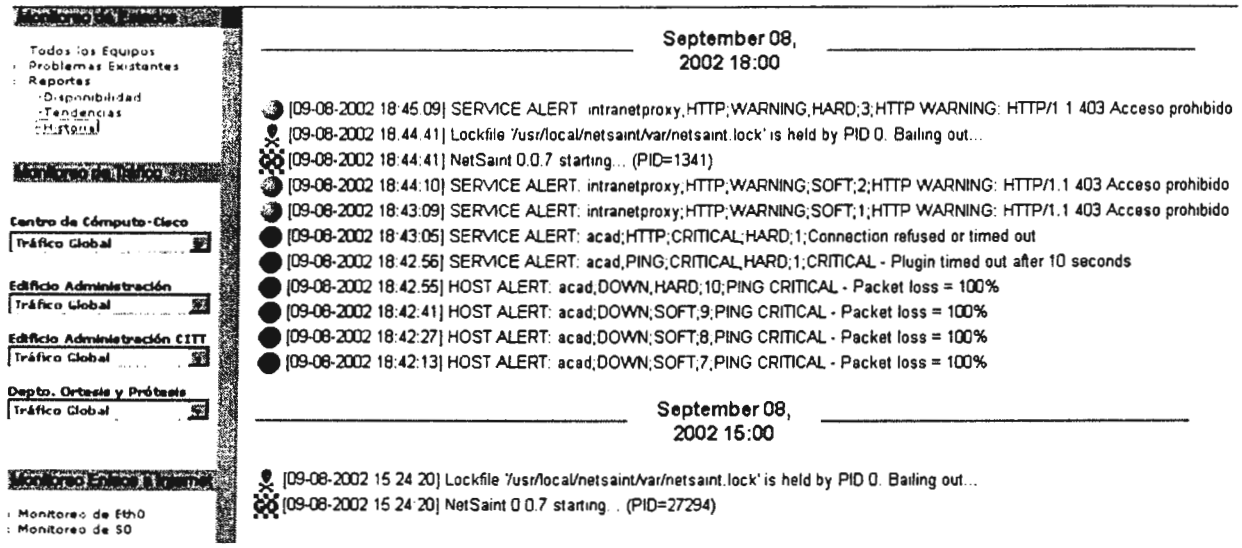


Figura M. Reporte Histórico de Eventos en la Red.

2. Monitoreo de Tráfico.

El objetivo es registrar el tráfico de las redes, ya sea con fines estadísticos o de detección de congestión. Este tipo de monitor también puede tener "alarmas" y por ende, enviar una señal al administrador cuando una variable monitoreada halla excedido un umbral prefijado (considerado como alarmante).

Dentro de la Interfaz web de Monitoreo Remoto se pueden analizar cuatro redes, la cuales son:

- Centro de Cómputo – Cisco

- Edificio Administración
- Edificio Administración CITT
- Departamento Ortesis y Prótesis.

Dentro cada una de éstas redes se monitorea lo siguiente:

- ✓ Tráfico Global
- ✓ Carga de la Red
- ✓ Datos Transmitidos(Tx)
- ✓ Datos Recibidos(Rx)

NOTA: Debido a que el tipo de información que se monitorea es igual en cada una de las redes incluidas en la interfaz web, se procederá a realizar un ejemplo general de cada una de las opciones del monitoreo de tráfico, independientemente de la red que se este monitoreando.

Tráfico Global.

Utilice ésta opción cuando desea conocer la distribución de tráfico global: *multicast, unicast y broadcast*, a la vez, saber el trafico IP y el tráfico que no es IP en la red seleccionada.(ver figura N).

Además de analizar *host* de manera individual, ésta opción también reporta estadísticas de tráfico global. Como se muestra en la figura 7-41, aquí se genera un grafico de barras sobre la Distribución global de protocolos que se usan en la red, por ejemplo: TCP, UDP, ICMP, IPX, Netbios, RARP, IGMP, entre otros.(ver figura O)

Puede hacerse un análisis del tráfico de protocolos TCP/UDP en la red (figura P): FTP, HTTP, DNS, TELNET, MAIL y Bios-IP.

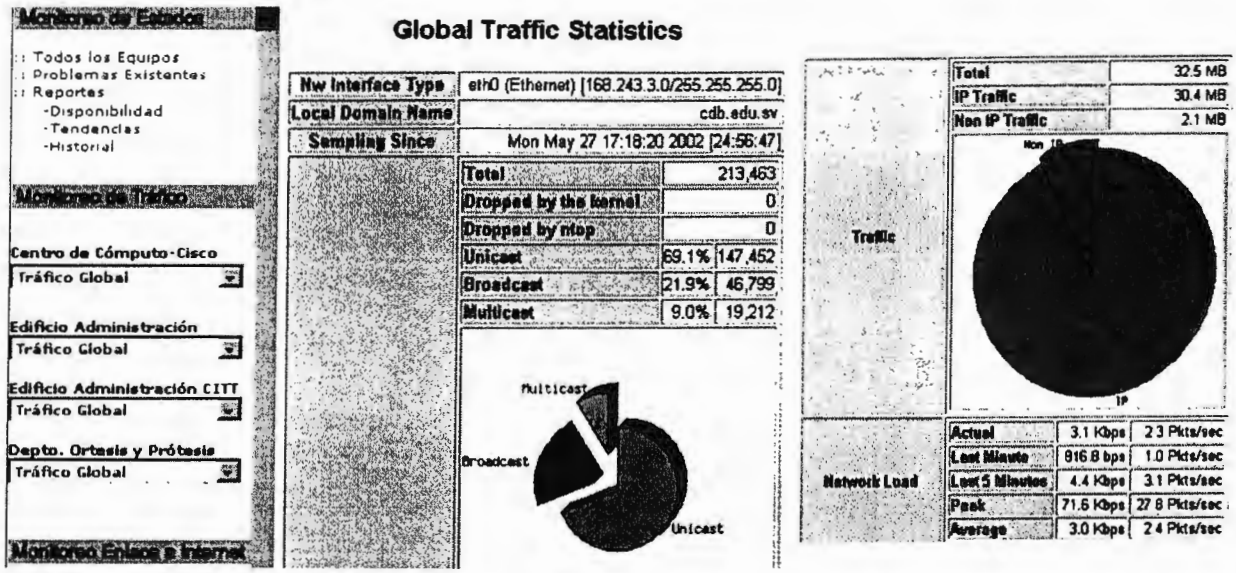


Figura N. Distribución de tráfico global en la red seleccionada.

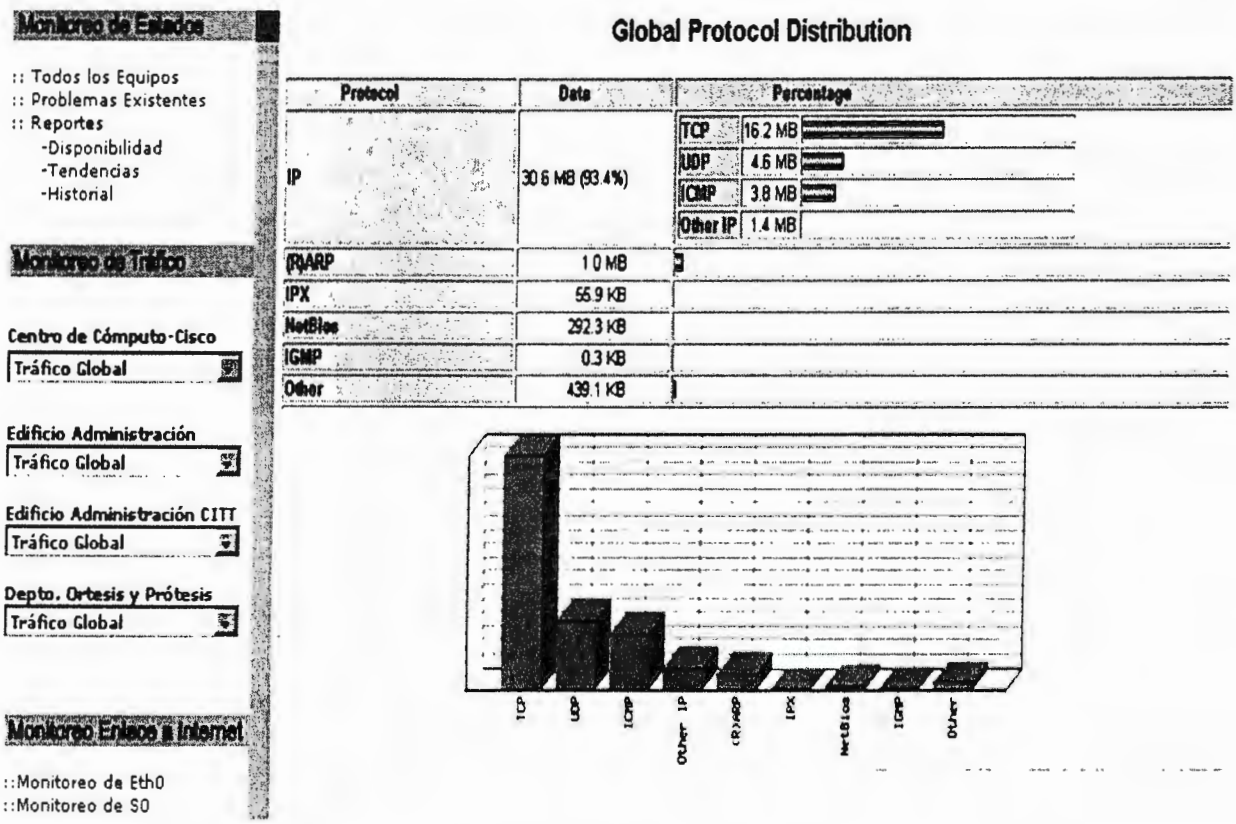


Figura O. Distribución Global de Protocolos

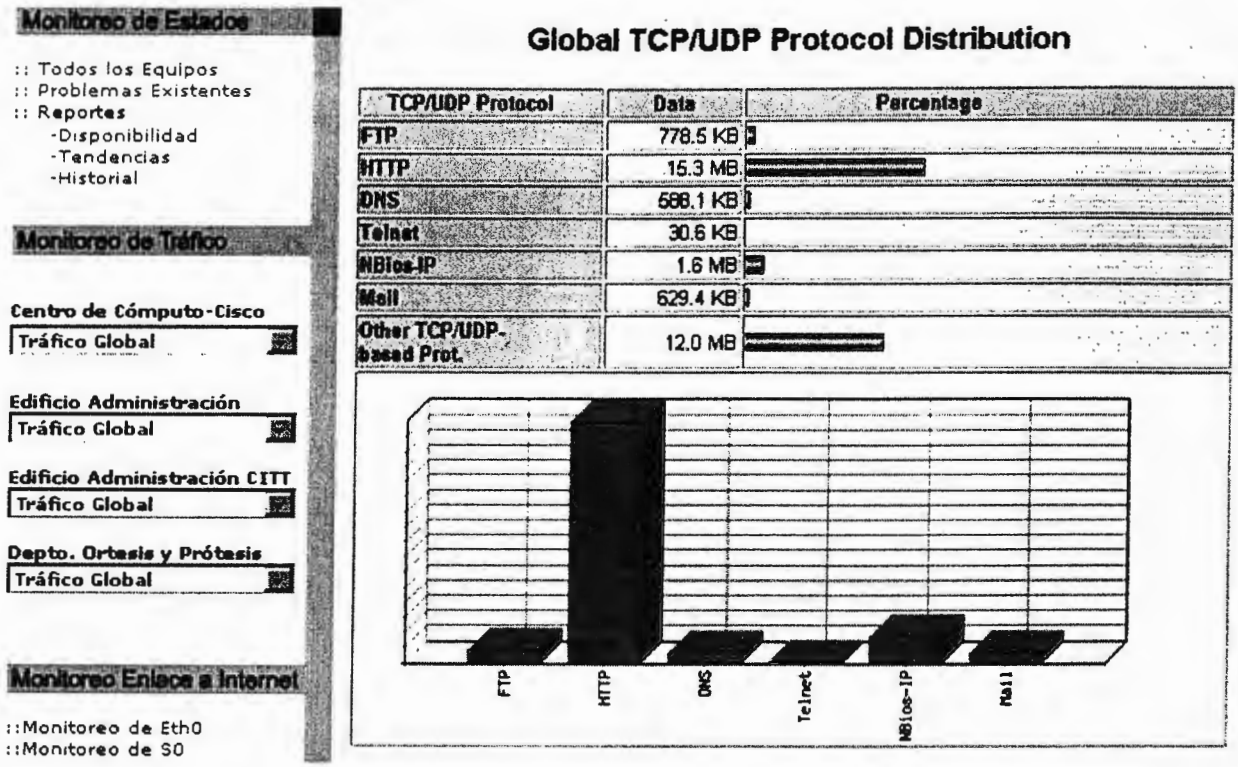


Figura P. Análisis del Tráfico de Protocolos TCP/UDP en la Red

Carga de La Red

Utilice esta opción si se desea obtener un reporte a cerca del uso de la red, véase la figura Q, en ella se muestra la carga de la red en la última hora (también es posible obtenerlo por 24 horas y por mes).

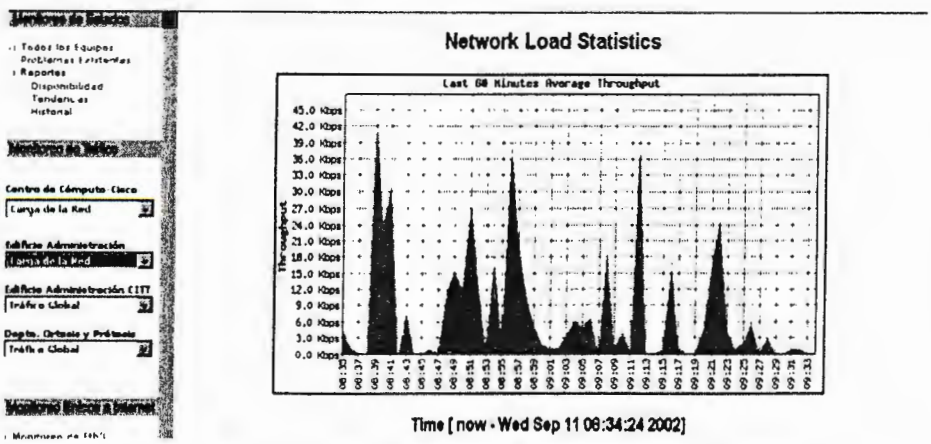


Figura Q. Carga de la red, en los últimos 60 minutos

Datos Transmitidos(Tx).

Utilice esta opción cuando desee obtener las estadísticas de datos Transmitidos por los *hosts*, a través del uso de diversos protocolos en la red analizada(figura R).

Datos Recibidos(Tx).

Utilice esta opción cuando desee obtener las estadísticas de datos recibidos por los *hosts*, a través del uso de diversos protocolos en la red analizada(figura S).

Network Traffic: Data Sent

Host	Domain	Sent		TCP	UDP	ICMP	DLC	IPX	Decnet	RARP	AppleTalk	OSPF
data		8.0 MB	12.1 %	8.0 MB	0	0	0	0	0	0	0	0
G7K4N1.admon-gral (dyn)		2.5 MB	3.9 %	2.5 MB	10.1 KB	124	0	0	0	7.2 KB	0	0
lucrecia		2.4 MB	3.7 %	2.3 MB	99.6 KB	0	0	0	0	6.1 KB	0	0
mercy.admon-gral (dyn)		2.2 MB	3.3 %	2.1 MB	90.2 KB	124	0	0	0	1.0 KB	0	0
Fatima.admon-gral (dyn)		2.1 MB	3.2 %	1.9 MB	134.6 KB	124	0	0	0	8.5 KB	0	0
Atillio120.admon-gral (dyn)		1.2 MB	1.8 %	1.1 MB	56.7 KB	4.4 KB	0	0	0	28.2 KB	0	0
I-router2.admon-gral		1.1 MB	1.6 %	19.6 KB	1.0 MB	1.0 KB	0	0	0	41.2 KB	0	0
Cacy.admon-gral (dyn)		979.3 KB	1.5 %	969.5 KB	5.9 KB	62	0	0	0	3.9 KB	0	0
Brenda.admon-gral (dyn)		662.0 KB	1.0 %	588.1 KB	71.8 KB	124	0	0	0	2.0 KB	0	0
Belloso.admon-gral (dyn)		600.2 KB	0.9 %	580.5 KB	10.5 KB	0	0	0	0	9.1 KB	0	0
adminyst.admon-gral (dyn)		296.4 KB	0.4 %	151.1 KB	143.8 KB	62	0	0	0	1.4 KB	0	0
10.0.1.110		213.3 KB	0.3 %	193.3 KB	18.7 KB	62	0	0	0	1.2 KB	0	0
10.0.1.121		204.3 KB	0.3 %	124.0 KB	79.5 KB	0	0	0	0	920	0	0
GBWPE.admon-gral (dyn)		154.2 KB	0.2 %	148.7 KB	4.6 KB	124	0	0	0	874	0	0
Alex.admon-gral (dyn)		45.3 KB	0.1 %	43.1 KB	1.6 KB	62	0	0	0	552	0	0
Gflores.admon-gral (dyn)		29.5 KB	0.0 %	0	29.3 KB	62	0	0	0	138	0	0
ns		1.0 KB	0.0 %	0	1.0 KB	0	0	0	0	0	0	0
dns.cdb.edu.sv		170	0.0 %	0	170	0	0	0	0	0	0	0

Figura R. Datos transmitidos por los *host* pertenecientes a una red específica.

Network Traffic: Data Received

Host	Domain	Received		TCP	UDP	ICMP	DLC	IPX	Decnet	(R)ARP	AppleTalk	OSPF
Fatima.admon-gral (dyn)		13.5 MB	20.5%	13.4 MB	8.9 KB	124	0	0	0	5.0 KB	0	0
lucrecia		10.7 MB	16.3%	10.7 MB	544	0	0	0	0	3.4 KB	0	0
Cacy.admon-gral (dyn)		6.3 MB	9.6%	6.3 MB	2.3 KB	62	0	0	0	2.2 KB	0	0
G7K4N1.admon-gral (dyn)		5.5 MB	8.3%	5.4 MB	3.3 KB	124	0	0	0	4.3 KB	0	0
Adilio120.admon-gral (dyn)		4.6 MB	7.0%	4.4 MB	160.3 KB	124	0	0	0	17.3 KB	0	0
mercy.admon-gral (dyn)		4.3 MB	6.6%	4.3 MB	4.2 KB	124	0	0	0	336	0	0
Brenda.admon-gral (dyn)		1.9 MB	2.8%	1.9 MB	2.6 KB	124	0	0	0	924	0	0
data		1.6 MB	2.5%	1.6 MB	0	0	0	0	0	0	0	0
10.0.1.110		1.5 MB	2.3%	1.5 MB	1.5 KB	62	0	0	0	726	0	0
Balloeo.admon-gral (dyn)		1.2 MB	1.8%	1.2 MB	17.1 KB	0	0	0	0	5.4 KB	0	0
GBWPE.admon-gral (dyn)		644.8 KB	1.0%	642.1 KB	2.2 KB	124	0	0	0	476	0	0
adminyst.admon-gral (dyn)		642.1 KB	1.0%	636.7 KB	2.6 KB	62	0	0	0	726	0	0
10.0.1.121		464.6 KB	0.7%	464.1 KB	324	0	0	0	0	214	0	0
Alex.admon-gral (dyn)		253.6 KB	0.4%	252.2 KB	1.0 KB	62	0	0	0	308	0	0
i-router2.admon-gral		102.9 KB	0.2%	12.2 KB	42.7 KB	4.7 KB	0	0	0	43.3 KB	0	0
Gflores.admon-gral (dyn)		1.1 KB	0.0%	0	1.0 KB	62	0	0	0	28	0	0
216.34.71.148		930	0.0%	930	0	0	0	0	0	0	0	0
216.34.94.93		930	0.0%	930	0	0	0	0	0	0	0	0
216.34.71.150		372	0.0%	372	0	0	0	0	0	0	0	0
216.34.94.84		186	0.0%	186	0	0	0	0	0	0	0	0
dns.cdb.edu.sv		146	0.0%	0	76	70	0	0	0	0	0	0

Figura S. Datos recibidos por los *host* pertenecientes a una red específica.

3. Monitoreo Enlace a Internet.

Ésta opción se utilizará para cuando se quiera analizar la interfaz *ethernet(eth0)* del router de la Universidad Don Bosco y la Interfaz *Serial0(S0)* del mismo equipo. Con el fin de poder como está el nivel de consumo del ancho de banda en la red interna de la Universidad Don Bosco y el nivel de consumo del ancho de banda hacia Internet (enlaces WAN).

3.1 Monitoreo de Eth0.

Para ésta opción, se muestra la actividad diaria del router en la interfaz Ethernet (para este ejemplo en promedio, en un período de 5 minutos), además, muestra datos relevantes sobre la interfaz *ethernet* del enrutador, como los son su

descripción, el tipo de interfaz (en este caso ethernet CSMA/CD), velocidad máxima y la dirección IP. La fecha de la última actualización de los datos y la fecha desde que la interfaz se encuentra "arriba". (Figura T).

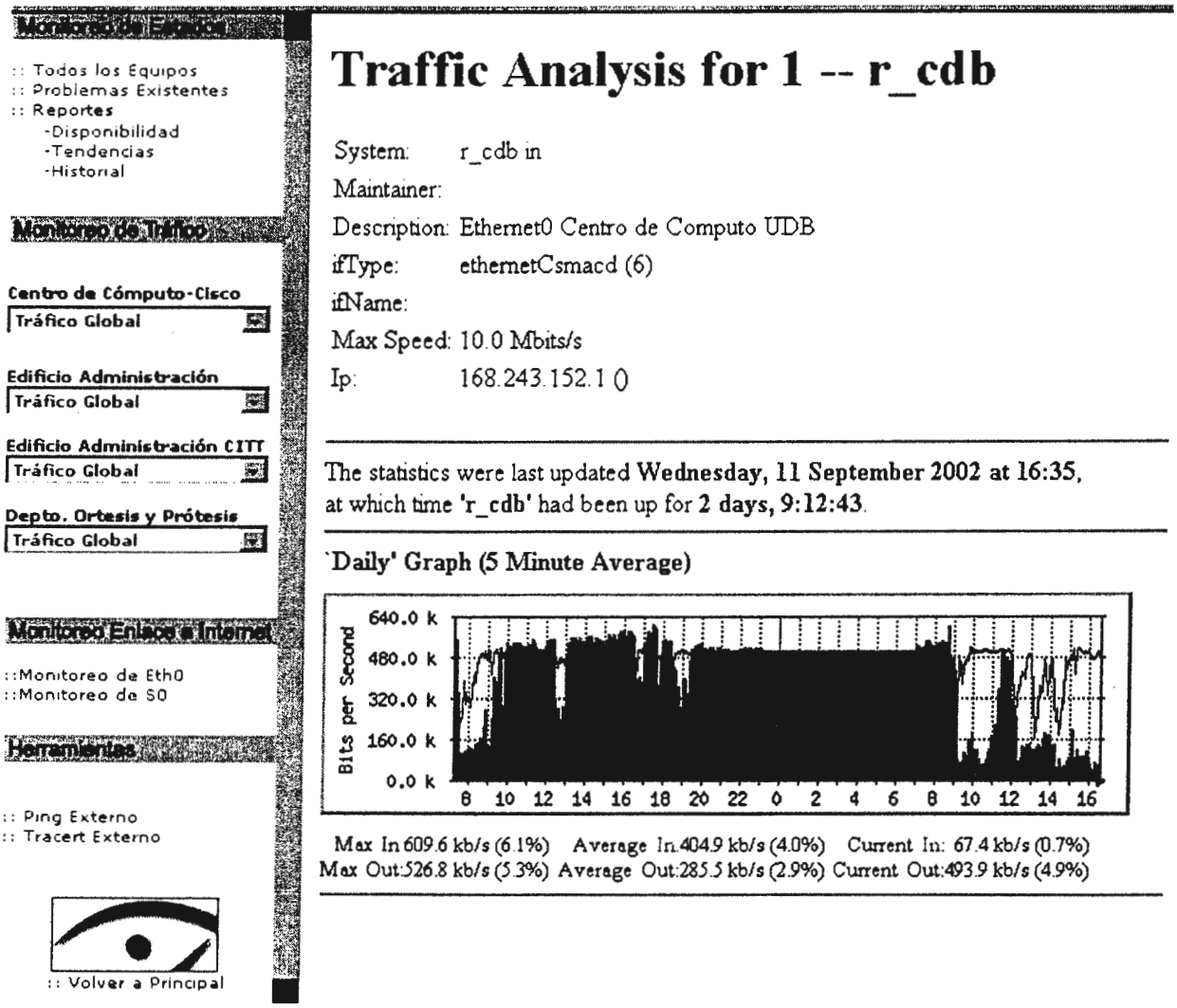


Figura T. Monitoreo de la interfaz Ethernet.0

3.2 Monitoreo de SO.

Ésta Opción es utilizada cuando se desea un reporte descriptivo de la interfaz *Serial0* del router de la UDB. La figura U. Presenta datos como: Descripción de la

serial, tipo de enlace wan (PPP, para el caso), el ancho de banda (512 Kbps), y la fecha desde que está *"Up"* o "arriba". Como en el caso de la interfaz *ethernet*, MRTG despliega gráficas semanales, mensuales y anuales del tráfico entrante y saliente. A manera de ejemplo se muestra el reporte diario del tráfico en la Serial0(ver figura U).

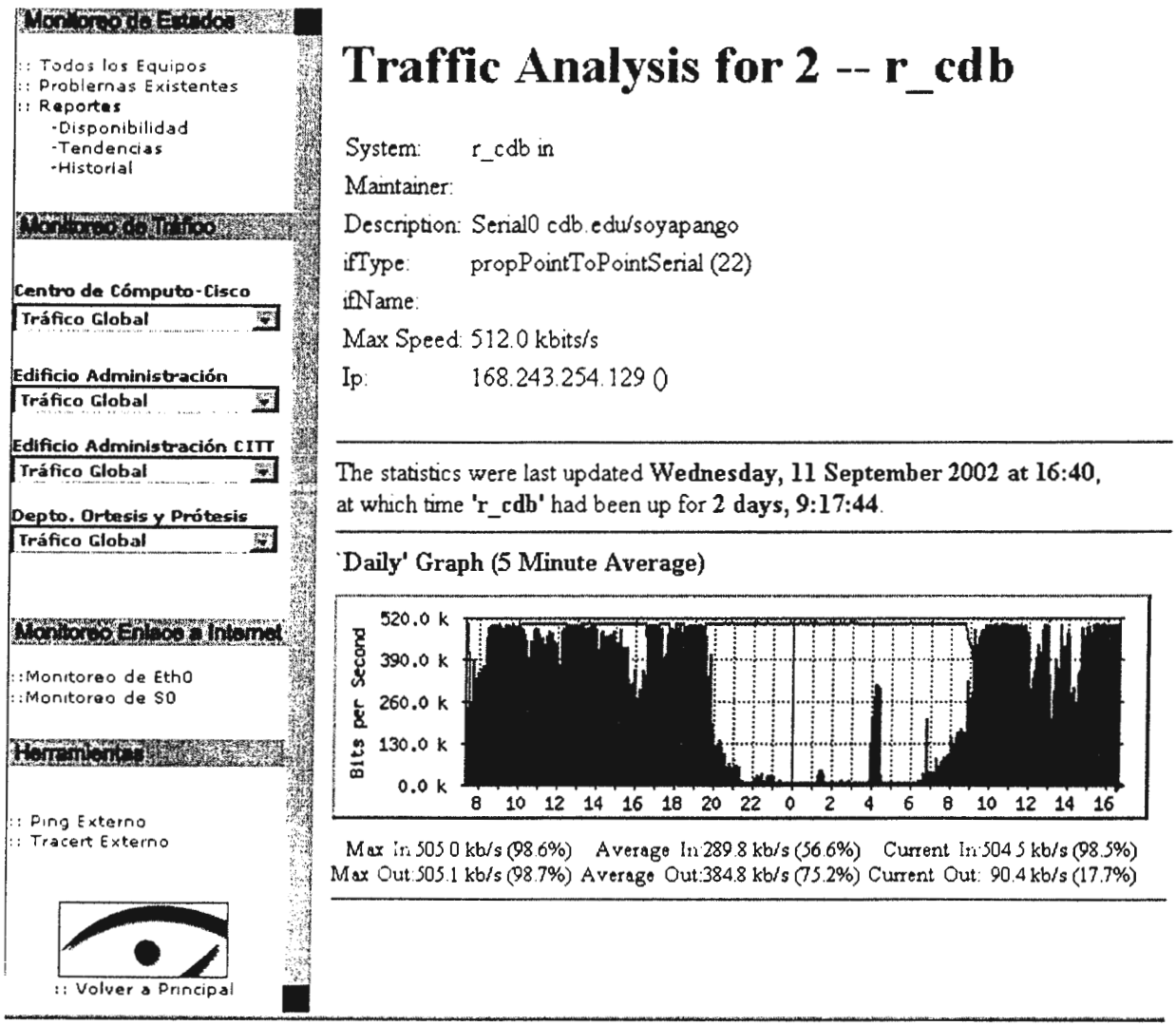
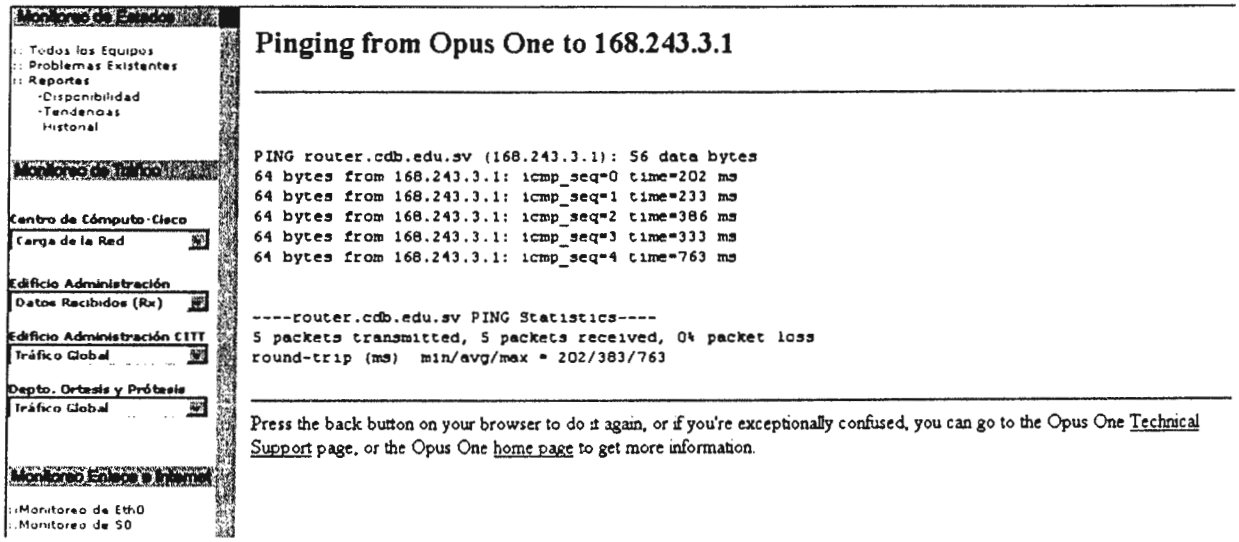


Figura U. Monitoreo de la interfaz Serial0 del Router de la UDB.

4. Herramientas

4.1 Ping Externo

En esta opción lo que se realiza, es una petición hacia un servidor externo a la red de Universidad Don Bosco, dicha petición consiste en que, desde este servidor externo, se realice un intercambio de paquetes hacia una dirección IP perteneciente a la red de la Universidad Don Bosco (en este caso, la ip corresponde a la interfaz de nuestro enrutador). El propósito es verificar que la red local es alcanzable desde redes externas.



4.2 Tracert Externo.

En esta opción lo que se realiza, es una petición hacia un servidor externo a la red de Universidad Don Bosco, dicha petición consiste en que, desde este servidor externo, se realice un trazo de todos los saltos que se deben hacer hasta llegar a una dirección IP perteneciente a la red de la Universidad Don Bosco (en este caso, la ip corresponde a la interfaz del enrutador de la UDB). El objetivo de esta herramienta es que en caso de que la red de la UDB no se alcanzable, se determine en que punto (salto) existe el problema.

Tracing from Opus One to 168.243.3.1

```
traceroute to 168.243.3.1 (168.243.3.1), 30 hops max, 40 byte packets
 1  moe.Firewall.Opus1.COM (192.245.12.96)  5.859 ms
 2  Opus-GW (207.182.35.49)  19.530 ms
 3  610.ATM1-0.GW3.PHX2.ALTER.NET (157.130.235.181)  25.389 ms
 4  109.ATM3-0.XR2.LAX2.ALTER.NET (152.63.114.142)  24.412 ms
 5  0.so-0-0-0.XL2.LAX2.ALTER.NET (152.63.115.229)  24.413 ms
 6  0.so-7-0-0.TL2.LAX2.ALTER.NET (152.63.2.82)  25.389 ms
 7  0.so-7-0-0.TL2.SCL2.ALTER.NET (152.63.1.69)  34.178 ms
 8  0.so-4-0-0.XL2.PAO1.ALTER.NET (152.63.54.82)  37.107 ms
 9  POS1-0.XR2.PAO1.ALTER.NET (152.63.54.78)  37.107 ms
10  188.ATM7-0.GW10.PAO1.ALTER.NET (152.63.53.21)  38.084 ms
11  opentransit2-gw.customer.ALTER.NET (157.130.196.202)  82.026 ms
12  P12-0.PALBB2.Palo-alto.opentransit.net (193.251.240.26)  107.415 ms
13  P10-0.SJOCR2.San-jose.opentransit.net (193.251.242.5)  108.392 ms
14  So1-0-0.DALCR1.Dallas.opentransit.net (193.251.129.113)  115.227 ms
15  218.145.63.71 (218.145.63.71)  192.370 ms
16  210.142.200.222 (210.142.200.222)  171.864 ms
17  Otemachi-gw1-FE00.ptop.ad.jp (210.142.200.196)  175.770 ms
18  TelecomElSalvador1.GW.opentransit.net (193.251.250.70)  192.370 ms
19  61.83.146.99 (61.83.146.99)  192.370 ms
20  168.243.254.54 (168.243.254.54)  192.370 ms
21  210.142.198.65 (210.142.198.65)  67.378 ms
```

CAPÍTULO IX. GUIAS DE LABORATORIO.

Como se definió en el capítulo I sobre el planteamiento del problema, se estructuró una serie de alcances, entre los cueles se definió que como parte del proyecto de tesis se incluirán guías de laboratorio prácticos para los estudiantes de la Universidad Don Bosco. Las asignaturas que se cubrirán son:

- Protocolos de comunicación
- Redes de área local (LAN)
- Redes de área amplia (WAN)
- Comunicación de datos.

En cada una de las asignaturas antes mencionadas se definió una guía que comprende el estudio de temas relevantes al contenido de cada una de ellas definidas por la escuela de computación.

El contenido de ***las guías de laboratorio*** (Véase Anexo C), se basó, en gran parte, en aquellas herramientas que no fueron incluidas en la solución implementada, ya que a pesar de que estas no cumplían con la mayoría de criterios para ser aprobada; se concluyo que dichas herramientas(las usadas en las guías) poseen material suficiente para estructurar una guía de laboratorio, según la materia que se vea involucrada.

Las herramientas usadas en el desarrollo de las guías son:

- **Nmap**
- **Cheops.**
- **Etherape**

En el capítulo VI. Utilidades y Herramientas Comunes se descubrieron que los comandos nativos del NOS realizan un análisis adecuado según la función que estas

realizan, es por ello que se ha estructurado una guía de laboratorio que se basa en una de estas herramientas comunes, dicha herramienta es : **tcpdump(**monitor de tráfico de propósito general que puede capturar y mostrar el contenido de los paquetes que viajan en la red).

Dentro de las herramientas incluidas en la solución se incluye una de ellas en la estructuración de una guia de laboratorio, dicha herramienta es: **MRTG**, la cual como se explico en el capitulo VII sobre Implementación de Herramientas de Monitoreo y Diagnóstico de Fallas de Red, es una herramienta para monitorear la carga de tráfico en los enlaces de una red.

ESTRUCTURACION DE LAS GUIAS DE LABORATORIO

1. OBJETIVOS
2. INTRODUCCIÓN TEORICA
3. MATERIAL Y EQUIPO
4. PROCEDIMIENTO
5. INVESTIGACIÓN COMPLEMENTARIA
6. REFERENCIAS

ESQUEMA DE ESTRUCTURACIÓN DE LAS GUIAS DE LABORATORIO

GUIA DE LABORATORIO (Titulo)	ASIGNATURA	HERRAMIENTAS UTILIZADAS	TEMAS QUE CUBRE	ENTIDAD	
				UDB	CISCO
Monitoreo de Redes	Redes de Area Local	Cheops	Protocolos de comunicac.	X	
		Etherape	(Unidad I)		
			Diseño y manejo de la Red.		
			(Unidad V)		
Análisis y Escaneo de puertos	Comunicación de Datos	nmap	Comunicación entre	X	
			Computadoras (Unidad I)		
			Recomendaciones CITT		
			(Unidad VII).		
Análisis de tramas y protocolos	Protocolos de Comunicación	tcpdum	Protocolos de enlaces de	X	X
			datos. (Unidad II)		
			Redes con sondeo		
			(Unidad IV)		
			Analisis de protocolos		
			(CISCO). Pract. Sem I.		
Monitoreo de Interfaces	Redes de Area Amplia	MRTG	Arquitectura de la red	X	X
de Enrutadores			(UNIDAD III)		
			Administracion y Monitoreo		
			de red (CISCO)		
			Semestre III y IV		

CAPÍTULO X. CONCLUSIONES Y RECOMENDACIONES.

Con el desarrollo de este estudio sobre la evaluación e implementación de herramientas de monitoreo de redes informáticas, se han establecido una serie de conclusiones sobre aspectos relevantes al tema de estudio, a la vez se presentan una serie de recomendaciones que se consideran necesarias para futuras modificaciones a la solución implementada.

10.1 Conclusiones

1. No existe un monitor de red que cumpla con todas las características deseadas, más bien para un propósito específico existe un monitor adecuado.

2. La interfaz Web elaborada permite reunir en una sola página Web los elementos más sobresalientes de las herramientas Netsaint, Ntop y MRTG, permitiendo así detectar y asistir en la solución de problemas de administración de red.

3. En base al estudio realizado se determinó que con respecto a los programas de distribución libre:

    a) Su funcionalidad le permite competir con software comercial.
    b) Existe el respaldo de una comunidad, en caso de necesitar asistencia.
    c) Existe una tendencia creciente de respaldo de grandes compañías (por ejemplo IBM,Oracle) referente al uso de los mismos.

10.2 Recomendaciones

1. Es necesario definir un mecanismo por parte del centro de computo para el acceso de la pagina Web de monitoreo, es recomendable que dicha restricción se haga definiendo que direcciones IP tendrán acceso al servidor donde está alojada la pagina Web.

2. En caso de crecimiento de la red, si se necesita incluirla en el sistema de monitoreo, seguir los pasos descritos en el anexo "B".

3. Con la documentación proporcionada (descripción de herramientas, guías del administrador e interfaz desarrollada), queda abierta la posibilidad para las personas encargadas del laboratorio de redes de elaborar guías de laboratorio adicionales que se apeguen al contenido de los cursos.

4. Fomentar al estudiante el uso de sistema operativo Linux como también los programas de libre distribución.

5. Para el personal de soporte técnico se recomienda la revisión periódica del monitor de red para garantizar la disponibilidad de los recursos de red, el buen uso en general de la red.

6. Es importante ir agregando nuevas características a la interfaz elaborada para mantenerla como una herramienta práctica en el monitoreo de redes. Se recomienda fomentar los aportes de la comunidad estudiantil para generar una segunda versión de la misma.

BIBLIOGRAFIA

[1] Craig Hunt Craig; Robert Bruce Thompson
TCP/IP Network Administration.
Oreilly and Associates.
USA, 1998.

[2] Steve Maxwell.
Red Hat Linux Network Management Tools.
McGraw- Hill.
USA, 2000.

[3] Kendal & Kendal
Análisis y diseño de sistemas.
Tercera edición.
Prentice Hall.
México, 1997.

[4] Douglas E. Comer
Computer Networks and Internet
3ra Edición, McGraw-Hill
USA

5] Craick Zacker; Paul Doyle
Upgrading and Reparing Networks
QUE
USA

6] Managing MultiVendors Networks
John Enck, Dan W. Blacharski
QUE
USA

Sitios web:

ttp://www.gnu.org

ttp://www.linux.org

GLOSARIO DE TERMINOS.

ADMINISTRACIÓN DE FALLAS:

asegurar la detección y el control de las fallas de red.

ADMINISTRACIÓN DE RED:

Término genérico que se usa para describir sistemas o acciones que ayudan a mantener, describir o solucionar los problemas de una red.

ADMINISTRACIÓN DE LA CONFIGURACIÓN:

Los subsistemas de administración de configuración son responsables por la detección y determinación del estado de una red.

ADMINISTRACIÓN DE RENDIMIENTO:

Los subsistemas de administración de rendimiento tienen la responsabilidad de analizar y controlar el rendimiento de la red, incluyendo el rendimiento y los índices de error

ADMINISTRACIÓN DE SEGURIDAD:

Los subsistemas de administración de seguridad son responsables por el control del acceso a los recursos de red.

ANCHO DE BANDA:

Describe la capacidad de una red para la transmisión de datos a través del medio.

ARP:

Protocolo de Resolución de Direcciones. Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC.

ARPWATCH:

Arpwatch rastrea las parejas ethernet/dirección IP. Registra su actividad a través de syslog e informa de ciertos cambios vía correo electrónico.

CATALYST:

Serie de switches de grupo de trabajo de Cisco que mejoran el desempeño de red de los grupos de trabajo cliente / servidor Ethernet.

CITT:

Centro de Investigación y Transferencia de Tecnología de la Universidad Don Bosco.

DNS:

Sistema de resolución de nombres de dominio.

ENRUTADOR (ROUTER):

Dispositivo de que se encarga de tomar decisiones a cerca de cuál es la ruta óptima para enviar el tráfico de red. Envía paquetes desde una red a otra basándose en la información de la capa de red.

ETHERNET:

Principal tecnología de redes de área local (LAN). que se ejecuta en la mayoría de las LAN.

ETHEREAL :

Analizador de tráfico de red para sistemas operativos Unix y clónicos.
Es más o menos una versión gráfica de "tcpdump".

FPING:

Programa ping que utiliza la petición de eco del Protocolo de Control de Mensajes Internet (ICMP) para determinar si el host objetivo está respondiendo. 'fping' se diferencia de ping en que se puede especificar cualquier numero de objetivos en la línea de comandos, o especificar un archivo conteniendo la lista de objetivos a hacer ping

GNU:
Sistemas de software de libre distribución, completo, compatible con Unix.

HOST:
Sistema informático en una red. Similar al término nodo , salvo que host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y routers.

HTTP:
El Protocolo de transferencia de hipertexto funciona con la World Wide Web.

INTERNET.
Término utilizado para referirse a la internetwork más grande del mundo, que conecta decenas de miles de redes de todo el mundo.

INTERNETWORK:
Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (en general) como una sola red.

INTERNETWORKING:
Término general utilizado para referirse a la industria que ha surgido en torno de la cuestión de la conexión de redes entre sí.

IPCONFIG:

verifica la configuración IP de una computadora que ejecuta sistema operativo Microsoft Windows NT.

ISO:

Organización Internacional para la Normalización. Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a la networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking.

LAN:

Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada.

MIB:

Base de información de administración. Base de datos de información de administración de la red utilizada y mantenida por un protocolo de administración de la red, por ejemplo, SNMP.

MONITOR DE RED:

Dispositivo de control de la red que mantiene información estadística con respecto al estado de la red y de cada dispositivo conectado a ella.

NETBIOS:

Sistema básico de entrada / salida de red. Interfaz de programación de aplicación que usan las aplicaciones de una LAN IBM para solicitar servicios a los procesos de red de nivel inferior. Estos servicios incluyen establecimiento y terminación de sesión, y transferencia de información.

NBTSTAT:

Muestra estadísticas de protocolos y las actuales conexiones de TCP/IP usando NBT (NetBIOS sobre TCP/IP).

NETSTAT:

Comando que proporciona un informe del estado en cada momento de las conexiones TCP/IP de un host .

NMAP:

Es básicamente un escáner de puertos, que permite comprobar los sistemas encendidos en la red y los servicios que estos ofrecen.

NODO:

Punto final de la conexión de red o una unión que es común para dos o más líneas de una
red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo

NOS:

Sistema operativo de red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos.

PING:

Instrucción utilizada por el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de red.

POP3:

Sistema rápido y eficaz de recibir y enviar correo de Internet, mediante el cual la conexión al servidor (buzón donde reside el correo) se realiza sólo cuando se recogen los mensajes.

PROTOCOLO:

Descripción formal de un conjunto de reglas y convenciones que rigen la forma en la que los dispositivos de una red intercambian información.

RMON:

Monitoreo remoto. Especificación del agente MIB que define las funciones del monitoreo remoto de dispositivos de la red.

SMTP:

Protocolo de transferencia de correo simple. Protocolo Internet que suministra servicios de correo electrónico.

SNMP:

Protocolo de administración de red simple. Protocolo de administración de red que se utiliza casi exclusivamente en redes TCP/IP. SNMP suministra un medio para supervisar y
controlar los dispositivos de red, y para administrar configuraciones, recoger estadísticas, el desempeño y la seguridad.

TCPDUMP:

Muestra las cabeceras de los paquetes que circulan por un interfaz de red Ethernet. Puede utilizarse para depurar problemas específicos de la red.

TCP/IP:

Protocolo de control de transporte / protocolo Internet. Nombre común para el conjunto de protocolos desarrollados por el Departamento de Defensa de los EE.UU. en los años '70 para soportar el desarrollo de internetwork a nivel mundial.

TELNET:

software de emulación de terminal (Telnet) tiene la capacidad de acceder de forma remota a otro computador

TRACE:

Comando que utiliza valores de tiempo de existencia (TTL) para generar mensajes desde cada router que se utiliza a lo largo de la ruta. Es muy poderoso en cuanto a su capacidad para ubicar fallas en la ruta desde el origen hasta el destino.

WAN:

Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por proveedores de servicio comunes

XTRACEROUTE:

Puede observar el camino que siguen los paquetes IP desde una computadora origen a un host distante sobre un mapa mundial gráfico. Comando exclusivo para sistemas UNÍX.

ANEXO “A”

Como agregar un nuevo equipo / Red al sistema de Monitoreo UDB.

Nuevo *Host*

En caso de requerir el monitoreo de la disponibilidad de un nuevo equipo de red o los servicios que este equipo ofrezca, se deberá hacer ciertos cambios en el archivo de configuración de NetSaint, llamado *hosts.cfg.*
Los cambios que deben realizarse son como sigue:

1. Ingresar al equipo en el cual esta instalado el monitor de red.
2. Accesar el directorio de instalación de NetSaint
3. Accesar el directorio /etc
4. Abrir con un editor el archivo *hosts.cfg*
5. Definir el *host* a monitorear en la sección ***hosts***.
6. De ser necesario crear un nuevo nombre de grupo para este *host*, en la sección ***groups.***
7. Incluir al *host* definido en el paso 5 en cualquier de los grupos existentes (en la sección *groups*).
8. En la sección ***services*** se deben definir los servicios que desean monitorearse.

Se puede consultar la documentación que acompaña la instalación de NetSaint en el caso de necesitar mayores detalles sobre el procedimiento anterior.

Nueva Red

En el caso de necesitarse el monitoreo de tráfico de una red externa al centro de cómputo que forma parte de la Intranet de UDB, esta podrá agregarse al monitoreo siempre y cuando se este utilizando una computadora con Linux funcionando como ***router***, en cuyo caso pueden seguirse los siguientes pasos:

1. Tomando como referencia los pasos de la guía de administrador de Ntop (anexo B), instalar Ntop en la computadora que se utilizara como ***router*** en la red externa.
2. En la computadora donde esta instalado el monitor de red crear las rutas estáticas (utilizando Linuxconf) para que las computadoras de monitoreo y la que se utilizara como ***router*** de la red externa puedan comunicarse.
3. Seguir los pasos del procedimiento anterior (**Nuevo Host**) para que la computadora que se utilizara como ***router*** de la red externa quede definida en el monitoreo de disponibilidad de equipos.
4. De ser necesario hacer los cambios requeridos en la interfaz de monitoreo para agregar los enlaces de las nuevas páginas html residentes en la computadora que funciona como ***router*** en la red externa.

ANEXO “B”

NTOP
(Network Top)

Guía del Administrador

1. Introducción

Ntop permite determinar los sistemas que están activos en una red y el tipo de tráfico enviado y recibido por estos sistemas.
El trafico de red es ordenado por protocolo, los protocolos de red más comunes son reconocidos, incluyendo la pila de protocolos TCP/IP.
A diferencia de otras herramientas de la misma categoría NTOP provee información estadística acerca de los paquetes de la red, no del contenido de los mismos.

Ntop no requiere el uso de un servidor Web para su funcionamiento, dado que soporta el protocolo HTTP internamente. Ntop es una herramienta de gran utilidad cuando se necesite determinar la actividad de la red en un momento determinado

1.1 Requerimientos de Instalación

Los requerimientos mínimos de instalación para Ntop Network Monitor son los siguientes:

- Red Hat Linux (o cualquier variante de Unix)
- Compilador C
- Procesador Pentium II o mayor (PIII recomendado)
- 64 MB de RAM (125 MB recomendado)
- 200 MB de espacio en disco libre
- TCP/IP configurado
- Derechos de administrador (root)

1.2 Licenciamiento

Ntop es software gratuito y puede ser utilizado, copiado, modificado etc. Conforme a los principios del software de distribución libre. Información sobre este tipo de licenciamiento puede ser encontrada en www.opensource.org

2. Instalación del programa

Los instaladores de NTop pueden obtenerse de http://ntop.org/download. Una vez que se cuentan con los archivos en formato tar.gz (el formato de comprensión de Linux) deben seguirse los siguientes pasos:

2.1 Descomprimir los archivos instaladores.

Para descomprimir los archivos de Ntop, digite desde la consola de Linux lo siguiente:

gunzip ntop-02.02.06.tar.gz
tar -xvf ntop-0.0.7.tar

Al finalizar la descompresión de los archivos se creara el directorio ntop-02-02-06 que ha sido creado en el directorio actual. Dentro de este directorio se encuentra los programas binarios de Ntop

2.2 Compilación de Archivos Binarios

Se creara el directorio base donde residirán los programas ejecutables de Ntop y luego se compilaran los archivos binarios:

cd (hacia el directorio donde estan los archivos binarios)
./configure
make (hace la compilación de los archivos binarios)
make check (hace una verificación pre instalación para determinar que no haya problemas)

make install (hace la instalación de los programas y de los archivos de ayuda)

make clean (hace una limpieza de los archivos temporales utilizados por la instalación)

1. Como iniciar Ntop

Para iniciar Ntop es necesario ejecutar la siguiente instrucción:

Ntop –d –w 3000

En este caso ntop estará esperando solicitudes en el puerto 3000 del servidor donde ha sido instalado.

Netsaint Network Monitor

Guía del Administrador

1. Introducción

Netsaint es un programa de monitoreo de *hosts* y servicios de red. Tiene la capacidad de enviar correos cuando sucede un problema y cuando este es resuelto. Netsaint esta escrito en lenguaje C y esta diseñado para correr bajo la plataforma Linux, sin embargo es compatible con la mayoría de versiones de Unix.

Este programa puede correr como un proceso normal o como un demonio [1], Realizando revisiones periódicas de los servicios especificados. Las revisiones periódicas de los servicios son ejecutados por módulos de programas externos a Netsaint que le proporcionan información al programa.

1.1 Requerimientos de Instalación

Los requerimientos mínimos de instalación para Netsaint Network Monitor son los siguientes:

- Red Hat Linux (o cualquier variante de Unix)
- Compilador C
- Procesador Pentium o mayor (PII recomendado)
- 32 MB de RAM (64 MB recomendado)
- 100 MB de espacio en disco libre
- TCP/IP configurado
- Apache Web Server
- Derechos de administrador (root)

1.2 Soporte Técnico

La instalación de Netsaint instala el manual del mismo, esta debe ser la primera fuente de referencia del programa.

[1] Es un proceso que corre en segundo plano y ejecuta operaciones especificas en tiempos predefinidos o en respuesta a ciertos eventos.

Otra fuente de referencia técnica son los foros de discusión sobre Netsaint los cuales se pueden encontrar en Internet, por tanto si no se puede encontrar la respuesta en el manual de referencia se puede buscar en los foros de discusión. Si la solución del problema no es encontrada en los archivos de los foros de discusión, puede publicarse un mensaje en el foro de discusión apropiado al tipo de problema en cuestión.

1.3 Licenciamiento

Netsaint es software gratuito y puede ser utilizado, copiado, modificado etc. Conforme a los principios del software de distribución libre. Información sobre este tipo de licenciamiento puede ser encontrada en www.opensource.org

2. Instalación del programa

Los instaladores de Netsaint pueden obtenerse de http://netsaint.org/download. Una vez que se cuentan con los archivos en formato tar.gz (el formato de comprensión de Linux) deben seguirse los siguientes pasos:

2.1 Descomprimir los archivos instaladores.

Para descomprimir los archivos de Netsaint, digite desde la consola de Linux lo siguiente:

```
gunzip netsaint-0.0.7.tar.gz
tar xf netsaint-0.0.7.tar
```

Al finalizar la descompresión de los archivos se creara el directorio Netsaint-0.0.7 que ha sido creado en el directorio actual. Dentro de este directorio se encuentra los programas binarios de Netsaint.

2.2 Compilación de Archivos Binarios

Se creara el directorio base donde residirán los programas ejecutables de Netsaint y luego se compilaran los archivos binarios:

mkdir /usr/local/netsaint

./configure

make all

make install

make install-config

make install-init

Luego de compilar los archivos binarios se formara una estructura de 5 subdirectorios, la siguiente tabla muestra el propósito de cada subdirectorio:

Sub-Directorio	Contenido
bin/	Programa principal de Netsaint
etc/	Los archivos de configuración netsaint.cfg, hosts.cfg, resource.cfg, and nscgi.cfg.
sbin/	CGIs
Share/	Archivos HTML (para la interface web y la documentación en línea)
var/	Directorio vacío para los archivos historiales (logs)

2.3 Instalación de Módulos

La siguiente parte de la instalación de Netsaint comprende la compilación de los módulos que ejecutaran la verificación de los servicios y de los equipos, los cuales constituyen la base del monitoreo. Estos se encuentran en el archivo **netsaint-plugins-1.2.9-4.tar.gz** , luego de la compilación los módulos residirán en el directorio libexec/ ubicado en el directorio donde se ha instalado Netsaint.

gunzip netsaint-plugins-1.2.9-4.tar.gz

tar -xvf netsaint-plugins-1.2.9-4.tar

cd netsaint-plugins-1.2.9-4

./configure

make all

make install

2.4 Instalación de la Interface Web

Como requisito para la instalación de la interface Web es necesario que se este utilizando como servidor Web a Apache, dentro del ambiente Linux generalmente este el preferido para servidores Web.

Configuración de Alias para archivos HTML y CGIs

Con el propósito de hacer accesibles desde navegadores web los archivos HTML y CGIs es necesario hacer ciertos cambios en la configuración del servidor Web.

cd /etc/httpd/conf/httpd.conf

pico httpd.conf

Desplácese hasta la parte de declaración de alias y agregue la siguiente línea:

Alias /netsaint/ /usr/local/netsaint/share/

Lo anterior permite que netsaint pueda ser accesado utilizando un URL como http://servidor/netsaint/, donde servidor es el nombre de la pc donde Netsaint ha sido instalado.

A continuación se harán los cambios en la configuración del servidor Web para permitir el acceso de los CGI, utilizando la nomenclatura de URL http://servidor/cgi-bin/netsaint/.

Dentro del archivo de configuración desplácese hasta la parte de declaraciones de **ScriptAlias**, agregue la siguiente línea al principio de las declaraciones:
ScriptAlias /cgi-bin/netsaint/ /usr/local/netsaint/sbin/

Una vez se hayan completado los cambios en el archivo de configuración de Apache, es necesario reiniciar el servidor web, para lo cual debe utilizar el siguiente comando:

/etc/rc.d/init.d/httpd restart

3. Configuración del programa

La configuración de netsaint se lleva a cabo con la edición de dos archivos: el archivo de configuración principal y el archivo donde se agregan los nodos a monitorear

3.1 Archivo de configuración principal.

Durante la instalación de netsaint se genera el archivo **netsaint.cfg**, en este archivo se definen la ubicación y nombres de los otros archivos de configuración, temporales y de sistema.

Usualmente no es necesario hacer ningún cambio en este archivo a menos que se desee realizar cambios en los parámetros originales del programa. En caso de necesitar realizar algún cambio el archivo se encuentra ubicado en /usr/local/netsaint/etc, cada parámetro de configuración esta bien detallado. A continuación se incluye un fragmento con los parámetros de configuración más importantes de este archivo:

```
##############################################################
#
# Ejemplo de archivo NETSAINT.CFG para NetSaint 0.0.6
#
##############################################################

# Define donde se guardara el historial de inicio o cierre del
# programa

log_file=/usr/local/netsaint/var/netsaint.log
     b
# Define donde esta ubicado el archivo de configuración donde # se
definen los equipos que se monitorearan

cfg_file=/usr/local/netsaint/etc/hosts.cfg

# Especifica el nombre y ubicación del archivo de
# Configuración de módulos

cfg_file=/usr/local/netsaint/etc/commands.cfg
```

```
# Archivo de estados
# Es donde se almacena el estado actual de los servicios y #
# equipos monitoreados.

status_file=/usr/local/netsaint/var/status.log


# Usuario NETSAINT
# Define con que usuario se correra el programa


netsaint_user=netsaint


# Grupo NETSAINT
# Define con que grupo se correra el programa

netsaint_group=netsaint


# Modo del programa
# Define el modo inicial con que correra Netsaint, hay dos
# valores posibles Modo activo y modo pasivo. Recomendamos no #
cambiar el valor por defecto (a)

program_mode=a



# Archivo Temporal
# Define el nombre y ubicación del archivo que se utilizara
# como almacenamiento de variables temporales del sistema

temp_file=/usr/local/netsaint/var/netsaint.tmp


# Metodo de Rotación de los registros
# Este define el metodo a utilizar para la rotación del
# historial de Netsaint.Los pobiles valores son los
# siguientes:
#      n      = Ninguno, no existe rotación de historial
#      h      = Rotación cada hora
#      d      = Rotación diaria
#      w      = Rotación semanal
#      m      = Rotación mensual

log_rotation_method=n
```

3.2 Archivo de configuración equipos a monitorear

Durante la edición de los archivos deben tomarse en cuenta lo siguiente:

1. Las líneas que comienzan con un carácter "#" es tomada como comentario y no será procesado por el programa.

2. Los nombres de variables deben comenzar al inicio de las líneas, no son permitidos los espacios en blancos antes del nombre.
3. Los nombres de las variables son sensibles al uso de mayúsculas y minúsculas.

Un ejemplo del archivo de configuración es creado durante la instalación de Netsaint. El nombre del archivo de configuración de equipos a monitorear se llama **hosts.cfg** que esta ubicado en el directorio **/usr/local/netsaint/etc/.**
A continuación se incluye un fragmento con los parámetros de configuración más importantes de este archivo:

```
##############################################
# Ejemplo de hosts.cfg para Netsaint.
#
##############################################

# La definicios de host es utilizada para defini un servidor
# Fisico, estación de trabajo, dispositivo, etc. que reside
# en la red.

host[es-gra]=ES-GRA Server;192.168.0.1;;check-host-alive;3;120;24x7;1;1;1;


# La definición de grupos es utilizado para agrupar uno o mas hosts juntos
# con el proposito de simplificar notificaciones.
# Formato: hostgroup[<Nombre_de_grupo>]=<alias_grupo>;<grupos_contactos>;<hosts>

hostgroup[nt-servers]=All NT Servers;nt-admins;rosie,dev,liatris


# La definición de contactos
# La definición de contactos es utilizado para identificar quien debe ser contactado
# cuando ocurra un problema en la red.

contact[egalstad]=Ethan Galstad;24x7;24x7;1;1;1;1;1;1;notify-by-email,
notify-by-epager;host-notify-by-epager;egalstad@nospam.extension.umn.edu;
pagegalstad@pagenet.com


# La definición de servicios es utilizado para determinar que servicio se monitoreara de un equipo
# determinado.

service[rosie]=FTP;0;24x7;3;5;1;nt-admins;120;24x7;1;1;1;;check_ftp
service[dev]=HTTP;0;24x7;3;5;1;nt-admins;240;24x7;1;1;1;;check_http2!192.168.0.2!/!88
service[real]=Zombie Processes;0;24x7;3;5;1;linux-
admins;240;24x7;1;1;1;;check_procs!5!10!Z
```

4. Como iniciar Netsaint

Existen cuatro diferentes formas en las que se puede iniciar Netsaint:

1. Manualmente, como un proceso corriendo en primer plano.
2. Manualmente, como un proceso corriendo en segundo plano.
3. Manualmente. Como un ***Daemon***
4. Automáticamente al iniciar Linux.

4.1 Manualmente, como un proceso corriendo en primer plano.

Este método es el recomendado cuando se quiere investigar alguna posible falla en el programa, dado que todo lo que el programa esta realizando será mostrado en pantalla. Para correr NetSaint como un proceso en primer plano se deben seguir los siguientes pasos:

[root@monitor /root]# cd ..

[root@monitor /]# cd /usr/local/netsaint/bin/

[root@monitor bin]# ./netsaint /usr/local/netsaint/etc/netsaint.cfg

Para parar este tipo de corrida simplete presione ctrl.+ c.

4.2 Manualmente, como un proceso corriendo en segundo plano.

Para correr NetSaint como un proceso en Segundo plano, se deben realizar los siguientes pasos:

[root@monitor /root]# cd ..

[root@monitor /]# cd /usr/local/netsaint/bin/

[root@monitor bin]# ./netsaint /usr/local/netsaint/etc/netsaint.cfg &

Nótese que la variación respecto al método anterior es que se agrega el carácter & al final de la última instrucción.

4.3 Manualmente. Como un *Daemon.*

Para poder ejecutar Netsaint como un proceso del sistema, lo cual se conoce como *daemon* en el ambiente de Linux, se debe utilizar el parámetro **–d** al iniciar el programa:

root@monitor /root]# cd ..

[root@monitor /]# cd /usr/local/netsaint/bin/

[root@monitor bin]# ./netsaint –d /usr/local/netsaint/etc/netsaint.cfg

4.4 Automáticamente al iniciar Linux.

Este es el método recomendado, con el cual se puede estar seguro que Netsaint iniciara al iniciar el sistema operativo. Para lograr lo anterior es necesario crear un *script* de inicio en el directorio **/etc/rc.d/init.d/**.

Durante la instalación la instrucción make install-init se encarga de realizar los cambios necesarios para que Netsaint inicie automáticamente.

5. Como Detener / reiniciar NetSaint

La siguiente tabla detalla las instrucciones que deben invocarse para, reiniciar o recargar la configuración de Netsaint.

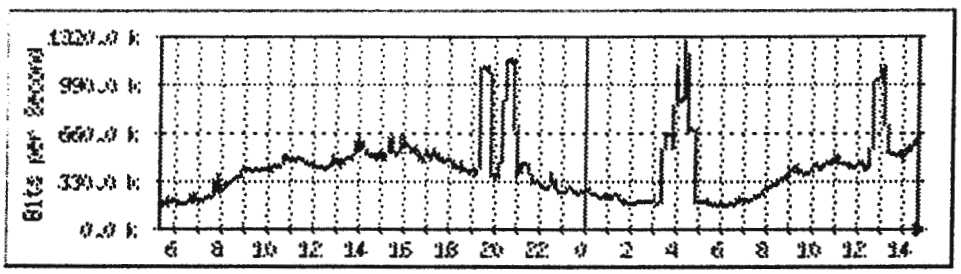
Acción	Instrucción	Descripción
Detener NetSaint	**/etc/rc.d/init.d/netsaint stop**	Detiene el programa por completo.
Reiniciar NetSaint	**/etc/rc.d/init.d/netsaint restart**	Reinicia NetSaint.
Recargar la configuración	**/etc/rc.d/init.d/netsaint reload**	Solicita a NetSaint volver a leer los archivos de configuración y si hay cambios hacerlos efectivos en el monitoreo.

MRTG

Guía del Administrador

1. Introducción

Multi-Router Traffic Grapher puede monitorear y graficar el trafico de la red obtenidos de dispositivos que utilizan **SMNP**. Como el nombre lo indica, muestra la utilización de trafico y otra información estadística obtenida de enrutadores y otros dispositivos de red. Genera páginas html e imágenes gif proporcionando una representación visual del rendimiento de la red vía navegadores Web.



El método principal que MRTG utiliza para recolectar información es el comando **snmpget.** Sin embargo se puede personalizar MRTG para mostrar información derivada de otras fuentes. Por ejemplo, MRTG puede mostrar la carga y utilización de espacios en disco de un sistema unix. Como resultado de estas capacidades, hay muchos usos prácticos para MRTG incluyendo, pero no limitado a lo siguiente:

- ✓ desplegar el uso de red en enlaces LAN y WAN.
- ✓ Desplegar la carga de cpu en dispositivos de red.
- ✓ Desplegar utilización de memoria en dispositivos de red.
- ✓ Desplegar la utilización de MODEM en un enlace a acceso remoto.

1.1 Requerimientos de Instalación

Los requerimientos mínimos de instalación para MRTG son los siguientes:

- Red Hat Linux (o cualquier variante de Unix)
- Compilador C
- Procesador Pentium
- 32 MB de RAM
- 50 MB de espacio en disco libre

- TCP/IP configurado
- Apache Web Server.
- Derechos de administrador (root)
- Lenguaje Scripting PERL instalado.
- Librerías gd, libpng, zlib instaladas.

1.2 Soporte Técnico

La instalación de MRTG instala el manual del mismo, esta debe ser la primera fuente de referencia del programa.

Otra fuente de referencia técnica son los foros de discusión sobre MRTG los cuales se pueden encontrar en Internet, por tanto si no se puede encontrar la respuesta en el manual de referencia se puede buscar en los foros de discusión. Si la solución del problema no es encontrada en los archivos de los foros de discusión, puede publicarse un mensaje en el foro de discusión apropiado al tipo de problema en cuestión.

1.3 Licenciamiento

MRTG es software gratuito y puede ser utilizado, copiado, modificado etc. Conforme a los principios del software de distribución libre.

Información sobre este tipo de licenciamiento puede ser encontrada en www.opensource.org

2. Instalación del programa

Previo a la instalación de MRTG deben instalarse ciertas librerías que permitirán la generación de los archivos gráficos.

2.1 Instalación de librerías (pre-instalación)

Librerías Zlib

Puede obtener los instaladores de esta librerías de la siguiente dirección de Internet: **http://www.gzip.org/zlib/zlib-1.1.4.tar.gz.**

Luego hay que ejecutar las siguientes instrucciones:

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

Librerías LibPng

Puede obtener los instaladores de esta librerías de la siguiente dirección de Internet: **http://www.libpng.org/pub/png/src/libpng-1.0.12.tar.gz**

Luego hay que ejecutar las siguientes instrucciones:

```
wget http://www.libpng.org/pub/png/src/libpng-1.0.12.tar.gz
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 ..
```

Librerías Gd

Puede obtener los instaladores de esta librerías de la siguiente dirección de Internet: http://www.boutell.com/gd/http/gd-1.8.3.tar.gz

Luego hay que ejecutar las siguientes instrucciones:

```
gunzip -c gd-1.8.3.tar.gz |tar xf -
mv gd-1.8.3 gd
cd gd
```

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

2.2 Instalación de MRTG (compilación)

Los instaladores de Netsaint pueden obtenerse de http://people.ee.ethz.ch/~oetiker/webtools/mrtg/pub/mrtg-2.9.22.tar.gz . Una vez que se cuentan con los archivos en formato tar.gz (el formato de comprensión de Linux) deben seguirse los siguientes pasos:

cd /usr/local/src
gunzip -c mrtg-2.9.22.tar.gz | tar xvf -
cd mrtg-2.9.22
./configure --prefix=/usr/local/mrtg-2
make
make install

3. Configuración de SNMP en equipos Cisco

Antes de configurar MRTG en un equipo Cisco es necesario habilitar SNMP en dicho equipo, para ello pueden seguirse los siguientes pasos:

snmp-server community 5urf5h0p RO

snmp-server location Universidad Don Bosco Soyapango

snmp-server contact net-admin@citt.cdb.edu.sv

snmp-server enable traps

snmp host 168.243.3.1 traps SNMPv1

A continuación se detalla el propósito de cada comando:

Comando	Utilizado para
snmp-server community 5urf5h0p RO	Asigna un *community* de solo lectura. Solo consultas de lecturas son permitidas. En este caso el *community* 5urf5h0p no permite realizar cambios en la configuración del equipo
snmp-server location Universidad Don Bosco Soyapango	Para propósitos administrativos especifica la ubicación del equipo
snmp-server contact net-admin@citt.cdb.edu.sv	Especifica el nombre del contacto en caso ocurra un problema con el SNMP.
snmp-server enable traps	Habilita SNMP para que notifique cuando ocurren cambios de: configuración, variables ambientales y condiciones criticas del equipo.
snmp host 168.243.3.5 traps SNMPv1	Identifica el equipo al que serán enviadas las notificaciones especificadas en el comando anterior.

Generalmente para que MRTG pueda funcionar correctamente unicamente es necesario ejecutar las primeras tres lineas de commando del procedimiento anterior.

4. CONFIGURACION DE MRTG

MRTG utiliza un archivo de configuración para especificar cuales dispositivos serán monitoreados. Los instaladores de MRTG no vienen acompañados por una configuración predefinida porque los dispositivos listados variarían de red a red. En lugar de ello los instaladores incluyen un programa llamado ***CFGMAKER***, el cual es utilizado para construir configuraciones básicas. El propósito de este programa es analizar un dispositivo de red que utiliza SNMP y construir un archivo de configuración el cual luego puede personalizarse.

La sintaxis de **cfgmaker** es como sigue:

cfgmaker cominnity@device

Dos parámetros son requeridos: El ***community*** asignado al dispositivo y la dirección IP o nombre de host.

Para ilustrar el uso de este programa de configuración, asumamos que queremos monitorear un router cisco 7500, llamado ***remote-wg***, con nombre de ***community*** UDB. En base a esto la instrucción de comando seria:

cfgmaker UDB@remote-gw > cisco.conf

El comando anterior construirá un archivo de configuración mrtg el cual tendrá el nombre de cisco.conf. Asumiendo que los parámetros provistos al cfgmaker son correctos y que el dispositivo responde a la solicitudes SNMP, el siguiente listado muestra la configuración que se generaría:

```
# Created by Hugo Orellana
# ./cfgmaker --global 'WorkDir: /var/www/html/mrtg' --global 'Options[_]: bits,growright' --#
output /usr/local/mrtg-2/bin/e1.cfg mrtg@168.243.3.1

#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

WorkDir: /var/www/html/mrtg
Options[_]: bits,growright
##################################################################
# System: remote-gw
# Description: Cisco Internetwork Operating System Software
#          IOS (tm) RSP Software (RSP-DSV-M), Version 12.1(7), RELEASE SOFTWARE
(fc1)
#       Copyright (c) 1986-2001 by cisco Systems, Inc.
#       Compiled Wed 21-Feb-01 15:36 by kellythw
# Contact:
# Location:
##################################################################


### Interface 1 >> Descr: 'Ethernet0' | Name: 'Se0/0' | Ip: '' | Eth: '' ###

Target[168.243.3.1_1]: 1:mrtg@168.243.3.1:
SetEnv[168.243.3.1_1]: MRTG_INT_IP="" MRTG_INT_DESCR="Ethernet0"
MaxBytes[168.243.3.1_1]: 193000
Title[168.243.3.1_1]: Traffic Analysis for 1 -- remote-gw
PageTop[168.243.3.1_1]: <H1>Traffic Analysis for 1 -- remote-gw</H1>
 <TABLE>
  <TR><TD>System:</TD>     <TD>remote-gw in </TD></TR>
  <TR><TD>Maintainer:</TD> <TD></TD></TR>
  <TR><TD>Description:</TD><TD>Ethernet0 Red UDB </TD></TR>
  <TR><TD>ifType:</TD>     <TD>ppp (23)</TD></TR>
  <TR><TD>ifName:</TD>     <TD>Se0/0</TD></TR>
```

```
  <TR><TD>Max Speed:</TD>  <TD>1544.0 kbits/s</TD></TR>
 </TABLE>


 ### Interface 2 >> Descr: 'Serial0' | Name: 'Se0/1' | Ip: '' | Eth: '' ###

 Target[168.243.3.1_2]: 2:mrtg@168.243.3.1:
 SetEnv[168.243.3.1_2]: MRTG_INT_IP="" MRTG_INT_DESCR="Serial0"
 MaxBytes[168.243.3.1_2]: 193000
 Title[168.243.3.1_2]: Traffic Analysis for 2 -- remote-gw
 PageTop[168.243.3.1_2]: <H1>Traffic Analysis for 2 -- remote-gw</H1>
  <TABLE>
   <TR><TD>System:</TD>     <TD>remote-gw in </TD></TR>
   <TR><TD>Maintainer:</TD> <TD></TD></TR>
   <TR><TD>Description:</TD><TD>Serial0 Enlace Internet UDB</TD></TR>
   <TR><TD>ifName:</TD>     <TD>Se0/1</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>1544.0 kbits/s</TD></TR>
  </TABLE>
```

En este caso en particular el ***router*** tiene tres interfaces (una ethernet y dos seriales), pero cfgmaker solo reporta dos interfaces. Porque la tercera interfase esta administrativamente apagada, cfgmaker omite esta interfase. EL archivo de configuración mrtg utiliza el formato de html, en particular construye una tabla para mostrar la información del dispositivo, esta tabla se denota por las instrucciones HTML <TABLE> y </TABLE>. La configuración también incluye una o mas palabra reservadas que controlan que dispositivos son monitoreados y como la información es graficada.

Target[etiqueta]:puerto:community@dispositivo

En esta instrucción el parámetro etiqueta se refiere a la dirección IP del equipo que se esta monitoreando y puerto es el número de la interface.

Ejemplo:

Target[168.243.3.1]:1:public@168.243.3.1

MaxBytes

Define el limite superior para las estadísticas de trafico y determina el rango del eje Y para los gráficos.

El valor de MaxBytes es generalmente especificado en *bytes* por segundo.

Ejemplo:

MaxBytes[168.243.3.1_1]: 193000

Title

Permite definir el texto que aparecerera en una interfaz particular que esta siendo monitoreada.

Ejemplo:

Title[168.243.3.1_1]: Traffic Analysis for 1 -- remote-gw

PageTop

Permite especificar información adicional que aparecerá al inicio del reporte, de esta forma puede ser más descriptiva la información de la interfaz.

Ejemplo:

PageTop[168.243.3.1_2]: <H1>Traffic Analysis for 2 -- remote-gw</H1>

5.Como iniciar MRTG

Asumiendo que el archivo de configuración de MRTG se llama cisco.conf, la instrucción para iniciar MRTG es como sigue:

cd /usr/local/mrtg/bin

mrtg cisco.conf

ANEXO “C”

	GUÍA No.	

acultad : Ingeniería.
scuela : Electrónica.
signatura : Protocolos de Comunicación
tulo : Análisis de tramas y protocolos.

OBJETIVO

1. Capacidad de análisis del tráfico de una red.
2. Utilizar una herramienta de dominio público (tcpdump) para el análisis de protocolos.
3. Distinguir los distintos protocolos y servicios.
4. Capturar tramas para su posterior análisis.

INTRODUCCIÓN TEORICA

pdump es una herramienta de red elaborada en la Universidad de California (Lawrence Berkeley ational Laboratory, LBNL) para el monitoreo de redes. Permite monitorear tanto una interfaz hernet como una comunicación punto a punto (por ejemplo: interfaz serial).
pdump es un programa de red que pone la tarjeta de red en *modo promiscuo:* recibe todos los quetes/tramas que pasan por esa interfaz independientemente de que la dirección MAC destino sea la la tarjeta (normalmente la tarjeta solo captura aquellas tramas que contienen su dirección destino). o significa que **tcpdump** captura todas las tramas que pasan por la interfaz a la que esta conectada.
pdump usa un software llamado BPF (BSD Packet Filter) que le permite poner la tarjeta en modo omiscuo, de forma que cada vez que se transmite o se recibe una trama por el controlador *(driver)* de la jeta de red, BPF recibe una copia de esa trama. De esta forma BPF puede procesar y filtrar los quetes de red que el usuario considera más interesantes: el comando **tcpdump** permite filtrar por otocolos (ip, tcp, udp, arp, ether, fddi, ...), por interfaz (eth0, S0), por puerto TCP/UDP o dirección IP.

PROCEDIMIENTO

tes de pasar al desarrollo de la practica es necesario conocer el formato de salida de **tcpdump**.
formato general de salida del **tcpdump** es el siguiente:
ha src > dst: flags data-sqno ack window urgent options

nde:

ha:
la hora en que se produjo el evento en formato

ra:minutos:segundos.microsegundos:
milisegundos dependiendo de la resolución del reloj).

y dst:
n las direcciones IP y puertos TCP/UDP de las conexiones fuente y destino.

ags:
ɔn una combinación de los posibles flags de un segmento/datagrama TCP/UDP: S (SYN), F (FIN), P 'USH), R (RST).

ıta-sqno:
escribe el número de secuencia de la porción de datos.

ɔk:
ɜ el número de secuencia del próximo byte que espera recibir el otro extremo
ɔP/UDP.

indow:
ɜ el tamaño de la ventana que advierte el receptor al transmisor.

'gent:
dica que hay datos urgentes en ese segmento/datagrama.

ptions
ɔn las opciones TCP que suelen estar entre corchetes del tipo < >, por ejemplo el tamaño máximo del gmento (ejemplo. <mss 1024>)

ɔr ejemplo ejecutando el comando:

ɔot@galatzo/root]# tcpdump -i eth0

observa todo lo que pasa por la tarjeta de red de la PC. Una línea de salida de **tcpdump** sería:
':58:58.470000 giralt.ac.upc.es.6000 > galatzo.ac.upc.es.4228: P 1191656817:1191656849(32) ack 35973568 win 61320 (DF)

ɔnde se indica que a las 17:58:58.470000 se recibió una trama con origen giralt (nombre de una áquina) y destino galatzo (hay una opción para que escriba las direcciones IP en vez de los nombres). s puertos TCP usados son el 6000 en origen y el 4228 en destino. P indica que el flag PUSH del gmento TCP estaba activado. Giralt ha enviado 32 bytes de datos con números de secuencia mprendidos entre el 1191656817 y el 1191656849. Como la conexión estaba ya empezada cuando se ɔnitorizo la conexión, los números de secuencia son absolutos.

tcpdump monitoriza una conexión desde el inicio, los números de secuencia son relativos al número secuencia inicial. Giralt reconoce haber recibido de galatzo el dato 2435973567 y espera que el ɔximo que envíe sea el 2435973568. Finalmente, giralt anuncia una ventana de 61320 y avisa que no fragmenten los datagramas IP.

rea 1:
se desea ver el contenido del paquete en hexadecimal podemos ejecutar el comando:
***ɔdump** -x -s100 -i eth0*, que nos indica que capturemos los primeros 100 bytes (incluidos cabeceras IP TCP/UDP y excluidas las cabeceras Ethernet) del paquete. De esta forma también podemos observar lores de la cabecera IP (ejemplo: TTL, tipo).

rea 2:
ıta: Averigüe cual es la dirección IP de la computadora de su compañero de al lado.
ra visualizar todos los paquetes de datos que llegan desde o parten hacia el host de su compañero ıite la siguiente línea de comando

ot@galatzo/root]# tcpdump host [Dir_IP_Compañero]

i no se produce ninguna actividad entre las dos computadoras, pídale a su compañero que realice ping acia su computadora.
note algunas líneas del resultado para su posterior análisis.
ıtercambien roles con su compañero.

area 3: Analizando paquetes IP.

ara visualizar todos los paquetes IP entre dos nodos utilice la siguiente línea de comando:

ɔot@galatzo/root]# tcpdump ip host [Dir_IP_Compañero]

area 4:
l objetivo de este ejercicio es observar los distintos campos del protocolo IP. Para ello capturaremos con :**pdump** una conexión ftp (dale el username y el password y a continuación desconectate). Por ejemplo ıa conexión ftp con origen en la máquina galatzo y destino la maquina rogent sería:
alatzo:~> ftp v rogent
onnected to rogent.ac.upc.es.
20 rogent FTP server (SunOS 5.7) ready.
ame (rogent:joseb):
31 Password required for joseb.
assword:
30 User joseb logged in.
emote system type is UNIX.
sing binary mode to transfer files.
ɔ> bye
21 Goodbye.
alatzo:~>
a captura con el **tcpdump** tiene que ser de forma que obtengais el contenido de los datagramas IP (flag del **tcpdump**

. Investigación Complementaria.

1. Investigue el formato de la trama TCP y defina cada uno de sus componentes.
2. Investigue a que se refiere el termino "Saludo de tres vías"
3. Que es una ventana deslizante

eferencias.

tp://www.tcpdump.org

	GUÍA No. 3 **Monitoreo de Redes**	

acultad : Ingeniería.
scuela : Electrónica.
signatura : Redes de Área Local.

OBJETIVO

Utilizar herramientas de dominio público **(Cheops y Etherape)**, como herramientas para el monitoreo de tráfico y el monitoreo de los estados de servicios en los host s que forman parte de una red.

INTRODUCCIÓN TEORICA

Existen varias razones por las que hay que "vigilar" una red, pero los dos motivos principales son predicción de los cambios para el crecimiento en el futuro y la detección de sucesos no esperados en estado de la red, como por ejemplo: fallas de dispositivos de red, inaccesibilidad de servicios (Correo ectrónico, Internet, bases de datos, etc). Si no se posee un plan de monitoreo de red, la persona cargada de administrarla, solo es capaz de reaccionar a los problemas a medida que estos se den, en ıar de prevenirlos.

Uno de los métodos básicos usados por los administradores de una red se da diariamente en el ɔmento en que los usuarios comienzan a conectarse a dicha red; en este momento se verifica si las nexiones funcionan correctamente; de lo contrario, será necesario contactar al administrador para que te se encargue de resolver el problema.

Existen programas de operación sencilla que permiten que el administrador ingrese una grupo de ecciones IP de los computadores, y se ejecuta el comando "ping" a estas direcciones de forma riódica. Si se detecta un problema de conexión, el programa advierte al administrador que existe un ɔblema de conexión. Otra desventaja de este tipo de monitoreo es que el comando "ping" solamente ɜ indica que determinado host tiene problemas de conectividad a la red, sin embargo no monitorea otro

ɔo de aplicaciones o servicios que pudieran estarse ejecutando en dicho host como por ejemplo ervicios de Correo Electrónico, WEB, FTP, DNS, Telnet, etc.

En conclusión el uso de "ping" es una forma ineficiente de monitoreo de red, sin embargo es referible realizar este tipo de pruebas en lugar de no hacer absolutamente nada.

ue es un Monitor de red?

Un Monitor de Redes de Computadores es un instrumento que entrega datos acerca de la red en cual esta conectado, para extraer de ella información de tipo estadístico, evolución de parámetros de ıncionamiento, histogramas, tráfico por cada enlace, estado de los servicios, etc. Esta información es ıostrada en forma de gráficos que hacen más fácil su interpretación.

. MATERIAL Y EQUIPO.

1. Una pc con sistema operativo Linux.
2. Conexión a Internet.

'. PROCEDIMIENTO

ARTE I: DESCUBRIMIENTO DE RED Y MONITOREO DE SERVICIOS CON CHEOPS.

Cheops es una herramienta de administración de red para mapear y monitorear la red. Posee una ncionalidad de descubrimiento automático de red y de hosts, así como también la capacidad de ɜtectar el sistema operativo que se ejecuta en la estación de trabajo monitoreada.

heops es capaz de examinar las estaciones de trabajo para observar que servicios se ejecutan en ellas. ara algunos servicios, cheops actualmente es capaz de ver que programa se encuentra ejecutándose ara un servicio determinado y la versión del programa, por ejemplo puede detectar para un servicio http ue se ejecutando, a través del programa Internet Information Server 4.0 (IIS 4.0).

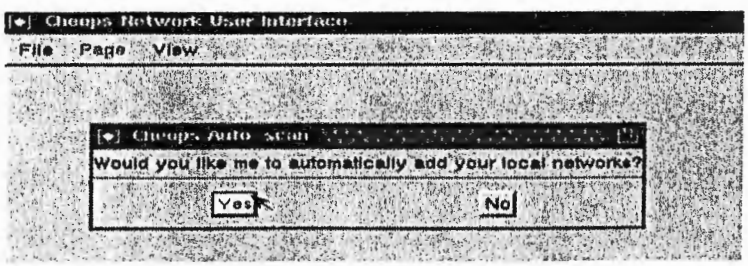
Ingrese al modo gráfico de su sistema operativo Linux:

ɔot@linux /root]#startx

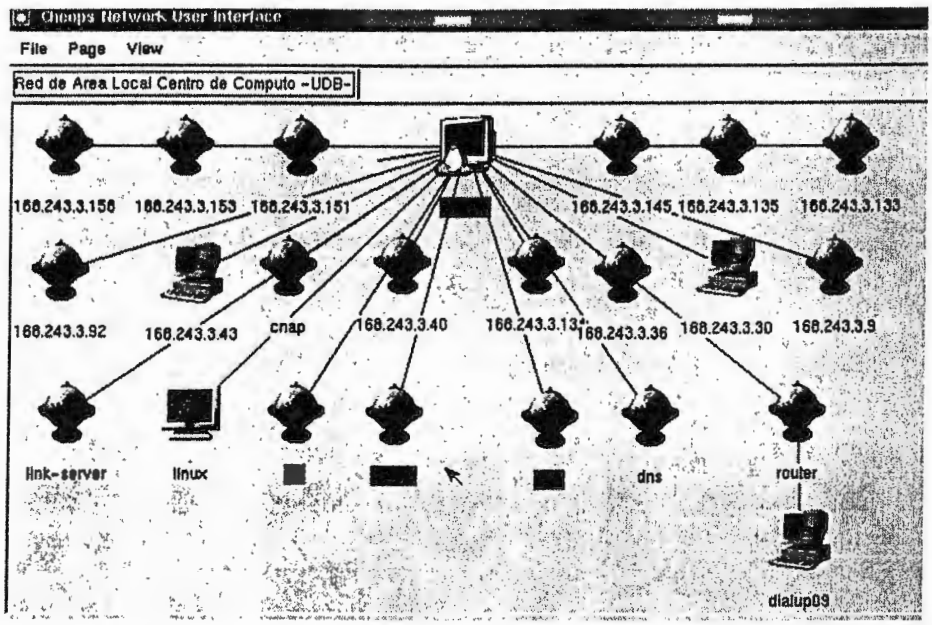
Ejecute el programa cheops con la siguiente línea de comando, abriendo una emulación de terminal

ɔot@linux /root]#cheops

ɔarecerá una ventana donde se pregunta si se desea que se realice el descubrimiento automático de la d. Presione "Yes".

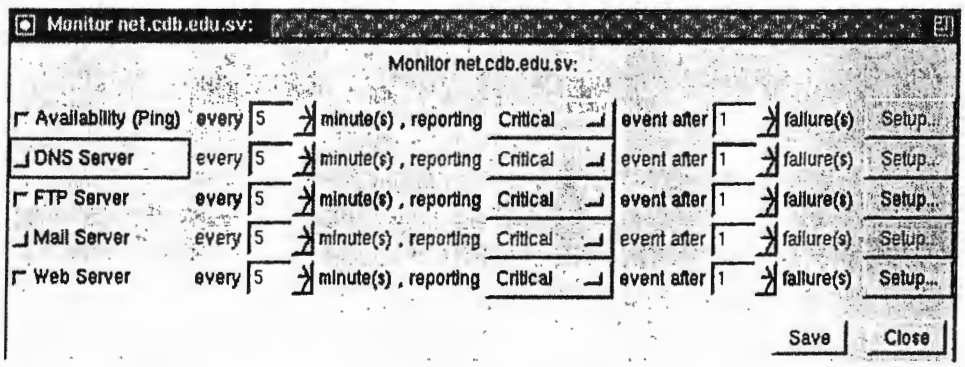


Aparecerá un área donde cheops muestra los host que pertenecen a la red a la cual esta conectado.



egún el esquema, que resultados son obtenidos por cada hosts?

Seleccione una de las computadoras que aparecen en el panel, y haga clic derecho y seleccione la ción "Monitoring..."



serve que en esta ventana pueden establecerse las variables que se pueden monitorear en los hosts. tablezca para el host que usted ha seleccionado las siguientes variables para monitorear: availability, eb Server y FTP Server. Finalmente haga clic en el botón save.

elva al panel donde aparecen los host y observe que pasa con el host a cual se le establecieron los rámetros de monitoreo. Que observa:

Sobre el host que establecio los parametros de monitoreo de un clic derecho y escoja la opción "Event log". Que es lo que observa

_____

_____

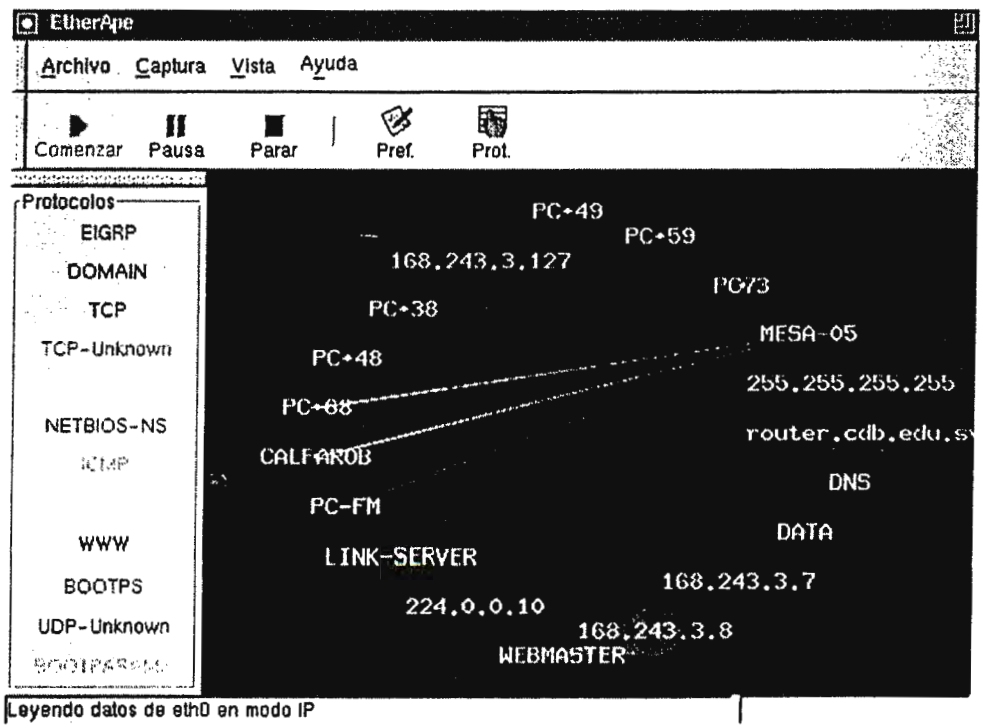
ARTE II: MONITOREO DE TRAFICO DE PROTOCOLOS EN UNA RED.

Etherape es un monitor de red gráfico creado para sistemas operativos UNÍX. Despliega áficamente la actividad de la red, donde el trafico generado por cada protocolo se identifica con un color specífico. Etherape soporta Ethernet, FDDI, Token Ring, ISDN, PPP y SLIP.
ntes de empezar con cada uno de los pasos, debe conocer cual es la dirección IP de su computadora.

uede conseguir su propia dirección ejecutando el comando: [root@linux /root]#ifconfig

Ingrese al modo gráfico de su sistema operativo Linux:
oot@linux /root]#startx
Ejecute el programa etherape con la siguiente línea de comando, abriendo una emulación de terminal
oot@linux /root]#etherape

sted obtendrá una ventana similar a esta:



ste los protocolos que se estan ejecutando en la red:

Haga clic en el botón "Prot." que se encuentra en la barra superior de la interfaz de Etherape. Y llene la siguiente tabla por lo menos con la información de 7 protocolos.

Protocolo	Tráfico Instantáneo	Tráfico Acumulado	Última Vez	Paquetes

Abra una emulación de terminal y ejecute la siguiente línea de comando

ɔot@linux /root]#ping [Dir_Ip]

ıora verifique lo que sucede en el panel de Etherape. Anote sus resultados:

l. Investigación Complementaria.

1. Investigue sobre las principales tareas de un administrador de red.
2. Que otros software de distribución libre recomendaría para la tarea de monitoreo de redes.
3. Investigue sobre la operación de el protocolo SNMP para la administración y monitoreo de redes.

eferencias.

tp://www.cdb.edu.sv/monitor (ver sección monitoreo de estados y monitoreo de tráfico)

tp://software.linux.com/projects/

	GUÍA No. 3	

acultad : Ingeniería.
scuela : Electrónica.
signatura : Comunicación de Datos
ítulo : Análisis y Escaneo de Puertos.

OBJETIVO

1. Utilizar una herramienta de dominio público ***(nmap)***, para detectar de manera automática los puertos y servicios en operación en los host que forman parte de una red.
2. Identificar posibles vulnerabilidades en los host, para evitar posibles ataques.

. INTRODUCCIÓN TEORICA

l escaneo o barrido de puertos es una técnica para descubrir canales de omunicación disponibles en un servidor, mediante las herramientas apropiadas es osible realizar un análisis y posterior reporte de los puertos abiertos del sistema bjetivo. Esta técnica consiste en realizar un *scan* o barrido de un host o grupo de llos de manera de obtener un listado con sus puertos abiertos, muchas veces esta formación es crucial al momento de diagnosticar la seguridad de un host ya que abiendo los puertos que atiende es posible determinar los ataques a los que esta xpuesto. El origen de esta técnica se remonta a antes de la aparición de Internet y el uso masivo de computadoras, se usaba esta técnica para descubrir números lefónicos no incluidos en guía, detrás de los cuales se encontraba a la escucha omputadoras, probando sistemáticamente números, bien al azar o de forma ecuencial, uno de los sistemas mas famosos en su época fue Toneloc que usaba el

ıodem para discar en busca que una computadora que contestara desde el otro lado e la línea.

:on la aparición de Internet llegaron también los ataques a los servidores, esta vez lo ue se escanea son los puertos abiertos del host.

'map es un software de distribución libre para plataformas Unix, diseñado para ermitir a los administradores de sistemas el monitoreo de redes, *para determinar que ervidores se encuentran activos y que servicios ofrecen.* Nmap soporta un gran úmero de técnicas de escaneo tales como: UDP, TCP Conect() (simplemente tratar de brir una conexión como es habitual), TCP Syn (escaneos SYN semi-abiertos), ICMP. ntre otras características *nmap* presenta la capacidad para la detección remota del stema operativo de un host, detección de servidores inactivos por medio de pings aralelos, detección de filtrado de puertos, entre otras.

. PROCEDIMIENTO

ara la ejecución de este laboratorio se utilizará la versión 2.54 de nmap.
ı sintaxis es la siguiente:
nap [Tipos(s)de escaneo] [Opciones] <servidor o red #1 ... [#N]>

ealice los siguientes escaneos:

Obtener ayuda –h: Esta opción tan practica muestra una pantalla de referencia rápida sobre las opciones de uso de nmap.

ot@linux /root]#nmap –h

. *Escaneo TCP connect():*Es la forma más básica de escaneo TCP. La llamada de stema connect() proporcionada por el sistema operativo se usa para establecer una onexión con todos los puertos de la computadora.

oot@linux /root]#nmap –sT *[dir_ip_server]*

omplete la tabla :

Puerto	Estado	Servicio

. *Escaneo ping:* A veces únicamente se necesita saber que servidores en una red se ncuentran activos. Nmap puede hacer esto enviando peticiones de respuesta CMP a cada dirección IP de la red que se especifica.

oot@linux /root]#nmap –sP *[dir_ip_server]*

espuesta obtenida:_____

Escaneo de Protocolo IP: Esta opción para determinar que protocolos IP son portados por el host.

[root@linux /root]#nmap –sO *[dir_ip_server]*

Protocolo	Estado	Nombre

. *Escaneo Udp:* Este método se usa para saber que puertos UDP (Protocolo de atagrama de Usuario) están abiertos en un servidor. La técnica consiste en enviar aquetes UDP de 0 bytes a cada puerto de la maquina objetivo. Si se recibe un ıensaje ICMP de puerto no alcanzable, entonces el puerto esta cerrado. De lo ɔntrario, se asume que esta abierto.

oot@linux /root]#nmap –sU [dir_ip_server]

omplete:

Puerto	Estado	Servicio

Escaneo de Sistema Operativo –O: Esta opción activa la detección remota del stema operativo por medio de TCP/IP.

ɔot@linux /root]#nmap –O [dir_ip_server]

ue sistema operativo remoto reporta este escaneo:_____

Puede escanear un rango de puertos específicos con la opción –p <rango_puertos> sta opcion determina los puertos que se quieren specificar. Por ejemplo, '-p 23' obara solo el puerto 23 del servidor(es) objetivo. "-p 21-25" probara los puertos 21, 22, 3. 24 y 25.

root@linux /root]#nmap –p 21-25 [dir_ip_server]

\note sus resultados:

Puerto	Estado	Servicio

. Nmap permite mezclar sus opciones para obtener información más amplia por cada escaneo, por ejemplo es posible realizar un escaneo TCP en un servidor y a la vez veriguar que sistema operativo se ejecuta.

oot@linux /root]#nmap –sT –O [dir_ip_server]

Puerto	Estado	Servicio

ipo de sistema operativo:_____

I. Investigación Complementaria.

1. Investigue para que sirven las opciones de nmap: -sS, -sF, -v, -Pl.
2. Investigue sobre los diferentes números de puertos y como se da la comunicación de puerto a puerto.
3. Cual es la utilidad de un software de esta naturaleza dentro de una red.
4. Investigue sobre otros software que desempeñan una tarea similar a nmap.

eferencias.

ttp://www.insecure.org

	GUÍA No. Monitoreo de Interfaces de Enrutadores	

Facultad : Ingeniería.
Escuela : Electrónica.
Asignatura : Redes de Área Amplia
Tiempo de Ejecución : 2 horas.

I. OBJETIVO

1. Instalar y configurar una herramienta de distribución libre (Multi Router Traffic Grapher-MRTG), para monitorear la carga de tráfico de los enlaces de una red.

II. INTRODUCCIÓN TEORICA

El MRTG consiste en un programa en Perl que usa SNMP para leer los contadores de tráfico de los enrutadores y de un rápido programa en C el cual archiva los datos de tráfico y crea imágenes que representan el tráfico en la conexión de red monitoreada. Esos gráficos se insertan en páginas web que pueden ser vistas desde cualquier browser.

Además de una vista diaria detallada, el MRTG crea también representaciones visuales para el tráfico de los últimos siete días, las cuatro últimas semanas y los últimos doce meses. Esto es posible pues el MRTG mantiene un archivo de todos los datos que ha obtenido del enrutador. Este archivo es consolidado automáticamente, así que no crece con el tiempo, pero contiene todos los datos relevantes del tráfico de los últimos dos años. Todo esto se realiza de una manera eficiente. Por lo tanto, es posible monitorear 200 o más enlaces de red desde cualquier máquina con sistema operativo Linux.

El MRTG no está limitado al monitoreo de tráfico, es posible monitorear cualquier variable SNMP que se elija. Puede hasta usar un programa externo para recolectar datos que serán monitoreados por el MRTG. Organizaciones están usando el MRTG para monitorear variables como Carga del Sistema, Logueo de Sesiones, disponibilidad de módems y más.

III. MATERIAL Y EQUIPO.

1. Una pc con sistema operativo Linux.
2. Conexión a Internet.

IV. PROCEDIMIENTO.

Instalación del programa

Previo a la instalación de MRTG deben instalarse ciertas librerías que permitirán la generación de los archivos gráficos.

Instalación de librerías (pre-instalación)

Librerías Zlib

Puede obtener los instaladores de esta librerías de la siguiente dirección de Internet: **http://www.gzip.org/zlib/zlib-1.1.4.tar.gz.**

Luego hay que ejecutar las siguientes instrucciones:

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

Librerías LibPng

Puede obtener los instaladores de esta librerías de la siguiente dirección de Internet: **http://www.libpng.org/pub/png/src/libpng-1.0.12.tar.gz**

Luego hay que ejecutar las siguientes instrucciones:

```
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 ..

Librerías Gd

Puede obtener los instaladores de esta librerías de la siguiente dirección de Internet: http://www.boutell.com/gd/http/gd-1.8.3.tar.gz

Luego hay que ejecutar las siguientes instrucciones:

gunzip -c gd-1.8.3.tar.gz |tar xf -

mv gd-1.8.3 gd

cd gd

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

cd ..

Instalación de MRTG (compilación)

Los instaladores de Netsaint pueden obtenerse de http://people.ee.ethz.ch/~oetiker/webtools/mrtg/pub/mrtg-2.9.22.tar.gz . Una vez que se cuentan con los archivos en formato tar.gz (el formato de comprensión de Linux) deben seguirse los siguientes pasos:

cd /usr/local/src

gunzip -c mrtg-2.9.22.tar.gz | tar xvf -

cd mrtg-2.9.22

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

make

make install

Configuración de SNMP en equipos Cisco

Antes de configurar MRTG en un equipo Cisco es necesario habilitar SNMP en dicho equipo, para ello pueden seguirse los siguientes pasos:

snmp-server community 5urf5h0p RO

snmp-server location Universidad Don Bosco Soyapango

snmp-server contact net-admin@citt.cdb.edu.sv

snmp-server enable traps

snmp host 168.243.3.1 traps SNMPv1

A continuación se detalla el propósito de cada comando:

Comando	Utilizado para
snmp-server community 5urf5h0p RO	Asigna un *community* de solo lectura. Solo consultas de lecturas son permitidas. En este caso el *community* 5urf5h0p no permite realizar cambios en la configuración del equipo
snmp-server location Universidad Don Bosco Soyapango	Para propósitos administrativos especifica la ubicación del equipo
snmp-server contact net-admin@citt.cdb.edu.sv	Especifica el nombre del contacto en caso ocurra un problema con el SNMP.
snmp-server enable traps	Habilita SNMP para que notifique cuando ocurren cambios de: configuración, variables ambientales y condiciones criticas del equipo.
snmp host 168.243.3.5 traps SNMPv1	Identifica el equipo al que serán enviadas las notificaciones especificadas en el comando anterior.

Generalmente para que MRTG pueda funcionar correctamente unicamente es necesario ejecutar las primeras tres lineas de commando del procedimiento anterior.

CONFIGURACION DE MRTG

MRTG utiliza un archivo de configuración para especificar cuales dispositivos serán monitoreados. Los instaladores de MRTG no vienen acompañados por una configuración predefinida porque los dispositivos listados variarían de red a red. En lugar de ello los instaladores incluyen un programa llamado ***CFGMAKER***, el cual es utilizado para construir configuraciones básicas. El propósito de este programa es analizar un dispositivo de red que utiliza SNMP y construir un archivo de configuración el cual luego puede personalizarse.

La sintaxis de **cfgmaker** es como sigue:

cfgmaker cominnity@device

Dos parámetros son requeridos: El ***community*** asignado al dispositivo y la dirección IP o nombre de host.

Para ilustrar el uso de este programa de configuración, asumamos que queremos monitorear un router cisco 7500, llamado ***remote-wg***, con nombre de ***community*** UDB. En base a esto la instrucción de comando seria:

cfgmaker UDB@remote-gw > cisco.conf

El comando anterior construirá un archivo de configuración mrtg el cual tendrá el nombre de cisco.conf. Asumiendo que los parámetros provistos al cfgmaker son correctos y que el dispositivo responde a la solicitudes SNMP, el siguiente listado muestra la configuración que se generaría:

```
# Created by Hugo Orellana
# ./cfgmaker --global 'WorkDir: /var/www/html/mrtg' --global 'Options[_]: bits,growright' --# output /usr/local/mrtg-2/bin/e1.cfg mrtg@168.243.3.1

#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

WorkDir: /var/www/html/mrtg
Options[_]: bits,growright
##################################################################
# System: remote-gw
# Description: Cisco Internetwork Operating System Software
#       IOS (tm) RSP Software (RSP-DSV-M), Version 12.1(7), RELEASE SOFTWARE (fc1)
#       Copyright (c) 1986-2001 by cisco Systems, Inc.
#       Compiled Wed 21-Feb-01 15:36 by kellythw
# Contact:
# Location:
##################################################################


### Interface 1 >> Descr: 'Ethernet0' | Name: 'Se0/0' | Ip: '' | Eth: '' ###

Target[168.243.3.1_1]: 1:mrtg@168.243.3.1:
SetEnv[168.243.3.1_1]: MRTG_INT_IP="" MRTG_INT_DESCR="Ethernet0"
MaxBytes[168.243.3.1_1]: 193000
Title[168.243.3.1_1]: Traffic Analysis for 1 -- remote-gw
PageTop[168.243.3.1_1]: <H1>Traffic Analysis for 1 -- remote-gw</H1>
 <TABLE>
  <TR><TD>System:</TD>     <TD>remote-gw in </TD></TR>
  <TR><TD>Maintainer:</TD> <TD></TD></TR>
  <TR><TD>Description:</TD><TD>Ethernet0 Red UDB </TD></TR>
  <TR><TD>ifType:</TD>     <TD>ppp (23)</TD></TR>
  <TR><TD>ifName:</TD>     <TD>Se0/0</TD></TR>
  <TR><TD>Max Speed:</TD>  <TD>1544.0 kbits/s</TD></TR>
 </TABLE>


### Interface 2 >> Descr: 'Serial0' | Name: 'Se0/1' | Ip: '' | Eth: '' ###

Target[168.243.3.1_2]: 2:mrtg@168.243.3.1:
```

```
SetEnv[168.243.3.1_2]: MRTG_INT_IP="" MRTG_INT_DESCR="Serial0"
MaxBytes[168.243.3.1_2]: 193000
Title[168.243.3.1_2]: Traffic Analysis for 2 -- remote-gw
PageTop[168.243.3.1_2]: <H1>Traffic Analysis for 2 -- remote-gw</H1>
 <TABLE>
  <TR><TD>System:</TD>     <TD>remote-gw in </TD></TR>
  <TR><TD>Maintainer:</TD> <TD></TD></TR>
  <TR><TD>Description:</TD><TD>Serial0 Enlace Internet UDB</TD></TR>
  <TR><TD>ifName:</TD>     <TD>Se0/1</TD></TR>
  <TR><TD>Max Speed:</TD>  <TD>1544.0 kbits/s</TD></TR>
 </TABLE>
```

Como iniciar MRTG

Asumiendo que el archivo de configuración de MRTG se llama cisco.conf, la instrucción para iniciar MRTG es como sigue:

cd /usr/local/mrtg/bin

mrtg cisco.conf

Antes de pasar a la siguiente operación, verifique cual es su dirección IP. Con el comando ifconfig.

Revise los datos que el MRTG ha comenzado a capturar, iniciando una sesión con su browser y digitando la siguiente dirección:

http://su_direccion_IP/mrtg/

V. Investigación Complementaria.

1. Investigue la forma de monitorear la carga del disco duro de un servidor.

VII. Referencias.

http://www.cdb.edu.sv/monitor (ver sección monitoreo de enlace a Internet).

http://people.ee.ethz.ch/~oetiker/webtools/mrtg/es/