UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SISTEMA DE ADMINISTRACIÓN PARA EL LABORATORIO DE REDES Y SEGURIDAD

T E S I S

que para obtener el título de

INGENIERO EN COMPUTACIÓN

P R E S E N T A N

DIANA JESSICA MARTÍNEZ MARTÍNEZ

PAULA BOURGET GARDUÑO

DIRECTORA DE TESIS:
M.C. MA. JAQUELINA LÓPEZ BARRIENTOS

Ciudad Universitaria Octubre 2005

A la Universidad Nacional Autónoma de México:

Por habernos brindado la oportunidad de estudiar en sus aulas y por todos los conocimientos y enseñanzas adquiridos en ella.

A la Facultad de Ingeniería:

Por haber encontrado en ella un segundo hogar, por todos los conocimientos que adquirimos durante nuestra estancia y por los momentos agradables que vivimos ahí. Agradecemos a los profesores que laboran en esta facultad por su paciencia, dedicación y por todos los conocimientos que nos transmitieron.

A la Profesora M.C. Ma. Jaquelina López Barrientos:

Por aceptar dirigir este proyecto, por habernos transmitido sus conocimientos y por la ayuda y paciencia brindada en los momentos en que lo requerimos. Gracias por su dedicación y esfuerzo sin lo cual no hubiéramos concluido este trabajo.

GRACIAS
JESSICA Y PAULA

A Dios:

Gracias por darme fuerza para seguir adelante en los momentos difíciles.

A mi papá, Carlos Martínez Nava:

Gracias por tus consejos y tu apoyo, por enseñarme que uno siempre puede lograr lo que quiere y nunca debe dejarse vencer. Quiero decirte que eres para mí el ejemplo más grande de lucha, superación, esfuerzo y dedicación. Este trabajo también es tuyo y lo que soy te lo debo a ti por enseñarme a ser tan responsable y trabajadora como tú. Que Dios Te Bendiga Papi.

A mi mamá, Rebeca Martínez Arnava:

Gracias por entregarme siempre lo mejor de ti, porque no tengo como pagarte tus cuidados, cariño, sacrificios, apoyo y desvelos, sólo puedo decirte que eres la mujer a la que más admiro y respeto. Te dedico este trabajo y todo el esfuerzo que hay puesto en él con todo mi cariño y como una muestra del infinito agradecimiento que te tengo, porque esta meta también es tuya ya que lo que soy es un reflejo de todo lo que te has esforzado por mí. Que Dios Te Bendiga Mami.

A mi hermano, Carlos Mauricio:

Gracias por tu apoyo, tu cariño y por estar siempre conmigo. Te agradezco mucho la ayuda que me brindaste siempre que te necesité y te reitero mi cariño y mi apoyo siempre.

A mis tíos y primos:

Gracias por la ayuda, confianza, apoyo y los consejos que me brindaron siempre, pero sobre todo muchas gracias a todos por su cariño.

A mis amigos, en especial a Paula:

Gracias por todos los momentos buenos y malos que pasamos juntos, por su apoyo incondicional y su ayuda pero principalmente por su amistad sincera. Siempre los recordaré.

GRACIAS
JESSICA

A mis padres:

Mi más grande agradecimiento por darme la oportunidad de dejar que me dedicara a lo que yo quise sin ponerme obstáculos de por medio. Así también por la confianza que tuvieron en mí para que terminara mi carrera, por todo su apoyo para que pudiera realizar este sueño, así como por sus consejos y su ánimo para que no desistiera, esto es por y para ustedes. Y mil gracias por su preocupación y paciencia al ver que pasaba el tiempo y no veían llegar el fin de este proyecto.

A mis hermanos, Isaac y Mauricio:

Porque directa o indirectamente siempre me ayudaron y me apoyaron para que terminara mi carrera, así como por su alegría la cual hacía que el tiempo no fuera tan pesado y pasara más rápido. Gracias.

A Juan A. González:

Gracias por haber estado los últimos años de mi carrera a mi lado y por todo el apoyo y comprensión brindados en todo momento para que pudiera terminarla. También quiero agradecerte por echarme porras para que no me desanimara ni desistiera de este proyecto, así también por tu paciencia, confianza y amistad. Mil gracias por todo.

A Jessica Martínez:

Por tu amistad y por estar siempre en las buenas y en las malas; así como por haberme ayudado a que la estancia en la Facultad fuera agradable y divertida. Gracias por tu paciencia, comprensión y por tus ideas aportadas para que esta tesis saliera adelante.

Y en general, gracias a todos aquellos que me animaron, me apoyaron y me preguntaron una y mil veces cómo iban las cosas y para cuándo acabábamos. Todos han hecho posible que me sienta orgullosa de este trabajo.

GRACIAS
PAULA

ÍNDICE

PÁGINA

PÁGINA

PÁGINA

INTRODUCCIÓN

"La sabiduría es un adorno en la prosperidad y un refugio en la adversidad".

En el campo de las tecnologías de la información, la tendencia más importante en estos momentos la constituyen las redes de computadoras. Siendo así, la mayoría de las computadoras trabajan conectadas a una red, a través de la cual los usuarios pueden acceder a recursos remotos, comunicarse, trabajar en grupo, etc.

La mayoría de las organizaciones tienden a distribuir sus sistemas informáticos. A medida que aumenta la criticidad y la importancia de estos sistemas, su complejidad y la inversión realizada crece de forma paralela.

Llega entonces el momento en que los sistemas se hacen demasiado complejos para ser administrados manualmente y se hacen imprescindibles técnicas y herramientas que permitan llevar a cabo dicha administración, de manera controlada y automatizada, garantizando que los sistemas funcionen y cuando no es así, minimizando el tiempo en el que el sistema está parado, es decir, optimizando la fiabilidad y la disponibilidad.

Para lograr todo lo anterior y tener una correcta **Administración de Red**, algunos conceptos importantes que se deben conocer sobre Administración de Red son los siguientes:

- La administración cubre todas las precauciones y actividades para asegurar el uso eficiente de la red.

- Proceso que consiste en la planeación, organización y control de las actividades que envuelven el funcionamiento de la red dentro de una organización.

- Se define como administración al monitoreo, control y coordinación de los recursos de computadora, los recursos usados en la conexión y comunicación de las mismas, y las aplicaciones usadas en esas computadoras.

- La Administración de Red es el conjunto de tareas de monitoreo, información y control necesarias para operar efectivamente una red. Estas tareas pueden estar distribuidas sobre diferentes nodos de la red, lo cual puede requerir repetidas acciones de recolección de datos y análisis cada vez que sucede un nuevo evento en la red.

Objetivos de la Administración de Redes

- **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:** Debemos incrementar la eficiencia de otros objetivos de la administración, pero dependerá de otros factores tales como utilización, costo operacional, costo de migración y flexibilidad.

- **Facilidad de uso:** El uso de aplicaciones de administración de redes debe ser fácilmente entendible para el administrador.

- **Seguridad:** Existen casos en donde la seguridad es un aspecto a tener en cuenta tales como información de contaduría, información gerencial, etc.

Los elementos que pueden ser objeto de control por un **Sistema de Administración de Red** en las redes de área local son fundamentalmente: redes y subredes, cableado, equipos de interconexión (concentradores, repetidores, puentes, ruteadores o dispositivos de encaminamiento) y equipos finales (servidores, terminales, computadoras personales y estaciones de trabajo).

Áreas Funcionales de la Administración de Red

De acuerdo con la clasificación establecida por **ISO**, las áreas funcionales de la Administración de Red pueden agruparse en administración de rendimiento, de configuración, de fallas, de cambios y de seguridad.

Administración de Rendimiento

Es el conjunto de tareas encargadas de la cuantificación, medición, informe y control de los tiempos de respuesta, disponibilidades y utilización de la red o de los componentes de la misma. Los datos suministrados por estos procesos de administración del rendimiento, pueden ser utilizados para la detección de problemas, determinar umbrales de operatividad y planificación de capacidad.

Administración de Configuración

Esta disciplina es la encargada de monitorear y controlar la información necesaria para identificar física y lógicamente los recursos de red.

La administración de configuración proporciona los servicios para la adaptación de los recursos de la red, así como ayudas para la administración de inventario de recursos y asiste a otras funciones de administración como:

- **Administración de Fallas:** Utiliza los datos para determinar la identificación física de un recurso, localización y punto de contacto.

- **Administración de Cambios:** Utiliza estos datos para la planificación de cambios y para analizar como podría afectar a la red un cambio determinado.

Administración de Fallas

Esta disciplina o tarea, también conocida como **Administración de Problemas**, es la encargada de detectar y controlar los comportamientos anormales en la red. Puede ser dividida en una serie de procesos:

- **Detección e informe de problemas:** Este proceso, tanto por medio de mecanismos activos como pasivos, detecta las fallas e informa de las mismas a los administradores de red o a los procesos designados para tal efecto.

- **Determinación de problemas:** Este se encarga de aislar el problema en un recurso determinado, hardware, software, medio de transporte o en una causa externa, para así poder identificar al personal específico responsable de su diagnóstico y resolución.

- **Puenteo o recuperación de problemas:** Este proceso trata de minimizar o eliminar el efecto del problema y de tomar las acciones requeridas para su resolución.

- **Seguimiento y control del problema:** Este proceso, que se encuentra referenciado en inglés como *Trouble Ticketing*, proporciona los mecanismos necesarios para el seguimiento del problema a lo largo de su vida, es decir, desde su detección hasta su resolución.

Administración de Cambios

Es la encargada de la planificación, control y realización de cualquier cambio o modificación que afecte la estructura de la red o a componentes de hardware o software de la misma, incluyendo:

- Cambios en el software en forma de "parches", reemplazo completo de módulos o adaptaciones en los mismos.

- Cambios en el hardware como la instalación de un nuevo componente y modificación o retirada de uno ya existente.

Administración de Seguridad

Bajo esta disciplina, los aspectos más importantes a controlar son:

- **Autenticación** (autenticidad e integridad)

- **Control de accesos** (para asegurar que los recursos son utilizados por los usuarios autorizados)

- **Privacidad** (secreto o confidencialidad)

El objetivo final de la Administración de Red es mantener los sistemas de una organización en un estado óptimo de funcionamiento.

El objetivo principal de este trabajo es implementar un **Sistema de Administración de Redes** en el **Laboratorio de Redes y Seguridad** de la **Facultad de Ingeniería**, analizando algunos de los diversos sistemas de administración ya existentes, para obtener el que más se adecue a las necesidades y características de dicho laboratorio; logrando con esto, que los alumnos tengan disponibilidad del sistema y del laboratorio siempre que ellos lo necesiten. Además de tener un control de los recursos con los que cuenta la red y un monitoreo de los cambios que los usuarios pudieran realizar a la red y que pudieran poner en peligro la disponibilidad y el acceso a la misma afectando así el funcionamiento del laboratorio en general.

CAPÍTULO I

SISTEMAS DE ADMINISTRACIÓN DE REDES

"No hay libro tan malo del que no pueda aprenderse algo bueno".

I.1 CARACTERÍSTICAS DE LOS PRODUCTOS DE ADMINISTRACIÓN DE RED EN LAS REDES DE ÁREA LOCAL

Los agentes y consolas son los conceptos claves en la administración de redes.

- **Consola:** Es una estación de trabajo convenientemente configurada para visualizar la información recogida por los agentes.

- **Agentes:** Son programas especiales que están diseñados para recoger información específica de la red.

Entre las características de los agentes cabe destacar:

- Están basados en software.

- Son transparentes a los usuarios. Se ejecutan en los puestos de trabajo sin afectar el rendimiento de los mismos.

- La información que recogen la almacenan en bases de datos que después son exploradas a través de las consolas.

Tradicionalmente, los Agentes de Administración de Red contemplan soluciones parciales, tales como análisis de tráfico, administración de servidores y de estaciones de trabajo.

Los productos actuales, sin embargo, proporcionan soluciones integradas que permiten una visión global de la red.

Entre las funciones más significativas de los **Agentes de Administración de Red** pueden citarse las siguientes:

I.1.1 Administración de Servidores y Estaciones de Trabajo

Comprende el control de configuraciones, la identificación automática de estaciones inactivas, la pérdida de las conexiones físicas de la red y el registro de estadísticas e informes.

I.1.2 Administración del Hardware

La administración del hardware es una actividad esencial para el control del equipamiento y sus costos asociados, así como, para asegurar que los usuarios disponen del equipamiento suficiente para cubrir sus necesidades.

Para evitar una visita física a los equipos, se utilizan agentes que se ejecutan en los puestos de trabajo y que realizan el inventario del hardware de forma autónoma y remota.

Una vez que la información de inventario es recogida, la administración de red puede hacer las siguientes funciones:

- Añadir información relativa a puestos de trabajo no instalados en red.
- Añadir información sobre otros aspectos como la localización física, condiciones en que se encuentra, entre otros.
- Realizar el seguimiento de averías de los componentes de las estaciones de trabajo.
- Anotar información al inventario referente a los componentes que forman la estación de trabajo (tarjetas, discos, etc).

El inventario se realiza periódicamente cada vez que se ponen en marcha los puestos o durante su tiempo de funcionamiento.

En los servidores, además se suele realizar un seguimiento de los parámetros de funcionamiento como pueden ser actividad del CPU, de los discos, espacios disponibles, número de conexiones, entre otros.

I.1.3 Monitoreo de Aplicaciones

Supervisa la operación de las aplicaciones, entre otras razones, para controlar el adecuado uso de las licencias. Así, determina el número de usuarios que acceden simultáneamente a una aplicación, utilizando eventualmente opciones de bloqueo.

Las funciones del monitoreo de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas al personal responsable del buen funcionamiento de la red.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención se pueden utilizar diferentes métodos de notificación como son:

- **Mensajes en la consola:** Se suelen codificar con colores en función de su importancia.

- **Mensajes por correo electrónico:** Conteniendo el nivel de prioridad y el nombre e información del evento.

- **Mensajes a móviles:** Cuando el evento necesita intervención inmediata se suele comunicar a los técnicos de guardia a través de este método.

Además de los eventos, otra característica importante es el monitoreo del tráfico de red:

- Se toman nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.

- Se almacenan para su posterior análisis.

Del análisis se obtienen conclusiones, bien para resolver problemas concretos o bien para optimizar la utilización de la red.

I.1.4 Planificación de Procesos

En vez de tener que recordar y realizar trabajos periódicos o en horas no laborables, el administrador puede programar un agente que realice las tareas programadas en los momentos previstos.

Además, estos agentes recogen información sobre el estado de finalización de los procesos para un posterior análisis por el administrador.

Los procesos típicos que se suelen planificar son: copias de seguridad, búsqueda de virus, distribución de software, impresiones masivas, etc.

I.1.5 Distribución de Software

Permite la instalación de software, tanto del sistema como de aplicación, facilitando su actualización de forma remota. La distribución de software puede ser planificada, normalmente mediante programas en los que se indican la fecha y hora de la distribución, las estaciones que deben ser actualizadas, etc.

Las actividades relativas a la administración de software permiten a la administración de red determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red.

De igual forma que en el hardware, se utilizan agentes que realizan la función de obtener toda la información acerca del software en la red.

I.1.6 Topología de Red

Esta función permite realizar un diagrama topológico de la red, mediante el descubrimiento de los componentes de la misma, enlaces, puentes, encaminadores y otros. Normalmente el descubrimiento se realiza mediante el mandato **echo** del **Protocolo ICMP**, en caso de utilizarse **Protocolos TCP/IP**.

I.1.7 Protección contra Virus

Permite la detección y protección automática y centralizada contra virus informáticos.

La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en los puestos de trabajo.

La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador y protección de los discos, etc.

Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

I.1.8 Seguridad

Controla los accesos de los usuarios a las aplicaciones y datos. Pueden proporcionar funciones de cifrado de la información. Monitorea el uso de las aplicaciones para controlar los privilegios de los usuarios.

Para cada recurso en la red, el administrador dispone de los mecanismos para establecer permisos de utilización, así como monitorear el uso que se hace de los recursos.

Todas estas tareas son muy complejas por lo que se utilizan actualmente **Políticas de Seguridad**. Las políticas de seguridad permiten establecer aspectos de seguridad en forma de perfiles que afectan a grupos de usuarios.

Una vez definidas las políticas, el administrador sólo tiene que añadir los usuarios a los grupos establecidos con lo que adquieren los perfiles de seguridad. De esta forma la actualización de medidas de seguridad se hace sobre las políticas y no sobre los usuarios directamente.

Otro aspecto a considerar es el del monitoreo y registro de las actividades de los usuarios pudiendo denegar el acceso a los usuarios en función de que intenten realizar actividades para las que no tienen permiso.

I.1.9 Utilidades

Entre las funciones de administración, se pueden considerar utilidades como administración de impresoras y colas de impresión, administración de almacenamiento, planificación de tareas y copias de seguridad en la red.

La administración centralizada de impresoras en la red permite reducir el tiempo y el esfuerzo que necesitan los usuarios para configurar la impresión desde unos puertos de trabajo y también permiten al administrador realizar una administración unificada de todas las impresoras de la red.

I.1.10 Síntesis de Prestación de Administración de Red

En el listado que se muestra a continuación se reflejan las prestaciones de Administración de Red más frecuentemente utilizadas, las cuales pueden ser de utilidad para evaluar los productos de Administración de Red.

I.1.10.1 Administración de Servidores

- Alertas de posibles condiciones de error
- Resolución automática de problemas
- Monitoreo de rendimiento, tráfico y utilización de recursos
- Protección contra virus
- Administración de inventario

- Seguridad y copias de seguridad
- Administración de cuentas de los usuarios
- Administración de colas de impresión

I.1.10.2 Administración de Estaciones de Trabajo

- Monitoreo y estadísticas
- Administración de inventario
- Protección contra virus
- Notificación automática de cambios de configuración
- Identificación y corrección de problemas
- Control de acceso de archivos y utilización de aplicaciones

I.1.10.3 Administración de Infraestructura de Red

- Identificación de redes sobrecargadas y toma de acciones correctoras (rutas alternativas)
- Identificación de usuarios muy activos
- Monitoreo de tráfico entre estaciones
- Notificación de problemas
- Administración de dispositivos SNMP, como concentradores y encaminadores

I.1.10.4 Administración de Sistemas

- Permite la definición de dominios
- Archivos de bases de datos protegidos
- Niveles de acceso de los usuarios
- Visualización de espacio libre de disco en servidor y en estaciones de trabajo

I.2 SISTEMAS DE ADMINISTRACIÓN DE REDES

I.2.1 NETVIEW

I.2.1.1 Perspectiva

Netview podría ser descrito como una colección de programas de aplicación unidos con el paso del tiempo. Las raíces de NetView pueden ser localizadas desde los años 70's.

Por ejemplo, el **NCCF** (**N**etwork **C**ommunications **C**ontrol **F**acility) fue anunciado en 1978. NCCF es un comando de interfaz. Después, en 1979 el programa **NPDA** (**N**etwork **P**roblem **D**etermination **A**pplication) fue anunciado.

Otros componentes fueron desarrollados después de 1979 y en 1986 NetView fue lanzado formalmente.

NetView tiene considerable presencia en las **Redes SNA** como se muestra en la figura I.1. Ha ido evolucionando junto con el mercado y ha ido desarrollándose y creciendo, tanto como la tecnología y las necesidades de expansión lo han ido requiriendo.

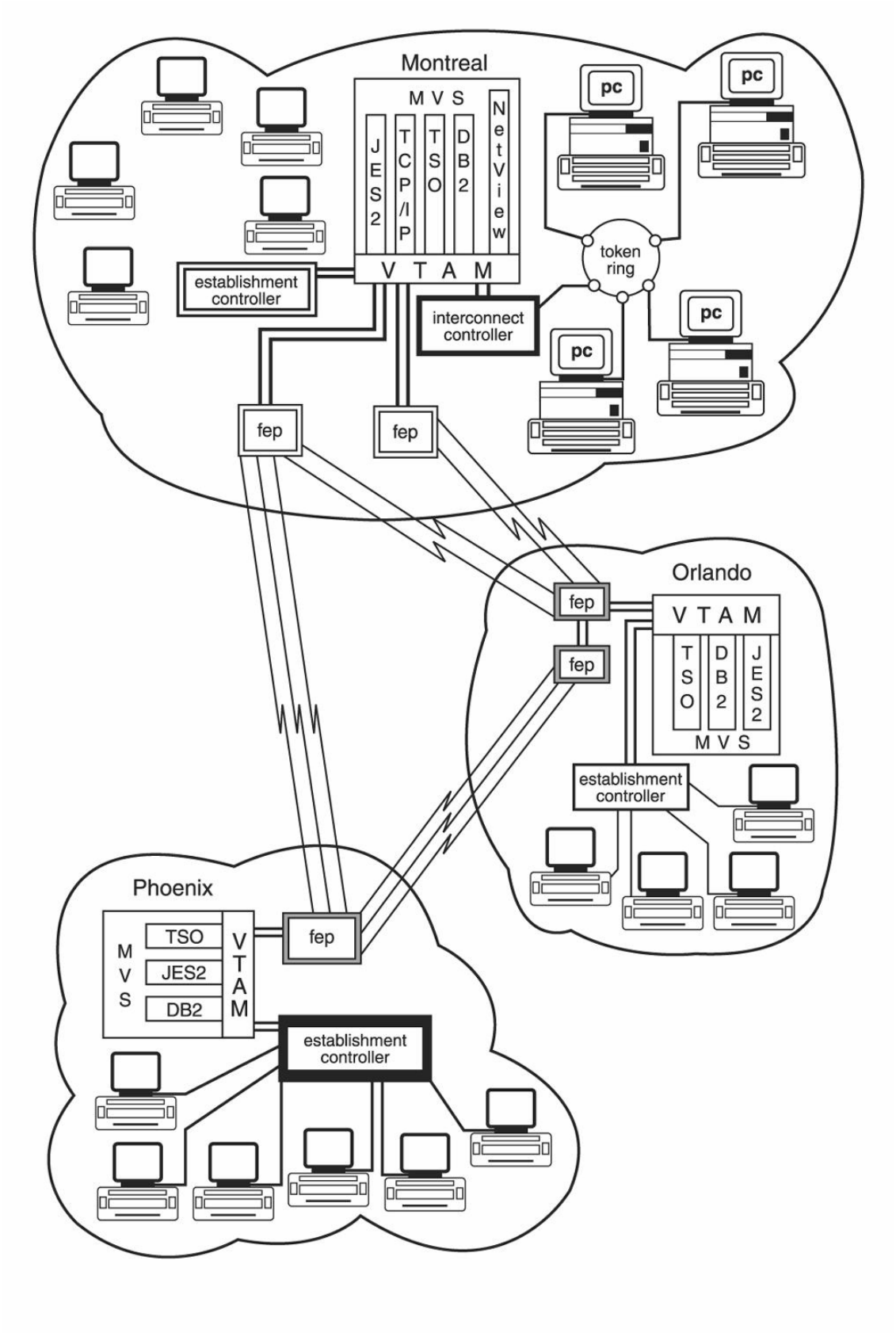


Figura I.1 Ejemplo de una implementación de NetView

La ilustración de la figura I.1 muestra un típico ambiente **SNA**. **Netview** está localizado en un anfitrión; sin embargo, tres anfitriones están conectados junto con variantes en sus configuraciones. NetView puede proveer información acerca de todas las locaciones al anfitrión donde NetView está localizado.

Algunos componentes de NetView se explicarán brevemente a continuación.

I.2.1.2 Network Communications Control Facility (NCCF)

NCCF es aplicado como una instrucción de línea. Es un poderoso componente de NetView. Por medio de NCCF un operador puede emitir comandos tipo **V**irtual **T**elecommunications **A**ccess **M**ethod (**VTAM**) o **MVS**.

NCCF puede ser utilizado para activar o desactivar el controlador en dos sitios en los cuales esté instalado NetView, aunque éstos se encuentren en lugares distintos.

El componente NCCF de NetView reemplaza la necesidad del operador de tener presente físicamente una consola procesador. Las ramificaciones de este componente solo cambian la percepción de la administración de redes.

I.2.1.3 Network Logical Data Manager (NLDM)

La herramienta **N**etwork **L**ogical **D**ata **M**anager (**NLDM**) es conocida también como **Session Monitor**. Este componente se enfoca en información sobre unidades lógicas (LUs). Es en particular útil cuando los sitios interactúan intensamente en una terminal con una aplicación de un subsistema.

La información recibida por medio de NLDM puede ser clasificada de acuerdo a las siguientes categorías:

- Localización de datos.
- Tiempo de respuesta.
- Sesión de conocimiento.
- Ruta de datos.
- Disponibilidad y contabilidad de la red.

La **localización de datos** puede ser obtenida con sesiones específicas. Ésta es de particular interés cuando se requiere resolver problemas de datos en la red. Las instancias en que las sesiones están en el mismo dominio que NetView pueden tener sesiones de datos almacenadas en la base de datos conocida como **Session History Database**, ésta es usada para análisis comparativos.

El **tiempo de respuesta** de datos es una información crítica para aquellos sitios en los que se usa esta opción. Monitorear el tiempo de respuesta es un método para obtener información verdadera del desempeño de la red.

El tiempo de respuesta es presentado por NetView con forma de gráfico. El gráfico puede incluir el nombre de la LU, identificando una LU particular la cual es asociada con la información de la pantalla.

También la pantalla presenta el porcentaje de los tiempos de respuesta desde la terminal y el promedio de los programas de aplicación y provee el número de instancias dando un porcentaje de sucesos ocurridos.

Las **sesiones de conocimiento (SAW)** emiten reportes de datos acerca de **SSCP**, PU y LUs. La información obtenida por SAW incluye **T**iempos de **R**espuesta de **M**onitoreo de datos (**RTM**), pérdidas de información **BIND**, sesiones fallidas así como localización de datos.

La **ruta de datos** en la red puede también ser obtenida por medio de la sesión de monitoreo. La información tanto como la identificación de grupos de transmisión y la localización puede ser identificada. Adicionalmente, también puede ser obtenida explícitamente la ruta de la información.

La información de la **contabilidad de la red** también puede ser obtenida por medio de la sesión de monitor. Tanto la información como la **disponibilidad de la red** y los recursos de distribución pueden ser obtenidos vía la sesión de monitoreo.

I.2.1.4 Network Problem Determination Application (NPDA)

NPDA, también llamado **Monitoreo del Hardware**, mantiene información acerca de entidades como: módems, enlaces, adaptadores de comunicación, terminales, impresoras, controladores, dispositivos de discos y otros dispositivos específicos.

Dos tipos de información pueden ser obtenidos: **eventos** y **alertas**.

Los **eventos** son datos recibidos por **VTAM** de PU's. Un evento es un suceso predefinido.

La información de un evento puede ser en el formato de protocolo **N**etwork **M**anagement **V**ector **T**ransport **(NMVT)**, **N**etwork **C**ontrol **P**rogram **(NCP)**, **M**iscellaneous **D**ata **R**ecords **(MDR)** o registros vía **REC**ord **M**aintenance **S**tatistics **(RECMS)** de SNA.

Un evento es considerado como un suceso que requiere atención por sus efectos en un recurso SNA.

Las **alertas** son condiciones predeterminadas encontradas por un cliente o por productos IBM. Las alertas requieren atención inmediata.

I.2.1.5 Monitoreo de Estado

El monitoreo de estado reúne información acerca de los recursos en una red. Esta información es desplegada en columnas y renglones por medio de NetView. La información de red reunida en el monitoreo de estado puede ser desplegada gráficamente vía Network Graphic Monitor de NetView.

La información de la red puede ser vista como una simple unidad representando un recurso(s) de la red, o la información puede ser completamente detallada dado un recurso en una red.

Un aspecto interesante concerniente a la operación del monitoreo de estado es una de sus funciones con VTAM. Definiendo recursos y especificando operaciones, algunos parámetros son ejecutados durante lo que se considera un proceso de generación. En la comunidad técnica de SNA, este proceso o referencia a la(s) definición(es) es normalmente llamado un **GEN**.

I.2.1.6 Característica APPNTAM de NetView

APPNTAM, es una topología de red par a par avanzada y un administrador de contabilidad, puede ser mejor descrito como una característica que como un componente. Esta característica es desarrollada porque usa otros componentes y características de NetView. Como su nombre lo indica, proporciona la habilidad a NetView para trabajar con **APPN**, APPN mixto y SNA.

APPNTAM trabaja como el resultado de un agente y una función de un programa de aplicación. La información acerca de una red APPN es vista a través del **N**etView **G**raphic **M**onitor **F**acility (**NGMF**).

La información es desplegada en una estación de trabajo como resultado de la comunicación entre un agente de un programa de aplicación con el anfitrión de NetView sobre una sesión LU6.2. Los datos vienen del **R**esource **O**bject **D**ata **M**anager (**RODM**). Esta característica de NetView maneja los datos a través de NetView.

RODM es un software que maneja información de bases de datos orientadas a objetos. RODM funciona como un subsistema MVS y la información que maneja es la que está en la memoria principal.

Los recursos son tratados como objetos, ellos pueden ser almacenados en categorías y controlados en un ambiente definido. RODM logra este método de almacenamiento a través de clases. Los datos obtenidos acerca de la redes APPN son realizados dinámicamente, pero pueden ser almacenados de manera permanente.

NetView reúne información acerca de los nodos APPN y enlaces a través de agentes. Estos agentes se comunican con el administrador de la topología y éste, a su vez, se comunica con la estación de trabajo y de esta manera es realizado el mapa de la topología APPN.

Debido a la interacción de componentes y características dentro de NetView, los resultados son la información presentada al administrador de la red en tiempo real.

I.2.2 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMP se basa en el conjunto de protocolos TCP/IP y se diseñó para uso en entornos de proceso de datos distribuido con computadoras personales, estaciones de trabajo y computadoras centrales. Se encuentra ampliamente implementado por distintos fabricantes para la administración de redes de área local, puentes, encaminadores o servidores.

SNMP no es resultado de ningún fabricante en particular. El concepto SNMP fue concebido en abril de 1987 por cuatro personas: Jeffery Case, de la Universidad de Tennessee, James Davin, del Massachussets Institute or Technology y Martín Schoffstall y Mark Fedor de Performance Systems International.

I.2.2.1 El modelo SNMP

En una primera aproximación, el modelo de administración SNMP es un **modelo cliente/servidor** compuesto de estaciones administradoras y agentes, actuando los administradores como clientes (pidiendo información a los agentes) y los agentes como servidores (suministrando información a los administradores), utilizando para este diálogo el protocolo SNMP. El modelo SNMP se muestra en la figura I.2.

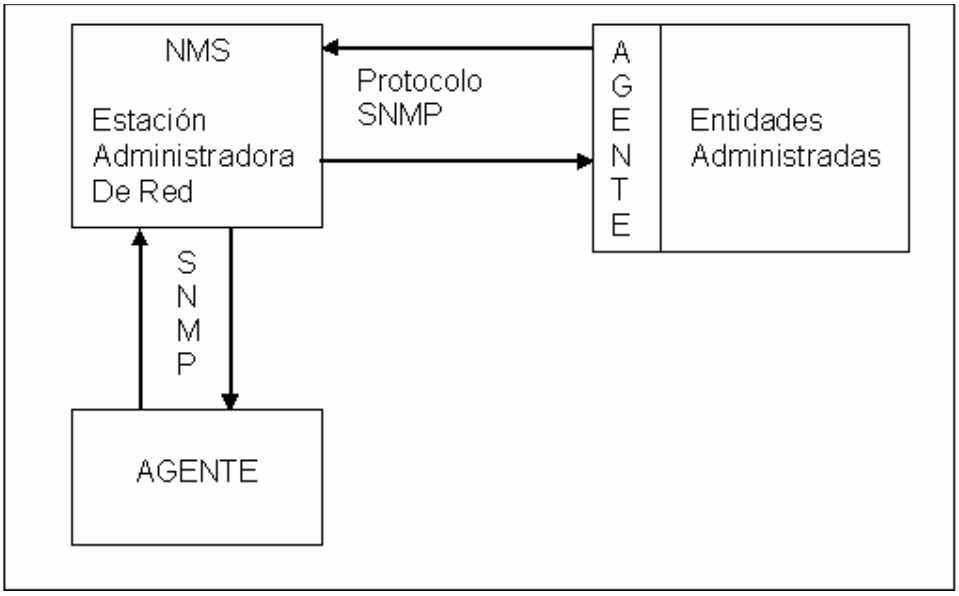


Figura I.2 Modelo SNMP

Es un modelo simple basado en el principio de que la implantación de la administración de red ha de causar un impacto mínimo sobre la misma. Se compone solamente de **tres entidades**:

1. Nodos Administrados
2. Estaciones Administradoras de Red
3. Protocolo de Administración de Red

Los **Nodos Administrados** (**MN**, ***M**anaged **N**odes*) son los elementos de red como los anfitriones, pasarelas, puentes, encaminadores, etc. (un requerimiento mínimo es que deben tener capacidades **IP** y **UDP**). En estos nodos reside el agente administrador (Agente SNMP), encargado de llevar a cabo las funciones de administración requeridas por la Estación Administradora.

Esta comunicación, de información de administración entre administrador y agente, se lleva a cabo utilizando el Protocolo SNMP. A menudo, a los nodos administrados se les denomina, por extensión, **Agentes SNMP**.

Una **Estación Administradora** (**NMS**, ***N**etwork **M**anagement **S**tation)* es un nodo en el que se ejecuta la **Aplicación Administradora de Red** (**NMA**, ***N**etwork **M**anagement **A**pplication*) que monitorea y controla a las estaciones administradas. A menudo, a la Estación Administradora se le denomina **Administrador SNMP**.

El **Protocolo de Administración de Red** (Protocolo SNMP) define la comunicación entre los nodos administrados y las estaciones administradoras o lo que es lo mismo, entre agentes y administradores SNMP.

Las funciones del agente consisten únicamente en la alteración o inspección de ciertos valores limitando de esta forma, a sólo dos, las funciones esenciales de administración y eludiendo la necesidad de un protocolo más complejo. En la otra dirección, desde el agente al administrador, se utiliza un limitado número de mensajes no solicitados para informar sobre sucesos asíncronos.

De la misma forma, para salvaguardar la simplicidad, el intercambio de información requiere sólo un servicio de datagrama y cada mensaje es completa e independientemente representado por un datagrama de transporte simple.

Los mecanismos del SNMP son generalmente adecuados para una gran variedad de servicios de transporte. La **RFC** 1157 especifica el intercambio de mensajes por medio del protocolo UDP, pero puede ser utilizada una gran variedad de otros protocolos de transporte.

I.2.2.1.1 Mandatos y Protocolo SNMP

Una de las claves de la flexibilidad del SNMP es el uso de "variables" como forma de representación de los recursos, tanto físicos como lógicos, en los sistemas administrados. En cada nodo administrado, el agente SNMP proporciona una base de datos llamada **MIB** (***M**anagement **I**nformation **B**ase*), que contiene objetos de datos, conocidos como "variables MIB".

El monitoreo del nodo lo lleva a cabo la estación administradora, la cual, periódicamente, lee los valores de estas variables. El control del nodo se realiza mediante el cambio de valores en las variables. Adicionalmente, existe una operación de **trap** para permitir al nodo administrado informar a una estación administradora sobre determinadas condiciones o eventos inusuales.

En **SNMP** existen **cinco mandatos**:

Get: Enviado por la estación administradora para obtener las variables MIB específicas de un nodo administrado. El agente responde con un *get-response* conteniendo las variables requeridas o un mensaje de error.

Get-next: Es enviado por la estación administradora a la administrada para obtener la variable MIB siguiente a la especificada. El agente responde con un *get-response* que contiene la variable solicitada o un mensaje de error. Mediante el uso de una serie de mandatos *get-next*, la estación administradora puede obtener todas las variables MIB de un nodo administrado.

Get-response: Es enviado por el nodo administrado a la estación administradora como respuesta a mandatos get, get-next o set.

Set: Enviado por la estación administradora para dar un valor determinado a una variable MIB de un nodo administrado. El nodo administrado responde con un mandato *get-response* idéntico al solicitante o con una indicación de error.

Trap: Es enviado por un nodo administrado a la estación administradora, de una forma no solicitada, para informar de ciertos eventos o cambios de estado en las variables.

La figura I.3 muestra el flujo de mandatos entre la estación administradora y el nodo administrado.

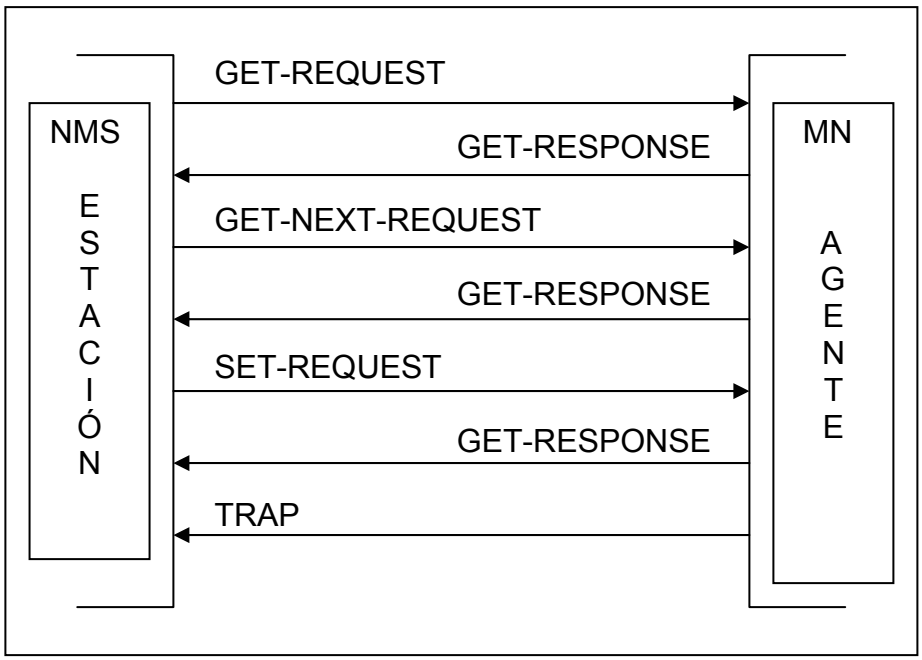


Figura I.3 Flujo de mandatos SNMP

En general, la estación administradora obtiene y guarda información actualizada sobre el estado de los objetos que administra mediante un **poleo (*polling*)** a intervalos regulares de tiempo.

En aquellos casos en los que los nodos administrados desean informar a su(s) administrador(es) de un acontecimiento extraordinario, sin esperar a ser preguntados, hacen uso del mecanismo de los traps.

Los **traps** se asocian a menudo a las alertas de la arquitectura de administración de red SNA. Sin embargo, existe una diferencia importante en la filosofía de concepción de ambas. Una alerta se utiliza para describir con gran detalle un problema, incluyendo información sobre configuración, probable causa de error, acción recomendada, entre otras.

Por el contrario, los traps son estructuras simples que no contienen gran detalle de información. El trap actúa como un disparador para provocar que el administrador SNMP solicite información adicional al agente.

I.2.2.1.2 Tramas SNMP

El envío de mandatos y respuestas SNMP se lleva a cabo mediante el intercambio de **mensajes UDP** (datagramas).

Un **datagrama** incluye el identificador de versión, el nombre de la comunidad y la **U**nidad de **D**atos del **P**rotocolo (**PDU**). Uno o más agentes se emparejan con un grupo de administradores SNMP formando lo que se llama una **Comunidad SNMP**. El nombre de la comunidad puede considerarse como una contraseña y es enviado siempre en cualquier tipo de trama.

I.2.2.2 Management Information Base (MIB)

La información de administración usada con SNMP se define como un conjunto de objetos administrados, utilizando la sintaxis abstracta **ASN.1**.

A una colección de objetos, referentes a un área de administración común, se le conoce con el nombre de "módulo MIB" o simplemente **MIB** (**M**anagement **I**nformation **B**ase).

También se conoce por MIB a la base de objetos de los agentes que pueden ser observados y controlados desde los administradores SNMP. Podemos decir, que la MIB define y contiene los objetos susceptibles de ser administrados.

Conceptualmente, la MIB representa una base de datos de "parámetros de administración". Los parámetros de administración son almacenados en una base de datos con estructura de árbol, similar a la estructura de archivos **DOS** o **UNIX**.

Las entradas cercanas a la raíz del árbol definen las organizaciones de las cuales dependen los diferentes parámetros. La MIB parece ser la mejor forma de representar globalmente los diferentes parámetros de administración que requieren los distintos dispositivos físicos.

I.2.2.2.1 MIB-I y MIB-II

Al primer conjunto de objetos aceptado como estándar por la **IAB** se le conoce por MIB-I. Se definió en la RFC 1156 y, actualmente, está clasificado como no-recomendable, debido a la revisión que sufrió y que dio lugar a un nuevo conjunto que se conoce como MIB-II (RFC 1223).

Dentro de la MIB estándar Internet, los objetos se encuentran clasificados en grupos:

- **Sistema:** Contiene información sobre la entidad, como el hardware y software del sistema y su versión, el tiempo desde la última iniciación, la persona de contacto, la localización física, entre otros.

- **Interfaces:** Contiene todas las interfaces por las que los nodos pueden enviar/recibir datagramas IP y tablas con el nombre de dichas interfaces (**Ethernet, Token-Ring**). Contiene también contadores para paquetes enviados/recibidos y errores.

- **Traducción de direcciones:** Contiene información para traducir una dirección de red en una dirección específica de subred o física.

- **IP:** Contiene información del nivel IP, como el número de datagramas enviados, recibidos y propagados. Incluye dos tablas: la tabla de direcciones IP, conteniendo la información de direccionamiento IP para la entidad, y la tabla de encaminamiento IP, que contiene una entrada para cada ruta actualmente conocida.

- **ICMP:** Contiene las estadísticas de entrada y salida del Protocolo de Mensaje de Control de Internet (***I**nternet **C**ontrol **M**essage **P**rotocol)*.

- **TCP:** Contiene información sobre las conexiones TCP, como el número máximo de conexiones que puede soportar la entidad, número total de segmentos transmitidos y recibidos, información acerca de las conexiones actuales, entre otros.

- **UDP:** Contiene información sobre el nivel UDP, como contadores de datagramas enviados y recibidos.

- **EGP:** Estadísticas y configuración de las funciones del Protocolo de Pasarela Externa (***E**xternal **G**ateway **P**rotocol)* soportadas, como el número de mensajes enviados y recibidos, contadores de error, entre otros.

- **Transmisión:** Información específica de cada medio de transmisión.

- **SNMP:** Contiene información sobre el agente SNMP, como el número de paquetes SNMP recibidos, el número de peticiones SNMP con nombres erróneos de comunidad, entre otros.

Cada agente SNMP (nodo administrado) soporta sólo aquellos grupos que le son apropiados. Por ejemplo, si no existe una pasarela, el grupo de objetos EGP no necesita ser soportado. Pero, si un grupo es apropiado, todos los de ese grupo deben estar soportados.

I.2.3 SUNNET MANAGER

Es un producto de la Administración de Red de SunSoft. Este producto tiene raíces con la compañía que ofrece sistemas informáticos basados en **SUN**.

I.2.3.1 Perspectiva

SUN Microsystems ha estado particularmente orientado hacia diseñar, desarrollar y traer sistemas de informática robustos para comercializar. Clasificar sistemas SUN con respecto al tamaño podría ser injusto. Algunos de sus sistemas pueden parecer ser físicamente pequeños pero muy poderosos.

A finales de los años 80 SUN tenía una interfaz de usuario muy utilizable basada en el sistema **X Windows**. Los sistemas SUN han estado categóricamente basados en TCP/IP en términos de orientación de red. Una red basada en TCP/IP puede comunicarse con una red basada en SNA.

SunNet Manager puede ser utilizado con eficacia en este panorama. La administración de la red TCP/IP completa se puede alcanzar por medio del sistema SUN y del software de administración.

I.2.3.2 Componentes

SunNet Manager es software construido sobre la arquitectura de la serie del protocolo TCP/IP. Además, utiliza **OpenLook** (el administrador de la ventana de SUN) que opera bajo el control del sistema X Windows.

X es un protocolo independiente y completo aunque es parte de la serie del protocolo TCP/IP. Sin embargo, X utiliza TCP como mecanismo de transporte. El poder del componente es realizado vía la síntesis en las capacidades de la administración a través de SunNet Manager.

SunNet Manager se explica mejor examinando sus componentes principales (Figura I.4), que incluyen:

- Aplicación de la administración
- Agentes
- Agentes proxy

La **aplicación de la administración** es software usado para recoger y administrar datos reunidos sobre nodos en todas partes de la red(es).

Los **agentes** son también software; ellos son los programas que recuperan la información sobre nodos cuando son solicitados por la aplicación de la administración.

Los **agentes proxy** son similares a los agentes en que ellos realizan las mismas funciones, con dos excepciones: (1) ellos son capaces de manejar múltiples protocolos debido al empleo de las técnicas de "Llamada de Procedimiento Remoto" (**RPC**) y (2) ellos son capaces de obtener la información sobre múltiples nodos, haciendo así la centralización posible cuando existen redes densas.

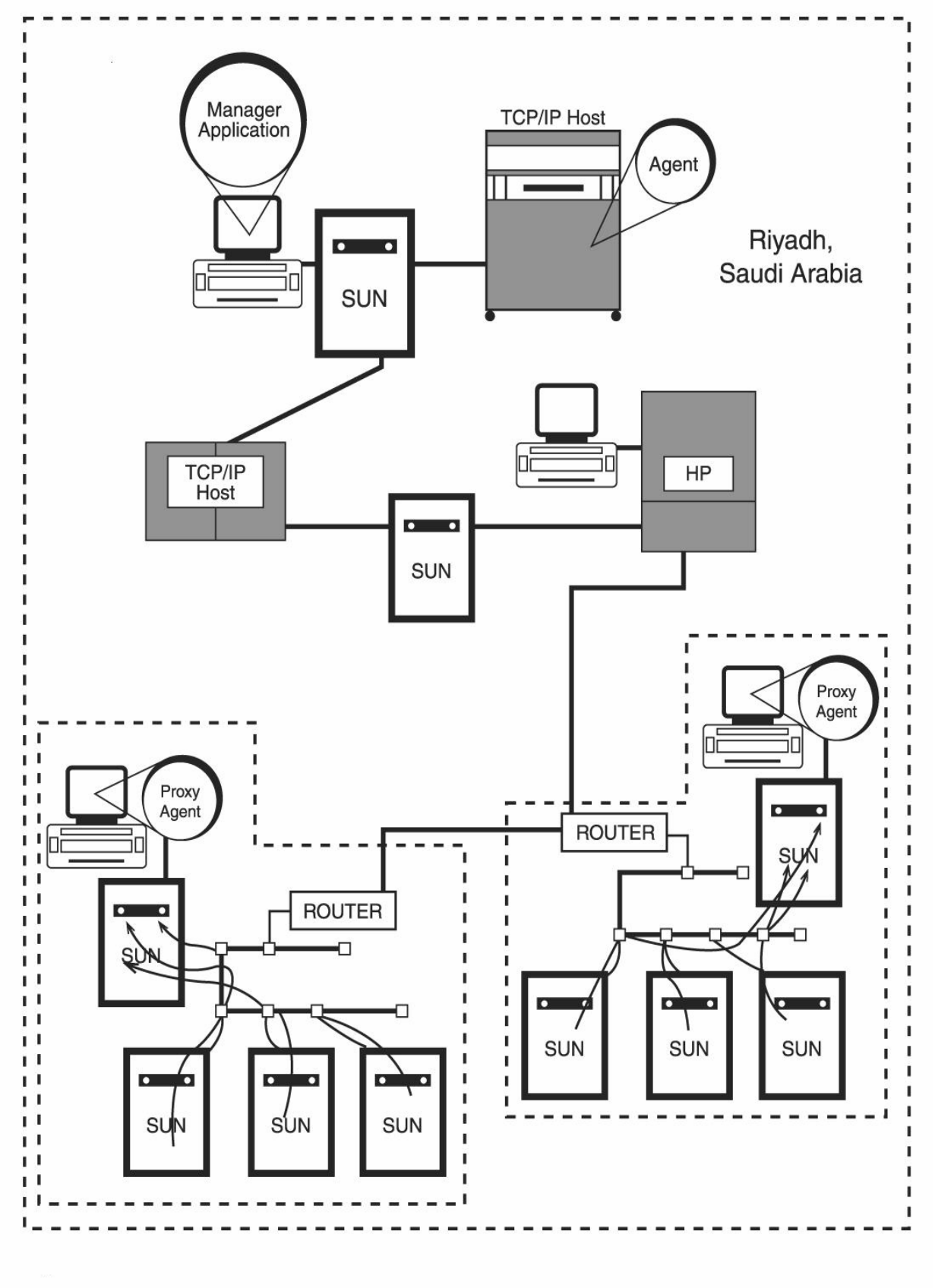


Figura I.4 Componentes de SunNet Manager

Esta ilustración muestra múltiples redes y múltiples anfitriones en estas redes. Los agentes proxy mostrados sirven como punto focal para la comunicación con la aplicación de la administración localizado en una red diferente. El efecto neto es que la aplicación de la administración es capaz de comunicarse indirectamente con los anfitriones en las redes.

Este arreglo de estructura de administración proporciona una estructura poderosa para la administración de red con múltiples protocolos y topologías.

I.2.3.3 La Consola de Administración

La **consola de administración** es el punto central para la interacción entre los usuarios humanos y las aplicaciones del software. La consola de administración es manejada por software, de éste las tareas de administración del software y la información mostrada pueden ser obtenidas.

El **informe de los datos** se puede realizar en cuadro, gráfico o formato de registro. Los informes de agentes pueden ser determinados periódicamente. El programa SunNet Manager proporciona las herramientas para ver y analizar datos del usuario.

El **evento informado** es simplemente eso. Cuando ocurre un evento especificado (definido por el usuario), los agentes envían estos datos a la aplicación del administrador.

Los datos informados por los agentes son almacenados en una base de datos para múltiples propósitos.

I.2.3.4 La Base de Datos de la Administración

La base de datos de la administración incluye una variedad de información. Alguna de esta información incluye el tipo de elemento de la red que es representado en la consola del SunNet Manager. Esto significa la identificación de una estación de trabajo, del encaminador u otro dispositivo.

Además de la definición del elemento está el caso del tipo de elemento. Un **caso** es el nombre del elemento de la red. Las solicitudes predefinidas que pueden ser invocadas también se enumeran en esta base de datos.

Estas definiciones son generalmente específicas del sitio. La definición del agente también se proporciona. Esto es crítico porque los agentes pueden ser ajustados para devolver diferentes atributos a la aplicación del administrador.

El uso de la consola del SunNet Manager, de agentes, de agentes proxy y de otros componentes del programa SunNet Manager categóricamente son definidos por el tipo de configuración.

I.2.3.5 Vista de la Red

La consola del SunNet Manager tiene que ser considerada una visión CASERA. Algunos consideran esta visión como la visión "crítica". Esta visión aparece normalmente en una de dos formas sin prioridad del orden de apariencia. Una es con detalles mínimos y la otra lo opuesto.

La visión que muestra la perspectiva total de la red es mejor cuando la red es densa con subredes y componentes. Considerada de esta manera, la red es vista en un **modelo árbol** formado de las raíces y del tronco hacia arriba y hacia afuera de las ramas (componentes individuales de la red).

I.2.3.6 Reunión de la Información y la Consola

Los home de la consola almacenan el menú de la administración y sirven como la interfaz entre los usuarios humanos y el SunNet Manager. La información del menú puede ser recopilada en una de tres maneras:

1. **Informes de datos:** La Información proporcionada por los informes de datos incluye valores de atributo para elementos de la red durante un período predeterminado de tiempo.

   Hay dos formas de solicitudes: solicitudes del **S**un**N**et **M**anager (**SNM**) y solicitudes personalizadas que pueden ser formuladas para preguntar por un elemento específico de la red. Ellas hacen que un agente dado envíe los atributos del elemento (datos) a una aplicación del administrador.

2. **Reportes de eventos:** Cuando la información es obtenida por reportes de eventos, un agente notifica a la aplicación del administrador, de cambios en los valores de

atributos del elemento. Este tipo de información puede ser considerada como el reporte de condiciones anormales dentro de un elemento o de una red dada.

El reporte de evento es logrado a través de la comunicación vía un agente o agente proxy y la aplicación de la administración. Un evento puede accionar un mensaje de E-mail, una alarma audible, un reporte a un programa u otra función que el usuario final determina asegurando la comunicación óptima entre el agente y la aplicación del administrador.

3. **Descargas rápidas:** Como el término implica, con este método, la reunión de la información es "rápida" y el conjunto de información es la "descarga". La información proporcionada por este método refleja la información en un grupo de agente y/o una tabla del agente.

Esta información puede ser obtenida seleccionando el elemento de la red vía el menú de solicitud de la consola. La otra manera de obtener esta información es usando las palabras claves en el menú glyph. Una vez que el elemento objeto es seleccionado, la información es recuperada.

I.2.3.7 Requisitos de Instalación

El SunNet Manager requiere ciertas especificaciones mínimas de hardware y de software, incluyendo:

- 32 Mbytes de memoria
- Espacio libre en disco:
  - 15 Mbytes para el SunNet Manager
  - Libro de respuestas (ninguna opción) < 1 Mbyte
  - Libro de respuestas (opción media) ≈ 7 Mbytes
  - Libro de respuestas (opción pesada) ≈ 27 Mbytes
  - Aproximadamente de 10 a 15 Mbytes para el tiempo de corrida de la base de datos
- SunOS 4.1.3 U1, revisión B (Solaris 1.1.1)
- OpenWindows 3.0
- Privilegios de Súper usuario para lectura, escritura y ejecución

I.2.4 OPENVIEW

Este producto, ofrecido por Hewlett-Packard, se puede utilizar para administrar TCP/IP, SNA y las redes de **NetWare**. Puede funcionar en las PC con Windows o en los sistemas basados en UNIX. Visto conceptualmente, esto se muestra en la Fig. I.5.

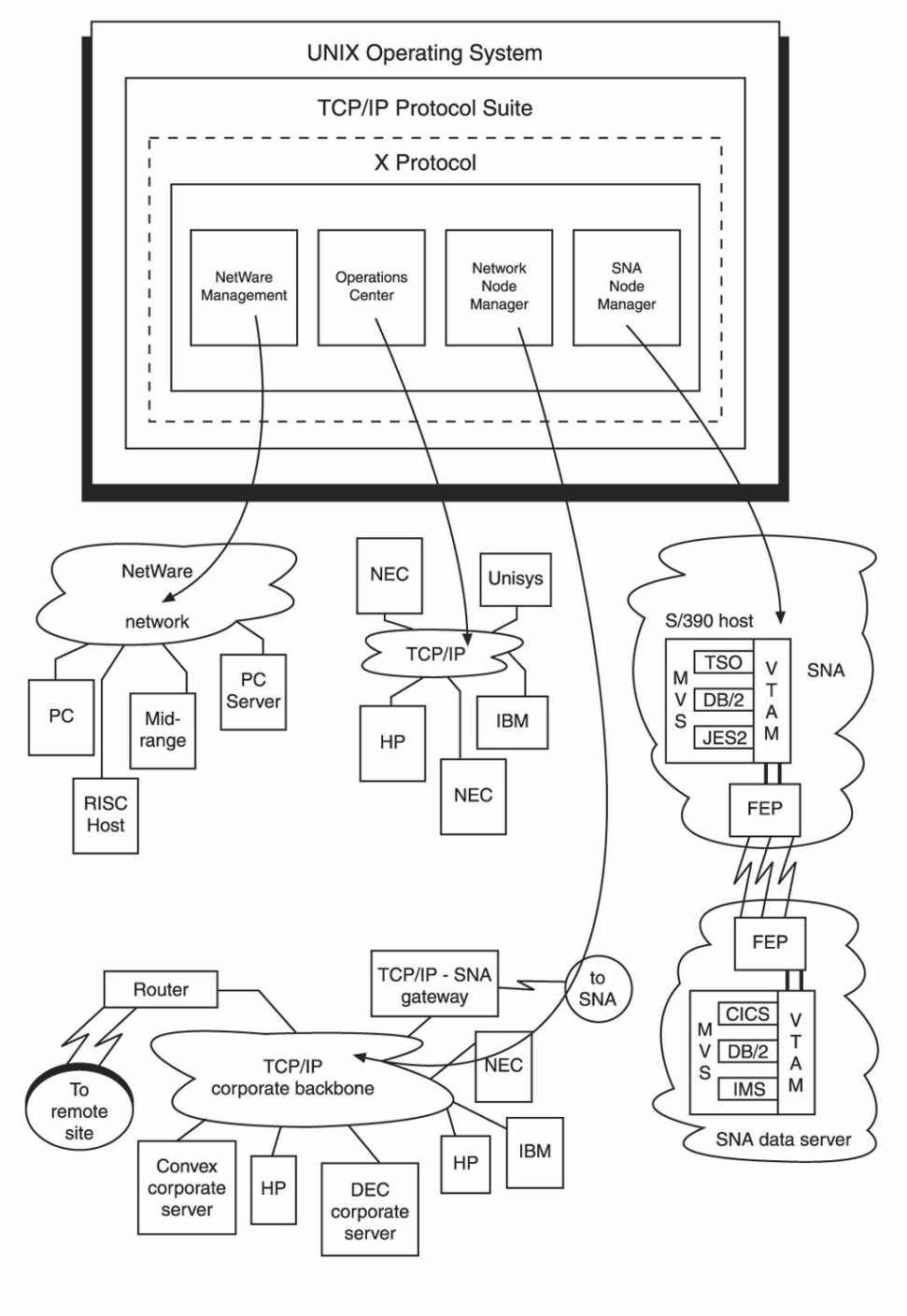


Figura I.5 Vista conceptual de OpenView

La figura I.5 es una vista que destaca los componentes individuales del producto de OpenView. Note la línea punteada al separar el protocolo X y el TCP/IP. En realidad, esto no es así; X es un protocolo de cinco capas en si mismo y utiliza TCP como un mecanismo de transporte.

OpenView utiliza el **protocolo X**, que es el que proporciona la capacidad del ventaneo en un ambiente UNIX. Un componente no mostrado es la base de datos utilizada por los componentes de OpenView. Esta base de datos trabaja con OpenView como una aplicación ordinaria en el ambiente UNIX.

Su diversidad proporciona flexibilidad y fuerza robusta para la administración de la red de multiplataforma. La figura I.6 ilustra esta idea.

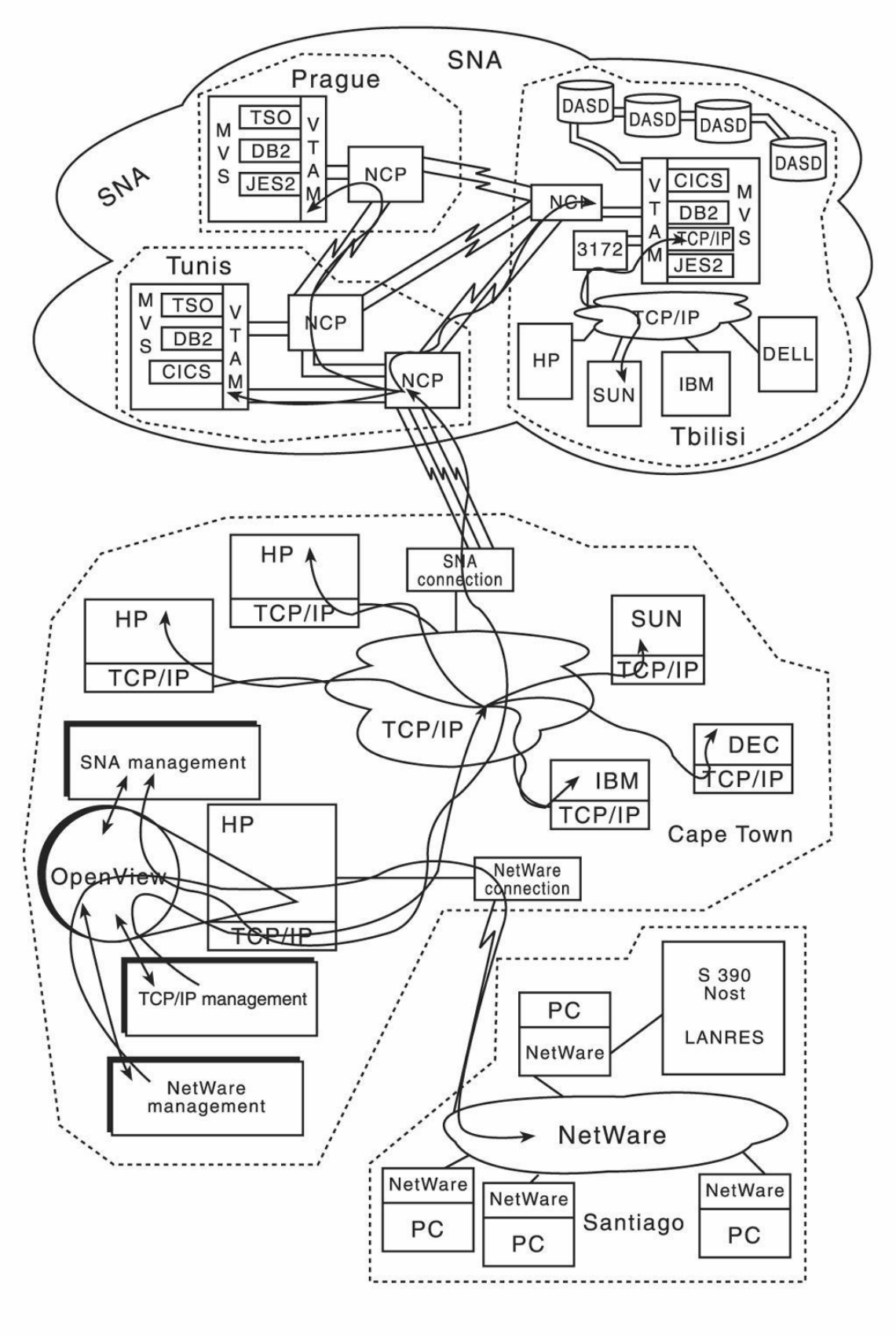


Figura I.6 Vista detallada de OpenView

I.2.4.1 Componentes de OpenView

El Administrador de Nodo de Red (**NNM**) es la parte del software basada en UNIX de OpenView usada para manejar redes basadas en TCP/IP, sean **LANs** o **WANs**. El NNM funciona conjuntamente con una base de datos almacenada en un sistema basado en UNIX.

La base de datos Ingres es donde NNM almacena su información sobre la red(es) que administra. NNM de HP puede también operar sobre el sistema operativo Solaris de SUN.

NNM puede funcionar bajo ventanas de **MS**. Este producto es llamado el **Administrador de Nodo de Windows de OpenView** (**OWNM**). OWNM está basado en PC-DOS o MS-DOS y trabaja absolutamente bien en las PC para supervisar la información estadística LAN.

Otro campo de OpenView es el Administrador Distribuido, llamado **OpenView DM**. Este se enfoca en los ambientes más complejos y sostiene estos ambientes por su amplia base de interfaces de programa de aplicación (**APIs**).

I.2.4.2 Arquitectura de OpenView

OpenView puede ser comprendido mejor cuando se examina claramente el ambiente total en el cual opera. Considere la Figura I.7.

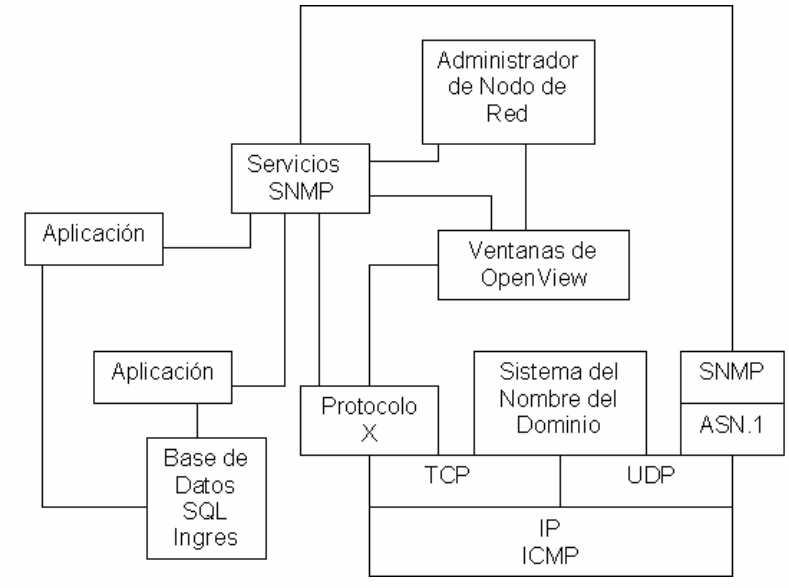


Figura I.7 Arquitectura y componentes de OpenView

Esta figura ilustra una visión general arquitectónica de OpenView. Una nota importante es la presuposición de OpenView y de su operación con una pila de TCP/IP. Note que OpenView utiliza el protocolo X.

X, alternadamente, es parte de las pilas más comunes del protocolo TCP/IP. Note que X utiliza servicios de SNMP también. Note también en la figura que X utiliza TCP como un protocolo de transporte.

I.2.4.3 Previa Vista del Administrador de Nodo de Red (NNM)

NNM está basado en servicios SNMP. Esto es parcialmente debido al diseño arquitectónico del producto de HP y parcialmente debido a la naturaleza operacional de cómo NNM interacciona con el Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP), el protocolo de red.

Por lo tanto, NNM tiene paralelos operacionales a SNMP cuando opera en ambientes de TCP/IP.

I.2.4.4 Operaciones del Componente de NNM

NNM puede ser explicado por componentes fundamentales y lo que ellos hacen. Aquí se explican los siguientes componentes que trabajan con NNM de OpenView:

- La plataforma de la administración SNMP
- Aplicaciones SNMP
- Evento de configuración SNMP
- El colector de datos MIB
- El constructor de aplicación MIB

La **plataforma de la administración SNMP** es un grupo de aplicaciones de tiempo de corrida. Ellos son la esencia del Administrador de Nodo de Red. Las aplicaciones personalizadas también pueden trabajar junto a estas aplicaciones de tiempo de corrida, proporcionando así un usuario con una interfaz de usuario común.

Las **aplicaciones SNMP** son simplemente esos programas de software que hace el Administrador de Nodo de Red (NNM). Diferentes aplicaciones proporcionan diferente información.

El **evento de configuración SNMP** es un programa que los usuarios usan para administrar cuántos "eventos" son mostrados en una ventana en un instante dado. El programa permite a los usuarios personalizar el reconocimiento de eventos específicos que ellos consideran apropiados para su localización.

El **colector de datos MIB** recoge datos de dispositivos específicos que son monitoreados en una red. El colector de datos MIB trabaja conjuntamente con el evento de configuración SNMP. Entre ellos dos, un usuario puede definir el umbral del evento; cuando este umbral es alcanzado, una alarma es activada para notificar al usuario.

El **constructor de aplicación MIB** permite a los usuarios crear pantallas personalizadas. Este programa realmente permite a un usuario mostrar datos en un texto, un gráfico o un formato tabular. La información mostrada por el usuario viene desde los MIBs.

I.2.4.5 Una Visión más Cercana

OpenView es una interfaz de ventaneo. Considere la figura I.8.

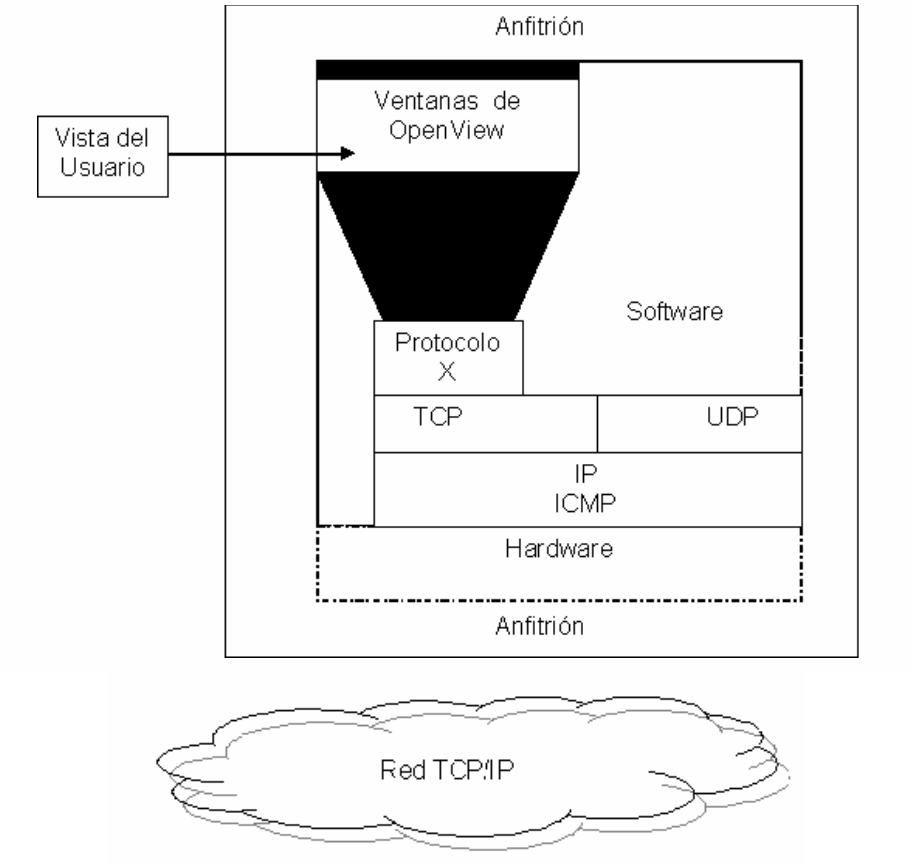


Figura I.8 OpenView percibido como un sistema de ventaneo

Note que OpenView mostrado usa el protocolo X. X no es un protocolo de la capa de transporte. X es un protocolo que puede ser dividido a sí mismo en cinco capas. X apoya un interfaz de ventaneo y las variaciones de programas que usan sus servicios.

I.2.4.6 La Interfaz

Los usuarios ven OpenView como un ambiente trabajador en el cual "las cosas" pueden ser manipuladas. Para entender la operación de esta interfaz se requiere un conocimiento de términos frecuentemente usados para describir y explicar el ambiente OpenView.

Los términos **objetos**, **mapas, submapas** y **símbolos** son fácilmente entendidos, pero a veces su uso para llevar un significado específico es sesgado, por lo cual se explicarán a continuación.

Un **objeto** se define mejor como algo que tiene atributos específicos mantenidos en la base de datos de OpenView. Así un objeto podría ser un encaminador, una computadora anfitrión, etc. En términos de la computadora, un objeto puede ser lógico o físico.

Un **mapa** es una colección de objetos, símbolos y submapas. Un mapa es la presentación de datos almacenados en la base de datos que define objetos. Los mapas pueden ser entendidos mejor examinando submapas.

Un **submapa** es una vista de una parte específica de una red.

Un **símbolo** representa un objeto vía la representación gráfica del objeto a través de un submapa. Los símbolos tienen un tipo y un estado que pueden serles atribuidos. El **tipo** se refiere a cómo el símbolo aparece en la pantalla. Su **estado** (es decir, su naturaleza operacional) se muestra por colores.

Diferentes colores implican diferente estado. Otro aspecto interesante de los símbolos es que ellos como se dice tienen un comportamiento; un símbolo es o ejecutable o explorable. Lo anterior implica que una función dada o un evento pasan una vez que un símbolo es seleccionado.

I.2.4.7 Requisitos de OpenView

Algunos requisitos básicos que requiere OpenView para operar incluyen:

- NetWare 3.1 (Nivel mínimo)
- TCP/IP NLM
- Mínimo procesador 386 en una PC
- Mínimo 4 MB de RAM en una PC
- Mínimo 4 MB de espacio en disco
- HP 9000 (serie 700 u 800)
- Mínimo 40 MB en disco duro
- Mínimo HP – UX versión 8.07 con X y OSF/Motif

I.2.5 MICROSOFT OPERATIONS MANAGER (MOM)

I.2.5.1 Descripción de MOM 2005

MOM 2005 proporciona el evento, la administración de funcionamiento, el monitoreo activo y alerta, el reporte y el análisis de tendencia, el sistema y aplicación de conocimiento específico y tareas para mejorar la posibilidad de administración de servidores Windows y aplicaciones.

I.2.5.1.1 Descripción de Características MOM 2005

Las siguientes son características de **MOM 2005**.

I.2.5.1.1.1 Seguridad

MOM implementa un modelo de seguridad que permite al personal y componentes trabajar con las cuentas que tienen niveles de privilegio inferiores.

I.2.5.1.1.2 Velocidad y Facilidad de Despliegue

Usar combinados la automatización y los Wizards es posible y dependiendo la escala de despliegue, desplegar MOM es un asunto de horas.

I.2.5.1.1.3 Amplitud de Banda Baja o Redes No Confiables

La aplicación de agentes de MOM asegura que la colección de datos sobre entidades administradas siga aún si hay una interrupción de red temporal.

I.2.5.1.1.4 Diagnóstico Extendido de Problema

Como MOM conserva datos operacionales en su propia base de datos, los analistas tienen un tiempo más largo para emplear en el diagnóstico.

I.2.5.1.1.5 Volumen de Datos

Múltiples vistas de MOM, el modelo de salud y la supervisión inteligente permiten a clientes filtrar y reducir los volúmenes grandes de datos de alerta.

I.2.5.1.1.6 Reporte Flexible, Robusto y Seguro

El Reporte MOM usa al Servidor Microsoft SQL y Servicios de Reporte del Servidor SQL que soportan el almacenamiento de largo plazo, reportan la utilización, exportaciones de datos, revisión, planificación y la seguridad de reporte.

I.2.5.1.1.7 Alta Disponibilidad

El modelo de administración de MOM le permite añadir servidores de administración, así se pueden ajustar para eliminar un solo punto de fracaso.

I.2.5.1.1.8 Adaptabilidad

El diseño de MOM es tal que se pueden administrar miles de recursos.

I.2.5.1.1.9 Alto Nivel de Integración

MOM proporciona el **M**arco **C**onector de **M**OM (**MCF**) y las APIs extensibles que le permite integrar MOM con virtualmente cualquier clase de sistema de administración o aplicación.

I.2.5.2 Componentes de Operaciones MOM 2005

La figura I.9 ilustra como los componentes de MOM primarios trazan un mapa del modelo de administración de operaciones.

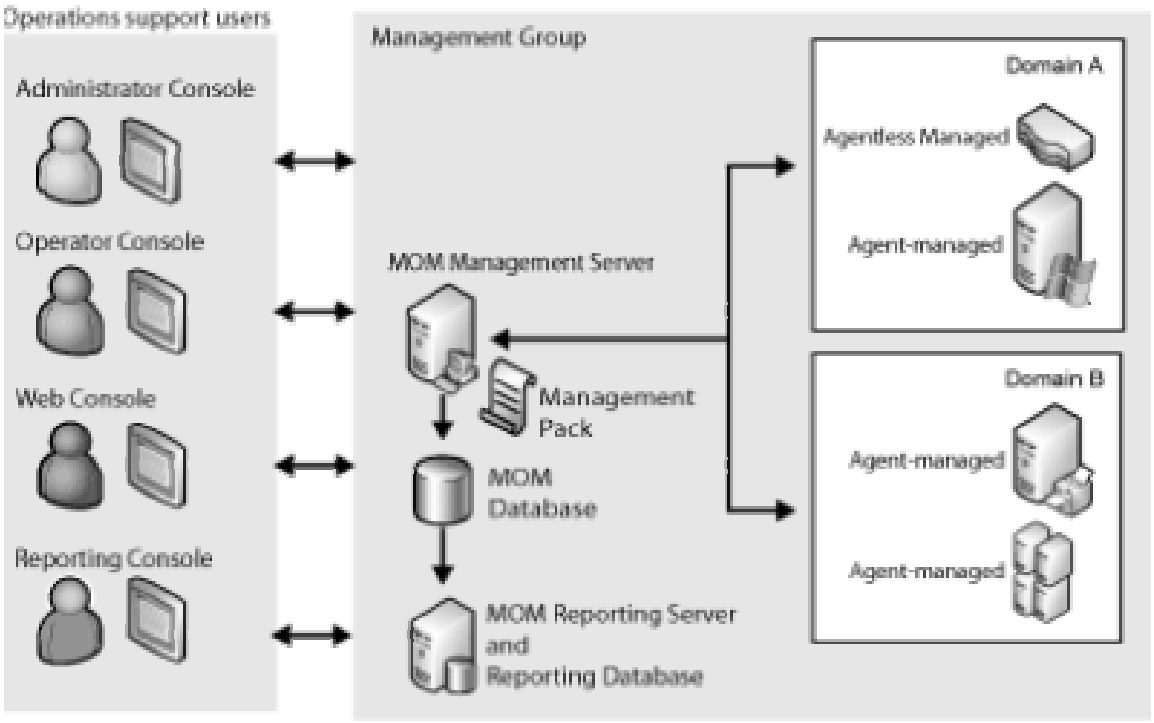


Figura I.9 Componentes de administración de operaciones MOM

La unidad de administración de operaciones fundamental es el **Grupo de Administración**. Los componentes siguientes están en este grupo:

- **El Servidor de Administración MOM:** Realiza varios papeles críticos en el ambiente de administración:

  - Despliega la información de configuración del Paquete de Administración a las computadoras administradas por agente.
  - Proporciona un ambiente para la creación, la modificación y la aplicación de Paquetes de Administración.
  - Proporciona las herramientas para administrar el ambiente de MOM.

- **Computadora Administrada:** Al menos una computadora administrada. MOM implementa dos accesos a computadoras administradas:

  - *Agente administrado*: Controla un servicio local en la computadora donde usted lo instaló y monitorea esta computadora usando las reglas del Paquete de Administración que son instaladas como parte de la instalación del agente.
  - *Agente menor administrado*: No se instala ningún software en la computadora que se quiera administrar. En cambio, el Agente de MOM, recoge datos desde la computadora administrada.

- **El Paquete de Administración:** Al menos un Paquete de Administración, que contiene las reglas que son aplicadas a computadoras administradas en el Grupo de Administración.

  Los Paquetes de Administración sirven como un contenedor y vehículo de distribución que MOM utiliza para desplegar la información de configuración requerida para administrar computadoras y aplicaciones.

  Un Paquete de Administración consiste en una colección de reglas, conocimientos y vistas públicas. El Paquete de Administración hace posible recolectar un amplio rango de información desde diferentes fuentes.

  Los Paquetes de Administración son usados para determinar como un servidor de administración MOM reúne, maneja y responde a los datos.

- **Interfaces de Usuario:** La siguiente es una lista de las interfaces de usuario de MOM.

    - Consola de Administrador
    - Consola de Operador
    - Consola Web
    - Consola de Reporte

I.2.5.3 Consola de Administrador

La Consola de Administrador sirve para **dos objetivos**. **Primero**, proporciona todas las herramientas que un Administrador de MOM necesita para administrar y mantener un ambiente de MOM. Esto incluye tareas tales como instalar/quitar agentes y cambios en los ajustes de la configuración.

El **segundo** objetivo es el proporcionar las herramientas que se pueden usar para cambiar el ambiente de monitoreo definido por los Paquetes de Administración que son instalados. Por ejemplo, ellos pueden añadir, borrar, inhabilitar y cambiar reglas.

I.2.5.4 Consola de Operador

Es escrita en el código administrado y proporciona la mirada y el sentido que usted esperaría tanto del MMC como de la interfaz de navegador. La Consola de Operador da a su personal de operaciones la interfaz que ellos necesitan para:

- Ver la salud, en tiempo real, de las computadoras que monitorean
- Obtener diferentes vistas de la información que viene de computadoras administradas
- Obtener la información de alto nivel y detallada acerca de un evento específico o alerta
- Trabajar con alertas, por ejemplo, reconocer una alerta o asignar el problema a otro empleado
- Las tareas controladas predefinidas que son proporcionadas en la consola

I.2.5.5 Consola Web

La Consola Web está basada y diseñada en navegadores para proporcionar una interfaz que puede ser usada para dar la funcionalidad básica para situaciones de monitoreo distribuidas que sólo requieren vistas limitadas y la capacidad de administración de alertas.

Las vistas incluyen Alertas, Eventos y Computadoras. Dependiendo de la vista que usted selecciona, usted puede examinar la vista de la información o el estado de cambio de alerta.

I.2.5.6 Consola de Reportes

Accediendo desde el menú de Inicio o desde la consola de Administrador de MOM, la Consola de Reporte está basada en navegadores y es implementada por los Servicios de Reporte del Servidor Microsoft SQL.

Esta interfaz provee un fin frontal al Servidor de Reporte de MOM, que aplica plantillas de reportes a los datos apropiados que son almacenados en la Base de Datos de Reportes de MOM.

La Base de Datos de Reportes contiene una copia de los datos operacionales que es almacenada en la Base de datos de MOM.

I.2.5.7 Conceptos de MOM 2005

Esta sección destaca algunos conceptos claves.

I.2.5.7.1 Datos de MOM

Durante el descubrimiento de computadora y el monitoreo de la aplicación, los datos que son generados son almacenados en la Base de datos de MOM. El monitoreo produce cuatro tipos de datos: datos de evento, de funcionamiento, de alerta y de descubrimiento.

I.2.5.7.1.1 Datos de Evento

Los datos de eventos recogidos pueden ser usados para:

- Ver los datos operacionales en la consola de Operador
- Proporcionar un contexto para problemas (en forma de Alertas) que son detectados
- Proporcionar información sobre el monitoreo de MOM y las actividades de administración
- Proporcionar información sobre el estado de la computadora

I.2.5.7.1.2 Datos de Funcionamiento

Los datos de funcionamiento numéricos son recopilados de fuentes como contadores de funcionamiento de Windows e Instrumentación de Administración de Windows (**WMI**). Los datos de funcionamiento recogidos pueden ser usados para:

- Ver datos de funcionamiento en la consola de Operador usando diferentes formatos como formas, listas y gráficos

I.2.5.7.1.3 Datos de Alerta

Los datos de alerta representan un problema que es detectado en las computadoras administradas. Las alertas son los indicadores que informan a los usuarios sobre la salud de las computadoras administradas. Las alertas también proporcionan la base para el monitoreo de estado.

I.2.5.7.1.4 Datos de Descubrimiento

A diferencia de otros datos de operaciones, los datos de descubrimiento no están directamente expuestos al usuario. Los datos de descubrimiento son expuestos como diagramas de topología, atributos de computadora, listas de servicios o de computadora.

I.2.5.7.2 Grupos de Computadora

Los grupos de computadora contienen una lista de las computadoras que son vistas y administradas como una sola entidad.

La ventaja de usar grupos de computadora es que el monitoreo de vistas y la responsabilidad de operaciones pueden reflejar el modo en que su negocio está organizado.

Las reglas de grupo de computadora son usadas para definir como computadoras similares son agrupadas.

I.2.5.7.3 Grupos de Regla y Reglas

Los Grupos de Regla contienen las colecciones de Reglas para monitorear los diferentes aspectos de una computadora administrada.

MOM usa reglas para determinar como recoger, procesar y responder a datos generados por computadoras administradas. Dependiendo del tipo de información de una regla procesada, las reglas son clasificadas como reglas de evento, de alertas y de funcionamiento.

- **Reglas de evento:** MOM usa reglas de Evento para monitorear eventos y en algunos casos, especificar que las alertas son generadas y las respuestas son iniciadas. La mayoría de eventos y sus alertas asociadas son almacenados en la base de datos.

- **Reglas de alerta:** Especifican una respuesta para una alerta o para una colección de alertas predefinidas.

- **Reglas de funcionamiento:** Definen como los datos del contador de funcionamiento y los datos numéricos de la Instrumentación de Administración de Windows (WMI) son procesados.

I.2.5.7 Estado de Monitoreo

El estado de monitoreo es usado para indicar si o no una computadora administrada está saludable en un tiempo dado. MOM actualiza el estado de las computadoras

administradas expuestas al usuario y presenta su estado en la vista del estado de monitoreo.

En resumen, el estado de una computadora administrada es un valor de severidad de alerta que especifica que tan severo es el problema - si este existe - en el ambiente de una computadora administrada.

I.2.5.7.5 Vistas de MOM

MOM proporciona las vistas siguientes que se pueden usar y personalizar cuando se trabaja con la Consola de Operador.

- **Vista de Alertas:** Esta dividida en dos categorías, Alertas y Excepciones de Nivel de Servicio. Esta vista muestra la información resumida y expandida para una alerta específica.

- **Vista de Estado:** Muestra la información agregada sobre alertas y sus entidades asociadas (por ejemplo, grupos de computadora, computadoras, e instancias de aplicación).

- **Vista de Eventos:** Es dividida en dos categorías, Eventos y el estado de Tarea para las tareas que usted controla desde la consola de Operador. Esta vista muestra todas las categorías de los eventos que son generados.

- **Vista de Diagrama:** Usa una simple ventana para generar un diagrama de topología que está basado en su grupo de administración y el Paquete(s) de Administración que es seleccionado.

- **Mis Vistas:** Muestran cualquier vista personalizada que usted crea.

I.2.5.8 Requerimientos de MOM 2005

Comprobar los datos específicos de hardware para cualquier computadora que reciba la Base de Datos de MOM, el Servidor de Administración, las Consolas MOM y los Agentes frente a hardware mínimo y requerimientos de software que son especificados. Quitar cualquier computadora que no contenga el hardware mínimo o la especificación de software.

I.2.5.8.1 Configuraciones Soportadas por MOM 2005

En esta parte se proporciona la información sobre Sistemas Operativos soportados, configuraciones de hardware y requerimientos de software para MOM 2005.

I.2.5.8.1.1 Sistemas Operativos Soportados

Las tablas en esta sección, consideran los Sistemas Operativos soportados (Windows XP y Windows Server 2003), para cada componente de MOM 2005. Hay dos tablas para cada Sistema Operativo; cada una considera el soporte a un conjunto diferente de componentes de MOM.

Soporte para Microsoft WINDOWS XP

Sistema Operativo	Servidor de Administración MOM (32-bit)	Base de Datos MOM (32-bit)	Consola Administrador y Consola Operador MOM (32-bit)	Servidor de Reportes MOM (32-bit)
Windows XP Home Edition con cualquier paquete de servicio	No	No	No	No
Windows XP Media Center Edition con cualquier paquete de servicio	No	No	No	No

Tabla I.1 Sistemas Operativos soportados en Microsoft WINDOWS XP (Parte 1)

Sistema Operativo	Servidor de Administración MOM (32-bit)	Base de Datos MOM (32-bit)	Consola Administrador y Consola Operador MOM (32-bit)	Servidor de Reportes MOM (32-bit)
Windows XP Tablet PC Edition con cualquier paquete de servicio	No	No	No	No
Windows XP Professional sin ningún paquete de servicio	No	No	No	No
Windows XP Professional con SP 1 o posterior	No	No	SI	No
Windows XP 64-Bit Edition con Service Pack 1 o posterior	No	No	No	No
Windows XP Embedded (cualquier liberación)	No	No	No	No

Sí = Sistema Operativo soportado; No = Sistema Operativo no soportado

Tabla I.1 Sistemas Operativos soportados en Microsoft WINDOWS XP (Parte 1) (Continuación)

Sistema Operativo	Computadora administrada por agente (32-bit)	Computadora administrada por agente (64-bit)	Computadora administrada por agente menor (32-bit)	Vista de Reportes MOM (32-bit)
Windows XP Home Edition con cualquier paquete de servicio	No	No	No	No
Windows XP Media Center Edition con cualquier paquete de servicio	No	No	No	No
Windows XP Tablet PC Edition con cualquier paquete de servicio	No	No	No	No
Windows XP Professional	SI	No	SI	SI

Tabla I.2 Sistemas Operativos soportados en WINDOWS XP (Parte 2)

Sistema Operativo	Computadora administrada por agente (32-bit)	Computadora administrada por agente (64-bit)	Computadora administrada por agente menor (32-bit)	Vista de Reportes MOM (32-bit)
Windows XP Professional con Service Pack 1 o posterior	SI	No	SI	SI
Windows XP 64-Bit Edition con Service Pack 1 o posterior	No	No	SI	SI
Windows XP Embedded (cualquier liberación)	No	No	No	No

Sí = Sistema Operativo soportado; No = Sistema Operativo no soportado

Tabla I.2 Sistemas Operativos soportados en WINDOWS XP (Parte 2) (Continuación)

Soporte para Microsoft Windows Server 2003 Family

Sistema Operativo	Servidor de Administración MOM (32-bit)	Base de Datos MOM (32-bit)	Consola Administrador y Consola Operador MOM (32-bit)	Servidor de Reportes MOM (32-bit)
Windows Server 2003, Edición estándar	SI	SI	SI	SI
Windows Server 2003, Edición de empresa	SI	SI	SI	SI
Windows Server 2003, Edición Datacenter	SI	SI	SI	SI
Windows Server 2003, Edición Web	SI	SI	SI	SI
Windows Server 2003, Edición estándar con Service Pack 1	SI	SI	SI	SI

Tabla I.3 Sistemas Operativos soportados por Microsoft Windows Server 2003 Family (Parte 1)

Sistema Operativo	Servidor de Administración MOM (32-bit)	Base de Datos MOM (32-bit)	Consola Administrador y Consola Operador MOM (32-bit)	Servidor de Reportes MOM (32-bit)
Windows Server 2003, Edición de empresa con Service Pack 1	SI	SI	SI	SI
Windows Server 2003, Edición Datacenter con Service Pack 1	SI	SI	SI	SI
Small Business Server 2003 con Service Pack 1	SI	SI	SI	SI
Windows Server 2003, Edición Web con Service Pack 1	SI	SI	SI	SI

Tabla I.3 Sistemas Operativos soportados por Microsoft Windows Server 2003 Family (Parte 1) (Continuación)

Sistema Operativo	Servidor de Administración MOM (32-bit)	Base de Datos MOM (32-bit)	Consola Administrador y Consola Operador MOM (32-bit)	Servidor de Reportes MOM (32-bit)
La versión de 64-bit de Windows Server 2003, Edition de empresa para Sistemas de 64-Bit basados en Itanium	No	SI(1)	No	No
La version de 64-bit de Windows Server 2003, Edición Datacenter para sistemas de 64-Bit basados en Itanium	No	SI(1)	No	No

Sí = Sistema Operativo soportado; No = Sistema Operativo no soportado

Tabla I.3 Sistemas Operativos soportados por Microsoft Windows Server 2003 Family (Parte 1) (Continuación)

Sistema Operativo	Computadora administrada por agente (32-bit)	Computadora administrada por agente (64-bit)	Computadora administrada por agente menor (32-bit)	Vista de Reportes MOM (32-bit)
Windows Server 2003, Edición estándar	Si	No	Si	Si
Windows Server 2003, Edición de empresa	Si	No	Si	Si
Windows Server 2003, Edición Datacenter	Si	No	Si	Si
Windows Small Business Server 2003	Si	No	Si	Si

Tabla I.4 Sistemas operativos soportados en Windows Server 2003 Family (Parte 2)

Sistema Operativo	Computadora administrada por agente (32-bit)	Computadora administrada por agente (64-bit)	Computadora administrada por agente menor (32-bit)	Vista de Reportes MOM (32-bit)
Windows Server 2003, Edición Web	Si	No	Si	Si
Windows Server 2003, Edición estandar con Service Pack 1	Si	No	Si	Si
Windows Server 2003, Edición de empresa con Service Pack 1	Si	No	Si	Si

Tabla I.4 Sistemas operativos soportados en Windows Server 2003 Family (Parte 2) (Continuación)

Sistema Operativo	Computadora administrada por agente (32-bit)	Computadora administrada por agente (64-bit)	Computadora administrada por agente menor (32-bit)	Vista de Reportes MOM (32-bit)
Windows Server 2003, Edición Datacenter con Service Pack 1	Si	No	Si	Si
Small Business Server 2003 con Service Pack 1	Si	No	Si	Si
Windows Server 2003, Edición Web con Service Pack 1	Si	No	Si	Si

Tabla I.4 Sistemas operativos soportados en Windows Server 2003 Family (Parte 2) (Continuación)

Sistema Operativo	Computadora administrada por agente (32-bit)	Computadora administrada por agente (64-bit)	Computadora administrada por agente menor (32-bit)	Vista de Reportes MOM (32-bit)
La version de 64-bit de Windows Server 2003, Edición de empresa para sistemas de 64-Bit basados en Itanium	No	Si	Si	Si
La version de 64-bit de Windows Server 2003, Edición Datacenter para sistemas de 64-Bit basados en Itanium	No	Si	Si	Si

Sí = Sistema Operativo soportado; No = Sistema Operativo no soportado

Tabla I.4 Sistemas operativos soportados en Windows Server 2003 Family (Parte 2) (Continuación)

I.2.5.8.1.2 Requerimientos Mínimos de Hardware

Esta sección perfila los requerimientos mínimos y recomendados de hardware para cada componente MOM. Si usted quiere instalar más de un componente MOM sobre la misma computadora, siga los más altos requerimientos mínimos de hardware para cualquiera de los componentes MOM combinados.

Para instalar todos los **Componentes de MOM** sobre una Computadora, usted debe tener:

- Procesador dual Compatible Pentium de 550 MHz o más alto
- 1 GB de RAM (4 GB o más alto recomendado)
- 1 GB de espacio de disco duro disponible (Para el Reporte, mucho más espacio de unidad de disco podría ser necesario)
- Unidad de CD-ROM (Si está instalando MOM en esta computadora)
- Adaptador de Red

Para usar al **Servidor de Administración de MOM 2005,** usted debe tener:

- Procesador Compatible Pentium de 550 MHz o más alto (procesadores duales compatibles Pentium de 450 MHz o más alto recomendado)
- 512 MB de RAM (1 GB o más alto recomendado)
- 5 GB de espacio de disco duro disponible
- Unidad de CD-ROM (Si está instalando MOM en esta computadora
- Adaptador de Red

Para usar la **Base de Datos MOM 2005**, usted debe tener:

- Procesador Compatible Pentium de 550 MHz o más alto (procesadores duales compatibles Pentium de 450 MHz o más alto recomendado)
- 512 MB de RAM (1 GB o más alto recomendado)
- 5 GB de espacio de disco duro disponible
- Adaptador de Red

Para usar la **Consola de Administrador** y la **Consola de Operador de MOM 2005**, usted debe tener:

- Procesador Compatible Pentium de 500 MHz o más alto (procesador compatible Pentium de 1 GHz o más alto recomendado)
- 128 MB de RAM (256 MB o más alto recomendado)
- 150 MB de espacio de disco duro disponible
- Windows 2000 - adaptador compatible de vídeo de gráficos capaz de mostrar una resolución de 1024 × 768 con color de 24 bit o más alto recomendado
- Adaptador de Red
- Mouse u otro dispositivo de señalamiento

Para cada **computadora administrada por agente**, usted debe tener:

- Procesador Compatible Pentium de 200 MHz o más alto (procesador compatible Pentium de 300 MHz o más alto recomendado)
- 128 MB de RAM (más memoria podría ser necesaria dependiendo cuáles paquetes de administración use)
- El tamaño del software de agente instalado es aproximadamente 3 MB. Le recomiendan que usted asigne 100 MB de espacio de disco duro disponible para el uso de agente (más espacio de disco duro podría ser necesario dependiendo de cuáles paquetes de administración use)
- 3 MB de espacio de disco duro adicional es necesario para cada grupo de administración al cual un agente es añadido

I.2.5.8.1.3 Requerimientos Mínimos de Software

Esta sección perfila los requerimientos mínimos de software que usted debe tener para cada componente MOM más allá del sistema operativo. Si usted quiere instalar más de un componente MOM sobre la misma computadora, usted debe instalar el prerrequisito de software para todos los componentes de MOM combinados**.**

Para usar al **Servidor de Administración de MOM 2005**, usted debe tener:

- Microsoft Data Access Components (MDAC) versión 2.8.1022.0 o posterior
- Microsoft .NET Framework version 1.1

Para usar la **Base de Datos MOM 2005**, usted debe tener:

- Microsoft SQL Server 2000 Edición estándar o de empresa con Service Pack 3.0a o posterior

Para usar la **Consola de Administrador de MOM 2005** y la **Consola de Operador**, usted debe tener:

- Microsoft .NET Framework versión 1.1
- Uno de los navegadores siguientes:
  - Microsoft Internet Explorer 6 con Service Pack 1
  - Microsoft Internet Explorer 5.5 con Service Pack 2
  - Netscape 4.78 o posterior

Para usar al **Agente de MOM 2005**, usted debe tener:

- Para instalar al Agente MOM, no hay requerimientos adicionales de software más allá de un sistema operativo soportado

I.2.5.9 Seguridad en MOM

I.2.5.9.1 Seguridad del Servidor de Administración

Lo nuevo en MOM 2005 es el Marco Conector de MOM (MCF), que da a MOM la capacidad de recibir datos de, y enviar datos a, otros productos de administración. El Servidor de Administración cuenta con los servicios citados abajo para proporcionar seguridad.

I.2.5.9.1.1 Servicio de Acceso de Datos (DAS)

El componente DAS corre en el Servidor de Administración y los accesos y datos de actualizaciones en la Base de datos de MOM (OnePoint). El componente DAS se comunica sobre OLEDB, con el Servidor de Base de Datos de MOM.

Por defecto esta transmisión no es cifrada, pero usted puede usar o **IPSec** o el Cifrado OLEDB (**SSL**) para asegurar estos datos.

I.2.5.9.1.2 Cuenta de Acción

La Cuenta de Acción es nueva en MOM 2005 y es usada para juntar datos de operaciones de, y correr respuestas en, el Servidor de Administración. Esto también puede ser usado para instalar agentes en computadoras remotas o actualizar ajustes de agente.

I.2.5.9.1.3 Autenticación Mutua

Esta característica es nueva en MOM 2005 y requiere al Servidor de Administración y al agente para autenticarse el uno al otro antes de la comunicación. Esta usa el protocolo de autenticación Kerberos v5 proporcionado en Windows 2000, Windows XP y Windows Server 2003.

I.2.5.9.1.4 Canal de Comunicaciones Seguro

Las comunicaciones entre el agente de MOM 2005 y el Servidor de Administración son siempre cifradas y digitalmente marcadas por defecto y también son autenticadas (si permiten la autenticación mutua).

I.2.5.9.2 Seguridad de la Base de Datos de MOM

La Base de Datos usada por MOM es instalada con permisos suficientemente seguros, sin embargo, usted puede aumentar la seguridad usando o la política IPSec o el cifrado OLEDB para cifrar los datos que han sido transmitidos a o de la base de datos.

I.3 ADMINISTRACIÓN DE SISTEMAS ABIERTOS: UNA VISIÓN GENERAL

Tanto **CCITT** como **ISO** han propuesto normas para las redes de administración. La ISO y el CCITT son grupos diferentes pero abrazan las mismas ideas referentes a las normas de la administración.

I.3.1 Información General de la Administración de Sistemas

Hay **tres grupos** principales de **normas** de la administración de sistemas:

1. Normas que especifican **funciones** de las administraciones de sistemas
2. Normas que especifican **objetos** administrados
3. Servicio de la capa de aplicación y las normas del **protocolo** para comunicar la información de la función de la administración

Las **cinco áreas** de las actividades de **administración de sistemas** requeridas son:

1. Administración de fallas
2. Administración de la configuración
3. Administración de la contabilidad
4. Administración de la funcionalidad
5. Administración de la seguridad

I.4 TABLA CON LAS CARACTERÍSTICAS MÁS IMPORTANTES DE LOS SISTEMAS DE ADMINISTRACIÓN

En las siguientes tablas se muestra un listado con las características más importantes con las que debe de contar un sistema de administración de redes, haciendo una comparación entre los sistemas de acuerdo con sus características particulares; para así obtener el sistema que se adecue a las características y necesidades del Laboratorio de Redes y Seguridad de la Facultad de Ingeniería.

SISTEMAS / CARAC-TERÍSTICAS	NETVIEW	SNMP	SUNNET MANAGER	OPENVIEW	MOM 2005
Alertas de posibles condiciones de error	✓	✓	✓	✓	✓
Resolución automática de problemas	✓				
Monitoreo de rendimiento, tráfico y utilización de recursos	✓	✓	✓	✓	✓
Seguridad		✓			✓
Administración de cuentas de los usuarios		✓			✓
Monitoreo y estadísticas	✓	✓	✓	✓	✓
Notificación automática de cambios de configuración		✓			✓
Administración de dispositivos SNMP	✓	✓	✓	✓	✓
Recopilación de datos de hardware y software	✓	✓	✓	✓	✓

Tabla I.5 Comparación entre sistemas de administración

SISTEMAS / CARAC-TERÍSTICAS	NETVIEW	SNMP	SUNNET MANAGER	OPENVIEW	MOM 2005
Administración de los cambios de software					✓
Informes sobre utilización de aplicaciones	✓	✓	✓	✓	✓
Archivos de bases de datos protegidos	✓	✓	✓	✓	✓
Niveles de acceso de los usuarios		✓	✓		✓
Visualización de espacio libre de disco en servidor				✓	
Visualización de espacio libre de disco en estaciones de trabajo				✓	
Empresa creadora	IBM	VARIOS FABRI-CANTES	SUN MICRO-SYSTEMS	HP	Microsoft

Tabla I.5 Comparación entre sistemas de administración (Continuación)

CAPÍTULO II

EVALUACIÓN DEL LABORATORIO DE REDES Y SEGURIDAD

"Las ciencias y las letras son el alimento de la juventud y el recreo de la vejez".

II. 1 OBJETIVO DE UN CENTRO DE CÓMPUTO

La computadora como herramienta de solución para problemas de cálculo de operaciones, investigación de procesos, enseñanza, etc. establece las bases para determinar el objetivo de un **Centro de Cómputo** que es el conjunto de recursos físicos, lógicos y humanos necesarios para la organización, realización y control de las actividades informáticas de una institución.

Dichas actividades deben satisfacer las necesidades de información de la institución, de manera veraz y oportuna y su función principal es apoyar la labor de la institución mediante una más acertada toma de decisiones y así hacerla más segura, fluida y simplificada.

Un centro de cómputo, tiene la responsabilidad de acaparar, centralizar, custodiar y procesar la mayoría de los datos con los que opera una institución.

II.2 ORGANIZACIÓN DE UN CENTRO DE CÓMPUTO

Para lograr el objetivo de un centro de cómputo planteado en el punto anterior es necesario contemplar la organización de éste, ya que la importancia que tiene dentro de la institución lo coloca en una posición que influye incluso en una gran parte de las decisiones administrativas y de proyección de la institución.

Prácticamente todas las actividades de la institución se basan en la información que les procesa el centro de cómputo, por lo tanto debe tener una organización adecuada para obtener información al día, mediante procesos precisos y de alta calidad, ya que un centro de cómputo mal organizado repercutirá en la perdida de la información, que no podrá ser recuperada bajo ningún tipo de inversión.

Por lo tanto para lograr una buena organización del centro de cómputo se han agrupado sus diferentes actividades con el fin de simplificar las mismas y sus funciones.

Así, las principales funciones que se requieren para operar un centro de cómputo son las siguientes:

- Operar el sistema de computación central y mantener el sistema disponible para los usuarios
- Ejecutar los procesos asignados conforme a los programas y calendarios preestablecidos, dejando el registro correspondiente en las solicitudes de proceso
- Revisar los resultados de los procesos e incorporar acciones correctivas
- Realizar las copias de respaldo (back-up) de la información y procesos de cómputo, conforme a parámetros preestablecidos
- Marcar y/o señalar los procesos ejecutados
- Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados
- Realizar labores de mantenimiento y limpieza de los equipos del centro de cómputo
- Aplicar en forma estricta las normas de seguridad y control establecidas

II.3 PRINCIPALES DEPARTAMENTOS DE UN CENTRO DE CÓMPUTO

Dentro de una institución, el **C**entro de **P**roceso de **D**atos (**CPD**) o Centro de Cómputo cumple las diversas funciones mencionadas en el punto anterior que justifican los puestos de trabajo establecidos que existen en él, los cuales se engloban a través de los siguientes departamentos:

- **Explotación de sistemas o aplicaciones**. La explotación u operación de un sistema informático o aplicación informática consiste en la utilización y aprovechamiento del sistema desarrollado. Consta de previsión de fechas de realización de trabajos, operación general del sistema, control y manejo de soportes, seguridad del sistema, supervisión de trabajos, etc.

- **Soporte técnico a usuarios**. El soporte, tanto para los usuarios como para el propio sistema, se ocupa de seleccionar, instalar y mantener el sistema operativo adecuado, del diseño y control de la estructura de la base de datos, el estudio y evaluación de las necesidades y rendimientos del sistema y, por último, la ayuda directa a usuarios.

- **Administración del propio Centro de Procesamiento de Datos**. Las funciones de administración de un Centro de Procesamiento de Datos engloban operaciones de supervisión, planificación y control de proyectos, seguridad y control de proyectos, seguridad general de las instalaciones y equipos, administración financiera y administración de los propios recursos humanos.

En lo que respecta al Laboratorio de Redes y Seguridad, el área más importante con que cuenta debido a que es un laboratorio muy pequeño es el área de soporte técnico, es por ello que se explicará a continuación.

II.3.1 Área de Soporte Técnico

Es el área responsable de la administración del hardware y del software dentro de las instalaciones del Centro de Cómputo, entendiendo por administración: estrategia, planificación, instalación y mantenimiento.

Algunas funciones principales generales que realiza esta área son:

- Planificar la modificación e instalación de software y hardware

- Evaluar los nuevos paquetes de software y nuevos productos de hardware

- Dar el soporte técnico necesario para el desarrollo de nuevos proyectos, evaluando el impacto de éstos en el sistema instalado

- Asegurar la disponibilidad del sistema y la coordinación necesaria para la resolución de los problemas técnicos

- Proponer las notas técnicas y recomendaciones para el uso óptimo de los sistemas instalados

- Participar en el diseño de la Arquitectura de Sistemas

Para su correcto funcionamiento, el centro de cómputo debe contar con dos puestos que son de suma importancia, el jefe del centro de cómputo y el administrador de la red, los cuales se explicarán a continuación:

Jefe del centro de cómputo

Es el responsable de mantener en forma permanente la disponibilidad del hardware y software en condiciones para permitir la operatividad de las unidades usuarias que reciben el servicio. Sus funciones principales son:

- Estructura los planes de servicio requeridos por las unidades usuarias
- Establece los planes de instalación, puesta en marcha y mantenimiento del hardware y software requerido por los sistemas
- Verifica que los métodos de trabajo establecidos sean respetados y puestos en práctica
- Lleva el control para los servicios de mantenimiento de hardware, software e instalaciones diversas
- Lleva un registro de fallas de hardware, software y toma las acciones para su corrección
- Coordina juntas para evaluar si los niveles de servicio cubren las necesidades de información de las distintas unidades usuarias
- Recibe solicitudes de operación de nuevos sistemas, variantes en los calendarios de servicio, instalación de hardware y software adicionales y se asegura de que tales solicitudes sean satisfechas según los calendarios establecidos
- Elabora informes de compromisos adquiridos, avances, logros, requerimientos y cualquier dato de importancia
- Realiza estudios de factibilidad para la selección de equipo y servicio de cómputo, a fin de mantenerlos actualizados

Administrador de la red

Es el encargado de crear espacios de comunicación, atender sugerencias, mantener las herramientas y el espacio requerido por cada usuario a tiempo y de buena forma, mantener en buen estado la(s) red(es) a su cargo, mantener documentación que describa la red, el hardware y el software que administra, respetar la privacidad de los usuarios y promover el buen uso de los recursos.

Algunas de las funciones que realiza son:

- Configurar los programas que se inician junto con el sistema
- Administrar cuentas de usuarios
- Administrar los programas y la documentación instalada
- Configurar los programas y los dispositivos
- Administrar espacio en discos y mantener copias de respaldo
- Configurar servicios que funcionarán en red
- Solucionar problemas con dispositivos o programas
- Revisar bitácoras, solucionar y prevenir inconvenientes de seguridad

II.4 IMPORTANCIA DE UNA RED EN UN CENTRO DE CÓMPUTO

La optimización en el uso de los sistemas informáticos es uno de los elementos de interacción y desarrollo que rige los destinos de la ciencia informática en la actualidad. Es por ello que la aparición de las plataformas de interconexión de equipos de computación o redes informáticas, resultan ser uno de los elementos tecnológicos más importantes al momento de definir un sistema informático en una organización determinada.

Cuando el entorno de trabajo es sencillo (una máquina, una impresora y un escáner, por ejemplo), basta con conectar estos componentes. Pero cuando hay muchos usuarios, cada uno con su computadora, que quieren usar el mismo dispositivo a la vez, la cosa se complica.

Se hace necesario conectar todo en red de manera que los usuarios tengan acceso a los dispositivos de hardware, a la Web, a la información y a ciertos datos de la institución.

Algunas de las ventajas de conectarse en una red son:

- ✓ Compartir recursos, especialmente información
- ✓ Proveer la confiabilidad
- ✓ Permitir la disponibilidad de programas y equipos para cualquier usuario de la red que así lo solicite, sin importar la localización física del recurso y del usuario
- ✓ Permitir al usuario acceder a una misma información sin problemas llevándola de un equipo a otro

II.5 IMPORTANCIA DEL LABORATORIO DE REDES Y SEGURIDAD

Para la carrera de **Ingeniero en Computación** es de suma importancia contar con los conocimientos necesarios en materia de redes y seguridad informática, para ello en la propuesta del nuevo plan de estudios se incluyen dos materias de carácter obligatorio:

- ➢ Redes de Datos
- ➢ Administración de Redes

Además del módulo terminal **"Redes y Seguridad"** el cual constará de cuatro materias obligatorias:

- ➢ Seguridad Informática I
- ➢ Seguridad Informática II
- ➢ Criptografía
- ➢ Arquitecturas Cliente-Servidor

De manera que será necesario que se cuente con un laboratorio y que éste cuente con la administración necesaria, ya que en él se realizarán las prácticas correspondientes a dichas materias, en las cuales los alumnos harán cambios en la configuración de los equipos, que podrían poner en riesgo la funcionalidad de la red o de algún dispositivo.

Es por ello que se hace necesaria una buena organización contando con un sistema de administración de red para prevenir o corregir fallas y cambios que se presenten en los equipos.

Para ello se evaluarán las características del laboratorio tomando en cuenta los usos para los que será destinado y de esta manera encontrar el sistema de administración que se adecue a dichas características.

II.6 REPRESENTACIÓN GRÁFICA DEL LABORATORIO

El Laboratorio de Redes y Seguridad forma parte del **Departamento de Ingeniería en Computación** y se encuentra ubicado en la planta baja del edificio **Luis G. Valdés Vallejo**.

Este laboratorio cuenta hasta el momento con 11 computadoras conectadas en red, incluyendo el servidor.

Cada computadora cuenta con los sistemas operativos Linux y Windows con el objeto de que los usuarios del laboratorio conozcan y realicen prácticas bajo estos dos sistemas operativos diferentes.

La figura II.1 muestra una representación de la distribución de las computadoras dentro del laboratorio.

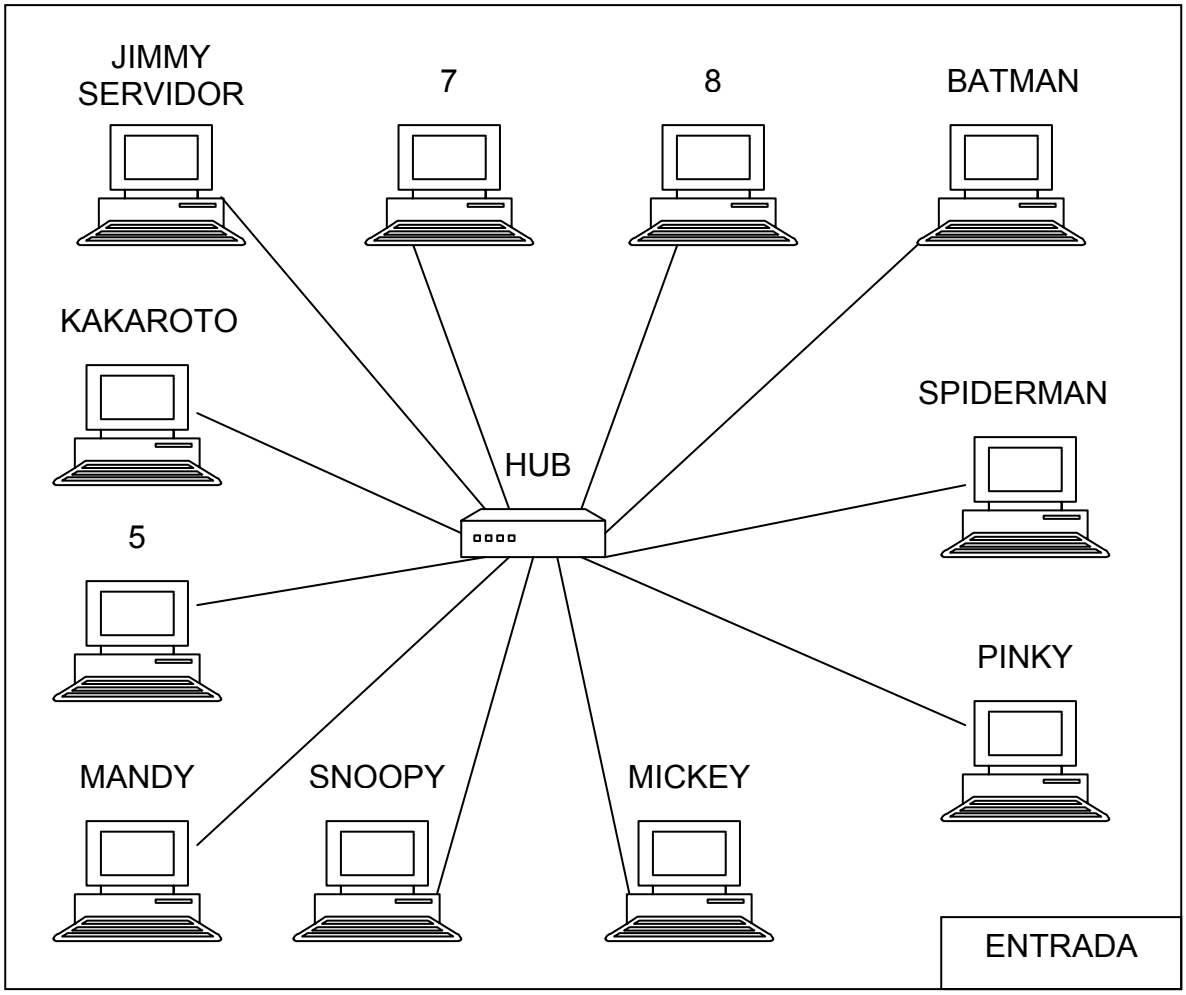


Figura II.1 Vista del laboratorio de redes y seguridad

II.7 TOPOLOGÍA DE LA RED DEL LABORATORIO

La topología o forma lógica de una red se define como la forma de conectar, a través de cables, estaciones de trabajo individuales, por muros, suelos y techos del edificio.

La topología en una red es la configuración adoptada por las estaciones de trabajo para conectarse entre si.

La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

Podemos distinguir **dos aspectos** diferentes a la hora de considerar una topología:

1. La **topología física:** Es la disposición real de las máquinas, dispositivos de red y cableado en la red.

2. La **topología lógica:** Es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

II.7.1 Principales Topologías de Red

Bus

Esta topología permite que todas las estaciones reciban la información que se transmite; una estación transmite y todas las restantes escuchan. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red. Todos los nodos de la red están unidos a este cable, el cual recibe el nombre de "**Cable Backbone**".

Los nodos en una **red de bus** transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información. La figura II.2 muestra un ejemplo de esta topología.

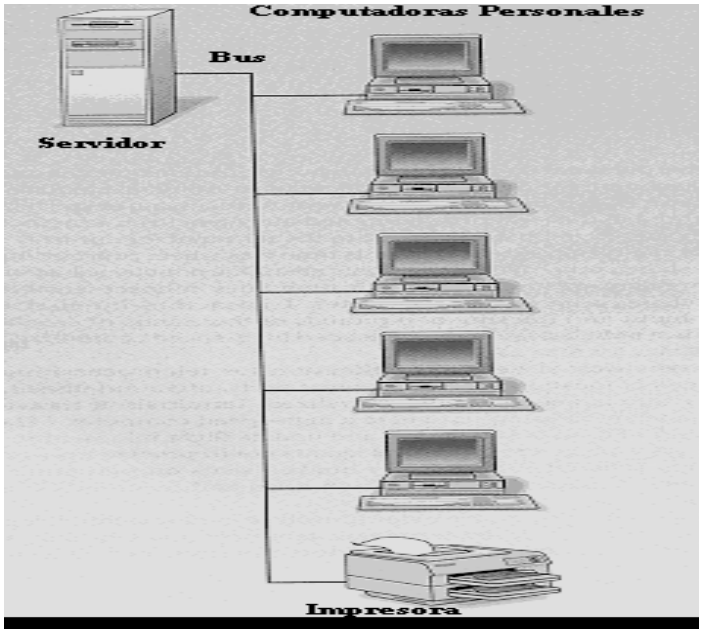


Figura II.2 Topología bus

Anillo

Las estaciones están unidas unas con otras formando un círculo por medio de un cable común. El último nodo de la cadena se conecta al primero cerrando el anillo (Figura II.3). Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo.

Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo.

La desventaja del anillo es que si se rompe una conexión, se cae la red completa.

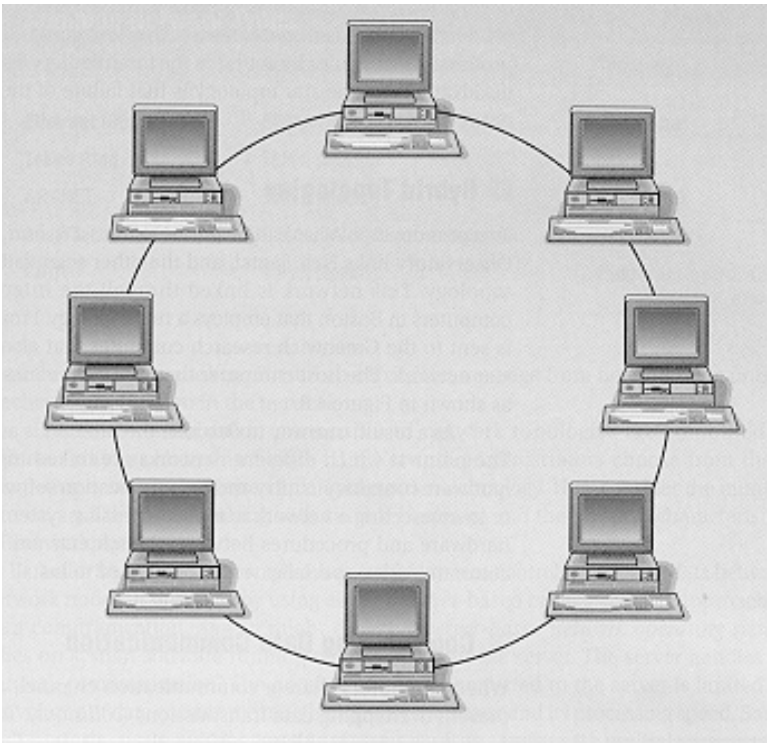


Figura II.3 Topología anillo

Estrella

En una topología de estrella (Figura II.4), las computadoras en la red se conectan a un dispositivo central conocido como **concentrador** (**hub**) o a un **conmutador de paquetes** (**swicth**). Cada computadora se conecta con su propio cable (típicamente **par trenzado**) a un puerto del concentrador o conmutador de paquetes.

Las computadoras escuchan el cable y contienden por un tiempo de transmisión.

Debido a que la topología estrella utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el concentrador o conmutador de paquetes (aunque se pueden conectar concentradores o conmutadores de paquetes en cadena para así incrementar el número de puertos).

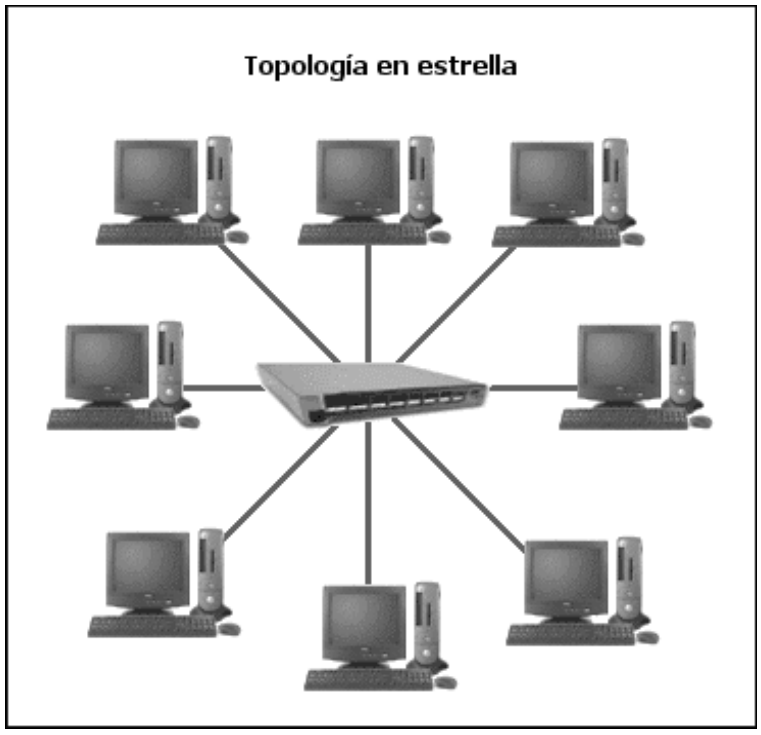


Figura II.4 Topología en estrella

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja de esta topología es la centralización de la comunicación, ya que si el concentrador falla, toda la red se cae.

Híbridas

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

Anillo en Estrella: Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

Bus en Estrella: El fin es igual a la topología anterior. En este caso la red es un bus que se cablea físicamente como una estrella por medio de concentradores.

Estrella Jerárquica: Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica. Un ejemplo de esta red se muestra en la figura II.5.

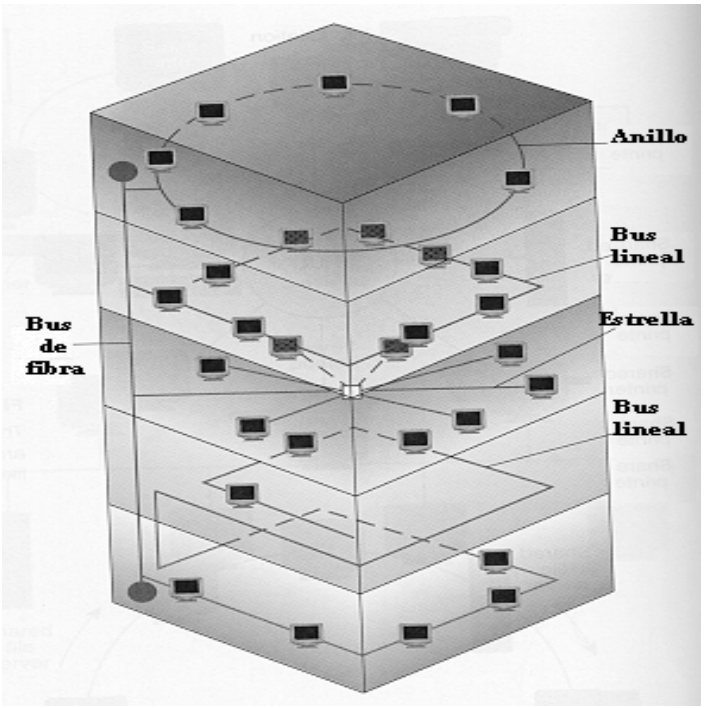


Figura II.5 Topologías híbridas

Árbol

Es una generalización de la **topología en bus**. Esta topología (Figura II.6) comienza en un punto denominado cabezal o raíz (headend). Uno ó más cables pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse.

Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras.

Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.

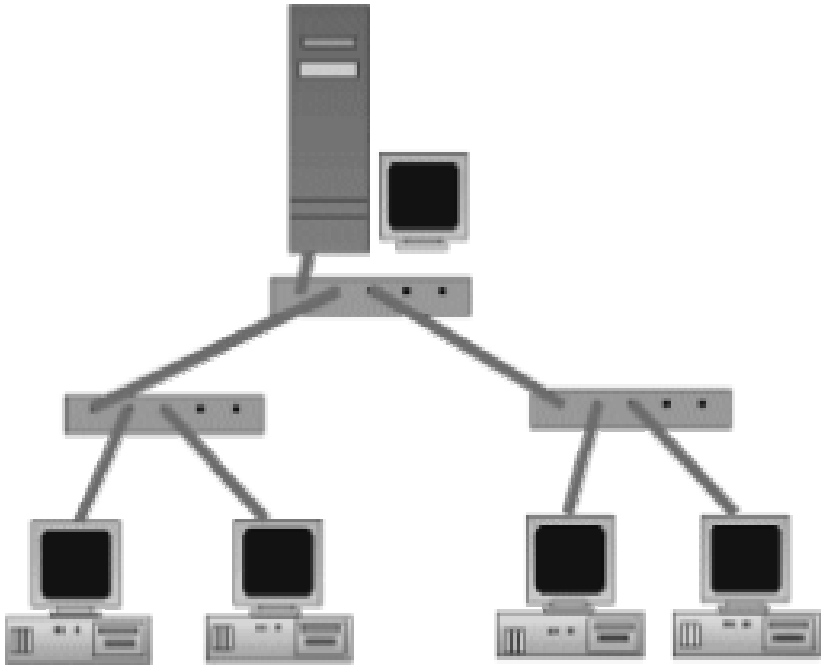


Figura II.6 Topología de árbol

La topología de la red que se usa en el laboratorio es una estrella física y su protocolo de comunicación es Ethernet.

II.8 CARACTERÍSTICAS DE LAS COMPUTADORAS DEL LABORATORIO

Computadora 1: JIMMY (SERVIDOR)

- Marca ensamblada
- Procesador AMD K6 a 400 MHz
- Disco duro de 6.2 GHz
- Sistema Operativo Red Hat 9.0
- Memoria RAM de 64 MB
- Servicios: Gateway, Firewall y servicio de Web Apache

Computadora 2: MICKEY

- Marca DELL
- Modelo OPTIPLEX GX260
- Procesador Pentium IV a 2.0 GHz
- Disco duro de 40 GB
- Sistema Operativo Windows XP Professional Service Pack 2
- Memoria RAM de 256 MB

Computadora 3: SNOOPY

- Marca DELL
- Modelo OPTIPLEX GX260
- Procesador Pentium IV a 2.8 GHz
- Disco duro de 20 GB
- Sistema Operativo Windows XP Professional Service Pack 2
- Memoria RAM de 256 MB

Computadora 4: MANDY

- Marca COMPAQ
- Modelo Presario SR 1220LA
- Procesador Pentium IV a 2.8 GHz
- Disco duro de 80 GHz
- Sistema Operativo Windows XP Home Edition Service Pack 1
- Memoria RAM de 256 MB

Computadora 5

- Marca COMPAQ
- Modelo Presario SR 1220LA
- Procesador Pentium IV a 2.8 GHz
- Disco duro de 80 GHz
- Sistema Operativo Windows XP Home Edition Service Pack 1
- Memoria RAM de 256 MB

Computadora 6: KAKAROTO

- Marca DELL
- Modelo OPTIPLEX 170L
- Procesador Pentium IV a 3.2 GB
- Disco duro de 60 GHz
- Sistema Operativo Windows XP Home Edition Service Pack 2
- Memoria RAM de 512 MB

Computadora 7

- Marca DELL
- Modelo OPTIPLEX 170L
- Procesador Pentium IV a 3.2 GB
- Disco duro de 60 GHz
- Sistema Operativo Windows XP Home Edition Service Pack 2
- Memoria RAM de 512 MB

Computadora 8

- Marca DELL
- Modelo OPTIPLEX 170L
- Procesador Pentium IV a 3.2 GB
- Disco duro de 60 GHz
- Sistema Operativo Windows XP Home Edition Service Pack 2
- Memoria RAM de 512 MB

Computadora 9: BATMAN

- Marca DELL
- Modelo OPTIPLEX 170L
- Procesador Pentium IV a 3.2 GB
- Disco duro de 60 GHz
- Sistema Operativo Windows XP Home Edition Service Pack 2
- Memoria RAM de 512 MB

Computadora 10: SPIDERMAN

- Marca DELL
- Modelo OPTIPLEX GX260
- Procesador Pentium IV a 2.8 GB
- Disco duro de 20 GHz
- Sistema Operativo Windows XP Professional Service Pack 1
- Memoria RAM de 256 MB

Computadora 11: PINKY

- Marca HP
- Modelo HP 5500
- Procesador Pentium IV a 2.4 GHz
- Disco duro de 30 GB
- Sistema Operativo Windows XP Profesional Service Pack 2
- Memoria RAM de 128 MB

II.9 USOS DEL LABORATORIO

Como se mencionó con anterioridad, para las asignaturas de redes de computadoras del nuevo plan de estudios: redes de datos y administración de redes, se requerirá trabajar con prácticas relacionadas con los temas vistos en cada una de dichas materias, para lo cual será necesario utilizar los equipos con que cuenta el laboratorio.

Además, con la creación del módulo terminal "redes y seguridad" que abarcará las materias: Seguridad en cómputo I, Seguridad en cómputo II, Criptografía y Arquitecturas Cliente-Servidor se hará necesaria también la utilización de este laboratorio para de igual manera realizar prácticas relacionadas con la teoría vista en cada una de las materias antes mencionadas.

En el caso de las materias relacionadas con Redes de Computadoras las prácticas que se tienen previstas son:

- Las capas del modelo OSI
- Una introducción al manejo básico del Sistema Operativo Linux
- Aprender a instalar una red LAN
- Armado de cables para conectar una red
- Instalación y configuración de las tarjetas de red

De igual manera en el caso de las asignaturas del módulo terminal "Redes y Seguridad", se contará en un futuro próximo con algunas prácticas de seguridad que ayuden a reforzar los conocimientos vistos en la parte teórica.

CAPÍTULO III

SISTEMA DE ADMINISTRACIÓN PARA EL LABORATORIO DE REDES Y SEGURIDAD

"Aún cuando el esfuerzo de hacer algo bueno falle, es laudable la voluntad".

III.1 VENTAJAS DE INSTALAR SNMP EN EL LABORATORIO DE REDES Y SEGURIDAD

La ventaja fundamental de usar **SNMP** es que su diseño es simple, por lo que su implementación es sencilla en grandes redes y la información de administración que se necesita intercambiar ocupa pocos recursos de la red.

Otra ventaja de SNMP es que en la actualidad es el sistema de administración de redes más extendido. La popularidad la ha conseguido al ser el único protocolo que existió en un principio y por ello casi todos los fabricantes de dispositivos diseñan sus productos para soportar SNMP.

La posibilidad de expansión es otra ventaja del protocolo SNMP, ya que debido a su sencillez es fácil de actualizar.

Debido a las ventajas mencionadas anteriormente y a que SNMP es un estándar de uso libre que cuenta con características que permiten su aplicación en plataformas LINUX y WINDOWS y dado que el laboratorio cuenta con ambas plataformas para las redes que maneja, recomendamos su aplicación como sistema de administración en dicho laboratorio.

III.2 ¿QUÉ ES SNMP?

Es un protocolo llamado **S**imple **N**etwork **M**anagement **P**rotocol (Protocolo de Administración de Red Simple). Diseñado en los años 80, su principal objetivo fue el integrar la administración de diferentes tipos de redes mediante un diseño sencillo y que produjera poca sobrecarga en la red.

SNMP trabaja sobre el conjunto de protocolos TCP/IP en la capa de aplicación y usa **UDP/IP** para comunicarse con la red interna y así consultar los diferentes elementos que forman dicha red, ignorando los aspectos específicos del hardware sobre el que funcionan dichos elementos.

Este protocolo se define en el RFC 1448. La forma normal de su uso es que la estación administradora envía una solicitud a un agente pidiéndole información o mandándole actualizar su estado.

Idealmente, la respuesta del agente simplemente es la información solicitada o la confirmación de que ha actualizado su estado según se solicitó. Los datos se envían empleando la sintaxis de transferencia del ASN.1. Sin embargo, también pueden informarse varios errores.

Este protocolo define cinco mensajes que pueden enviarse. Los cinco mensajes se listan y se describen en la tabla III.1

Mensaje	Descripción
Get-request	Solicita el valor de una o más variables.
Get-next-request	Solicita la variable que sigue a ésta.
Set-request	Actualiza una o más variables.
Get-response	Devuelve la respuesta a la solicitud pedida.
Trap	Informa de interrupciones de agente a administrador.

Tabla III.1 Tipos de mensajes SNMP

III.3 HISTORIA DE SNMP

El desarrollo de SNMP sigue un patrón histórico similar al desarrollo total del conjunto de protocolos TCP/IP.

A finales de 1970, no había ningún protocolo de administración como tal. Una herramienta que fue eficientemente usada para la administración fue el Protocolo de Mensaje de Control de Internet (ICMP).

ICMP proporciona el medio para transferir mensajes de control de encaminadores y otros anfitriones a un anfitrión y proporciona la regeneración sobre problemas en el ambiente. ICMP está disponible en todos los dispositivos que soportan IP.

Fue sólo a finales de 1980, cuando el crecimiento de la Internet se hizo exponencial, por lo que la atención fue enfocada en el desarrollo de una capacidad de administración de red más poderosa.

Lo que se requería era un protocolo estandarizado que pudiera ser fácilmente aprendido y usado por una amplia variedad de personas con responsabilidades de administración de red.

Para cumplir con este requisito, se realizaron varios esfuerzos para desarrollar un protocolo de administración de red, surgiendo las tres propuestas siguientes:

1. **Sistema de Administración de Entidad de Alto Nivel (HEMS)**: Este era una generalización de quizás el primer protocolo de administración de red usado en la Internet, el protocolo de supervisión-anfitrión (HMP).

2. **Protocolo Simple de Administración de Red (SNMP)**: Este era una versión perfeccionada del protocolo simple de supervisión-arranque (SGMP).

3. **CMIP sobre TCP/IP (CMOT)**: Este era una tentativa para incorporar al protocolo de información de administración común, sus servicios y su estructura de base de datos estandarizada por la ISO para la administración de red.

El protocolo simple de administración de red no cobró vida hasta 1988.

El precursor de SNMP, **SGMP** fue desarrollado por Davin Case, Fedor y Schoffstall quienes propusieron sus especificaciones en el RFC 1028. Aunque fue creado para monitorear encaminadores, éste fue usado también para supervisar otros sistemas.

A principios de 1988, la **I**nternet **A**ctivities **B**oard (**IAB**) repasó estas propuestas y aprobó el remoto desarrollo de SNMP como una solución a corto plazo y CMOT como la solución a largo plazo.

HEMS tenía más capacidad que SNMP, pero un esfuerzo extra sobre un callejón sin salida pareció injustificado. Mientras tanto, si CMIP podría ser implementado para correr sobre TCP, entonces podría ser posible desplegar **CMOT**.

Para solidificar esta estrategia, el IAB dictó que tanto SNMP como CMOT usaran la misma base de datos de objetos administrados. Así, sólo una estructura simple de información de administración y una base de información de administración simple serían definidas para ambos protocolos.

Pronto se hizo evidente que esta obligación de los dos protocolos en el nivel de objeto era poco práctica. En la administración de red de **OSI**, los objetos administrados son vistos como entidades sofisticadas con atributos, procedimientos asociados, capacidades de notificación y otras características complejas asociadas con la tecnología orientada a objetos.

Para mantener simple a SNMP, no había que trabajar con tales conceptos sofisticados. De hecho, los objetos en SNMP no son realmente objetos en absoluto desde punto de vista de tecnología orientada a objetos; más bien son simplemente variables con unas características básicas, como el tipo de datos y si la variable es sólo para leer o leer-escribir.

De acuerdo con el IAB se relajó su condición a **SMI/MIB** común y permitió el desarrollo de SNMP y CMOT para continuar por separado y en paralelo.

SNMP pronto se extendió y prosperó dentro de la Internet. Además, SNMP pronto se hizo el protocolo de administración estandarizado para el usuario general. Tal como TCP/IP ha durado más que todas las predicciones de su tiempo de vida útil, también SNMP parece seguir sus mismos pasos debido a que el despliegue extendido de administración de red de OSI sigue siendo tardado. Y mientras tanto, el esfuerzo CMOT languidece.

III.3.1 Normas Relacionadas con SNMP

Las especificaciones de SNMP en sus varias etapas han sido publicadas como RFCs. Además de datos específicos formales como SNMP y los protocolos del conjunto de TCP/IP, existen muchos documentos interesantes que contienen información técnica.

El proceso para proponer una especificación para la adopción de una norma es descrito en el RFC 1310, el **Proceso de Normas de Internet**. Esta evolución es representada en la Figura III.1.

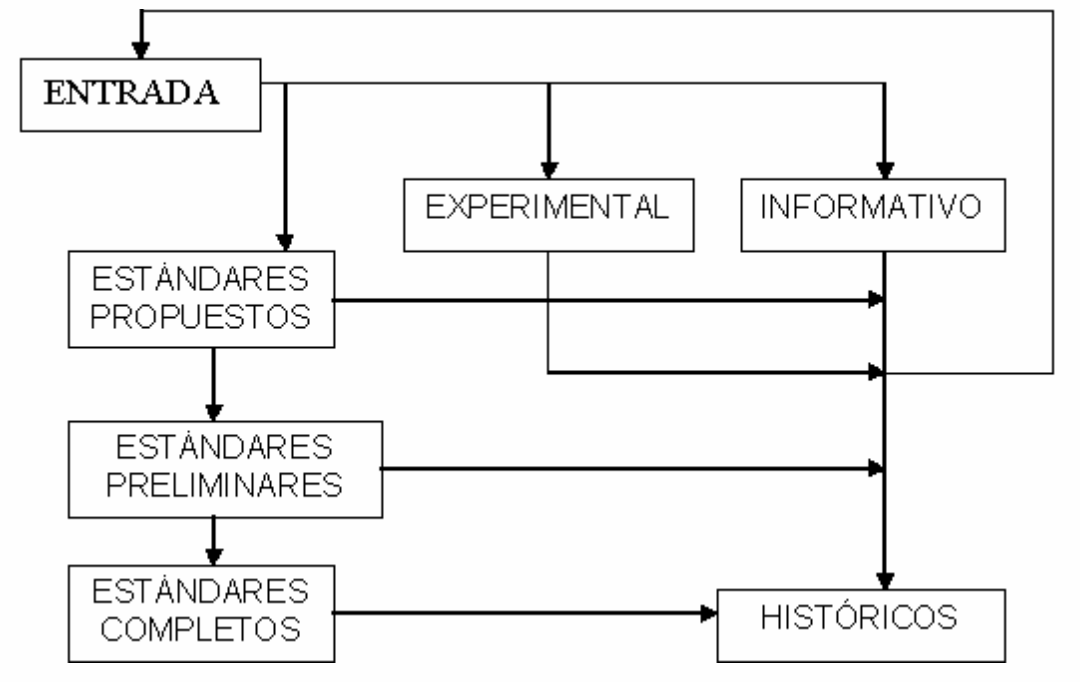


Figura III.1 Evolución de especificaciones de normas

Una especificación de las normas entra y es rastreada para poder asumir el estado de **propuesto**, **experimental**, o **informativo**. Los datos específicos experimentales e informativos no son requeridos o no llenan las exigencias para hacerse normas completas.

Un estándar propuesto debe ser estable, encontrar una recepción buena y ser considerado de valor. Después de al menos seis meses y dos o más implementaciones, el estándar propuesto puede ser considerado para el estado **preliminar**.

Después de cuatro meses, este puede hacerse un estándar **completo**. Dentro de un tiempo, la especificación puede ser sustituida por una versión más reciente; en cuyo caso, la antigua especificación recibe un estado **histórico**.

Las **tres normas** principales que comprenden a **SNMP** (**SMI**, **MIB** y el **protocolo**) son todas Normas Completas.

La tabla III.2 muestra una vista del estado de varios RFCs de SNMP y sus normas relacionadas:

Estándares Completos
RFC 1155: Estructura de Administración de Información
RFC 1157: Protocolo Simple de Administración de Red
RFC 1212: Definiciones de MIB concisas
RFC 1213: Base de Información de Administración (MIB-II)
Estándares Preliminares
RFC 1398: Ether-like Interfaz tipo MIB
Estándares Propuestos
RFC 1229: Extensiones para la Interfaz Genérica MIB
RFC 1230: IEEE.802.4 Token Bus Interfaz tipo MIB
RFC 1231: IEEE 802.5 Token Ring Interfaz tipo MIB
RFC 1269: MIB Versión 3
RFC 1351: Modelo Administrativo SNMP
RFC 1352: Protocolos de Seguridad SNMP
RFC 1353: Grupo MIB SNMP
Experimentales
RFC 1187: Recuperación de Tablas de Tamaño con SNMP
RFC 1224: Técnicas para la Administración de Alertas generadas asíncronamente.
Informativas
RFC 1147: Catálogo de Herramientas de Administración de Red
RFC 1215: Convención para definir trampas para uso con SNMP
RFC 1270: Servicios de comunicación SNMP
RFC 1303: Convención para describir agentes basados en SNMP
RFC 1321: Algoritmo de compendio de mensajes MD5
Históricas
RFC 1156: Base de Información de Administración (MIB-I)
RFC 1161: SNMP sobre OSI

Tabla III.2 Compendio de normas SNMP

III.4 COMPONENTES DE SNMP

Podemos decir que SNMP cuenta con 6 componentes principales:

- Estación Administradora
- Sistema de Administración de Redes (SAR)
- Elementos administrados
- Un agente SNMP
- El protocolo SNMP
- Base de Información de la Administración (MIB)

La **estación administradora** es típicamente un dispositivo independiente. En cualquier caso, la estación administradora sirve como la interfaz para el administrador humano con el sistema de administración de red.

El **SAR** es el software que ejecuta aplicaciones de administración y monitoreo sobre los elementos administrados. Se encuentra instalado en la estación administradora.

Los **elementos administrados** son cualquier nodo de la red que contiene un agente SNMP, son elementos como: servidores, ruteadores, impresoras, etc., los cuales recopilan información administrable para el SAR, que es accedida por medio del protocolo SNMP.

El **agente SNMP** es un software que reside en el elemento administrado, el cual toma la información de administración recopilada por este elemento y la traduce para que sea compatible con el SAR. El agente de administración responde a la petición de información y la petición de acciones desde la estación administradora y asincrónicamente puede proporcionar a la estación administradora información importante pero no solicitada.

SNMP es el protocolo por medio del cual el elemento administrado se comunica con la estación administradora para proporcionar la información de administración al SAR.

Y por último, la **MIB** que es una **base de datos** (organizada por objetos (o variables) y sus atributos (o valores)) que contiene información del estado y es actualizada por los agentes.

La figura III.2 muestra los componentes antes mencionados.

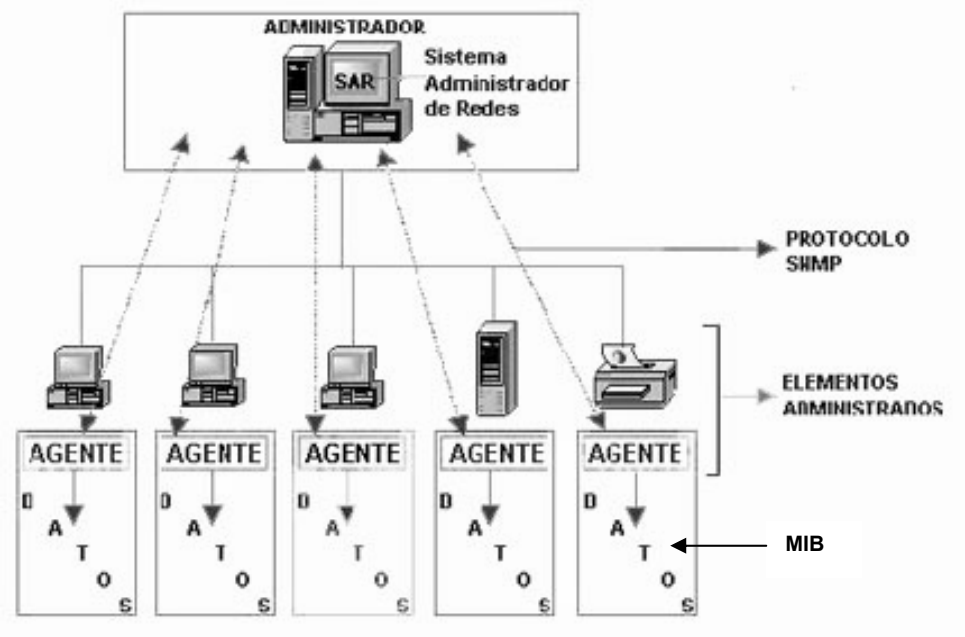


Figura III.2 Componentes de SNMP

III.5 SNMP: FUNCIONAMIENTO

SNMP cuenta con una arquitectura cliente-servidor, en la cual el agente desempeña el papel de servidor y el administrador hace el de cliente.

La forma normal de uso de SNMP es:

- **Pregunta:** La estación administradora envía una solicitud a un agente pidiéndole información o mandándole actualizar su estado. Este método se conoce como sondeo.

- **Respuesta:** La información recibida del agente es la respuesta o la confirmación a la acción solicitada.

- **Interrupción:** Es mejor que un agente pueda mandar la información al nodo administrador puntualmente, ante una situación predeterminada, por ejemplo una anomalía detectada en la red. Este método es conocido como interrupción.

La posibilidad de ampliación del protocolo está directamente relacionada con la capacidad del MIB de almacenar nuevos elementos.

III.5.1 Cómo Trabaja el Protocolo

A continuación veremos detalladamente cómo el SAR y el agente operan respecto a cómo el protocolo es utilizado.

Desde el punto de vista del **SAR**, un comando inicia la construcción de un requerimiento de SNMP. Esta operación puede ser un set, un get o un get next request. El SAR crea un mensaje SNMP rellenando los valores de cabecera apropiados para transmitir el mensaje sobre la red interna al agente de destino.

Este asigna el nombre de comunidad, el número de versión y el requerimiento ID. El tipo de **PDU** es escogido y los miembros de la Lista de Unión de Variables son insertados en el mensaje. El mensaje SNMP es entregado a la capa de transporte de UDP para la transmisión. El mensaje es enviado.

El SAR debe recordar el **requerimiento ID** que este ha insertado en el requerimiento para permitir una respuesta que podría recibir más tarde. Los temporizadores también son iniciados para manejar condiciones de interrupción. En cualquier momento, el SAR debe estar preparado para recibir y procesar Traps enviados por agentes en su comunidad.

Después de iniciar, los agentes esperan recibir los **mensajes SNMP** en su destino por medio de un dispositivo de red por el puerto 161 de transporte UDP. Cuando el agente recibe un mensaje satisfactoriamente, éste llama a la rutina para descifrar el formato de ASN.1 en un formato interno más utilizable.

Si el mensaje está en un formato impropio de ASN.1, es desechado y el agente simplemente regresa a esperar el ciclo. El siguiente paso es verificar el número de versión. Si es incorrecto, este mensaje también es desechado y el agente regresa a esperar el siguiente mensaje.

Cuando el mensaje ha pasado satisfactoriamente estas dos primeras comprobaciones, el agente llama a la función de autenticación para verificar el mensaje. Si este falla, el agente tiene la capacidad de enviar el mensaje de **Trap** de authenticationFailure, el Trap es enviado y el mensaje es desechado.

Si el mensaje es auténtico, la información de transporte es salvada para el mensaje de respuesta y el agente está ahora listo para descifrar el mensaje SNMP correcto.

El agente sigue descifrando el formato de **ASN.1** del mensaje y comienza a construir un GetResponse-PDU. En este punto, cualquier condición de error no daña el mensaje entrante, más bien el GetResponse-PDU es usado para indicar la causa de la falla. La información de error apropiada es insertada en los campos de ErrorIndex y ErrorStatus.

Cuando el agente completa el GetResponse-PDU, este codifica el mensaje en ASN.1, lo presenta al servicio de transporte de **UDP** para la transmisión al requerimiento del SAR y vuelve a esperar el ciclo.

Todas las variables apropiadas que el agente usa para registrar su operación, tales como objetos acerca de SNMP mismo, han sido propiamente incrementadas para la inspección posterior por el SAR.

III.6 MENSAJES SNMP

Como se mencionó anteriormente el administrador de red de la estación y los agentes instalados en los elementos administrados se comunican enviando mensajes SNMP.

Un mensaje SNMP debe estar totalmente contenido en un **datagrama IP**.

El protocolo especifica el comando y los mensajes de respuesta que pueden ser usados para varios diálogos entre un SAR y sus agentes. Cada comando y respuesta son un mensaje SNMP independiente. La figura III.3 muestra el mensaje.

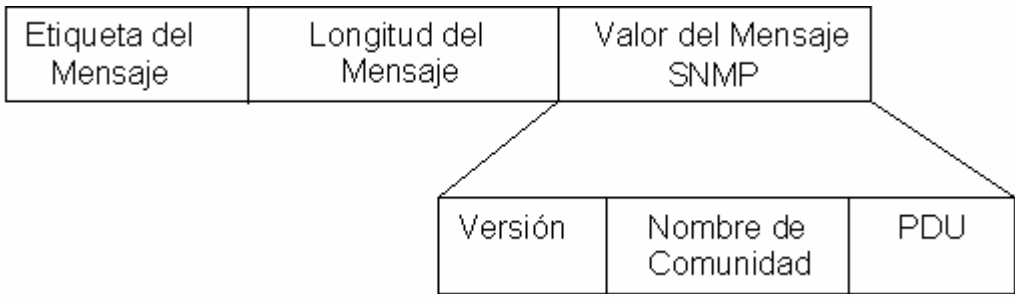


Figura III.3 El mensaje SNMP

Sus campos principales incluyen:

- El Campo de Versión
- El Campo de Nombre de Comunidad SNMP
- La Unidad de Datos de Protocolo (PDU)

El **Campo de Versión** es usado para la compatibilidad SNMP. El número de versión para el estándar actual definido por el RFC 1157 es la versión 1. Si el campo de versión de un mensaje recibido es incorrecto, el mensaje es desechado.

El **Campo de Nombre de Comunidad** es una cadena de octectos que contiene el nombre de la comunidad usado en el proceso de autenticación. Un agente puede contener una lista de cadenas de comunidad válida y comprobar la cadena de comunidad del mensaje SNMP recibido contra su lista. Si hay una pareja, el mensaje es procesado. Si no hay ninguna pareja, el mensaje es desechado.

SNMP especifica que la **Unidad de Datos del Protocolo** debe ser uno de los cinco tipos de mensajes soportados:

- GetRequest-PDU
- GetNextRequest-PDU
- GetResponse-PDU
- SetRequest-PDU
- Trap-PDU

La figura III.4 muestra la secuencia de los mensajes PDU que soporta SNMP.

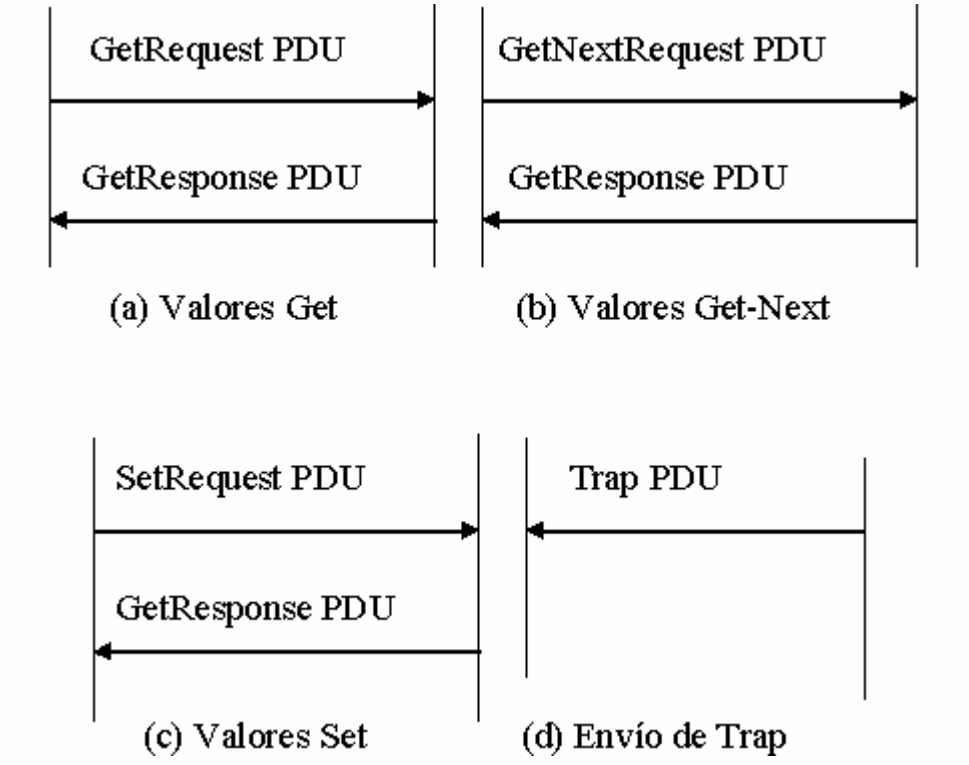


Figura III.4 Secuencias PDU en SNMP

III.6.1 GetRequest PDU

El GetRequest PDU es emitido por una entidad SNMP en una aplicación de una estación administradora de red. La entidad de enviar incluye los campos siguientes en el PDU:

- **Tipo PDU:** Indicación de que esto es un GetRequest PDU
- **Petición-id:** La petición-id permite a la aplicación SNMP relacionar respuestas entrantes con peticiones pendientes
- **Uniones de Variables:** Una lista de los casos de objeto cuyos valores son pedidos

La recepción de una entidad SNMP responde a un GetRequest PDU con un GetResponse PDU conteniendo la misma petición-id (Figura III.4, parte [a]). Si la entidad que responde es capaz de proporcionar valores para todas las variables mencionadas en la lista de uniones de variables entrantes, entonces el GetResponse PDU incluye el campo de uniones de variables, con un valor suministrado para cada variable.

III.6.2 GetNextRequest PDU

El formato del GetNextRequest-PDU es exactamente el mismo que el GetRequest-PDU pero el número de comando, llamado la indicación de tipo de PDU, tiene el valor de 1.

La figura III.5 muestra el GetNextRequest-PDU a través de la red interna, siendo procesado por el agente y causando el GetResponse-PDU para ser enviado al SAR.

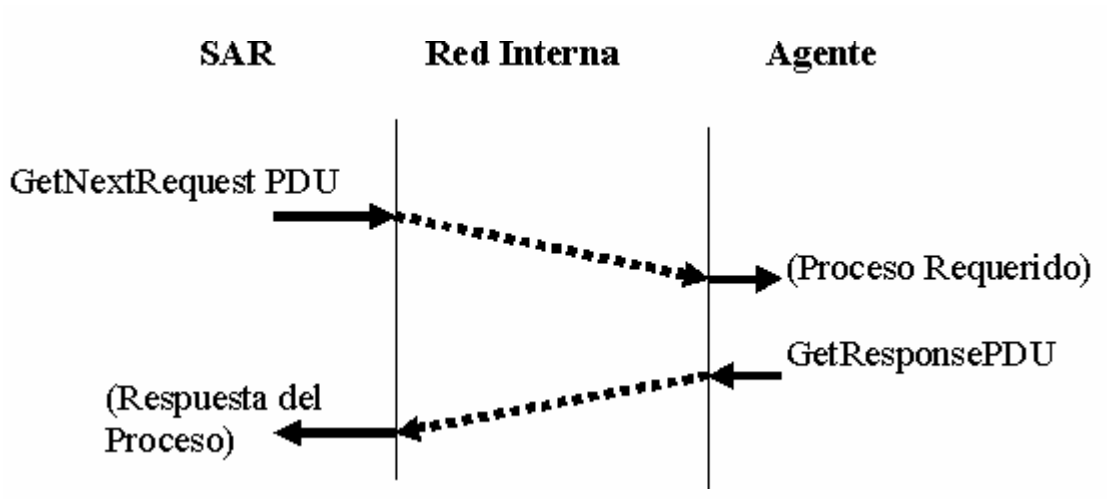


Figura III.5 Mensaje GetNextRequest

El comando GetNextRequest es similar a GetRequest pero el agente intenta recuperar el siguiente valor más grande lexicográficamente que el caso del objeto administrado solicitó.

El agente verifica que ahí existe el objeto lexicográficamente más grande que el siguiente objeto especificado en la lista de uniones de variables.

En cada caso el GetResponse-PDU debe ser enviado, el campo de requestID es puesto al valor encontrado de la marcha GetNextRequest-PDU recibido del SAR. El mensaje entonces es enviado de regreso al SAR que originó el comando.

III.6.3 SetRequest PDU

El SetRequest PDU es emitido por una entidad SNMP en una aplicación de estación administradora de red. Este tiene el mismo modelo de cambio de PDU (Figura III.4, parte [c]) y el mismo formato que el GetRequest PDU, pero el número de comando tiene el valor de 3. La diferencia es que el SetRequest es usado para escribir un valor de objeto contrario a leer uno.

La recepción de una entidad SNMP responde a un SetRequest PDU con un GetRequest PDU conteniendo la misma petición-id. Si la entidad que responde es capaz de poner valores para todas las variables mencionadas en la lista de uniones de variables entrantes, entonces el GetResponse PDU incluye el campo de uniones de variables, con un valor suministrado para cada variable.

III.6.4 GetResponse PDU

El formato del GetResponse-PDU es exactamente el mismo que el GetRequest-PDU pero el número del comando tiene el valor de 2.

El GetResponse-PDU es enviado por el agente siempre que éste haya procesado un GetRequest-PDU, un GetNextRequest-PDU o un SetRequest-PDU. El SAR recibe las necesidades del GetResponse para comprobar los valores de los campos en el mensaje y entonces procesa los datos pertinentes.

III.6.5 Trap PDU

Los **Traps** son notificaciones asíncronas que un agente puede enviar a la Estación Administradora de Red para informar al SAR de un acontecimiento extraordinario. Estos acontecimientos extraordinarios son predefinidos y deben ser conocidos dentro de la actividad tanto del agente como del SAR. La figura III.6 muestra al agente enviando el Trap-PDU a través de la red interna al SAR para procesarlo.

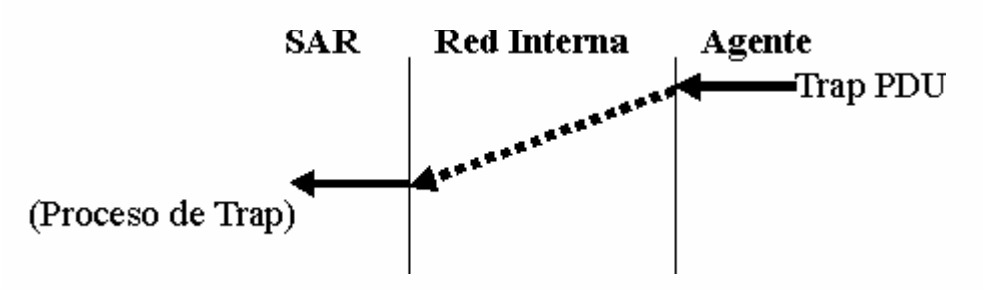


Figura III.6 Mensaje Trap

Hay caminos en una Estación de Administración de Red para mantener actualizados los eventos extraordinarios y significativos dentro de la red:

- **Reportes de Manejo de Interrupciones:** Es el envío de mensajes de alarma en tiempo real como ellos ocurren en la estación agente. La ventaja de esta aproximación es que la notificación es inmediata.

  Hay varias desventajas como, los recursos necesarios en el agente para la generación de estos mensajes Trap, las entradas estrictas que tienen que ser implementadas para prohibir el tráfico excesivo de red, la comprobación de entradas que puede impedir el funcionamiento del agente y el agente que es limitado con su propia vista del dispositivo.

- **Sondeo:** Es el esquema por el cual el SAR de vez en cuando preguntara a cada agente en su comunidad si tiene algunos eventos extraordinarios para informar. La ventaja de este acercamiento consiste en que el SAR conoce que pasa con la actividad de la red. La desventaja es que este sondeo requiere tiempo, recursos y usa el ancho de banda de la red.

Cuando un evento extraordinario ocurre en el agente, el nodo administrado por lo general envía un Trap solo y simple al SAR. El SAR inicia remotas interacciones con el agente sobre el nodo administrado para determinar la naturaleza y extensión del problema.

A diferencia del GetRequest, GetNextRequest y SetRequest PDUs, la Trap PDU no evoca una respuesta de otro lado (Figura III.4, parte [d]).

III. 7 ¿QUÉ ES MIB?

SNMP define un estándar separado para los datos administrados por el protocolo. Este estándar define los datos mantenidos por un dispositivo de red, así como las operaciones que están permitidas.

Los datos están estructurados en forma de árbol; en el que sólo hay un camino desde la raíz hasta cada variable. Esta estructura en árbol se llama **M**anagement **I**nformation **B**ase (**MIB**) y reside en cada elemento administrado.

La definición de un elemento concreto MIB implica la especificación del tipo de dato que puede contener. Normalmente, los elementos de un MIB son enteros, pero también pueden almacenar cadenas de caracteres o estructuras más complejas como tablas.

La base de datos contiene una serie de objetos (variables), que son datos reunidos sobre recursos en el elemento administrado. Los objetos son los nodos hoja del árbol MIB y pueden tener más de una instancia.

Características de los objetos (o variables)

- **Parámetros** que corresponden a un grupo del elemento administrado: *system, at, ip, tcp, udp, egp, etc*
- Poseen **atributos** (o valores) que representan el estado del objeto
- Los únicos **métodos** que operan sobre los atributos son escribir y leer
- Es un **subconjunto** de SMI

Dicha variable u objeto MIB se puede definir especificando la sintaxis, el acceso, el estado y la descripción de la misma.

- **Sintaxis:** Especifica el tipo de datos de la variable, entero, cadena, dirección IP, etc.
- **Acceso:** Especifica el nivel de permiso como: leer, leer y escribir, escribir
- **Estado:** Define si la variable es obligatoria u opcional
- **Descripción:** Describe textualmente a la variable

El estándar que define e identifica las variables MIB es llamado "**S**tructure of **M**anagement **I**nformation" (**SMI**). SMI especifica las variables MIB, éstas se declaran empleando un lenguaje formal ISO llamado ASN.1, que hace que tanto la forma como los contenidos de estas variables sean no ambiguos.

SMI presenta una estructura en forma de árbol global como se muestra en la figura III.7 para la información de administración, convenciones, sintaxis y las reglas para la construcción de MIBs.

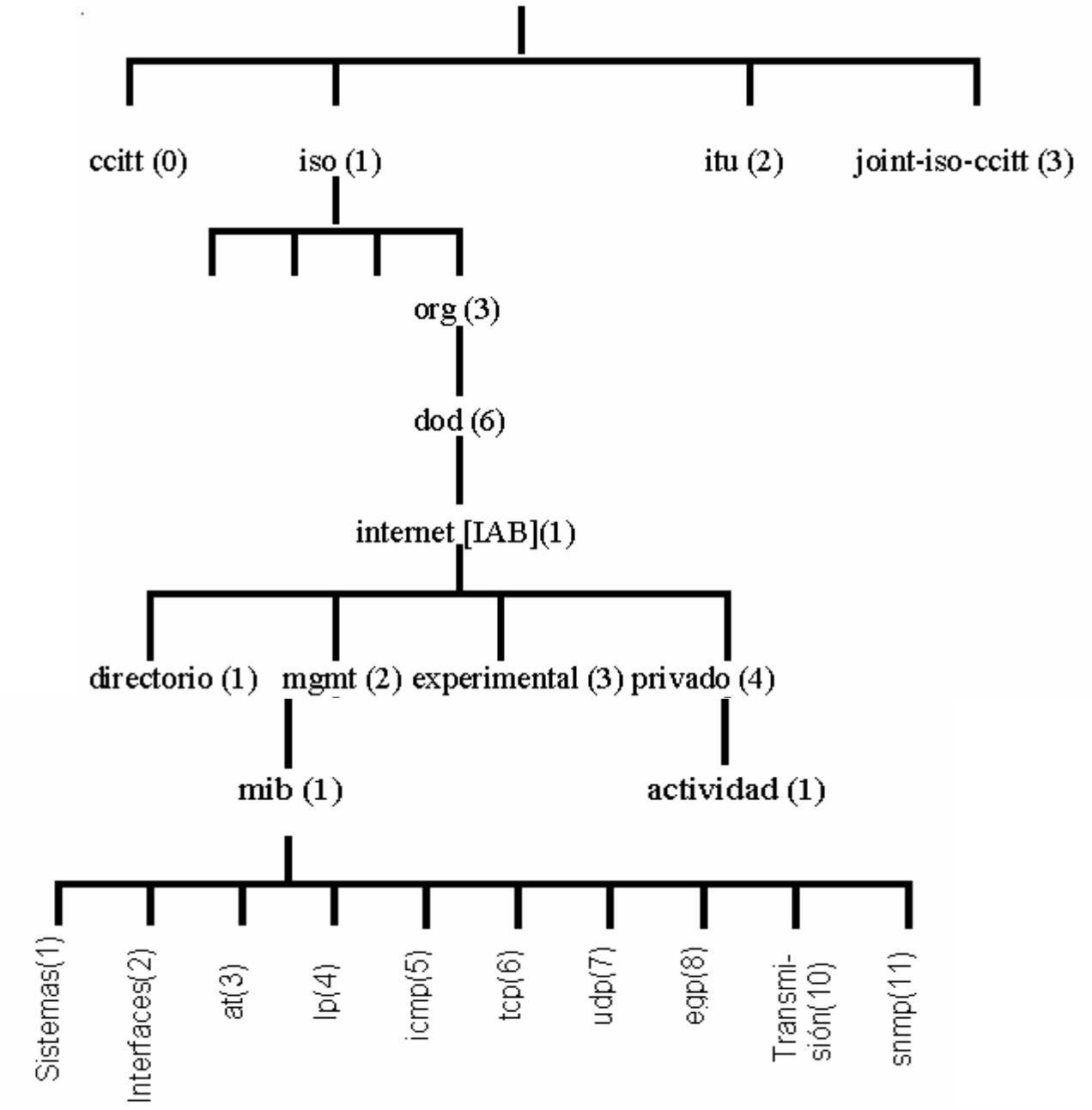


Figura III.7 Árbol organizacional TCP/IP

Comenzando con la raíz del árbol del objeto, cada valor del componente del objeto identifica un arco en el árbol. Comenzando de la raíz, hay cuatro nodos en el primer nivel; iso, ccitt, itu y joint-iso-ccitt. Bajo el nodo iso, un subárbol es para el uso de otras organizaciones y uno de estos es el Departamento de Defensa Estadounidense (dod). El RFC 1155 hace la suposición que un subárbol bajo dod será asignado para la administración por el Consejo de Actividades de Internet (IAB) como sigue:

IDENTIFICADOR DE OBJETO de Internet: = [iso org (3) dod (6) 1]

Esto es ilustrado en la figura III.10. Así, el nodo de Internet tiene el valor de identificador de objeto de 1.3.6.1. Este valor sirve como el prefijo para los nodos en el siguiente nivel más abajo del árbol.

Como es mostrado, el documento SMI define cuatro nodos bajo el nodo de Internet:

1. **directorio:** Este subárbol es reservado para el futuro uso con el directorio OSI (X.500).

2. **mgmt:** Este subárbol es usado para objetos definidos en documentos aprobados de IAB.

3. **experimental:** Este subárbol es usado para identificar objetos usados en experimentos de Internet.

4. **privado:** Este subárbol es usado para identificar objetos definidos unilateralmente.

El subárbol mgmt contiene las definiciones de las bases de información de administración que han sido aprobadas por el IAB. Actualmente, dos versiones del MIB han sido desarrolladas: mib-1 y mib-2. El segundo MIB es una extensión del primero. Ambos son proporcionados por el mismo identificador de objeto en el subárbol, donde sólo uno de los MIBs estaría presente en cualquier configuración.

El subárbol privado actualmente tiene sólo un nodo infantil definiendo el nodo de actividades. Esta parte del subárbol es usada para permitir a los vendedores mejorar la administración de su dispositivo y compartir esta información con otros usuarios y vendedores que podrían necesitar interoperar con sus sistemas. Una rama dentro del subárbol de actividades es asignada a cada vendedor que se registra.

La división del nodo de Internet en cuatro subárboles proporciona una fundación fuerte para la evolución de los MIBs. Como los vendedores y otros implementadores experimentan con nuevos objetos, ellos, en efecto, ganan muchos conocimientos prácticos antes de que estos objetos sean aceptados como la parte de la especificación estandarizada (mgmt).

Así, el MIB es útil inmediatamente para administrar objetos que caben dentro de la parte estandarizada del MIB y es bastante flexible para adaptarse a cambios de ofrecimientos de producto y tecnología.

La MIB-I define 126 objetos de administración, divididos en los siguientes grupos:

- Grupo de Sistemas
- Grupo de Interfaces
- Grupo de Traducción de Dirección (AT)
- Grupo IP
- Grupo TCP
- Grupo ICMP
- Grupo UDP
- Grupo EGP

La versión actual de TCP/IP MIB es la 2 (MIB-II) y se encuentra definida en el RFC 1213. En ella se divide la información que un dispositivo debe mantener en las ocho categorías de MIB-I y dos categorías más añadidas por MIB-II. Estas diez categorías son explicadas a continuación. Cualquier variable ha de estar en una de estas categorías.

El grupo Sistemas proporciona información general sobre el sistema administrado permitiendo al administrador encontrar el nombre del dispositivo, su constructor, el hardware y el software que contiene, su ubicación y lo que se supone que hace.

El grupo Interfaces registra la información genérica acerca de cada interfaz de red como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados, etc.

El grupo Traducción de Dirección (AT) proporciona información sobre la correspondencia de direcciones. Comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar.

El grupo IP contiene la información relevante a la implementación y la operación de IP en un nodo. Almacena información propia de la capa IP, como: datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc.

El grupo ICMP contiene la información relevante a la implementación y la operación de ICMP en un nodo. Este grupo consiste únicamente en los mostradores de varios tipos de mensajes ICMP enviados y recibidos. Trata los mensajes de error de IP.

El grupo TCP supervisa la cantidad actual y acumulada de conexiones abiertas, segmentos enviados y recibidos, así como varias estadísticas de error.

El grupo UDP lleva una bitácora de la cantidad de datagramas UDP enviados y recibidos.

El grupo EGP se usa para ruteadores que manejan el protocolo de pasarela exterior.

El grupo de Transmisión es requerido para contener los objetos que proporcionan detalles sobre el medio de comunicación subyacente para cada interfaz sobre un sistema. Soporta múltiples tipos de medios de comunicación, como: cable coaxial, cable UTP y cable de fibra óptica.

El grupo SNMP es requerido para recolectar estadísticas sobre la operación de él mismo.

Cabe señalar que un elemento de red, solo necesita soportar los grupos que tienen sentido para él.

III.8 LA SEGURIDAD EN SNMP

El protocolo SNMP proporciona mecanismos para el acceso a un almacén de información jerárquica compuesta por un conjunto de variables. Se distinguen dos tipos distintos de acceso a dicha información: un acceso para lectura que permite consultar los valores asociados a cada una de las variables y un acceso para escritura que permite modificar dichos valores.

Los mensajes del protocolo incluyen una cadena de caracteres denominada **nombre de comunidad** que se utiliza como un sencillo mecanismo de control de acceso a la información. Los agentes que implementan el protocolo disponen generalmente de dos comunidades o conjuntos de variables identificadas por un nombre de comunidad configurable por el administrador del sistema.

Una de dichas comunidades recibe el nombre de comunidad pública y sus variables pueden ser accedidas sólo para lectura. Por el contrario los valores asociados a las variables que componen la otra comunidad, denominada comunidad privada, pueden ser modificados.

Aproximadamente cuatro años después de su introducción, el marco de SNMP fue mejorado en 1992 para incorporarle características de seguridad. En Julio de 1992 los RFC's 1351, 1352, y 1353 fueron publicados. Estas nuevas adiciones a SNMP han proporcionado valiosas entradas para extender el marco de la administración. La tabla III.3 muestra dichos RFC's.

RFC	Título
1351	Modelo Administrativo SNMP
1352	Protocolos de Seguridad SNMP
1353	Definición de Objetos Administrados para la Administración de partes de SNMP
1321	Algoritmo de Compendio de Mensajes 5

Tabla III.3 RFCs de SNMP

SNMP propone al modelo administrativo extendido proporcionar las características de seguridad. El concepto importante detrás de este nuevo modelo es la noción de cómo los agentes y los SARs se comunican vía las comunidades.

Una comunidad se define formalmente como "un contexto de la ejecución conceptual y virtual cuyo funcionamiento se restringe (para seguridad u otros propósitos) a un subconjunto administrativamente definido de todos los posibles funcionamientos de una entidad de protocolos particulares de SNMP".

El uso de este modelo administrativo para ofrecer seguridad es proporcionado por medio de criptografía vía el **D**ata **E**ncryption **S**tandard (**DES**) y el uso del **M**essage **D**igest **5** (**MD5**) para autenticación. MD5 es presentado en el RFC 1321, *The MD5 Message Digest Algorithm*.

En términos de los mensajes, SNMP involucra la adicional inclusión de campos en la cabecera.

III.8.1 Descripción

Examinando cualquier aproximación de una red y la seguridad de las comunicaciones, **tres conceptos** deben ser considerados:

1. **Amenaza de Seguridad:** Cualquier acción que comprometa la seguridad de la información poseída por una organización.

2. **Servicio de Seguridad:** Un servicio de comunicaciones que mejore la seguridad de los sistemas de procesos de datos de una organización y la transferencia de información. El servicio es requerido para contar las amenazas de seguridad.

3. **Mecanismo de Seguridad:** Un mecanismo de comunicaciones que es diseñado para detectar, prevenir o reponerse de una amenaza de seguridad.

III.8.1.1 Amenazas de Seguridad

Para entender varios tipos de amenazas a la seguridad, necesitamos tener una definición de los requerimientos de seguridad. La computadora y la seguridad de la red se dirigen hacia **cuatro requerimientos**:

1. **Secreto:** La información en un sistema informático y la transmitida sólo deben ser accesibles para leer por partes autorizadas.

2. **Autenticidad:** El origen de un mensaje debe ser correctamente identificado, con el aseguramiento de que la identidad no es falsa.

3. **Integridad:** El sistema informático y la información transmitida deben ser modificables sólo por las partes autorizadas. La modificación incluye la escritura, el cambio, el estado de cambio, la supresión y la creación.

4. **Disponibilidad:** El sistema informático debe estar disponible a las partes autorizadas cuando lo necesiten.

Los tipos de amenazas a la seguridad de un sistema informático o red son mejor caracterizados viendo la función del sistema informático como la de proveer información.

En general, hay un flujo de información de una fuente, como un archivo o una región de memoria principal, a un destino, a otro archivo o a un usuario. Este **flujo normal** es representado en la Figura III.8, parte (a).

El resto de la figura muestra **cuatro categorías** generales de amenazas:

1. **Interrupción:** Un activo del sistema es destruido o se hace no disponible o inutilizable. Esta es una amenaza a la disponibilidad. Los ejemplos incluyen la destrucción de un pedazo de hardware, como un disco duro, el recorte de una línea de comunicación o la incapacidad de la administración de archivos del sistema (Figura III.8, parte (b)).

2. **Intercepción:** Una parte no autorizada gana el acceso a un activo. Esta es una amenaza al secreto. La parte no autorizada podría ser una persona, un programa o una computadora. Los ejemplos incluyen la intervención de las conexiones telefónicas para capturar datos en una red o el copiar ilícitamente archivos o programas (Figura III.8, parte (c)).

3. **Modificación:** Una parte no autorizada no sólo gana el acceso, sino que se entromete en un activo. Esta es una amenaza a la integridad. Los ejemplos incluyen valores que se cambian en el fichero de datos, cambiando un programa de modo que éste funcione de manera diferente o la modificación al contenido de mensajes que son transmitidos en una red (Figura III.8, parte (d)).

4. **Enmascaramiento:** Una parte no autorizada inserta objetos falsificados en el sistema. Esta es una amenaza a la autenticidad. Los ejemplos incluyen la inserción de mensajes falsos en una red o la adición de registros a un archivo (Figura III.8, parte (e)).

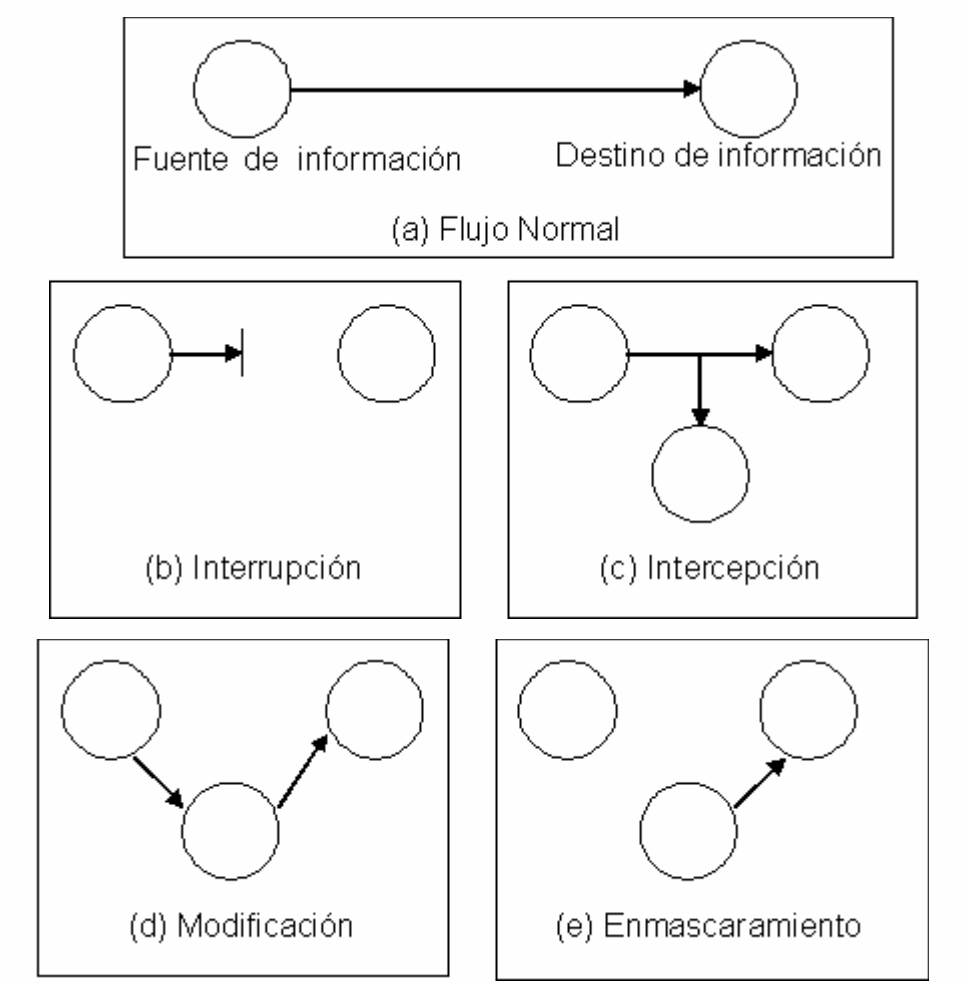


Figura III.8 Amenazas de Seguridad

III.8.1.2 Amenazas en el Contexto de SNMP

La descripción precedente de amenazas de seguridad puede ser aplicada en el contexto de SNMP para identificar las amenazas específicas involucradas en el uso de SNMP para la administración de red. Las amenazas siguientes pueden ser identificadas:

- **Enmascaramiento:** Alguna entidad que no está autorizada para realizar ciertas operaciones de administración puede intentar realizar esas operaciones asumiendo la identidad de una entidad autorizada.

- **Modificación de información:** Una entidad puede cambiar un mensaje en tránsito generado por una entidad autorizada para efectuar operaciones de administración no autorizadas, incluyendo el ajuste de valores de objeto.

- **Secuencia de mensaje y modificación de sincronización:** SNMP es diseñado para funcionar sobre un protocolo de transporte de menor conexión. Hay una amenaza que un mensaje SNMP podría reordenar, retrasar o repetir (duplicar) para efectuar operaciones de administración no autorizadas.

- **Descubrimiento:** Una entidad puede observar cambios entre un administrador y un agente y así aprender los valores de objetos administrados y aprender de eventos notificados.

- **Negación de servicio:** Un atacante puede prevenir cambios entre un administrador y un agente.

- **Análisis de tráfico:** Un atacante puede observar el modelo general de tráfico entre administradores y agentes.

III.8.1.3 Servicios de Seguridad de SNMP

Para oponerse a aquellas amenazas de seguridad consideradas relevantes para SNMP, los siguientes servicios de seguridad son proporcionados por SNMP:

- **Integridad de Datos:** Asegura que los mensajes sean tanto recibidos como enviados, sin una duplicación, inserción, modificación o repetición.

- **Autenticación de Origen de Datos:** Proporciona la corroboración de la fuente de un mensaje.

- **Confidencialidad de Datos:** Asegura que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

Los mecanismos usados en SNMP son tal, que la autenticación de origen de datos y la integridad de datos son ambos proporcionados por el mismo conjunto de mecanismos. Así, la provisión de uno de estos dos servicios implica la provisión del otro. La confidencialidad de datos es un servicio opcional que puede ser agregado a los otros dos servicios en una implementación dada.

III.8.1.4 Mecanismo de Seguridad de SNMP

Para proporcionar los tres servicios de seguridad definidos en la lista precedente, SNMP incluye los siguientes mecanismos:

- **Integridad de Datos:** Un algoritmo de resumen de mensaje es usado para calcular un resumen de 128 bits sobre la parte apropiada de un mensaje SNMP. Este resumen es incluido con el mensaje para asegurar que este no ha sido modificado. El mensaje también incluye una fecha cuyo valor está basado en el mantenimiento de relojes sincronizados libremente entre administradores y agentes.

  El destinatario de un mensaje usa la fecha para verificar que el mensaje es reciente y para determinar la secuencia apropiada de múltiples mensajes. La fecha también puede ser usada para detectar mensajes repetidos. No proporcionan ninguna protección contra la destrucción de mensajes no autorizados. SNMP seguro usa el algoritmo de resumen de mensajes MD5.

- **Autenticación de Origen de Datos:** El resumen de mensaje en realidad es calculado sobre la parte apropiada de un mensaje SNMP y un valor secreto prefijo para ese mensaje. El valor debe ser conocido a priori al remitente y al destinatario y no es incluido en el mensaje. El uso del valor secreto previene una tercera parte de la forma añadida al resumen correcto a un mensaje falso.

- **Confidencialidad de Datos:** Para proporcionar la confidencialidad, una parte apropiada de un mensaje SNMP es cifrada usando un algoritmo de cifrado simétrico. SNMP usa el algoritmo DES (estándar de cifrado de datos).

Como se mencionó anteriormente es necesaria una interfaz entre el sistema de administración y el encargado de la administración; para ello, la interfaz que se ocupará en este proyecto como consola de administración será WhatsUp Professional de Ipswitch, la cual es una interfaz gráfica que permitirá al administrador ver los sucesos que ocurren en la red del laboratorio. El funcionamiento de esta se explicará a continuación.

III.9 ¿QUÉ ES WHATSUP PROFESSIONAL?

WhatsUp Professional es una poderosa solución de monitoreo de red diseñada para ayudar a proteger el crecimiento de un negocio. WhatsUp Professional usa una base de datos para almacenar información sobre los dispositivos de red que están siendo monitoreados por la aplicación. Esta información permite a la aplicación ver con eficacia por medio de **poleo**, dispositivos y servicios sobre la red, escuchando mensajes enviados a través de la red.

Dependiendo de la respuesta de este poleo, WhatsUp Professional entonces inicia acciones basadas en el cambio de **estado del dispositivo** que es invocado por la respuesta o el mensaje.

WhatsUp Professional proporciona una serie de **reportes** que le dejan ver datos históricos basados en los dispositivos y monitores configurados en su base de datos del dispositivo.

Los componentes con los que cuenta WhatsUp Professional son:

- El servidor de la base de datos, que es Microsoft Server 2000 Desktop Engine (MSDE 2000)
- Una instancia de base de datos WhatsUp en MSDE
- Un Nombre de Fuente de Datos (DSN), que le indica a WhatsUp Professional donde encontrar la base de datos WhatsUp
- La aplicación de WhatsUp Professional

III.10 DISPOSITIVOS

En WhatsUp Professional, los dispositivos son representaciones virtuales de los recursos (computadoras, servidores, concentradores, etc.) que están conectados a la computadora por una LAN, una red inalámbrica o sobre Internet.

WhatsUp Professional ve estos dispositivos por medio de la conexión de red. Cuando esos recursos de red no pueden establecer una comunicación con WhatsUp Professional, el dispositivo es considerado abajo y una acción puede ser configurada para iniciar.

WhatsUp Professional no es una herramienta de arreglo. Este dirá cuando la red suba o baje, pero no dirá que hacer para arreglar la caída de la red. Para esto, se tendrá que inspeccionar el recurso afectado y su respectiva documentación.

III.10.1 Propiedades del Dispositivo

Hay nueve Propiedades disponibles. Sus descripciones vienen a continuación.

III.10.1.1 General

La sección General de las propiedades del dispositivo lista cajas de diálogo o le permite modificar información básica para el dispositivo seleccionado.

- **Nombre del despliegue:** Un nombre identificador para el dispositivo actual. Este nombre es puesto durante el Descubrimiento, pero puede ser cambiado en cualquier momento. El cambio del nombre no cambiará cómo el dispositivo es poleado, sólo cómo es mostrado en WhatsUp Professional.

- **Tipo de poleo:** Muestra el tipo de poleo que se quiere que WhatsUp Profesional use para este dispositivo.

    - ICMP (TCP/UDP)
    - IPX
    - NetBios

- **Usar poleo:** Muestra si se quiere que WhatsUp Professional use la dirección IP o el nombre (DNS) del dispositivo para el poleo.

- **Nombre del anfitrión (DNS):** Este debería ser el nombre de red oficial del dispositivo si el método de poleo es ICMP. El nombre de red debe ser un nombre que puede ser resuelto a una dirección IP.

- **Dirección:** Introducir una dirección IP.

- **Interfaces de red adicionales:** Configura una Interfaz de Red adicional para el dispositivo actual.

- **Tipo de dispositivo:** Muestra el icono del dispositivo apropiado. El icono mostrado representará el dispositivo en todas las vistas.

III.10.1.2 Monitores Activos

Los Monitores Activos cuestionan servicios de red instalados sobre un dispositivo, entonces esperan respuesta. Si una respuesta no es recibida, o si la respuesta no responde lo que esperan, el servicio es considerado abajo y un cambio de estado ocurre sobre el dispositivo. Si la pregunta es devuelta con la respuesta esperada, el servicio es considerado arriba.

III.10.1.2.1 Biblioteca de Monitor Activo

La Biblioteca de Monitor Activo es el almacén central de todos los Monitores Activos que han sido configurados para su red. Cuando los cambios son hechos a los Monitores Activos catalogados en este diálogo, esos cambios afectan cada caso de ese monitor particular a través de sus grupos de dispositivos.

III.10.1.2.2 Monitores Activos Soportados

La siguiente es una lista de todos los tipos de Monitores Activos que son soportados por WhatsUp Professional.

- **Monitor DNS:** Este es un monitor de servicio simple que comprueba el DNS (Servidor de Nombre de Dominio) sobre el puerto 53.
- **Monitor SNMP:** Protocolo Simple de Administración de Red es el protocolo que gobierna la administración de red y supervisión de dispositivos de red y sus funciones.
- **Monitor Telnet:** Este monitor comprueba un servidor Telnet sobre el puerto 23.
- **Monitor Ping:** Este monitor envía un comando ICMP (ping) al dispositivo.
- **Monitor TCP/IP:** Este monitor es usado para supervisar un servicio de TCP/IP que no aparece en la lista de servicios estándar o usa un número de puerto no estándar.
- **Monitor de Servicio NT:** Este monitor le permite comprobar el estado de un servicio sobre una máquina Windows e intentar un reinicio de ese servicio (si los permisos de Administrador apropiados existen).

III.10.1.3 Monitores Pasivos

Algunos elementos sobre una red no pueden proveer una aclaración o baja de estado cuando son cuestionados. Por ejemplo, un mensaje puede ser registrado en el registro de acontecimiento del sistema por otra aplicación (como una aplicación de antivirus alertando cuando un virus es encontrado).

Estos mensajes/eventos pueden ocurrir en cualquier momento y un Oyente de Monitor Pasivo los "escucha" y notifica a WhatsUp Professional cuando ocurren.

III.10.1.3.1 Configurando Oyentes de Monitor Pasivo

El **Oyente de Monitor Pasivo** es un ejecutable separado que escucha un evento a ocurrir y luego notifica a WhatsUp Professional. Este deja conseguir la notificación de un evento cuando este ocurre.

El Oyente de Monitor Pasivo es únicamente responsable de cómo supervisa sus eventos. Esto quiere decir que el servidor podría escuchar el tráfico de la red, cambios de archivos o eventos de aplicaciones específicas.

- **Monitor Pasivo SNMP (SNMP Trap):** Es un mensaje SNMP no solicitado enviado de un dispositivo para indicar un cambio de estado.

- **Monitor Pasivo Syslog:** Es usado para examinar mensajes Syslog expedidos de otros dispositivos para un registro específico y/o texto específico dentro de un registro.

- **Monitor Windows Event Log:** Este podría supervisar cuando un servicio es iniciado o detenido, si hubiera un fracaso de conexión o cualquier otra entrada en el Windows Event Log.

III.10.1.3.2 Biblioteca de Monitor Pasivo

Este diálogo muestra los tipos de Monitores Pasivos que han sido creados para WhatsUp Professional. Estos tipos son configuraciones específicas de traps SNMP, Windows Log Events y Syslog Events. Una vez que los tipos de monitor han sido configurados, se pueden asociar a dispositivos sobre la sección de Monitores Pasivos de Propiedades de Dispositivo.

III.10.1.4 Acciones

Las Acciones proporcionan el mecanismo para notificarlo acerca de cambios en el estado de un dispositivo o un monitor, o para mandar un programa en respuesta a un cambio de estado.

En este diálogo, se puede seleccionar una Política de Acción para usar sobre el dispositivo seleccionado o configurar acciones específicamente para ese dispositivo.

Alternativamente, las acciones configuradas aparecen en la lista de aplicar acciones individuales, mostrando el tipo de acción que debe ser iniciada y el cambio de estado que provocará la acción. Se pueden tener múltiples acciones sobre un solo dispositivo.

III.10.1.4.1 Biblioteca de Acción

La Biblioteca de Acción es el almacén central de todas las acciones que han sido configuradas para su red. Cuando son hechos cambios a una acción listada en este diálogo, estos cambios afectan a cada instancia de cada acción particular a través de sus grupos de dispositivos.

III.10.1.4.2 Tipos de Acción

Una Acción asignada a un dispositivo o monitor, se activa cuando un cambio de estado especificado ocurre. WhatsUp Professional soporta los siguientes tipos de acciones:

- **Sonido:** Suena una alarma activando un archivo de sonido seleccionado en la consola de WhatsUp Professional
- **Beeper:** Activa un Beeper
- **Paginador:** Envía un mensaje a un paginador
- **E-mail:** Envía un mensaje mail SMTP
- **SMS:** Envía una notificación de Servicio de Mensaje Corto (SMS) a un paginador o teléfono celular
- **Winpop-up:** Despliega un mensaje en una ventana pop-up sobre un sistema Windows NT

- **Syslog:** Envía un mensaje a un anfitrión que está corriendo un servidor Syslog
- **Text-to-Speech:** Envía una notificación text-to-speech a un hablante
- **Programa:** Corre otro programa (ejecutable) para tomar una acción
- **Reinicio de Servicio:** Detiene o reinicia un Servicio Windows NT
- **Política de Acción:** Envía un grupo de acciones que incluyen cualquiera de los tipos mencionados

III.10.1.4.3 Políticas de Acción

Las Políticas de Acción le permiten apilar múltiples acciones juntas en una política simple. Se puede entonces asignar estas acciones a cualquier dispositivo. Una vez asignadas, se puede editar las políticas en el diálogo de Políticas de acción sin tener que hacer cambios a todos los dispositivos que usan esa acción particular.

III.10.1.5 SNMP

Este diálogo muestra las propiedades SNMP de un dispositivo. El Protocolo Simple de Administración de Red es el protocolo que gobierna el monitoreo y la administración de dispositivos de red y sus funciones.

Si la opción de dispositivo administrable SNMP es seleccionada durante el Descubrimiento, la cadena de comunidad SNMP correcta es usada durante el proceso de descubrimiento y si el dispositivo es SNMP administrable, entonces esta opción es seleccionada automáticamente.

- **Comunidad de lectura:** Es una contraseña usada por WhatsUp Professional para leer los datos SNMP del dispositivo.
- **Comunidad de escritura:** Es una contraseña que da acceso de escritura a los datos SNMP del dispositivo.
- **Objeto del Dispositivo ID (OID):** Es el identificador de objeto SNMP para el dispositivo. Éste puede haber sido usado durante el descubrimiento para determinar el tipo de dispositivo.

III.10.1.6 Poleo

Poleo es el término usado para el monitoreo de dispositivos descubiertos en WhatsUp Professional. Este permite configurar opciones de poleo y/o programar tiempos de mantenimiento para el dispositivo seleccionado.

III.10.1.6.1 Poleo

- **Intervalo de Poleo:** Esta opción determina cuan a menudo WhatsUp Professional polea el dispositivo seleccionado.

- **Colector de datos estadísticos de Monitor Activo para reportes:** Esta opción tiene el tiempo de ida y vuelta recogido por el monitor ping del dispositivo. Los datos aparecen en los reportes de funcionamiento del dispositivo y del grupo.

III.10.1.6.2 Mantenimiento

En esta sección, se puede poner manualmente el estado de mantenimiento a un dispositivo, o programar un estado de mantenimiento semanal para un cierto período de tiempo. Cualquier dispositivo colocado en modo de mantenimiento no será poleado y las acciones no serán iniciadas, pero permanece en la lista de dispositivo y los datos históricos son conservados.

III.10.1.7 Notas

Esta sección le da la capacidad de entrar en notas de forma libre a la base de datos del dispositivo.

Se puede registrar información histórica acerca de un dispositivo, la información de localización física o quizás notas relacionadas a las acciones configuradas para el dispositivo. El uso de esta sección es completamente personal.

III.10.1.8 Menú

Este diálogo es usado para crear un menú de contexto para un dispositivo.

- **Personalizar el menú sobre un dispositivo:** Esta opción sirve para crear y/o modificar un menú de contexto para un dispositivo.

- **Lista de menú:** Esta caja muestra los comandos que actualmente están configurados para el dispositivo.

III.10.1.9 Atributos

Este diálogo lista atributos añadidos a un dispositivo, como persona de contacto, localización, etc. Los primeros atributos en la lista son añadidos por WhatsUp Professional cuando el dispositivo es añadido a la base de datos o por el **Wizard Descubrimiento de Dispositivo**.

III.10.2 Grupos de Dispositivos

En esencia, los grupos de dispositivos son carpetas organizadas que le permiten encontrar y diagnosticar problemas rápidamente con dispositivos en su base de datos. Se pueden organizar estas carpetas de manera que tengan sentido para el administrador. Se tendrá un mapa diferente para cada grupo de dispositivo.

III.10.2.1 Descubrimiento

Durante el descubrimiento, los grupos de dispositivo son creados para cada subred que es encontrada sobre la red que fue escaneada. En el nivel superior del árbol de red, el escaneo entero está contenido en una carpeta identificando el tipo y la fecha de escaneo en que fue hecho.

A través del Wizard de descubrimiento de dispositivo, se puede escanear la red de dispositivos usando el protocolo(s) y ajustes que se escojan. Una vez que los dispositivos son encontrados, seleccionar los que se quieran monitorear y WhatsUp Professional creará un dispositivo en la base de datos para cada elemento que se escoja. Los grupos de dispositivos son creados basados en subredes que son encontradas durante el escaneo.

Tipos de escaneo

Hay **cuatro opciones** para descubrir dispositivos. Ellas son:

1. **SNMP SmartScan:** SmartScan descubre dispositivos leyendo información SNMP sobre la red. Este tipo de escaneo usa un ruteador SNMP habilitado para identificar dispositivos de red y subredes.
2. **Escaneo de Rango IP:** WhatsUp Professional escanea un rango de direcciones IP y encuentra los dispositivos que responden a uno o más de los servicios escogidos.

3. **Network Neighborhood:** Escaneando con Network Neighborhood, se crea una lista de dispositivos escaneando la red Windows a la cual la computadora está conectada y encontrando los otros sistemas sobre la red.

4. **Hosts File Import:** WhatsUp Professional importa dispositivos del archivo del anfitrión del sistema, el cual es un archivo de texto que lista los nombres del anfitrión y sus direcciones IP sobre una red.

III.10.2.1.1 Descubrimiento Activo

Con el Descubrimiento Activo se puede programar WhatsUp Professional para escanear la red para nuevos monitores y dispositivos sobre una base regular. El Descubrimiento Activo trabaja con **dos tipos de descubrimiento** de dispositivos.

1. **SNMP SmartScan:** WhatsUp Professional descubre dispositivos leyendo información SNMP de la red. Este tipo de escaneo usa un ruteador SNMP habilitado para identificar los dispositivos en la red y también identifica subredes dentro de la red.

2. **Escaneo de Rango IP:** WhatsUp Professional escanea un rango de direcciones IP y encuentra los dispositivos que responden a un mensaje enviado via Internet Control Message Protocol (ICMP).

III.10.2.1.2 Estado del Dispositivo

Cada carpeta en el árbol de red tiene un indicador de estado de dispositivo en el icono de la carpeta. Este indicador muestra el peor estado a través de todos los dispositivos contenidos en esa carpeta.

III.10.3 Reconocimiento

Cuando un estado de dispositivo cambia, a pesar de cualquier acción que ha sido colocada sobre el dispositivo, WhatsUp Professional usa la característica de reconocimiento para informar el cambio de estado. El nombre del dispositivo aparece en sobresaliente en la lista de dispositivo y en la vista del mapa, el nombre del dispositivo aparece sobre un fondo negro.

III.11 CONSOLA DE WHATSUP PROFESSIONAL

La Consola de WhatsUp Professional es la **interfaz** primaria para la configuración y la administración de la aplicación y la base de datos. A continuación se describen las diferentes partes de la consola y cómo navegar en ella.

III.11.1 Descripción de la Consola

Lo siguiente es una descripción de las características principales encontradas en la consola de WhatsUp Professional. La figura III.9 muestra la ubicación de estas características.

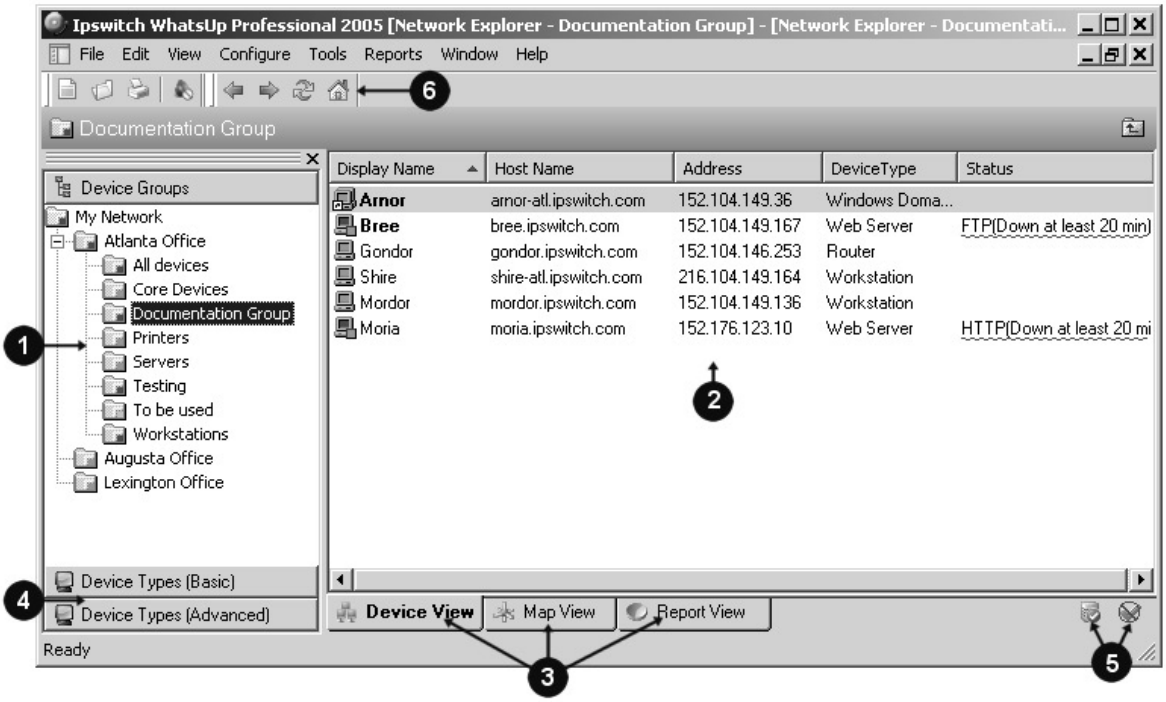


Figura III.9 Características de la consola

1 Árbol de grupo de dispositivos: Es una lista de todos los grupos de dispositivos creados por WhatsUp Professional. Cuando se realiza un descubrimiento de escaneo, WhatsUp Professional crea una carpeta de nivel superior para ese escaneo particular.

2 Cuadro de vista: Muestra el grupo de dispositivo seleccionado basado en la vista de las etiquetas abajo.

3 Selectores de vista: Elige el modo que se quiere para ver los grupos de dispositivo. Cada una de estas vistas es explicada detalladamente a continuación.

- **Vista del dispositivo:** Proporciona una descripción de cada dispositivo y subgrupo en un grupo de dispositivo seleccionado.
- **Vista del mapa:** Muestra una representación gráfica de los dispositivos y subgrupos en un grupo de dispositivo seleccionado.
- **Vista del reporte:** Es usada para solucionar y monitorear datos históricos que han sido reunidos durante la operación de WhatsUp Professional.

4 Grupos de tipo de dispositivo: Pulsar la etiqueta Básica o Avanzada para ver los tipos de dispositivo contenidos en esta sección. Estos tipos pueden ser arrastrados en el cuadro de vista para crear un nuevo dispositivo basado en ese tipo de dispositivo.

5 Iconos de indicador de poleo: Indican el estado actual de la máquina de poleo.

6 Barra de tareas de WhatsUp Professional: Los iconos en esta barra de tareas cambian según la vista que se use.

III.11.2 Vista del Dispositivo

Con una vista y sentido similar al Explorador de Windows, la Vista del Dispositivo de WhatsUp Professional da otra opción para ayudar a mantener una red compleja, organizada y funcionando correctamente. En esta vista, los dispositivos son organizados por el grupo de dispositivo y aparecen en la lista en orden alfabético basado en el nombre de la carpeta o el nombre mostrado del dispositivo. La figura III.10 es un ejemplo de esta vista.

Display Name	Host Name	Address	DeviceType	Status
Arnor	arnor-atl.ipswitch.com	152.104.149.36	Windows Doma...	Ping(Down); DNS(Down); I
Bree	bree.ipswitch.com	152.104.149.167	Web Server	Ping(Down); HTTP(Down).
Gondor	gondor.ipswitch.com	152.104.146.253	Router	Ping(Down); Interface(1)(D
Mordor	mordor.ipswitch.com	152.104.149.136	Workstation	Ping(Down)
Moria	moria.ipswitch.com	152.176.123.10	Web Server	Ping(Down); HTTP(Down .
Shire	shire-atl.ipswitch.com	216.104.149.164	Workstation	

Figura III.10 Vista del dispositivo

Cada icono del dispositivo proporciona información sobre su estado y el de los monitores asociados a ese dispositivo. Además, la columna de estado indica que el monitor específico está abajo y la duración de la interrupción.

III.11.3 Vista del Mapa

A través de la Vista del Mapa de WhatsUp Professional, se tiene la capacidad de crear representaciones gráficas de la red. Los dispositivos pueden ser colocados en tantos mapas como se necesite, sin ser esos dispositivos poleados múltiples veces. La figura III.11 es un ejemplo de la vista de un mapa de red.

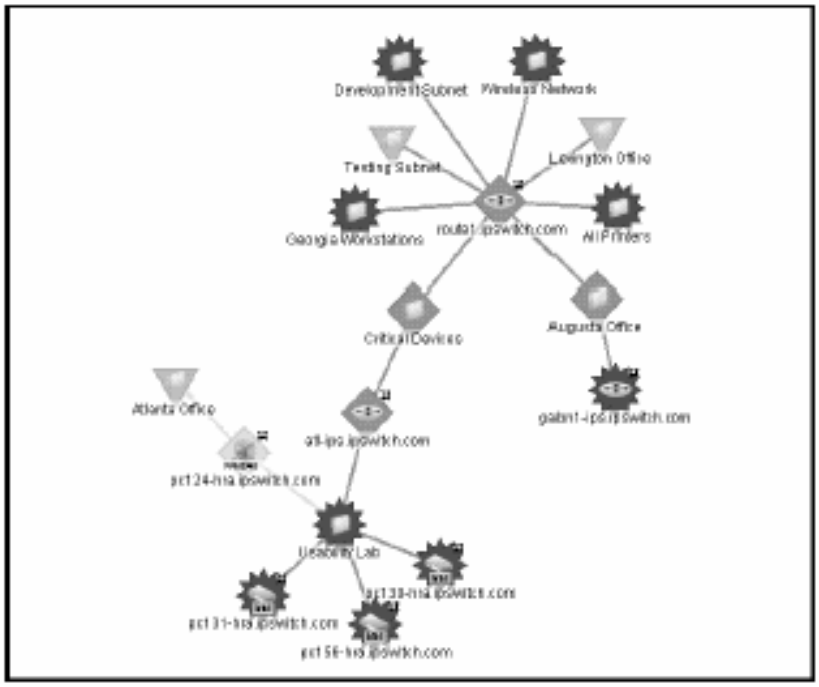


Figura III.11 Vista del mapa

El mapa de la figura anterior fue creado por WhatsUp Professional durante un escaneo SNMP durante el descubrimiento de dispositivo. Este muestra la relación entre las diferentes subredes que están conectadas una a una vía las estructuras de red representadas aquí.

III.11.4 Vista del Reporte

La Vista del Reporte es usada para solucionar y monitorear los datos históricos que han sido reunidos durante la operación de WhatsUp Professional. Los reportes pueden ser vistos en la consola de WhatsUp Professional o la Interfaz Web y ellos pueden ser enviados por correo electrónico a una dirección de correo que se identifique con la característica de Reporte Recurrente.

III.12 REPORTES DE WHATSUP PROFESSIONAL

En WhatsUp Professional los reportes son usados para solucionar y supervisar los datos históricos que han sido recogidos durante la operación de la aplicación. Los reportes pueden ser vistos en la consola y ellos pueden ser enviados por correo electrónico a una dirección de e-mail a través de la característica de Reporte Recurrente.

III.12.1 Lista de Reportes

Las tablas III.4, III.5 y III.6 son una lista de todos los reportes que están disponibles en WhatsUp Professional.

Reportes de Sistema	
Registro de Actividad	El reporte de registro de actividad es una historia categorizada de todos los mensajes generados por WhatsUP Professional.
Entradas Syslog	Este reporte muestra eventos syslog registrados durante un periodo de tiempo.
Registro Trap SNMP	El registro SNMP Trap proporciona una historia de traps SNMP que han ocurrido durante un periodo de tiempo.

Tabla III.4 Reportes de Sistema de WhatsUp Professional

Reportes de Sistema	
Windows Event Log	Este reporte muestra eventos Windows registrados para todos los dispositivos durante un periodo de tiempo.
Acciones Aplicadas	El reporte de acciones aplicadas muestra como las acciones son aplicadas a dispositivos y monitores en el sistema. Cada entrada muestra una acción y el dispositivo, el monitor y el estado que lo provocó.
Resultados de Descubrimiento Activo	Una vez que una tarea de descubrimiento activa descubre nuevos dispositivos o servicios, este reporte es poblado con los resultados de esa exploración.
Reconocimiento de Cambio de Estado	Cuando un dispositivo cambia de estado, independientemente de cualquier acción que ha sido colocada sobre el dispositivo, WhatsUp Professional usa la característica de reconocimiento para avisarle del cambio de estado ocurrido.
Registro de Acción	El registro de acción muestra todas las acciones que WhatsUp Professional ha intentado mostrar, basado en la configuración de la acción.
Registro de Error General	El registro de error general muestra una lista de mensajes de error generados por WhatsUp Professional para un periodo de tiempo deseado.
Registro de Error de Monitor Pasivo	Este reporte muestra todos los errores de monitor pasivo que ocurren durante la operación de WhatsUp Professional.
Registro de Reporte Recurrente	Este reporte muestra un registro de todos los reportes recurrentes que han ocurrido durante un periodo de tiempo seleccionado.

Tabla III.4 Reportes de Sistema de WhatsUp Professional (Continuación)

Reportes de Grupo	
Resumen de Estado	Este reporte es un resumen de estados de dispositivo en el grupo seleccionado actualmente.
Disponibilidad	Este reporte despliega un porcentaje del tiempo que cada dispositivo monitoreado en el grupo seleccionado ha estado UP y respondiendo al poleo durante un periodo de tiempo.
Salud	Este reporte despliega el estado actual de los dispositivos en el grupo seleccionado, de acuerdo con cada monitor configurado para estos dispositivos.
Funcionamiento	Este reporte muestra el tiempo de respuesta de cada dispositivo en el grupo.
Línea de Tiempo de Cambio de Estado	Este reporte muestra una línea de tiempo de cuando cada monitor en un dispositivo en el grupo seleccionado cambió de un estado a otro durante el periodo de tiempo desplegado.
Acciones Aplicadas	El reporte de grupo de acciones aplicadas muestra como son aplicadas las acciones a dispositivos y monitores en el grupo actual. Cada entrada muestra una acción y el dispositivo, monitor y estado que le fue aplicado.

Tabla III.5 Reportes de Grupo de WhatsUp Professional

Reportes de dispositivo	
Disponibilidad	Este reporte muestra estadísticas acerca de la disponibilidad del dispositivo seleccionado.
Salud	Este reporte muestra el estado actual (una vista) del dispositivo seleccionado y todos los monitores en ese dispositivo. Cada monitor muestra su propio estado de dispositivo, el estado actual de cada elemento, cuanto ha estado el dispositivo en ese estado y la primera hora a la que el estado fue reportado.
Funcionamiento	Este reporte muestra el promedio de tiempo de respuesta de cada monitor unido al dispositivo seleccionado.

Tabla III.6 Reportes de Dispositivos de WhatsUp Professional

Reportes de dispositivo	
Línea de Tiempo de Cambio de Estado	Este reporte muestra una línea de tiempo de cuando cada monitor sobre un dispositivo seleccionado cambió de un estado a otro durante un periodo de tiempo mostrado.
Entradas Syslog	Este reporte muestra eventos Syslog registrados para el dispositivo seleccionado durante un periodo de tiempo.
Registro Trap SNMP	El registro Trap SNMP proporciona una historia de traps SNMP que han ocurrido para el dispositivo seleccionado durante un periodo de tiempo.
Registro Windows Event	Este reporte muestra eventos Windows registrados para el dispositivo seleccionado durante un periodo de tiempo.

Tabla III.6 Reportes de Dispositivos de WhatsUp Professional (Continuación)

III.12.2 Reportes Recurrentes

A través de esta característica, usted puede configurar WhatsUp Professional para enviar reportes a direcciones e-mail en intervalos programados regularmente. Cada entrada representa una dirección diferente de e-mail o reporte que está enviándose.

III.13 REQUISITOS DE WHATSUP PROFESSIONAL

- Los sistemas operativos soportados son: Windows 2003 Server; Windows XP SP1 o posterior; Windows 2000
- 256 MB de espacio de disco libre

  Nota: Esto es el requerimiento para la instalación. Se necesitará más espacio para la base de datos. Una base de datos MSDE puede crecer al límite de 2 GB.
- 256 MB de RAM

Para usar la página Web, mensajes SMS o acciones de beeper, son requeridos una línea telefónica y un módem local.

CAPÍTULO IV

INSTALACIÓN Y PRUEBAS DEL SISTEMA DE ADMINISTRACIÓN AL LABORATORIO DE REDES Y SEGURIDAD

"El triunfo no está en vencer siempre, sino en nunca desanimarse".

IV.1 ACTIVACIÓN DEL SERVICIO SNMP

Para utilizar el servicio SNMP se debe primero activar dicho servicio de la siguiente manera:

1. Abrir el Panel de Control.
2. Dar doble clic en la opción de "Agregar/Quitar programas".
3. Seleccionar la opción de "Agregar/Quitar Componentes de Windows".
4. Habilitar la opción "Herramientas de Administración y Monitoreo".
5. Dar clic en el botón de "Detalles".
6. Verificar en el recuadro la opción "Protocolo Simple de Administración de Redes" y dar clic en "Aceptar" y se despliega una ventana de "Wizard".
7. Dar clic en "Siguiente" para terminar de instalar el agente.

IV.2 INSTALACIÓN DE WHATSUP PROFESSIONAL

Los pasos a aplicar para una exitosa instalación de WhatsUp Professional serán citados a continuación.

1. Bajar de la página **www.ipswitch.com** el programa de instalación de WhatsUp Professional.
2. Ejecutar el programa de instalación. Se iniciará un Wizard que indica los pasos a seguir durante la instalación.
3. Aparecerá una pantalla de bienvenida, dar clic en Next. La figura IV.1 muestra esta pantalla.

Figura IV.1 Pantalla de bienvenida

4. Leer el contrato de licencia, seleccionar Acept y luego dar clic en Next.

5. En la pantalla de destino, dar la dirección destino donde se desea instalar el programa y dar clic en Next.

6. En la siguiente pantalla que aparece dar clic en Next.

7. Dar clic en Install. Y comenzará la instalación de los archivos de aplicación de WhatsUp Professional.

8. Aparecerá la pantalla que indica que la Instalación ha sido completada. Dar clic en Finish.

9. Buscar el ícono de IPswitch en el menú Inicio/Todos los programas y crear un acceso directo al escritorio.

10. Dar clic en el ícono de IPswitch que acabamos de crear en el escritorio.

11. En la pantalla para activar la aplicación WhatsUp Professional dar clic en Active Later debido a que se utilizará la versión de prueba.

12. Aparecerá la pantalla que indicará que es lo que se va configurar, dar clic en Next.

13. En la pantalla siguiente activar la opción IP Range Scan y dar clic en Next, como se muestra en la figura IV.2.

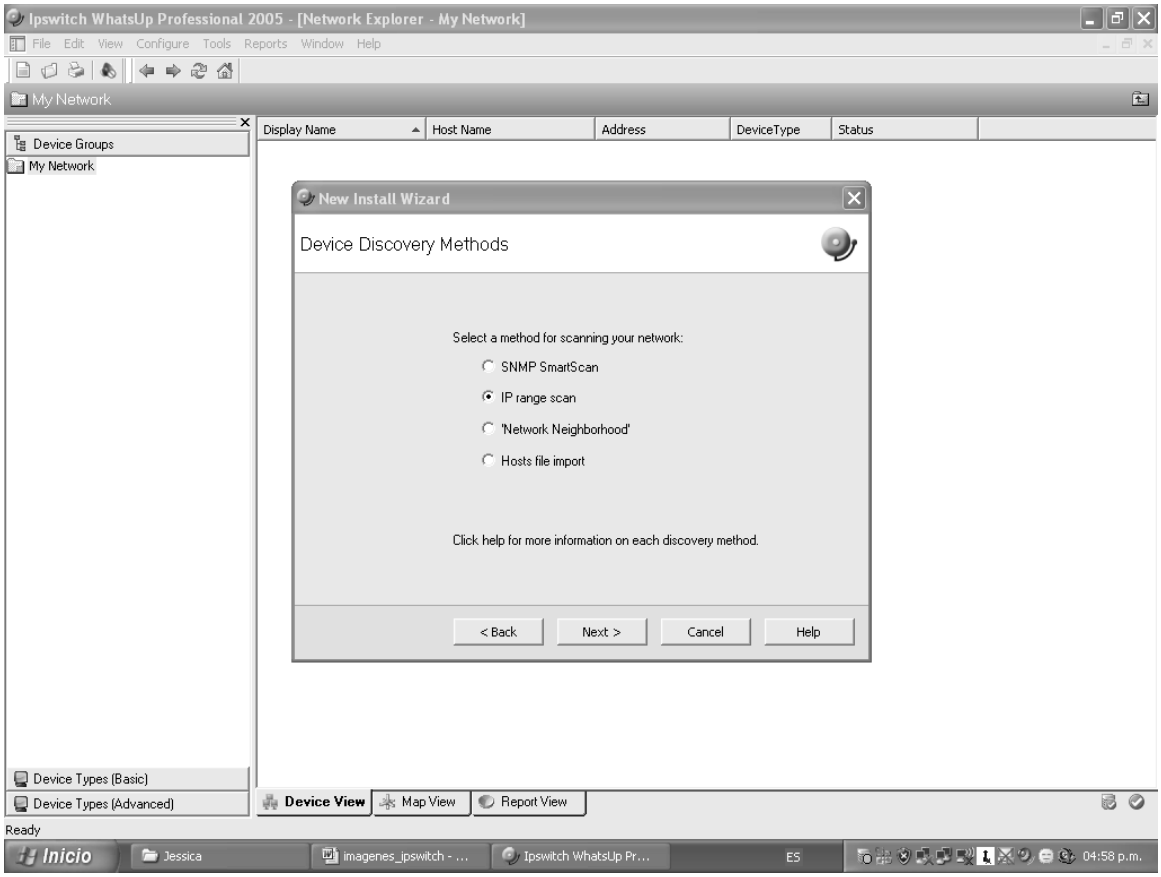


Figura IV.2 Activación de la opción IP Range Scan

14. En la siguiente pantalla marcar el rango de direcciones IP que queremos que escanee.

15. Dar clic en Advanced y deshabilitar la casilla de limit scan to class c sub ranges. Y dar OK.

16. Dar clic en Next.

17. En la siguiente pantalla habilitar la casilla de Identify devices via SNMP y dar el nombre de la comunidad el cual por defecto es public. Dar clic en Next.

18. En la pantalla siguiente habilitar todas las opciones que se deseen escanear y dar clic en Next, como se muestra en la figura IV.3.

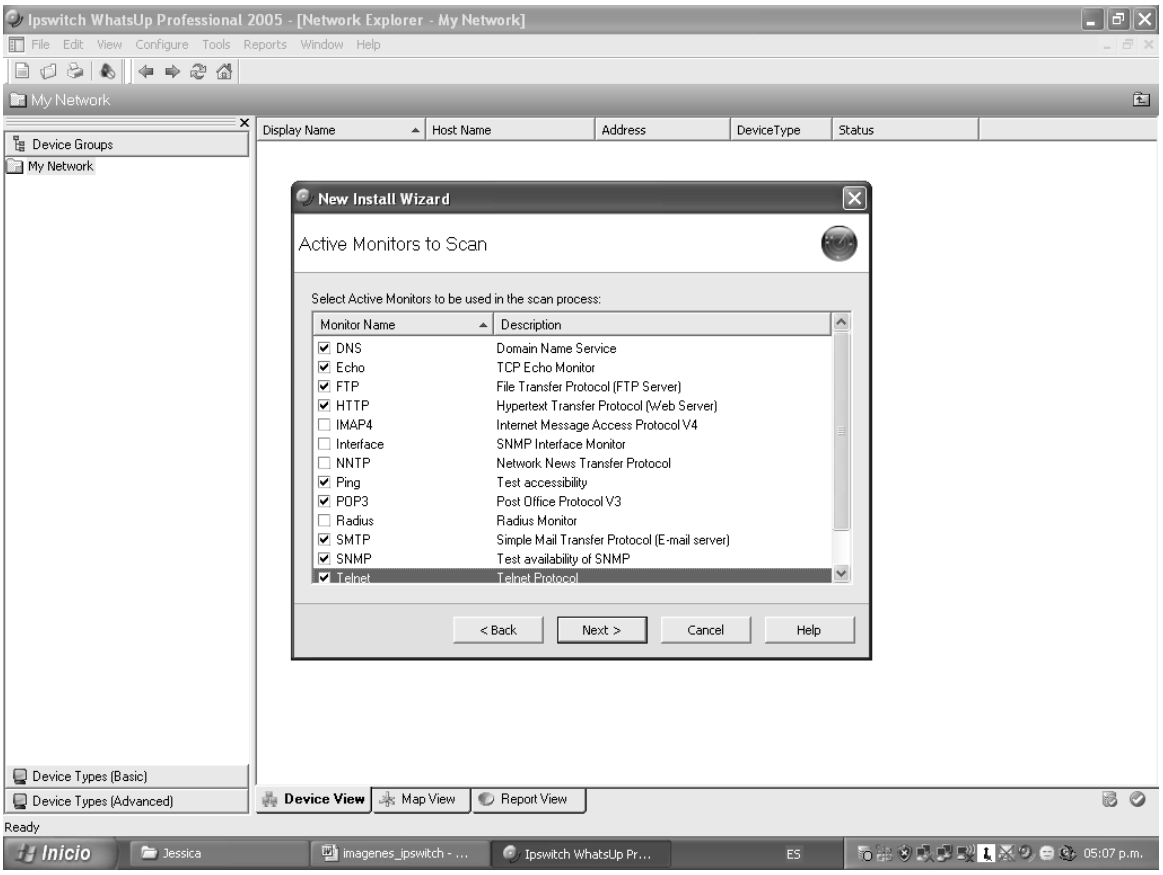


Figura IV.3 Opciones para escanear

19. Comenzará el escaneo de las direcciones IP.

20. En la siguiente pantalla aparecerán los dispositivos que reconoció para monitorear. Dar clic en Next.

21. En la pantalla de selección de políticas de acción habilitar la opción de Asist in creating a new action policy y dar clic en Next.

22. Aparecerá una pantalla de tipos de acción, habilitar las opciones por medio de las cuales queremos que nos llegue una notificación de fallas. Dar clic en Next.

23. Será mostrada una pantalla con un resumen de las políticas de acción que queremos aplicar. Dar clic en Next.

24. En la siguiente pantalla se resumirán los dispositivos encontrados, dar clic en Finish.

25. La instalación de la aplicación está completa.

En la pestaña de **Device View** aparecerán las máquinas que reconoció el programa. La figura IV.4 muestra la vista de las máquinas del laboratorio.

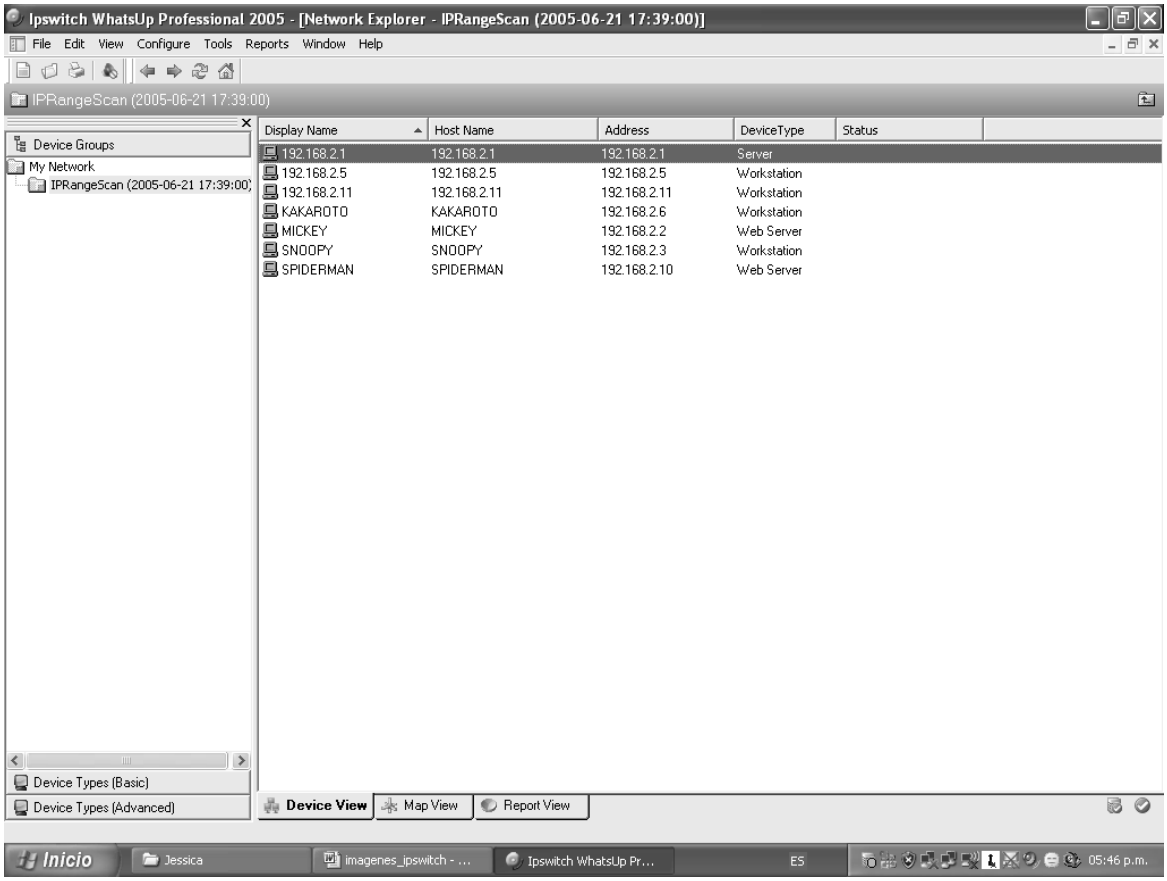


Figura IV.4 Vista de los dispositivos del laboratorio

Y en la pestaña de **Map View** aparecerán los gráficos de los dispositivos reconocidos. La figura IV.5 es la vista gráfica de los dispositivos del laboratorio.

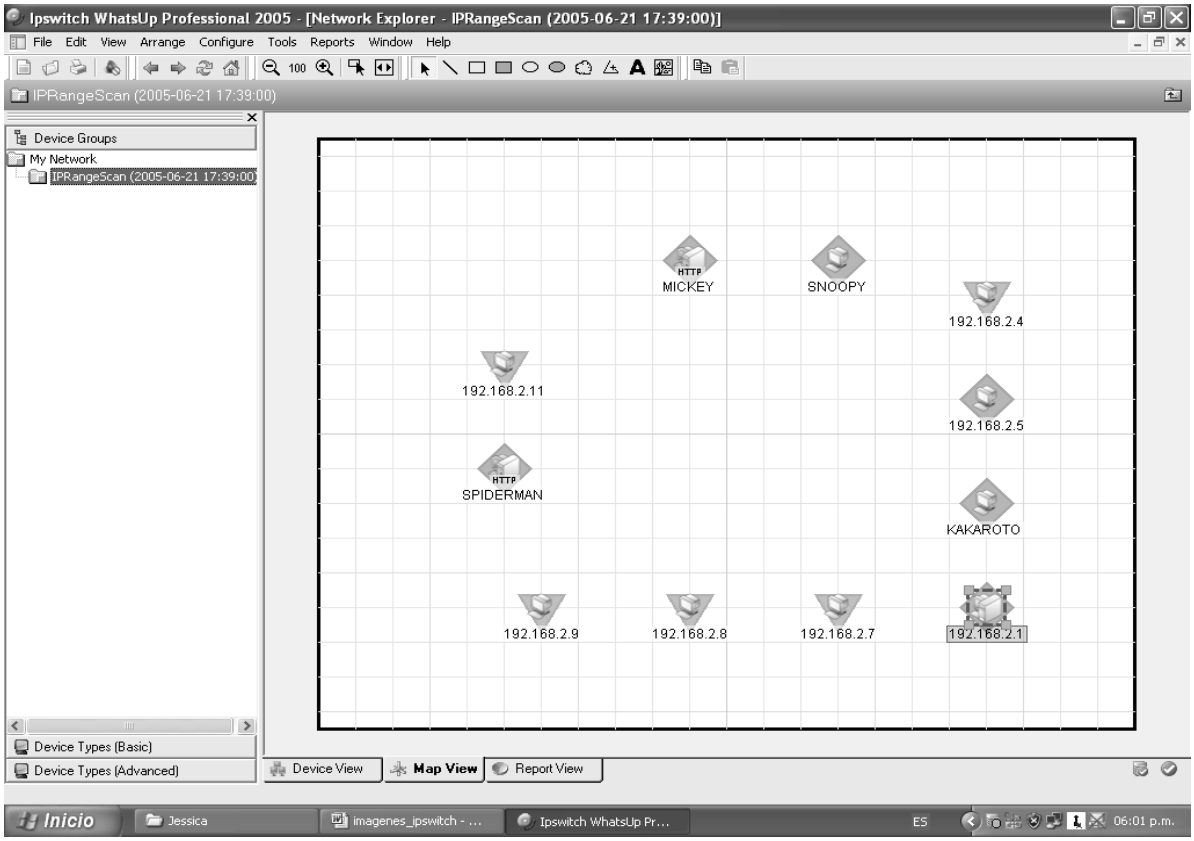


Figura IV.5 Vista gráfica de los dispositivos del laboratorio

IV.3 CONFIGURACIÓN DE LAS PROPIEDADES DE LOS DISPOSITIVOS

Se pueden modificar propiedades de los dispositivos individuales (Figura IV.6) pulsando el botón derecho del ratón sobre el icono del dispositivo en la vista del mapa y seleccionar propiedades. Pulsar los iconos en el cuadro de inspección izquierdo para ver o modificar cada propiedad.

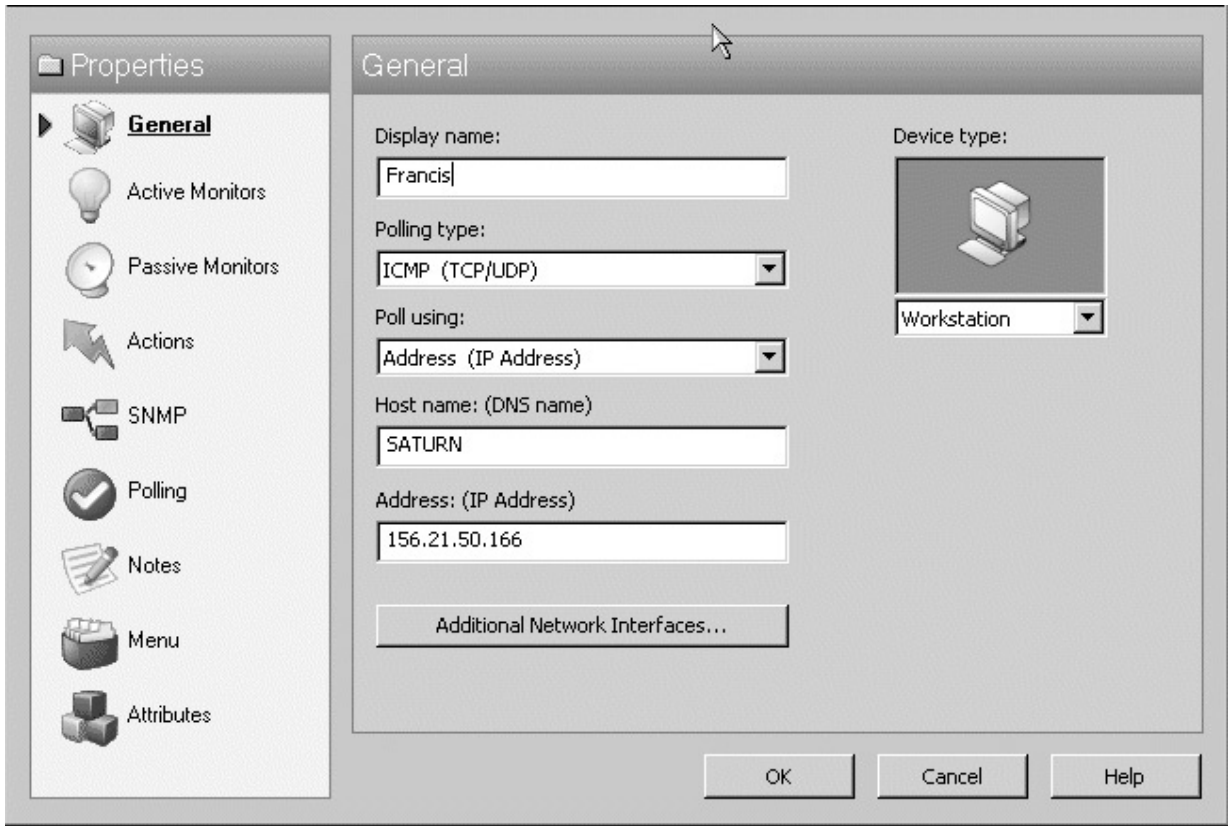


Figura IV.6 Propiedades de los dispositivos

IV.3.1 Monitores Activos

Los cambios que se pueden hacer sobre un Monitor Activo son:

- Add para configurar un nuevo monitor activo.
- Seleccionar un monitor activo y pulsar Edit para cambiar la configuración.
- Seleccionar un monitor activo y pulsar Delete para quitar el monitor del dispositivo.
- Pulsar Discover para hacer que WhatsUp Professional escanee el dispositivo para monitores activos.

IV.3.1.1 Biblioteca de Monitor Activo

Para acceder a la biblioteca de monitor activo del menú principal de la consola WhatsUp Professional, seleccione Configure>Active Monitor Library.

Este diálogo es usado para configurar tipos de monitor activos nuevos o existentes. La lista muestra todos los tipos actualmente configurados para usar en WhatsUp Professional.

- Dar clic en New para configurar un nuevo tipo.
- Seleccionar un tipo existente y dar clic en Edit para cambiar la configuración actual de un tipo.
- Seleccionar un tipo de Active Monitor y dar clic en Copy para hacer una copia de ese tipo y añadirlo a la lista

.

- Seleccionar un tipo de Active Monitor y dar clic en Delete para quitarlo de la lista.
- Seleccionar un Active Monitor y dar clic en Test para probar el Monitor Activo seleccionado sobre un dispositivo.

IV.3.2 Monitores Pasivos

Los cambios que se pueden hacer sobre un Monitor Pasivo son:

- Add para configurar un nuevo Monitor Pasivo.
- Seleccionar un Monitor Pasivo y pulsar Edit para cambiar la configuración.
- Seleccionar un Monitor Pasivo y pulsar Delete para quitar el monitor del dispositivo.

IV.3.2.1 Configurando Oyentes de Monitor Pasivo

Antes de configurar monitores pasivos, se deben configurar estos oyentes.

- Del menú principal de la consola WhatsUp Professional, seleccionar Configure>Program Options.
- En Program Options, seleccionar Pasive Monitor Listeners.
- Seleccionar al oyente que se quiere configurar y dar clic en Configure.
- Escribir la información apropiada basada en el oyente que está siendo configurado.
- Dar clic en OK para salvar los cambios.

IV.3.2.2 Biblioteca de Monitor Pasivo

Para acceder a la Biblioteca de Monitor Pasivo sobre la consola de WhatsUp Professional, seleccionar Configure>Passive Monitor Library.

- Dar clic en New para crear un nuevo tipo.
- Seleccionar un tipo en la lista y dar clic en Edit para cambiar los ajustes.
- Seleccionar un tipo y dar clic en Copy para crear un nuevo tipo basado en el tipo seleccionado.
- Seleccionar un tipo y dar clic en Delete para quitarlo de la lista.

IV.3.3 Acciones

IV.3.3.1 Biblioteca de Acción

Para abrir la biblioteca de acción, del menú principal de la consola de WhatsUp Professional, seleccionar Configure>Action Library.

Este diálogo es usado para configurar una nueva o existente acción.

- Dar clic en New para configurar una nueva acción. Después seleccionar el tipo de Acción.
- Para cambiar la configuración de una acción, seleccionarla, después dar clic en Edit.
- Para crear una nueva acción basada en una existente, seleccionar una acción existente, después dar clic en Copy.

IV.3.3.2 Probar la Acción

Para probar una acción, seleccionarla en la Biblioteca de Acción, después dar clic en la parte inferior en Test. WhatsUp Professional corre una prueba y responde con un mensaje de éxito o de fracaso. Esta prueba verifica la información especificada en la acción.

IV.3.3.3 Asignar la Acción a un Dispositivo

El siguiente paso en la configuración de una acción es asignarla al dispositivo o monitor. Los pasos a seguir son los siguientes:

1. En la Lista de Dispositivos, seleccionar el dispositivo, después dar clic con el botón derecho y seleccionar Properties del menú. Las Propiedades del Dispositivo aparecen.
2. Seleccionar las Propiedades de Acción.
3. Seleccionar Apply Individual Actions, luego pulsar Add. El Wizard de Construcción de Acción aparece.

4. Seleccionar Select an Action from the Action Library, luego pulsar Next.

5. Seleccionar la acción, después seleccionar provocar esta acción.

6. Pulsar Finish para asignar esta acción.

IV.3.3.4 Políticas de Acción

Para crear una política de acción se deben seguir los siguientes pasos:

1. De la barra de menú, seleccionar Configure>Action Policies. El diálogo de Políticas de Acción aparece.

2. Sobre el diálogo de Políticas de Acción, dar clic en New.

3. En el diálogo de New Action Policy, dar un nombre en la caja de Policy Name. Este nombre es usado para identificar la política más adelante.

4. Añadir acciones existentes a la Política de Acción, o crear nuevas acciones y añadirlas.

   Dar clic en Add. El Wizard de constructor de acción aparece.

5. Seguir las instrucciones en el Wizard.

6. Dar clic en Finish para finalizar el Wizard para añadir la Acción a la Política.

7. Añadir tantas acciones como se necesiten para completar la Política. Se pueden mover acciones hacia arriba y hacia abajo de la lista dando clic en los botones Up y Down debajo de la lista de acción.

8. Una vez que todas las acciones han sido añadidas, dar clic en OK para crear la política y añadirla a la lista activa.

9. Asignar la política de acción a un dispositivo o monitor.

Para editar o borrar una Política de Acción al dispositivo, seleccionar una de ellas del menú desplegable de Políticas de Acción.

- Seleccionar una acción configurada y pulsar Edit para cambiar los ajustes para esa acción.

- Seleccionar una acción configurada y pulsar Delete para borrar la acción de la lista.

IV.3.4 Poleo

Poleo

Insertar el número de segundos que usted quiere que pase entre poleos.

Mantenimiento

- **Manualmente poner este dispositivo en modo de mantenimiento ahora** - Seleccionar esta opción para poner el dispositivo en modo de mantenimiento. Limpiar la opción para reanudar el poleo del dispositivo.

- **Tiempos de mantenimiento programados** - Esta caja muestra todos los tiempos de mantenimiento programados para el dispositivo.

    - Pulsar Add para programar un nuevo tiempo de mantenimiento para el dispositivo.
    - Seleccionar una entrada y pulsar Edit para cambiar un tiempo programado.
    - Seleccionar una entrada y pulsar Delete para borrar un tiempo programado de la lista.

IV.3.5 Menú

Una vez que un nuevo artículo de menú ha sido configurado, aparece sobre el menú cuando se pulsa el botón derecho del ratón sobre ese dispositivo en la lista de dispositivo. Cuando se selecciona el artículo de menú, el comando asociado es iniciado con los argumentos que han sido introducidos en su configuración.

Los cambios que se pueden hacer sobre el Menú son:

- Add para añadir un nuevo artículo de menú.
- Seleccionar un artículo y pulsar Edit para cambiar los ajustes.
- Seleccionar un artículo y pulsar Delete para quitarlo de la lista.

IV.3.6 Atributos

Los cambios que se pueden hacer sobre los Atributos son:

- Add para crear un nuevo atributo para el dispositivo.
- Seleccionar un atributo existente y pulsar Edit para cambiar el atributo.
- Seleccionar un atributo existente y pulsar Delete para quitar el atributo del dispositivo.

IV.4 CONFIGURACIÓN DE REPORTES

IV.4.1 Colectar Datos Estadísticos

Por defecto, la estadística de funcionamiento no es guardada para los monitores asignados a los dispositivos en la base de datos. Cuando se ve un informe para estos monitores, se verá la frase siguiente en el gráfico de funcionamiento, como se muestra en la figura IV.7:

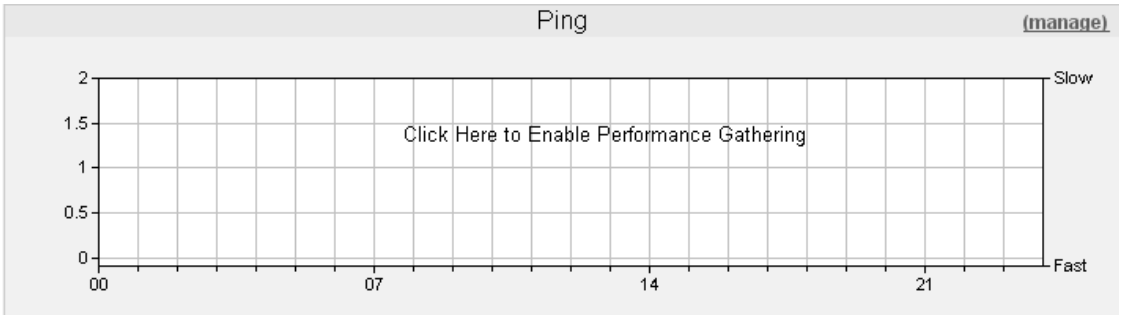


Figura IV.7 Gráfico de funcionamiento

Hay **dos modos** de comenzar a recoger estos datos, y son:

1. Dar clic sobre el link en el centro del gráfico de funcionamiento para acceder a la página de Configure Statistics Gathering. Seleccionar la opción que más se ajuste a las necesidades.

   Si se selecciona Inherit from device setitings, se debe regresar a reunirlos en Propiedades de Dispositivo.

2. Acceder a Device Properties>Polling para el dispositivo sobre el cual usted quiere comenzar a reunir datos estadísticos.

   Seleccionar la opción Collect Active Monitor Statistical data for reports. Esto regresa la reunión sobre todos los monitores asociados a este dispositivo.

IV.4.2 Reportes Recurrentes

Los cambios que se pueden hacer sobre los Reportes Recurrentes son:

- Dar clic en New para crear un nuevo reporte recurrente.
- Seleccionar una entrada y dar clic en Edit para hacer cambios a la entrada.
- Seleccionar una entrada y dar clic en Copy para crear una copia de esa entrada. Se puede entonces editar la nueva copia como sea necesario.
- Dar clic en Delete para remover un reporte recurrente.
- Seleccionar una entrada y dar clic en Test para probar el reporte recurrente.

IV.5 CONFIGURACIÓN DE DISPOSITIVOS

IV.5.1 Añadir un Solo Dispositivo

Cuando se añade manualmente un dispositivo seleccionando New Device en el menú al presionar el botón derecho del ratón, se pone el cursor para dar la dirección IP. Dar clic en Advanced para seleccionar los Monitores Activos para ser usados en el proceso de escaneo.

Una vez que se da clic en OK sobre el diálogo Add New Device, WhatsUp Professional tratará de resolver la dirección IP, entonces escanea ese dispositivo para Monitores Activos. Cuando el escaneo está completo, propiedades del dispositivo aparece, permitiendo configurar el dispositivo como sea necesario.

Los pasos a seguir son:

1. Dar <CTRL+N> o clic derecho sobre la vista de mapa y seleccionar New>New Device.

2. El diálogo Add New Device aparece. Escribir la dirección IP para el dispositivo dentro de la caja.

3. Si se da clic en el boton Advanced, el diálogo Select Active Monitor Scan Properties aparece. Si se desea seleccionar uno o más, dar clic en OK y regresar al diálogo Add New Device. Dar clic en OK. Si el dispositivo ya existe en otro grupo, se tendrá un mensaje para tal efecto.

4. El diálogo propiedades del dispositivo aparece. Se puede o no aceptar las propiedades pobladas por defecto cuando se añade el dispositivo o se modifica usando este diálogo. Si se acepta, dar clic en OK.

5. Cuando se da clic en OK, el icono del nuevo dispositivo aparece en la Vista de Mapa.

IV.6 DESINSTALACIÓN DE WHATSUP PROFESSIONAL

Para desinstalar WhatsUp Professional, pulsar Inicio>Ajustes>Panel de control, luego seleccionar Añadir o Quitar Programas. Seleccionar Ipswitch WhatsUp Professional, luego seleccionar Quitar cuando esté señalado.

También se puede correr el ejecutable de Ipswitch WhatsUp Professional y seleccionar Delete.

IV.7 PRUEBAS Y GRÁFICAS DE WHATSUP PROFESSIONAL

La tabla IV.1 muestra los diferentes iconos con sus colores utilizados para cada cambio de estado.

Icono	Estado
	UP por menos de 2 minutos
	UP por más de 2 minutos
	DOWN por menos de 2 minutos
	DOWN por más de 2 minutos
	DOWN por más de 5 minutos
	DOWN por más de 20 minutos
	En estado de mantenimiento
	No reconocida

Tabla IV.1 Iconos de cambio de estado

Como primera prueba se mantuvieron todas las máquinas de la red en **estado UP**; esto significa que el color de su icono está en **verde**.

Debido a que algunas de las máquinas del laboratorio estaban en **mantenimiento** presentan un icono en forma circular en color **naranja** y una máquina con icono triangular en color **gris** representa una máquina **no reconocida**.

La figura IV.8 muestra esta prueba.

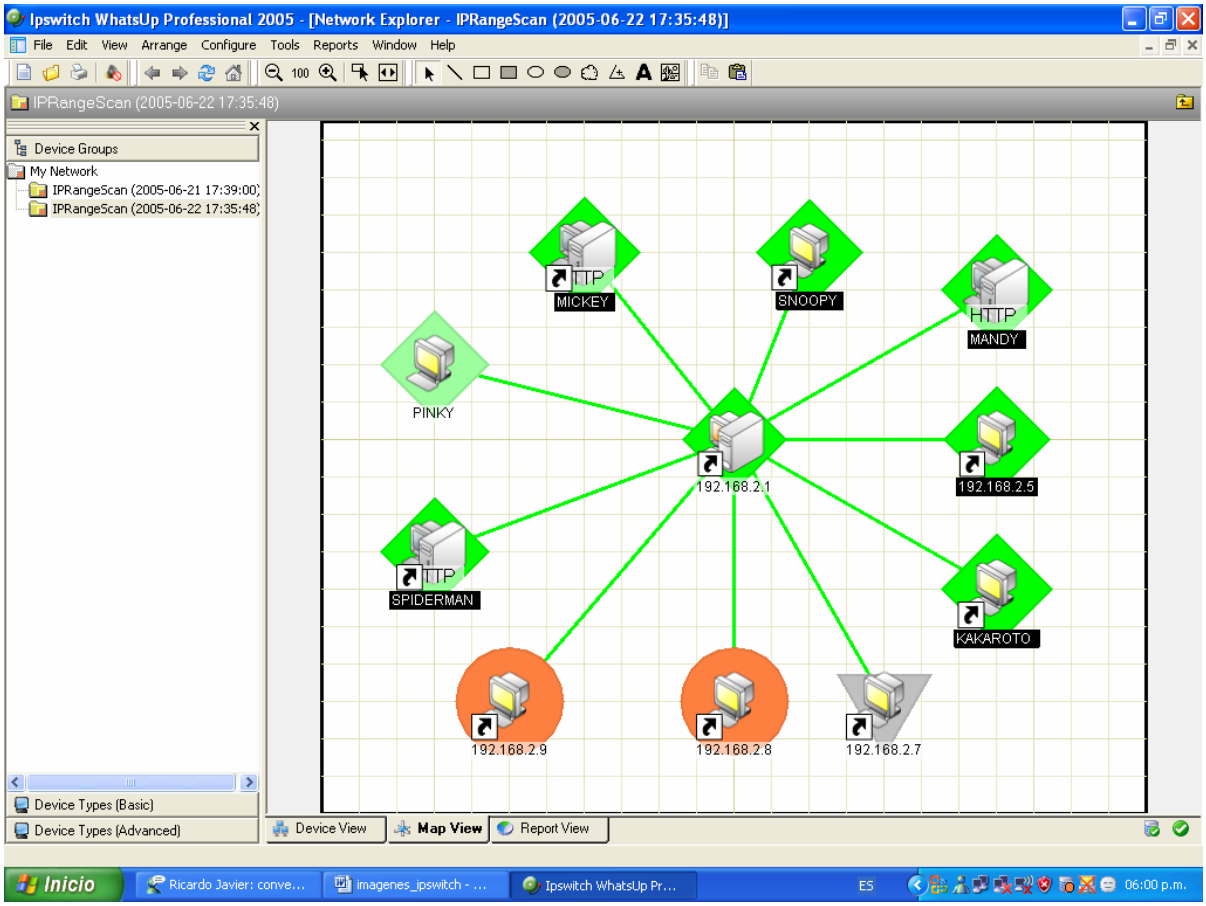


Figura IV.8 Representación de las máquinas en estado UP

En la siguiente prueba se visualiza como van cambiando los iconos de las máquinas cuando éstas van pasando de un estado a otro dependiendo del tiempo de inactividad.

En este ejemplo observamos que las máquinas Spiderman, Mickey y Kakaroto permanecen en **estado UP**, esto quiere decir que están conectadas a la red.

La máquina Pinky ha estado durante 2 minutos o menos en estado inactivo; la máquina 9 nos indica que su estado de inactividad ha sido de entre 2 y 5 minutos. Snoopy y la máquina 5 han estado más de 5 minutos en **estado DOWN**, mientras que Mandy ha permanecido DOWN por más de 20 minutos.

Como se mencionó en la figura anterior la máquina 7 sigue sin ser reconocida y la máquina 8 continúa en mantenimiento.

La figura IV.9 representa estos estados en la opción de **Vista del Mapa**. Y la figura IV.10 muestra estos mismos estados en la opción **Vista del Dispositivo**.

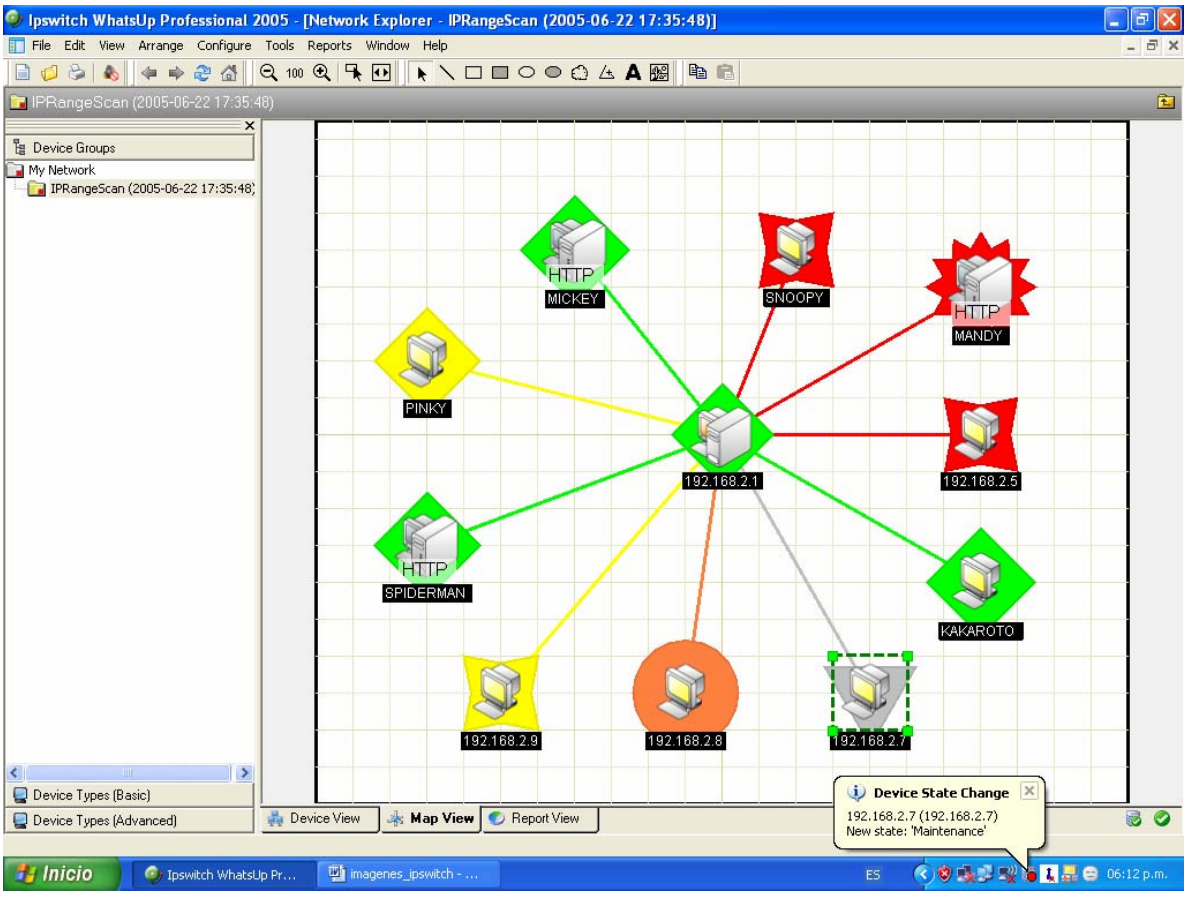


Figura IV.9 Representación de los diferentes estados de inactividad

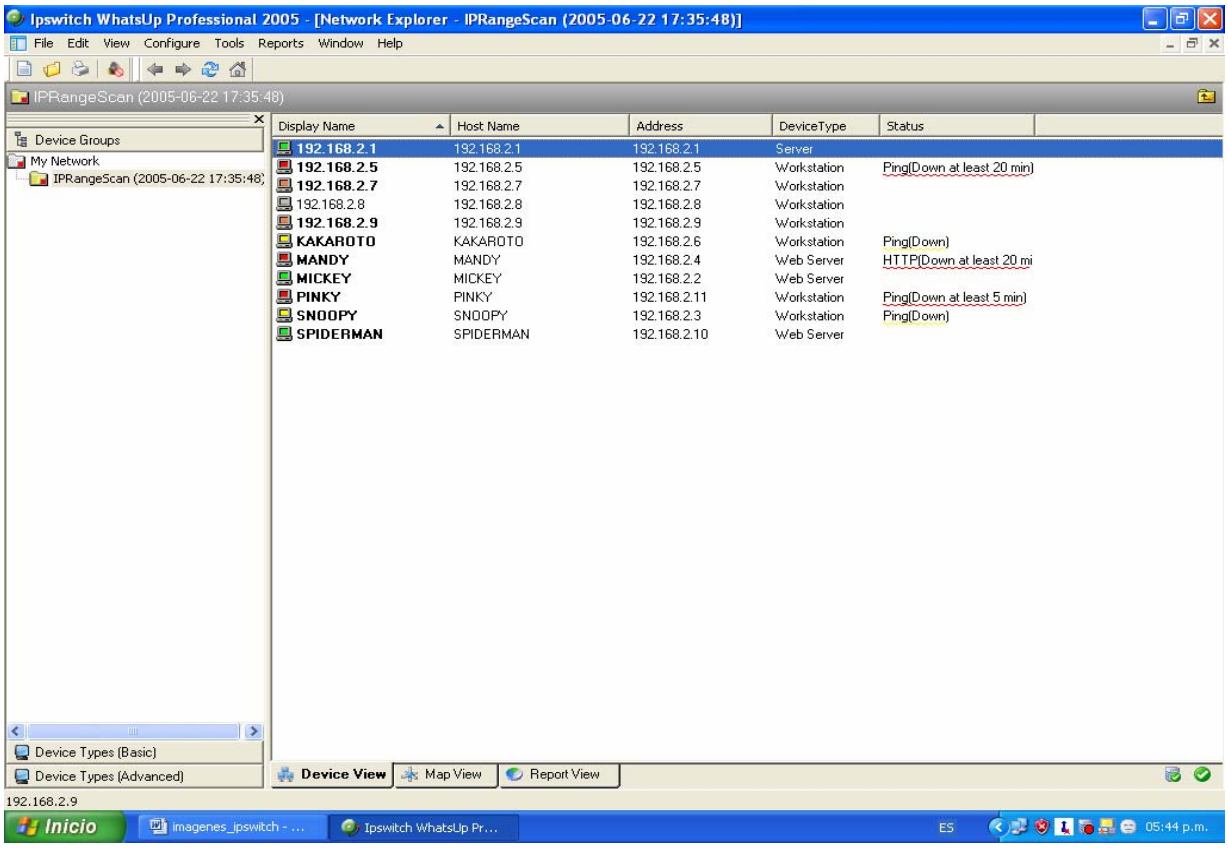


Figura IV.10 Vista del dispositivo

La prueba siguiente es una vista de los **mensajes** que WhatsUp Professional manda cada vez que un dispositivo cambia su estado. Para este caso el mensaje está avisando que el nuevo estado de Kakaroto es DOWN por más de 5 minutos. La figura IV.11 muestra esta prueba. Y la figura IV.12 es una vista más cercana de este mensaje.

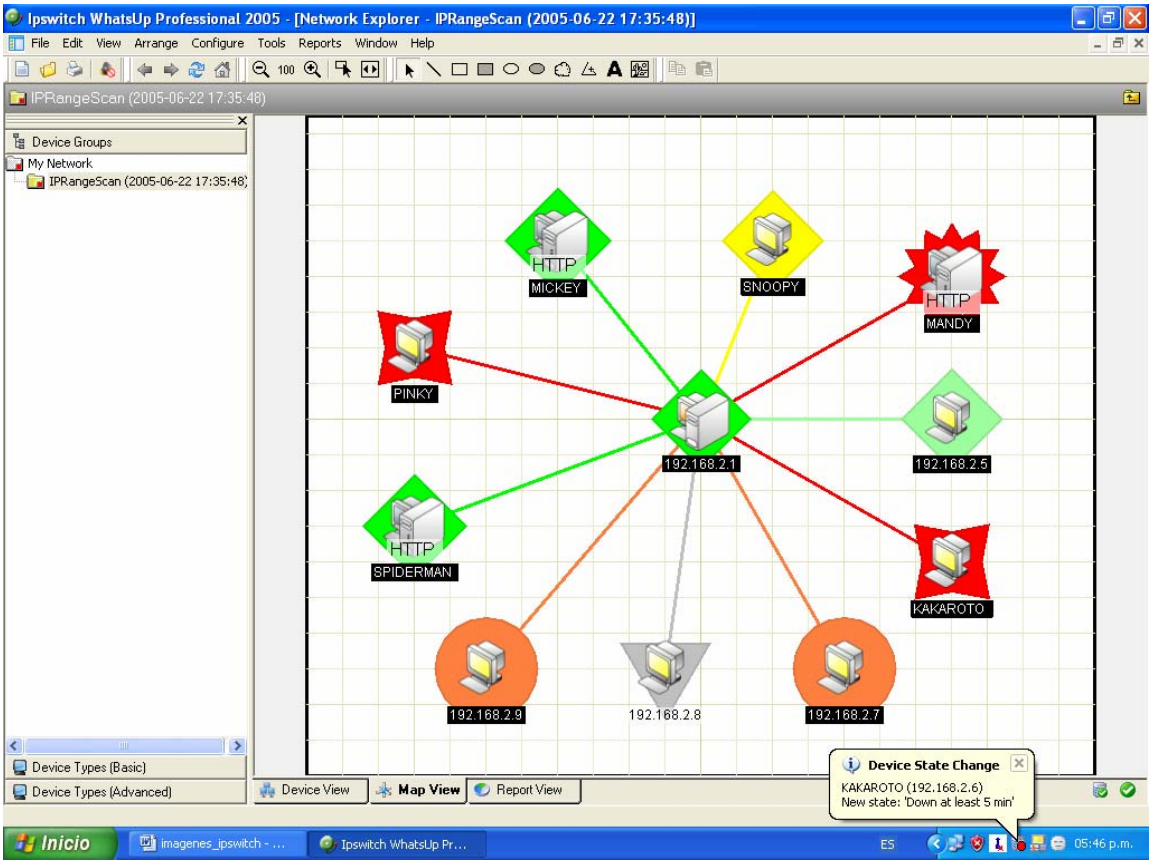


Figura IV.11 Mensaje de cambio de estado

Figura IV.12 Vista cercana del mensaje

En la **Vista de Reporte** se proporciona un resumen de todo el **grupo de dispositivos** en la que se observa el número de dispositivos que están en cada uno de los estados antes mencionados (Figura IV.13).

Más abajo se muestra el estado de los dispositivos, el dispositivo y sus monitores activos.

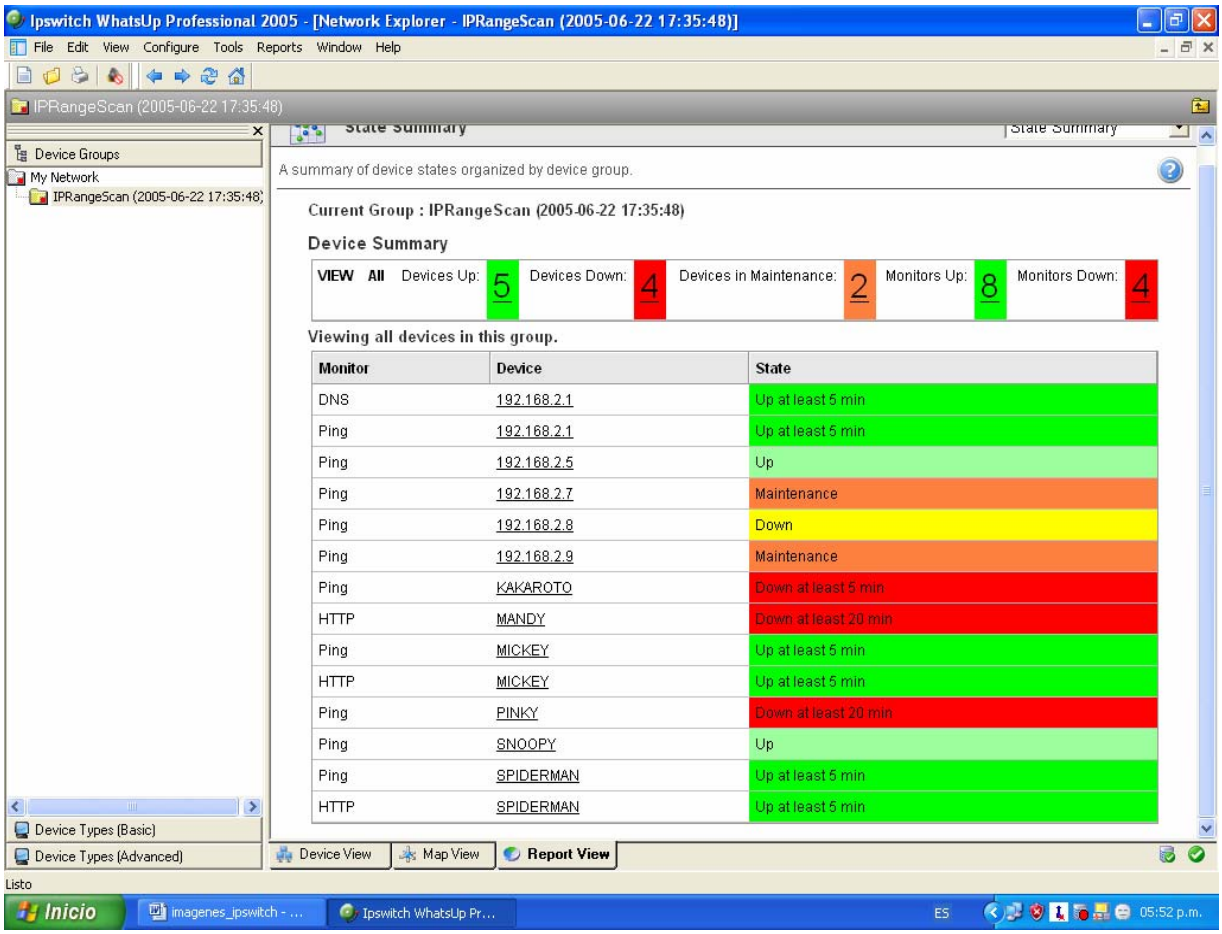


Figura IV.13 Resumen del grupo de dispositivos

Otro tipo de reportes es el historial de cambio de estado (Figura IV.14).

En este se muestra una historia por fecha para un grupo de dispositivos donde se indica el cambio de estado que han tenido los dispositivos y la duración de dicho estado.

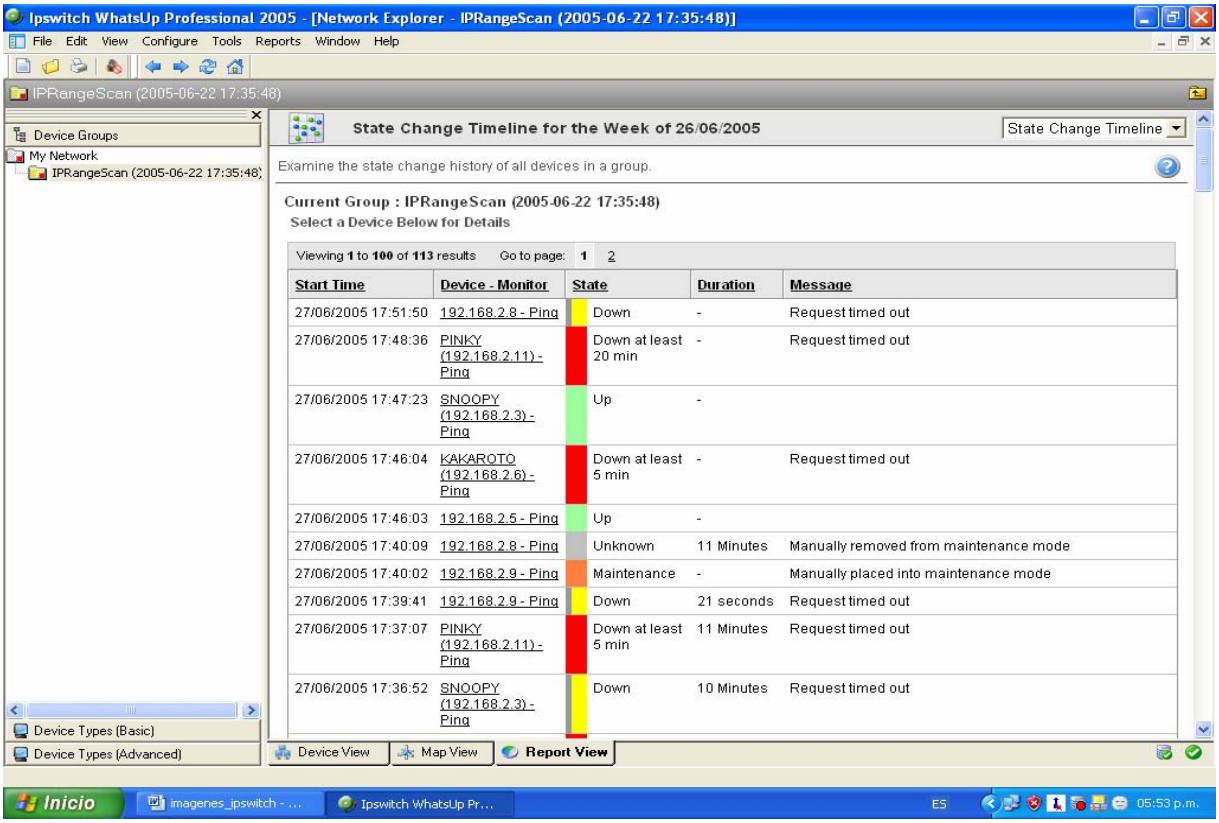


Figura IV.14 Historial de cambio de estado

Otro tipo de reportes que WhatsUp proporciona es el de registro de actividad. En este reporte se presenta una historia de la configuración del sistema y los mensajes de inicio de aplicación generados por WhatsUp (Figura IV.15).

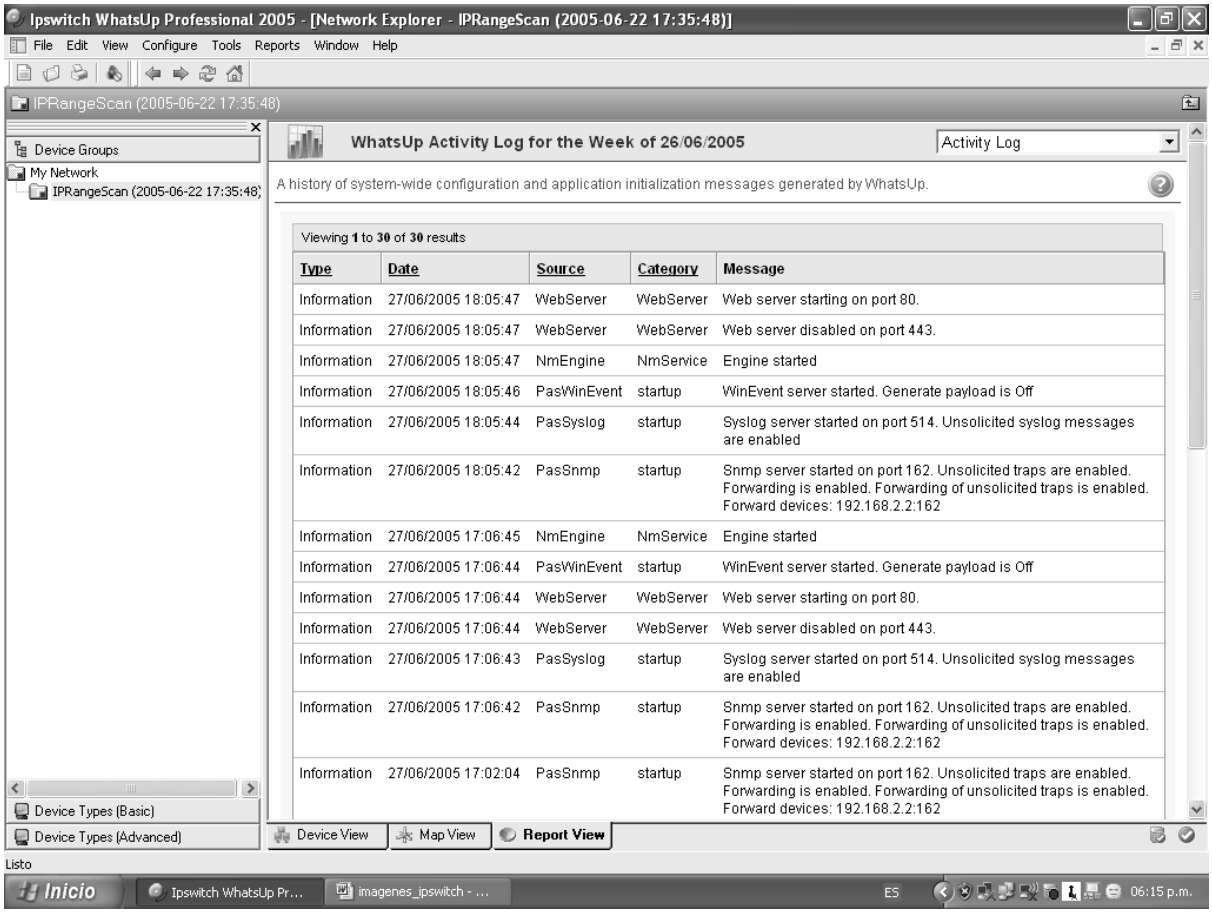
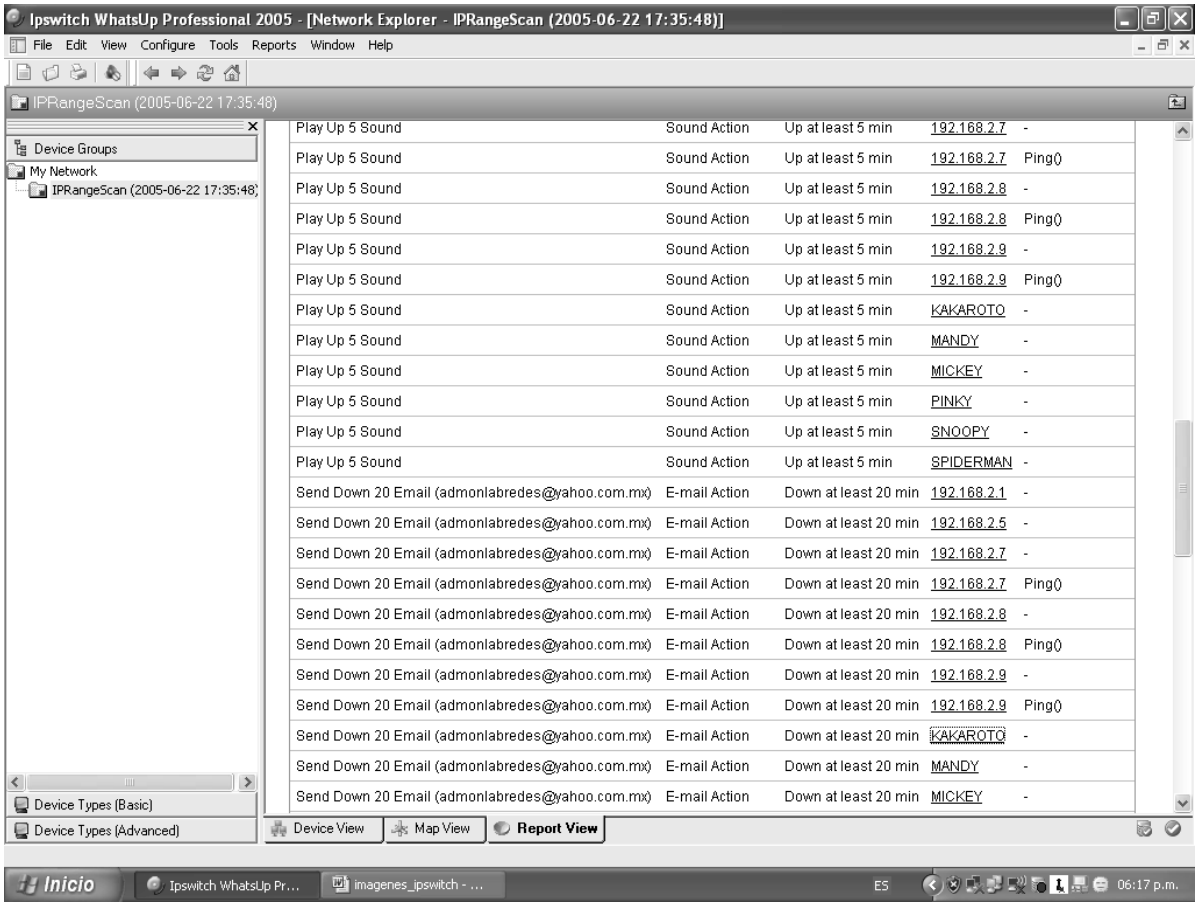


Figura IV.15 Pantalla de registro de actividad

WhatsUp Professional cuenta también con un servicio de reportes de las acciones que lleva a cabo para cada máquina para informar al administrador cuando un dispositivo cambia de estado (Figura IV.16). Dichas acciones son las que se decidió configurar previamente.



Play Up 5 Sound	Sound Action	Up at least 5 min	192.168.2.7	-
Play Up 5 Sound	Sound Action	Up at least 5 min	192.168.2.7	Ping()
Play Up 5 Sound	Sound Action	Up at least 5 min	192.168.2.8	-
Play Up 5 Sound	Sound Action	Up at least 5 min	192.168.2.8	Ping()
Play Up 5 Sound	Sound Action	Up at least 5 min	192.168.2.9	-
Play Up 5 Sound	Sound Action	Up at least 5 min	192.168.2.9	Ping()
Play Up 5 Sound	Sound Action	Up at least 5 min	KAKAROTO	-
Play Up 5 Sound	Sound Action	Up at least 5 min	MANDY	-
Play Up 5 Sound	Sound Action	Up at least 5 min	MICKEY	-
Play Up 5 Sound	Sound Action	Up at least 5 min	PINKY	-
Play Up 5 Sound	Sound Action	Up at least 5 min	SNOOPY	-
Play Up 5 Sound	Sound Action	Up at least 5 min	SPIDERMAN	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.1	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.5	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.7	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.7	Ping()
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.8	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.8	Ping()
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.9	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	192.168.2.9	Ping()
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	KAKAROTO	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	MANDY	-
Send Down 20 Email (admonlabredes@yahoo.com.mx)	E-mail Action	Down at least 20 min	MICKEY	-

Figura IV.16 Reporte de acciones

Una vista detallada de la disponibilidad de cada dispositivo es mostrada en la figura IV.17, en la cual se muestra una gráfica de tiempo contra disponibilidad de los monitores activos de un dispositivo. En esta vista se puede apreciar el tiempo que un monitor a permanecido UP, DOWN o en mantenimiento y los diferentes cambios de estado que ha tenido.

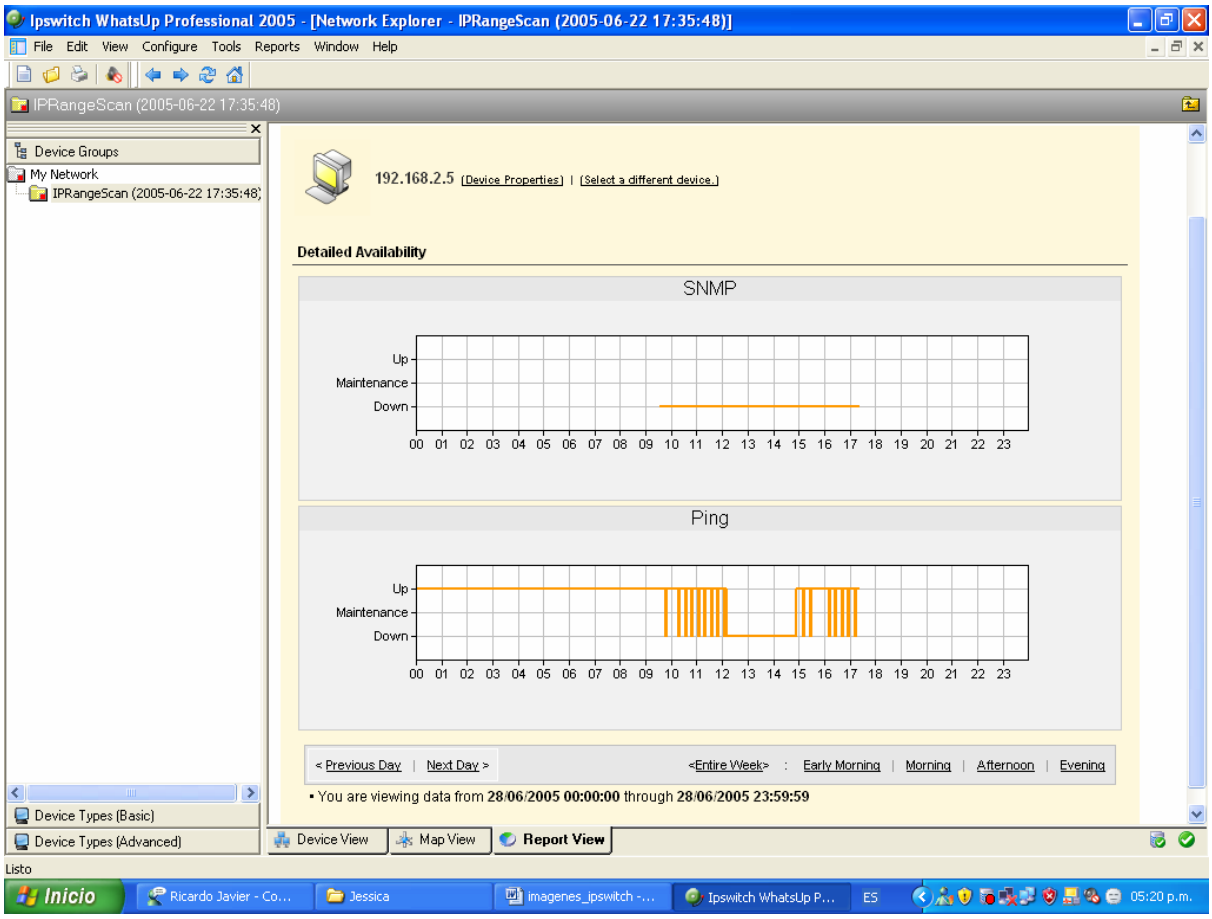


Figura IV.17 Disponibilidad detallada de un dispositivo

Estas son solo algunas de las vistas y pruebas que se pueden obtener por medio de WhatsUp Professional. Se cuentan con muchas otras vistas las cuales por ser muy semejantes a las mostradas aquí no se incluyeron en este trabajo; ya que aquí solo se pretende ejemplificar los aspectos más importantes de la administración de redes por medio de SNMP y WhatsUp Professional.

CONCLUSIONES

"La confianza en sí mismo
es el primer secreto del éxito".

Actualmente las redes de computadoras son accesadas por muchas personas, con intereses y grados de libertad diferentes. Debido a lo anterior, las redes han crecido mucho y paralelamente ha aumentado la necesidad de una buena administración y una gran seguridad en la operación de los sistemas y la información que son manipulados mediante dichas redes.

Para ello ha sido de gran utilidad el uso de herramientas que permiten realizar de forma centralizada la administración de múltiples redes y protocolos.

En este trabajo se realizó una investigación bibliográfica detallada sobre los Sistemas de Administración Informáticos, centrada fundamentalmente en su operación, con dependencia en su naturaleza y la de sus componentes.

El principal resultado de este trabajo ha sido la instalación de un sistema de administración que se adecua al Laboratorio de Redes y Seguridad, facilitando la administración y mantenimiento de los distintos servicios y aplicaciones ofrecidos por el laboratorio para los alumnos de la Facultad de Ingeniería.

La aportación consistió en la implementación de un Sistema de Administración de Red, que se adapta a las características del hardware y del software con que cuenta dicho laboratorio, con el fin de mantener en estado óptimo los servicios, aplicaciones y equipos con que cuenta.

Por lo que se cumplió con el objetivo principal de la Administración de Red, que es mantener la funcionalidad y disponibilidad de la red, satisfaciendo las necesidades de los usuarios.

El Sistema de Administración sirve como administrador de la red del laboratorio y a la vez como ejemplo de aplicación para los alumnos que realizarán prácticas en éste, por lo que se propone incluir su instalación como parte del temario de prácticas de la asignatura Administración de Redes, ya que mediante el empleo de éste, los alumnos se familiarizarán con el manejo de los Sistemas de Administración de Redes y colaborarán a que el laboratorio se encuentre permanentemente administrado.

En cuanto al programa WhatsUp Professional, que se utilizó para monitorear el laboratorio, se llegó a la conclusión de que aunque es un programa en apariencia sencillo, que no proporciona todas las características que los otros sistemas analizados en este trabajo, se consideró como el sistema idóneo para las características del laboratorio, debido a que está empezando su funcionamiento teniendo algunas limitaciones en cuanto a hardware.

Debido a lo mencionado anteriormente, se requirió instalar un programa cuyos requerimientos no fueran tan extensos y que fueran cubiertos por las computadoras del laboratorio; al analizar algunos otros sistemas, los requerimientos eran demasiado elevados comparados con los recursos con los que se contaba.

Es por ello que WhatsUp Professional en adición con SNMP fueron las herramientas más adecuadas a los recursos con los que se cuenta cubriendo las necesidades de monitoreo que tiene el laboratorio.

Además los otros sistemas estudiados, eran principalmente para monitoreo de redes de gran tamaño, por ello sus requerimientos resultaban imposibles de cubrir ya que la red del laboratorio con que se cuenta es muy pequeña y los recursos que se necesitan cubrir no son tantos, WhatsUp Professional logra satisfacer las necesidades de administración actuales.

Los otros sistemas estudiados pertenecen a compañías que además de ser proveedoras de software, lo son de su propia marca de hardware, por lo tanto, sus sistemas de administración están diseñados para reconocer solamente equipos de su propia marca y el laboratorio cuenta con máquinas de diferentes marcas y características.

WhatsUp Professional y SNMP son dos sistemas adecuados al uso de redes de pequeña y gran escala.Previniendo el futuro crecimiento de la red del laboratorio, algunas de las ventajas de monitorear la red por medio de WhatsUp Professional y SNMP son:

- ✓ Permiten la interoperabilidad
- ✓ Pueden ser implementados y adecuados a cualquier tipo de red
- ✓ Pueden monitorearse cualquier número de dispositivos
- ✓ Pueden migrar fácilmente a nuevas versiones
- ✓ Pueden utilizarse para servir como una herramienta tanto de práctica como de enseñanza para los alumnos de la Facultad

Para finalizar, el tema de administración de redes es muy amplio; por lo que este trabajo es solo una parte de las medidas preventivas que se pueden llevar a cabo para que una red y un centro de cómputo, en nuestro caso, la red y el Laboratorio de Redes y Seguridad de la Facultad de Ingeniería se mantengan en excelentes condiciones, ayudando a que su operabilidad y disponibilidad se vean lo menos afectadas posible.

APÉNDICES

"No hay delito mayor que la audacia de destacar".

APÉNDICE A

ASN.1
Notación de Sintaxis Abstracta Uno

La Notación de Sintaxis Abstracta Uno (**ASN.1**) proporciona un modo estándar de representar datos que viajan a través de Internet, red inteligente, comercio electrónico, servicios electrónicos de seguridad, voz sobre IP y otros.

Esta estandarización es necesaria porque los datos pueden ser representados de modos incompatibles dentro de diferentes dispositivos de computación de red. ASN.1 es usado para describir el formato de cómo **mensajes SNMP** pueden ser enviados entre los agentes y los administradores de red.

A.1 Historia

ASN.1 primero fue estandarizado en 1984 por el **CCITT** (**C**omité de **C**onsultoría **I**nternacional para **T**elefonía y **T**elegrafía, ahora llamado **ITU-T**, Unión Internacional de Telecomunicaciones –Sector de Estandarización de Telecomunicaciones) bajo el nombre "Recomendación X.409".

Un poco más tarde, **ISO** (Organización Internacional para la Estandarización) decidió adoptar esta notación y dividir esta recomendación en dos documentos separados: la sintaxis abstracta (ASN.1) y las reglas de codificación (**BER**).

En 1987, ISO publicó estos documentos como el 8824 y el 8825. En 1988, ISO se combinó con el **IEC** (Comisión Internacional Electrotécnica) para la formación de un comité conjunto técnico llamado **ISO/IEC JTC 1**, que es ahora responsable de la norma ASN.1.

Para el *Libro Azul*, en 1989, el CCITT publicó las recomendaciones X.208 y X.209, una nueva publicación para la norma ASN.1, que fue provista de extensiones que son resultado de un trabajo común con el JTC 1.

En abril de 1999, una nueva norma llamada ASN.1:1997 fue publicada, con modificaciones principalmente en la editorial e integración de las correcciones técnicas

que se emitieron entre 1994 y 1997. El Comité ASN.1 estuvo trabajando sobre una nueva publicación de la norma que fue publicada en 2002.

En términos del Modelo de Referencia **OSI**, ASN.1 se sitúa en la capa seis, la capa de presentación, para proveer las transformaciones de datos básicas necesarias para las aplicaciones para comunicarse correctamente.

A.2 Componentes Principales

El concepto de módulo de ASN.1 es usado en todas partes de SNMP para organizar objetos de ASN.1. Un módulo en ASN.1 es una colección de descripciones relacionadas. Estas descripciones pueden referirse al SMI, al protocolo o a muchos grupos de objetos de MIB.

Hay **tres componentes** principales de ASN.1 de interés para SNMP:

1. **Tipo de notación** para definir tipos de datos de objetos administrados.
2. **Valor de notación** para definir valores de tipo de datos o instancias.
3. **Sintaxis de transferencia** para transmitir y recibir mensajes ASN.1 codificados.

El tipo de notación y el valor de notación distribuyen con la sintaxis ASN.1 definiciones y valores. La sintaxis de transferencia es un tópico especial que es definido según las Reglas de Codificación Básicas. BER es una aplicación de las reglas de ASN.1.

Uno de los motivos principales para el éxito de ASN.1 es que esta notación está asociada con varias reglas de codificación estandarizadas, como el BER (Reglas de Codificación Básicas) o más recientemente el **PER** (Reglas de Codificación Empaquetadas), que provee útiles aplicaciones que sufren restricciones en términos de banda ancha.

Estas reglas de codificación describen como los valores definidos en ASN.1 deberían ser codificados para la transmisión, independientemente de la máquina, el lenguaje de programación o como es representado en un programa de aplicación.

Las codificaciones de ASN.1 son más modernizadas que muchas notaciones que compiten, permitiendo la transmisión rápida y confiable de mensajes extensos. Como ASN.1 ha sido una norma internacional desde 1984, sus reglas de codificación son maduras y tienen un registro de trayectoria largo de confiabilidad e interoperabilidad.

APÉNDICE B

BER
REGLAS DE CODIFICACIÓN BÁSICA

Cómo la sintaxis es codificada en octectos y transferida sobre la interred, es especificado en la **Norma ISO 8825**, especificación de Reglas de Codificación Básicas para la Notación de Sintaxis Abstracta Uno (**ASN.1**).

Las Reglas de Codificación Básicas (**BER**) son un algoritmo que toma los valores de ASN.1 y codifica los bits en el formato de octecto apropiado para la transmisión sobre la interred.

El BER especifica que el bit más significativo es el BIT 8 y el bit menos significativo es el BIT 1. EL BIT 8 es el primer bit presentado en la red. Es también significativo que los enteros que pueden ser negativos o positivos son representados usando la notación de complemento a dos. Para números enteros no negativos, una representación no signada también puede ser usada para representar arbitrariamente números positivos grandes.

APÉNDICE C

CCITT
Comité de Consultoría Internacional para Telefonía y Telegrafía

El **CCITT** es un comité de la Unión de Telecomunicaciones Internacional (**ITU**), que es una organización de tratado de Naciones Unidas. Por consiguiente, los miembros del CCITT son gobiernos. El reglamento del CCITT es "estudiar y emitir recomendaciones sobre técnica, funcionamiento y tarifar preguntas relacionadas con la telegrafía y la telefonía".

Su **objetivo** primario es estandarizar, al grado necesario, técnicas y operaciones en telecomunicaciones para alcanzar la compatibilidad de punta a punta de conexiones de telecomunicación internacionales, independientemente de los países de procedencia y destino.

El CCITT está organizado en 15 grupos de estudio que preparan normas, llamadas recomendaciones por el CCITT.

El trabajo dentro del CCITT es conducido en ciclos de cuatro años. Cada cuatro años, es sostenida una asamblea plenaria. El programa de trabajo para los próximos cuatro años es establecido en la asamblea en forma de peticiones sometidas por varios grupos de estudio, basados en requerimientos hechos a dichos grupos por sus miembros. La asamblea evalúa las peticiones, repasa el alcance de los grupos de estudio, crea nuevos grupos de estudio o suprime existentes y les asigna peticiones.

Basado en estas peticiones, cada grupo de estudio prepara recomendaciones preliminares. La técnica tradicional es someter todas las recomendaciones propuestas a la siguiente asamblea, cuatro años por consiguiente. Una recomendación es aprobada si obtiene mayoría de votos. Todas las recomendaciones aprobadas, son publicadas como un paquete de "libros" una vez cada cuatro años.

APÉNDICE D

IEC
Comisión Internacional Electrotécnica

El **IEC**, como **ISO**, es una organización voluntaria compuesta de miembros nacionales. El IEC se enfoca en los aspectos técnicos de electricidad.

Cada miembro es supuesto para representar todos los intereses eléctricos dentro de su país, incluyendo a usuarios, fabricantes, asociaciones comerciales, gobierno y asociaciones académicas.

Frecuentemente, el representante de un país al IEC es el mismo que su representante a ISO.

Los procedimientos para la adopción de nuevas normas son similares a los de ISO.

APÉNDICE E

ISO
Organización Internacional de Estándares

La **ISO** es una agencia internacional para el desarrollo de normas sobre una amplia gama de temas. Es un sólo órgano, la organización de no tratado cuyos miembros son los cuerpos de normas designados de naciones participantes, más organizaciones de observadores sin derecho de voto.

Aunque ISO no sea un cuerpo gubernamental, más del 70 por ciento de miembros de ISO son instituciones de normas gubernamentales u organizaciones incorporadas por la ley pública. El miembro estadounidense es el Instituto de Normas Americano Nacional (ANSI).

ISO fue fundada en 1946 y ha emitido más de 7,000 normas en una amplia gama de áreas. Su objetivo es el de promover el desarrollo de estandarización y actividades relacionadas para facilitar el cambio internacional de bienes y servicios y desarrollar la cooperación en la esfera de actividad intelectual, científica, tecnológica y económica.

Un área importante de estandarización trata con las interconexiones de sistemas abiertos (**OSI**), la arquitectura de comunicaciones y las normas en cada capa de la arquitectura OSI.

El desarrollo de una norma ISO desde la primera propuesta hasta la publicación real de la norma sigue un proceso de siete pasos. El **objetivo** es asegurar que el resultado final sea aceptable para tantos países como sea posible. Los pasos son brevemente descritos en la siguiente lista.

1. Un nuevo artículo de trabajo es asignado al comité apropiado técnico y dentro de ese comité técnico, al grupo de trabajo apropiado. El grupo de trabajo prepara las especificaciones técnicas para la norma propuesta y publica estos como un *proyecto del comité* (CD). El CD es difundido entre miembros interesados para la votación y

el comentario técnico. Al menos tres meses son permitidos y puede haber iteraciones. Cuando hay acuerdo sustancial, el CD es enviado al brazo administrativo de ISO, conocido como la Secretaría Central.

2. El CD es registrado en la Secretaría Central dos meses antes de su aprobación final por el comité técnico.

3. La Secretaría Central corrige el documento para asegurar la conformidad con prácticas de ISO; ningunos cambios técnicos son hechos. El documento corregido entonces es emitido como una *Norma Preliminar Internacional* (DIS).

4. La DIS es circulada por un período de votación de seis meses. Para hacerse una norma final, la DIS debe recibir una aprobación mayoritaria de los miembros del comité técnico y la aprobación del 75 por ciento de todos los miembros de votación. Las revisiones pueden ser hechas para resolver cualquier voto negativo. Si más de dos votos negativos permanecen, es improbable que la DIS sea publicada como una norma final.

5. La aprobada, posiblemente revisada DIS, es devuelta dentro de tres meses a la Secretaría Central para la sumisión al Consejo ISO, que actúa como la junta directiva de ISO.

6. La DIS es aceptada por el consejo como una *Norma Internacional* (IS).

7. La IS es publicada por ISO.

Dentro de los campos de comunicaciones de datos y procesamiento de información, tradicionalmente hubo una división entre los intereses del **CCITT** y de ISO.

El CCITT principalmente ha estado preocupado con emisiones de red de comunicación y transmisión de datos. Aproximadamente, estos ocupan las tres capas inferiores de la arquitectura ISO.

ISO tradicionalmente ha estado preocupada con las emisiones de procesamiento distribuido y comunicaciones de computadora, que corresponden aproximadamente a las capas 4 a 7.

APÉNDICE F

JTC 1
Comité Conjunto Técnico 1

Tal como hay una superposición creciente entre los intereses de telecomunicaciones del **CCITT** y los intereses de tecnología de información de **ISO**, hay una superposición creciente entre los intereses de ISO y los de **IEC**.

En consecuencia en 1987, ISO e IEC formaron un Comité Conjunto Técnico contra la tecnología de información. **JTC 1** combina el trabajo del Comité Técnico ISO 97 sobre sistemas de procesamiento de información con el comité técnico IEC relacionado.

Las normas resultantes de JTC 1 llevan el doble logo de ISO e IEC y son publicadas según los procedimientos descritos antes en el apéndice para ISO. Todas las normas OSI relacionadas emitidas por ISO ahora son publicadas por el JTC 1.

APÉNDICE G

OSI
INTERCONEXIÓN DE SISTEMAS ABIERTOS

El **objetivo** del esfuerzo **OSI** es definir un conjunto de normas que habilitarán los sistemas abiertos localizados en todas partes del mundo para cooperar interconectándose a través de algunas facilidades de comunicaciones estandarizadas y ejecutando protocolos OSI estandarizados.

La interconexión de sistemas abiertos está basada en el concepto de cooperación de aplicaciones distribuidas. En el **modelo OSI**, un sistema consiste en una computadora, todo su software y cualquier dispositivo periférico conectado a ella, incluyendo terminales.

Una aplicación distribuida es cualquier actividad que implica el cambio de información entre dos sistemas abiertos.

G.1 El Modelo OSI

Una técnica de estructuración extensamente aceptada y el escogido por OSI, es la basada en **capas**. Las funciones de comunicaciones son divididas en un conjunto jerárquico de capas. Cada capa realiza un subconjunto relacionado de las funciones requeridas para comunicarse con otro sistema.

Esto proporciona servicios a la siguiente capa más alta y confía en la siguiente capa más abajo tanto para realizar funciones más primitivas como para ocultar los detalles de esas funciones. Idealmente, las capas deberían ser definidas de modo que los cambios de una capa no requieran cambios en las otras capas.

La Figura G.1 ilustra la arquitectura OSI.

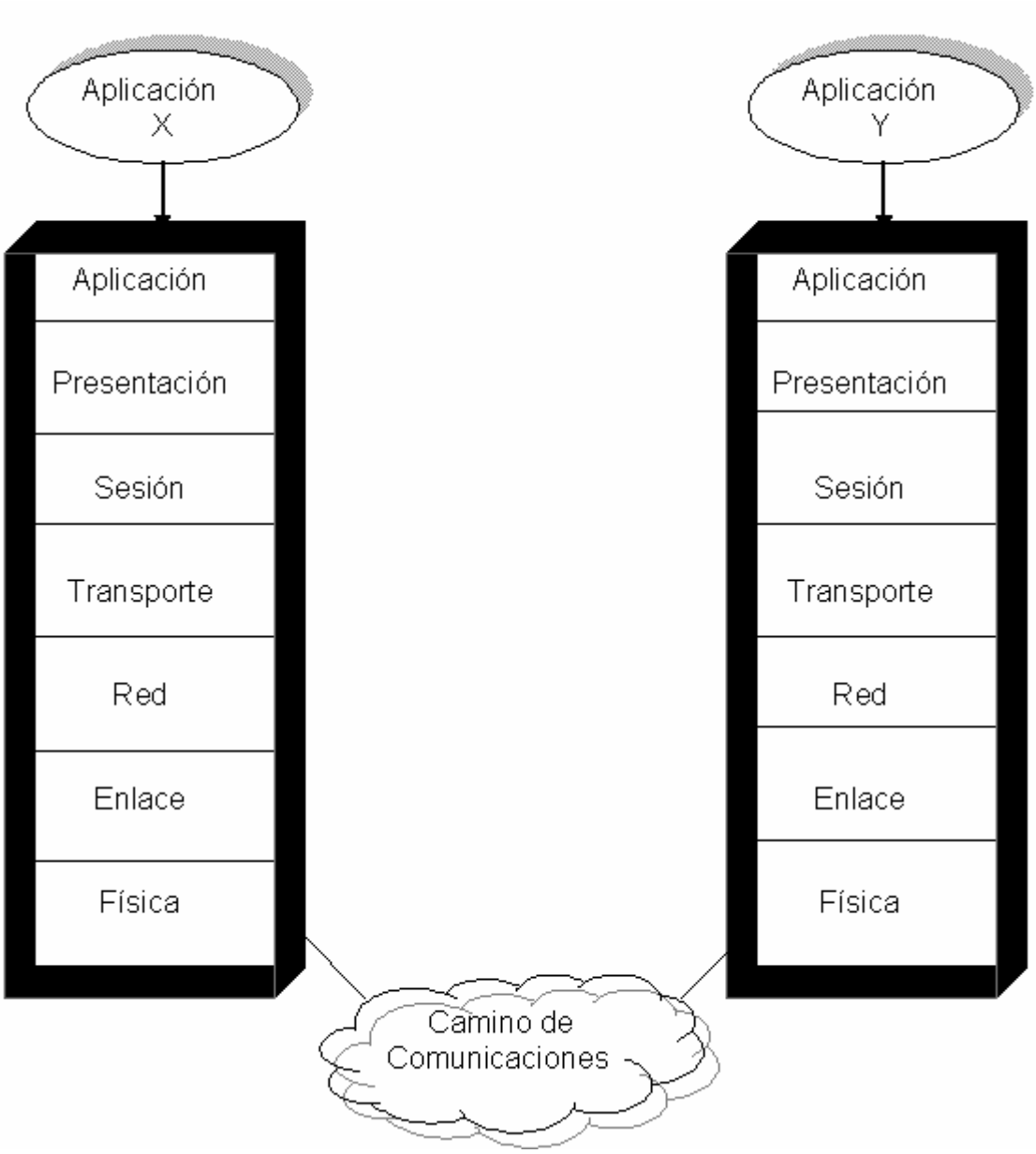


Figura G.1 Arquitectura OSI

Cada sistema contiene las **siete capas**. La comunicación es entre las aplicaciones en las dos computadoras, la aplicación etiquetada X y la aplicación Y en la figura. Si la aplicación X desea enviar un mensaje a la aplicación Y, esta invoca a la capa de aplicación (capa 7).

La capa 7 establece una relación par con la capa 7 de la computadora objeto, usando un protocolo capa 7 (protocolo de aplicación). Este protocolo requiere servicios de la capa 6, para que las dos entidades capa 6 usen su propio protocolo y así sucesivamente baje a la capa física, que realmente transmite bits sobre un medio de transmisión. Note que no hay ninguna comunicación directa entre las capas par excepto en la capa física.

G.2 Las Capas OSI

El modelo final de OSI consta de 7 capas, las cuales se explican brevemente a continuación.

G.2.1 Capa Física

La **capa física** cubre la interfaz física entre dispositivos y reglas según las cuales los bits son pasados de uno a otro. La capa física tiene cuatro importantes características:

1. **Mecánico:** Se relaciona con las propiedades físicas de la interfaz a un medio de transmisión. Típicamente, la especificación es de un conector que une a uno o varios conductores de señal, llamados circuitos.

2. **Eléctrico:** Se relaciona con la representación de bits (ej., en términos de niveles de voltaje) y la tarifa de transmisión de datos de bits.

3. **Funcional:** Especifica las funciones realizadas por los circuitos individuales de la interfaz física entre un sistema y el medio de transmisión.

4. **Procesal:** Especifica la secuencia de eventos por los cuales los flujos de bit son cambiados a través del medio físico.

La capa física se diferencia de las otras capas OSI en que no puede confiar en una capa inferior para transmitir sus PDUs. Más bien, debe hacer uso de un medio de transmisión cuyas características no sean parte del modelo OSI. No hay ninguna estructura de capa física PDU como tal; ninguna cabecera de información de control de protocolo es usada. El PDU simplemente consiste en un bloque o flujo de bits.

G.2.2 Capa de Enlace

La **capa de enlace** debe tratar tanto los requerimientos de la facilidad de comunicaciones como los requerimientos del usuario. Mientras la capa física proporciona sólo un servicio de flujo de bit novato, la capa de enlace intenta hacer el enlace físico confiable y proporciona el medio para activar, mantener y desactivar el enlace.

El servicio principal proporcionado por la capa de enlace a capas más altas es la de detección de errores y control. Así, con un protocolo de capa de enlace totalmente funcional, la siguiente capa más alta puede asumir la transmisión sin error sobre el enlace.

G.2.3 Capa de Red

La **capa de red** proporciona la transferencia de información entre sistemas a través de algún tipo de red de comunicaciones. Esto releva a capas más altas de la necesidad de conocer algo del ataque a la transmisión de datos subyacente y tecnologías de conmutación usadas para conectar sistemas.

En esta capa, el sistema de computación emplea un diálogo con la red para especificar la dirección de destino y solicitar ciertas facilidades de red, como la prioridad.

G.2.4 Capa de Transporte

La **capa de transporte** proporciona un mecanismo para el cambio de datos entre sistemas finales. El servicio de transporte orientado por conexión asegura que los datos son entregados sin error, en secuencia, sin pérdidas o duplicaciones.

La capa de transporte también puede estar interesada en la optimización del uso de servicios de red y suministro de una calidad solicitada de servicio a entidades de sesión. Por ejemplo, la entidad de sesión puede especificar tarifas de error aceptables, retraso máximo, prioridad y seguridad.

El tamaño y la complejidad de un protocolo de transporte depende de qué tan confiable o inconfiable es la red subyacente y los servicios de capa de red.

G.2.5 Capa de Sesión

La **capa de sesión** proporciona el mecanismo para controlar el diálogo entre aplicaciones y sistemas finales. En muchos casos, habrá poca o ninguna necesidad de servicios de capa de sesión, pero para algunas aplicaciones, tales servicios son usados. Los servicios claves proporcionados por la capa de sesión incluyen:

- **Disciplina de diálogo:** Esto puede ser simultáneo de dos maneras (lleno-doble) o alternado de dos maneras (medio-doble).
- **Agrupación:** El flujo de datos puede ser marcado para definir grupos de datos.
- **Recuperación:** La capa de sesión puede proporcionar un mecanismo de puntos de comprobación, de modo que si el fracaso de alguna clase ocurre entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación.

G.2.6 Capa de Presentación

La **capa de presentación** define el formato de los datos para ser cambiados entre aplicaciones y ofrece a programas de aplicación un conjunto de servicios de transformación de datos.

La capa de presentación define la sintaxis usada entre entidades de aplicación y proporciona la modificación subsecuente y la selección de la representación usada. Ejemplos de servicios específicos que pueden ser realizados en esta capa incluyen la compresión de datos y el cifrado.

G.2.7 Capa de Aplicación

La **capa de aplicación** proporciona el medio para que los programas de aplicación tengan acceso al ambiente OSI. Esta capa contiene funciones de administración y mecanismos generalmente útiles para soportar aplicaciones distribuidas.

Además, las aplicaciones de propósito general como la transferencia de archivo, el correo electrónico y el acceso terminal a computadoras remotas son consideras para residir en esta capa.

APÉNDICE H

PDU
Unidad de Datos del Protocolo

Un protocolo se preocupa del cambio de flujo de datos entre dos entidades. Usualmente, la transferencia puede ser caracterizada como la correspondencia de una secuencia de bloques de datos de algún tamaño limitado, referidos como Protocolo de Unidad de Datos (**PDUs**).

Cada PDU contiene la información de control que es usada para coordinar la operación conjunta de las dos entidades ocupadas en el protocolo. Además, algunos de los PDUs contienen datos de usuario de la siguiente capa más alta.

La figura H.1 ilustra el uso de PDUs en la arquitectura **OSI**. Cuando una aplicación X tiene datos que enviar a una aplicación Y, transfiere los datos a una entidad de aplicación en la capa de aplicación.

Una cabecera que se compone de la información del protocolo de control para la entidad par capa-7 es añadida a los datos, formando una aplicación PDU. Este PDU ahora es pasado como una unidad a la capa 6. La entidad de presentación trata la unidad entera como datos y añade su propia cabecera.

Este proceso continúa hacia abajo hasta la capa 2, que generalmente añade tanto una cabecera como un remolque. Este PDU capa 2 es entonces pasado por la capa física en el medio de transmisión como un flujo de bits.

Cuando el DL-PDU es recibido por el sistema objeto, el proceso inverso ocurre. Como los datos ascienden, cada capa quita de la cabecera exterior, actos sobre la información del protocolo de control contenida allí y pasa el resto a la siguiente capa.

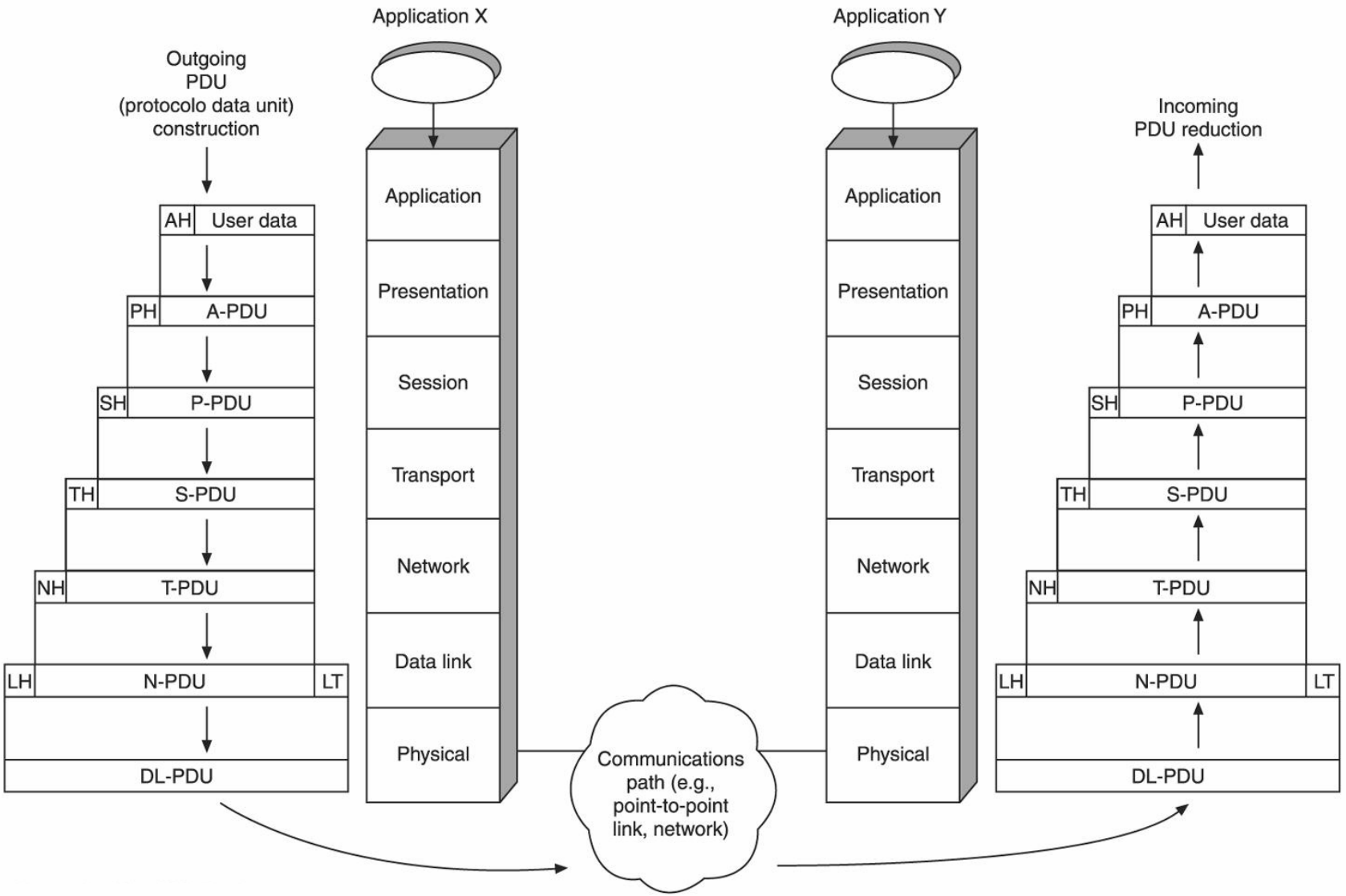


Figura H.1 Proceso de un paquete y adición de cabeceras de información

APÉNDICE I

SMI
Estructura para la Administración de Información

La estructura para la administración de información, que es especificada en el **RFC 1155**, define el marco general dentro del cual un **MIB** puede ser definido y construido. El SMI identifica los tipos de datos que pueden ser usados en el MIB y como los recursos dentro del MIB son representados y nombrados.

El **SMI** no soporta la creación o la recuperación de estructuras de datos complejas. Está en contraste con lo usado en la administración OSI, que proporciona estructuras de datos complejas y modos de recuperación para soportar la funcionalidad mayor.

SMI evita tipos de datos complejos para simplificar la tarea de implementación y mejorar la interoperabilidad.

SMI da las **reglas** de cómo los objetos en el MIB son definidos y codificados para la transferencia sobre el protocolo. Primero fue definido en agosto de 1988 y más tarde alcanzó el estado de estándar completo como RFC 1155.

El SMI es la descripción de las estructuras comunes y los tipos genéricos, junto con el esquema de identificación, que ha sido usado en la implementación. El SMI es a menudo comparado con el esquema de una base de datos.

Tal como un esquema describe el formato y la disposición del SMI, es que las definiciones formales de los objetos administrados serán descritas usando la Notación de Sintaxis Abstracta Uno (**ASN.1**).

La colección de objetos administrados, que son explícitamente definidos para cada implementación como su MIB particular, es llamada tipos de objeto en el lenguaje formal de SMI.

Estos tipos de objetos tienen tres atributos básicos que los describen y les permiten ser propiamente usados en la implementación de **SNMP**. Estos tres atributos pueden ser vistos como facetas del tipo de objeto que está necesariamente en las varias fases de la implementación. Los **tres aspectos** definibles de un tipo de objeto SNMP son:

1. Su NOMBRE
2. Su SINTAXIS
3. Su CODIFICACIÓN

I.1 Nombre de Tipo de Objeto

El **Nombre de Tipo de Objeto** es una **representación única** usada como el medio para identificar un objeto. También se conoce como el **identificador de objeto**. Es representado como una secuencia de enteros que atraviesan un árbol global que contiene todos los objetos conocidos en SNMP.

Todos estos objetos conocidos son definidos en una jerarquía. El punto de esta jerarquía debe asignar la autoridad para asignar nombres a muchas organizaciones diferentes interesadas.

Por lo tanto, aunque cualquier número de estos grupos pueda asignar nombres de objeto de SNMP, esta convención de esquema de numeración asegura que todos los nombres creados son únicos y absolutos porque cada uno conoce el esquema global mientras que es asignada su propia "rama" individual.

I.2 Sintaxis de Tipo de Objeto

La **Sintaxis** es la **definición** formal de la **estructura del tipo de objeto** que usa la notación ASN.1. Esta sintaxis define la estructura de datos abstracta correspondiente a ese objeto particular. Hay cuatro atributos estándar que deben ser definidos para cada objeto para tenerlo correctamente declarado para el **MIB**.

Estos **cuatro atributos** son:

1. Tipo de Sintaxis.
2. Modo de acceso.
3. Estado.
4. Valor de Nombre.

El **tipo de sintaxis** es uno de un conjunto de opciones ASN.1 predefinidas. Hay 12 opciones actualmente definidas y estas opciones pueden ser subdivididas en tres grupos básicos: simple, por todo el uso y simplemente construido.

La **modalidad de acceso** es un nivel de permisos que el agente examina por demanda de cada objeto. Hay cuatro valores de acceso actualmente definidos: sólo para leer, leer - escribir, sólo escritura y no - accesible.

El **estado** define la responsabilidad del nodo manejado de poner en práctica este objeto particular. Hay tres estados actualmente definidos: obligatorio, opcional, y anticuado.

El **valor de nombre** es un nombre corto textual, llamado descriptor de objeto, que es igual a su identificador de objeto correspondiente.

I.3 Codificación de Tipo de Objeto

En cuanto los casos de los tipos de objeto han sido definidos y declarados, su valor puede ser transmitido al y del agente y SAR aplicando las **reglas de codificación** especificadas de **ASN.1** a la sintaxis para el tipo de objeto. La notación de sintaxis de transferencia usada en **SNMP** son las Reglas de Codificación Básicas (**BER**).

APÉNDICE J

TCP/IP
Protocolo de Control de Transmisión / Protocolo de Internet

J.1 Historia

El Protocolo de Internet (**IP**) y el Protocolo de Transmisión (**TCP**), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (**ARPA**) del Departamento Estadounidense de Defensa.

Internet comenzó siendo una red informática de ARPA, llamada **ARPAnet**, que conectaba redes de computadoras de varias universidades y laboratorios de investigación en Estados Unidos.

J.2 Definición y Arquitectura de TCP/IP

TCP/IP es el protocolo común utilizado por todas las computadoras conectadas a Internet, de manera que éstas puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectadas computadoras de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión.

Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encarga de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto.

La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos y que se relacionan con los **niveles OSI** de la siguiente manera:

- **Aplicación:** Corresponde a los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (**SMTP**), transferencia de ficheros (**FTP**), conexión remota (**TELNET**) y otros más recientes como el protocolo **HTTP** (**H**yper**T**ext **T**ransfer **P**rotocol).

- **Transporte:** Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como **TCP** y **UDP**, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

- **Internet:** Es el nivel de red del modelo OSI. Incluye al protocolo **IP**, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

- **Físico:** Análogo al nivel físico del OSI.

- **Red:** Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces más conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo, hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP.

Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. En TCP/IP cada una de estas unidades de información recibe el nombre de **"datagrama" (*datagram*)** y son conjuntos de datos que se envían como mensajes independientes.

J.3 Protocolos TCP/IP

La figura J.1 muestra los protocolos de TCP/IP.

FTP, SMTP, TELNET	SNMP, X-WINDOWS, RPC, NFS
TCP	UDP
IP, ICMP, 802.2, X.25	
ETHERNET, IEEE 802.2, X.25	

Figura J.1 Conjunto de Protocolos de TCP/IP

- **FTP (File Transfer Protocol).** Se utiliza para transferencia de archivos.
- **SMTP (Simple Mail Transfer Protocol)**. Es una aplicación para el correo electrónico.
- **TELNET:** Permite la conexión a una aplicación remota desde un proceso o terminal.
- **RPC (Remote Procedure Call).** Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.
- **SNMP (Simple Network Management Protocol).** Se trata de una aplicación para el control de la red.
- **NFS (Network File System).** Permite la utilización de archivos distribuidos por los programas de la red.
- **X-Windows**. Es un protocolo para el manejo de ventanas e interfaces de usuario.

J.4 Características de TCP/IP

Ya que dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características.

- La tarea de **IP** es llevar los datos a granel de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas ruteadores) utilizan IP para trasladar los datos. En resumen IP mueve los paquetes de datos a granel, mientras **TCP** se encarga del flujo y asegura que los datos estén correctos.

- Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo y se ordenará y combinará cuando llegue a su destino.

- Los datos no tienen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino.

- Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar necesariamente por la misma ruta, ni tienen que llegar todos al mismo tiempo.

- La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando usted envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia afuera y los distribuye.

  En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

J.5 Cómo Funciona TCP/IP

J.5.1 IP

IP a diferencia del protocolo X.25, que está orientado a conexión, es sin conexión. Está basado en la idea de los datagramas, los cuales son transportados transparentemente, pero no siempre con seguridad, desde el anfitrión fuente hasta el anfitrión destinatario, quizás recorriendo varias redes mientras viaja.

El **protocolo IP** trabaja de la siguiente manera; la capa de transporte toma los mensajes y los divide en datagramas. Cada datagrama se transmite a través de la red, posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final, cuando

todas las piezas llegan a la computadora destinataria, la capa de transporte los reensambla para así reconstruir el mensaje original.

Un **datagrama IP** consta de una parte de cabecera y una parte de texto. El **campo Versión** indica a qué versión del protocolo pertenece cada uno de los datagramas.

El **campo Opciones** se utiliza para fines de seguridad, encaminamiento fuente, informe de errores, depuración, sellado de tiempo, así como otro tipo de información.

Debido a que la longitud de la cabecera no es constante, un campo de la cabecera, IHL, permite que se indique la longitud que tiene la cabecera en palabras de 32 bits.

El **campo Tipo de Servicio** le permite al hostal indicarle a la subred el tipo de servicio que desea. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad.

La **Longitud Total** incluye todo lo que se encuentra en el datagrama tanto la cabecera como los datos.

El **campo Identificación** se necesita para permitir que el hostal destinatario determine a qué datagrama pertenece el fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación.

Enseguida viene un bit que no se utiliza y después dos campos de 1 bit. Las letras DF quieren decir no fragmentar. Esta es una orden para que las pasarelas no fragmenten el datagrama, porque el extremo destinatario es incapaz de poner las partes juntas nuevamente.

Las letras MF significan más fragmentos. Todos los fragmentos, con excepción del último, deberán tener ese bit puesto. Se utiliza como una verificación doble contra el campo de Longitud total, con objeto de tener seguridad de que no faltan fragmentos y que el datagrama entero se reensamble por completo.

El desplazamiento de fragmento indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos, con excepción del último, deberán ser un múltiplo de 8 octetos, que es la unidad elemental de fragmentación.

El **campo Tiempo de Vida** es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiéndose un tiempo de vida máximo de 255 segundos.

Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitará saber qué hacer con él. El campo Protocolo indica, a qué proceso de transporte pertenece el datagrama.

Protocolo: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino.

El código de redundancia de la cabecera es necesario para verificar que los datos contenidos en la cabecera IP son correctos. La dirección de origen contiene la dirección del anfitrión que envía el paquete.

La dirección de destino: Esta dirección es la del anfitrión que recibirá la información. Los ruteadores o pasarelas intermedios deben conocerla para dirigir correctamente el paquete.

J.5.2 TCP

Una entidad de transporte **TCP** acepta mensajes de longitud arbitrariamente grande procedentes de los procesos de usuario, los separa en pedazos y transmite cada pedazo como si fuera un datagrama separado.

La capa de red, no garantiza que los datagramas se entreguen apropiadamente, por lo que TCP deberá utilizar temporizadores y retransmitir los datagramas si es necesario. Los datagramas que consiguen llegar, pueden hacerlo en desorden y dependerá de TCP el hecho de reensamblarlos en mensajes, con la secuencia correcta.

TCP utiliza una cabecera, al igual que IP. Enseguida se analizará minuciosamente campo por campo esta cabecera.

Los **campos Puerto Fuente y Puerto Destino** identifican los puntos terminales de la conexión. Cada anfitrión deberá decidir por sí mismo cómo asignar sus puertos.

La Longitud de la cabecera TCP indica el número de palabras que están contenidas en la cabecera de TCP. Esta información es necesaria porque el campo Opciones tiene una longitud variable y por lo tanto la cabecera también.

El **Puntero Acelerado** se emplea para indicar un desplazamiento en octetos a partir del número de secuencia actual en el que se encuentran datos acelerados. Esta facilidad se brinda en lugar de los mensajes de interrupción.

El **bit SYN** se utiliza para el establecimiento de conexiones. La solicitud de conexión tiene SYN=1 y ACK=0, para indicar que el campo de asentimiento en superposición no se está utilizando.

El **Control de Flujo** en TCP se trata mediante el uso de una ventana deslizante de tamaño variable. Es necesario tener un campo de 16 bits, porque la ventana indica el número de octetos que se pueden transmitir más allá del octeto asentado por el campo ventana.

El **Código de Redundancia** también se brinda como un factor de seguridad extrema. El algoritmo de código de redundancia consiste en sumar simplemente todos los datos, considerados como palabras de 16 bits y después tomar el complemento a 1 de la suma.

El **campo de Opciones** se utiliza para diferentes cosas, durante el procedimiento de establecimiento.

J.6 En qué se Utiliza TCP/IP

Muchas grandes redes han sido implementadas con estos protocolos, incluyendo **DARPA** Internet "**D**efense **A**dvanced **R**esearch **P**rojects **A**gency Internet", en español, Red de la Agencia de Investigación de Proyectos Avanzados de Defensa.

De igual forma, una gran variedad de universidades, agencias gubernamentales y empresas de computadoras, están conectadas mediante los protocolos TCP/IP. Cualquier computadora de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes en una red virtual llamada Internet. Las computadoras en Internet son denominadas "anfitriones" o nodos.

TCP/IP proporciona la base para muchos servicios útiles, incluyendo correo electrónico, transferencia de ficheros y login remoto.

El correo electrónico está diseñado para transmitir ficheros de texto pequeños. Las utilidades de transferencia sirven para transferir ficheros muy grandes que contengan programas o datos. También pueden proporcionar chequeos de seguridad controlando las transferencias.

El login remoto permite a los usuarios de una computadora acceder a una computadora remota y llevar a cabo una sesión interactiva.

APÉNDICE K

UDP
Protocolo de Datagrama de Usuario

Además de **TCP**, hay otro protocolo de nivel de transporte que está en uso común como parte del conjunto de protocolos TCP/IP: el Protocolo de Datagrama de Usuario (**UDP**), especificado en el **RFC 768**. El UDP proporciona un servicio de conexión baja para procedimientos de nivel de aplicación. Así, permite procedimientos para enviar mensajes a otros procedimientos con un mínimo de mecanismos de protocolo. **SNMP** hace uso de UDP.

UDP añade dos servicios de transporte:

- La capacidad de distinguirse entre múltiples destinos, llamadas a puertos, desde múltiples fuentes.
- El apoyo a una adicional y opcional facilidad de suma.

UDP se sitúa encima de **IP**. Como es de conexión baja, UDP tiene muy poco para hacer. Esencialmente, adiciona una capacidad de direccionamiento de puerto a IP. Esto es mejor visto examinando la cabecera de UDP, mostrada en la figura K.1.

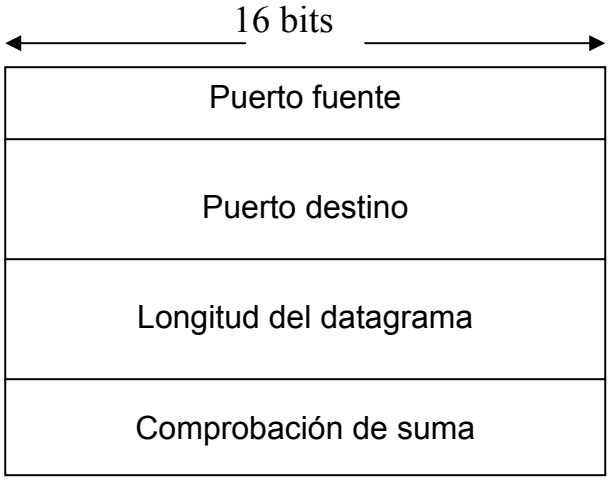


Figura K.1 Cabecera UDP

La cabecera incluye un **puerto fuente** y un **puerto destino**, que identifica a los usuarios de TCP enviando y recibiendo. El **campo de longitud** contiene la longitud en octetos del segmento entero UDP, incluyendo la cabecera y los datos.

La **comprobación de suma** se aplica al segmento entero UDP más una pseudocabecera prefijada a la cabecera UDP en el momento del cálculo.

El campo de comprobación de suma en UDP es opcional. Si no es usado, es puesto en 0. Sin embargo, debería ser indicado que la comprobación de suma IP se aplica sólo a la cabecera IP y no al campo de datos IP, que en este caso, consiste en la cabecera UDP y los datos de usuario.

GLOSARIO

"Quien no puede lo que quiere, quiera lo que pueda".

A

Administrador: Persona que se encarga de una red y de dar órdenes de monitoreo. Puede ser también un software en una estación de administración de red que habilita la estación para enviar requerimientos o actualizar variables MIB y recibe traps de un agente.

Agente: Software que se habilita en un dispositivo para responder a los requerimientos del administrador para ver o actualizar datos MIB y enviar traps reportando problemas o eventos significativos.

Anfitrión: Es la computadora donde se conecta para recibir algún servicio de ella. Cualquier computadora que pueda hacer las veces de punto inicial y final de una transferencia de datos. Sistema de computación en una red. En ingles host.

API: **A**pplication **P**rogram(ming) **I**nterface (Interfaz de Programa de Aplicación). Es un punto direccionable que sirve a la función para traer juntas dos o más entidades.

Aplicación: Programa que cumple funciones específicas orientadas a las necesidades del usuario, por ejemplo: planilla de cálculo o electrónica, procesador de textos, administrador de base de datos, sistemas orientados a la gestión administrativa.

APPC: **A**dvanced **P**eer – to – **P**eer **C**ommunications (Comunicaciones Par a Par Avanzadas). El significado básico de APPC es la comunicación entre programas: específicamente transacciones de programas. Este tipo de protocolo permite la comunicación entre programas escritos en diferentes lenguajes. Protocolo de IBM para comunicaciones SNA entre dos dispositivos del mismo nivel.

APPN: **A**dvanced **P**eer – to – **P**eer **N**etwork (Red Par a Par Avanzada). Mejoramiento de la arquitectura original SNA de IBM. APPN maneja el establecimiento de una sesión entre nodos iguales, cálculos de ruta transparentes y dinámicos y prioritización del tráfico APPC. Desarrollado por IBM, se trata de una extensión a SNA que facilita la conexión de computadoras en redes de área local. Es un protocolo de capa superior de red basado en tecnología de par.

ARPANET: Es el precursor de Internet, fue una red de área amplia creada por la Agencia de Proyecto de Investigación Avanzada de la Defensa de los Estados Unidos (**ARPA**). Establecido en 1969, ARPANET sirvió como un banco de pruebas para nuevas tecnologías conectadas a una red, uniendo muchas universidades y centros de investigación.

AT: **A**dvanced **T**echnology. Las computadoras personales basadas en el procesador 80386 de Intel, que son capaces de direccionar 4 GB de memoria RAM.

B

Backbone: Espina dorsal de red. Es la infraestructura de conexión principal de una red y está constituida por los enlaces de mayor velocidad dentro de dicha red.

Backup: Copia de respaldo, copia de seguridad, copia de ficheros o datos de forma que estén disponibles en caso de que una falla produzca la perdida de los originales. Esta sencilla acción evita numerosos y a veces irremediables, problemas si se realiza de forma habitual y periódica.

Base de Datos: Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa. Las bases de datos proporcionan la infraestructura requerida para los sistemas de apoyo a la toma de decisiones y para los sistemas de información estratégicos.

Beeper: Pequeño dispositivo de comunicación que permite la recepción de mensajes escritos, emitiendo un pitido (*beep*) cuando se recibe el mensaje. El mensaje pude ser enviado a través de Internet.

BIND: En SNA es una solicitud de activación de sesión entre unidades lógicas.

BIT: **B**inary **D**igit, abreviación de Dígito Binario. Unidad mínima de información con que trabajan internamente las computadoras, puede ser un cero (0) o un uno (1). Unidad de medida más pequeña de espacio en disco.

Bridge: Véase puente.

Broadcast: Véase Ethernet.

C

Cableado: Columna vertebral de cualquier sistema de red, ya que lleva la información de un nodo a otro.

Cable coaxial: Conductor eléctrico redondo y aislado, formado por una malla tubular o blindaje y un alambre central, generalmente hecho con hilo de cobre ligeramente rígido. Posee un relleno dieléctrico aislante.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

CDRSC: **C**ross-**D**omain **R**e**S**our**C**e (Recurso de Dominio Cruzado). Es un término usado en SNA referido a un recurso (típicamente software) que reside en otro dominio, bajo el control de un VTAM diferente.

Cifrado, codificado: Encryption. Método para proteger los datos de un acceso no autorizado a los mismos. Se utiliza normalmente en Internet para sustraer el correo electrónico.

Cliente: Es un programa o computadora que accede a recursos y servicios brindados por un servidor, generalmente en forma remota.

Cliente-Servidor: Es una forma de dividir y especializar programas y equipos de computo a fin de que la tarea que cada uno de ellos realiza se efectúe con la mayor eficiencia y permita simplificar las actualizaciones y mantenimiento del sistema.

CMIP: **C**ommon **M**anagement **I**nformation **P**rotocol (Protocolo de Información de Administración Común). Es otro protocolo de administración sobre OSI (CMIP se encuentra en el nivel de aplicación OSI) y más complejo que SNMP.

CMOT: **C**ommon **M**anagement Information Services and Protocol **O**ver **T**CP/IP, Protocolo sobre TCP/IP y Servicios de Información de Administración Común. Es una especificación para usar protocolos de administración OSI en redes TCP/IP.

Colisión: Suceso que ocurre en una red CSMA/CD cuando dos estaciones intentan transmitir de manera simultánea. Las señales se interfieren y obligan a las dos estaciones a retroceder e intentar de nuevo.

Compaq: Compaq Computer Corporation. Fabricante líder de computadoras personales fundado en 1982 por Rod Canion, Bill Murto y Jim Harris. Compaq ha sido muy valorada por sus computadoras personales.

Comunidad SNMP: Emparejamiento de un agente SNMP con un conjunto de entidades de aplicación SNMP.

Concentrador: Dispositivo que concentra todas las señales de los nodos y servidores de una red y las envía, una por una, a la computadora central y recibe de ésta la respuesta que envía al nodo correspondiente de acuerdo con un código de dirección. En inglés hub.

Configurar: Adaptar una aplicación software o un elemento hardware al resto de los elementos del entorno y a las necesidades específicas del usuario. Es una tarea esencial antes de trabajar con cualquier nuevo elemento.

Conmutador de Paquetes: Dispositivo que conecta computadoras. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

Consola: Se trata de una o varias terminales conectadas a la computadora central, que permiten monitorear su funcionamiento, controlar las operaciones que realiza, regular las aplicaciones que deben ejecutarse, etc.

Controlador: Software que permite a la computadora "entenderse" con los componentes que tiene instalados. Cada componente necesita su propio controlador (Tarjeta de Sonido, Módem, CD-ROM, etc.) Driver en Inglés.

CPD: **C**entro de **P**roceso de **D**atos. En las grandes empresas, todos los sistemas informáticos centrales se instalan en un mismo lugar, generalmente equipado con sofisticadas medidas de seguridad para controlar el acceso al centro.

Criptografía: Es la ciencia que estudia los métodos y procedimientos, mediante algoritmos matemáticos, para modificar los datos de tal manera que solamente las personas que tengan la llave adecuada puedan a) tener acceso a la versión original de los mismos (confidencialidad) y b) asegurar que estos datos no fueron modificados entre el remitente y el destinatario (integridad).

CSMA/CD: **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection (Acceso Múltiple de Sentido de Carga con Detección de Colisión). Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

D

Datagrama: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual.

Datagrama IP: Unidad fundamental de información transmitida a través de Internet. Contiene direcciones origen y destino junto con datos y una serie de campos que definen cosas tales como la longitud del datagrama, la suma de verificación del encabezado y señaladores para indicar si el datagrama se puede fragmentar o ha sido fragmentado.

DELL: Dell Computer Corporation. Compañía productora de computadoras personales fundada en 1984 por Michael Dell.

DES: **D**ata **E**ncryption **S**tandard (Estándar de Cifrado de Datos). Esquema de cifrado estandarizado. DES fue desarrollado por el Departamento de Estándares Nacional de E.U. y es parte de la seguridad de SNMP.

Dirección IP: Se refiere al número único, que identifica a las computadoras a nivel individual en Internet; cada una tiene su propia dirección IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred y un número de anfitrión. También denominada dirección de Internet (Dirección IP).

Dispositivos: Son estructuras sólidas, electrónicas y mecánicas las cuales son diseñadas para un uso especifico. Éstos se conectan entre sí para crear una conexión en común y obtener los resultados esperados siempre y cuando cumplan con las reglas de configuración.

Dispositivos de encaminamiento: Encaminador, elemento de red que se encarga de buscar el camino más corto para los paquetes de información. Opera en el nivel 3 del modelo OSI. En inglés router.

DNS: **D**omain **N**ame **S**ervice (Servicio de Nombre de Dominio). En ambientes TCP/IP este es un protocolo para igualar nombres de objetos y direcciones de red. Fue diseñado para reemplazar la necesidad de archivos de participación de entidades por toda la red.

Dominio: Es una parte de una red de computadoras, en la cual los recursos de procesamiento de datos están bajo un control común. También es una parte del DNS nombrado jerárquicamente.

DOS: **D**isk **O**perating **S**ystem (Sistema Operativo en Disco). Conjunto de programas que permite la administración del equipo; es un sistema monousuario, comúnmente usado en PC.

Driver: Véase controlador.

DTE: **D**ata **T**erminal **E**quipment (Equipo Terminal de Datos). Parte de una estación de datos, la cual constituye una fuente de datos, una conexión de datos o ambos. DTE se conecta a una red de datos y utiliza en forma típica señales de sincronización. DTE incluye dispositivos tales como computadoras, traductores de protocolo y multiplexores.

E

Echo: Comando que se utiliza para mostrar un mensaje o variable de ambiente en la pantalla.

EGP: **E**xterior **G**ateway **P**rotocol (Protocolo de Pasarela Exterior). Es un protocolo que anuncia el bloque de redes que pueden alcanzarse dentro de un sistema autónomo. EGP habilita esta información para ser compartida con otros sistemas autónomos.

Encaminadores: Véase dispositivos de encaminamiento.

Enlace: Es el establecimiento de comunicación entre dos puntos; esto es, cuando existe conexión física (medio de transmisión) y conexión lógica (software). Conexión entre dos archivos y objetos de modo que el cambio en uno produce la actualización del otro. Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

Entidades: Son objetos concretos o abstractos que presentan interés para el sistema y sobre los que se recoge información que será representada en un sistema de bases de datos.

Estación: Es cualquier nodo en una LAN que participa en el protocolo de control de acceso al medio de la LAN.

Estación de trabajo: Una computadora conectada a la red, que solicita los servicios de otros sistemas de la red, pero que no proporciona servicios a otros nodos.

Ethernet: Significa que cada anfitrión envía sus datos hacia todos los demás anfitriones del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita.

Evento: Es una tabla de entrada que identifica un mensaje de notificación que será enviado como resultado de una alarma.

F

Fichero: Archivo. Agrupación de información que puede ser manipulada de forma unitaria por el sistema operativo de una computadora. Un fichero puede tener cualquier tipo de contenido (texto, ejecutables, gráficos, etc.) y posee una identificación única formada por un 'nombre' y un 'apellido', en el que el nombre suele ser de libre elección del usuario y el apellido suele identificar el contenido o el tipo de fichero.

Firewall: Pared de fuego. Mecanismo utilizado para proteger una red o computadora conectada a Internet de accesos no autorizados. Una firewall puede construirse con software, con hardware o con una combinación de ambos.

FTP: **F**ile **T**ransfer **P**rotocol (Protocolo de Transferencia de Archivos). Como su nombre lo indica, define los mecanismos y reglas para transferir archivos entre las diversas computadoras de la red

G

Gateway: Ver Pasarela.

Grupo MIB: Es un bloque nombrado de definiciones MIB estrechamente relacionadas dentro de un módulo.

H

Hardware (equipo físico): Conjunto de componentes físicos de una computadora o de una red.

HEMS: **H**igh-Level **E**ntity **M**anagement **S**ystem (Sistema de Administración de Entidad de Alto Nivel). Primer propuesta de la estructura de administración de red. Está documentado en el RFC 1076.

Host: Véase anfitrión.

HP: **H**ewlett-**P**ackard. Esta compañía norteamericana es uno de los principales suministradores de sistemas informáticos. Sus impresoras DeskJet y LaserJet se consideran ya un estándar.

Hub: Véase concentrador.

I

IAB: **I**nternet **A**rchitecture **B**oard (Comité de Arquitectura de Internet). Reglas que vigilan el protocolo de Internet y los procesos de desarrollo y estandarización.

IBM: **I**nternational **B**usiness **M**achines Corporation. Es una empresa de cómputo fundada en 1911. Es también uno de los mayores vendedores de software, servicios y equipos de comunicaciones.

ICMP: **I**nternet **C**ontrol **M**essage **P**rotocol (Protocolo de Mensajes de Control en Internet). Protocolo usado para reportar problemas que entran como datagramas IP. ICMP también provee varios servicios útiles de preguntas. Documentado en RFC 792.

Instancia: Es la declaración específica de un objeto que es realizado por cada implementación de un agente.

Interfaz: software y hardware que habilita un protocolo de capa de red para transmitir un protocolo de unidad de datos hacia un medio de transmisión. Una interfaz puede componerse de varias subcapas.

internet: Una red hecha de subredes conectadas por uno o más ruteadores. Abreviatura de internetwork.

Internet: Es una malla mundial de computadoras y redes de computadoras de todo tipo de topologías interconectadas. También es una red abierta de redes con cobertura internacional orientada originalmente a la investigación.

IPX: Se refiere al intercambio de paquetes entre redes; IPX es el protocolo nativo de Netware y el que se utiliza en la mayoría de redes de área local.

ITU-T: **I**nternational **T**elecommunication **U**nion - **T**elecommunications Standardization Sector (Unión de Telecomunicaciones Internacional - Sector de Estandarización de Telecomunicaciones). Organización que crea las recomendaciones y regulaciones internacionales de protocolos de comunicaciones de datos.

L

LAN: **L**ocal **A**rea **N**etwork (Red de Área Local). Es una colección de computadoras y otros dispositivos relacionados conectados que cumplen con algunos permisos dentro de un área geográfica limitada.

Línea: Es la porción de un circuito externo de datos a un equipo de circuito de terminación de datos.

Link: Véase enlace.

LINUX: Nombre con el que se denomina al kernel de un sistema operativo, que esta bajo la licencia GNU. Su creador es Linus Torvalds y del nombre de éste se genera un acrónimo "**LINU**s uni**X**".

M

MD5: **M**essage **D**igest **5** (Compendio de Mensajes 5). Es un algoritmo de cifrado utilizado por diversos proveedores. Se usa en programas de cifrado, para realizar firmas digitales para identificar unívocamente un archivo.

Módem (Modulador-Demodulador): Dispositivo que convierte señales digitales a una forma adecuada para transmisión sobre medios de comunicación analógicos y viceversa. Dispositivo que permite transferir datos a través de la red telefónica.

Modo de Acceso: Nivel de acceso a un archivo, puede ser: sólo lectura, lectura-escritura o ninguno.

Monitor: Es un dispositivo que escucha todo el tráfico en una LAN, recoge las estadísticas y captura el tráfico.

MS: **M**anagement **S**ervices (Servicios de Administración). Los servicios de administración son proporcionados para asistir en la administración de redes SNA.

MVS: **M**ultiple **V**irtual **S**torage (Almacenaje Virtual Múltiple). Sistema operativo de IBM para sus grandes computadoras, muy conocido y de gran implantación. Igual que el sistema operativo estándar para las computadoras personales es el MS-DOS, puede afirmarse que en el terreno de la informática corporativa el MVS es el entorno estándar.

N

Navegador: Son programas de computadora diseñados para facilitar la visualización de páginas Web en Internet.

NCP: **N**etwork **C**ontrol **P**rogram (Programa de Control de Red). Es un programa de utilidad interactivo que permite el control y monitoreo de una red. Es un programa que controla las operaciones del controlador de comunicación.

NetBIOS: **Net**work **B**asic **I**nput/**O**utput **S**ystem (Sistema Básico de Entrada/Salida de una 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 finalización de sesión, así como transferencia de información.

Netscape: Navegador WWW creado en 1995 por Marc Andreessen, de la empresa norteamericana Netscape. Es uno de los navegadores de Internet más difundidos.

NetWare: Familia de sistemas operativos de la compañía Novell. Tipo de red de área local (LAN), muy utilizado. Proporciona acceso remoto transparente a archivos y varios otros servicios de red distribuidos.

NGMF: **N**etView **G**raphic **M**onitor **F**acility **(**Facilidad de Monitoreo Gráfico de NetView). Es un programa por medio del cual se despliega la información de la red APPN.

NMS: **N**etwork **M**anagement **S**tation (Estación Administradora de Red). Sistema que tiene la responsabilidad de administrar por lo menos parte de una red. Por regla general, un NMS es una computadora bastante potente y bien equipada. Los NMS se comunican con los agentes para ayudar a realizar un seguimiento de las estadísticas y los recursos de la red.

NMVT: **N**etwork **M**anagement **V**ector **T**ransport (Vector de Transporte de Administración de Red). Es un protocolo usado para los servicios de administración en una red SNA.

Nodo: Punto final de una conexión de red o una unión de dos o más líneas en una red.

Nombre de comunidad: Está denominado por una cadena de octetos.

O

Objeto: Nombre genérico que designa una imagen, línea o gráfico, que forman parte de un documento.

OpenLook: Interface gráfico de usuario para X-Windows, desarrollado por la firma Sun Microsystems.

P

Paquete: Agrupamiento lógico de información que incluye un encabezado que contiene información de control y usualmente datos del usuario. Los paquetes se utilizan más frecuentemente para hacer referencia a las unidades de datos de las capas de red.

Pasarela: Dispositivos de comunicación de redes que permite comunicar dos redes con protocolos distintos.

Pentium: Nombre comercial del procesador Intel denominado técnicamente 80856.

PING: **P**acket **IN**ternet **G**roper. Aplicación que usa mensajes de eco ICMP para probar la conectividad básica entre dos nodos de direccionamiento IP.

Plataforma: Arquitectura de software y hardware que soporta una aplicación.

Poleo: El término viene del inglés «poll». Es una forma de control en redes de comunicaciones de tipo LAN, según la cual la unidad central de proceso pide, de acuerdo con una programación determinada a cada puesto de trabajo conectado a la red, si ha de enviar alguna información.

Procesador: Es el microchip encargado de ejecutar las instrucciones y procesar los datos que son necesarios para todas las funciones de la computadora. Se puede decir que es el cerebro de la computadora.

Proceso: En informática se manejan varias definiciones que aluden a diversos elementos: puede ser simplemente una operación o conjunto combinado de operaciones con datos, o bien una secuencia de acontecimientos definida única y delimitada, que obedece a una intención operacional en condiciones predeterminadas. También se denomina proceso a una función que se está ejecutando.

Protocolo: Conjunto de reglas para lograr la comunicación entre computadoras en una red.

Protocolo de administración de red: Protocolo de aplicación por el que las variables de la MIB de un agente pueden ser inspeccionadas o alteradas.

Proxy: Servidor que se ubica entre una red interna e Internet. Se le utiliza para almacenar las páginas Web más solicitadas por los usuarios de la red interna, lo que acelera el tiempo de carga.

Puente: Elemento de hardware en una red de cómputo cuya función es conectar dos o más segmentos de red. Los puentes funcionan en los niveles de la capa 1 y de la capa 2. En inglés bridge.

Puerto: En Internet se refiere a la parte de un URL que va inmediatamente después de un nombre de dominio y que está precedido por dos puntos (:). Se utiliza para indicar que los servicios de dicho servidor no están ejecutándose en el puerto estándar.

R

RAM: **R**andom **A**ccess **M**emory (Memoria de Acceso Aleatorio). Almacenamiento de información que permite al usuario mover y colocar los datos de cualquier manera posible.

Recurso: Son los elementos de la computadora que utilizan los dispositivos para poder funcionar correctamente. Muchos de estos recursos, no pueden ser compartidos.

Red: Organización de equipos de cómputo conectados mediante un medio de conexión guiado o no para compartir recursos. Agrupación de computadoras, impresoras, ruteadores, conmutadores de paquetes y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Repetidor: Elemento de red que se encarga de restaurar las señales que son atenuadas. Dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

RFC: **R**equest **F**or **C**omments (Petición De Comentarios). Son un conjunto de documentos que contienen protocolos de Internet y discusiones acerca de tópicos relacionados.

Router: Véase dispositivos de encaminamiento.

RPC: **R**emote **P**rocedure **C**all (Llamada de Procedimiento Remoto). Base tecnológica de la arquitectura cliente/servidor. Las RPC son llamadas de procedimiento que los clientes crean o especifican y que se ejecutan en los servidores. Los resultados se devuelven a los clientes a través de la red.

RTM: **R**esponse **T**ime **M**onitor (Monitor de Tiempo de Respuesta). Sirve para monitorear el tiempo de respuesta de una red, el cual es proporcional al número de usuarios, la localización y la complejidad de la red.

Ruteador: Véase dispositivos de encaminamiento.

S

SAW: **S**ession **AW**areness (Sesión de Conocimiento). Es una colección de datos hecha por el programa NetView acerca de una sesión que incluye el tipo de sesión, los nombres de los compañeros de sesión e información acerca del estado de activación de la sesión. Esta es coleccionada por sesiones, SSCP-PU y SSCP-SSCP.

Servidor: Computadora conectada a una red que se encarga de las peticiones de datos, el correo electrónico, la transferencia de archivos o cualquier otro servicio brindado a esa red.

Sesión: Conjunto relacionado de transacciones de comunicaciones orientadas a conexión entre dos o más dispositivos de red. En SNA, una conexión lógica que permite que dos unidades de red direccionables se comuniquen.

Session monitor: Es un componente de NetView que colecciona y correlaciona sesiones y relaciones de datos y provee accesos en línea a esta información.

SGMP: **S**imple **G**ateway **M**onitoring **P**rotocol (Protocolo de Monitoreo de Pasarela Simple). Estructura de administración de red que evolucionó dentro de SNMP. SGMP es definido en el RFC 1028.

Símbolo: También conocido como "prompt". Es la forma en la que el sistema operativo indica al usuario que está preparado para recibir comandos que ejecutar. En MS-DOS el símbolo de sistema o prompt suele mostrar también el directorio de trabajo, como por ejemplo C:\>

Sistema de administración: Es el que permite la administración y el control dentro de una organización. Está compuesto por personas que interactúan con otras personas y con computadoras, que juntos fijan las metas y objetivos, delinean las estrategias y tácticas y desarrollan los planes, programas y controles necesarios para dirigir una organización.

Sistema Operativo: Conjunto de programas que permite la administración y disposición del equipo y periféricos. Se ejecuta inmediatamente después de encender la máquina.

SMTP: **S**imple **M**ail **T**ransfer **P**rotocol (Protocolo de Trasferencia de Correo Simple). Protocolo que se usa para trasmitir correo electrónico entre servidores. Protocolo original para el intercambio de correo en Internet.

SMS: **S**hort **M**essage **S**ystem (Sistema de Mensajes Cortos). Procedimiento de envío y recepción de mensajes escritos de pequeño tamaño a través del teclado y la pantalla de los teléfonos móviles.

SNA: **S**ystems **N**etwork **A**rchitecture (Arquitectura de Red de Sistemas). Es la descripción de IBM de la estructura lógica, formatos, protocolos y secuencias operacionales para una red.

Software (componentes lógicos): Conjunto de instrucciones lógicas diseñadas para el funcionamiento computacional. Programas o elementos lógicos que hacen funcionar una computadora o una red o que se ejecutan en ellas.

Solaris: Variante del sistema operativo Unix desarrollada por Sun Microsystems. Solaris incluye OpenWindows, interfaz gráfica de usuario (GUI) basada en X-Windows.

SSCP-PU: En SNA es una sesión entre un SSCP y un PU. Una sesión SSCP-PU permite que SSCP envíe solicitudes y reciba información de estado de nodos individuales en orden para controlar la configuración de la red.

SSCP-SSCP: **S**ystem **S**ervices **C**ontrol **P**oint (Punto de Control de Servicios de Sistema). Es una sesión entre un dominio y otro dominio SSCP. Este tipo de sesiones son usadas para iniciar y terminar dominios mezclados de sesiones LU-LU.

SSL: **S**ecure **S**ocket **L**ayer. Un protocolo de bajo nivel que permite establecer comunicaciones seguras entre un servidor Web y FrontPage o un explorador de Web.

Subárea: Es una porción de la red SNA, consistente de nodos periféricos conectados y recursos asociados.

Sun Microsystems Inc.: Una de las firmas norteamericanas más importantes en la fabricación y comercialización de estaciones de trabajo.

SunOS: Sistema operativo de Sun Microsystems conforme con UNIX.

Switch: Véase Conmutador de Paquetes.

T

Tarjeta de red: También conocida como NIC (Network Interface Card), es el elemento que conectamos a la PC para proporcionar el soporte de red.

Telnet: Protocolo estándar de Internet que permite al usuario conectarse a una computadora remota y utilizarlo como si estuviera en una de sus terminales.

Terminal: Generalmente entendido como un punto de entrada con una pantalla y un teclado.

Token Ring: Es una tecnología de red de área local basada en una topología de anillo. Las estaciones en el anillo pasan un mensaje especial, llamado token, alrededor del anillo. El poseedor actual del token tiene el derecho de transmitir datos por un periodo limitado de tiempo. El estándar IEEE 802.5 define las redes de Token-Ring.

U

UNIX: Es un sistema operativo multiproceso y multitarea utilizado por un número significativo de servidores en Internet; los programas UNIX no son compatibles con Windows. Sistema operativo desarrollado en 1969 en Bell Laboratories.

Usuario: Individuo que interactúa con la computadora al ejecutar alguna aplicación.

V

Variable: Véase definición de Objeto.

VTAM: **V**irtual **T**elecommunications **A**ccess **M**ethod (Método de Acceso de Telecomunicaciones Virtuales). De acuerdo con la documentación de IBM, este es un programa que controla la comunicación y el flujo de datos en una red SNA. Provee dominios simples, múltiples dominios y capacidad de interconexión de redes.

W

WAN: **W**ide **A**rea **N**etwork (Red de Área Amplia). Son redes que cruzan límites municipales, estatales e internacionales. Los enlaces se realizan con los servicios públicos y privados de telecomunicaciones, además con los enlaces por satélites y microondas.

Web: Por éste término se suele conocer a **WWW** (**W**orld **W**ide **W**eb), creado por el Centro Europeo de Investigación Nuclear como un sistema de intercambio de información y que Internet ha estandarizado. Supone un medio cómodo y elegante, basado en multimedia e hipertexto, para publicar información en la red. Inicial y básicamente se compone del protocolo http y del lenguaje html.

Windows: Sistema operativo desarrollado por la empresa Microsoft y cuyas diversas versiones (3.1, 95, 98, NT, 2000, Me) dominan de forma abrumadora el mercado de las computadoras personales. La palabra windows significa literalmente "ventanas".

X

X.25: Es un estándar de CCITT para conectar computadoras en una red que provee la transmisión de datos basada en circuitos virtuales.

X Windows: Es un sistema de red transparente que corre sobre una GUI. Es usado en la mayoría de los UNIX's. El sistema X Windows (abreviado "X") se desarrolló dentro del ámbito del proyecto Athena en el MIT (Massachusetts Institute of Technology).

BIBLIOGRAFÍA

"Haz aquello que quieras haber hecho cuando mueras".

- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/index.php
- www.eveliux.com/telecom/topologias.html
- www.htmlweb.net/redes/topologia/topologia_2.html
- Multiplatform Network Management
  Edgar Taylor, Jay Ranade
  Series Advisor
  Ed. McGraw-Hill Series on Computer Communications.
- Redes para proceso distribuido. Área local, Arquitecturas, Rendimiento y Banda Ancha.
  Jesús García Tomás, Santiago Ferrando, Mario Prattini
  2ª. Edición actualizada
  Ed. Ra-Ma.
- www.pin.uax.edu.mx/monica/mac.html
- www.informatica.uv.es/iiguia/2000/R/snmp.ppt
- www.pín.uax.edu.mx/monica/snmp.html
- www.rediris.es/rediris/boletin/50-51/ponencia16.html
- www.snmp.cs.utwente.nl/software/
- www.david-guerrero.com/papers/snmp/lj.es.html
- www.itver.edu.mx/comunidad/material/servcomputo/ascc/Index_julia.html
- www.webmaster.bankhacker.com/monitorizacion/mrtg.phtml
- www.es.tldp.org/Articulos-periodisticos/jfs/snmp/snmp.html
- www.mrtg.org
- www.topology.org/comms/snmp.html
- www.yolinux.com/TUTORIALS/LinuxTutorialNetworking.html

- www.linuxhomenetworking.com/
- www.microsoft.com/windows2000/es/advanced/help/sagSNMPtopnode.htm
- www.microsoft.com/windows2000/es/advanced/help/snmp_install.htm
- www.arrakis.es/~gepetto/redes/rog08p2.htm
- www.gestiopolis.com/recursos/documentos/fulldocs/ger/adredesis.htm
- www.universia.net.mx/contenidos/nuevoInternet/tutoriales/varios/Modelo-Funcional-articulo.doc
- www.ilustrados.com/publicaciones/EpZVZuklAVloNPORHT.php
- www.netsnmp.org
- http://net-snmp.sourceforge.net/INSTALL.txt
- www.ucd-snmp.ucdavis.edu/tutorial
- www.snmp.com
- www.et.put.poznan.pl/snmp/
- www.netcom-sys.com/documents/snmp4dom.doc
- www.php.us.themoes.org/manual/es/ref.snmp.php
- www.sourceforge.net/proyects/net-snmp
- www.et.put.poznan.pl/snmp/main/glossar4.html
- www.noc.unam.mx/tech-docs/tmn-unam2.ppt
- www.aldealinux.com/manuales.shtml
- www.ecomchaco.com.ar/utn/AdmRedes/Traduccion/cap1.doc
- www.tucuman.linux.org.ar/glosario.shtml

- www.redaccionvirtual.com/redaccion/glosario/default.asp
- www.ares.unimet.edu.ve/electrica/fpie22/GLOSARIO_1.htm
- www.educ.ar/educar/ayuda/glosario/index.jsp
- www.terra.com.mx/acceso/articulo/078596/pagina2.htm
- www.conatel.gov.ec/espanol/ glosario/contenido_glosarioI.htm
- www.ati.es/novatica/glosario/glosario_internet.html#glosa
- www.lawebdelprogramador.com/diccionario/
- www.ipswitch.com
- http://www.microsoft.com/mom/techinfo/productdoc/default.mspx