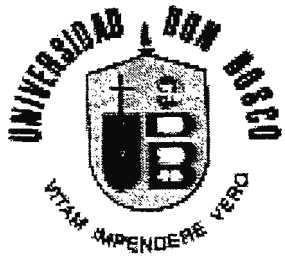


SISTEMA DE MONITOREO PARA REDES DE DATOS BASADO EN EL PROTOCOLO SNMP

TRABAJO DE GRADUACION
PREPARADO PARA LA FACULTAD DE INGENIERIA

PARA OPTAR AL GRADO DE

INGENIERO ELECTRONICO

POR

HERBERT EDGARDO ASCENCIO HURTADO
CARLOS ALBERTO BOLAÑOS GUERRERO
RAFAEL ADALBERTO COBOS MELENDEZ

MARZO – 2001

SOYAPANGO - EL SALVADOR - CENTROAMERICA

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELECTRÓNICA

RECTOR
ING. FEDERICO HUGET

DECANO
ING. CARLOS BRAN

Ing. Roberto Carlos Alvarenga
ASESOR

Ing. Francisco Emilio Morales
JURADO

Ing. José Armando Hernández
JURADO

A **Dios**, nuestros padres, hermanos, familiares y amigos
por todas las muestras de apoyo, comprensión
y confianza depositada en nosotros
para el logro de ésta meta.

Agradecimientos especiales para
FEPADE y
Americatel El Salvador
por toda la colaboración prestada.

A todos gracias.

Herbert Ascencio

Carlos Bolaños

Rafael Cobos

INDICE

Contenido **Página**

INDICE DE TABLAS

Tabla **Página**

INDICE DE FIGURAS

Figura **Página**

INTRODUCCIÓN

Las redes de telecomunicaciones son un conjunto de elementos discretos, interconectados a través de un medio de transmisión y con una organización de conectividad basada en una topología definida. Las redes de telecomunicaciones transportan la información de los usuarios, estableciendo caminos entre los dos (o más) extremos que comunican. De acuerdo a esta característica, las redes pueden clasificarse en dos grandes grupos: Redes de Conmutación de Circuitos y Redes de Conmutación de Paquetes.

Las redes de conmutación de paquetes transportan la información de los usuarios a través de los elementos de red, haciendo uso de la información que posee cada uno de los paquetes, la cual se clasifica en dos tipos, uno de ellos es el encabezado, que consiste en información sobre el direccionamiento, detección de errores, etc. y el otro es la información del usuario, que ha sido previamente fraccionada para adecuarse al tamaño manejado de paquetes en la red.

Con la creación de modelos de comunicación para las redes de datos, se ha desarrollado una gran variedad de sistemas de comunicación por parte de los fabricantes de Hardware y Software. El Protocolo de Internet (IP) es uno de los más utilizados en la capa de red de muchos sistemas de comunicación.

Los sistemas de administración de redes de datos, son una herramienta necesaria para la relación de los operadores de telecomunicaciones con los dispositivos de comunicación dentro de la red. Una red administrada permite realizar cambios de manera fácil, supervisar la operación, detectar y controlar fallas en el sistema.

En un sistema administrado cada uno de los elementos de red contiene agentes de software y bases de datos con variables que contienen información

sobre su configuración y estado. Estas variables son transferidas a un elemento específico dentro de la red, que contiene un sistema de administración que recibe e interpreta estas variables al administrador de la red.

El protocolo utilizado para la trasferencia de esta información sobre la red IP es el SNMP (Simple Network Management Protocol), que es parte del grupo de #2. protocolos del modelo TCP/IP y es el protocolo de administración más utilizado actualmente por los fabricantes para la administración de equipos de comunicación.

El presente documento se encuentra dividido en dos grandes partes, la primera que contiene un estudio teórico sobre los fundamentos de redes de comunicaciones y el protocolo SNMP, para en la segunda desarrollar una guía práctica para el diseño de un sistema prototipo que realiza las funciones básicas del monitoreo de redes y los requerimientos para su implementación.

Capítulo I
Generalidades

1.1 ANTECEDENTES DEL PROBLEMA.

El tamaño y la complejidad de las redes han ido creciendo aceleradamente debido, en gran parte, a la aparición de las redes públicas de datos como Internet y a la creciente oferta de servicios de comunicaciones de valor agregado soportados sobre redes de conmutación de paquetes.

En la operación de la transferencia de información a través de las primeras redes, surgió la necesidad de implementar sistemas de gestión, es decir, sistemas capaces de controlar los recursos que la componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnósticos y planificación.

La gestión de red es un concepto que comprende la administración de los diferentes recursos que constituyen una red, tomando forma de seguimiento, coordinación y control de los recursos informáticos y de comunicaciones.

Una de las funciones que realiza un sistema de gestión de red es la supervisión constante del funcionamiento adecuado de cada uno de los elementos que componen el sistema de comunicación, constituyendo en forma global el monitoreo efectuado a la red, que constituye el elemento clave en la detección y corrección de errores y fallas dentro de la red.

Los sistemas de monitoreo de redes se pueden clasificar de acuerdo al tipo de red al que están orientados:

- Sistemas de Monitoreo de equipos de comunicaciones.
- Sistemas de Monitoreo de redes de comunicaciones.
- Sistemas de Monitoreo de Arquitecturas de computadoras.
- Sistemas de Monitoreo de redes de área local (LAN).

Las compañías operadoras de Servicios de Telecomunicaciones y fabricantes de computadoras han desarrollado Sistemas de Monitoreo propios para controlar los servicios que brindan sus redes y recursos de comunicaciones (dispositivos y protocolos) propios de su arquitectura de comunicaciones, entre los cuales existen:

- Netview de IBM.
- Cisco Works de Cisco Systems.
- UNMA (Unified Network Management Architecture) de ATT.
- ENMA (Enterprisewide Management Architecture) de DEC.

Dado el crecimiento de redes de área local instaladas, existen también diversos Sistemas de Monitoreo desarrollados para controlarlas:

- LAN Manager.
- Vines.
- Netware.
- Whats up

La mayor parte del desarrollo de normas para el Monitoreo de redes se basan en los dos modelos siguientes:

- Gestión OSI para las redes basadas en protocolos OSI.
- Gestión SNMP para las redes basadas en el modelo TCP/IP.

Algunas corporaciones se han decidido por las soluciones particulares para la gestión y monitoreo, ya sea, desarrollando sistemas propios o utilizando los sistemas de fabricantes específicos.

1.2 IMPORTANCIA Y JUSTIFICACIÓN

Los sistemas de monitoreo de redes de comunicaciones han evolucionado con el desarrollo tecnológico en esta última década, como resultado de los beneficios que ofrecen:

- Supervisión continua de la operación de los elementos una red.
- Disminución en el tiempo de respuesta en la detección de problemas de operación, permitiendo un nivel elevado de disponibilidad, que implica calidad en el servicio que la red presta.
- Información visual de la ubicación de una falla dentro de la red administrada, que permite al operador identificarla inmediatamente para realizar las correcciones necesarias.
- Medición de tráfico generado en elementos o grupos de elementos, que proporciona un parámetro de calidad de la operación actual de la red, permitiendo al proveedor de servicio la planeación de su crecimiento y posibles cambios en su topología.
- Medición de los recursos físicos (memoria, unidad de procesamiento o puertos de comunicación) y lógicos (Sistema operativo) utilizados en el sistema, en los elementos de red y en los enlaces de comunicación para planificar la actualización en un elemento específico.
- Realización de tareas de monitoreo en tiempos programados que permitan un punto de equilibrio en la utilización de recursos y la veracidad de la información de supervisión.

Los fabricantes de equipos de comunicaciones desarrollan, además, herramientas para la administración de los sistemas de red, lo cual implica lo siguiente:

- Altos costos de adquisición del sistema de administración.

- Costos adicionales por la contratación de servicios profesionales, especializados en el área de administración de redes, para su implementación y capacitación del personal que opera la red.

Esta segunda implicación, es causa de la carencia de los conocimientos fundamentales en el área de administración de redes, en las empresas de telecomunicaciones de nuestro país, lo cual justifica la investigación de técnicas eficientes, que permitan desarrollar aplicaciones para el monitoreo de redes y la introducción de los avances tecnológicos relacionados a esta área en El Salvador.

En el país se ha generado un alto crecimiento en la demanda de servicios de comunicación de datos y acceso a Internet, obligando a las empresas a ser más competitivas en la calidad de los servicios que brindan, para lo cual es sumamente indispensable un sistema que permita conocer el estado actual de los diferentes elementos que forman parte de la red, en forma continua.

1.3 DEFINICIÓN DEL PROBLEMA

El funcionamiento de las redes de conmutación de paquetes está sujeto a los siguientes problemas:

- Los protocolos de conmutación de paquetes como IP han sido creados para que la información (en paquetes) fluya dentro de la red por caminos disponibles y cercanos a su destino, sin tomar en cuenta enlaces fuera de servicio, por lo que no es inmediata la detección de problemas en un enlace de comunicación sin una herramienta que verifique su funcionamiento.
- Los sistemas de administración y monitoreo de redes tienen elevados costos y requieren, para su implementación, de personal especializado que generalmente proviene del extranjero.

- Una red de comunicaciones requiere un elemento que supervise la operación del funcionamiento de la misma.
- En El Salvador no se ha realizado una investigación sobre el funcionamiento del protocolo SNMP y los conceptos fundamentales de su operación, para el desarrollo de sistemas de aplicación específicos.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL:

- Desarrollar un sistema que permita establecer procedimientos de monitoreo sobre elementos específicos ubicados en una red de comunicación de datos, por medio del protocolo SNMP.

1.4.2 OBJETIVOS ESPECÍFICOS:

- Investigar las principales características que poseen los sistemas de comunicación de datos para determinar las estrategias de monitoreo sobre su operación.
- Conocer las principales normas de administración de redes para el desarrollo de un sistema que cumpla con las características necesarias para efectuar una supervisión por medio del protocolo SNMP.
- Determinar los requerimientos y funciones de cada elemento de una red administrada.
- Desarrollar un sistema de supervisión, basado en un sistema operativo, capaz de funcionar en una red, como gestor de las variables involucradas en ella.

1.5 ALCANCES

Con el desarrollo del presente proyecto se logrará:

- Proporcionar una guía práctica para desarrollar un sistema de monitoreo para la administración de redes.
- Brindar conocimientos generales para la comprensión del protocolo SNMP y conceptos relacionados.
- Crear un sistema de monitoreo de redes basado en estándares internacionales de administración.
- Analizar por medio del sistema creado, la información de administración mediante una interfaz de operador, que permita una fácil y rápida comprensión de los resultados obtenidos.
- Determinar los procedimientos de actualización del sistema para el monitoreo de nuevos dispositivos que sean administrables por medio del protocolo SNMP.

1.6 LIMITACIONES

- Los procedimientos de actualización del sistema dependen directamente de la capacidad de integración en sistemas de administración de equipos específicos de comunicaciones creados por ciertos fabricantes.
- Los procedimientos de escritura sobre los elementos administrados estarán limitados por el acceso que los diferentes fabricantes permiten de sus equipos.
- La cuantificación del número máximo de elementos que forman parte de una red administrada, por un solo sistema de monitoreo, depende de diversos elementos específicos de una red.
- El desarrollo del Sistema de Monitoreo para Redes de Datos basado en el Protocolo SNMP será una aplicación de tipo general, que para su operación

será configurado con una marca específica ampliamente utilizada en las empresas locales.

1.7 METODOLOGÍA DE INVESTIGACIÓN

La investigación a realizar es directa como también de tipo documental. En una primera fase se pretende recopilar información bibliográfica y documentación digital, centrando esta investigación en lo que son los protocolos de gestión de administración de redes, así como lo relacionado con las redes de comunicaciones.

Como segunda fase se llevará a cabo una investigación acerca de aplicaciones en sistemas de monitoreo de redes utilizando el protocolo de gestión SNMP.

1.7.1 TECNICAS UTILIZADAS EN LA INVESTIGACION.

- ***Correo electrónico.***

Ha permitido la comunicación con personas que en alguna medida están involucradas en el desarrollo de sistemas de administración de redes, profesionales y otro tipo de personas que tienen conocimiento en aplicaciones similares a la que se está implementando, así como de aquellos foros de discusión en los cuales se tratan temas afines al sistema propuesto.

- ***Investigación bibliográfica.***

Se ha realizado una investigación bibliográfica sobre los diferentes componentes necesarios para la implementación Sistema de Monitoreo para Redes de Datos, Basado en el Protocolo SNMP. El material utilizado incluye libros, revistas, documentación y otro tipo de literatura con información de gran ayuda para el desarrollo del trabajo.

- ***Entrevistas con profesionales.***

Llevadas a cabos con profesionales en el área de Internet y de tecnología de información encargadas o responsables del departamento operaciones de empresas privadas, debido a que estas personas están en contacto con los distintos equipos y tienen relación directa con los problemas que se observan en el mantenimiento de una red de comunicaciones.

- ***Información disponible en WWW.***

Como se sabe Internet es una fuente que permite tener acceso a la más variada información sobre un tema en particular, razón por la cual se ha convertido en la principal técnica de investigación para el presente trabajo, esto porque permite conocer los diferentes aspectos relativos a como llevar a cabo la implementación de cualquier sistema o desarrollo de alguna aplicación en particular, así como también documentación sobre diferentes proyectos y aplicaciones referentes a lo que son los sistemas de gestión y monitoreo.

El WWW se ha convertido en la principal fuente para obtener información para llevar a cabo este trabajo, ya que en El Salvador se cuenta con muy poca documentación relativa a este tipo de aplicación.

Capítulo II
Marco Teórico

2.1 MARCO HISTÓRICO

Desde el desarrollo de los dispositivos semiconductores y la integración en alta escala de dispositivos, las comunicaciones han evolucionado aceleradamente, tanto el campo de la comunicación de voz, como de la comunicación de equipos electrónicos, hasta lograr la integración de las comunicación en las actuales redes de conmutación de paquetes con la capacidad de operar múltiples servicios.

En un principio la comunicación de datos se realizó en forma experimental y regional en organismos militares y de investigación en Estados Unidos y Rusia.

En 1973, la DARPA inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basó en la transmisión de paquetes de información y tenía por objetivo la interconexión entre redes. De este proyecto surgieron dos redes: ARPANET (para investigación) y MILNET (de uso exclusivamente militar).

Para comunicar redes se desarrollaron básicamente dos protocolos: El Protocolo de Internet (IP) y el Protocolo de Control de Transmisión (TCP) que posteriormente se integraron para formar el conjunto de protocolos TCP/IP.

En 1980, se incluyó en el UNIX 4.2 de Berkeley, el conjunto TCP/IP y fue el protocolo militar estándar en 1983. Con el nacimiento en 1983 de Internet, este grupo de protocolos fue extensamente popularizado para formar una interred que es la principal fuente de información en la actualidad.

En 1985, la ARPANET fue ampliamente utilizada y llegó a presentar congestión en los servicios de comunicación, en respuesta a este hecho, la Fundación Nacional de Ciencia, inició la fase 1 del desarrollo de la red NSFNET.

La NSFNET se formó por múltiples redes regionales y redes punto a punto como la "NASA SCIENCE NET", conectadas a través de una estructura constituida sobre la NSFNET.

En 1986, la NSFNET se extendió, como estructura jerárquica, conectando redes regiones y redes de centros de investigación el cual se encontraba conectado a un núcleo principal formado por el enlace entre seis centros de *"Supercomputadoras".*

Los enlaces originales tenían un ancho de banda de 56kbps, el cual fue incrementado en 1988 a enlaces estándar T1 (1.544Mbps). Este fue el resultado de los altos requerimientos de los servicios de comunicación demandados por la NSF.

La red ARPANET dejó de funcionar oficialmente en 1990 y en 1991 el tráfico de datos fue incrementado considerablemente, generando la necesidad de un incremento de los enlaces del núcleo de la NSFNET a enlaces T3 (45Mbps).

En la actualidad el núcleo del Internet se encuentra formado por un conjunto de empresas que se denominan Proveedores de Servicios de Internet (ISP, *Internet Service Providers*) que poseen puntos de conexión, denominados Puntos de Presencia (POS, *Points Of Presence*) en muchas regiones alrededor del planeta.

El término "Proveedores de Servicios de Internet" se utiliza actualmente para cualquier empresa que proporcione conectividad entre redes, sin embargo es común que se pueda distinguir entre proveedores de mayor capacidad (NSP, National Service Providers) y puntos de presencia que permiten el acceso (NAP, *Network Access Point*) a empresas de menor capacidad.

Dada la cobertura global de las empresas dedicadas a la interconexión de redes, el tráfico sé incrementado en forma proporcional, por lo que se han desarrollado nuevas tecnologías para la transmisión sobre medios como fibra óptica con WDM y DWDM, Packet Over SONET (*Syncronous Optical Network*), con estándares de velocidad basados en una Jerarquía SDH (Jerarquía Digital Síncrona) desde 155Mbps hasta el desarrollo de interfaces hasta de 10Gbps.

2.2 FUNDAMENTOS

2.2.1 REDES DE COMUNICACIONES

Una red de comunicaciones consiste en un conjunto de elementos interconectados entre sí por medio de enlaces que permiten la interacción entre cada uno de ellos para soportar el transporte de información de un sitio a otro. Cuando la información transferida en la red posee formato digital y pertenece a dispositivos informáticos se denomina una *red de comunicación de datos*.

Las redes de comunicación de datos pueden clasificarse, en forma general, de acuerdo a dos criterios: por tecnología de transmisión y por escala de cobertura.

Las redes de comunicación de datos, de acuerdo a la tecnología de transmisión que utilizan pueden clasificarse en:

- Redes de Medios Compartidos (Broadcast): Un solo canal de comunicación es compartido por todos los dispositivos o elementos de red. Un paquete de datos enviado por uno de ellos es recibido por todos los restantes, donde se encuentra incluido

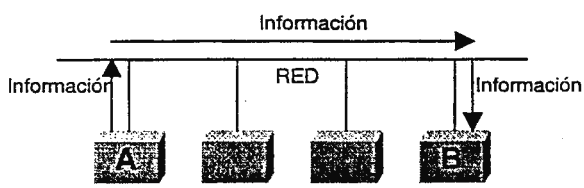


Figura 1. Transmisión Broadcast

restantes, donde se encuentra incluido el destinatario del paquete.

- Redes Punto a Punto: Existen conexiones entre pares individuales de elementos de red. Los paquetes que se envían de un elemento A a un elemento B, pueden circular a través de elementos C y D, donde se utiliza el enrutamiento (*routing*) para dirigirlos.

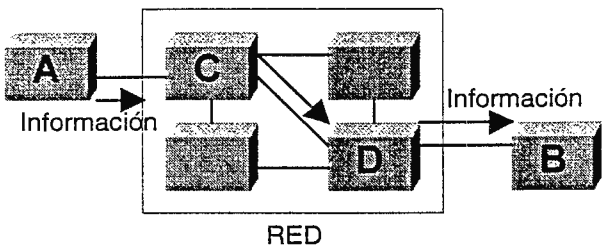


Figura 2. Red Punto a Punto

Generalmente las redes de medios compartidos se emplean en redes de área local, mientras que las redes de Punto a punto en redes de área extensa.

Por la escala de cobertura, las redes pueden clasificarse como:

- Redes de Área Local (LAN): Posee distancias entre elementos de red menores a 1km y altas velocidades de transmisión.
- Redes de Área Extensa (WAN): realizan el enrutamiento de los paquetes para dirigir la información entre dos elementos de red y pueden extenderse hasta 1,000km.

TOPOLOGÍA DE RED

La topología o arquitectura de un sistema de comunicación de datos, identifica la forma en que varias estaciones o elementos de la red se encuentran interconectados. La figura 3 muestra la disposición de la interconexión en cada una de ellas.

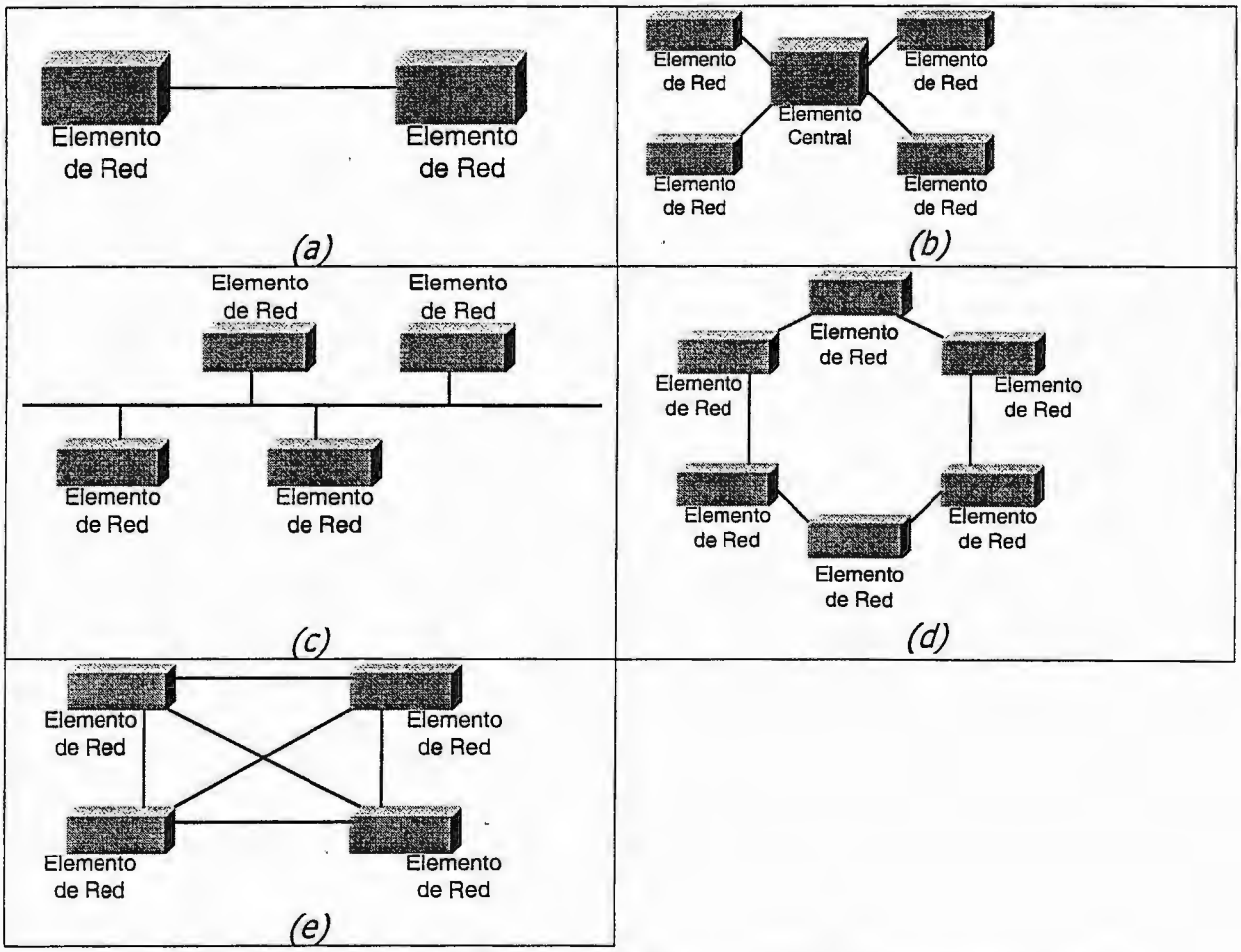


Figura 3. Topologías de red. (a) Punto a Punto; (b) Estrella; (c) Bus o medio compartido; (d) Anillo; (e) Malla Completa.

2.2.2 PROTOCOLOS

De la misma forma que los protocolos están presentes en todo proceso para el establecimiento de comunicación humana, en los dispositivos electrónicos es esencial, desde los de más bajo nivel (por ejemplo, la transmisión de bits en un medio físico) hasta aquellos de más alto nivel (como la ejecución de aplicaciones cliente-servidor en una red informática).

Tomando al modelo OSI (Open Systems Interconection) como referencia podemos afirmar que para cada capa o nivel que él define existen uno o más

protocolos interactuando. Los protocolos se ejecutan entre pares de dispositivos lógicos o físicos iguales.

Por lo tanto, los protocolos establecen una descripción formal de los formatos en que deberán presentar los mensajes para poder ser intercambiados por equipos de comunicaciones y además definen las reglas que se deben seguir para lograr el flujo de la información.

2.2.3 MODELOS DE REFERENCIA.

2.2.3.1 MODELO OSI.

Una de las necesidades más crítica de un sistema de comunicaciones es el establecimiento de estándares, sin ellos sólo podrían comunicarse entre sí, equipos del mismo fabricante y de igual tecnología.

La conexión entre equipos electrónicos ha sido estandarizando paulatinamente siendo las redes telefónicas las pioneras en este campo, por ejemplo la histórica CCITT definió los estándares de telefonía: PSTN, PSDN e ISDN.

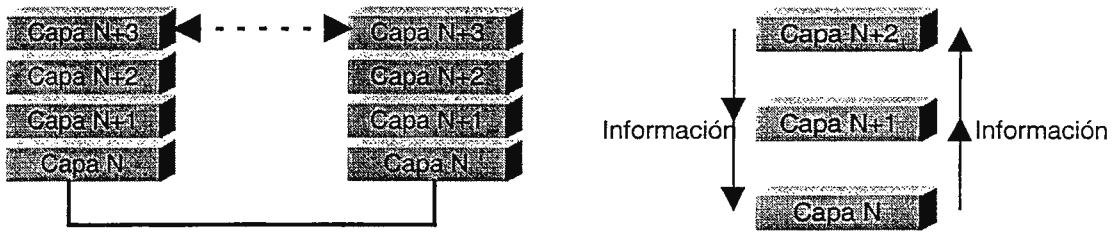
Otros organismos internacionales que generan normas relativas a las telecomunicaciones son: ITU-TSS (antes CCITT), ANSI, IEEE e ISO.

La ISO (International Organization for Standarization) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, proporciona una herramienta teórica para comprender mejor el funcionamiento de las redes de comunicación de datos.

El modelo OSI no garantiza la comunicación entre equipos pero establece las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los aplique estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca.

El modelo OSI consta de 7 capas o niveles. Las características generales de las capas son las siguientes:

- Cada una de las capas desempeña funciones bien definidas.
- Los servicios proporcionados por cada nivel son utilizados por el nivel superior.
- Existe una comunicación virtual entre las mismas capas durante una conexión, de manera horizontal.
- Existe una comunicación vertical entre una capa de nivel **N** y la capa de nivel **N + 1**.



a) Comunicación horizontal entre capas iguales.

b) Comunicación vertical entre capas adyacentes.

Figura 4. Modelo de Capas.

En la tabla 1 se detallan las funciones y aplicaciones de cada unas de las capas del modelo OSI.

Nivel	Nombre	FUNCION	Dispositivos y protocolos
1	Físico	Establece la transmisión del flujo de bits a través del medio.	Cables, tarjetas y hubs. RS-232, X.21, V.35.
2	Enlace	Divide el flujo de bits en unidades con formato (tramas) intercambiándolas mediante el empleo de protocolos de línea.	Bridges, Switches HDLC, PPP y LLC.

3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red. Además proporciona el direccionamiento lógico.	Routers. IP, IPX, AppleTalk.
4	Transporte	Garantiza la entrega confiable de segmentos al receptor por medio de mensajes de reconocimiento. Además establece el control del flujo.	Gateways. UDP, TCP, SPX.
5	Sesión	Administra la comunicación entre las aplicaciones y permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	Gateways.
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de archivos con características diferentes.	Gateways. Compresión, encriptado, VT100.
7	Aplicación	Este nivel proporciona servicios estandarizados para poder realizar funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un archivo).	X.400

Tabla 1. Capas del modelo OSI.

La comunicación en el modelo OSI siempre se realiza entre dos sistemas. Cuando la información se genera en el nivel 7 del emisor, desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7.

En este proceso, cada uno de los niveles divide la información y agrega a los datos información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas o datos de control, formando en cada una *unidades de datos de protocolo* (PDU).

De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va descartando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos transmitidos.

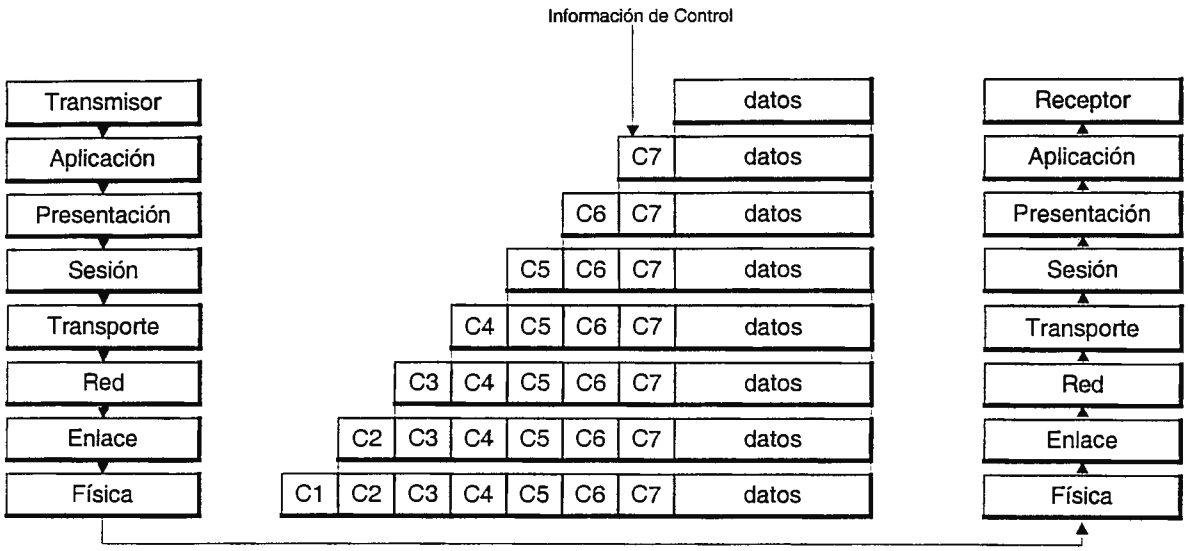


Figura 5. Flujo de Datos, modelo de capas (CN información de control del nivel N).

De esta forma, la información de control que se adiciona en los paquetes, permite que, como ejemplo, el nivel 5 de un sistema local establezca una conexión virtual con el nivel 5 del sistema remoto, de tal forma que la información debe recorrer los niveles 4 al 1 en el sistema local y del 1 al 4 del sistema remoto. A las normas de comunicación entre niveles iguales es a lo que se denomina protocolo.

Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo que garantiza que para modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto.

En las familias de protocolos más utilizadas en redes de computadoras (TCP/IP, IPX/SPX, etc.), se suele encontrar con funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.

2.2.3.2 MODELO TCP/IP.

Las funciones propias de una red de comunicaciones pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI).

Sin embargo la implementación real de una arquitectura puede diferir de este modelo.

El Modelo TCP/IP propone cuatro capas, donde las funciones de las capas de Sesión y Presentación son responsabilidad de la capa de Aplicación y las capas de Enlace de Datos y Física son vistas como la capa de Interface a la Red. Por tal motivo para TCP/IP sólo existen las capas Interface de Red, la de Red, la de Transporte y la de Aplicación.

Como puede verse TCP/IP presupone independencia del medio físico de comunicación, sin embargo existen estándares bien definidos a los nivel de Enlace de Datos y Físico que proveen mecanismos de acceso a los diferentes medios y que en el modelo TCP/IP deben considerarse la capa de Interface de Red; siendo los más usuales el proyecto IEEE 802, Ethernet, Token Ring y FDDI.

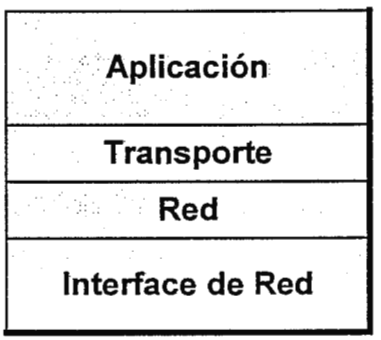


Figura 6. Capas del modelo TCP/IP.

Para entender el funcionamiento de los protocolos TCP/IP debe tenerse en cuenta la arquitectura que ellos proponen para comunicar redes. Tal arquitectura ve como iguales a todas las redes a conectarse, sin tomar en cuenta el tamaño de ellas, ya sean LAN o WAN. Define que todas las redes que intercambiarán información deben estar conectadas a un mismo dispositivo de comunicación o equipo de procesamiento, a tales dispositivos se les denomina *"Puertas de Enlace (Gateways)"*, que generalmente son dispositivos como *"Routers"* o *"Bridges"*.

En la figura 7 se establece una relación entre el conjunto de protocolos TCP/IP y el modelo OSI.

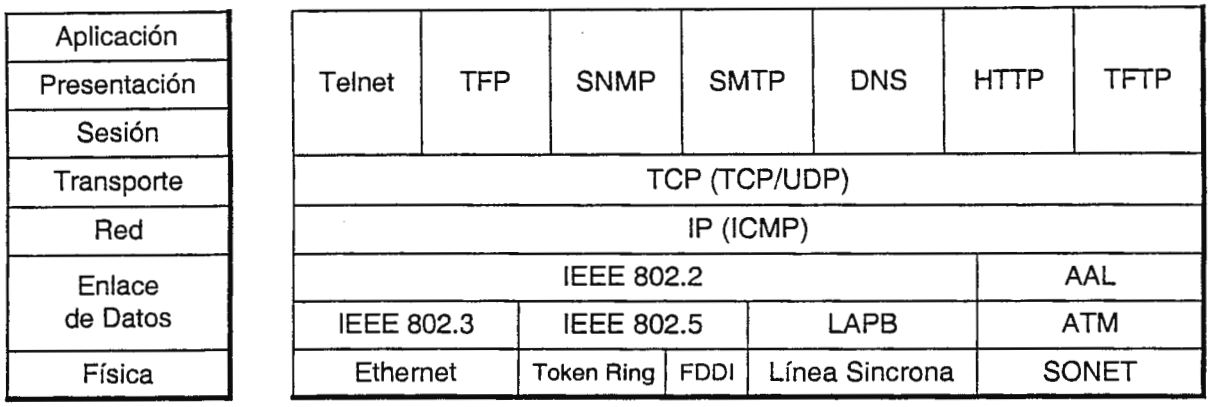


Figura 7. (a) Capas del modelo OSI; (b) Estructura de Protocolos del Modelo TCP/IP.

La figura 7 (b) esquematiza lo que se denomina "Estructura de Protocolos TCP/IP", donde Ethernet, Token Ring, FDDI, Línea síncrona (Redes de Área Ancha) y SONET, son tecnologías de interconexión que definen estándares de acuerdo al medio de transmisión utilizado por cada uno de ellos (Cobre, Fibra Óptica, Radio).

Las normas IEEE 802.2 definen el formato de las tramas que establecen el enlace en la comunicación. AAL es un protocolo de adaptación que se utiliza para la interconexión de redes sobre una plataforma ATM (Modo de Transferencia Asíncrona).

2.3 MARCO CONCEPTUAL

2.3.1 ANTECEDENTES DE LA GESTIÓN DE REDES

El organismo que administra y regula la red Internet encargó en 1987, a un grupo técnico (que se encarga de encontrar soluciones a los problemas técnicos

que plantea el funcionamiento de la red), una solución de gestión integrada para dicha red.

Este grupo técnico propuso una solución que sé dividió en dos fases:

- En la primera fase, utilizar un único protocolo capaz de ser entendido por todos los dispositivos de la red Internet, como solución provisional a corto plazo.
- Posteriormente cuando se desarrollaran las normas OSI, utilizar los protocolos de gestión OSI soportados sobre la plataforma de comunicaciones de Internet. Esta solución se conoce como CMOT (CMIP sobre TCP/IP).

2.3.2 PROTOCOLOS DE GESTION DE REDES

Las cuatro principales arquitecturas de gestión de red que actualmente existen son:

- **Modelo OSI**
- **Modelo TMN**
- **Modelo Internet (SNMP)**
- **RMON**

2.3.2.1 MODELO OSI

ISO ha definido una arquitectura de gestión OSI cuya función es permitir supervisar, controlar y mantener una red de datos. El modelo de Gestión de red OSI está dividido en cinco categorías de servicios de gestión denominadas Áreas Funcionales Específicas de Gestión (*Specific Management Functional Areas*, SMFA). Estas categorías son las siguientes:

- **Gestión de configuración**

La gestión de configuración comprende una serie de facilidades mediante las cuales se realizan las siguientes funciones:

- Activación y desactivación de elementos.
- Definición o cambio de parámetros de configuración.
- Recolección de información de estado.
- Denominación de los elementos de la red.

- **Gestión de fallos**

Detección, diagnóstico y corrección de los fallos de la red y de las condiciones de error en sus elementos. Incluye los siguientes procedimientos:

- Notificación de fallos
- Sondeo periódico en busca de mensajes de error
- Establecimiento de alarmas

- **Gestión de prestaciones**

Se define como la evaluación del comportamiento de los elementos de la red. Para hacer posible este análisis es preciso mantener un histórico con datos estadísticos y de configuración.

- **Gestión de contabilidad**

Determinación de los costos asociados a la utilización de los recursos de la red y la asignación de los correspondientes cargos para los usuarios.

- **Gestión de seguridad**

Comprende el conjunto de facilidades mediante las cuales el administrador de la red modifica la funcionalidad que proporciona seguridad que restringe el acceso no autorizado. Incluye aspectos como la gestión de claves, firewalls e históricos de seguridad.

El proceso de supervisión y control de un objeto *"Gestionable"* se realiza mediante una serie de interacciones. Estas interacciones pueden ser de dos tipos:

- **De operación:** el gestor solicita información al objeto gestionable o requiere realizar una acción sobre él.
- **De notificación:** el objeto gestionable envía información al gestor como consecuencia un evento ocurrido en el dispositivo.

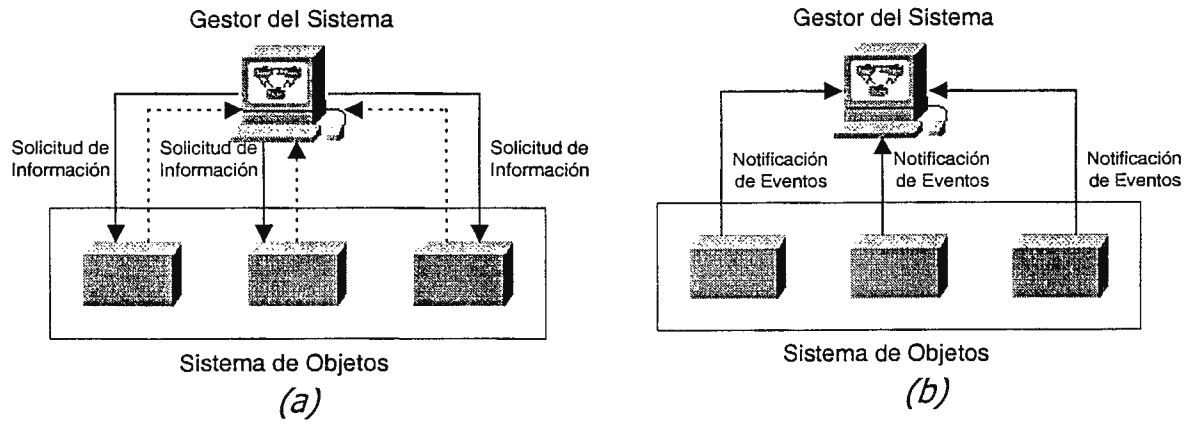


Figura 8. (a) Interacción de Operación; (b) Interacción de Notificación.

Un objeto gestionable se caracteriza además por un conjunto de atributos que son las propiedades, o características del objeto, y un comportamiento en respuesta a las operaciones solicitadas.

Otros componentes de la arquitectura de gestión OSI son:

- **Estructura de la Información de Gestión (*Structure of Management Information,* SMI).** Define la estructura lógica de la información de gestión OSI. Establece las reglas para nombrar, codificar e identificar a los objetos gestionables y a sus atributos. Define un conjunto de subclases y tipos de

atributos que son en principio aplicables a todos los tipos de clases de objetos gestionables.

- **Base de Información de Gestión (*Management Information Base*, MIB)**. Representa la información que se está utilizando, modificando o transfiriendo en la arquitectura de los protocolos de gestión OSI. La MIB conoce todos los objetos gestionables y sus atributos. No es necesario que este centralizada físicamente en un lugar concreto, puede estar distribuida a través del sistema y en cada uno de sus niveles.

- **CMIS (*Common Management Information Services*)**. Consiste en un conjunto de reglas que identifican las funciones de una interfaz OSI entre aplicaciones, utilizado por cada aplicación para intercambiar información. CMIS define la estructura de la información que es necesaria para describir el entorno.

2.3.2.2 MODELO TMN

El término TMN (Telecommunications Management Network) fue introducido por la ITU-T, y está definido en la recomendación M.3010. Aunque en un principio no hubo mucha colaboración entre los grupos de gestión de red de la ISO y el CCITT (antecesor de la ITU-T), posteriormente fueron incorporados los siguientes conceptos del modelo OSI al estándar TMN:

- Se adoptó el modelo gestor-agente del modelo OSI.
- Se siguió el paradigma de la orientación a objetos de la arquitectura OSI.
- Se trabajó conjuntamente en el desarrollo del concepto de dominios de gestión.

Una diferencia entre ambos modelos consiste en la introducción, en el modelo TMN, de una red separada de aquella que se gestiona, con el fin de transportar la información de gestión (Fuera de Banda).

A diferencia del modelo OSI, en el cual se definen cinco áreas funcionales, el estándar TMN no entra en consideraciones sobre las aplicaciones de la información gestionada. Por el contrario, el modelo TMN define las siguientes funcionalidades:

- El intercambio de información entre la red gestionada y la red TMN.
- El intercambio de información entre redes TMN.
- La conversión de formatos de información para un intercambio consistente de información.
- La transferencia de información entre puntos de una TMN.
- El análisis de la información de gestión y la capacidad de actuar en función de ella.
- La manipulación y presentación de la información de gestión en un formato útil para el usuario u operador de la red.
- El control del acceso a la información de gestión por los usuarios autorizados.

Arquitectura TMN

El modelo TMN define su arquitectura en tres grandes grupos:

a) **Arquitectura funcional**, que describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN.
b) **Arquitectura física**, que describe las interfaces y el modo en que los bloques funcionales se implementan en equipos físicos.

c) **Arquitectura de la información,** que sigue los principios de los modelos OSI de gestión (CMIS y CMIP).

En general la arquitectura del modelo TMN trabaja, basado en bloques funcionales que ejecutan los procedimientos de supervisión y control sobre la red gestionada. En la arquitectura funcional se definen cinco tipos de bloques funcionales. Estos bloques capacitan a la TMN para realizar sus tareas de gestión:

- **Función de operación de sistemas (OSF).** Los OSF procesan la información relativa a la gestión de la red con el objeto de monitorear y controlar las funciones de gestión. Es posible definir múltiples OSF dentro de una única TMN.

- **Función de estación de trabajo (WSF).** Este bloque funcional proporciona los mecanismos para que un usuario pueda interactuar con la información gestionada por la TMN.

- **Función de elemento de red (NEF).** Es el bloque que actúa como agente, susceptible de ser monitoreado y controlado. Estos bloques proporcionan las funciones de intercambio de datos entre los elementos de la red y el sistema de gestión.

- **Adaptadores Q (QAF).** Este tipo de bloque funcional se utiliza para conectar a la TMN aquellas entidades que no soportan los puntos de referencia estandarizados por TMN.

- **Función de mediación (MF).** La función de mediación se encarga de garantizar que la información intercambiada entre los bloques del tipo OSF o NEF cumple los requisitos demandados por cada uno de ellos. Puede realizar

funciones de almacenamiento, adaptación, filtrado y condensación de la información.

Estándar TMN

El estándar TMN define una serie de capas o niveles de gestión mediante las cuales se pretende abordar la gran complejidad de la gestión de redes de telecomunicación. Cada uno de estos niveles agrupa un conjunto de funciones de gestión. El estándar LLA define cuáles son esos niveles y las relaciones entre ellos.

Se definen los siguientes niveles:

- **Nivel de Elementos de Red.** Incluye las funciones que proporcionan información en formato TMN del equipamiento de red así como las funciones de adaptación para proporcionar interfaces TMN a elementos de red no-TMN.

- **Nivel de Gestión de Elementos.** Incluye la gestión remota e individual de cualquier elemento de red que se precise para el establecimiento de conexiones entre dos puntos finales para proporcionar un servicio. Este nivel proporcionará funciones de gestión para monitorear y controlar elementos de gestión individuales en la capa de elemento de red.

- **Nivel de Gestión de Red.** Incluye el control, supervisión, coordinación y configuración de grupos de elementos de red constituyendo redes y subredes para la realización de una conexión.

- **Nivel de Gestión de Servicios.** Incluye las funciones que proporcionan un manejo eficiente de las conexiones entre los puntos finales de la red, asegurando un óptimo aprovisionamiento y configuración de los servicios prestados a los usuarios.

- **Nivel de Gestión de Negocio.** Incluye la completa gestión de la explotación de la red, incluyendo contabilidad, gestión y administración, basándose en las entradas procedentes de los niveles de Gestión de Servicios y de Gestión de Red.

2.2.3.3 MODELO DE INTERNET (SNMP)

En 1988, el IAB (Internet Activities Board, Comité de Actividades Inter- Red) determinó la estrategia de gestión para el modelo TCP/IP (Transfer Control Protocol/Internet Protocol). Esto significó el nacimiento de dos esfuerzos paralelos: la solución a corto plazo, SNMP, y la solución eventual a largo plazo, CMOT (CMIP sobre TCP/IP).

CMOT implantaría los estándares del modelo de gestión OSI en el entorno Internet (TCP/IP). CMOT tuvo que afrontar los problemas derivados de la demora en la aparición de especificaciones y la ausencia de implementaciones prácticas. Como consecuencia de ello, la iniciativa CMOT fue paralizada en 1992.

Actualmente, la gestión SNMP es un directo competidor de la Gestión OSI y se siguen definiendo normas para la gestión SNMP. La última implementación del protocolo SNMP es la norma SNMP versión 3, que actualmente esta en la fase de pruebas y desarrollo.

El protocolo SNMP procede del protocolo SGMP (Simple Gateway Management Protocol), que es un Protocolo Sencillo para Gestión de Equipos Informáticos que efectúan enrutamiento de datagramas IP en Internet.

El protocolo SNMP fue desarrollado por los mismos autores que el protocolo SGMP. Estas personas tienen una visión práctica de las redes y desarrollaron el protocolo en solamente unos meses.

SNMP se ha convertido, debido al enorme éxito que ha tenido desde su publicación, en el estándar más popular de gestión de redes. Prácticamente todo el equipamiento de redes puede ser gestionado por SNMP.

Algunas de las funciones que proporciona SNMP son:

- Supervisión del rendimiento de la red y su estado.
- Control de los parámetros de operación.
- Obtención de informes de fallos.
- Análisis de fallos.

Debido a que SNMP es el protocolo gestión central de esta investigación será estudiado con detalle en secciones posteriores.

2.3.2.4 RMON

La especificación RMON (*Remote MONitor*, monitoreo remoto) es una base de información de gestión (MIB) desarrollada por el organismo IETF (Internet Engineering Task Force) para proporcionar capacidades de monitoreo y análisis de protocolos en redes de área local (segmentos de red). Esta información proporciona a los gestores una mayor capacidad para planificar y ejecutar una política preventiva de mantenimiento de la red.

Las implementaciones de RMON consisten en soluciones cliente/servidor. El cliente es la aplicación que se ejecuta en la estación de trabajo de gestión, presentando la información de gestión al usuario. El servidor es el agente que se encarga de analizar el tráfico de red y generar la información estadística. La comunicación entre aplicación y agente se realiza mediante el protocolo SNMP.

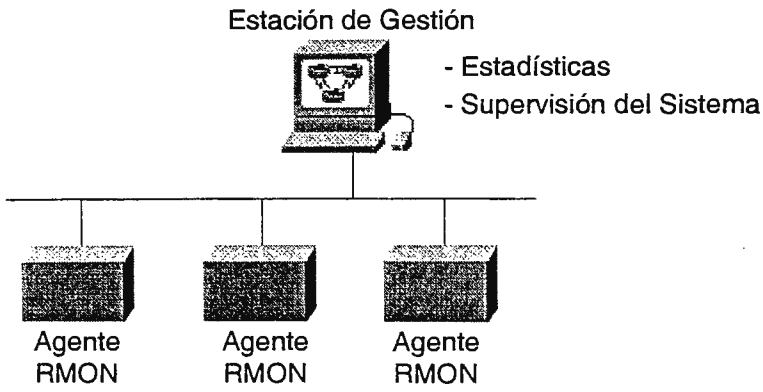


Figura 9. Monitoreo Remoto

RMON es una herramienta muy útil para el gestor de red pues le permite conocer el estado de un segmento de red sin necesidad de desplazarse físicamente hasta el mismo y realizar medidas con analizadores de redes y protocolos.

Las iniciativas se dirigen actualmente hacia la obtención de una mayor y más precisa información. En concreto, se trabaja en la línea de analizar los protocolos de nivel superior, monitoreando aplicaciones concretas y comunicaciones extremo a extremo (niveles de red y superiores). Estas facilidades se incorporarán en versiones sucesivas de la especificación (RMON II).

2.3.2.5 COMPARACION SNMP/CMIP.

A continuación se hace una comparación entre los protocolos SNMP y CMIP:

- SNMP está basado en técnicas de sondeo, mientras que CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.
- CMIP es un protocolo orientado a conexión mientras que SNMP es un protocolo sin conexión. Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino. La seguridad de los datos no es prioritaria para SNMP.

- CMIP permite la implementación de comandos condicionales sofisticados, mientras que SNMP necesita el nombre de cada objeto.
- CMIP permite, mediante una única petición, la recolección de gran cantidad de datos de los objetos gestionables, enviando información de retorno en múltiples respuestas. Esto no está permitido en SNMP.
- CMIP está especialmente preparado para gestionar grandes redes distribuidas; mientras que SNMP está recomendado para la gestión inter-red.
- CMIP realiza una distinción clara entre los objetos y sus atributos. En SNMP no está permitido esto, lo cual hace imposible la reutilización de atributos y definiciones.
- SNMP es, por el contrario de CMIP, un Modelo de Gestión práctico y de rápida implementación y con la instalación de Sistemas de Administración de Red es posible crear funciones que permitan al operador de red hacer más sencilla la tarea sobre la red. Es por esta razón que este protocolo es el seleccionado como estándar universal entre los fabricantes de equipos de telecomunicaciones para su instalación en redes administradas.

2.3.3 DEFINICIÓN DE SISTEMA DE GESTIÓN DE REDES

Se entiende por "Gestión de Redes y servicios de telecomunicaciones" al conjunto de actividades destinadas a garantizar los servicios que prestan las redes.

Actualmente los Sistemas de Comunicaciones prestan servicios a los usuarios utilizando Redes Privadas y Redes públicas. La interconexión entre las mismas proporciona mejores posibilidades en la provisión de servicios pero complica el control de las redes.

El término *"gestión"*, utilizado en muchos y diversos entornos del comportamiento humano, está relacionado con la planificación, el seguimiento, evaluación de costos, control de recursos y actividades.

Aplicando este término al entorno de redes, la gestión de red comprende la administración de los diferentes recursos que constituyen una red. La gestión de red toma la forma de seguimiento, coordinación y control de recursos informáticos y de comunicaciones.

En la actualidad, y debido a la competencia de servicios, las organizaciones y empresas que no disponen de una buena gestión de sus redes y servicios de comunicaciones son cautivas de la tecnología y, en vez de emplear los recursos informáticos para hacer negocios, sus recursos informáticos pueden estar impidiendo el progreso de su negocio.

Entre los problemas que se presentan en la interconexión de redes están:

- Dispositivos diferentes: la interconexión de redes permitió la inserción de diferentes tipos de dispositivos fabricados por diferentes empresas lo que dificulta la integración de un sistema de gestión.

- Administraciones diferentes: la interconexión entre redes de distinto propósito y distinto tamaño, se administran y gestionan de distinta forma.

- Tecnologías de interconexión diferentes: existen redes interconectadas con diferentes topologías, utilizando diferentes tecnologías de transmisión y protocolos.

Ante esta problemática tecnológica surgió la necesidad de implementar una metodología para la gestión de redes capaz de gestionar la configuración de sus componentes, la seguridad, las fallas y el desempeño. Distintos proveedores intentaron resolver algunos de estos problemas en forma puntual y aislada. Unificando las funcionalidades de estos esfuerzos surge el concepto "Network

Management System" (NMS) o Sistema de Gestión de Redes, que fue definido como:

El elemento capaz de realizar el conjunto de actividades que controlan o vigilan el uso de los recursos y proporcionar la posibilidad de supervisar el estado, medir el rendimiento, reconocer actividades anormales en la red y notificar al operador para recuperar el servicio.

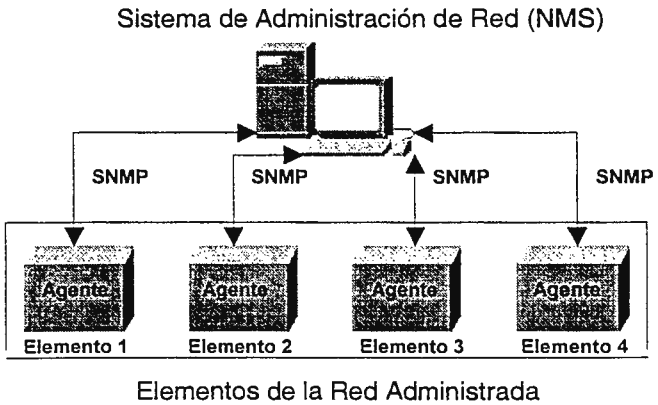


Figura 10. Sistema de Administración de Red (NMS)

El principal objetivo de la gestión de red es garantizar un nivel de servicio en los recursos gestionados con el mínimo costo.

2.3.4 NORMATIVAS PARA LA GESTION DE REDES

El Comité Asesor de Internet (IAB) ha elaborado o adoptado varias normas para la administración de la red. En su mayoría, éstas se han diseñado específicamente para ajustarse a los requerimientos del TCP/IP, aunque, cuando es posible, cumplen con la arquitectura OSI. Un grupo de trabajo en Internet, responsable de las normas para la administración de la red, adoptó un enfoque de dos pasos para cubrir las necesidades actuales y futuras.

El primer paso comprende el uso del Protocolo Simple para Administración de la Red (SNMP), el cual fue diseñado y aplicado por el grupo de trabajo. SNMP

se utiliza actualmente en muchas redes Internet, y está integrado dentro de muchos de los productos comerciales que están disponibles. Conforme se ha mejorado la tecnología, SNMP ha evolucionado y se ha vuelto más completo.

El segundo paso comprende las normas OSI para administración de la red, llamados Servicios Comunes de Información sobre la Administración (Common Management Information Services, CMIS), y al Protocolo Común de Información sobre la Administración (Common Management Information Protocol, CMIP), los cuales se utilizarán en las futuras aplicaciones de TCP/IP. IAB ha publicado *"Common Management Information Services and Protocol over TCP/IP* (CMOT) como una norma para TCP/IP y para la administración OSI.

Tanto SNMP como CMOT utilizan el concepto de los administradores de red que intercambian información con los procesos que se encuentran dentro de los dispositivos de la red, como las estaciones de trabajo, bridges, routers, hubs, multiplexores, etc. La estación de administración primaria se comunica con los diferentes procesos de administración, construyendo la información sobre el estado de la red.

La arquitectura tanto de SNMP como de CMOT es tal, que la información recopilada se almacena en un formato que permite a otros protocolos leerla.

2.4 PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE REDES (SNMP)

2.4.1 ANTECEDENTES.

SNMP realmente no fue el primer protocolo de administración definido para uso en Internet. En 1987, el SGMP fue definido por RFC (Request For Comment) para administrar la red en constante expansión de routers en Internet. Fue un

diseño provisional para pruebas hasta que se desarrollara un protocolo más elaborado.

Un RFC es un documento que circula por Internet con especificaciones de un "estándar" o parte de uno. Desde una introducción general, pedagógica y divertida sobre TCP/IP, hasta las particularidades del SNMP sobre redes IPX. Los RFC's contienen las verdaderas especificaciones de funcionamiento de Internet.

En 1989 se comenzó a desarrollar el protocolo SNMP, teniendo la experiencia proporcionada por la corta vida de SGMP y de la necesidad de administrar otros dispositivos además de routers. Actualmente, la RFC 1157, escrita en 1990, es la actualización más reciente de SNMP versión 1. Relacionado a los estándares SNMP están asociados los estándares *"Management Information Base I y II"*, los cuales definen los contenidos del agente.

Posteriormente aparecieron dos nuevos protocolos: por un lado, la segunda versión del SNMP, que incorpora muchas de las funciones del original (que sigue en uso) e incluye nuevas características que mejoran sus deficiencias. Por otro lado, el CMIP, que estaba mejor organizado y contenía muchas más funciones que las dos versiones del SNMP. Existen muchos protocolos disponibles. Los dos principales son SNMP y CMIP. Generalmente, SNMP trabaja bajo el modelo TCP/IP y CMIP trabaja bajo el modelo OSI.

Típicamente los Sistemas de Administración de Red proveen funcionalidad a ciertas clases de dispositivos. Si se observa el modelo de referencia OSI se notará que la mayoría de los sistemas de administración de red (NMSs) operan hasta la capa 3 y algunas veces hasta la 4. Si se sigue este modelo, entonces la administración debería abarcar por lo menos los siguientes dispositivos:

- **Capa Física**: *Módems, DSU/CSU, multiplexores, HUBs, Repetidores* o algún otro dispositivo que provea acceso físico a un medio de transmisión.

- **Capa de Enlace de datos**: *Bridges, Switches*, o algún otro dispositivo que defina la señalización de datos en un medio físico.
- **Capa de Red**: *Routers, Gateways, Switches layer 3*, o algún otro dispositivo que tome decisiones acerca de dónde los datos irán basados en algún esquema de direccionamiento de red.
- **Capa 4. Transporte**. (opcional) Incluye TCP y UDP, IPX/NCP, SPX o algún otro protocolo que provea conexión orientada a servicios de conexiones entre los nodos finales.

SNMP implementado bajo TCP/IP o aún IPX/SPX, provee administración para muchos de estos dispositivos en forma general sin un software adicional. Nótese que las primeras tres capas especifican dispositivos de hardware, mientras que la capa 4 es expresada puramente en software. La información de la capa 4 puede proveer información útil para la administración de una red, como por ejemplo determinar si un servidor UNIX que está corriendo sobre TCP/IP, tiene conexión TCP con otros servidores y en qué puerto o cuantos broadcast UDP ha generado el servidor.

Para el desarrollo de la administración de redes en Inter-redes basadas en TCP/IP, el IAB decidió seguir una estrategia en la cual a corto plazo se designó el SNMP para administrar los nodos, y se proponía para largo plazo la estructura de administración de redes OSI. Se escribieron entonces dos documentos para definir la administración de la información: RFC 1065 que norma la Estructura de la Información de Administración, SMI; y RFC 1066, que norma la Base de Información de Administración, MIB. Ambos documentos fueron diseñados para ser compatibles con la estructura SNMP y la administración de redes OSI.

Algunas de las especificaciones en el diseño de SNMP fueron:

a) **Administración de red integrada**: capacidad de administrar redes incorporando componentes que vinieran de una variedad de fabricantes con una simple aplicación.

b) **Interoperabilidad:** capacidad de implementar un dispositivo de un proveedor, administrado por el sistema de un proveedor diferente.

c) **Estándares:** definen métodos comunes de comunicación y estructuras de datos de manera que redes diferentes puedan ser integradas con una única administración de red.

Posteriormente se observó que los requerimientos de SNMP y los de administración de redes basadas en el modelo OSI diferían más de lo esperado en un principio, por lo que los requerimientos de compatibilidad entre el SMI y el MIB y ambas estructuras fueron suspendidas.

La IAB ha designado al SNMP, a la SMI y a la Internet MIB inicial como "Protocolos Estándar", con status de "Recomendado" (RFC). Por medio de esta acción, la IAB recomienda que todas las implementaciones de IP y TCP sean administradas por red, y que las implementaciones que son administrables por red se espera que los adopten e implementen.

Así pues, la actual estructura para administración de redes basadas en TCP/IP consiste en:

- Estructura e identificación de la Información de Administración para redes basadas en TCP/IP, que describe cómo se definen los objetos administrados contenidos en el MIB tal y como se especifican en la RFC 1155.

- Protocolo de Administración de Redes Simples, que define el protocolo usado para administrar estos objetos, según se expone en la RFC 1157.

Recomendación	Normalización
RFC1065	Define la estructura de Información (SMI)
RFC1066	Define el formato de las Bases de Información (MIB)
RFC1155	Especifica el contenido de los MIBs
RFC1157	Definición de SNMP Versión 1

Tabla 2. Recomendación para Gestión SNMP.

2.4.2 ¿QUE ES SNMP?

El Protocolo Simple para Administración de la red (SNMP) no es sólo un protocolo, sino tres protocolos que juntos forman una familia; todos diseñados para trabajar en procedimientos de administración. Los protocolos que conforman la familia SNMP y sus papeles se muestran a continuación:

- **Base de Información de la administración (MIB):** Una base de datos, generada por el agente de un elemento administrado, que contiene información del estado de los objetos que compone el elemento en estudio.
- **Estructura e identificación de la información sobre la administración (SMI):** Una especificación que define las entradas en una MIB.
- **Protocolo simple para administración de la red (SNMP):** El conjunto de normas que permiten la comunicación entre los dispositivos administrados y los servidores de administración.

Los dispositivos que tienen integradas las capacidades para SNMP corren un módulo de software agente para administración, cargado como parte de un ciclo de arranque o incluído en la memoria fija (firmware) del dispositivo. A los dispositivos que poseen agentes SNMP se les denomina ***dispositivos administrados.***

Los dispositivos administrados por SNMP se comunican con el software servidor SNMP que está localizado en un elemento de la red. El dispositivo se comunica con el servidor , al igual que el modelo de Gestión OSI, de dos formas: por *sondeo* o por *interrupción.*

En el sondeo de un dispositivo (físico o lógico), el servidor de administración consulta al elemento administrado sobre su condición o sobre sus estadísticas actuales. El sondeo en ocasiones se hace en intervalos regulares, teniendo al servidor conectado a todos los dispositivos administrados de la red. Una desventaja del sondeo es que la información no siempre se encuentra actualizada y por otra parte, el tráfico de la red se incrementa con el número de dispositivos administrados y la frecuencia del sondeo.

Un sistema SNMP basado en la interrupción hace que el dispositivo administrado envíe mensajes al servidor cuando algunas condiciones lo requieran. De esta forma, el servidor conoce inmediatamente cualquier problema (a menos que el dispositivo falle, en cuyo caso la notificación debe hacerse desde otro dispositivo que haya tratado de comunicarse con el dispositivo que falló).

Los sistemas de administración basados en la interrupción tienen, al igual que los basados en sondeo, sus propias desventajas. En primer lugar entre los problemas está la necesidad de ensamblar un mensaje para el servidor, lo que puede requerir de una gran cantidad de ciclos del CPU, todos los cuales se toman de la rutina normal del dispositivo. Si el mensaje que va a enviarse es extenso, como sucede cuando contiene una gran cantidad de estadísticas, la red puede padecer de una notable degradación mientras el mensaje se ensambla y transmite.

Por otra parte, en un sistema de administración basado en interrupción, si existe una falla mayor en cualquier parte de la red, como cuando falla el suministro de energía eléctrica, cada dispositivo administrado por SNMP tratará de

enviar al mismo tiempo, mensajes controlados por interrupción hacia el servidor, para reportar el problema. Esto puede congestionar la red y producir una información errónea en el servidor.

Frecuentemente se utiliza una combinación de sondeo y de interrupción para sobreponerse a todos estos problemas de los sistemas de administración. La combinación se llama sondeo dirigido por trampa (trap), e implica que el servidor haga un sondeo de las estadísticas a intervalos regulares o cada vez que lo ordene el administrador del sistema. Además, cada dispositivo administrado por SNMP puede generar un mensaje de interrupción cuando se presenten ciertas condiciones, pero estos mensajes tienden a estar más rigurosamente definidos que en el simple sistema controlado por interrupción. Después de recibir un mensaje de interrupción con sondeo dirigido por trampa, el servidor puede seguir sondeando al dispositivo para mayores detalles, en caso de ser necesario.

Por lo general, SNMP se utiliza como una aplicación cliente/servidor asincrónica, lo que significa que tanto el dispositivo administrado como el software servidor SNMP pueden generar un mensaje para el otro y esperar una respuesta, en caso de que haya que esperar una. Ambos lo empaquetan y manejan el software para red (como el IP) como lo haría cualquier otro paquete. SNMP utiliza UDP como un protocolo de transporte de mensajes. El puerto 161 de UDP se utiliza para todos los mensajes, excepto para las trampas, que llegan al puerto 162 de UDP. Los agentes reciben sus mensajes del administrador a través del puerto UDP 161 del agente.

Puerto UDP	**Mensajes**
161	Solicitud de información/configuración
162	Mensajes asíncronos (Traps)

Tabla 3. Puertos utilizados para las conexiones SNMP.

SNMP versión 2 añade algunas nuevas posibilidades a la versión anterior de SNMP, de las cuales, la más útil para los servidores es la operación *get-bulk.* Esta permite que se envíen un gran número de entradas MIB en un solo mensaje, en vez de requerir múltiples consultas *get-next* como lo hace SNMP versión 1. Además, SNMP v2 tiene mayor seguridad que SNMP v1, evitando que los intrusos observen el estado o la condición de los dispositivos administrados. Tanto la encriptación como la autentificación están soportadas por SNMP v2. SNMP v2 es un protocolo más complejo y no se usa tan ampliamente como SNMP v1.

EL SNMP reúne todas las operaciones en el *paradigma obtener-almacenar* (fetch store paradigm). Conceptualmente, el SNMP contiene sólo dos comandos que permiten a un administrador buscar y obtener un valor desde un elemento de datos o almacenar un valor en un elemento de datos. Todas las otras operaciones se definen como consecuencia de estas dos operaciones.

La interacción entre un NMS y el dispositivo administrado se puede llevar a cabo a través de cuatro diferentes tipos de comandos:

a) **Lectura:** para monitorear los dispositivos administrados, los Sistemas de Administración leen las variables contenidas dentro de los dispositivos.

b) **Escritura:** para controlar los dispositivos administrados, los Sistemas de Administración escriben variables que son almacenadas dentro de los dispositivos administrados.

c) **Operaciones transversales:** Los Sistemas de Administración utilizan esta operación para determinar cuales variables son soportadas por un dispositivo administrado y la secuencia para obtener estas variables de las tablas de información, por ejemplo las tablas de ruteo IP, en los dispositivos administrados.

d) Trampas: los dispositivos administrados utilizan trampas (traps) para reportar asincrónicamente ciertos eventos a los Sistemas de Administración.

La mayor ventaja de usar el paradigma obtener-almacenar es la estabilidad, simplicidad, flexibilidad. El SNMP es especialmente estable ya que sus definiciones se mantienen fijas aun, cuando nuevos elementos de datos se añaden al MIB y se definen nuevas operaciones como efectos del almacenamiento de esos elementos.

A pesar de su extenso uso, SNMP tiene algunas desventajas. La más importante es que ese apoya en UDP. Puesto que UDP no tiene conexiones, no existe contabilidad inherente al enviar los mensajes entre el servidor y el agente. Otro problema es que SNMP proporciona un solo protocolo para mensajes, por lo que no pueden realizarse los mensajes de filtrado. Esto incrementa la carga del software receptor. Finalmente, SNMP casi siempre utiliza el sondeo en cierto grado, lo que ocupa una considerable cantidad de ancho de banda.

2.4.3 TECNOLOGIA SNMP

Sorprendentemente, SNMP v2 no proporciona gestión de red. En lugar de eso SNMP v2 proporciona un marco de trabajo en el que se pueden construir aplicaciones de gestión de red. Estas aplicaciones, como la gestión de fallos, monitoreo del rendimiento, contabilización de tiempo, etc. están fuera del ámbito del estándar. Lo que proporciona SNMP v2 es la infraestructura de la gestión de la red.

La esencia de SNMP v2 es un protocolo que se utiliza para intercambiar información de gestión. Cada elemento en un sistema de gestión de red mantiene una base de datos local de la información relevante de gestión de red, conocida como base de información de gestión (MIB). El estándar SNMP v2 define la

estructura de esta información y los tipos de datos permitidos; esta definición se conoce como estructura de información de gestión (SMI). El estándar también proporciona varias MIB que son generalmente útiles para la gestión de red. Además, los vendedores y los grupos de usuarios pueden definir nuevas bases de datos sobre información de administración (MIBs).

SNMP v2 dará apoyo a una estrategia de gestión de red altamente centralizada o distribuida. En este último caso, algunos sistemas operan con ambas funciones, el de gestor y el de agente. En su papel de agente, un sistema aceptará órdenes de un sistema de gestión superior. Algunas de estas órdenes están relacionadas con la MIB local en el agente. Otras órdenes requieren que el agente actúe como delegado para dispositivos remotos. En este caso, el agente delegado asume el papel de gestor para acceder a la información en un agente remoto, y después asume el papel de agente para pasar esa información a un gestor superior.

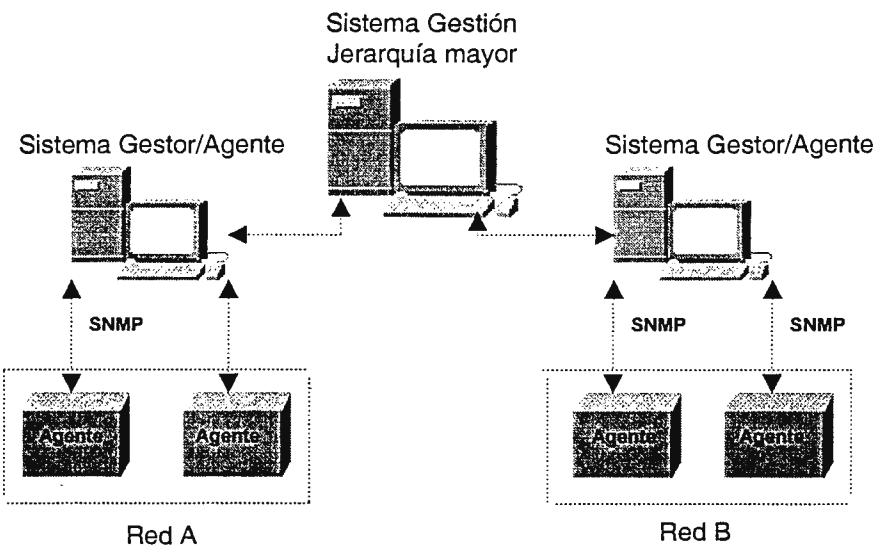


Figura 11. Sistemas Jerárquicos de Administración.

2.4.4 OPERACIÓN DEL PROTOCOLO SNMP.

2.4.4.1 FUNCIONAMIENTO DEL PROTOCOLO.

El funcionamiento del protocolo se puede entender a partir de dos instancias: los elementos de procedimiento y la estructura de una PDU[1].

Elementos de procedimiento.

A continuación se describen las acciones que realiza una entidad de protocolo en una implementación SNMP. Se definirá la dirección de transporte como una dirección IP seguida de un número de puerto UDP, asumiendo que se está utilizando el servicio de transporte UDP.

a) Cuando una entidad de protocolo envía un mensaje, realiza las siguientes acciones:
   - Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1
   - Pasa la PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autenticación. Este servicio generará en respuesta otro objeto en ASN.1
   - La entidad construye ahora un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autenticación y el nombre de la comunidad.
   - Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.

b) Cuando una entidad de protocolo recibe un mensaje, realiza las siguientes acciones (esquematizado en la figura 12):

[1] PDU es la unidad de datos de protocolo y constituye el formato de los mensajes enviados en la red para transferir información.

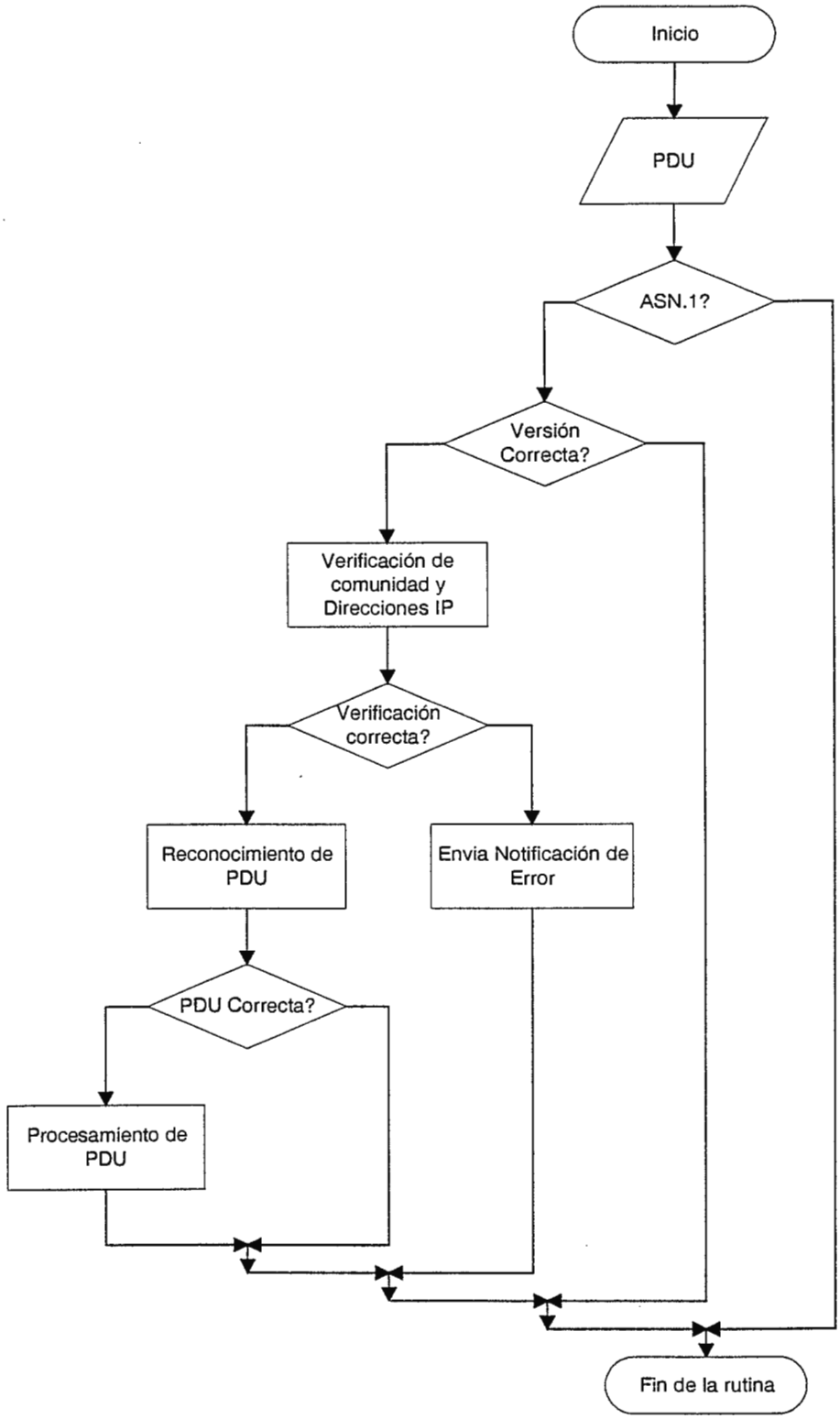


Figura 12. Diagrama de flujo para el proceso de recepción de una PDU - SNMP.

- Hace un pequeño análisis para ver si el datagrama recibido se corresponde con un mensaje en ASN.1. Si no lo reconoce, el datagrama es descartado y la entidad no realiza más acciones.
- Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.
- Pasa los datos de usuario, el nombre de comunidad y las direcciones de transporte de fuente y destino al servicio de autenticación. Si es correcto, este devuelve un objeto ASN.1 Si no lo es, envía una indicación de fallo. Entonces la entidad de protocolo puede generar una trampa (trap), descarta el datagrama y no realiza más acciones.
- La entidad intenta reconocer la PDU. Si no la reconoce, descarta el datagrama. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU. Si la PDU exige respuesta, la entidad iniciará la respuesta ahora.

Estructura de una PDU.

Una PDU Genérica contiene los datos mostrados en la figura 13.

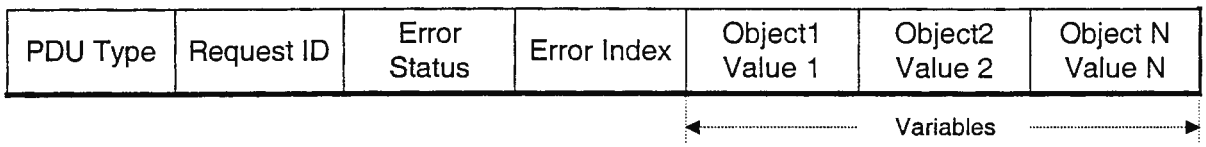


Figura 13. Campos de una PDU -SNMP Genérica.

- **PDU type:** Número entero que indica el orden de emisión de los datagramas. Este parámetro sirve también para identificar datagramas duplicados en los servicios de datagramas poco fiables.

- **Request ID:** Identificación de Requisición, asocia las demandas de SNMP con las peticiones.

- **Error Status:** Estado de Error, indica la presencia de errores y el tipo de errores. Solamente una operación de respuesta es posible en éste campo. Otras operaciones colocan éste campo en cero. Puede tomar los valores mostrados en la tabla 4.

Valor de Error	Tipo de Error	Descripción
(0)	NoError	No existe Error
(1)	TooBig	Exedido el tamaño máximo
(2)	NoSuchName	Nombre desconocido
(3)	BadValue	Valor erróneo
(4)	ReadOnly	Valor de Solo lectura
(5)	GenErr	Error General

Tabla 4. Tipos de Error en el campo de error de una PDU Genérica.

- **Error Index:** Indice de Error. asocia un error con un objeto de instancia en particular. Solamente una operación de respuesta puede colocar éste campo. Otras operaciones colocan éste campo en cero.

- **VarBindList (variables):** Lista de nombre de variables con su valor asociado. Algunas PDU quedan definidas sólo con los nombres, pero aún así deben llevar valores asociados. Se recomienda para estos casos la definición de un valor nulo (NULL).

Para la construcción de un datagrama de PDU, el protocolo SNMP se auxilia de cinco comandos básicos, que permiten extraer o colocar la información en los agentes administrados. Los comandos son:

a) GetRequest-PDU y GetNextRequest-PDU (Mensaje de Solicitud y Mensaje de próxima solicitud, en los casos que se realizan múltiples requisiones)

b) SetRequest-PDU (Mensaje de solicitud de configuración de parámetros en el elemento administrado).
c) GetResponse-PDU (Mensaje de solicitud de respuesta).

A continuación se describe más detalladamente el significado de cada uno de los tipos de PDU.

a) GetRequest-PDU y Get NextRequest-PDU.

Son PDUs que solicitan a la entidad destino los valores de ciertas variables. En el caso de GetRequest-PDU estas variables son las que se encuentran en la lista VarBindList; en el de GetNextRequest-PDU son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista. Como se puede observar, GetNextRequest-PDU es útil para completar tablas de información sobre un MIB específico.

Siempre tienen a cero los campos ErrorStatus y ErrorIndex. Son generadas por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Estas PDUs siempre esperan como respuesta una GetResponse-PDU.

b) SetRequest-PDU.

Ordena a la entidad destino poner a cada objeto reflejado en la lista VarBindList el valor que tiene asignado en dicha lista. Es idéntica a GetRequest-PDU, excepto por el identificador de PDU. Es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Espera siempre como respuesta una GetResponse-PDU.

c) GetResponse-PDU.

Es una PDU generada por la entidad de protocolo sólo como respuesta a GetRequest-PDU, GetNextRequest-PDU o SetRequest-PDU. Contiene o bien la información requerida por la entidad destino o bien una indicación de error.

Cuando una entidad de protocolo recibe uno de los comandos anteriores, sigue las siguientes reglas:

- Si algún nombre de la lista (o el sucesor lexicográfico de un nombre en el caso de Get NextRequest-PDU) no coincide con el nombre de algún objeto en la lista del MIB al que se pueda realizar el tipo de operación requerido ("Set" o "Get"), la entidad envía al remitente del mensaje una Get Response-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 2 (noSuchName), y con el campo ErrorIndex indicando el nombre de objeto en la lista recibida que ha originado el error.

- De la misma manera actúa si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era una GetRequest-PDU.

- Si se ha recibido una SetRequest-PDU y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, salvo en que el campo ErrorStatus tendrá el valor 3 (badValue) y el campo ErrorIndex señalará el objeto de la lista que ha generado el error.

- Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 1 (tooBig).

- Si el valor de algún objeto de la lista no puede ser obtenido (o alterado, según sea el caso) por una razón no contemplada en las reglas anteriores, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 5 (genErr) y el campo ErrorIndex indicando el objeto de la lista que ha originado el error.

Si no se llega a aplicar alguna de estas reglas, la entidad enviará al remitente una GetResponse- PDU de las siguientes características:

- Si es una respuesta a una GetResponse-PDU, tendrá la lista VarBindList recibida, pero asignado a cada nombre de objeto el valor correspondiente.

- Si es una respuesta a una GetNextResponse-PDU, tendrá una lista VarBindList con todos los sucesores lexicográficos de los objetos de la lista recibida, que estén en la lista del MIB relevante y que sean susceptibles de ser objeto de la operación "Get", junto con cada nombre, aparecerá su correspondiente valor.

- Si es una respuesta a una SetResponse-PDU, será idéntica a esta, pero antes la entidad asignará a cada variable mencionada en la lista VarBindList su correspondiente valor. Esta asignación se considera simultánea para todas las variables de la lista.

En cualquiera de estos casos, el valor del campo ErrorStatus es 0 (noError), igual que el de ErroIndex. El valor del campo RequestID es el mismo que el de la PDU recibida.

d) Trap-PDU.

Es una PDU que indica una excepción o trampa. Es generada por una entidad de protocolo sólo a petición de una entidad de aplicación SNMP. Cuando una entidad de protocolo recibe una Trap-PDU, presenta sus contenidos a su entidad de aplicación SNMP.

Los datos que incluye una Trap-PDU son los siguientes:

- **enterprise:** Determina el tipo de objeto que ha generado la trampa.
- **agent-addr:** Dirección del objeto que ha generado la trampa.
- **generic-trap:** Número entero que indica el tipo de trampa. Puede tomar los valores mostrados en la tabla 5.
- **specific-trap:** entero con un código específico.
- **Time-stamp:** tiempo desde la última indicación de la entidad de red y la generación de la trampa.
- **Variable-bindings:** lista tipo VarBindList con información de posible interés.

Valor de Error	Tipo de Error	Descripción
(0)	coldStart	Arranque frío
(1)	warmStart	Arranque Caliente
(2)	linkDown	Conexión perdida
(3)	linkUp	Conexión establecida
(4)	authenticationFailure	Fallo en la autenticación
(5)	egpNeighborLoss	Vecindad egp perdida
(6)	enterpiseSpecific	Trap específica

Tabla 5. Tipos de Trampa Generados por una entidad de protocolo SNMP.

A continuación se describen las trampas genéricas mostradas en la tabla 5.

Trampa de arranque frío (COLDSTART)

la entidad de protocolo remitente se está reinicializando de forma que la configuración del agente o la implementación de la entidad de protocolo puede ser alterada. Por ejemplo, un trap podría ser mandado por un router que recién ha sido configurado y requiere reiniciarse para que los cambios tengan efecto.

Trampa de arranque caliente (WARMSTART)

La entidad de protocolo remitente se está reinicializando de forma que ni la configuración del agente ni la implementación de la entidad de protocolo se altera.

Trampa de conexión perdida (LINKDOWN)

La entidad de protocolo remitente reconoce un fallo en uno de los enlaces de comunicación representados en la configuración del agente. Esta Trap-PDU contiene como primer elemento de la lista variable-bindings el nombre y valor de la interfaz afectada. Por ejemplo, una interfase en un router que se ha dañado o un archivo en un servidor con un NIC^2 fallo.

Trampa de conexión establecida (LINKUP)

La entidad de protocolo remitente reconoce que uno de los enlaces de comunicación de la configuración del agente se ha establecido. El primer elemento de la lista variable-bindings es el nombre y el valor de la interfaz afectada.

Trampa de fallo de autenticación (AUTHENTICATIONFAILURE)

La entidad de protocolo remitente recibe un mensaje de protocolo que le indica que no ha sido autenticado.

Trampa de pérdida de vecino egp (EGPNEIGHBORLOSS)

Un vecino EGP con el que la entidad de protocolo remitente estaba emparejado ha sido seleccionado y ya no tiene dicha relación. El primer elemento de la lista variable-bindings es el nombre y el valor de la dirección del vecino afectado.

Trampa específica (ENTERPRISESPECIFIC)

La entidad remitente reconoce que ha ocurrido algún evento específico. El campo *specifictrap* identifica qué trampa en particular se ha generado.

El protocolo SNMP por sí sólo es un protocolo de consulta y respuesta. El NMS puede enviar múltiples consultas sin recibir ninguna respuesta, ya que no es un protocolo orientado a la conexión. Sin embargo la operación del protocolo SNMP se puede definir a partir de seis comandos básicos:

- **Get:** permite al administrador (NMS) recibir un objeto de instancia de parte de un elemento administrado.

- **GetNext:** permite al administrador recibir el próximo objeto de instancia de una tabla o de una lista contenida en un elemento administrado.

- **GetBulk:** es un comando nuevo para la versión 2 de SNMP. La Operación GetBulk fue agregada para hacer más fácil la operación de adquirir grandes cantidades de información sin necesidad de realizar la operación GetNext. La operación GetBulk fue creada para eliminar virtualmente la necesidad de utilizar la operación GetNext.

[2] NIC, Iniciales de Network Interface Card (Tarjeta de Interface de Red).

- **Set:** permite al administrador NMS colocar un valor en el objeto de instancia con la ayuda de un agente.

- **Trap:** usado por el agente en forma asincrónica para informar al NMS de algunos eventos ocurridos en el elemento administrado.

- **Inform:** comando nuevo en SNMP v2. El comando de información fue creado para permitir al NMS enviar información de un trap a otro NMS.

SEGURIDAD EN SNMP

El protocolo SNMP v2 incluye dos protocolos de seguridad: uno para la autenticación y el otro para la privacidad. Estos dos protocolos son llamados: *Digest Authentication Protocol* y el *Symmetric Privacy Protocol.*

El ***Digest Authentication Protocol*** verifica que el mensaje recibido es el mismo que fue enviado. La integridad de los datos es protegida usando un mensaje parecido de 128 bits, el cual es calculado de acuerdo al algoritmo MD5 (Message Digest 5). El mensaje es calculado al enviar lo y encapsularlo de acuerdo al SNMPv2. El receptor verifica el mensaje parecido (digest). Un valor conocido solamente por el emisor y el receptor, es utilizado como prefijo del mensaje. Después de que el digest es usado para verificar la integridad del mensaje, el valor secreto es usado para verificar el mensaje de origen.

Para garantizar la privacidad del mensaje, se utiliza el ***Symetric Privacy Protocol*** (El protocolo de simetría de privacidad), el cual utiliza una llave de encriptación secreta que es conocida solamente por el emisor y el receptor. Después de que el mensaje es autenticado, éste protocolo utiliza el algorítmo *Data Encryption Standard* (DES), estándar de encriptación de datos, para efectuar la

privacidad. El protocolo DES está documentado por la ANSI (American National Standards Institute) y la NIST (National Institute of Standards and Technology).

2.4.4.2 ESTRUCTURA DEL PROTOCOLO.

Los mensajes SNMPv2 constan de un encabezado y una PDU. La estructura básica se muestra en la figura 14.

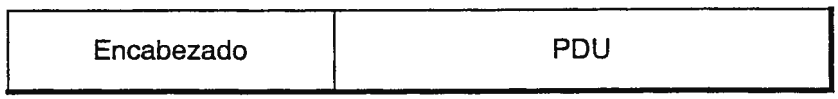


Figura 14. Estructura básica del mensaje SNMP Versión 2.

- **Encabezado del mensaje:** el encabezado del mensaje en SNMPv2 consta de dos campos: Número de versión y Nombre de la comunidad.

  a) Número de versión: especifica la versión de SNMP que se está utilizando en el mensaje.

  b) Nombre de la comunidad: define un ambiente de acceso para un grupo de NMSs. Se dice que los NMSs dentro de una comunidad existen dentro del mismo dominio administrativo. Los nombres de comunidad sirven como una forma vaga de autenticación ya que los dispositivos que no saben el nombre adecuado de la comunidad son eliminados de las operaciones en SNMP.

- **PDU**: SNMPv2 especifica dos formatos de PDU, dependiendo de la operación del protocolo SNMP, una es la PDU que hace referencia a los comandos Get, GetNext, Inform, Response, Set y Trap; y la otra PDU es la que hace referencia al comando GetBulk.

a) PDU para Get, GetNext, Inform, Response, Set y Trap.

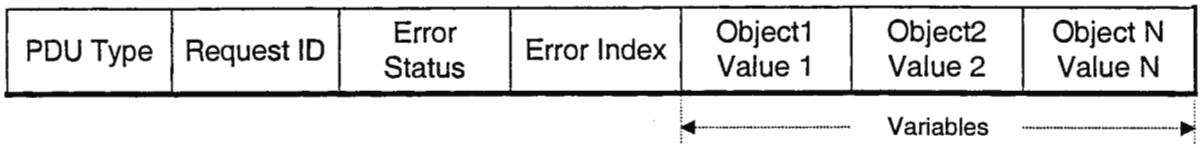


Figura 15. PDU utilizado en SNMP v2 para los comandos Get, GetNext, Inform, Response, Set y Trap.

- **Tipo de PDU:** identifica el tipo de PDU transmitido (Get, GetNext, Inform, Response, Trap).

- **Solicitud de ID:** asocia las solicitudes de SNMP con respuestas.

- **Status de error:** indica uno de muchos errores y tipos de error. Solamente la operación respuesta activa este campo. Las demás operaciones fijan el valor de este campo en cero.

- **Indice de error:** asocia un error con una instancia de objeto particular. Solamente la operación respuesta activa este campo. Las demás operaciones fijan el valor de este campo en cero.

- **Enlace de variables:** sirven como el campo de datos del PDU en SNMPv2. Cada enlace de variable asocia una instancia de objeto particular con su valor actual (a excepción de las solicitudes Get y GetNext, para las que se ignora el valor).

b) PDU para GetBulk.

La PDU enviada en la operación GetBulk está formada por los siguientes campos:

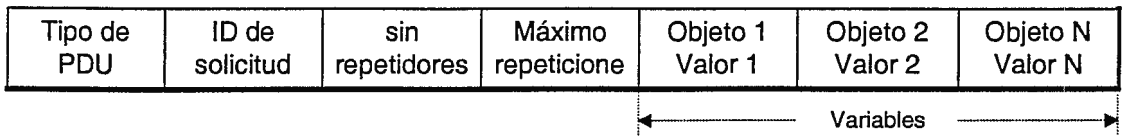


Figura 16. PDU utilizado para el comando GetBulk en SNMP v2.

- **Tipo de PDU:** Identifica la PDU como una operación GetBulk.

- **Solicitud de ID:** Asocia las solicitudes de SNMP con respuestas.
- **Sin repetidores:** Especifica el número de instancias del objeto en el campo de enlaces que se deben acceder no más de una vez desde el comienzo de la solicitud. Este campo se utiliza cuando algunas de las instancias son objetos escalares con una sola variable.

- **Máximo de repeticiones:** Define la cantidad máxima de veces que se deben acceder otras variables, que no sean las especificadas en el campo sin repeticiones.

- **Variables:** Sirve como el campo de datos de PDU en SNMPv2. Cada enlace de variables asocia una instancia de objeto particular con su valor actual (a excepción de las solicitudes Get, GetNext, para las cuales se ignora el valor).

2.5 BASE DE INFORMACION PARA LA ADMINISTRACION (MIB).

Es un método de descripción de objetos administrados especificando los nombres, tipos y el orden de los campos que hacen el objeto. Hay un solo árbol MIB definido por ISO. Sin embargo, parte de este árbol tiene secciones para propietarios específicos. Usualmente cada propietario tiene su propio MIB que contiene sus propios nombres de variables (por ejemplo, IBM, HP, etc). Los MIB's

de empresas son hechas por propietarios de sus objetos particulares. Hay muchas MIB's de empresas, por ejemplo: CISCO Systems, Cabletron, IBM, RAD, etc.

Existen dos tipos de MIB, llamados MIB-1 y MIB-2. Las estructuras son diferentes, MIB-1 se utilizó a principios de 1988 y tiene 114 entradas en la tabla, las cuales están divididas en grupos. Para que un dispositivo administrado pueda ser compatible con MIB-1, debe manejar grupos que son aplicables a ésta. Por ejemplo, una impresora administrada no tiene que aplicar todas las entradas que traten con el Protocolo para Gateway Exterior (Exterior Gateway Protocol, EGP), el cual generalmente lo aplican solamente los routers y los dispositivos similares.

MIB-2 es una ampliación a MIB-1 hecha en 1990, está formada por 171 entradas que están divididas en diez grupos. Las adiciones amplían algunas de las entradas de los grupos básicos de MIB-1 y agregan tres nuevos grupos. Al igual que con MIB-1, un dispositivo SNMP que pretenda ser compatible con MIB-2 debe adaptar todos esos grupos que son aplicables a ese tipo de dispositivo. Muchos dispositivos que son compatibles con MIB-1 no son compatibles con MIB-2.

En general, las versiones MIB-1 y MIB-2 definen los objetos que están contenidos dentro del agente. Cuando los estándares para SNMP fueron escritos se determinó que había necesidad de tener un formato estándar para la información dentro de un agente que se comunicara con el protocolo de administración. Este formato estándar fue definido como la Estructura de Administración de Información (SMI). El MIB es un árbol jerárquico que contiene definiciones para una lista estándar de funciones o características para ser administradas en el dispositivo. Estas funciones o características son referidas como objetos.

Cada objeto en el MIB tiene un número de características que le permiten trabajar con SNMP para proveer sus funciones básicas (Get, GetNext, Set, Trap). Las características que son comunes a cada objeto son:

Característica del objeto	Definición	Valores
Acceso	Acceso Directo al MIB	• Sólo lectura • Lectura - escritura • Sólo escritura • No Accesible
Estado	El estado indica si este objeto deberá ser implementado por el objeto MIB, es decir, si un agente deberá o no seguir un punto en particular del dispositivo monitoreado.	• Obligatorio • Opcional • Obsoleto
Descripción	Describe el objeto que provee.	-
Sintaxis	Describe el formato propio para el valor que deberá tener el objeto.	-

Tabla 6. Características de un objeto MIB.

Cada objeto en el MIB es únicamente identificado por una clase de direccionamiento llamado Objeto Identificador (OID). El OID es una notación conveniente para localizar un objeto en el MIB, y frecuentemente será referido a los administradores de red cuando le solicite información de estado a un dispositivo.

Cuando la IETF definió el MIB intentó construir en "árbol" que incluyera no solo información del MIB sino otros tipos de información, definiciones para otras organizaciones, además de la IETF, y otros tipos de información además de administración de redes. Mientras esto parecía mucha información, el MIB-2 representa solo una "rama" en el árbol.

La información de la MIB (que es la base de datos de información mantenida por el agente, de la que el gestor puede solicitar o fijar datos) pertenece al tipo de datos identificador de objetos (object identifier). Un identificador de objetos es un tipo de dato que especifica un objeto nombrado por una autoridad u organización responsable en un grupo de identificadores. El identificador de objeto es una secuencia de números enteros separados por puntos, y sigue una estructura que está de acuerdo con el árbol MIB jerarquizado.

La estructura y jerarquía del árbol MIB se muestra en la figura 17.

Un número MIB se divide en grupos, que a su vez pueden subdividirse en más subgrupos, y cada dato de la MIB puede tener atributos de lectura, escritura, o ambos, además de estar definido dentro de alguno de los grupos de datos anteriormente anunciados.

Cada variable de la MIB debe ser identificada cuando se la referencia a través de SNMP, y sólo se podrán referenciar nodos simples, no columnas enteras. Las variables simples se referencian añadiendo un ."0" al identificador de objeto de la variable.

Hay un orden implícito en la MIB basado en el orden de los identificadores de objeto. Todas las entradas de las tablas de la MIB están ordenadas según sus identificadores de objeto. Esto supone que habrá un "antes" y un "después" de cada variable (se recorren las columnas de la tabla en vertical, y de las columnas de la izquierda hacia las de la derecha).

El contenido del MIB de un agente concreto se define usando la ASN.1 (Abstract Syntax Notation) lo que permite al software gestor incorporar a su base de datos la información de gestión de cualquier nuevo agente.

Manejando adecuadamente un número MIB, un gestor SNMP puede realizar:

- Modificaciones de las tablas de ruteo de un router.
- Conocer las estadísticas de funcionamiento de un servidor.
- Desconectar una estación de trabajo de la red.
- Ver los paquetes que circulan por una subred.
- Conocer la temperatura de funcionamiento de un módem.

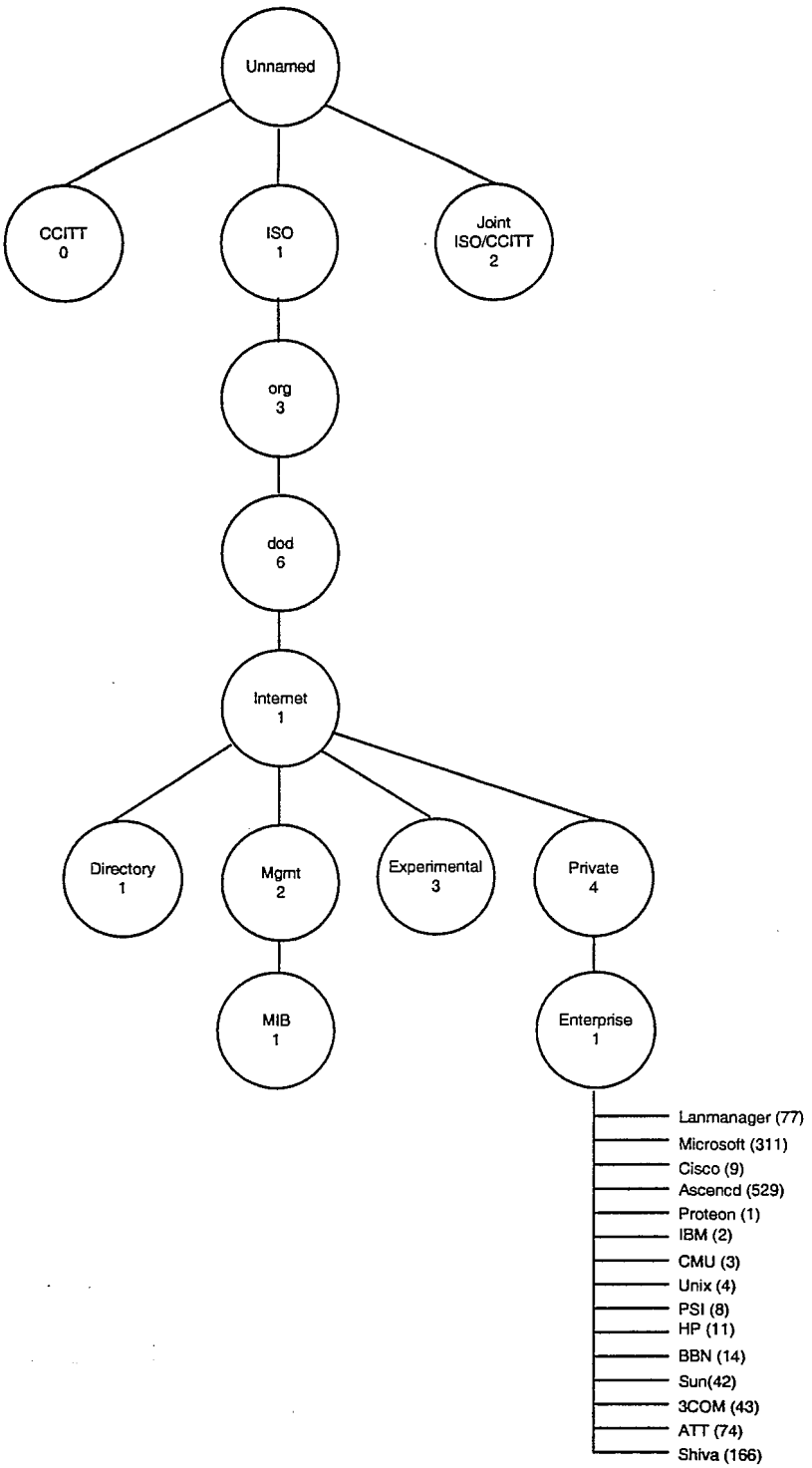


Figura 17. Estructura para las Bases de Información de Administración (MIBs).

Los tipos de objetos utilizados en las variables almacenadas en las MIBs se detallan en la tabla 7.

Categoría MIB	Incluye información sobre:
system	Sistema operativo del anfitrión o del router.
interfaces	Interfaz de red individual.
addr.trans	Dirección de traducción.
ip	Software de Protocolo de Internet.
icmp	Software de Protocolo de Mensajes de Control de Internet.
tcp	Software de Protocolo de Transmisión de Internet
udp	Software de Protocolo de Datagrama de Usuario.
egp	Software de Protocolo de Compuerta Exterior.

Tabla 7. Categoría de las Bases de Información de Administración.

Los objetos en una MIB se organizan en una estructura de árbol, y el identificador de un objeto se encuentra caminando por el árbol desde su raíz a la posición del objeto en la estructura del árbol. Para los objetos escalares, este esquema proporciona un identificador único para un ejemplar de un objeto dado. Para objetos en tablas, hay un ejemplar de cada objeto para cada fila de la tabla, por tanto se necesita una posterior cualificación. Lo que se hace es concatenar el valor del objeto *INDEX* al identificador de cada objeto en la tabla.

2.6 ESTRUCTURA DE LA INFORMACION DE ADMINISTRACION (SMI).

Además del estándar MIB, el cual especifica variables de administración de red y sus significados, un estándar separado especifica un conjunto de reglas utilizadas para definir e identificar variables MIB. Las reglas se conocen como especificaciones *"Structure of Management Information" (SMI).*

Para mantener los protocolos de administración de red simples, SMI establece restricciones a los tipos de variables permitidas en MIB, especifica las reglas para nombrar tales variables y crea reglas para definir tipos de variables. Por ejemplo, el estándar SMI incluye definiciones de términos como *IpAddress* (definiéndolo como una cadena de cuatro octetos) y *Counter* (definida como un entero en el rango de 0 a $2^{32} - 1$) y especifica que son los términos utilizados para definir variables MIB. Algo muy importante, las reglas en SMI describen cómo se refiere MIB a las tablas de valores (por ejemplo, la tabla de ruteo).

Uno de los principales objetivos de SMI es proveer la simplicidad y la amplitud dentro de una MIB, de tal forma que puede almacenar solamente tipos de datos sencillos: escalares y matrices de dos dimensiones escalares, llamadas tablas. La SMI no permite la creación o la recuperación de estructuras complejas. Esta filosofía es la contraria a la utilizada en los sistemas de gestión OSI, que proporcionan estructuras de datos complejas y la recuperación de modos para permitir una funcionalidad mayor. SMI evita los tipos y estructuras de datos complejos para simplificar la tarea de la implementación y mejorar la interoperabilidad. Las MIB inevitablemente contendrán tipos de datos creados por el vendedor y, a menos que se impongan fuertes restricciones en la definición de tales tipos de datos, la interoperabilidad se verá afectada.

Los tipos de datos permitidos por SMI para SNMPv2 son:

Tipo de dato	Descripción
Integer	Enteros en el rango -2^{31} a $2^{31} - 1$.
Uinteger 32	Enteros en el rango de 0 a $2^{32} - 1$.
Counter 32	Un entero no negativo que se puede incrementar módulo 2^{32}.
Counter 64	Un entero no negativo que se puede incrementar módulo 2^{64}.
Gauge 32	Un entero no negativo que se puede incrementar o decrementar, pero no excederá un valor máximo. El valor no puede ser mayor que $2^{32} - 1$.
TimeTicks	Un entero no negativo que representa el tiempo, módulo 2^{32}, en centésimas de segundo.
Octet String	Cadena de octetos para datos arbitrarios binarios o textuales, puede estar limitada a 255 caracteres.
IP Address	Una dirección de Internet (IP) de 32 bits.
Opaque	Un campo de bits arbitrario.
Bit String	Una enumeración de bits con nombre.
Object Identifier	Nombre asignado administrativamente a objetos u otros elementos normalizados. El valor es una secuencia de hasta 128 enteros no negativos.

Tabla 8. Tipos de datos utilizados en SNMP Versión 2.

Existen realmente tres elementos claves en la especificación de la SMI. En el nivel más bajo la SMI especifica los tipos de datos que se pueden almacenar. Después, la SMI especifica la técnica formal para definir los objetos y tablas de objetos. Finalmente, SMI proporciona el esquema para asociar un identificador único con cada objeto real en un sistema, para que los datos de un agente se puedan referenciar por un gestor.

En la tabla 8 se muestran los tipos de datos que se permiten por SMI, el cual es un conjunto bastante restringido de formatos, por ejemplo, no se permiten los números reales. Sin embargo, es suficiente para satisfacer la mayoría de los requisitos de la gestión de red.

Capítulo III

Estudio sobre Sistemas de Monitoreo y Control

3.1 OPERACIÓN DE LOS SISTEMAS DE MONITOREO Y CONTROL

Como hemos visto hasta ahora la supervisión de redes puede realizarse de dos formas, mediante una estación de gestión, la cual es una estación de trabajo que recibe mensajes de los dispositivos de la red administrados, ó que la estación de gestión pregunte regularmente el estado de los dispositivos.

Una estación de gestión debe contar con ciertos componentes básicos los cuales realizaran la operación de monitoreo, control o administración. Estos elementos son los descritos a continuación (ver figura 18).

- *Interfaz de Usuario:* La cual debe ser capaz de permitir la interacción del usuario y el sistema ya sea en modo texto o modo gráfico de manera que, los datos recolectados por el sistema sean de fácil comprensión para el operador y permita tomar rápidamente la mejor solución en caso de identificar un problema.

- *Base de datos:* Es la encargada de mantener cualquier información de la red, dividiéndose en dos partes; una de ella esta encargada de mantener las descripciones de los diferentes parámetros, configuración de contadores, tipo de agentes residentes en los elementos administrados, etc., la otra parte se encarga de mantener almacenada la información recolectada por el sistema desde los elementos administrados la cual contiene datos como: tráfico entrante, tráfico saliente, carga del procesador, memoria libre y otros parámetros de importante influencia en la operación del elemento administrado.

- *Programa Monitor:* Se encarga de supervisar las condiciones actuales y determinar las condiciones futuras. Visualiza las alarmas activadas por los agentes, y realiza las actualizaciones mediante sondeos regulares.

- *Protocolo de Gestión:* Controla las operaciones de administración entre el gestor y el agente.

La estación encargada de supervisar a los objetos administrados puede acceder a ellos de tres maneras diferentes:

- En Banda (In-band): La administración del objeto se realiza utilizando el canal dedicado a las comunicaciones entre la red.

- Fuera de Banda (Out-of-band): El sistema accede a los objetos administrados a través de otros canales. Esto puede realizarse mediante un terminal conectado a un puerto del objeto administrado o que este tenga algún tipo de visualizador o panel de control.

- Supervisión Remota: La supervisión se realiza desde otra estación que no es la estación principal ya sea mediante: Una estación adicional operadora que permita monitorear todo el sistema o partes de él, utilizando una estación remota conectada a otro segmento de la red que da servicio a estaciones locales, o bien, por medio de un dispositivo encargado de localizar al operador mediante un beeper o correo electrónico, etc.

En la figura 18 se observa la arquitectura de un sistema de administración con cada uno de los elementos que se mencionan anteriormente, en la consola administrativa se despliega la información obtenida por parte del sistema administrador de la red (NMS) el cual desempeña una función de administrador ya que a través de este se sondean a los objetos administrados. La base de datos de estadísticas de red que reside en el NMS mantiene la información recolectada desde los agentes la cual puede ser graficada o presentada en un formato comprensible para el operador, pudiendo mantener estadísticas diarias, semanales

o mensuales, información que puede servir para determinar las necesidades existentes en la red a través de un período de evaluación largo, determinando por ejemplo si es necesario incrementar el ancho de banda requerido en algún punto de la red el cual puede estar saturado y de alguna forma disminuyendo la eficiencia de la red, implicando un cuello de botella para los demás puntos de la misma. Se puede determinar la disponibilidad de cada uno de los objetos administrados dando lugar a la identificación de fallas en algún punto especifico.

La información de los MIB debe de almacenar e identificar en forma abstracta a cada uno de los objetos que conforman la red, a manera de saber que variables o que información solicitar a cada uno de los agentes, distinguir entre las distintas marcas, ya que como se observa en el árbol jerárquico de los MIB cada fabricante de equipo tiene y crea sus propios MIB diferentes de los estándar que cada agente SNMP debe de tener.

En los objetos administrados reside un agente que no es mas que un equipamiento lógico, el cual almacena los datos de gestión. Estos agentes almacenan la información de su estado y mediante una petición con la identificación necesaria es enviada hacia la estación central en forma de datos en formatos interpretados por SNMP que posteriormente son transformados, por el sistema residente en la estación central, en información comprensible al usuario y es tal como se despliega en la consola administrativa.

El protocolo de gestión es que el medio que utiliza un sistema de administración para comunicarse con un dispositivo administrado, SNMP es otro método a través del cual puede acceder a los dispositivos de red. Obteniendo estadísticas o configurando al dispositivo, obteniendo estadísticas con los comandos *get* y configuración con *set*. Cada uno de los mensajes SNMP tiene asociado una cadena de caracteres que se refiere a la comunidad a la cual pertenecen los dispositivos administrados y la estación administradora, la cual esta

escrita en texto no encriptado y es enviada en cada uno de los paquetes con los cuales se comunican los dispositivos. Esta comunidad es usada para autenticar los mensajes enviados entre el administrador y el agente, permitiendo que solamente cuando la estación central envíe un mensaje con la comunidad correcta el agente responderá.

Algunos dispositivos, con agente SNMP permiten configurar diferentes comunidades para acceso a en modos privilegiados y no privilegiado. Permitiendo la configuración de comunidades de solo lectura o lectura / escritura respectivamente.

Además de los objetos administrados y las estaciones centrales de administración, existen las estaciones locales, las cuales actúan como objetos administrados y a la vez como estaciones administradoras. Es importante notar que este modelo de entidad de doble función (objeto Gestor/Agente) solo puede funcionar en aquellos dispositivos con capacidad para realizar esta doble función.

Estas estaciones son de mucha utilidad cuando el número de dispositivos existentes en la red es demasiado grande, ya que SNMP puede en un momento dado, ser ineficiente, debido a que el administrador debe sondear periódicamente todos los dispositivos que administra, pudiendo llevar tiempos muy grandes que podrían dejar escapar fallas momentáneas en el dispositivo administrado o mostrando datos en tiempos no reales.

Teniendo esto en cuenta, se pueden construir relaciones jerárquicas entre las estaciones de administración. Por ejemplo, se puede construir un sistema de administración donde cada segmento de una LAN tiene una aplicación de administración que controla el estado de los dispositivos de ese segmento; estas aplicaciones deberían informar a aplicaciones de estaciones de administración regionales, las cuales deberían informar a estaciones de administración entre empresas. En este ejemplo, el software de cada estación realiza un papel de

administrador al monitorizar y controlar dispositivos que dependen de él jerárquicamente, y un papel de agente al informar y actuar según los comandos proporcionados por sistema de jerarquía superior.

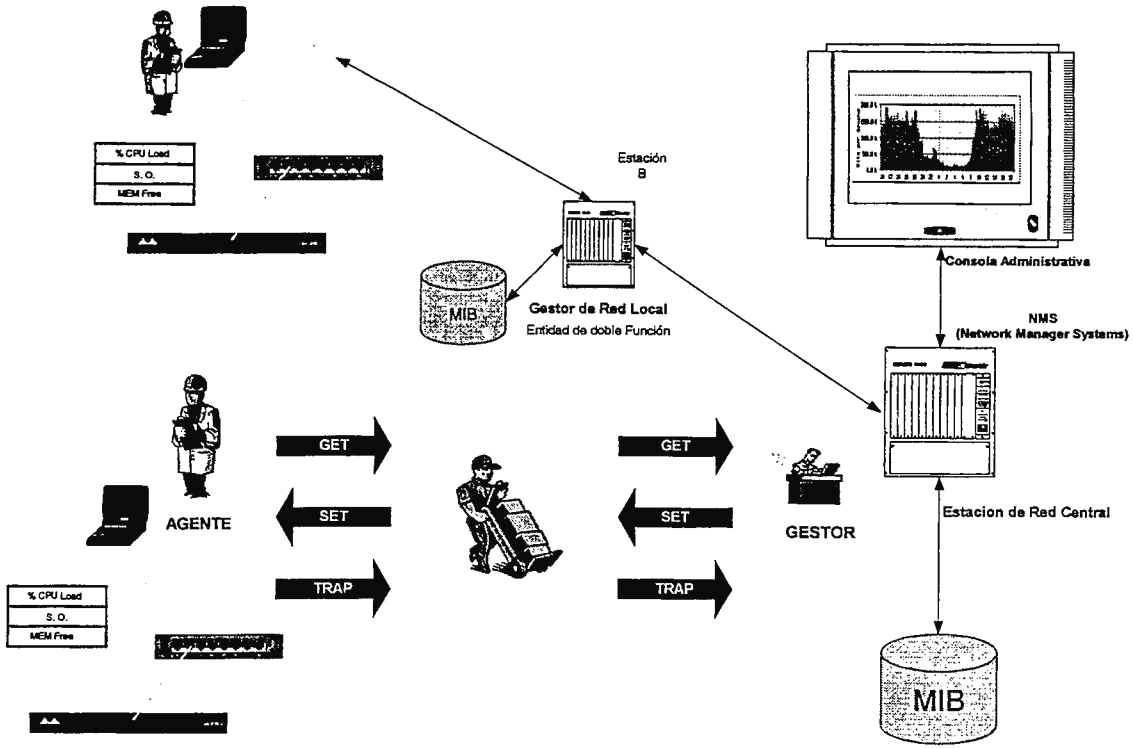


Figura 18. Proceso de Gestión de una Red por medio de SNMP.

3.2 PROCESO DE ADQUISICIÓN DE DATOS

Un sistema de monitoreo de redes se encarga de visualizar el estado de los distintos dispositivos de red que tiene bajo su cargo, sea, disponibilidad, cuantificación de tráfico en una interfaz en particular, cargas en el CPU, temperatura y todos aquellos datos que el agente posea. A través de los comandos GET de SNMP pueden obtenerse estos valores, los cuales son enviados al sistema administrado cada vez que este interrogue al dispositivo administrado. Como se observa en la figura 18, el gestor del sistema envía una petición GET hacia el objeto administrado con el cual se quiere comunicar, este mensaje incluye la comunidad a la que pertenecen tanto el dispositivo administrado como el sistema

de administración, la comunidad define la relación entre las entidades SNMP, además de los datos que definen una operación SNMP y los operandos asociados como por ejemplo el MIB correspondiente para la información requerida por el sistema administrador.

Un MIB es obtenido de acuerdo a la estructura del árbol jerárquico, y esta indica el identificador del objeto para cada variable, por ejemplo la MIB 1.3.6.1.4.1.9.2.1.1.51 identifica la variable HostconfigAddr de Cisco, que identifica la dirección IP del objeto administrado, siendo el identificador de objeto iso.org.dod.internet.private.enterprise.cisco.localvariables.interfacegroup.Hostconfi Addr tal como se observa en el árbol mostrado en la figura 17 y la cual debe formar parte de la base de datos donde se encuentra almacenada la información de cada dispositivo.

Con esta información enviada el agente identifica cual es la variable solicitada por parte del gestor, de manera que el agente debe de tomar lectura de este valor y transportarlo hacia el gestor para que este lo procese posteriormente y lo presente como una dirección IP en la interfaz del usuario y a la vez almacena en la base de datos estadística de la red si así es requerido.

Un sistema de gestión va más allá del proceso descrito anteriormente, ya que además es capaz de enviar información al objeto administrado, como por ejemplo en el caso anterior; en lugar de "leer" la dirección IP, se configure en el dispositivo administrado por medio de un comando SET de SNMP.

3.3 TENDENCIAS TECNOLÓGICAS DE LAS REDES DE COMUNICACIONES Y LOS SISTEMAS DE MONITOREO Y CONTROL.

Las redes de comunicaciones de datos se han convertido en un componente fundamental dentro de la infraestructura corporativa de una empresa, estas imponen exigencias cada vez más altas a los sistemas de monitoreo y control. Las

plataformas actuales no son suficientes cuando se trata de responder a estas necesidades, especialmente cuando se aplican a redes de gran escala y de misión crítica.

Las principales tendencias en los segmentos monitoreo y control para dar solución a los problemas anteriores son:

- ***Sistemas Distribuidos:*** Con el objetivo de evitar que toda la información de administración llegue en una única estación central, la tendencia hoy en día se dirige hacia la distribución de la inteligencia y la información por toda la red. Se pretende de este modo simplificar el monitoreo y control por medio de la automatización, de forma que las decisiones básicas se tomen cerca del origen del problema. Mediante la gestión distribuida es posible controlar redes de gran extensión de una manera más efectiva, dispersando entre varias estaciones de gestión las tareas de monitoreo, recogida de información y toma de decisiones.

La funcionalidad básica que ha de ofrecer un sistema distribuido es la siguiente:

- Escalabilidad para poder satisfacer las necesidades de gestión de redes de complejidad creciente en recursos y en información almacenada.
- Capacidad para distribuir entre distintas estaciones remotas de la red las funciones de supervisión, recogida de datos y sondeo de estado.
- Capacidad para gestionar entornos enormemente heterogéneos en el tipo de recursos de red y sistemas que los componen.
- Capacidad para incorporar nuevos servicios e integrarlos con los existentes
- Capacidad para interoperar con diversos entornos

- ***Administración orientada a servicios:*** La aproximación tradicional a la problemática de la gestión de redes se ha centrado en los dispositivos de red. Esto ha dado lugar en muchos casos, a situaciones en las que a pesar de

mantener un alto nivel de rendimiento en los componentes aislados, no se obtenía la calidad del servicio requerido. En gran medida esto se debe a que resulta difícil establecer una conexión entre monitoreo de dichos componentes de red y los procesos de negocio a los que están dando soporte dentro de la red.

- ***Administración basada en Web:*** El gran crecimiento de Internet y la introducción en las redes empresariales de las tecnologías que le son propias, está llegando también al ámbito del monitoreo y control redes. Mediante la adopción de este paradigma se posibilita un acceso universal a los sistemas de gestión desde cualquier plataforma que soporte los estándares de Internet (HTML, Java). En esta línea, los fabricantes de dispositivos de red están integrando en sus equipos el software que les permite actuar como servidores web.

Del mismo modo, se están realizando esfuerzos para la definición de nuevos estándares de monitoreo y control que, integrando protocolos como SNMP, HTTP y otros en una misma arquitectura, permita la gestión desde cualquier plataforma. Los esfuerzos para definir una interfaz de usuario basado en Java, también se enmarcan dentro de esta estrategia unificadora. Se trata en este caso de aprovechar la característica de que los módulos de software desarrollados en este lenguaje puedan ser ejecutados en cualquier plataforma.

Las razones para proceder a la adquisición de un sistema de monitoreo o control de redes pueden estar determinadas por diferentes factores. Es labor del operador la realización de un análisis de necesidades existentes dentro de su organización que permita determinar las necesidades actuales y futuras de los usuarios y las limitaciones o restricciones que ha de plantearse respecto al

dimensionamiento del sistema. Es necesario tener en cuenta y analizar con profundidad los costos y beneficios asociados para obtener argumentos de peso en la toma de decisiones.

En la fase de análisis de necesidades, fase inicial del proceso de adquisición, hay que tener en cuenta todos aquellos requisitos, limitaciones y restricciones que afecten, entre otros, a los siguientes puntos:

- ***Elementos Administrados.***

  El operador debe analizar los tipos de elementos que deben ser gestionados:

  - Cables físicos.
  - Dispositivos de red.
  - Topología de red.
  - Sistemas operativos de red.

- ***Equipos de comunicaciones que son gestionados e interoperatividad de protocolos.***

  En el momento de comprar un sistema de supervisión de red, el usuario debe analizar cuáles son sus necesidades relativas a qué protocolos deben ser soportados, de modo que el sistema que se adquiera ofrezca los máximos niveles en cuanto a flexibilidad, adaptabilidad y capacidad de expansión. Se deben realizar estimaciones de crecimiento de la red y tenerlas en cuenta durante esta fase.

- ***Interfaz gráfica de usuario.***

  Si las redes que van a ser monitoreadas se encuentran geográficamente dispersas por un campus, conectan varias plantas de un edificio, interconectan diferentes edificios..., resulta muy interesante que el sistema de monitoreo disponga de una interfaz gráfica de usuario capaz de mostrar al usuario los datos obtenidos en una forma de interpretación sencilla.

Capítulo IV

Desarrollo del Sistema

4.1 DEFINICIÓN DE LA CAPACIDAD DEL SISTEMA

La definición de la capacidad del sistema, requiere dos partes importantes:

- Definición de los criterios de diseño
- Determinación de los recursos que compondrán el sistema.

4.1.1 CRITERIOS DE DISEÑO

Los criterios de diseño que se consideraron para el desarrollo del proyecto son:

- **Elementos Supervisados.**

El Sistema desarrollado en el presente proyecto, se encuentra orientado a la supervisión de equipos de comunicaciones que realizan la conmutación de paquetes de capa 2 y 3, en un sistema de red que opera con el conjunto de protocolos TCP/IP.

Los dispositivos supervisados deben ser administrados bajo el protocolo SNMP, por lo que tienen una estructura MIB establecida para su gestión. Cada fabricante desarrolla una estructura privada adicional a las exigencias de los estándares SNMP.

Dado que una de las limitantes de la estructura MIB, es que existe una diversidad de parámetros que difiere de un fabricante de equipo a otro, el proyecto presentado en este documento se encuentra configurado básicamente para una marca en particular. Se ha seleccionado la marca CISCO SYSTEMS, por tener el más alto porcentaje de presencia a nivel mundial, además de ser una de las compañías que ofrece una gran cantidad de información característica y técnica de cada uno de sus productos en forma gratuita. CISCO ha desarrollado una serie de

MIB privados que permiten monitorear de forma amplia muchas variables involucradas en la operación de los dispositivos en general.

(a) (b) (c) (d) (e)

Figura 19. Principales elementos administrables con un sistema SNMP. (a) Ruteador; (b) Servidor de Acceso; (c) Giga Switch Router; (d) Switch de alta velocidad, ATM; (e) Switch de capa 2.

- **Distribución del Procesamiento el sistema.**

De acuerdo a las tendencias tecnológicas de los sistemas de administración, en la actualidad se implementan sistemas de aplicación Cliente-Servidor, las cuales hacen uso de un servidor que ejecuta la aplicación y una estación desde donde el cliente interactúa con ésta.

- **Aplicaciones de Servidor.**

En el sistema de monitoreo para redes de datos, al igual que en todos los sistemas de administración basado en el protocolo SNMP, MIB y SMI, los procesos de almacenamiento y recolección de información se realizan en el servidor.

El manejo de los datos almacenados y recolectados, se realizan en una base de datos que reside en el servidor. Esta base de datos contiene la información requerida para las aplicaciones que se realizan en el sistema.

Todas las aplicaciones que han de ejecutarse en el servidor, ya sea para interactuar con el usuario, base de datos o dispositivos administrados; necesitan de un lenguaje de programación capaz de realizar estas operaciones.

Una interfaz WEB que permita accesar al sistema desde cualquier parte, esto permite al cliente acceder al la información de los dispositivos remotamente.

- **Aplicaciones del Cliente**

para la administración de la supervisión de la red, los requerimientos de las estaciones cliente se limitan a un navegador, que se encuentra disponible en todos los sistemas operativos actuales y no tiene requerimientos de alto desempeño y capacidad de procesamiento.

4.2 ESQUEMA GENERAL DE LA SOLUCIÓN

En la figura 20 se muestra el esquema general de la implementación del Sistema de Monitoreo para Redes de Datos basado en el Protocolo SNMP.

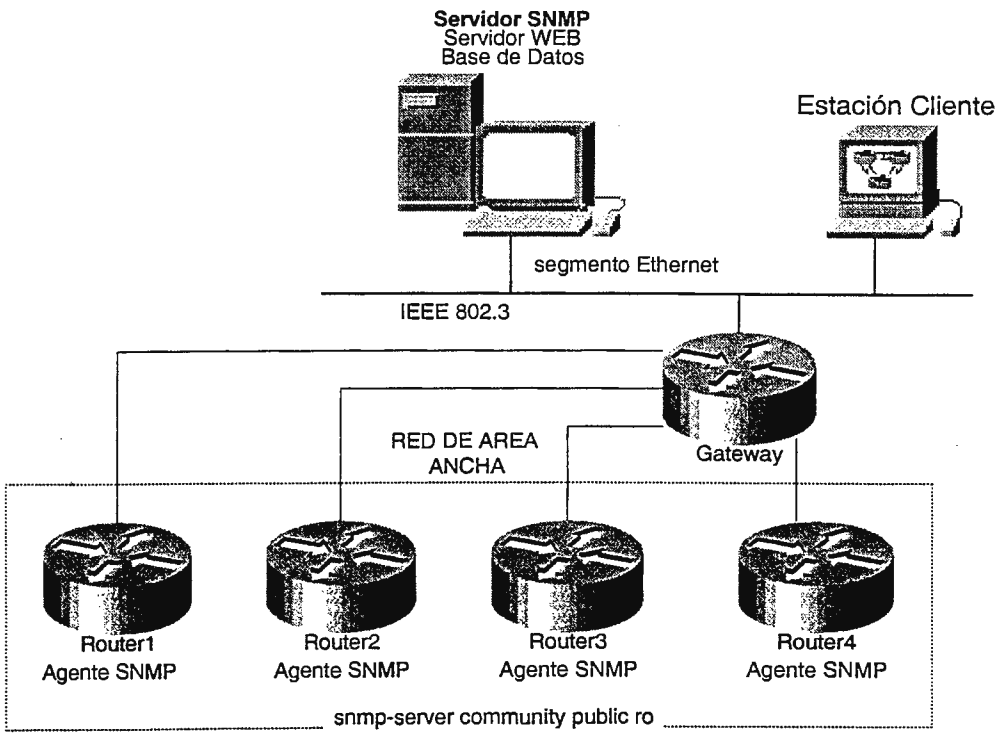


Figura 20. Esquema general de la solución.

En el gráfico de la figura 20 se muestra el esquema general de la aplicación. Los elementos de red pueden clasificarse en cuatro grupos:

- Elementos Administrados.
- Servidor SNMP.
- Estación Cliente de administración.
- Enlaces.

Elementos Administrados

Dada la orientación específica del presente proyecto al monitores de una red de datos, los elementos administrados se encuentran centrados en equipos ruteadores, de paquetes IP (*routers*) que representan la mayoría de los elementos de las redes de datos e Internet en la actualidad.

En la figura puede observarse que cada uno de los dispositivos ruteadores posee un agente, que opera como un proceso dentro de la rutina de funcionamiento del elemento de red. El proceso se inicia en forma sencilla, para SNMP Versión 1, únicamente especificando el nombre de la comunidad, por ejemplo en equipos Cisco se efectúa con la siguiente línea, en el modo de configuración global:

```
router(config)#snmp-server community public ro
```

Donde *"public"* es el nombre de comunidad para la administración de red, que es un ejemplo característico, en forma general, el administrador de la red debe especificar un nombre de comunidad para todos los equipos que desea administrar por un único sistema de gestión o monitoreo. La especificación *"ro"*, permitida por esta marca, indica una comunidad que únicamente puede ser utilizada para la lectura de variable MIB (operación Get-Request).

Servidor de Administración de la Red (NMS)

El Servidor NMS posee cuatro elementos básicos para el funcionamiento del sistema.

- Conectividad IP con cada uno de los elementos de red, es decir, requiere el establecimiento de rutas en la red, ya sea estáticas o generadas por un protocolo de enrutamiento (*RIP, OSPF, IGRP,* etc.).
- Soporte del protocolo SNMP en el sistema operativo. Se logra instalando y compilando librerías para ejecución del protocolo, sin embargo algunas distribuciones de Linux, como RedHat 7 lo integran como parte de las utilerías del sistema. El principal beneficio de utilizar una distribución de Linux es que su distribución es gratuita, los términos de la licencia pública se especifican en un documento denominado GPL.

- Base Datos. Almacena toda la información proveniente de los elementos administrados. En el siguiente capítulo se detalla la implementación de un sistema con bases de datos.

- Servidor WEB. Es una aplicación que se ejecuta en el sistema para que los clientes puedan accesar a la información del Sistema de Monitoreo por medio del protocolo de transferencia de Hipertexto (HTTP, *Hiper-Text Transfer Protocol*).

Estación Cliente

La estación cliente únicamente requiere la conectividad a la red TCP/IP.

Enlaces

Los enlaces en una red TCP/IP pueden clasificarse en LAN y WAN. A continuación se definen las características de cada uno de ellos.

a) Enlaces LAN.

Se encuentra definidos por tecnologías como Ethernet, Token Ring y FDDI. El estándar más utilizado para la interconexión de elementos en una red local es el IEEE 802.3 que es totalmente compatible con Ethernet. En el diagrama de la figura 20 se encuentra el Segmento de red local, representado por líneas azules.

Dentro de la red local es necesario incluir un elemento denominado "GATEWAY", que es un dispositivo interface entre la red local y la red de banda ancha. Una de sus interfaces debe ser compatible con la tecnología LAN utilizada, que para el presente proyecto es Ethernet y otro debe estar interconectado con un elemento de la red WAN.

b) Enlaces WAN.

Los enlaces WAN se encuentran representados por las líneas de color negro y transfieren información entre redes de área local y hacia Internet. Los enlaces WAN utilizan un protocolo de línea (de capa 2) que puede ser HDLC, PPP, Frame-Relay o una implementación de ATM.

La implementación del sistema de monitoreo es independiente del protocolo de línea empleado.

4.3 DEFINICION DE LA ESTRUCTURA DE LA BASE DE DATOS

La base de datos utilizada para almacenar cada uno de los parámetros que forman parte del Sistema de Monitoreo cuenta con siete tablas cada uno con sus respectivos campos los cuales se explican con más detalle a continuación:

Algunas de estas tablas almacenan información correspondiente a los parámetros de los dispositivos agregados para ser monitoreados y otras en particular almacenan información utilizada para llevar efectuar el monitoreo en la cual se almacena información general y especifica para del proceso.

En la tabla 9 se listan los nombres de las tablas que forman la base de datos en el sistema de monitoreo. A continuación se describe cada uno de lo campos utilizados en cada tabla.

No.	Nombre de Tabla	Descripción
1	ROUTERS	Información de los elementos monitoreados o dispositivos
2	TIPOS_TARGET	Define Interfaces para los Elementos monitoreados
3	VELOCIDADES	Velocidad del flujo de bits posibles en un interface
4	TARGETS	Información general de las interfaces de un dispositivo
5	MIBS	Tipos de MIB permitidas
6	TARGET_MIB	Relaciona los MIB con la tabla ROUTER
	HISTORICO	Registra datos para estadísticas

Tabla 9. Estructura de la Base de Datos.

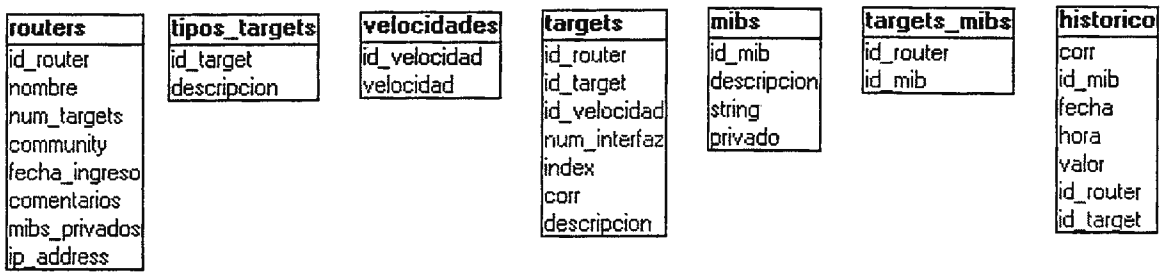


Figura 21. Estructura de la base de datos.

4.3.1 ROUTERS

En esta tabla se almacena toda la información general junto a la descripción de cada uno de los dispositivos monitoreados, en ella se utilizan los siguientes campos:

- **Id_router**: Este campo representa el identificador único de cada uno de los dispositivos supervisados por el sistema de monitoreo, este campo esta definido como la llave primaria para esta tabla y es del tipo *serial* (numérica) de manera que vaya incrementando automáticamente según sean adicionados nuevos dispositivos.

- **Nombre**: Identifica el nombre asignado por el administrador a cada dispositivo que forma parte del sistema de monitoreo es del tipo *varchar* con una longitud de 50 caracteres.

- **Num_targets**: Indica el numero de interfaces que van a ser monitoreadas por dispositivo.

- **Community**: Representa la comunidad SNMP a la que pertenece el dispositivo que será monitoreado, siendo una campo del tipo *varchar* de longitud 30.

- **Fecha_ingresado**: Indica la fecha en que fue ingresado el dispositivo a la base de datos, asignando automáticamente la hora del sistema donde se corre la aplicación.

- **Comentarios**: Este campo contiene toda información que proporcione referencia para el administrador que indique una cualidad particular para el dispositivo asignado, y esta representado por una variable del tipo *varchar* de una longitud de 100 caracteres.
- **Mibs_privados**: Esta es una variable del tipo *boolean* donde solamente existen dos condiciones, verdadero o falso, indica si para este dispositivo se han de asignar MIB privadas o si solamente le serán aplicadas las estándar.

- **Ip_address**: En este campo puede leerse la dirección IP con la cual fue ingresado cada dispositivo y sobre la cual se conecta al dispositivo para obtención de la información para el monitoreo.

4.3.2 TIPOS_TARGET

En esta tabla se ingresan todos los tipos de interfaces que pueden ser integradas a los dispositivos que han de ser incluidas en el sistema de monitoreo. Posee los siguientes campos:

- **Id_target**: Representa un identificador único para cada uno de los tipos de interfaces, esta variable es del tipo serial (numérica) siendo además la llave primaria para esta tabla.

- **Descripción**: Contiene el nombre de la interfaz ingresada al sistema.

4.3.3 VELOCIDADES

Aquí se encuentra descritas todas las posibles velocidades que pueden ser asignadas a una interfaz seleccionada.

- **Id_velocidad**: Define un identificador numérico único para cada una de las velocidades ingresadas en esta tabla.

- **Velocidad**: Representa el valor numérico para cada uno de las velocidades del flujo de bits, mas comúnmente usadas en los medios de transmisión.

4.3.4 *TARGETS*

La información general de cada una de las interfaces seleccionadas para cada dispositivo están contenidas en esta tabla que posee los siguientes campos:

- **Id_router**: Este campo define una relación entre esta tabla y la de ROUTERS, y representa en ambas el identificador único numérico para cada dispositivo.

- **Id_target**: Con este campo están relacionadas esta tabla junto a *TIPOS_TARGET*, de esta manera se identifica sobre que Interface se ha de ejecutar el monitoreo.

- **Id_velocidad**: De manera similar al campo anterior, por medio de esta se hace una relación a la tabla de VELOCIDADES.

- **Num_interfaz**: Representa el número de cada interfaz integrada para cada dispositivo, tal como es identificada en el hardware del dispositivo.

- **Index**: Este campo identifica el número tal como es reconocida por el software del dispositivo y sirve para hacer referencia al sistema sobre cual Interface ha de ejercerse el monitoreo.

- **Corr**: Este valor es un identificador numérico único para cada una de las interfaces agregadas por dispositivo.

4.3.5 MIBS

- **Id_mib**: Identifica como única a cada una de las MIB ingresadas al sistema de monitoreo.
- **Descripción**: Como su nombre lo indica describe el significado para cada uno de estas MIB.

- **String**: Esta es la cadena de caracteres que representa al MIB como parámetro que ha de entender el agente SNMP para obtener el valor requerido por el NMS. Por ejemplo: .1.3.6.1.4.1.9.2.1.58.0

- **Privado**: Este campo es un valor de tipo *boolean* el cual sirve para identificar si la MIB ingresada es privada o estándar (Ver figura 17).

4.3.6 TARGET_MIB

- **Id_router**: Definen la misma característica en la tabla ROUTER y es relacionada a esta por medio de este campo.

- **Id_mib**: Relaciona esta tabla con la tabla MIB.

4.3.7 HISTORICO

- **Corr**: identificador numérico único para cada valor tomado y que es ingresado a la base de datos para luego ser graficada.

- **Id_mib**: Relación con las tablas TARGET_MIB y MIBS.

- **Fecha**: Esta es la fecha en la cual están siendo tomados los datos, y en base al cual se tendrá un histórico para obtener un gráfico con referencia al día seleccionado.

- **Hora**: Es la hora en la cual fue consultado el agente SNMP para cada una de las MIB integradas en cada dispositivo. Los agentes serán consultados cada cinco minutos.

- **Valor**: Este es el valor devuelto por el agente cuando se realiza una consulta SNMP (*SNMPGET*). La gráfica será construida de forma valor contra tiempo tomando como referencia cada uno de los parámetros incluidos en cada tabla y la fecha sobre la cual se quiere obtener el monitoreo.

4.4 DISEÑO DE LA BASE DE DATOS.

El objetivo principal de la base de datos es almacenar la información histórica del estado de los dispositivos que quieren ser monitoreados. Sin embargo, esta información sería poco descriptiva si no se contara con la información detallada de los dispositivos que se monitorean, las MIB que son utilizados, etc. Es por eso que vamos a dividir las tablas de la base de datos en dos grupos:

1. **Tablas transaccionales**: que guardan toda la información del monitoreo.

2. **Tablas de parámetros del sistema**: las cuales guardan los valores que la herramienta de monitoreo desarrollada necesita para trabajar.

Para las tablas transaccionales solamente tenemos la tabla **histórico** que es la que guarda todas las lecturas del monitoreo y a la cual se le consulta toda la información necesaria para graficar y presentar reportes en pantalla.

Las tablas de parámetros son las que le van a dar significado a la información que tiene la tabla **histórico**, ya que sin ellas los datos que veríamos son los siguientes:

Corr	id_mib	fecha	hora	valor	id_router	id_target
1	11	02/05/2000	5:00	1	17	15

Tabla 10. Contenido de la tabla Histórico

El ejemplo muestra que es difícil identificar a qué router nos referimos, que interfaz fue registrada y que MIB se utilizó para la consulta.

Auxiliándonos de las otras tablas y haciendo uso de sentencias SQL SELECT (explicadas en el capítulo V), que enlacen las tablas, veremos lo siguiente:

Corr	id_mib	fecha	hora	valor	router	id_target
1	Avg CPU busy	02/05/2000	5:00	1	Frame Relay	Ethernet 0

Tabla 11. Descripción de valores de tabla histórico

Esta información es más clara debido a que se le han agregado las descripciones de los parámetros que el sistema utilizó (nombre del mib, router y target).

Es importante señalar que se pudo haber diseñado la tabla para que guardara toda la información (parámetros y sus respectivas descripciones) y evitarse el tener que recurrir a otras tablas, pero esto habría utilizado demasiado espacio en disco, este hecho se describe a continuación:

Imaginemos la tabla histórico mal diseñada con 10 registros.

Corr	mib	fecha	hora	valor	router	target
1	Temperatura	02/05/2000	5:00	1	Frame Relay	Ethernet 0
2	Temperatura	02/05/2000	5:05	1	Frame Relay	Ethernet 0
3	Temperatura	02/05/2000	5:10	1	Frame Relay	Ethernet 0
.						
.						
10	Temperatura	02/05/2000	5:45	1	Frame Relay	Ethernet 0

Tabla 12. Ejemplo de mal diseño de tabla histórico.

Tal y como se mira en el ejemplo, se repite en todos los registros lo siguiente: Temperatura, Frame Relay y Ethernet 0. Si esta información se guardara así en disco ocuparían demasiado espacio y la base de datos se quedaría corta de espacio libre en disco al poco tiempo de ser utilizada.

Para hacer más claro el hecho de la utilización de disco veamos el caso de la cadena "Frame Relay", la cual tiene una longitud de 11 caracteres. Debido a que una cadena de caracteres requiere de un byte para almacenar un carácter, se requeriría de 11 bytes para almacenar una vez la cadena "Frame Relay"; esto quiere decir que para almacenar 10 registros necesitaríamos de 110 bytes de disco para almacenar todas las ocurrencias de la cadena. (Esto sin contar los bytes que utilizan las otras cadenas: "Temperatura" y "Ethernet0")

Es por esto que se opta por sustituir todas las ocurrencias de cadenas por "símbolos" que las representen y que ocupen menos espacio en disco.

Por ejemplo, designemos el entero 1 a la cadena "Frame Relay" y dejemos constancia de ello en la tabla Routers de la siguiente manera:

Id_router	Descripción
1	Frame Relay

Tabla 13. Ejemplo de asignación de valores en tabla routers

Id_router constituye el "símbolo" que representa a Frame Relay en toda la base de datos, así que debemos procurar que solo Frame Relay utilice el 1 como Id_router para que después no hayan problemas con otros dispositivos.

Habiendo hecho esta sustitución, la tabla histórico debería quedar así:

Corr	mib	fecha	hora	valor	id_router	target
1	Temperatura	02/05/2000	5:00	1	1	Ethernet 0
2	Temperatura	02/05/2000	5:05	1	1	Ethernet 0
3	Temperatura	02/05/2000	5:10	1	1	Ethernet 0
.						
.						
10	Temperatura	02/05/2000	5:45	1	1	Ethernet 0

Tabla 14. Ejemplo de tabla histórico con sustitución de símbolos

Ahora ya sabemos que donde aparezca id_router y un 1 nos estamos refiriendo a "Frame Relay" y el espacio en disco se reduce significativamente, ya que si el 1 es declarado de tipo entero (el cual ocupa 4 bytes de espacio en disco para ser almacenado) y aparece 10 veces, sólo requerirá de 40 bytes en disco para ser almacenado.

Los mismos reemplazos son hechos en las tablas targets y mibs:

Id_mib	Descripción
7	Temperatura

Tabla 15. Ejemplo de asignación de valores en tabla mibs

Id_target	Descripción
11	Ethernet 0

Tabla 16. Ejemplo de asignación de valores en tabla targets

Y la tabla histórico se convierte en:

Corr	mib	Fecha	hora	valor	id_router	target
1	7	02/05/2000	5:00	1	1	11
2	7	02/05/2000	5:05	1	1	11
3	7	02/05/2000	5:10	1	1	11
.						
.						
10	7	02/05/2000	5:45	1	1	11

Tabla 17. Ejemplo de asignación de valores en tabla Histórico

Reduciendo el espacio en disco.

Como estar recordando qué "símbolo" representa qué cosa es poco práctico, los manejadores de base de datos presentan la opción de mostrar la información ya traducida de "símbolo" a lo que representa:

SELECCIONAR historico.id_router, routers.descripcion, fecha, hora
DE historico, routers
DONDE historico.id_router = routers.id_router

La sintaxis anterior selecciona el id, la fecha y la hora de la tabla históricos y al mismo tiempo selecciona la descripción de la tabla routers, poniendo como restricción que el id que salga en la tabla histórico sea igual al id que sale en la tabla routers para que la traducción de símbolo a valor real sea correcta.

La respuesta que se obtiene es la siguiente:

Corr	id_router	descripcion	fecha	hora
1	1	Frame Relay	02/05/2000	5:00
2	1	Frame Relay	02/05/2000	5:05
3	1	Frame Relay	02/05/2000	5:10
.				
.				
10	1	Frame Relay	02/05/2000	5:45

Tabla 18. Ejemplo de lectura de valores en la base de datos

Es importante resaltar que los manejadores de bases de datos, al hacer una consulta de selección no escribe nada en disco, sino que obtiene los datos y los muestra en pantalla.

Es por el uso eficiente de espacio en disco que se requirió dividir la tabla histórico en varias tablas que almacenaran la información de forma eficiente.

Capítulo V

Implementación del Sistema

5.1 REQUERIMIENTOS DEL SISTEMA

Como se mencionó anteriormente, el sistema funciona bajo una plataforma cliente-servidor. Por el lado del cliente únicamente es requerido un navegador de internet sean estos: Internet explorer, Netscape, neoplanet, etc, corriendo sobre cualquier sistema operativo Windows, Linux, MAC, etc. Este programa es el que permite al usuario interactuar con el sistema ya sea para la administración o monitoreo de los dispositivos ingresados por el administrador del sistema.

La aplicación que se ejecuta en el servidor necesita de los siguientes programas:

5.1.2 Linux redhat 7.0

ya que es un sistema operativo de altas prestaciones, eficiente y robusto. Su mayor fortaleza es la idea sobre la cual esta desarrollado. Es un sistema operativo libre, distribuido bajo la Licencia General Pública de la Free Software Foundation, que garantiza a los usuarios libertad para usarlo como estimen conveniente, reproducirlo y distribuirlo sin ninguna limitación y acceso al código fuente para estudiar su funcionamiento, hacerle cambios para adaptarlo a situaciones particulares o introducirle mejoras.

5.1.3 PERL

(Practical Extraction & Report Languaje) el cual es un lenguaje de programación surgido para facilitar la elaboración de tareas comunes en sistemas tipo UNIX. Además facilita la realización de los llamados CGI, interfaces para comunicar recursos del servidor con un servicio de Internet, por lo que se convierte en una herramienta que facilita el proceso del manejo de grandes volúmenes de información sin sacrificar el rendimiento del microprocesador.

5.1.4 UCD-SNMP

Incluye varias herramientas para la interacción con el protocolo SNMP, como por ejemplo un agente extensible, una librería SNMP, herramientas para la consulta o seteo de información en los agentes, así como también herramientas compatibles con MIB browser en Tk/PERL. La versión utilizada en el desarrollo de esta aplicación es **ucd-snmp-4.1.2.**

5.1.5 POSTGRESQL

Es una implementación SQL que consta de un servidor de base de datos, un cliente y varias herramientas adicionales. Es un sistema que se ha convertido en la mas popular de las bases de datos libre de licencias comerciales.

Postgresql es una base de datos que se encuentra a la altura de Oracle, Sybase o Interbase, soporta transacciones y claves ajenas manejando aplicaciones orientadas a objetos, convirtiendose en una base de datos seria y segura ya que su consistencia de la base de datos es fundamental.

5.1.6 APACHE WEB SERVER

La publicación de hojas WEB se realiza mediante la utilización de un servidor WEB que utiliza un **servidor Apache**, el cual es un sistema compilador, poderoso y flexible, de un servidor de red que implementa el protocolo http, siendo altamente configurable y extendible debido a que es modular, provee gran cantidad de fuentes de códigos lo cual le permite correr en cualquier plataforma, además posee licencia gratuita.

Para la implementación del proyecto se escogieron los programas anteriores debido, principalmente, a que son de libre distribución y todos se pueden ejecutar bajo el mismo sistema operativo. Estos programas tienen un alto desempeño, los cual nos es de gran beneficio ya que permiten tener una alta capacidad de procesamiento y almacenamiento de información. Se cuenta además con una gran

cantidad de documentación y sitios de Internet relacionados, permitiéndonos tener información y tutoriales disponibles para consulta y ejemplos.

5.2 COMANDOS BASICOS PARA LA OPERACION DEL SISTEMA

En éste apartado del documento se pretende dar una guía básica de los comandos que se utilizan para desarrollar el programa implementado en el proyecto.

5.2.1 LIBRERIAS A UTILIZAR PARA INICIO DE PROGRAMACIÓN.

#!/usr/bin/perl : Llama al compilador de PERL y es necesario al inicio de cada programa que se ejecuta en PERL.
use Pg; : Requerida para la interacción con la base de datos Postgresql.

Use CGI qw(:standard); : Requerida para la creación de objetos CGI (Common Gateway Interface).

5.2.2 SENTENCIAS SQL PARA ESTABLCER LA CONEXIÓN.

$conn = Pg::connectdb("dbname='tesis' user='root' password='tesis' ");
: ésta sentencias es la que permite conectarse a la base de datos Postgresql.

5.2.3 SENTENCIAS SQL PARA INTERACTUAR CON LA BASE DE DATOS.

5.2.3.1- Conexión para la lectura de datos.

$datos = $conn->exec(sentencia_SQL); : en la variable **$datos** se almacena toda la información que ha sido devuelta por la sentencia SQL ejecutada.

Ejemplo:

```
$mibsPrivados = $conn->exec("SELECT * FROM mibs WHERE Privado = '1'");
$result = $conn->exec("SELECT * FROM tipos_targets");
$resultVelocidad = $conn->exec("SELECT * FROM velocidades");
```

En estos tres ejemplos vemos como los valores devueltos por la sentencia SQL son asignados a las variables respectivas.

5.3.1.2- CONEXIÓN PARA LA ESCRITURA DE DATOS.

$conn->exec(sentencia_SQL); : la sentencia SQL contiene los cambios que han de realizarse en la base de datos: agregar, modificar o eliminar.
Ejemplo:

#Generamos el SQL base

```
$SQL = "INSERT INTO tipos_targets(descripcion) SELECT '" . $descripcion . "' ";
```

#Escribimos a la base de datos

```
$conn->exec($SQL);
```

En este ejemplo vemos como se escribe dentro de la base de datos los parámetros enviados en la sentencia SQL.

5.3.1.3 SENTENCIAS DE LECTURA DE LOS ARREGLOS DE LA BASE DE DATOS.

while(@values = $datos->fetchrow){

} : éste bloque de programa nos permite almacenar en el arreglo **@values** la primera fila del arreglo devuelto por la ejecución de la sentencia SQL que se ha almacenado en la variable **$datos** , realizando éste proceso n-veces como n-filas tenga el arreglo.

$values[x] : ésta variable contiene el valor del elemento **X** del arreglo **@values,** donde **@values** es el arreglo al que se le asigna lo devuelto por **$datos->fetchrow**

Ejemplo:

```
while(@results = $targets->fetchrow){
    print "<tr>";
    print "<td>$results[1]</td>";
    print "<td><div align = Center>$results[2]</div></td>";
    print "<td><div align = Center>$results[3]</div></td>";
    print "<td>$results[4]</td>";
    print "<td>$results[5]</td>";
    print "<td>";
    print a{href=>"devicemod_int_mod.pl?corr=$results[0]"},"modificar");
    print "</td>";
    print "<td>";
    print a({href=>"devicemod_int_del.pl?corr=$results[0]"},"eliminar");
    print "</td>";
print "</tr>";
```

En este ejemplo los valores devueltos por la sentencia SQL son puestos en una tabla en formato HTML generándose un número de filas igual a las que el arreglo devuelve, conteniendo la primera columna los valores devueltos en **$results[1],** y así sucesivamente.

5.3.1.4 TIPOS DE SENTENCIAS SQL PARA EL MANEJO DE DATOS.

1. Para seleccionar registros

SELECT nombres_de_campos FROM tabla WHERE criterio_de_seleccion ORDER BY criterio_de_orden : ésta sentencia SQL selecciona de las tablas, de la base de datos, los valores en los **nombres_de _campos** de la tabla **tabla** donde se cumpla el **criterio_de_selección** ordenandolos por **criterio_de_orden.**

Ejemplo:

```
$query = "SELECT id_router,nombre FROM routers ORDER BY nombre";
```

Se observa como son seleccionados todos los dispositivos desde la tabla routers devolviendo únicamente su **id_router** y **nombre** ordenados en orden alfabético de acuerdo a la variable nombre.

2. Para borrar registros

DELETE FROM tabla WHERE criterio_de_eliminacion: ésta sentencia SQL borra de la tabla **tabla** los valores de los campos donde se cumpla el **criterio_de_eliminacion.**

Ejemplo:

```
DELETE FROM tipos_targets WHERE id_target = " . $id_target;
```

En este ejemplo eliminamos las interfaces de la tabla **tipos_traget** siempre y cuando corresponda a la variable **$id_target.**

3. Para actualizar registros

UPDATE tabla SET nombre_de_campos = valores WHERE criterio_actualizacion : con ésta sentencia se actualiza la tabla **tabla** en la base de datos con los **valores** contenidos en **nombre_de_campos** y que cumplan con el **criterio_actualizacion.**

Ejemplo:

```
UPDATE routers SET nombre = "$nombre", ip_address = "$ip" WHERE
ip_address = "$ip1"
```

Se observa como es actualizado el nombre y la dirección IP enviados en las variables **$nombre** y **$ip** en aquellos registros donde ip_address= **$ip1.**

4. Para agregar registros

INSERT INTO tabla(nombre_campos) SELECT valores_a_agregar : ésta sentencia agrega en la tabla **tabla** los **valores_a_agregar** en **nombre_campos** donde éstos deben de estar colocados en el mismo orden en ambos arreglos.

Para el desarrollo de la aplicación realizada se han estructurado programas en PERL que ejecutan las sentencias de SQL descritas anteriormente, por ejemplo:

Ejemplo:

INSERT INTO routers(nombre, num_targets, community, fecha_ingreso, comentarios, mibs_privados, ip_address) SELECT "FRAME RELAY", 5, "public", "02/05/2001","dispositivo de prueba", "t","10.10.10.10"

En este ejemplo se agrega en la tabla routers un nuevo registro con los campos enviados en cada una de las variables.

5.2.4 UTILIZACIÓN DEL MÓDULO UCD-SNMP

Las instrucciones del programa que ejecutan las peticiones SNMP son erjecutadas en líneas de comando según las siguientes sintaxis.

5.2.4.1 SNMPGET

Se comunica con una entidad de la red usando peticiones SNMP GET.

SYNOPSIS

snmpget <hostname> {<community>} [<objectID> ...]

Donde :

- Hostname: Se refiere a la dirección IP o nombre del Host al cual se le hacen las peticiones GET.

- Community: Indica la comunidad SNMP a la cual pertenece el dispositivo.
- ObjetctID: Especifica la variable SNMP la cual se genera en base a la estructura del árbol MIB, por ejemplo:
  - **.1.3.6.1.2.1.1.1.0**
  - **.iso.org.dod.internet.mgmt.mib.system.sysdescr.0**
  - **.1.3.6.1.2.1.1.sysdescr.0**

De cualquiera de estas tres formas se hace referencia a una variable MIB llamada sysdescr la cual devuelve el nombre del dispositivo.

Por ejemplo para obtener el estado de operación de una interface se ejecuta el siguiente comando:

Snmpget 10.10.10.10 public .1.3.6.1.2.1.2.2.1.7.IfIndex

Se obtiene de resultado:

interfaces.ifTable.ifEntry.ifAdminStatus.1 = up(1)

5.2.4.2 SNMPWALK

Se comunica con una entidad de la red usando peticiones SNMP GET NEXT.

snmpwalk <hostname> {<community>} [<objectID>]

Los argumentos para este comando tienen el mismo significado que las del comando anterior.

Snmpwalk 10.10.10.10 public .1.3.6.1.2.1.2.2.1.7

Obteniendo el resultado siguiente:

interfaces.ifTable.ifEntry.ifAdminStatus.1 = up(1)
interfaces.ifTable.ifEntry.ifAdminStatus.2 = up(1)
interfaces.ifTable.ifEntry.ifAdminStatus.3 = up(1)

5.3 MODELO CLIENTE_SERVIDOR

Como muchas otras aplicaciones de red, el World Wide Web se ajusta al modelo cliente-servidor. La comunicación entre el cliente y el servidor ocurre sobre la red, la cual en el caso del WWW es Internet (o intranet sin ningún problema). El

cliente y el servidor pueden estar corriendo en diferentes sistemas operativos, sobre diferentes arquitecturas, haciendo nuestro modelo independiente de la plataforma.

a) El Cliente

En este caso, el cliente es un browser como se explicó anteriormente. El browser lo que hace es pedirle un documento a un servidor (utilizando un localizador uniforme de recursos, URL ó Uniform Resource Locators), para luego procesarlo (transformarlo para ser presentado en pantalla).

b) El Servidor

El servidor se encarga de manejar archivos, responde a las peticiones del cliente y envía las respuesta a las preguntas realizadas. El servidor también provee un enlace a aplicaciones que no son clientes http, por medio de CGI (el cual puede ser una base de datos, un programa de diagnostico, un simulador, etc).

La siguiente ilustración muestra como es la interacción entre un par de clientes y un servidor.

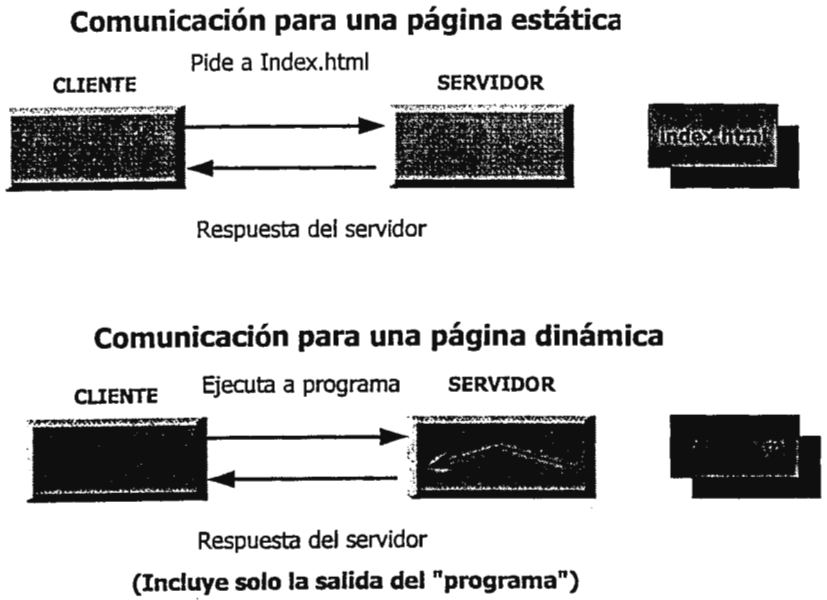


Figura 22. Comunicación entre un cliente y un servidor

Una página HTML puesta en un servidor, utiliza el primer método de interacción cliente-servidor. En el segundo tipo el servidor no necesita saber como interpretar los datos que devuelve el programa, el solo los pasa al cliente.

5.4 CGI

CGI (Common Gateway Interface) es el medio que tiene un servidor que habla http para comunicarse con un programa. La idea es que cada cliente y un programa servidor (independientemente del sistema operativo) se adhieran a los mismos mecanismos para el flujo de datos entre el cliente, el servidor y el programa que hace el puente.

Cuando se habla de un cliente de un puente, se dice que puede ser un programa que actúa como intermediario entre el servidor http y otro programa que puede ser ejecutado por medio de línea de comandos.

Cuando se habla de una interfaz, se dice que es un mecanismo estándar que le permite a los programadores trabajar dentro de un entorno productivo.

a) Funcionamiento del CGI

Un transacción con CGI ejecuta los siguientes pasos:

1. El cliente envía una petición conformada con el formato estándar de un URL a el servidor (se incluye el tipo de servicio, ubicación del servicio). Además se envía un encabezado con datos provistos por el cliente.
2. El servidor procesa la petición de llegada y decide que hacer luego, dependiendo del tipo de servicio solicitado, si es un archivo html lo devuelve, pero si es un programa CGI entonces:
   - El encabezado con datos es recibido por el cliente, si existe. Estos datos son pasados al programa como variables de entorno.

- Los parámetros de ejecución del programa si existen, son tomados por el programa o por la entrada estándar. La forma en como el cliente ha de enviar los datos la decide el programador cuando crea la interfaz.

3. El programa CGI devuelve una respuesta, como un documento html, al servidor. El programa CGI siempre debe devolver una respuesta.
4. La salida es devuelta al cliente por el servidor y se corta la comunicación.

5.5 GENERACION DINAMICA DE HTML

Para generar códigos HTML los archivos han de colocarse en el directorio **/cgi-bin** del servidor, los cuales deben tener permisos de ejecución para todo el mundo.

#!/usr/bin/perl
use CGI qw(:standard);

Las líneas anteriores son las básicas para la creación de programas en PERL en el cual se han de utilizar los métodos CGI.

En las líneas posteriores se observa como se crea un objeto CGI con el cual se genera un código HTML, el cual recibe parámetros del usuario en donde indica el número de interfaces y si el dispositivo ha de utilizar MIB privados, los valores ingresados por el cliente servirán de parámetros para luego ser procesados en otros bloques de programas.

```
$cgi = new CGI; #creamos el objeto cgi
print $cgi->header;
print $cgi->start_html('Opciones de Mantenimiento');
print "<Center>";
print $cgi->h1('Pantalla de Ingreso de Dispositivos');
print "</Center>";
print $cgi->startform;
print p,$cgi->h2('Par&aacute;metros de Configuraci&oacute;n del Dispositivo'),p;
print "<table border>";
print "<tr>";
print "<td><div align=right>Numero de Interfaces:</div></td><td>",$cgi->textfield('interfaces','',2,2),"</td>";
print "</tr><tr>";
print "<td><div align=right>Utiliza MIBS privados:</div></td><td>",$cgi->checkbox(-name=>'privados', -
value=>'seleccionado', -label=
>''),"</td>";
```

```
print "</tr></table>";
print ("<A HREF = \"../infointerfacestest.pl\"target=\"blank\">¿Conocer Indice de las Interfaces?</A>");
print p,p,$cgi->submit('encabezado','Configurar');
print $cgi->endform;
```

5.6 PROGRAMA PRINCIPAL PARA LA OBTENCION DE DATOS EN LOS DISPOSITIVOS MONITOREADOS

```
#!/usr/bin/perl
Use Pg;
($year,$mon,$mday,$hour,$min,$sec) = (localtime)[5,4,3,2,1,0]; # recuperamos la Hora y Fecha actual
$year += 1900;
$mon++;
$fecha = "$mday\/$mon\/$year";
$hora = "$hour:$min:$sec";
$conn = Pg::connectdb("dbname='tesis' user='root' password='tesis' "); #Nos conectamos a la Base de datos
$query = "SELECT a.id_router, a.ip_address, b.id_target, b.index, c.id_mib, c.string,  a.community, c.privado ";
$query = $query."FROM routers AS a, targets AS b,  mibs AS c, targets_mibs AS d ";
$query = $query."WHERE  a.id_router = b.id_router AND a.id_router = d.id_router AND     d.id_mib = c.id_mib ";
$query = $query."ORDER BY a.id_router, b.id_target, c.id_mib";
$objetivos = $conn->exec($query);  # Leemos de la base datos
while(@rows = $objetivos->fetchrow){   #Recorremos el arreglo devuelto por la consulta a la base de datos
      @valor = split(/=/,(`snmpget $rows[1] $rows[6] $rows[5]$rows[3]`)) if ( $privado == '0' ); # si es mib standard
      @valor = split(/=/,(`snmpget $rows[1] $rows[6] $rows[5]`)) if ( $privado == '1' ); # si es mib privado
      $valor[1] =~ s/ +//;
      $correlativo = $conn->exec("SELECT corr FROM Historico ORDER BY corr DESC");
      $corr = $correlativo->fetchrow;
      $corr++;
      $conn->exec("INSERT INTO historico VALUES($corr, $rows[4],\'$fecha\',\'$hora\', $valor[1],$rows[0],$rows[2])");
```

Se observa en el programa anterior como son obtenidas las variables para la generación de las graficas de los MIB de tráficos en las interfaces tanto de salida como entrada, para tantas interfaces según hayan sido seleccionadas.

Se puede ver como se genera la fecha, la cual esta de acuerdo a la del sistema sobre el cual se ejecuta la aplicación, de igual forma se hace con la hora, estos datos son almacenados en las variables **$fecha** y **$hora** respectivamente, estas sirven de referencia para generar el grafico en un día en particular, luego se ha de conectar a la base de datos de donde recuperará las variables además de los argumentos requeridos para la ejecución del comando **snmpget ($communnity, $ip_address, $string)** , el **$id_router** para identificar al dispositivo al cual pertenecen las interfaces que se están monitoreando, la cual se identifica mediante **$id_target** e **$index,** una vez construida la instrucción **snmpget** con todos sus argumentos es ejecutada y los valores devueltos son asignados a la variable

$objetivos y mediante la utilización de **fetchrow->** apuntando hacia el arreglo **@valor** se agregan a la base de datos según el orden que se muestra en la sentencia SQL utilizando INSERT.

Utilizando la función **crontab** de linux, la cual ejecuta una tarea según sea programada en este, podemos obtener el estado del dispositivo en períodos de tiempo cortos a fin de observar su comportamiento detalladamente. Modificando esta herramienta de la siguiente manera, podemos ejecutar esta tarea cada cinco minutos y obtener de esta forma los valores devueltos por los dispositivos:

[root@snmp /etc]# crontab –e

Con esta línea se ejecuta el modo de edición del crontab en el cual deberá quedar de la siguiente manera si se ejecuta el comando:

[root@snmp /etc]# crontab –l
 # DO NOT EDIT THIS FILE - edit the master and reinstall.
 # (/tmp/crontab.1753 installed on Wed Mar 7 10:02:49 2001)
 # (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
***/5 * * * * /home/tesis/snmpget.pl**

Como se observa se ha agregado la línea:
***/5 * * * * /home/tesis/snmpget.pl** la cual se lee de la siguiente manera:

El archivo que contiene el programa que se listó anteriormente llamado **snmpget.pl** con la ruta **/home/tesis** se ejecutara todos los minutos entre cinco, que corresponde a realizarlo cada cinco minutos, todas las horas, todos los días lo cual se indica con asteriscos.

5.7 ESTRUCTURA DEL SISTEMA

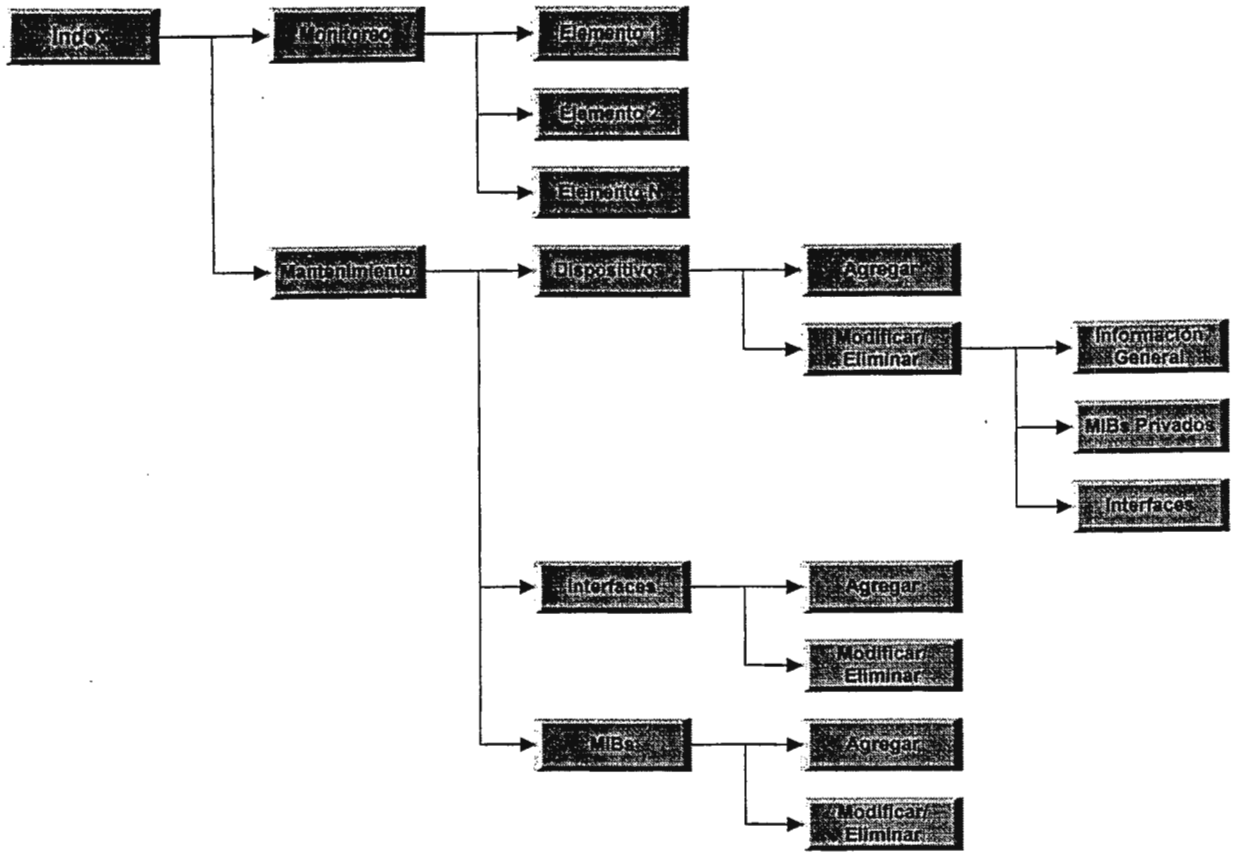


Figura 23. Estructura de la Interfaz Gráfica.

Una vez que se ha establecido la sesión entre el cliente y el servidor del Sistema de Monitoreo, el operador de red debe escribir la dirección IP o el nombre (sí se ha configurado el Servicio de Nombre de Dominio), en el navegador WEB. Las acciones del administrador pueden clasificarse en dos grandes grupos: Mantenimiento y Monitoreo.

En la figura 23 se esquematiza la estructura de la interfaz Web del sistema de monitoreo.

La opción de Mantenimiento del sistema se refiere a la introducción, modificación o eliminación de los elementos fundamentales del sistema: Interfaces, Dispositivos y MIB. La función de mantenimiento, permite al operador de la red, modificar la información almacenada en la base de datos y que son de fundamental importancia para la supervisión.

La función de Monitoreo permite al operador de la red, acceder a la información recolectada por el sistema, para cada uno de los elementos de red, integrados en forma manual en la opción de *mantenimiento*.

Los elementos son presentados en una lista, con enlaces hacia las páginas que contienen la información específica de cada uno de ellos: Descripción, Tipo, Nombre de MIB, Disponibilidad, Estado y acceso al gráfico del tráfico de una interface específica.

5.8 OPERACIÓN DEL SISTEMA

Una vez la estación cliente se encuentra en red, le es posible acceder al servidor de monitoreo escribiendo el nombre del host definido por un sistema de nombre de dominio o simplemente escribir la dirección IP asignada al sistema de monitoreo.

En esta pantalla encontraremos dos opciones en las cuales podemos dar mantenimiento al sistema en general permitiendo agregar, eliminar o modificar los parámetros en base a los cuales se realiza el monitoreo, y el monitoreo en sí de aquellos dispositivos que previamente han sido ingresados en los mantenimientos.

Figura 24. Pantalla de inicio del Sistema

5.8.1 MANTENIMIENTOS.

5.8.1.1 DISPOSITIVOS

En los mantenimientos se detallan todos los parámetros que han de servir para monitorear los dispositivos que forman parte de la red, así como también los tipos de interfaces que estos pueden tener dependiendo la función que este dispositivo ejecute, además de los MIB's que contienen la información de la variable sobre la cual se desea ejecutar el monitoreo.

En general se inicia con tres opciones mas como se observa en la figura 25, que permiten realizar cambios sobre los parámetros más importantes que componen el sistema, ya sean estos agregar uno nuevo, como modificar o eliminar alguno ya existente.

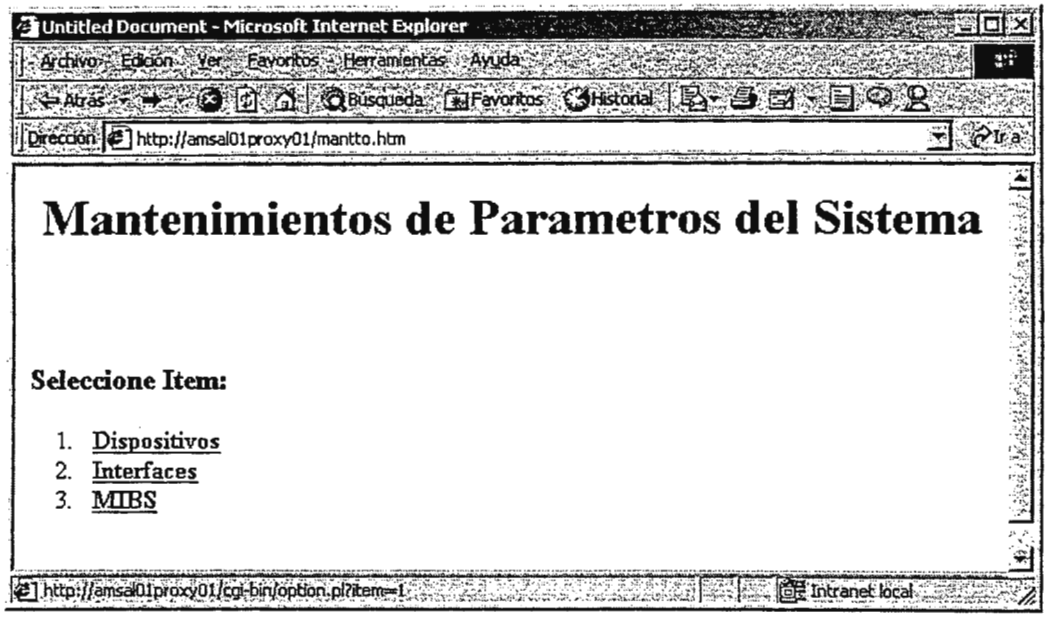


Figura 25. Pantalla de Mantenimientos de Parámetros del Sistema.

Si se desea agregar un nuevo dispositivo, siguiendo la ruta de mantenimiento, luego dispositivo y agregar llegamos a una pantalla como la que se muestra en la figura 26, que contiene información de la pantalla de Ingreso de Dispositivos, requiriendo en un primer momento dos parámetros de configuración del dispositivo, como son el número de interfaces a ser monitoreadas y si utiliza MIB privados, entendiendo por MIB privados aquellos que servirán para ser consultas sobre un dispositivo en particular y de acuerdo a cuales de ellos son seleccionados en una lista que se muestra después de hacer un clic en configurar.

Figura 26. Pantalla de Ingreso de Dispositivos

Por otra parte mas adelante en esta misma pantalla será necesario conocer los índices de las interfaces si no se conocen se puede hacer uso del link que apunta hacia información de las interfaces observándose una nueva pantalla como la que se muestra en la figura 27, en la cual solamente sé digita la comunidad a la que pertenece el dispositivo y su dirección IP devolviendo la descripción de cada una de las interfaces así como del índice de cada una de ellas, el cual nos servirá para identificar sobre cual interfaz se desea realizar la acción de monitoreo.

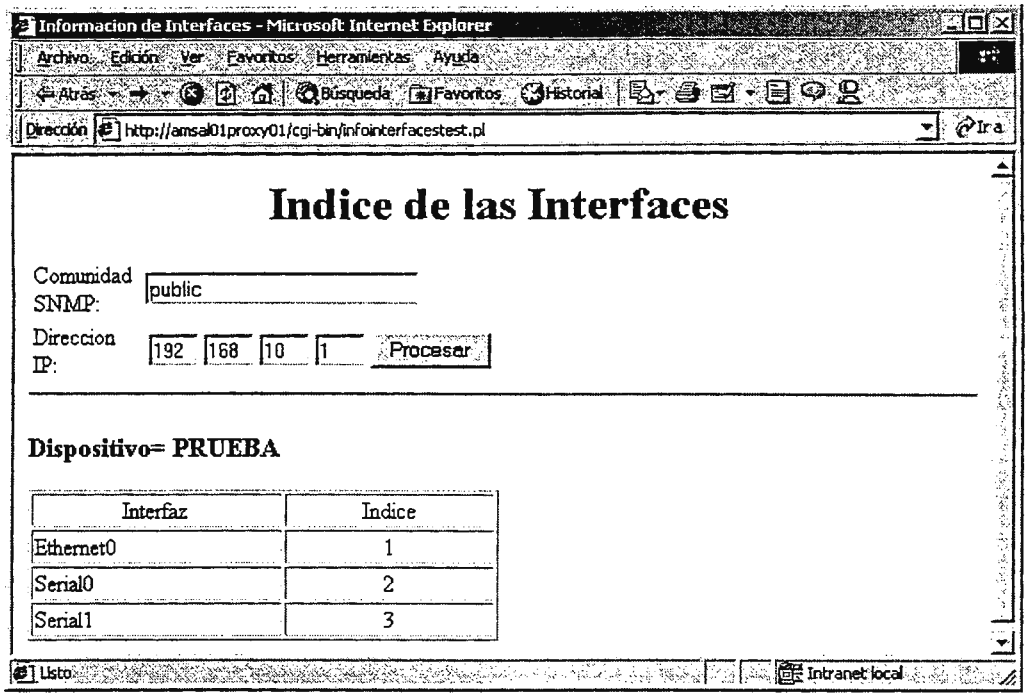


Figura 27. Pantalla para determinar el índice de las interfaces.

Una vez recolectada la información de las interfaces, es necesario colocar la información general del dispositivo donde se requieren los parámetros que se muestran en la figura 28, que corresponde a la información general de cada uno de los dispositivos a ingresar. La asignación de MIB's privados se hace marcando con un cheque sobre aquellos en los cuales se quieren monitorear, los cuales son seleccionados desde una base de datos y pueden ser modificados en las opciones de mantenimiento correspondientes a los MIB's, así como también la selección del tipo de interfaz o las velocidades de esta que pueden ser modificadas.

Haciendo un click en procesar y llenando correctamente cada uno de los campos que se requieren el dispositivo será agregado con éxito.

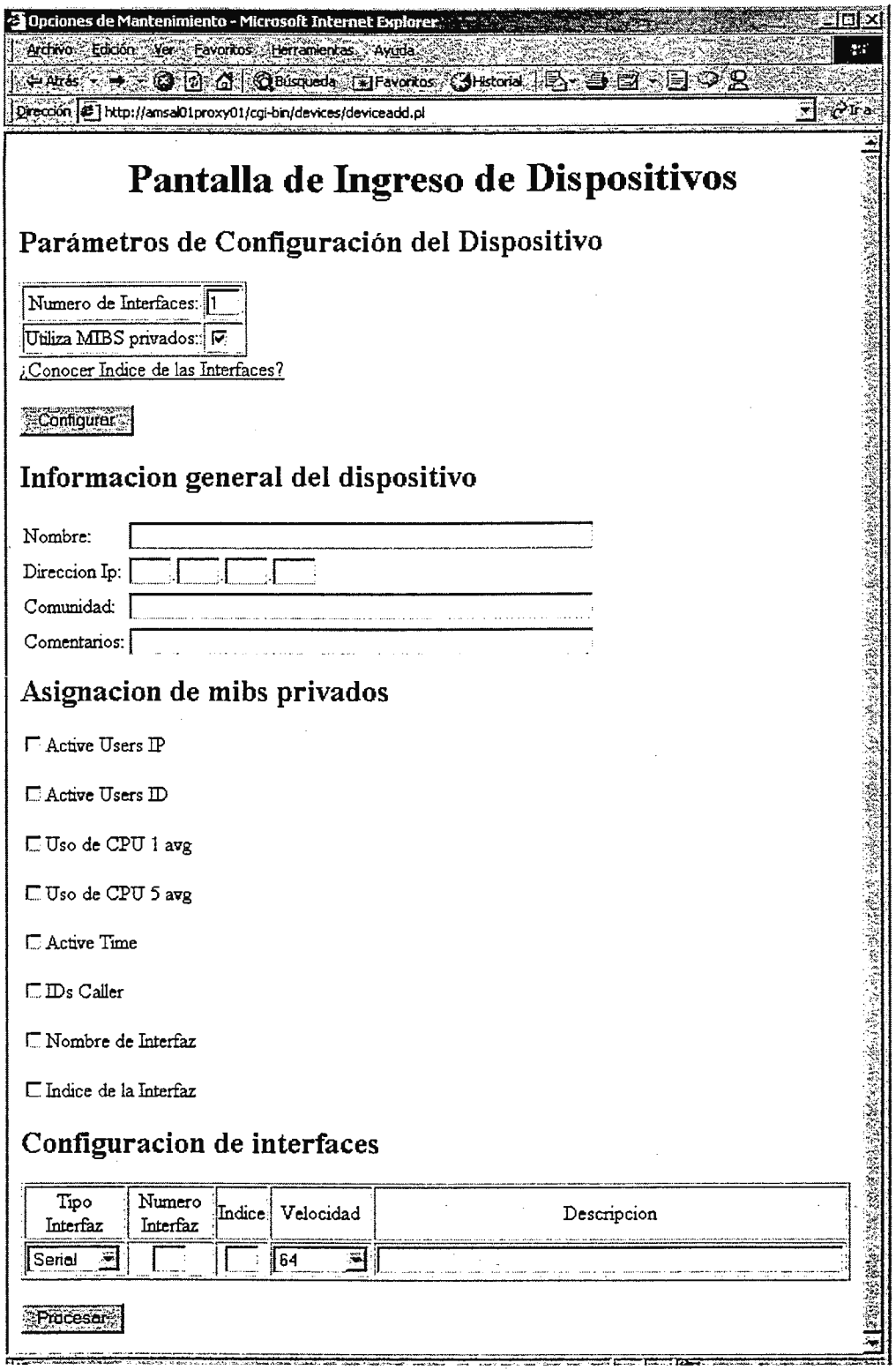


Figura 28. Pantalla de Información general del dispositivo.

Seleccionando la opción de modificar / eliminar, es necesario saber sobre cual dispositivo se quiere realizar el cambio, por medio de la pantalla de búsqueda del dispositivo y como se muestra en la figura 29, se puede encontrar a este conociendo su dirección IP o el nombre de estos, una vez encontrado podemos seleccionar la acción a realizar sobre este.

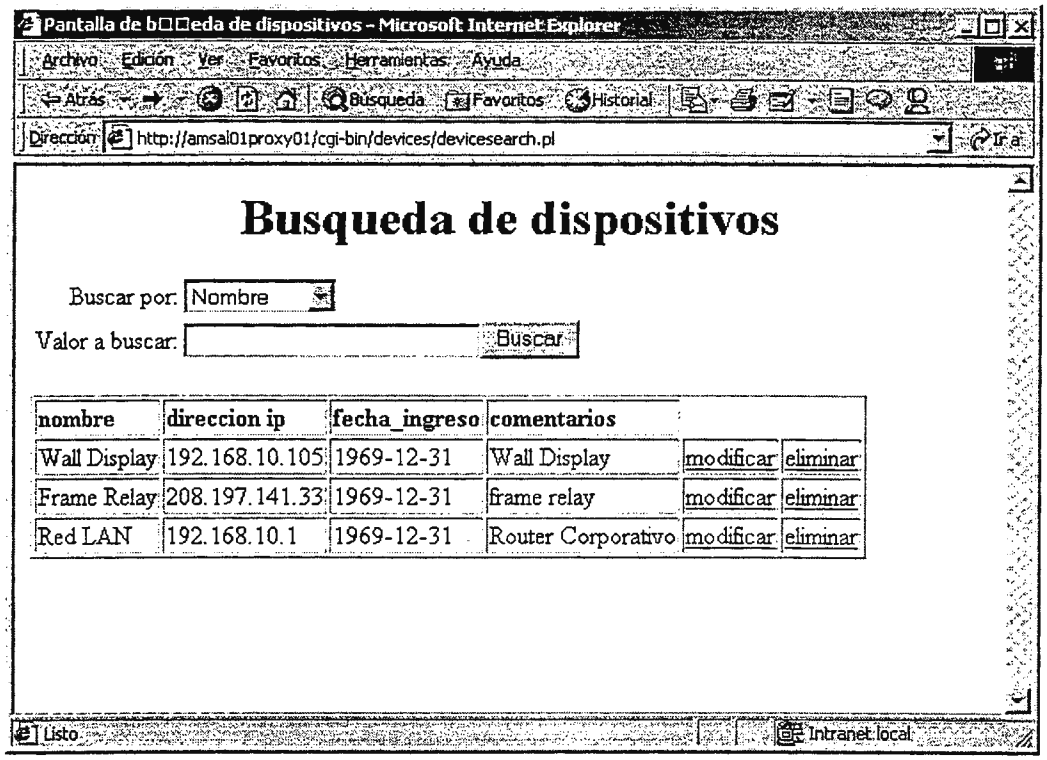


Figura 29. Pantalla de Búsqueda de Dispositivos

Las modificaciones sobre un dispositivo pueden hacerse ya sea sobre la información general, los MIB's privados o las interfaces que fueron ingresados en un principio, observando opciones como las que se muestran en la pantalla de Modificación de dispositivos que se presenta en la figura 30,

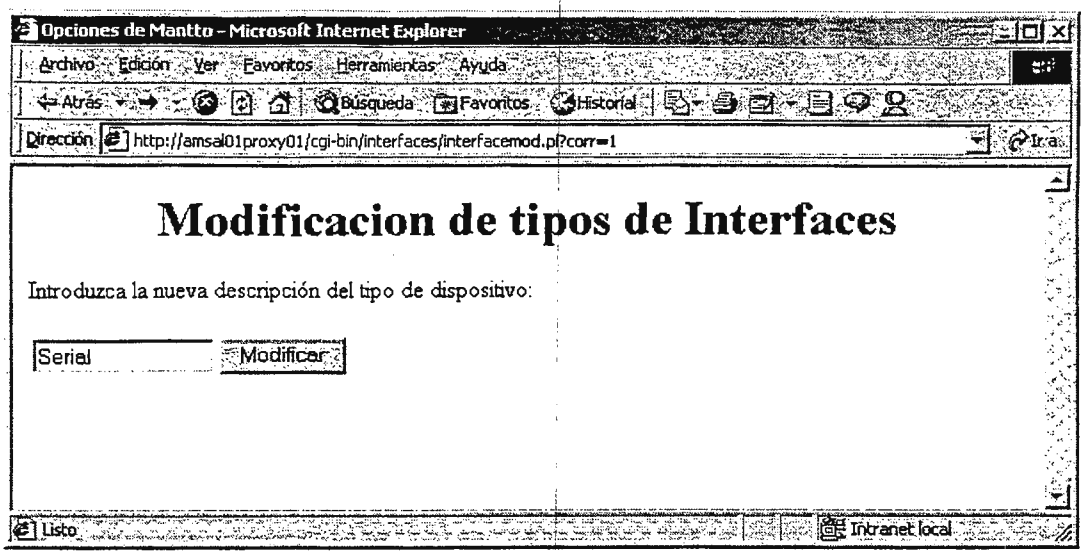


Figura 30. Pantalla de modificación de Dispositivos

La información general puede ser modificada sobre los campos que se observan en la figura 31, realizando los cambos y haciendo un clic sobre el botón de modificar.

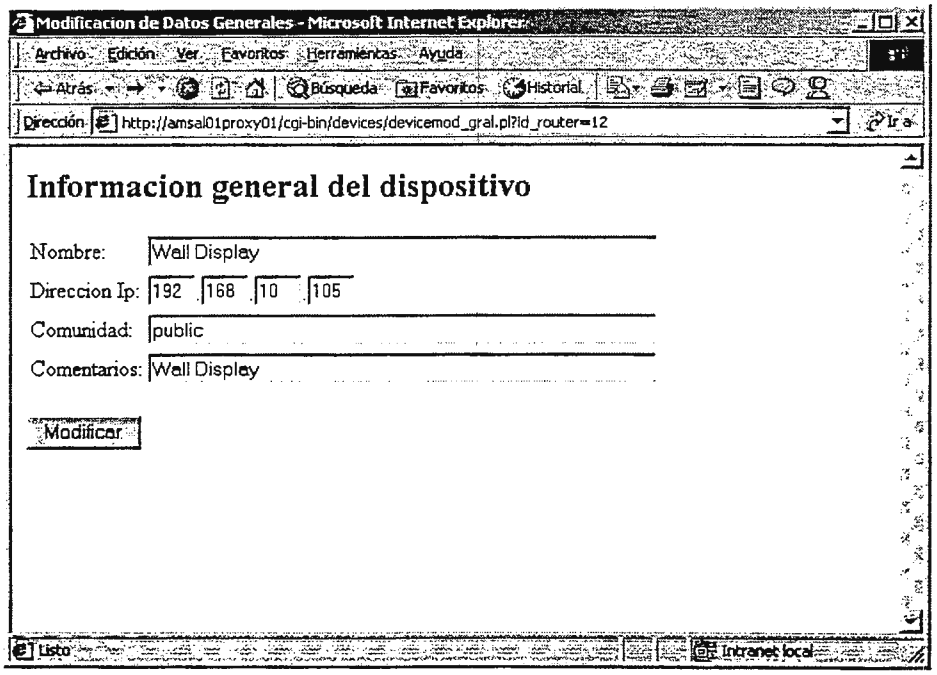


Figura 31. Pantalla de modificación de Información del Dispositivos

Los MIB's privados seleccionados en un inicio pueden ser modificados seleccionando o quitando el cheque de los ya existentes tal y como se observa en la pantalla de Modificación de MIB's Privados cuya lista se modifica desde el mantenimiento de MIB's presentándose aquí aquellos los cuales están disponibles.

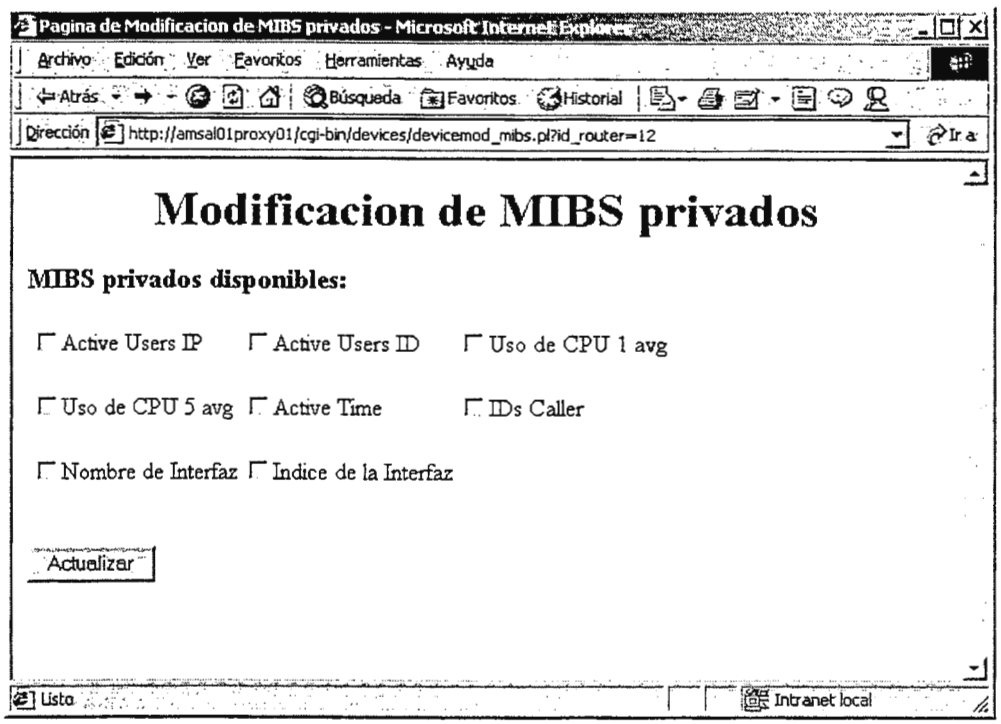


Figura 32. Pantalla de MIB agregados a un Dispositivo.

La modificación de las interfaces del dispositivo puede hacerse sobre una ya existente cambiando algunos parámetros de su información o eliminándola por completo así como también la posibilidad de agregar una nueva interfaz para ser monitoreada, tal como se observa en la figura 33.

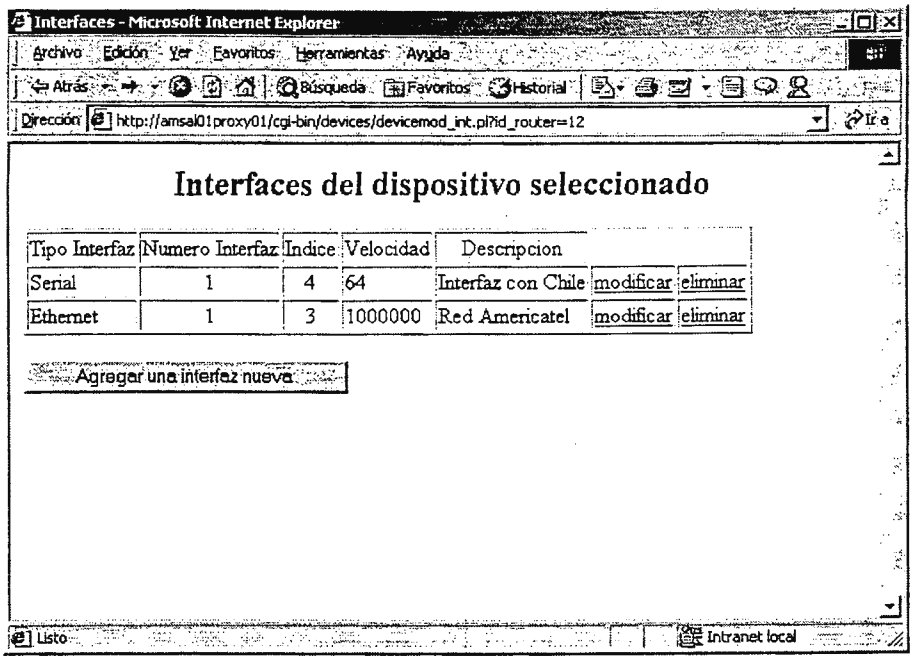


Figura 33. Pantalla de Modificación de interfaces seleccionadas

5.8.1.2 INTERFACES

El mantenimiento de las Interfaces corresponde a agregar, modificar o eliminar los tipos de interfaces sobre los cuales se quiere ejercer el monitoreo, en un primer momento solo están agregados los tipos más comunes que corresponden a las interfaces WAN o seriales y las LAN o Ethernet como se observa en la figura 34, se permite modificar esta tabla de manera que al realizar algún cambio sobre algún dispositivo anteriormente ingresado en la tabla de dispositivos pueda seleccionarse y observarse los cambios realizados sobre las interfaces, ya sea que se haya ingresado algún tipo nuevo, renombrado o eliminado una de las ya existentes.

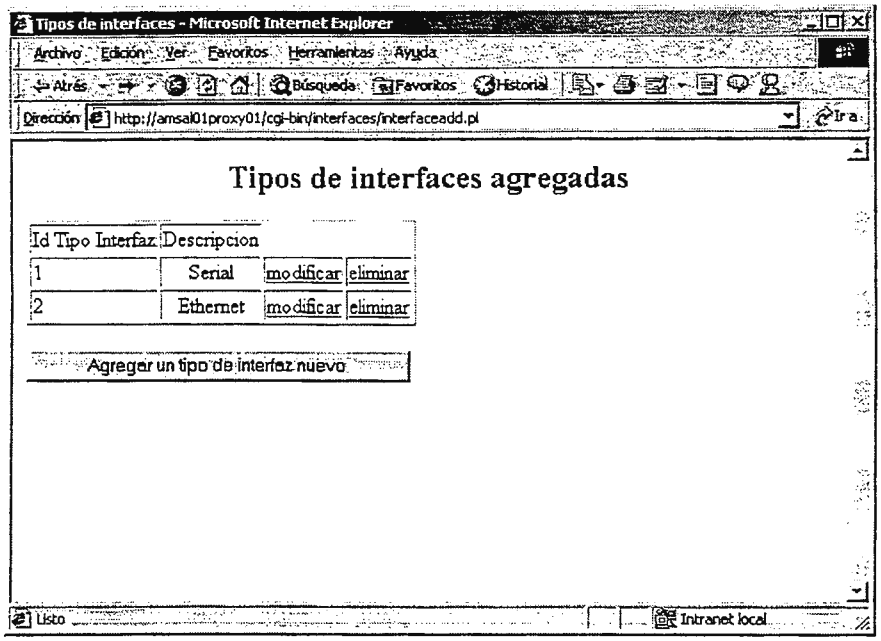


Figura 34. Pantalla de Modificación de interfaces agregadas

5.8.1.3 MIBS

Al igual que en los mantenimientos anteriores se puede agregar modificar o eliminar MIB's para realizar la obtención de la información, en base a ello y tal como se muestra en la figura 35, se puede observar la tabla de MIB's existentes junto a su descripción, string y las opciones de agregar modificar o eliminar estos datos. Si queremos modificarlo obtendremos una pantalla como la que la que se muestra en la figura, donde se modifican los detalles para este MIB en particular.

Para agregar un Nuevo MIB tendremos una pantalla muy parecida a la anterior en la cual se detallan los datos correspondientes a este nuevo MIB.

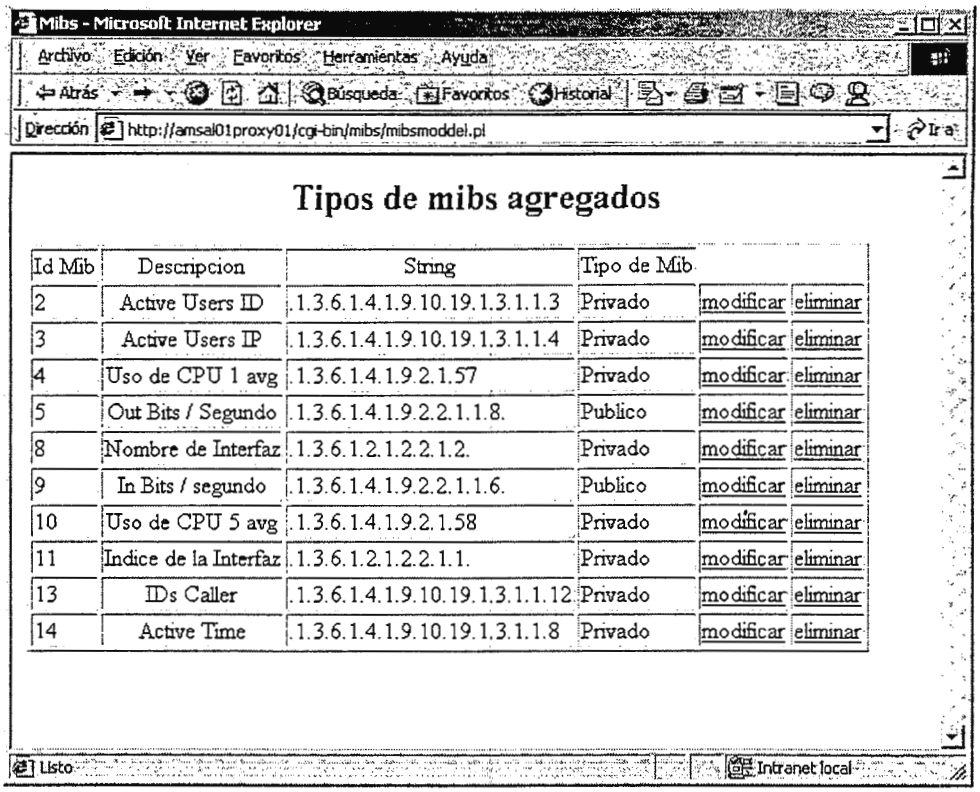


Figura 35. Tipos de MIB existentes

Estas MIB pueden ser modificadas o eliminadas según sea la selección, si en caso se desea hacer algún cambio sobre alguna ya existente presionamos en modificar y nos aparece la siguiente pantalla.

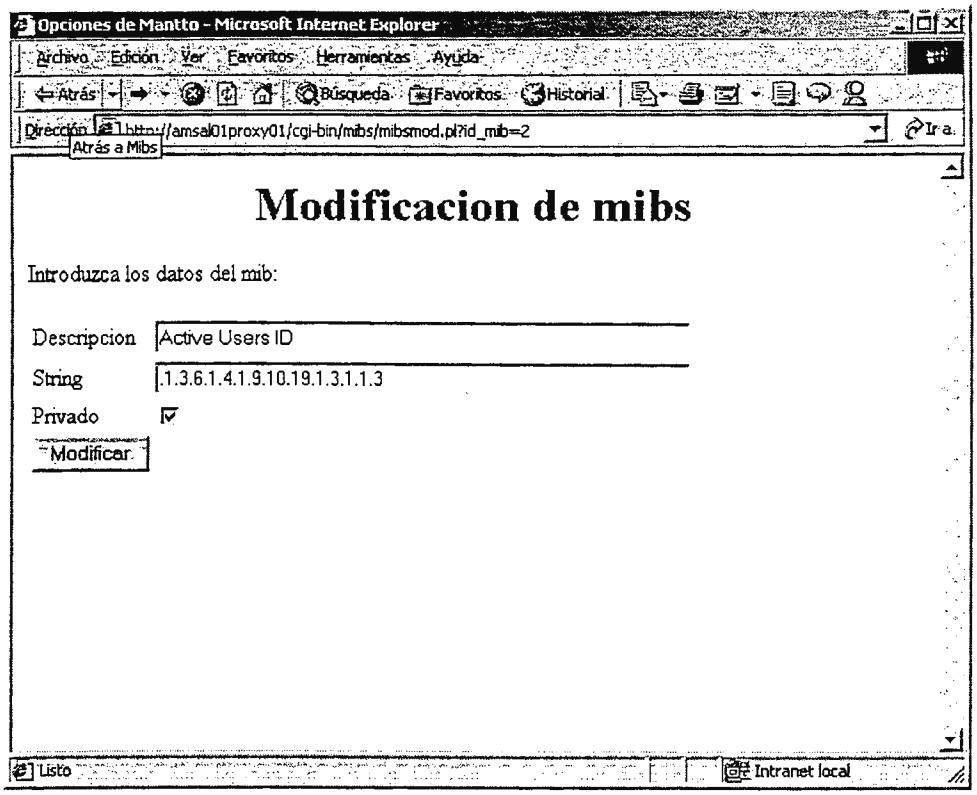


Figura 36. Pantalla de Modificación de MIB.

5.8.2 MONITOREO

La opción de monitoreo es la que permite observar el comportamiento de los dispositivos administrados. En una primera pantalla se enlistan todos los dispositivos sujetos a monitoreo, previamente ingresados en la etapa de mantenimiento tal como se muestra en la figura 37, en esta pantalla se nombran los dispositivos tal y como fueron introducidos en la pantalla de adición de dispositivos.

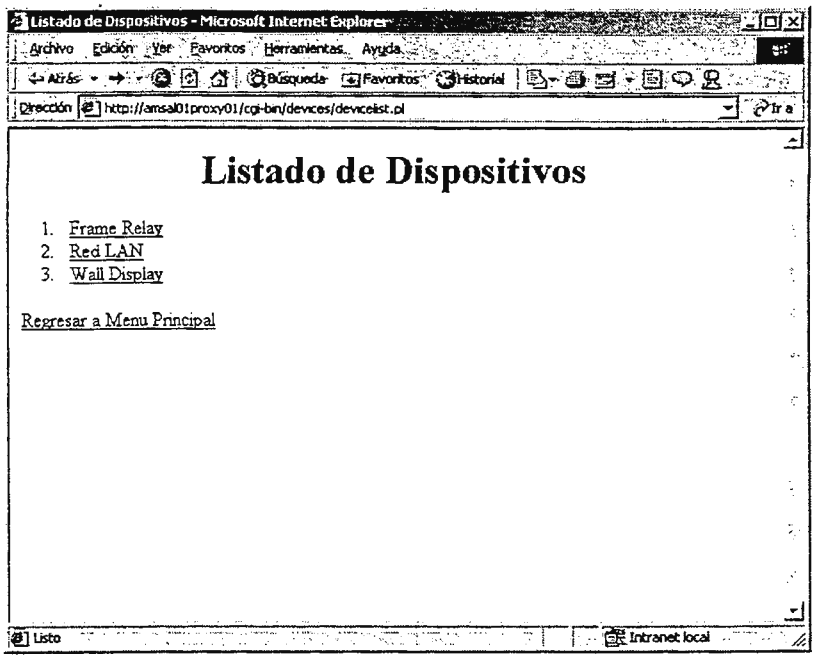


Figura 37. Pantalla de listado de dispositivos.

Haciendo click en cada uno de los nombres de los dispositivos podemos acceder a otra pantalla en la cual se muestra el estado de los parámetros anteriormente seleccionados para cada uno de ellos. Esta pantalla contiene una tabla dividida en seis columnas que se describen a continuación:

a) **Descripción:** Contiene el nombre con el cual el usuario identifica la interfaz seleccionada.
b) **Tipo:** Corresponde al tipo de interfaz que esta siendo monitoreada.
c) **MIB**: Contiene la descripción de la MIB con que el agente devuelve la información requerida por el NMS.
d) **Disponibilidad**: Es el resultado del estado de administración de la interfaz del dispositivo seleccionado. Un icono en "verde" corresponde a un estado de administración disponible para ser utilizado (Encendida), y un icono en "rojo" indica el estado contrario (apagado).
e) **Estado**: indica la operación de la Interface a la cual se hace referencia. La operación de la Interface esta sujeta a la disponibilidad de la misma, es decir un estado de administración apagado corresponde a un estado

operacional "down" el cual se representa por un icono en "rojo", el estado "up" indica un estado de operación capaz de transportar información según sea el protocolo seleccionado en la misma, estado representado por un icono "verde", sin embargo, existe la posibilidad de que la Interface este administrativamente operacional (encendida) pero los protocolos de línea o estado operacional este "down", representándose por un icono "verde" en la columna de disponibilidad y uno "rojo" en la que corresponde al estado.

f) **Gráfico**: Este es un link hacia el grafico que muestra el comportamiento histórico de los valores que han sido devueltos por los agentes, en el cual se muestra un comportamiento diario de la MIB seleccionada contra el tiempo.

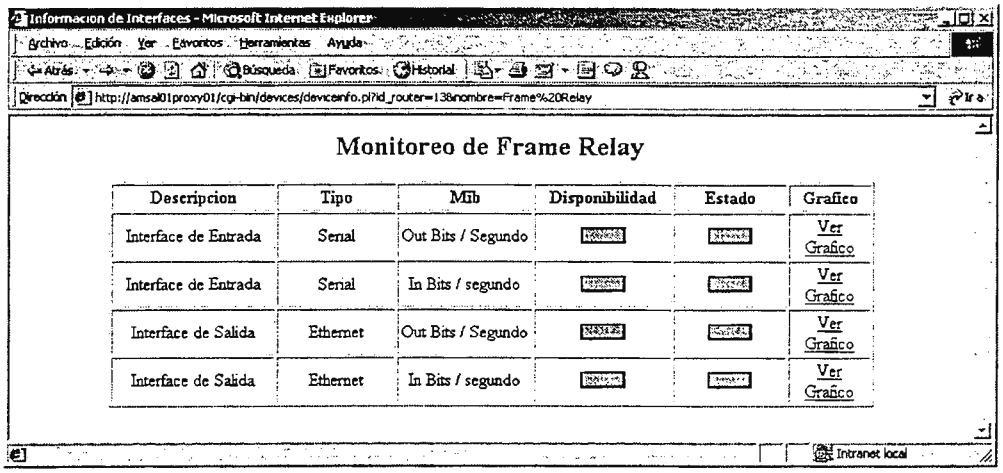


Figura 38. Pantalla de Información de parámetros del dispositivo.

En caso en el que a algún dispositivo se le hayan seleccionado MIB privados para ser monitoreados se presentará una pantalla como la que se muestra a continuación:

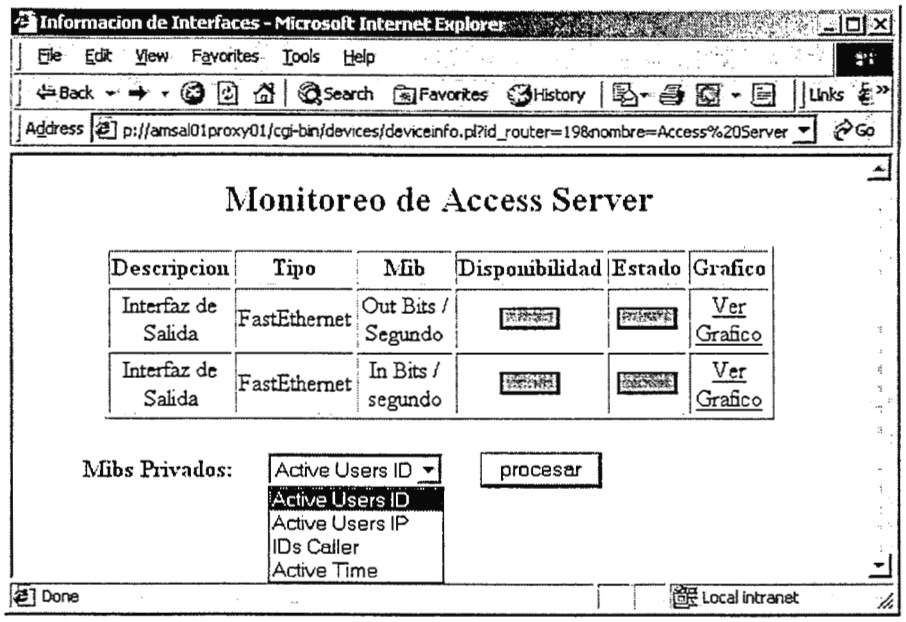


Figura 39. Pantalla de Información de Dispositivos con MIB privados

Como se observa en la pantalla anterior este dispositivo tiene MIBS privados seleccionando cualquiera de ellas obtendremos una pantalla como la siguiente según sea el MIB requerido.

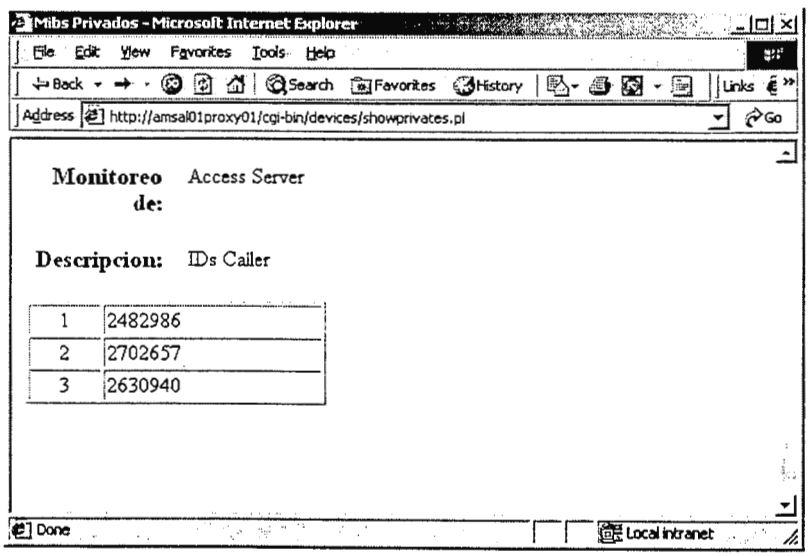


Figura 40. Pantalla de valores de MIB privados

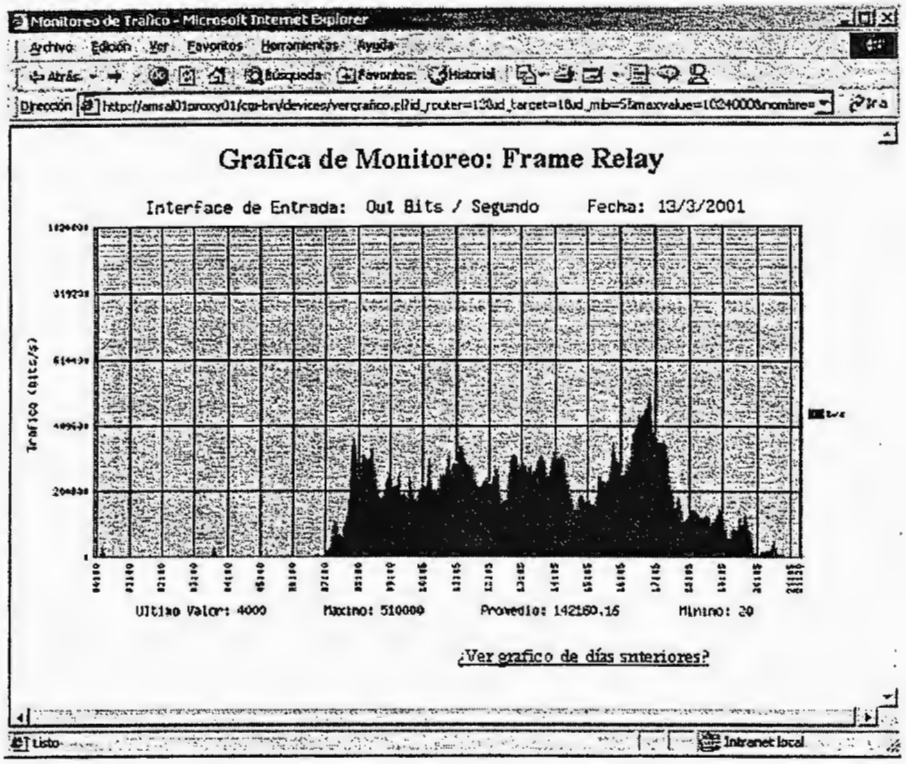


Figura 41. Grafica de parámetros

Un gráfico de los días anteriores puede ser obtenido digitando la fecha la cual se quiere observar haciendo click en el link que nos guiará hasta ella.

Conclusiones

CONCLUSIONES

Con la realización del Sistema de Monitoreo para Redes de Datos Basado en el Protocolo SNMP, ha sido posible desarrollar una herramienta para operadores de red y proporcionar las bases para la innovación de sistemas en el área de comunicación de datos e Internet en El Salvador.

La implementación de un sistema que permita supervisar la operación de una red de comunicación de datos, facilita al administrador realizar el monitoreo continuo y general sobre todos los elementos de la red, contribuyendo en la disminución del tiempo de respuesta en la detección y solución de fallas, y cuantificación de los recursos disponibles como insumo para la planificación e ingeniería del crecimiento de la red.

El crecimiento de las redes actuales, intranets, Internet y la integración de servicios de Voz y Redes Privadas Virtuales a través de redes de paquetes justifica a una empresa la inversión en un sistema de monitoreo, sin embargo tienen costos elevadamente altos y en nuestro país no se ha promovido la investigación y el desarrollo de herramientas que hagan de las redes de comunicación de datos, una ventaja competitiva para las empresas proveedoras de servicio en El Salvador.

Como primera fase de la solución, se ha realizada una profunda investigación sobre las características de los Sistemas de Administración de Redes, los cuales se han basado en Modelos de Referencia, siendo el estándar más utilizado actualmente y con perspectivas para las futuras generaciones de Internet, la administración basada en el modelo TCP/IP.

La investigación se ha centrado en el fundamento de información de administración, el cual está formado por tres estándares internacionales: SNMP, MIB y SMI, que forman parte del grupo de protocolos TCP/IP.

Se incluyó un estudio sobre Sistemas de Monitoreo y Control, determinando las características de los sistemas, en cuanto a operación, elementos, requerimientos, esquemas de funcionamiento y tendencias tecnológicas de las redes de comunicación para el establecimiento del Monitoreo y Control de sus recursos.

Como segunda parte de la solución, se realizó el diseño, considerando elementos de red específicos, centrándose en dispositivos ruteadores y servidores de acceso remoto, gestionando recursos como disponibilidad, cuantificación de tráfico en interfaces y obtención de parámetros específicos ambientales, de operación del hardware, que varían de acuerdo a la aplicación del equipo.

En la implementación del sistema se desarrolló una aplicación, basada en la filosofía cliente-servidor, para integrar las funciones de un Sistema de Administración de Redes (NMS), que corresponden al monitoreo de una red de datos, considerando una interfaz gráfica, basada en Web, de fácil comprensión para el operador de red y presentando el método utilizado para proporcionar una guía práctica para que futuras investigaciones puedan continuar el trabajo iniciado con este proyecto.

Finalmente se ha proporcionado la herramienta para la actualización del sistema, integrando una base de datos que permite adicionar parámetros a supervisar con el ingreso a la función de Mantenimiento del sistema, con la única restricción de conocer los identificadores de objeto específicos (MIB) de la marca del equipo que se quiere integrar o la función que se desea implementar.

Recomendaciones

RECOMENDACIONES

De igual forma que se innova constantemente en el desarrollo de sistemas de comunicación de datos, integrando nuevos servicios e incrementando los requerimientos, surge la necesidad de investigar nuevas funcionalidades que supervisen el perfecto funcionamiento de nuevos parámetros y aplicaciones de misión crítica en una red que soporta múltiples servicios de comunicación.

Dada la constante necesidad de estándares para la interoperatividad entre sistemas de comunicación, es necesario estandarizar también las normas de administración de red, actualmente se ha integrado la versión 2 de SNMP, sin embargo, los grupos de trabajo se encuentran en la fase de prueba de la versión 3. Los estándares para la interoperatividad se encuentran documentos en textos denominados RFC, que deben ser incluidos como parte fundamental de operación del sistema de Monitoreo de Redes Basado en el protocolo SNMP.

Bibliografía

BIBLIOGRAFÍA

- STALLINGS, William. **Comunicaciones y Redes de Computadores.** Editorial Prentice Hall Iberia, 5ª Edición. Madrid, 1997. Pág. 681-692.

- FORD, Merilee. **Tecnologías de Interconectividad de Redes.** Editorial Prentice Hall. México 1998, Pág. 557.

- COMER, Douglas; STEVENS, David L. **Interconectividad de Redes con TCP/IP**
  Volumen II. Diseño e Implementación.
  Editorial Prentice Hall, Tercera Edición, México 2000.

- DOYLE, Jeff. **CCIE Professional Development, Routing TCP/IP**
  Volumen I.
  Editorial Cisco Press, U.S.A. 1998.

- AMATO, Vito. Cisco Networking Academy Program: First-Year Companion Guide.
  Editorial Cisco Press, Cisco Systems, Inc. Indianapolis, IN.

- Microsoft Corporation. **Transact-SQL Reference.**
  Microsoft Corporation, U.S.A. 1995.

- AFERGAN, Michael. **PROGRAMACIÓN EN WEB 6 EN 1.**
  Editorial Prentice Hall Hispanoamericana. Edición en Español, México 1997.

Documentos de Internet:

- White Paper: **Cisco Enterprise Network Management.** www.cisco.com

- White Paper: **Configuring Simple Network Management Protocol.** www.cisco.com

- White Paper: **Configuring System Features.** www.cisco.com

- White Paper: **SNMP Commands.** www.cisco.com

- White Paper: **SNMP Inform Request.** www.cisco.com

- Network Working Group, Request for Comments: 1155, **Structure and Identification of Management Information for TCP/IP-based Internets**, May 1990.

- Network Working Group, Request For Comments: 1156, **Management Information Base for Network Management of TCP/IP-based Internets**, May 1990.

- Network Working Group, Request for Comments: 1157, **A Simple Network Management Protocol (SNMP)**, May 1990

- Network Working Group, Request for Comments: 1158, `Management Information Base for Network Management of TCP/IP-based internets: MIB-II`, May 1990

Sitios WEB:

www.cisco.com/techsupport

www.cpan.org

www.perldoc.com

www.activeperl.com

http://ucd-snmp.ucdavis.edu

http://net-snmp.sourceforge.net

www.linux.org.sv

www.linux.com

www.redhat.com

www.postgresql.org

www.apache.org

www.cisco.com

www.rfc-editor.org

www.ipswitch.com

www.rediris.es/ftp/docs/network/rfc/

www.snmp.com

Documentación Técnica:

- Cisco Systems, Inc. Catalyst 1900 Series Installation and Configuration Guide. Corporate Headquarters, San Jose, CA.

Glosario

GLOSARIO

10BaseT

Especificación Ethernet de banda base de 10 Mbps que utiliza dos pares de cableado de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y el otro para recibirlos. 10BaseT forma parte de la especificación IEEE 802.3, tiene un límite de distancia de aproximadamente 100 metros por segmento.

100BaseT

Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la que se basa, 100BaseT envía impulsos de enlace a través del segmento de la red cuando no se detecta tráfico. Sin embargo, estos impulsos de enlace contienen más información que los utilizados en 10BaseT. Se basa en el estándar IEEE 802.3.

AAL:

Capa de Adaptación del modo de transferencia asíncrona (ATM)

Administración de costos

Una de las cinco categorías de administración de red definidas por ISO para la administración de las redes OSI. Los subsistemas de administración de costos son responsables por la recolección de datos de red relacionados con el uso de los recursos.

Administración de la configuración

Una de las cinco categorías de administración de red definidas por ISO para la administración de redes OSI. Los subsistemas de administración de configuración son responsables por la detección y determinación del estado de una red.

Administración de rendimiento

Una de las cinco categorías de administración de la red definidas por ISO para la administración de redes OSI. Los subsistemas de administración de rendimiento tienen la responsabilidad de analizar y controlar el rendimiento de la red, incluyendo el rendimiento y los índices de error.

Administración de seguridad

Una de las cinco categorías de administración de red definidas por ISO para la administración de las redes OSI. Los subsistemas de administración de seguridad son responsables por el control del acceso a los recursos de red.

Administración de errores

Una de las cinco categorías de administración de red definidas por ISO para la administración de las redes OSI. La administración de errores pretende asegurar la detección y el control de las fallas de red.

Administrador de la red

Persona a cargo del funcionamiento, mantenimiento y administración de una red.

Agente

1. Por lo general, software que procesa consultas y envía respuestas en nombre de una aplicación.
2. En los NMS, un proceso que reside en todos los dispositivos administrados e informa sobre los valores de variables especificadas a las estaciones de administración.
3. En la arquitectura de hardware de Cisco, una tarjeta de procesador individual que proporciona una o más interfaces de medios.

Agrupación MIB

Técnica de sondeo utilizada por el protocolo SNMP para reunir la información necesaria para controlar la red.

Alarma

Mensaje que notifica a un operador o administrador que existe un problema en la red.

ANSI

Instituto Nacional Americano de Normalización. Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante

organizaciones normalizadoras internacionales. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la ISO (Organización Internacional para la Normalización).

ARP

Protocolo de Resolución de Direcciones. Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826.

ATM

Modo de Transferencia Asíncrona.

Base de Datos

Una biblioteca ha de mantener listas campos que posee, de los usuarios que tiene.

Un gestor de base de datos es un programa que permite introducir y almacenar datos, ordenarlos y manipularlos; organizarlos de manera significativa para que se pueda obtener información no visible como totales, tendencias o relaciones de otro tipo. Debe permitir en principio:

- Introducir datos

- Almacenar datos

- Recuperar datos y trabajar con ellos

Bridge

Dispositivo puente entre dos segmentos de red local.

Broadcast

Proceso de transmisión de un dispositivo a muchos dispositivos.

CCITT

Comité Consultivo Internacional Telegráfico y Telefónico. Organización internacional responsable por el desarrollo de estándares de comunicación. Actualmente ha pasado a llamarse UIT-T.

CGI

Medio que utiliza un servidor que habla http para comunicarse con un programa.

CMIP

Protocolo de información de administración común. Protocolo de administración de red de OSI, creado y estandarizado por ISO para el control de redes heterogéneas.

CMIS

Servicios de información de administración común. Una interfaz de servicio de administración de red de OSI creada y estandarizada por ISO para la supervisión y control de redes heterogéneas.

CMOT

CMIP sobre TCP/IP.

Comunidad

En SNMP, un grupo lógico de dispositivos administrados y NMS en el mismo dominio administrativo.

Comunidades SNMP

Esquema de autenticación que permite que un dispositivo de red inteligente valide las peticiones SNMP de los orígenes por ejemplo, el NMS. Un switch ATM LightStream 2020, por ejemplo, responde sólo a las peticiones SNMP que provienen de miembros de comunidades conocidas y que tienen los privilegios de acceso que se requieren para esa petición.

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. Los datagramas IP son las unidades principales de información de la Internet. Los términos *trama, paquete, segmento y mensaje* también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Dirección

Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o dispositivo de red en particular.

Dirección IP

1. Dirección de 32 bits asignada a los hosts que usan TCP/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 host.. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet.
2. Instrucción utilizada para establecer la dirección de red lógica de esta interfaz.

Direcciones IP de origen y de destino

Campo dentro de un datagrama IP que indica las direcciones de origen y de destino de 32 bits.

DNS

Protocolo de Servicio de Nombres de Dominio, convierte el nombre de un Host a una dirección IP.

Enrutamiento

Proceso de descubrimiento de una ruta hacia el host de destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host de destino.

Estándar

Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Ethernet

Protocolo de enlace de datos empleado generalmente para redes de área local.

FTP

Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP utilizado para la transferencia de archivos entre nodos de red. El FTP se define en RFC 959.

Gateway

En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término *router* se utiliza para describir nodos que desempeñan esta función y *gateway* se refiere a un dispositivo especial que realiza una conversión de capa de aplicación de la información de una pila de protocolo a otro.

GUI

Interfaz gráfica del usuario. Entorno del usuario que utiliza representaciones gráficas y textuales de las aplicaciones de entrada y salida y la estructura jerárquica o de otro tipo de los datos en la que se almacena la información. Las convenciones como botones, iconos y ventanas son típicas, y varias acciones se realizan mediante un apuntador (como un ratón). Microsoft Windows y Apple Macintosh son ejemplos importantes de plataformas que usan GUI.

Host

Sistema informático en una red. Similar al término *nodo* , salvo que *host* normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y routers.

HTML

Lenguaje de etiquetas por hipertexto. Formato simple de documentos en hipertexto que usa etiquetas para indicar cómo una aplicación de visualización, como por ejemplo un navegador de la Web, debe interpretar una parte determinada de un documento.

HTTP

Protocolo de Transferencia de Hipertexto.

Hub

1. Por lo general, se usa este término para describir un dispositivo que sirve como centro de una red con topología en estrella.
2. Dispositivo de hardware o software que contiene múltiples

módulos independientes pero que están conectados a los equipos de red y de internetwork. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten las señales sino simplemente dividen las señales enviadas a través de ellos).
3. En Ethernet y IEEE 802.3, un repetidor multipuerto de Ethernet que se conoce a veces como *concentrador*.

IAB

Comité de Actividades de Internet.

IEEE.

Instituto de Ingeniería Eléctrica y Electrónica. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares que predominan en las LAN de la actualidad.

IETF

Fuerza de tareas de Ingeniería de Internet.

Informes MIB

Técnica utilizada por el protocolo CMIP para obtener la información necesaria para controlar la red. Depende de los dispositivos de red para iniciar los informes con respecto al estado de la estación de control central de la red.

Interfaz

1. Conexión entre dos sistemas o dispositivos.
2. En terminología de enrutamiento, una conexión de red.
3. En telefonía, un límite compartido definido por características en común de interconexión física, características de señal y significados de las señales intercambiadas.
4. Límite entre capas adyacentes del modelo de referencia OSI.

Internet

Término utilizado para referirse a la internetwork más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la

llamó *Internet DARPA*. No debe confundirse con el término general *Internet*.

Interrupción

Mensaje que envía un agente SNMP al NMS, a una consola, o a una terminal para indicar que se ha producido un evento significativo, por ejemplo, que se ha producido una condición o umbral definido específicamente.

IP

Protocolo Internet. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork no orientada a la conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Documentado en RFC 791.

ISO

Organización Internacional para la Normalización. Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a la networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking.

LAN

Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y la señalización en la capa física y la capa de enlace de datos del modelo de referencia OSI. Ethernet, FDDI y Token Ring son tecnologías de LAN ampliamente utilizadas.

MAN

Red de área metropolitana. Red que abarca un área metropolitana. Generalmente, una MAN abarca un área geográfica más grande que una LAN, pero cubre un área geográfica más pequeña que una WAN.

MIB

Base de información de administración. Base de datos de información de administración de la red utilizada y mantenida por un

protocolo de administración de la red, por ejemplo, SNMP o CMIP. El valor de un objeto MIB se puede modificar o recuperar mediante las instrucciones SNMP o CMIP. Los objetos MIB se organizan en una estructura de árbol que incluye las ramas públicas (estándar) y privada (propietaria).

Modelo de referencia OSI

Modelo de referencia para interconexión de sistemas abiertos. Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, por ejemplo, direccionamiento, control de flujo, control de errores, encapsulamiento y transferencia confiable de mensajes. La capa superior (la capa de aplicación) es la más cercana al usuario; la capa inferior (la capa física) es la más cercana a la tecnología de medios. Las dos capas inferiores se implementan en el hardware y el software, y las cinco capas superiores se implementan sólo en el software. El modelo de referencia OSI se usa a nivel mundial como método para la enseñanza y la comprensión de la funcionalidad de la red.

Navegador WWW

Aplicación de cliente de hipertexto basada en interfaz gráfica del usuario como, por ejemplo, Navigator o Netscape Explorer, que se utiliza para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a lo largo de la WWW y la Internet.

Networking

Interconexión de cualquier grupo de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NEF

Función de elemento de red, el cual es un bloque funcional de la arquitectura de gestión TMN.

NMS

Sistema de Administración de Redes.

NOC

Centro de operaciones de la red. Organización que tiene la responsabilidad de mantener una red.

Nodo

1. Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales, pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra *dispositivo*.
2. En SNA, el componente básico de una red y el punto en el que una o más unidades funcionales conectan canales o circuitos de datos.

Objeto administrado

En la administración de red, un dispositivo de red que puede ser administrado por un protocolo de administración de red.

Operador de la red

Persona que regularmente supervisa y controla una red, ejecutando tareas tales como revisar y responder las interrupciones, supervisar el rendimiento, configurar nuevos circuitos y solucionar los problemas.

OSI

Interconexión de sistemas abiertos. Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

Paquete

Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. El término "paquete" se usa con mayor frecuencia para referirse a las unidades de datos de la capa de red.

PERL

Lenguaje de programación, el cual deriva su nombre por sus siglas en ingles PERL (Practical Extraction and Report Language). Surgió de otras herramientas de UNIX como son: sed, grep, C, C++, etc. Principalmente sirve para labores de procesamiento de texto consolidándose como "el lenguaje para programar aplicaciones para WWW".

Ping

Instrucción utilizada por el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de red. Este es un mecanismo de prueba sumamente básico.

PostgreSQL

Postgres intenta ser un sistema de bases de datos de mayor nivel que MySQL, a la altura de Oracle, Sybase o Interbase.

Protocolo

1. Descripción formal de un conjunto de reglas y convenciones que rigen la forma en la que los dispositivos de una red intercambian información.
2. Campo dentro de un datagrama IP que indica el protocolo de capa superior (Capa 4) que envía el datagrama.

Protocolo de enrutamiento

Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. IGRP, OSPF y RIP son ejemplos de protocolos de enrutamiento.

Puente (Bridge)

Dispositivo que conecta y transmite paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Los puentes operan en la capa de enlace de datos (Capa 2) del modelo de referencia OSI. En general, un puente filtra, envía o inunda la red con una trama entrante sobre la base de la dirección MAC de esa trama.

Puerto

1. Interfaz en un dispositivo de internetworking (por ejemplo, un router).
2. En la terminología IP, un proceso de la capa superior que recibe

información de las capas inferiores.
3. Volver a escribir el software o el microcódigo para que se ejecute en una plataforma de hardware o en un entorno de software distintos de aquellos para los que fueron diseñados originalmente 4. Un enchufe hembra en un panel de conmutación que acepta un enchufe del mismo tamaño que el del jack RJ45. Los cables de conmutación se usan en estos puertos para establecer una conexión cruzada entre computadores cableados al panel de conmutación. Esta interconexión es la que permite que las LAN funcionen.
4. Un enchufe hembra en un panel de conmutación que acepta un enchufe del mismo tamaño que el del jack RJ45. Los cables de conmutación se usan en estos puertos para interconectar computadores cableados al panel de conmutación. Esta interconexión es la que permite que las LAN funcionen.

Red

1.) Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de un medio de transmisión.
2.) Instrucción que asigna una dirección basada en la NIC con la cual el router está directamente conectado.
3.) Instrucción que especifica cualquier red conectada directamente que se desee incluir.

RMON

Monitoreo remoto. Especificación del agente MIB descrita en RFC 1271 que define las funciones del monitoreo remoto de dispositivos de la red. La especificación RMON suministra varias capacidades de monitoreo, detección de problemas e informes.

Router

Dispositivo de la capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Envía paquetes desde una red a otra basándose en la información de la capa de red. De vez en cuando denominado *gateway* (aunque esta definición de gateway se está tornando obsoleta).

Servidor

Nodo o programa de software que suministra servicios a los clientes.

Servidor de acceso

Procesador de comunicaciones que conecta dispositivos asíncronos a una LAN o WAN a través de la red y el software de emulación de terminales. Realiza el enrutamiento síncrono y asíncrono de los protocolos soportados. A veces se denomina *servidor de acceso a la red.*

SGMP

Protocolo de monitoreo de gateway simple. Protocolo de administración de red que se tuvo en cuenta para la normalización de la Internet y es el origen de SNMP. Documentado en RFC 1028.

SNMP

Protocolo de administración de red simple. Protocolo de administración de red que se utiliza casi exclusivamente en redes TCP/IP. SNMP suministra un medio para supervisar y controlar los dispositivos de red, y para administrar configuraciones, recoger estadísticas, el desempeño y la seguridad.

SNMP2

SNMP Versión 2. Versión 2 del popular protocolo de administración de red. SNMP2 soporta estrategias de administración de red centralizadas y distribuidas, e incluye mejoras en el SMI, operaciones de protocolo, arquitectura de administración y seguridad.

Sondeo

Método de acceso en el cual un dispositivo de red principal pregunta, de forma ordenada, si los dispositivos secundarios tienen datos que deban transmitir. La pregunta se realiza bajo la forma de un mensaje a cada dispositivo secundario que le otorga a estos dispositivos el derecho a transmitir.

Subred

1. En redes IP, una red que comparte una dirección de subred específica. Las subredes son redes segmentadas de forma arbitraria por el administrador de la red para suministrar una estructura de enrutamiento jerárquica, de varios niveles mientras protege a la subred de la complejidad de direccionamiento de las redes conectadas. A veces se denomina *subnet.*
2. En redes OSI, un conjunto de sistemas finales y sistemas

intermedios bajo el control de un dominio administrativo único y que utiliza un protocolo de acceso de red exclusivo.

Switch

1. Dispositivo de red que filtra, envía e inunda la red con tramas según la dirección de destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.
2. Término general que se aplica a un dispositivo electrónico o mecánico que permite que una conexión se establezca según sea necesario y se termine cuando ya no haya ninguna sesión para soportar.

Tabla de enrutamiento

Tabla almacenada en un router o en algún otro dispositivo de internetworking que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

TCP

Protocolo para el control de la transmisión. Protocolo de la capa de transporte orientado a conexión que proporciona una transmisión confiable de datos de full dúplex. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP

Protocolo de control de transporte / protocolo Internet. Nombre común para el conjunto de protocolos desarrollados por el DOD de los EE.UU. en los años '70 para soportar el desarrollo de internetwork a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Telnet

Instrucción utilizada para verificar el software de capa de aplicación entre estaciones de origen y de destino. Este es el mecanismo de prueba más completo disponible.

Terminal

Dispositivo simple en el que se pueden introducir o recuperar datos de una red. En general, las terminales tienen un monitor y un teclado, pero no tienen procesador o unidad de disco local.

Trace

Comando que utiliza valores de tiempo de existencia (TTL) para generar mensajes desde cada router que se utiliza a lo largo de la ruta. Es muy poderoso en cuanto a su capacidad para ubicar fallas en la ruta desde el origen hasta el destino.

Trama

Agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión. Generalmente se refiere al encabezado y a la información final, utilizados para la sincronización y el control de errores, que rodean los datos de usuario contenidos en la unidad. Los términos *datagrama*, *mensaje*, *paquete* y *segmento* también se utilizan para describir las agrupaciones de información lógica en las distintas capas del modelo de referencia OSI y en distintos círculos de tecnología.

UDP

Protocolo de datagrama de usuario. Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin acuse de recibo o garantía de entrega y que requiere que el procesamiento y retransmisión de errores sean manejados por otros protocolos. UDP se define en la RFC 768

UIT-T

Sector de Normalización de la Unión Internacional de Telecomunicaciones(UIT-T) (anteriormente el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT)). Organismo internacional que desarrolla estándares de comunicación.

UNIX

Sistema operativo desarrollado en 1969 en los laboratorios Bell. UNIX ha pasado por varias iteraciones desde sus comienzos. Esto incluye UNIX 4.3 BSD (Distribución Estándar de Berkeley), desarrollado en la universidad de California en Berkeley, y UNIX System V, versión 4.0, desarrollado por AT&T.

WAN

Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por proveedores de servicio comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

WWW

World Wide Web. Red de servidores de Internet de gran tamaño que suministra hipertexto y otros servicios para terminales que ejecutan aplicaciones cliente tales como un navegador WWW.

Anexo I
Número identificador de Objeto para variables CISCO Systems INC.

Object Identifier Numbers for Variables

The figures in this section provide a visual overview of the Cisco MIB variables along with the object identifier numbers for each MIB variable. The MIB variables are arranged alphabetically within each figure (in the same order in which they appear in the sections of this guide).

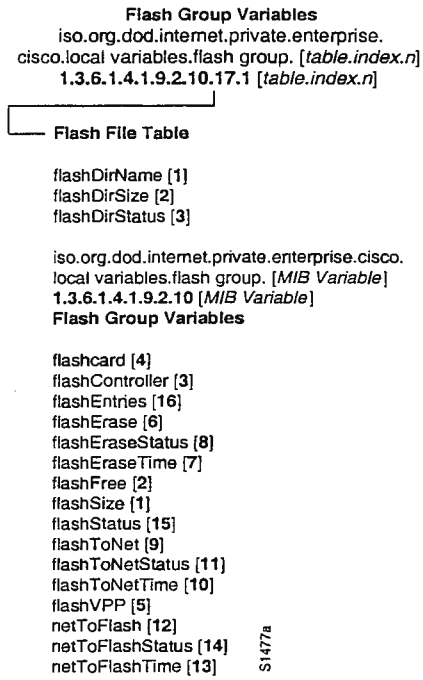


Figure 5 Local Variables: Flash File Table and Flash Group

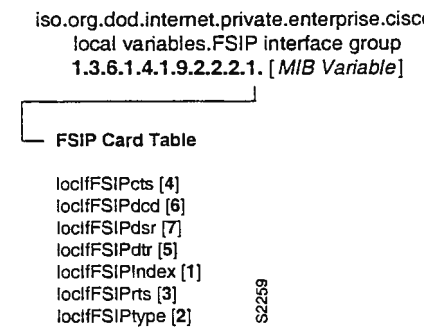


Figure 6 FSIP Group Variables

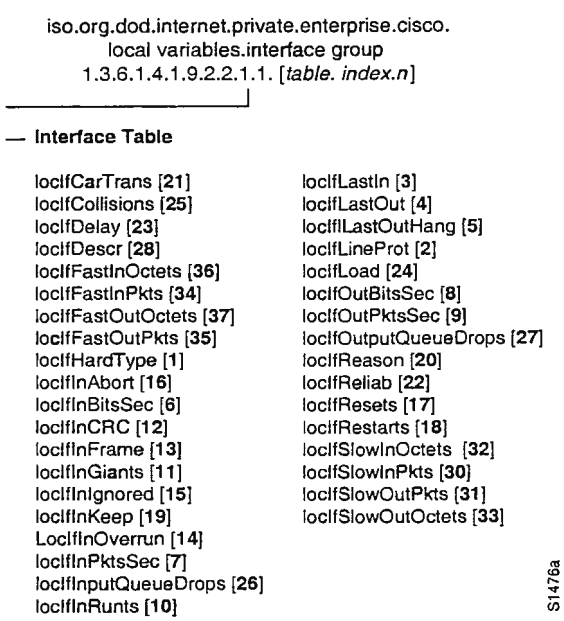


Figure 7 Local Variables: Interface Group Table

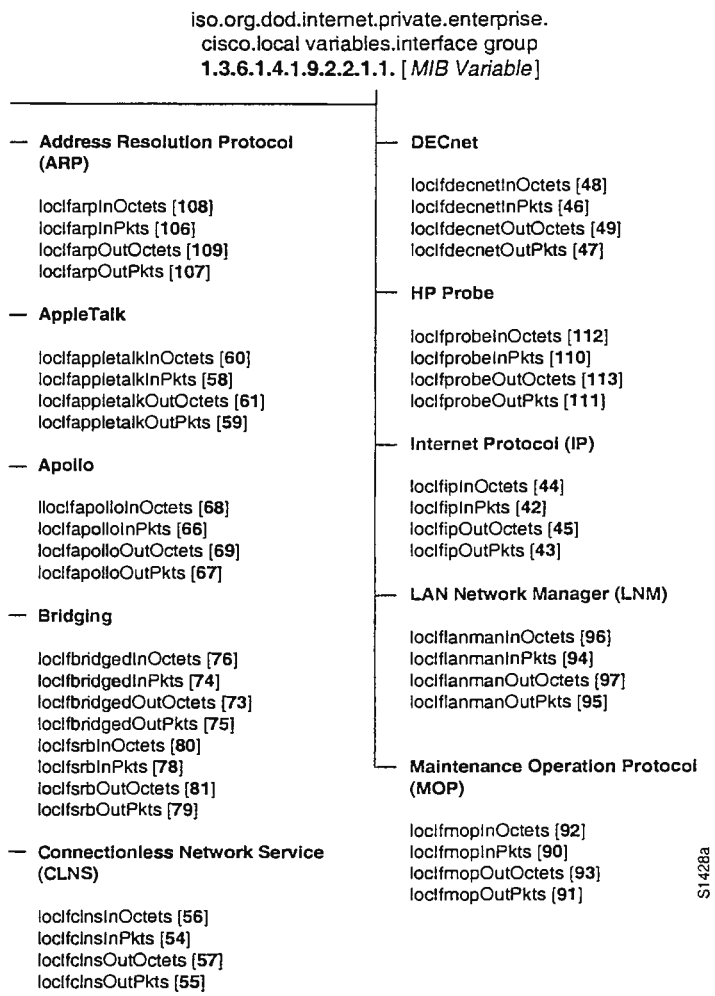


Figure 8 Local Variables: Interface Group—ARP, AppleTalk, Apollo, Bridging, CLNS, DECnet, HP Probe, IP, LNM, and MOP

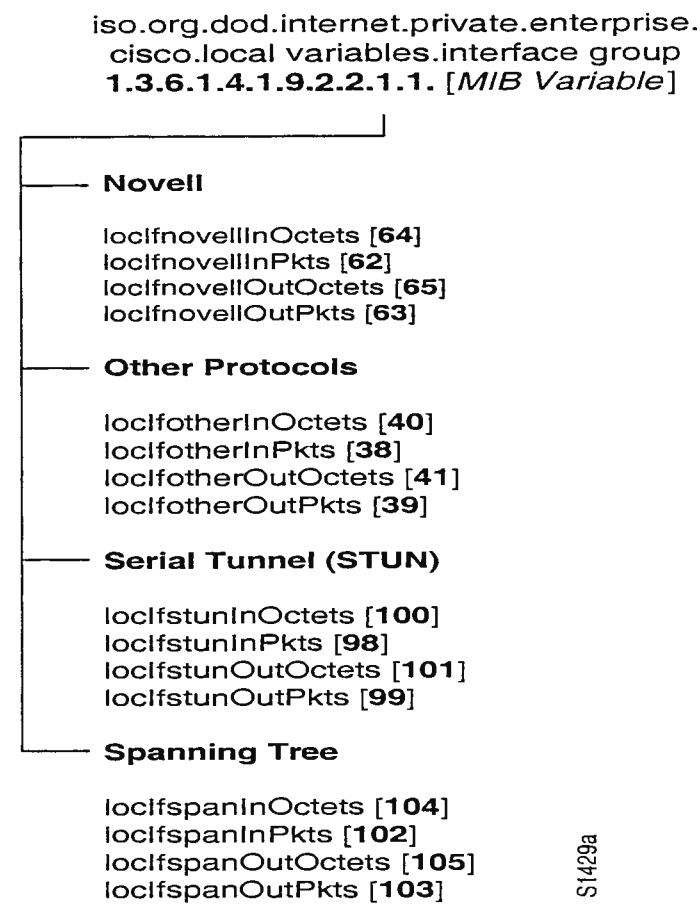


Figure 9 Local Variables: InterfaceGroup—Novell, Other Protocols, STUN, Spanning Tree

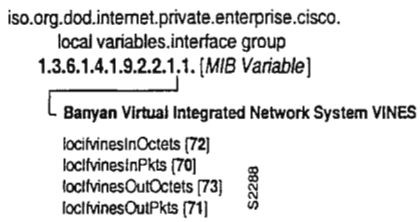


Figure 10 Local Variables: Interface Group—Vines

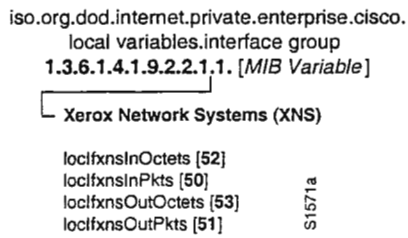


Figure 11 Local Variables: Interface Group—XNS

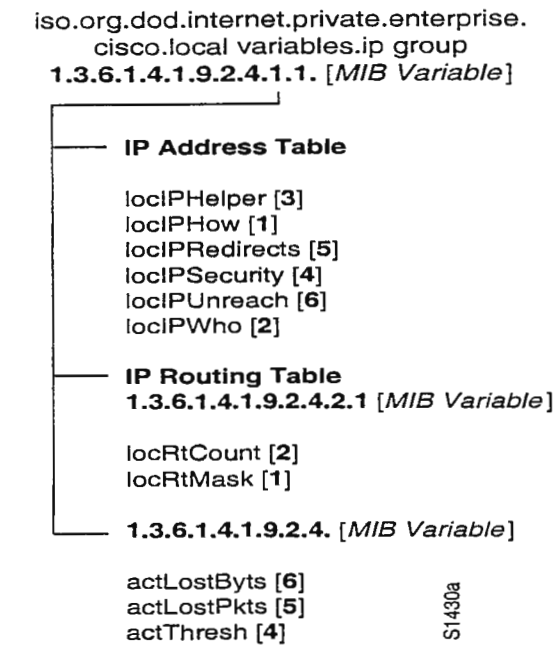


Figure 12 Local Variables: Internet Protocol (IP) Group

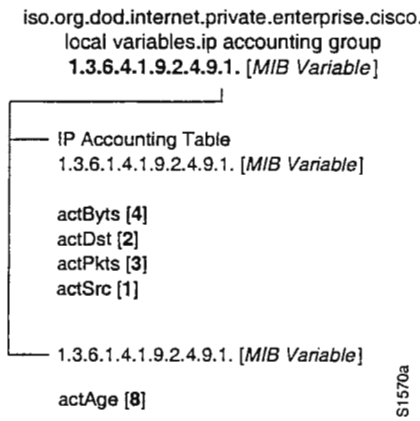


Figure 13 Local Variables: IP Accounting Table

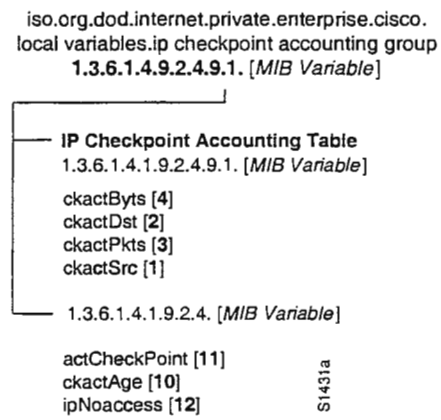


Figure 14 Local Variables: IP Checkpoint Accounting Table

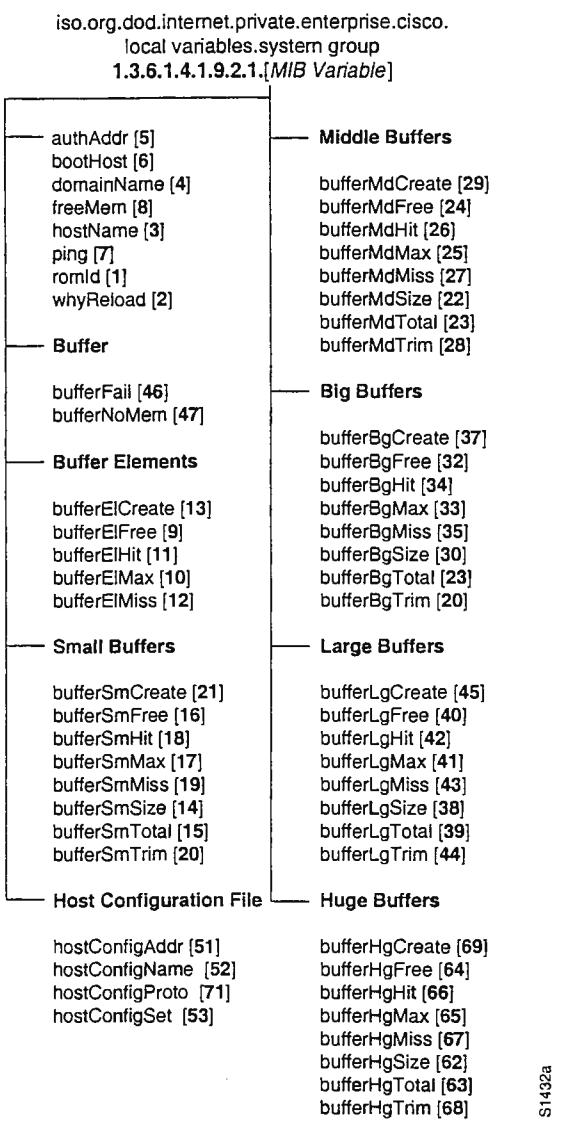


Figure 15 Local Variables: System Group—Buffers

Figure 16 Local Variables: System Group—CPU Utilization and Environmental Monitor Card

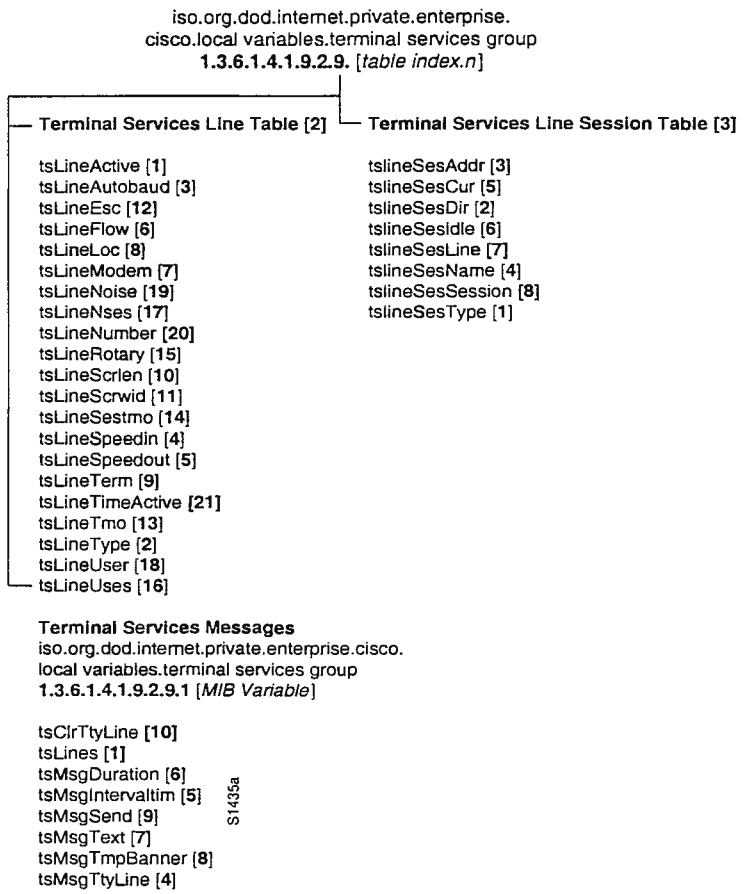


Figure 17 Local Variables: Terminal Server Group

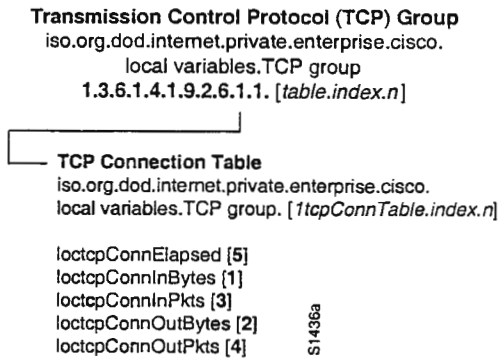


Figure 18 Local Variables: Transmission Control Protocol (TCP) Connection Table

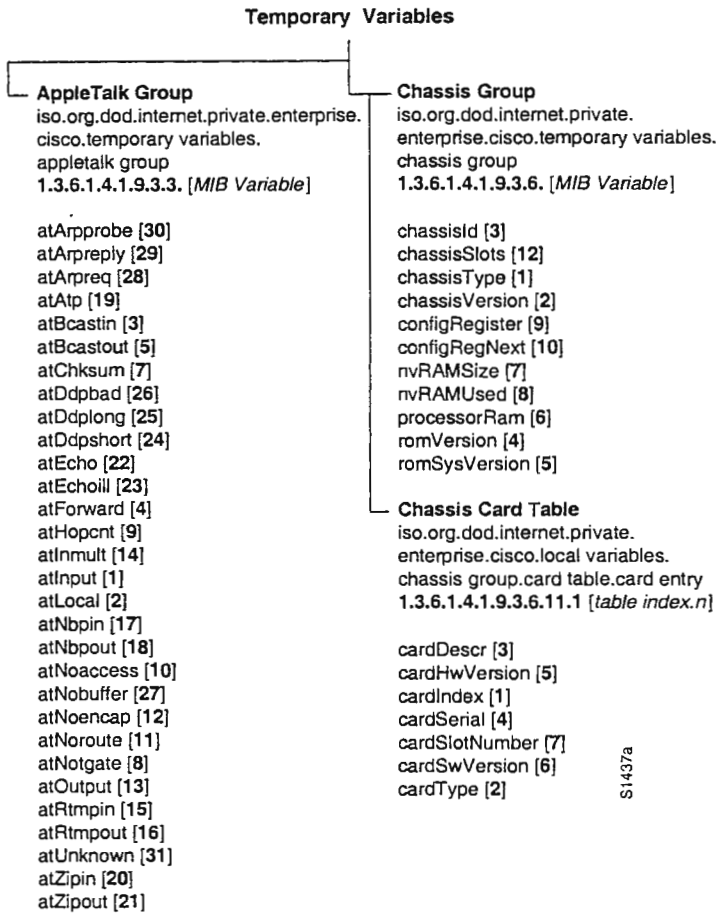


Figure 19 Temporary Variables: AppleTalk and Chassis

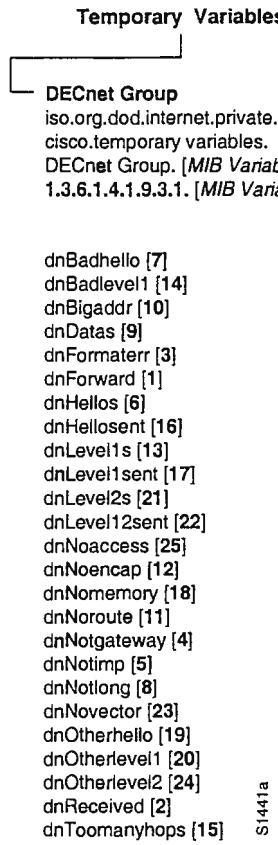


Figure 20 Temporary Variables: DECnet

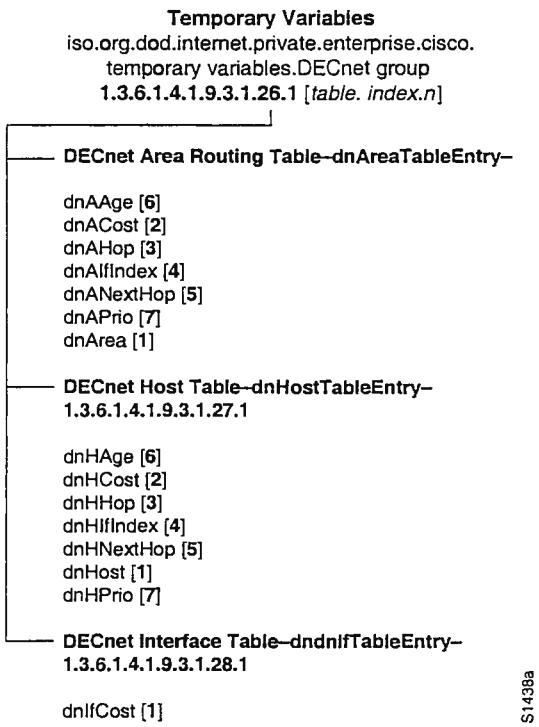


Figure 21 Temporary Variables: DECNet Tables

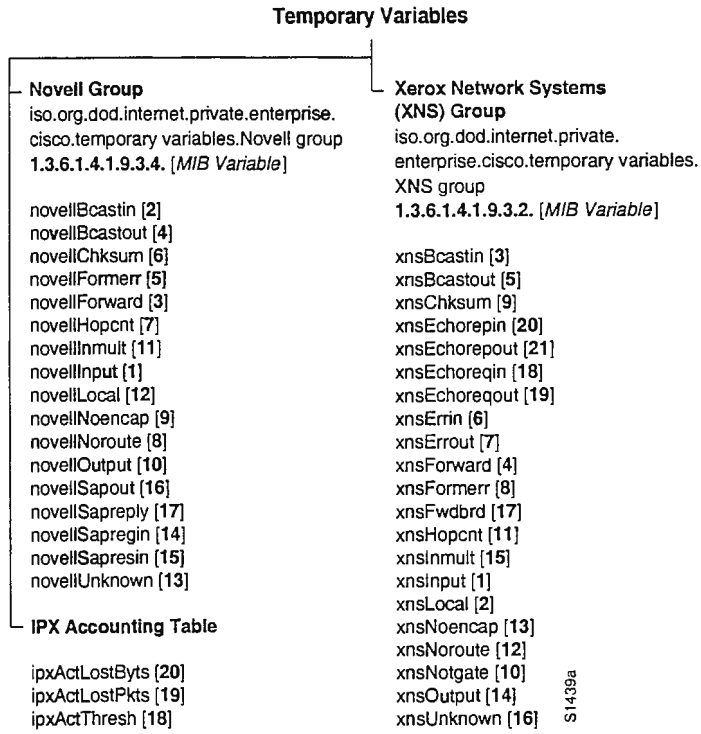


Figure 22 Temporary Variables: Novell and XNS

Virtual Integrated Network Service (VINES) Group
iso.org.dod.internet.private.enterprise.cisco.
temporary variables.vines group
1.3.6.1.4.1.9.3.5. [*MIB Variable*]

vinesBcastfwd [7]
vinesBcasttin [5]
vinesBcastout [6]
vinesCksumerr [12]
vinesClient [28]
vinesEchoIn [22]
vinesEchoOut [23]
vinesEncapsfailed [15]
vinesFormaterror [11]
vinesForwarded [4]
vinesHopcount [13]
vinesIcpIn [17]
vinesIcpOut [18]
vinesInput [1]
vinesLocaldest [3]
vinesMacEchoIn [20]
vinesMacEchoOut [21]
vinesMetricOut [19]
vinesNet [26]
vinesNocharges [10]
vinesNoroute [14]
vinesNotgt4800 [9]
vinesNotlan [8]
vinesOutput [2]
vinesProxy [24]
vinesProxyReply [25]
vinesSubnet [27]
vinesUnknown [16]

S2584

Figure 23 Temporary Variables: VINES I

Virtual Integrated Network Service (VINES) Interface Table
iso.org.dod.internet.private.enterprise.cisco.
temporary variables.Vines group
1.3.6.1.4.1.9.3.5.29. [*If*].[*Variable*]

vinesIfAccesslist [3]
vinesIfArpEnabled [5]
vinesIfEnctype [2]
vinesIfFastOkay [11]
vinesIfInputRouterFilter [81]
vinesIfLineup [10]
vinesIfMetric [1]
vinesIfInputNetworkFilter [82]
vinesIfOutputNetworkFilter [83]
vinesIfPropagate [4]
vinesIfRedirectInterval [8]
vinesIfRouteCache [12]
vinesIfRxArp0 [25]
vinesIfRxArp1 [26]
vinesIfRxArp2 [27]
vinesIfRxArp3 [28]
vinesIfRxArpIllegal [29]
vinesIfRxBcastDuplicate [47]
vinesIfRxBcastForwarded [46]
vinesIfRxBcastHelpered [45]
vinesIfRxBcastin [20]
vinesIfRxChecksumError [24]
vinesIfRxEcho [48]
vinesIfRxFormatError [18]
vinesIfRxForwarded [21]
vinesIfRxIcpError [30]
vinesIfRxIcpIllegal [32]
vinesIfRxIcpMetric [31]
vinesIfRxIpc [33]
vinesIfRxLocalDest [19]
vinesIfRxMacEcho [49]
vinesIfRxNoRoute [22]
vinesIfRxNotEnabled [17]
vinesIfRxProxyReply [50]
vinesIfRxRtp0 [34]
vinesIfRxRtp1 [35]
vinesIfRxRtp2 [36]
vinesIfRxRtp3 [37]
vinesIfRxRtp4 [38]
vinesIfRxRtp5 [39]
vinesIfRxRtp6 [40]
vinesIfRxRtpIllegal [41]
vinesIfRxIpUnknownCnt [43]
vinesIfRxIpcUnknownCnt [44]
vinesIfRxSpp [42]
vinesIfRxZeroHopCount [23]
vinesIfServerless [6]
vinesIfSplitDisabled [9]
vinesIfTxArp0 [63]
vinesIfTxArp1 [64]
vinesIfTxArp2 [65]
vinesIfTxArp3 [66]
vinesIfTxBcast [52]
vinesIfTxBcastForwarded [61]
vinesIfTxBcastHelpered [62]
vinesIfTxEcho [78]
vinesIfTxFailedAccess [55]
vinesIfTxFailedDown [56]
vinesIfTxFailedEncaps [54]
vinesIfTxForwarded [53]
vinesIfTxIcpError [67]
vinesIfTxIcpMetric [68]
vinesIfTxIpc [69]
vinesIfTxMacEcho [29]
vinesIfTxNotBcastNotgt4800 [54]
vinesIfTxNotBcastNotlan [58]
vinesIfTxNotBcastPpcharge [60]
vinesIfTxNotBcastToSource [57]
vinesIfTxProxy [80]
vinesIfTxRtp0 [70]
vinesIfTxRtp1 [71]
vinesIfTxRtp2 [72]
vinesIfTxRtp3 [73]
vinesIfTxRtp4 [74]
vinesIfTxRtp5 [75]
vinesIfTxRtp6 [76]
vinesIfTxSpp [77]
vinesIfTxUnicast [51]

S2585

Figure 24 Temporary Variables: VINES II