UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ADMINISTRACION DE REDES UTILIZANDO EL PROTOCOLO SNMP

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

RENATTO GUSTAVO GONZALES FIGUEROA

PROMOCIÓN
2002 - I

LIMA – PERÚ
2006

ADMINISTRACION DE REDES UTILIZANDO EL PROTOCOLO SNMP

Este informe esta dedicado a mi familia, sin su apoyo incondicional y constante insistencia seria muy difícil alcanzar el nivel profesional al que estoy logrando.

SUMARIO

El presente trabajo trata acerca del uso del protocolo SNMP en la administración de redes de datos. Este protocolo de uso bastante extendido nos permite con su ligereza y sencillez cubrir los requisitos necesarios para la administración de las redes. La necesidad de implementación de este tipo de soluciones es crucial para las empresas ya que el aumento de dispositivos en sus redes es cada vez mayor. Para mantener entonces a estas en optimas condiciones debemos saber reconocer los problemas y como prevenirlos o solucionarlos. En este informe reconoceremos los principales problemas en una red y luego daremos las pautas para la implementación de una solución SNMP desde la ubicación de los puntos administrables hasta la configuración de software libre de gestión.

INDICE

PROLOGO

El propósito de este informe es presentar un panorama de los posibles problemas que se encuentran en una red de datos, como en realidad estudiar detalladamente todos los problemas que pueden presentarse en una red seria motivo de un libro completo, nos limitaremos a mencionar los mas comunes, sus características y la estrategia de solución posible; para luego plantear el uso de herramientas de administración, estudiando en detalle al protocolo SNMP.

Para cumplir este objetivo iniciaremos con el **Capitulo I,** un capitulo introductorio a las tecnologías de gestión de redes, veremos cuales son las características comunes entre ellas y a que están orientadas. Continuaremos con el **Capitulo II,** un pequeño fundamento teórico sobre redes de datos, protocolos TCP/IP y dispositivos utilizados en las redes de datos, que nos servirá para enmarcar el contexto donde implementaremos las soluciones de gestión, así nos será fácil reconocer cuales son los dispositivos que debemos gestionar de acuerdo a sus funciones dentro de una red.

Luego, ya con el fundamento teórico desarrollado en el **Capitulo III,** mencionaremos los protocolos de mayor uso en las redes de datos y telecomunicaciones. Que estándares hay en el mercado y cuales están en uso o cuales no. Una vez que tengamos el panorama completo pasaremos a estudiar con mayor detalle en el **Capitulo IV** el protocolo SNMP, analizaremos su modo de funcionamiento, con que elementos interactuará en la red y como está constituído. También veremos su evolución a lo largo del tiempo, desde sus inicios como un protocolo provisional hasta nuestros días donde es el protocolo de gestión mas utilizado. Para esto mencionaremos sus versiones SNMPv1, SNMPv2 y SNMPv3, haciendo hincapié en los cambios que se han producido al pasar de una versión a otra.

En el **Capitulo V** nos tocara reconocer los principales errores dentro de una red, aquí veremos los problemas, las posibles causas y las posibles acciones que se deberían tomar. Todo esto acompañado de sugerencias de cómo implementar SNMP en la red.

Finalmente en le **Capitulo VI** veremos unos ejemplos de aplicación de software SNMP, para esto hemos empleado como modelo 2 aplicaciones libres de costo que hay en Internet, una en entorno de comandos y otra que emplea un entorno grafico y genera reportes vistosos que nos facilitan la interpretación de la información. Adicionalmente

veremos una solución comercial ACTIVE SNMP como otra alternativa de elección para la implementación de SNMP.

La conclusión final a la que se pretende llegar en este informe, es que para manipular la información de administración necesaria en una red, debemos utilizar aplicaciones que utilicen protocolos de gestión. Y se ha seleccionado el uso de SNMP por ser ligero, y fácil de utilizar, así como el de uso mas extendido, siendo una de sus ventajas adicionales el ser parte de la suite de protocolos TCP/IP, lo que asegura que su despliegue se extienda a redes de diferentes tipos y tamaños.

CAPITULO I
INTRODUCCION A LA ADMINISTRACION DE REDES

1.1 Introducción

En los años 80 observamos una gran expansión en el área de la implementación de redes de datos. Las compañías se dieron cuenta de los beneficios y el aumento en productividad generado por las tecnologías de red, lo que motivo que empezaran a implementar redes y a expandir las ya existentes tan rápido como las nuevas tecnologías y productos iban ingresando al mercado. Mas o menos en los mediados de los años 80 algunas compañías comenzaron a experimentar problemas por implementar diferentes (y muchas veces incompatibles) tecnologías de red.

Los problemas asociados con la expansión de las redes afectan tanto la administración diaria de la operación de la red como la planificación estratégica del crecimiento de la red. Cada nueva tecnología requiere sus propios expertos. Esto causo que en los inicios de los años 80 los requerimientos de personal para gestionar grandes redes heterogéneas sea crítico para las compañías.

De esta manera apareció la necesidad de una administración automática de las redes que pueda ser integrada a través de diferentes entornos y tecnologías.

La gestión de redes puede interpretarse de diferentes formas. En algunos casos involucra a un solo administrador de red monitorizando la actividad de la red con un software analizador de protocolos. En otros casos involucra una base de datos distribuida, un polling automático de dispositivos de red y estaciones de trabajo generando en tiempo real gráficos de la topología y tráfico de la red.

La mayoría de las arquitecturas de gestión de redes usan la misma estructura y relaciones entre sus elementos. Estaciones finales (equipos administrados), tales como computadoras y otros dispositivos de red, que ejecutan software que les permite enviar alertas cuando identifican problemas. Una vez recibidas estas alertas las entidades administradoras son programadas para reaccionar ejecutando uno o varios grupos de

acciones, incluyendo una notificación al operador, log de eventos, apagado del sistema y intentos de reparación automática del sistema.

Las entidades administradoras además hacen consultas (polling) a las estaciones finales (equipos administrados) para verificar ciertas variables. Estas consultas pueden ser automáticas o iniciadas por los usuarios pero el software (agentes) en los equipos administrados responderá a todas ellas. Estos agentes son módulos de software que primero recolectan información sobre el equipo administrado donde residen, luego almacenan esta información en una base de datos y después la envían a las entidades administrativas a través de algún protocolo de administración.

Los eventos típicos que son monitorizados suelen ser:

- Ejecución de tareas como pueden ser realización de copias de seguridad o búsqueda de virus.
- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de los cambios que se producen en el inventario de hardware.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro del arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones.

Como se vio anteriormente las redes grandes son heterogéneas, esto hace necesario una unificación de la información administrada y del protocolo de administración, lo que nos obliga a recurrir a la estandarización.

1.2 Conceptos de Administración de Redes

El término administración o gestión se refiere a crear el entorno necesario que nos permita llevar a cabo las acciones necesarias para: Planificar, Organizar, Dirigir y Controlar.

- **Planificar:** consiste en analizar el entorno y fijar metas (objetivos), este paso es muy importante ya que nos permite trazar el camino hacia donde deberemos seguir. Esto nos permite orientar nuestros esfuerzos hacia un punto determinado que es el que deseamos alcanzar.

- **Organizar:** consiste en la asignación de recursos, para alcanzar el objetivo planificado es importante conocer los recursos con los que contamos y como serán distribuidos de manera eficiente.
- **Dirección:** esta relacionado con el liderazgo y motivación, fundamentales para mantenernos siempre constantes hacia la dirección establecida.
- **Control:** consiste en realizar seguimientos y correcciones, a los resultados que vamos logrando, para estar siempre alertas a las incidencias que se presentaran en el transcurso del camino hacia el objetivo planificado.

Todo esto va relacionado directamente con la **Toma de Decisiones.** La Toma de Decisiones es el eje fundamental cuando planteamos cualquier modelo de gestión, para que las decisiones sean eficientes y certeras deben ser tomadas en el momento exacto y con la rapidez necesaria. Por lo tanto el ente encargado de la toma de decisiones debe recibir información veraz, confiable y a tiempo, si desea cumplir con este objetivo. Como vemos la necesidad de contar con información confiable, real y en el tiempo adecuado es crucial en el momento de realizar una buena gestión.

Cuando hablamos de la gestión de redes se cumplen los mismos principios y deberemos trazar nuestros objetivos de acuerdo al modelo de gestión de red que deseemos plantear. La gestión de redes cubre un concepto bastante amplio y abarca desde la asignación de políticas de usuarios, aquí se incluye como organizamos la forma en que los usuarios serán capaces de acceder a la red y a que recursos o servicios podrán acceder en ella; hasta el despliegue de equipos (hardware) y aplicativos (software) que permitan la captura y/o envió de información, y la realización de acciones correctivas o preventivas necesarias de acuerdo a la información adquirida.

Aquí hay algunas preguntas que deberíamos contestar cuando pensamos en gestionar una red:

¿Qué es lo que nos motiva a gestionar las redes? Esta pregunta es muy importante cuando deseamos determinar el objetivo a cumplir en la etapa de planificación. Las respuestas pueden ser muy variadas, de acuerdo a las expectativas que cada administrador de una red quiera cumplir, pero principalmente podríamos dar las siguientes respuestas, por ser las más comunes:

- Control de Activos Estratégicos Corporativos.

- Control de Complejidad.
- Mejorar Servicio.
- Equilibrar necesidades.
- Reducir indisponibilidad.
- Control de Costes.

¿Cómo llevare a cabo la Gestión de la red? Desde el punto de vista funcional no encontraremos un patrón común. La funcionalidad dependerá de:

- Tipo de Red gestionada
- Tipo de Equipos gestionados.
- Objetivos específicos de la gestión de red.

1.2.1 ¿Qué vamos a administrar?

Administración del desempeño: para gestionar el desempeño de una red es necesario definir indicadores de desempeño como:

- Orientados a servicio
    - Disponibilidad
    - Tiempo de Respuesta
    - Fiabilidad
- Orientados a eficiencia
    - Throughput
    - Utilización

Aquí haremos mención de dos de los indicadores más importantes:

Disponibilidad de servicios:

Es necesario traducirlo a disponibilidad de componentes individuales

Objetivo: maximizar (cumplir) la disponibilidad de los objetos. Aquí se cumple lo siguiente:

D= MTBF/ (MTBF+MTTR)

MTBF: Mean Time Between Failures, se refiere al tiempo que debe transcurrir entre fallas del equipo, actúa además como indicador de calidad del equipo.

MTTR: Mean Time To Repair, indica el tiempo que transcurre entre el momento que se ingresa una falla hasta que es solucionada. Aquí influye mucho el tiempo de detección del fallo y la política de mantenimiento utilizada.

Tiempo de Respuesta:

Se relaciona al tiempo que demoran en responder alguna consulta los servicios de la red. Aquí mencionamos algunos rangos:

- > 15 seg. Inaceptable para servicios interactivos
- > 4 seg. Dificultan servicios interactivos encadenados (con memoria del usuario)
- 2 a 4 seg. Dificultan servicios interactivos que requieran concentración del usuario
- 2 seg. Limite aceptable normalmente
- Décimas de segundo: para aplicaciones de tipo gráfico
- < 0,1 seg. servicios de eco.

Aquí se debe considerar además 2 componentes:

- Tiempo de transmisión (ida y vuelta)
- Tiempo de proceso de servicio

Administración de la contabilidad: nos permite gestionar aspectos relacionados con los costos, tarificación y facturación. Aquí debemos considerar:

- Identificación de componentes de coste
- Establecimiento de políticas de tarificación
- Definición de procedimientos para tarificación
- Gestión de facturas
- Integración con la Contabilidad Empresarial

Administración de la seguridad: indispensable para mantener la red entre los parámetros de seguridad óptimos. Aquí debemos considerar:

- Funciones que proporcionan protección continuada de la red y sus componentes en los distintos aspectos de seguridad:
    - Acceso a las redes
    - Acceso a los sistemas
    - Acceso a la información en transito
- Funciones de la gestión de seguridad:
    - Definición de análisis de riesgos y política de seguridad
    - Implantación de servicios de seguridad e

- Infraestructura asociada
- Definición de alarmas, registros e informes de seguridad

Administración de la configuración: aquí encontramos los parámetros necesarios para mantener la configuración de los dispositivos y servicios acordes a los requerimientos pre-establecidos. Aquí gestionamos:

- **Gestión de Inventario:** es decir de los componentes de hardware y software que componen los equipos en la red. Aquí haremos uso además de:
  - Herramientas de autodescubrimiento
  - Combinación con herramientas CAD de gestión de cableado

- **Gestión de Topología:** la topología se refiere a como están físicamente interconectados los dispositivos en la red. Aquí haremos uso de:
  - Herramientas de auto-topología
  - Distintas vistas topológicas

- **Gestión de Servicios de Directorio.**

- **Gestión de SLAs (Service Level Agreements):** Esto es fundamental cuando además de los servicios que proporciona nuestra red internamente en la compañía, damos servicios a terceros. Estos parámetros son definidos en el contrato entre cliente/proveedor o entre proveedores sobre servicios a proporcionar y calidades asociadas

  - Identificación de las partes contractuales
  - Identificación del trabajo a realizar
  - Objetivos de niveles de servicio
  - Niveles de servicio proporcionados
  - Multas por incumplimiento
  - Fecha de caducidad
  - Cláusulas de renegociación
  - Prestaciones actuales proporcionadas

  - **Gestión de Incidencias: TTS (Trouble Ticket Systems).** se registra la fecha y hora de:

- Informe de Incidencia
- Resolución de Incidencia
- Usuario/Localización
- Equipo afectado
- Descripción problema
- ESTADO
- Operador(es)
- Grado de Severidad
- Historial de Incidencia
- Comentarios.

Administración de fallos: debemos mantener activamente el nivel de servicio detectando y resolviendo o anticipándonos a los fallos que pudieran producirse. Aquí empleamos dos tipos de gestión:

- **Gestión proactiva**: evitar fallos detectando "tendencias" hacia fallos determinando umbrales de ciertos parámetros. Para esto debemos monitorizar estos umbrales o programar notificaciones automáticas.
  Como se menciono en la gestión preactiva debemos adelantarnos a los fallos para esto la Gestión de Pruebas Preventivas consta de:
  - Pruebas de Conectividad
  - Pruebas de Integridad de Datos
  - Pruebas de Integridad de Protocolos
  - Pruebas de saturación de datos
  - Pruebas de saturación de conexiones
  - Pruebas de tiempo de respuesta
  - Pruebas de bucle
  - Pruebas de diagnóstico

- **Gestión reactiva:** asumir que existen fallos inevitables detectarlos lo antes posible. Monitorización periódica (no es posible notificación).
  Las incidencias que detectamos en la red tienen un ciclo de vida y es importante que sea gestionado adecuadamente. Por lo general el ciclo de vida es el siguiente:

- **Detección de problema:** alarma de Usuarios, alarma de Herramientas.
- **Determinación del problema:** La información sobre el fallo puede no ser fiable en cuanto a la fuente del fallo.
- **Diagnosis del problema:** procedimentado.
- **Resolución del problema:**

  Por operadores de help-desk (80-85%)

  Por operadores técnicos (5-10%)

  Por especialistas en comunicaciones (2-5%)

  Por especialistas en aplicaciones (1-3%)

  Por fabricantes (1-2%)

Sin embargo a bajo nivel encontraremos que todos los métodos se basan en la monitorización y control de la red. Como la adquisición de la información es vital para la toma de desiciones, la monitorización adquiere principal importancia.

1.2.2 Monitorización

La monitorización es un conjunto de mecanismos que utilizamos para adquirir la información necesaria que nos permita luego tomar las decisiones adecuadas. Dada por lo tanto la importancia de la monitorización ampliaremos un poco más los aspectos involucrados en este tema. La monitorización se lleva acabo en 4 etapas:

- Definición de la información de gestión que se desea monitorizar.
- Acceso a la información de monitorización.
- Diseño de mecanismos de monitorización.
- Procesado de la información de monitorización.

Definición de la Información que vamos a Monitorizar: De acuerdo a su naturaleza, existen los siguientes tipos:

- **Información estática:** No cambia con la actividad de la red.
- **Información dinámica:** Evoluciona con la propia actividad de la red.
- **Información estadística:** Postprocesado de la información dinámica que proporciona un mayor significado de gestión

Hemos definido los tipos de información que se puede monitorizar, pero ¿Qué información vamos a Monitorizar?, la respuesta dependerá de la aplicación y de la red, por ejemplo:

- **Para gestión de prestaciones:** información estadística, generada a partir de información dinámica (tráfico, retardo, etc.)
- **Para gestión de fallos:** información dinámica (cambios de estados)
- **Para gestión de configuraciones:** información estática (inventario de la red)

Acceso a la Información Monitorizada: Es importante que tengamos acceso de forma eficiente a la información que estamos monitorizando; esto involucra en la mayoría de las veces el acceso remoto a la información monitorizada. Para esto es necesario lo siguiente:

- Un centro de control centralizado (NOC), que nos permita gestionar de forma centralizada los dispositivos distribuidos en la red.
- Cooperación entre los gestores y los equipos gestionados, los equipos deben poder ser gestionados, para esto se instala el software de gestión adecuado.
- Método común de acceso a la información de gestión, independientemente de la tecnología o fabricante del equipo monitorizado.
- Modelos de gestión de red integrada: proporcionan la interoperabilidad.

Diseño de Mecanismos de Monitorización: Los mecanismos de monitorización podemos dividirlos principalmente en:

- **Polling o Sondeo:** se refiere al acceso periódico a la información de gestión. Se hace un sondeo (o polling) a los objetos administrados.
  Ventaja: Los objetos solo deben estar preparados para responder a los sondeos esto hace simplicidad.
  Desventaja: Aumenta el trafico de la red.

- **Event Reporting o notificaciones:** los propios objetos envían notificaciones bajo ciertas condiciones especificadas por le administrador.
  Ventaja: se minimiza el tráfico de gestión por la red.
  Desventaja: Mayor complejidad en el software instalado en los objetos gestionados.

Por lo tanto desde los puntos de vista anteriores podemos mencionar que hay dos formas de realizar la gestión:

- Descargar la complejidad hacia los gestores. Lo que implica que la complejidad se centralice en las consolas de gestión.
- Balancear complejidad entre gestores y equipos gestionados. Lo que implica balancear la carga de gestión tanto en las consolas como en los objetos gestionados.

Procesado de la información de Monitorización: esto tiene que ver con que es lo que haremos con la información registrada y como la mostraremos para su análisis e interpretación. Esto involucra herramientas estadísticas que nos permitan visualizar la información recogida en gráficos, cuadros, etc.

Como se ha mencionado la adquisición de información y la forma de mostrarla al para una eficiente toma de decisiones es de vital importancia. Por este motivo es importante la selección de herramientas adecuadas, hardware y software, para la implementación de una plataforma de gestión, que se adecue a los requerimientos particulares de cada red y nos permita alcanzar los objetivos que nos planteamos en la etapa de planeamiento.

CAPITULO II
FUNDAMENTOS DE REDES DE DATOS

Este capitulo no pretende ser una guía completa acerca de las redes de computadoras, sino daremos una visión rápida de las tecnologías involucradas en el desarrollo de este informe. Haremos énfasis en la arquitectura TCP/IP, por ser la suite de protocolos mas importante y de uso mas extendido.

2.1 Clasificación de las Redes.-

Una rápida visión a las redes de datos nos obliga a comenzar por su clasificación, Iniciaremos la clasificación por su cobertura geográfica. Es decir por el área geográfica que estas redes pueden abarcar las clasificamos en:

Redes LAN, son redes de Área Local, su cobertura puede ser una oficina, edificio o campus. Ver Fig. 2.1

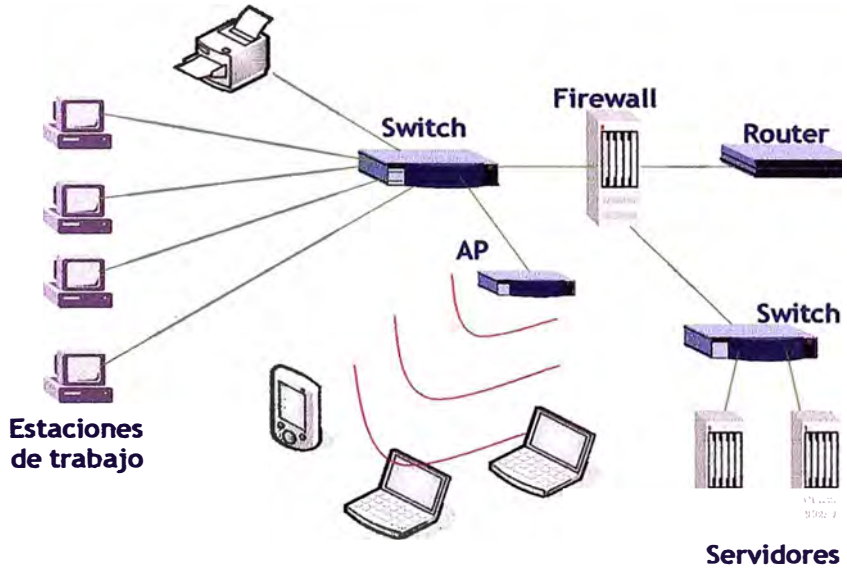


Fig. 2.1 Red LAN

Aquí Ethernet es quien predomina, utiliza el broadcast para enviar la información, alcanza 10, 100 y 1000 Mbps. de velocidad de transmisión cubriendo distancias de hasta 100 mts. sin necesidad de equipos repetidores.
Además de las redes cableadas también tenemos un estándar inalámbrico WI-FI, a través de APs (Access Points) podemos comunicarnos inalambricamente con estaciones de trabajo conformando lo que conocemos como WLAN (Wireless LAN), una LAN inalámbrica. En la WLAN alcanzamos velocidad de hasta 54 Mbps (según el estándar) y distancias de hasta 100mts. en interiores.

En las redes LAN podemos distinguir diferentes topologías, llamamos topología a la forma como están interconectadas físicamente las computadoras y otros dispositivos de red. Las topologías que observamos en las redes LAN pueden ser:

Topología Bus: Los dispositivos son conectados a través de un bus de datos.
Ver Fig. 2.2

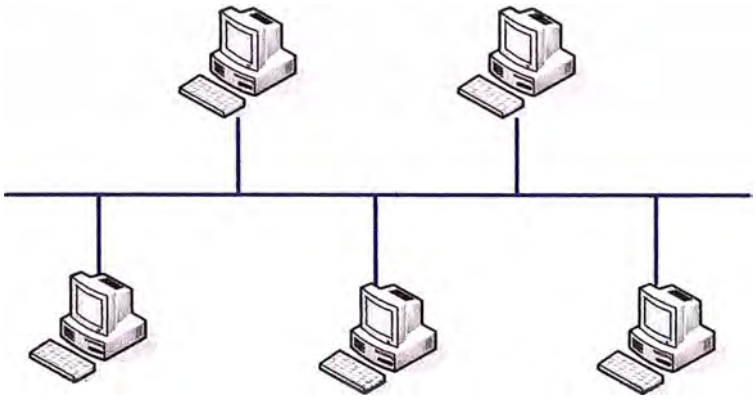


Fig. 2.2 Topología BUS

Esta era la topología de nuestras redes Ethernet antiguas cuando usaban cable coaxial como medio de transmisión.

Topología Anillo: Los dispositivos son conectados formando un anillo.
En esta topología encontramos como método de acceso al medio a Token Ring propuesto por IBM.
Ver Fig. 2.3

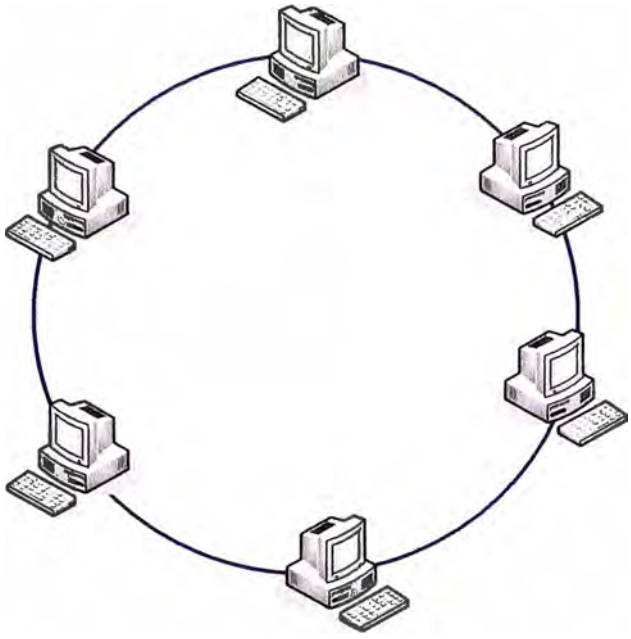


Fig. 2.3 Topología Anillo

Topología Estrella: Los dispositivos son conectados a un dispositivo central quien se encarga de la interconexión. Ver Fig 2.4

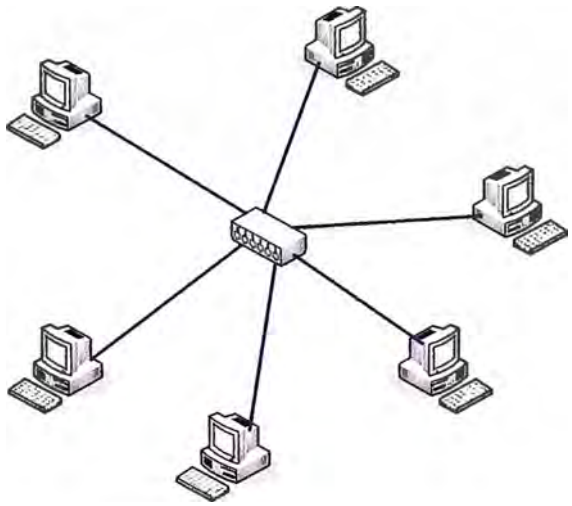


Fig. 2.4 Topología Estrella

En las redes **LAN** esta mas extendido el uso de la topología en estrella. Y el uso de Ethernet como estándar de transmisión.

Redes MAN, son redes de Área Metropolitana, su cobertura alcanza una ciudad. Un ejemplo de red MAN son las redes de televisión por cable.

Redes WAN, son redes de Área Amplia, su cobertura abarca ciudades, países o continentes. Una red WAN une redes LAN y otras redes WAN. Ver Fig. 2.5

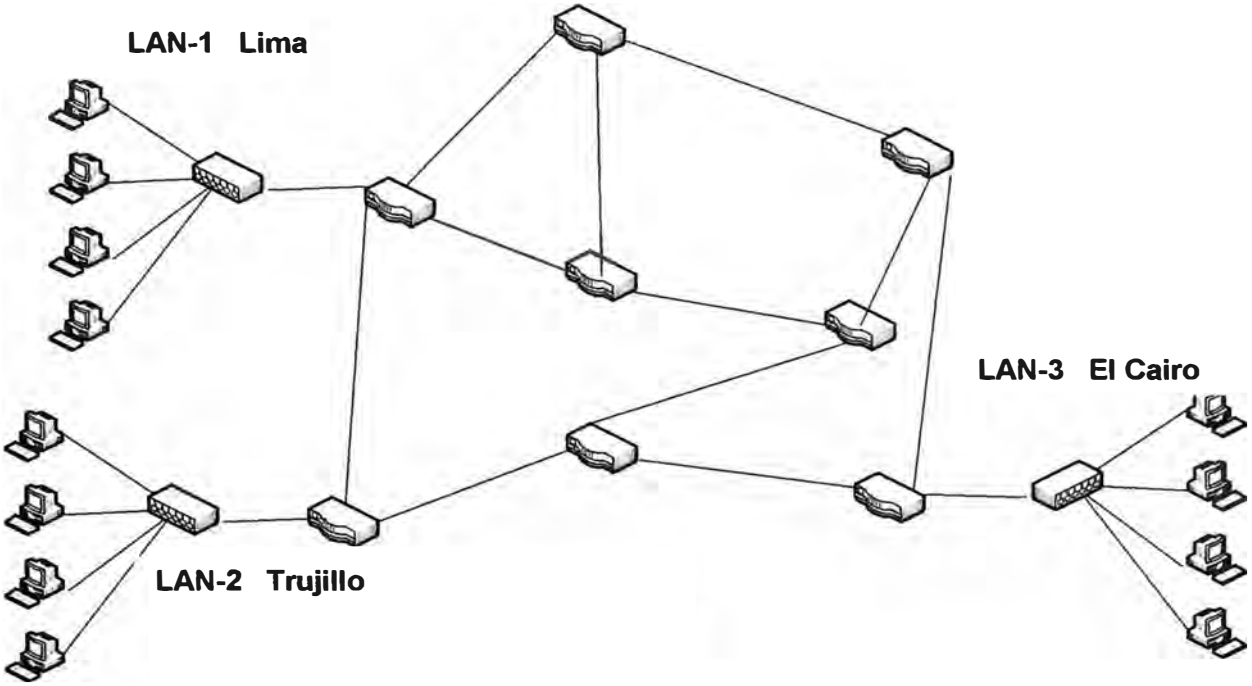


Fig. 2.5 Red WAN

Las redes WAN presentan topologías variadas siendo algunas de ellas:

Topología en Árbol: ver Fig 2.6

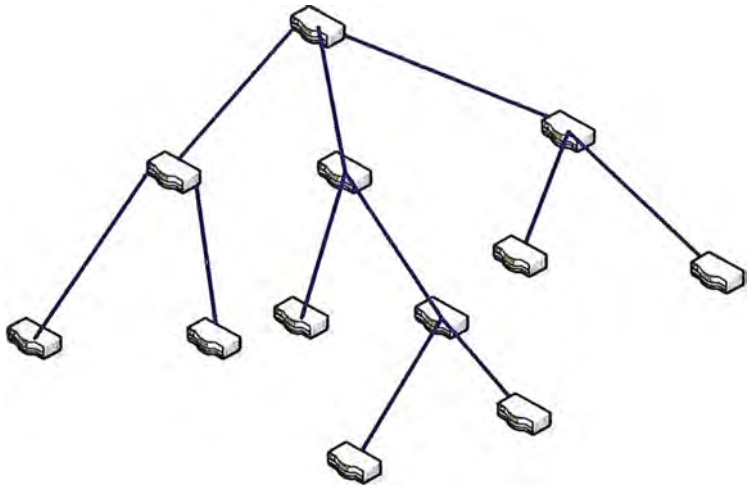


Fig. 2.6 Topología en Árbol

Topología en Anillo: ver Fig. 2.7

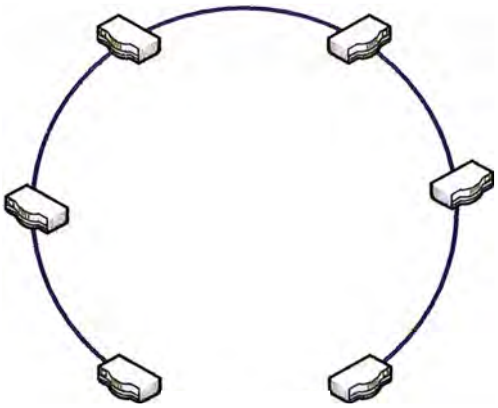


Fig. 2.7 Topología en anillo

Topología en malla: ver Fig. 2.8

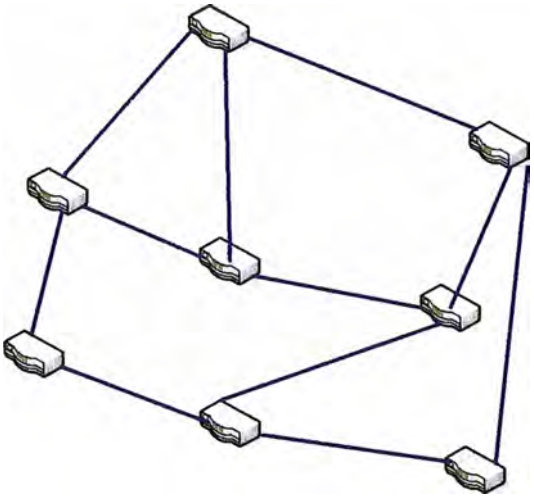


Fig. 2.8 Topología en malla

Aquí predominan las tecnologías punto a punto en vez del broadcast y podemos encontrar a: X25, ATM, Frame Relay, MPLS, etc.

Redes PAN, son redes de Área Personal, su cobertura abarca todos dispositivos que pueden ser manejados por una sola persona como, PCs, LapTops, Celulares, PDAs teclados, impresoras, audífonos, etc. Por lo general son redes inalámbricas y el estándar mas utilizado para interconectar estos dispositivos es BlueTooth.

Estas redes se están haciendo cada vez mas comunes en nuestro medio siendo. Pero no serán tema de estudio en este informe. Ver Fig. 2.9

Fig. 2.9 Red PAN

2.2 Arquitectura TCP/IP.-

Las redes de datos además de tener una topología tienen una arquitectura, la arquitectura a diferencia de la topología no describe como se conectaran físicamente los dispositivos entre sí; más bien define como se organizan en capas los protocolos de comunicación para interconectar los dispositivos.

En el caso de TCP/IP tenemos una suite de protocolos organizada en 4 capas (a diferencia de OSI que tiene 7 capas). Cada una de ellas implementa varios protocolos que hacen posible la comunicación siendo entre ellos el protocolo IP (Internet Protocol) quien mantiene toda la arquitectura unida.

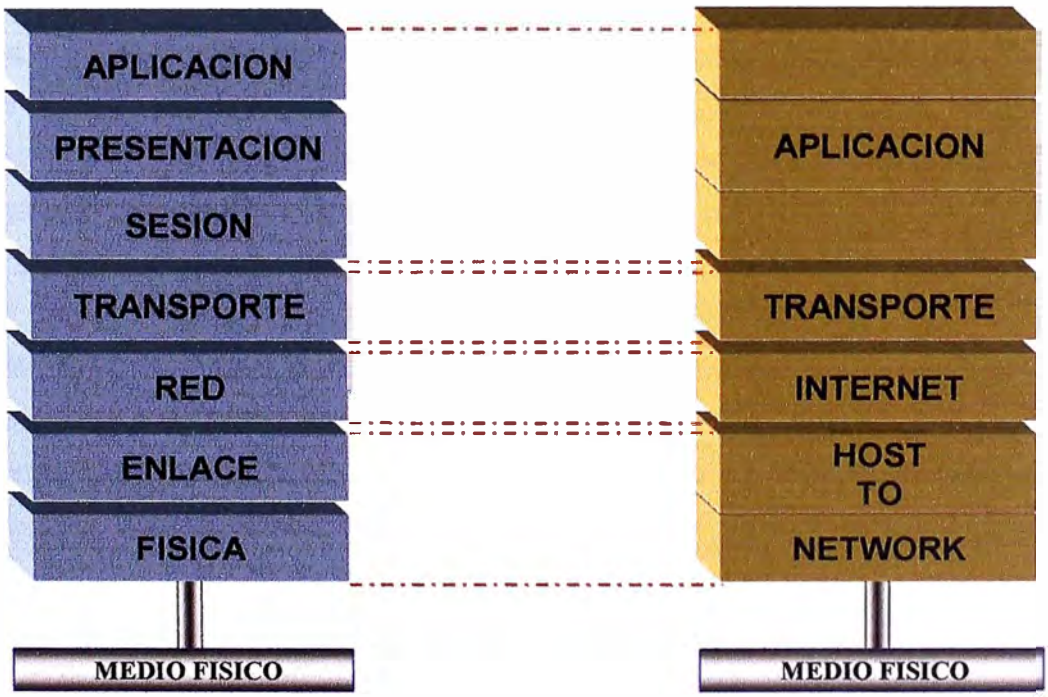


Fig. 2.10 Capas del modelo OSI y del modelo TCP/IP

En la Fig. 2.10 podemos ver una equivalencia entre las capas de TCP/IP con las del modelo OSI.

A continuación analizaremos cada una de las capas de esta arquitectura.

2.2.1 Capa de HOST A RED.- (Acceso a la Red)

Esta capa corresponde a los niveles OSI Físico y de enlace. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host. Es decir de coloca los paquetes TCP/IP en la red, ya sean en enlaces punto a punto o a través de broadcast.
En esta capa TCP/IP no define protocolos específicos, mas bien deja libre el uso de protocolos que le permitan conectarse a la red. Esto le da la ventaja que los protocolos TCP/IP puedan viajar encapsulados en diferentes protocolos de enlace como:

- Ethernet → redes LAN.
- Token Ring, Token Bus → LAN
- ATM → redes WAN
- Frame Relay → redes WAN
- PPP, SLIP, FDDI, etc. → WAN

2.2.2 Capa de INTERRED.- (INTERNET)

Esta capa implementa la capa de RED el modelo OSI. Esta capa es responsable de las funciones de direccionamiento, empaque y enrutamiento de la información entregada por las capas superiores. Aquí podemos encontrar diversos protocolos, siendo el más importante el protocolo IP (Internet Protocol) encargado de cumplir las principales tareas de esta capa.

Protocolo IP, es un protocolo enrutable, sin conexiones responsable del direccionamiento IP y de la fragmentación y ensamble de los paquetes.
El direccionamiento es realizado a través de direcciones lógicas de red que conocemos como direcciones IP o números IP. Este protocolo hace uso de estas direcciones para dirigir los paquetes a través de las redes. Además cumple funciones de fragmentación de paquetes, en caso que nuestros paquetes necesiten cruzar a través de redes que tengan predeterminado un tamaño de paquetes más pequeño que el paquete que desea ingresar a esa red.

Aquí también aplicaremos calidad de servicio a la información que estamos tratando de transmitir. Esto es importante en el momento de querer distinguir el tipo de tráfico que estamos direccionando.

La cabecera del protocolo IP consta de 20 Bytes como observamos en la Fig 2.11

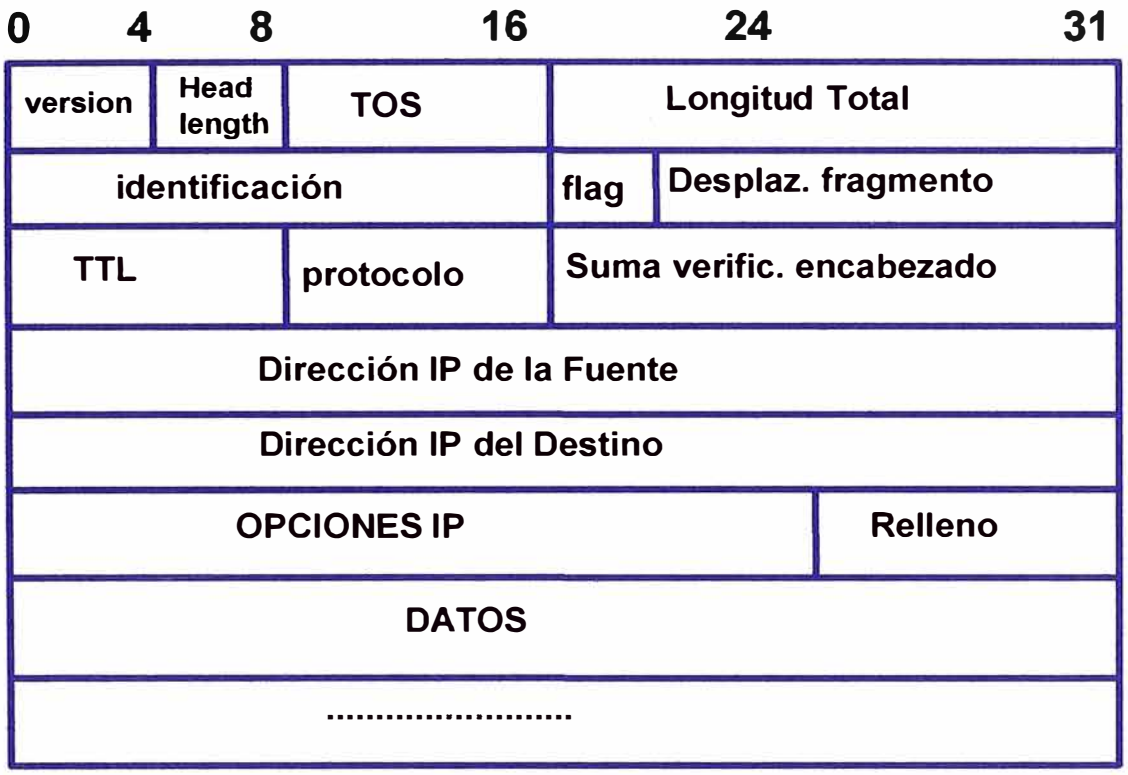


Fig. 2.11 Cabecera del protocolo IP

Este es el protocolo más representativo de la capa de Interred. Pero trabaja acompañado de otros protocolos que mencionamos a continuación:

Protocolo ICMP, (Internet Control Message Protocol) es el protocolo que envía los mensajes de control en la capa de interred. Como el protocolo IP es sin conexiones, ICMP proporciona funciones de diagnóstico y de reporte de errores o de condiciones referentes a la entrega de los paquetes IP.
Un ejemplo del uso de ICMP es el comando Ping quien utiliza mensajes ICMP para pedir respuesta de otros dispositivos conectados en la red.

Protocolo ARP, (Address Resolution Protocol) es responsable de la conversión de las direcciones de la capa de Internet a las direcciones de la capa de la host a red, tales como las direcciones MAC.

El protocolo ARP es utilizado en las redes LAN; cada vez que un Host intenta comunicarse con otro, una vez que ha comprobado que esta dentro de su misma red, envía una petición ARP (ARP request) hacia todas las maquinas. El dispositivo dueño de la dirección IP destino responderá con su respectiva dirección MAC, luego esta dirección MAC se guarda en una memoria en el dispositivo (**Ejm:** Tarjetas de RED) para no llenar la red de tráfico ARP.

En esta capa también encontramos otros protocolos conocidos como protocolos de enrutamiento, que se encargan de buscar y establecer las diferentes rutas entre las redes utilizando al protocolo IP. No es tema de este informa ahondar en ellos por lo que solo los mencionaremos: RIP, OSPF, BGP, EGP, etc.

2.2.3 Capa de TRANSPORTE.-

Esta capa implementa la capa de transporte del modelo OSI. Es responsable de establecer comunicaciones de extremo a extremo, proporcionando los servicios de sesión y datagramas. Para entregar estos servicios de extremo a extremo y manejar sesiones independientes a través de la misma dirección IP (proporcionada por la capa de red) establece el uso de puertos.

Un puerto es un numero que identificara cada dialogo establecido en cada extremo de la comunicación. Hay puertos que son bien conocidos e identifican a ciertas aplicaciones en particular. Ejm: La aplicación de Terminal virtual TELNET utiliza el puerto 23 para comunicarse.
Para establecer estas conexiones extremo a extremo la capa de transporte ofrece dos tipos de servicio, un servicio Orientado a la Conexión y un servicio No Orientado a la Conexión, a través de dos protocolos:

Protocolo TCP, (Transfer Control Protocol) un protocolo orientado a la conexión, confiable, que asegura la entrega de información extremo a extremo. Se encarga por lo tanto de establecer una conexión, secuenciar y controlar la entrega de paquetes, verificar y retransmitir los paquetes perdidos o que presenten errores, cerrar la conexión.
Esto hace que TCP sea un protocolo confiable pero que introduce retardo en la transmisión de información.

La cabecera de este protocolo consta de 20 Bytes e incluye una variedad de campos que le permiten implementar estos mecanismos de control. El tamaño de esta cabecera causa

además retardos en el procesamiento de los paquetes, al tener cada dispositivo que leer los diversos campos que contiene.

Ver Fig 2.12

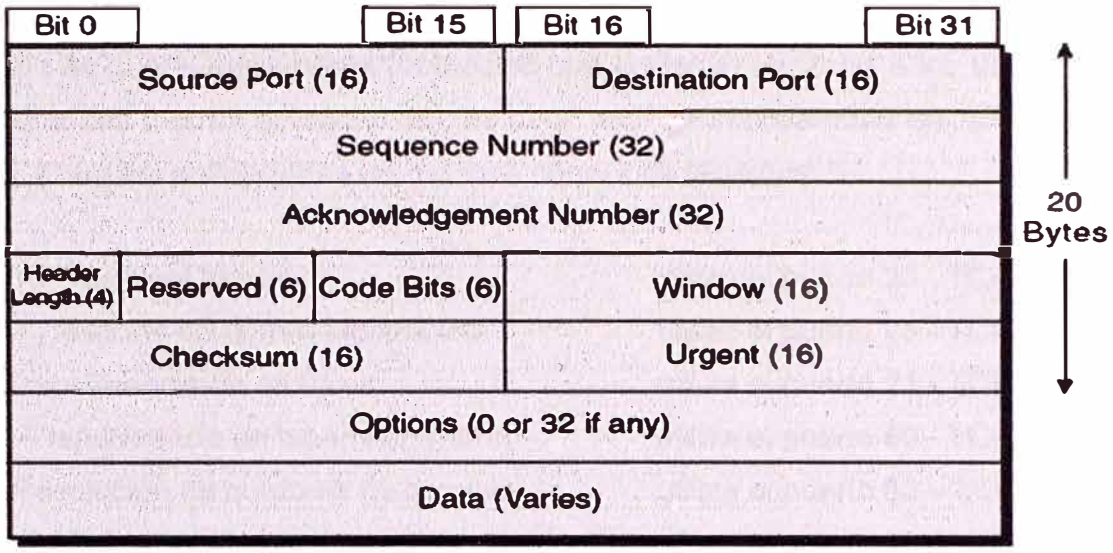


Fig. 2.12 Cabecera del protocolo TCP

Protocolo UDP, (User Datagram Protocol) un protocolo no orientado a la conexión, por lo tanto aquí no contamos con mecanismos, que nos permitan establecer conexiones, secuenciar y controlar envió de paquetes, etc.

Al ser un protocolo sin conexiones UDP es un protocolo no confiable, pero introduce menos retardo que TCP. Como observamos la cabecera de UDP solo consta de 8 bytes.

Ver Fig 2.13

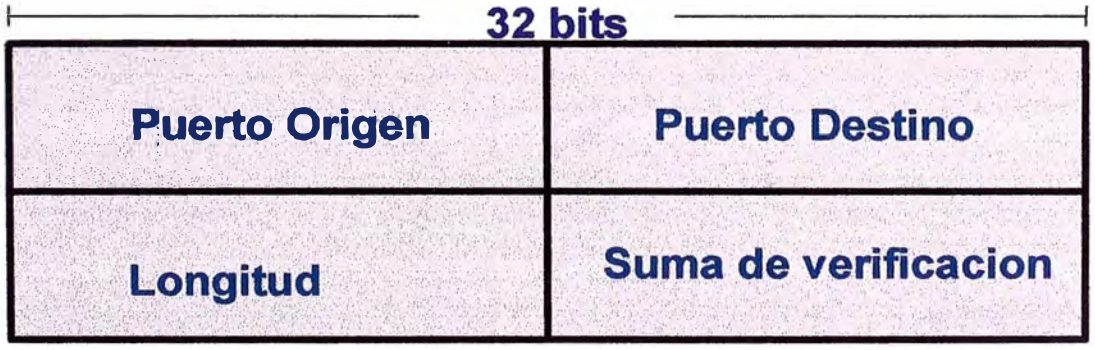


Fig. 2.13 Cabecera del protocolo UDP

Este protocolo es utilizado cuando:

Nuestra transmisión tiene como prioridad la velocidad antes que la confiabilidad. **Ejm**: transmisiones de voz y video en tiempo real.

La cantidad de datos a ser transferidos es pequeña. **Ejm:** la realización de consultas coma las del protocolo DNS.

Cuando la confiabilidad en la entrega es proporcionada por protocolos en capas superiores.

2.2.4 Capa de APLICACION.-

Esta capa es la que implementa protocolos que entregan servicios a los usuarios finales (sean personas u otras aplicaciones), es decir aquí se implementan las APLICACIONES de RED. Entre las aplicaciones de red mas conocidas tenemos:

TELNET – Terminal Virtual	utiliza el puerto 23 - TCP
SMTP – Trasporte de correo electrónico	utiliza el puerto 25 - TCP
FTP – Transferencia de archivos	utiliza el puerto 21 - TCP
HTTP – Transferencia de hipertexto (html)	utiliza el puerto 80 - TCP
DNS – Resolución de nombres de dominio	utiliza el puerto 53 – UDP
TFTP – Transferencia de archivos	utiliza el puerto 69 – UDP
SNMP – Administración de red	utiliza el puerto 161- UDP

Como observamos el protocolo SNMP que nos permite administrar dispositivos en la red es parte de la capa de aplicación de la suite de protocolos TCP/IP y utiliza UDP como protocolo de transporte. Este es el protocolo tema de este informe y será analizado con mayor detalle en capítulos posteriores.

La Fig. 2.14 nos muestra un resumen de la arquitectura TCP/IP

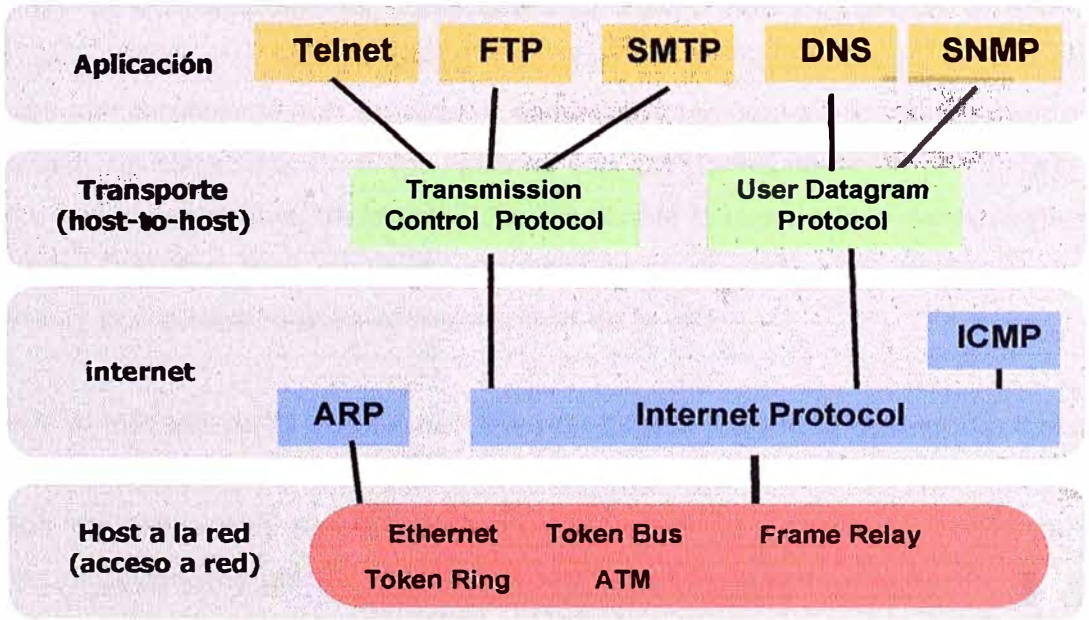


Fig. 2.14 arquitectura TCP/IP

2.3 Dispositivos de Red.-

Los dispositivos de red son piezas de hardware que cumplen diversas funciones en una red de acuerdo a que capas del modelo OSI sean implementadas. Estos dispositivos se distribuyen en la red y se encargan de llevar y procesar la información en la red, de su correcto funcionamiento depende que la red sea confiable, segura y tenga un buen desempeño. Estos son los dispositivos que vamos a administrar y de acuerdo a su ubicación y función en la red será mas critica su administración o no.

Mencionaremos los principales dispositivos en una red y sus principales características. Ya que estos serán los dispositivos que luego administraremos con el protocolo SNMP.

2.3.1 Hub.-

Son dispositivos que se encargan de interconectar otros dispositivos en la red como estaciones de trabajo y servidores. Poseen puertos donde conectamos cada dispositivo que deseamos interconectar. Podemos tener hubs de 5, 8, 16, 24, 48 puertos. Lo que nos dice cuantos dispositivos podemos interconectar.

Los hubs operan en la capa 1 del modelo OSI, es decir solo se ocupa de la parte física y no ve protocolos de capas superiores. Por este motivo el hub solo copia la data que recibe por un puerto a todos los puertos activos que tenga presente.

El hub mantiene a los dispositivos interconectados dentro del mismo dominio de colisiones. Si dos dispositivos conectados al mismo hub transmiten al mismo tiempo ocurre una colisión y los paquetes transmitidos se distorsionan, convirtiéndose en paquetes con errores, el hub en vez de eliminarlos los copia a todos los puertos y todos los dispositivos conectados a él los reciben. Las colisiones aumentarán cuando aumente el tráfico entre dispositivos de la red. Esto causa por lo tanto que el rendimiento de la red disminuya. Cuantos mas equipos conectemos a un hub aumentara el dominio de colisiones y por lo tanto bajara el desempeño de la red.

Los hubs al trabajar en la capa 1 de OSI, no realizan ningún tipo de comprobación en la estructura de paquetes permitiendo el paso de paquetes con errores. No permiten la conexión de redes que tengan diferentes métodos de acceso al medio, es decir no pueden unir redes que utilicen CSAM/CD con Token Ring por ejemplo.

Divide el ancho de banda total de la red entre la cantidad de sus puertos activos.

Por estas características los hubs ya no son utilizados como equipos principales de conectividad en la red, en su reemplazo ahora utilizamos switches, de los cuales hablaremos mas adelante.

Aun así los hubs pueden ser útiles en otras situaciones: cuando queremos conectar servidores en cluster y queremos enviar el "Heart Beat", o cuando deseamos capturar los paquetes que van a un determinado puerto de un switch donde ya tenemos un dispositivo conectado.

2.3.2 Bridge.-

Al igual que un hub el bridge une segmentos de red. Sin embargo puede dividir una red para aislar los problemas de tráfico ocasionados por las colisiones y realizar un tráfico de paquetes, más inteligente. El bridge trabaja hasta la capa 2 del modelo OSI.

Ver Fig 2.15

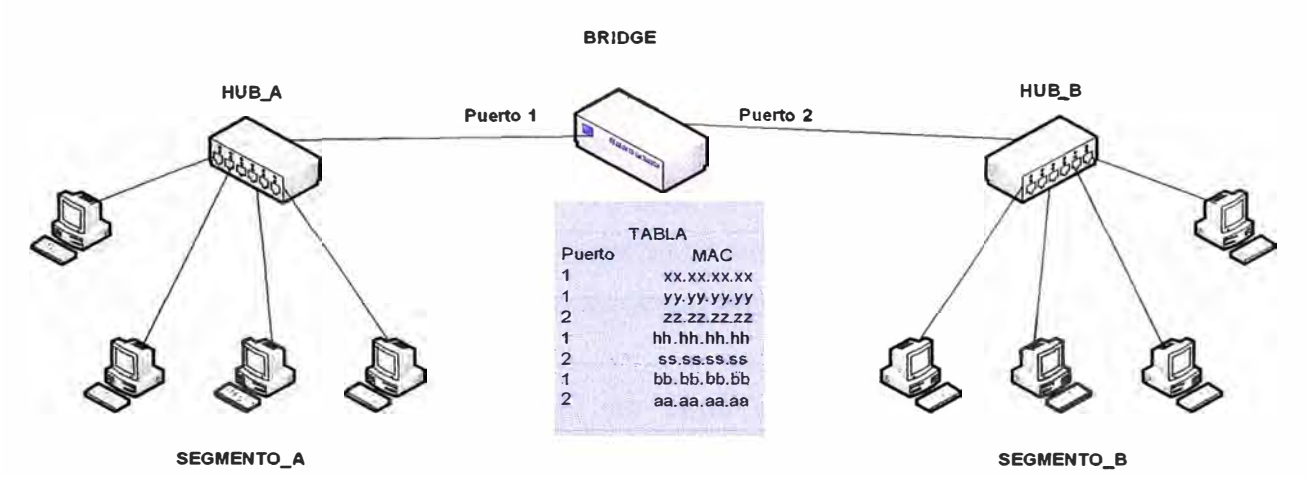


Fig 2.15 Uso de un Bridge

Une dos segmentos de red, pero separa las colisiones de cada segmento. Como el bridge funciona hasta capa 2 trabaja leyendo las direcciones MAC, escucha todo el trafico que recibe en cada puerto, escucha las direcciones MAC de los paquetes que recibe y las almacenas en una tabla relacionando cada MAC de acuerdo a que puerto del bridge este conectado. Cuando recibe un paquete lee la dirección MAC destino, si la MAC se encuentra en el mismo segmento donde recibió el paquete, el bridge elimina el paquete y no lo pasa al otro segmento. Si al leer el paquete la MAC destino se encuentra en otro segmento, el bridge saca el paquete por el otro puerto. SI no encuentra la MAC registrada en su tabla repite el paquete por todos sus puertos.

Los bridges además nos permiten interconectar segmentos que tengan diferentes métodos de acceso al medio como por ejemplo conectar un segmento que use CSM/CD (Ethernet) con otro segmento Token Ring. Ver fi

2.3.3 Switch.-

Son dispositivos que se encargan de interconectar otros dispositivos en la red, al igual que los hubs, como segmentos de red, estaciones de trabajo y servidores. Y al igual que los hubs también poseen puertos para conectar cada dispositivo de que deseamos interconectar. El numero de puertos también varia desde 5, 8, 16, 24, etc.

Los switches operan hasta la capa 2 del modelo OSI y examinan las direcciones de capa 2 para conmutar los datos entre sus puertos activos. En el caso de redes Ethernet los switches leen las direcciones MAC. Algunos switches además proveen funciones adicionales como la creación de VLANS por ejemplo e incluso de conmutación en capa 3 del modelo OSI.

Cuando los switches reciben un paquete por uno de sus puertos leen la dirección MAC de destino y envían el paquete al puerto donde se encuentra el dispositivo destino en vez de copiar el paquete a todos los puertos. De esta forma la información no pasa por toda la red lo que reduce considerablemente la carga de tráfico en la red. Esto permite aumentar el rendimiento de la red separando los dominios de colisiones.

El switch aprende la dirección MAC de cada dispositivo conectado a un puerto, almacenando esta información en una tabla que relaciona cada puerto con direcciones MAC. Para conocer las direcciones MAC de los dispositivos conectados en cada puerto el switch inunda la red con paquetes preguntando a cada puerto por las direcciones MAC (Flooding).

Los switches entre otras características que pueden poseer, permiten la creación de VLANS (LANs Virtuales), estas consisten en agrupar (utilizando software de administración) dispositivos en redes Virtuales sin importar si están en la mismo switch o en switches diferentes. De esta forma segmentamos el broadcast, ya que será propagado solo entre los miembros de una misma red Virtual.

Las ventajas que presenta un switch frente a un hub son obvias, permitiendo mantener el rendimiento de la red, al separar los dominios de colisión y mantener el ancho de banda por puerto.

Con la baja de precios de los switches las redes LAN actuales han dejado de usar hubs, reemplazándolos enteramente por switches, llevando el nombre de redes LAN conmutadas.

2.3.4 Routers.-

Los routers o ruteadores operan hasta la capa 3 del modelo OSI, su función es rutear el tráfico basándose en las direcciones IP de los paquetes que reciben, ubicando las redes destino. Nos permiten interconectar LAN con LAN, LAN con WAN y WAN con WAN.

Para esto el router dispone de diferentes interfases:

Interfases LAN: para la conexión con redes LAN, pueden ser Ethernet, Fast Ethernet, etc.

Interfases WAN: para la conexión de redes WAN estas pueden ser ISDN, Frame Relay, xDSL, etc.

Puerto de consola: para la configuración de los dispositivos.

Los routers trabajan utilizando tablas de ruteo, en las cuales se almacenan las direcciones hacia las redes conocidas, los posibles caminos entre routers, etc. Estas tablas pueden ser:

Estáticas: Son tablas creadas manualmente por el administrador de la red. Tienen que ser actualizadas manualmente cada vez que se produzca un cambio en la red. Estas rutas no son conocidas por otros routers.

Dinámicas: Son tablas obtenidas de otros routers en forma automática, las actualizaciones se hacen en todos los routers automáticamente cuando hay cambios en la red. Las rutas son públicas debido a que son conocidas por todos los routers de la red. Para su creación se utilizan protocolos de ruteo.

Cuando un paquete llega al ruteador, este lee la cabecera de red y busca la dirección destino. Luego busca esta dirección en sus tablas de ruteo, si la encuentra en su tabla selecciona la mejor ruta y envía el paquete al siguiente router. Si no encuentra la dirección en su tabla envía el paquete a una ruta por defecto (default router), en caso que no exista el router por defecto, el paquete es eliminado.

Uno de los usos de los ruteadores es conectarnos a Internet, a estos ruteadores los conocemos como ruteadores de borde o de frontera.

2.3.5 Access Points.- (APs)

Un Access Point (punto de acceso) opera en la capa 2 del modelo OSI, es un dispositivo que se encarga de interconectar las LAN inalámbricas y las LAN cableadas (Ver Fig. 2.16). Cuenta con una interfase ethernet y una (o más) antenas que permiten la conexión de otros dispositivos inalámbricos que soporten el estándar 802.11x como PCs, Laptops, Pdas, etc.

Como método de acceso al medio utilizan una variación de CSMA/CD (usado en Ethernet) llamada CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance). Esto le permite prevenir las colisiones cuando varias estaciones intentan comunicarse al mismo tiempo.

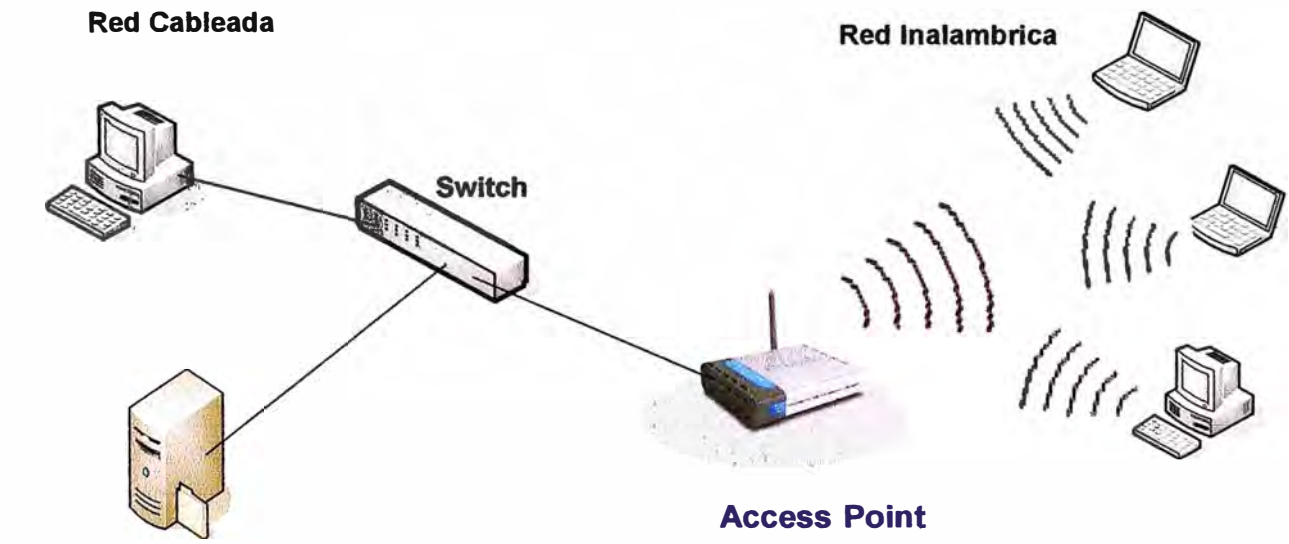


Fig. 2.16 Red Inalámbrica

Los APs (Ver Fig. 2.17) nos permiten agregar movilidad a las redes y el despliegue de equipos es mas fácil al no tener que realizar cableado incómodos. Y son excelentes cuando deseamos implementar estaciones de trabajo en exteriores o que se encuentran dispersas.

Las velocidades alcanzadas son menores que las redes LAN cableadas, según el estándar 802.11g alcanzamos hasta 54 Mbps. Esto hace que su uso no sea

recomendable durante la implementación de soluciones que requieran elevados anchos de banda.

Fig. 2.17 Access Point

Hemos finalizado esta breve explicación sobre algunas tecnologías fundamentales en las redes de datos como marco para iniciar la explicación del protocolo SNMP utilizado en la administración de redes.

CAPITULO III
PROTOCOLOS DE ADMINISTRACION DE REDES

3.1 Introducción

La mayoría de las arquitecturas de administración de redes, utilizan la misma estructura básica y conjunto de relaciones.

- **Estaciones finales (dispositivos administrados),** tales como computadoras y otros dispositivos en la red, corriendo software que les permite enviar alertas cuando por ejemplo detectan problemas (Cuando se ha excedido alguno de los parámetros de referencia establecido).

- **Entidades administradoras,** quienes reciben estas alertas y están programadas para reaccionar ejecutando una o un grupo de acciones. Estas pueden ser desde notificación al operador, log de eventos, apagado del sistema y reparaciones automáticas. Las entidades administradoras además también pueden hacer un polling a las estaciones finales para monitorear valores de ciertas variables. establecidas. El polling también puede ser automático o manual iniciado por le usuario, los agentes en las estaciones finales responderán a cualquiera de estos requerimiento s de información.

- **Los agentes**, son módulos de software que primero compilan información sobre el dispositivo administrado en el cual residen. Luego almacenan esta información en una base de datos de administración; y finalmente la proveen (proactiva o reactivamente) a las entidades administradoras a través de la red utilizando un Sistemas de administración de red (Network Management Systems – NMS's) vía un protocolo de administración de red.

- **Protocolos de administración de redes,** son los encargados de manejar el intercambio de información entre dispositivos administrados, entre ellos se incluyen al Protocolo Simple de administración de Red (Simple Network

Management Protocol – SNMP) y al Protocolo Común de administración de información (Common Management Information Protocol – CMIP)

- **Proxies de administración**, son entidades que proveen información de administración a favor de otras entidades que no utilicen el mismo protocolo.

En la Fig. 3.1 podemos observar como interactúan todos estos elementos.

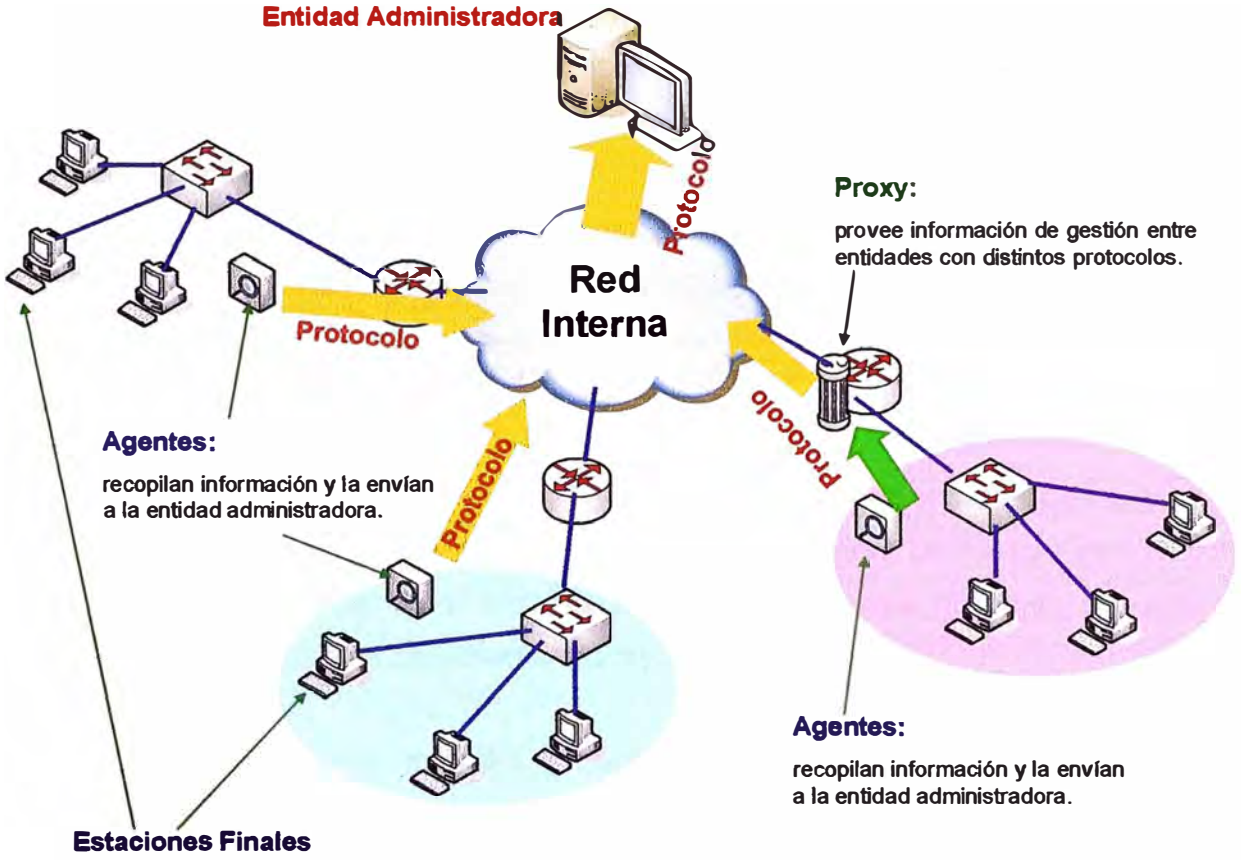


Fig. 3.1 Elementos de una red administrada

3.2 Modelo de Administración de Red de ISO

Este modelo es el primer paso para entender las funciones principales de los sistemas de administración de red. Consiste de 5 áreas conceptuales:

- Administración del desempeño.
- Administración de la configuración.

- Administración de cuentas.
- Administración de Fallas.
- Administración de Seguridad.

3.2.1 Administración del Desempeño: El objetivo es medir y poner a disposición diferentes aspectos del desempeño, de tal manera que podamos mantener este desempeño en un nivel aceptable. Entre las variables de desempeño que podemos observar están: tiempos de respuesta de los usuarios, tiempos de respuesta de la red, uso de los enlaces, etc.

Administrar el desempeño involucra tres pasos principales:

- Los datos de desempeño son recolectados en variables definidas por el administrador de la red.
- Los datos son analizados para determinar funcionamiento en niveles normales.
- Luego se determinan los valores referenciales apropiados por cada variable medida. Si estos valores de referencia son excedidos indicaría problemas en la red.

Las entidades Administradoras monitorean continuamente las variables de desempeño; cuando uno de los valores de referencia es excedido se genera un alerta y es enviada al sistema de administración de la red. Cada uno de los pasos descritos es parte del procedimiento para preparar un sistema reactivo.

También es posible utilizar métodos proactivos. Por ejemplo hacer simulaciones del funcionamiento de la red para proyectamos como el crecimiento de la red puede afectar el desempeño establecido. Estas simulaciones pueden prevenir a los administradores de posibles problemas de tal manera que tomen medidas anticipadas.

3.2.2 Administración de la Configuración: El objetivo es monitorear la configuración de la red y el sistema; de tal manera que los efectos, en la operación de la red, de las diferentes versiones de software y hardware puedan ser registrados y administrados adecuadamente.

Cada dispositivo en la red tiene información de versiones de software y hardware asociadas tales como:

- Versión del Sistema Operativo
- Versión de la interfase Ethernet
- Versión del software TCP/IP
- Versión del software NFS
- Versión del software SNMP

El sistema que administra la configuración de los dispositivos guarda esta información en una base de datos para que su acceso sea sencillo, y al presentarse un problema se pueda buscar en ella las pistas que nos lleven a resolver el problema.

3.2.3 Administración de Cuentas: El objetivo es medir parámetros de uso de la red. De esta manera se puede regular apropiadamente el uso de la red por parte de usuarios individuales o grupos de usuarios. Tal regulación puede minimizar problemas en la red, asignando los recursos de la red de acuerdo a las necesidades y las capacidades de esta.

También podemos distinguir tres pasos básicos para esta implementación:

- Medir el uso de todos los recursos importantes de la red.
- Analizar los resultados nos permite ver los patrones comunes de uso y así establecer las cuotas de uso adecuadas. Luego se irán haciendo correcciones hasta alcanzar el valor óptimo de uso.
- De este punto en adelante la medición del uso de recursos se empleara en la facturación así como en mantener constantemente el uso de la red en los valores óptimos.

3.2.4 Administración de Fallas: El objetivo es detectar, registrar, notificar y reparar automáticamente los problemas en la red para mantenerla funcionando con eficiencia. Como las fallas pueden causar una degradación de la red que haga inaceptable su desempeño, la administración de fallas es probablemente la forma de administración utilizada con mayor frecuencia.

Los pasos que distinguimos son los siguientes:

- Determinar síntomas y aislar el problema.
- Corregir el problema y probar la solución.
- Finalmente registrar la detección y la solución del problema.

3.2.5 Administración de Seguridad: El objetivo es controlar el acceso a los recursos de la red de acuerdo a políticas de tal manera que esta no pueda ser saboteada (intencionalmente o no) protegiendo la información más sensible para la empresa de accesos no apropiados.

Algunas de sus funciones son:

- Identificar recursos de la red como archivos, aplicaciones, etc.
- Mapear los recursos sensibles de la red con los usuarios autorizados.
- Registrar los accesos autorizados y no autorizados.

3.3 Protocolos de Administración de Redes

Como se menciono en capítulos anteriores que es indispensable la adquisición de información para la toma de decisiones; la tarea de los protocolos de gestión de redes es justamente esa, capturar información y permitir su intercambio entre los dispositivos administrados y los administradores. De estos protocolos depende que este intercambio sea rápido, confiable y eficiente sin sobrecargar de tráfico a la red administrada.

Aquí mencionamos los principales estándares utilizados en la gestión de las redes de hoy:

3.3.1 CMIP.- (Common Management Information Protocol)

CMIP es un protocolo de gestión de red que se implementa sobre el modelo de Interconexión de Redes Abiertas OSI que ha sido normalizado por la ISO. Tras la aparición de SNMP como protocolo de gestión de red, a finales de los 80, gobiernos y grandes corporaciones plantearon el Protocolo Común de Gestión de Información CMIP (Common Management Information Protocol). CMIP fue diseñado teniendo en cuenta a SNMP, ya que soluciona todos sus errores y fallos volviéndose un gestor de red mayor y más detallado.

Según el modelo OSI el CMIP es un protocolo de gerencia definida. Esto quiere decir que CMIP especifica como va a ser realizado el cambio de información entre el administrador y el agente en el Sistema de Gerencia.

En efecto, los procesos de aplicación llamados administradores residen en las estaciones de gestión mientras que los procesos de aplicación llamados agentes residen en los

elementos de red. CMIP define una relación igual a igual entre el administrador y el agente incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de gestión. Las operaciones CMIS (Common Management Information Services) se pueden originar tanto en gestores como en agentes, permitiendo relaciones simétricas o asimétricas entre los procesos de gestión. Sin embargo, la mayor parte de los dispositivos contienen las aplicaciones que sólo le permiten hacer de agente.

El CMISE (Common Management Information Service Element) proporciona a CMIP los servicios básicos de gestión confirmados y no confirmados para reportar eventos y manipular datos de gestión; utiliza dos aplicaciones de servicio comunes (Son aplicaciones de servicio común aquellas aplicaciones que ofrecen servicios no solo de aplicaciones de gestión, así como todas las otras.), ACSE y ROSE. La primera trata del establecimiento y liberación de conexiones entre un equipamiento y otro. La segunda ofrece servicios de pedido de operaciones remotas.

3.3.2 SNMP.- (Simple Network Management Protocol)

Para el desarrollo de la gestión de redes en inter-redes (Internets) basadas en TCP/IP, el IAB (Internet Activities Board) decidió seguir una estrategia en la cual a corto plazo se usaba el Simple Network Management Protocol (SNMP) para gestionar los nodos, y se proponía para largo plazo la estructura de gestión de redes OSI. Se escribieron entonces dos documentos para definir la gestión de la información: RFC 1065 que definía la Estructura de la Información de Gestión (Structure of Management Information, SMI), y RFC 1066, que definía la Base de Información de Gestión (Management Information Base, MIB). Ambos documentos fueron diseñados para ser compatibles con la estructura SNMP y la de gestión de redes OSI.

El SNMP es usado para comunicar información de gestión entre las estaciones de gestión de red y los agentes en los elementos de red. Como primer objetivo minimiza explícitamente el número y complejidad de las funciones de gestión realizadas por el propio agente de gestión. Esta característica es importante por lo siguiente:

- El costo de desarrollo del software del agente de gestión necesario para soportar el protocolo se reduce acordemente.
- El grado de funciones de gestión soportado remotamente se incrementa, posibilitando un uso completo de los recursos de Internet en la tarea de gestión.
- El grado de funciones de gestión soportado remotamente se incrementa,

imponiendo así las mínimas restricciones posibles en la forma y sofisticación de herramientas de gestión.

- Los conjuntos simplificados de funciones de gestión son fácilmente entendibles y usados por los creadores de herramientas de gestión de red.

Un segundo objetivo del protocolo es que el paradigma funcional para monitorizar y controlar sea lo suficientemente flexible como para posibilitar aspectos de gestión y operación de la red adicionales y posiblemente no anticipados.
Un tercer propósito es que la arquitectura sea en lo posible independiente de la arquitectura y mecanismos de hosts o gateways particulares.

En la Fig. 3.2 vemos la distribución de los agentes SNMP y su interacción con la consola de administración.

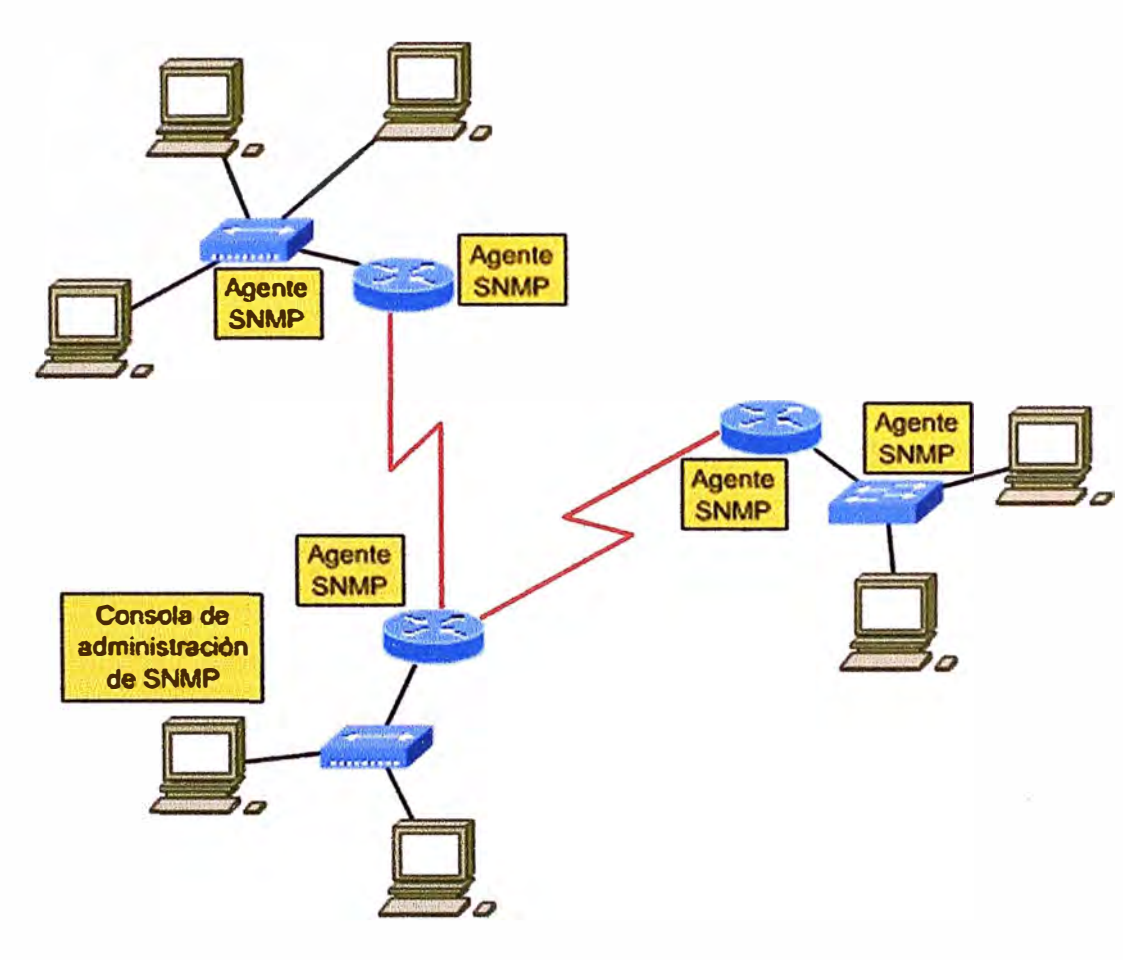


Fig. 3.2 Distribución de Agentes SNMP

3.3.3 TMN.- (Telecommunications Management Network)

La gestión de redes y servicios de telecomunicaciones se puede definir como el conjunto de procesos y actividades que realiza una operadora para ofrecer a sus clientes los servicios de telecomunicaciones, de tal forma que se cumplan tanto los criterios de calidad y coste establecidos en los objetivos de la empresa, como los reflejados en los correspondientes contratos con los clientes.

Las redes y servicios de telecomunicaciones surgen para cubrir la necesidad de comunicación entre varios puntos alejados geográficamente dentro de un área. Es por esto que la infraestructura necesaria para la prestación de estos servicios se debe desplegar a lo largo varios (cientos, miles...) kilómetros. Intentar realizar estas tareas de mantenimiento de forma manual se convierte por lo tanto en una tarea inviable sino se dispone de sistemas de gestión adecuados.

Para cubrir este requerimiento TMN proporciona funciones de gestión y comunicaciones para la operación, administración y mantenimiento de una red de telecomunicaciones y sus servicios en un entorno de múltiples fabricantes.

¿Por que usar la arquitectura TMN?

- Heterogeneidad en la tecnología de redes de telecomunicaciones: redes analógico-digitales
- Demandas sobre: posibilidad de introducir nuevos servicios, posibilidad de reorganizar las redes, métodos eficientes de trabajo para operar las redes y competencia entre empresas operadoras privadas.

El modelo TMN se basa en el modelo OSI para la interconexión de sistemas abiertos, que adopta el modelo gestor-agente, como se ha mencionado ya anteriormente, para las relaciones entre sistemas o entre sistemas y equipos. Hay tres aspectos que considera para la conexión de sistemas:

- **Funcional.** Define las actividades que hay que realizar y la organización de las mismas. El modelo funcional representa el contexto de una comunicación, ya que un término puede tener diferentes significados según donde se utilice.

- **De información.** Modela la información de gestión que se intercambia entre el gestor y el agente. Este modelo depende de las funciones que se realicen y de los

recursos que se quieran gestionar. El modelo de información es la parte semántica de la comunicación, se encarga del significado de cada frase.

- **De comunicación.** Especifica los protocolos de comunicaciones utilizados para el intercambio de información entre sistemas. Su objetivo es permitir la transferencia e interpretación correcta de la información de gestión. El modelo de comunicación define la sintaxis de la comunicación, describiendo su forma.

En la Fig. 3.3 observamos la distribución de una red TMN

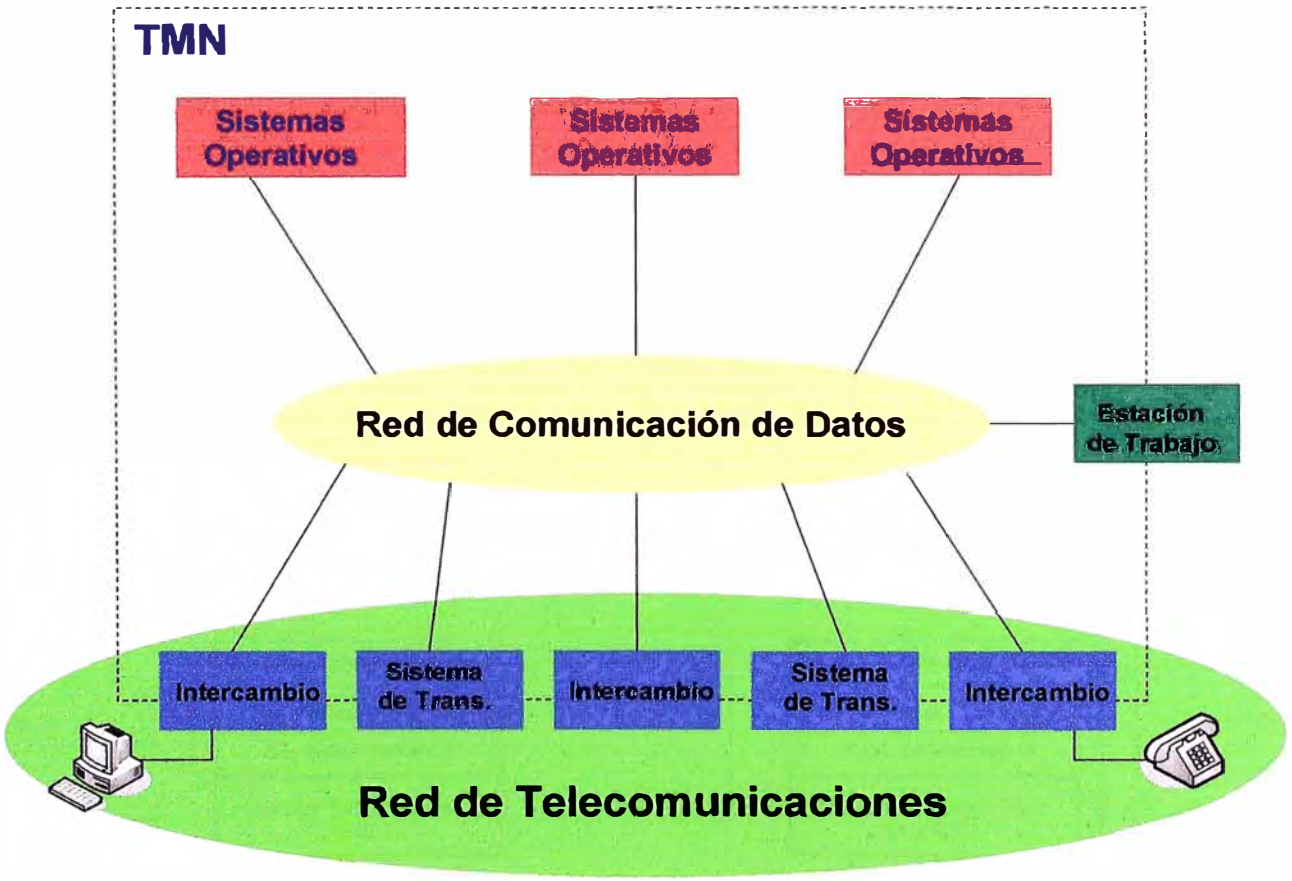


Fig. 3.3 Una red TMN

Hemos dado un vistazo rápido a los principales estándares para gestión de redes, el tema de este informe se enfocara en la gestión utilizando el estándar SNMP. Este estándar será estudiado con mayor profundidad en el siguiente capitulo.

CAPITULO IV
PROTOCOLO SNMP

4.1 El protocolo SNMP

El protocolo Simple Network Management Protocol (SNMP) permite gestionar redes TCP/IP. Fue aprobado por el IAB en 1988 y está basado en SGMP que permite manejar los routers en Internet. SNMP añadió las mejoras de muchos años de experiencia con SGMP y le permitió trabajar con los objetos definidos en el MIB con la representación del SIM.

SNMP trabaja en la capa de aplicación del modelo TCP/IP, utiliza los servicios del protocolo UDP de transporte a través del puerto 161. El uso del protocolo UDP hace que sea un protocolo más rápido y no aumente demasiado el tráfico en la red. En la Fig. 4.1 observamos donde se ubica SNMP dentro del modelo de capas TCP/IP

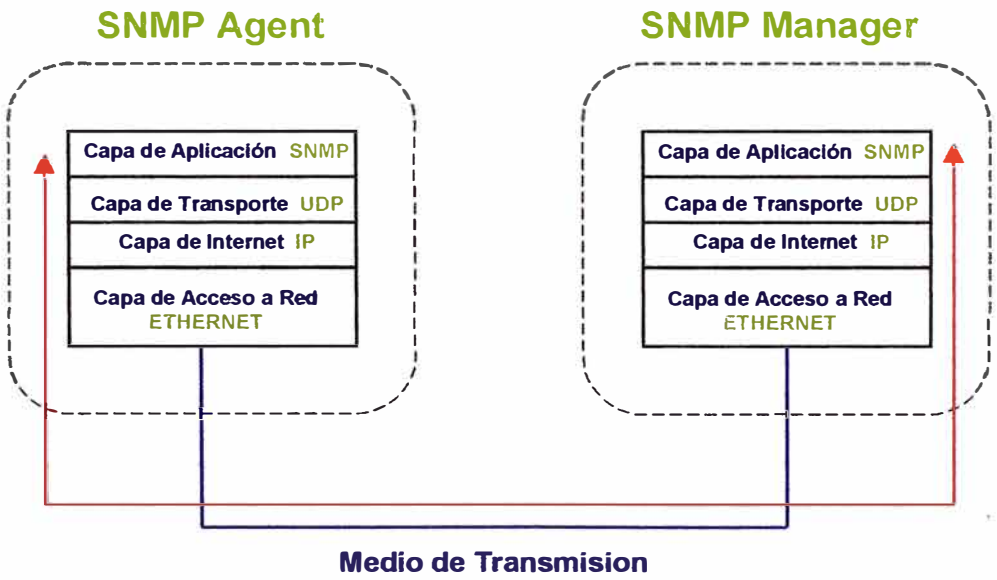


Fig. 4.1 SNMP y el modelo TCP/IP

SNMP también puede gestionar dispositivos no-SNMP utilizando agentes proxy. Un agente proxy es un conversor de protocolo que traduce las órdenes SNMP a las comprensibles por el protocolo de gestión propio del dispositivo. Actualmente SNMP está

soportado en muchos sistemas distintos tales como switches, PC's, estaciones de trabajo, routers, servidores, hubs, y tarjetas avanzadas ethernet, token ring y FDDI.

SNMP se basa en un modelo administrador/agente que consiste en un administrador, un agente una base de datos de información de administración, objetos administrados y un protocolo de red. El administrador provee la interfase entre el administrador humano en la red y el sistema de administración. El agente provee la interfase entre el administrador y el dispositivo físico administrado. SNMP se utiliza para la comunicación de información entre los administradores y los agentes. Ver Fig 4.2

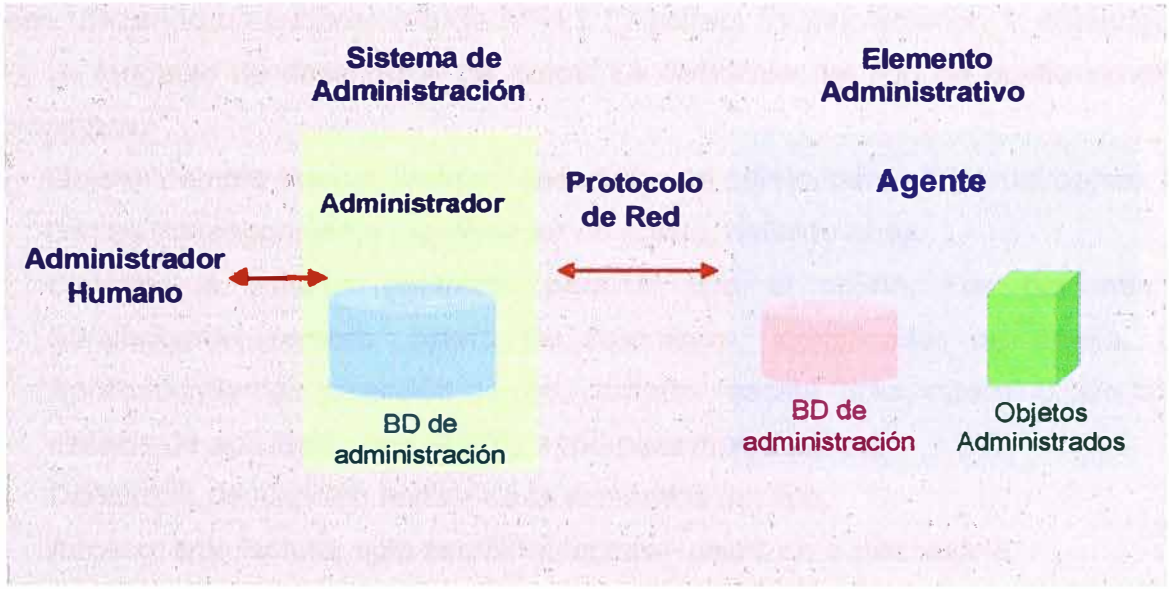


Fig. 4.2 Modelo administrador-agente de SNMP

Sus componentes son los siguientes:

- Gestores (NMS's)
- Agentes (nodos administrados)
- MIB (base de datos con información)
- SMI (administración de la base de datos)

NMS (Network Management Systems).- Un NMS es un software que ejecuta aplicaciones que monitorean, y controlan a los dispositivos administrados. Proveen la estructura del proceso de administración y los recursos necesarios para la administración en la red. Se instala en un dispositivo que actuara como estación de monitoreo. En una red pueden haber uno o mas NMS's de acuerdo a la implementación que se desee hacer.

Agentes (Nodos Administrados).- Son programas que residen en los dispositivos que vamos a administrar. Los agentes tienen el conocimiento local de la información de administración que recolectan de los dispositivos donde se alojan, la almacenan y traducen en un formato compatible con SNMP y la envían al NMS. Los agentes están distribuidos en toda la red administrada, en diferentes dispositivos: Pcs, Routers, Switches, etc.

4.2 SMI (Structure and Identification of Management Information)

El SMI define las reglas para describir los objetos gestionados y cómo los protocolos sometidos a la gestión pueden acceder a ellos. La descripción de los objetos gestionados se hace utilizando un subconjunto de ASN.1 ("Abstract Syntax Notation 1, estándar ISO 8824), un lenguaje de descripción de datos. La definición del tipo de objeto consta de cinco campos:

- Objeto: nombre textual, llamado *descriptor del objeto*, para el tipo del objeto, junto con su correspondiente *identificador de objeto*, definido abajo.
- Sintaxis: la sintaxis abstracta para el tipo el objeto. Las opciones son SimpleSyntax (entero, octeto de caracteres, identificador de objeto, Null), ApplicationSyntax (dirección de red, contador, escala, ticks, opaco) u otro tipo de sintaxis de aplicación (ver el RFC 1155 para más detalles).
- Definición: descripción textual de la semántica del tipo.
- Acceso: sólo lectura, sólo escritura, lectura - escritura o inaccesible.
- Status: obligatorio, opcional u obsoleto.

Como ejemplo, podemos tener el siguiente Objeto: (Ver Fig 4.3)

```
OBJECT
        sysDescr { system 1 }
Syntax  OCTECT STRING
Definition  Este valor debería incluir el nombre completo y la identificación
            de versión del tipo de hardware del sistema, sistema operativo, y
            software de red. Es obligatorio que solo contenga caracteres
            imprimibles ASCII.
Access read-only.
Status  mandatory.
```

Fig. 4.3 Un objeto SMI

Este ejemplo muestra la definición de un objeto contenido en el MIB. Su nombre es sysDescr y pertenece al grupo sistema; ver en la Fig 4.4.

Un objeto gestionado no sólo ha de ser descrito, también debe ser identificado. Esto se hace utilizando el identificado de objeto ("Object Identifier") ASN.1 como si fuera un número de teléfono, reservando grupos de números para distintas localizaciones. En el caso de la gestión de red para TCP/IP, el número reservado fue 1.3.6.1.2 y SMI lo usa como base para la definición de nuevos objetos.

Este número se obtiene al unir a grupos de números con el siguiente significado:

- El primer grupo define el nodo administrador:
  - (1) para ISO
  - (2) para CCITT
  - (3) para la unión ISO-CCITT.
- El segundo grupo para el nodo administrador ISO define (3) para su uso por parte de otras organizaciones.
- El tercer grupo define (6) para su uso por parte del DoD ("U.S. Department of Defense").
- En el cuarto grupo, el DoD no ha indicado cómo ha de gestionarse ese grupo correspondiente por lo que la comunidad de Internet ha asumido (1).
- El quinto grupo fue aprobado por el IAB para ser:
  - (1) para el uso del directorio OSI en Internet
  - (2) para la identificación de objetos con propósitos de gestión
  - (3) para la identificación de objetos con fines experimentales
  - (4) para la identificación de objetos para uso privado

En el ejemplo, {system 1} significa que el identificador del objeto es 1.3.6.1.2.1.1.1. Es el primer objeto en el primer grupo (sistema) en el MIB.

4.3 MIB (Management Information Base)

El MIB define los objetos que pueden ser gestionados para cada capa en el protocolo TCP/IP. Hay dos versiones, MIB-I y MIB-II. MIB-I fue definida en el RFC 1156, y está clasificado ahora como protocolo histórico con *status no recomendado*.

En la Fig 4.4 podemos observar la definición de grupos para la MIB-II

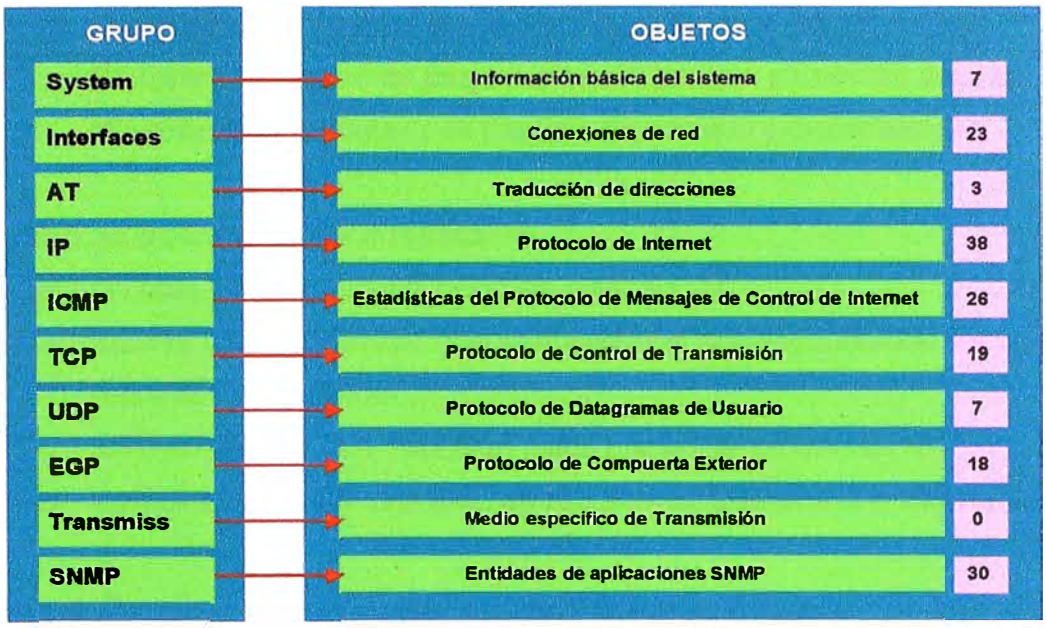


Fig. 4.4 Definición de grupos para la MIB II

Cada nodo gestionado soporta sólo los grupos apropiados. Por ejemplo, si no hay pasarela, el grupo EGP no tiene por qué estar incluido. Pero si un grupo es apropiado, todos los objetos en ese grupo deben estar soportados.

La lista de objetos gestionados definidos deriva de aquellos elementos considerados esenciales. Este enfoque, consistente en tomar sólo los objetos esenciales no es restrictivo, ya que el SMI proporciona mecanismos de extensibilidad tales como la definición de una nueva versión de MIB o de objetos privados o no estandarizados.

Debajo hay algunos ejemplos de objetos de cada grupo. La lista completa está definida en el RFC 1213.

- **Grupo de sistema**
  - sysDescr - Descripción completa del sistema(version, HW, OS)
  - sysObjectID - Identificación que da el distribuidor al objeto
  - sysUpTime - Tiempo desde la última reinicialización
  - sysContact - Nombre de la persona que hace de contacto
  - sysServices - Servicios que ofrece el dispositivo

- **Grupo de interfaces**
  - ifIndex - Número de interfaz
  - ifDescr - Descripción de la interfaz
  - ifType - Tipo de la interfaz
  - ifMtu - Tamaño máximo del datagrama IP
  - ifAdminisStatus - Status de la interfaz

- ifLastChange - Tiempo que lleva la interfaz en el estado actual
- ifINErrors - Número de paquetes recibidos que contenían errores
- ifOutDiscards - Número de paquetes enviados y desechados

- **Grupo de traducción de direcciones**
  - atTable - Tabla de traducción de direcciones
  - atEntry - Cada entrada que contiene una correspondencia de dirección de red a dirección física
  - atPhysAddress - La dirección física dependiente del medio
  - atNetAddress - La dirección de red correspondiente a la dirección física

- **Grupo IP**
  - ipForwarding - Indicación de si la entidad es una pasarela IP
  - ipInHdrErrors - Número de datagramas de entrada desechados debido a errores en sus cabeceras IP
  - ipInAddrErrors - Número de datagramas de entrada desechados debido a errores en sus direcciones IP
  - ipInUnknownProtos - Número de datagramas de entrada desechados debido a protocolos desconocidos o no soportados
  - ipReasmOKs - Número de datagramas IP reensamblados con éxito
  - ipRouteMask - Máscara de subred para el encaminamiento

- **Grupo ICMP**
  - icmpInMsgs - Número de mensajes ICMP recibidos
  - icmpInDestUnreachs Número de mensajes ICMP "destino inalcanzable"(destination unreachable) recibidos
  - icmpInTimeExcds - Número de mensajes ICMP "time exceeded"(tiempo excedido) recibidos
  - icmpInSrcQuenchs Número de mensajes ICMP "source quench(desbordamiento del emisor) recibidos
  - icmpOutErrors - Número de mensajes ICMP no enviados debido a problemas en ICMP

- **Grupo TCP**
  - tcpRtoAlgorithm - Algoritmo que determina el timeout para retransmitir octetos para los que no se ha recibido reconocimiento

- tcpMaxConn - Límite en el número de conexiones TCP que puede soportar la entidad
- tcpActiveOpens - Número de veces que las conexiones TCP han efectuado una transición directa del estado SYN-SENT al estado CLOSED
- tcpInSegs - Número de segmentos recibidos, incluyendo aquellos con error
- tcpConnRemAddress - La dirección IP remota para esta conexión TCP
- tcpInErrs - Número de segmentos desechados debido a errores de formato
- tcpOutRsts - Número de resets generados

- **Grupo UDP**
  - udpInDatagrams - Número de datagramas UDP entregados a usuarios UDP
  - udpNoPorts - Número de datagramas UDP recibidos para los que no existía aplicación en el puerto de destino
  - udpInErrors - Número de datagramas UDP recibidos que no se pudieron entregar por razones otras que la ausencia de la aplicación en el puerto de destino
  - udpOutDatagrams - Número de datagramas UDP enviados por la entidad
  -
- **Grupo EGP**
  - egpInMsgs - Número de mensajes EGP recibidos sin error
  - egpInErrors - Número de mensajes EGP con error
  - egpOutMsgs - Número de mensajes EGP generados localmente
  - egpNeighAddr - La dirección IP del vecino de esta entrada EGP
  - egpNeighState - El estado EGP del sistema local con respecto a la entrada EGP vecino

Esta no es la definición completa del MIB pero sirve de ejemplo de los objetos de cada grupo.

El grupo de interfaces contiene dos objetos de nivel superior: el número de interfaces del nodo (ifNumber) y una tabla con información de estas (ifTable). Cada entrada de la tabla (ifEntry) contiene los objetos de esa interfaz. Entre ellos, el tipo de interfaz (ifType) se identifica en el árbol MIB con notación ASN.1 como 1.3.6.1.2.1.2.2.1.3. Para un adaptador de red en anillo, su valor sería 9 ("iso88025-tokenRing") Para ver cual es la secuencia para identificar un objeto observamos la Fig 4.5

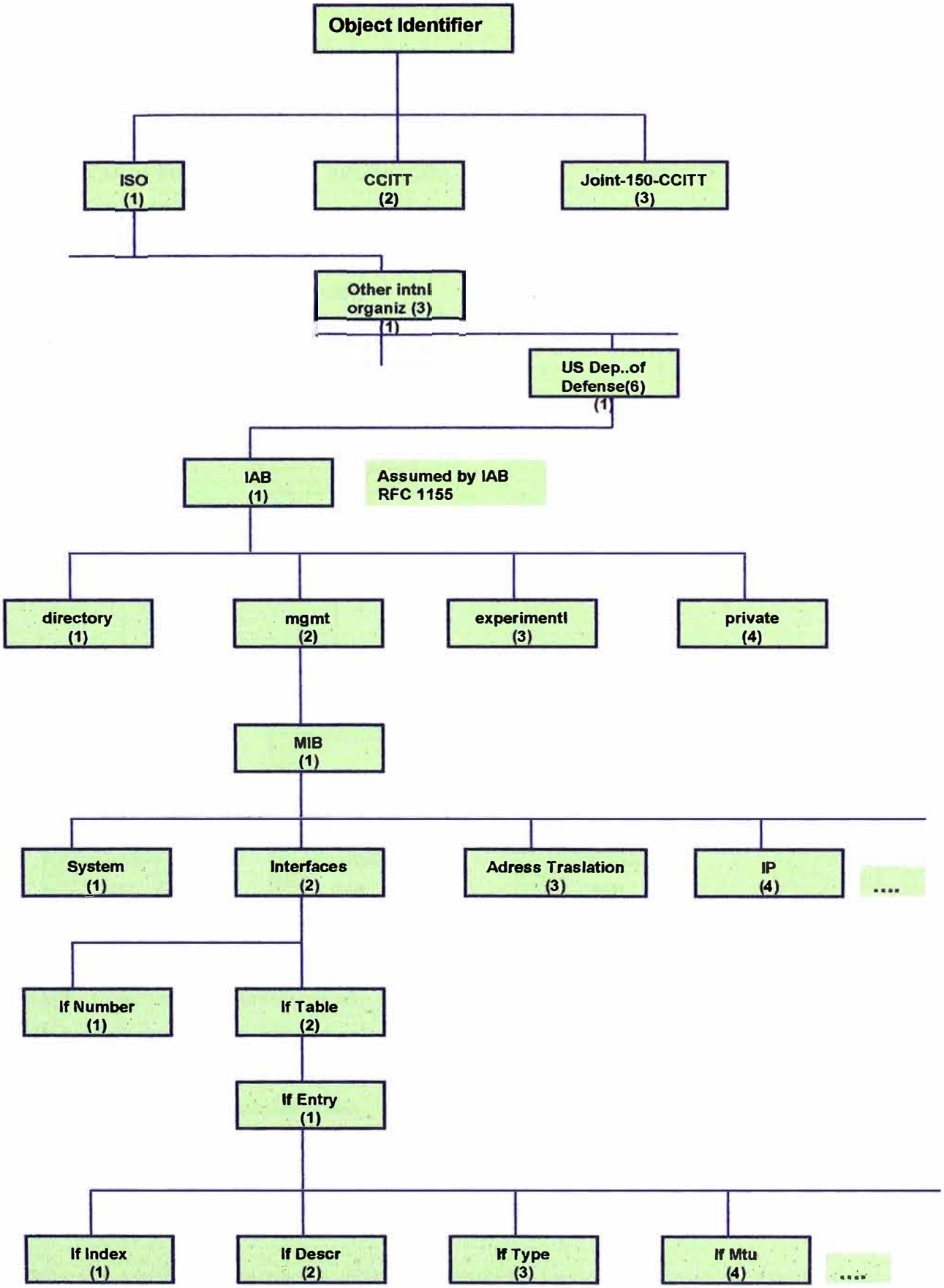
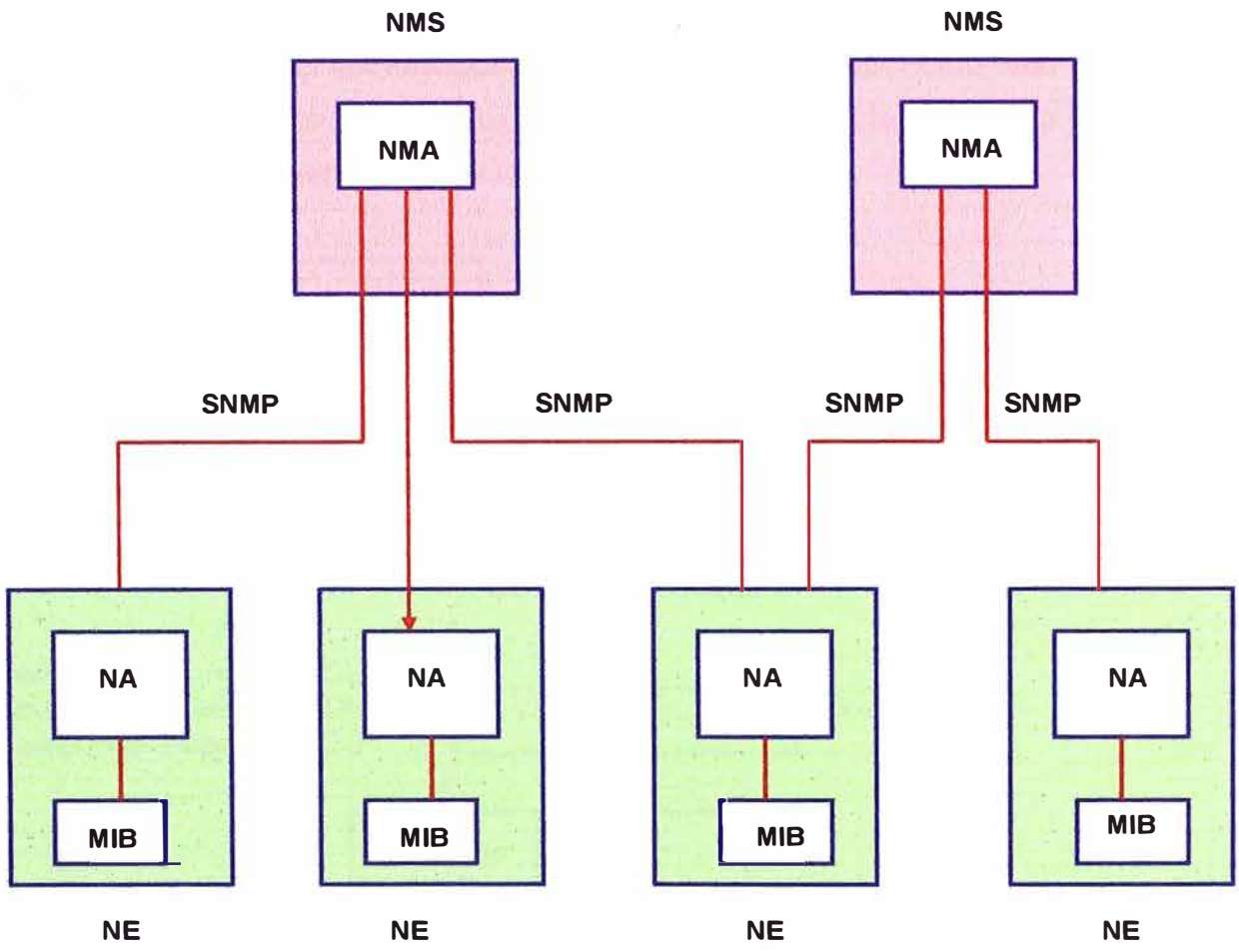


Fig. 4.5 Árbol de direcciones MIB

4.4 Funcionamiento de SNMP

SNMP como ya mencionamos trabaja bajo la arquitectura administrador/agente, sus componentes ya los hemos mencionado, por lo que aquí describiremos como funcionan para lograr el intercambio de información. En la Fig. 4.6 podemos observar como los componentes SNMP interactúan.



NMS : Estación de Administración de Red
NMA : Aplicación de Administración de Red
NE : Elemento de Red
MA : Agente de Administración
MIB : Base de Información Administrativa

Fig. 4.6 Interacción entre componentes SNMP

Todas las funciones de los MA son sólo alteraciones (set) o consultas (get) de variables, limitando así el número de funciones esenciales a dos y simplificando el protocolo. En la comunicación NE-NMS, se utilizan un número limitado de mensajes no solicitados (traps)

para informar de eventos asíncronos. Del mismo modo, en un intento de mantener la sencillez, el intercambio de información requiere sólo un servicio de datagramas y cada mensaje se envía en un único datagrama. Esto significa que SNMP es adecuado para una gran variedad de protocolos de transporte. El RFC 1157 especifica el intercambio de mensajes vía UDP, aunque es posible emplear otros.

Las entidades que residen en las NMS y los elementos de red que se comunican con otros a través de SNMP se denominan entidades de aplicación de SNMP. Los procesos que las implementan son las entidades de protocolo. Un agente SNMP con un conjunto arbitrario de entidades es una comunicad SNMP, en la que cada entidad se nombra con una ristra de bytes que debe ser unívoca para esa comunidad.

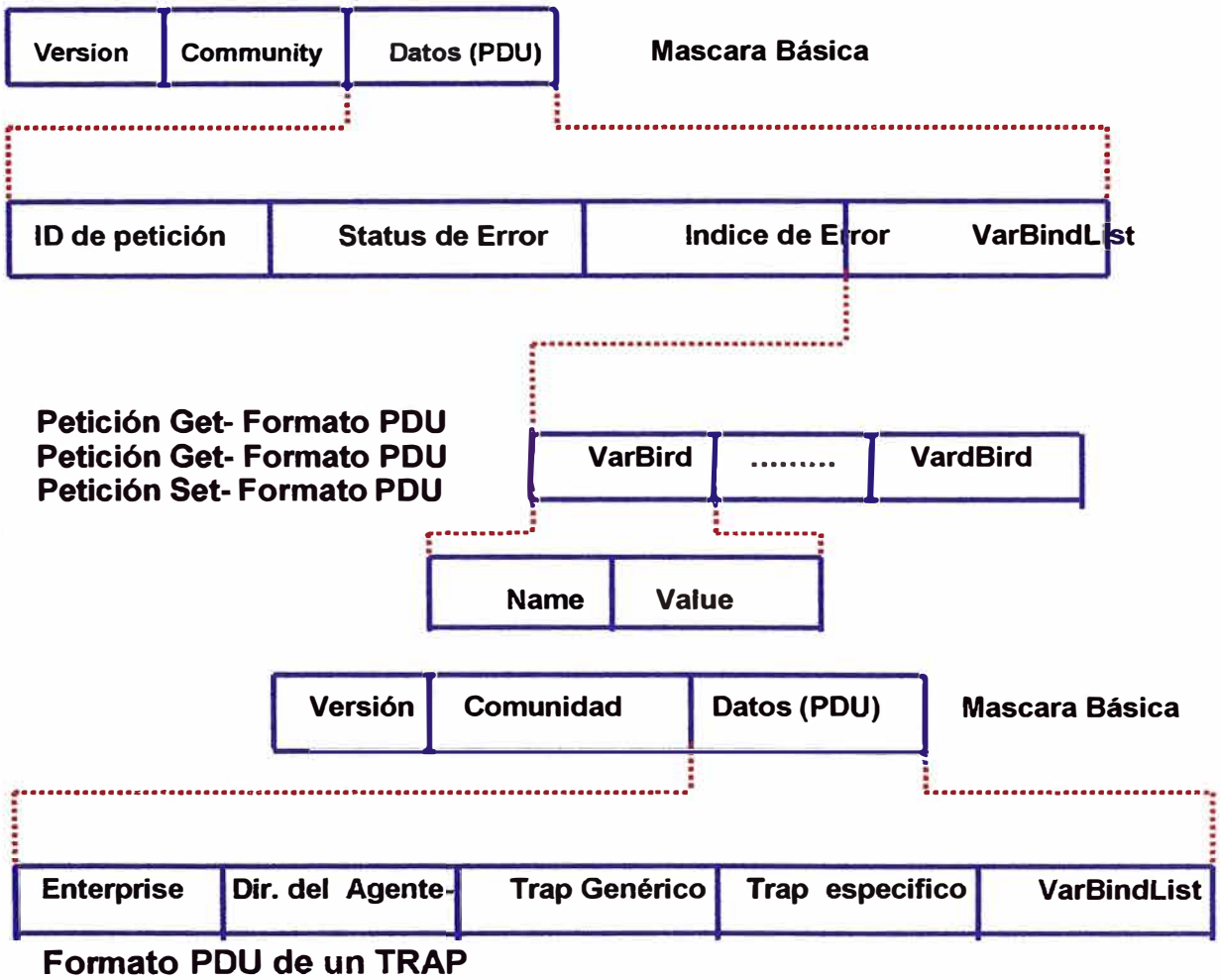


Fig. 4.7 Formato de paquetes SNMP

Un mensaje de SNMP consiste en un identificador de la versión, un nombre de la comunidad SNMP y un PDU ("protocol data unit"). Toda implementación de SNMP debe soportar las cinco PDUs siguientes:

- **GetRequest**: Recuperar los valores de un objeto del MIB
- **GetNextRequest**: Recorrer parte del MIB
- **SetRequest**: Alterar los valores de un objeto del MIB
- **GetResponse**: Respuesta de GetRequest, GetNextRequest y SetRequest
- **Trap**: Capacidad de los elementos de red para generar eventos como la inicialización., reinicio o fallo en el enlace del MA. Hay siete tipos de traps definidos en el RFC 1157: coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss y enterpriseSpecific.

En la Fig. 4.7 podemos observar estos formatos

4.5 El DPI de SNMP (SNMP Distributed Programming Interface)

SNMP define un protocolo que permite efectuar operaciones en una serie de variables. Este conjunto de variables (el MIB) y un conjunto básico o núcleo está predefinidas. Sin embargo, el diseño del MIB cuenta con la posibilidad de expandir este núcleo sea expandido. Desafortunadamente, las implementaciones convencionales de agentes SNMP no suministran mecanismos para que el usuario cree nuevas variables. El DPI enfoca esta cuestión proporcionando mecanismos que permiten al usuario añadir, borrar o reemplazar dinámicamente variables en el MIB local sin tener que recompilar el agente SNMP. Esto es posible gracias a un subagente que se comunica con el agente a través del DPI. El RFC 1228 lo describe.

El DPI de SNMP habilita a un proceso para registrar la existencia de una variable MIB en el agente SNMP, que pasará la solicitud al subagente. El subagente devuelve a su vez la respuesta apropiada al agente. Este, finalmente, empaqueta una respuesta SNMP y envía la respuesta a la NMS que inició la solicitud. El subagente es completamente invisible (transparente) para la NMS.
La comunicación entre el agente SNMP y sus clientes (subagentes) tiene lugar sobre un canal. Típicamente se trata de una conexión TCP, pero se pueden emplear otros protocolos de transporte orientados a conexión.

El agente en el DPI puede:

- Crear y borrar subárboles del MIB
- Crear un paquete de solicitud de registro para que el subagente informe al agente SNMp

- Crear un paquete de respuesta para que el subagente responda a la solicitud del agente SNMP
- Crear un paquete de solicitud TRAP.

La Fig. 4.8 muestra el flujo entre el agente SNMP y el subagente.

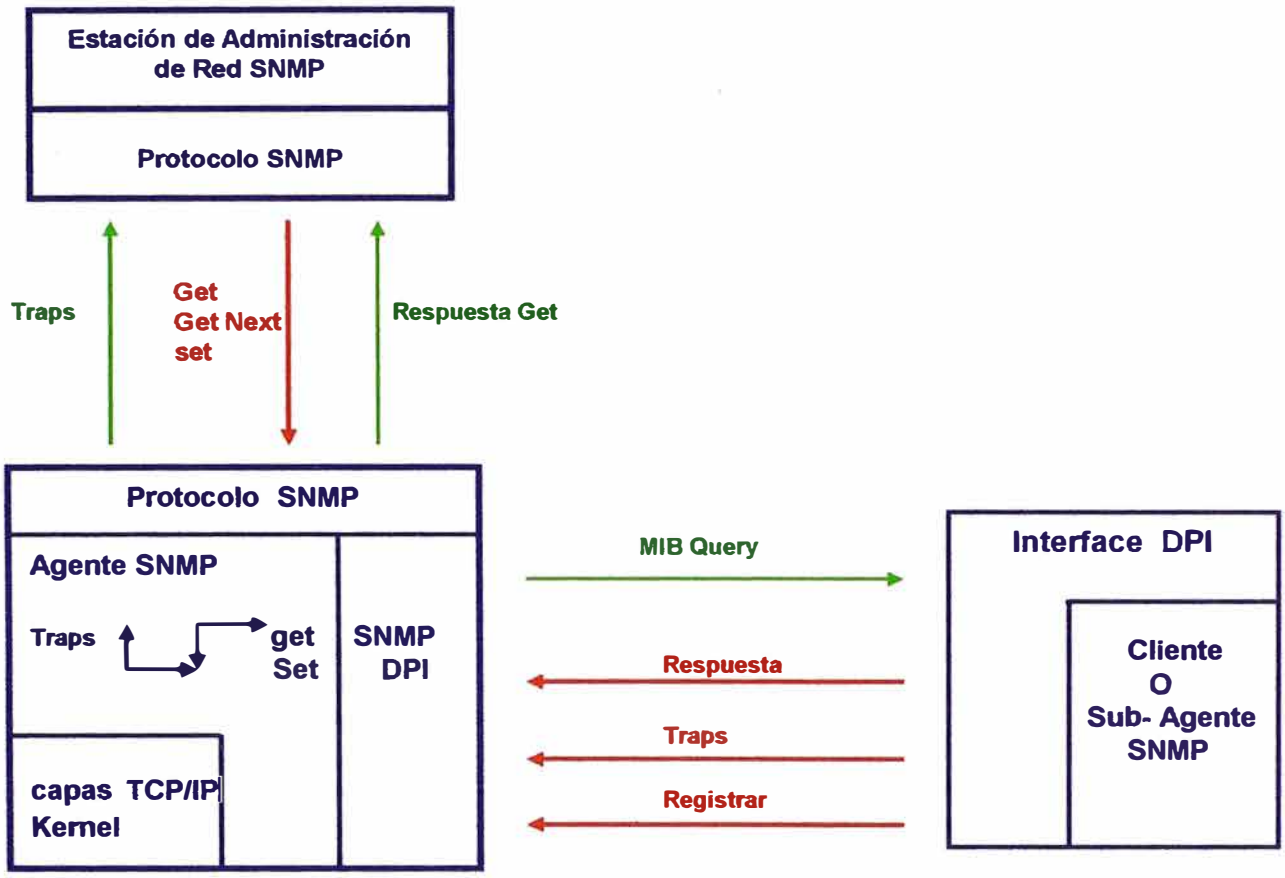


Fig. 4.8 Intercambio de información entre el agente y el sub-agente

- El agente SNMP se comunica con el manager por medio de SNMP.
- La comunicación del agente con las capas TCP/IP y con el núcleo del sistema operativo depende de la implementación.
- Un subagente SNMP, ejecutando un proceso a parte (que potencialmente puede estar en otra máquina), puede registrar objetos con el agente SNMP(Register).
- El agente SNMP decodificará los paquetes. Si un paquete contiene una solicitud Get/GetNext o Set para un objeto registrado en el subagente, se la enviará en el correspondiente paquete (MIB query).
- El subagente SNMP responde con un paquete RESPONSE (Reply).
- El agente codifica la respuesta en un paquete SNMP y lo envía al manager.

- Si el subagente desea informar de un cambio de estado importante, envía un Trap al agente que a su vez lo codificará y enviará al manager.

4.6 SNMPv2 (Simple Network Management Protocol, Version 2)

La infraestructura de la versión 2 de SNMP se publicó en abril de 1993 y consiste en 12 RFCs, incluyendo el primero, el 1441, que es una introducción. En agosto de 1993 los 12 RFCs se convirtieron en un estándar con status electivo.

Esta infraestructura consta de las siguientes disciplinas:

- **SMI("Structure of Management Information")**

  Definición del subconjunto de ASNN.1 para la creación de módulos MIB. Descripción en el RFC 1442.

- **Convenios textuales**

  Definición del conjunto inicial de convenios textuales disponible para todos los módulos MIB. Descripción en el RFC 1443.

- **Operaciones del protocolo**

  Definición de las operaciones del protocolo con respecto a las PDUs enviadas y recibidas en el RFC 1448.

- **Mapeados de transporte**

  Definición del mapeado de SNMPv2 sobre un conjunto inicial de dominios de transporte ya que se puede utilizar en diferentes pilas de protocolo. El mapeado en UDP es el preferido. El RFC también define OSI, AppleTalk, IPX, etc. Descripción en el RFC 1449.

- **Instrumentación del protocolo**

  Definición del MIB y del MIB Manager-Manger. Descripción en los RFCs 1450 y 1451.

- **Infraestructura administrativa**

  Definición de SNMPv2 Party, SP("Security Protocols") y Party MIB. Descripción en los RFCs 1445, 1446 y 1447.

- **Compatibilidades**

  Definición de la *compatibilidad* o *capacidad* de notación de los agentes. Descripción en el RFC 1444.

Las siguientes secciones describen las principales diferencias y mejoras desde SNMPv1 a SNMPv2.

4.6.1 Entidad SNMPv2

Una entidad SNMPv2 es un proceso real que realiza operaciones de gestión de red mediante la generación y/o respuesta a/de mensajes SNMPv2. Todas las posibles operaciones de una entidad se pueden restringir a un subconjunto de las operaciones que puede efectuar el entorno de gestión ("SNMPv2 Party" o EG). Una entidad SNMPv2 podría pertenecer a múltiples entidades gestoras, y mantiene las siguientes bases de datos locales:

- Una base de datos para todos los EG que conoce la entidad, que podrían ser:
  - Operación local
  - Operación local realizada por interacciones con EG o dispositivos remotos
  - Operación realizada por otras entidades SNMPv2
- Otra base de datos que representa todos los recursos de los objetos gestionados que conoce la entidad
- Como mínimo, una base de datos que representa una política de control de acceso que define los privilegios de acceso de acuerdo con los EG conocidos.

Una entidad SNMPv2 puede actuar como agente o como manager SNMPv2.

4.6.2 Entorno de gestión ("SNMPv2 Party" o EG)

Un entorno de gestión es un entorno de ejecución virtual cuyas operaciones se restringen, por razones de seguridad o de otra índole, a un subconjunto definido administrativamente de todas las operaciones que puede realizar una entidad SNMPv2 particular. Arquitectónicamente, cada EG comprende:

- Una identidad unívoca del entorno
- Una localización lógica de red en la que se ejecuta el EG, caracterizada por un dominio del protocolo de transporte y por información de direccionamiento del nivel de transporte.
- Un sólo protocolo de autentificación y parámetros asociados con los que se autentifican el origen y la integridad de los mensajes del protocolo generados por el entorno.
- Un sólo protocolo de privacidad y parámetros asociados con los que los mensajes de protocolo que recibe el entorno se protegen de cualquier intrusión.

4.6.3 GetBulkRequest

El GetBulkRequest está definido en el RFC 1448 y forma por tanto parte de las operaciones del protocolo. Un mensaje GetBulkRequest se genera y se transmite como una petición de una aplicación SNMPv2. Su fin es solicitar la transferencia de una cantidad de datos potencialmente elevada, incluyendo, sin que ello le condicione, la rapidez y eficiencia en la recuperación de grandes tablas. GetBulkRequest es más eficiente que GetNextRequest en la recuperación de grandes tablas MIB de objetos. Su sintaxis es:

GetBulkRequest [non-repeaters = N, max-repetitions = M]
(RequestedObjectName1,
RequestedObjectName2,
RequestedObjectName3)

Donde:

RequestedObjectName1, 2, 3 Identificador MIB del objeto, como sysUpTime, etc. Los objetos están en una lista ordenada léxicamente. Cada identificador de objeto está ligado como mínimo a una variable. Por ejemplo, el identificador *ipNetToMediaPhysAddress* está ligado a una variable para cada dirección IP de la tabla ARP y su contenido es la dirección MAC asociada.

N Especifica el valor de non-repeaters, lo que significa que se solicita sólo el contenido de la variable inmediata al objeto indicado en la solicitud, para los primeros N objetos nombrados entre paréntesis. Se trata de la misma función que desempeña GetNextRequest.

M Especifica el valor max-repetitions, lo que significa que se solicita del resto de los objetos (habiéndose solicitado N) el contenido de las M variables inmediatas al objeto indicado en la solicitud. Es similar a un GetNextRequest iterado pero transmitido en una sola solicitud.

Con GetBulkRequest se pueden conseguir los valores de sólo la siguiente variable o de las siguientes M variables con una sola solicitud.

Asumiendo la Tabla Nro 4.1 ARP en un host que ejecuta un agente SNMPv2:

Tabla Nro. 4.1 ARP en un host que ejecuta SNMP V2

Numero de interfase	Direc. de Red	Direc. Física	Tipo
1	10.0.0.51	00:00:10:01:23:45	estatica
1	9.2.3.4	00:00:10:54:32:10	dinamica
2	10.0.0.15	00:00:10:98:76:54	dinamica

Un administrador SNMPv2 envía la siguiente respuesta para conseguir sysUpTime y la tabla ARP completa:

GetBulkRequest [non-repeaters = 1, max-repetitions = 2]
(sysUpTime,
ipNetToMediaPhysAddress,
ipNetToMediaType)

La entidad SNMPv2 que actúa como agente responde con la PDU Response:

Response ((sysUpTime.0 = "123456"),
(ipNetToMediaPhysAddress.1.9.2.3.4 =
"000010543210"),
(ipNetToMediaType.1.9.2.3.4 = "dynamic"),
(ipNetToMediaPhysAddress.1.10.0.0.51 =
"000010012345"),
(ipNetToMediaType.1.10.0.0.51 = "static"))

La entidad SNMPv2 que hace de manager continúa con:

GetBulkRequest [non-repeaters = 1, max-repetitions = 2]
(sysUpTime,
ipNetToMediaPhysAddress.1.10.0.0.51,
ipNetToMediaType.1.10.0.0.51)

El agente responde con:

Response ((sysUpTime.0 = "123466"),
(ipNetToMediaPhysAddress.2.10.0.0.15 =
"000010987654"),

(ipNetToMediaType.2.10.0.0.15 =
"dynamic"),
(ipNetToMediaNetAddress.1.9.2.3.4 =
"9.2.3.4"),
(ipRoutingDiscards.0 = "2"))

Esta respuesta señala el final de la tabla al manager. Con GetNextRequest se hubieran necesitado cuatro solicitudes para conseguir la misma información. Si se hubiera fijado el valor *max-repetition* de GetBulkRequest a tres, en este ejemplo sólo se hubiera necesitado una solicitud.

4.6.4 InformRequest

Un mensaje InformRequest se genera y se transmite como una solicitud de una aplicación de una entidad manager SNMPv2 que desea notificar a otra aplicación, que se ejecuta también en un manager SNMPv2, información en el ámbito del MIB(MIB view) para un entorno local a la aplicación que envía el mensaje. El paquete se utiliza para indicar al manager del otro entorno de la información accesible en el emisor. (Comunicación manager-manager a través de los límites del entorno). Las dos primeras variables en la lista de asociaciones de variables de un mensaje InformRequest son sysUpTime.0 y snmpEventID.i respectivamente. Les pueden seguir otras variables.

El MIB para SNMPv2 Este MIB define los objetos gestionados que determinan el comportamiento de la entidadSNMPv2.
Nota: No es una sustitución del MIB-II.

Las siguientes son algunas definiciones de objetos para hacerse una idea de sus contenidos:

```
snmpORLastChange OBJECT-TYPE
   SYNTAX     TimeStamp
   MAX-ACCESS read-only
   STATUS     current
   DESCRIPTION
        "El valor de sysUpTime en el momento del cambio más reciente en el valor o
        estado de cualquier instancia de snmpORID."
warmStart NOTIFICATION-TYPE
```

STATUS current
DESCRIPTION
"Un trap warmStart significa que la entidad SNMPv2, actuando como agente, se está reinicializando a sí misma de tal modo que la configuración no se altere."

EG del MIB("Party MIB")

El EG del MIB define los objetos gestionados que se corresponden con las propiedades asociadas a un EG SNMPv2. Un ejemplo de algunos objetos del MIB:

partyIdentity OBJECT-TYPE
SYNTAX Party
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"Un identificador de EG unívoco para un EG de SNMPv2 particular."

partyAuthProtocol OBJECT-TYPE
SYNTAX OBJECT IDENTIFIER
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"El protocolo de autentificación por el que se autentifican el origen y la integridad de todos los mensajes que genera el EG. El valor noAuth significa que los mensajes no están autentificados. Una vez que se crea una instancia de este objeto, su valor no puede ser alterado."

4.6.5 MIB Manager-Manager

La finalidad de este MIB es proporcionar los medios para la coordinación entre múltiples estaciones de gestión. Es decir, los medios por los que las funciones de control y monitorización de la gestión de red se pueden distribuir entre múltiples NMS en una gran red. Específicamente, este MIB suministra mecanismos para que una NMS solicite servicios de gestión de otra. Por tanto, una entidad SNMPv2 puede tener un doble papel; cuando proporciona información de gestión a otro manager, actúa como agente, y cuando pide información, actúa como manager.

El MIB manager-manager consta de las tres tablas siguientes:

- Alarmas
- Eventos
- Notificaciones

Cada alarma es una condición específica detectada mediante la monitorización periódica, en un intervalo de muestreo configurable, de los valores de una determinada variable con información de gestión. Un ejemplo de condición de alarma es cuando la variable monitorizada toma un valor fuera de rango. Cada condición de alarma dispara un evento, que puede a su vez desencadenar una o más notificaciones para otras NMS usando el InformRequest.

4.6.6 SAPP (Single Authentication and Privacy Protocol)

El protocolo de autentificación proporciona un mecanismo para que la gestión de SNMPv2 permita identificar que las comunicaciones que genera un entorno se originan efectivamente en ese entorno.

El protocolo de autentificación proporciona un mecanismo para que la gestión de SNMPv2 permita proteger las comunicaciones que genera un entorno de cualquier intrusión.

Las principales amenazas contra las que el protocolo de seguridad de SNMPv2 aporta protección son:

- Modificación de información
- Enmascaramiento
- Modificación del flujo de mensajes
- Intrusión en la información

Los siguientes servicios de seguridad proporcionan medidas contra las anteriores amenazas:

- **Integridad de los datos**

  La proporciona el algoritmo de condensación de mensajes MD5. Se calcula un resumen o extracto de 128 bits de la porción indicada del mensaje SNMPv2 y se incluye como parte del mensaje enviado al receptor.

- **Autentificación del origen de los datos**

  A cada mensaje se le añade un prefijo con un valor secreto que comparten el emisor del mensaje y el receptor, antes de calcular el extracto.

- **Delay o retardo del mensaje**

  En cada mensaje se incluye un sello de tiempo.

- **Confidencialidad de los datos**

  La proporciona el protocolo simétrico de privacidad que encripta una porción adecuada del mensaje de acuerdo con una llave secreta conocida sólo por el emisor y el receptor. Este protocolo se usa conjuntamente con el algoritmo simétrico de encriptación, en el modo de encadenamiento de cifrado de bloques, que forma parte del DES ("Data Encryption Standard"). La parte designada del mensaje se encripta y se incluye como parte el mensaje enviado el receptor.

4.6.7 El nuevo modelo administrativo

Uno de los propósitos del modelo administrativo para SNMPv2 es definir como la infraestructura administrativa se aplica para llevar a cabo una administración de red efectiva en diversas configuraciones y entornos.

El modelo implica el uso de diferentes identidades en el intercambio de mensajes. De esta forma, representa abandonar el esquema basado en comunidades del SNMPv1 original. Al identificar sin ambigüedad al emisor y al receptor de cada mensaje, esta nueva estrategia mejora el esquema histórico de comunidades ya que permite un diseño del control de acceso a los datos más conveniente así como el empleo de protocolos de seguridad asimétricos (con llave pública) en el futuro.

La Fig. 4.9 nos muestra la nueva estructura del formato SNMPV2

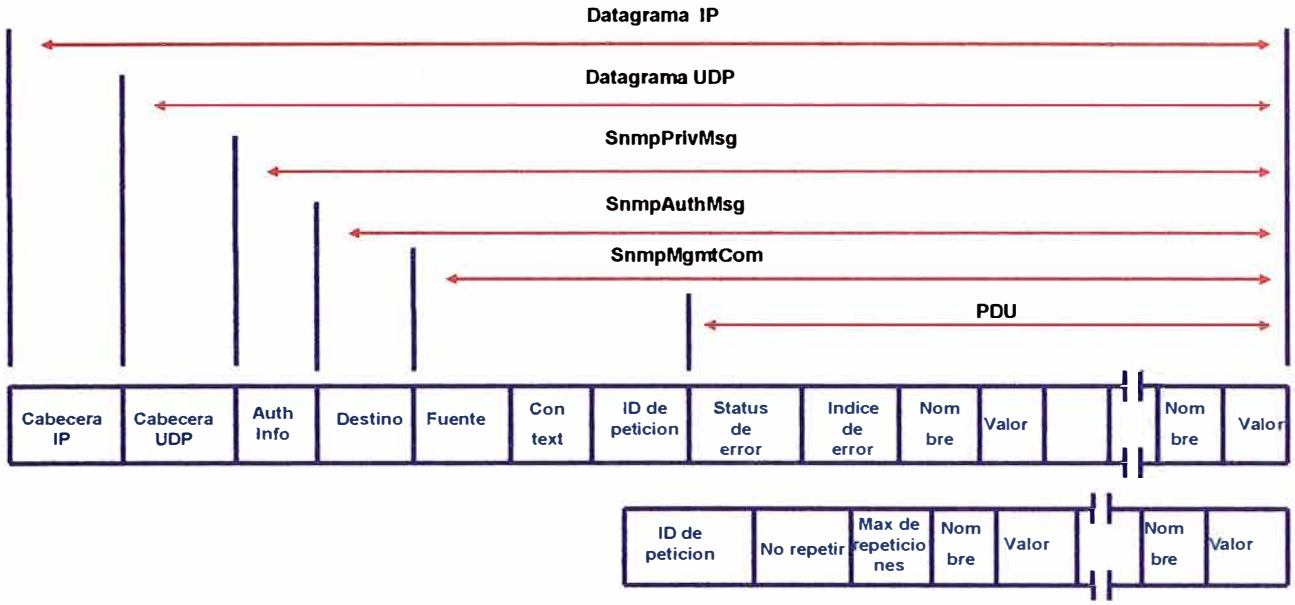


Fig. 4.9 Estructura del formato SNMP V2

PDU Incluye una de las siguientes PDUs

- GetRequest
- GetNextRequest
- Response
- SetRequest
- InformRequest
- SNMPv2-Trap

El GetBulkRequest tiene un formato de PDU distinto al mostrado más arriba.

Nota: El SNMP-Trap tiene ahora el mismo formato que las demás solicitudes.

SnmpMgmtCom ("SNMP Management Communication")

Añade el identificador del entorno emisor (srcParty), del receptor (dstParty) y el contexto a la PDU. El contexto especifica el ámbito de SNMPv2 que contiene la información de gestión a la que referencia la comunicación.

SnmpAuthMsg

Este campo se utiliza como información de autentificación para el protocolo de información usado por el entorno en cuestión. El SnmpAuthMsg está serializado de acuerdo con ASN.1 BER por lo que puede ser encriptado.

SnmpPrivMsg SNMP Private Message

El SNMPv2 Private Message es un mensaje SNMPv2 autentificado que posiblemente está protegido de intrusiones en la información que contiene. Un destino privado (privDst) se añade al entorno de destino.

El mensaje pasa a ser encapsulado en un datagrama UDP/IP normal y se envía a su destino a través de la red.

4.7 SNMPv3 (Simple Network Management Protocol, Version 3)

SNMPv3 es una versión mejorada del protocolo SNMP, que agrega características de seguridad y administración. Se desarrollo para corregir las deficiencias en seguridad de SNMPv1/SNMPv2, por lo tanto podemos decir que SNMPv3 es SNMPv2 mas seguridad y administración.

Entre sus principales mejoras tenemos:

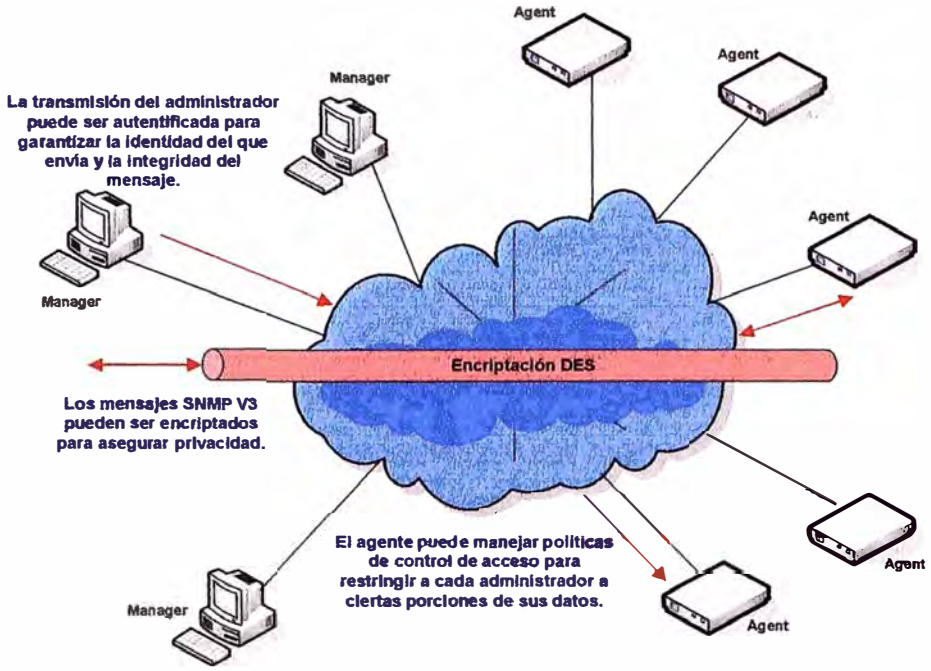
- Mejoras de Seguridad
  - Autenticación del origen de los datos
  - Verificación de integridad de datos.
  - Encriptación de datos.

- Mejoras de administración
  - Nomenclatura de entidades
  - Usuarios y políticas
  - Configuración remota

SNMPv3 incluye 3 servicios importantes: Autenticación, Privacidad y Control de acceso.

En la Fig. 4.10 podemos observar como interactúan estos servicios.

La cabecera de los mensajes SNMPv3 contienen información de seguridad que puede ser usada para autenticación y manejo de privacidad. Esto lo observamos en la Fig. 4.11



4.10

Fig. 4.10 Servicios en SNMP V3

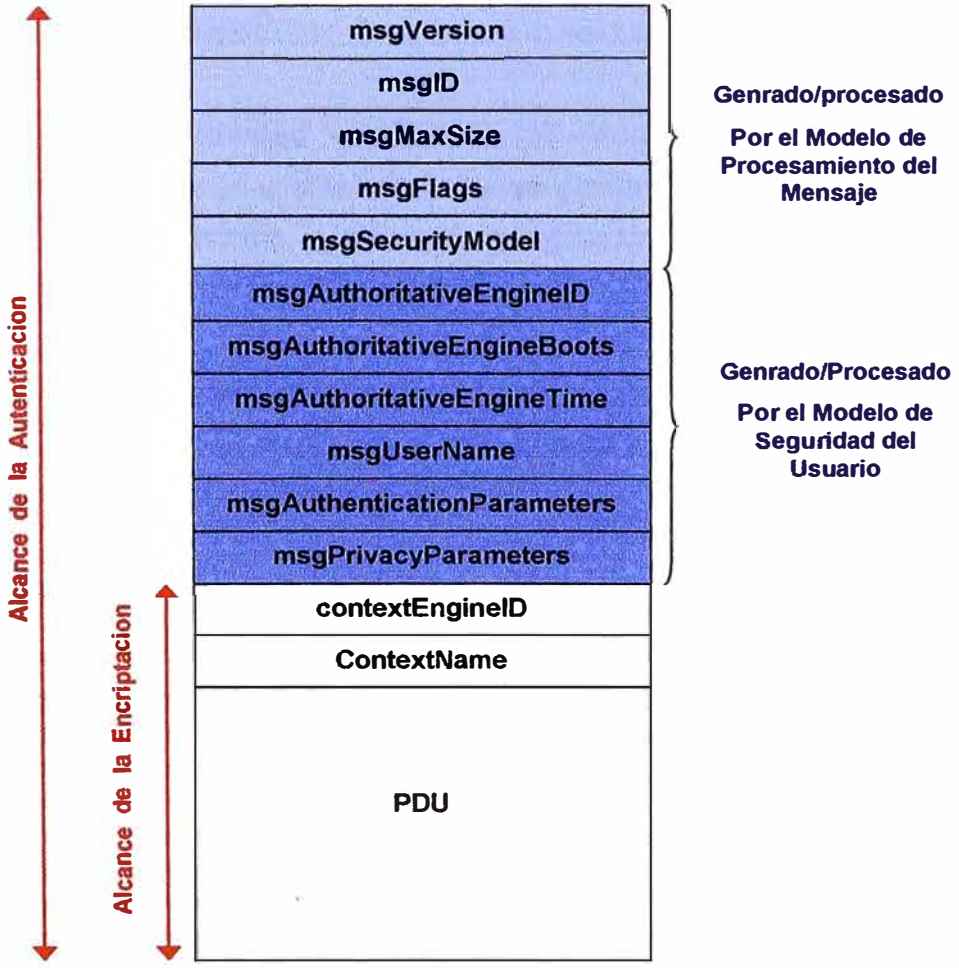


Fig. 4.11 Cabecera SNMP V3

CAPITULO V
SOLUCION DE PROBLEMAS EN LA RED

Network Troubleshooting significa reconocer y diagnosticar problemas en la red con el objetivo de mantener la red funcionando de manera optima. La principal preocupación de un administrador de red es mantener la conectividad de todos los dispositivos que forman parte de ella (este proceso se llama comúnmente manejo de fallas). Además de eso debe evaluar y hacer mejoras en el rendimiento de la red. En este capitulo trataremos acerca de cómo hacer Trobleshooting a la red, que tipos de problemas son los mas comunes y que consideraciones debemos tener para evitarlos o darles solución.

5.1 Problemas de conectividad.-

Estos problemas ocurren cuando las estaciones de trabajo no pueden comunicarse con otras computadoras o dispositivos dentro de una red Lan o WAN. Los principales son:

- **Perdida de conectividad -->** Cuando los usuarios no pueden acceder a otros dispositivos o áreas de una red, esto causa que la compañía quede dividida y aísla a los usuarios a servicios y recursos menguando el rendimiento operativo de la compañía.

- **Conectividad intermitente -->** Cuando los usuarios tienen acceso a los recursos algunas veces y otras veces no. Generalmente estos problemas indican que la red esta el borde de una caída completa.

- **Problemas de tiempo vencido -->** Estos problemas se refieren a pérdidas de conectividad debidas a que las conexiones no se realizan o se pierden por causa del vencimiento de los tiempos establecidos para la conexión o el mantenimiento de la misma. Generalmente son indicadores de un bajo rendimiento en la red.

5.2 Problemas de rendimiento (performance).-

Una red tiene problemas de rendimiento cuando no esta operando con la eficacia que debería. Algunos de los principales signos de bajo rendimiento en una red son:

- Tiempos de respuesta lentos.
- La red no esta disponible en todo momento como debiera.
- Los usuarios se quejan de que les toma mucho más tiempo del normal el realizar sus tareas.

Algunos problemas se presentan de manera intermitente, otros empiezan pequeños y van creciendo con el tiempo.

5.3 Estrategias para solucionar problemas

En la solución de problemas en la red generalmente empleamos las herramientas y conocimientos que encontramos a disposición. Si tenemos un conocimiento profundo de la red que administramos gran parte de la tarea esta hecha; pero además necesitaremos herramientas de software y hardware que nos permitan ubicar estos problemas en la red. Estas herramientas pueden ser tan sencillas como famosísimo comando "Ping", o más avanzadas como los analizadores de red.

Para que estas herramientas nos sean útiles y podamos sacarles el mejor provecho necesitamos plantearnos una estrategia para el reconocimiento, análisis y solución de problemas en la red.

¿Como sabemos que esta ocurriendo un problema en la red?

La respuesta a esta pegunta depende de la configuración particular de cada red y del comportamiento normal que debemos conocer. Si notamos cambios en la red deberíamos hacernos las siguientes preguntas:

- ¿Es un cambio esperado o inusual?
- ¿Ha ocurrido antes este evento?
- ¿El cambio afecta a un dispositivo o enlace para el cual tenemos un back up?
- ¿El cambio interfiere alguna operación vital en la red?
- ¿El cambio afecta a uno o varios dispositivos o enlaces en la red?

Después de tener una idea de como estos cambios afectan la red, podremos reconocer si son críticos o no, y proceder a su solución. Hay que recalcar que todo problema en la red debe ser solucionado sea critico o no, la diferencia entre ellos solamente será el tiempo que dispondremos para solucionar uno u otro.

El empleo de una estrategia nos permite aproximarnos a los problemas metódicamente y resolverlos con una mínima interrupción observada por los usuarios. Aquí enumeramos algunos pasos que pueden ser una guía en la implementación de estrategias de solución:

- Reconocer los síntomas
- Entender el problema.
- Identificar y probar las posibles causas del problema
- Resolver el problema

5.3.1 Reconocer los Síntomas:

El primer paso para resolver un problema es identificar e interpretar los síntomas. Hay varias formas como podemos enterarnos de que hay un problema:

- Comentarios de los usuarios → Aunque es posible solucionar muchos problemas de la red sin que los usuarios se den cuenta, es inevitable recibir la realimentación de los usuarios sobre como esta funcionando la red:
    - No se puede imprimir
    - No pueden acceder al servidor de aplicaciones
    - Toma demasiado tiempo copiar archivos a través de la Red.
    - Cuando envían un correo hacia laguna dirección externa reciben un mensaje de error.
    - etc.

- Alertas del sistema de monitoreo de red → Los sistemas de gestión y monitoreo de red nos proporcionan alertas que nos avisan de malos funcionamientos o cambios en la red, estas pueden ser alertas en pantalla, alertas enviadas por correo electrónico, etc.

  Estos avisos generalmente vienen acompañados de información adicional que nos permite enfocarnos al área exacta donde ha ocurrido dicho problema.

5.3.2 Analizando los Síntomas:

Cuando un síntoma ocurre es aconsejable hacernos las siguientes preguntas con el fin de acercarnos más al área posible donde ocurre un problema:

- ¿En qué sub-red ocurre el problema?

- ¿El usuario trata de conectarse a un servidor, estación de trabajo o dispositivo en la misma sub-red o en una distinta?
- ¿Son muchos los usuarios que experimentan el mismo problema?
- ¿Los problemas son intermitentes o permanentes

5.3.3 Entendiendo el problema:

Las redes están diseñadas para que lleven información desde un dispositivo a otro. Cuando la comunicación se vuelve problemática se debe determinar por que la información no está circulando como debería. Las 2 principales causas son:

- La conexión física se ha interrumpido (el cable esta desconectado, roto o deteriorado)
- Algún dispositivo no esta funcionando adecuadamente y no envía o recibe los datos completos.

Los programas de monitoreo pueden ubicar y reportar fácilmente interrupciones en las conexiones físicas. (Problemas de capa 1) Pero es mucho mas complicado determinar que dispositivo y por que no esta operando como se espera (generalmente problemas de capa 2 y capa 3).

Para averiguar por que un dispositivo no esta trabajando adecuadamente debemos fijarnos primero en:

- **Servicio Valido.-** Verificar que el dispositivo este bien configurado para el tipo de servicio que debería entregar. Por ejemplo verificar los parámetros adecuados de QoS.

- **Acceso Restringido.-** Verificar que las estaciones de trabajo u otros dispositivos tienen los permisos adecuados para establecer esa conexión. Verificar si algún otro dispositivo (Ej. un firewall) esta bloqueando es conexión.

- **Configuración correcta.-** Verificar que la configuración es la correcta: Direcciones IP, mascara de subred, gateways dirección de broadcast. Muchos problemas aparecen por errores en la configuración de equipos nuevos recién agregados a la red o equipos que han sido reconfigurados.

5.3.4 Identificando y probando la causa del problema.-

Después de desarrollar una teoría acerca de la causa del problema, hay que probar esa teoría, esta prueba demostrara si la teoría que asumimos era la correcta o no.

Dos reglas generales para la solución de problemas son:

- Si no se puede reproducir el problema, el problema no existe a menos que ocurra otra vez por su cuenta.
- Si el problema es intermitente y no puede ser reproducido, se debe configurar la red para que un programa analizador de redes capture el problema.

A pesar que las herramientas de administración pueden proporcionar una importante cantidad de información sobre los problemas y su ubicación; siempre será necesario reemplazar equipos y componentes hasta ubicar el punto exacto del problema.

Ejemplo: Análisis de un problema:

Este ejemplo nos mostrará el análisis de un problema típico en la red.

Un usuario en su red no puede acceder a un servidor de correo. Necesitaremos establecer dos áreas de información:

- **Que sabemos.-** En este caso, la estación de trabajo del usuario no puede comunicarse con el servidor de correo.

- **Que no sabemos y necesitamos probar.-**
  - ¿Puede la estación de trabajo comunicarse con la red, o el problema se limita a la comunicación con el servidor? Probar enviando un "Ping" o conectándose a otros dispositivos.
  - ¿Es la estación de trabajo el único dispositivo que es incapaz de comunicarse con el servidor, u otras estaciones de trabajo tienen el mismo problema? Probar la conectividad a otras estaciones de trabajo.
  - ¿Si otras no pueden comunicarse con el servidor, pueden estas comunicarse con otros dispositivos de red? Otra vez probar la conectividad.

El proceso de análisis sigue los siguientes pasos:

1. ¿Puede la estación de trabajo comunicarse con algún otro dispositivo en la sub-red?
   - **No**, ir al paso 2.
   - **Si**, determine sí solo el servidor es inalcanzable.

- Si sólo el servidor no puede ser alcanzado, esto sugiere un problema de servidor. Confirme haciendo el paso 2.
- Si otro dispositivo no puede ser alcanzado, esto sugiere un problema de conectividad en la red. Confirme haciendo el paso3.

2. ¿Pueden otras estaciones de trabajo comunicarse con el servidor?
   - **No**; es muy probable que sea un problema del servidor. Ir al paso 3.
   - **Si**; entonces el problema es que la estación de trabajo no se esta comunicando con la subred.

3. ¿Pueden otras estaciones de trabajo comunicarse con otros dispositivos de red?
   - **No**, entonces es muy probable que sea un problema en la red.
   - **Si**, entonces es muy probable que sea un problema en el servidor.

Después de determinar que el problema esta en el servidor, sub-red, o estación de trabajo, podremos analizar el problema, de la siguiente manera:

- **Problema con el servidor** – Examinar sí el servidor esta funcionando, si esta apropiadamente conectado con la red, y si esta configurado apropiadamente.
- **Problema con la subred** – Examinar cada dispositivo en el camino entre los usuarios y el servidor.
- **Problema con la estación de trabajo** – Examinar si la estación de trabajo puede acceder a otros recursos de red y sí esta configurado para comunicarse con ese servidor en particular.

5.3.5 Solucionando el problema.-

Muchos problemas de en la red, son fáciles de resolver, pero otros pueden no tener muchos síntomas. La solución del problema generalmente involucra:

- Hacer un upgrade de software y hardware.
- Hacer balanceo de carga analizando:
  - Que usuarios se comunican con que servidores.
  - Cuales son los niveles de tráfico que manejan los usuarios en cada segmento de la red.

  Con esos datos es posible decidor como redistribuir el tráfico.

- Agregar segmentos a la red para mejorar la distribución de tráfico.
- Reemplazar equipos que están fallando.

Para esto es conveniente tener a la mano:

- Equipos de backup (fuentes de poder, puertos, etc.) del hardware mas critico.
- Mantener copias recientes de las configuraciones para recargar las memorias flash que puedan corromperse.

5.4 Diseñando la red para la solución de problemas (TroubleShooting).-

Acceder a dispositivos claves en la red cuando esta experimentando problemas de conectividad o funcionamiento es importante para minimizar los tiempos de solución de problemas. Por lo tanto tener un adecuado acceso a la administración de los equipos depende de estos criterios de diseño:

- Ubicar la estación de administración de tal manera que pueda recoger la mayor cantidad de datos de la red a través del protocolo de gestión como SNMP.
- Distribuir las sondas (equipos que tomaran los datos) adecuadamente en la red.
- Habilidad para comunicarse con cada dispositivo aun cuando su estación de administración no pueda acceder a la red.

Siguiendo poscriterios anteriores veremos como diseñar la red:

5.4.1 Ubicando la estación de administración SNMP:

En una red LAN típica la estación de administración debe ir conectada directamente al Backbone donde puede conducir mejor el trafico SNMP y manejar los dispositivos en la red. Usualmente es el backbone la mejor ubicación por que:

- El backbone no esta sujeto a las fallas de routers o switches de subredes individuales.
- En una interrupción parcial de la red, la información recogida por una estación de administración en el backbone es probablemente más exacta que la de una estación con ruta a una subred.
- El backbone es usualmente protegido con energía y tecnología redundante, como FDDI, eso le permite corregir sus propios problemas. Esta redundancia asegura que el backbone siga siendo operacional, aún cuando otras áreas de la red tienen problemas.
- El backbone es típicamente más rápido y tiene mas ancho de banda que otras áreas de la red, siendo el lugar más eficiente para una estación de administración.

Hay que asegurarnos que la capacidad del backbone puede acomodarse al tráfico SNMP generado por la aplicación de administración. Ver Fig. 5.1

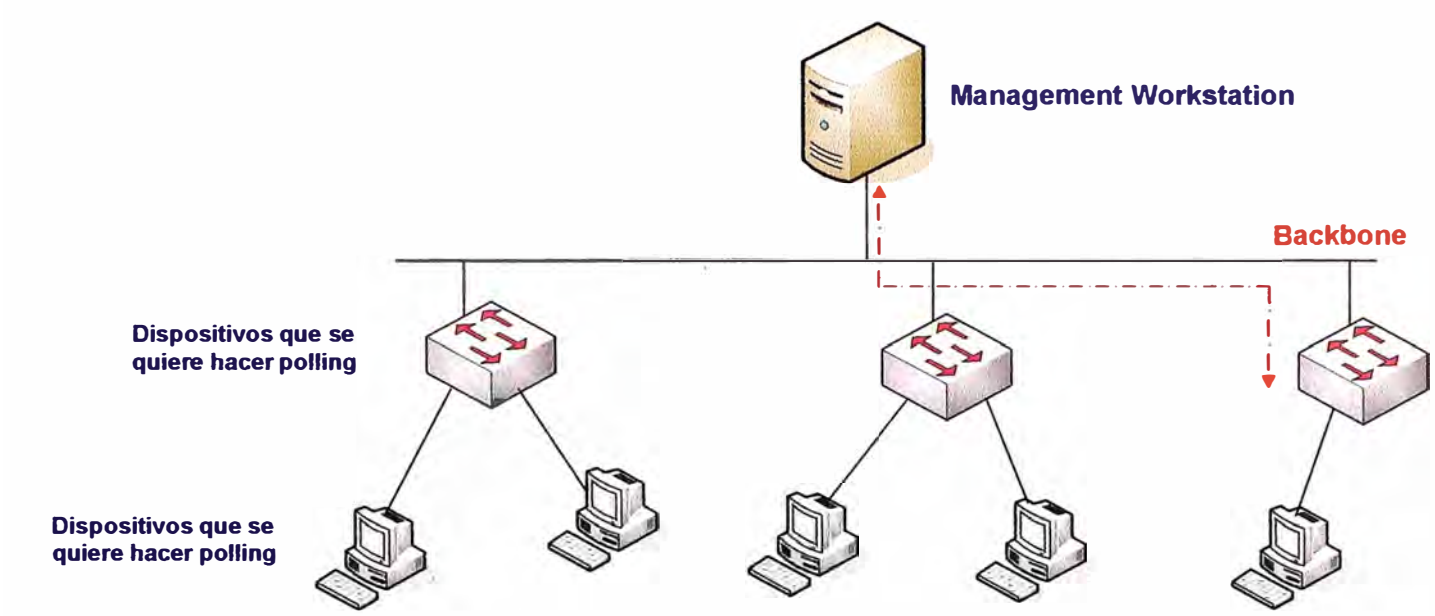


Fig. 5.1 Asegurando el backbone en SNMP

Aunque el administrador SNMP en el backbone es una buena manera de saber que sucede en la red, no debemos confiar exclusivamente en el. Debido a que la administración SNMP se ejecuta en banda (es decir, el tráfico SNMP comparte banda ancha de la red con el tráfico de datos), podríamos encontrar los siguientes problemas:

- El tráfico pesado de datos o una avería en la red, pueden hacer difícil o incluso imposible para una estación de administración hacer consultas a los dispositivos.
- El tráfico generado por las consultas SNMP podrían contribuir a los problemas que experimenta la red.

5.4.2 Usando Sondas:

Para minimizar la frecuencia de trafico SNMP en la red, se deben colocar una o varias sondas para recolectar datos monitoreados remotamente (RMON) por los dispositivos de red. En el modelo distribuido que observamos en la Fig. 5.2, la estación de administración usa las consultas SNMP para recolectar datos de las sondas en lugar de hacerlo de todos los dispositivos de red. De esta manera distribuyendo la administración sobre toda la red aseguramos que haya una recolección fluida de datos aunque se presenten problemas en la red.

Hay que tomar en cuenta que hay muchos dispositivos que soportan solo las MIBs de SNMP en vez de las MIBs de RMON, por esta razona si usemos sondas RMON, habrá que hacer polling SNMP a estos dispositivos independientemente.

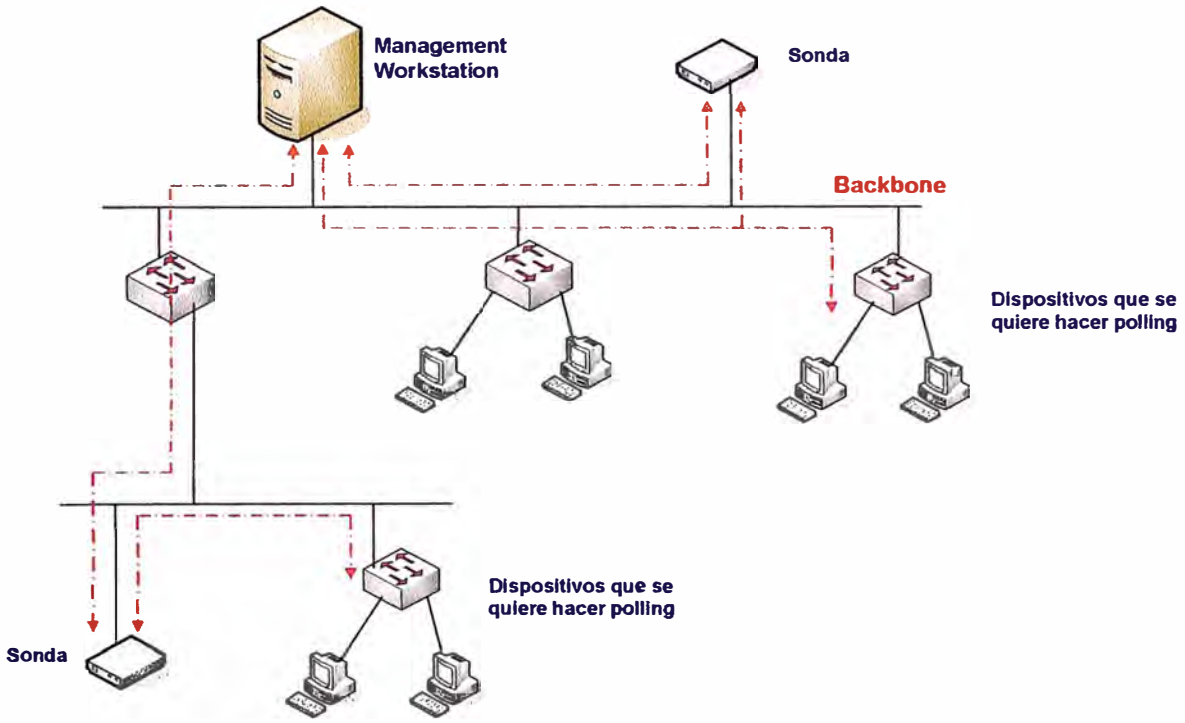


Fig. 5.2 Uso de sondas en SNMP

Para extender las capacidades de monitoreo remoto, podemos usar sondas RMON embebidas o hacer Roving Análisis (monitorear un puerto por un periodo de tiempo, moverse a otro puerto por otro periodo y así consecutivamente), la desventaja de este ultimo es que no se puede ver un análisis histórico de los puertos.

También debemos tomar en cuenta que las sondas no entregan información de que puerto fue el que fallo. Esta información si la podríamos recolectar de switchs o hubs que tengan su propio modulo de administración.

5.4.3 Monitoreando algunos puntos críticos en la red.-

Monitoreando el enlace WAN hacia Internet:

El enlace a Internet debe ser un punto activo de monitoreo por las siguientes razones:

- Representa un costo externo para la empresa.
- Es una fuente continua de tráfico hacia y desde el exterior de la red.
- Es una posible fuente de problemas de seguridad.

Aquí nos enfocamos principalmente en el volumen de tráfico, los reportes de tráfico indican si uno esta pagando pro demasiado ancho de banda (el enlace esta sobredimensionado) o si necesitamos comprar mas ancho de banda.
Verificar el nivel de uso de este enlace por departamento y por usuario. Verificar cual es el tipo de trafico mas utilizado y buscar trafico no deseado o inesperado que pueda indicar huecos en nuestra seguridad.

Monitoreando los Switches de la red:
La siguiente área de interés es el número de enlaces entre los switches y los hosts. Aquí verificamos disponibilidad, volumen de tráfico por puerto y tipo de tráfico.
Disponibilidad, se refiere a verificar que los puertos y enlaces estén disponibles, que no tengan problemas de conectividad.

Volumen de tráfico por puerto, se refiere a verificar que cada puerto mueva el tráfico esperado y detectar puertos que repentinamente generen o reciban tráfico fuera de lo normal.
Tipo de tráfico, verificar que el tipo de tráfico que se esta cursando sea el esperado y no se estén abriendo puertos o utilizando protocolos no esperados.

5.4.4 Consejos para la configuración de una estación administrativa.-

- Configurar las estación de monitoreo independiente de cualquier conexión a la red como NIS, NFS, DNS lookups.
- Tener mas de una interfase de red disponible, es recomendable además conectar las sondas y otros dispositivos de monitoreo en un interfase aparte formando una LAN independiente para los equipos de monitoreo.
- No darle a la estación de monitoreo privilegios de administrador en la red, tales como el de logearse sin necesidad de contraseñas, etc. Los hackers toman como punto principal de ataque este tipo de estaciones.
- Conectar la estación de monitoreo a una fuente de poder que no se interrumpa como un UPS para protegerla de cortes repentinos de energía.
- Hacer backups regulares de la estación de monitoreo.
- Proveerla de algún tipo de acceso remoto para mantener el monitoreo de la activad de la red remotamente.
- Mantener copias de las configuraciones de todos los dispositivos en algún servidor de archivos o en la estación de monitoreo.

5.5 Principales problemas en la red.-

Ahora exponemos algunos ejemplos de los clásicos problemas que pueden aparecer en una red de datos

5.5.1 Verificando el ancho de Banda.-

Para determinar como opera día a día nuestra red es necesario examinar el uso de ancho de banda. Las variaciones en el uso del ancho de banda nos alertan de problemas actuales o potenciales, así como posibles huecos en la seguridad.

Entendiendo el problema:

El uso del ancho de Banda es determinado por como esta configurada nuestra red, que servicios entrega a los usuarios y que permisos tienen ellos para el uso de la red. Hay que conocer para esto los parámetros normales de funcionamiento y vigilarlos de manera cercana para detectar cualquier variación.

Identificando el problema:

Determinar la utilización normal de todos los dispositivos y enlaces en la red (Ethernet, Fibra óptica, modos de transferencia, etc.) y monitorearlos de cerca para ver cual puede estar excediendo los parámetros establecidos como normales.

En la mayoría de las redes, el uso del ancho de banda se incrementa gradualmente cuando los usuarios empiezan a utilizar más recursos de la red. Por lo tanto hay que verificar cual de estos usos excede los parámetros establecidos, o cual de estos recursos están siendo utilizados por usuarios que no deberían.

Hay que examinar las tendencias históricas de la red y ubicar donde la red esta presentando un incremento o disminución gradual o repentina de uso.

- Un aumento repentino indica una condición anormal. Hay que verificar el área donde aparece esta anomalía.
- Un aumento o disminución sostenida en el uso del ancho de banda en un segmento de la red indica el aumento o disminución de la carga en la red. Balancear esta carga es indispensable para mejorar el desempeño de la red.

Una alta tasa de uso de ancho de banda puede resultar en tasas altas de paquetes fragmentados. Cuando excedemos el parámetro de uso el aumento de paquetes fragmentados se hace común.

Resolviendo el problema:

- Ubicar los puertos que presentan anomalías de uso excesivo o bajo de ancho de banda.
- Limitar el uso de servicios a los usuarios de esos puertos si fuera el caso.
- Redistribuir el tráfico de la red para balancear la carga, si es necesario segmentando la red con un switch, router o bridge.
- Verificar que el mal funcionamiento de del hardware de algún dispositivo no sea la causa del problema, si lo es reemplazarlo inmediatamente.

5.5.2 Broadcast Storm.-

Un broadcast storm hace referencia al excesivo tráfico de broadcast o multicast en la red. Generalmente un broadcast storm resulta en una caída de la red por perdida de conectividad a medida que el aumento de paquetes de broadcast o multicast aumenta.

Entendiendo el problema:

Paquetes de broadcast o multicast son parte normal de la operación de una red. Para determinar cuando se convierten en un Broadcast Storm debemos identificar cuando este tráfico se vuelve anormal.

Identificando el problema:

Uno puede sospechar que esta en medio de un Broadcast Storm cuando los tiempos de respuesta en la red se vuelven demasiado lentos y las operaciones de red presentan con frecuencia cierres de conexión por exceder el tiempo establecido. A medida que el broadcast Storm aumenta los usuarios presentaran problemas para loguearse a los servidores, a sus cuentas de correo; hasta que en un momento la red simplemente no podrá ser utilizada.

Cuando la red este operando normalmente debemos monitorear y determinar el porcentaje normal de broadcast y multicast en la red. Y utilizar estos datos como parámetro para determinar luego el aumento de este tráfico.

Resolviendo el problema:

Un Broadcast Storm puede ocurrir cuando un equipo esta fallando o es configurado incorrectamente, cuando el protocolo spannig tree no esta configurado correctamente o por el uso indiscriminado de programas que hagan broadcast o multicast.

Por lo tanto para resolver el problema debemos:

- Deshabilitar la interfase que esta originando el broadcast. Corregir el problema y conectarla a otra vez a la red.
- Corregir la configuración del spanning tree, esto lo hacemos verificando si este protocolo esta activado en el puerto que esta causando el problema.

5.5.3 Direcciones duplicadas.-

Las redes pueden generar direcciones MAC o IP duplicadas. Estos casos de duplicidad causan problemas en la entrega de paquetes y pueden incluso deshabilitar completamente los servicios en la red.

Entendiendo el problema:

Los problemas de direcciones MAC duplicadas son causados por problemas en la capa de Enlace, en el momento de pasar las cabeceras al momento que los protocolos se comunican. Las direcciones IP duplicadas son causadas pro problemas en la capa de red o pro errores de los administradores en el momento de asignar o configurar las direcciones IP en los equipos.

Identificando el problema:

Para identificar estos problemas de direcciones IP duplicadas se recomienda le uso de software analizador de red.

Corrigiendo el problema:

Una vez identificada la fuente del error corregir manualmente la configuración de las direcciones IP o cambiar el hardware que pudiera estar causando el problema de direcciones MAC duplicadas.

5.5.4 Perdida de Paquetes en Ethernet.-

Si la red presenta signos de congestión, podría estar experimentando perdidas de paquetes. Cuando una red se congestiona, usualmente es por el aumento en su uso, entonces los paquetes empiezan a ser descartados ya que los buffers están sobrecargados.

Muchas veces estos problemas se relacionan con el aumento de las colisiones. Esto puede significar que es necesario realizar una segmentación de la red, para distribuir la carga.

Si el uso de la red se mantiene en los parámetros normales pero las colisiones parecen aumentar, entonces estamos frente aun problema n la capa física. Debemos revisar la

integridad de los cables, el buen estado de las interfases y los puertos de conexión tanto en los dispositivos como en las tarjetas de red.

Una vez reconocidos los principales problemas en la red y además dadas las pautas necesarias para implementar soluciones de administración como SNMP, continuaremos en el siguiente capitulo viendo la implementación de soluciones de administración utilizando SNMP.

CAPITULO VI
APLICACIONES DEL PROTOCOLO SNMP

En este capítulo veremos la implementación de aplicaciones que utilizan el protocolo SNMP, desde software comercial hasta software libre que empleamos para monitorear nuestros dispositivos SNMP.

6.1 SNMP en Software Libre

Dada la creciente demanda por aplicaciones de software libre, la administración de redes usando SNMP no es la excepción. Aquí mostramos algunas de las herramientas de software libre que podemos descargar de Internet sin costo alguno, y como las podemos configurar. Algunas son únicamente en entorno de comandos y otras nos muestran de forma gráfica los resultados de las consultas SNMP que hacen los administradores a las estaciones administradas.

Para continuar con el uso del software libre estas aplicaciones han sido implementadas sobre una plataforma Linux.

6.1.1 CMU-SNMP

Uno de los paquetes más populares de SNMP es el CMU-SNMP. Diseñado originalmente en la Universidad de Carnegie Mellon, ha sido transportado a Linux por Juergen Schoenwaelder y Erik Schoenfelder. Es completamente compatible con el estándar SNMPv1 e incluye algunas de las nuevas funcionalidades de SNMPv2.

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

Una valiosa característica añadida que viene con CMU-SNMP es un SNMP C-API, que permite a los programadores construir complejas herramientas de gestión basadas en las capacidades de red de la distribución.

La instalación en un sistema Linux es sencilla, si bien algo diferente de la instalación original. Existe una distribución con los ejecutables pre-compilados de las herramientas de gestión, el demonio y la biblioteca API. Lo primero que haremos es decidir si "bajarse" la distribución con las fuentes, o la distribución con los ejecutables. La distribución binaria se instala y ejecuta sin problema alguno en los Linux que soporten ELF. Si bien explicaremos cómo instalar la distribución binaria, es una buena práctica el bajarse las distribuciones binarias únicamente de servidores Internet de confianza para evitar caballos de Troya y otros problemas de seguridad.

Para iniciar la instalación podemos descargar la aplicación de:
ftp://sunsite.unc.edu/pub/Linux/system/network/admin/cmu-snmp-linux-3.4-bin.tar.gz

Copia el fichero **cmu-snmp-linux-3.4-bin.tar.gz** en el directorio raíz (/). Descomprímelo y extrae los ficheros del tar con con la siguiente orden:
tar zxvf cmu-snmp-linux-3.4-bin.tar.gz
Ahora tendremos todas las utilidades y bibliotecas correctamente instaladas en el sistema, a excepción del fichero de configuración del agente: /etc/snmpd.conf. Lo podemos crear ejecutando el siguiente "script":
/tmp/cmu-snmp-linux-3.4/etc/installconf
Con los siguientes parámetros:
/tmp/cmu-snmp-linux-3.4/etc/installconf -mini password
Donde password es la palabra clave pública (*community*) que se vaya a utilizar. Ahora se puede editar el nuevo fichero de configuración /etc/snmpd.conf. En él, se pueden cambiar el valor de puerto UDP empleado por el agente, las variables systemContact, sysLocation y sysName, así como los parámetros de velocidad de las interfases para las tarjetas de red y los puertos PPP.

Las herramientas más importantes de gestión de este paquete son:

- **/usr/bin/snmpget** Un programa diseñado para consultar un valor concreto a un agente MIB de la red (un router, un hub, etc).

- **/usr/bin/snmpgetnext** Permite leer el siguiente objeto de un árbol MIB sin necesidad de conocer el nombre.
- **/usr/bin/snmpset** Una herramienta para escribir valores en los objetos de agentes remotos.
- **/usr/bin/snmpwalk** Herramienta que lee un objeto completo o una serie de objetos sin necesidad de especificar la instancia exacta. Es útil para pedir objetos tipo tabla.
- **/usr/bin/snmpnetstat**
- **/usr/bin/snmptrapd** Demonio que escucha los "traps" de los agentes.
- **/usr/bin/snmptest** Herramienta interactiva diseñada para demostrar las posibilidades del API.

El agente se encuentra en el directorio /usr/sbin/snmpd.

CMU_SNMP también instala un fichero MIB en /usr/lib/mib.txt. Éste es un buen lugar en donde buscar qué tipo de información se le puede pedir a un dispositivo de red. El agente se tiene que lanzar a ejecución cuando se pone en marcha la máquina. Esto se puede hacer añadiendo el siguiente comando en alguno de los ficheros de arranque (por ejemplo en /etc/rc.f/rc.local):

/usr/sbin/snmpd -f; echo 'Arrancando snmpd'

Una vez se tiene el agente SNMP en ejecución en la máquina Linux, se puede comprobar su funcionamiento con alguna de las herramientas de gestión, por ejemplo:

/usr/bin/snmpget localhost public interfaces.ifNumber.0

la cual retornará el número de interfaces configurados en el sistema, y:

/usr/bin/snmpwalk localhost public system

devuelve todos los valores en el subárbol "system" del MIB. Esto lo vemos a continuación:

```
dragon:~$ /usr/bin/snmpwalk
usage: snmpwalk gateway-name community-name object-identifier
dragon:~$ /usr/bin/snmpwalk localhost public system
system.sysDescr.0 = "Linux version 2.0.24 (root@dragon)
(gcc version 2.7.2) #6 Mon Nov 25 15:08:40 MET 1996"
system.sysObjectID.0 = OID: enterprises.tubs.ibr.linuxMIB
system.sysUpTime.0 = Timeticks: (39748002) 4 days, 14:24:40
system.sysContact.0 = "David Guerrero"
system.sysName.0 = "dragon "
```

```
system.sysLocation.0 = "Madrid (SPAIN)"
system.sysServices.0 = 72
system.sysORLastChange.0 = Timeticks: (39748006) 4 days, 14:24:40
system.sysORTable.sysOREntry.sysORID.1 = OID:
enterprises.tubs.ibr.linuxMIB.linuxAgents.1
system.sysORTable.sysOREntry.sysORDescr.1 = "LINUX agent"
system.sysORTable.sysOREntry.sysORUpTime.1 = Timeticks: (39748007) 4
days, 14:24:40
dragon:~$
```

El C-API está en el directorio /lib/libsnmp.so.3.4.
Se pueden ojear los ficheros de cabecera relacionados con la biblioteca en

- /usr/include/snmp/snmp.h
- /usr/include/snmp/snmp_impl.h
- /usr/include/snmp/asn1.h
- /usr/include/snmp/snmp_api.h

Se puede encontrar más información en las páginas del manual snmp_api(3) y variables(5).
Existe también un módulo Perl de interfase con CMU C_API con el que se pueden realizar fácilmente llamadas a esta biblioteca desde programas Perl (Perl-scripts).

6.1.2 MRTG: Multi Router Traffic Grapher

MRTG es una avanzada utilidad gráfica escrita por Tobias Oetiker y Dave Rand para representar gráficamente los datos que los gestores SNMP leen de los agentes SNMP. Produce unas vistosas páginas HTML con gráficos GIF sobre el tráfico entrante y saliente en los interfaces de red prácticamente tiempo real. Con esta herramienta se evita el tener que trabajar directamente con las utilidades CMU-SNMP mediante línea de comandos. Ésta es una herramienta potente y fácil de utilizar que podemos encontrar en la Internet; para descargarlo podemos hacerlo en:

MRTG utiliza una implementación de SNMP escrita completamente en Perl, por tanto, no es necesario instalar otros paquetes. El programa principal está escrito en "C" para acelerar el proceso de toma de muestras y la generación de imágenes GIF. Los gráficos

son generados con la ayuda de la biblioteca GD escrita por Thomas Boutell, autor de la FAQ WWW.
El paquete contiene algunas utilidades para analizar los interfaces de enlace, extraer sus características y generar los ficheros de configuración base, que luego se pueden modificar para adaptarlos a las necesidades concretas.

Otra característica interesante del MRTG es la cantidad de información que produce. Permite cuatro niveles de detalle para cada interfase: tráfico en las últimas 24 horas, la última semana, el último mes y un gráfico anual. Esto permite recoger información para realizar estadísticas. Guarda toda esta información en una base de datos utilizando un algoritmo de consolidación que impide que los ficheros crezcan de forma desmesurada.

También genera una página principal que contiene las imágenes GIF de los detalles diarios de cada interfase del ruteador, lo que permite hacerse una idea general de qué es lo que está pasando en el ruteador con un sólo vistazo. Veamos las Fig. 6.1

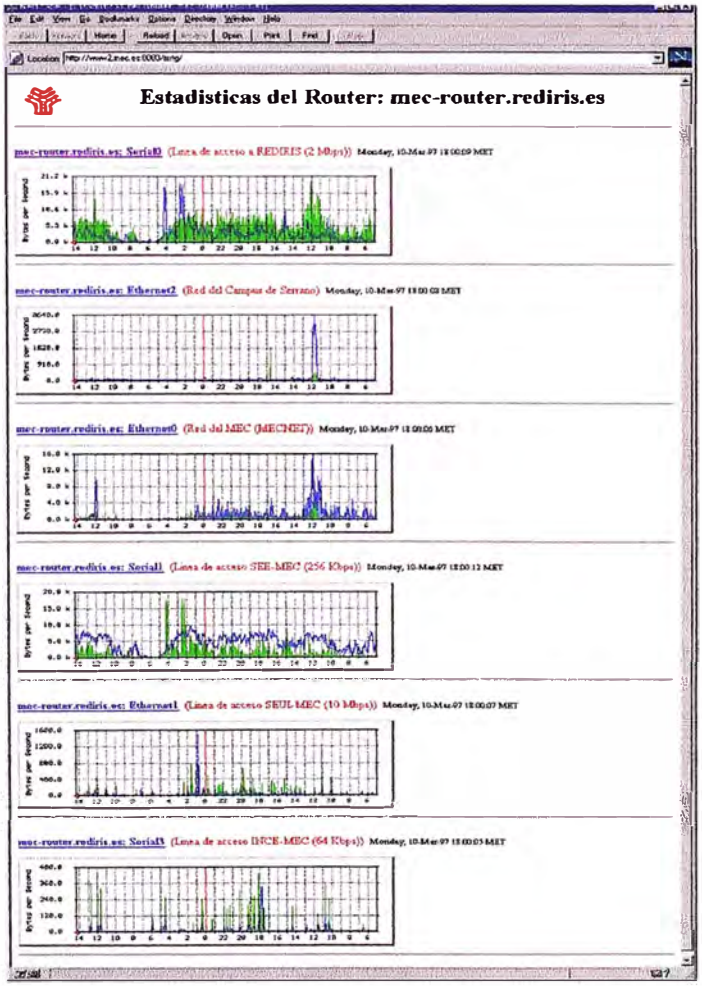


Fig 6.1 Reporte generado por MRTG

Procedimiento básico de instalación. Lo primero que se necesita es la distribución que podemos obtenerla en: http://www.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html
Antes de comenzar la instalación del MRTG es necesario instalar la biblioteca GD. Comenzamos compilando el paquete MRTG. Extrae la distribución y edita el fichero Makefile para indicar donde se encuentra la biblioteca y los archivos de cabecera de GD, así como cual es el fichero ejecutable Perl 5.003: normalmente se encuentra en /usr/bin/perl o en /usr/local/bin/perl.
Construye el programa principal tecleando make rateup; cuando termine la compilación, teclea make substitute para incluir el path correcto del intérprete de Perl en los scripts de Perl que utiliza MRTG.
Copia los siguientes ficheros su directorio destino final (por ejemplo: /usr/local/mrtg): BER.pm, SNMP_Session.pm, mrtg y rateup. También se han de copiar en este directorio los dos ficheros de configuración: indexmaker y cfgmaker.
Asegurémonos que todos los programas tienen permiso de ejecución. Ya está todo listo para crear un fichero de configuración sencillo. Es necesario tener acceso SNMP de lectura al ruteador. Para un ruteador de la marca Cisco, las líneas de configuración que dan permiso son:

```
access-list 99 permit 193.147.0.8
access-list 99 permit 193.147.0.9
access-list 99 permit 193.147.0.130
snmp-server community public RO 99>
```

Esto permite peticiones de sólo lectura desde las direcciones especificadas en la lista 99, empleando la palabra clave "public" como *community*. Si lo que se quiere es permitir el acceso desde cualquier máquina en modo sólo lectura al ruteador, entonces la línea ha de ser la siguiente:

```
snmp-server community public RO
```

Si el ruteador de la red es de otra marca, entonces se ha de consultar el manual para determinar cómo permitir el acceso SNMP.
El script cfgmaker simplifica mucho la tarea de construir el fichero de configuración. Todo lo que hay que hacer es ejecutarlo con los siguientes parámetros:

```
cfgmaker <community>@<router-host-name or IP>
```

Por ejemplo:

```
cfgmaker public@mec-router.rediris.es > mrtg.cfg
```

Localizará todos los interfaces del ruteador mec-router.rediris.es y escribirá una sección en el fichero con las especificaciones del número de interfaces, velocidad máxima, descripción, etc., junto con algunas etiquetas HTML para que puedan ser incluidas en la página detallada. Es posible editar este fichero HTML para traducirlo al idioma y preferencias propias. A continuación vemos la salida de una de las interfases del ruteador:

```
Target[mec-router.1]: 1:public@mec-router
MaxBytes[mec-router.1]: 1250000
Title[mec-router.1]: mec-router.rediris.es (mec-router.mec.es): Ethernet0
PageTop[mec-router.1]: <H1>Estadisticas del puerto Ethernet0<BR>
Red del MEC (MECNET)</H1>
<TABLE>
<TR><TD>System:</TD><TD>mec-router.rediris.es en RedIRIS </TD></TR>
<TR><TD>Maintainer:</TD><TD>david@mec.es</TD></TR>
<TR><TD>Interface:</TD><TD>Ethemet0 (1)</TD></TR>
<TR><TD>IP:</TD><TD>mec-router.mec.es (193.147.0.1)</TD></TR>
<TR><TD>Max Speed:</TD>
<TD>1250.0 kBytes/s (ethemetCsmacd)</TD></TR>
</TABLE>
```

Ahora se puede ejecutar el programa mrtg por primera vez. Sencillamente ejecuta:
./mrtg mrtg.cfg

Si todo va bien, el programa se pondrá en contacto con el ruteador, pedirá algunos valores y generará algunos ficheros de registro y algunos ficheros GIF en el directorio actual. No hay que sorprenderse por las quejas respecto los ficheros de registro y de gráficos que no ha encontrado, esto sólo sucede la primera vez que se ejecuta. Elimina los ficheros de gráficos que genera y vuelve a ejecutar el programa otra vez. El gráfico generado mostrará el tráfico producido en el intervalo desde la última ejecución del programa. También genera páginas HTML para cada interface.
Ahora vamos a indicarle a MRTG como ejecutarse adecuadamente en el sistema. Primero se ha de crear un directorio dentro del directorio principal del web servidor (suponiendo que en el sistema haya un servidor web en funcionamiento) para contener las páginas y gráficos que MRTG generará cada vez que se ejecute. Añade este directorio en la cabecera del fichero de configuración con la directiva WorkDir:

/usr/local/web/mrtg (suponiendo que el directorio raíz está situado en /usr/local/web). La próxima vez que MRTG se ejecute, creará los ficheros de registro y de gráficos en este directorio, pudiendo accederse vía http://your_host.domain/mrtg.
Ahora vamos a construir la página principal para todos los interfaces como la que aparece en la Figura Nro 6.1. Esto se puede llevar a cabo con la utilidad indexmaker.
Ejecutamos: indexmaker mrtg.cfg <router-name regexp> > /usr/local/web/mrtg/index.html

Se generará un documento HTML con gráficos diarios de aquellos interfaces cuyo nombre de ruteador coincida con la expresión regular anterior y los enlaza con la página individual detallada.
Como se puede imaginar, el programa MRTG se ha de ejecutar a intervalos regulares para recoger datos en cada intervalo y generar los gráficos periódicamente, de forma que de la impresión de ser una monitorización en tiempo real. Esto se puede conseguir mediante la siguiente línea en el fichero /etc/crontab (suponiendo /usr/local/mrtg-bin como el directorio donde reside el programa mrtg):

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * \
/usr/local/mrtg-bin/mrtg \
/usr/local/mrtg-bin/mrtg.cfg > \
/dev/null 2>&1
```

En caso de tratarse de una distribución Red Hat, la línea que se tendría que añadir sería:

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * root \
/usr/local/mrtg-bin/mrtg \
/usr/local/mrtg-bin/mrtg.cfg > \
/dev/null 2>&1
```

Si no se ha producido ningún problema, ahora se puede dedicar algún tiempo para acabar de configurar y ajustar la página índice HTML. Una buena mejora consiste en incluir en la sección de cabecera de esta página un código <META .....> para obligar al visor web a recargar la información cada 300 segundos.

Otra mejora que se puede incluir en el fichero de configuración es la directiva WriteExpire, que fuerza a MRTG a crear ficheros ".meta" para cada fichero GIF y página HTML, eliminando innecesarias operaciones de "cache" tanto en los servidores proxy como en los propios visores web. Para ello también es necesario configurar el servidor

Apache (suponiendo que sea éste el servidor) para que lea estos ficheros ".meta" y envíe correctamente las cabeceras "Expire" con la directiva MetaDiren el fichero.
Se pueden encontrar más directivas en el fichero de configuración ejemplo que viene con la distribución; que por cierto, está muy bien documentado. Es posible modificar la disposición de las imágenes generadas por MRTG.

6.1.3 Otros Programas

Existe un programa similar llamado Router-Stats, escrito por Iain Lea, el autor del famoso programa lector de correo "tin". Router-Stats actualiza los gráficos una vez al día y muestra información estadística muy interesante sobre la utilización por horas y otros aspectos. El único problema es que se apoya en muchos programas externos. (SMU-SNMP para las tareas con SNMP, GNUPLOT para trazar gráficos, NetPBM y GIFTOOL para trabajar con gráficos).
Hay otra categoría de software que da un paso más allá en la tarea de gestión de redes, ofreciendo una solución completa tanto para monitorizar como para configurar toda la red. Este tipo de solución permite obtener una compleja representación gráfica de la red y ojear fácilmente los nodos que la componen, verificando detalles de configuración específicos y otras cuestiones de interés.
Pero por supuesto que existen soluciones disponibles públicamente con una funcionalidad más o menos similar. Uno de los paquetes que he encontrado es el Scotty. Scotty es un paquete basado en TCL que permite crear programas específicos a las necesidades de la red propia, empleando un API de alto nivel de cadenas de caracteres. Un paquete similar es el Tkined. Es un editor de red que ofrece extensiones para crear un entorno de trabajo completo, integrando algunas herramientas para localizar redes IP, soporte para el proceso de instalación de la red o resolución de problemas en redes IP utilizando SNMP en combinación con otras utilidades estándar (por ejemplo traceroute). Scotty también incluye un visor gráfico MIB que permite explorar fácilmente información MIB.

6.2 Aplicaciones Comerciales

Así como tenemos algunas aplicaciones libres que nos permiten descargar herramientas gratis de la Web y utilizarlas en la administración de redes, también tenemos aplicaciones comerciales de administración.

6.2.1 Active SNMP

Esta es una aplicación desarrollada en Java, por lo tanto puede correr en cualquier sistema operativo que cumpla con los requisitos mínimos. Ha sido desarrollada para proveernos una herramienta grafica fácil de usar sobre nuestra implementación SNMP, permitiéndonos además el acceso remoto a la información administrada. Ver Fig. 6.2

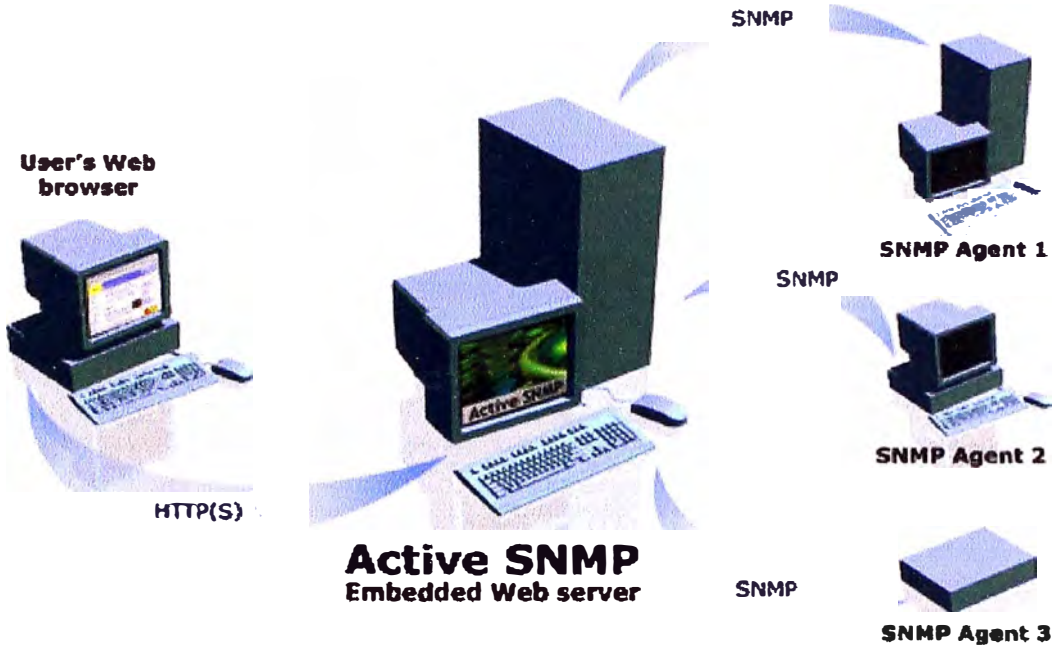


Fig. 6.2 red utilizando Active SNMP

Requisitos mínimos para su instalación:

- Cualquier sistema operativo pero que tenga instalado Java 2 Runtime Enviroment 1.4
- 60Mb libres de disco duro disponible para la instalación.
- Un Web browser que soporte frames, Java Script y CSS.

Instalación de Active SNMP:

Visto que esta aplicación corre sobre Java 2, veremos la instalación en los 2 sistemas operativos mas utilizados. La versión demo de esta aplicación la podemos descargar de: http://www.cscare.com/activesnmp/download.php

Instalación sobre Windows:

Descargamos la última versión del enlace que hemos dado y ejecutamos **ActiveSNMP30.exe**

Instalación sobre Linux:

Para esto descargamos la ultima versión en el enlace dado y instalamos el rpm **activeSNMP-3.0-0.i386.rpm**

Aqui mostramos algunas imágenes:

Buscando información:

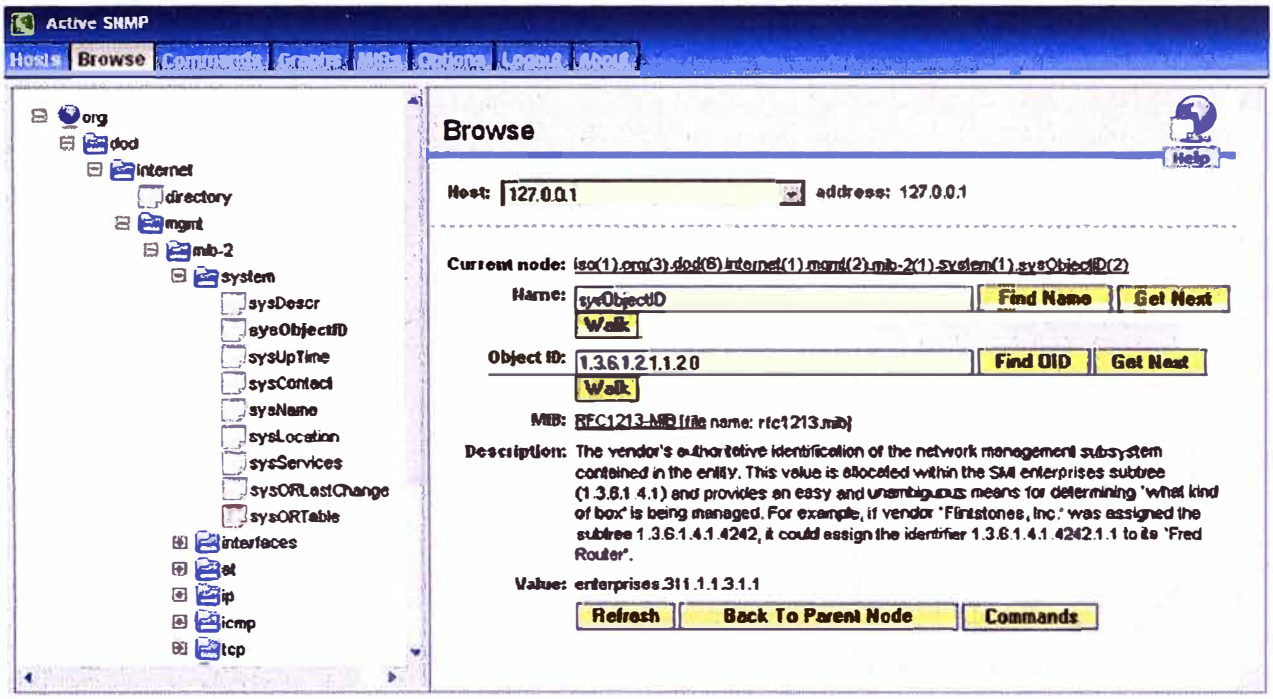


Fig. 6.3 Interfase de búsqueda de información en active SNMP

Administración de las MIBs:

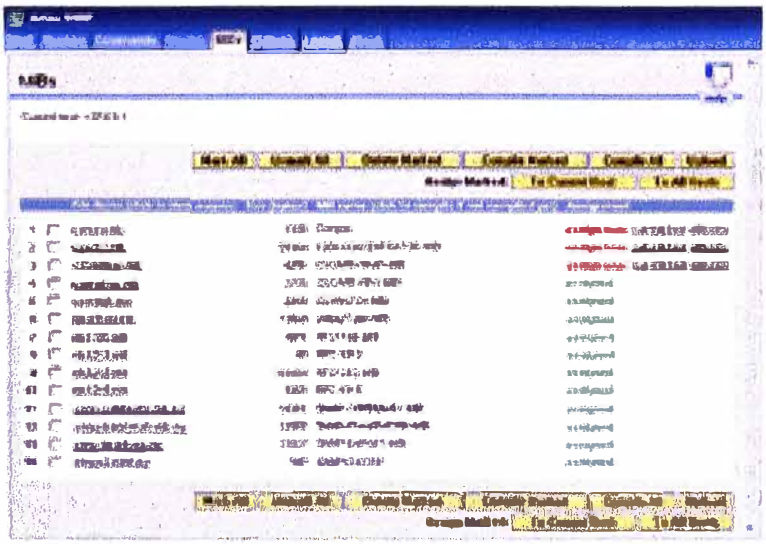


Fig. 6.4 Administración de las MIs

Mostrando información:

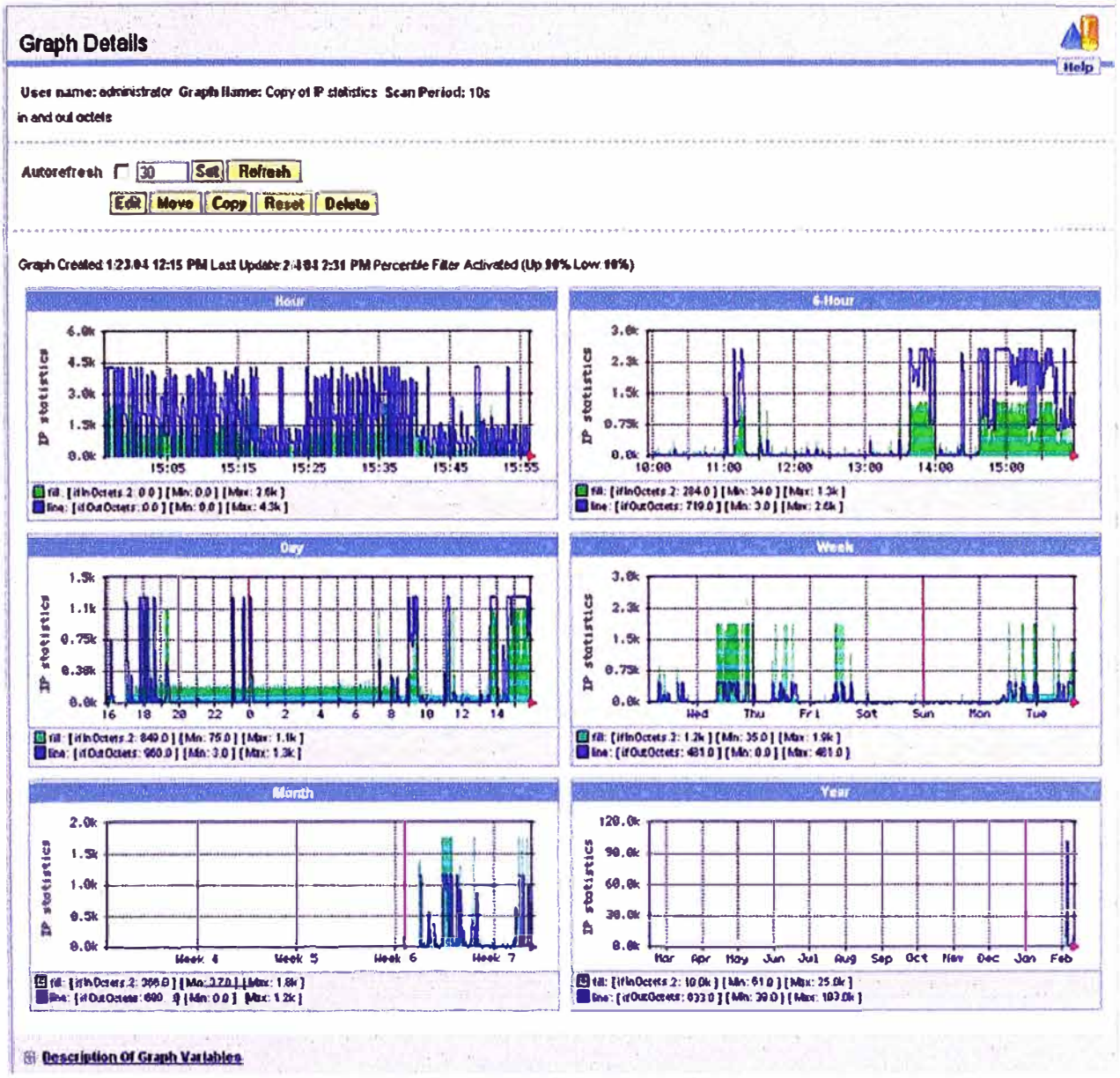


Fig. 6.5 Reporte generado por ActiveSNMP

CONCLUSIONES

1. Las redes de computadoras a medida que incrementan su tamaño (aumento del numero de usuarios, hardware y software), se hacen mas propensas a fallos que disminuyan su rendimiento.

2. La solución a problemas es muy variada y dependen principalmente de tener información adecuada en el momento correcto. Para esto necesitamos mecanismos que nos permitan intercambiar información de gestión entre los dispositivos que deseamos administrar.

3. El protocolo SNMP es un conjunto de especificaciones, para gestionar dispositivos en una red, bastante simple y requiere los mínimos recursos necesarios para realizar la gestión de red.

4. Como el protocolo SNMP requiere de pocos recursos de la red, lo hace un protocolo ligero y de uso extendido en reces de todos los tamaños.

5. Tanto CMIP o CMOT (CMIP sobre TCP/IP) son sistemas de gestión muy bien diseñados que hacen muchas mejoras a las deficiencias de SNMP, esto los hace sistemas completos pero grandes, en consecuencia solo pueden ser implementados en redes muy bien equipadas para ser soportados.

6. Podemos concluir que SNMP presenta las siguientes ventajas:

    - Como principal ventaja mencionaremos que es un protocolo ligero (la información de gestión que necesita intercambiar exige pocos recursos de la red) y fácil de implementar en redes de todos los tamaños.

    - Permite a los usuarios definir las variables que desea monitorear con solo definir:
        - El título de la variable.

- El tipo de datos de las variables.
- Si la variable es de solo lectura, escritura o ambos.
- El valor de la variable.

Esto hace que además sea también sencillo para el usuario (administrador de la red) la definición y administración de objetos en su red.

- Es el sistema con uso más extendido, su implementación sobre TCP/IP (la suite de protocolos de uso más extendido en las redes) mantienen su uso en todo tipo de redes. Esto hace que los fabricantes de switches, bridges, routers, etc. Se preocupen por incluir siempre soporte para este protocolo en sus equipos.
- Otra ventaja es su facilidad de expansión, debido a su sencillez es fácil de actualizar.

7. También podemos concluir las siguientes desventajas:

- Como primera desventaja podemos mencionar que SNMPv1 tienen grandes fallos de seguridad que pueden permitir a intrusos acceder a información que se intercambia en la red. Algunas de estas fallas fueron corregidas por SNMPv2 y luego SNMPv3.

- Una de sus mayores deficiencias es que por ser un estándar tan sencillo la información esta poco organizada. Esto se debe a que en sus inicios fue creado como un protocolo provisional. SNMPv2 soluciona algunos de estos inconvenientes al incluir una separación más detallada de variables y estructuras de datos que facilitan su manipulación.

8. En Internet encontramos soluciones de software libre que bien instaladas e implementadas nos permiten administrar nuestras redes con una mínima inversión económica.

BIBLIOGRAFIA

1. Andrew Tanenbaum, "Redes de Computadoras",
   Pearson Education de México, 2003

2. William Stallings, "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2",
   Diciembre 22, 1998

3. Peter J. Welcher "Configuring SNMP in CISCO routers", Netcraftsmen, http://www.netcraftsmen.net/welcher/papers/snmprouter.html

4. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid3, sitio Web de cisco donde se detalla SNMP

5. http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.html, Tutorial de SNMP, DPS Telecom

6. http://people.ee.ethz.ch/~oetiker/webtools/mrtg/, sitio web del MRTG TRAFIC ROUTER

7. http://www.boutell.com/lsm/lsmbyid.cgi/000030, sitio web para descargar CMU SNMP

8. http://www.cscare.com/activesnmp/features.php, sitio web de ACTIVE SNMP.