Administración de Redes

1.-Generalidades

Sabemos que las **redes de computadores ó redes digitales de comunicaciones** son:

- un **grupo de equipos digitales**(fundamentalmente computadores, pero hay otros con funciones específicas como repetidores, puentes, concentradores, enrutadores, etc).
- **unidos** entre sí por **medios físicos**(fibra óptica, cable de cobre trenzado[UTP,STP ó telefónico] ó cable coaxial) ó por **medios inalámbricos** (cada día más populares).
- que poseen un software llamado **protocolos de comunicaciones** que les permite compartir recursos de impresión, de comunicaciones, de bases de datos y otros, y/o implementar servicios de gran aceptación como correo electrónico, transferencia de archivos, conversación entre usuarios, telefonía, videoconferencia, juegos y muchos otros.

Estas redes pueden clasificarse de acuerdo a la distancia entre procesadores(hay otras clasificaciones: una en base a la conexión entre los equipos ó topología de la red[malla, anillo, estrella, mixta y jerárquica] y otra en base a la arquitectura[conmutadas y de difusión]) en LAN,MAN y WAN.

Por otra parte las redes, que generalmente comienzan como redes de área local (LANs), se **interconectan entre sí** dando lugar a las redes metropolitanas (MANs), y a las de área amplia (WAN) de donde deriva uno de los mayores logros del siglo XX y que sigue desarrollándose pujante en nuestro siglo XXI: **la red de redes ó Internet.**

Esta realidad se vive en diversos ámbitos, por ejemplo en una Universidad hay infinidad de redes que pertenecen a departamentos docentes, áreas de investigación, bibliotecas, areas administrativas docentes(control de estudios, decanatos, escuelas, etc) ó puramente administrativas (nómina, personal, seguros, previsión social, servicios médicos y odontológicos, servicio de farmacia, etc), diversas dependencias (Postgrado, Deportes, Seguridad, Extensión, Prensa, Radio, Televisión, etc), esas redes se integran entre sí, utilizando concentradores, switches, enrutadores, etc) en una MAN, que a su vez se conecta a través de una red interuniversitaria (WAN) a Internet. En las empresas según sean estas pequeñas,medianas ó grandes sucede algo similar : redes pequeñas que se interconectan entre sí, dando lugar a MANs y/o WANs y que a su vez todas se conectan a Internet.

Debido a la importancia de las redes normalmente uno ó más Ingenieros de Redes tienen la responsabilidad de planificarlas, instalarlas y **administrarlas**.

Obviamente estas redes, que surgen por el interés de los usuarios ó por política de la institución:

- son complejas tanto por el número y variedad de equipos y software, como por los medios físicos y/o inalámbricos utilizados y la organización necesita conocer donde están los equipos, que dirección tienen, como están interconectados, etc o sea conocer la **configuración** ó **mapa de la red**, y también contar con la posibilidad de poder **modificar remotamente**(desde una consola de control, por ejemplo) algún parámetro de los equipos que componen la red..
- la organización necesita conocer como se comporta la red, su **rendimiento** ó **desempeño**, a fin de saber el uso que se la da a la red: si hay congestión, si hay algún problema(como muchos paquetes multicast)que deba ser investigado, si el uso de la red está creciendo de modo tal que pronto colapsará, etc.

- también es necesario estar pendiente de las **fallas** que ocurran, estas deben ser detectadas cuanto antes, si es posible antes que los usuarios se den cuenta que existe una falla. Es deseable que muchas de las fallas puedan ser corregidas sin necesidad de ir hasta donde están los equipos haciendo uso de la consola, mencionada más arriba, que permite acceder **remotamente** a ellos.
- por otra parte la organización tiene gran interés en evitar el acceso malicioso de intrusos(hackers, crackers, espías, etc) a áreas de la red donde se encuentra información privada ó información que solo puede ser modificada por personal autorizado ó software vital para el funcionamiento de la red, etc. Entonces la **seguridad** de la red debe ser asegurada.
- como la red es un recurso compartido debe asegurarse un uso equitativo de ellos entre los usuarios, además en muchas redes los servicios se prestan con un fin comercial, por ello la organización debe contar con un sistema de **contabilidad** a fin de asegurar que cada usuario reciba el servicio de acuerdo a las normas convenidas y pague por el.

Estas tareas de: **configuración**, **rendimiento**, **fallas**, **seguridad** y **contabilidad** constituyen las áreas fundamentales de la **administración de redes** tal como las enumera OSI (ISO).

La **administración de redes**, que algunos autores denominan **manejo de la red** (por network management) ó **gerencia de la red**, es :

- Un conjunto de procesos para controlar una red de datos compleja.
- Quiere maximizar la eficacia y la productividad
- Engloba administración, organización y regulación
- Es clave para mejorar el funcionamiento
- Por qué administración?. Con el crecimiento indetenible de las redes, hay una multiplicación bienal de conexiones y aumento de la demanda en aplicaciones, protocolos y operaciones, que las convierten en más complejas cada día

Esta actividad de **administración de redes**, es cada vez más importante tanto debido a la complejidad actual de las redes, como a su necesidad de crecimiento racional y organizado, además es necesario **automatizar** estas actividades que además de complejas requieren de mucho tiempo y por si fuera poco, de respuestas rápidas.

En la redes donde no hay administración los administradores de la red (las personas responsables de la configuración, funcionamiento y crecimiento de la red) no tienen información precisa para su tarea, ignoran si sus instalaciones son eficaces y de costo razonable, no pueden medir la confiabilidad y disponibilidad de los equipos y de los servicios, las fallas son difíciles de identificar y corregir, especialmente si son intermitentes porque carecen de bases de datos sobre el cableado y equipos para poder detectar la causa de una falla y corregirla rápidamente, y no saben si las redes necesitan ampliación y en que medida.

Recuérdese además que las fallas son muy costosas y que en gran proporción son producidas por el cableado, además si una red colapsa por un crecimiento no previsto de su uso, la solución del problema es larga porque hay que estudiar: como crecerá la red, con qué tecnología, con qué equipos, de donde saldrán los recursos financieros y que impacto tendrá en la red actual el proceso de instalación de la nueva tecnología y de los nuevos equipos.

Téngase en cuenta que dependemos en tal medida de las redes que minutos, y no digamos horas y días, sin acceso a la red significa pérdidas enormes, ya que los usuarios se quedan sin saber que hacer para trabajar y mantener la organización funcionando, y generalmente todo se paraliza, con un drenaje considerable de tiempo, de dinero y hasta vidas como en el caso de hospitales, servicios de emergencia, seguridad y otros servicios críticos donde no se ha previsto redundancia ó enrutamientos alternativos rápidos en las redes respectivas.

A mediados de los 80 la OSI (**ISO**, **I**nternational **S**tandards **O**rganization) estableció las bases para **observar**, **controlar** y **coordinar** los recursos que se administran dentro de un **sistema abierto**[1]**.**

El **Marco de Administración de OSI**:

- ✓ Establece el modelo y las bases para todas las normas de administración, análogo al Modelo de Referencia de OSI.
- ✓ El paquete completo de normas se compone de:
  - la definición de terminología y de los conceptos de administración de OSI.
  - la especificación de un modelo abstracto y de la estructura de todos los propósitos de la administración.
  - la especificación de un protocolo de administración donde se incluyen todas las actividades administrativas.

El **marco de administración global de OSI** tiene tres componentes:

1. **Administración de sistemas**, administra todos los objetos controlados dentro del medio administrativo de OSI.
2. **Administración de niveles**, proporciona mecanismos de administración para los 7 niveles del modelo de capas de OSI y para su coordinación, asegura la integridad de los niveles individuales, los parámetros administrativos se pueden intercambiar y modificar sobre una base de igual a igual, y define funciones: parámetros del nivel de lectura, parámetros del nivel de modificación, comprobación activa de niveles y servicios de activación de niveles.
3. **Administración de protocolos**, lleva a cabo todas las funciones de control para transacciones individuales de comunicación en los niveles de protocolos.

De acuerdo a lo descripto en el inicio (y resaltado en azul) las **áreas de actuación en Administración de Redes(CPFSA** según sus siglas en inglés**)** son cinco:

- **Administración de Configuración(Configuration Managment).**
- **Administración de Rendimiento(Performance Managment).**
- **Administración de Fallas(Fault Managment).**
- **Administración de Seguridad(Security Managment).**
- **Administración de Contabilidad(Accounting Managment).**

Cada área tiene objetivos específicos, ellos son:

- **Administración de la Configuración:** monitorear la red y la información sobre la configuración del sistema para que los efectos de las diferentes versiones de hardware y software sobre el funcionamiento de la red puedan ser seguidos y administrados. Los subsistemas de administración de la configuración almacenan la información en bases de datos de fácil acceso: OS(Sistema Operativo), número de versión; interfaz Ethernet, número de versión; software de TCP/IP, número de versión; software de NFS, número de versión; software de SNMP, número de versión; etc.
  La Administración de la Configuración consiste en los siguientes pasos:
  1. Obtención de la información de la configuración actual de la red.
  2. Utilización de los datos para modificar la configuración de los dispositivos de la red.
  3. Guardar los datos, de manera de mantener un inventario de todos los componentes de la red y de ser capaz de producir informes.

[1] abierto significa no propietario, pues hasta ese momento solo existían sistemas de administración propietarios de los fabricantes de hardware.

- **Administración de Rendimiento:**
  Tiene como objetivo medir y hacer disponibles varios aspectos del funcionamiento de la red para que la interconexión pueda hacerse a niveles aceptables. Las variables de desempeño típicas son: rendimiento(network throughput) de la red, tiempo de respuesta del usuario, utilización de las líneas, etc.
  Generalmente involucra los siguientes pasos:
  1. Reúne los datos sobre las variables de interés.
  2. Analiza los datos para determinar los valores normales(línea de base).
  3. Determina los umbrales de funcionamiento adecuados para cada variable, de manera que el sobrepasar dichos umbrales implica que hay un problema en la red que debe ser atendido.
  4. Simulación de la red.

Se hace con **métodos reactivos ó proactivos**. En los **reactivos** cuando la función se hace inaceptable debido a que un usuario ha sobrepasado un umbral, el sistema reacciona enviando un mensaje al sistema de administración de la red, en los **proactivos** se utiliza simulación para evaluar los efectos del crecimiento de la red en los parámetros de desempeño.

- **Administración de Fallas:**
  Tiene como objetivos detectar, registrar, notificar a los usuarios y, si es posible, solucionar los problemas de la red automáticamente, con el fin de mantener un funcionamiento eficiente de la red.
  Envuelve los siguientes pasos:
  1. Determina los síntomas del problema.
  2. Aísla el problema.
  3. Soluciona el problema.
  4. Comprueba la reparación en todos los subsistemas que son importantes.
  5. Graba la detección del problema y la resolución.

- **Administración de Seguridad:**
  Tiene como objetivo controlar el acceso a los recursos de la red de acuerdo a lo establecido localmente de modo que la red no pueda ser saboteada y que no pueda accederse a información importante sin la debida autorización. Estos sistemas trabajan subdividiendo los recursos de la red en áreas autorizadas y áreas no autorizadas.
  No debe confundirse con la seguridad de los sistemas operativos que envuelva la instalación de archivos, directorios y programas de protección, ni con la seguridad física que tiene que ver con evitar el ingreso no autorizado a las áreas de los equipos, instalación de de tarjetas de acceso a los sitemas, bloqueo de teclados, etc.
  Envuelve los siguientes pasos:
  1. Identifica los recursos sensibles de la red.
  2. Determina correspondencia entre recursos sensibles de la red y series de usuarios.
  3. Monitorea los puntos de acceso a recursos sensibles de la red.
  4. Registra los accesos no autorizados a recursos sensibles de la red.

- **Administración de Contabilidad:**
  Tiene como objetivo medir los parámetros de utilización de la red de manera que el uso individual ó de grupos pueda ser regulado adecuadamente. Esta regulación minimiza los problemas de la red ya que los recursos pueden repartirse según la capacidad disponible y además mejora la imparcialidad en el acceso de los usuarios a la red.

Envuelve los siguientes pasos:

1. Mide la utilización de todos los recursos importantes de la red.
2. Analiza esos resultados para determinar los patrones ó estilos de utilización de la red. En base a esto pueden fijarse cuotas de utilización.
3. La medida del uso de los recursos permite facturar y asegurar una utilización óptima de los recursos.

2.-Herramientas de Administración de Redes.

En la última década gracias al advenimiento de computadores de gran capacidad de procesamiento y almacenamiento y de bajo costo, se han desarrollado herramientas muy eficaces para la administración de redes, comenzaremos por las más sencillas como **ping** y **traceroute** y luego veremos otras más complejas empezando por **SNMP v1** , hablaremos de **SNMP v2** y mencionaremos otras herramientas adicionales.

Ping: es una de las herramientas más utilizadas en la detección de fallas en redes que incluye dos mensajes: **solicitud de eco (echo request)** y **respuesta de eco (echo reply).** Ambos son mensajes ICMP (Internet Control Message Protocol) que es un protocolo parte de toda implementación de IP[2], y realizan esas simples tareas: "interrogan" a un equipo ubicado según su dirección IP mediante la solicitud de eco, y el equipo interrogado al recibir este mensaje responde con una respuesta de eco. Con este simple mecanismo puede determinarse si un destino es accesible ó nó y si responde.Como puede determinarse en tiempo que se tardó en responder esa información puede suministrarse al usuario, también pueden enviarse múltiples mensajes ICMP de solicitud de eco y proporcionar estadísticas sobre tiempo de respuesta y pérdida de paquetes.

Traceroute: es otra herramienta que hace envía una serie de mensajes UDP a una dirección IP y espera, si recibe respuesta ICMP puede trazar la ruta completa entre los dos puntos extremo (el que envió los mensajes y el destinatario cuya dirección IP se dio).

Las herramientas descriptas son simples y muy utilizadas pero limitadas,por ello se crearon otras más sofisticadas,veamos:

3.- SNMP

SNMP es un protocolo de la **capa de aplicación** de TCP/IP que constituye un estándar "de facto" para al administración de redes, es muy sencillo pero suficientemente potente para administrar redes heterogéneas y fue diseñado para facilitar el intercambio de información de administración entre los dispositivos de la red.

El **IAB**(**I**nternet **A**ctivities **B**oard), que es el Grupo de Supervisión de Internet, en 1988 desarrolló tres protocolos de administración de redes:

- Sistemas de Administración de Entidad de Alto Nivel (HEMS).
- Protocolo de Monitoreo de Entrada Simple (SGMP).
- Protcolo de Información de Administración Común (CMIP).

Luego de un corto tiempo el IAB tomó la decisión de poner en uso el protocolo SNMP, que está basado en SGMP, para ser usado en redes TCP/IP.

[2] ICMP es un mecanismo de reporte de errores y proporciona una forma para que los enrutadores que encuentren un error lo reporten a la fuente original. Cualquier máquina puede enviar un mensaje ICMP a cualquier otra máquina sea este enrutador ó máquina de extremo(host) y así comunicarse con ella.

Usando SNMP para acceder a los datos de información para administrar ó manejar la red (tales como paquetes por segundo, tasa de errores de la red, etc) los administradores de redes pueden administrar el rendimiento de la red, así como buscar y resolver problemas de red.

Hay dos versiones de SNMP, la versión 1 que es la original de SNMP, que fue desarrollada por *Case, McGlorie, Rose y Waldbuser,* y la versión 2 que incorpora: mejoras de seguridad, así como mejoras en las operaciones del protocolo y en la arquitectura de la administración.

4.- SNMP v1.

4.1.-Partes fundamentales del esquema cliente-servidor de administración SNMPv1.

Para que exista un **sistema de administración de redes**, es necesario contar con las piezas que lo constituirán bajo un esquema **cliente-servidor**, ellas son:

- **Objetos Administrados.**
- **Agentes de Administración.**
- **Sistemas de Manejo de Red (Network Managment System, NMS)**
- **Agentes Proxy.**

Objetos Administrados.

Los dispositivos de red que habitualmente se administran son dispositivos de hardware, ó **entidades físicas**, tales como puentes, enrutadores,switches, multiplexores, servidores y unidades de extremo (computadores ó estaciones de trabajo).

Un **Objeto Administrado (ó Gestionado)** es la **representación lógica** de una **entidad física de la red**, que contiene un nombre, así como propiedades y atributos que constituyen **variables**. Esas variables (por ejemplo dirección del nodo, tablas de enrutamiento, contadores de errores, etc) pueden ser **escalares**, que significa que hay una instancia, ó **tabular**, indicando que puede haber ninguna, una,dos ó más instancias.

De esta forma se representan los objetos administrados en la **Base de Datos de Información(MIB,** por **M**anagment **I**nformation **B**ase) que está en el **Sistema de Manejo de Red** que describiremos dentro de poco.

Agentes de Administración.

Dentro de cada **entidad física** existe un módulo de software **servidor**, llamado **Agente de Administración**, o simplemente **agente**, que captura,procesa los datos concernientes a los parámetros de red del dispositivo y los almacena en una **MIB** a la espera de alguna acción por parte del **Sistema de Manejo de Red.**

Sistemas de Manejo de Red (Network Managment System, NMS)

Una estación de trabajo llamada **Consola de Gestión** ó **Estación de Manejo**, cuenta con un módulo de software **cliente**, que proporciona funciones básicas de administración para una gran variedad de dispositivos de diversos fabricantes y además sirve de soporte para herramientas de administración más completas y específicas. Ademas cuenta con una **Base de Datos de Información (MIB**, por **M**anagment **I**nformation **B**ase), que es donde se almacenan los datos recogidos por los agentes.

Normalmente el software mencionado, que se denomina **Sistema de Manejo de Red**, interroga a los **agentes** y guarda las respuestas en la **MIB**.

Existen también MIB remotas llamadas **RMON** (**R**emote **MON**itoring) sobre las que volveremos más tarde.

Agentes Proxy

Algunos dispositivos no son capaces de ejecutar su propio agente. Un **Agente Proxy** es un dispositivo, al que aquellos están conectados en una topología estrella y que es capaz de ejecutar los agentes de tales dispositivos, proporcionándoles las funciones de SNMP.

La **Figura 1** muestra un arquitectura de un Sistema de Administración de Redes.

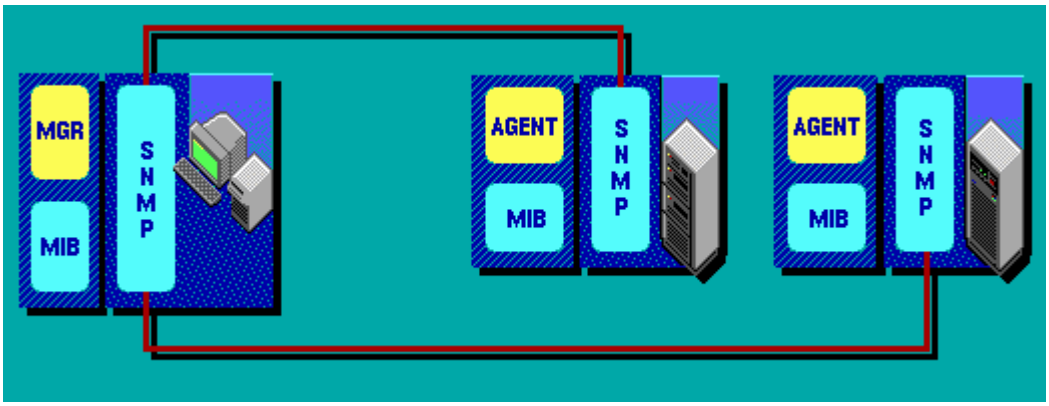

Figura 1. Sistema de Manejo(MGR),Base de Datos(MIB) y Agentes enlazados por SNMP.

Las funciones básicas de este **Sistema de Manejo de Red(MGR)** son:

- Interfáz gráfica de usuario(GUI), para facilitar el acceso al sistema de manejo.
- Mapa de la red. Es una representación gráfica de la misma donde se muestran los diferentes equipos, segmentos, subredes e interconexiones que conforman la red. El mapa sirva para localizar rápidamente cualquier evento, pues estos se reflejan en los íconos que representan los diferentes elementos como cambio de color.
- Base de Datos(MIB), ya descripta.
- Método estándar para interrogar los objetos administrados.
- Registro de eventos: cuando ocurre un evento el Sistema debe ser capaz de registrarlo.
- Interfaz con programas de aplicación(API), a fin de servirle de base a otras herramientas más complejas y/o específicas.
- Sistema de Seguridad: por su carácter delicado debe evitarse el acceso y/o modificación indefinida de los datos.

La **Arquitectura** de un Sistema de Administración de Redes(**SAR**) puede tomar tres variantes, (la primera de ellas es la de SNMP) :

- **Centralizada**, tiene el **Sistema de Manejo** en una sola estación de trabajo ubicada en un lugar establecido para labores de administración. Recibe todos los eventos y alertas de la red, toda la información de la red y provee acceso a todas las aplicaciones de administración.Tiene las ventajas de que los reportes están en un solo punto desde donde se administra toda la red, además desde el punto de vista de la seguridad es más fácil controlar el acceso a un solo punto. Como desventajas tenemos que por estar toda la información en una sola estación debemos efectuar respaldos frecuentes y su falla interrumpe las labores de administración, además consume más ancho de banda que otros sistemas por ser centralizado.
- **Jerárquica**, tiene un Sistema de Manejo **central** maestro donde residen algunas funciones de administración y Sistemas de Manejo **locales (RMON)** que colectan datos y luego los envían a la estación maestra, todo con la idea de distribuir funciones y ahorrar ancho de banda.
- **Distribuída**, usa múltiples sistemas de manejo(en diversas partes de la red) que funcionan como un sistema de administración igual a igual(peer to peer).

4.2.- Estructura de la Información de Administración(SMI, Structure of Managment Information) y MIB(Managment Information Base).

La esencia de un Sistema de Administración de redes es recolectar y modificar los valores de ciertos elementos ó variables de red.

Para que tanto los agentes como los sistemas de manejo y las aplicaciones se entiendan para el intercambio de datos debe haber un estándar que identifique cada una de las variables de la red, ese estándar es SMI.

La sintaxis para **identificar** las variables MIB está estandarizada por SMI que usa ANSI.1 (Abstract Syntax Notation One) y es una **secuencia de números decimales, separados por puntos, y jerarquizados en forma de árbol** para poder identificar cada una de las variables de red de manera normalizada.

Esa jerarquización en forma de árbol es similar al sistema de numeración telefónica, así por ejemplo veamos uno de esos árboles compuestos de **nodos**, que tienen un número que los identifica(por ejemplo iso (1)) y organizados jerarquicamente.

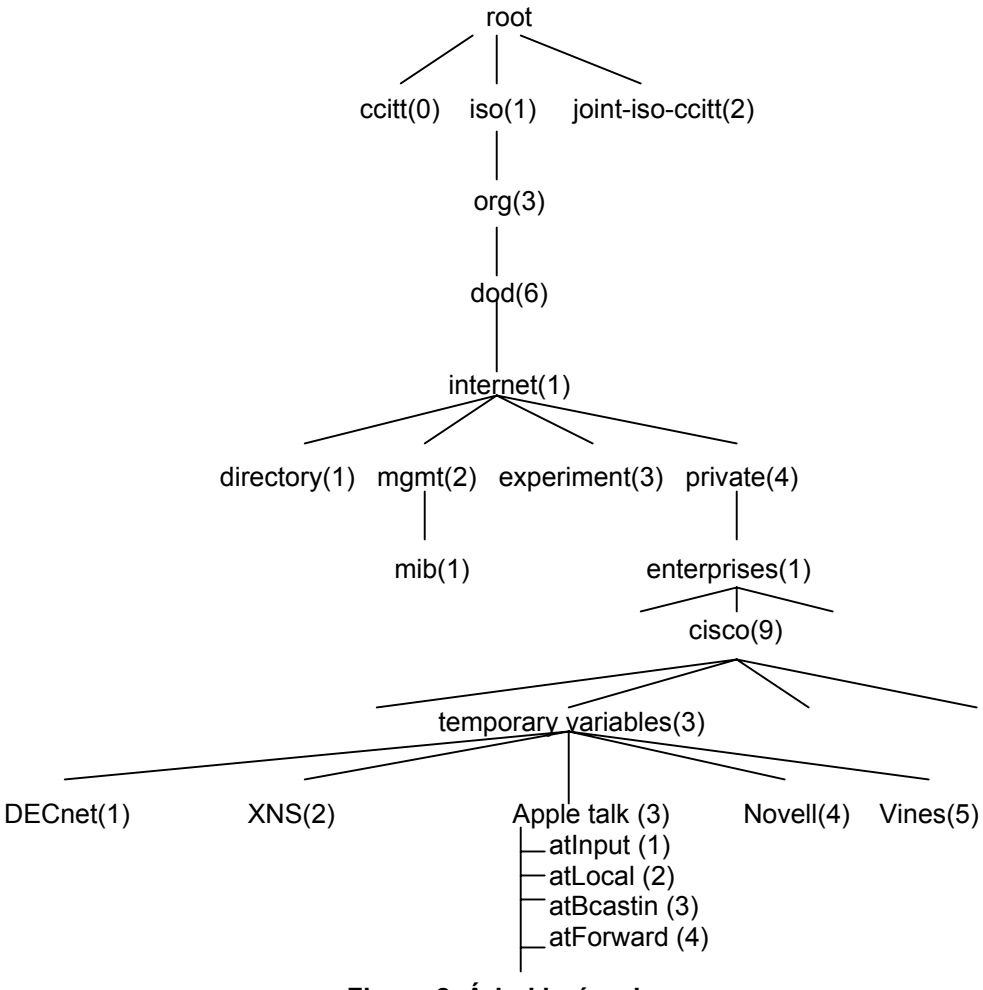

Figura 2. Árbol jerárquico

En este caso podemos decir que un objeto manejado **atInput** (escalar que dá el número de paquetes Appletalk entrantes a un enrutador Cisco) puede ser identificado por el **Identificador de Objetos(OID)** respectivo que viene dado por el **nombre del objeto: iso.org.dod.internet.private.enterprise.cisco.temporary variables.AppleTalk.atInput** ó por el **descriptor de objetos equivalente**, **1.3.6.1.4.1.9.3.3.1.**

Esto no termina aquí ccitt y joiny-iso-ccitt generan sus propios subárboles, lo mismo ocurre con iso, org, dod y los demás.

Además de identificar el objeto debemos dar el ó los datos respectivos, eso se hace también según la norma ASN.1 que define dos tipos de datos: **simples** y de **amplia aplicación**.

Los datos simples ASN.1 pueden ser : ENTEROS, OCTETOS, CADENAS DE CARACTERES e IDENTIFICADORES DE OBJETOS.

Los datos de **amplia aplicación** son de siete tipos:

- **Direcciones de red:** representan una dirección de una familia de protocolos en particular.SNMPv1 solo soporta direcciones IP de 32 bits.
- **Contadores**: son enteros positivos que se incrementan hasta alcanzar un valor máximo. El número total de bytes recibido en una interfaz es un ejemplo de un contador.
- **Gauges** (calibradores) : son enteros positivos que pueden incrementarse o decrementarse pero retienen el número máximo alcanzado. La longitud de la cola de espera(en número de paquetes) es un ejemplo.
- **Time ticks** : son centesimas de segundo desde que ocurre un evento. Un ejemplo es el tiempo que dura un interfaz en alcanzar el estado actual.
- **Opaque** : es una codificación arbitraria usada para pasar cadenas de información por medio del tipo de datos usado esctrictamente por SMI.
- **Enteros** : corresponden a enteros con signo.
- **Enteros sin signo** : corresponden a variables que solo pueden ser positivas.

La **Estructura de la Información de Administración (SMI)** se detalla en la **RFC** (**R**equest **F**or **C**omments) 1155.

4.3.-Tipos de mensajes SNMPv1.

SNMP tiene solo cinco tipos de mensajes que realizan operaciones muy sencillas pero suficientemente poderosas:

- **Get-request** : solicita la información de un objeto determinado del agente.
- **Get Next-request** : solicita información del próximo objeto desde una tabla o lista dentro de un agente.
- **Set-request** : establece valores de parámetros de un determinado objeto dentro de un agente.
- **Get-response** : es la respuesta del agente a Get-request,Get Next-request y Set-request.
- **Trap** .: informa de forma asíncrona (o sea por sí misma) a la estación de administración de red de algún evento. A diferencia de Get-request,Get Next-request y Set-request, el Trap no espera respuesta de la estación de administración.

Los primeros cuatro tipos de mensajes son UDP usando el puerto 161, mientras que cuando se habilita Trap los mensajes son UDP por puerto 162.

4.4.-Formato de los mensajes SNMPv1.

El formato de los mensajes SNMPv1 no tiene campos fijos y utilizan la codificación ASN.1 estándar y contiene tres partes;

- Número de la versión de protocolo.
- Un identificador *commnity* de SNMP (utilizada para reunir los enrutadores administrados por un solo administrador y también como forma alterna de autenticación para el acceso)
- Unidad de Datos del Protocolo ó PDU (Protocol Data Unit).

Estos datagramas UDP no necesitan ser mayores de 484 bytes, pero es recomendable que las implementaciones de este protocolo soporten longitudes mayores.

Obviamente hay cinco tipos de PDUs, uno para cada tipo de mensaje SNMP, sin embargo los cuatro primeros son similares, solo el PDU del Trap es muy diferente tal como muestra la **Figura 3**.

Formato del PDU para : Get-request,Get Next-request ,Set-request y Get-response.

ID de la Solicitud	Estado de error	Índice de error	Asociación de la variable

Formato del PDU para Trap

Empresa	Dirección del Agente	Tipo de Trap Génerico	Tipo de Trap Específico	Time Stamp	Asociación de la variable

Figura 3. Formatos de PDU.

Los formatos de PDU para los Request(Get-request,Get Next-request y Set-request) y para Get-response consisten en una solicitud (enviada por el cliente) (request) ó una respuesta (mandada por el servidor) (response) e incluyen:

- **ID de la solicitud(Request ID)** : Entero que indica el orden de emisión del datagrama y asocia una solicitud con una respuesta.
- **Estado de Error(Status Error)** : indica si ha existido un error y su tipo. Puede tomar los siguientes valores: noError(0) , tooBig(1), noSuchName(2) , badValue(3), readOnly(4) , genErr(5).
- **Indice de error(Error Index)** : Entero que en caso de error indica que variable de una lista ha generado el error.
- **Asociación de la Variable(VarBindList)** : Contiene los datos del PDU SNMPv1. Cada uno de estos campos asocia una variable con su valor actual(con excepción de Get y Get-next para los cuales se ignora su valor.

En el caso de un Trap los campos son los siguientes:

- **Empresa(Enterprise)** : Tipo de Objeto que ha generado el Trap.
- **Dirección del Agente(Agent-Addr)** : Dirección del Agente que ha generado el Trap.
- **Tipo de Trap Genérico(Generic-Trap)** : Entero que indica el tipo de Trap, puede tomar los siguientes valores; coldStart(0), warmstart(1), linkDown(2), linkUp(3), autenticationFailure(4), egpNeighborLoss(5), enterpriseSpecific(6).
- **Código Trap Específico(Specific Trap)** : Proporciona el código para un Trap específico.

- **Time Stamp** : Tiempo desde la última iniciación de la entidad de red y de la generación de ese Trap.
- **Asociación de la Variable(Variable Bindings)** : Lista tipo varBindList con información de posible interés.

Los Generic-Trap son muy interesantes pues indica condiciones de arranque, estado de los enlaces, fallas de autenticación, etc.

4.5.-Ejemplo de un Mensaje Codificado SNMPv1.

La codificación ASN.1 utiliza campos de longitud variable para representar los elementos. En general cada campo comienza con un encabezado que especifica el tipo de objeto y su longitud en octetos ó bytes, en la **Figura 4** se muestra la cadena de octetos codificados de un mensaje **Get-request** para elementos de datos **sysDescr** (identificador de objeto numérico 1.3.6.1.2.1.1.1)

30	29	02	01	00
SEQUENCE	len=41	INTEGER	len=1	vers=0

04	06	70	75	62	6C	69	63
string	len=6	p	u	b	l	i	c

A0	1C	02	04	05	AE	56	02
getreq	len=28	INTEGER	len=4	-------	request	ID	---------

02	01	00	02	01	00
INTEGER	len=1	status	INTEGER	len=1	error index

30	0E	30	0C	06	08
SEQUENCE	len=14	SEQUENCE	len=12	objectid	len=8

2B	06	01	02	01	01	01	01
1.3	. 6	. 1	. 2	. 1	. 1	. 1	. 1

05	00
null	len=0

Figura 4.- Forma codificada de un Get-request para el elemento de datos sysDescr con octetos que se muestran en exadecimal y con sus significados en la parte inferior de cada uno.Los octetos relacionados se han colocado en líneas, en los mensajes son contínuos.

El mensaje comienza con un código para SEQUENCE, luego dá la longitud: 41 octetos, sigue con tres octetos para la **versión**(uno especifica que es entero, otro su longitud y otro el número de la versión , 0 significa versión 1)

El campo siguiente es **community** donde se especifica que es literal, que tienen una longitud de 8 octetos y se dá public como palabra.

La **Get-request PDU** ocupa el resto del mensaje, el código inicial especifica una operación Get-request, debido a que el bit de orden superior está activado, la interpretación *depende del contexto*. Es decir el valor exadecimal A0 solo indica un Get-request PDU cuando se utiliza en un mensaje SNMP, no es un valor reservado universalmente. El octeto siguiente especifica la longitud de la solicitud(28 octetos). El ID de la solicitud es de 4 octetos, pero los estados de error y los índices de error son de un octeto. Luego contiene una asignación, un solo identificador de objeto unido a un valor *null*. El **identificador de objeto** está codificado como se espera salvo que las dos primeras etiquetas númericas están combinadas dentro de un solo octeto.

4.6.- Ventajas y desventajas de SNMPv1.

La ventaja fundamental de SNMPv1 es que su diseño es simple por lo que su implantación es sencilla en grandes redes y la información de administración que se necesite ocupa pocos recursos de la red.

Otra ventaja es que en la actualidad es el sistema más utilizado debido que durante mucho tiempo fue el único que existió y muchos fabricantes de puentes y enrutadores diseñan sus productos para soportarlo.

Además tiene la posibilidad de expensión por lo que es fácil de actualizar.

Como desventajas podemos citar;

Tiene graves fallas de seguridad pues puede permitir el acceso de intrusos a la información, y lo que es más estos pueden llegar a bloquear terminales.

Otro grave problema es que SNMPv1 es tan simple que la información está poco organizada, lo que no lo hace adecuado para administrar las grandes redes de hoy. Esto se debe a que fue un protocolo provisional que no ha sido sustituído.

5.-RMON.

Como se ha mencionado existe una arquitectura jerárquica de Administración de Redes con un Sistema Central de Manejo y Sistemas de Manejo Locales ó **RMON**, así se muestra en la **Figura 5.**

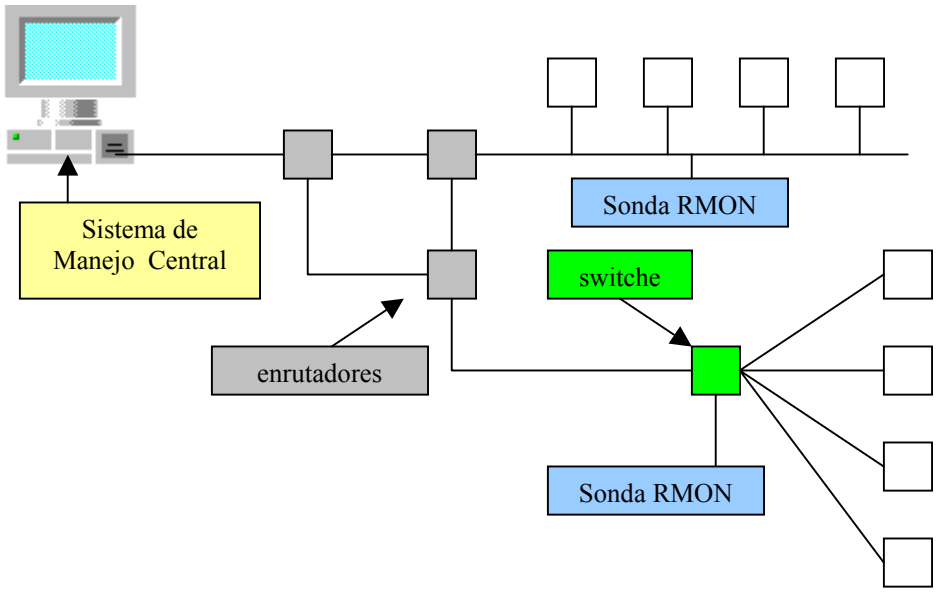

Figura 5. Estación de Manejo central y Estaciones de Manejo Remotas.

RMON (**R**emote **MON**itoring) es una herramienta de monitoreo remoto de redes definida en la **RFC** (**R**equest **F**or **C**omments) 1757 y antes publicada en la RFC 1271.

La **RMON MIB** ó Base de Información sobre Administración para el Monitoreo Remoto de Redes permite el diagnóstico de fallas de red más amplio, planificado y con características de rendimiento superiores a las anteriores soluciones de monitoreo.

En RMON se define un **dispositivo para el monitoreo remoto** llamado **sonda (probe)**, este dispositivo ó **sonda** purde tener su memoria, procesador y una interfaz de red, estos dedicados a la ejecución de las tareas relacionadas con la gestión de la red. La sonda uede tener interfaces en múltiples segmentos, y reunir los datos de cada uno en forma individual.

La ejecuación del monitoreo remoto implica que el dispositivo tenga sus interfaces "escuchando" cada una de las tramas en los segmentos de red donde se encuentra ubicado. Esto puede dar como resultado una disminución en el rendimiento de las interfaces de las estaciones de trabajo de la red, y acelera el impacto en el resto de los dispositivos en cuanto al rendimiento se refiere cuando sus interfaces se encuentran también en ese modo. Puede citarse el caso de un enrutador, normalmente este dispositivo lee solo el encabezado de una trama para determinar si requiere enrutamiento, sin embargo de ser él un dispositivo RMON, puede necesitar examinar la trama completa sin importarle si vá ó nó a ser enrutado. Existe la opción de colocar una sonda funcionalmente inteligente en el cableado de un concentrador (hub), este tipo de dispositivo está disponible por parte de varios fabricantes.

6.-SNMPv2.

SNMPv2 es una evolución de SNMPv1 derivada de dos especificaciones publicadas en Julio de 1992 : Secure SNMP y The Simple Managment Protocol.

Secure SNMP definió características de seguridad que no están disponibles en SNMPv1, pero Secure SNMP usó un formato de mensajes no compatible con SNMPv1.

Comparado con SNMPv1 SNMPv2 ofrece mayor flexibilidad en función de los recursos que éste puede manejar, el tamaño de la data transferida y el entorno en el cúal opera (redes OSI y otras arquitecturas además de redes TCP/IP). Un subconjunto de SNMP permite la capacidad de interoperar con SNMPv1.

SNMPv2 incluye mejoras en el SMI (incorpora nuevos tipos de datos e incluye una nueva convención para crear y borrar filas conceptuales en una tabla), en las operaciones de protocolo, en la arquitectura de la administración y en la seguridad.

BIBLIOGRAFÍA:

[1] Ponzo Roberto, Reyes Jesús,"Implementación de un Sistema de Administración y Supervisión para la red de datos de la Universidad de Carabobo basado en el modelo de Manejo de Redes de la OSI", Trabajo Especial de Grado UC 1998.
[2] Hsu John, "Computer Networks",Artech House, Capítulo 10.
[3] Comer Douglas, "TCP/IP",Prentice Hall, Capítulo 26.
[4] Herrera Nelquis, Estevez José, "Desarrollo de una aplicación para la administración de fallas en la red de la Facultad de Ingeniería basado en el modelo de manejo de redes de OSI",Trabajo Especial de Grado UC 2001 Sec. 3.5.6.

