Universidad Autónoma de Querétaro
Facultad de Informática

Tesina

SNMP: Protocolo Simple de Administración de Red

Que para obtener el título de
Licenciado en Informática

Presenta
Guadalupe Rivera Domínguez

Generación
1998-2002

Querétaro, Qro. Octubre de 2003

CARTA DE ACEPTACIÓN

Por este medio, se otorga constancia de aceptación de tesina para obtener el título de Licenciado en Informática, que presenta la pasante **GUADALUPE RIVERA DOMÍNGUEZ** con el tema denominado ***"Protocolo Simple de Administración de Redes (SNMP)".***

Este trabajo fue desarrollado como una investigación derivada del curso de titulación **"ADMINISTRACIÓN DE REDES CON WINDOWS 2000 SERVER",** dando cumplimiento a uno de los requisitos contemplados en el artículo 34 del reglamento de titulación vigente, en lo referente a la opción de titulación por realización y aprobación de cursos de actualización.

Se extiende la presente para los fines legales a que haya lugar y para su inclusión en todos los ejemplares impresos de la tesina, a los veinticuatro días del mes de septiembre del dos mil tres.

ATENTAMENTE

I.S.C. CÉSAR CONTRERAS GUERRERO
PROFR. CURSO DE TITULACIÓN

Agradecimientos

A Dios,

Por darme la vida y rodearme de seres tan especiales como mis padres, hermanas, amigos y Francisco. Además por permitirme la realización de un gran sueño.

A mis Padres Felipe y Rosa,

Por su amor y apoyo incondicional, paciencia, confianza y consejos basados en su experiencia, por todo aquello que me han demostrado haciéndome sentir una hija muy orgullosa de ustedes. Y por sus esfuerzos para brindarme lo mejor.

A mis hermanas Diana y Rosita,

Por su cariño y apoyo, pero sobre todo por comprender el tiempo que sacrifique ante ustedes dedicándolo a mi preparación.

A mi sobrinita Jacqueline,

A esa pequeñita que con su ternura e inocencia ha llenado de felicidad y motivación mi vida.

A mi novio Francisco,

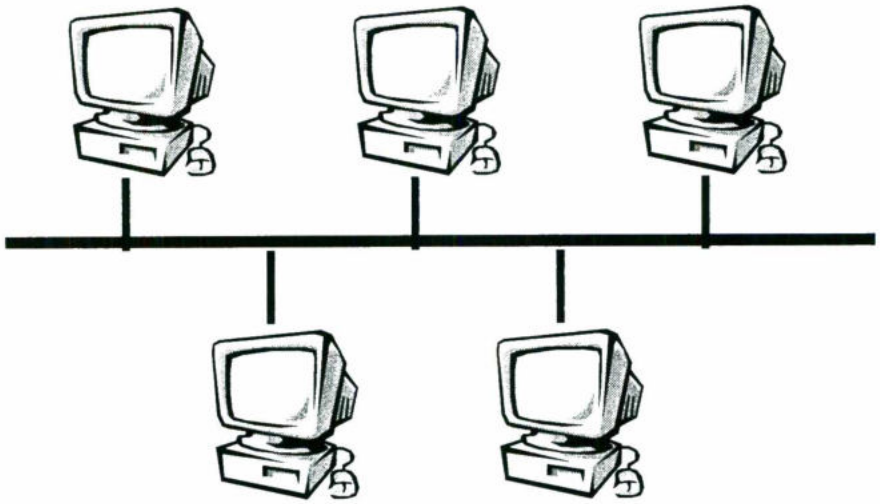
Por compartir este sueño lleno de alegrías y tristezas, desvelos y preocupaciones, pero ante todo de amor, confianza, motivación y apoyo.

A todos.... Gracias.

Índice

SNMP

Protocolo Simple de Administración de Redes



Presenta

Guadalupe Rivera Domínguez

1. Introducción

La proliferación de redes de datos a lo largo de la década de los 90, tanto LANs como WANs, y el interfuncionamiento entre ellas hace que los aspectos relativos a su control y gestión sean tomados en cuenta cada vez más, convirtiéndose en algo a lo que todos los responsables de redes han de prestar gran atención.

Dado que la tendencia natural de una red cualquiera es a crecer, conforme se añaden nuevas aplicaciones y más usuarios hacen uso de la misma, los sistemas de gestión empleados han de ser lo suficientemente flexibles para poder soportar los nuevos elementos que se van añadiendo, sin necesidad de realizar cambios drásticos en la misma.

Este punto, el de la administración de red, es uno de los más controvertidos en teleinformática, ya que, prácticamente, no existe una solución única, aceptada por todos y que sea fácilmente implantable. Las soluciones existentes suelen ser propietarias, por ejemplo: Netview de IBM, OpenView de HP, etc., lo que hace que en una red compleja, formada por equipos de múltiples fabricantes, no exista un único sistema capaz de realizar la gestión completa de la misma, necesitándose varias plataformas, una por cada fabricante, lo que dificulta y complica enormemente la labor del gestor de red.

Con la idea de presentar una solución única, válida para cualquier tipo de red, varios grupos de normalización están trabajando en ello y, aunque hay dos tendencias claras, sólo **SNMP** es la que está consiguiendo una aceptación e implantación amplia, a lo que ha contribuido su sencillez y rapidez de desarrollo.

Dentro del contenido principal de este documento se podrá encontrar toda la información necesaria para conocer a fondo sobre el Protocolo SNMP, su concepto, estructura, elementos básicos, el RFC que lo define, información acerca del SNMP versión 2, así como ventajas y desventajas sobre el uso del mismo.

2. Antecedentes de SNMP

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

En 1988 se implementó y comenzó a utilizarse un protocolo de gestión denominado SNMP (Simple Network Management Protocol), un protocolo sencillo para la gestión de red. Este protocolo ha sido muy aceptado desde entonces y la mayoría de los fabricantes lo implementan en sus equipos con protocolos TCP/IP.

El Protocolo Simple de Administración de Red (SNMP) es un protocolo de la capa de aplicación que facilita el intercambio de la información de la gerencia entre los dispositivos de la red. Es parte del protocolo de control Protocol/Internet de la transmisión (TCP/IP). El SNMP permite a administradores de la red manejar el funcionamiento de la red, encontrar y solucionar problemas de la red, y además de generar un plan para el crecimiento de la red.

El enfoque de gestión de red estándar consiste en considerar todos los elementos de red que se deben administrar (protocolos, puentes, pasarelas, etc.) como objetos gestionados. A cada objeto gestionado se asocia un conjunto definido de información relacionada con la gestión, la cual incluye variables (también llamadas atributos) que el gestor de red puede leer o modificar a través de la red. Dicha información contiene también, un conjunto de informes de fallos que un objeto gestionado envía cuando ocurre un fallo relacionado con él.

Existen dos versiones del SNMP: versión 1 (SNMPv1) del SNMP y versión 2 (SNMPv2) del SNMP. Ambas versiones tienen un número de características en común, pero son de mayor realce las características del SNMPv2, tales como operaciones adicionales del protocolo. La estandardización de otra versión del SNMP, versión 3 del SNMP (SNMPv3) está pendiente.

El SNMP facilita el intercambio de la información de la red entre los dispositivos.

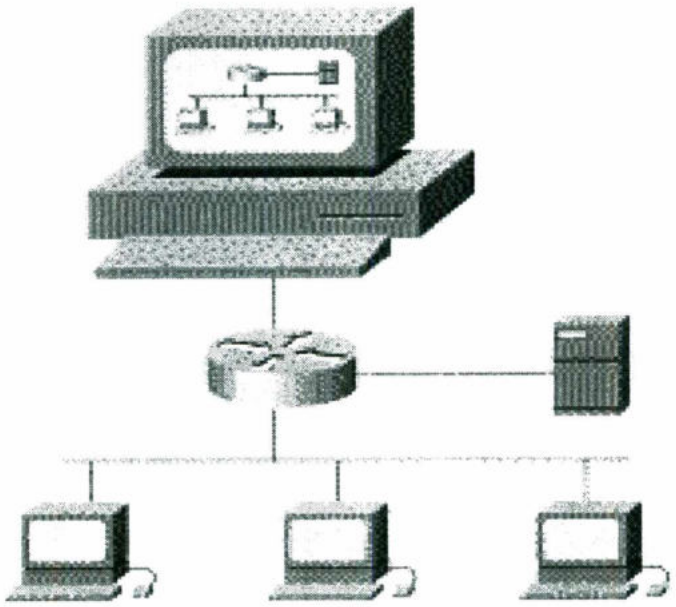


Figura 2.1: La figura ilustra una red básica manejada por SNMP.

2.1 Sistema de Gestión de Red

Un sistema de gestión de red es una colección de herramientas para monitorizar y controlar la red y que está integrado en los siguiente sentidos:

- ☑ Una interfaz de operador sencilla con un conjunto de órdenes potentes, pero agradables para el usuario, para llevar a cabo la mayoría o todas las tareas de gestión de red.

- ☑ Una cantidad mínima de equipo separado del sistema de gestión. Esto es, la mayor parte del hardware y el software requeridos para la gestión de red están incorporados en el equipo del usuario.

Un sistema de gestión de red consta de hardware extra y software adicional implementados entre los componentes de red existentes. El software se utiliza para efectuar las tareas de gestión de red que residen en los computadores y en los procesadores de comunicaciones (por ejemplo, procesadores frontales y controladores de grupo de terminales).

Un sistema de gestión de red está diseñado para ver la red entera como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto y los atributos específicos de cada elemento y enlace del sistema conocidos. Los elementos activos de la red proporcionan una realimentación regular de información de estado al centro de control de red.

Un sistema de gestión de red tiene los siguientes elementos clave:

- ☑ Estación de gestión o gestor.
- ☑ Agente.
- ☑ Base de información de gestión.
- ☑ Protocolo de gestión de red.

La **Estación de Gestión** es normalmente un dispositivo autónomo pero puede ser implementado en un sistema compartido. En cualquier caso, la estación de gestión sirve como interfaz entre el gestor de red humano y el sistema de gestión de red. La estación de gestión tendrá como mínimo:

- ☑ Un conjunto de aplicaciones de gestión para el análisis de los datos, recuperación de fallos, etc.
- ☑ Una interfaz a través de la cual el gestor de red puede monitorizar y controlar la red.
- ☑ La capacidad de trasladar los requisitos del gestor de red a la monitorización y control real de los elementos en la red.
- ☑ Una base de datos de información de gestión de red extraída de la bases de datos de todas las entidades gestionadas en la red.

El otro elemento activo es un sistema de gestión de red es el **Agente**. Las plataformas claves, como las computadoras, puentes, dispositivos de encaminamiento y concentradores se pueden equipar con software de agentes para que puedan ser gestionados desde la estación de gestión.

La colección de objetos se conoce como **Base de Información de Gestión MIB** (Management Information Base). La MIB funciona como una colección de puntos de accesos al agente por parte de la estación de gestión. Estos objetos están normalizados a través de los sistemas de una clase particular (por ejemplo, todos los puentes contienen los mismos objetos de gestión). La estación de gestión lleva a cabo la función de monitorización mediante el acceso a los valores de los objetos MIB. Una estación de gestión puede causar que una acción tenga efecto en un agente o pueda cambiar la configuración de un agente mediante la modificación de los valores de variables específicas.

La estación de gestión y el agente están enlazados por el **Protocolo de Gestión de Red**. El protocolo utilizado para la gestión en redes TCP/IP es el Protocolo Sencillo de Gestión de Red (SNMP). Para las redes basadas en OSI, se está desarrollando el protocolo de información de gestión común (CMIP, Common Management Information Protocol).

Una versión mejorada de SNMP, conocida como SNMPv2, está proyectada para ambos tipos de redes, basadas en OSI y en TCP/IP. Cada uno de estos protocolos incluye las siguientes capacidades clave:

- ☑ Get: permite a la estación de gestión obtener del agente los valores de objetos.
- ☑ Set: permite a la estación de gestión establecer valores de objetos del agente.
- ☑ Notify: permite a un agente notificar a una estación de gestión la producción de eventos significativos.

En un esquema tradicional de **gestión de red centralizado**, un computador en la configuración tiene el papel de estación de gestión; puede haber posiblemente una o dos estaciones de gestión con una misión de respaldo. El resto de los dispositivos en la red contiene software de agente y una MIB para permitir la monitorización y control por parte de la estación de gestión. Conforme las redes crecen en tamaño y en carga de tráfico, un sistema centralizado como el indicado no es práctico. Hay demasiada carga situada en la estación de gestión, y hay también mucho tráfico, con informes desde cada agente atravesando la red entera hasta llegar al punto central. En tales circunstancias, una técnica descentralizada y distribuida funciona de mejor forma.

En un **esquema descentralizado** de gestión de red, puede haber múltiples estaciones de gestión del nivel más alto, que se podrían denominar servidores de gestión. Cada uno de estos servidores podrían gestionar directamente una parte del conjunto total de agentes. Sin embargo, para muchos de estos agentes, el servidor de gestión delega la responsabilidad a un gestor intermedio. El gestor intermedio juega el papel de un gestor para monitorizar y controlar los agentes bajo su responsabilidad. También juega el papel de agente para proporcionar información y aceptar control desde un servidor de gestión de un nivel más alto. Este tipo de arquitectura dispersa la carga de procesamiento y reduce al tráfico total de la red.

3. SNMP – Protocolo Simple de Administración de Red

3.1 Concepto general

SNMP (Simple Network Management Protocol) :

El Protocolo de administración de redes se encuentra implementado en la capa de aplicación y pertenece al grupo de protocolos de TCP/IP. El SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

Es un estándar ampliamente aceptado para el manejo de dispositivos de red, incluidos adaptadores, switches, ruteadores, servidores y estaciones de trabajo.

El Protocolo Simple de Gestión de Red (SNMP) definido en el RFC 1157, no se ocupa de servicios de usuario, sino más bien de la gestión de todos los protocolos de comunicación dentro de cada sistema anfitrión y de los diversos elementos de equipos de red que proveen estos servicios, es decir, del entorno de red total.

Si en cualquier entorno de red ocurre un fallo y se interrumpe el servicio, los usuarios esperarán que el fallo se corrija y se restablezca el servicio normal con un mínimo de retardo. A esta función suele llamársele Gestión de Fallos. En forma análoga, si el rendimiento de la red, por ejemplo, su tiempo de respuesta o su volumen de transmisión comienza a variar como consecuencia de un aumento en el nivel de tráfico en algunas regiones de la red, los usuarios esperarán que dichas regiones se identifiquen y se introduzca equipo/capacidad de transmisión adicional para aliviar el problema. Éste es un ejemplo de Gestión de Rendimiento. El SNMP se definió para ayudar a un gestor de red a realizar las funciones de gestión de fallos y de rendimiento.

El enfoque de gestión de red consiste en considerar todos los elementos de red que se deben administrar (protocolos, puentes, pasarelas, etc.), como **objetos gestionados**. A cada objeto gestionado se asocia un conjunto definido de información relacionada con la gestión, la cual incluye variables, también llamadas atributos, que el gestor de red puede leer o modificar a través de la red. Dicha información contiene también un conjunto de **informes de fallos** que un objeto gestionado envía cuando ocurre un fallo relacionado con él.

El SNMP es un protocolo de aplicación, así que se debe utilizar una plataforma de comunicación estándar para hacer posible la transferencia de los mensajes, PDU, para ello, el SNMP suele utilizar TCP/IP. El esquema general es el que se ilustra en la figura 3.1.1.

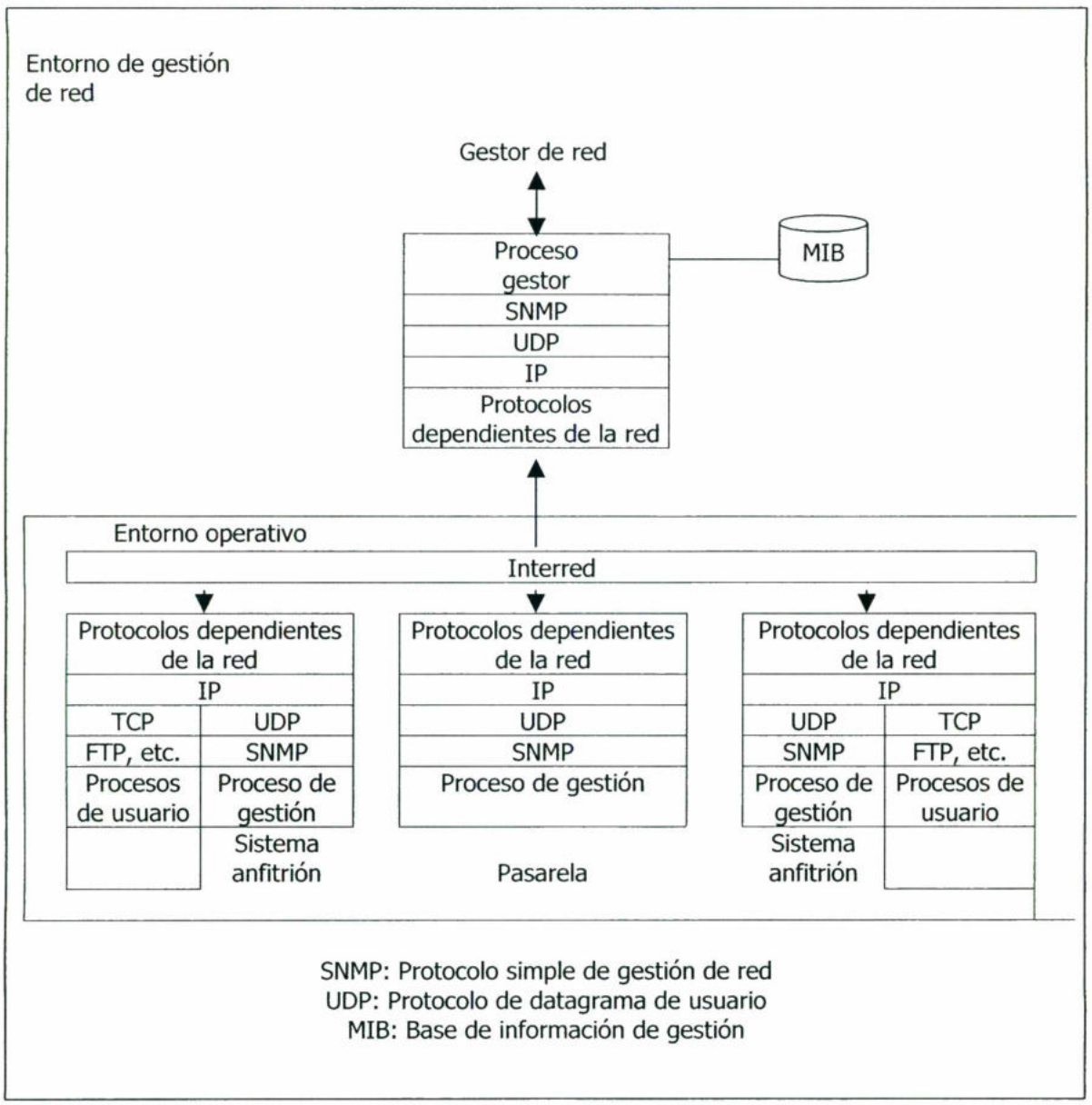


Figura 3.1.1 Software de gestión de red SNMP.

El papel del SNMP es permitir que el **Proceso Gestor** de la estación gestora intercambie mensajes relacionados con la gestión con los procesos de gestión que se ejecutan en los diversos elementos gestionados: sistemas anfitriones, pasarelas, etc. El proceso de gestión de estos elementos realiza las funciones administrativas asociadas a ellos; por ejemplo, responder a solicitudes de variables especificadas, recibir variables operativas actualizadas y generar y enviar informes de fallo.

La información de gestión asociada a una red/interred se mantiene en la estación (sistema anfitrión) del gestor de red en una **Base de Información de Gestión (MIB)**. El gestor de red cuenta con una variedad de servicios para consultar la información adicional, e iniciar cambios de configuración de la red. La estación gestora es el centro nervioso de toda la red, y por ello se implantan mecanismos de seguridad y de autenticación muy estrictos.

Debido a la amplia variedad de objetos por gestionar, la información de gestión con frecuencia se almacena en una Base de Datos Relacional, ya que la información que se mantienen para un solo objeto gestionado suele utilizarse en varias partes de la base de datos. En la figura 3.1.2 se ilustra una estructura jerárquica sencilla.

En la cima de la jerarquía está la interred, que consta de varias entidades mayores, como los servicios de directorio, los elementos de red y los servicios de seguridad. Entre los elementos de red están las redes, las pasarelas interiores y exteriores y, si intervienen subredes, enrutadores y puentes. En las hojas de las ramas están los objetos gestionados, cada uno de los cuales tienen un nombre único. Además, cada objeto tiene asociado un conjunto definido de variables/informes de fallo. Por todo lo anterior, una función primordial de la autoridad encargada de gestionar y controlar una interred consiste en definir la estructura, el llamado árbol de información de gestión y el contenido de la MIB.

Los objetos gestionados y por tanto la información de gestión asociados a una interred pueden variar de un sistema abierto a otro. Por ello, se ha definido el SNMP de modo que pueda recabar información de gestión en diversos entornos de red. Así, el significado de la información de gestión que se transfiere es transparente para el SNMP, el cual simplemente ofrece un conjunto definido de servicios, cada uno con su correspondiente conjunto de parámetros. Los distintos procesos de gestión interpretan la información o las órdenes recibidas de acuerdo con cierta definición.

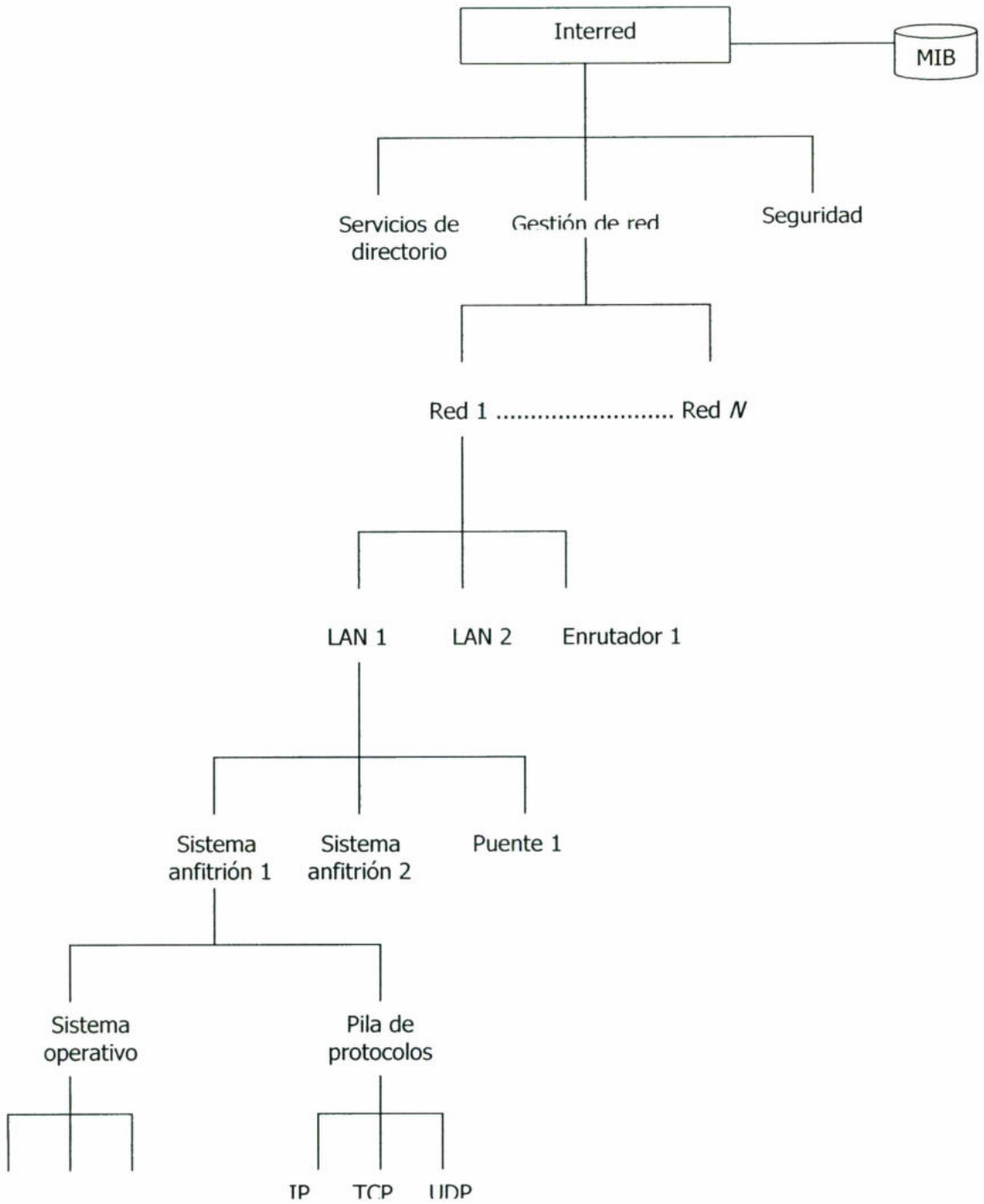


Figura 3.1.2 Jerarquía de objetos de gestión (árbol de información).

Los servicios de usuario/órdenes y las PDU correspondientes asociados al SNMP son del tipo procedimiento/operación remoto y por tanto son muy sencillos. El proceso gestor dispone de tres primitivas:

- ☑ **Get-request** (solicitud de obtener).
- ☑ **Get-next-request** (solicitud de obtener siguiente).
- ☑ **Set-request** (solicitud de fijar).

Y dos primitivas que están disponibles para el proceso de gestión (de agentes):

- ☑ **Get-response** (respuesta de obtención).
- ☑ **Trap** (atrapar).

Todos los mensajes (PDU) generados por el SNMP en respuesta a estas primitivas se intercambian mediante UDP y se definen en ASN.1. Las dos entidades de protocolo de SNMP no conservan información de estado, lo que significa que el proceso gestor puede tener varias solicitudes pendientes en espera de una respuesta. Por tanto, cada PDU GETrequest contiene un identificador de solicitud (requestID) que también aparece en la respuesta subsecuente y permite al proceso gestor de red relacionarla con una solicitud específica.

Con el crecimiento de tamaño y complejidad de las interredes basadas en TCP/IP, la necesidad de la administración de redes comienza a ser muy importante. El espacio de trabajo de la administración de redes actual para las interredes basadas en TCP/IP consiste en:

- ☑ **SMI** (RFC 1155) → describe cómo se definen los objetos administrados contenidos en el MIB.
- ☑ **MIB-II** (RFC 1213) → describe los objetos administrados contenidos en el MIB.
- ☑ **SNMP** (RFC 1098) → define el protocolo usado para administrar estos objetos.

El IAB emitió un RFC detallando su recomendación, que adoptó dos enfoques diferentes:

- ☑ A corto plazo debería usarse SNMP.

  IAB recomienda que todas las implementaciones IP y TCP sean redes que puedan administrarse. En el momento actual, esto implica la implementación de MIB-II Internet (RFC 1213), y al menos el protocolo de administración recomendado SNMP (RFC 1157).

- ☑ A largo plazo, se podría investigar el uso del protocolo de administración de redes OSI emergente: **CMIP (Protocolo de Información de Gestión Común)**. Cuando el CMIP se usa con un conjunto TCP/IP recibe el nombre de **CMIP sobre TCP/IP (CMOT).**

  SNMP y CMOT usan los mismos conceptos básicos en la descripción y definición de la administración de la información llamado **Estructura e Identificación de Gestión de Información** (SMI) descrito en el RFC 1155 y **Base de Información de Gestión** (MIB) descritos en el RFC 1156.

Por lo general, SNMP se utiliza como una aplicación cliente/servidor asincrónica, lo que significa que tanto el dispositivo administrado como el software servidor SNMP pueden generar un mensaje para el otro y esperar una respuesta, en caso de que haya que esperar una.

Ambos lo empaquetan y manejan el software para red (como el IP) como lo haría cualquier otro paquete. SNMP utiliza UDP como un protocolo de transporte de mensajes. El puerto 161 de UDP se utiliza para todos los mensajes, excepto para las trampas, que llegan el puerto 162 de UDP. Los agentes reciben sus mensajes del administrador a través del puerto UDP 161 del agente.

SNMP puede utilizarse para:

- ☑ **Configurar dispositivos remotos.** La información de configuración puede enviarse a cada host conectado a la red desde el sistema de administración.

- ☑ **Supervisar el rendimiento de la red.** Puede hacer un seguimiento de la velocidad de procesamiento y el rendimiento de la red, y recopilar información acerca de las transmisiones de datos.

- ☑ **Detectar errores en la red o accesos inadecuados.** Puede configurar las alarmas que se desencadenarán en los dispositivos de red cuando se produzcan ciertos sucesos. Cuando se dispara una alarma, el dispositivo envía un mensaje de suceso al sistema de administración. Entre las causas más frecuentes de alarma se incluye un dispositivo que se cierra y se reinicia, un error de un vínculo detectado en un enrutador y un acceso inadecuado.

- ☑ **Auditar el uso de la red.** Puede supervisar el uso general de la red para identificar el acceso de un grupo o usuario, y los tipos de uso de servicios y dispositivos de la red. Puede utilizar esta información para generar una facturación directa de las cuentas o para justificar los costos actuales de la red y los gastos planeados.

3.2 Componentes Básicos del SNMP

Una red administrada con SNMP consiste de tres componentes dominantes: **dispositivos**, **agentes** y **sistemas de gestión de red** (**NMSs**).

- ☑ Un **dispositivo manejado** es un nodo de red que contiene un agente del SNMP y que reside en una red administrada. Los dispositivos manejados recogen y almacenan la información de la gerencia y ponen esta información a disposición de los NMSs usando los dispositivos de SNMP. Los dispositivos manejados, a veces llamados elementos de la red, pueden ser servidores de acceso, interruptores y puentes o impresoras.

- ☑ Un **agente** es un módulo del software de la red manejada que reside en un dispositivo manejado. Un agente tiene conocimiento local de la información de la gerencia y traduce esa información a una forma compatible con el SNMP.

  Un agente es un computador que ejecuta el software de agente SNMP. La obligación principal de un agente es ejecutar las tareas iniciadas por los comando SNMP que han sido requeridas por el sistema de gestión de red.

Un agente no responderá a una solicitud de un sistema de gestión de red distinto a aquellos que tenga configurados (un agente puede pertenecer a varias comunidades a la vez).

☑ Los **Sistemas de Gestión de Red (NMS)** ejecutan el control que deberán manejar los dispositivos. NMSs proporciona el conjunto de recursos del proceso y de la memoria requeridos para la dirección de la red. Uno o más NMSs debe existir en cualquier red manejada.

Un sistema de gestión es un computador que ejecuta un software de administración SNMP.

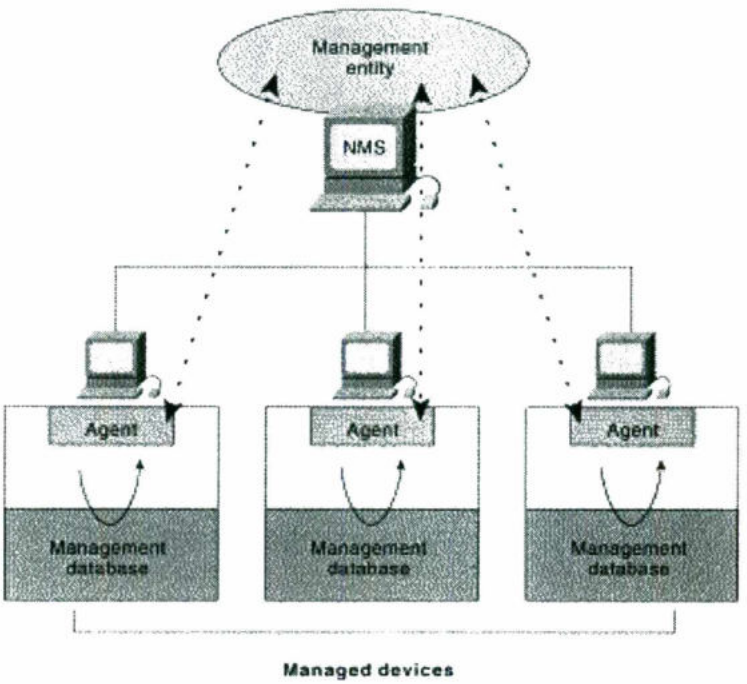


Figura 3.2.1: Ilustra las relaciones de estos tres componentes.

3.3 Comandos Básicos del SNMP

Los dispositivos manejados se supervisan y se controlan usando cuatro comandos básicos del SNMP: **lectura**, **escritura**, **trampa**, y las **operaciones traversal**.

- ☑ El **comando lectura** es utilizado por los NMSs para supervisar los dispositivos manejados. Los NMSs examinan diversas variables que son mantenidas por los dispositivos manejados.

- ☑ El **comando de escritura** es utilizado por los NMSs para controlar los dispositivos manejados. Los NMSs cambian los valores de las variables almacenadas dentro de los dispositivos manejados.

- ☑ El **comando de la trampa** es utilizado por los dispositivos manejados para divulgar acontecimientos a los NMSs. Cuando ocurren ciertos tipos de acontecimientos, un dispositivo manejado envía una trampa a los NMSs.

- ☑ Las **operaciones traversal** son utilizadas por los NMSs para determinar qué variables ayudan a manejar un dispositivo y recopilar secuencialmente la información en tablas variables, tales como una tabla de encaminamiento.

Los comandos SNMP que se utilizan pertenecen a los siguientes tipos:

- ☑ **GetRequest:**
  Lo utiliza el sistema de gestión para solicitar información a un agente.

- ☑ **GetNextRequest:**
  También es empleado por el sistema de gestión para solicitar información al agente y se utiliza si dicha información se encuentra en forma de tabla o matriz (se usa de forma repetitiva hasta que se hayan conseguido todos los datos de la matriz).

- **GetResponse:**
  El agente consultado utiliza este comando para contestar a una solicitud hecha por el sistema de gestión.

- **SetRequest:**
  El sistema de gestión lo utiliza para cambiar el valor de un parámetro de MIB.

- **Trap:**
  Lo utiliza un agente para informar al sistema de gestión de un suceso determinado que se ha producido.

3.4 Representación de Datos del SNMP

El SNMP debe explicar y ajustar las incompatibilidades entre los dispositivos manejados. Las computadoras utilizan diversas técnicas de la representación de datos que pueden comprometer la capacidad del SNMP para intercambiar la información entre los dispositivos manejados. El SNMP utiliza un subconjunto del **Abstract Syntax Notation One (ASN.1)** para acomodar la comunicación entre los diversos sistemas.

Característica:

- Define reglas para describir información de gestión
- Define la estructura de una MIB particular.
- Define cada objeto, la sintaxis y valor.
- Codifica el valor de los objetos.
- Representación común en la red (codificación)

Notación:

- **Tipo de datos:**
  Primitivos: Integer, octect string, object ID, Null, Sequence y Sequence of.
  De aplicación: networks addresses, counters, gauges, time ticks, opaques, integers, unsigned integers.
- **Construcción de un tipo:** NombreTipo::= tipo
- **Definición de valor de un tipo:** nombrevalor NombreTipo::= valor

Reglas de Codificación:

- ☑ La sintaxis distingue entre mayúsculas y minúsculas.
- ☑ Los nombres de *Tipo* empiezan con mayúsculas.
- ☑ Los nombres de los *Tipos Primitivos* se escriben con mayúsculas.
- ☑ Los nombres de *valores* y de los campos de un tipo estructurado se escriben con minúscula.
- ☑ El valor *nulo* se expresa con NULL.

Definición de Módulos:

NombreMódulo DEFINITIONS ::=
BEGIN
    Enlaces
    Declaraciones de tipos y estructuras
END

- ☑ Enlaces son utilizados para:
  Importación o exportar declaraciones de otros módulos o hacia otros módulos.

Macros:

La organización ISO proporciona al ASN.1 un mecanismo para hacer mas cómoda esta notación, que son las macros, estructuras que en si no añaden nada pero que establecen la definición de ciertas estructuras complejas. La definición de macros aporta una mayor flexibilidad a la sintaxis.

```
OBJECT-TYPE MACRO ::=
BEGIN
TYPE NOTATION ::=
      "Syntax" type(ObjectSyntax)
      "ACCESS" ACCESS
      "STATUS" Status
VALUE NOTATION ::= value (VALUE ObjectName)
      Access ::= "read-only" | "read-write" | "write-only" |
"not-accesible"
      Status ::= "ramdatory" | "optional" | "obsolete" |
"deprecated"
END

ObjectName ::= OBJECT IDENTIFIER
ObjectSintax ::= CHOICE {simple simplesintax,
                         Application-wide AplicationSyntax}

SimpleSintax ::= CHOICE {number INTEGER, string OCTET STRING,
                     Object OBJECT IDENTIFIER, empty NULL}
ApplicationSintaxt ::= CHOICE {address NetworkAddress, counter
Counter, gauge Gauge, ticks Timeticks, arbitrary Opaque}
```

Figura 3.4.1: Macro utilizada para definir objetos de MIB's (RFC 1155)

Reglas de Codificación (BER)

- ☑ BER (Basic Encode Rules) define cómo codificar los valores definidos en ASN.1 para ser transmitidos.
- ☑ La codificación de cada campo consta de tres o cuatro campos:
- ☑ Tipo: etiqueta que identifica el valor.
- ☑ Longitud: del valor en octetos.
- ☑ Valor: codificado según el tipo.
- ☑ Marca de fin de valor: si la longitud es indefinida.
- ☑ Se utiliza la siguiente notación: valores expresados en hexadecimal, cada octeto se separa por un espacio en blanco.

3.5 MIB – Management Information Base del SNMP

Una **Base de Información de Gestión (MIB)** es una colección de la información que se organiza de manera jerárquica. El MIB es accesado con un protocolo de gestión de red tal como SNMP. Se componen de objetos manejados y son reconocidos por los identificadores del objeto. Un objeto manejado (a veces llamado un objeto del MIB o un MIB) cumple con cualquiera de las características específicas de un dispositivo manejado. Los objetos manejados se componen de unos o más casos del objeto, que son esencialmente variables.

Existen dos tipos de objetos manejados: escalar y tabular.

- ☑ **Los objetos escalares** definen un solo caso del objeto.
- ☑ **Los objetos tabulares** definen los casos relacionados múltiples del objeto que se agrupan en tablas del MIB.

Un ejemplo de un objeto manejado es el **atInput**, que es un objeto escalar que contiene un solo caso del objeto, el valor del número entero que indica el número total de los paquetes de Appletalk de la entrada en una interfaz.

Un identificador del objeto reconoce únicamente un objeto manejado en la jerarquía del MIB. La jerarquía del MIB se puede representar como un árbol con una raíz sin nombre, los niveles de la cual son asignados por diversas organizaciones. La figura 3.5.1 ilustra el árbol del MIB.

Las identificaciones a nivel superior del objeto del MIB pertenecen a diversas organizaciones de estándares, mientras que las identificaciones de nivel inferior del objeto son asignadas por organizaciones asociadas.

Los vendedores pueden definir los ramas privadas que incluyen los objetos manejados para sus propios productos. MIBs que no se han estandardizado típicamente se coloca en el rama experimental.

El atInput manejado del objeto se puede identificar únicamente por el nombre del objeto:

iso.identified-organization.dod.internet.private.enterprise.cisco.temporary variables .AppleTalk.atInput

o por el descriptor equivalente del objeto: 1,3,6,1,4,1,9,3,3,1.

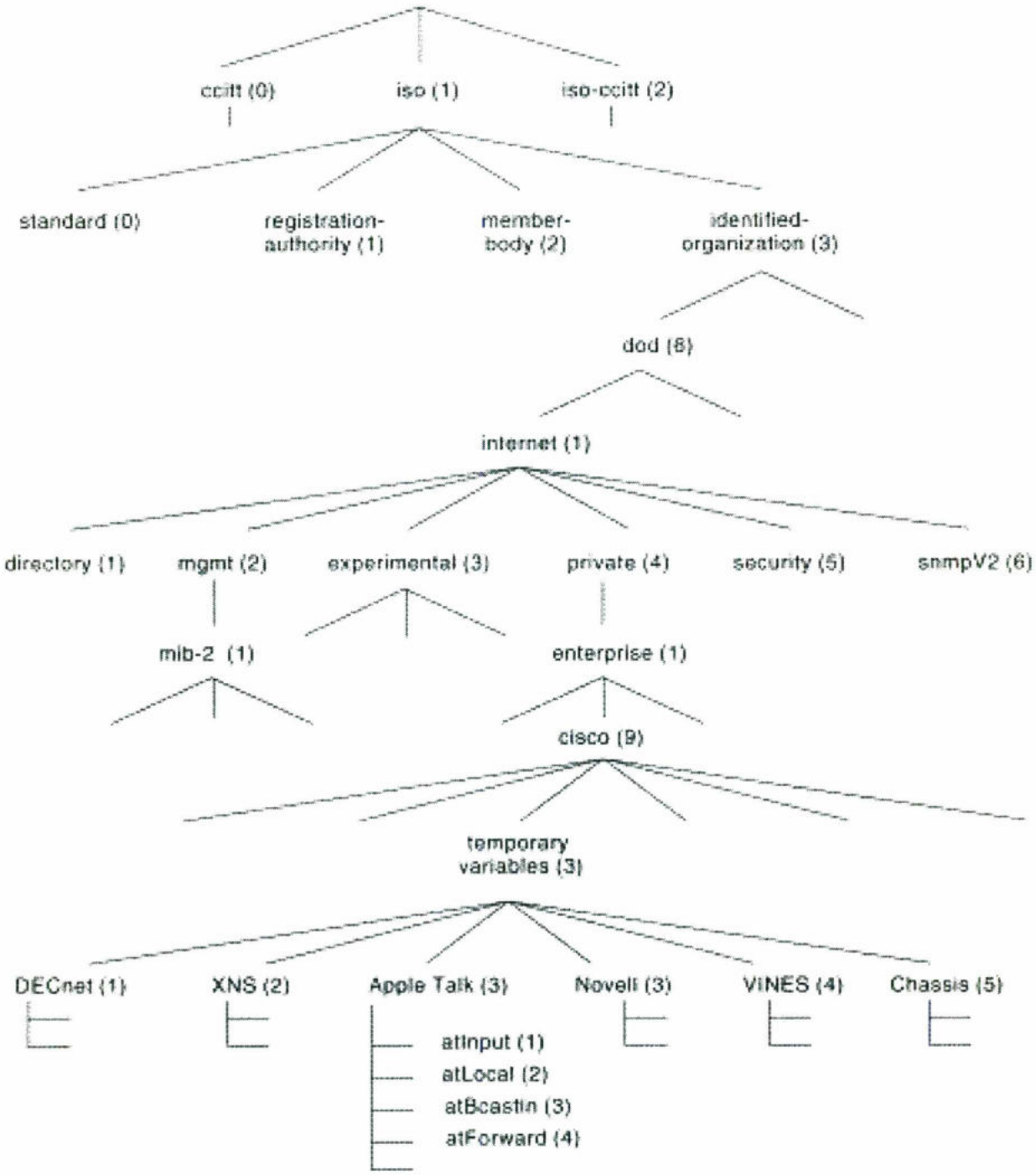


Figura 3.5.1: El árbol del MIB ilustra las varias jerarquías asignadas por diferentes organizaciones.

MIB registra y almacena información sobre el computador en el que se está ejecutando. Un administrador SNMP puede solicitar y recoger información de un agente MIB así como revisar o alterar los objetos que contiene.

El servicio SNMP de Microsoft soporta los siguiente valores MIB:

- ☑ **Internet MIB II**.

  Es un conjunto mejorado de Internet MIB I (base de datos estándar) que define varios objetos esenciales para controlar cualquier fallo o análisis de la configuración. Su documentación oficial está descrita en el RFC 1213.

- ☑ **LAN Manager MIB II**.

  Define varios objetos diseñados de forma específica para computadores con Windows 2000 tales como sesiones, información de las conexiones, usuarios, comparticiones, etc.

- ☑ **DHCP MIB**.

  Define varios objetos para controlar la actividad de un servidor DHCP.

- ☑ **WINS MIB**.

  Define varios objetos para controlar la actividad de un servidor WINS.

4. Versión 1 del SNMP

La versión 1 (SNMPv1) del SNMP es la puesta en práctica inicial del protocolo del SNMP. Se describe en el Request For Comments (RFC) 1157 y tiene funciones dentro de lo especificado de la Estructura e Identificación de Gestión de Información (Structure of Management Information, SMI).

SNMPv1 funciona con protocolos tales como User Datagram Protocol (UDP), Protocolo de Internet (IP), el servicio de red sin conexión de la OSI (CLNS) y el intercambio del paquete de Internet de Novell (IPX). SNMPv1 se utiliza de manera extensa en la red gestionada dentro de la comunidad del Internet.

La forma en que actúa el protocolo SNMP es la siguiente:

1. El sistema de administración envía primero una solicitud al agente para obtener el valor de una variable de MIB.

2. El agente contesta a la solicitud en función del nombre de la comunidad que acompaña a la solicitud.

Una comunidad comprende un grupo de computadores que ejecutan el servicio SNMP. El uso de un nombre de comunidad proporciona una seguridad mínima para los agentes que reciben solicitudes e inician capturas (traps) así como para las tareas iniciadas por los sistemas de gestión.

4.1 SMI – Structure of Management Information

La **Estructura e Identificación de Gestión de Información** (SMI) define las reglas para describir la información gestionada, usando el Abstract Syntax Notation One (ASN.1). El SMI del SNMPv1 se define en RFC 1155.

El SMI hace tres especificaciones dominantes: Tipos de datos ASN.1, tipos de datos SMI-específicos y tablas del MIB del SNMP.

☑ Siete tipos de datos de aplicación amplia existen en el SMI SNMPv1: direcciones de red, contadores, calibradores, señales del tiempo, números enteros, oscuros y enteros sin signo.

1. Las direcciones de red representan una dirección de una familia particular del protocolo. SNMPv1 apoya solamente direcciones 32-bit del IP.

2. Los contadores son los números enteros no negativos que aumentan hasta que alcanzan un valor máximo y después vuelven a cero. En SNMPv1, se especifica un tamaño contrario 32-bit.

3. Los calibradores son los números enteros no negativos que pueden aumentar o disminuir pero que conserve el valor máximo alcanzado.

4. Una señal del tiempo representa un centésimo de un segundo desde un cierto acontecimiento.

5. Un oscuro representa una codificación arbitraria que se utiliza para pasar las secuencias arbitrarias de la información que no se conforman con mecanografiar los datos usados por el SMI.

6. Un número entero representa la información número-valorada firmada. Este tipo de dato redefine el tipo de dato del número entero, que tiene la precisión arbitraria en ASN.1 pero precisión limitada en el SMI.

7. Un entero sin signo representa la información número-valorada sin firmar y es útil cuando los valores son siempre no negativos. Este tipo de dato redefine el tipo de dato del número entero, que tiene la precisión arbitraria en ASN.1 pero precisión limitada en el SMI.

Tablas del MIB del SNMP

El SMI del SNMPv1 define las tablas altamente estructuradas que se utilizan para agrupar los casos de un objeto tabular (es decir, un objeto que contiene variables múltiples). Las tablas se componen de cero o más fila, que se ponen en un índice de una manera que permita que el SNMP recupere o altere una fila entera con un solo **Get** , **GetNext** o el comando **Set**.

4.2 Operaciones del Protocolo SNMPv1

El SNMP es un protocolo simple de request/response. El sistema de la red gestionada publica una petición y una respuesta de vuelta, manejadas por los dispositivos. Este comportamiento es puesto en ejecución usando una de cuatro operaciones del protocolo: Get, GetNext, Set y Trampa.

- ☑ La operación de **Get** es utilizada por los NMSs para recuperar el valor de unos o más casos del objeto de un agente. Si el agente que responde a la operación del conseguir no puede proporcionar los valores para todo el objeto cita como ejemplo en una lista, él no proporciona ningunos valores.

- ☑ La operación de **GetNext** es utilizada por los NMSs para recuperar el valor del caso siguiente del objeto en una tabla o una lista dentro de un agente.

- ☑ La operación del **Set** es utilizada por los NMSs para fijar los valores de los casos del objeto dentro de un agente.

- ☑ La operación de la **Trampa** es utilizada por los agentes asíncronos para informar a los NMSs un acontecimiento significativo.

4.3 Ventajas del Protocolo SNMPv1

SNMP minimiza el número y la complejidad de las funciones realizadas por el administrador y cuenta con las siguientes ventajas:

- ☑ Reduce el coste de desarrollo del software del agente de administración necesario para soportar este protocolo.

- ☑ Aumenta el grado de las funciones de administración utilizadas de forma remota, permitiendo un uso completo de los recursos de Internet en dichas tareas.

- ☑ Permite que las funciones de administración sean de fácil comprensión y uso por parte de los desarrolladores de herramientas de administración de la red.

5. Versión 2 del SNMP

Con una utilización tan amplia, las deficiencias de SNMP han llegado a ser bastante aparentes; éstas incluyen deficiencias funcionales y la falta de una herramienta de seguridad. Como resultado en 1993 se publicó una versión mejorada, conocida como SNMPv2.

La versión 2 del SNMP es una evolución de la versión inicial SNMPv1. Originalmente, SNMPv2 fue publicada como sistema de estándares propuestos del Internet en 1993; actualmente, es un estándar de bosquejo. Como con SNMPv1, SNMPv2 funciona dentro de lo especificado en la Estructura e Identificación de Gestión de Información (SMI).

En teoría, SNMPv2 ofrece un gran número de mejoras a SNMPv1, incluyendo operaciones adicionales del protocolo.

SNMP v2 añade algunas nuevas posibilidades a la versión anterior de SNMP, de las cuales, la más útil para los servidores es la operación **get-bulk.** Ésta permite que se envíen un gran número de entradas MIB en un solo mensaje, en lugar de requerir múltiples consultas **get-next** para SNMP v1.

Además, SNMP v2 tiene mucho mejor seguridad que SNMP v1, evitando que los intrusos observen el estado o la condición de los dispositivos administrados. Tanto la encriptación como la autentificación están soportadas por SNMP v2.

Es una herramienta sencilla para la gestión de red. Define una base de información de gestión (MIB) limitada y fácil de implementar de variables escalares y tablas de dos dimensiones, y define un protocolo para permitir a un gestor obtener y establecer variables MIB y para permitir a un agente emitir notificaciones no solicitadas, llamadas intercepciones (traps). Esta simplicidad es la potencia de SNMP. Se implementa de una forma fácil y consume un tiempo modesto del procesador y de recursos de red. También, la estructura del protocolo y de la MIB es suficientemente directa de forma que no es difícil alcanzar la interacción entre estaciones de gestión y software de agente de varios vendedores.

Tipos de datos ASN.1

El SMI del SNMPv1 especifica que todos los objetos manejados tienen cierto subconjunto de tipos de datos del Abstract Syntax Notation One (ASN.1) asociados a ellos. Se requieren tres tipos de datos ASN.1: **nombre, sintaxis, y codificación**.

- ☑ Los servicios del **nombre** funcionan como el identificador del objeto.
- ☑ La **sintaxis** define el tipo de datos del objeto (por ejemplo, número entero o secuencia). El SMI utiliza un subconjunto de las definiciones de la sintaxis ASN.1.
- ☑ Los datos de **codificación** describen cómo la información asociada a un objeto manejado se ajusta a un formato como serie de artículos de datos para la transmisión sobre la red.

Tipos de datos SMI-Específicos

El SMI del SNMPv1 especifica el uso de un número de tipos de datos SMI-específicos, que se dividen en dos categorías: **tipos de datos simples** y **tipos de datos de aplicación amplia.**

- ☑ Tres tipos de datos simples se definen en el SMI del SNMPv1, que son valores únicos: números enteros, secuencias del octeto e identificaciones del objeto.

  1. El tipo de dato del número entero es un entero con signo en la gama de -2.147.483.648 a 2.147.483.647.
  2. Las secuencias del octeto son secuencias pedidas de 0 a 65.535 octetos.
  3. Las identificaciones del objeto vienen del sistema de todos los identificadores del objeto asignados según las reglas especificadas en ASN.1.

5.1 Elementos de SNMPv2

SNMPv2 no proporciona gestión de red. En lugar de eso SNMPv2 proporciona un marco de trabajo en el que se pueden construir aplicaciones de gestión de red. Estas aplicaciones, como la gestión de fallos, monitorización de rendimiento, contabilización de tiempo, etc. están fuera del ámbito del estándar.

Lo que proporciona SNMPv2 es la infraestructura de la gestión de red. La figura 5.1.1 es un ejemplo de una configuración que muestra esta infraestructura.

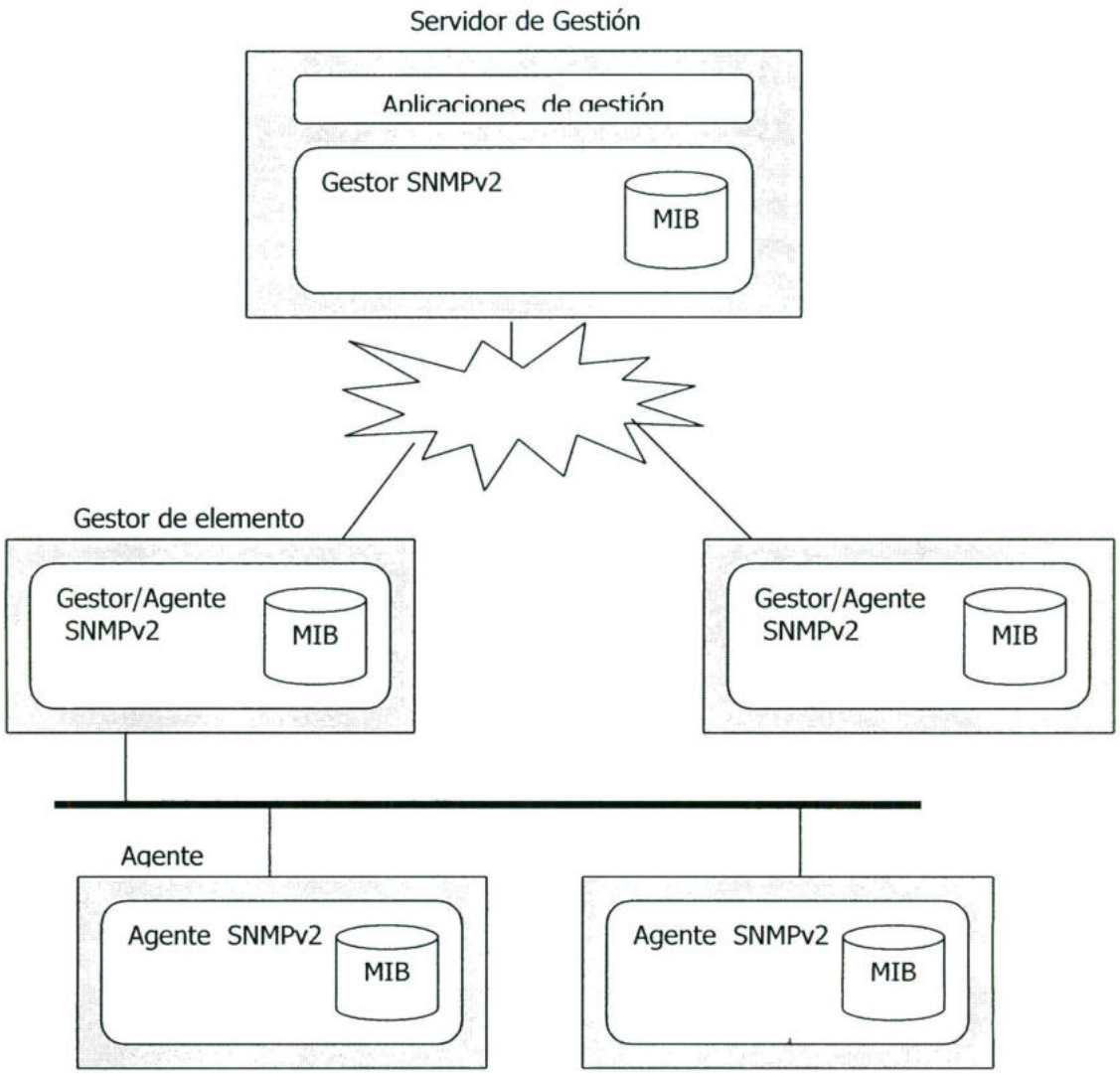


Figura 5.1.1 Configuración gestionada por SNMPv2.

La esencia de SNMPv2 es un protocolo que se utiliza para intercambiar información de gestión. Cada elemento en un sistema de gestión de red mantiene una base de datos local de información relevante de gestión de red, conocida como base de información de gestión (MIB). El estándar SNMPv2 define la estructura de esta información y los tipos de datos permitidos; esta definición se conoce como estructura de información de gestión (SMI). Esto constituye el lenguaje para definir la información de gestión. El estándar también proporciona varias MIB que son generalmente útiles para la gestión de red.

La menos un sistema de la configuración debe ser responsable de la gestión de red. Es aquí donde se debe instalar cualquier aplicación de gestión de red. Debería de haber más de una de estas estaciones de gestión, para proporcionar redundancia o simplemente dividir las obligaciones en una red grande. La mayoría del resto de los sistemas actúan con un papel de agente. Un agente recoge información localmente y la almacena para accesos posteriores de un gestor. La información incluye datos sobre el mismo sistema y también pueden incluir información del tráfico de la red o redes a las que está conectado el agente.

SNMPv2 dará apoyo a una estrategia de gestión de red altamente centralizada o distribuida. En este último caso, algunos sistemas operan con el papel de gestor y el de agente. En su papel de agente, un sistema aceptará órdenes de un sistema de gestión superior. Algunas de estas órdenes están relacionadas con la MIB local en el agente. Otras órdenes requieren que el agente actúe como delegado para dispositivos remotos. En este caso, el agente delegado asume el papel de gestor para acceder a información en un agente remoto, y después asume el papel de agente para pasar esa información a un gestor superior.

Todos estos intercambios se realizan utilizando el protocolo SNMPv2, que es un protocolo sencillo del tipo petición/respuesta. Normalmente, se implementa encima del protocolo de datagrama de usuario (UDP), que es parte del conjunto de protocolos TCP/IP. Ya que los intercambios SNMPv2 son del tipo de pares solicitud-respuesta discretos, no se requiere una conexión segura.

5.2 SMI – Structure of Management Information

La Estructura de la Información de Gestión (SMI) define el marco de trabajo general dentro del que se puede definir y construir la MIB. La SMI identifica los tipos de datos que se pueden utilizar en la MIB y cómo se pueden representar y nombrar los recursos dentro de la MIB. La filosofía que subyace en la SMI es animar la simplicidad y la amplitud dentro de una MIB. Así, la MIB pude almacenar solamente tipos de datos sencillos: escalares y matrices de dos dimensiones de escalares, llamadas tablas. La SMI no permite la creación o la recuperación de estructuras de datos complejas.

Esta filosofía es la contraria a la utilizada en los sistemas de gestión de OSI, que proporciona estructuras de datos y modos de recuperación complejos para permitir una funcionalidad mayor. SMI evita los tipos y estructuras de datos complejos para simplificar la tarea de la implementación y mejorar la interoperabilidad. Las MIB inevitablemente contendrán tipos de datos creados por el vendedor y, a menos que se impongan fuertes restricciones en la definición de tales tipos de datos, la interoperabilidad se verá afectada.

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

La tabla 5.2.1 muestra los tipos de datos que se permiten por SMI. Éste es un conjunto bastante restringido de tipos. Por ejemplo, los números reales no se permiten. Sin embargo, es lo bastante rico como para permitir la mayoría de los requisitos de la gestión de red.

Tipo de dato	Descripción
INTEGER	Enteros en rango de -2^{31} a 2^{31} -1.
Unterger 32	Enteros en rango de 0 a 2^{32} -1.
Counter 32	Un entero no negativo que se puede incrementar modulo 2^{32}.
Counter 64	Un entero no negativo que se puede incrementar modulo 2^{64}.
Gauge 32	Un entero no negativo que se puede incrementar o decrementar, pero no excederá un valor máximo de $2^{32}-1$.
Time ticks	Un entero no negativo que represente el tiempo, modulo 2^{32}, en centésimas de segundo.
OCTE STRING	Cadena de octetos para datos arbitrarios binarios o textuales; limitado a 255 caracteres.
IpAdrees	Dirección de Internet de 32 bits.
Opaque	Un campo de bits arbitrario.
BIT STRING	Una enumeración de bits con nombre.
OBJECT IDENTIFIER	Nombre asegurado administrativamente a objetos u otros elementos normalizados.

Tabla 5.2.1 Tipos de datos permitidos en SNMP v2.

5.3 Funcionamiento del protocolo

El corazón del entorno de trabajo de SNMP v2 es el protocolo mismo. El protocolo proporciona un mecanismo básico y directo para intercambiar información de gestión entre un gestor y un agente.

La unión básica de intercambio es el mensaje, que consta de un envoltorio de mensaje exterior y una unidad de datos de protocolo interior (PDU). La cabecera de mensaje exterior está relacionada con la segunda.

Se puede transmitir siete tipos de PDU en un mensaje de SNMP. El formato general de estos se muestra en la figura 5.3.1. Existen varios campos que son comunes a varias PDU. El campo identificativo de solicitud es un entero asignado de forma que las solicitudes que se produzcan se identifiquen de una forma única. Esto permite que un gestor relacione las respuestas de entrada con las soluciones de salida. También permite que un agente trate el problema de dos o más PDU duplicadas generadas por un servicio de transporte no seguro. El campo de variable colección contiene una lista que recolecta los identificadores de objetos; dependiendo en el PDU, la lista puede incluir un valor de cada objeto.

- ☑ Todos los paquetes contienen dos campos:
  - El número de versión de SNMP
  - Un nombre de comunidad

- ☑ El resto del paquete depende del tipo del mismo, y se denomina PDU (Protocol Data Unit) de SNMP

El **PDU GetRequest,** emitido por un gestor incluye una lista de uno o más nombres de objetos para lo que se solicita un valor. Si la operación de obtener valores tiene éxito, el agente que responde enviará un PDU Response. La lista de la variable colección contendrá el identificador y el valor de datos los objetos obtenidos. Para cualquier variable que no es relevante desde el punto de vista de la MIB, se devuelve el identificador y un código de error en la lista de la variable colección. Así, SNMPv2 permite respuestas parciales a un GetRequest, lo que da lugar a una mejora significativa con respecto a SNMP. En SNMP, si una o más variables en GetRequest no se permite, el agente devuelve un mensaje de error con un estado de noSuchName. Para poder tratar estos errores, el gestor SNMP no debe devolver valores a la aplicación solicitante o debe incluir un algoritmo que responda ante un error eliminado las variables perdidas, reenviando la solicitud, y enviando un resultado parcial a la aplicación.

Versión	Comunidad	PDU de SNMP

(a) Mensaje SNMP

Tipo de PDU	Identificativo solicitud	0	0	Variable colección

(b) PDU GetRequest, PDU GetNextRequest, PDU SetRequest, PDU SNMPv2-Trap

Tipo de PDU	Identificativo solicitud	Categoría de error	Índice de error	Variable colección

(c) PDU Response

Tipo de PDU	Identificativo solicitud	No repetidor	Repetición máxima	Variable colección

(d) PDU GetBulkRequest

Nombre1	Valor1	Nombre2	Valor2	Nombre n	Valor n

(e) Variable colección

Figura 5.3.1 Formato de PDU de SNMPv2.

La **PDU GetNextRequest** también es emitida por un gestor e incluye una lista de uno o mas objetos. En este caso, para objeto cuyo nombre se encuentra en el campo de la variable colección se devuelve un valor para ese objeto que es el siguiente en orden lexicográfico, lo que es equivalente a decir siguiente en la MIB en términos de su posición en la estructura de identificadores de objetos. Como con la PDU GetRequest, el agente devuelve valores para tantas variables como le sea posible. Una de las ventajas de la PDU GetNextRequest es que permite a un gestor descubrir la estructura de una MIB dinámicamente. Esto es útil si el gestor no conoce a priori el conjunto de objetos que asociados a un agente o que están en una MIB particular.

Una de las principales mejoras proporcionadas por SNMPv2 es la PDU **GetBulkRequest**. El objetivo de esta PDU es minimizar el número de intercambios de protocolo requeridos para obtener gran cantidad de información de gestión. La PDU GetBulkRequest permite a un gestor SNMPv2 solicitar que la respuesta sea tan grande como sea posible dada la restricción del tamaño del mensaje.

La **PDU SetRequest** se emite por un gestor para solicitar que el valor de uno o más objetos se modifique. La entidad SNMPv2 que la recibe responde con una PDU Response que contiene el mismo identificador de solicitud. La operación de SetRequest es atómica: o se actualizan todas las variables o ninguna. Si la entidad que responde es capaza de establecer los valores de todas las variables indicadas en la lista entrante de la variable colección, entonces la PDU Response incluye el campo de la variable colección con un valor proporcionado para cada variable. Si al menos uno de los valores de variable no se puede proporcionar, entonces no se devuelven valores ni se actualizan éstas. En este último caso, el código de estado de error indica la razón del fallo y el campo de índice de error indica la variable en la lista de variables colección que causó el fallo.

La **PDU de SNMPv2 Trap** se genera y transmite por un agente SNMPv2 actuando en su papel de agente cuando ocurre un evento inusual. Se utiliza para proporcionar a la estación de gestión una notificación asíncrona de algún evento significativo. La lista de la variable colección se utiliza para contener la información asociada con el mensaje Trap. A diferencia de GetRequest, GetNextRequest, GetBulkRequest, SetRequest e InformRequest, la PDU SNMPv2 Trap no provoca una respuesta de la entidad que lo recibe; es un mensaje no confirmado.

La **PDU InformRequest** se envía por una entidad SNMPv2 actuando como gestor, en representación de una aplicación, a otra entidad SNMPv2 en su papel de gestor, para proporcionar información de gestión a una aplicación utilizando la última entidad. Como con la PDU SNMPv2 Trap, la lista de la variable colección se utiliza para llevar la información asociada. El gestor que recibe una InformRequest las confirma con una PDU Response.

Tanto para Trap como para InformRequest, se pueden definir varias condiciones que indican cuándo se genera la notificación; también se especifica la información que se va a enviar.

5.4 Ventajas y Desventajas de SNMPv2

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

La mayor **ventaja** de usar el paradigma obtener-almacenar es la estabilidad, simplicidad y flexibilidad.

- ☑ El SNMP es especialmente estable ya que sus definiciones se mantienen fijas aún cuando nuevos elementos de datos se añadan al MIB y se definan nuevas operaciones como efectos del almacenamiento de esos elementos.
- ☑ Desde el punto de vista de los administradores, por supuesto, el SNMP se mantiene oculto al usuario de una interfaz para software de administración de red puede expresar operaciones como comandos imperativos (por ejemplo, arrancar). Así pues, hay una pequeña diferencia visible entre la forma en que un administrador utiliza SNMP y otros protocolos de administración de red.

A pesar de su extenso uso, SNMP tiene algunas **desventajas**. La más importante es que se apoya en UDP.

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

Un paquete de software servidor SNMP puede comunicarse con los agentes SNMP y transferir o solicitar diferentes tipos de información. Generalmente, el servidor solicita las estadísticas del agente, incluyendo el número de paquetes que se manejan, el estado del dispositivo, las condiciones especiales que están asociadas con el tipo de dispositivo (como las indicaciones de que se terminó el papel o la pérdida de la conexión en un módem) y la carga del procesador.

El servidor también puede enviar instrucciones al agente para modificar las entradas de su base de datos MIB (Base de Información sobre la Administración). El servidor también puede enviar los límites o las condiciones bajo las cuales el agente SNMP debe generar un mensaje de interrupción para el servidor, como cuando la carga del CPU alcanza el 90 por ciento.

Las comunicaciones entre el servidor y el agente se llevan a cabo de una forma un tanto sencilla, aunque tienden a utilizar una notación abstracta para el contenido de sus mensajes. El agente nunca envía datos hacia el servidor a menos que se genere una interrupción o se haga una solicitud de sondeo. Esto significa que pueden existir algunos problemas constantes sin que el servidor SNMP sepa de ellos, simplemente porque no se realizó un sondeo ni se generó interrupción.

6. Versión 3 del SNMP

Se publicó SNMPv3 como un conjunto de Estándares Propuestos en enero de 1998 (actualmente RFC 2570 a 2575). Este conjunto de documentos no proporciona una capacidad SNMP completa si no que define una arquitectura general de SNMP y un conjunto de capacidades en seguridad.

SNMPv3 proporciona tres servicios importantes: **Autentificación**, **Privacidad** y **Control de Acceso**. Los dos primeros forman parte del modelo de Seguridad Basada en Usuarios (USM, User-Based Security) y el último se define en el Modelo de Control de Acceso Basado en Consideraciones (VACM, View-Based Control Model). Los servicios de seguridad están gobernados por la identidad del usuario que solicita el servicio; que puede ser un individuo o una aplicación o un grupo de individuos o aplicaciones.

En lo que se refiere a la arquitectura de SNMP se dice que es de tipo modular, y está basada en las siguientes especificaciones:

- ☑ Utiliza un lenguaje de definición de datos
- ☑ Definición de administración de información (MIB)
- ☑ Definición protocolar
- ☑ Seguridad y Administración.

SNMPv3 extiende estos principios arquitectónicos y basándose sobre éstos incorpora nuevas capacidades de seguridad y de administración en la arquitectura.

Para corregir las deficiencias de seguridad que hasta ahora venían arrastrando SNMPv1/SNMPv2 fueron presentadas una serie de recomendaciones. Estas recomendaciones están orientadas a definir una arquitectura y nuevas capacidades en cuanto a seguridad.

SNMPv3 es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encriptación de paquetes que trafican por la red. Las capacidades de seguridad que SNMPv3 proporcionan son:

- ☑ Integridad del Mensaje: Asegura que el paquete no haya sido violado durante la transmisión.
- ☑ Autenticación: Determina que el mensaje proviene de una fuente válida.
- ☑ Encriptación: Encripta el contenido de un paquete como forma de prevención.

6.1 Generalidades de SNMPv3

☑ ESTRUCTURA DE LA INFORMACIÓN DE DIRECCIÓN

La información de dirección es una colección de objetos manejados por un administrador. La Base de Información de Administración (MIB) es la descripción lógica de todos los datos de administración de la red.

Estructura de Nombres

Se basa en el uso de un método consistente en la definición de nombres de las diferentes variables a ser utilizadas.

Una estructura de árbol cumple con los requisitos y recibe el nombre de Estructura de Información de Administración (SMI). El SMI está dividido en tres partes:

1. **Definiciones de modulo**. Utilizadas para describir los módulos de información. Se usa para llevar consistentemente la semántica de un módulo de información.

2. **Definiciones de Objeto**. Se utilizan para describir los objetos manejados y para llevar consistentemente la semántica de un objeto.

3. **Definiciones de Notificación**. Se usan al describir transmisiones de información de dirección y para llevar consistentemente la sintaxis de una notificación.

☑ OPERACIÓN DE PROTOCOLOS

El protocolo de dirección mantiene el intercambio de mensajes que lleva la información de dirección entre los agentes y la dirección de estaciones. La forma de estos mensajes es en forma de paquete, el cual encapsula una Unidad de Datos Protocolar (PDU).

Las especificaciones de los servicios protocolares de SNMPv3, están incorporados en RFC 1905, también se define el funcionamiento del protocolo con respecto al recibimiento y envío de PDUs.

☑ TRANSPORTE

Pueden usarse mensajes de SNMP con una gran variedad de colecciones protocolares, dentro de las cuales se pueden nombrar IPX y UDP.

En RFC 1906, se establecen las diferentes categorías de transporte. Aunque se definen varías categorías se seleccionó UDP como el transporte preferido, ya que es simple y se puede implementar con poco código. Además de esto es la opción más fiable en caso de que el dispositivo esté dañado o sobrecargado.

☑ ARQUITECTURA, SEGURIDAD Y ADMINISTRACIÓN

La arquitectura de SNMPv3, se basa principalmente en el mejoramiento de la seguridad y de la administración, por este hecho está enfocado en los siguientes puntos:

a) Los Instrumentos y Aplicaciones.

b) Las entidades (Proveedores de servicio).

c) Las Identidades (Usuarios de Servicio)

d) La información de dirección, incluyendo apoyo para múltiple contextos lógicos.

En RFC 2571 se especifica mas detalladamente la arquitectura de SNMPv3.

☑ MENSAJES QUE PROCESA Y DESPACHA

Los administradores y los agentes se comunican entre sí enviándose mensajes de SNMPv3. Algunos de estos mensajes son los siguientes:

a) Get-Request. Solicita uno o más valores de una MIB del sistema administrado.

b) Get-Next-Request. Permite al administrador obtener los valores secuencialmente.

c) Set- Request. Permite al administrador actualizar las variables.

d) Response. Devuelve el resultado de una operación de Get, get-Next o Set.

e) Trap. Permite a un agente avisar de eventos importantes.

f) Get-Bulk. Solicita a un agente que devuelva tanta información de la solicitada como pueda

g) Información sobre confirmación de excepciones.

En RFC 2572 se describe el proceso de los mensajes y despacho de los mismos.

☑ APLICACIONES DE SNMPv3

SNMPv3 posee cinco tipos de aplicaciones, las cuales pueden asociarse con cada uno de sus instrumentos. Dichas aplicaciones son las siguientes:

a) Generadores de Orden

b) Generador de Respuestas

c) Creadores de la Notificación

d) Receptores de la notificación

e) Proxy

f) Forwarders (Expedidores)

En RFC 2573 se describen detalladamente este tipo de aplicaciones.

☑ COEXISTENCIA Y TRANSICIÓN DE SNMPv3

SNMPv3 permite la transición y coexistencia de los diferentes documentos MIB generados en la versión 1 (SNMPv1) y la versión 2 (SNMPv2).

Por otra parte, también permite la coexistencia de las entidades que soportan las diferentes versiones de SNMP en una red multi-lenguaje y además el procesamiento de operaciones protocolares en los múltiples lenguajes implementados.

En el modelo de procesamiento de mensajes de SNMPv1 y el Modelo de Seguridad de esta misma versión, existen mecanismos para adaptar estas versiones y las de SNMPv2 al Modelo de Control de Acceso de Vista (VACM- View Based Access Control Model).

El VACM puede simultáneamente asociarse con un solo instrumento de implementación, el cual puede procesar múltiples mensajes y múltiples modelos de seguridad.

6.2 Servicios de Seguridad de SNMPv3

☑ TIPOS DE SERVICIOS DE SEGURIDAD

Los servicios de seguridad que ofrece el modelo de SNMPv3 permiten proteger un mensaje de un determinado retraso e impide la repetición del mismo. Los servicios son los siguientes:

1. Integridad de los datos.
2. Su objetivo es prevenir la alteración y/o destrucción de los datos por entes no autorizados.
3. Autenticación del origen de los datos.
4. Permite comprobar el origen de los datos exigiendo la identidad del usuario. Corrobora que los datos estarán en el lugar donde se originó la petición.
5. Confidencialidad de los datos.
6. Permite garantizar que los datos no serán accesados por usuarios no autorizados, entidades o procesos desconocidos.
7. Módulo de Tiempo y protección de repetición limitada.

☑ ORGANIZACIÓN DEL MÓDULO DE SEGURIDAD

Los protocolos de seguridad están divididos en tres módulos diferentes y cada uno tiene sus responsabilidades específicas:

1. Módulo de Autenticación.
2. Está encargado de la Integridad y de la Autenticación del origen de los datos. Cuando se efectúa el proceso de autenticación el mensaje completo es chequeado para garantizar su integridad en el modulo de autenticación.

3. Módulo de Tiempo.

4. Ofrece protección contra el retraso o repetición del mensaje. El chequeo de tiempo solo se realiza si se ha concluido el proceso de autenticación.

5. Módulo de Reserva.

Ofrece protección contra el descubrimiento de los datos, garantizando la confidencialidad de los mismos. En este caso se necesita también que el mensaje sea autenticado.

☑ PROTECCIÓN CONTRA LA REPETICIÓN DEL MENSAJE, RETRASO Y REDIRECCIÓN

Con el objeto de ofrecer protección contra el retraso, la repetición y la redirección de los mensajes, SNMPv3 utiliza sus instrumentos y establece una serie de mecanismos, los cuales se resumen a continuación:

1. Instrumento SNMPv3 de autoridad.

2. SNMPv3 asigna uno de sus instrumentos para controlar el retraso, la repetición y la redirección, el cual está involucrado en cada proceso de comunicación y constituye o representa la autoridad. Cuando un mensaje de SNMP está en espera de una respuesta, el receptor de tales mensajes es autorizado para recibirla.

3. Mecanismos. Los mecanismos utilizados contra la repetición del mensaje, retraso y redirección son los siguientes:

- ☑ Para proteger un mensaje de la **amenaza de repetición o retraso**, se utiliza un juego de indicadores de tiempo (Timeliness) en el instrumento de autoridad de SNMP. El indicador de tiempo se utiliza para determinar si un mensaje fue recibido en forma reciente. Un instrumento de SNMP puede evaluar dichos indicadores y asegurarse que un mensaje recibido es más o menos reciente que otro que proviene del mismo origen. Estos mecanismos detectan e identifican los mensajes que no son generados recientemente.

- ☑ **Verificación de Mensajes** enviados por un instrumento SNMP. Cada uno de los mensajes enviados por un instrumento de autoridad, que en este caso sería el Remitente, incluye una identificación única (identificador), la cual está asociada con su destinatario. Cada uno de los mensajes son chequeados de forma tal que se asegure que están en el destino correcto.

- ☑ **Identificación de mensajes generados no recientemente**. Un juego de indicadores de tiempo es incluido en el mensaje, mostrando el tiempo de generación del mismo. Los mensajes que posean indicadores de tiempo no recientes, son considerados no auténticos, por lo que los instrumentos SNMP suspenden cualquier respuesta hasta que no se normalice la transmisión o no exista una demanda excelente. El receptor de un mensaje (destinatario) verifica la identificación del instrumento de autoridad y se asegura que verdaderamente ese es su destino final.

☑ SERVICIO DE PRIVACIDAD

El servicio de privacidad de USM habilita a los gestores y a los agentes a encriptar mensaje. De nuevo, el gestor director y el agente director deben compartir una clave secreta. En este caso, si los dos están configurados para utilizar la facilidad de privacidad, todo el tráfico entre ellos es encriptado utilizando el estándar de encriptado de datos (DES). El director que envía encripta el mensaje utilizando el algoritmo DES y su clave secreta y envía el mensaje al director receptor que lo desencripta utilizando el algoritmo DES y la misma clave secreta.

☑ SERVICIO DE CONTROL DE ACCESO

El servicio de control de acceso hace posible configurar los agentes para que proporcionen diferentes niveles de acceso a la base de información de gestión (MIB) del agente a diferentes gestores. Un director agente puede restringir el acceso a su MIB a un director gestor de dos formas. Primero, puede restringir el acceso a cierta porción de su MIB.

Por ejemplo, un agente podría restringir a la mayoría de los gestores ver las estadísticas relacionadas con el rendimiento y permitir solamente a un único director gestor designado para ello a ver y actualizar los parámetros de configuración. Segundo, el agente puede limitar las operaciones que un gestor utiliza en esa porción de la MIB. Por ejemplo, un director gestor particular podría limitar el acceso de sólo lectura a una porción de la MIB de un agente. El criterio de control de acceso que utilice un agente para cada gestor se debe preconfigurar y esencialmente consiste en una tabla que detalla los privilegios de acceso de los diferentes gestores autorizados.

7. Otros aspectos del protocolo SNMP

7.1 Servicio SNMP de Microsoft

El servicio SNMP de Microsoft únicamente proporciona servicio de agente SNMP y se puede ejecutar en cualquier computador Windows 2000 que tenga instalado el protocolo TCP/IP.

Para poder utilizar el protocolo SNMP se necesita instalar en otra computadora (que tenga instalado el protocolo TCP/IP) un software de administración SNMP y realizar las siguientes operaciones:

- ☑ Registrar la dirección IP y el nombre de las computadoras que van a recibir las solicitudes.
- ☑ Añadir los nombres de las computadoras que van a recibir las solicitudes y su dirección IP al método utilizado para resolución de nombres (se puede utilizar WINS, DNS, un archivo HOSTS o un archivo LMHOSTS).
- ☑ Indicar el sistema de administración SNMP utilizado y los agentes SNMP.

7.2 Cómo instalar el Servicio SNMP

Para instalar el servicio SNMP de Microsoft en un servidor Windows 2000 se deben seguir los siguientes pasos:

1. Ejecute el icono Agregar o quitar programas del Panel de Control de Configuración del menú Inicio.
2. Pulse en Agregar o quitar componentes de Windows.

3. Sitúese sobre Herramientas de administración y supervisión (sin activar ni desactivar la casilla correspondiente) y pulse en Detalles.

4. Active la casilla Simple Network Management Protocol y marque Aceptar para volver a la pantalla anterior.

5. Marque en Siguiente y comenzará a configurar los componentes.

6. Cuando haya acabado, marque en Finalizar y, después, pulse en Cerrar y cierre el Panel de control.

7.3 Cómo configurar el Servicio SNMP

Para configurar el servicio SNMP de Microsoft en un servidor Windows 2000 seguir los siguientes pasos:

1. Ejecute la utilidad Administración de equipos que se encuentra en Herramientas administrativas de Programas del menú Inicio y verá la pantalla principal de la utilidad.

2. Pulse en el signo + que hay a la izquierda de Servicios y Aplicaciones.

3. Pulse con el botón izquierdo del ratón sobre Servicios y mostrará los servicios disponibles en el panel derecho.

4. Sitúese sobre Servicio SNMP, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione Propiedades y aparecerá la pantalla correspondiente a Servicio SNMP Propiedades (Equipo Local). Dentro de ella encontrará las siguientes fichas con sus respectivos apartados:

   ☑ **Ficha General**

   - **Nombre de servicio.** Corresponde al nombre del servicio.
   - **Descripción.** Muestra una breve comentario sobre el servicio.
   - **Tipo de inicio.** Muestra el tipo de inicio del servicio: Automático, Manual, Deshabilitado.
   - **Estado del Servicio.** Indica el estado en que se encuentra en ese momento el servicio.
   - **Iniciar.** Al pulsar el botón se iniciará el servicio.

☑ **Ficha Iniciar Sesión**

- **Cuenta del sistema local.** Al activar esta casilla, se está indicando que el servicio se inicie con la cuenta del sistema en lugar de con una cuenta de usuario.
- **Permitir a los servicios interactuar con el Escritorio.** Al activar esta casilla, se está indicando que el servicio cuente con una interfaz de usuario en el escritorio que pueda se utilizado por cualquier usuario conectado en el momento de iniciarse sesión.
- **Perfil de hardware.** Permite ver el perfil del hardware en uso para el servicio seleccionado y habilitarlo o deshabilitarlo.

☑ **Ficha Recuperación**

- **Primer error.** En este apartado se muestra la acción que se realizará durante el primer intento de recuperación al fallar el servicio.
- **Reiniciar el servicio después de.** En este apartado se puede indicar el número de minutos que se esperará antes de reiniciar el servicio.
- **Archivo.** En este apartado se puede indicar la ubicación y el nombre del archivo que se ejecutará si falla el servicio.
- **Parámetros de línea de comandos.** En este apartado se pueden indicar los parámetros que se pasarán al archivo en el apartado anterior.

☑ **Ficha Dependencias**

- En ella se encuentran las dependencias del servicio seleccionado.

☑ **Ficha Agente**

- **Contacto.** En este apartado se puede indicar el nombre del usuario que administra el equipo.
- **Ubicación.** En este apartado se puede indicar la ubicación física del equipo.
- **Servicio.** En estas casillas se han de indicar los servicios que proporciona el equipo y serán de los que informará el sistema de administración (están marcados por defecto: Aplicaciones, Internet y De extremo a extremo).

☑ **Ficha Capturas**

- **Nombre de comunidad.** En este apartado se ha de identificar la comunidad a la que se desea que el equipo envíe capturas (traps) sobre sucesos extraordinarios que se produzcan.
- **Destinos de capturas.** En esta lista se muestran los computadores de cada comunidad seleccionada a los que se van a enviar las capturas (traps). Para hacerlo, estando seleccionada previamente la comunidad deseada, marque en Agregar, que se encuentra debajo de Destinos de captura, introduzca el nombre del equipo, su dirección IP o IPX, pulse agregar.

☑ **Ficha Seguridad**

- **Enviar captura de autentificación.** Si se activa esta casilla, se está indicando que se envíe al sistema de administración capturas de autentificaciones fallidas por no tener nombre de comunidad o no corresponder con las que este agente acepta.
- **Nombres de comunidad aceptados.** En esta lista se identifican las comunidades de las que se va a aceptar solicitudes.
- **Aceptar paquetes SNMP de cualquier host.** Activando esta casilla no rechazará ninguna petición SNMP recibida.

Cuando haya finalizado, marque en Aceptar y volverá a la pantalla principal de la utilidad.

Cómo ver lo errores del servicio SNMP

Para ver los errores del servicio SNMP, se deberá hacer con el Visor de Sucesos que se encuentra en Herramientas administrativas de Programas del menú Inicio.

Allí se encontrarán todos los sucesos ocurridos con los componentes del protocolo SNMP y los problemas ocurridos en el inicio de dicho servicio.

7.4 Normas estándar de SNMP: RFC

Las peticiones de comentarios (RFC, *Requests For Comments*) son una serie de informes, proposiciones de protocolos y normas estándar de protocolos utilizados en Internet. Las especificaciones del protocolo simple de administración de redes (SNMP) se definen en las RFC publicadas por el Grupo de Trabajo de Ingeniería de Internet (IETF) y otros grupos de trabajo.

Las siguientes RFC especifican las normas estándar principales de SNMP:

RFC	Descripción
1155	Estructura e identificación de información de administración para Internet basada en TCP/IP.
1157	Protocolo simple de administración de redes.
1213	Base de datos de información para la administración de redes de Internet basada en TCP/IP: MIB-II.

Tabla 7.4.1: Descripción de RFC

Los estándares de TCP/IP están publicados en varios documentos denominados Solicitudes de Comentarios (RFC). Las RFC son un conjunto de informes, propuestas de protocolos y estándares de protocolos que describen el funcionamiento interno de TCP/IP e Internet.

Aunque los estándares TCP/IP se publican siempre en forma de RFC, no todas las RFC son especificaciones de estándares.

☑ RFC 1155

El RFC 1155, está titulado como "**Estructura e Identificación de la Información Administrable para redes basadas en TCP/IP**". En este documento se describen las estructuras comunes y la identificación de los esquemas para la definición de la información administrable usada en redes basadas en TCP/IP. Incluye las descripciones de un modelo de objetos (información) para redes administradas junto con un conjunto de tipos genéricos usados para describir información administrable. Todas las descripciones formales de la estructura definida en este documento son creadas usando la Notación de Sintaxis Abstracta Uno (ASN.1).

☑ RFC 1157

El RFC 1157, titulado como "**Protocolo simple de administración de redes SNMP**". Es un documento donde se define el funcionamiento de un protocolo para la administración de redes llamado SNMP.

Define el protocolo SNMP para administrar nodos en la comunidad de Internet y el OSI Network Management Framework.

☑ RFC 1156

El RFC 1156, llamado "**Base de Información Administrable para Redes en Internet basadas en TCP/IP**", es un documento donde se define la primera versión de la Base de Información Administrable (MIB).

En esta especificación del MIB se definen las variables necesarias para el monitoreo y control de varios componentes en redes. No todos los grupos de variables definidas son obligatorios para todos los componentes de redes.

☑ **RFC 1213**

A partir de que se creó el RFC 1155, donde se definió el primer MIB, ha habido algunos cambios en cuanto a la información administrable, por lo tanto surgió un nuevo MIB, definido en el RFC 1213. El RFC 1213 está titulado como "**Base de Información Administrable para redes basadas en TCP/IP**" y es comúnmente conocido como MIB II. En este RFC se describen los cambios que han surgido para cada objeto definido en el RFC 1155, así también se describen los nuevos objetos que han sido definidos.

7.5 Ventajas y Desventajas generales de SNMP

- ☑ Es un protocolo maduro, estándar de facto aceptado por la industria.
- ☑ Está disponible en gran cantidad de productos.
- ☑ Es fácil de implementar y requiere pocos recursos del sistema.
- ☑ Falta de seguridad:
  - Cualquier estación puede resetear variables con SetRequest, por lo que muchos fabricantes no implementan este comando.
  - No hay control de acceso: al recibir un PDU un agente no comprueba si ha sido enviado por una estación autorizada.
- ☑ La identificación de comunidad viaja tal cual.
- ☑ Mala utilización del ancho de banda:
  - No existe la posibilidad de transferir información por bloques.
- ☑ Limitaciones en el mecanismo de traps:
  - Sólo se puede informar de algunos eventos previstos.
  - No son reconocidas.
- ☑ No es apropiado para gestionar redes muy grandes (por el sondeo).

7.6 RMON: Monitoreo Remoto

RMON: Remote MONitor (Monitoreo Remoto). Monitorización global de una subred. Especificación del agente MIB descrita en RFC 1271 que define las funciones del monitoreo remoto de dispositivos de la red. La especificación RMON suministra varias capacidades de monitoreo, detección de problemas e informes.

Ciertos fabricantes están cooperando para el desarrollo de extensiones particulares para ciertas clases de productos y la gestión remota de dispositivos, conocidas como **RMON (Remote MONitor)**, normas RFC 1757 (antes 1271) para Ethernet y RFC 1513 para Token Ring del IETF (Internet Engineering Task Force), que incluyen sobre unos 200 objetos clasificados en 9 grupos: Alarmas, Estadísticas, Historias, Filtros, Ordenadores, N Principales, Matriz de Tráfico, Captura de Paquetes y Sucesos. Con RMONv2 se decodifican paquetes a nivel 3 de OSI, lo que implica que el trafico puede monitorizarse a nivel de direcciones de red (puertos de los dispositivos) y aplicaciones específicas.

RMON define las funciones de supervisión de la red y las interfaces de comunicaciones entre la plataforma de gestión SNMP, los monitores remotos y los agentes de supervisión que incorporan los dispositivos inteligentes.

Características:

☑ Define una MIB de monitorización remota:

El efecto es la definición de funciones e interfaces entre consolas de gestión basadas en SNMP y monitores remotos.

☑ Objetivos:

- Operación Off-line
- Monitorización Apropiativa
- Detección y notificación de problemas
- Datos de valor añadido
- Gestores múltiples

☑ Control de monitores remotos:

- Aparatos dedicados o una función disponible en un sistema.
- El monitor remoto debe ser configurado para la captura de datos, especificando el tipo de datos y la forma en que van a ser recogidos.
  Tabla de control: describe la configuración del monitor RMON especificando la información que captura.
  Tabla de datos: almacena la información recogida.

☑ Invocación de una acción:

- Mediante operaciones SNMP puede enviarse un mandato, empleando un objeto para representar un estado de modo que se realice una determinada acción cuando dicho objeto cambia de estado.

☑ La MIB RMON:

Se divide en nueve grupos:

- Estadísticas: De error y bajo nivel de utilización para cada subred.
- Historia: Estadísticas periódicas de la información disponible.
- Alarma: Intervalo de muestreo y umbral de alarma para cualquier dato grabado por el agente RMON.
- Host: Datos sobre tipos de tráfico de y hacia nodos conectados a la subred.
- HostTopN: Estadísticas agrupadas en una lista basadas en la tabla "host".
- Matriz: Información sobre errores y utilizaciones en forma de matriz, para cualquier par de direcciones de la red.
- Filtro: Observar paquetes que casan con el filtro.
- Captura de paquetes: Modo de envío de los datos a la consola de gestión.
- Evento: Una tabla con todos los eventos generados por el agente RMON.

8. Conclusión

El protocolo de administración SNMP facilita de una manera simple y flexible el intercambio de información en forma estructurada y efectiva.

Por otro lado, el protocolo SNMP no se ocupa de servicios de usuario, sino más bien de la gestión de todos los protocolos de comunicación dentro de cada sistema anfitrión y del entorno de red en general.

La estructura SNMP ha evolucionado de SNMPv1, a través de SNMPv2, a SNMPv3; haciendo sus componentes más ricos y claramente definidos; pero su estructura en general ha permanecido consistente. Como resultado, SNMPv3 puede pensarse como SNMPv2 con adicional seguridad y capacidad de administración.

Como muchos otros protocolos utilizados en Internet hoy en día, SNMP se encontró con el problema de seguridad y privacidad. Por lo que se requería de una solución, por ello un grupo de expertos se reunieron para realizar una serie de propuestas dando como resultado SNMPv3, versión que ciertamente promete grandes avances en las capacidades de Autenticación, Privacidad y Control de Acceso.

Esta nueva versión del Protocolo de Administración de Redes, a introducido nuevos mecanismos que permiten incrementar la seguridad a nivel de la capa IP, debido a que en este nivel es probable que se pueda efectuar la captura de algún tipo de tráfico que circula por la red, además de esto, puede que el mismo sea utilizado y/o repetido, falsificando su dirección IP, originando con esto, datagramas no confiables. Por esta razón SNMPv3, ha hecho especial énfasis en el proceso de identificación de los usuarios de la red, en mantener la integridad de los datos y en asegurar la confidencialidad de la información.

9. Glosario

☑ **Abstract Syntax Notation One (ASN.1) :**

Notación de Sintaxis Abstracta 1. Es el lenguaje usado por SNMP para definir objetos estándar, así como sus reglas de codificación.

☑ **Basic Encode Rules (BER) :**

Define cómo codificar los valores definidos en ASN.1 para ser transmitidos.

☑ **Common Management Information Service/Protocol (CMIS/CMIP) :**

Gestión que surge como esfuerzo de estandarización de la administración en el marco del Modelo de Referencia para Interconexión de Sistemas Abiertos.

☑ **Common Management Information Protocol (CMIP) :**

Protocolo de información de gestión común. Esta norma internacional proporciona servicios similares a los del SNMP.

☑ **CMIP over TCP/IP (CMOT) :**

CMIP sobre TCP/IP.

☑ **DES :**

Estándar de encriptado de datos.

☑ **Internet Engineering Task Force (IETF) :**

Grupo de Trabajo de Ingeniería de Internet.

☑ **Management Information Base (MIB) :**

Base de Información de Gestión. Es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/valores que se pueden adoptar), con identificadores exclusivos para cada objeto.

☑ **Microsoft Management Console (MMC) :**

Alberga herramientas administrativas que puede utilizar para administrar equipos, servicios, otros componentes del sistema y redes.

☑ **Network-Management Systems (NMS) :**

Sistema de Gestión de Red. Ejecuta aplicaciones que monitorean y controlan dispositivos. Puede haber uno o varios por red.

☑ **Request For Comments (RFC) :**

Petición de Comentarios. Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP. Las RFC pueden encontrarse en línea en distintas fuentes.

☑ **Remote MONitor (RMON) :**

Monitoreo Remoto. Monitorización global de una subred. Especificación del agente MIB descrita en RFC 1271 que define las funciones del monitoreo remoto de dispositivos de la red.

☑ **Simple Network Management Protocol (SNMP) :**

Protocolo Simple de Administración de Red. Protocolo utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

☑ **Structure of Management Information (SMI) :**

Estructura e Identificación de Gestión de Información.

☑ **User-Based Security (USM) :**

Seguridad Basada en Usuarios

☑ **User Datagram Protocol (UDP) :**

Protocolo de Datagrama de Usuario. Protocolo de transporte sin conexión, no confiable. Cuenta el número de datagramas UDP, enviados, recibidos y entregados. El UDP se describe en el RFC 768.

☑ **View-Based Control Model (VACM) :**

Modelo de Control de Acceso Basado en Consideraciones.

10. Índice de figuras y tablas

11. Bibliografía

- ✓ Halsall, Fred, *Comunicación de datos, redes de computadoras y sistemas abiertos*, 4ª. Edición, México, Pearson Educación, 1998.
- ✓ Raya, José Luis; Raya, Cristina, *TCP/IP para Windows 2000 Server*, Colombia, Alfaomega Ra-Ma, 2001.
- ✓ S. Tanenbaum, Andrew, *Redes de Computadoras*, 3era. Edición, México, Prentice Hall.
- ✓ Stallings, William, *Comunicaciones y redes de computadoras*, 6ª. Edición, España, Prentice Hall, 2000.
- ✓ Zacker, Craig, *Redes "Manual de Referencia"*, España, McGraw Hill, 2002.
- ✓ http://www.cisco.com/univercd/cc/td/doc/ cisintwk/ito_doc/snmp.htm
- ✓ http://www.ciscoredaccionvirtual.com/redaccion/glosario/default.asp
- ✓ http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5010/cap0904.htm
- ✓ http://www.info-ab.uclm.es/asignaturas/42621/transpas/dmrTema3a-bn.pdf
- ✓ http://www.microsoft.com/windows2000/es/advanced/help/default.asp?url=/windows2000/es/advanced/help/choosing_components_to_install.htm
- ✓ http://www.monografias.com/trabajos7/tcp/tcp.shtml
- ✓ http://www.neutron.ing.ucv.ve/revista-e/No6/ Briceño%20Maria/SNMPv3.html
- ✓ http://pin.uax.edu.mx/monica/snmp.html
- ✓ http://www2.rad.com/networks/1995/snmp/snmp.htm