PROTOCOLO SNMP “SIMPLE NETWORK MANAGEMENT PROTOCOL”

ANDRÉS PARRA CARABALLO
SHARON MENDIETA BUENO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
CARTAGENA DE INDIAS D. T. Y C.
2005.

PROTOCOLO SNMP “SIMPLE NETWORK MANAGEMENT PROTOCOL”

ANDRÉS PARRA CARABALLO
SHARON MENDIETA BUENO

Trabajo de monografía presentado como requisito para optar al titulo de Ingeniero Electrónico

DIRECTORA
MARGARITA UPEGUI FERRER
MAGÍSTER EN CIENCIAS COMPUTACIONALES

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
CARTAGENA DE INDIAS D. T. Y C.
2005.

Cartagena D. T. Y C., Octubre de 2005

Señores

COMITÉ CURRICULAR

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La ciudad

Respetados señores:

Con toda atención nos dirigimos a ustedes con el fin de presentarles a su consideración, estudio y aprobación la monografía titulada PROTOCOLO SNMP “SIMPLE NETWORK MANAGEMENT PROTOCOL” como requisito parcial para optar al titulo de ingeniero electrónico.

Atentamente

ANDRÉS PARRA CARABALLO. SHARON MENDIETA BUENO.

Cartagena D. T. Y C., Octubre de 2005

Señores

COMITÉ CURRICULAR

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La ciudad

Cordial saludo:

A través de la presente me permito entregar la monografía titulada PROTOCOLO SNMP “SIMPLE NETWORK MANAGEMENT PROTOCOL” para su estudio y evaluación la cual fue realizada por los estudiantes ANDRÉS PARRA CARABALLO y SHARON MENDIETA BUENO, de la cual acepto ser su director.

Atentamente,

MARGARITA UPEGUI FERRER
Magíster en Ciencias Computacionales

AUTORIZACIÓN

Yo ANDRÉS PARRA CARABALLO, identificado con la cedula de ciudadanía número 8.854.744 de Cartagena, autorizo a la universidad tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo on-line de la biblioteca.

ANDRÉS PARRA CARABALLO

AUTORIZACIÓN

Yo SHARON MENDIETA BUENO, identificado con la cedula de ciudadanía número 32.906.488 de Cartagena, autorizo a la universidad tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo on-line de la biblioteca

SHARON MENDIETA BUENO

TABLA DE CONTENIDO

TABLA DE FIGURAS

INTRODUCCIÓN

El monitoreo de redes tiene como principal objetivo compilar información útil a cerca del funcionamiento de la red, y luego utilizarla para detectar irregularidades y planear un mejor desempeño de la misma. También permite reducir cuellos de botella optimizando el servicio, detectar fallas para sacar al sistema de crisis y realizar diagnósticos que permitan lograr arreglos antes de que los usuarios finales vean mensajes de error e incrementar la disponibilidad y utilización del sistema teniendo en cuenta políticas de seguridad.

Las primeras herramientas utilizadas para el monitoreo de redes fueron herramientas muy simples como ping, para detectar la conectividad entre direcciones; ARP para detectar interfaces de red; TRACEROUTE para detectar posibles rutas para que un paquete alcance su destino; TELNET y FINGER para chequear el funcionamiento de las operaciones con el protocolo TCP; NETSTAT para ver las tablas de ruteo en sistemas UNIX.

SNMP (Simple Network Management protocol) o protocolo simple de administración de redes es el protocolo más utilizado para esta tarea. Comúnmente se usa sobre un protocolo de transporte no orientado a la conexión, que generalmente es UDP. Tuvo su primera versión en el año 1988, cuando se lo presentó como un protocolo básico para la administración de redes. La segunda versión del protocolo (comúnmente llamada SNMPv2) apareció en el año de 1993,

el cual tuvo como objetivo principal mejorar la transferencia de información entre agentes y gestores, y aunque la propuesta del protocolo incluía cuestiones de seguridad, las mismas no pudieron ser implementadas. Muchas implementaciones de SNMPv1 y SNMPv2 debieron ser limitadas a aplicaciones de solo lectura por la falta de encriptación y la falta de autenticación. Además el protocolo se implementaba solamente con un gestor y varios agentes; un modelo que se vuelve ineficiente cuando el tamaño de las redes crece. En 1998 se publica SNMPv3, la versión mas reciente de SNMP que aborda especialmente deficiencias de seguridad. Para ello se define una arquitectura general de gestión SNMP, nuevos servicios de seguridad como autenticación, privacidad y control de acceso. Tiene como objetivo principal proteger contra los siguientes tipos de ataques: modificación del contenido de los mensajes, modificación del orden, repetición o retención de los mensajes, suplantación de una identidad para realizar operaciones no permitidas y escuchas en la red.

FUNDAMENTACION

En este capítulo se describe la importancia que tiene la Administración de Redes como elemento de gestión en las redes de computadoras. Se exponen las características de las redes actuales y los problemas que se buscan solucionar con la implementación de protocolos de gestión.

1. FUNDAMENTACION.

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

- Mezclas de diversas señales en un solo canal de transmisión tales como: voz, datos y video.

- Interconexión de varios tipos de redes, como WAN, LAN y MAN.
- El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo, RF y microondas.
- Diversos protocolos de comunicación, incluyendo TCP/IP, SPX/IPX, SNA, OSI.
- El empleo de muchos sistemas operativos, como DOS, Netware, Windows NT, UNÍX, OS/2, LINUX.
- Diversas arquitecturas de red, incluyendo Ethernet 10 base T, Fast Ethernet, Token Ring, FDDI y Fiber channel.
- Varios métodos de compresión, códigos de línea, etc.

La Necesidad de administrar redes conlleva varios problemas que se presentan en la interconexión de redes que son principalmente dos:

a**.** Dispositivos diferentes: La interconexión de redes permite diferentes tipos de dispositivos, todos ellos soportando el protocolo TCP/IP. Debido a esto, la administración de redes se presenta como un problema. Sin embargo, usar una tecnología de interconexión abierta permitió que existieran las redes formadas por dispositivos de distintos fabricantes, por lo que para administrar estas redes, habrá que usar una tecnología de administración de redes abierta.

b. Administraciones diferentes: Como se permite la interconexión entre redes de distinto propósito y distinto tamaño, hay que tener en cuenta que también están administradas, gestionadas y financiadas de distinta forma.

El sistema de administración de red opera bajo los siguientes pasos básicos:

1. Recopilación de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
2. Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
3. Transporte de la información del equipo monitoreado al centro de control.
4. Almacenamiento de los datos compilados en el centro de control.
5. Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
6. Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.

1.1. ELEMENTOS INVOLUCRADOS EN LA ADMINISTRACIÓN DE RED

Los elementos que están involucrados en la administración de la red son los siguientes:

A) Objetos: son los elementos de más bajo nivel y constituyen los aparatos administrados.

B) Agentes: un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. El agente genera el grado de administración apropiado para ese nivel y transmite información al administrador central de la red acerca de:

- Notificación de problemas.
- Datos de diagnóstico.
- Identificador del nodo.
- Características del nodo.

C) Administrador del sistema: Es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

1.2. OPERACIONES DE LA ADMINISTRACIÓN DE RED.

Las operaciones principales de un sistema de administración de red son las siguientes:

- ✧ *Administración de fallas.*

La administración de fallas maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

a) Detección de fallas.

b) Diagnóstico del problema.

c) Darle la vuelta al problema y recuperación.

d) Resolución.

e) Seguimiento y control.

✧ *Control de fallas.*

Esta operación tiene que ver con la configuración de la red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

✧ *Administración de cambios.*

La administración de cambios comprende la planeación, la programación de eventos e instalación.

✧ *Administración del comportamiento.*

Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye: El número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

✧ *Servicios de contabilidad.*

Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

- Tiempo de conexión y terminación.
- Número de mensajes transmitidos y recibidos.
- Nombre del punto de acceso al servicio.
- Razón por la que terminó la conexión.

✧ *Control de Inventarios.*

Se debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.

✧ *Seguridad.*

La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

- Identificación y autentificación del usuario, una clave de acceso y un password.
- Autorización de acceso a los recursos, es decir, solo personal autorizado.
- Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración, rendimiento, seguridad e inventarios.

1.3. SEGURIDAD

En éste método los datos del transmisor se transforman por medio de un algoritmo público de criptografía con una llave binaria numérica privada solo conocida por el

transmisor y por el receptor. El algoritmo más conocido de este tipo es el DES (Data Encription Standard).

El algoritmo opera así:

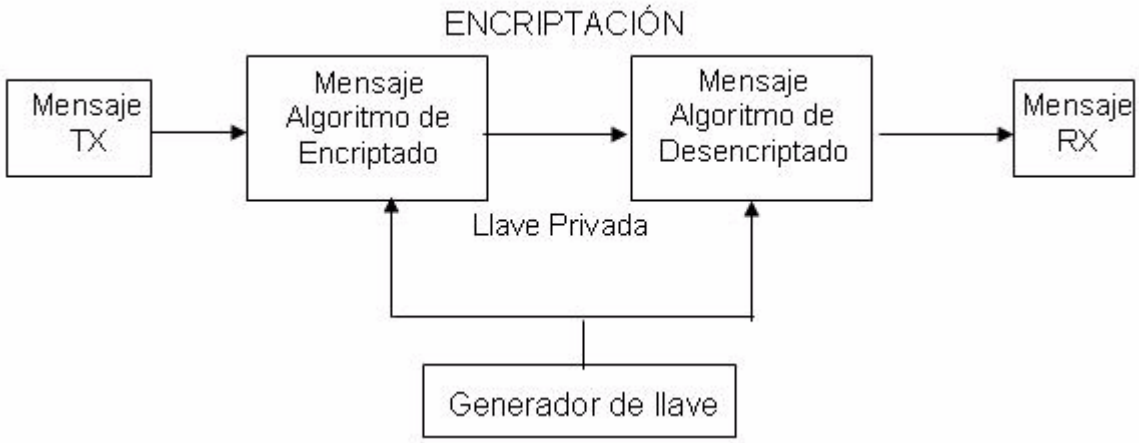


Figura 1. Algoritmo de encriptación.

1.4. FUNCIONES DE ADMINISTRACIÓN DEFINIDAS POR OSI.

OSI define las cinco funciones de administración básicas siguientes:

- Configuración
- Fallas
- Contabilidad
- Comportamiento
- Seguridad.

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.

La función de fallas incluye la detección, el aislamiento y la corrección de fallas en la red.

La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red.

La función de comportamiento mantiene el comportamiento de la red en niveles aceptables.

La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

El modelo OSI incluye cinco componentes claves en la administración de red:

CMIS: (Common Management Information Services). Éste es el servicio para la colección y transmisión de información de administración de red a las entidades de red que lo soliciten.

CMIP: (Common Management Information Protocol). Es el protocolo de OSI que soporta a CMIS, y proporciona el servicio de petición/respuesta que hace posible el intercambio de información de administración de red entre aplicaciones.

SMIS: (Specific Management Information Services). Define los servicios específicos de administración de red que se va a instalar, como configuración, fallas, contabilidad, comportamiento y seguridad.

MIB: (Management Information Base). Define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información en el MIB incluye: número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, etc.

Servicios de Directorio*:* Define las funciones necesarias para administrar la información nombrada, como la asociación entre nombres lógicos y direcciones físicas.

1.5. PROTOCOLO DE ADMINISTRACIÓN DE RED TCP/IP.

El sistema de administración de red de TCP/IP se basa en el protocolo SNMP (Simple Network Management Protocol), que ha llegado a ser un estándar en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado por múltiples fabricantes de puentes, repetidores, ruteadores, servidores y otros componentes de red[1].

Para facilitar la transición de SNMP a CMOT (Common Management Information Services and Protocol Over TCP/IP), los dos protocolos emplean la misma base de administración de objetos MIB (Management information Base).

Para hacer más eficiente la administración de la red, la comunidad de TCP/IP divide las actividades en dos partes:

a) Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
b) Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas.

[1] http://www.monografias.com/trabajos7/tcp/tcp.shtml

¿Pero realmente que se puede administrar con este protocolo? Muy buena pregunta, la cual podemos darle respuesta diciendo que se puede administrar prácticamente de todo. Desde servidores informáticos hasta sistemas de aire acondicionado, calefacción, centrales, redes locales, routers, etc. Si no existiera este Standard, deberíamos controlar cada uno de los sistemas anteriores con soluciones propietarias.

Las aplicaciones prácticas de cualquier método de gestión son múltiples. Hay proyectos ya implementados en subestaciones eléctricas, centrales telefónicas, procesos industriales, gestión centralizada de servidores informáticos, redes locales, ferrocarriles, autopistas, control de tráfico, etc. SNMP se ha creado, para implantar una gestión "universal", de una forma fiable, segura, sencilla y sobre todo económica.

INTRODUCCIÓN A SNMP

A continuación se encontrará una descripción detallada de todos los aspectos que hacen parte del protocolo como son los comandos de gestión, los componentes de la red y la composición del mensaje típico del protocolo.

2. INTRODUCCIÓN A SNMP

SNMP es un Protocolo Simple para Administración de la Red, de nivel de aplicación para consultar a los diferentes elementos que forma una red, (routers, switches, hubs, hosts, módems, impresoras, etc.). Cada equipo conectado a la red ejecuta unos procesos, para que se pueda realizar una administración tanto remota como local de la red. Estos procesos se van actualizando de manera constante en una base de datos[2].

El protocolo SNMP se basa en codificar toda la información que se desea gestionar, en árboles jerarquizados de variables, denominados árboles MIB. Toda consulta o acción en dichas variables, lee o actúa en el sistema a vigilar.

Para controlar funciones muy especificas, (temperaturas, tensiones eléctricas, ocupaciones de discos duros y memoria, bases de datos, etc.), los fabricantes han creado nuevas ramas de variables en estos árboles, que actúan directamente en los sistemas que deseamos gestionar. Bastara con cargar el archivo MIB proporcionado por el fabricante, para que la plataforma de gestión SNMP pueda controlar el sistema.

Para recoger información, la plataforma lanza un comando GET indicando las variables que desea recibir. Luego la presenta como curvas, avisos, mensajes, etc. Cuando se desea escribir un comando, se rellena un valor de una

[2] http://www.pablin.com.ar/computer/info/varios/snmp.htm

determinada variable MIB y se envía con un comando SET. El agente SNMP lo interpreta y actúa en consecuencia.

Junto a dichos comandos se acompaña una "clave de acceso", llamada comunidad. Los agentes SNMP solo responderán a comandos GET y SET, que vengan con el mismo nombre de comunidad que tengan definidos internamente. Por defecto, casi todos los agentes SNMP vienen definidos con "public". Si se desea crear una mayor seguridad de acceso, bastara con cambiarlo por otro nombre de comunidad.

Ante situaciones que sobrepasen unos umbrales determinados, el agente SNMP puede enviar una alarma, trap, que tras ser recibida, puede generar determinadas respuestas. Dichas respuestas pueden pasar desde llamadas a los teléfonos móviles del personal de mantenimiento, indicando con un mensaje el problema, a interaccionar directamente en el sistema con uno o varios comandos SET. Esta funcionalidad permite vigilar los sistemas de forma remota.

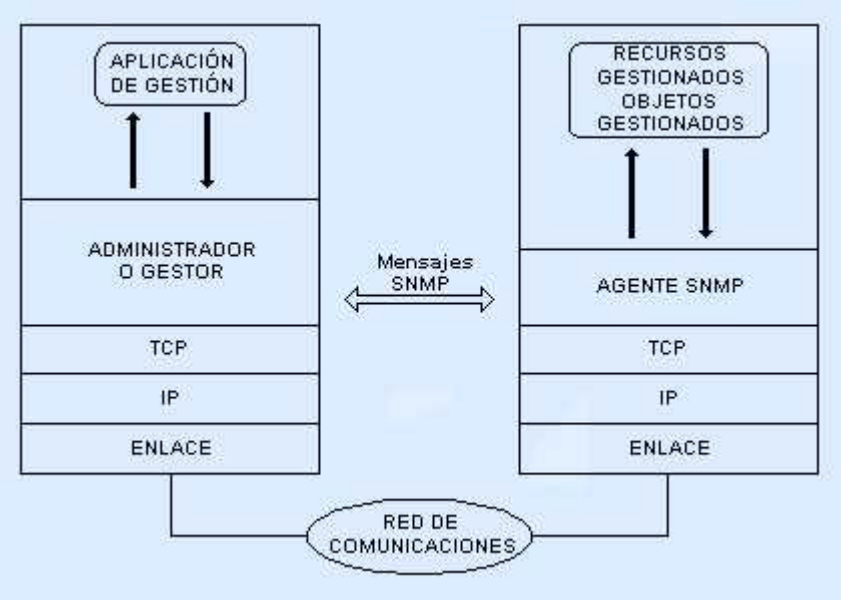


Figura 2. Comunicación entre capas del protocolo

2.1. ESQUEMA DE ADMINISTRACIÓN.

Como se observa en la Figura 2, el agente y la MIB residen dentro del aparato que es monitoreado y controlado. La estación administradora contiene software que opera los protocolos usados para intercambiar datos con los agentes, y software de aplicación de administración de red que provee la interfaz de usuario para a fin de habilitar a un operador para saber el estado de la red, analizar los datos recopilados e invocar funciones de administración.

Figura 3. Esquema de administración

El administrador de red controla un elemento de red pidiendo al agente del elemento que actualice los parámetros de configuración y que le de un informe sobre el estado de la MIB. El agente intercambia mensajes con el administrador de la red con el protocolo SNMP. Cualquier elemento que participe en la red puede ser administrado, incluidos host, ruteadores, hubs, puentes, multiplexores, módems, switches de datos, etc... Cuando el aparato controlado no soporta SNMP, se usa un agente Proxy. El agente Proxy actúa como un intermediario entre la aplicación de administración de red y el aparato que no soporta SNMP.

SNMP define el formato y el significado de los mensajes que intercambian el administrador y el agente[3]. En lugar de definir muchas operaciones, el SNMP utiliza el paradigma de obtención y almacenamiento, en el cual el administrador manda solicitudes de obtención y almacenamiento de valores en variables. Todas

[3] Se usara el término agente, refiriéndose a un dispositivo que actúa como servidor.

las operaciones se definen como efectos colaterales de las operaciones de almacenamiento.

SNMP no define el grupo de variables que se pueden emplear. En cambio, las variables y sus significados se definen en normas distintas, lo que permite la definición de diferentes grupos de variables MIB para cada dispositivo de hardware o protocolo.

La base de información de administración (MIB) contiene el grupo de objetos a los cuales puede acceder el SNMP.

Los nombres de las variables MIB se definen de acuerdo con la norma ASN.1 (Notación de Sintaxis Abstracta.1); todas las variables MIB tienen nombres jerárquicos ASN.1 grandes que se traducen en una representación numérica más compacta para su transmisión. Aunque la ASN.1 no incluye una operación de identificación de los tipos de datos agregados como tablas o arreglos, una variable MIB puede ser una tabla; la información de identificación se agrega al nombre.

A finales de los años 70, las redes de ordenadores experimentaron un espectacular crecimiento y empezaron a conectarse entre sí. A estas nuevas redes se les llamó inter-redes o Internet. Pronto se hicieron muy difíciles de gestionar, y se hizo necesario el desarrollo de un protocolo de gestión.

El primer protocolo que se usó fue el SNMP. Se diseñó como algo provisional para establecer una plataforma, que en su futuro impulsara al desarrollo de otro protocolo más elaborado.

2.2. COMPONENTES DE SNMP

Una red que utiliza SNMP contiene tres componentes dominantes: dispositivos, agentes, y sistemas manejados de la red-gerencia (NMS's).

Un dispositivo manejado es un nodo de red que contiene un agente del SNMP y que reside en una red monitoreada. Los dispositivos manejados recogen y almacenan la información de la gerencia y ponen esta información a disposición de los NMS's usando el SNMP. Los dispositivos manejados, a veces llamados los elementos de la red, pueden ser enrutadores, servidores de acceso, switches, puentes, hubs, host, o impresoras.

Un agente es un módulo del software de administración 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.

Los NMS's ejecutan las aplicaciones de monitoreo y control en los dispositivos de la red. Estos proporcionan gran parte de los recursos del proceso y de la memoria requeridos para la administración de la red. Uno o más NMS's debe existir en cualquier red manejada.

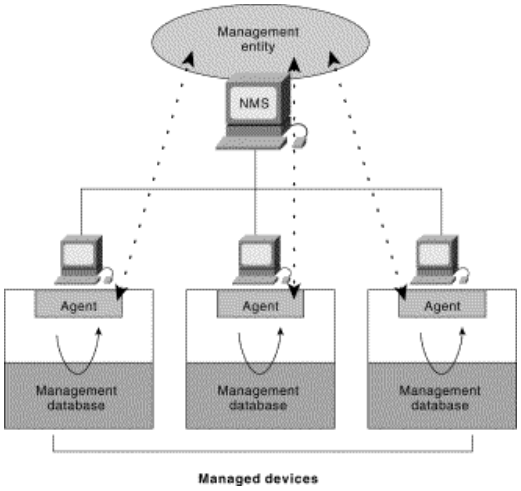


Figura 4. Componentes de SNMP.

2.3. COMANDOS BÁSICOS

Para el control y monitoreo de las redes, SNMP tiene cuatro comandos básicos, los cuales son:

READ: es utilizado por los NMS's para supervisar los dispositivos manejados. Los NMS's examinan diversas variables que sean mantenidas por los dispositivos administrados.

WRITE: es utilizado por los NMS's para controlar los dispositivos manejados. Los NMS's cambian los valores de las variables almacenadas dentro de los dispositivos administrados.

TRAP: es utilizado por los dispositivos manejados asincrónicamente para darle a conocer acontecimientos a los NMS's. Cuando ocurren ciertos tipos de acontecimientos, un dispositivo manejado envía una TRAP o mensaje a los NMS's.

LAS OPERACIONES DE MONITORIZACIÓN: que son usadas por los NMS's para determinar cuales son las variables y ayudas que soportan los equipos, para recopilar secuencialmente la información en tablas variables, tales como una tabla de enrutamiento.

2.4. BASE DE INFORMACIÓN DE DIRECCIÓN DEL SNMP

Una Base de Información de Dirección (MIB) es una colección de información que esta jerárquicamente organizada.

Se acceden por medio de MIBs usando un protocolo de administración de red como SNMP. Ellos se comprenden de objetos manejados y se identifican por los identificadores del objeto.

Un objeto manejado (a veces llamado un objeto MIB, un objeto, o un MIB) es cualquier número de características específicas de un dispositivo manejado. Los objetos manejados se comprenden de uno o más procesos del objeto que son esencialmente las variables.

Existen dos tipos de objetos manejados, los cuales son: escalares y tabulares. Los objetos escalares definen un solo caso del objeto. Los objetos tabulares definen los múltiples casos relacionados con el objeto que se agrupan en las tablas del MIB.

Un identificador del objeto (u objeto ID) singularmente identifica un objeto manejado en la jerarquía de MIB. La jerarquía del MIB puede pintarse como un

árbol con una raíz anónima, los niveles de que se asigna por las organizaciones diferentes.

En la parte alta de los MIBs hay objetos con IDs, que pertenecen a las organizaciones de las normas diferentes, mientras en la parte baja de la organización están los objetos que tienen IDs, las cuales son asignadas por las organizaciones asociadas. Se posicionan MIBs que no se han estandarizado típicamente en la rama experimental. El objeto manejado a la Entrada puede identificarse singularmente, por el nombre del objeto o por el descriptor equivalente del objeto.

2.4.1. REFERENCIAS MIB AMBIGUAS

Debido a que el alcance de cualquier operación SNMP está conceptualmente confinado a los objetos relevantes a un único elemento de red, y ya que todas las referencias SMI (Structure of Management Information - Estructura para la información de gestión) a objetos MIB son por medio de nombres de variables únicos, no hay posibilidad de que una referencia SNMP a cualquier tipo de objeto definido en el MIB se pueda resolver entre múltiples casos de ese tipo.

SMI presentas un marco general donde se especifica el MIB. Define los objetos gestionados y como acceder a ellos. No soporta la creación ni recuperación de datos complejos para mantener la simplicidad y facilitar la implementación de las estructuras.

SMI especifica reglas para:

- Los mecanismos de identificación de los objetos;
- Los tipos de datos que podrán usarse.
- La descripción de los objetos.

Como convenciones se determina que: muchos espacios en blanco se considerarán como un único espacio, los comentarios se delimitarán por un par de guiones; los identificadores comienzan con letra minúscula; la referencia a un módulo comienza con una letra en mayúsculas; los tipos de datos que representan notaciones estándares se escriben con mayúscula.

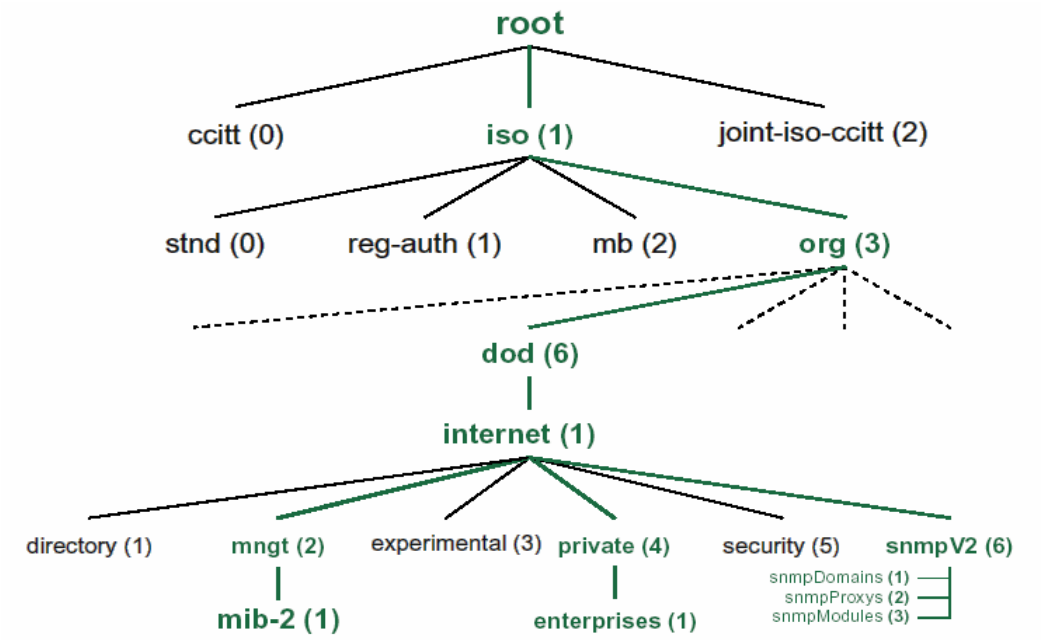


Figura 5. Árbol MIB

2.4.2. REFERENCIAS ENTRE VERSIONES MIB

El objeto referenciado por cualquier operación SNMP es exactamente el especificado como parte de la operación de petición, o en el caso de una operación Get-next su sucesor en el conjunto de MIB. En particular, una referencia a un objeto como parte de una versión del MIB estándar de Internet, no se aplica a ningún objeto que no sea parte de dicha versión, excepto en el caso de que la operación sea Get-next, y que el nombre del objeto especificado sea el último lexicográficamente entre los nombres de todos los objetos presentados como parte de dicha versión.

2.4.3. IDENTIFICACIÓN DE LOS CASOS DE OBJETOS

Cada caso de un tipo de objeto definido en el MIB se identifica en las operaciones SNMP por un nombre único llamado “nombre de variable”. En general, el nombre de una variable SNMP es un identificador de objeto de la forma *x.y*, donde *x* es el nombre del tipo de objeto no agregado definido en el MIB, e *y* es un fragmento de un identificador de objeto que de forma única para dicho tipo de objeto, identifica el caso deseado. Esta estrategia de denominación admite la completa explotación de la semántica de la PDU GetNextRequest, dado que asigna nombres para variables relacionadas de forma que sean contiguas en la ordenación lexicográfica de todas las variables conocidas en el MIB.

2.5. SNMP Y REPRESENTACIÓN DE DATOS

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

Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU (Protocol Data Unit – Unidad de datos de protocolo). Estos datagramas no necesitan ser mayores de 484 bytes, pero es recomendable que las implementaciones de este protocolo soporten longitudes mayores.

SNMP maneja los siguientes tipos de datos:

Enteros: Para expresar, por ejemplo, el MTU (Maximum Transfer Unit).

Dirección IP: Se expresa como cuatro bytes. Recuérdese que cada elemento de red se configura con al menos una dirección IP.

Dirección física: Se expresa como una cadena de octetos de longitud adecuada; por ejemplo, para una red Ethernet o Token Ring, la dirección física es de 6 octetos.

Contador: Es un entero no negativo de 32 bits, se usa para medir, por ejemplo, el número de mensajes recibidos.

Tabla: es una secuencia de listas.

Cadena de Octetos: Puede tener un valor de 0 a 255 y se usa para identificar una comunidad.

2.6. ELEMENTOS DE PROCEDIMIENTO

Se describirán a continuación las acciones que realiza una entidad de protocolo en una implementación SNMP. Definiremos dirección de transporte como una dirección IP seguida de un número de puerto UDP (Si se está usando el servicio de transporte UDP).

Cuando una entidad de protocolo envía un mensaje, realiza las siguientes acciones:

1. Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1
2. Pasa esta PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autentificación. Este servicio generará en respuesta otro objeto en ASN.1
3. La entidad construye ahora un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autentificación y el nombre de comunidad.
4. Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.

Cuando una entidad de protocolo recibe un mensaje, realiza las siguientes acciones:

Hace un pequeño análisis para ver si el datagrama recibido se corresponde con un mensaje en ASN.1. Si no lo reconoce, el datagrama es descartado y la entidad no realiza más acciones.

1. Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.
2. Pasa los datos de usuario, el nombre de comunidad y las direcciones de transporte de fuente y destino al servicio de autentificación. Si es correcto, este devuelve un objeto ASN.1. Si no lo es, envía una indicación de fallo. Entonces la entidad de protocolo puede generar una trampa (trap), descarta el datagrama y no realiza más acciones.
3. La entidad intenta reconocer la PDU. Si no la reconoce, descarta el datagrama. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU. Si la PDU exige respuesta, la entidad iniciará la respuesta al instante.

2.7. ESTRUCTURA DE UNA PDU

Los datos que incluye una PDU genérica son los siguientes:

- RequestID: es un número, el cual indica el orden de emisión de los datagramas. Este parámetro sirve también para identificar datagramas duplicados en los servicios de datagramas poco fiables.
- ErrorStatus: número que indica si ha existido un error. Puede tomar los siguientes valores, que se explicarán posteriormente:

- noError (0)
- tooBig (1)
- noSuchName (2)
- badValue (3)
- readOnly (4)
- genErr (5)

- ErrorIndex: numero que en el caso de error indica qué variable de una lista ha generado ese error.
- VarBindList: Lista de nombres de variables con su valor asociado. Algunas PDU quedan definidas sólo con los nombres, pero aún así deben llevar valores asociados. Se recomienda para estos casos la definición de un valor NULL.

✧ GetRequest-PDU y GetNextRequest-PDU

Son PDU's que solicitan a la entidad destino los valores de ciertas variables. En el caso de GetRequest-PDU estas variables son las que se encuentran en la lista VarBindList; en el de GetNextRequest-PDU son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista. Como se puede observar, GetNextRequest-PDU es útil para confeccionar tablas de información sobre un MIB. Siempre tienen a cero los campos ErrorStatus y ErrorIndex. Son generadas por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Estas PDU's siempre esperan como respuesta una GetResponse PDU.

- ✧ SetRequest-PDU

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

- ✧ GetResponse-PDU

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

Cuando una entidad de protocolo recibe una GetRequest-PDU, una SetRequest-PDU o una GetNextRequest-PDU, sigue las siguientes reglas:

1. Si algún nombre de la lista (o el sucesor lexicográfico de un nombre en el caso de GetNextRequest-PDU) no coincide con el nombre de algún objeto en la vista del MIB al que se pueda realizar el tipo de operación requerido ("set" o "get"), la entidad envía al remitente del mensaje una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 2 (noSuchName), y con el campo ErrorIndex indicando el nombre de objeto en la lista recibida que ha originado el error.
2. De la misma manera actúa si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era una GetRequest-PDU.

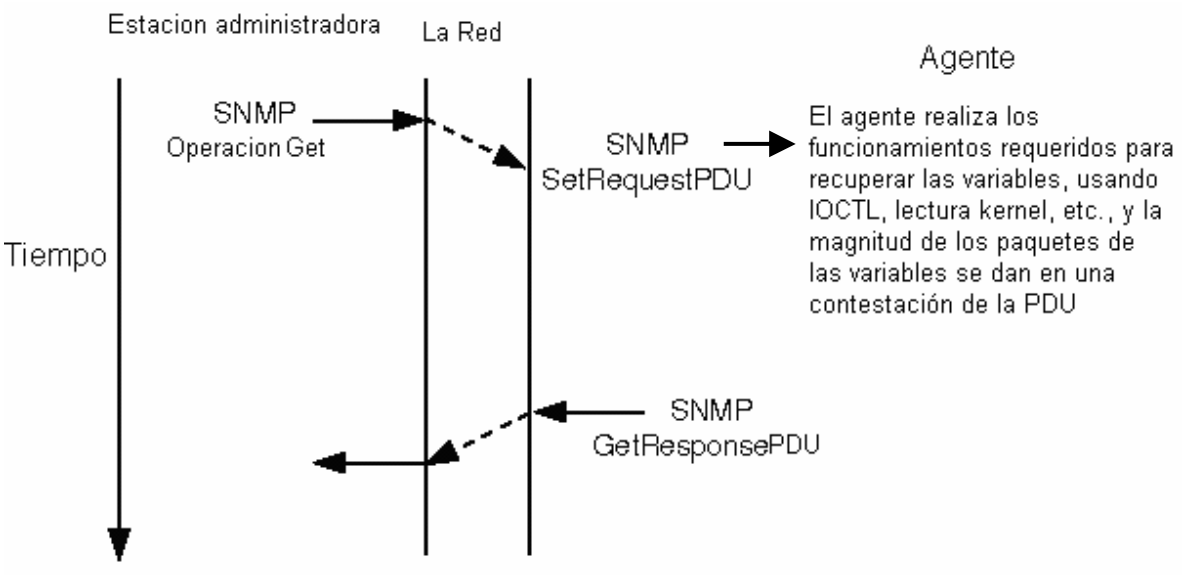
3. Si se ha recibido una SetRequest-PDU y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, salvo en que el campo ErrorStatus tendrá el valor 3 (badValue) y el campo ErrorIndex señalará el objeto de la lista que ha generado el error.
4. Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 1 (tooBig).
5. Si el valor de algun objeto de la lista no puede ser obtenido (o alterado, según sea el caso) por una razón no contemplada en las reglas anteriores, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 5 (genErr), y el campo ErrorIndex indicando el objeto de la lista que ha originado el error.

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

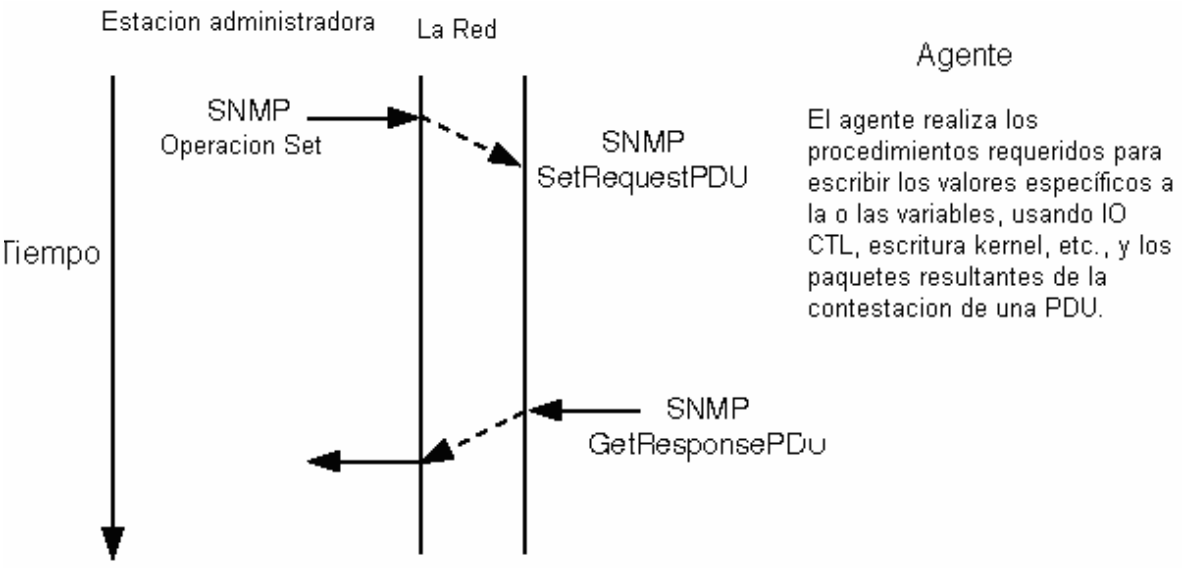
- Si es una respuesta a una GetResponse-PDU, tendrá la lista varBindList recibida, pero asignando a cada nombre de objeto el valor correspondiente.
- Si es una respuesta a una GetNextResponse-PDU, tendrá una lista varBindList con todos los sucesores lexicográficos de los objetos de la lista recibida, que estén en la vista del MIB relevante y que sean susceptibles de ser objeto de la operación "get". Junto con cada nombre, aparecerá su correspondiente valor.

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

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



(a)



(b)

Figura 6. (a) Diagrama de flujo para la operación Get / Getnext y (b) Diagrama de flujo para la operación Set

✧ Trap PDU

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

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

- enterprise: tipo de objeto que ha generado la trampa.
- agent-addr: dirección del objeto que ha generado la trampa.
- generic-trap: entero que indica el tipo de trampa. Puede tomar los siguientes valores:
    - coldStart (0)
    - warmStart (1)
    - linkDown (2)
    - linkUp (3)
    - authenticationFailure (4)
    - egpNeighborLoss (5)
    - enterpriseSpecific (6)
- specific-trap: entero con un código específico.
- time-stamp: tiempo desde la última inicialización de la entidad de red y la generación de la trampa.
- variable-bindings: lista tipo varBindList con información de posible interés.

Dependiendo del valor que tenga el campo generic-trap, se iniciarán unas u otras acciones:

- Trampa de arranque frío (coldStart): La entidad de protocolo remitente se está reinicializando de forma que la configuración del agente o la implementación de la entidad de protocolo puede ser alterada.
- Trampa de arranque caliente (warmStart): La entidad de protocolo remitente se está reinicializando de forma que ni la configuración del agente ni la implementación de la entidad de protocolo se altera.
- Trampa de conexión perdida (linkDown): La entidad de protocolo remitente reconoce un fallo en uno de los enlaces de comunicación representados en la configuración del agente. Esta Trap-PDU contiene como primer elemento de la lista variable-bindings el nombre y valor del interfaz afectado.
- Trampa de conexión establecida (linkUp): La entidad de protocolo remitente reconoce que uno de los enlaces de comunicación de la configuración del agente se ha establecido. El primer elemento de la lista variable protegida es el nombre y el valor del interfaz afectado.
- Trampa de fallo de autentificación (authentication Failure): La entidad de protocolo remitente es la destinataria de un mensaje de protocolo que no ha sido autentificado.
- Trampa de pérdida de vecino EGP (egpNeighborLoss): Un vecino EGP con el que la entidad de protocolo remitente estaba emparejado ha sido seleccionado y ya no tiene dicha relación. El primer elemento de la lista de

las variables protegidas es el nombre y el valor de la dirección del vecino afectado.

- Trampa específica (enterprise Specific): La entidad remitente reconoce que ha ocurrido algún evento específico. La posición especifica o specific-trap identifica qué trampa en particular se ha generado.

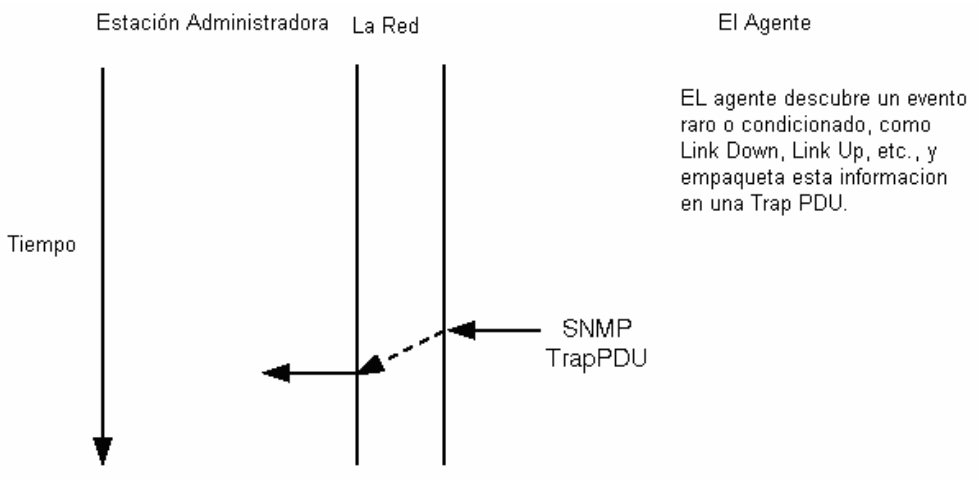


Figura 7. Diagrama de flujo para las operaciones Trap.

SNMPv1

En esta sección se apreciará de una manera descriptiva el desarrollo la primera versión del protocolo SNMP haciendo especial énfasis en sus características y estableciendo las bondades y deficiencias que trae consigo la implementación inicial del protocolo.

3. SNMPv1

SNMP versión 1 (SNMPv1) es la aplicación inicial del protocolo de SNMP. Se describe en el Request For Comments (RFC) 1157 y las funciones dentro de las especificaciones de la Estructura de Información de Dirección (SMI). SNMPv1 opera encima de los protocolos como: el Usuario el Protocolo de Datagrama (UDP), Protocolo de Internet (IP), Red de Servicio OSI sin conexión (CLNS), Protocolo de Entrega de Datagramas AppleTalk (DDP), y el Intercambio de Paquetes Novell (IPX). SNMPv1 se usa ampliamente y es el protocolo de administración de red de *de Facto* en la comunidad de Internet.

La Estructura de Información de Dirección (SMI) define las reglas por describir la información de dirección, usando la notación de Sintaxis Abstracta Uno (ASN.1). El SNMPv1 SMI se define en RFC 1155. El SMI hace tres característica técnicas importantes: El tipo de datos en ASN.1, los tipos de datos específicos SMI y las tablas del MIB del SNMP.

3.1. SNMPv1 Y LOS TIPOS DE DATOS EN ASN.1

El SMI SNMPv1 especifica que todos los objetos manejados tienen cierto subconjunto de tipos de datos de la Sintaxis Abstracta de Anotación Uno (ASN.1) asociados a ellos. Se requieren tres tipos de datos ASN.1: nombre, sintaxis, y codificación. El nombre sirve como el identificador del objeto (el objeto ID). 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 codificados describen cómo la información asociada a un objeto manejado se ajusta al formato como serie de artículos de datos para la transmisión sobre la red.

3.2. SNMPv1 Y LOS TIPOS DE DATOS ESPECÍFICOS SMI

El SMI SNMPv1 especifica el uso de un número de tipos de datos SMI, que se dividen en dos categorías: tipos de datos simples y tipos de aplicación de datos de gran capacidad.

Tres tipos de datos simples se definen en el SMI SNMPv1, que son valores únicos: números enteros, secuencias del octeto, e identificaciones del objeto. Los tipos de datos del número entero es un entero con signo en el intervalo de -2.147.483.648 a + 2.147.483.647. Las cadenas de octetos son las sucesiones que van desde 0 a 65,535 octetos. Las direcciones del objeto vienen del sistema de todos los identificadores del objeto asignados según las reglas especificadas en ASN.1.

Siete tipos de aplicación de los datos extensos existen en el SNMPv1 SMI: las direcciones de la red, contadores, calibradores, señales de tiempo, protecciones, números enteros, y los números enteros sin signo. Las direcciones de la red representan una dirección de una familia protocolar particular. SNMPv1 soporta sólo 32-bits de las direcciones IP. Los contadores son enteros no negativos que aumentan hasta que ellos alcancen un valor máximo y entonces vuelven para

ponerse en cero. En SNMPv1, se especifica un contador de 32-bits. Los calibradores son enteros no negativos que pueden aumentar o pueden disminuir pero pueden retener el valor máximo alcanzado. Una señal de tiempo representa una centésima de segundo desde que pasa algún evento. Una protección representa una codificación arbitraria que se usa para pasar cordones de información arbitrarios que no conforman los datos al ser escritos de manera específica, que son usados por el SMI. Un número entero representa la información que es tasada o estimada. Este tipo de datos redefine los números enteros y que tiene la precisión arbitraria en ASN.1 pero esa precisión esta limitada en el SMI.

Un número entero sin signo representa la información que no es tasada o estimada y es útil cuando los valores siempre son no negativos. Este tipo de datos redefinen los datos de los números enteros que tienen la precisión arbitraria en ASN.1 pero precisión limitada en el SMI.

3.3. TABLAS DEL MIB DEL SNMP

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

3.4. OPERACIONES DEL PROTOCOLO SNMPv1

SNMP es un protocolo simple de demanda y de la contestación. El sistema de administración de red emite una demanda, y los dispositivos devuelven las contestaciones. Esta conducta se lleva a cabo usando uno de cuatro funcionamientos protocolares: Get, GetNext, Set, y Trap. El funcionamiento del Get se usa por el NMS para recuperar el valor de uno o más casos del objeto de un agente. Si el agente que responde a la operación hecha por el Get no puede mantener los valores en todos los casos del objeto en una lista, este no proporcionara ningún valor. El funcionamiento de GetNext se usa por el NMS para recuperar el valor del próximo caso del objeto en una tabla o una lista dentro de un agente. El funcionamiento del Set se usa por el NMS para poner los valores de éste en un objeto dentro de un agente. El Trap es utilizado por los agentes para informar al NMS de manera asincrónica de un evento significante.

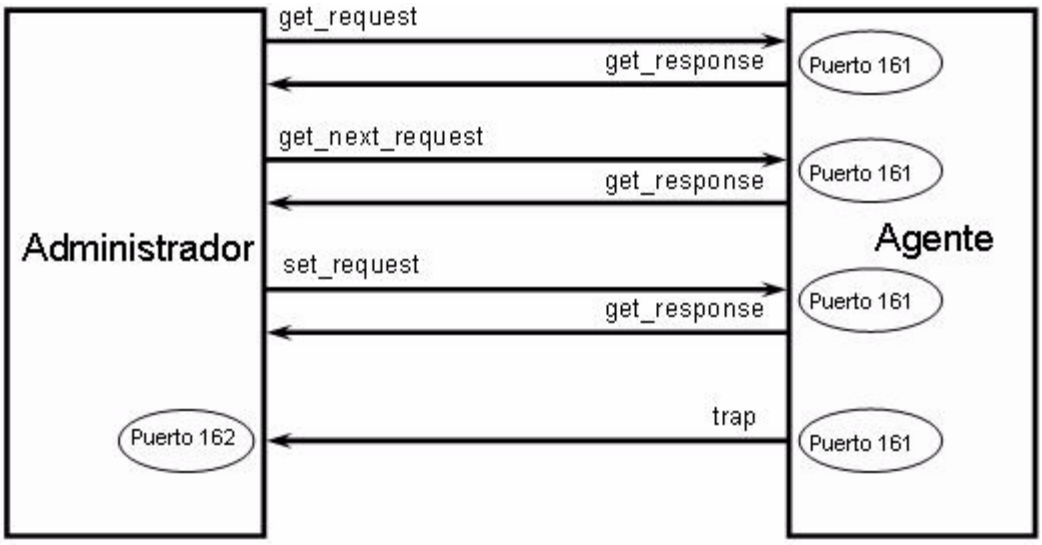


Figura 8. Proceso de comunicación entre el administrador y el agente.

3.5. FORMATO DEL MENSAJE DE SNMPv1

Los mensajes de SNMPv1 contienen dos partes: un título del mensaje y una unidad del datos protocolar (PDU). La siguiente figura ilustra el formato básico de un mensaje de SNMPv1, la cual consiste en un Título y una unidad de PDU.

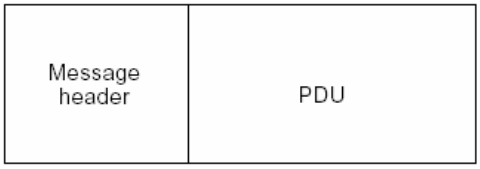


Figura 9. Estructura de un mensaje SNMPv1.

Los SNMPv1 contienen dos campos en la cabecera del titulo: El Número de la versión y el Nombre de la Comunidad que es como un estilo de contraseña y en el campo de la PDU puede tener una o mas de éstas, esto se asume como una autenticación trivial.

Las descripciones siguientes resumen estos campos:

- ✧ Número de versión: Especifica la versión de SNMP que se usó.
- ✧ El nombre del grupo: Define un ambiente de acceso para un grupo de NMSs. Se dicen NMSs dentro del grupo para existir dentro del mismo dominio administrativo. El nombre del grupo sirve como un formulario débil de autenticación porque se evitan dispositivos que no saben el nombre de la comunidad no son apropiados para el funcionamiento de las operaciones del SNMP.

3.6. UNIDAD DE DATOS DEL PROTOCOLO (PDU)

Las PDU del protocolo SNMPv1 contienen un orden específico (Get, Set, etc) y las operaciones que indican los casos del objeto involucrados en la transacción de datos. Los campos de la PDU en SNMPv1 son variables en longitud, según lo prescrito en ASN.1.

La siguiente grafica muestra los campos del SNMPv1, tales como Get, GetNext, Response y las transacciones (Set) de PDUs Fijas.

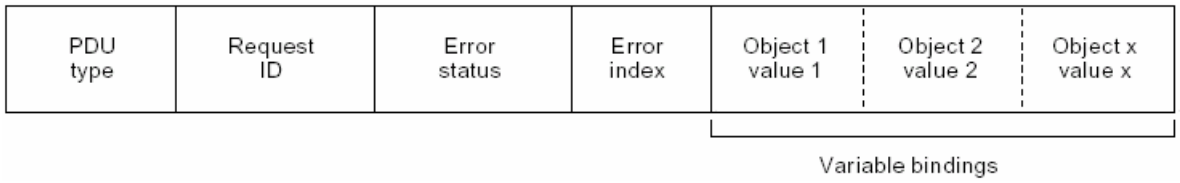


Figura 10. Campos de un mensaje de SNMPv1.

Las siguientes descripciones resumen los campos ilustrados en la figura:

- ✧ Tipo de PDU: especifica el tipo de PDU transmitido.
- ✧ La identificación de la petición: asocia peticiones del SNMP a las respuestas.
- ✧ El error de estado: indica un número de errores y de tipos de error. Sólo el funcionamiento de la contestación utiliza este campo. Otras operaciones fijan este campo en cero.
- ✧ El índice de error: asocia un error a un caso particular del objeto. Sólo el funcionamiento de la contestación maneja este campo. Otras operaciones fijan este campo en cero.

- ✧ Variables enlazadas: sirven como la zona de informaciones de la PDU del SNMPv1. Cada enlace de la variable asocia un caso particular del objeto a su valor actual (a excepción de las peticiones Get y de GetNext, para estas peticiones se ignora el valor).

3.6.1. FORMATO TRAP DE LA PDU

El siguiente diagrama muestra los campos de la Trap (trampa) de la PDU de SNMPv1.

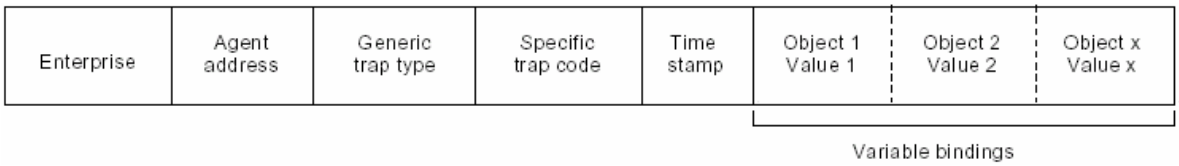


Figura 11. Campos de un mensaje TRAP.

Las descripciones siguientes resumen los campos ilustrados:

- ✧ Enterprise: Identifica el tipo de objeto manejado que genera la trampa.
- ✧ La dirección del agente: Proporciona la dirección del objeto manejado que genera la trampa.
- ✧ El tipo de la trampa genérica: Indica uno de varios tipos de la trampa genéricos.
- ✧ El código de la trampa específico: Indica uno de varios códigos de la trampa específicos.
- ✧ Control de tiempo: proporciona la cantidad de tiempo que ha transcurrido entre la reiniciación de la red y la generación de la trampa.

- ✧ Variables enlazadas: Es la zona de informaciones de la PDU de la trampa SNMPv1. Cada atascamiento de la variable asocia un caso particular del objeto a su valor actual.

3.7. LOS PROTOCOLOS DE COMUNICACIÓN SUBYACENTES

SNMP asume que ningún camino de comunicación es organizado de antemano y se establece anterior a la transmisión de datos. Como resultado, SNMP no hace ninguna garantía sobre la entrega fiable de los datos aunque en la práctica la mayoría de los mensajes termina, y los que no, no pueden ser retransmitidos. Los protocolos primarios que implementa SNMP son el Protocolo de Datagrama de Usuario (UDP) y el Protocolo de Internet (IP). SNMP también requiere los protocolos de enlace de datos tales como Ethernet o Token Ring que establecen la comunicación entre el administrador y el agente manejado.

La simplicidad de SNMP y la no conexión de la comunicación también producen un grado de robustez; ni el administrador ni el agente confía en el otro para su funcionamiento. Así, un administrador puede continuar funcionando aun cuando un agente remoto falla. Cuando el agente vuelve a la red, puede enviar una trampa al administrador, para notificarle de su cambio en el estado de operación. Esta característica le permite el descubrimiento y la reparación del error a la NMS (Estación administradora de red) e incluso al agente. Sin embargo hay que tener presente que SNMP es de hecho un transporte independiente (aunque el diseño original era el transporte orientado a la no conexión, función que corresponde al

protocolo UDP) y también puede llevarse a cabo en otros transportes, como lo son:

TCP (Orientado a conexión).

Mapping directo hacia Ethernet a nivel de las MAC.

Encapsulamiento en el protocolo X.25.

Encapsulamiento en una celda de ATM.

3.7.1. MECANISMO DE TRANSPORTE DE SNMP UTILIZANDO UDP

Los siguientes diagramas representan la forma de cómo se realiza el proceso de comunicación entre el administrador y los equipos monitoreados vía UDP:

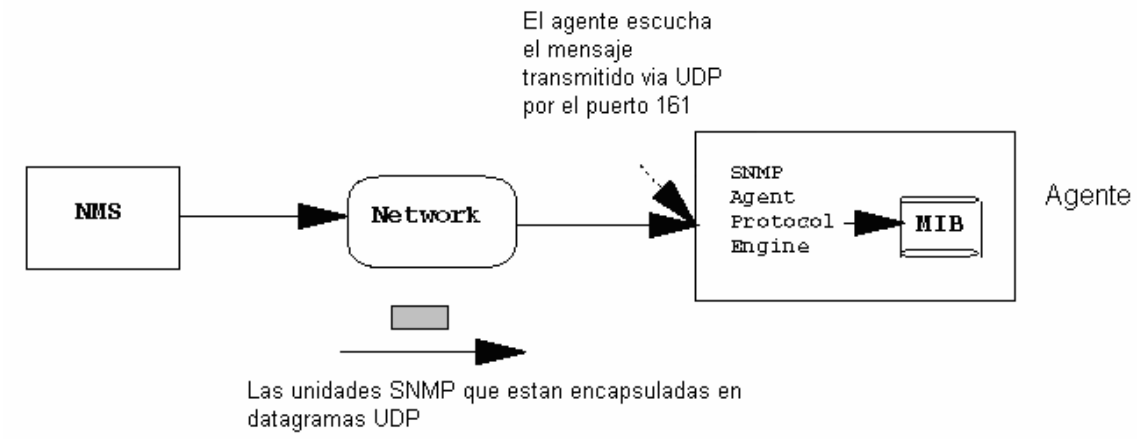
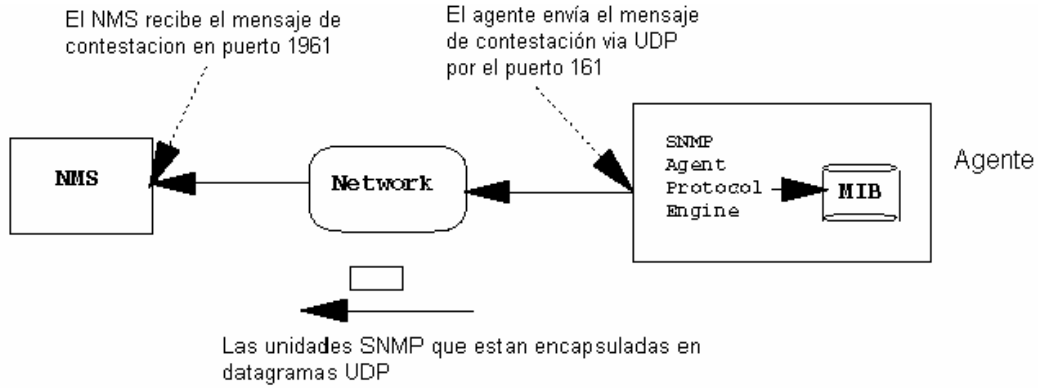


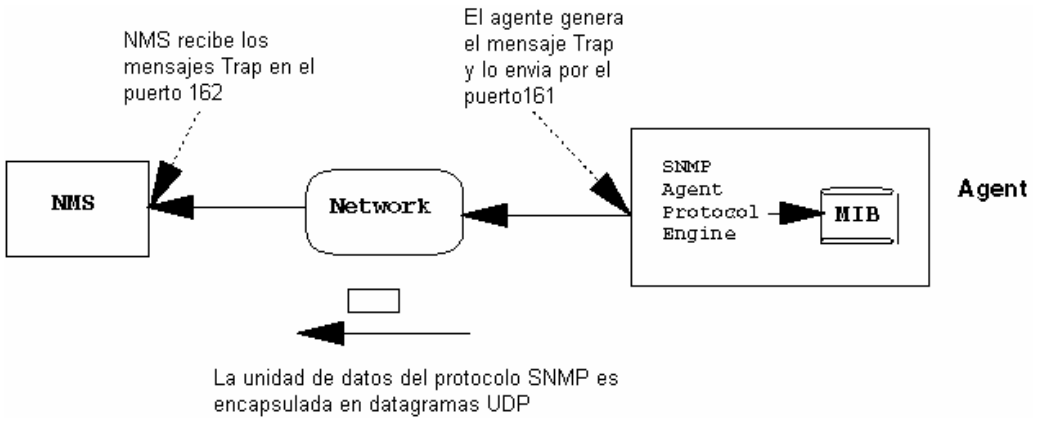
Figura 12. Proceso de comunicación entre el administrador y equipos monitoreados.

3.7.2. TRANSPORTE UDP.

- El agente escucha por el puerto 161.
- Las contestaciones son enviadas al puerto NMS (Network Managment Station) de donde se originó el mensaje, desde un puerto dinámico, aunque muchos agentes utilizan el puerto 161 para este propósito.
- El tamaño máximo del mensaje de SNMP esta limitado por el tamaño máximo de UDP (i.e 65535 octetos).
- Todas las aplicaciones de SNMP tienen que recibir los paquetes que tienen por lo menos 484 octetos en la longitud.
- Algunas aplicaciones de SNMP pueden ser incorrectas o que exceden paquetes de 484 octetos.
- Los Traps asincrónicos son recibidos en el puerto 162 del NMS.
- UDP es más conveniente que TCP cuando los cambios de la ruta dinámicos ocurren a menudo, un ejemplo es cuando hay problemas en la red.
- Los paquetes de UDP minimizan las demandas puestas en la red (ningún recurso esta orientado a modo de conexión).
- El agente y el NMS son responsables para determinar la recuperación del error.



(a)



(b)

Figura 13. (a) Arquitectura de transporte de UDP y (b) Transporte asincrónico del Trap.

SNMPv2

A continuación se describe la implementación de las mejoras iniciales hechas a la primera versión del protocolo obtenidas luego de la revisión de sus características y funcionalidad. También se conocerá la transición entre versiones luego de realizadas dichas mejoras.

4. SNMPv2

La primera revisión a SNMP se publicó en marzo de 1991, como MIB-II[4]. Entre sus muchas novedades, se expandió la lista de objetos usada para las redes administradas y se reformaron algunas de las definiciones originales. A finales de 1992, la industria de la red reconoció que SNMP se convirtió en el *de facto* estándar y que estaba hecho para una extensa duración. Pronto surgieron las propuestas para mejorarlo no solo centrándose en la corrección de los MIBs.

Por ejemplo, había una necesidad desesperada de una mejor seguridad. Con la especificación de SNMP existente, usted no podía autenticar la fuente de un mensaje de dirección o prevenir la intromisión de agentes externos. Sin la capacidad de la autenticación, SNMP era vulnerable a ataques que podrían modificar o desactivar las configuraciones de la red. Como resultado, muchos vendedores del equipo de SNMP escogieron no llevar a cabo el comando Set de SNMP el cual permite cambiar la configuración de un agente; esto redujo las capacidades de cambiar la configuración de un agente lo que redujo las opciones de administración en los equipos de monitoreo de redes.

Otro aspecto para mejorar era el comportamiento. Esto se implementa en SNMPv2 con la introducción de un PDU llamado GetBulk que reduce el número de demandas y contestaciones, razón por la cual se mejora la recuperación de los árboles de MIB enteros. Se agregaron otros PDUs también.

Un tercer ítem en la lista de mejoras era el de poder compartir la información entre administradores. Las grandes redes tienen administración distribuida, para poder atender a los agentes más lejanos. El modelo de una sola aplicación del administrador no aplicó.

La mayoría de las redes de hoy en día usan protocolos mixtos. Mientras los dispositivos de protocolo mixto se encaminan a mejorar el MIB-II, SNMP permitió la comunicación entre sus agentes y administradores solo en las redes de UDP/IP.

Estas mejoras se delinearon en el mes de abril de 1993, en los IETF RFCs 1441 hasta el 1452. Aunque ellos están todavía en la fase de propuesta, algunos diseñadores están llevando a cabo las reformas aprobadas.

4.1. MEDIDAS DE SEGURIDAD

Las nuevas características de la seguridad de SNMPv2[5] se diseñan para proporcionar tres servicios seguridad que están relacionados: privacidad, autentificación del mensaje, y control de acceso.

La privacidad es la protección de los datos transmitidos contra los puertos que se encuentran activos, ya sea escuchando o tratando de interceptar paquetes en la red. La privacidad requiere que el contenido de cualquier mensaje esté disfrazado de modo que solamente el agente previsto pueda recuperarla.

La autenticación del mensaje habilita secciones de las comunicaciones para verificar que nadie ha alterado los mensajes recibidos y que sus fuentes son

---

[4] RFC 1213

auténticas. Esto incluye la verificación de la puntualidad de un mensaje para asegurarse de que no se haya retrasado y reproducido.

El control de acceso se asegura de que solamente los usuarios autorizados tengan acceso a un Management Information Base particular.

La seguridad del SNMP utiliza los conceptos del partido y del contexto. Un partido es un administrador o un agente con los atributos de seguridad asignados. Un contexto especifica si un intercambio entre un administrador y un agente involucra datos que son local al agente (en que el caso el contexto indica el subconjunto pertinente de la información de dirección del agente) o si involucra un dispositivo remoto para que el agente actúe como un apoderado (en este caso el contexto identifica el dispositivo más cercano de la red).

Como con SNMPv1, SNMPv2 se realiza el intercambio de la información en forma de un mensaje que incluye una cabecera y uno de varios tipos de PDU diferentes; cada PDU especifica un funcionamiento particular de administración. La cabecera del mensaje consiste en cinco campos requeridos: un campo de la sección de destino; un campo de la sección de la fuente; un campo del contexto; un campo de la autenticación que contiene la información sobre el nivel deseado de la autenticación; y un campo para presentar el nivel de privacidad de destino, que repite el identificador del agente destino.

---

[5] http://www.ietf.org/rfc/rfc2261.txt

Cuando se proporciona el nivel de privacidad, entonces el mensaje entero, incluso la cabecera y la PDU, pero excluyendo el campo de la sección de destino, se encripta. El campo o la sección de destino debe seguir siendo sin encriptar, para que el modulo de destino SNMP puede determinar el destinatario y las características de la privacidad del mensaje.

Para tener un nivel de privacidad, SNMPv2 usa el tipo de encriptación DES; para la autenticación, usa RSA (Rivest-Shamir-Adleman) la encriptación combinó funciones con el MD5 (el Compendio del Mensaje versión 5). Los últimos dos algoritmos tienen los mismos usos que el PGP (el Retiro Bastante Bueno). La autentificación también requiere que un mensaje, el cual tiene que ser oportuno para asegurarse de que no se ha retrasado y no se ha retransmitido.

SNMPv2 proporciona su tercera facilidad de seguridad mayor, la capacidad del control de acceso, a través de dos conceptos: Una vista de la sub estructura que consiste en un nodo en la estructura del MIB con todos sus elementos subordinados. Asociado con cada SNMP que el dispositivo lógico es una vista de MIB que consiste en un juego de subtrees de vista. Cada subtree de vista en la vista de MIB incluye o excluye todos los objetos que están contenidos en las subdivisiones. Asociado con cada contexto local de una entidad de SNMPv2 es una vista de MIB que define el Set de objetos que son visibles en este contexto; alternativamente, el contexto especifica que un administrador puede tener información de un dispositivo remoto de la red.

Cada fila de esta lista incluye varios elementos: el punto de partida, en el cual una de las funciones de operación de los administradores es forzar para que se cumplan estos privilegios de acceso; la sección del Subject, cuyos requerimientos para las operaciones del administrador son las de mantener este sistema de privilegios de acceso; El contexto que utiliza un subject para tener acceso a una blanco; y un número entero que codifica los privilegios del acceso para estos tres elementos target/subject/context. El elemento del número entero es, en efecto, una lista de las operaciones permisibles de la gerencia (es decir, PDUs) para este par de partidos usando este contexto.

4.2. EJECUCIÓN Y DESEMPEÑO

En el uso del mundo real, el funcionamiento del SNMP depende de cómo rápidamente los agentes pueden manejar peticiones. El requisito de la anchura de banda de los mensajes del SNMP es trivial, y los administradores están funcionando generalmente con un hardware lo suficientemente robusto para que a este proceso se le de poca importancia.

Pero reduciendo el número de las peticiones y de los mensajes del SNMP que los agentes necesitan generar, su carga es aligerada perceptiblemente. Porque muchas peticiones están para los bloques grandes de los objetos del MIB, el concepto de una operación de GetBulk es una manera obvia de aumentar funcionamiento. Después de todo, un agente puede procesar un pedido de varias entradas de la tabla casi tan rápidamente como puede para una sola entrada.

Por ejemplo, una estadística histórica de RMON típicas en las MIB puede tener 200 entradas. Sin una operación de GetBulk, el software de la gerencia que recupera esta información generaría 200 peticiones y 200 contestaciones. Con una operación de GetBulk, necesitan solamente de una petición y una contestación.

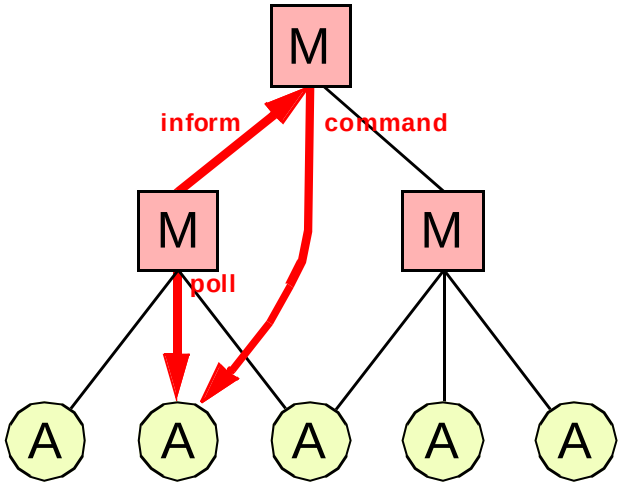
El problema de compartir la información del gerente también se resuelve por la abstracción de la sección. Una sección puede ser agente o administrador. Como agente, una sección esta definida por su MIB. Como administrador, apenas lee y entiende el mismo MIB. Así, el IETF es necesitado para realizar intercambio de l MIB entre administradores[6]. Con este MIB y la abstracción de la sección, cualquier administrador puede actuar como agente a cualquier otro gerente, pero solamente dentro de los apremios del MIB Es innecesario decir, que el control de acceso y otras medidas de seguridad son indispensables para a llevar a cabo las comunicaciones y el control entre los administradores.

4.3. LOS CUATRO REALCES PRINCIPALES DE SNMPV2.

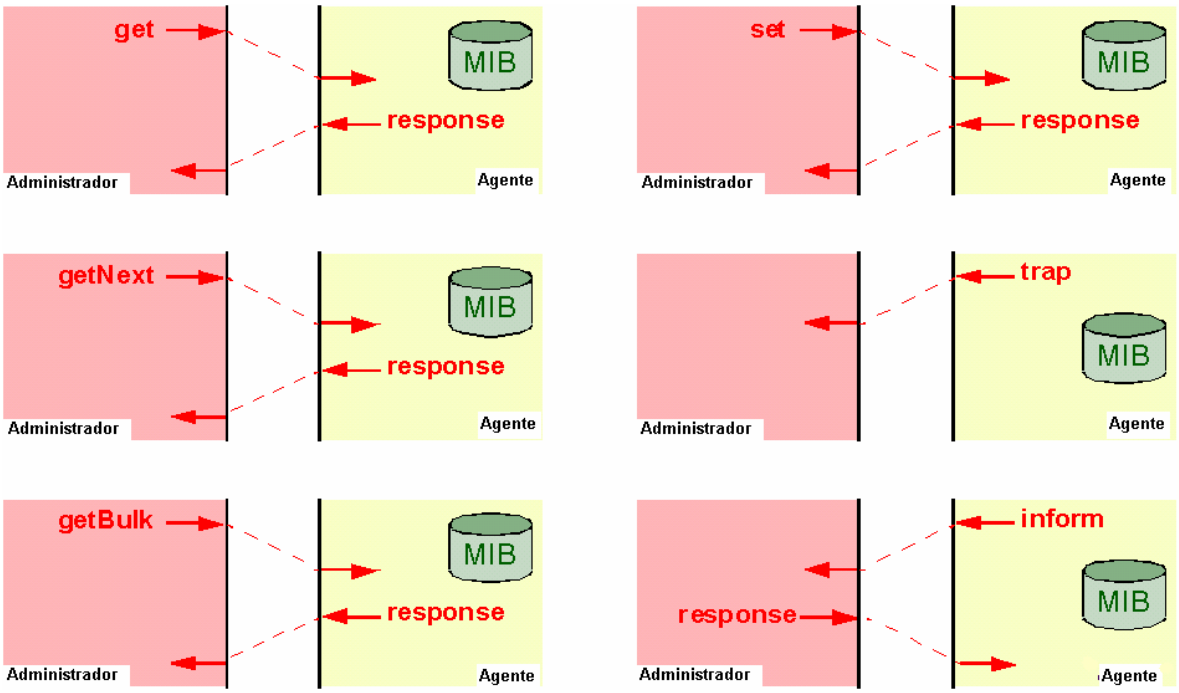
Los cuatro realces principales de la segunda versión de este protocolo son:

1. Ofrece una seguridad mejor agregando la autentificación de la petición.
2. Proporciona un funcionamiento mejor para las transferencias de las tablas.
3. Los encargados pueden compartir la información actuando como agentes.
4. El SNMP se está abriendo a otros protocolos subyacentes.

[6] RFC 1451



(a)



(b)

Figura 14. (a) Comunicación entre administradores (b) Operaciones del protocolo SNMPv2.

4.4. COEXISTENCIAS ENTRE SNMPv1 Y SNMPv2

Para garantizar la compatibilidad y coexistencia de las dos versiones del protocolo SNMP hay que tener encuesta las siguientes observaciones:

- ✦ Información de gestión

La forma que tiene SNMPv2 para manejar los objetos gestionados no es más que una extensión de SNMPv1. Así, ambas versiones utilizan el lenguaje ASN.1 para la notación. De hecho, lo que hace principalmente la versión 2 es normalizar la forma de definir los módulos MIB.

Para que un módulo MIB o una declaración en SNMP se haga compatible con SNMPv2 se necesita una serie de cambios. Normalmente estos cambios no exigen la invalidación de los objetos que contiene, ya que no son cambios muy drásticos. Son cambios referentes al vocabulario o la sintaxis (por ejemplo el guión se convierte en carácter prohibido en los nombres de variables), a definición de nuevos tipos, o a la conversión de ciertas partes del MIB de opcionales a obligatorias (por ejemplo, ahora todos los objetos deben tener una cláusula DESCRIPTION). Hay cambios que son obligatorios y hay cambios que son sólo recomendados.

- ✦ Operaciones de protocolo

Se considerarán dos áreas: el comportamiento del intermediario entre una entidad SNMPv2 y un agente SNMPv1, y el comportamiento de entidades de protocolo bilingües actuando como administradoras.

- ✦ *Comportamiento de un agente intermediario.*

Para conseguir la coexistencia a nivel de protocolo, se puede utilizar un mecanismo intermediario. Una entidad SNMPv2 actuando como agente puede ser implementada y configurada para realizar esta labor.

4.5 PASO DE SNMPV1 A SNMPV2

Para convertir respuestas enviadas de una entidad SNMPv1 agente hacia una entidad SNMPv2 administradora:

1- Si es una GetResponse-PDU, pasa por el intermediario sin alteraciones. No obstante hay que observar que aunque una entidad SNMPv2 nunca generará una PDU de respuesta con un campo error-status con un valor de "noSuchName", "badValue" o "readOnly", el agente intermediario no debe cambiar este campo. Así la entidad administradora podrá interpretar la respuesta correctamente.

Si se recibe una GetResponse-PDU con el campo error-status con el valor "tooBig", el intermediario eliminará los contenidos del campo de la variable bindings antes de propagar la respuesta. También aquí hay que señalar que aunque una entidad SNMPv2 nunca enviará una PDU de respuesta con un "tooBig" ante una GetBulkRequest-PDU, el agente intermediario debe propagar dicha respuesta.

2- Si se recibe una Trap-PDU, se convertirá en una Trap-PDU de SNMPv2. Esto se consigue colocando en el campo de la variable bindings dos nuevos elementos: sysUpTime.0, que toma el valor del campo time stamp de la

Trap-PDU, y snmp Trap OID.0, que se calcula así: Si el valor del campo generic-trap es "enterprise Specific", entonces el valor usado es la concatenación del campo enterprise de la PDU con dos subidentificadores: '0', y el valor del campo specific-trap. Si no es así, se utiliza el valor definido para las Trap-PDU en la versión 2. En este caso se pone un elemento más en el campo de la variable bindings: snmp Trap Enterprise.0, que toma el valor del campo enterprise de la PDU. Los destinos de esta Trap-PDU versión 2 se determinan según la implementación del agente intermediario.

4.6. PASO DE SNMPv2 a SNMPv1

Para convertir peticiones de una entidad SNMPv2 administradora en peticiones a una entidad SNMPv1 agente:

1. Si es una GetRequest-PDU, una GetNextRequest-PDU o SetRequest-PDU, el agente intermediario la pasa sin alterar.
2. Si es una GetBulkRequest-PDU, el intermediario pone los campos non-repeaters y max-repetitions a cero, y la convierte en una GetNextRequest-PDU.

- ✦ Comportamiento de un administrador bilingüe

Para conseguir la coexistencia a nivel de protocolo, una entidad de protocolo actuando como administradora podría soportar las dos versiones de SNMP. Cuando una aplicación de administración necesita contactar con una entidad de protocolo agente, la entidad administradora consulta una base de datos local

para seleccionar el protocolo de gestión adecuado. Para dar transparencia a las aplicaciones, la entidad administradora debe mapear las operaciones como si fuera un agente intermediario.

4.7. EVOLUCIÓN HISTÓRICA DE SNMPv2 A SNMPv3

Con el SNMPv2C se utilizó autentificación basada en los llamados "community strings". Posteriormente sacaron una versión mejorada que se llamó SNMPv2U y que contenía como componente mejorado la autenticación orientada a usuarios.

En la versión SNMPv2P se introdujeron muchas mejoras, pero su estudio y puesta en marcha anterior las versiones 2C & 2U. La versión más avanzada del SNMPv2 es el SNMPv2*, combina lo mejor de todas las anteriores. Nunca se publicaron RFC's al respecto

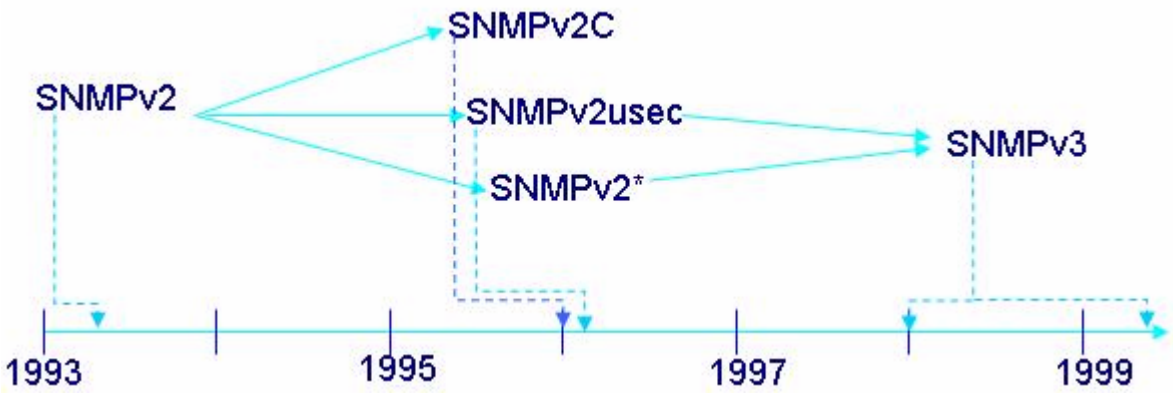


Figura 15. Evolución de SNMPv2.

SNMPv3

En este capítulo se hace una descripción de las respectivas mejoras realizadas en la última versión del protocolo. Se mostraran los últimos adelantos en la capacidad del mensaje del protocolo y en especial el avance obtenido en el campo de la seguridad de transmisión y recepción de comandos.

5. SNMPv3

Para corregir las deficiencias de seguridad que hasta ahora se venia teniendo en las versiones anteriores, se realizaron una serie de RFC´s[7], estas recomendaciones están orientadas a definir una arquitectura y nuevas capacidades en cuanto a seguridad.

SNMPv3 es un protocolo de manejo de red ínter operable, 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.

SNMPv3 proporciona tanto modelos como niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación que es configurada para los usuarios y los grupos en los cuales estos residen. Los niveles de seguridad se refieren al nivel permitido, que puede alcanzar un usuario dentro de un modelo de seguridad. La combinación de ambas cosas determinará que mecanismo de seguridad será el empleado cuando se maneje un paquete SNMP.

[7] RFC´s: 2271 - 2275

5.1. 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. Existen muchos documentos RFC que describen las variables de MIB, cada documento describe un módulo, que es un sub-conjunto de variables relacionadas.

El marco de definición de variables de administración de red debe incluir:

a. Una Estructura Administrativa.
b. Se usa para describir y llevar un seguimiento del reparto del trabajo y la delegación de la autoridad.
c. Una Estructura de Información.

Debido a que la información no es estática, ésta debe estar estructurada de forma tal que sea fácil extender y revisar antiguas tecnologías y a su vez añadir nuevas tecnologías. Para tal fin se creo una Estructura de Nombres que 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 tres requisitos antes mencionados y recibe el nombre de Estructura de Información de Administración (SMI). El SMI está dividido en tres partes:

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

b. Definiciones de Objeto. Se utilizan para describir los objetos manejados y para llevar consistentemente la semántica de un objeto.
c. Definiciones de Notificación. Se usan al describir transmisiones de información de dirección y para llevar consistentemente la sintaxis de una notificación.

5.2. OPERACIÓN DEl PROTOCOLO.

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.

5.3. TRANSPORTE.

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

En el RFC 1906, se establecen las diferentes categorías de transporte.

Aunque se definen varías categorías se seleccionó UDP como el transporte escogido, 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.

5.4. ARQUITECTURA, SEGURIDAD Y ADMINISTRACIÓN.

La arquitectura[8] 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 como los instrumentos en agentes y gerentes).
c. Las Identidades (usuarios de Servicio)
d. La información de dirección, incluyendo apoyo para múltiple contextos lógicos.

La siguiente ilustración muestra un ejemplo de la arquitectura de SNMPv3. Se muestran el subagente de DPI2, smux peer, el administrador de SNMP, y agente de SNMP. También se muestra cómo ellos comunican entre sí.

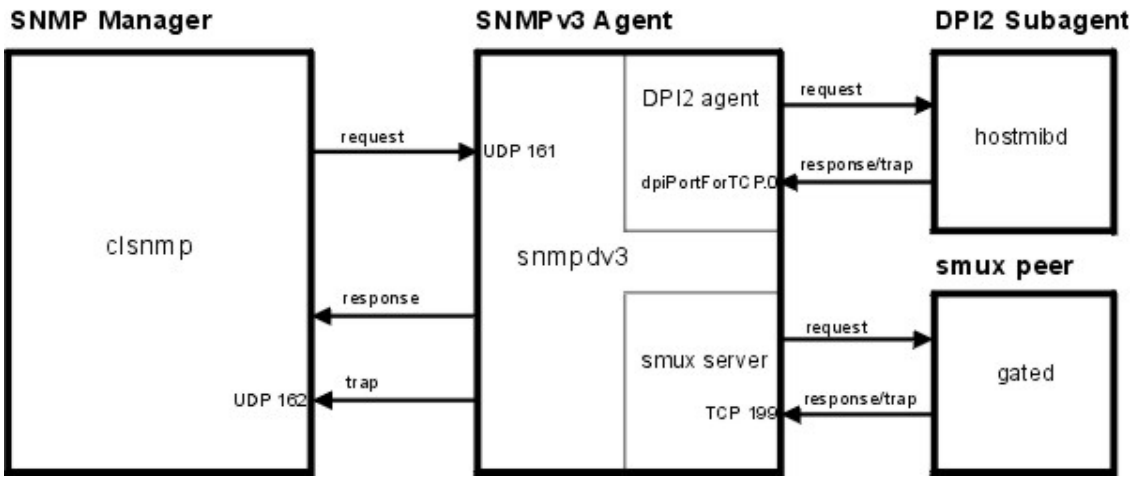


Figura 16. Arquitectura de SNMPv3.

[8] En el RFC 2571 se especifica de forma detallada la arquitectura de SNMPv3.

5.5. LAS ENTIDADES DE SNMPV3

Las entidades SNMPv3 están formadas por un motor y una o varias aplicaciones. Estas entidades tienen una composición modular, por lo que dependiendo de los módulos que se le asignen, se tratará de un gestor, un agente o una combinación de los dos.

Los módulos pueden reemplazarse o actualizarse fácilmente, lo que intenta cumplir con el objetivo de facilitar las actualizaciones del sistema y permitir la compatibilidad con sistemas anteriores.

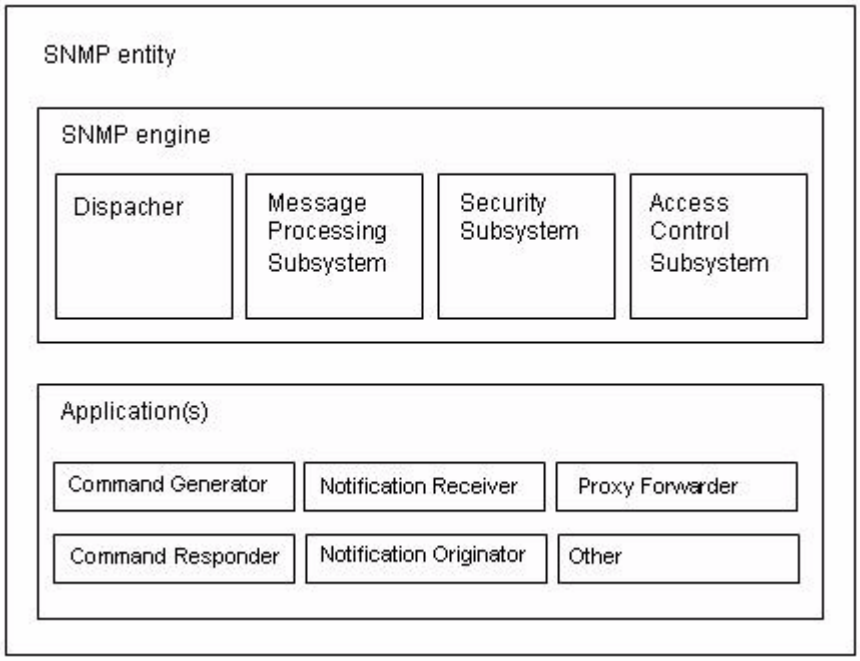


Figura 17. Entidades SNMPv3 según RFC 2571

Un motor SNMP se identifica por la variable snmpEngineID y puede estar formado por los siguientes módulos:

Dispatcher (distribuidor). Message Processing Subsistem (subsistema de proceso de mensajes).

Security Subsistem (Subsistema de seguridad).

Access Control Subsistem (Subsistema de Control de Accesos).

Este motor se acompaña de aplicaciones [RFC 2573], que pueden ser:

Command Generator (Generador de comandos)

Command Responder (Respondedor de Comandos)

Notification Receiver (Receptor de Notificaciones):

Notification Originator (Creador de notificaciones)

Proxy Forwarder

5.5.1. EL DISPATCHER

Es un "manejador de tránsito". Permite soporte a mensajes de múltiples versiones del protocolo SNMP y su tarea es:

Intercambiar mensajes con la red (enviar y recibir mensajes);

Determinar la versión del protocolo SNMP de los mensajes entrantes e interactuar con el subsistema de proceso de mensaje correspondiente para extraer los mensajes entrantes y armar los mensajes salientes;

Proveer una interfaz abstracta a las aplicaciones SNMP para entregar PDUs a las otras aplicaciones y a entidades remotas.

Colecciona estadísticas a cerca de las versiones de mensajes SNMP recibidos y enviados.

Solo puede haber un Dispatcher en una entidad SNMP.

Cuando es necesario preparar un mensaje para enviarlo a través de la red o cuando se necesita enviar datos a otras aplicaciones de la misma entidad, el Despachador llama al Subsistema de Proceso de Mensajes.

5.5.2. SUBSISTEMA DE PROCESO DE MENSAJES

El Subsistema de Proceso de Mensajes prepara los mensajes para que sean enviados agregándoles el header correspondiente a la versión necesaria y extrae los datos de los mensajes recibidos.

Este Subsistema puede estar compuesto por al menos un Modelo de Proceso de mensajes. Puede haber un Modelo de Proceso de Mensajes para cada versión de protocolo necesario en la red.

Por ejemplo podríamos tener un Subsistema de Procesos de mensajes que contenga distintos Modelos de proceso de mensajes [RFC 2571]:

Un modelo de proceso de mensajes que encripte y desencripte mensajes para el protocolo SNMPv1

Un modelo de proceso de mensajes que encripte y desencripte mensajes para el protocolo SNMPv2

Un modelo de proceso de mensajes que encripte y desencripte mensajes para el protocolo SNMPv3

Un modelo de proceso de mensajes que encripte y desencripte mensajes para otro protocolo ya sea existente o que pueda desarrollarse en el futuro.

Es el responsable de proporcionar compatibilidad con las versiones anteriores y futuras del protocolo. Para los mensajes entrantes la versión de protocolo es proporcionada por el Dispatcher (en algunos casos lo tomará del mensaje entrante y en otros casos lo podrá encontrar mediante un algoritmo) mientras que para los mensajes salientes el valor es provisto por las aplicaciones.

El subsistema de proceso de mensajes interactúa con el subsistema de seguridad para lograr la encriptación o desencriptación de los datos que la necesiten.

5.5.3. EL SUBSISTEMA DE SEGURIDAD

Potencialmente puede contener varios subsistemas. Es responsable de proveer los servicios de seguridad que pueden ser autenticación y privacidad en el mensaje. Este subsistema puede contener uno o varios Modelos de Seguridad.

Se ha desarrollado un Modelo de Seguridad Basado en Usuarios (User-Based Segurity Model), aunque este podría reemplazarse o utilizarse en conjunto con otro dependiendo de las necesidades.

Tiene como objetivos:

Verificar que los mensajes SNMP que se reciben no hayan sido modificados durante la transmisión;

Verificar la identidad de los usuarios que interactúan con el sistema;

Detectar si los mensajes que llegan a la entidad son recientes;

Cuidar la privacidad de la información enviada y recibida.

5.5.4. SUBSISTEMA DE CONTROL DE ACCESO

Provee un conjunto de servicios de autentificación de acceso que las aplicaciones pueden utilizarse ante operaciones de recuperación, generación de notificaciones.

El control de acceso posibilita restringir el acceso al MIB y limitar las operaciones que los gestores pueden realizar sobre los agentes.

Se define para utilizar con SNMP un Modelo de Control de Acceso basado en vistas, comúnmente llamado VACM (View-based Access Control Model).

El modelo de control de acceso basado en vistas está constituido por cinco elementos: grupos, nivel de seguridad, contexto, vistas de MIB y políticas de acceso.

5.5.5. APLICACIÓN GENERADOR DE COMANDOS

Inicia las PDUs SNMP Get, GetNext, GetBulk o SetRequest que envía el sistema local y procesa las respuestas a los pedidos que antes se habían enviado.

Para iniciar las respuestas deberá llamar al Dispatcher, dándole los datos que luego formarán parte del header del mensaje, entre los que se encontrarán el destino del mensaje, la versión del protocolo a utilizar, modelo de seguridad y nivel de seguridad que serán requeridos, la PDU y una bandera indicando si espera o no respuesta entre otros.

5.5.6. APLICACIÓN RESPONDEDOR DE COMANDOS

Recibe las solicitudes destinadas al sistema local y luego deberá desarrollar la operación de protocolos necesaria para generar una respuesta adecuada y reenviarla a la entidad solicitante. Deberá utilizar control de acceso para verificar si el solicitante está autorizado a obtener esa información u ordenar la modificación de datos.

Una vez recibida la solicitud y determinado que el mensaje debe responderse, esta aplicación deberá determinar el tipo de mensaje entrante, comunicarse con la base de datos, preparar la respuesta y luego entregar esa respuesta al Dispatcher para que éste la envíe.

Si por el contrario se determina que esa solicitud no debe responderse se envía al solicitante un mensaje comunicando una falla en el acceso.

5.5.7. APLICACIÓN CREADOR DE NOTIFICACIONES

Es el encargado de monitorear al sistema ante condiciones o eventos particulares y, de producirse una anormalidad, genera un mensaje Trap o Inform relativo a esas condiciones monitoreadas.

El Creador de notificaciones actúa de la siguiente manera: Primero, empleando mecanismos de filtro apropiados se determina cuál es la información que debe enviarse. Si el filtro determina que una notificación no debe enviarse se continúa el proceso, sino se recuperan variables de la Base de datos de Información local que permitan determinar la entidad a la que se le debe enviar el mensaje, el modelo de

seguridad a utilizar y el nivel de seguridad requerido. Luego se hace una verificación para determinar si debe enviarse o no la notificación. Una vez concluidos estos pasos se construye una PDU que si no necesita respuesta se envía al Despachador, en caso contrario antes de que la PDU sea enviada al Despachador se indica la necesidad de una respuesta, se cachean los datos del gestor al que se le envió la información ante la posible necesidad de retransmitir los datos.

5.5.8. APLICACIÓN RECEPTOR DE NOTIFICACIONES

Espera en modo pasivo la llegada de mensajes de notificación. Los mensajes de notificaciones son Inform (de gestor a gestor) y Trap (de agente a gestor). Si el mensaje que se recibe es de tipo Inform deberá responderse.

Lo primero que hace el Receptor de Notificaciones es registrar la llegada de la notificación y determinar de qué tipo de notificación se trata. Si se necesita una respuesta la prepara y se la envía al Despachador.

5.5.9. APLICACIÓN PROXY FORWARDER

Es una aplicación de implementación opcional, se implementa si:

Hay partes de la red que no soportan el protocolo SNMP; cuando es necesario tener información en cache para minimizar la carga de trabajo de los dispositivos; para autentificar y autorizar peticiones

Se encarga de adelantar mensajes. Usa primitivas del Despachador para adelantar cuatro tipos de mensajes:

Los mensajes creados por la aplicación Generador de Comandos, o sea los mensajes que el gestor le envía al cliente: determina a qué motor debería ir el mensaje y entrega la respuesta que antes se había recibido de ese motor.

Los mensajes creados por la aplicación Creador de Notificaciones, o sea que contienen notificaciones ya sea Trap o Inform: el Proxy Forwarder debe determinar qué motores deberán recibir la notificación.

Los mensajes creados por la aplicación respondedora de comandos, o sea las respuestas que el Agente le envía al Gestor: en este caso el Proxy determina las solicitudes y notificaciones que antes estuvieron en juego para adelantar la respuesta.

Mensajes que contienen indicaciones de reporte: el proxy determina qué clases internas de PDU y que notificaciones previas están en juego.

Para que el proxy pueda llevar a cabo su tarea debe basarse en la información de contexto que le permitirá determinar: qué motores accedieron a la información y cómo adelantar los mensajes y qué motor deberá recibir notificaciones de la información.

5.6. MENSAJES QUE PROCESA Y EXPIDE (MPD)

Los administradores y los agentes se comunican entre sí enviándose mensajes[9] de SNMP. Algunos de estos mensajes son los siguientes:

[9] En el RFC 2572 se describe el proceso de los mensajes y expedición de los mismos.

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. Inform. Confirmación de excepciones.

5.7. ESTRUCTURA DEL MENSAJE

El RFC 2272 define en forma general el modelo para el procesamiento del mensaje en SNMPv3. Este modelo es responsable de aceptar los PDUs del Generador, encapsularlo en mensajes, e invocar el USM (Modelo de Seguridad del Usuario) para insertar los parámetros relacionados con la seguridad en el encabezado del mensaje. El modelo de procesamiento del mensaje también se encarga de aceptar mensajes entrantes, invocar el USM para procesar los parámetros de seguridad que se encuentran en el encabezado del mensaje y entregar el PDU al generador.

En lo que a la estructura del mensaje se refiere, los primeros cinco campos son generados por el modelo de procesamientos de mensajes entrantes / salientes.

Los siguientes seis campos muestran los parámetros de seguridad usados por el USM. Finalmente el PDU, junto con el ContextEngineID y ContextName constituyen el PDU a ser procesado.

Los primeros cinco campos son los siguientes:

- msgVersion: Configurado para SNMPv3.
- MsgID: Un identificador único usado entre dos entidades SNMP para coordinar los mensajes de requerimiento y respuesta. Su rango es de 0 a $2^{31} – 1$.
- MsgMaxSize: Se refiere al tamaño máximo de un mensaje en octetos soportado por el que envía, con un rango de 484 a $2^{31} – 1$. Este es el máximo tamaño que una entidad que envía puede aceptar de otra SNMP Engine.
- MsgFlag: Un arreglo de octetos que contiene tres banderas en los tres bits menos significativos.
- ReportableFlag: Utiliza la posición en 1 para los mensajes enviados que contienen una requisición o un Informe, e igual a 0 para mensajes que contienen una Respuesta, Trap ó Reporte PDU.
- PriorFlag y AuthFlag: Son configuradas por el que envía el requerimiento para indicar el nivel de seguridad que le fue aplicado al mensaje.
- MsgSecurityModel: Es un identificador en el rango de $2^{31} – 1$ que indica que modelo de seguridad fue utilizado para el envío el mensaje, para que así el

receptor tenga conocimiento de que modelo de seguridad deberá usar para procesar el mensaje. Existen valores reservados:

- ✧ 1 para SNMPv1
- ✧ 2 para SNMPv2
- ✧ 3 para SNMPv3

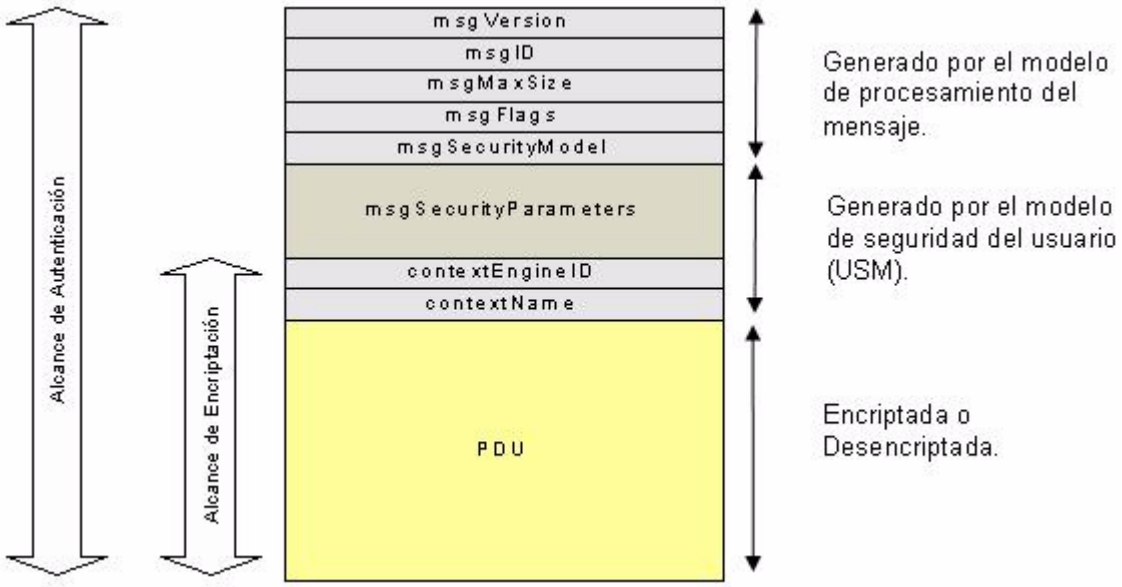


Figura 18. Estructura del mensaje de SNMPv3.

Los seis campos siguientes relacionados con los parámetros de seguridad y generados por la USM incluyen:

- MsgAuthoritativeEngineID: Se refiere al valor de la fuente de un Trap, Response ó Report y al destino de un Get, GetNext, GetBulk, Set ó Inform.

- MsgAuthoritativeEngineTime: Es un valor entero en el rango de $2^{31} – 1$ que representa el número de segundos desde que el snmpEngineBoots del SNMP Engine fue incrementado.
- MsgUserName: Usuario principal desde el cual el mensaje ha sido enviado.
- MsgAuthenticationParameters: Parámetro de autenticación. Si la autenticación no es utilizada, este valor es nulo. Este parámetro es generado usando un algoritmo llamado HMAC.
- MsgPrivacyParameters: Parámetro de privacidad. Si la privacidad no es utilizada, este valor es nulo. Este parámetro es generado usando un algoritmo llamado DES.

5.8. 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.

5.9. SERVICIOS DE SEGURIDAD DE SNMPv3

5.9.1. TIPOS DE SERVICIOS DE SEGURIDAD.

Los servicios de seguridad que ofrece el modelo de SNMPv3 son los siguientes:

a. Integridad de los datos. Su objetivo es prevenir la alteración y/o destrucción de los datos por entes no autorizados.
b. Autenticación del origen de los datos. 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.
c. Confidencialidad de los datos. Permite garantizar que los datos no serán accesados por usuarios no autorizados, entidades o procesos desconocidos.
d. Módulo de Tiempo (Timeless) y protección de repetición limitada. Permite proteger un mensaje de un determinado retraso e impide la repetición del mismo.

5.9.2. ORGANIZACIÓN DEL MÓDULO DE SEGURIDAD.

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

a. Módulo de Autenticación. 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.
b. Módulo de Tiempo (Timeless). Ofrece protección contra el retraso o repetición del mensaje. El chequeo de tiempo solo se realiza si se ha concluido el proceso de autenticación.
c. 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.

5.10. PROTECCIÓN CONTRA LA REPETICIÓN DEL MENSAJE, RETRASO Y REDIRECCIONAMIENTO.

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

a. Instrumento SNMP de autoridad. SNMP 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.

b. 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 (Timeless) 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. Ningún instrumento de autoridad puede transferir el mensaje o ser reemplazado por otro instrumento de autoridad, pero puede suceder que lo haga un instrumentos no autoritario, al cual se transfieren también los datos del SNMP autoritario, sin embargo esto no se considera una amenaza ya que la respuesta será descartada por el módulo de procesamiento de mensajes, porque será un mensaje de demanda no excelente.

- 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.

APLICACIONES DE SNMP

Después de conocer la evolución del protocolo se mencionan, en la siguiente sección, el empleo de éste en los diferentes sistemas operativos, en software y su implementación en equipos de la red mundial.

6. APLICACIONES DE SNMP

Conociendo el funcionamiento de este protocolo y la importancia que ha tomado en la configuración de redes de diferentes extensiones se consideró necesario abordar el tema de la implementación sobre los sistemas operativos[10] y software de mayor difusión en el mundo.

6.1. APLICACIONES DE SNMPv3.

SNMP posee cinco tipos de aplicaciones[11], 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 Forwarders (Expedidores).

El protocolo SNMP puede implementarse de forma centralizada: un gestor colecciona información de varios agentes que se distribuyen en distintos segmentos de la red, es decir el administrador actúa directamente sobre los agentes.

[10] Para LINUX referirse a la página http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=como-linux-snmp
[11] En el RFC 2573 se describen detalladamente este tipo de aplicaciones.

Es una implementación simple y útil cuando hay pocas necesidades de monitoreo y cuando los volúmenes de información que se deben transmitir entre administradores y agentes son escasos. Como ventaja existe un administrador único y los tipos de datos de monitoreo son simples y el polling tiene poca frecuencia. Tiene la desventaja de generar un throughput muy elevado, si la red crece esto generará congestiones y será necesario cambiar la estructura utilizada en el monitoreo.

Cuando la cantidad de agentes complica el monitoreo de la red, por causar congestiones, se puede reducir el tráfico utilizando un sistema distribuido. Este sistema distribuido necesitará gestores de nivel intermedio. Estos fueron introducidos por SNMPv2. Esta forma de implementar el protocolo se vale de un administrador de nivel superior y administradores de nivel intermedio y un grupo de agentes asignado a cada administrador de nivel intermedio.

Los gerentes de nivel intermedio funcionan como gerentes para los agentes de nivel inferior y como agentes para los administradores de un nivel superior. Esto permite un volumen de monitoreo de datos alto con un escaso throughput aunque el polling sea frecuente y los tipos de datos manejados sean complejos.

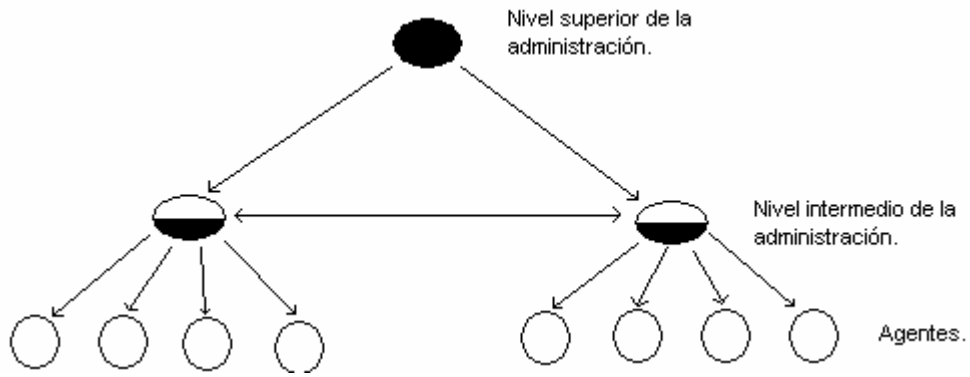


Figura 19. Estructura de un sistema distribuido con gestores de nivel intermedio.

.

6.2. VERSION DE SNMP DE WINDOWS SERVER 2003

El Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) es un estándar de administración de redes utilizado en redes TCP/IP.

SNMP proporciona un método de administración de hosts de redes como concentradores, puentes, enrutadores y equipos de servidor o estaciones de trabajo desde un equipo central donde se ejecuta software de administración de redes. SNMP realiza servicios de administración mediante una arquitectura distribuida de sistemas de administración y agentes.

Puesto que la administración de redes es fundamental para la administración de recursos y auditoria, 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 el cierre y reinicio de un dispositivo, 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.

✧ Servicio SNMP

El servicio de protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) se puede usar en equipos donde se ejecuten los protocolos TCP/IP e IPX. Es un servicio opcional que puede instalarse después de haber configurado correctamente el protocolo TCP/IP.

El servicio SNMP proporciona un agente SNMP que permite la administración remota y centralizada de equipos en los que se ejecute:

Microsoft windows XP

Microsoft windows 2000

Familia de servidores de Microsoft Windows Server 2003[12]

Además, el agente SNMP permite la administración de los servicios siguientes:

Windows XP o la familia de servidores de Windows Server 2003 y WINS basado en Microsoft Windows 2000.

Windows XP o en la familia de servidores de Windows Server 2003 y DHCP basado en Windows 2000.

Windows XP o la familia de servidores de Windows Server 2003 y Servicios de Internet Information Server basados en Windows 2000.

Microsoft LAN Manager.

Para tener acceso a la información que suministra el servicio del agente SNMP, necesita al menos una aplicación de software de sistemas de administración SNMP. El servicio SNMP admite, pero no incluye de momento, software de administración de SNMP. El software de administración SNMP debe ejecutarse en el host que actúe como sistema de administración.

- ✧ Agentes y sistemas de administración SNMP.

El uso de SNMP requiere dos componentes:

- Un sistema de administración SNMP.

[12] http://www.microwave.harris.com/products/starview/pdf/183a_s.pdf

El sistema de administración, también denominado *consola de administración*, envía solicitudes de actualización e información a un agente SNMP. Cualquier equipo donde se ejecute software de administración SNMP es un sistema de administración SNMP. No es necesario que la aplicación del software de administración se ejecute en el mismo host que el agente SNMP.

El sistema de administración SNMP solicita información de un equipo administrado, denominado agente SNMP, como la cantidad de espacio disponible en el disco duro o el número de sesiones activas. Si el sistema de administración ha recibido acceso de escritura sobre un agente, también puede iniciar un cambio en la configuración del mismo.

- Un agente SNMP.

  El agente SNMP responde a las solicitudes de información del sistema de administración. Cualquier equipo donde se ejecute el software de agente SNMP es un agente SNMP. El servicio SNMP, que es software de agente, responde a las solicitudes de información de uno o varios sistemas de administración. Puede configurarse para determinar qué estadísticas se están siguiendo y qué sistemas de administración están autorizados a solicitar información.

  En general, los agentes no originan mensajes sino que sólo los responden. Un mensaje de captura es la única comunicación SNMP iniciada por el agente y aumenta la seguridad. Una captura es un suceso que desencadena una alarma en un agente, como la reinicialización de un sistema o un acceso no válido.

Los agentes y hosts de administración pertenecen a una comunidad SNMP, que es un conjunto de hosts agrupados con fines administrativos. La definición de comunidades proporciona seguridad, ya que sólo permite que se comuniquen sistemas de administración y agentes de la misma comunidad.

✧ Mensajes de SNMP

Cuando los programas de administración del Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) envían solicitudes a un dispositivo de red, el software del agente de ese dispositivo recibe las solicitudes y recupera la información de las MIB. A continuación, el agente vuelve a enviar la información solicitada al programa de administración SNMP que lo inició. Para realizar estas tareas, el agente utiliza los siguientes tipos de mensaje:

✧ Mensaje de SNMP

- *Get*: Mensaje básico de solicitud de SNMP. Enviado por un sistema de administración SNMP, solicita información acerca de una única entrada de la base de datos MIB de un agente SNMP. Por ejemplo, la cantidad de espacio libre en el disco.

- *Get-next:* Tipo ampliado de mensaje de solicitud que puede utilizarse para examinar todo el árbol de objetos de administración. Cuando se procesa una solicitud Get-next para un objeto determinado, el agente devuelve la identidad y el valor del objeto que sigue lógicamente al objeto de la solicitud. La solicitud Get-next resulta útil en el caso de tablas dinámicas, como una tabla interna de rutas IP.

- *Set*: Si está permitido el acceso de escritura, este mensaje puede utilizarse para enviar y asignar un valor de MIB actualizado al agente.
- *Getbulk:* Solicita que el tamaño de los datos transferidos por el agente del host sea lo más grande posible, dentro de las limitaciones dadas para el tamaño de los mensajes. Esto reduce al mínimo el número de intercambios de protocolo necesarios para recuperar una gran cantidad de información de administración. El tamaño máximo del mensaje no debe ser superior a la unidad de transmisión máxima (MTU) de la ruta de acceso, el tamaño de trama máximo permitido para una única trama de la red, o de lo contrario se puede producir fragmentación.
- *Trap:* Un mensaje no solicitado enviado por un agente SNMP a un sistema de administración de SNMP cuando el agente detecta que se ha producido un tipo determinado de suceso localmente en el host administrado. La consola de administración de SNMP que recibe un

mensaje de captura se conoce como destino de captura. Por ejemplo, puede enviarse un mensaje de captura sobre un suceso de reinicio del sistema.

Cuatro de estos tipos de mensajes son protocolos de solicitud y respuesta simples en los que SNMP utiliza el Protocolo de datagramas de usuario (UDP, User Datagram Protocol). Esto significa que existe la posibilidad de que una solicitud del sistema de administración no llegue al agente y de que la respuesta del agente no llegue al sistema de administración. SNMP es un protocolo de red sin conexión, por lo que no existen garantías de que los mensajes SNMP lleguen a su destino.
Puede utilizar Seguridad del protocolo Internet (IPSec, Internet Protocol Security) para proteger el tráfico entre los sistemas de administración y los agentes SNMP.

- ✧ Proteger los mensajes de SNMP con IPSec

Si configura directivas IPSec en todos los agentes y administradores SNMP, puede impedir que usuarios malintencionados e intrusos intercepten mensajes SNMP. Si no puede configurar directivas IPSec en todos los hosts SNMP pero desea garantizar que todos los hosts pueden comunicarse entre si, debe configurar directivas IPSec que permitan la comunicación de texto simple. Sin embargo, el uso de la comunicación de texto simple no se recomienda.

IPSec no cifra automáticamente el tráfico SNMP. Deben crearse especificaciones de filtro en la lista de filtros IP apropiada para el tráfico entre los administradores y los agentes SNMP.

Para aumentar la protección de los mensajes SNMP, debe agregar dos conjuntos de especificaciones de filtro a una directiva IPSec nueva o existente en el host habilitado para SNMP. El primer conjunto de especificaciones de filtro regula el tráfico SNMP normal o los mensajes SNMP entre los administradores y los agentes SNMP. Este conjunto de especificaciones de filtro suele constar de una especificación de filtro para el tráfico de entrada y otra para el tráfico de salida.

Para utilizar el servicio de SNMP en este sistema operativo es necesario definir grupos:

Puede asignar grupos de hosts a comunidades de Protocolo simple de administración de redes (SNMP) con propósitos administrativos o para realizar una comprobación de seguridad limitada de agentes y sistemas de administración. Las comunidades se identifican por los nombres de comunidad que se les asignen. Un host puede pertenecer a varias comunidades al mismo tiempo, pero un agente no acepta ninguna solicitud de un sistema de administración que no esté incluido en su lista de nombres de comunidad aceptables.

Defina las comunidades de forma lógica para sacar el máximo partido al servicio de autenticación básica suministrado por SNMP.

En el ejemplo siguiente hay dos grupos: pública y pública 2.

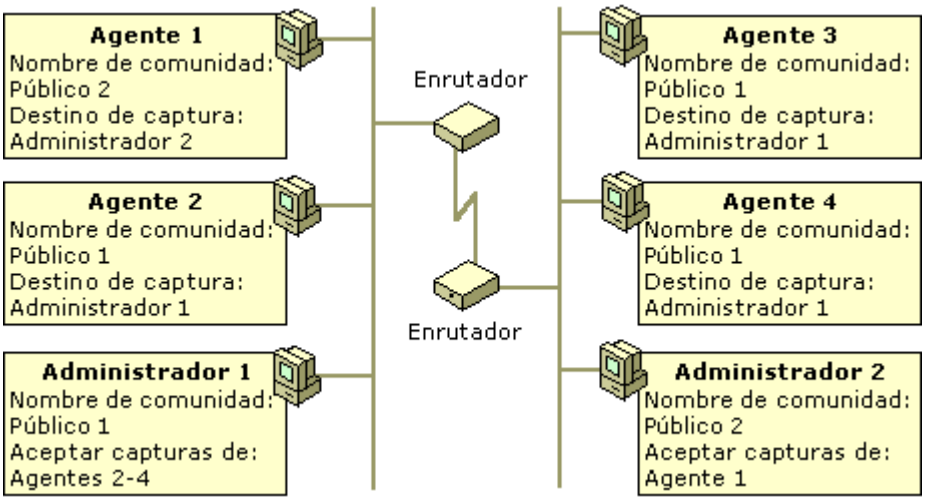


Figura 20. Comunicación entre grupos.

El agente 1 puede enviar capturas al administrador 2 y responder a solicitudes del administrador 2 porque ambos son miembros del grupo pública 2.

Los agentes 2 a 4 pueden enviar capturas al administrador 1 y responder a solicitudes del administrador 1 porque todos son miembros del grupo pública 1 de forma predeterminada.

Como notaciones importantes tenemos que:

- Los nombres de comunidad se envían a través de la red como texto sin formato. Los intrusos pueden leer el texto simple mediante software de análisis de red, por lo que el envío de nombres de comunidad SNMP a través de la red supone un posible riesgo de la seguridad. Sin embargo, es posible proteger los mensajes SNMP si se configura la seguridad del protocolo Internet (IPSec).
- No hay ninguna relación entre los nombres de comunidad y los nombres de dominio o de grupo de trabajo. Los nombres de comunidad representan una

contraseña compartida para los grupos de hosts de la red, y deben seleccionarse y modificarse igual que cualquier otra contraseña.

- Utilice los nombres de comunidad principalmente como elemento de organización, no de seguridad.
- No debe crear una comunidad con el nombre Público y concederle acceso de lectura. Asimismo, debería especificar los hosts cuyos paquetes pueden aceptarse, en lugar de hacer clic en Aceptar paquetes SNMP de cualquier host.

Estas son unas sugerencias por el equipo técnico de Windows para mantener el servidor con una seguridad alta ya que el protocolo tiene falencias en este campo. Prácticas recomendadas:

- Actualizar la configuración con regularidad: Asegúrese de supervisar y actualizar la configuración de nombre de host de forma continuada. Esto le permitirá garantizar la detección oportuna de cualquier acceso no autorizado.
- Permitir que los hosts sólo acepten paquetes de hosts específicos: Al configurar las opciones de seguridad, no haga clic en Aceptar paquetes SNMP de cualquier host.
- Configurar capturas de autenticación: Aproveche la comprobación de seguridad de SNMP; para ello configure capturas de autenticación en todos los agentes SNMP.

- Comprobar que los componentes específicos de servicios funcionan adecuadamente: Si va a supervisar componentes específicos de servicios, como el Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) o el Servicio de nombres Internet de Windows (WINS, Windows Internet Name Service), compruebe que todos estos servicios se hayan instalado y configurado correctamente.
- Utilizar IPSec para proteger los mensajes SNMP: Para reducir el riesgo de ataques internos, configure los sistemas del agente SNMP de modo que se rechacen los mensajes de solicitud provenientes de sistemas de administración no autorizados. Por motivos de seguridad, utilice Seguridad de protocolo Internet (IPSec) si desea proteger los mensajes SNMP; para ello, cree especificaciones de filtro en la lista de filtros IP apropiada entre los sistemas de administración y los agentes SNMP.
- Recordar que SNMP es un protocolo inseguro: Si decide utilizar SNMP para administrar redes, recuerde que SNMP es un protocolo poco seguro cuya eficacia depende exclusivamente de cómo se implemente.

6.3. MRTG: MULTI ROUTER TRAFFIC GRAPHER

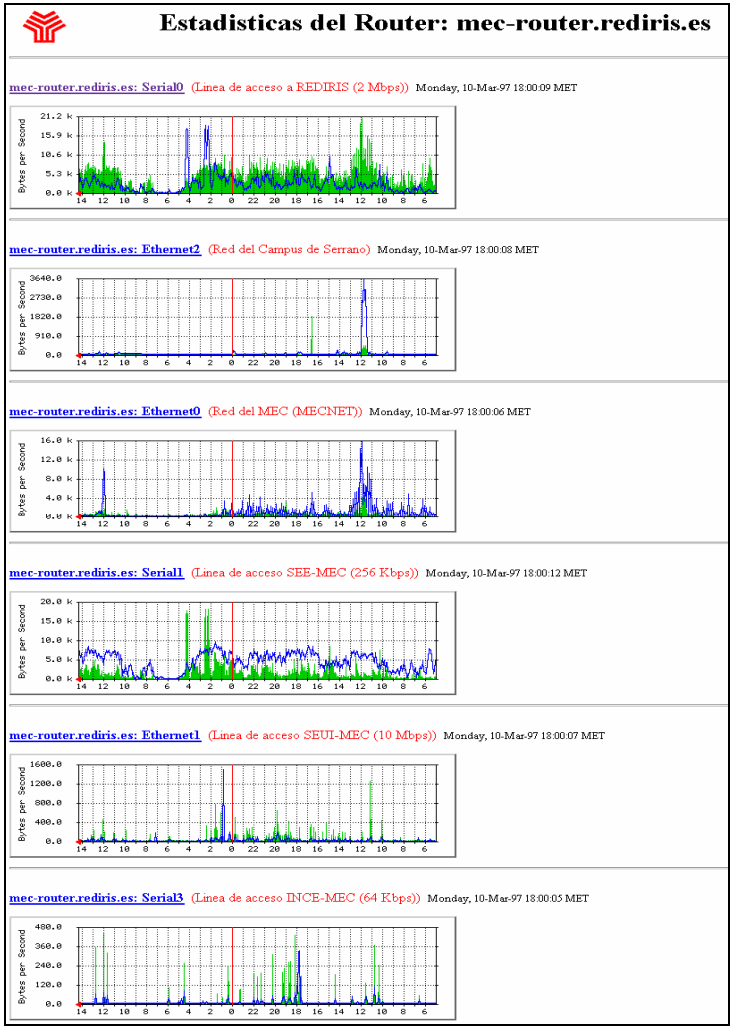
MRTG es una avanzada utilidad gráfica escrita por Tobias Oetiker y Dave Rand para representar gráficamente los datos que los gestores SNMP leen de los agentes SNMP. Produce unas vistosas páginas HTML con gráficos GIF sobre el

tráfico entrante y saliente en los interfaces de red prácticamente en tiempo real. Con esta herramienta se evita el tener que trabajar directamente con las utilidades CMU-SNMP mediante línea de comandos.

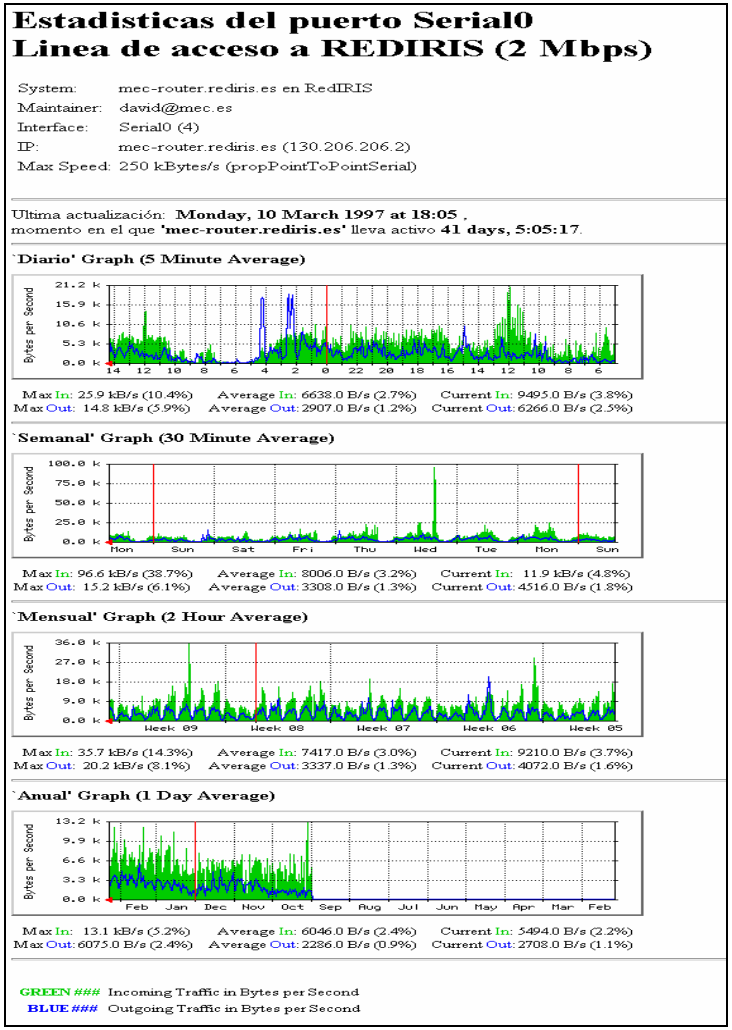
El programa principal está escrito en "C" para acelerar el proceso de toma de muestras y la generación de imágenes GIF. Los gráficos son generados con la ayuda de la biblioteca GD escrita por Thomas Boutell, autor de la FAQ WWW.

El paquete contiene algunas utilidades para analizar los interfaces de enlace, extraer sus características y generar los archivos de configuración base, que luego se pueden modificar para adaptarlos a las necesidades concretas.
Otra característica interesante del MRTG es la cantidad de información que produce. Permite cuatro niveles de detalle para cada interface: tráfico en las últimas 24 horas, la última semana, el último mes y un gráfico anual. Esto permite recoger información para realizar estadísticas. Guarda toda esta información en una base de datos utilizando un algoritmo de consolidación que impide que los archivos crezcan de forma desmesurada.

También genera una página principal que contiene las imágenes GIF de los detalles diarios de cada interface del router, lo que permite hacerse una idea general de qué es lo que está pasando en el router con un sólo vistazo. Se puede ver la página principal generada por MRTG en las Figuras a continuación.



(a)



(b)

Figura 21. (a) Interfaz de la página principal (b) Interfaz de la página detallada del interface

Veamos el procedimiento básico de instalación. Lo primero que se necesita es la distribución.

Antes de comenzar la instalación del MRTG es necesario instalar la biblioteca GD. La versión actual es la 1.2 y no debería haber problemas en compilarla e instalarla. Sencillamente hay que ejecutar make en el directorio en el que se ha desempaquetado la distribución y se genera como resultado el archivo llamado libgd.a. Se copia este archivo al directorio /usr/local/lib y los archivos con extensión .h al directorio /usr/local/include/gd.

En este punto el paquete GD debe estar correctamente instalado. Ahora se puede compilar el paquete MRTG. Se extrae la distribución y edita el archivo Makefile para indicar donde se encuentra la biblioteca y los archivos de cabecera de GD, así como cual es el archivo ejecutable Perl 5.003: normalmente se encuentra en /usr/bin/perl o en /usr/local/bin/perl.

Se construye el programa principal tecleando make rateup; cuando termine la compilación, teclea make substitute para incluir el path correcto del intérprete de Perl en los scripts de Perl que utiliza MRTG.

Se copia los siguientes ficheros su directorio destino final (por ejemplo: /usr/local/mrtg): BER.pm, SNMP_Session.pm, mrtg y rateup. También se han de copiar en este directorio los dos archivos de configuración: indexmaker y cfgmaker.

Asegúrese que todos los programas tienen permiso de ejecución. Ya está todo listo para crear un archivo de configuración sencillo. Es necesario tener acceso

SNMP de lectura al router. Para un router de la marca Cisco, las líneas de configuración que dan permiso son:

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

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

- snmp-server community public RO

Si el router de la red es de otra marca, entonces se ha de consultar el manual para determinar cómo permitir el acceso SNMP.

El script cfgmaker simplifica mucho la tarea de construir el archivo de configuración. Todo lo que hay que hacer es ejecutarlo con los siguientes parámetros:

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

Por ejemplo:

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

Localizará todos los interfaces del router mec-router.rediris.es y escribirá una sección en el archivo con las especificaciones del número de interfaces, velocidad máxima, descripción, etc., junto con algunas etiquetas HTML para que puedan ser incluidas en la página detallada. Es posible editar este archivo HTML para traducirlo al idioma y preferencias propias. Se puede ver en la Figura la salida de uno de los interfaces de un router.

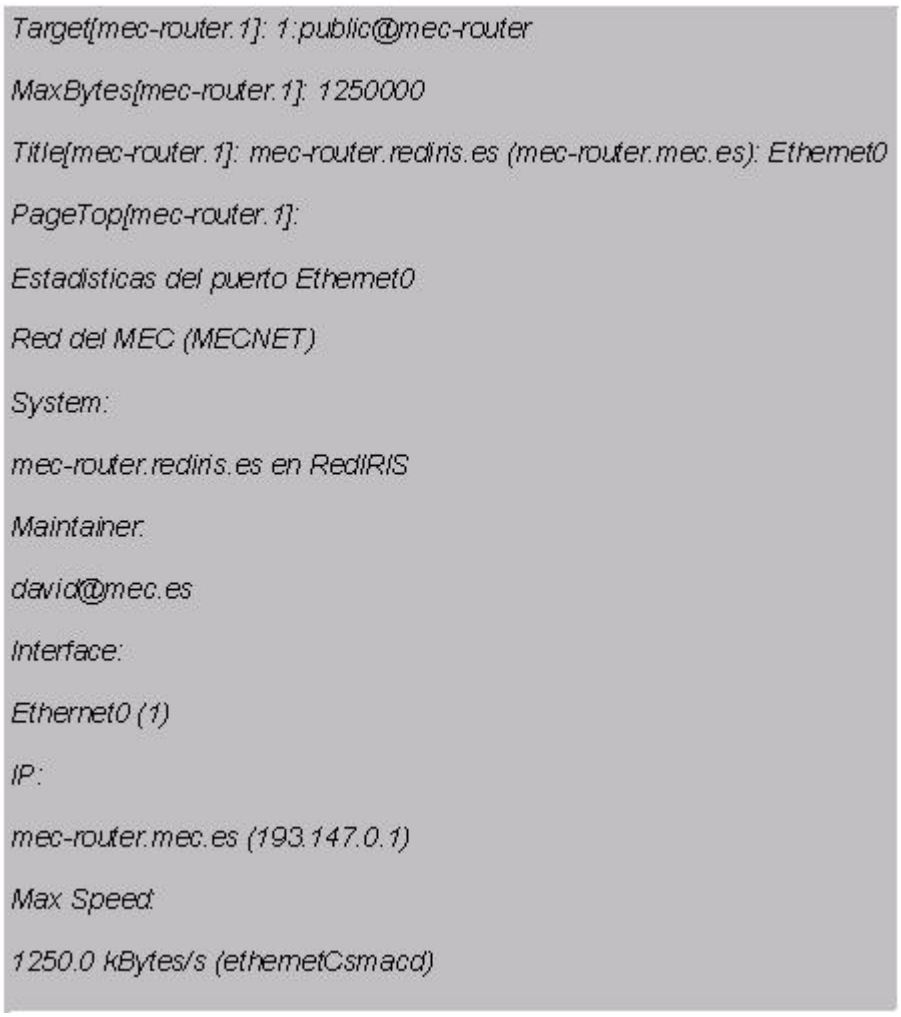


Figura 22. Interfaces de un router.

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

- ./mrtg mrtg.cfg

El programa se pondrá en contacto con el router, pedirá algunos valores y generará algunos archivos de registro y algunos archivos GIF en el directorio actual. La primera vez que se ejecuta pueden surgir quejas respecto los archivos de registro y de gráficos que no ha encontrado; no hay que preocuparse pues elimina los archivos de gráficos que genera y vuelve a ejecutar el programa otra vez. El gráfico generado mostrará el tráfico producido en el intervalo desde la última ejecución del programa. También genera páginas HTML para cada interface.

Para indicarle a MRTG como ejecutarse adecuadamente en el sistema, primero se ha de crear un directorio dentro del directorio principal del web servidor (suponiendo que en el sistema haya un servidor web en funcionamiento) para contener las páginas y gráficos que MRTG generará cada vez que se ejecute. Se añade este directorio en la cabecera del archivo de configuración con la directiva WorkDir: /usr/local/web/mrtg (suponiendo que el directorio raíz está situado en /usr/local/web). La próxima vez que MRTG se ejecute, creará los archivos de registro y de gráficos en este directorio, pudiendo accederse vía http://your_host.domain/mrtg.

Ahora vamos a construir la página principal para todos los interfaces como la que aparece en la Figura 21 (a). Esto se puede llevar a cabo con la utilidad indexmaker. Ejecuta:

- indexmaker mrtg.cfg > /usr/local/web/mrtg/index.html

Se generará un documento HTML con gráficos diarios de aquellos interfaces cuyo nombre de router coincida con la expresión regular anterior y los enlaza con la página individual detallada.

Como se puede imaginar, el programa MRTG se ha de ejecutar a intervalos regulares para recoger datos en cada intervalo y generar los gráficos periódicamente, de forma que de la impresión de ser una monitorización en tiempo real. Esto se puede conseguir mediante la siguiente línea en el archivo /etc/crontab (suponiendo /usr/local/mrtg-bin como el directorio donde reside el programa mrtg):

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

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

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

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

Otra mejora que se puede incluir en el archivo de configuración es la directiva WriteExpire, que fuerza a MRTG a crear archivos ".meta" para cada archivo GIF y página HTML, eliminando innecesarias operaciones de "cache" tanto en los servidores proxy como en los propios visores web. Para ello también es necesario configurar el servidor Apache (o el servidor usado) para que lea estos archivos ".meta" y envíe correctamente las cabeceras "Expire" con la directiva MetaDiren el archivo XXXX.

Se pueden encontrar más directivas en el archivo de configuración ejemplo que viene con la distribución; que por cierto, está muy bien documentado. Es posible modificar la disposición de las imágenes generadas por MRTG.

MRTG es de libre distribución y debe ser utilizado bajo los términos de *GNU General Public License.*[13]

6.4. MACINTOSH OS

Las herramientas de estos gestores de redes se basan siempre en ordenadores con sistema operativo Unix o Windows NT y herramientas de gestión de Microsoft o bien, cuando la red a gestionar se trata de una auténtica internet con subredes y múltiples equipos de comunicaciones, se basa en herramientas SNMP, siendo la más popular OpenView de Hewlett Packard (Simple Network Management Protocol, un protocolo utilizado en la gestión de redes para la monitorización de los dispositivos de red, sin estar exclusivamente limitado a redes TCP/IP). Además de esta herramienta, máximo exponente de los productos de gestión de red, el administrador de una red hace uso de múltiples utilidades en su trabajo diario. Programas que le permiten ver si un equipo está conectado, analizar el tráfico que circula por su red, etc.

La gran sorpresa para estos administradores de red y también para muchos usuarios es descubrir que existen utilidades en el mercado que permiten realizar las mismas tareas desde un Macintosh, con la misma facilidad que ofrece este entorno para otro tipo de aplicaciones y en muchos casos a un coste inferior al

[13] ***Para la descarga de la aplicación***: http://www.mrtg.org/

planteado con el mismo conjunto de soluciones en otros entornos. Aunque gran parte de las aplicaciones existentes en el mercado son “maccentricas” y están orientadas exclusivamente a la gestión, monitorización y depuración de errores en redes de Macintosh, muchas otras son multiplataforma y permiten manejar redes compuestas de máquinas Windows, Unix, Macintosh e incluso routers, switches y otros equipos de gestión de redes.

- ✧ Monitorización de red IP

Un administrador de red que cuente con un número importante de equipos a monitorizar entre los que se incluyan routers, switches y otros elementos de comunicaciones, necesita una herramienta gráfica que le permita ver rápidamente todos los equipos de su red y el estado en que se encuentran. Aunque OpenView es la aplicación “estándar”, una alternativa para Mac es InterMapper 3.0.4 de la compañía Dartware, un programa con una filosofía parecida a la de OpenView, ya que muestra un mapa de toda la red y cada equipo aparece identificado por su nombre o dirección IP, cambiando de color (y también con acompañamiento de sonido) en función de que un equipo tenga un fallo menor, un fallo mayor o directamente no responda.

- ✧ Automatice el Mapa de red.

El programa, al igual que OpenView, dispone de una posibilidad de autodescubrimiento de redes que funciona francamente bien y que en pocos

minutos es capaz de mostrarle en pantalla una estructura de red compleja. Al utilizarla se descubre un aspecto muy interesante de este producto, ya que aparte de explorar y descubrir dispositivos SNMP, es capaz de sacar a la luz cualquier máquina IP que responda a pings y el usuario puede elegir qué tipo de prueba (aunque sólo es posible realizar una sobre un equipo) quiere utilizarse con el dispositivo para probar su funcionamiento: SNMP, Telnet, HTTP o cualquier otro protocolo de red, e incluso es posible definir las respuestas aceptables en cada caso. Además, el programa también permite analizar equipos AppleTalk, integrándolos en el mismo mapa.

El resultado es una herramienta sumamente potente y que puede consultarse desde cualquier punto de la red, ya que incorpora un servidor web desde el que pueden observarse tanto el mapa como la lista de dispositivos, pudiendo ver las características de cada uno en una pantalla personalizada.

- ✧ La información al detalle.

Como complemento a este programa, Dartware también ofrece la aplicación SNMP Watcher 1.0, un navegador de las MIB (Management Information Base) de SNMP, encargadas de identificar cada parámetro de dispositivos como routers y switches y algunos tipos de servidores, para obtener una gran cantidad de información acerca de su funcionamiento. Por ejemplo el tipo de interfaces, la cantidad de información que transmiten, el número de errores, etc.

El programa es muy sencillo de manejar, ya que se basa en una sola ventana que permite recorrer de forma jerárquica toda la estructura de MIB y ver en una ventana independiente los valores de cada una de ellas.

El principal fallo o carencia que se le puede achacar a SNMP Watcher es que como su propio nombre indica, solo es un observador de SNMP y no permite, al contrario de otros programas del mercado, modificar valores del dispositivo.

De aquellos valores que tienen contadores, por ejemplo en los interfaces de red es posible leer el número de bytes que han transmitido y recibido, se puede mostrar también una ventana con un listado histórico de uno de dichos contadores, lo que permite ver la evolución del tráfico cursado por una conexión o la cantidad de errores que se producen en determinados intervalos de tiempo.

La unión de InterMapper y SNMP Watcher es una solución de gestión de redes con una gran potencia, aunque no llegue al nivel de OpenView, y que permite utilizar un Macintosh, (no hace falta que sea el modelo más alto de la gama), para gestionar redes de un gran número de equipos. Por ejemplo, en una de las pruebas realizadas se logró monitorizar desde un portátil la red corporativa de una empresa con más de cuatrocientos equipos, incluyendo servidores, routers, conmutadores y por supuesto un gran número de ordenadores portátiles.

6.5. OTROS PROGRAMAS

CiscoWorks 2000

- Permiten ver la configuración
- Muestran la topología de la red
- Facilita la obtención de reports
- Permite actualizar IOS y descubrir nuevas versiones

Extensiones:

- Cisco View.
- PIX Management.
- IDS Management.
- Router Management.
- Security Monitor Center
- Wireless LAN solution Engine

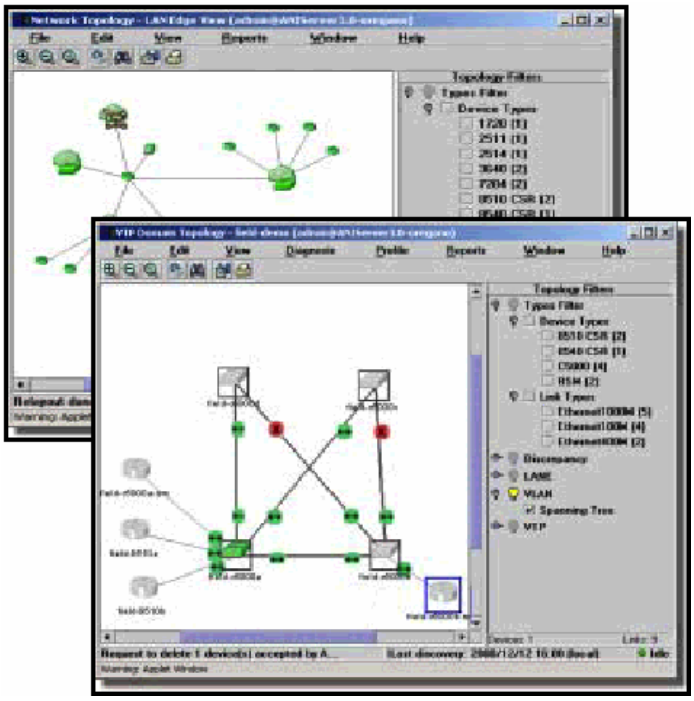


Figura 23. Monitoreo en routers de CISCO

Router-Stats actualiza los gráficos una vez al día y muestra información estadística muy interesante sobre la utilización por horas y otros aspectos. El único problema es que se apoya en muchos programas externos. (SMU-SNMP para las tareas con SNMP, GNUPLOT para trazar gráficos, NetPBM y GIFTOOL para trabajar con gráficos).

Hay otra categoría de software que da un paso más allá en la tarea de gestión de redes, ofreciendo una solución completa tanto para monitorizar como para configurar toda la red. Este tipo de solución permite obtener una compleja representación gráfica de la red y ojear fácilmente los nodos que la componen, verificando detalles de configuración específicos y otras cuestiones de interés.

A este nivel podemos hablar de dos soluciones comerciales ampliamente utilizadas: "HP-OpenView" de Hewlett-Packard y "SunNet Manager" de Sun. Estas herramientas ofrecen una plataforma integrada para la gestión de los recursos de red, a través de impresionantes interfaces gráficos. Entre otras utilidades, disponen de herramientas para localizar los nodos de la red en los que se están ejecutando agentes SNMP. Otra característica importante es la capacidad de integrar productos de otros fabricantes, como el CiscoWork de Cisco, que permite al administrador mantener una base de datos con todas las configuraciones de los routers e incluso monitorizar gráficamente los paneles traseros de los routers con todas sus conexiones.

Los dos inconvenientes fundamentales de estos productos es que son comerciales y no están disponibles para Linux. Pero por supuesto que existen soluciones disponibles públicamente con una funcionalidad más o menos similar. Uno de los paquetes que he encontrado es el Scotty. Scotty es un paquete basado en TCL que permite crear programas específicos a las necesidades de la red propia, empleando un API de alto nivel de cadenas de caracteres. Un paquete similar es el Tkined. Es un editor de red que ofrece extensiones para crear un entorno de trabajo completo, integrando algunas herramientas para localizar redes IP, soporte para el proceso de instalación de la red o resolución de problemas en redes IP utilizando SNMP en combinación con otras utilidades estándar (por ejemplo

traceroute). Scotty también incluye un visor gráfico MIB que permite explorar fácilmente información MIB.

CONCLUSIONES

Es extremadamente común que los términos redes de computadoras y sistemas distribuidos sean usados muchas veces indistintamente, pero el punto clave que los distingue es el hecho de que en un sistema distribuido la existencia de múltiples computadoras interconectadas sea transparente al usuario, esto es que se puede teclear un comando para iniciar un programa y observar que como lo hacer. El trabajo de seleccionar el mejor procesador, encontrar y transportar todos los archivos de entrada al procesador y poner los resultados en el lugar apropiado, depende enteramente del sistema operativo distribuido. Un sistema operativo distribuido es efectivamente un caso especial de una red, aquel cuyo software da un alto grado de cohesividad y transparencia. Por lo tanto, la diferencia entre red y un Sistema Distribuido está más bien en el software que en el hardware.

En los sistemas distribuidos como en una Internet, se conectan varias redes entre sí con el uso de dispositivos de conexión y transmisión y un protocolo de interconexión de redes, de modo que los dispositivos de conexión usan el protocolo para encubrir las características de las redes y proporcionar un servicio uniforme entre ellas, es decir, aunque cada red use una tecnología distinta y unas reglas específicas de transmisión, los hosts de cada red la ven de igual manera. Este es el poder de la abstracción de la interconexión entre redes.

La principal tecnología de interconexión de redes es el conjunto de protocolos de Internet llamados TCP/IP, que son los que se usan en redes WAN, MAN y LAN.

SNMP se sitúa en el tope de la capa de transporte de la pila OSI, o por encima de la capa UDP de la pila de protocolos TCP/IP. Siempre es en la capa de transporte.

La necesidad de administrar redes nos lleva a varios problemas que se presentan en la interconexión de redes que son principalmente dos:

Dispositivos diferentes: La interconexión de redes permite diferentes tipos de dispositivos, todos ellos soportando el protocolo TCP/IP. Debido a esto, la administración de redes se presenta como un problema. Sin embargo, usar una tecnología de interconexión abierta permitió que existieran las redes formadas por dispositivos de distintos fabricantes, por lo que para administrar estas redes, habrá que usar una tecnología de administración de redes abierta.

Administraciones diferentes: Como se permite la interconexión entre redes de distinto propósito y distinto tamaño, hay que tener en cuenta que también están administradas, gestionadas y financiadas de distinta forma.

El manejo de este protocolo, se basaba en el intercambio de información de red a través de mensajes (PDU's). Por ser un protocolo fácilmente extensible a toda la red, su uso se estandarizó entre usuarios y empresas en la gestión de sus sistemas informáticos dentro de una red. Este protocolo tiene muchas ventajas como la introducción de mecanismos de seguridad, para proteger la privacidad de los datos, autentificación y autorización a los usuarios, junto con el control del acceso. Se tuvo también el mayor detalle en la definición de las variables, se

añaden estructuras de la tabla de datos para facilitar el manejo de los datos. El hecho de poder usar tablas hace aumentar el número de objetos capaces de gestionar, el uso de leguajes orientados a objetos (Java, C++, etc.), para la construcción de los elementos propios del protocolo. Estas técnicas confieren consistencia y llevan implícita la seguridad, con todo esto el aumento de redes de diferentes tipos dejo de ser un problema.

Los beneficios de establecer este protocolo para la gestión de red en el sistema son muchos. Además de garantizar una protección de los datos, seguridad de transmisión y el control del flujo de los mismos, el SNMP permite reiniciar la máquina, cambiar las variables e incluso en algunas situaciones se puede ejecutar programas en el host. Estos beneficios son los que hacen del protocolo una herramienta útil para elevar la calidad del servicio ya que se pueden tomar medidas preventivas y correctivas de eventos inesperados con acciones trasparentes al usuario final.

BIBLIOGRAFÍA

- Mauro Douglas R., Schmidt Kevin J. ESSENTIAL SNMP. John Wiley & Sons, 1999.
- Zeltserman David, Zeltserman Dave. PRACTICAL GUIDE TO SNMPV3 AND NETWORK MANAGEMENT. 1ª edición (Mayo 1999) Prentice Hall.
- William Stallings. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Addison-Wesley Pub Co. 3a edición.
- Craig Hunt, Gigi Estabrook (Editor). TCP/IP NETWORK ADMINISTRATION, 2a edición 1998.
- http://www.linux-es.org/art.php?id=6.

  Esta dirección contiene un artículo en el que se expresan las características generales del protocolo y algunas aplicaciones en los diferentes sistemas operativos.
- http://www.mg-soft.si/snmpv3.html.

  En esta dirección se encuentra un breve historial de SNMPv3 y un software que utiliza el protocolo SNMP en su tercera versión para monitorear redes.
- http://www.ericsson.com/support/telecom/part-h/h-8-3.shtml
- http://www.snmp.com/snmpv3/index.html

  Esta pagina es el sitio Web principal del protocolo SNMP hay se encuentran varios RFC`s y enlaces a otras paginas para encontrar mayor información de este protocolo.

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid1

  en esta pagina se va a encontrar una descripción breve sobre el protocolo en sus versiones 1 y 2.
- http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap7.php

  En esta página se encuentra una breve descripción sobre el tema de la administración de redes y su importancia.

GLOSARIO

- Agente: Agente que se ejecuta en cada nodo de la red y recoge información del terminal y de la red que se encuentran en el MIB.
- Agente intermediario SNMP: Agente SNMP asociado con una política de acceso intermediaria.
- CMIP: Common Management Information Protocol, Protocolo Común de Gestión de Información, es otro protocolo de gestíon sobre OSI (CMIP se encuentra en el nivel de aplicación OSI) y más complejo que SNMP.
- CMIS: Common Management Information Services, Servicio común de gestión de información.
- CMISE: Common Management Information Service Element, Elemento de servicio de gestión de información, es el encargado de transferir la información de gestión de un sistema a otro por lo que trabaja mano a mano con CMIP. CMISE mapea todas sus acciones en operaciones CMIP sobre el terminal remoto. Es decir, es CMISE el que manda a CMIP que envíe una PDU para realizar cierta acción, y en recepción CMIP pasa el evento a CMISE el cual lo hace llegar al usuario.
- Comunidad SNMP: Emparejamiento de un agente SNMP con un conjunto de entidades de aplicación SNMP.
- Dirección de transporte: En el servicio UDP, dirección IP seguida por un número de puerto UDP.
- Entidades de aplicación SNMP: Entidades en las estaciones de gestión y los elementos de red que se comunican utilizando el SNMP.

- Entidades de protocolo: Procesos que implementan el SNMP y por tanto soportan a las entidades de aplicaciones SNMP.
- Esquema de autentificación: Conjunto de reglas por las que un mensaje SNMP es reconocido como un mensaje SNMP auténtico para una cierta comunidad SNMP.
- Gestión de red: Se define como el proceso o control de la información compleja que circula por la red para maximizar su eficiencia y productividad. Las áreas fundamentales en las que actúa son la gestión de fallos, gestión de la configuración, gestión de la seguridad, gestión de la ejecución y gestión de la contabilidad.
- ISO: International Organization for Standardizations, Organización Internacional de Estándares.
- Manager: Gestor que se encuentra localizado en el servidor principal de la red. Su papel principal es recorrer los agentes (agents) para pedirles información importante para la gestión de la red.
- Mensaje auténtico SNMP: Mensaje SNMP originado por una entidad de aplicación SNMP que de hecho pertenece a la comunidad SNMP denominada por el componente de comunidad de dicho mensaje.
- MIB: Management Information Base, es una base de datos donde se guarda toda la información relativa a la gestión de la red. El MIB tiene una estructura en árbol, donde en la parte superior se encuentra la información más general sobre la red, y conforma avanzamos por las ramas se consigue información

más específica y detallada. Cada nodo del árbol MIB se conoce como variable, y la parte superior del árbol MIB se denomina "Internet". Aunque la ISO ha definido un MIB modelo, cada fabricante de equipos tiene el suyo propio, el que en general aunque las variables se denominen de diferente manera la información contenida en ellas es la misma.

- Modo de acceso SNMP: Elemento del conjunto {READ-ONLY, READ-WRITE}.
- Nombre de comunidad: Toda comunidad SNMP está denominada por una cadena de octetos, que forman el nombre de comunidad.
- OSI: Open Systems Interconnection, Interconexión de sistemas abiertos, protocolo de comunicación de red estructurado en 7 niveles: físico, enlace, red, transporte, sesión, presentación y aplicación. En el nivel de aplicación es donde se sitúa el protocolo CMIP. Aparición después que TCP/IP y requiere muchos más recursos en la red, por lo que su aplicación práctica es limitada en la actualidad.
- PDU: Protocol Data Unit, Unidad de datos de protocolo.
- Perfil de comunidad SNMP: Emparejamiento de un modo de acceso SNMP con un SNMP MIB view.
- Protocolo de administración de red: Protocolo de aplicación por el que las variables de la MIB de un agente pueden ser inspeccionadas o alteradas.
- Servicio de autentificación: Implementación de una función que identifica los mensajes SNMP auténticos de acuerdo a uno o más esquemas de autentificación.

- SMI: Structure of Management Information, Estructura para la información de gestión.
- SNMP: Simple Network Management Protocol, Protocolo simple de gestión de red, es un protocolo diseñado para dar al usuario capacidad de manejar remotamente otro ordenador, preguntándole y dándole valores y monitorizando los eventos que ocurren en la red. Está compuesto del MIB, del gestor (manager) y del agente gestionado (agent). SNMP funciona sobre TCP/IP en su nivel de aplicación.
- SNMP MIB View: Subconjunto de objetos en el MIB que son propios a un elemento de red.
- TCP/IP: Transport Control Protocol / Internet Protocol, es el protocolo base para las comunicaciones por Internet que permite que subredes con distinto protocolo en su interior puedan comunicarse entre sí.
- UDP: User Datagram Protocol, Protocolo de datagramas de usuario. Se trata de un servicio de transporte no orientado a conexión.