ANÁLISIS DEL FUNCIONAMIENTO DEL PROTOCOLO SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

Rafael Gómez Abreo

Ginet Vanessa Rodríguez Garcés

Universidad Industrial de Santander

Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones

Facultad de Ingenierías Físico-mecánicas

Especialización en Telecomunicaciones

Bucaramanga, Colombia

2012

ANÁLISIS DEL FUNCIONAMIENTO DEL PROTOCOLO SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

Rafael Gómez Abreo

Ginet Vanessa Rodríguez Garcés

Trabajo de investigación presentado como requisito parcial para optar al título de:
Especialista en Telecomunicaciones

Director (a):
Ing. De Sistemas y Especialista en Telecomunicaciones Raúl Bareño Gutiérrez

Línea de Investigación:
Línea estratégica de aporte al desarrollo regional

Universidad Industrial de Santander
Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones
Facultad de Ingenierías Físico-mecánicas
Especialización en Telecomunicaciones
Bucaramanga, Colombia
2012

A C UE R D O No. 164 DE 2003
(Diciembre 16)

ARTÍCULO 2º. Derogar el Acuerdo Académico No. 080 del 27 de abril de 1999.

COMUNÍQUESE Y CÚMPLASE,

Expedido en Bucaramanga, a los dieciséis (16) días del mes de diciembre de 2003.

LA PRESIDENTA DEL CONSEJO ACADÉMICO,

LUCILA NIÑO BAUTISTA
Vicerrectora Académica

LA SECRETARIA GENERAL, LILIA AMANDA PATIÑO DE CRUZ

Agradecimientos

A Dios Por haberme permitido llegar hasta este punto, logrando así cumplir con un objetivo de mi vida, además de su infinita sabiduría y amor.

A mis padres Rafael y Libia por haberme apoyado en todo momento, por sus consejos, sus valores y la motivación constante que me permitió seguir a delante para culminar una etapa más de mi vida

Rafael Gómez Albreo

Primero gracias a Dios por darme la fuerza para seguir adelante y darme la sabiduría y el entendimiento para cumplir mis metas

A mis padres, Gerardo y Stella por su apoyo, esfuerzo y por ser el motor para alcanzar mis metas.

Gineth Vanessa Rodríguez Garcés

Contenido

Pág.

Introducción **14**

1. Planteamiento del Problema **16**
1.1 Justificación 16
1.2 Objetivo General 17
1.3 Objetivos Específicos 17

2. Antecedentes y Marco Conceptual **18**
2.1 Antecedentes 18

3. Marco Teórico **24**
3.1 Documentación sobre SNMP 24
3.1.1 ¿Qué es SNMP? 24
3.1.2 Arquitectura Modelo organizativo 25
3.1.3 Estructura PDU en SNMP 30
3.2 SNMPV2 34
3.2.1 Características adicionales de la SMI 35
3.2.2 Nuevos protocolos de operación 36
3.2.3 Posibilidad de comunicación gestor – gestor. 38
3.2.4 Características adicionales en seguridad. 38
3.3 SNMPv3 40
3.3.1 Arquitectura snmpv3. 43
3.3.2 Estructura de Mensaje 51
3.3.3 Modelo de seguridad basado en usuarios (USM) 53

4. Parámetros de caracterización del protocolo **55**
4.1 RFCs 55
4.2 Particularidades de SNMP 67

5. Caracterización del protocolo **80**

6. Conclusiones y recomendaciones **86**
6.1 Conclusiones 86

Bibliografía **87**

Lista de figuras

Pág.

Figura 1: Línea de tiempo SNMP……..19
Figura 2: Arquitectura del Modelo de Gestión…….25
Figura 3: Diagrama entidad SNMPv3 ……..44
Figura 4: Formato del mensaje SNMPv3…….51

Lista de tablas

Pág.

Tabla 1 Antecedentes……18

Tabla 2: PDUs de SNMPv2……36

Tabla 3. RFCs donde se describe a SNMPv3……..41

Tabla 4: Receptores SNMP……72

Tabla 5: Recepción traps pandora FMS……..73

Resumen

TITULO: **ANÁLISIS DEL FUNCIONAMIENTO DEL PROTOCOLO SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) ***

AUTORES: Rafael Gómez Abreo, Ginet Vanessa Rodríguez Garcés * *

PALABRAS CLAVES: SNMP, Dispositivo, Red, Sistema, Software.

SNMP es un protocolo que permite realizar la gestión de la red de forma estandarizada, puede utilizar una tecnología común para intercambiar información de manera consistente entre los dispositivos de la red y también es usado para gestionar sistemas software, está basado en diferentes componentes como lo son la Estructura de Administración de la Información, la Administración de la base de Información y la capacidad de seguridad y administración de objetos, los cuales permiten realizar una mejor administración a la red deseada todo esto mediante un único protocolo y estándar.

En este trabajo se caracteriza el funcionamiento del protocolo SNMP a través de parámetros que permitan la identificación de los principales aspectos del protocolo, como lo son la administración, información de entrada e información de salida, identificando las diversas categorías que este tiene, así como la evolución que el protocolo ha ido teniendo entre sus diferentes versiones pudiendo ver las características más relevantes de cada una y los cambios de seguridad que estas han tenido para realizar una mejor gestión. Por otra parte se tienen las plataformas de uso comercial en las cuales el protocolo funciona dejando ver las particularidades más relevantes de las mismas al momento de ser requeridas.

* Proyecto de Grado

* * Facultad: Ingenierías Físico-mecánicas Escuela. Ingeniería Eléctrica, Electrónica y de Telecomunicaciones Director. ING. RAÚL BAREÑO GUTIÉRREZ

Abstract

TITTLE: **ANALYSIS OF THE FUNCTIONING OF THE PROTOCOL SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) ***

AUTHORS: Rafael Gómez Abreo, Ginet Vanessa Rodríguez Garcés **

KEYWORDS: SNMP, Network Device, Software, Protocol, Information.

SNMP is a protocol that allows the network management in a standardized way, you can use a very common technology to consistently share information between network devices and is also used to manage software systems, is based on different components as they are Structure of Information Management, Management Information base and capacity management and security objects, which allow a better management to the desired network all this through a unique protocol and standard.

This work characterizes the SNMP protocol operation through the parameters that allow identify the principal aspects of the protocol, as they are administration, information input and output information, identifying the different categories that it has, and the evolution that has been taking the protocol between the different versions can see the most relevant characteristics of each security and these changes have been for better management. Furthermore they have commercial platforms in which the protocol operates revealing the most significant characteristics of the same when being requested.

* Proyecto de Grado

* * Facultad: Ingenierías Físico-mecánicas Escuela. Ingeniería Eléctrica, Electrónica y de Telecomunicaciones Director. ING. RAÚL BAREÑO GUTIÉRREZ

Introducción

Con la manera tan diversa en que han crecido las redes, se requiere que se creen formas de trabajo innovadoras que proporcionen al administrador de red la facilidad de hacer seguimientos a todos los recursos de la red y es por eso que surge el desarrollo de los modelos de gestión, para ofrecer a las empresas sistemas estándares que contribuyan a llevar un mejor registro acerca de sus recursos informáticos y así mismo mejorar la calidad del servicio a sus usuarios.

La gestión de dispositivos antes de que surgiera SNMP era muy diferente a la que se utiliza actualmente, antes existían estaciones dedicadas de gestión, algunas con varias ventanas para diferentes tipos de información como estadísticas, actividades entre otras y cada una era específica de cada fabricante, De hecho era muy poco común que un fabricante tuviera una estación de gestión común para todos sus dispositivos. No existía un protocolo común, si no una gran cantidad de protocolos propietarios, por este motivo se desarrolló SNMP (Simple Network Management Protocol) para solucionar este inconveniente.

Desde que se publicó el primer RFC de SNMP hace más de 20 años, SNMP ha sido actualizado varias veces y se ha convertido en un estándar que se implementa en prácticamente todo los dispositivos de red.
Teniendo en cuenta los factores ya mencionados surge la idea de realizar un análisis del protocolo SMNP, que facilite al lector el entendimiento y funcionamiento del mismo, a través de una caracterización del protocolo que permita observar las diferentes plataformas comerciales (IBM, Solarwinds, Castle

Rock, Ca Spectrum), además de mostrar un ejemplo de su configuración que le dé una noción al lector de cómo se realiza esta.

En este documento se presenta el desarrollo del proyecto bajo seis (6) capítulos los cuales son: Planteamiento del problema, antecedentes y marco conceptual, marco teórico, parámetros de caracterización del protocolo, caracterización del protocolo y conclusiones y recomendaciones. El en el primero se describe el problema y sus elementos, se justifica la realización del proyecto y se establecen los objetivos, en el segundo: antecedentes y marco conceptual, se dan a conocer antecedentes de tipo histórico y práctico, así mismo la manera en que surge SNMP, en el tercero: el marco teórico en el cual se muestra qué es SNMP, su modelo organizativo, las estructuras de sus PDU, SNMPv2 y SNMPv3, en el cuarto: parámetros de caracterización del protocolo se define el software para la administración de la red y sus diferentes categorías, en el quinto: caracterización del protocolo se definen las principales características de las plataformas comerciales y por último en el sexto capítulo: conclusiones y recomendaciones se comparte la experiencia como profesionales al realizar el proyecto y se dan algunas recomendaciones para proyectos que traten la misma temática en un futuro.

1. Planteamiento del Problema

Al momento de realizar la administración de una red de computadores, no hay una solución única que sea fácil de implementar y sea aceptada por todos. Las que se encuentran, suelen ser propietarias y entran en conflicto cuando en la re se encuentran conectadas unidades de diferentes fabricantes, necesitando una plataforma por fabricante y haciendo que la administración de la red se vuelva compleja.

Es por esto que se quiere realizar el análisis del funcionamiento del protocolo SNMP, con el fin de identificar la información acerca de los diferentes componentes de la red que se pueden obtener mediante este protocolo, además de observar el flujo del tráfico de la red.

1.1 Justificación

Debido al crecimiento de las redes tanto LAN, como WAN y su intercomunicación, es necesario que los sistemas de gestión de red sean flexibles, capaces de soportar nuevos elementos que se van agregando a esta, sin necesidad de realizar grandes modificaciones.

Para poder solucionar este tipo de problemas, la Internet Architecture Board (IAB), encargada de establecer las políticas de internet, definió el SNMP como marco de administración de red y fijó un conjunto de protocolos estándar que permiten agilizar estos procesos.

Por tanto, es necesario tener en cuenta este protocolo ya que facilita al administrador al momento de integrar diferentes soluciones a la red.
Debido a que la información que hay sobre la configuración del protocolo SNMP no está unificada, se quiere que este proyecto sea una guía de consulta para el entendimiento de este protocolo al momento de realizar una administración de red.

1.2 Objetivo General

Caracterizar el funcionamiento del protocolo simple de administración de red (SNMP), con sus componentes básicos tales como: Dispositivos administrados, agentes y sistema de administración de red (NMS'S) teniendo en cuenta las características más relevantes de dichos componentes.

1.3 Objetivos Específicos

- Estudiar el protocolo SNMP basado en la literatura existente.

- Seleccionar los parámetros para la caracterización de los principales aspectos del protocolo tales como: administración, información de entrada e información de salida.

- Valorar los principales aspectos del protocolo SNMPv3 a partir de los parámetros seleccionados.

2. Antecedentes y Marco Conceptual

2.1 Antecedentes

ANTECEDENTE	AUTOR	INFORMACIÓN DE REFERENCIA	APORTE PROYECTO	FECHA VISUALIZACIÓN
ADMINISTRACIÓN DE REDES UTILIZANDO PROTOCOLO SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)	Velásquez HernándezJhon Eduarson (2009)	http://www.bdigital.unal.edu.co/799/	En este antecedente se identifica el modelo de gestión SNMP, Se analiza el protocolo, sus servicios y niveles de seguridad que son necesarios para la protección de la red.	3 Septiembre de 2011
MODELO DE GESTIÓN DE SEGURIDAD CON SOPORTE A SNMP.	Botero Arana Nicolás (2005)	http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf	Permite observar la manera en cómo se crea un modelo de gestión de seguridad de red. A través de módulos para monitorear su monitoreo.	28 Septiembre de 2011
PROTOCOLO SNMP (PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE REDES).	Briceño Caryuly Rosales (2004)	http://redalyc.uaemex.mx/pdf/784/78430108.pdf	Destaca la importancia que representan las plataformas tecnológicas con un conjunto de equipos necesarios para la administración de redes por medio de SNMP.	12 Octubre de 2011
DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA MULTIPLATAFORMA DE MONITORIZACIÓN Y ADMINISTRACIÓN DE RED, CON INTERFAZ WEB PARA EL USUARIO Y UTILIZANDO EL PROTOCOLO SNMPv3.	Fausto Vinicio Castañeda Villareal (2011)	http://bibdigital.epn.edu.ec/bitstream/15000/2784/1/CD-3432.pdf	Da una noción de los fundamentos del protocolo SNMP, y muestra un análisis del protocolo SNMPv3.	24 Enero de 2011

ESTUDIO Y DESARROLLO DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN Y ADMINISTRACIÓN DE RED PARA LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO (UTEQ)	Olga Alexandra Rosero Vlasova, Diego Alejandro Proaño Sarasti (2009)	http://dspace.epn.edu.ec/bitstream/15000/8936/5/T%2011276%20CAPITULO%201.pdf	Da a conocer una reseña histórica y conceptos generales del funcionamiento del protocolo SNMP.	8 Febrero de 2011

Tabla 1: Antecedentes Fuente: Los autores

Revisando la línea de tiempo (Figura 1) se puede ver que el desarrollo de SNMP inicio después del protocolo de transferencia FTP, Control remoto de hosts Telnet y el protocolo de sistemas de correo SMTP.

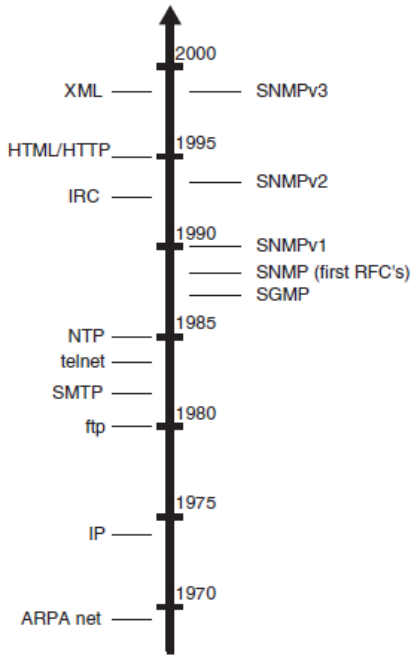

Figura 1: Línea de tiempo SNMP [1]

En agosto de 1988, la IAB (Internet Architecture Board) encargada de establecer las políticas de internet, decide definir un marco de administración de red y fijar un conjunto de protocolos estándar que permitieran agilizar estos procesos. Esto conlleva a que SNMP surja para resolver los problemas de administración de

redes TCP/IP, debido a que el crecimiento apresurado y desmesurado de este tipo de redes ha hecho que la administración y gestión de las mismas se convierta en una labor intensa.

SNMP es una herramienta sencilla para la gestión de red. Define una base de información de gestión (MIB) limitada y fácil de implementar de variables escalares y tablas de dos dimensiones, y define un protocolo para permitir a un gestor obtener y establecer variables MIB, para permitir a un agente emitir notificaciones no solicitadas llamadas intersecciones (traps). SNMP se implementa de una forma fácil y consume un tiempo modesto de procesador y de recursos de red. [1]

SNMP está formado por cuatro componentes básicos:

- BASE DE DATOS LÓGICA: Se almacena información referente a la configuración, estado y rendimiento.
- AGENTES: Es un software que responde a peticiones, realiza actualizaciones e informa los problemas.
- ADMINISTRADORES: Contiene un software de administrador, el cual se encarga de enviar y recibir los mensajes Snmp. Además de esto existen otra serie de aplicaciones de administración que se comunican con los sistemas de red, mediante el administrador.
- BASE DE INFORMACIÓN DE ADMINISTRACIÓN: Denominadas MIB, constituye la descripción lógica de todos los datos de administración de la red. La MIB contiene información del estado y del sistema, estadísticas de rendimiento y parámetros de configuración.

La arquitectura de Snmp es de tipo modular y está basado en las siguientes especificaciones:

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

SNMP define el formato y el significado de los mensajes que intercambia el administrador y el agente. En lugar de definir muchas operaciones el protocolo utiliza el paradigma de obtención y almacenamiento, en el cual el administrador manda las solicitudes de obtención y almacenamiento de valores en variables.

SNMPv1 es un protocolo de fácil entendimiento con amplio soporte hardware y software, usado en diferentes soluciones de aplicaciones de administración consumiendo poco recursos permitiendo ser implementado en dispositivos de gama baja.

SNMPv1 tiene la desventaja en conceptos de seguridad y la perdida de ancho de banda causada por las PDU y sus mecanismos.

Debido al gran uso del protocolo se revelan las deficiencias funcionales y la falta de una herramienta de seguridad es por este motivo se crean las versiones SNMPv2 y SNMPv3.

En Abril de 1993 las especificaciones del protocolo de administración de red simple versión 2 (SNMPv2) fue modificado en RFC1441 a RFC1452. Algunas de estas especificaciones fueron marcadas como históricas, mientras otras, como el modelo de seguridad fue revisado y mejorado por nuevas especificaciones (RFC1901) a (RFC19010) publicado en enero de 1996.

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

Mientras SNMPv1 define una relación clara entre el administrador y un número de agentes, la versión 2 no, trabaja con entidades, cada entidad toma ambos roles los de un administrador y un agente, ejerciendo una función doble, esta versión soporta diferentes protocolos de transporte como Novel IPX, Apple talk.

SNMPv2 fue un gran avance al momento de ser publicado, este llevaba la versión SNMPv1 a todas las áreas, pero estas extensiones también incrementaron la complejidad de cada implementación así como un pago base era requerido para encriptar y autenticar si estas características eran usadas. La utilización del protocolo en su segunda versión permite tener una mejor conciencia en la definición de los módulos MIB, mientras no todos los macros pueden ser usados por la misma extensión por diseñadores MIB.

SNMPv3 surgió en 1998 como un conjunto de estándares RFC 2570 a 2575, para corregir las deficiencias en seguridad de SNMPv1 y SNMPv2, este protocolo no proporciona una capacidad de SNMP completa si no que define una arquitectura general de SNMP y un conjunto de capacidades en seguridad.

El protocolo en su última versión proporción tres servicios importantes:

- Autentificación
- Privacidad
- Control de acceso

Los dos primeros forman parte del modelo de seguridad basada en usuario y el último está definido en el modelo de control de acceso basado en consideraciones.

Con SNMPv3 el área de seguridad fue mejorada después de diferentes soluciones que fueron propuestas y fallidas en su versión anterior por otra parte el enfoque modular para la descripción de una entidad SNMP ayudó a crear soluciones modulares. [2]

3. Marco Teórico

El presente capítulo describe de manera detallada el protocolo de administración de red simple SNMP, este protocolo permite el acceso a las bases de datos del dispositivo y modificar parámetros asociados a las mismas, con lo que los cambios se reflejan de manera inmediata. SNMP es un protocolo que permite la gestión de los recursos que están disponibles en una red. Dentro de un entorno de red gestionado con SNMP habrá un conjunto de nodos de la red que se encarguen de la gestión y un conjunto de componentes de la red (Host, routers, módems) que podrán ser gestionados por estaciones.

3.1 Documentación sobre SNMP

3.1.1 ¿Qué es SNMP?

Es el protocolo empleado para la administración de redes basados en TCP/IP como lo es internet, siendo esta la configuración de redes más extendida.

El entorno de trabajo de este protocolo se basa en los siguientes componentes:

- SMI (Estructura de administración de la información): Define la estructura lógica de la información de gestión, cómo se identifica y describe. Los objetos MIB se especifican a partir de este lenguaje.
- ADMINISTRACION DE LA BASE DE INFORMACIÓN: Conforma la descripción lógica de todos los datos de administración de la red, los objetos MIB definen la información de administración que mantiene un dispositivo y aquellos que están relacionados.

- Capacidad de seguridad y administración de objetos. [3]

3.1.2 Arquitectura Modelo organizativo

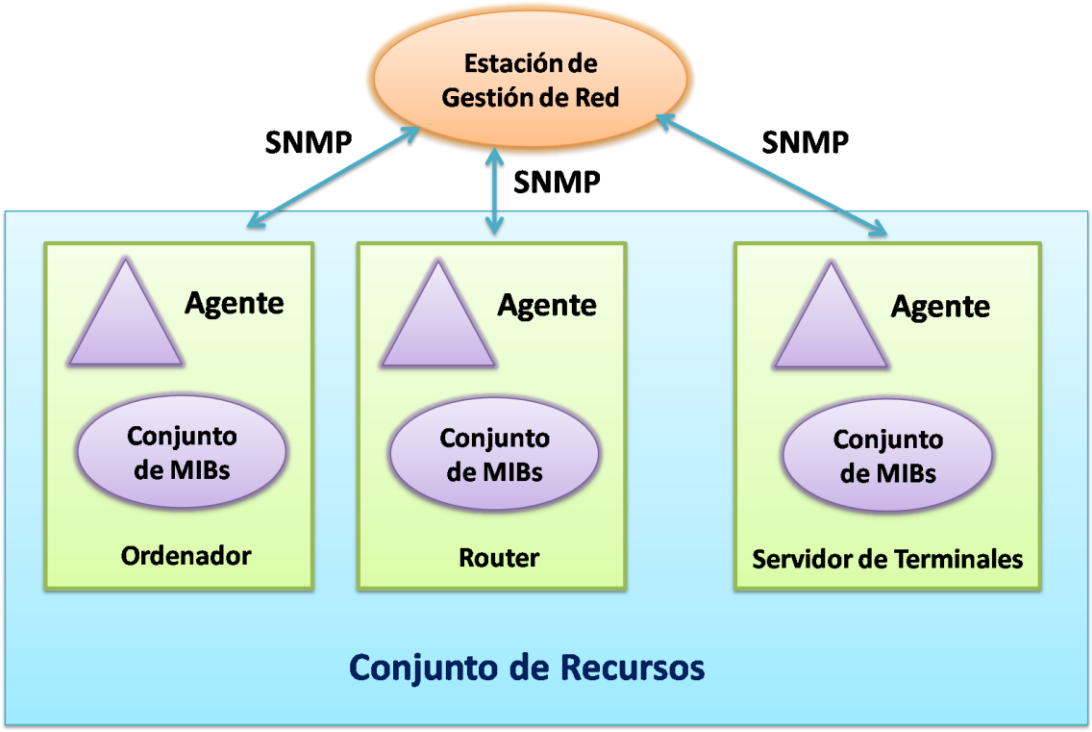

Figura 2: Arquitectura del Modelo de Gestión [4]

El modelo organizativo de la administración de redes basado en SNMP, se compone de los siguientes elementos:

- AGENTE DE GESTIÓN: Es el encargado de supervisar los elementos de la red, se comunica con el gestor para atender sus peticiones e informarle de eventos del objeto gestionado. Se encuentra en una estación de trabajo o nodo que ejecuta un sistema operativo común y corriente, dispone de una

cantidad de RAM suficiente que le permite almacenar todas las aplicaciones de administración que se están ejecutando al mismo tiempo, sin embargo también se puede implementar en diversos sistemas .

Incluye una variedad de software llamado NMA (Aplicación de Administración de Red) que incorpora una interfaz gráfica de usuario para permitir a los administradores autorizados controlar la red.

- AGENTE: El agente es un software que permite el acceso a la información, responde a peticiones, realiza actualizaciones e informa los problemas. Representa a la parte del servidor en la medida que tiene la información que se desea administrar y espera los comandos por parte del cliente (entidad administradora).

  Todos los datos del agente se almacenan en su MIB y entre las principales funciones que un agente puede controlar son:

  - ✓ Número de bytes y paquetes entrantes.
  - ✓ Mensajes de difusión enviados y recibidos.
  - ✓ Interfaces de red que han caído y que se han activado.
  - ✓ Número de ciertos tipos de mensajes de error.

- BASE DE INFORMACIÓN DE ADMINISTRACIÓN: Denominada MIB constituye la descripción lógica de todos los datos de administración de la red. La MIB contiene información de estado y del sistema, estadísticas de rendimiento y parámetros de configuración.

La estructura de funcionamiento se encuentra definida en el SMI la cual define los tipos de datos que pueden utilizarse para almacenar un objeto, como deben nombrarse dichos objetos y cómo deben codificarse para su transmisión sobre la red.

Existen varios tipos de estas:

- ✓ MIB estándares.
- ✓ MIB experimentales.
- ✓ MIB privadas.

Los valores que se encuentran almacenados en la MIB son consultados y actualizados por una entidad administradora enviando mensajes SNMP al agente que se está ejecutando, en un dispositivo administrado en representación de la entidad administradora.

- PROTOCOLO DE GESTIÓN: Es el protocolo que especifica cómo se realizará la comunicación entre los agentes de gestión y el gestor. En este caso sería el protocolo SNMP, la comunicación se realiza en base a requerimientos, respuestas y notificaciones.

  Existen dos formas de comunicación entre los agentes y entidades administradoras:

  - ✓ MODO PETICIÓN RESPUESTA: Comúnmente usado por SNMP donde la entidad administradora envía una petición a un agente que la recibe, realizando una acción y enviando una respuesta a tal petición.

- ✓ MODO DE NOTIFICACIONES: El agente envía un mensaje no solicitado denominado mensaje trampa, a una entidad administradora. Dichos mensajes se utilizan para notificar una situación específica que lleva a realizar cambios en los valores de los objetos MIB.

El encargado de efectuar la comunicación entre el administrador y el agente es un protocolo de administración de la capa de transporte, mediante un intercambio de mensajes que ejecutan las operaciones de administración.

Es posible clasificar a los mensajes en tres grupos de acuerdo a los modos de operación de SNMP los cuales son:

- ✓ LECTURA: Sucede cuando el administrador recupera distancias de objetos administrados de un agente, permitiendo obtener el estado del dispositivo administrado. Un ejemplo claro son las PDU Get, GetNext, GetBulk.

- ✓ ESCRITURA: Se crea o modifica las instancias de objetos administrados en un agente, permitiendo actuar sobre el dispositivo administrado, se tienen los mensajes de tipo escritura, ejemplo; el mensaje Set.

- ✓ NOTIFICACIONES: El agente informa al administrador de una situación inesperada a través de este tipo de mensajes, ejemplo: TRAP, SNMPV2-TRAP.

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, una PDU (Unidad de datos de protocolo) y un nombre de comunidad SNMP, estos datagramas no necesitan ser mayores de 4,84 bytes pero es recomendable que las implementaciones de este protocolo soporten longitudes mayores. Todas las implementaciones de SNMP soportan 5 tipos de PDU.

Los datos que incluyen una PDU genérica son los siguientes:

- RequestID: Entero que indica el orden de misión de los datagramas, funciona para identificar datagramas duplicados en los servicios de datagramas poco fiables.
- ErrorStatus: Entero que indica si ha sucedido algún error y puede adquirir los siguiente valores:
  - ✓ NoError (0)
  - ✓ ToBig (1)
  - ✓ NoSuchName (2)
  - ✓ BadValue (3)
  - ✓ ReadOnly (4)
  - ✓ GenErr (5)

- ErrorIndex: Entero que en 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 solo con nombres, pero aún así deben llevar valores asociados, se recomienda para estos casos la definición de un valor NULL. [5]

3.1.3 Estructura PDU en SNMP

GetRequest-PDU y GetNextRequestPDU: Estas PDU solicitan a la entidad destino los valores de ciertas variables. En el caso de GetRequest-PDU las variables son las que se encuentran en la lista VarBindList, en GetNextRequestPDU son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de las listas.

Estas PDU siempre esperan como repuesta una GetResponsePDU.

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 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:

- Si algún nombre de la lista 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.
- Si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era una GetRequest-PDU.
- Si se ha recibido una SetRequest-PDU y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, salvo en que el campo ErrorStatus tendrá el valor 3 (badValue) y el campo ErrorIndex señalará el objeto de la lista que ha generado el error.
- Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 1 (tooBig).
- Si el valor de algún objeto de la lista no puede ser obtenido por una razón no contemplada en las reglas anteriores, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida.

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.

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 de la interfaz afectada.

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

- Trampa de fallo de autentificación (authenticationFailure): 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 variable-bindings es el nombre y el valor de la dirección del vecino afectado.

- Trampa específica (enterpriseSpecific): La entidad remitente reconoce que ha ocurrido algún evento específico. El campo specific-trap identifica qué trampa en particular se ha generado. [4]

3.2 SNMPV2

Las limitaciones que surgen con SNMP lleva a la creación de dos nuevos protocolos, S-SNMP (SNMP seguro) el cual da seguridad al protocolo SNMP y

SMP (Simple Management Protocol) un nuevo protocolo sin características de seguridad pero que fortalece las características de funcionalidad y rendimiento del SNMP. Es por esto que en 1993 se unen estas dos aproximaciones dando como resultado SNMPv2.

SNMPv2 se diferencia de sus anteriores versiones en diversas secciones como se puede ver en la siguiente lista:

3.2.1 Características adicionales de la SMI

Se añaden nuevas sintaxis:

- ✓ Integer32: para complemento a 2 en 32 bits.
- ✓ UInteger32: números naturales hasta 32 bits.
- ✓ BitString: numeración de bits en octetos.
- ✓ Counter32: contador más amplio.
- ✓ NSAPAddress: direcciones OSI.
- ✓ Counter64: si el de 32 bits se llena en menos de una hora.

Se incluye una cláusula adicional UNITS para indicar la unidad de medida asociada con un objeto de medida.

Se pueden definir 4 tipos de acceso:

- ✓ Not-accesible.
- ✓ Read-only
- ✓ Read-write

- ✓ Read-create
- ✓ Accesible-for-notify

Varios tipos de estructuras:

- ✓ Textual Conventions: Formalizan la semántica de tipos de datos.
- ✓ Module Identity: Macro con información administrativa sobre la MIB, revisión, persona de contacto, etc.
- ✓ Object Groups: Macro para formalizar la agrupación de objetos en grupos.
- ✓ Notification Type: Define información a enviar cuando se produce un evento excepcional.
- ✓ Module-Compliance: Lo mínimo que un agente debe implementar de esa MIB.
- ✓ Agent-Capabilities: Lo que realmente implementa un agente.

3.2.2 Nuevos protocolos de operación

Las PDUs de SNMPv2 son encapsuladas en un mensaje. En la cabecera de dicho mensaje se determina cuáles serán las políticas de autentificación y autorización.

SNMPv2	**Dirección**	**Descripción**
GetRequest	Gestor -->Agente	Solicita el valor de cada

		objeto en la lista
GetNextRequest	Gestor -->Agente	Solicita el siguiente valor para cada objeto listado
GetBulkRequest	Gestor -->Agente	Solicita múltiples valores
SetRequest	Gestor -->Agente	Establece el valor para cada objeto listado
InformRequest	Gestor -->Agente	Transmite información de gestión no solicitada
Response	Agente --> Gestor Gestor --> Gestor (SNMPv2)	Responde a una petición de un gestor .
SNMPv2-Trap	Agente --> Gestor	Transmite información no solicitada asociada a un evento.

Tabla 2: PDUs de SNMPv2 [3]

Caracterización de las PDUs

Se definen dos nuevas operaciones en el protocolo:

- ✓ **GetBulkReques:** Permite recuperación de tablas de una forma eficiente, minimizando el número de intercambios. Opera de forma parecida a GetNextRequest, pero este indica varios sucesores a uno dado, Se pueden especificar variables de recuperación simple y variables de recuperación múltiple.

Incluye dos nuevos parámetros en su PDU:

- non-repeaters: Número de variables de la lista de la que se realizará recuperación simple.
- max-repetitions: Número de veces para recuperaciones múltiples.

✓ **InformRequest:** Esta operación permite establecer comunicación entre gestores, La configuración de estas comunicaciones son a través de la M2M MIB.

Hay dos tipos de comunicaciones, por la aparición de algún evento o a petición de algún gestor

3.2.3 Posibilidad de comunicación gestor – gestor.

Es un conjunto de objetos que describen el comportamiento de una entidad SNMPv2 la cual actúa de gestor, Por medio de esta MIB se realizan las comunicaciones entre gestores SNMPv2.

Contiene dos grupos, Alarm y Event.

3.2.4 Características adicionales en seguridad.

La seguridad es el mayor cambio que se origina con respecto a la primera versión de SNMP, permite dotar de privacidad y autenticidad a las primitivas de SNMPv2.

Incorpora el concepto de party heredado de S-SNMP, Se incorpora a la cabecera del mensaje información del contexto (vista MIB) sobre el que actuará el mensaje.

La generación de un mensaje consta de los siguientes pasos:

- ✓ Se construye el valor del SnmpMgmtCom donde:
  - SrcParty: identifica la parte origen.
  - DstParty: identifica al destino.
  - Context: indica la vista MIB sobre la que se actuará.
  - PDU: representa la operación de gestión deseada
- ✓ Se construye el valor de SnmpAuthMsg donde:
  - AuthSrcTimestamp: indica el clock del origen.
  - AuthDstTimestamp: indica el clock del destino.
  - AuthDigest: resumen generado por MD-5 en la parte origen.
- ✓ Se encripta el SnmpAuthMsg.
- ✓ Se ubica en el campo privDst de SnmpPrivMsg el identificador de la parte destino.

La recepción del mensaje consta, a su vez, de los siguientes pasos:

- ✓ Si el privDst no es válido, se rechaza el mensaje.
- ✓ Se desencripta el privData para obtener el SnmpAuthMsg.
- ✓ Se rechaza el mensaje si no casa el privDst con dstParty o se desconoce el srcParty.
- ✓ Se rechaza el mensaje si no cuadran los Timestamp dentro del margen.
- ✓ Se extrae el valor del authDigest y se compara con el nuevo cálculo.

- ✓ Se consulta el contexto para ver si la operación solicitada es posible.

3.3 SNMPv3

Esta versión del protocolo SNMP incluye la funcionalidad de las versiones anteriores y tiene como principales objetivos lo siguiente:

- Proporciona seguridad a través de la verificación de la integridad del mensaje (asegura que el paquete no haya sido violado durante la trasnmisión), realizar encriptación (como una forma de prevención) y autentificación (esto determina si el mensaje viene de una fuente válida).
- Usar al máximo el hardware existente
- Proporcionar compatibilidad con el software existente,
- Realizar la implementación de las actualizaciones del protocolo de forma sencilla.
- Permitir el soporte adecuado para monitoreo de grandes redes, cumpliendo los objetivos de forma sencilla y relativamente económico.

Este protocolo está basado en tres tipos de elementos básicos:

- Managers o gestores: tiene asignado el puerto 162. Está formado por uno o varios nodos que funcionan como agentes, con los cuales se comunica utilizando comandos, debe contener generadores de comandos y algún módulo que le permita recibir notificaciones. Puede ser único o puede tratarse de un sistema de gestores que trabajen juntos, en cuyo caso deben tener un protocolo de administración que les permita comunicarse entre ellos.

- Agents o agentes: Tiene asignado el puerto 161. Es responsable de responder a los comandos ejecutados por el gestor para modificar los parámetros de operación o configuración local, proporcionar información al gestor; ya sea solicitada o avisando anormalidades; y para poder llevar a cabo esas tareas deberá recolectar y mantener información sobre la configuración y funcionamiento del ambiente local en una base de datos.

- MIB (Management Information Base) o base de información de administración: contiene información reciente e histórica a cerca de la configuración local y del tráfico que maneja la entidad que la mantiene (que puede ser un agente, un gestor o una combinación de ambos).

La IETF propone un conjunto de RFC desde la 2271 a la 2275 que definen un conjunto de medidas para implementar las tres grandes falencias que poseía el protocolo SNMP, Autenticación, Seguridad, y control de acceso.

Estos estándares definen la nueva versión del protocolo SNMPv3, el fin de este es definir una arquitectura modular que de flexibilidad hacia futuras expansiones.

Número	Titulo	Fecha
RFC 2271	An Architecture for Describing SNMP Management Frameworks	Enero 1998
RFC 2272	Message Processing and Dispatching for SNMP	January 1998
RFC 2273	SNMPv3 Applications	January 1998

RFC 2274	User-Based Security Model for SNMPv3	January 1998
RFC 2275	View-Based Access Control Model (VACM) for SNMP	January 1998

Tabla 3. RFCs donde se describe a SNMPv3 [6]

Según el RFC 2574 el protocolo SNMPv3 mediante el uso de algoritmos de autenticación y de encripción fue diseñado para proteger de las amenazas de seguridad que se muestran a continuación:

- Poca Privacidad: el intercambio de mensajes entre un agente y una consola de administración para aprender los valores de los objetos puede ser visto por una entidad.
- Enmascaramiento (masquerade): Las operaciones que no están autorizadas para un usuario específico pero pueden ser ejecutadas asumiendo la identidad de otro usuario que esté autorizado.
- Modificación de la Información: una entidad puede realizar la modificación de un mensaje generado por otra que este autenticada dando como resultado una acción autorizada en la entidad que va a recibir el mensaje, el inconveniente es que se puede modificar algún parámetro de configuración.
- Reenvío de mensajes: hay riesgo de que un mensaje SNMP sea almacenado por un tercero pudiendo ser reenviado o duplicado para realizar operaciones de administración no autorizadas.

Así mismo, el protocolo no está diseñado para la prevención de los siguientes tipos de ataque:

- Análisis de tráfico: el atacante puede conocer el patrón de tráfico entre las dos unidades.
- Denegación de servicio: prevención en el intercambio de mensajes entre el agente y la consola de administración. [7]

Este protocolo de gestión, ofrece 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 vulnerado durante la transmisión.
- **Autenticación:** Determina que el mensaje proviene de una fuente válida.
- **Encripción:** Porque encripta el contenido de un paquete como forma de prevención

3.3.1 Arquitectura snmpv3.

SNMPv3 se basa en una arquitectura modular la cual ofrece los servicios de seguridad, como Autenticación, Privacidad, Control de Acceso.

Para poder ofrecer estos servicios el Protocolo maneja una entidad en la cual la mayoría de los servicios son procesados, esta entidad puede actuar en forma individual en un rol particular, como una aplicación o un conjunto de estas. La entidad opera desde una estación y envía comandos SNMP hacia los agentes, el

trabajo de unión entre la entidad y el agente determinan las capacidades de seguridad que serán llamadas, tales como autenticación, privacidad y control de acceso.

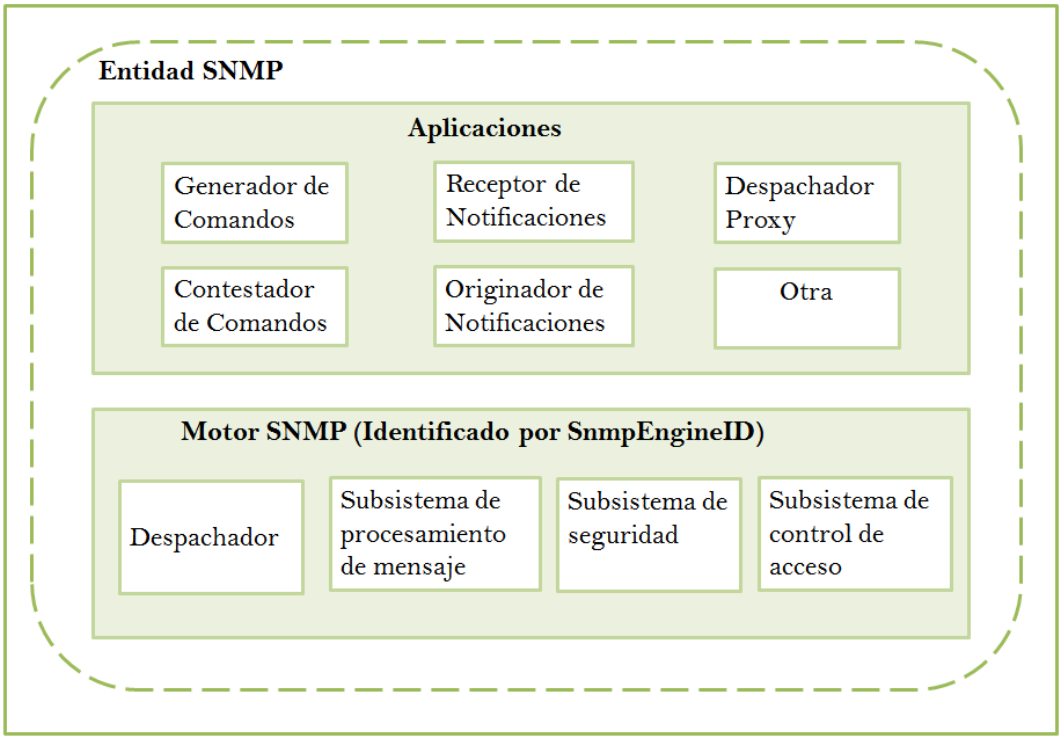

Figura 3: Diagrama entidad SNMPv3 [8]

Como se puede ver en el diagrama anterior, cada entidad contiene sólo un motor SNMP que implementa funciones de envío y recibo de mensajes, autenticación y encriptación de mensajes, así como el control de acceso.

Los componentes de una entidad SNMP son:

- SNMP ENGINE
  - ✓ Despachador:

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.

- ✓ Subsistema de procesamiento de mensajes:

Es el encargado de preparar los mensajes para su envío y la extracción de la información 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 se podría tener un Subsistema de Procesos de mensajes que contenga distintos Modelos de proceso de mensajes:

- Un modelo de proceso de mensajes que encapsule y desencapsule mensajes para el protocolo SNMPv1
- Un modelo de proceso de mensajes que encapsule y desencapsule mensajes para el protocoloSNMPv2
- Un modelo de proceso de mensajes que encapsule y desencapsule mensajes para el protocolo SNMPv3
- Un modelo de proceso de mensajes que encapsule y desencapsule mensajes para otro protocolo ya sea existente o que pueda desarrollarse en el futuro.

Es el encargado de suministrar la compatibilidad con las versiones anteriores del protocolo, para los mensajes que entran la versión de protocolo es suministrada por el Disparcher (lo puede obtener del mensaje entrante y en otra ocasión lo puede encontrar mediante un algoritmo), en cambio para los mensajes salientes el valor es dado 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.

- ✓ Subsistema de seguridad: ofrece servicios de seguridad de autenticación y privacidad de los mensajes. Este puede contener varios subsistemas, siendo responsable de suministrar los servicios de seguridad que pueden ser autenticación y privacidad en el mensaje. Este subsistema puede tener uno o varios modelos de seguridad.

Este modelo puede ser basado en usuarios (User Based Security Model), sin embargo este puede ser reemplazado o usado en conjunto con otro dependiendo de lo que se necesite.
El subsistema tiene como objetivo:

- Verificación de que los mensajes SNMP recibidos no hayan sido modificados durante su transmisión.
- Comprobar la identidad de los usuarios que están interactuando con el sistema.
- Verificar si los mensajes que están llegando a la entidad son recientes. Detectar si los mensajes que llegan a la entidad son recientes.
- Salvaguardar la privacidad de la información enviada y recibida.

✓ Subsistema de control de acceso:

Proporciona servicios de autorización a recursos, decide cual aplicación tiene derecho y el tipo de acceso que está tendrá, El control de acceso permite la restricción del acceso al MIB y limitación de las operaciones que los gestores pueden realizar sobre los agentes.

Este subsistema define un control de acceso basado en vistas, y está constituido por los siguientes elementos:

- Grupos
- Nivel de seguridad

- Contexto
- Vistas de MIB
- Políticas de Acceso

- Aplicaciones
  - ✓ Generador de comandos:

    Da inicio a las PDU's SNMP Get, GetNext, GetBulk, SetRequest que envía el sistema local y procesa las respuestas a los pedidos que antes se habían enviado.

    Para dar inicio a las respuestas se debe llamar al Dispatcher, el cual se da los datos que luego va a formar parte del header del mensaje, entre los que se va a encontrar 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.

  - ✓ Contestador de comandos:

    Recibe las solicitudes que están destinadas al sistema local y así desarrollar la operación de protocolos necesaria para generar una respuesta adecuada y reenviarla a la entidad que la solicita. Este deberá usar un control de acceso para verificar si el solicitante tiene autorización para obtener la información o a ordenar la modificación de los datos.

    Al momento de recibir la solicitud y se apruebe la respuesta del mensaje, está aplicación determinará el tipo de mensaje entrante, para comunicarse con la base de datos, preparar la respuesta y luego entregar esa respuesta al Dispatcher para que este la envíe. Si

se determina que la solicitud no se debe responder de envía al solicitante un mensaje comunicando la falla al acceso.

- ✓ Originador de notificaciones:

  Monitorea el sistema por algún evento o condición en particular, si es necesario procede a generar una operación trap.

  El creador de notificaciones primero emplea mecanismos de filtros apropiados para determinar cuál es la información que se va a enviar. Si el filtro determina que una notificación no se debe enviar, el proceso continúa. Si esto no sucede se recuperan variables de la base de datos de información local que permitan determinar la entidad a la que se debe enviar el mensaje, el modelo de seguridad que se va a usar, y nivel de seguridad necesario. Después se realiza una verificación para determinar si se debe enviar o no la notificación. Al finalizar estos pasos se construye una PDU la cual si no necesita respuesta se envía al despachador, si ocurre lo contrario antes de que la PDU se envíe al despachador se indica la necesidad de una respuesta.

- ✓ Receptor de notificaciones:

  Escucha por mensajes de notificación y a continuación genera mensajes de respuesta, los mensajes de notificación son Inform (gestor a gestor) y Trap (agente a gestor). Si el mensaje que se recibe es tipo inform se debe responder.

Lo que hace el receptor de notificaciones es registrar la llegada de la notificación y determinar de qué tipo de notificaciones se trata, si es necesaria una respuesta la prepara y es enviada al despachador.

- ✓ Despachador proxy:

  Es el encargado de direccionar los mensajes SNMP y es una aplicación de implementación opcional, se puede implementar si:

  - Hay partes de la red que no soportan el protocolo SNMP
  - Es necesario tener información en cache para minimizar la carga de trabajo de los dispositivos.
  - Autenticar y autorizar peticiones

  Es el encargado de enviar mensajes, hay cuatro tipos de estos:

  - Los mensajes creados por aplicación generador de comandos, los mensajes que el gestor le envía al cliente: Determinando a que motor debe ir el mensaje y entrega la respuesta que antes se había recibido de ese motor.
  - Los mensajes creados por la aplicación creador de notificaciones, el proxy Forwarder determina que motor deberá recibir la notificación.
  - Los mensajes creados por la aplicación receptor de notificaciones, o sea las respuestas que el agente envía al gestor, el proxy debe determinar las solicitudes y notificaciones que estuvieron en juego para adelantar respuesta.

- Mensajes que contienen las indicaciones de reporte, El proxy debe determinar que clases internas de PDU y cuales notificaciones previas están en juego. [4]

3.3.2 Estructura de Mensaje

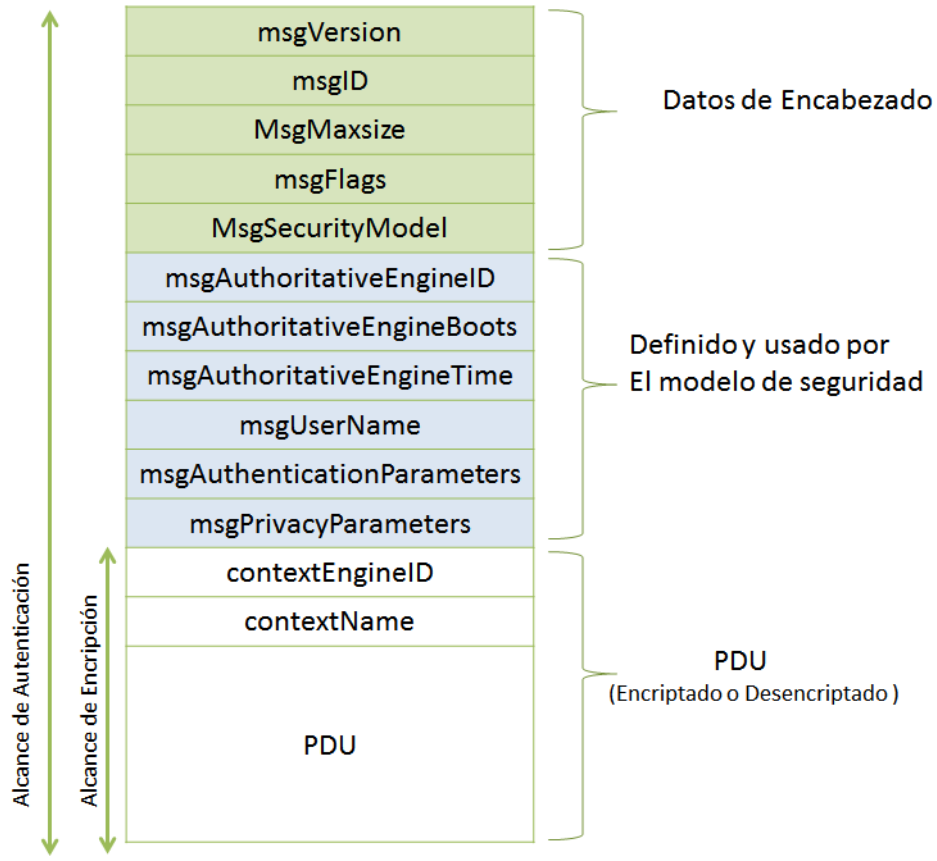

Figura 4: Formato del mensaje SNMPv3 [6]

Los campos a continuación son generados por el modelo de procesamientos de mensajes entrantes o salientes.

- **msgVersion:** Configurado para SNMPv3.
- **MsgID:** Un identificador único usado entre dos entidades SNMP para coordinar los mensajes de envío y respuesta.
- **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
- **MsgFlag:** Un arreglo de octetos que contiene tres banderas en los tres bits menos significativos.
- **MsgSecurityModel:** Es un identificador en el rango de 2^{31} – 1 que indica que modelo de seguridad fue utilizado por el que envió 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

Los 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 o Inform.

- **MsgAuthoritativeEngineBoots:** Es un entero que representa el número de veces que el SNMP Engine se ha iniciado o reiniciado desde su configuración inicial.

- **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. [7]

3.3.3 Modelo de seguridad basado en usuarios (USM)

La definición de USM para SNMPv3 es definida en el RFC 2274, Consiste en:

- Autenticación: Ofrece la integridad de datos y autenticación, usa algoritmos MD5 o SHA-1
- Timeliness: protege contra retardo o el reenvío de mensajes.
- Privacidad: realiza la encripción del contenido, usa el algoritmo DES.
- Formato del mensaje: precisa el formato del campo msgSecurityParameters.

- Descubrimiento: especifica procedimientos mediante el cual un motor SNM obtiene la información de otro.
- Administración de llaves: especifica el procedimiento para generar, actualizar y usar las llaves. [9]

4. Parámetros de caracterización del protocolo

4.1 RFCs

La entidad encargada de defender los protocolos estándar que gobiernan el tráfico de internet es la IETF (The internet Engineering Task Force). Esta entidad anuncia petición de comentarios (RFCs), las cuales son especificaciones de diferentes protocolos que existen. Estos documentos ingresan a una evaluación estándar, después cambian de ser borradores a dos categorías designadas, históricas y experimentales, definen un documento que ha sido remplazado por una nueva RFC y un documento que no está listo para ser estándar. A continuación se puede observar una lista de las versiones SNMP con sus respectivos RFCs.

- SNMP versión 1 (SNMPv1). Está definido con el RFC1157 y es un estándar histórico de IETF. Es la versión inicial del protocolo SNMP, su seguridad está basada en comunidades, las cuales no son más que contraseñas entre estos: texto plano, cadenas las cuales permiten que cualquier aplicación basada en SNMP y sepan las condiciones para acceder a la administración del dispositivo. Existen tres comunidades en SNMPv1: solo lectura, lectura y escritura, y trap.

- SNMP versión 2 (SNMPv2). Técnicamente nombrado SNMPc2c, está definido con RFC 1436, RFC 3416, RFC 3417 y RFC 3418.

- SNMP versión 3 (SNMPv3). Es la última versión de SNMP. Ofrece varias características en la administración de seguridad de la red, permite un

fuerte soporte en la autenticación y comunicación privada entre las entidades administradas. En el año 2002 se hace la transición del estándar de borrador a estándar completo. Los siguientes RFCs son los que definen el estándar: RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418 y RFC 2576. [8]

A continuación se describen las principales RFC de SNMPv3:

RFC3410 Coexistencia entre la versión 1, versión 2, versión 3, del marco de gestión del estándar de internet.

El marco de gestión estándar SNMPv2 ofrece varias ventajas sobre el protocolo SNMPv1, las cuales son:

- Aumento en el tipo de datos, un ejemplo contador de 64 bit
- Improvisar eficiencia y rendimiento, operador get-bulk
- Notificación de eventos, operador informes
- Manejo de error, errores y excepciones
- Conjunto de mejoras, especialmente en creación de filas y eliminación.

Sin embargo, el marco SNMPv2 está incompleto en que no conocer las metas del diseño original del proyecto SNMPv2. Los objetivos insatisfechos incluyen la administración y mejoramiento de seguridad como:

- Autenticación: Identificación de origen, integridad del mensaje y algunos aspectos de protección.
- Privacidad: Confidencialidad de los datos.
- Autorización y control de acceso

La versión del protocolo SNMPv3 se encarga de corregir estas deficiencias significativas.

Es así que el grupo de trabajo definió los siguientes objetivos:

- Suministrar un rango amplio en un ambiente operacional con diferentes demandas de administración.
- Facilitar la transición de protocolos anteriores a SNMPv3
- Facilitar actividades de instalación y mantenimiento.

En el desarrollo inicial de SNMPv3 el grupo de trabajo se enfocó en la seguridad y administración, incluyendo:

- Privacidad y autenticación
- Autorización y vista basada en control de acceso
- Estándar basado en configuración remota de los anteriores ítems.

El protocolo SNMP en su tercera versión debe soportar por lo menos un mensaje del modelo de procesamiento, así como puede soportar más de una por ejemplo en un sistema multilingüe el cual ofrece soporte simultáneo de SNMPv3, SNMPv1 y SNMPv2.

Modelo de seguridad basado en Usuario (USM)

En él se definen los elementos de los procedimientos de concesión de SNMP a nivel de mensajes de seguridad.

Se describe dos amenazas primarias y secundarias que pueden ser prevenidas por este modelo, las cuales son Modificación de la información, máscara, modificación de mensajes en trasmisión.

El modelo se basa en MD5 y algoritmos de seguridad para asegurar la integridad de los datos.

- Protección contra los ataques en modificación de datos.
- Proveer autenticación en los datos.
- Defender con ataques de mascara. [10]

RFC 2271 An Architecture for Describing SNMP Management Frameworks

Esta arquitectura fue desarrollada por estos objetivos:

- Usar el material existente basado en proyectos anteriores como SNMPv2
- Atender las necesidades de soporte del comando SET, el cual es considerado como la deficiencia más importante en la versión SNMPv1 y SNMPv2.
- Definir una arquitectura SNMP que perdure
- Mantener SNMP tan simple como sea posible
- Poder realizar una actualización del protocolo sin la necesidad de perder o des configurar todo el entorno SNMP
- Poder realizar soporte en una red grande

Requerimientos de seguridad para esta arquitectura:

Varias amenazas clásicas en los protocolos de red son relevantes con problemas de administración es por esto que será aplicado en un modelo de seguridad usado en la administración de red SNMP. A continuación se muestra las amenazas:

- Modificación de la información

  Esta amenaza se refiere al peligro de que una entidad no autorizada SNMP pueda alterar mensajes SNMP que estén en tránsito, o puedan realizar operaciones de administración no autorizadas, incluyendo falsificación de valores en un objeto.
- Enmascaramiento

  Esta amenaza se refiere al peligro de las operaciones de administración no autorizadas, asumiendo la identidad de una que tenga autorización para realizar esta administración.
- Modificación del Flujo de mensajes

  El protocolo SNMP se basa generalmente en un servicio de transporte sin conexión, que puede operar a través de cualquier servicio de subred, La reordenación, el retraso o repetición de mensajes puede ocurrir y ocurre. Esta amenaza es peligrosa ya que los mensajes pueden ser maliciosamente reordenados, retrasados o redistribuidos lo cual indica que puede modificar el flujo de información de la red.
- Reenvío

  Esta amenaza es peligrosa ya que puede espiar el intercambio de entidades, la protección a estas amenazas puede ser requerida como parte de políticas locales. [11]

RFC2272 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

El distribuidor es una pieza clave de un motor SNMP. Sólo hay una en un motor SNMP, y su trabajo consiste en enviar tareas a los múltiples modelos específicos de la versión de procesamiento de mensajes, así como a expedir PDU a varias aplicaciones.

Para los mensajes salientes, una aplicación que proporciona un PDU que se enviarán, además de los datos necesarios para preparar y enviar el mensaje, y la aplicación especifica qué versión específica del modelo de procesamiento de mensajes se utiliza para preparar el mensaje con el proceso de seguridad deseada. Una vez que el mensaje se prepara, el distribuidor envía el mensaje.

Para los mensajes entrantes, el distribuidor determina la versión de SNMP del mensaje entrante y pasa el mensaje al modelo de mensaje específico de la versión de procesamiento para extraer los componentes del mensaje y para coordinar la tramitación de los servicios de seguridad para el mensaje. Después de la versión específica del procesamiento, el distribuidor PDU determina que la aplicación, en su caso, debe recibir el PDU para el procesamiento y la envía en consecuencia.

Subsistema de procesamiento de mensajes:

El subsistema de procesamiento de mensajes SNMP es parte de un motor SNMP que interactúa con el distribuidor para manejar los mensajes SNMP específicos de la versión. Contiene uno o más modelos de procesamiento de mensajes.

Elementos de la tramitación y expedición de mensajes:

- Modelo de procesamiento de mensajes

  Identifica un modelo de procesamiento de mensajes, Un modelo de procesamiento de mensajes se describen los procedimientos específicos

de la versión para la extracción de datos de mensajes, mensajes de generación, que insta a un modelo de seguridad para solicitar sus servicios de seguridad a los mensajes, para convertir los datos de un formato de mensaje específicas de la versión en un formato utilizable genérico por el distribuidor , y para convertir los datos de formato de Dispatcher en un formato de mensaje específica de la versión.

- Versión de la PDU

  El valor de la versión PDU representa una versión específica de funcionamiento del protocolo y sus asociados, como SNMPv1 o SNMPv2. Los valores de las versiones de la PDU son específicos de la versión del PDU contenida en un mensaje, y los PDU procesados por las aplicaciones. Una aplicación específica de esto es cuando lo solicite el distribuidor PDU para enviar un PDU a otro motor SNMP. El despachador pasa la versión de PDU a un modelo de procesamiento de mensajes, así que sabe cómo manejar adecuadamente la PDU.

- Tipo de PDU

  Un valor de tipo de PDU representa un tipo específico de funcionamiento del protocolo. Los valores de Tipo PDU son específicos para la versión del PDU contenida en un mensaje.

  Para los mensajes entrantes, el tipo de PDU se proporciona al distribuidor por un módulo de mensaje específico de la versión de procesamiento. Se utiliza a continuación para enviar el PDU a la aplicación que ha registrado para el tipo de PDU para el contextEngineID de la scopedPDU asociado.

- Manejo Tipo de PDU

  Este identificador se genera para la coordinación de la tramitación de las solicitudes y respuestas entre el motor SNMP y una aplicación. El manejo debe ser único en todos los modelos de procesamiento de mensajes específicos de la versión, y solamente es de importancia local. [12]

RFC2273 Aplicaciones SNMPv3

Se describen cinco tipos de Aplicaciones:

- Generadores de Comandos

  Aplicaciones que inician SNMP Get, GetNext, Getbulk, Set Request, Así como el procesamiento de la respuesta a una solicitud que se ha generado.

- Respuesta de comandos

  Una aplicación de comando de respuesta recibe SNMP Get, GetNext, GetBulk, y / o conjunto de peticiones destinados para el sistema local como se indica por el hecho de que la contextEngineID en la solicitud recibida es igual a la del motor local a través del cual se recibió la petición. La solicitud de comando de respuesta llevará a cabo la operación de protocolo adecuado, utilizando el control de acceso, y generará un mensaje de respuesta que se enviará al autor de la solicitud.

- Notificación de Origen

  Una notificación originada por una aplicación de un evento o monitoreo de un sistema en particular y generar Trap o informes de mensajes pasados en condiciones de eventos. Esta notificación debe tener un mecanismo el cual determina hacia donde serán enviados los mensajes, así como cual

versión de SNMP y que parámetro de seguridad usar cuando se envía el mensaje.

- Solicitudes de aplicación del receptor
  Una aplicación de receptor está a la escucha de un mensaje de notificación y genera mensajes de respuesta cuando un mensaje que contiene informe PDU es recibido.

- Reenvío de aplicaciones Proxy
  Esta aplicación reencia mensajes SNMP [13]

RFC 2274 modelo de seguridad basado en el usuario

A continuación se muestra la arquitectura del modelo:

- Modelo de seguridad basado en usuarios
  Las operaciones que realizan este modelo de seguridad deben asegurarse que se identifique la entidad en los usuarios. Para cualquier usuario en cuyo nombre las operaciones de gestión estén autorizadas en un motor SNMP particular, la administración debe tener conocimiento de este usuario. Un motor SNM que desee comunicarse con otro motor SNMP debe tener conocimiento del motor del usuario conocido, así mismo los atributos que se pueden aplicar a ese usuario.

  Un usuario y sus atributos se definen de la siguiente forma:

- ✓ Nombre de usuario: Una cadena que representa el nombre del usuario.
- ✓ Nombre de seguridad: Una cadena legible que representa al usuario en un formato que es modelo de seguridad independiente.
- ✓ authProtocol: Una indicación de si los mensajes enviados en nombre de este usuario se puede autenticar y si es así, el tipo de protocolo de autenticación que se utiliza.
- ✓ authKey: Si los mensajes enviados en nombre de este usuario se puede autenticar, de la clave de autenticación para su uso con el protocolo de autenticación. Tenga en cuenta que una clave de autenticación del usuario que normalmente será diferente en los diferentes motores de SNMP autorizados.
- ✓ authKeyChange and authOwnKeyChange: la única forma para actualizar la clave de forma remota. Se realiza en forma segura, así que la actualización se puede realizar sin la necesidad de emplear protección de privacidad.
- ✓ Privprotocol: Una indicación de si los mensajes enviados en nombre de este usuario puede ser protegida de divulgación, y si es así, el tipo de protocolo de privacidad que se utiliza.
- ✓ privKey: Si los mensajes enviados en nombre de este usuario puede estar en / descifrado, la clave de privacidad para su uso con el protocolo de privacidad.
- ✓ privKeyChange and privOwnKeyChange:

  La única manera de actualizar remotamente la clave de cifrado. La actualización se puede realizar sin la necesidad de emplear protección de la privacidad. [14]

RFC 2275 Modelo control de acceso basado en vista (VACM) para el protocolo de administración de red simple (SNMPP)

Elementos que componen el modelo:

- Grupos

  Un grupo es un conjunto de cero o más tuplas <securityModel, securityName> en nombre de la cual los objetos de administración SNMP se puede acceder. Un grupo define los derechos de acceso que ofrece a todos los securityNames que pertenecen a ese grupo. La combinación de una securityModel y unos mapas securityName a lo sumo un grupo.

- Nivel de seguridad

  Derechos de acceso diferentes para los miembros de un grupo se puede definir para diferentes niveles de seguridad, identifica el nivel de seguridad que se supone en la comprobación de los derechos de acceso. El modelo de acceso basado en Vista de Control requiere que el nivel de seguridad se pasa como entrada al módulo de control de acceso cuando se le llama para comprobar si los derechos de acceso.

- Contexto

  Un contexto de SNMP es un conjunto de gestión de la información accesible por una entidad SNMP. Un elemento de información de gestión puede existir en más de un contexto.

  La vista basada en el Modelo de control de acceso define una tabla Contexto VACM que enumera los contextos disponibles a nivel local por el nombre de contexto.

- MIB Views and View Families

  Por razones de seguridad, a menudo es útil poder para restringir los derechos de acceso de algunos grupos a sólo un subconjunto de la

información de gestión en el ámbito de la gestión. Para proporcionar esta capacidad, el acceso a un contexto es a través de un "punto de vista MIB", que detalla un conjunto específico de tipos de objetos administrados (y, opcionalmente, los casos específicos de los tipos de objeto) dentro de ese contexto. Por ejemplo, para un contexto dado, habrá por lo general siempre será un punto de vista MIB, que proporciona acceso a toda la información de gestión en ese contexto, y muchas veces habrá otros puntos de vista MIB cada uno de los cuales contiene un subconjunto de la información:

- ✓ View Subtree Una vista sub árbol es el conjunto de todas las instancias de objetos MIB que tienen un prefijo común de ASN.1 OBJECT IDENTIFIER a sus nombres. Una vista sub árbol se identifica por el valor de identificador de objeto que es el prefijo de objeto más largo identificador común a todas las instancias de objetos (potencial) MIB en ese subárbol.
- ✓ ViewTreeFamily

Una familia de subárboles de vista es una pareja formada por un valor de identificador de objeto (llamado el nombre de la familia), junto con un valor de cadena de bits (llamada la máscara de la familia). La máscara de la familia indica que los sub-identificadores de nombre de la familia son importantes asociados a la definición de la familia.

Para cada instancia de objeto administrado sea posible, esa instancia pertenece a una ViewTreeFamily particular, si las dos condiciones siguientes son verdaderas:

- El nombre de identificador de objeto de la instancia de objeto administrado contiene al menos tantos sub-identificadores al igual que el nombre de la familia,
- cada código de identificación secundario en el nombre del identificador de objeto de la instancia de objeto administrado coincide con el subsistema correspondiente identificador del nombre de la familia cada vez que el bit correspondiente de la máscara de la familia asociada es distinto de cero.

  Cuando el valor configurado de la máscara de familia son todos unos, la familia vista subárbol es idéntica a la única visión subárbol identificado por el nombre de familia. Cuando el valor configurado de la máscara de familia es más corto que la requerida para realizar la prueba anterior, su valor se extiende implícitamente por otras. En consecuencia, una familia vista subárbol que tiene una máscara de familia de longitud cero siempre corresponde a una vista subárbol clave. [15]

4.2 Particularidades de SNMP

Para poder ejecutar el protocolo SNMP se debe tener en cuenta algunas características como la arquitectura de administración de red, esto para poder realizar una buena administración de red, una clave de este componente es realizar una correcta elección de hardware (una plataforma correcta en el cual se ejecutará el sistema de gestión de red) y poder asegurar que las estaciones están

ubicadas de tal forma que se puedan ver los dispositivos de la red de forma correcta.

Realizar la administración de una red extensa requiere un gran consumo de recursos en donde se está haciendo la gestión, en la actualidad las redes pueden llegar a ser tan amplias desde pocos nodos a miles de ellos. El proceso de envío y recibo de traps (alarmas) de cien o miles de entidades administradas debe ser operado por el mejor dispositivo hardware.

Es necesario determinar cuanta memoria RAM va a ser usada para llegar al nivel de rendimiento que se desea, normalmente se toma en cuenta el número de dispositivos que se van a administrar, la cantidad de información que requiere de cada dispositivo, y el intervalo de envíos que desea tener, así mismo el software con el que se va a ejecutar la aplicación.

Se debe tener en cuenta que los dispositivos que se van a administrar sean compatibles con el protocolo SNMP en sus diferentes versiones, permitiendo la ejecución de sus operaciones como lo son: Get, Get-next, Set, Get-response, Trap, Get-bulk, Inform , Notification , Report.

Software de administración de red:

Existen diversos paquetes de software SNMP para la administración, con diferentes plataformas de administración de red, soluciones comerciales como de código abierto que permiten realizar la gestión de la mejor forma posible.

El software de administración se basa en cinco categorías:

- **Agentes SNMP**

  Es el software que controla toda la comunicación SNMP desde cualquier dispositivo compatible con SNMP, en algunos dispositivos como los Routers Cisco, el software está integrado dentro del dispositivo y no necesita realizarse ninguna instalación, pero en otras plataformas se debe realizar la instalación del agente para poder ser ejecutado.

  Antes de seleccionar el tipo de agente que va a ser utilizado se debe verificar que dispositivos se tienen en la red y cuál es el tipo de información que se quiere recibir de ellos. Algunos agentes son básicos y devuelven información limitada, mientras otros pueden devolver información importante. Para iniciar, se debe determinar si se necesita recibir información del servidor (Windows, Unix, etc.) o de los dispositivos de la red (Routers, Switches, etc.).

  Algunos ejemplos de estos tipos de agentes son los siguientes:

  NET-SNMP

  NET-SNMP es un conjunto de aplicaciones usado para implementar el protocolo SNMP usando IPv4 e IPv6. Incluye:

  - ✓ Aplicaciones de línea de comandos para:

    - Tomar información de dispositivos capaces de manejar el protocolo SNMP, ya sea usando peticiones simples (snmpget, snmpgetnext) o múltiples (snmpwalk, snmptable, snmpdelta).

- manipular información sobre la configuración de dispositivos capaces de manejar SNMP (snmpset).
- conseguir un conjunto de informaciones de un dispositivo con SNMP (snmpdf, snmpnetstat, snmpstatus).
- traducir entre OIDs numéricos y textuales de los objetos de la MIB, y mostrar el contenido y estructura de la MIB (snmptranslate).

- Un navegador gráfico de la MIB (tkmib), usando Tk/perl.

- Un demonio para recibir notificaciones SNMP (snmptrapd). Las notificaciones
  Seleccionadas pueden guardarse en un log (como syslog o un archivo de texto plano), ser reenviadas a otro sistema de gestión de SNMP, o ser pasadas a una aplicación externa

✓ Un agente configurable para responder a peticiones SNMP para información de gestión (snmpd). Incluye soporte para un amplio rango de módulos de información de la MIB, y puede ser extendido usando módulos cargados dinámicamente, scripts externos y comandos.

✓ Una biblioteca para el desarrollo de nuevas aplicaciones SNMP, con APIs para C y Perl

SNMPTRAPD

Es la aplicación receptora del agente que permite la recepción de traps, ejecutándose como un servicio más del sistema, el cual se puede detener, ejecutar o reiniciar en la manera que sea necesaria.
Esta aplicación escucha por el puerto 162 de UDP.

Se puede configurar para aceptar notificaciones de entrada, a continuación se puede ver un ejemplo de estas:

traphandle OID|default PROGRAMA [ARGUMENTOS :
Esta directiva configura al demonio snmptrapd para que lance el programa especificado cada vez que llegue una notificación correspondiente a OID, o cualquier notificación cuyo OID no se corresponda con ninguna otra directiva traphandle si incluimos la palabra default en vez de un OID válido. El programa recibirá los detalles de la notificación entrante a través de su entrada estándar, con una entrada por línea y en el siguiente formato:

- ✓ HOSTNAME: El nombre del host que envió la notificación.
- ✓ IPADDRESS: La dirección IP del host que mandó la notificación.
- ✓ VARBINDS: Una lista de variables que describen la notificación y las variables involucradas en ésta.

Jffnms

Es un sistema de gestión y monitorización de red. Permite recolectar información de diferentes tipos de protocolos y servidores.

Por sí mismo JFFNMS no puede recibir traps requiere de un programa externo llamado snmptrapd para recibir y decodificar las trap de la red. En la figura se puede ver como JFFNMS maneja los traps.

Campo	Descripción
ID	El ID interno de la regla, solo es necesario para depuración.
Posición	La posición relativa de la regla en toda la tabla, JFFNMS procesa las reglas desde la posición más baja hasta la más alta.
Descripción	Descripción del tipo de trap y que es lo que hace.
Tipo de interfaz	El tipo de interfaz que debería ser aplicada de acuerdo al trap
OID Match	Las trap que tengan OID serán procesadas por esta regla.
Comando de recepción	Cual script en el directorio serán usados para ser procesados en los campos de eventos.
Parámetros	Los parámetros que irán al Script de recibidos.
Backend	Estado final del proceso de salida del comando en recepción.
Pare si encaja	No se hace mas chequeos si esta trap OID encaja.

Tabla 4: Receptores SNMP Fuente: Los autores

Snmptrapd está configurado para llamar un script sin JFFNMS el cual inserta el trap y sus variables en la base de datos del JFFNMS. Todos ls datos que JFFNMS conozca en este punto es el recurso de la trap, la trap OID y un conjunto de identificadores.

El programa consolida para después procesar las nuevas traps comparando el OID con la tabla de recepción de Traps, si hay alguna igualdad las variables son ubicadas en el comando de recepción y el resultado del comando es que estas pueden pasar a un estado final. Este estado puede hacer lo que desee con la información de Trap, pero algo muy común es usar el evento de estado final para ubicar una nueva fila dentro de la tabla en la base de datos y así este nuevo evento será mostrado en la ventana del operador.

Pandora FMS

Posee una consola de recepción de traps la cual permite visualizar los traps que envían los objetos montorizados y así añadir alertas a dichos traps. Estos traps se reciben por medio del demonio del sistema opetativo que el servidor SNMP de pandora FMS inicia cuando el servidor de pandora es ejecutado.

El programa puede recibir diferentes tipos de traps como: Cold start, Warm start, Link down, Link up, Authentication failure.

Se muestra un ejemplo de lista de recepción de traps que realiza el programa.

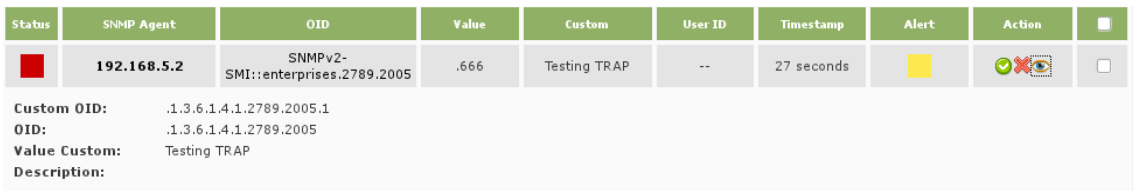

Tabla 5: Recepción traps pandora FMS [8]

Para cada traps aparecen las siguientes columnas:

STATUS: Cuadrado verde si el trap se ha validado y rojo si no se ha validado.

SNMP AGENT: Agente que ha enviado el trap.

OID DEL TRAP ENVIADO: Un trap solo puede enviar un dato en este campo.

VALUE: Campo value del trap enviado. Un trap solo puede enviar un dato en este campo.

CUSTOM OID, CUSTOM VALUE: Campos personalizados enviados en el trap. Pueden ser datos muy complejos, que tengan una lógica específica en función del dispositivo que envía el trap. Un trap puede enviar varios datos en este campo.

TIME STAMP: Tiempo que ha pasado desde que se ha recibido el trap.

ALERTA**:** Cuadrado amarillo si se ha lanzado alguna alerta con este trap o cuadrado gris, si no se ha lanzado ninguna alerta.

ACCIÓN: Campo para borrar o validar el trap.

Además los traps tiene un color (visto como color de fondo de la línea del trap) diferente según el tipo de trap.

Azul: los traps de tipo mantenimiento.
Morado: los traps de tipo información.
Verde: los traps de tipo Normal.
Amarillo: los traps de tipo Warning.
Rojo: los traps de tipo Crítico.

- **Suites NMS**

  Se refiere a un paquete software que reúne múltiples aplicaciones en un solo producto, es una de las piezas más importantes en la gestión de red, sin este el agente software es prácticamente inútil. Este paquete permite tener un control total de los servidores de la red, switches, routers, etc. En la mayoría de los casos se presenta la red de forma gráfica con iconos y etiquetas.

  Estos paquetes se pueden configurar y trabajar en la mayoría de los ambientes de red, algunas de estas suites NMS están enfocadas en la administración de los productos como routers, hubs, switches, y otras permiten la personalización de agentes, servidores y estaciones de trabajo, para así poderlos integrar de forma sencilla con el Software de gestión de red.

- **Administrador de Elementos**

  Estos paquetes de software están orientados hacia un determinado tipo de proveedor, un elemento administrado podría ser un producto que está enfocado en la administración de un switch específicamente. Es necesario

tener en cuenta el ambiente en el cual se está trabajando y el crecimiento que se tiene de la red.

- **Análisis Tendencia del Software**

  Cuando surgen problemas en la de red es bueno tener un histórico de la administración que se ha llevado a cabo en esta, para así poder saber desde cuándo se generan los fallos. Esto permite verificar que es lo que ha sucedido después de que un problema surja y así poder prevenirlo a futuro. Es necesario tener un conjunto de estadísticas para poder verificar las actividades del sistema.

- **Soporte de Software**

  Es un conjunto de características que son usadas en conjunto con el software de administración, algunos de estos paquetes pueden ser usados para crear aplicaciones SNMP. [8]

TRAPS SNMP

Las PDU de tipo Trap permiten a los agentes comunicar de manera asíncrona a los gestores de cualquier evento que haya sucedido al objeto gestionado y en el cual el cual el gestor tiene interés de ser informado.

Incluyen la siguiente información:

- Quien emite la Trap: Los parametros que especifican la dirección del agente y el tipo de sistema que está emitiendo el Trap.
- ¿Qué sucedió?: parámetros que identifican el tipo de evento.
- ¿Cuándo Sucedió?: El tiempo cuando el Trap fue generado por el sistema de emisión, en términos de disponibilidad del sistema, o desde el último reinicio del sistema.
- Información adicional, Transmitidas en un tiempo de variable de unión: estas variables pueden obtener objetos con sus OIDs y valores que pueden ser importantes para el administrador que lo recibe, en conjunto con varios eventos que sucedieron, por ejemplo, una trap que indica que una impresora sea bloqueado esté puede incluir la ubicación de la impresora.

Permite a un agente enviar datos que no han sido solicitados de forma explícita al gestor, para informar de eventos tales como: errores, fallos en la alimentación eléctrica, etc.

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.
- 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

El campo generis-trap indica que evento ha ocurrido, a continuación se puede ver una tabla donde se muestra los diferentes eventos que pueden ocurrir:

EVENTO	SIGNIFICADO
LinkDown	El dispositivo ha detectado un fallo en uno de sus enlaces a la red. El enlace que falla es especificado en el campo variable-bindings.
ColdStart	El dispositivo se ha reiniciado, por lo que la configuración del agente podría cambiar.
WarmStart	El dispositivo se ha reiniciado, pero el agente sigue intacto.
LinkUp	El dispositivo ha detectado que uno se sus enlaces con la red de ha activado. El nombre del enlace y el valor de la variable ifindex aparecenn en el campo variable – bindings.
Authentication Failure	El agente ha detectado un fallo en la autentificación de un mensaje.
EgpNeighborsLoss	Uno de los nodos colaboradores EGP se ha caído. El primer elemento del campo variable – bindings es el nombre y valor de la variable egpNeigAddr del nodo afectado.
EnterpriseSpecific	Evento de un fabricante particular. El evento se identifica con el campo specific-trap.

Tabla 6: Gestión de red Protocolo SNMP Fuente: los autores

Los agentes snmp en dispositivos como routers, switches, impresoras, servidores, etc. pueden enviar alarmas (traps) cuando ocurren ciertos eventos:

- Se “cae” una interfaz
- Se daña el ventilador de un router
- La carga de procesos excede un límite
- Se llena una partición de disco

- Un UPS cambia de estado

Es necesario un mecanismo inteligente para notificar al administrador, Una vez recogidos los Traps, es útil hacer dos cosas:

- Notificar inmediatamente al NOC de ciertos eventos
- Generar reportes diarios (tipo top-ten)

5. Caracterización del protocolo

En la actualidad existen diferentes herramientas comerciales y de código abierto que permiten la administración de red basadas en el protocolo SNMP, a continuación se dará a conocer algunas de ellas con sus características principales.

IBM Tivoli Monitoring

IBM Tivoli Monitoring permite optimizar el rendimiento y la disponibilidad de la infraestructura de TI. Este software proactivo de supervisión del sistema gestiona sistemas operativos, bases de datos y servidores en entornos distribuidos y de host. Al proporcionar las mejores prácticas para identificar y resolver problemas de infraestructura.

El agente SNMP no es una aplicación de gestión; es un programa de interfaz a través del cual la aplicación de gestión SNMP realiza peticiones para recuperar datos y establecer atributos de gestión. En el entorno de Tivoli, su software realiza el papel de la aplicación de gestión SNMP. El agente SNMP se comunica con una aplicación de gestión SNMP utilizando el protocolo UDP. El protocolo UDP también permite al agente SNMP y a la aplicación de gestión SNMP residir en la misma máquina o en máquinas diferentes. El software de Tivoli da soporte a ambas configuraciones.

Sus características son:

- Es posible identificar, arreglar interrupciones y atascos que amenazan aplicaciones clave antes de que afecten el desempeño de la red.

- Supervisa de manera proactiva los recursos del sistema para detectar problemas potenciales y responde automáticamente a eventos. Al identificar los problemas pronto, permite arreglarlos rápidamente antes de que los usuarios noten alguna diferencia en el rendimiento.

- Mejora la disponibilidad y la media de tiempo de recuperación gracias a la visualización rápida de incidentes y la búsqueda histórica de investigación rápida de incidentes. Puede identificar y resolver una interrupción de rendimiento o servicio en minutos en vez de horas.

- Facilita la supervisor del sistema con una interfaz de navegación común, flexible e intuitiva y espacios de trabajo personalizables. Además incluye un almacén de datos fácil de utilizar y funciones avanzadas de creación de informes.

- Recoge datos que puede utilizar para dirigir las actividades de rendimiento y planificación de la capacidad a tiempo y así evitar interrupciones debidas al exceso de uso de recursos. El software supervisa, alerta e informa de futuros atascos en la capacidad.

Solarwinds NPM Orion

Es una plataforma integral basada en Internet destinada a administrar fallos, anchos de banda y el rendimiento, proporciona al usuario una visión global de toda la red, permitiendo que este detecte, diagnostique, y resuelva los problemas de rendimiento y fallos en la red.

Este software permite supervisar el rendimiento de cualquier dispositivo de la red que esté basado en los protocolos SNMPv1, SNMPv2c o SNMPv3.

Sus principales características son:

- Administración de rendimiento y fallos: administra minuciosamente el rendimiento y los fallos, así como herramientas de disponibilidad de la red para garantizar que la red está siempre operativa en los momentos de máximo rendimiento, puede controlar los valores de medición del rendimiento de cualquier dispositivo que emplee el SNMP, como puede ser un enrutador, un conmutador, un cortafuegos o un servidor.

- Interfaz intuitiva: basada en Internet es extremadamente intuitiva y personalizable, permite ver remotamente los fallos de la red, la disponibilidad y la información de rendimiento mediante detallados gráficos, tablas y listas.

- Implementación al alcance de cualquiera: consiste en un proceso de tres pasos. En primer lugar, instalar y configurar el software con la interfaz del asistente. Después, NPM Orion realizará una exploración automática la red. Y, por último, se empieza a realizar el control de la red para detectar posibles fallos o problemas de rendimiento.

- Alertas avanzadas: El software permite configurar de forma sencilla y rápida potentes motores de alertas de red para responder a cientos de situaciones diferentes, como son las comprobaciones múltiples de problemas. Estas alertas de red permiten reconocer y corregir incidencias antes de que los usuarios sufran la degradación del servicio o problemas de disponibilidad.

- Sondeo universal de dispositivos: incluye una base de datos MIB que cubre una amplia variedad de los dispositivos de red más frecuentes. Pero, para esos dispositivos poco comunes que andan perdidos en la red o para los dispositivos más recientes que tienen tablas MIB, puede obtener información de administración valiosa y detallada.

- Control de accesos basado en roles: El software permite crear cuentas únicas y especificar qué tipos de información se muestra en la interfaz de Orion para un departamento, un grupo o un usuario en particular. De este modo, se asegura de que las personas que necesitan visualizar una información concreta tienen acceso a ella y, además, proporciona un mayor nivel de seguridad interna.

Gestión de Redes Castle Rock - SNMPc 7.0 Enterprise Edition

SNMPc es una aplicación desarrollada por CastleRock utiliza una arquitectura de agente de interrogación distribuida para brindar una solución de alto rendimiento con capacidad de monitoreo de redes desde varios cientos de equipos hasta decenas de miles.

Sus principales características son:

- Seguro: Monitorea equipos SNMP, vínculos WAN, Servidores y aplicaciones Gestiona de manera segura dispositivos con Autenticación y Encriptación SNMP v3. Vistas y capacidades administrativas a medida para cada administrador.

- Escalable: Utiliza rastreo distribuido y componentes de tipo servidor en configuraciones optimizadas para grupos de trabajo, grandes Intranets o Proveedores de Servicios.

- Conectado: Esta herramienta permite identificar de forma rápida los problemas existentes a través de correo electrónico, mensajes SMS o notificaciones a Buscapersonas, notificación de eventos por Email/Pager.
- Accesible: Monitoriza y gestiona la red desde localizaciones remotas con el cliente Windows de SNMPc o consolas WEB JAVA.
- Pro-Activo: Monitoriza el rendimiento LAN/WAN y la disponibilidad de servicios con informes WEB planificados que ayudan a realizar mejoras y a reducir el ancho de banda malgastado.
- Integrado: Exporta de manera automática mapas de topología de red, estadísticas de uso y registros de sucesos a bases de datos estándares.
- Multi-fabricante: Permite visualizar y modificar información privada y estándar de routers, hubs, switches o cualquier otro dispositivo de comunicaciones de cualquier fabricante.
- Configurable: Menús y tablas de datos a medida. Desarrolla vistas gráficas de sus dispositivos con la utilidad BitView y una gran variedad de interfaces de programación.

CA Spectrum

Es una infraestructura de administración de red, que permite el modelado de redes físicas, virtuales, Lan, Wan y wireless. Este software permite realizar análisis de impacto de la red, auto descubrimiento de la red, configuración y administración de los dispositivos, así como determinar y representar a la raíz del problema, y el impacto de una falla en la red.

Sus principales características son:

- Servicio de gestión de la infraestructura: Permite la administración, monitoreo de la infraestructura y los servicios de los usuarios que ejecutan esta aplicación, a través de una red virtualizada o ambientes en la nube Mediante la comprensión de las relaciones entre los activos, las configuraciones y los eventos que afectan a un servicio, este software es capaz de identificar la causa raíz de los problemas de servicio para una resolución rápida.

- Aislamiento de fallas y análisis: permite la gestión de fallos, descubre la infraestructura, mapea las relaciones, detecta y correlaciona eventos de suprimir alarmas innecesarias, automatiza la causa raíz y análisis de impacto, y administra las tecnologías de servicios IP.

- Monitoreo de conectividad IP: Está conformado por varias funciones que permiten el seguimiento y administración de servicios IP lógicos que se superponen en la red. [8]

6. Conclusiones y recomendaciones

6.1 Conclusiones

La realización de este trabajo nos ha permitido tener una mejor comprensión acerca del funcionamiento del protocolo SNMP y sus principales características.

Es de vital importancia que en una red computacional se realice una gestión de red apropiada y que satisfaga las necesidades de la misma.

Una gestión de red inadecuada da como resultado una red desorganizada por tal motivo el administrador de la red debe realizar revisiones constantes para evitar este tipo de problemas.

En transcurso del proceso de desarrollo del trabajo se tuvieron en cuenta los conocimientos aprendidos en el aula de clase, con el fin de darle un mejor enfoque al mismo y teniendo en cuenta algunas sugerencia realizadas por los docentes

Bibliografía

[1] Kunes Michael The Industrial Information Technology Handbook. Simple Network Management Protocol SNMP.

[2] Stallings William. Comunicaciones y redes computacionales. Gestión de red-SNMP. Sexta edición Prentice Hall. Pág. 653

[3] MACÍAS RÍOS, María Eugenia “Administración de Redes” [En línea]. [Octubre 21 de 2011]. Disponible en: (http://redyseguridad.fip.unam.mx/pp/maru/labpracticas/Protocolos%20_Administracion%20_Red.pdf)

[4] ROSERO VLASOVA, Olga Alexandra, PROAÑO SARASTI, Diego Alejandro “Estudio y desarrollo de una metodología para la Implementación de un modelo de gestión y Administración de red para la universidad técnica Estatal de quevedo (uteq)”. [En línea]. [Octubre 21 de 2011] Disponible en: (http://dspace.epn.edu.ec/bitstream/15000/8936/5/T%2011276%20CAPITULO%201.pdf)

[5] ARIAS FIGUEROA, Daniel “Herramientas de Gestión basada en Web”. [En línea]. [Diciembre 9 de 2011]. Disponible en: (http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Arias_Figueroa.pdf)

[6] STALLING William, “SSNMPV3: A SECURITY ENHANCEMENT FOR SNMP. [En línea]. [Marzo 10 de 2012]. Disponible en: (http://220.68.70.190/kut/graduate/nm/Stallings.pdf)

[7] BOTERO ARANA, Nicolás “Modelo de gestión de seguridad con soporte a SNMP” [En línea]. [Marzo 10 de 2012]. Disponible en: (http://hermes.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf)

[8] Douglas R. Mauro, Kevin J. Schmidt. Essential SNMP. SNMv3 O'Reilly & Associates, Inc.

[9] Internet standards track protocol for the Internet community, “User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)”. [En línea]. [Marzo 20 de 2012]. Disponible en: (http://tools.ietf.org/html/rfc2274)

[10] D. Partain Ericsson, B. Stewart, “Introduction and Applicability Statements for Internet Standard Management Framework”, En línea Marzo 20 de 2012, Disponible en: (http://www.ietf.org/rfc/rfc3410.txt)

[11] R. Presuhn, B. Wijnen, “An Architecture for Describing SNMP Management Frameworks”, En línea Marzo 20 de 2012, Disponible en: (http://tools.ietf.org/html/rfc2271#section-1.3)

[12] R. Presuhn, B. Wijnen, “Message Processing and Dispatching for the Simple Network Management Protocol SNMP” En línea Marzo 20 de 2012, Disponible en: http://www.ietf.org/rfc/rfc2272.txt

[13] P. Meyer, B. Stewart “SNMPv3 Applications” ” En línea Marzo 20 de 2012, Disponible en: http://www.ietf.org/rfc/rfc2273.txt

[14] B. Wijnen, “User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)” En línea Marzo 20 de 2012, Disponible en: http://tools.ietf.org/html/rfc2274

[15] B. Wijnen, R. Presuhn “View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)”)” En línea Marzo 20 de 2012, Disponible en: http://tools.ietf.org/html/rfc2275