IMPLEMENTACIÓN DE UN MÓDULO MIB PARA AGENTE SNMPv3

Ronald Paucar Curasma

Facultad de Ingeniería Electrónica, Universidad Nacional Mayor de San Marcos

RESUMEN: Se realiza un estudio experimental en la gestión o monitoreo de la información que un host o equipo de red realiza con el protocolo SNMP en su versión 3, el cual se caracteriza por su seguridad, autenticación y control de acceso. Asimismo, se desarrolla un MIB (Base de Información de Gestión) en lenguaje ASN1, que será leída y escrita a través del protocolo SNMPv3 verificándose la autentificación basada en el usuario. Se ilustra algunas configuraciones y resultados obtenidos.

SUMMARY: An experimental study is described about the administration or supervision of the information that a host carries out with the protocol SNMP in its version 3, which is characterized by its security, authentication and access control. Also, a MIB (Base of Information of Administration) is developed in language ASN1 that will be read and written through the protocol SNMPv3, where the authentication based on the user has been verified. It is shown some configurations and obtained results.

Palabras claves: protocolo SNMPv3, MIB.

I. INTRODUCCIÓN

La proliferación de redes de datos a lo largo de las últimas décadas, tanto LANs, WANs y el Internet interaccionando entre ellas hace que los aspectos relativos a su control y gestión llame la atención de los responsables de redes.

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

SNMP (Simple Network Management Protocol) en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP y que ha llegado a convertirse en un estándar. Surge a raíz del interés mostrado por la IAB (Internet Activities Board) en encontrar un protocolo de gestión válido para la red Internet debido a las grandes dimensiones que esta toma.

El protocolo SNMP define un intercambio de información de gestión de redes donde en la forma más básica existe un sistema Gestor y un Agente de Bases de Datos. Sin embargo, a pesar de su simplicidad tiene deficiencias como: problemas para transferir grandes cantidades de información, poca ó ninguna seguridad, y débiles mecanismos de autenticación y privacidad.

Las capacidades de SNMP para el manejo básico de una red son buenas, en 1993 se introduce la versión SNMPv2 la cual fue revisada en 1996. SNMPv2 estaba orientado a corregir las capacidades de transmisión de grandes cantidades de información. Sin embargo, esta versión seguía sin ofrecer solución a la seguridad y privacidad. Específicamente, ni SNMPv1, ni SNMPv2 pueden autenticar la fuente del mensaje de manejo y mucho menos proporcionar encriptación del mismo. En una red de gestión dónde no exista o no sea posible la autenticación, hay probabilidades de que usuarios no autorizados fácilmente puedan ejercer tareas de manejo ó más aún espiar la información que es pasada de un agente a un sistema Gestor. Es por ello que muchas implementaciones en SNMPv1/SNMPv2 son limitadas a capacidades de sólo lectura, lo que como consecuen-

a capacidades de sólo lectura, lo que como consecuencia reduce las utilidades de control y monitoreo de la red.

Para corregir estas importantes deficiencias se formó un grupo de trabajo que propuso los estándares SNMPv3. En estos documentos se definen las especificaciones de seguridad y control de acceso de las redes gestionadas con SNMP, e incluyen las funcionalidades de las versiones SNMPv1 y SNMPv2 respectivamente.

II. FUNDAMENTO DE SNMP

Para el entendimiento del protocolo SNMP, en la figura 1, se muestra los componentes del sistema de gestión de redes, los cuales son:

- Gestores
- Agentes
- MIB (Base de Información de Gestión)

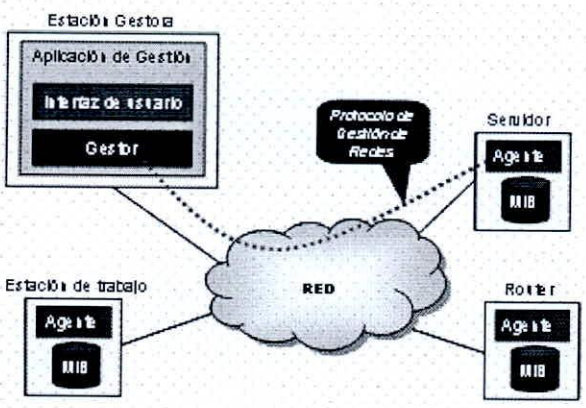

Figura 1. Sistema de Gestión de Redes con SNMP

En cualquier configuración, al menos un nodo Gestor posee un software que soporta SNMP. La estación Gestora generalmente proporciona una interfaz al administrador de la red para controlar y observar los procesos de manejo de la misma, permite al usuario realizar comandos (cómo por ejemplo desactivar un enlace, leer la dirección IP de un nodo y otros) y proporcionar información general del sistema. Como mínimo un sistema Gestor de redes incluirá aplicaciones básicas para desarrollar las funciones de monitoreo, control de configuración y administración de las cuentas de los usuarios. Sistemas más sofisticados podrían incluir aplicaciones más elaboradas para estas categorías y con más posibilidades para la corrección de las fallas.

Por otro lado, los dispositivos de red gestionados, incluyendo servidores, estaciones de trabajo, computadores personales, enrutadores, etc, son equipados con un módulo que incluye un software del Agente. El Agente es responsable de:

- Colectar y mantener información sobre su ambiente local.
- Proporcionar información al manejador de la red, ya sea en respuesta a un requerimiento o como un aviso de que algo anormal esta ocurriendo.
- Responder a los comandos ejecutados por el manejador para cambiar o alterar los parámetros de operación ó configuración local.

Para realizar estas funciones cada agente mantiene un MIB que contiene toda la información (tanto reciente como histórica) sobre su configuración local y el tráfico que maneja. La estación Gestora mantendrá un MIB global con la información resumida de todos los agentes. Es importante resaltar que todas las aplicaciones de gestión de red generalmente comparten un protocolo común en toda la red. Este protocolo proporciona las funciones fundamentales para requerir información y ejecutar comandos hacia los agentes. Este protocolo, en nuestro caso SNMP, hace uso de herramientas de comunicación como TCP/IP.

Específicamente las versiones SNMPv1 y SNMPv2 consisten de un conjunto de documentos que definen un protocolo de gestión de red, una estructura general MIB y un número especifico de datos estructurados de MIB para propósitos de manejo. En esencia, el protocolo proporciona cuatro funciones:

- Get.- usado por un gestor para realizar algún requerimiento a un MIB de un agente.
- Set.- usado por un gestor para cambiar algún valor en un MIB de un agente.
- Trap.- usado por un agente para enviar un mensaje de alerta al gestor.
- Inform.- usado por el gestor para enviar un mensaje de alerta a otro gestor.

III. SNMPv3

Para corregir las deficiencias de seguridad que presentan las versiones SNMPv1 y SNMPv2, fueron escritos una serie de recomendaciones orientadas a definir una arquitectura y nuevas capacidades en cuanto a seguridad.[2]

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

- Integridad del mensaje.- asegura que el paquete no haya sido violado durante la transmisión.
- Autenticación.- determina que el mensaje proviene de una fuente válida.
- Encriptación.- encripta el contenido de un paquete como forma de prevención.

3.1 Arquitectura utilizada

SNMPv3 proporciona tanto modelos como niveles de seguridad.[3] Un modelo de seguridad es una estrategia de autenticación que es configurada para los usuarios y los grupos en los cuales estos residen. Los niveles de seguridad se refieren al nivel permitido a un usuario dentro de un modelo de seguridad. La combinación de ambas determina que mecanismo de seguridad será el empleado cuando se maneje un paquete SNMP. SNMPv3 incluye tres servicios:

- Autenticación.
- Privacidad.
- Control de Acceso.

Para dar estos servicios de una forma eficiente, SNMPv3 introduce un nuevo concepto llamado Principal, el cual no es más que una entidad en la cual la mayor parte de los servicios son proporcionados ó procesados. Un Principal puede actuar en forma individual en un rol particular, como aplicación o conjunto de aplicaciones ó bien como una combinación de todos ellos. Esencialmente un Principal opera desde una estación gestora y envía comandos SNMP hacia los Agentes. La identidad del Principal y la del Agente juntos determinan las capacidades de seguridad que serán invocadas, incluyendo autenticación, privacidad y control de acceso.

Es posible definir SNMPv3 en una forma modular. Así, cada entidad SNMP incluye un simple SNMP Engine que implementa funciones para enviar/recibir, autenticar y encriptar/desencriptar mensajes y controlar el acceso a los objetos manejados. Las funciones son proporcionadas como servicios para una ó más aplicaciones que son configuradas con el SNMP Engine para así formar la SNMP Entity, como se ilustra en la siguiente figura 2.

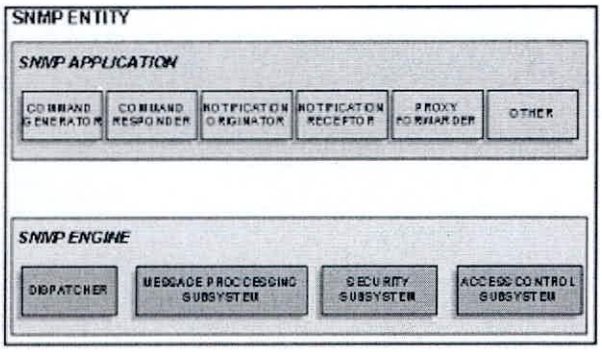

Figura 2. Arquitectura de Gestor SNMPv3

La arquitectura modular con la que se presenta proporciona algunas ventajas que se lista a continuación:

- El papel del SNMP Entity es determinado por módulos que están implementados en esa entidad.
- La estructura modular de las especificaciones permiten definir diferentes versiones de cada módulo, lo que hace posible que se puedan tomar ciertas capacidades y aspectos de SNMP sin la necesidad de ir a una nueva versión y tomar el estándar completo, de este modo se mantiene la coexistencia de varias versiones.

3.2 Elementos de una SNMP Entity

3.2.1 SNMP Engine

Despatcher.- Permite la concurrencia de múltiples versiones de mensajes SNMP en el SNMP Engine. Es responsable de:

- Aceptar los PDUs (Protocolos de Unidades de Datos) de las aplicaciones para transmitirlos a través de la red y de enviar los PDUs entrantes a las aplicaciones.
- Pasar los PDUs que salen al subsistema de procesamiento de mensajes para que sean preparados y pasar los PDUs entrantes al mismo subsistema para que sean extraídos.
- Enviar y recibir mensajes SNMP sobre la Red.

Message Proccessing Subsystem.- Responsable de preparar mensajes para enviar y extraer los datos de la información recibida.

Security Subsystem.- Proporciona los servicios de autenticación y privacidad del mensaje. Este subsistema potencialmente contiene múltiples modelos de seguridad.

Access Control Subsystem.- Proporciona un conjunto de servicios de autorización que una aplicación puede utilizar para el chequeo de acceso de los mensajes.

3.2.2 SNMP Aplication

Command Generador.- Son iniciados los PDUs SNMP Get, GetNext, GetBulk ó Set Request y procesa la respuesta a una requisición que ha sido generada.

Command Responder.- Recibe los PDUs SNMP Get, GetNext, GetBulk ó SetRequest destinados al sistema local y luego desarrolla la operación de los protocolos apropiados, usando control de acceso y genera un mensaje de respuesta para ser enviada a la estación que genero el requerimiento.

Notification Originator.- Monitorea un sistema para una condición o evento particular y genera un mensaje de Trap ó Inform basados en ellos. Un originador de Notificación debe tener un mecanismo para determinar donde enviar el mensaje y cual es la versión de SNMP y los parámetros de seguridad utilizados cuando se envíe el mensaje.

Notification Receptor.- Espera por los mensajes de notificación y genera respuestas cuando un mensaje recibido contenga un PDU tipo Inform.

Proxy Forwader.- Adelanta los mensajes SNMP, es una aplicación opcional.

3.3 Procesamiento del mensaje

Se define en forma general el modelo para el procesamiento del mensaje en SNMPv3.[4] Este modelo es responsable de aceptar los PDUs del Despachador, encapsularlo en mensajes, e invocar el USM (Modelo de Seguridad del Usuario) para insertar los parámetros relacionados con la seguridad en el encabezado del mensaje.[5] El modelo de procesamiento del mensaje también se encarga de aceptar mensajes entrantes, invocar el USM para procesar los parámetros de seguridad que se encuentran en el encabezado del mensaje y entrega el PDU al despachador. La estructura del mensaje se ilustra en la Figura 4. Los primeros cinco campos son generados por el modelo de procesamientos de mensajes entrantes/salientes. Los siguientes seis muestran los parámetros de seguridad usados por el USM. Finalmente, el PDU junto con el ContextEngineID y ContextName constituyen el PDU que será procesado. A continuación se presentan los primeros cinco campos.

msgVersion.- Configurado para SNMPv3.

mugid.- Un identificador único usado entre dos entidades SNMP para coordinar los mensajes de requisición y respuesta. Su rango es de 0 a 231 – 1.

msgMaxSize.- Se refiere al tamaño máximo de un mensaje en octetos soportado por el que envía, con un rango de 484 a 231 – 1. Este es el máximo tamaño que una entidad que envía puede aceptar de otra SNMP Engine.
msgFlag.- Un arreglo de octetos que contiene tres banderas en los tres bits menos significativos:

- ReportableFlag.-Utilizada igual a 1 para los mensajes enviados conteniendo una requisición o un Inform, e igual a 0 para mensajes conteniendo una Respuesta, Trap ó Reporte PDU.
- PriorFlag y AuthFlag.-Son configuradas por el que envía para indicar el nivel de seguridad que le fue aplicado al mensaje.
- msgSecurityModel.- Es un identificador en el rango de 231 – 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 seis campos siguientes relacionados con los parámetros de seguridad y generados por la USM se presentan a continación.

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

msgAuthoritativeEngineTime.- Es un valor entero en el rango de 231 – 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.

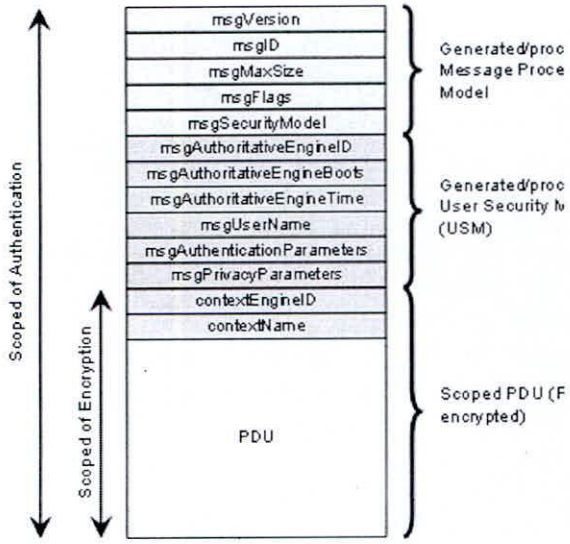

Figura 3. Estructura de mensaje SNMP

3.4 La clave de autenticación

El mecanismo de autenticación en SNMPv3 asegura que un mensaje recibido ha sido realmente transmitido por la entidad principal fuente que aparece en el identificador del encabezado del mensaje. Además, este mecanismo asegura que el mensaje no haya sido alterado durante la transmisión y de algún modo retardado o capturado y luego reenviado por otra fuente.

En el proceso de autenticación cada Engine de SNMP, Principal y remota que desee comunicarse deberá compartir una llave secreta de autenticación. La entidad que envía proporciona la autenticación incluyendo en el mensaje un código. Este código es una función del contenido del mensaje, de la identidad del Engine SNMP y del Principal, del tiempo de transmisión y de la llave secreta que sólo deberá de ser conocida por el que envía y el que recibe. La llave secreta debe ser configurada inicialmente por el administrador o manejador de la red, quien cargará estas llaves en las bases de datos de los agentes y los manejadores. Esto puede hacerse manualmente ó utilizando una forma segura de transferencia de datos.

Cuando la entidad receptora recibe el mensaje, ésta utiliza la misma llave secreta para calcular el código de autenticación del mensaje. Si el código calculado en el lado receptor coincide con el valor incluido en el mensaje enviado, entonces el receptor conocerá que el mensaje fue originado de un manejador autorizado y que el mismo no fue alterado durante su transmisión.

3.5 View-Based Access Control Model (VACM)

El Modelo de Control de Acceso (View-Based Access Control Model) hace posible configurar los agentes para proporcionar diferentes niveles de accesos a los MIB y a los diferentes Gestores. Un Agente puede restringir el acceso a sus MIBs a un Gestor en particular de dos formas: [6]

- Puede restringir acceso sólo a ciertas porciones del MIB.
- Puede limitar la operación de un Gestor en ciertas porciones del MIB.

El control de acceso a ser usado por un Agente para cada Gestor deberá ser preconfigurado. Esencialmente, consiste de una tabla que detalla los privilegios de accesos de varios Gestores autorizados. A diferencia de la autenticación la cual es hecha por el usuario, el control de acceso es hecho por grupo, dónde un grupo puede estar compuesto por una serie de usuarios. En la Figura 4, se ilustra la lógica de funcionamiento.

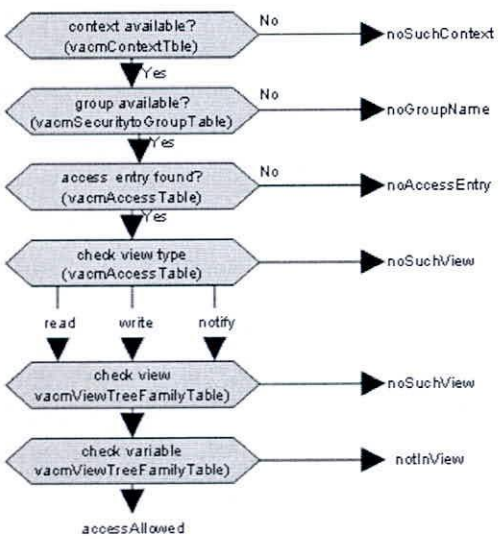

Figura 4. Lógica de funcionamiento de control de acceso

IV. IMPLEMENTACIÓN DEL MÓDULO MIB PARA SNMPV3

4.1 Configuración de usuario SNMPv3

Se detalla las configuraciones realizadas en el lado del Agente. Se crea el usuario quien va acceder a la información del agente remoto, ya que SNMPv3 utiliza una seguridad basada en usuario (USM) mediante los algoritmos MD5 y DES para la autentificación y encriptación respectivamente. Además, se puede observar que el usuario tiene el acceso de lectura y escritura para el Agente. A continuación se ilustra los comandos utilizados.

```
[root@ronald root]# net-snmp-config --create-snmpv3-user -a maestriatele ronald
Enter authentication pass-phrase:
maestriatele
Enter encryption pass-phrase:
[press return to reuse the authentication pass-phrase]
maestriatele
adding the following line to /var/net-snmp/snmpd.conf:
createUser ronald MD5 "maestriatele" DES maestriatele
adding the following line to
/usr/local/share/snmp/snmpd.conf:
rwuser ronald
```

4.2 Desarrollo de un MIB

El MIB desarrollado se realizó siguiendo la estructura del estándar SMI [RFC 1155] en uno de los nodos privados (Private) dentro del nodo intermedio (Internet). En la Figura 5, se ilustra la estructura de nodos que representa el MIB creado con sus respectivos objetos de tipo entero:[7]

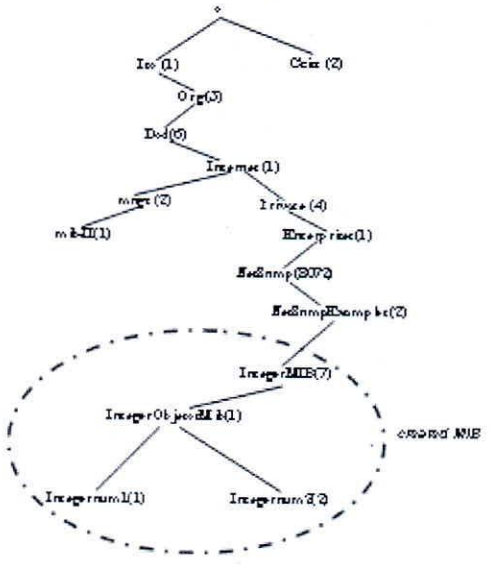

Fig. 5. Estructura del árbol MIB

El código escrito en el lenguaje ASN.1, contiene la estructura de árbol de la definición del MIB. Los nodos finales indican los objetos de tipo entero que serán leídos o escritos. Estos serán accesados por el usuario o usuarios configurados en el Agente que soporta el protocolo SNMPv3. El código escrito en el lenguaje ASN.1 se ilustra a continuación.

```
INIEGER-MIB DEFINITIONS ::= BEGIN
IMPORTS
netSnmpExamples
FROM NET-SNMP-EXAMPLES-MIB, MODULE-
IDENTITY FROM SNMPv2-SMI
MODULE-COMPLIANCE, OBJECT-GROUP
FROM SNMPv2-CONF;
integerMIB MODULE-IDENTITY
LAST-UPDATED "200311260000Z" -- 26 noviembre
2003, medianoche
ORGANIZATION "RONALD"
CONTACT-INFO "Ronald Paucar Curasma"
DESCRIPTION  "Un mib entero  para trabajo de ges-
tion en Linux" ::= { netSnmpExamples 7 }
integerObjetosMib
OBJECT IDENTIFIER ::= { integerMIB 1 } integer-
num1  OBJECT-TYPE
SYNTAX  Integer32
MAX-ACCESS  read-write
STATUS current
DESCRIPTION
"Este es un primer objeto que soporta un entero actuali-
zable cuando es compilado en el agente."
DEFVAL { 1 }
::= { integerObjetosMib 1 }
integernum2  OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS  read-write
STATUS     current
DESCRIPTION  "Este es un segundo objeto entero que
soporta un entero actualizable cuando es compilado en
el agente."
DEFVAL { 1 }
::= { integerObjetosMib 2 }
END
```

4.3 Envió de comandos SNMPv3

Los comandos son enviados por un Gestor indicando el nombre de usuario y la clave. Estos serán transmitidos encriptados usando el algoritmo DES y autentificados en el Agente mediante el algoritmo MD5. El envió de comandos para la medición del objeto MIB se muestra a continuación.

```
smUser 1 3 0x800007e5809c6e6a62a222673f
0x6e616c726f00 0x6e616c726f00 NULL
.1.3.6.1.6.3.10.1.1.2
0x9bcc88c563b9156d16348b8ade32c6f8
.1.3.6.1.6.3.10.1.2.2
0x9bcc88c563b9156d16348b8ade32c6f8 ""
[root@ronald root]# snmpget -v 3 -u ronald -l authNo-
Priv -a MD5 -A maestriatele localhost sysContact.0
SNMPv2-MIB::sysContact.0 = STRING:
RONALD PAUCAR
```

También se envía la transmisión encriptada de la siguiente manera:

```
[root@ronald root]# snmpget -v 3 -u ronald -l authNo-
Priv -a MD5 -A maestriatele -x DES -X maestriatele
localhost
sysContact.0SNMPv2-MIB::sysContact.0 = STRING:
RONALD_PAUCAR
```

V. CONCLUSIONES

En la actualidad como muchos otros protocolos utilizados en Internet, SNMP se encontró con el problema de seguridad y privacidad. Por ello el SNMPv3 tiene la capacidad de autenticación, privacidad y control de acceso a la información. Dando gran confianza a los usuarios del mercado. A diferencia de las versiones anteriores se caracteriza por el nivel de seguridad que presenta basado en usuario. Es por ello que se tiene la necesidad de crear un usuario con su respectiva clave.

La experiencia se realizó en software de libre distribución como Linux, usando paquete SNMP el cual contiene herramientas de gestión, archivos de configuración, entre otros, siendo fundamental en el desarrollo del modulo MIB.

REFERENCIAS

1. D. Harrington, R. Presuhn (1998). An Architecture for Describing SNMP Management Frameworks". IETF RFC 2271.
2. W. Stallings (2001). Security Comes to SNMP The New SNMPv3 Proposed Internet Standards.
3. J. Case, D. Harrington (1998). Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). IETF RFC 2272.
4. D. Levi, P. Meyer (1998). SNMPv3 Applications. IETF RFC 2273.
5. Blumenthal U., B. Wijnen (1998). User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). IETF RFC 2274.
6. Wijnen B., R. Presuhn (1998). View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). IETF RFC 2275.
7. http://net-snmp.sourceforge.net/