ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"SIMULACIÓN DE LAS PRIMITIVAS SNMPV2 EN UN ENTORNO DE UNA RED LAN"

TESINA DE SEMINARIO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

Ángel Xavier Ibarra Barahona

Germán Temístocles Ramos León

Guayaquil – Ecuador

2014

AGRADECIMIENTO

Primero que todo agradezco a Dios por haberme permitido culminar con éxito y tener cada día salud y prosperidad, a mis padres y hermanos por ser un constante apoyo durante todo este tiempo, a mi profesor de tesis el Magíster Washington Medina quien nos brindó su guía y consejo durante el transcurso del proyecto.

Ángel Xavier Ibarra Barahona

DEDICATORIA

Dedico este proyecto a Dios ante todo, a mis padres por apoyarme siempre en mis emprendimientos y metas, a mi novia Marcella, a mis tíos y abuelos quienes me enseñaron mucho y a quienes les dedico este logro.

Ángel Xavier Ibarra Barahona

AGRADECIMIENTO

Comienzo agradeciendo a Dios por guiarnos y cuidarnos en el largo camino de nuestras carrera y poderla culminar, a nuestros padres y hermanos por ser un apoyo incondicional durante todo este tiempo y a nuestro profesor de tesis el Magíster Washington Medina quien nos guio y aconsejo durante el transcurso del proyecto y de nuestra carrera profesional, al Ing. Luis Fernando Vásquez le agradezco por todo el apoyo brindado a lo largo de la carrera, por su tiempo, amistad y por los conocimientos transmitido.

Germán Temistocles Ramos León

DEDICATORIA

Gracias a Dios y a esas personas importantes en mi vida, que estuvieron listas para brindarme toda su ayuda, ahora me toca regresar un poco de todo lo inmenso que me han otorgado. Con todo mi amor esta tesis se la dedico a ustedes: Papá Temistocles, Mamá Mirian y hermanos.

Germán Temistocles Ramos León

TRIBUNAL DE SUSTENTACIÓN

Magíster Washington Medina

PROFESOR DEL SEMINARIO DE GRADUACIÓN

PhD. Boris Ramos

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesina nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL".

(Reglamento de exámenes y títulos profesionales de la ESPOL).

Ángel Xavier Ibarra Barahona

Germán Temistocles Ramos León

RESUMEN

Actualmente existen diferentes tipos de protocolo de red que permiten al usuario realizar distintas tareas entre dos dispositivos dentro de un mismo sistema de comunicación, uno de ellos son los protocolos de gestión utilizados para realizar la Gestión de la Red, algunos de estos sistemas de comunicación se los conoce como modelos de redes locales o remotas.

A nuestro alcance disponemos de distintas formas de lograr simular una red, incluso algunas nos permiten tener una red lo más semejante a las redes físicas existentes. De los escenarios planteados se simularan las primitivas SNMPv2 en una red LAN virtualizada mediante el software VIRTUALBOX, de los resultados obtenidos analizaremos el comportamiento de las primitivas SNMPv2.

ÍNDICE GENERAL

ABREVIATURAS

AIX	Advanced Interactive Executive
CMIP	Common Management Information Protocol
CMIS	Content Management Interoperability Services
CPU	Central Processing Unit
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
Gbps	Gigabits por segundo
GNS3	Graphical Network Simulator 3
GPL	General Public License
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IOS	Internetwork Operating System
ISO	International Organization for Standardization

LAN	Local Area Network
MAC	Media Access Control
Mbps	Megabits por segundo
MIB	Management Information Base
MPM	Modelo de Procesamiento de Mensajes
NIC	Network Interface Card
NMS	Network Management System
OID	Object Identifiers
OSI	Open System Interconnection
PC	Personal Computer
PDU	Protocol Data Unit
RAM	Random Access Memory
RDSI	Red Digital de Servicios Integrados
RFC	Requests for Comments
RPM	RedHat Package Manager
SNMP	Simple Network Management Protocol

SNMPV1	Simple Network Management Protocol version 1
SNMPV2	Simple Network Management Protocol version 2
SNMPV3	Simple Network Management Protocol version 3
SQL	Structure Query Language
TCP	Transmission Control Protocol
TI	Tecnologías de la Información
UDP	User Datagram Protocol
USM	User-based Security Model
VACM	View-based Access Control Model
VDI	Virtual Desktop Infrastructure

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el mundo de las telecomunicaciones, está en demanda disponer de redes con mayor control y administración de los dispositivos que las integran, lo cual solucionaremos realizando Gestión sobre la Red.

Con nuestro proyecto mostraremos como utilizar la simulación de las primitivas SNMPv2 en un entorno de red LAN, obteniendo resultados parecidos a los proporcionados por una red LAN con dispositivos físicos. Para lograrlo trataremos de cumplir con los siguientes objetivos:

- Describir las funciones de las primitivas de SNMPv2 para lograr una buena Gestión de redes LAN.
- Identificar el ambiente y los escenarios a utilizar para la simulación de las primitivas SNMPv2.
- Desarrollar la gestión de las primitivas SNMPv2 en la simulación de los escenarios propuestos.

Las primitivas realizaran gestión sobre los servidores ejes en cada escenario, para lo cual disponemos de MIBS propietarias y genéricas. De los objetos disponibles con las MIBS, se realizara la simulación de las primitivas GET, SET y TRAP sobre un objeto que represente a un recurso importante para el servidor.

CAPITULO 1

INTRODUCCION A LA GESTION DE REDES

La simulación de las primitivas snmpv2 en red trata sobre planificación, organización, supervisión y control de elementos de comunicación para garantizar un adecuado nivel de servicio, de acuerdo a un determinado costo. La función principal de la gestión de red consiste en mejorar la disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad.

En el nuevo mundo tecnológico existe mucha complejidad en administración de redes conformadas de routers, switches y servidores, que pueden parecer una tarea difícil de gestionar todos los dispositivos de la red y asegurarse de que estén en un funcionamiento correcto y también en un rendimiento óptimo.

Tradicionalmente, en la gestión de las redes se ha partido de soluciones propietarias y cerradas con un ámbito de actuación limitado a la propia empresa o dominio de la institución. Con el tiempo la evolución tecnológica ha permitido la entrada de múltiples fabricantes de equipos, de la misma forma que otros fabricantes de respetados nombres han desaparecido y en consecuencia, también el apoyo que prestaban a sus soluciones de red. Por lo tanto, bien sea porque ha ocurrido la absorción de empresas o bien por diversificación de las fuentes de los equipos, las redes actuales son cada vez más heterogéneas en equipos.

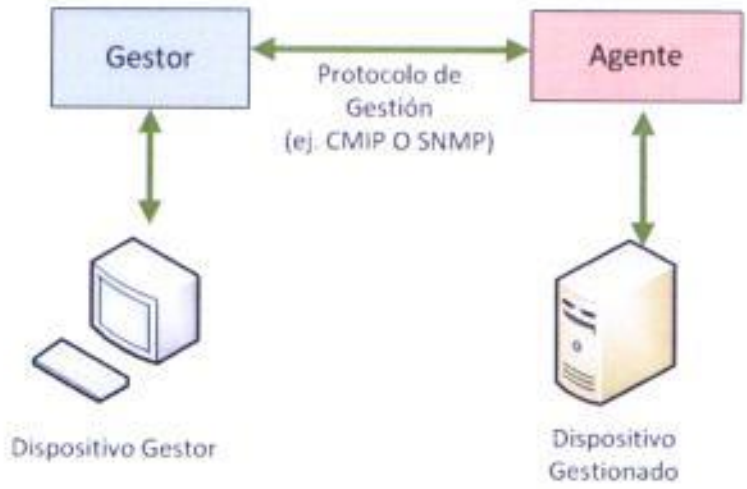


Figura 1.1 Paradigma Gestor - Agente

GESTIÓN DE FALLAS

La gestión de fallas se ocupa del conjunto de facilidades que permiten la detección, aislamiento y corrección de una operación anormal.

El determinar el máximo de información sobre las fallas es el elemento fundamental para su buena gestión. La información de fallas debe permitir detectarlas y aislarlas. Las fallas se detectan normalmente ante cambios de estado en los dispositivos.

Existen una serie de problemas relacionados con la detección de fallas. Por ejemplo, fallas no observables que sólo permiten detectar efectos laterales, o bien el caso de fallas inciertas, en los que la información sobre la falla puede no ser fiable en cuanto a su fuente.

GESTIÓN DE CONFIGURACIÓN

La gestión de configuración es un conjunto de facilidades que permiten controlar, identificar, recoger y proporcionar datos a objetos gestionados con el propósito de asistir a operar servicios de interconexión.

Entre las tareas relacionadas se puede destacar la definición de información de configuración en los recursos, la modificación de las propiedades de los recursos, la definición y modificación de relaciones entre los recursos, la inicialización y terminación de servicios de red o bien la distribución de software.[1]

GESTIÓN DE CONTABILIDAD

La gestión de tarificación son un conjunto de facilidades que nos permiten poder determinar el costo del uso de uno o varios componentes y establecer la cuenta a facturar al cliente. Se puede hablar de criterios sobre tarificación, entre ellos se pueden destacar: localización geográfica, distancia desde nodo central, zonas temporales (día/semana), descuentos por volumen, precio por paquete, códigos de área, rango de extensión por voz, email, identificación de equipos orientados a datos, etc.[1]

GESTIÓN DE DESEMPEÑO

Se compone de varios indicadores con lo que podremos medir y garantizar el rendimiento de la red gestionada. Entre los indicadores de prestaciones se pueden definir los orientados al servicio (disponibilidad, fiabilidad, tiempo de respuesta), orientados a la eficiencia (utilización, throughput).

GESTIÓN DE SEGURIDAD

La gestión de seguridad está relacionada con la generación, distribución y almacenamiento de claves de cifrado, información de contraseñas o bien

información de control de acceso y autorización que debe mantenerse y distribuirse.

Es decir, proporciona facilidades para incorporar mecanismos de seguridad contra los ataques a las comunicaciones, como protección contra interrupción del servicio, captura no autorizada de información, modificación de información o suplantación de entidad. [1]

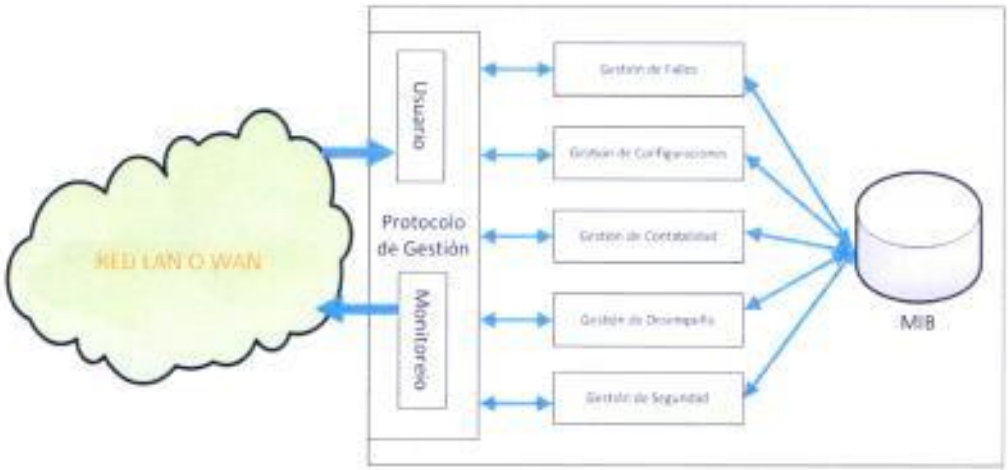


Figura 2.2 Modelo de Gestión de Red

MODELO GESTOR-AGENTE

La gestión de una red es una aplicación de procesamiento de información, en la cual intervienen elementos fundamentales como son:

- el agente,
- el gestor,
- el protocolo con que se gestiona, y

- la base de información gestionada (MIB, Management Information Base).

Figura 3.3 Protocolo de Gestión [2]

1.1. GESTOR

Es la estación de gestión que emite las operaciones de gestión, recibiendo notificaciones y respuestas. En la estación de gestión se debe disponer de la MIB relacionada al dispositivo bajo gestión y la interfaz del usuario.

Figura 4.4 Gestor

1.2. AGENTE

Tiene la función de responder a las directivas enviadas por el gestor y lo realiza accesando a la MIB para manipular los objetos involucrados en la operación. El agente se encuentra ubicado en el dispositivo de telecomunicaciones gestionado.[2]

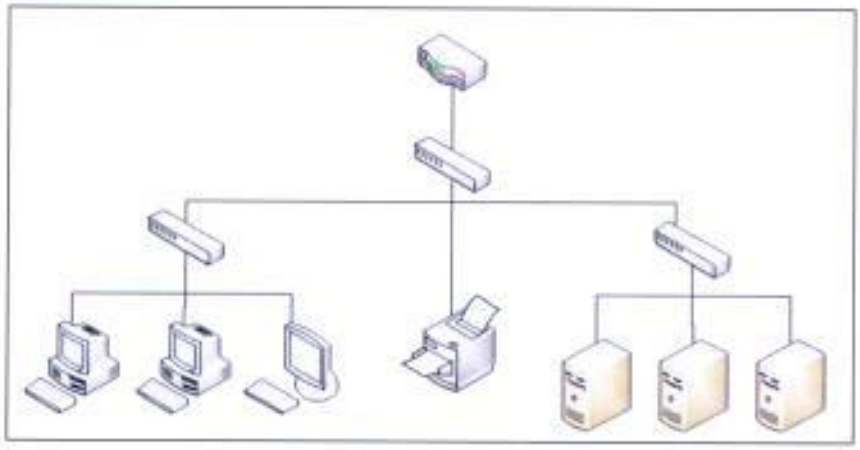


Figura 5.5 Agentes

1.3. MIB

Es un conjunto de objetos que contienen información de los recursos del dispositivo y de la red ordenada en forma jerárquica, teniendo su estructura como forma de árbol ypermitiendo algún tipo de gestión sobre cada uno de sus ramas o nodos. La MIB deberá estar ubicada en el dispositivoy en el gestor.

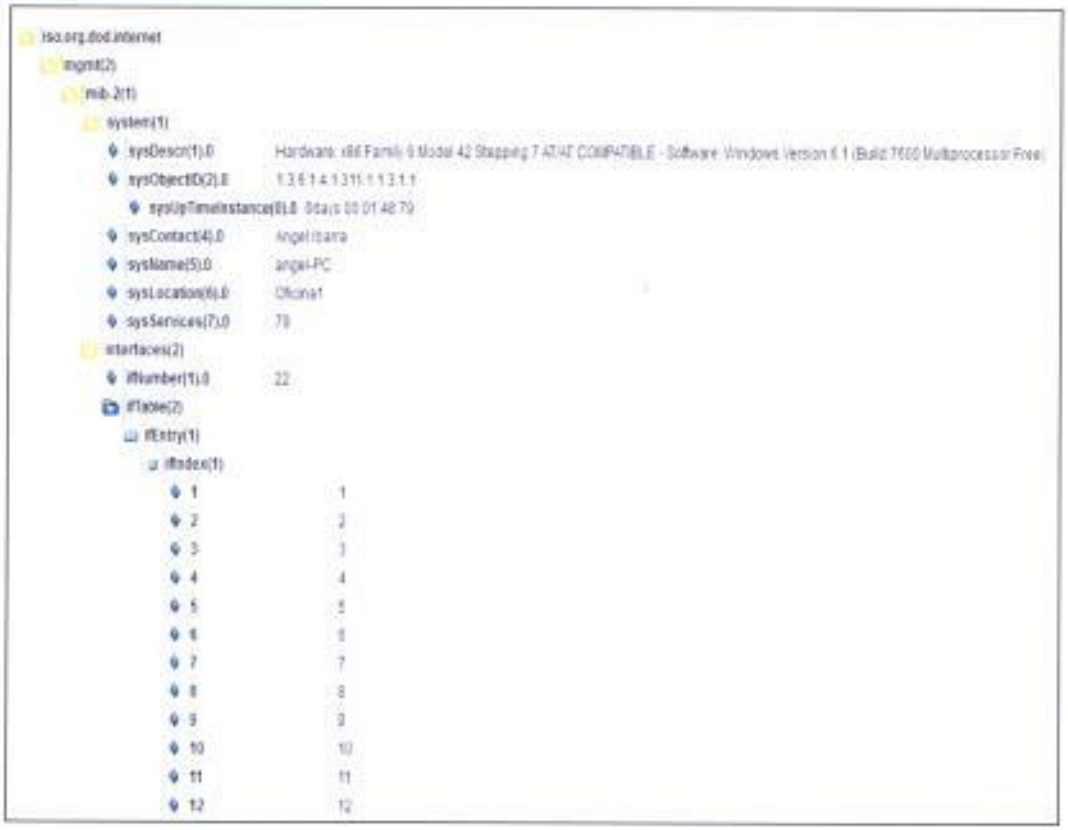


Figura 6.6 MIB Y OID

1.3.1. OBJETO

Los objetos pueden ser recursos de tipo físico, aplicación, internet, acceso a la red e incluso pueden ser implementados acorde a las necesidades de gestión. Como los objetos se forman en grupos, disponemos de una estructura de niveles o árbol.

El árbol está formado por ramas y nodos. En cada nodo existe una etiqueta consistente en un número entero y quizás un

texto breve. Cada nodo puede tener nodos hijos conectados a éste mediante líneas o ramas. El árbol comienza con un nodo inicial denominado root que se puede extender hasta cualquier nivel de profundidad. Este método usa los identificadores de objetos (OID, Object Identifiers).

Los OID se representan en una secuencia de enteros no negativos separados por un punto formando un árbol. Este árbol denominado de registro está estandarizado a nivel mundial por el estándar RFC3061 por la IETF, Por ejemplo, el OID: 1.3.6.1.1 identifica el objeto que se encontraría si, comenzando en el root, pasamos a la rama 3, después a la 6, a la 1 y finalmente a la rama 1.

1.4. PROTOCOLO DE GESTIÓN

Es el conjunto de especificaciones que facilitan el intercambio de información de gestión entre dispositivos de una red. En la actualidad los protocolos predominantes son SNMP (Simple Network Management Protocol), forma parte del modelo de red TCP/IP, y CMIP (Common Management Information Protocol), forma parte del modelo de red OSI.

1.5. CMIP Y SNMP

CMIP

El CMIP se define en el estándar 9596 de ISO. Este protocolo ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta para capas OSI. La especificación del protocolo describe precisamente cómo se ejecutan los servicios CMIS (Content Management Interoperability Services) individuales.

Las características más importantes del protocolo CMIP se pueden destacar las siguientes:

- CMIS/CMIP utiliza grandes cantidades de memoria y de CPU.
- La comunicación con los agentes es a través de TCP.
- Su estructura de funcionamiento es distribuida.
- El agente es responsable de monitorear sus recursos.
- Existe menor gestión del tráfico.
- La interacción con agentes es más compleja.

SNMP

Aquí es donde SNMP nos puede ayudar, debido que SNMP se maneja en el modelo TCP/IP bajo el cual trabajan todos los dispositivos que utilizamos en una red.

SNMP se introdujo en 1988 para satisfacer la creciente necesidad de un estándar para el manejo del protocolo de internet (IP, Internet Protocol) de los dispositivos.

SNMP proporciona a sus usuarios un conjunto de operaciones simples para la administración remota a dispositivos.

SNMP se comunica por medio de UDP (User Datagram Protocol) como protocolo de transporte para pasar datos entre gestores y agentes. UDP, definido en el estándar RFC 768, fue elegido sobre TCP (Transmission Control Protocol) por ser orientado a la no conexión; es decir, sigue una misma ruta de extremo a extremo, la transmisión se realiza entre el agente y el NMS (Network Management System) enviando paquetes o datagramas en ambos sentidos. Este aspecto de UDP le hace que sea poco fiable ya que no hay reconocimiento de los datagramas perdidos.Depende de la aplicación SNMP para determinar si los datagramas se pierden y las retransmiten si así lo desea.

Por lo menos en cuanto a las solicitudes de información regulares se refiere, el carácter poco fiable de UDP no es un problema real. En el peor de los casos, la estación de gestión emite una solicitud y nunca recibe una respuesta. Para las TRAPS, la situación es algo diferente. Si un agente envía una TRAP y esta nunca llega, el NMS no tiene manera de saber que fue enviado nunca.

El agente ni siquiera sabe que tiene que volver a enviar la TRAP ya que el NMS no tiene la obligación de enviar una respuesta al agente que acusa recibo de la trampa.

SNMP utiliza el puerto 161 para el envío y recepción de solicitudes y el puerto 162 para la transmisión de las notificaciones de incidencias.

Cada dispositivo que implementa SNMP debe utilizar estos números de puertos como los valores por defecto, pero algunos fabricantes permiten cambiar el valor por defecto de los puertos en la configuración del agente. Si se cambian estos valores predeterminados toda la red debe conocerlos.

Figura 7.7 SNMP [3]

1.5.1. SNMPV1

Cuando se utiliza SNMPV1, el agente SNMP utiliza un esquema de autenticación simple que consiste en tener habilitado el protocolo SNMP y con esto podrá la estación del administrador tener acceso a su base de información de administración (MIB).

Las primitivas del SNMPv1 son:

- GET REQUEST
- GET NEXT REQUEST

- SET REQUEST
- GET RESPONSE
- TRAP

GET REQUEST

A través de esta primitiva el NMS solicita al agente retornar el valor de un objeto de interés identificándolo por su nombre. En respuesta el agente envía una primitiva indicando el éxito o fracaso de la petición. Si la petición fue correcta, el mensaje resultante también contendrá el valor del objeto solicitado. Esta primitiva puede ser usada para recoger un valor de un objeto, o varios valores de varios objetos mediante el uso de listas.

GET NEXT REQUEST

Esta primitiva es usada para recorrer una tabla de objetos. Después de recoger el valor de un objeto con el mensaje GET REQUEST, se utiliza la primitiva GET NEXT REQUEST de ser necesaria repetir la operación con el siguiente objeto en la tabla de objetos. Siempre se utiliza el resultado anterior para

realizar una nueva consulta, de esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información existente.

SET REQUEST

Esta primitiva se la utiliza para modificar el valor de un objeto realizando una solicitud al agente y el objeto que se desea modificar. En algunos casos los dispositivos propietarios no dan muchos permisos de escritura como para poder uso de esta primitiva.

GET RESPONSE

Esta primitiva es usada por el agente para responder a un mensaje GET REQUEST, GET NEXT REQUEST, o SET REQUEST. En el campo "Id de Solicitud " se relaciona las primitivas que realizaron la solicitud con el mensaje GET RESPONSE que contiene su respectiva respuesta.

TRAP

Es un tipo mensaje de alerta que generan los agentes para informar o notificar diversas situaciones de cambios repentinos en el dispositivo.

ESTRUCTURA DEL PROTOCOLO SNMPV1

El formato de mensaje para todas las versiones de SNMP es similar, a excepción de su respectiva PDU (Protocol Data Unit), véase Fig. 1.8

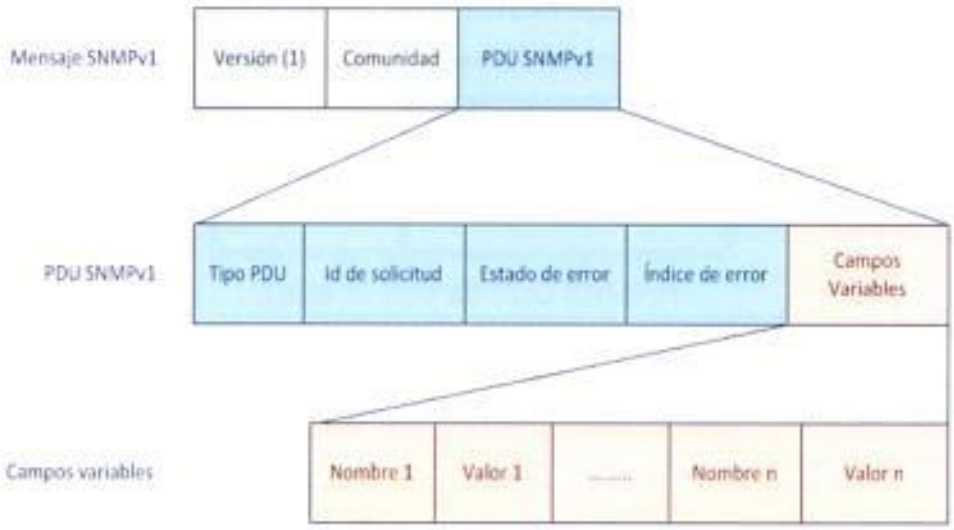


Figura 8.8 Formato de un paquete SNMPv1

El formato de la PDU GET REQUEST, GET NEXT REQUEST, GET RESPONSE Y SET REQUEST se muestra en la Figura 1.9

Figura 9.9 PDU SNMPv1

Tipo PDU: Especifica el tipo de PDU a transmitir, véase la Tabla.1.

Tipo PDU	PRIMITIVA
0	GET REQUEST
1	GET NEXT REQUEST
2	GET RESPONSE
3	SET REQUEST

Tabla 1. Tipo de PDU SNMPv1

ID de solicitud: Es utilizado para enviar las solicitudes y respuestas SNMPv1.

Estado de error: Indica un número de error y tipo de error. Sólo la operación de respuesta establece este campo. Otras operaciones establecen este campo a cero.

Índice de error: Asocia un error en una instancia de objeto determinada. Sólo la operación de respuesta establece este campo. Otras operaciones establecen este campo a cero.

Campos Variables: Sirve como el campo de datos de la PDU SNMPv1. Cada enlace asocia variables de una instancia de objeto determinada con su valor actual con la excepción de GET y GET NEXT peticiones, para lo cual se tiene en cuenta el valor.

El formato de la PDU TRAP se muestra en la Fig. 1.10

Enterprise	Dirección del Agente	Tipo de TRAP	Codigo Especifico de TRAP	Sellado de tiempo	Campos Variables

Figura 10.10 PDU TRAP SNMPv1

Enterprise: Identifica al software del agente que genero la TRAP.

Dirección del Agente: Dirección IP del agente que envió la TRAP.

Tipo de TRAP: Campo que describe el evento que se informa. Se basa de un valor numérico el cual está relacionado a su respectivo evento como se define en la Tabla.2.

Tipo de TRAP	Nombre
0	ColdStart
1	WarmStart
2	Link Down
3	Link Up
4	AutenticationFailure
5	EGP neighbourloss
6	Enterprise Specific

Tabla 2. Tipo de TRAP

Código Específico de TRAP: Se utiliza para identificar una trampa no genérica diferente de las conocidas, teniendo el valor 6 en el campo "tipo de TRAP" y visualizando en el campo "Enterprise" el Nombre de la TRAP. Está dirigido a las TRAPS desarrolladas por los fabricantes para sus respectivos productos.

Sellado de tiempo (Timestamp): Es el tiempo que se tiene desde que se activó el agente hasta que se generó la TRAP. Este tiempo se refleja en segundos.

1.5.2. SNMPv2

Es una evolución de la SNMPv1. El GET, GET NEXT, y las operaciones que se utiliza en SNMPv1 son exactamente los mismos que los utilizados en SNMPv2. Sin embargo, SNMPv2 añade y mejora algunas operaciones de protocolo. La operación TRAP SNMPv2, por ejemplo, cumple la misma función que el utilizado en SNMPv1, pero utiliza un formato de mensaje diferente y está diseñado para sustituir el TRAP SNMPv1.

Este protocolo de gestión consiste en la especificación de las políticas de acceso SNMP para SNMPv2. Una política de acceso SNMP es una relación administrativa que implique una relación entre una comunidad SNMP, un modo de acceso, y una vista MIB.

Una comunidad SNMP es un conjunto de uno o más huéspedes. El nombre de la comunidad es una cadena de

octetos que un administrador SNMP debe integrar en un paquete de solicitud SNMP con fines de autenticación.

El modo de acceso especifica a los dispositivos en la comunidad respecto a la recuperación y la modificación de los valores de uno o varios objetos de un agente SNMP específico. El modo de acceso puede ser: lectura, lectura y escritura o sólo escritura.

Una vista MIB define una o más sub-árboles MIB SNMP que una comunidad específica puede acceder. La vista MIB puede ser el árbol MIB o un subconjunto limitado de todo el árbol MIB.

Cuando el agente SNMP recibe una solicitud, el agente verifica el nombre de la comunidad con la dirección IP del host solicitante para determinar si el host solicitante es miembro de la comunidad SNMP identificado por el nombre de la comunidad. Si el host solicitante es miembro de la comunidad SNMP, el agente SNMP determina si el host solicitante se le permite el acceso especificado para las variables MIB específicos definidos en la política de acceso asociada a esa comunidad. Si todas las condiciones se cumplen, el agente

SNMP intenta honrar la solicitud. De lo contrario, el agente SNMP genera una trampa de error de autenticación o devuelve el mensaje de error correspondiente al host solicitante.

En SNMPv2 también se definen dos nuevas operaciones:

- GET BULK
- INFORM.

GET BULK

La operación GET BULK se utiliza para recuperar eficientemente grandes bloques de datos.

INFORM

La operación INFORM permite a un NMS enviar información de TRAPS a otra NMS y recibir entonces una respuesta. INFORM también pueden ser mensajes de un gestor a otros para intercambiar información, confirmaciones, errores, etc.

ESTRUCTURA DEL PROTOCOLO SNMPv2

Así se muestra el mensaje de SNMPv2, véase Fig. 1.11:

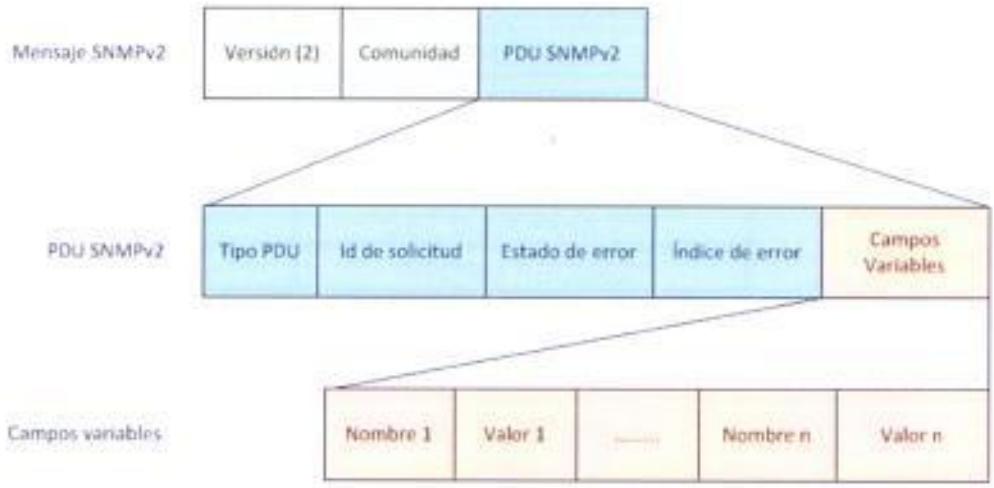


Figura 11.11 Mensaje SNMPv2

Para SNMPv2, GET REQUEST, GET NEXT REQUEST, GET RESPONSE, SET REQUEST y TRAP PDU se muestra en la Fig. 1.12.

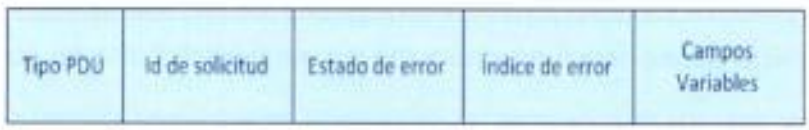


Figura 12.12 PDU SNMPv2

Tipo de PDU: Identifica el tipo de PDU transmitida.

Tipo PDU	PRIMITIVA
0	GET REQUEST
1	GET NEXT REQUEST
2	GET RESPONSE
3	SET REQUEST
4	NO ESTA EN USO(TRAP SNMPV1)
5	GET BULK REQUEST
6	INFORM REQUEST
7	TRAP SNMPv2
8	REPORT

Tabla 3. Tipo de PDU SNMPv2

ID de solicitud: Es utilizado para enviar las solicitudes y respuestas SNMPv2.

Estado de error: Indica un número de error y tipo de error. Sólo la operación de respuesta establece este campo. Otras operaciones establecen este campo a cero.

Índice de error: Relaciona un error en una instancia de objeto determinada. Sólo en la respuesta se obtiene información de este campo. Otras operaciones establecer este campo a cero.

Campos Variables: Sirve como el campo de datos (valor 1, valor 2) de la PDU SNMPv2. Cada enlace asocia variables de una instancia de objeto determinada con su valor actual con la

excepción de GET y GET NEXT peticiones, para lo cual se tiene en cuenta el valor.

El formato PDU GET BULK se muestra en la Fig. 1.13.

Figura 13.13 PDU GET BULK

Tipo PDU: Identifica la PDU como una operación GET BULK.

ID de solicitud: Es utilizado para enviar las solicitudes y respuestas SNMPv2.

Sin repetidores: Especifica el número de instancias de objeto en el campo variable que debe ser recuperado, no más de una vez desde el principio de la solicitud. Este campo se usa cuando algunos de los casos son objetos escalares con una sola variable.

Repeticiones Máxima: Define el número máximo de veces que otras variables además de los especificados por el campo sin repetidores deben ser recuperados.

Campos Variables: Sirve como el campo de datos (valor 1, valor 2) de la PDU SNMPv2. Cada enlace asocia variables de

una instancia de objeto determinada con su valor actual (con la excepción de GET y GET NEXT peticiones, para lo cual se tiene en cuenta el valor).

1.5.3. SNMPV3

La arquitectura SNMPv3 presenta el modelo de seguridad basado en el usuario (USM, User-based Security Model) para la seguridad de los mensajes y la vista basada en el Modelo de Control de Acceso (VACM, View-based Access Control Model) para el control de acceso. La arquitectura permite el uso concurrente de seguridad diferente, control de acceso, y los modelos de procesamiento de mensajes. [4]

USM utiliza el concepto de un usuario para que los objetos de seguridad se configuren tanto el agente y en el gestor. Los mensajes enviados usando USM están mejor protegidos que los mensajes enviados con base comunitaria de seguridad. Los mensajes intercambiados entre el gestor y el agente tiene la comprobación de la integridad de datos y autenticación del origen de datos. USM protege contra los retrasos de mensajes

y las repeticiones de mensajes mediante el uso de indicadores de tiempo y los indicadores de solicitud. [4]

La confidencialidad de los datos, o el cifrado, también está disponible, cuando esté permitido, como un producto instalable por separado. La versión cifrada SNMP se puede encontrar en el paquete de expansión AIX.

El uso de VACM implica que definen las colecciones de datos, los grupos de usuarios de los datos y las declaraciones de acceso que definen que un determinado grupo de usuarios pueden utilizar para la lectura, la escritura o recibo en una TRAP.

SNMPv3 también introduce la posibilidad de configurar dinámicamente el agente SNMP mediante los comandos SET de SNMP contra los objetos MIB que representan configuración del agente. Este soporte de configuración dinámica permite la adición, eliminación y modificación de entradas de configuración de forma local o remota.

ESTRUCTURA DEL PROTOCOLO SNMPV3

El formato del mensaje se muestra en la Fig. 1.14.

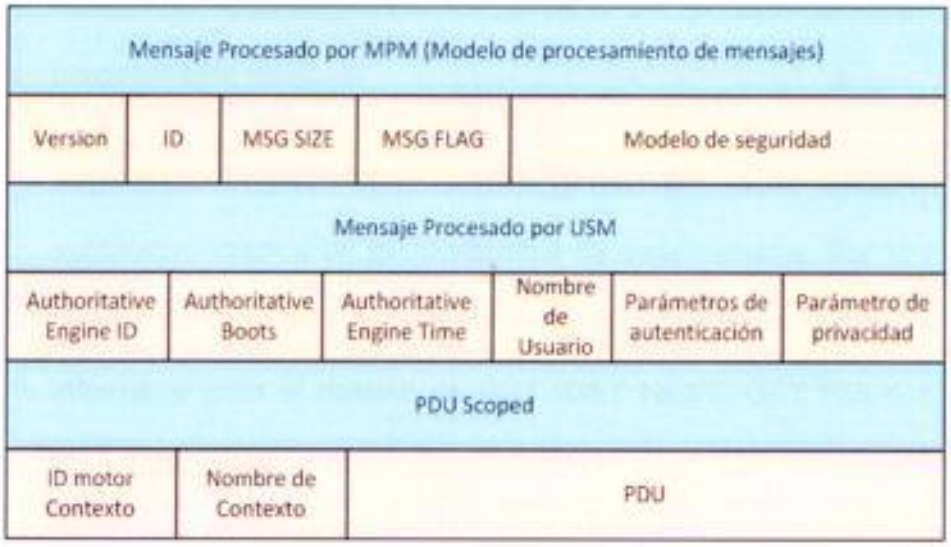


Figura 14.14 Mensaje SNMPv3

Version: El valor entero será "3" por ser SNMPV3.

ID: Un identificador único que se utiliza entre dos entidades SNMP para coordinar los mensajes de solicitud y respuesta.

MsgSize: El tamaño máximo de un mensaje en octetos apoyado por el remitente del mensaje.

MsgFlag: una cadena de octetos que contiene tres banderas en los tres bits menos significativos: reportableFlag, privFlag, authFlag.

Modelo de seguridad: Un identificador para indicar qué modelo de seguridad fue utilizado por el emisor y por lo tanto, que el

modelo de seguridad debe ser utilizado por el receptor para procesar este mensaje.

AuthoritativeEngine ID: El snmpEngineID del motor SNMP autoritativo implica en el intercambio de este mensaje. Por lo tanto, este valor se refiere al origen de una TRAP respuesta o informe, y para el destino de GET, GET NEXT, GET BULK, SET o INFORM.

AuthoritativeEngineBoots: Este campo indica el número de veces que la entidad SNMP autorizada haya arrancado. Este campo se utiliza en el mensaje autenticado para validar la puntualidad de un mensaje. [5]

AuthoritativeEngine Time: Este campo indica el tiempo transcurrido desde la entidad SNMP autorizada se haya reiniciado. Este campo se utiliza en los mensajes autenticados para validar la puntualidad de un mensaje.[5]

Nombre de usuario: El usuario (principal) en cuyo nombre el mensaje se intercambia.

Parámetros de autenticación: Null si la autenticación no se utiliza para este intercambio. De lo contrario, se trata de un parámetro de autenticación.

Parámetro de privacidad: Null si la privacidad no está siendo utilizado para este intercambio. De lo contrario, este es un parámetro de privacidad.

PDU: Los tipos de PDU para SNMPv3 son el mismo que el SNMPv2.

CAPITULO 2

GESTION DE UNA RED LAN CON SNMPV2

Una red comprende de usuarios e equipos integradores que simplifiquen, optimicen y permitan el acceso a los servicios disponibles, servidores equipados para brindar servicios como pueden ser correo electrónico, compartir archivos, base de datos, aplicaciones y muchos otros.

Debido a la existencia de distintos modelos de redes para compartir información, recursos o servicios; nuestro modelo de estudio serán las llamadas Redes LAN (Local Area Network).

2.1. Redes LAN

Una red LAN tiene la finalidad de interconectar una o varias computadoras y servidores. Hoy en día los dispositivos o periféricos que conforman las redes LAN han evolucionado lo suficiente como para lograr ser aprovechados en los centros educativos, pequeñas y medianas empresas, también se resalta su aplicación dentro de hogares conocido bajo el concepto de hogares inteligentes o como laboratorios para futuros profesionales TI(Tecnologías de la Información), dando lugar a la oportunidad de integrar tecnología de última generación aprovechando su amplia capacidad de conexión.

En comparación a los otros modelos de red, damos a resaltar algunas de las características importantes de una Red LAN:

- Transmisión de datos entre 10 Mbps (Megabits por segundo) y 10 Gbps(Giga bits por segundo).
- Tecnología broadcast de transmisión de datos compartida.
- Uso de un medio de comunicación privado.
- Utiliza distintos medios de transmisión (cable coaxial, cables telefónicos, fibra óptica y Wi-Fi (Wireless Fidelity)).
- Facilidad para efectuar cambios en el hardware y el software.
- Posibilidad de conexión a otras redes.

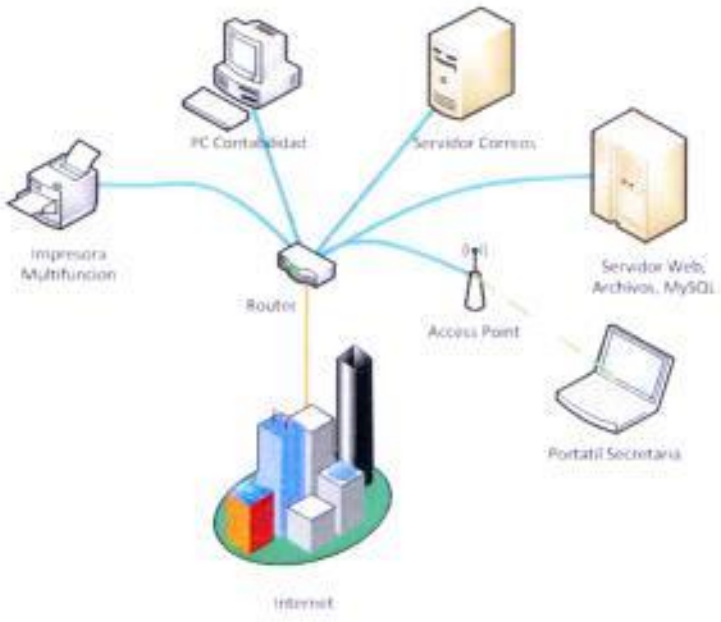


Figura 15.1 Red LAN

2.1.1. VENTAJAS DE UNA RED LAN

En una empresa suelen existir muchos dispositivos que forman parte de la red, los datos almacenados en un dispositivo pueden ser necesarios por otro dispositivo, los dispositivos que trabajen con los mismos datos deberán poseer el mismo software para manejar dichos datos.

La red de área local o LAN, permite compartir bases de datos, programas y periféricos como puede ser una tarjeta de red, una impresora, etc. Nos da la posibilidad de centralizar

información o procedimientos para facilidad de la administración y la gestión de los equipos.

Además, una red de área local nos proporciona un gran ahorro de tiempo gracias a la gestión de la información yeconómico debido a que a través de una conexión de Internet es posible conectar al Internet a varios dispositivos conectados en la red.

2.2. COMPONENTES DE UNA RED LAN

SERVIDORES

Son sistemas que responden a las solicitudes a través de una red de ordenadores para proporcionar o ayudar a proporcionar un servicio de red . Los servidores se pueden ejecutar en un equipo dedicado, que también se conoce como "el servidor" a menudo, pero muchos equipos de la red son capaces de albergar servidores. En muchos casos, un ordenador puede proporcionar varios servicios y tienen varios servidores que los ejecutan.

- **SERVIDOR WEB**

En esencia, un Servidor Web provee contenido a un Navegador Web. Este contenido será compilado y ejecutado por el Navegador Web, el cual para la transmisión de estos datos se suele utilizar el protocolo HTTP (Hypertext Transfer Protocol).

- **SERVIDOR DE CORREO**

Casi tan necesarios e importantes como los Servidores Web, un Servidor de Correo nos permite comunicar entre usuarios a través de redes corporativas e incluso a través de Internet. Siguiendo una serie de procesos se logra la comunicación entre usuarios, mediante la transportación de información al momento del envío de un correo electrónico.

- **SERVIDOR FTP (FILE TRANSFER PROTOCOL)**

Uno de los más antiguos de los servicios de Internet, transferencia de archivos hace posible mover uno o más archivos de forma segura entre los equipos mientras que proporciona seguridad de archivos y la organización, así como de control de transferencia.

- **SERVIDOR TELNET**

Un Servidor Telnet permite a los usuarios iniciar sesión en un equipo host y realizar tareas como si estuvieran trabajando en el mismo equipo remoto.

ESTACIÓN DE TRABAJO

Tienen a su disposición los recursos de la red y también los servicios a los cuales tenga acceso.

BRIDGES O PUENTES

Es un dispositivo conformado por software y hardware que interconecta dos redes entre sí. Estas pueden ser locales o remotas, los puentes locales son aquellos que interconectan entre dos redes físicamente cercanas mientras que los puentes remotos conectan redes ubicadas en áreas extensas, y dos o más redes locales a través de la red telefónica (RDSI), redes de fibra óptica de alta velocidad, conexiones microondas o por medio de satélites.

TARJETA DE RED

Conocido como NIC (Network Interface Card), nos permite comunicar el computador con la red. Dentro de la tarjeta de red se encuentra los protocolos de comunicación que permiten al computador comunicarse a través de una red. Se clasifican de acuerdo a su operación dentro de redes cableadas o inalámbricas siendo algunas compatibles para ambos tipos.

CABLES DE RED

Permiten la transmisión de información entre estaciones de trabajo en una Red LAN. Los medios físicos utilizados son el cable UTP o de par trenzado, el cable coaxial y la fibra óptica.

CONCENTRADORES DE RED

Un concentrador de red nos permite centralizar la red para así poder transmitir datos entre los dispositivos dentro de la red. Cuando se transmiten datos de un dispositivo al Concentrador de Red este es transmitido a todos los dispositivos en la red. El ancho de banda en una red LAN de un concentrador de red se comparte, lo que significa

que los dispositivos recibirán una parte del ancho de banda total disponible proporcional para cada dispositivo.

CONMUTADOR DE RED

Los conmutadores asignan a cada dispositivo perteneciente a la red una dirección MAC (Media Access Control). Esto permite a las redes el poder compartir información de rutas, configuración o cualquier otro componente lógico dentro los dispositivos. Como los conmutadores de red no transmiten a todos los dispositivos dentro de la red al mismo tiempo, se puede destinar el mismo ancho de banda a cada uno de los dispositivos.

ENRUTADORES

Los enrutadores de red interconectan redes entre sí, por ejemplo al tener dos áreas físicas distintas permitirles formar una única red Lan. Los enrutadores permiten comunicar dispositivos que estén separados por acceso, áreas de trabajo o pisos en un edificio. Son comunes en hogares donde permiten fácil acceso desde los computadores al Internet; aunque, también se utiliza para conectar redes de todo tipo. Los enrutadores de red actuales son el resultado de combinar un

enrutador, un conmutador de red y herramientas tales como un servidor DHCP y un cortafuego.

2.3. TOPOLOGÍA DE UNA RED LAN

La topología de red nos define la estructura en que se manejara la red. Una parte de la topología de la Red LAN es la topología física que comprende el ordenamiento físico de los cables o medios. Mientras por otro lado esta topología lógica que comprende la forma en cómo los hosts acceden a los medios para la transmisión de datos.

Las topologías más comúnmente usadas son las siguientes, véase Fig. 2.2:

TOPOLOGÍAS FÍSICAS

- Una topología de bus circular utiliza un solo cable backbone que debe terminarse en ambos extremos. Todos los dispositivos se conectan a este backbone. Su funcionamiento es simple y fácil de instalar aunque es sensible a problemas de tráfico, y un corte en el cable me inactiva toda la red.

- La topología de anillo se conecta mediante una conexión de entrada y salida en cada nodo, formando un anillo físico. Cuando se transmite información de un nodo a otro, esta pasará por todos los nodos hasta llegar a su destino. La comunicación en esta topología es unidireccional. Ya enviados los datos a otro nodo desdeel nodo anterior, continuará circulando el mensaje por la red hasta llegar de nuevo al nodo de origen, donde es eliminado. En esta topología al haber un corte en el enlace se cae la red.

- La topología en estrella conecta a un nodo central todos los demás nodos. El nodo central envía el mensaje de un nodo a otro. Al fallar un nodo no se afecta la red, a excepción que falle el nodo central lo que dejaría interrumpida las transmisiones.

- Una topología en estrella extendida comunica topologías estrellas entre sí mediante los dispositivos hubs o switches. Esta topología nos ayuda a aumentar la cobertura de la red.

- La topología de malla permite tener una red lo mas protegida para evitar posibles interrupciones de servicio. En esta topología, cada uno de los dispositivos posee conexiones independientes hacia los otros dispositivos.

- La topología de árbol posee varios dispositivos conectados a modo que nuestra red crecerá en forma de ramas desde un nodo principal. Un fallo en la conexión con el nodo principal interrumpiría las transmisiones.

- Una topología jerárquica similar a una estrella extendida pero en lugar de utilizar los dispositivos hubs o switches, el sistema se conecta con un dispositivo gestionador del tráfico de la red.

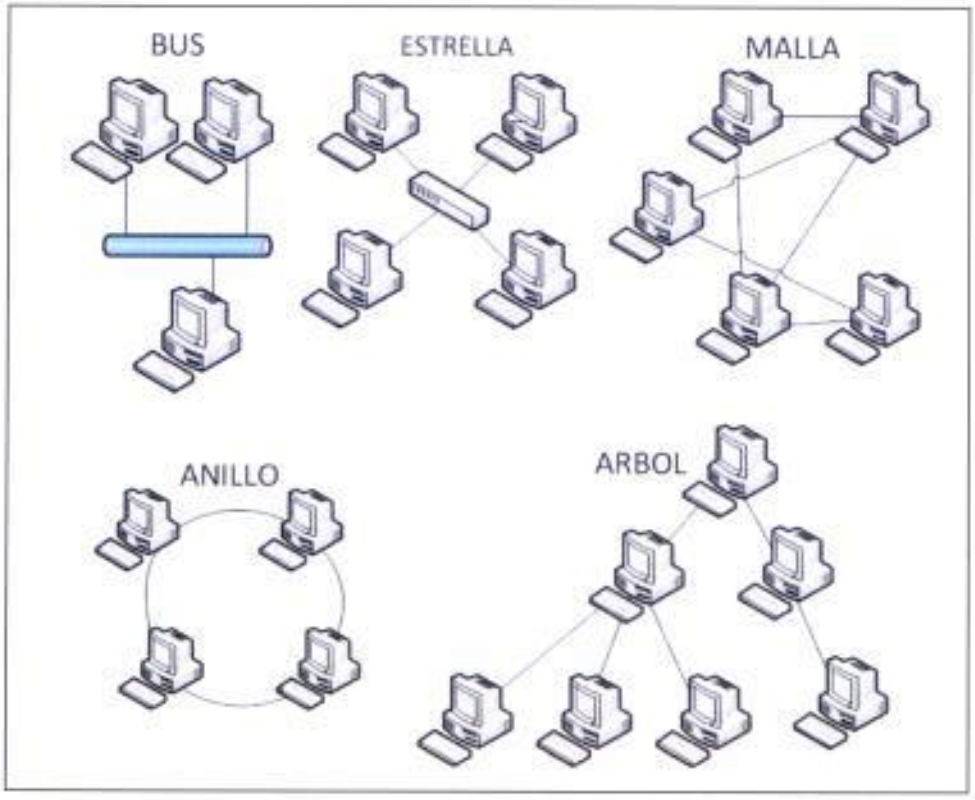


Figura 16.2 Topologías físicas

TOPOLOGÍAS LÓGICAS

La topología lógica de una red es la forma en que los dispositivos se comunican por medio del medio de transmisión. Los más comunes tipos de topologías lógicas son broadcast y transmisión de tokens, véase Fig. 2.3.

- La topología broadcast indica que cada dispositivo enviara sus datos a todos los dispositivos en la red. Las respuestas son enviadas por los otros dispositivos acorde al orden de llegada, por ejemplo Ethernet.

- La topología transmisión de tokens nos da controlen el acceso a la red transmitiendo tokens electrónico a cada dispositivo. Cuando un dispositivo recibe el token, este dispositivo podrá enviar los mensajes a la red, en caso de no transmitir un mensaje se procede a transmitir el token al siguiente dispositivo repitiendo el procedimiento anterior. Por ejemplo Token Ring o la Interfaz de Datos Distribuida por Fibra (FDDI, Fiber Distributed Data Interface).

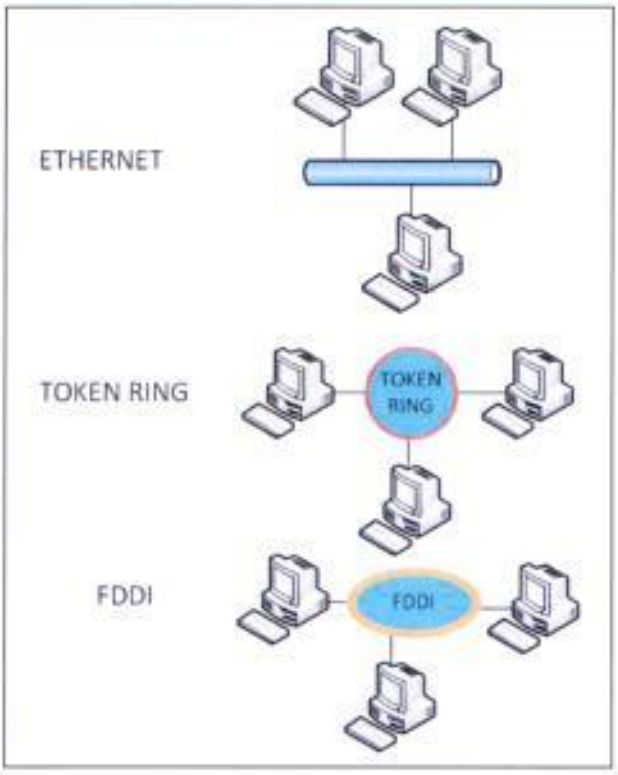


Figura 17.3 Topologías lógicas

2.4. GESTIÓN DE REDES LAN

La Gestión de redes requiere de plataformas que integren herramientas con la capacidad de adaptarse a los diferentes tipos de elementos de la red que en la actualidad están en constante cambio y mayores niveles de complejidad.

Para la gestión de redes, en su mayoría heterogéneas, se han adoptado diversas estrategias a lo largo del tiempo. Al comienzo se

implementó una integración de gestión de redes Lan jerárquica, dada por un esquema de gestor de gestores. Este esquema era válido pero no permitía suficiente flexibilidad en los cambios de configuración de la red, debido a que exigía constante modificación en los programas. También se volvió una limitación la existencia de un único nodo jerárquico superior (gestor de gestores) como procesador de la información y fiabilidad de una red de muchos nodos.

Tomando en cuenta la Gestión de Red como vital, se debería implantar hacia todos los recursos de la red. Por lo tanto el incluir Gestión de Red indica que el impacto deberá ser el mínimo posible, en la actualidad la mayoría de las herramientas de apoyo de gestión de red se basan en el modelo Gestor – Agente como los basados en el protocolo SNMPv2.

En comparación a otro protocolo de igual peso como lo es CMIP, el protocolo SNMPv2 nos permite desarrollar una gestión más simple y barata.

2.5. GESTIÓN DE RED CON SNMPv2

Desde el inicio de su concepción SNMP se volvió exitoso debido a su simplicidad, catalogado en sus principios como un protocolo orientado al monitoreo esencialmente simple y ha logrado mejorarse hasta lo que conocemos como SNMPv3, pero para nuestro interés realizaremos nuestra gestión exitosamente con SNMPv2.

SNMPv2 nos permite minimizar la complejidad de la gestión. Esto lo vuelve atractivo en los siguientes aspectos:

- Costos en desarrollo de software para la gestión.
- Gran alcance de administración vía remota.
- Gran alcance de administración vía remota.
- Conjunto simplificado de funciones de gestión son fáciles de entender y utilizar por los desarrolladores de herramientas de gestión de red.

MODO DE OPERACIÓN

El agente SNMP al recibir un Get-request proporcionara la respectiva Get-Response, conteniendo los valores de las variables de los objetos consultados. La operación Get-Request sólo devolverá los valores de las variables cuyos objetos estén disponibles y no posean error en

ellas. Si el agente puede proporcionar valores de todas las variables consultadas en la lista de la PDU Get-Request, la PDU Get-Response en la lista de variables proporciona los valores resultantes por cada variable, pero al faltar alguno la lista se devuelve vacía. Los errores que pueden producirse son los enumerados anteriormente. En algunos casos es posible mediante el campo índice conocer cuál es la variable que origino el problemas.

La PDU Get-Next-Request es casi idéntica a la PDU Get-Request, a diferencia de que en la Get-Next-Request el agente devuelve por cada variable de la lista el valor del objeto según el orden proporcionado en la MIB. Esto nos permite conocer el árbol de la MIB, las situaciones de error son similares a las que se producen en la PDU Get-Request.

La PDU Set-Request es generada al igual un Get-Request, con la diferencia de que Set-Request nos permite reescribir el valor de un objeto. Por lo tanto, se muestra el identificador del objeto y se incluye en la lista de variables el nuevo valor asignado.

La operación Set-Request implica que se deberán actualizar todas las variables relacionadas o ninguna, poniéndonos en las mismas condiciones de error que cuando utilizamos un Get-Request.

SNMP no posee mecanismo específico para ejecutar los comandos sobre un agente. SNMP solo lee y escribe variables; sin embargo, es posible utilizar un objeto para representar una orden, con lo que se realizara una acción concreta cuando al objeto se le asigna un valor específico.

CAPITULO 3

SELECCIÓN DE SIMULADORES Y PROGRAMA PARA GESTIONAR SNMPV2 EN UNA RED LAN

3.1. SIMULADOR DE RED

El estudio de las redes recibido lo hemos manejado utilizando libros, videos o en base a los apuntes de clases, que debido a la tecnología y economía que caracteriza a los dispositivos de la red nos encontramos limitados a tener acceso a ellos. Siendo más específicos mencionaremos algunas de las razones para el aprendizaje de las redes:

- Los dispositivos disponibles se encuentran desactualizados.
- La implementación representa un alto costo.

- No cuentan con una interfaz gráfica amigable al usuario, limitando la posibilidad de documentar lo realizado.
- La falta de experiencia en el manejo de estos dispositivos nos impide realizar una correcta configuración, administración y mantenimiento.

Por estas y más razones se han desarrollado los programas de simulación disponibles tanto de forma pagada o gratuita, resolviendo la necesidad de disponer de un programa capaz de simular gran variedad de dispositivos dentro de un entorno de red. Con esto el público en general, estudiantes de universidades o trabajadores dentro del ambiente de las redes podrá aprender, practicar o capacitarse en las varias especialidades que se desarrollan dentro de las redes y los dispositivos que la conforman.

La mayoría de estos programas de simulación son pagados y han surgido gracias a la iniciativa individual o conjunta de algunos de los fabricantes que desarrollan los dispositivos que integran la red, aunque no es común en algunos incluir toda la gama de sus dispositivos disponibles. Al practicar con estos simuladores iremos adquiriendo la experiencia necesaria para podernos adaptar sobre los

dispositivos existentes, que aunque sean de marcas o comandos distintos manejan la misma lógica de funcionamiento.

Los otros tipos de programas de simulación, al contrario de los anteriores son gratuitos para el público local y mundial, siendo desarrollados por iniciativa de universidades o un trabajo conjunto entre universidades y fundaciones teniendo como finalidad comprender y mejorar el manejo de las redes. Lo que proveerá a estudiantes y profesionales programas de simulación libres capaces de manejar extensas gamas de marcas y modelos de equipos.

Al utilizar un simulador de red disponemos de la posibilidad de realizar escenarios con amplia capacidad y dinámica, estructurados de dispositivos simulados o virtuales teniendo el alcance de aplicación y problemas como los que se presentan para realizar redes Lan con dispositivos físicos.

3.2. SIMULADORES DE RED EN EL MERCADO

Actualmente nos es posible tener acceso a simuladores de red cuya precisión de su desempeño sea semejante al de las redes Lan formadas por dispositivos físicos.

Entre los simuladores de red existentes enfocaremos nuestro interés sobre aquellos que dispongan de las siguientes características:

- Facilidad de manejo y configuración.
- Fácil mantenimiento y respaldo de la información.
- Comunicación entre distintos dispositivos basados en el modelo TCP/IP.
- Capaz de simular el comportamiento de una red trabajando con dispositivos encendidos y apagados.
- Permita implementar los conceptos sobre el cual está basada la gestión de las redes.
- Capaz de soportar el comportamiento de las primitivas SNMPv2 dentro de la red simulada.

Entre los programas existentes para simular una red, encontramos algunos que cumplen con las características y son de acceso gratuito

para el usuario. Por ello haremos una breve descripción de aquellos con los que probamos.

CISCO PACKET TRACER

El programa CISCO PACKET TRACER es un programa de simulación de redes desarrollado por CISCO y se caracteriza por ser muy poderoso y estar orientado a simular redes formadas solo de los dispositivos de la marca CISCO.

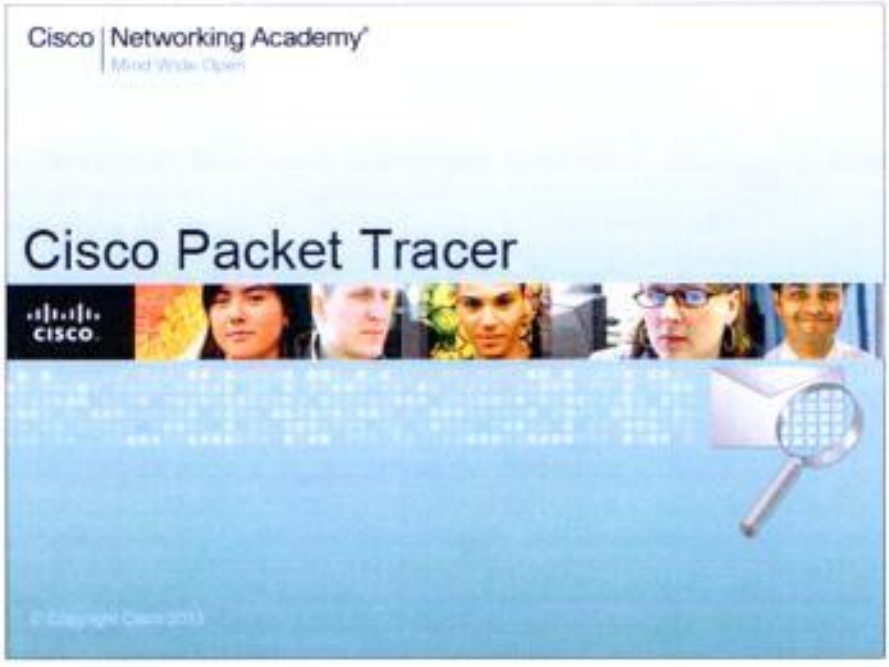


Figura 18.1 Logo de Cisco Packet Tracer[6]

Nos permite experimentar distintos ambientes de red, su uso está orientado a ser parte integral en el aprendizaje de la Academia de Redes de CISCO.

CISCO PACKET TRACER ofrece simulación, visualización, creación, evaluación y capacidades de colaboración y facilita la enseñanza y el aprendizaje de conceptos de tecnología compleja.[6]

CISCO PACKET TRACER reemplaza a los equipos físicos permitiendo a los estudiantes crear redes de mayor tamaño, fomentando la práctica para encontrar y resolver problemas.

CISCO PACKET TRACER complementa los planes de estudios de la Academia de Redes de CISCO, permitiendo a los instructores enseñar y demostrar fácilmente complejos conceptos técnicos y diseño de sistemas de redes.

El programa CISCO PACKET TRACER es permitido de forma gratuita para estudiantes, ex-alumnos, instructores y administradores que estén registrados a la Academia de Redes de CISCO.

SIMULADOR GNS3

GNS3 (Graphical Network Simulator 3) es un programa libre diseñado

para simular redes, funcionando de forma más parecida a las redes reales.

Figura 19.2 Logo del programa GNS3 [7]

Está diseñado con una interfaz gráfica intuitiva para el diseño y configuración de redes. Es posible ejecutarlo en toda gama de PC (Personal Computer) y utilizable sobre distintos sistemas operativos incluyendo Linux, MacOS X y Windows.

GNS3 para poder proporcionar una simulación más completa y precisa, utiliza los siguientes emuladores:

- Dynamips: Emulador de IOS (Internetwork Operating System) CISCO. [7]
- Qemu: Emulador de máquina genérica open source como CISCO ASA, PIX y IPS. [7]
- Virtualbox: Ejecuta sistemas operativos como Linux, MacOS X, Windows o JunOS. [7]

Estas características lo hacen una excelente alternativa para personas, ingenieros de red y administradores que necesiten complementar sus estudios con alguna herramienta de simulación de redes y lograr certificaciones como CCNA, CCNP, CCNIE, JNCIA, JNCIS, JNCIE mencionando algunas de las existentes.

VIRTUALBOX

VIRTUALBOX es un poderoso programa de virtualización que corre en la arquitectura x86 y AMD64, actualmente en desarrollo por ORACLE, creado para uso empresarial y de usuarios.

VIRTUALBOX no sólo es un producto muy rico en características y de alto rendimiento para clientes empresariales, es también la única solución profesional que está libremente disponible como programa de código abierto bajo los términos de la GNU General Public License (GPL) versión 2. [8]

Figura 20.3 Logo del programa Virtualbox [8]

Con VIRTUALBOX tenemos la posibilidad de disponer de sistemas operativos adicionales invitados cuyos recursos provienen de los recursos existentes físicamente. Estos estarán alojados dentro de una máquina anfitrión correspondiente al equipo físico.

De entre los sistemas operativos disponibles, VIRTUALBOX soporta WINDOWS NT/2000/XP/7/SERVER 2003/SERVER 2008, LINUX, SOLARIS, OPENSOLARIS y muchos otros más.

3.2.1. SIMULACIÓN DE UNA RED CON VIRTUALBOX

De los programas mencionados nos decidimos por utilizar VIRTUALBOX, con este lograremos cumplir con todos los

objetivos planteados y también realizar una óptima demostración de la simulación de las primitivas SNMPv2 en una Red LAN.

VIRTUALBOX ofrece muchas ventajas en comparación a otros programas, algunas de éstas son:

- Compatibilidad con distintas marcas de sistemas operativos permitiéndonos pluralidad de elección y aprendizaje.
- Realizar redes LAN virtuales.
- Uso eficiente de la memoria RAM (Random Access Memory).
- Permite abstracción de recursos de la máquina anfitrión y asignarlo a los dispositivos conocidos como máquinas virtuales.
- Permite realizar Gestión SNMPv2.

La simulación de la red, será realizada por VIRTUALBOX mediante la selección de las subredes privadas a utilizar y

asignando las direcciones IP de la subred a los equipos, con esto será suficiente para que formen parte de la subred y tener nuestra red Lan.

Con VIRTUALBOX realizaremos variedad de máquinas virtuales, algunas destinadas para ser servidores, máquinas clientes o máquinas administradoras. Con la virtualización dispondremos de la máquina anfitrión para poder abstraer recursos de CPU, Memoria RAM, Red y Almacenamiento y asignarlo a las máquinas virtuales; principalmente, dependeremos de la cantidad de Memoria RAM de la máquina anfitrión para la cantidad de máquinas virtuales que podamos crear.

La virtualización de sistemas operativos nos permite aprender, practicar y poder implementar máquinas virtuales para pre-producción o producción, teniendo libertad para instalación, configuración y mantenimiento de servicios de archivos, servicios de correo, servicios de intranet, agentes SNMP y Gestionador SNMP.

INSTALACION DE VIRTUALBOX

Instalaremos VIRTUALBOX en Windows:

a) Primero descargamos Virtualbox de la página web: ***www.virtualbox.org***, vamos a la carpeta en la que se guardó y damos doble click sobre el archivo que se descargó.

b) Nos saldrá una advertencia de seguridad, y escogemos Ejecutar. Nos mostrara la pantalla de bienvenida y damos NEXT, como vemos en la Fig. 3.4 se mostrara una pantalla que indica que reiniciara las conexiones de red para proceder con la instalación y damos click en YES.

Figura 21.4 Pantalla de instalación de Virtualbox, indicando el reinicio de las interfaces

c) En la siguiente pantalla nos preguntará si estamos listo para la instalación, por lo que para seguir damos click en INSTALL.

d) Durante la instalación se nos preguntará por la instalación de complementos a los cuales daremos click en INSTALAR. Una vez terminada la instalación solo damos click en FINISH y con esto ya podremos utilizar VIRTUALBOX.

CREACION DE MÁQUINAS VIRTUALES EN VIRTUALBOX

Como ya disponemos del simulador ahora nos faltara los dispositivos, que en Virtualbox se llamarían máquinas virtuales. Para crearlas hacemos lo siguiente:

a) Abrimos el programa dando click en el Escritorio sobre el icono de VIRTUALBOX.

b) Al abrir el programa, vamos a la barra de superior y damos click sobre NUEVA.

c) Se nos abrirá una nueva pantalla para Crear máquina virtual, nos solicitara Nombre tipo y versión del Sistema Operativo tal como se muestra en la Fig. 3.5. Una vez llenada la información damos NEXT.

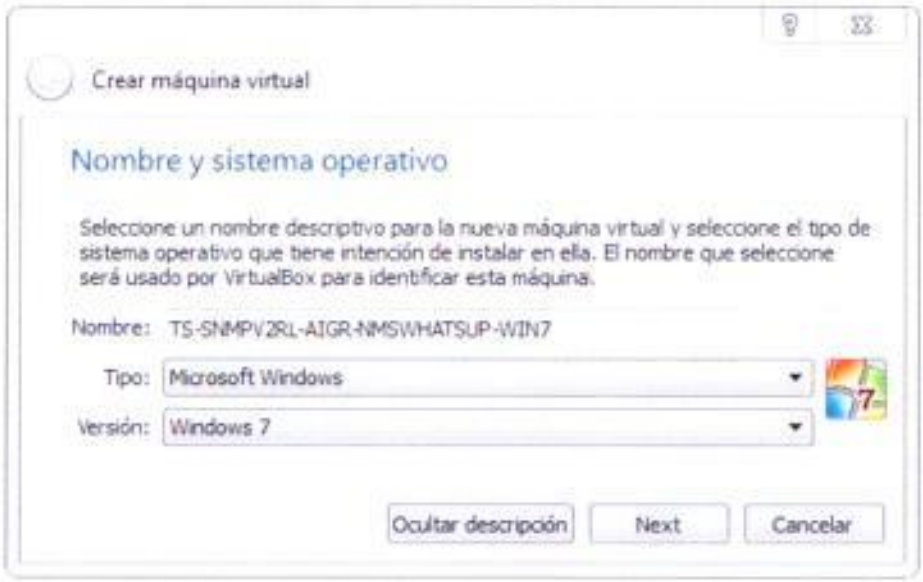


Figura 22.5 Pantalla para Crear máquina virtual solicitando Nombre y Sistema Operativo

d) Luego como vemos en la Fig. 3.6, asignamos la capacidad de memoria RAM siendo una abstracción de la existente en el equipo anfitrión y damos NEXT.

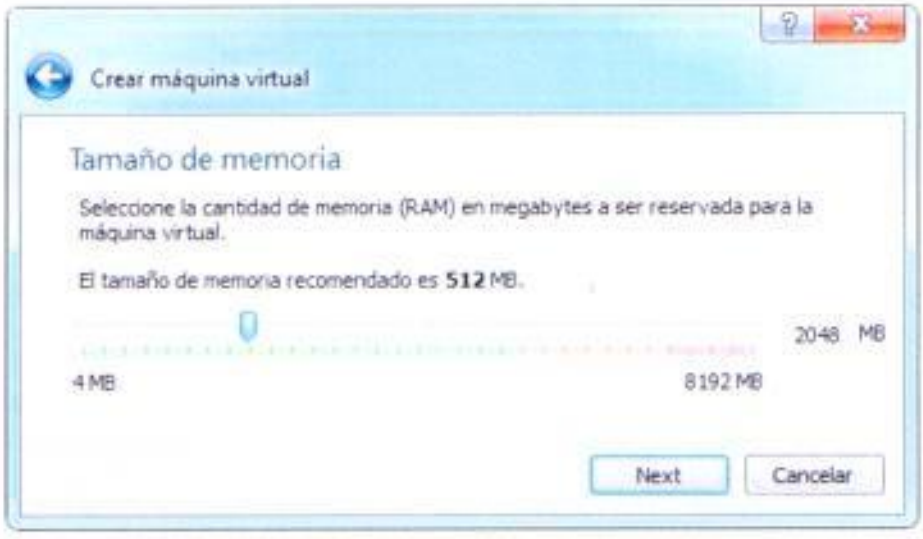


Figura 23.6 Asignando tamaño de memoria RAM en la Máquina Virtual

e) Ahora crearemos el disco duro para lo que escogemos la opción: Crear un disco duro virtual, como se muestra en la Fig. 3.7 y damos click en CREAR.

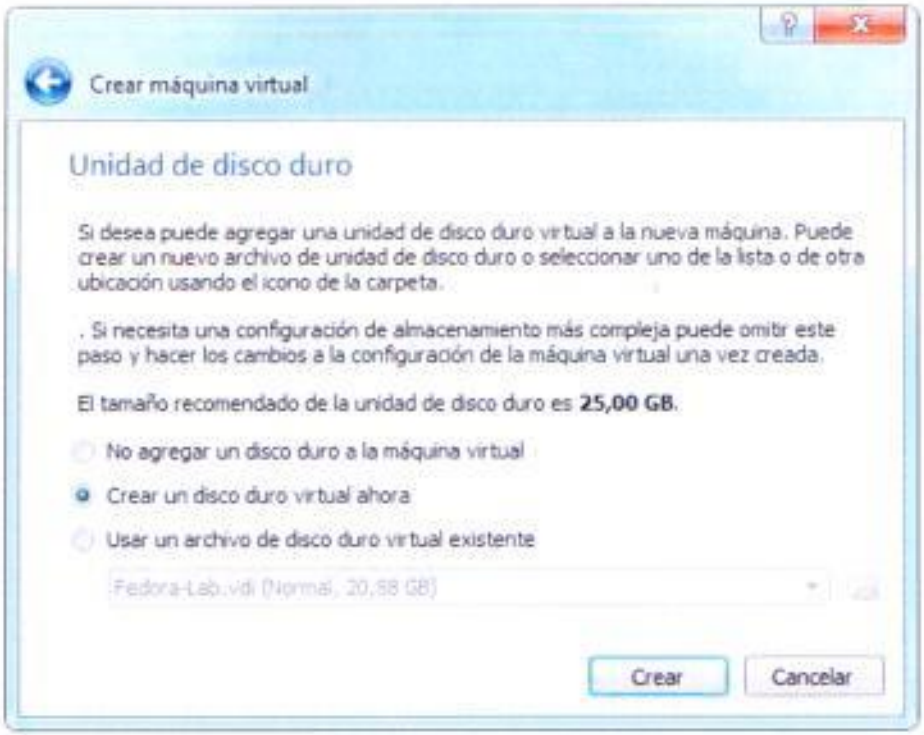


Figura 24.7 Creando el disco duro de la máquina virtual

f) Se nos pedirá seleccionar el tipo de archivo para la unidad de disco y lo dejaremos por defecto VDI (Virtual Desktop Infrastructure) y damos NEXT.

g) Dejamos por defecto RESERVADO DINAMICAMENTE para el tipo de almacenamiento en unidad de disco duro fisico y damos NEXT.

h) Ahora veremos en la Fig. 3.8 que seleccionaremos la ubicación del archivo el cual dejaremos por defecto, le

podremos de nombre: TS-SNMPV2RL-AIGR-NMSWHATSUP-WIN7 y seleccionaremos el tamaño límite asignado de Disco Duro. Damos click en CREAR y ya disponemos de nuestra nueva máquina virtual.

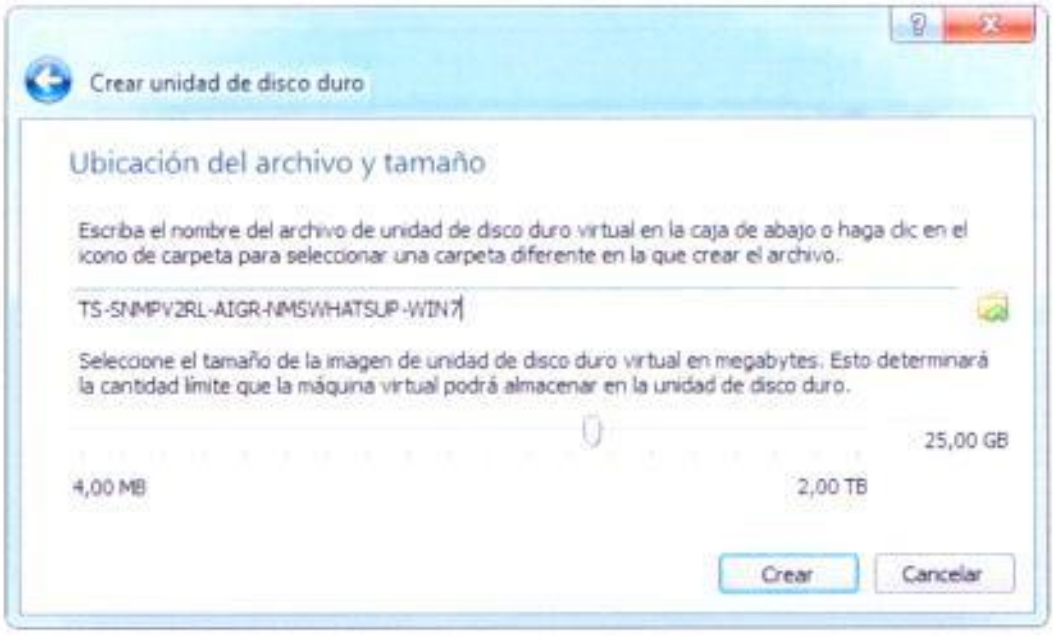


Figura 25.8 Ubicación de la máquina virtual y tamaño de disco duro

i) Sobre la máquina virtual daremos click derecho damos click sobre la opción de configuración, como vemos en la Fig. 3.9

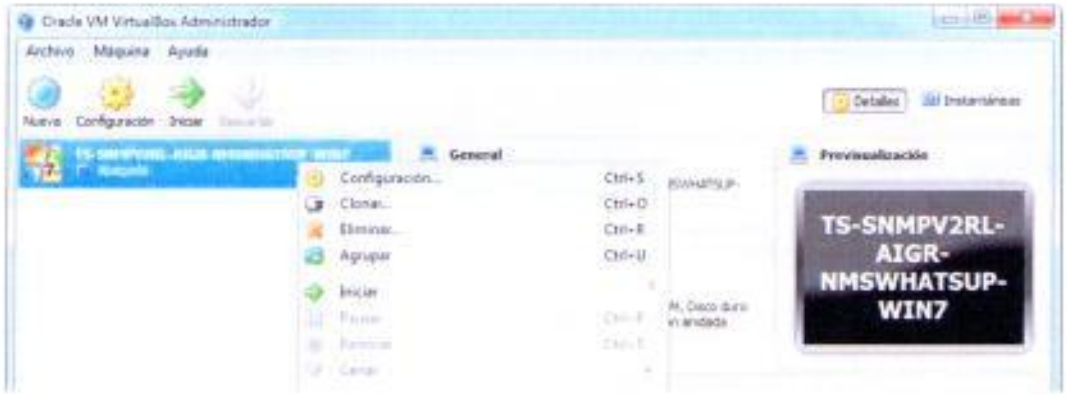


Figura 26.9 Opción Configuración de una máquina virtual

j) Se nos abrirá pantalla desde la cual podremos hacer cambios en la configuración cuando se encuentre apagada, como se ve en la Fig. 3.10 Del menú a la izquierda escogeremos Almacenamiento.

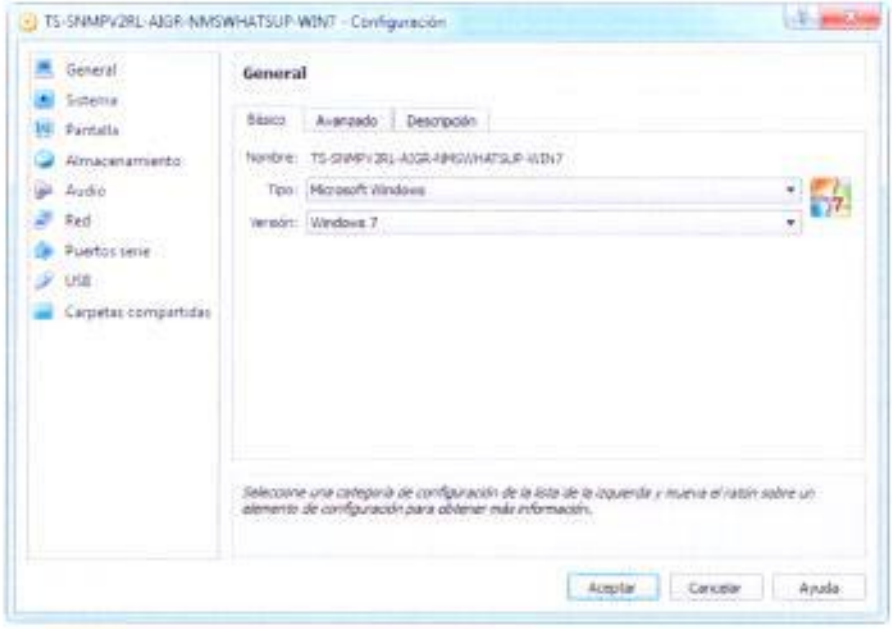


Figura 27.10 Pantalla de Configuración de una máquina virtual

k) Confirmaremos si la máquina virtual puede leer los discos desde la unidad D de la máquina anfitrión, como observamos en la Fig. 3.11 Desde esta unidad ingresaremos el disco de instalación del sistema operativo que deseamos tener.

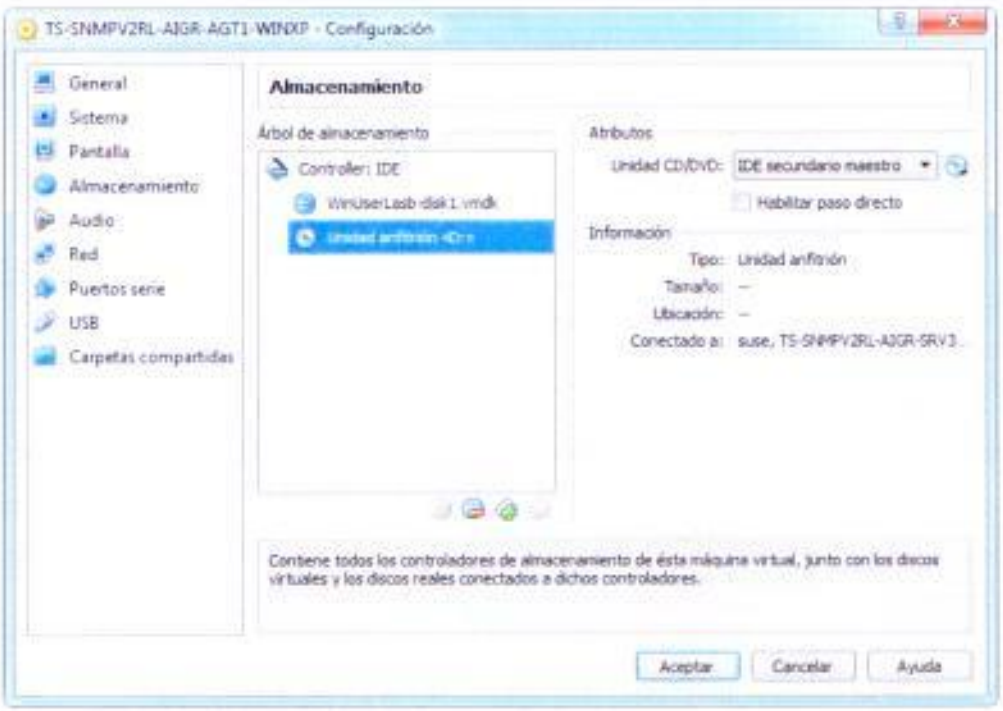


Figura 28.11 Configuración de Almacenamiento de una máquina virtual

l) Ahora ya solo nos falta habilitar la red interna, por lo que seleccionaremos en el menú de la izquierda la opción Red,

dentro habilitaremos un adaptador de red conectado a: Red interna y de Nombre: intnet, tal como se ve en la Fig. 3.12 Una vez realizado esto damos click en ACEPTAR.

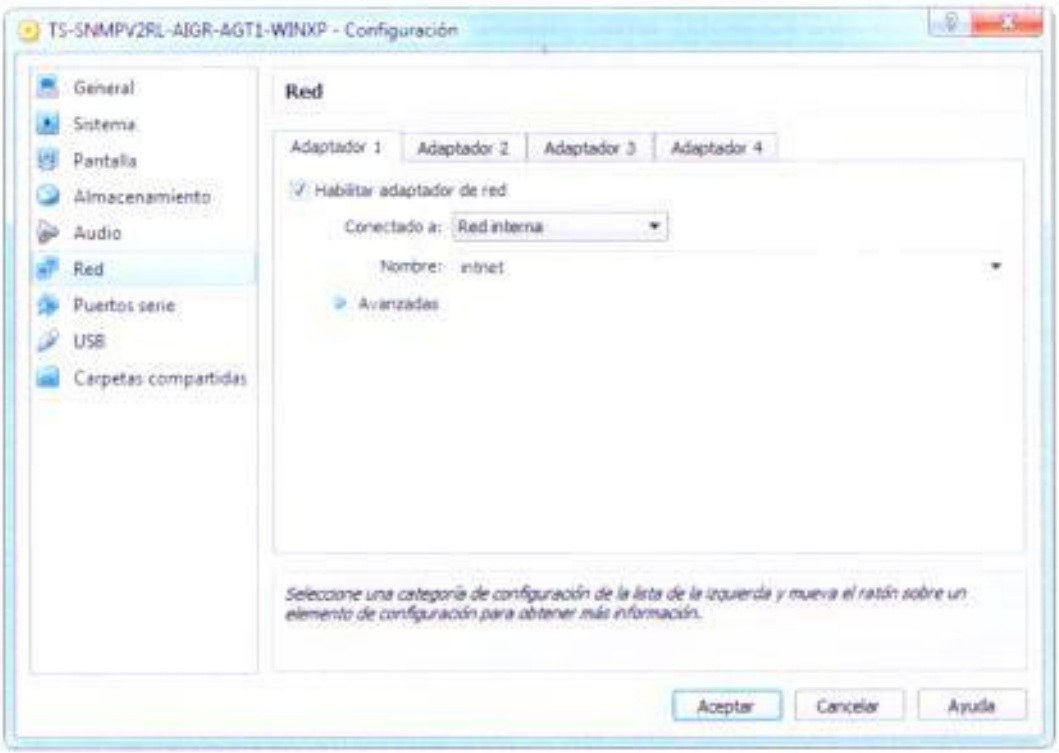


Figura 29.12 Configuración de Red de una máquina virtual

m) Con todo esto realizado, solo nos falta realizar la instalación del sistema operativo y ya podremos empezar a utilizar nuestra máquina virtual.

CLONACION DE MÁQUINAS VIRTUALES EN VIRTUALBOX

a) Como necesitamos varias máquinas virtuales, sobre la máquina virtual que vamos a clonar daremos click derecho y escogemos la opción Clonar, como podemos ver en la Fig. 3.13

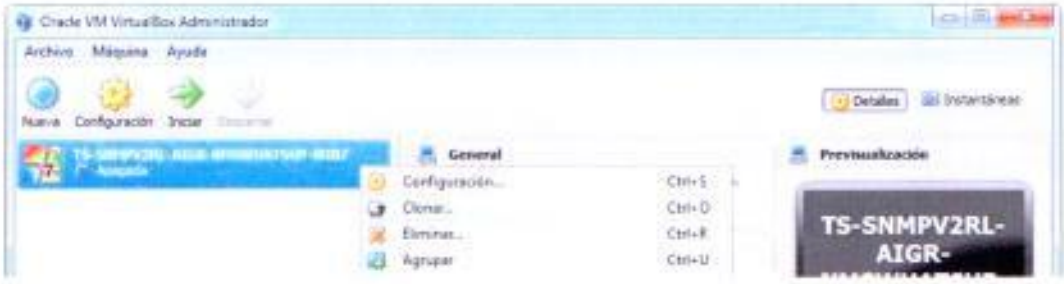


Figura 30.13 Opción Clonar de una máquina virtual

b) En la Fig. 3.14 vemos que se abrirá la pantalla para clonar máquina virtual, dentro se pondrá el Nombre de la nueva máquina y se pondrá visto en Reinicializar la dirección MAC de todas las tarjetas. Ahora damos NEXT.

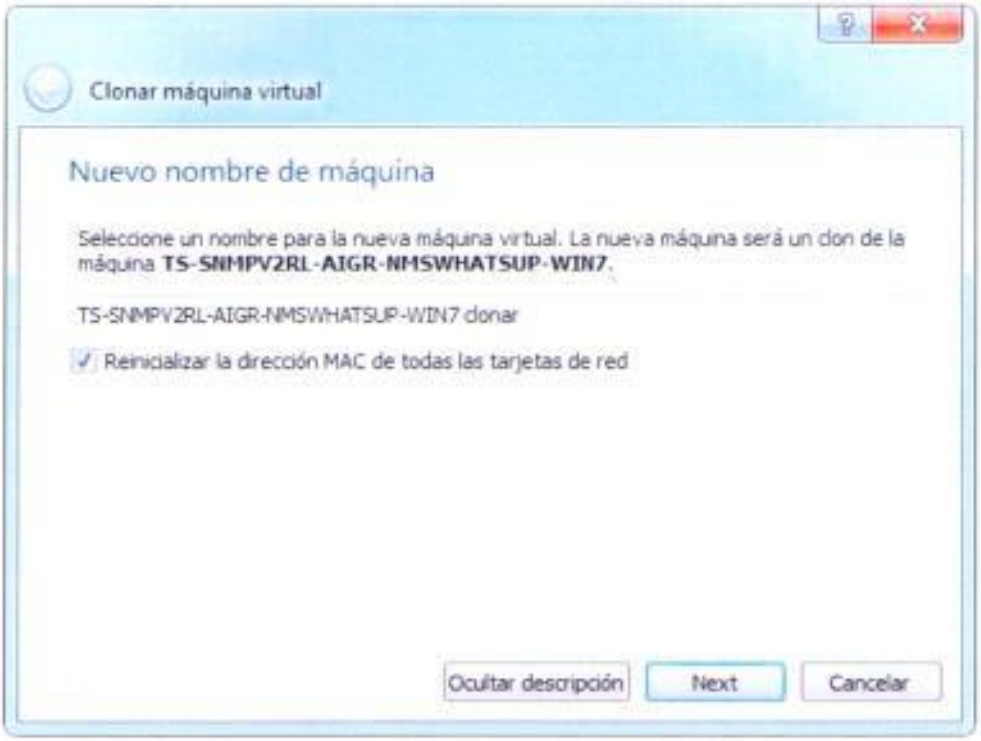


Figura 31.14 Nombre y Mac de la máquina virtual a Clonar

c) Luego en la Fig. 3.15 observamos que se nos preguntara por el tipo de clonación, a lo que dejamos la preestablecida que es Clonación completa y damos click en Clonar y una vez terminado el proceso ya tendremos una nueva máquina virtual que será una copia completa de la máquina que escogimos para clonar.

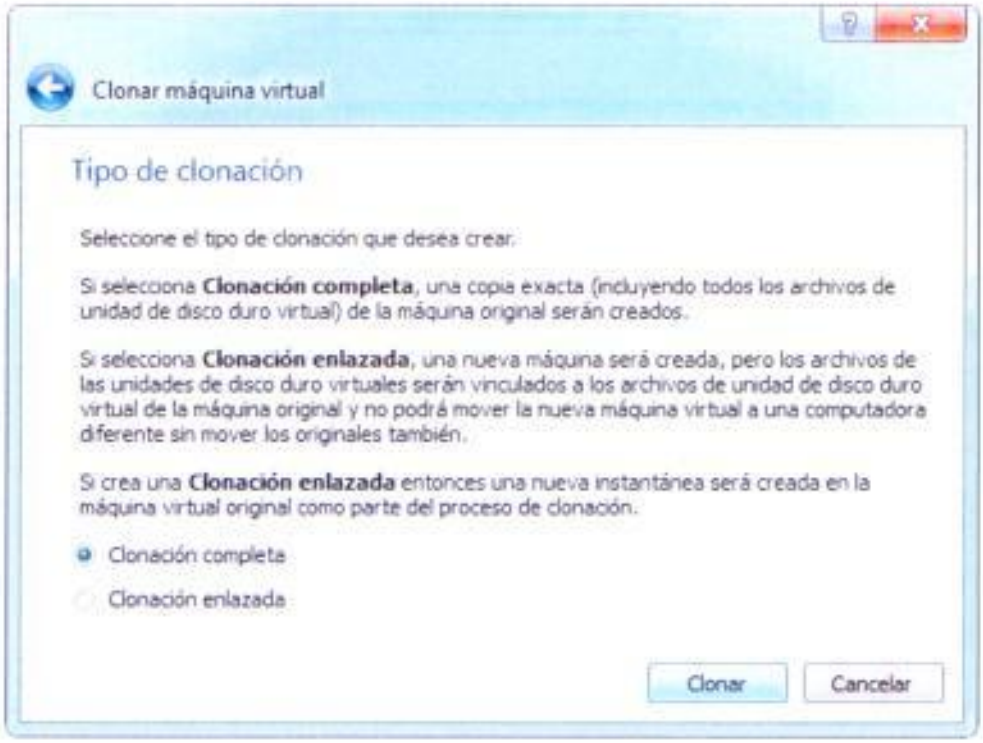


Figura 32.15 Selección del tipo de clonación de la máquina virtual

Una vez terminado este proceso ya dispondremos de las máquinas virtuales que necesitamos dentro de la red Lan.

3.3. SISTEMAS OPERATIVOS UTILIZADOS EN LA RED LAN

Entre los sistemas operativos existentes las máquinas virtuales manejaran Windows XP, Windows 7 y Windows 7 y Fedora 15 y Windows 7.

3.3.1. WINDOWS XP

Es un sistema operativo desarrollado por Microsoft, existen varias ediciones algunas creadas para ser usado en hogares, negocios, dispositivos portátiles y tablets estando disponibles para plataformas de 32 y 64 bits.

Posee varias características que lo posicionan como uno de los mejores sistemas operativos, una de ellas es disponer de un ambiente gráfico amigable, disponibilidad de conectar y desconectar dispositivos externos en caliente (dispositivo encendido), escritorio remoto para abrir una sesión desde otra computadora entre otras más aportadas desde versiones anteriores.

Algunos de los programas que deberemos tener instalados son: el agente SNMP, Mozilla Thunderbird y un Navegador Web.

3.3.1.1. AGENTE SNMP DE WINDOWS XP

WINDOWS XP no posee el servicio SNMP por defecto, por lo tanto será necesario que el usuario deba iniciar sesión como administrador, instalarlo

manualmente y proceder a la activación del servicio SNMP la cual se hace automáticamente después de la instalación.

ACTIVACION DE SNMP EN USUARIOS WINDOWS XP

a) Nos movemos a inicio y escogemos Panel de Control.
b) Luego escogeremos el icono para agregar o remover programas.
c) En el menú del lado izquierdo escogeremos la opción: Agregar o Remover componentes Windows.
d) En la Fig. 3.16, vemos que nos aparecerá un listado dentro del cual debemos seleccionar Herramientas de Administración Y Supervisión.

Figura 33.16 Asistente para componentes Windows

e) Una vez señalado damos click en el botón detalles que nos mostrara el contenido que también deberá estar señalado, como se ve en la Fig. 3.17.

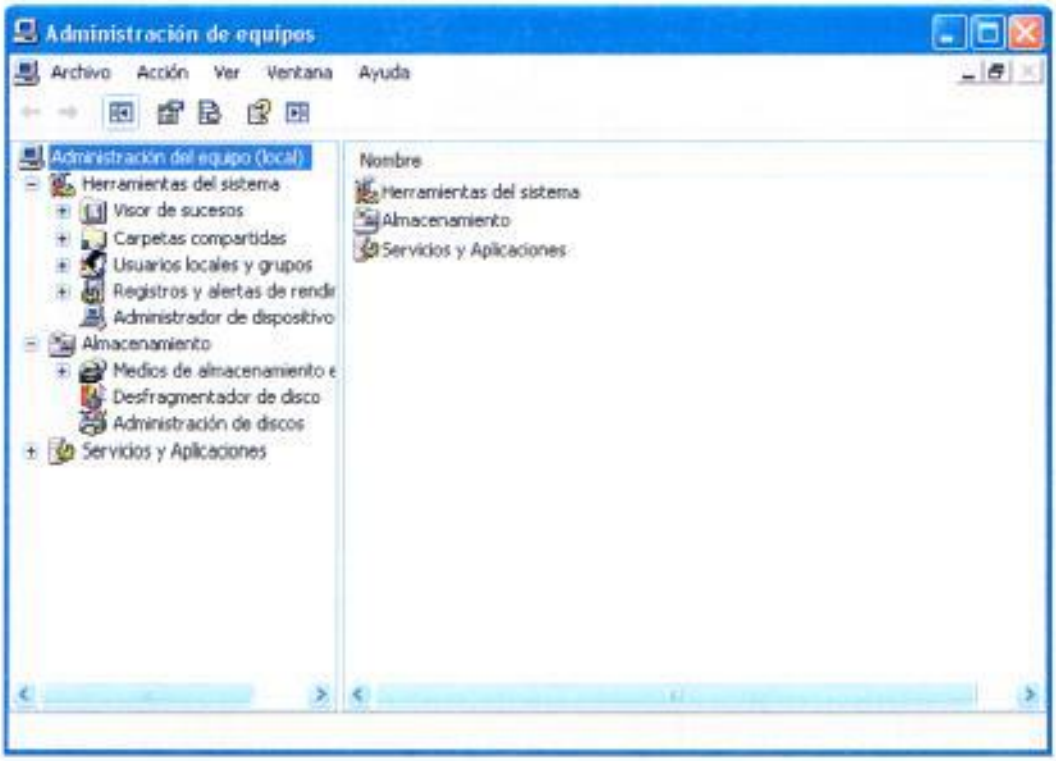
Figura 34.17 Subcomponentes de Herramientas de administración y supervisión

f) Damos Aceptar y una vez terminada la instalación damos FINISH.

g) Ahora ya tenemos disponible el servicio SNMP. La configuración de los parámetros lo haremos desde Panel de control y escogeremos el icono de Herramientas Administrativas.

h) Dentro escogeremos el icono Administración de Equipos.

i) Ahora tendremos dentro del cuadro Nombre tres opciones de las cuales escogeremos Servicios y



Aplicaciones, como se ve en la Fig. 3.18.

Figura 35.18 Ubicación de la opción Servicios y Aplicaciones

j) De igual forma como vemos en la Fig. 3.19, se muestra un listado y escogeremos la opción Servicios con lo que se nos mostrara un nuevo listado con todos los servicios que disponemos, dentro seleccionaremos Servicio SNMP.

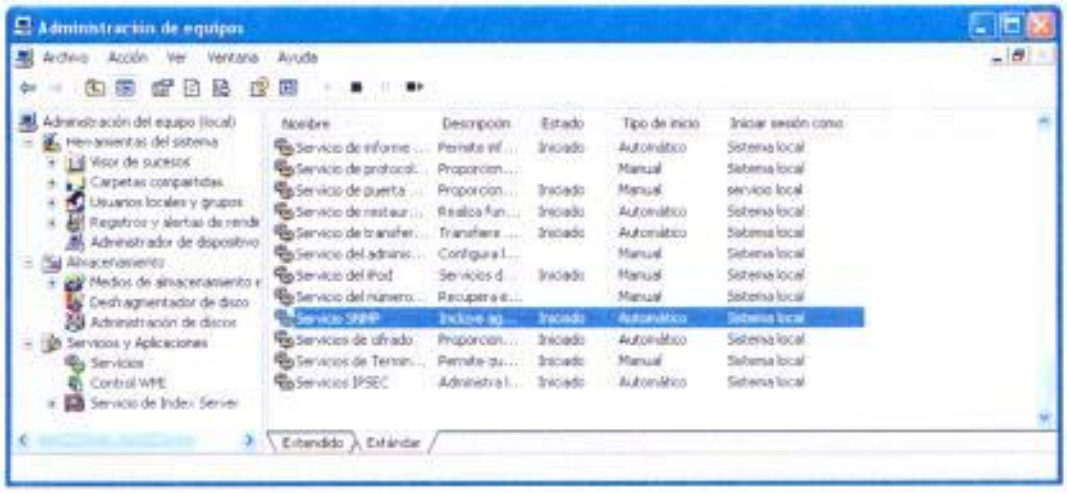


Figura 36.19 Ubicación del Servicio SNMP dentro se configura el Agente

k) En la Fig. 3.20 vemos que se nos mostrara un menú dentro del cual podremos configurar las credenciales SNMP escogiendo la pestaña Seguridad, dentro se ingresaran las credenciales

que necesitaremos dando click en Agregar para llenar la información de la comunidad y guardarla.

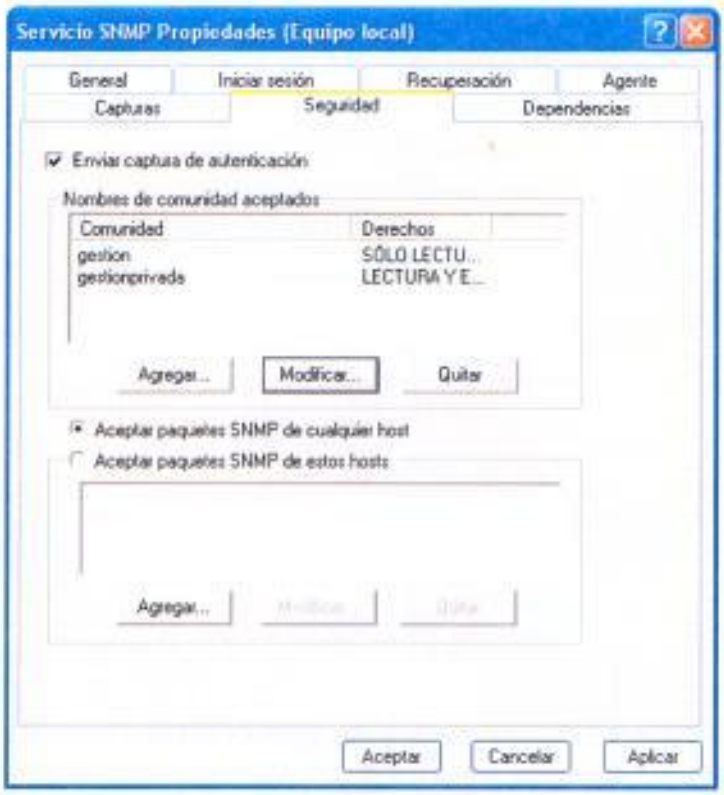


Figura 37.20 Propiedades del Servicio SNMP configuración de Seguridad

l) Una vez configuradas las credenciales para trabajar con SNMPv2, dentro de la pestaña Agente activaremos que recursos podrán ser vistos mediante la primitiva GET desde el gestionador.

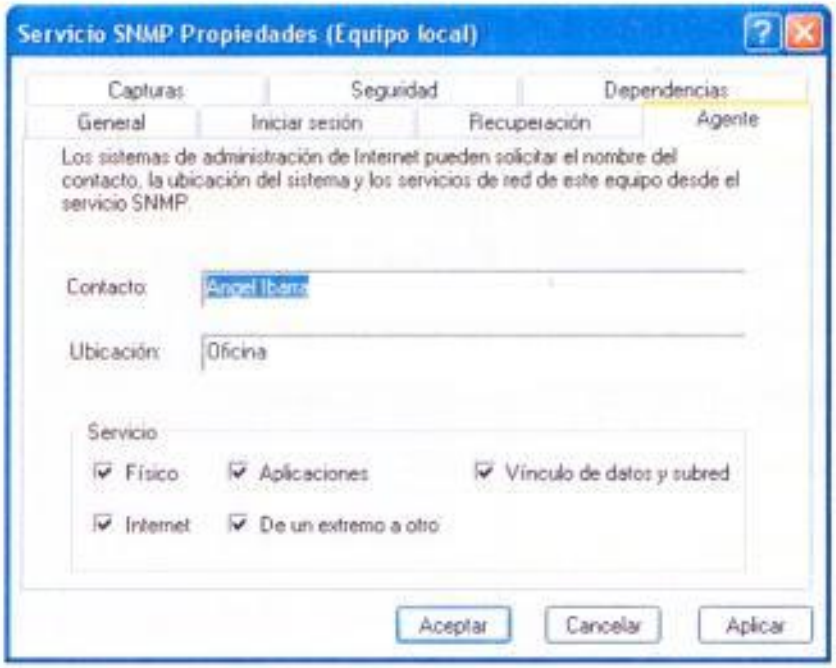


Figura 38.21 Propiedades del Servicio SNMP configuración de Agente

m) Con esto ya dispondremos de administración con SNMPv2 sobre este dispositivo.

3.3.1.2. MOZILLA THUNDERBIRD

Mozilla Thunderbird es un programa libre y gratuito, diseñado para el manejo de correo electrónico y soportado en múltiples sistemas operativos.

Se caracteriza por poder añadir contactos con un solo click, configuración automática de la cuenta de

correo con solo ingresar nombre, correo electrónico y contraseña, ser fácil para migrar gracias a su asistente de migración y otras ventajas más.

3.3.1.3. NAVEGADOR WEB

Se considera como Navegador web a los programas capaces de dar acceso a Internet, permitiendo tener acceso a múltiples contenidos como textos, imágenes, videos o contenido multimedia con lo que se conforman las páginas web.

Los contenidos se pueden encontrar almacenados dentro del mismo computador de donde se abre el navegador web, dentro de un dispositivo que forma parte de la red o dentro de un dispositivo conectado a Internet.

Entre los más conocidos podemos mencionar Internet Explorer, Mozilla Firefox y Google Chrome.

3.3.2. FEDORA 15

El sistema operativo Fedora 15 es un sistema operativogratuito basado en Linux, resaltando por estar considerado como un sistema estable. Se puede utilizar el

sistema operativo Fedora 15 o utilizarlo en conjunto en una partición diferente.

Algunas de las características por las cuales utilizar este sistema operativo son:

- Considerado totalmente un programa libre y de código abierto.
- Cuenta con aplicaciones de programa libre.
- Incluye SELinux para implementar una amplia variedad de políticas de seguridad.
- Distribución basada en RPM (RedHatPackage Manager) y respaldado por Red Hat.

Algunos de los programas que deberemos tener instalados son: el agente SNMP.

3.3.2.1. AGENTE SNMP EN FEDORA 15

Para disponer del servicio SNMP en Fedora 15 debemos tener instalado el paquete NET-SNMP

considerado como el programa cuyo grupo de aplicaciones nos permitirá implementar SNMP.

NET-SNMP por lo general está incluida en la mayoría de distribuciones Linux, cuyo grupo de aplicaciones permite la implementación y uso del protocolo SNMP en cualquiera de sus versiones. Está compuesta de módulos de Perl y Python, un agente SNMP, una librería y un grupo de líneas de comandos para las aplicaciones.

ACTIVACION DE SNMP EN USUARIOS LINUX

1. A diferencia de Windows que es considerado por poseer una interfaz amigable, en Fedora la activación se procede desde consola. Por lo que primero es necesario tener correctamente configurada las interfaces de red usando el

```
[root@localhost axib]# ifconfig p7p1
p7p1      Link encap:Ethernet  HWaddr 08:00:27:61:4A:F6
          inet addr:172.16.1.1  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe61:4af6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:4947 (4.8 KiB)
```

comando: ifconfig, como se ve en la Fig. 3.22

Figura 39.22 Información de interfaces de red

2. Una vez comprobado que tenemos conexión a la red, como vemos en la Fig. 3.23, procedemos a comprobar que se encuentre instalado el paquete correspondiente:

```
[root@localhost ~]# rpm -q net-snmp
net-snmp-5.6.1-7.fc15.i686
```

Figura 40.23 Consulta de paquete net-snmp

3. Como observamos en la Fig. 3.24, en caso de no poseer el paquete o de necesitar una actualización lo realizaremos con el siguiente comando: yum -y install net-snmp net-snmp-utils

```
[root@localhost ~]# yum -y install net-snmp net-snmp-utils
Loaded plugins: langpacks, presto, refresh-packagekit
Setting up Install Process
Package 1:net-snmp-5.6.1-7.fc15.i686 already installed and latest version
Package 1:net-snmp-utils-5.6.1-7.fc15.i686 already installed and latest version
Nothing to do
```

Figura 41.24 Instalación del paquete net-snmp net-snmp-utils

4. Realizada la verificación del paquete procederemos con la configuración la cual puede ser manual desde el archivo de configuración que

se encuentra en la ruta: /etc/snmp/snmpd.conf, como se ve en la Fig. 3.25

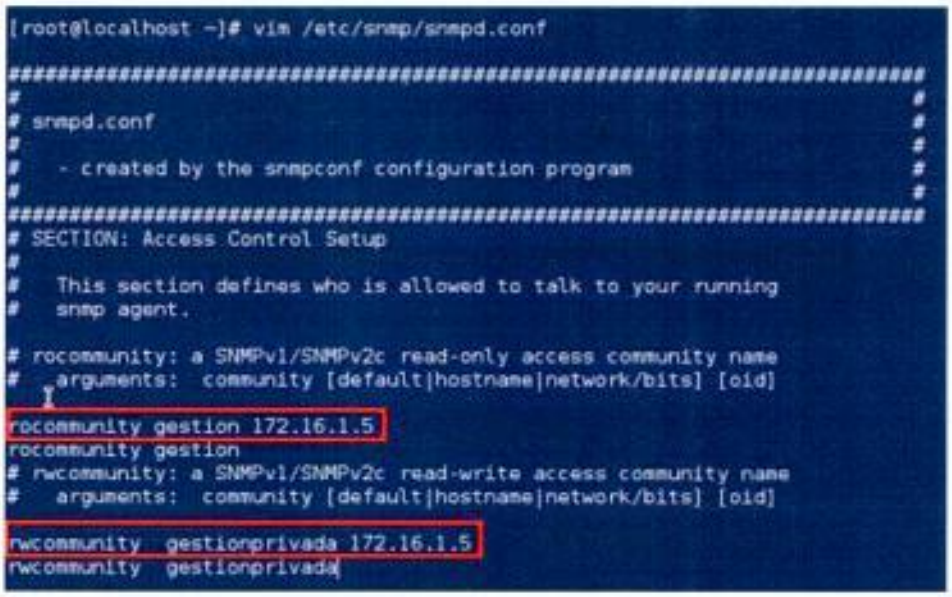


Figura 42.25 Comunidad de lectura (rocommunity) y de escritura (rwcommunity)

5. También podemos hacerlo ayudándonos del comando de SETUP con el comando: snmpconf –r none –g basic_setup, como vemos en la Fig. 3.26. Al inicio nos preguntara realizar cambios de información de la MIB, como no es de nuestro interés respondemos que no con "N".

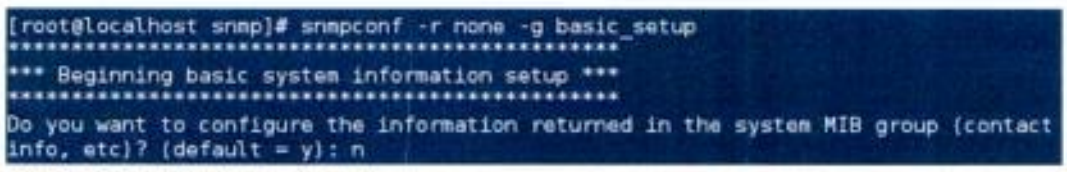


Figura 43.26 Configuración en la MIB

6. Lo primero que procederemos es a crear las comunidades para el dispositivo, de las permitidas nos interesa SNMPv2.
7. Llamaremos "gestion" a la comunidad de lectura y "gestionprivada" a la comunidad de escritura. Vamos a colocarlas apuntando a la dirección IP del Gestor, como se ve en la Fig. 3.27

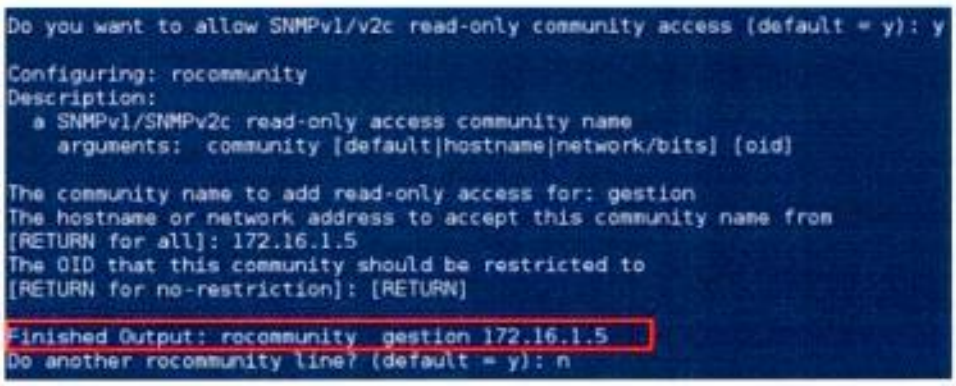


Figura 44.27 Configuración de SNMPv2 comunidades

8. Con esto ya tendremos comunicación con el protocolo SNMPv2, luego se nos preguntara para monitorear algunos de los recursos de nuestra máquina. A lo que daremos la opción "Y"; el primero en configurarse será el monitoreo de los procesos, que al dar Enter se guardaran las

configuraciones por defecto, como se observa en la Fig. 3.28.

```
****************************************
*** Beginning monitoring setup ***
****************************************
Do you want to configure the agent's ability to monitor various aspects of your
system? (default = y): y
Do you want to configure the agents ability to monitor processes? (default = y): y

Configuring: proc
Description:
  Check for processes that should be running.
      proc NAME [MAX=0] [MIN=0]
Name of the process you want to check on:
Maximum number of processes named '' that should be running [default = 0]:
Minimum number of processes named '' that should be running [default = 0]:

Finished Output: proc
Do another proc line? (default = y): n
```

Figura 45.28 Configuración de Procesos con SNMPv2

9. Luego como vemos en la Fig. 3.29, pasamos a la configuración del monitoreo del espacio de disco, colocamos "Y" y aceptamos las configuraciones pro defecto.

```
Do you want to configure the agents ability to monitor disk space? (default = y): y

Configuring: disk
Description:
  Check for disk space usage of a partition.
    |
Enter the mount point for the disk partion to be checked on:
Enter the minimum amount of space that should be available on :

Finished Output: disk
Do another disk line? (default = y): n
```

Figura 46.29 Configuración de Espacio en Discos con SNMPv2

10. De igual forma veremos en la Fig. 3.30, que avanzamos ahora a la configuración del promedio

de carga, colocamos los valores recomendados para continuar.

```
Do you want to configure the agents ability to monitor load average? (default = y): y

Configuring: load
Description:
  Check for unreasonable load average values.
    Watch the load average levels on the machine.

     load [1MAX=12.0] [5MAX=12.0] [15MAX=12.0]

Enter the maximum allowable value for the 1 minute load average: 12.0
Enter the maximum allowable value for the 5 minute load average: 12.0
Enter the maximum allowable value for the 15 minute load average: 12.0

Finished Output: load  12.0 12.0 12.0
Do another load line? (default = y): n
```

Figura 47.30 Configuración del Promedio de Carga con SNMPv2

11. Y por último en la Fig. 3.31 vemos que se nos permite configurar el monitoreo de tamaño de archivos (desde aquí podremos monitorear cualquier archivo en especifico que deseemos), el cual por defecto vera los principales directores y sin límite de tamaño. Luego ponemos "n" y terminamos con la ayuda.

```
Do you want to configure the agents ability to monitor file sizes? (default = y): y

Configuring: file
Description:
  Check on the size of a file.
    Display a files size statistics.
    If it grows to be too large, report an error about it.
    |
Enter the path to the file you wish to monitor:
Enter the maximum size (in kilobytes) allowable for :

Finished Output: file
Do another file line? (default = y): n
```

Figura 48.31 Configuración de un Archivo con SNMPv2

12. Al final nos deberá quedara el archivo con la configuración realizada, como vemos en la Fig. 3.32.

```
##############################################################################
# SECTION: Monitor Various Aspects of the Running Host
#   The following check up on various aspects of a host.

# proc: Check for processes that should be running.
#     proc NAME [MAX=0] [MIN=0]

proc

# disk: Check for disk space usage of a partition.
#   The agent can check the amount of available disk space, and make
#   sure it is above a set limit.
#    disk PATH [MIN=100000]

disk

# load: Check for unreasonable load average values.
#   Watch the load average levels on the machine.
#    load [1MAX=12.0] [5MAX=12.0] [15MAX=12.0]

load  12.0 12.0 12.0

# file: Check on the size of a file.
#   Display a files size statistics.
#   If it grows to be too large, report an error about it.

file
```

Figura 49.32 Archivo snmpd.conf con todas las configuraciones SNMPv2

3.3.3. WINDOWS 7

Considerado como una actualización a su antecesor Windows Vista, se logro mantener compatibilidad con aplicaciones y hardware a los que su antecesor ya era compatible. De igual manera es una versión diseñada en varias ediciones para ser

usadas en hogares, negocios, dispositivos portátiles y tablets estando disponibles para plataformas de 32 y 64 bits.

Entre las metas de esta nueva versión se pretende mejorar la interfaz logrando ser más accesible al usuario de forma fácil y en menos tiempo. Algunas de las otras características que se intento lograr con esta versión son soporte de los discos duros virtuales, mejora en rendimiento de arranque, soporte a sistemas que usen múltiples tarjetas gráficas de distintas marcas.

A continuación describimos los programas que deberemos tener instalados:

3.3.3.1. AGENTE SNMP EN WINDOWS 7

Para poder configurar SNMP en WINDOWS 7 deberemos encontrarnos dentro del usuario administrador y proceder con la instalación manual (debido a que no lo trae activado por defecto) una vez que está instalado por lo general se activa automáticamente.

Por disponer de una interfaz amigable y ser una versión con amplias ediciones, la elegimos para que albergue el programa con el cual realizaremos la Gestión de la Red.

ACTIVACION DE SNMP EN USUARIOS WINDOWS 7

Para proceder con la gestión es necesario que el gestionador y los agentes deban tener activados el servicio SNMP para poder transmitir la información entre estos dispositivos, lo que incluiría información de CPU (Central Processing Unit), uso de Memoria RAM o algo más crítico como el estado de red de un dispositivo que proporcione algún servicio a la red.

1. Nos moveremos a Inicio y escogeremos Panel de Control.
2. Dentro de este escogeremos el icono Programas y Caracteristicas.
3. Del menú del lado izquierdo escogemos la opción Activar O Desactivar las Caracteristicas de Windows.

4. Se nos mostrara un cuadro donde activaremos la opción correspondiente a SNMP y daremos click en Aceptar, como se ve en la Fig. 3.33.

Figura 50.33 Pantalla de activación y desactivación de componentes de Windows 7

5. Volvemos a abrir Panel de Control, dentro escogeremos el icono Herramientas Administrativas.
6. De los iconos que aparecen nos interesa abrir Administración de Equipos, ingresamos a Servicios y Aplicaciones y dentro escogemos el icono Servicios.

7. De todos los servicios listados, buscamos el que diga Servicio SNMP y lo abrimos.
8. Dentro tendremos las pestañas Seguridad sobre la cual crearemos las comunidades SNMPv2 y la pestaña Agente donde validaremos la información del dispositivo que deseamos que sea visible.
9. Y ya con esto tendremos configurado SNMP en nuestro dispositivo Gestionador.

3.3.3.2. WHATSUP GOLD PREMIUM EDITION v16

De entre los programas existentes en el mercado para Gestionar la Red, WHATSUP GOLD ha llegado a ser implementado en Centros de Datos de distintos países, siendo una solución confiable y segura que nos ofrece libertad de uso, escalable y ampliable.

El alcance que tiene sobre las redes puede ir desde pequeñas hasta empresas grandes, disponiendo de una red confiable y visible las 24 horas y los 7 días de la semana.

WHATSUP GOLD nos permitirá realizar Gestión con SNMP de nuestra red sin muchas complicaciones

permitiendo tener una completa cobertura de los dispositivos y aplicaciones que la integran.

Mediante el uso de Gestión con SNMP disponemos de información necesaria para comprender el comportamiento de algunos de los recursos principales de los dispositivos o aplicaciones.

REQUISITOS MINIMOS PARA LA INSTALACION DE WHATSUP GOLD

Para poder proceder con la instalación del programa antes deberemos revisar que la máquina virtual cumpla con los requisitos, estos son:

- Procesador de doble núcleo.
- 2GHz de velocidad del procesador.
- Microsoft Windows Server 2003/Windows Server 2008/Windows Vista/ Windows 7
- 2GB de memoria RAM.
- 2GB mínimo de espacio en disco duro.
- 100 Mbps en la tarjeta de interfaz de red.

INSTALACION DE WHATSUP GOLD

Una vez que confirmamos los requisitos del programa con la máquina virtual procedemos a instalar el programa WhatsUp Gold:

1) Procedemos a descargar el programa del sitio web www.whatsupgold.com, una vez terminada la descarga le damos doble click sobre el instalador para proceder con la instalación.
2) Nos mostrara una primera página de Welcome sobre la cual daremos click en la opción NEXT.
3) En nuestro caso primero nos preguntara si deseamos proceder debido a que nos recomienda utilizar Windows Server Y 4Gb de RAM, de todas maneras procedemos con la instalación como vemos en la Fig. 3.34.

Figura 51.34 Recomendación de asignar 4GB de memoria RAM

4) Ahora nos mostrara una página sobre la cual deberemos Aceptar los términos de licencia del programa y dar click en NEXT.
5) Luego nos mostrara una página sobre la cual nos indicara que se procederá con la instalación del programa Microsoft SQL Server 2008 R2 Express Edition que es el que manejara la base de datos, y damos click en el botón NEXT.
6) Ahora nos indicara en que ruta se instalaraSQL Server, sobre la cual no realizamos cambios y damos click en el botón NEXT.

7) En la Fig. 3.35 vemos que es muy importante, debido que aquí se creara el usuario y clave de administrador para SQL Server que deberá cumplir con los requisitos mínimos de seguridad, para el manejo de la base de datos. Una vez creadas las credenciales damos click en NEXT.

Figura 52.35 Configuración de credenciales para la administración de SQL Server

8) Una vez creadas los permisos de administrador, ahora nos solicitara crear los permisos para ingresar a la base de datos dándonos el usuario WhatsUpGold_ANGEL-PC e ingresamos un password y continuamos dando click en NEXT.

9) Ahora nos pedirá escoger una dirección IP sobre la cual utilizaremos para remotamente poder acceder a la aplicación Web de Whatsup Gold.

10) En esta siguiente pagina nos pedirá en que ruta realizar la instalación del programa WhatsUp Gold la cual dejaremos por defecto.

11) Ahora se mostrará en la Fig. 3.36, donde se nos indica mediante que puerto se nos permitirá comunicar con el servidor Web, el cual nos permitirá acceder desde fuera del equipo y poder revisar el estado de nuestros dispositivos. Lo dejaremos en la opción recomendada: puerto 80 (esto puede variar conforme a la disponibilidad del puerto) y daremos click en NEXT.

Figura 53.36 Confirmación de mantener el puerto 80

Notar que el mensaje solo indica sobre el cambio realizado y no representara problema alguno.

12) Ahora ya nos pedirá confirmar todo lo realizado hasta ahora y dará comienzo a la instalación.

13) Deberá instalarse todo sin problemas y se finaliza la instalación.

AGREGAR DISPOSITIVOS EN WHATSUP GOLD

1) Primero vamos a Inicio y damos doble click sobre el programa Whatsup Gold AdminConsole, como se ve en la Fig. 3.37

Figura 54.37 Icono para abrir programa Whatsup Gold

2) Una vez abierto el programa, en el menú principal elegiremos la opción Tool y damos click sobre la primera opción llamada DiscoverDevices.

3) Se nos abrirá una nueva ventana, en la Fig. 3.38 vemos dentro del menú izquierdo seleccionaremos ScanSettings, escogeremos en ScanType la opción IP RangeScan así se nos permitirá colocar el rango de direcciones IP que vamos a escanear. Una vez ingresada las direcciones IP de comienzo y fin damos click sobre el botón Start a Discovery Session.

Figura 55.38 Herramienta DiscoverDevices de Whatsup Gold

4) Al completar el proceso de escaneo, en la Fig 3.39 veremos los dispositivos que forman parte de nuestra red. Al señalar sobre cada uno en

"DeviceInformation" podremos observar la información de los dispositivos.

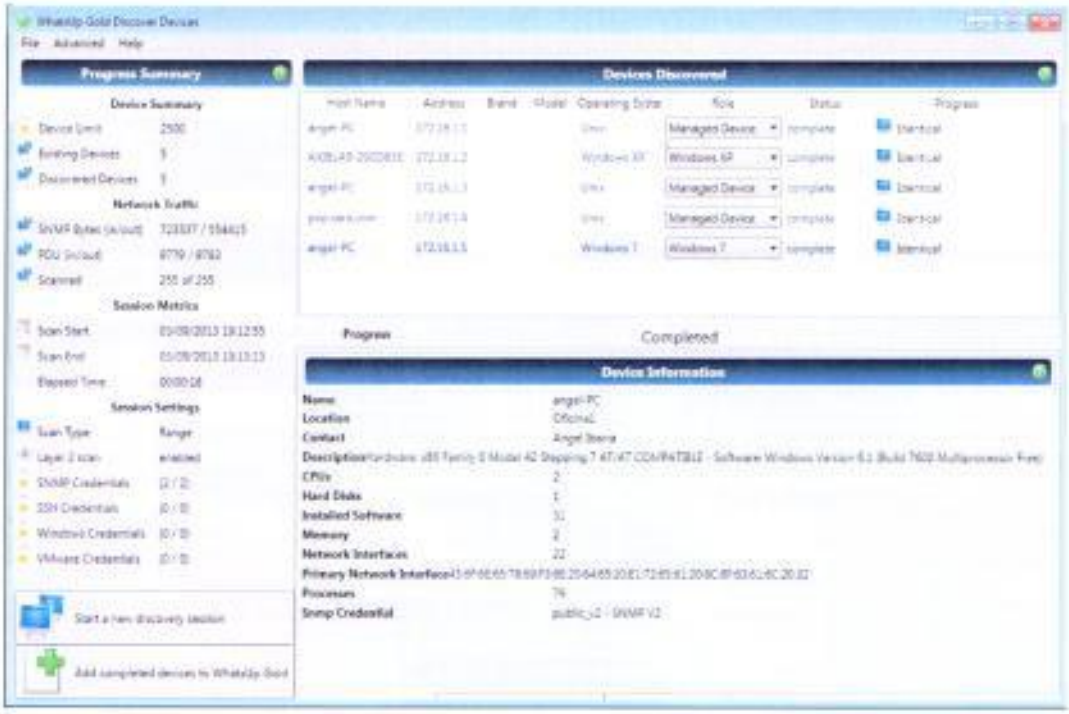


Figura 56.39 Dispositivos encontrados en la red 172.16.1.0/24

5) Finalmente necesitamos guardar lo realizado dando click en AddCompletedDevices to Whatsup Gold, en la Fig. 3.40 nos permitirá seleccionar los dispositivos que deseamos agregar a los ya existentes en el Whatsup Gold. Seleccionamos y damos click sobre el botón AddDevices to Whatsup Gold.

Figura 57.40 Dispositivos que deseamos agregar

3.3.3.3. WIRESHARK

Figura 58.41 Logo de Wireshark

Al disponer de WIRESHARK obtendremos un excelente analizador de protocolos para realizar análisis de la red y poder comprender la información de los paquetes de datos.

WIRESHARK es un programa libre, siendo accesible a administradores de redes, ingenieros, desarrolladores y estudiantes de redes disponible para la mayoría de los sistemas operativos.

Entre las características principales están poseer una interfaz flexible, captura de datos de la red, capaz de lograr gran filtrado, compatibilidad con varios protocolos, entre otras más.

Debido a que WIRESHARK realiza la captura de los paquetes desde la interfaz de red de la computadora se debe ejecutar con permisos de Administrador.

CAPITULO 4

DISEÑO DE ESCENARIOS PARA LA SIMULACION DE UNA RED LAN POR SNMPV2 CON WHATSUP GOLD Y MAQUINAS VIRTUALES

En este capítulo vamos a describir nuestro diseño de escenarios, orientando su distribución al desarrollo y crecimiento del recurso humano y sus principales necesidades de servicios.

Empezamos formulándonos varias preguntas, lo cual nos permitió darnos cuenta que debemos concentrarnos en los distintos ambientes sobre los que encontraremos implementado redes Lan, como: escuelas, casas, edificios, oficinas, empresas, centros comerciales, etc. Dada la importancia que tiene

el uso de servidores en una red Lan, nuestro objetivo estará dirigido al uso de servidores en empresas.

4.1. ESCENARIOS

Teniendo ya definido que nuestros escenarios van a desarrollarse en un ambiente de empresa, sabemos que tanto la empresa y su personal deberán ir creciendo en conocimiento, funciones y metas para volverse más robusta y prospera. Para lo cual la empresa al proporcionar un producto o servicio deberán contar con las herramientas necesarias para lograrlo.

Una de estas herramientas es el manejo de máquinas o computadores que estén comunicados mediante una red Lan. Estos trabajaran mejor mostrando un rendimiento de sus recursos eficiente bajo las instrucciones, enseñanzas y direcciones del Gestionador que administrará los dispositivos que formen parte de la red Lan.

Disponemos de una gran variedad de dispositivos que deberemos mantener gestionados, de estos dispositivos nos enfocaremos en aquellos que son administrados por el usuario y aquellos destinados a brindar servicios para los usuarios.

Debemos tener en cuenta que los dispositivos dentro de la red Lan deberán estar en capacidad de brindar gran calidad de servicio y escalabilidad, en base a estos fundamentos implementaremos en nuestros escenarios parámetros con los que demostraremos el actuar de las primitivas SNMPv2.

Como nuestro proyecto está orientado a desarrollarse sobre una estructura de simulación, utilizaremos máquinas virtuales. Al estar las máquinas virtuales sobre un programa como VIRTUALBOX los recursos de CPU, Memoria RAM, Red y Almacenamiento de la máquina virtual se reflejaran en el GESTOR mediante las primitivas del protocolo SNMPv2: GET REQUEST, GET NEXT REQUEST o GET BULK REQUEST.

Nuestros escenarios estarán divididos en función de representar a las pequeñas, medianas y grandes empresas dado que el crecimiento tanto de las empresas como el de las redes es heterogéneo.

4.1.1. ESCENARIO 1

La red LAN implementada en este escenario va dirigida a solventar las necesidades del usuario llamadas técnicamente servicios, que tendrían que ser satisfechas dentro de una red dirigida para las pequeñas empresas.

Por lo que en este primer escenario resolveremos uno de los primeros problemas a presentarse como lo es la necesidad de poder compartir los archivos que se manejan internamente.

El desarrollo de la red LAN consta de los elementos que son: el usuario, un servidor de archivos y el gestor. Estos trabajaran con los siguientes sistemas operativos:

- WINDOWS XP como usuario.
- FEDORA15 como servidor de archivos.
- WINDOWS 7 como gestor.

Con WINDOWS XP representaremos al usuario que hará uso del servicio, que como agente podrá ser gestionado.

Con FEDORA 15 como servidor de archivos disponemos del servicio de almacenamiento de archivos; mediante el cual, siendo el primer servicio gestionado luego nos daremos cuenta que la gestión es similar con los otros servicios que se implementaran en los otros escenarios.

El servidor de archivos proporciona a la red el servicio SMB el cual se obtiene teniendo instalado el paquete SAMBA que es el que permite a los sistemas operativos Fedora poder proporcionar la administración, almacenamiento y configuración de los archivos almacenados.

Con WINDOWS 7 representaremos al dispositivo Gestionador. Debido al papel que desarrolla sobre la red LAN será un dispositivo más robusto en comparación que el de los usuarios y deberá estar en la capacidad de soportar el Programa con el cual podremos realizar gestión a todos los equipos pertenecientes en la red LAN.

Todos los equipos se manejan con el modelo TCP/IP para la comunicación entre ellos, y a la red formada se le asignara la siguiente subred: 172.16.1.0/24 dentro de la cual estarán asignadas:

- WINDOWS XP: 172.16.1.2/24
- Servidor de archivos: 172.16.1.3/24
- WINDOWS 7: 172.16.1.5/24

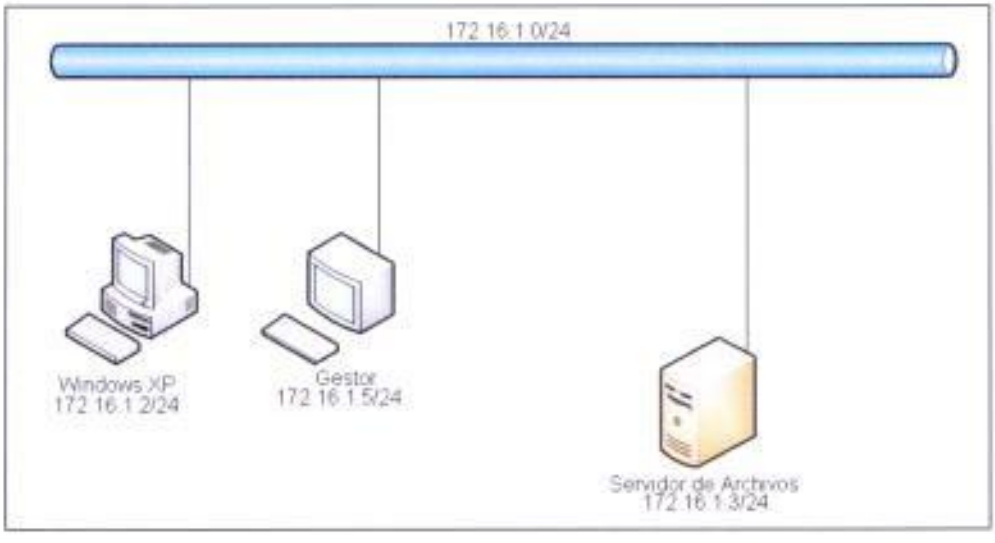


Figura 59.1 Diagrama Escenario 1

De los dispositivos mencionados podremos apreciar la cantidad de recursos que fueron asignados a cada uno de ellos en las gráficas adjuntas:

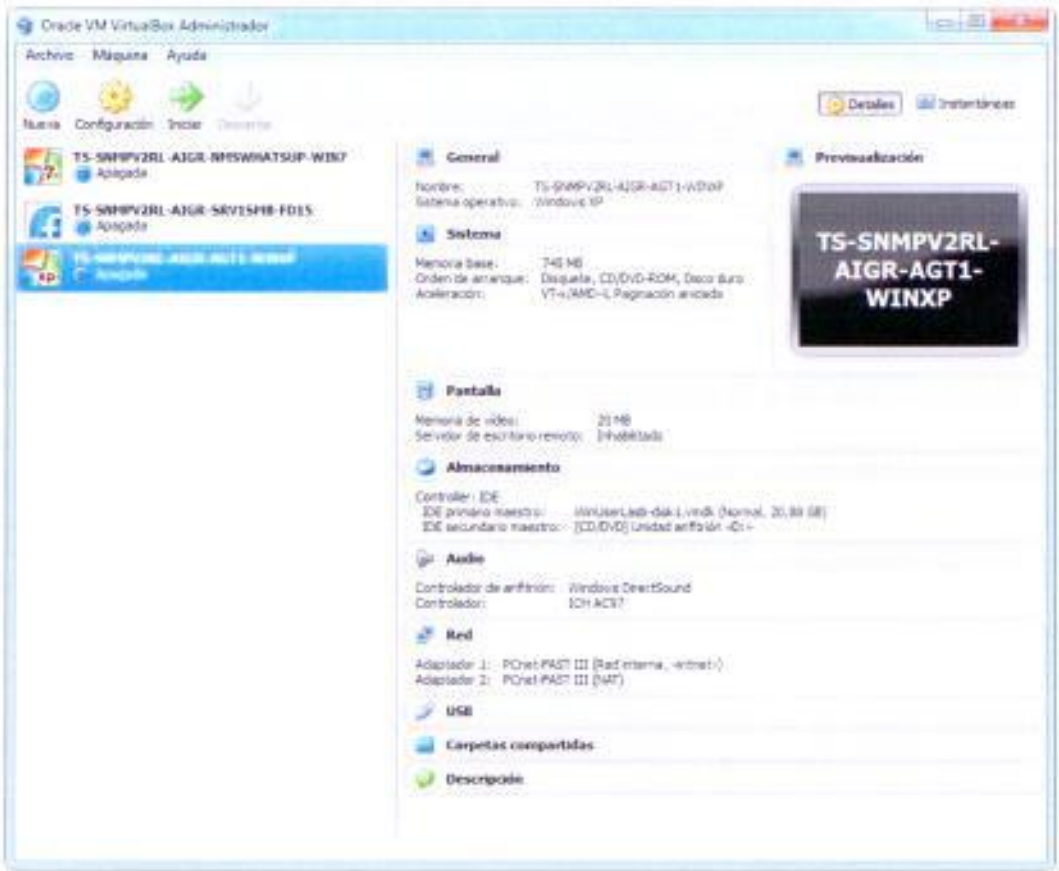


Figura 60.2 Características del dispositivo WINDOWS XP

La máquina de nombre: TS-SNMPV2-AIGR-AGT1-WINXP representa a los usuarios por lo que se le asigno las siguientes características:

- S.O.: WINDOWS XP
- 745 MB de memoria RAM
- 20 GB de espacio de disco duro.

Por el momento en este escenario no es necesario asignar gran cantidad de recursos a la máquina del usuario.

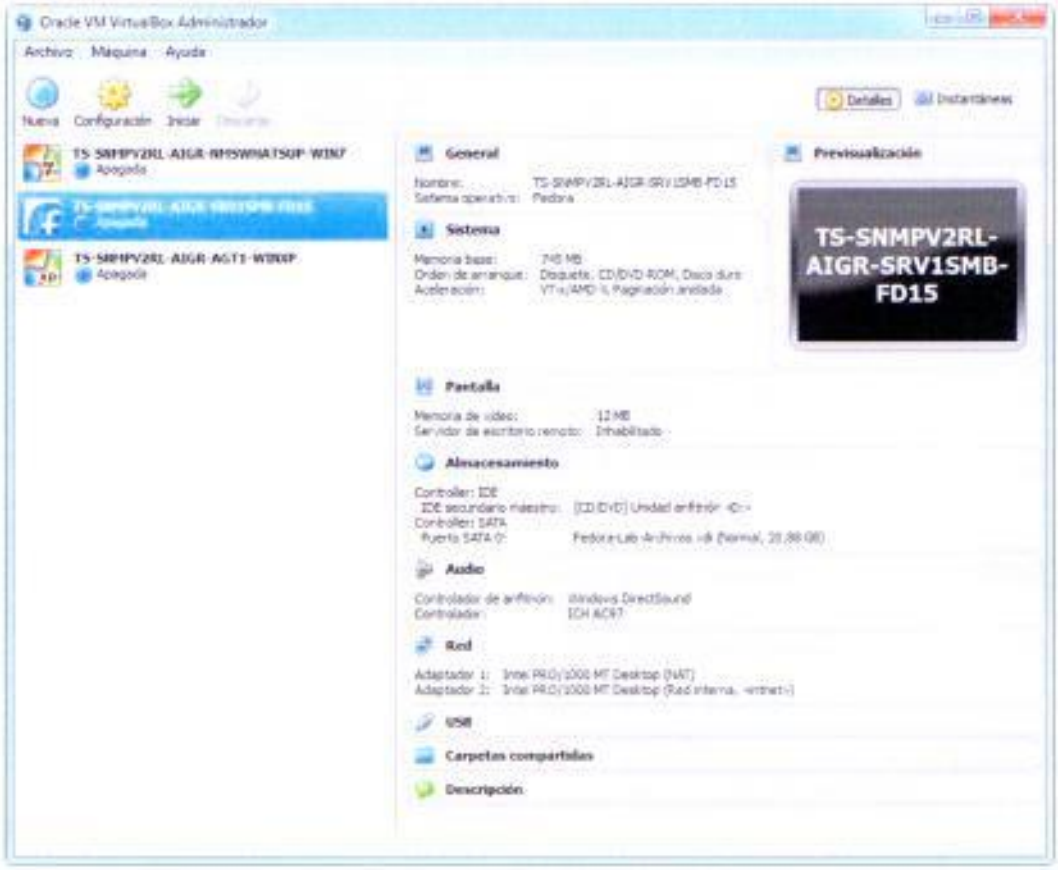


Figura 61.3 Características del Servidor de Archivos en FEDORA 15

La máquina de nombre: TS-SNMPV2-AIGR-SRV1SMB-FD15 alojara al Servidor de archivos por lo que se le asigno las siguientes características:

- S.O.: FEDORA 15
- 745 MB de memoria RAM
- 20 GB de espacio de disco duro.

Recibirá esta cantidad de recursos con la cual debemos tomar en cuenta la capacidad de disco duro debido a que el almacenamiento de archivos podrá crecer y su asignación estimará este evento.

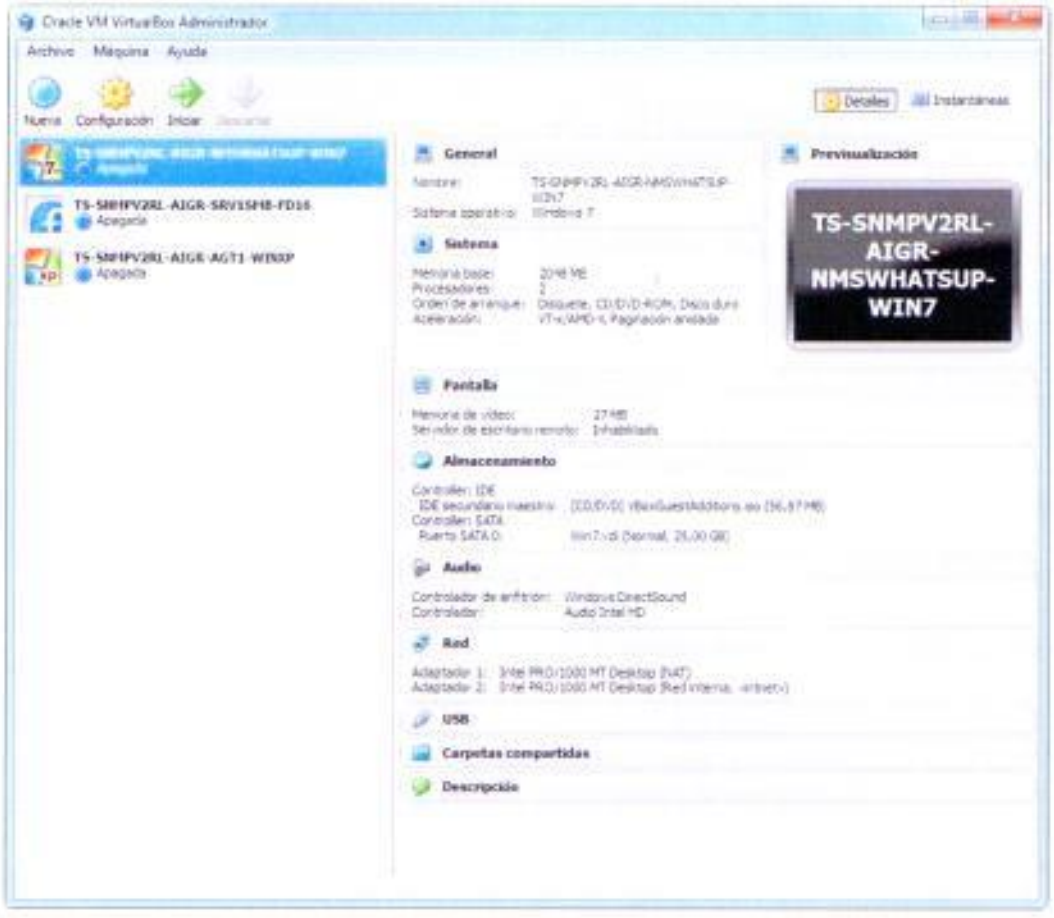


Figura 62.4 Características del dispositivo WINDOWS 7

La máquina de nombre: TS-SNMPV2-AIGR-NMSWHATSUP-WIN7 alojará al Gestor por lo que se le asignó las siguientes características:

- Procesador doble núcleo.
- S.O.: WINDOWS 7
- 2048 MB de memoria RAM
- 25 GB de espacio de disco duro.

Será más robusta en comparación a las otras porque instalaremos el programa Gestor.En nuestro caso el Gestor será WhatsUp Gold Premium Edition v16 que incluye un programa adicional para la administración de la base de datos.

4.1.2. ESCENARIO 2

Dentro de este escenario vamos a experimentar un crecimiento del recurso humano y nos conduce a tener que proporcionar un medio de comunicación entre los usuarios de la red Lan.

En el escenario 2 vamos a agregar un servidor de correos a la red Lan creada en el escenario 1, que logrará satisfacer la comunicación dentro de una red dirigida para las medianas empresas.

Con WINDOWS XP de igual manera que en el escenario 1, vamos a representar al grupo de usuarios los cuales serán más y son los que dispondrán tanto de los servicios del servidor de archivos y del servidor de correos.

El servidor de correos nos proporciona los servicios POP y SENDMAIL los cuales ya se encuentran incluidos en el sistema operativo FEDORA 15. Nos permitirá enviar y recibir

correos entre todos los usuarios que forman parte de la red Lan, teniendo la capacidad de administración, almacenamiento y configuración de los correos que serán manejados y a su vez respaldados o almacenados dentro del servidor.

Ahora disponemos de 4 dispositivos que formaran nuestro escenario, la subred será la misma y las IPs asignadas son las siguientes:

- WINDOWS XP: 172.16.1.2/24
- Servidor de archivos: 172.16.1.3/24
- Servidor de Correos: 172.16.1.4/24
- WINDOWS 7: 172.16.1.5/24

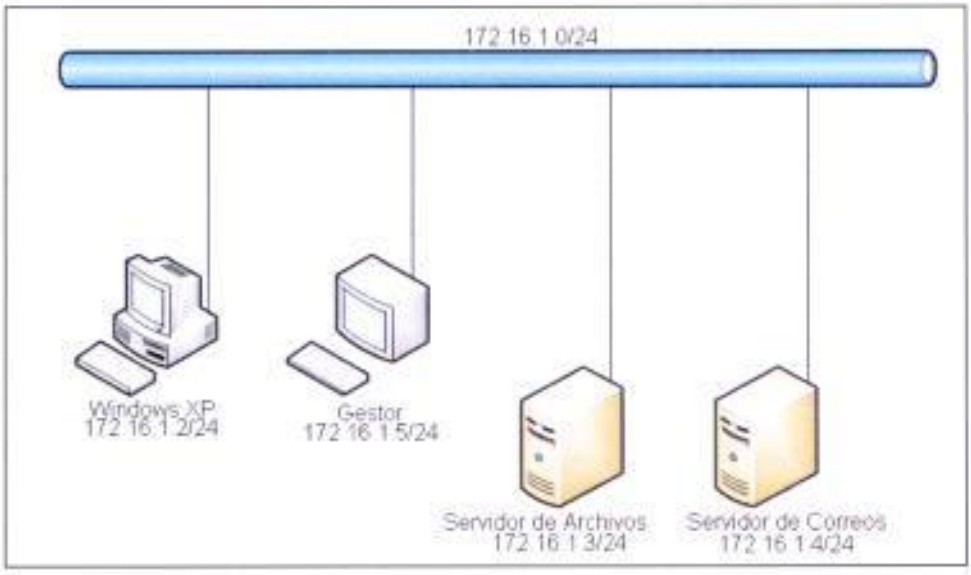


Figura 63.5 Diagrama Escenario 2

De los dispositivos mencionados vamos ahora a incluir el Servidor de correos, los recursos que fueron asignados al nuevo servidor se aprecian en la figura 4.6.

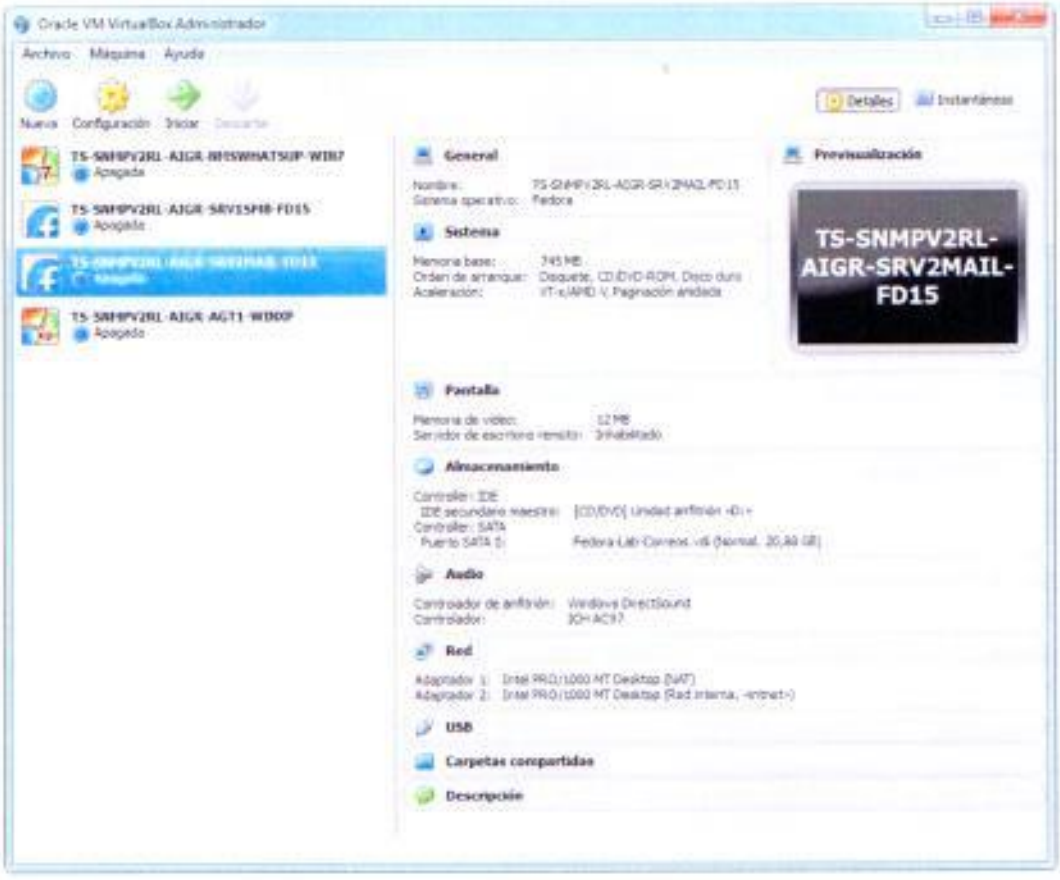


Figura 64.6 Características del Servidor de Correos en FEDORA 15.

4.1.3. ESCENARIO 3

En el escenario 3, debido a que la mediana empresa la convertiremos en una empresa grande la cantidad de

usuarios es mucho mayor que las anteriores, por lo que no es suficiente la comunicación entre usuarios.

Lo resolvemos al incluir el servicio de páginas web con las cuales los oficinistas, técnicos u otros usuarios podrán informarse de noticias, roles de pago, formatos de solicitudes de la empresa, e incluso presentar quejas o comentarios.

El escenario 3 será formado adicionando un Servidor Web (alojara las páginas web o Intranet) al escenario 2. La implementación de un servidor Web nos proporciona el servicio HTTPD con lo que seremos capaces de disponer de páginas web (almacenadas dentro del servidor Web), cuyo acceso será solo para la red Lan de la empresa; también se dispondrá del servicio NAMED dado por un servidor de DNS, que estará implementado dentro del Servidor Web.

Ahora disponemos de 5 dispositivos que forman parte de nuestro escenario, la subred será la misma y las IPs asignadas son las siguientes:

- WINDOWS XP: 172.16.1.2/24
- Servidor de archivos: 172.16.1.3/24
- Servidor de Correos: 172.16.1.4/24

- Servidor Web:172.16.1.1/24
- WINDOWS 7: 172.16.1.5/24

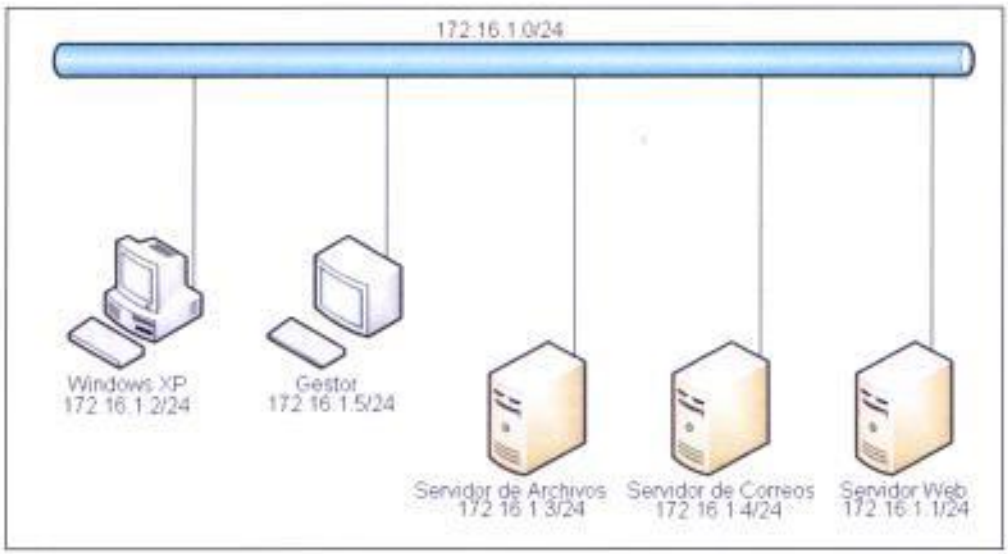


Figura 65.7 Diagrama Escenario 3

Del dispositivo mencionado podremos apreciar los requerimientos que fueron asignados al nuevo servidor en la figura 4.8.

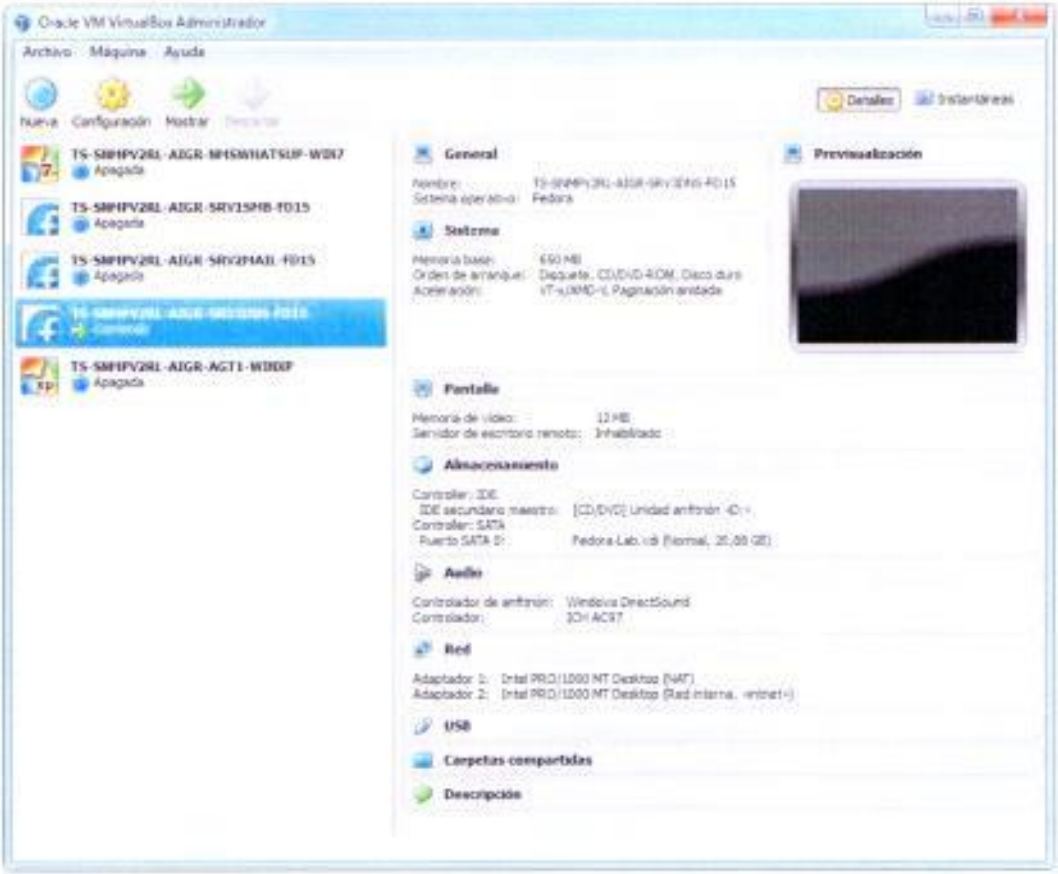


Figura 66.8 Características del Servidor Web en FEDORA 15.

CAPITULO 5

SIMULACION Y RESULTADOS

Vamos a realizar sobre cada escenario la simulación de las primitivas SNMPv2 con ayuda del programa Whatsup Gold para poder realizarlas en nuestra Red, en algunos casos creando parámetros en el agente para habilitar las respectivas OID y Wireshark para el análisis de los paquetes.

5.1. SIMULACION DE LOS ESCENARIOS

Las simulaciones que realizaremos se enfocarán sobre aspectos principales para el funcionamiento de cada uno de los servidores ejes de cada escenario.

5.1.1. SIMULACION ESCENARIO1

En nuestro primer escenario, vamos a realizar la simulación de las primitivas GET, SET y TRAP sobre el Servidor de Archivos. Para lo cual realizaremos lo siguiente:

SIMULACIÓN DE LA PRIMITIVA GET

Para probar la forma en cómo trabaja la primitiva GET, debemos ir al servidor y trabajar sobre el directorio donde se alojaran los archivos compartidos. En nuestro caso le crearemos un directorio llamado "ArchivosTesis" y lo crearemos como Volumen Lógico Con el comando: df –h, podremos ver las características del directorio "ArchivosTesis" como podemos ver en la Fig. 5.1

```
[root@localhost /]# df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/vg0-Archivos  62M  5.3M   54M   9% /ArchivosTesis
```

Figura 67.1 Espacio del disco compartido "ArchivosTesis" visualizado en el Servidor de Archivos

Con el agente instalado en el Servidor de Archivos debemos ingresar sentencias dentro del archivo de configuración para

poder realizar GET-REQUEST al directorio "ArchivosTesis" y guardar los cambios. Reiniciaremos el servicio Snmpd con el comando: service snmpd restart, para poder visualizar el cambio. Utilizaremos la sentencia: disk /ArchivosTesis 10% que nos permitirá ver los objetos de la OID del directorio "ArchivosTesis", véase Fig. 5.2

```
[root@localhost /]# vim /etc/snmp/snmpd.conf

disk /ArchivosTesis 10%
disk    100000

[root@localhost /]# service snmpd restart
Restarting snmpd (via systemctl):                          [  OK  ]
```

Figura 68.2 Configuración del directorio "ArchivosTesis" para poder trabajar con SNMPv2 y reinicio del servicio Snmpd.

Con el cambio realizado en el agente del Servidor de Archivos podremos visualizar todas las OID relacionadas al directorio "ArchivosTesis" utilizando la herramienta Snmp Mib Walker de Whatsup Gold.

En la Fig. 5.3 podremos ver los objetos correspondientes a las OID relacionadas al directorio "ArchivosTesis" que serán de nuestro interés al momento de realizar gestión sobre el servidor. Entre los cuales los más importantes pueden ser:

- dskPath: Nos muestra el directorio.

- dskMinPercent: Es el mínimo porcentaje permitido de espacio libre en el disco "ArchivosTesis".
- dskAvail: Cantidad de espacio en disco disponible.
- dskUsed: Cantidad de espacio de disco en uso.
- dskPercent: Porcentaje de disco en uso.

Figura 69.3 Objetos del directorio "ArchivosTesis" obtenidos por las primitivas SNMPv2

Al señalar sobre uno de estos objetos se nos mostrara la OID correspondiente. Cuando comenzamos a hacer la búsqueda con la herramienta SNMP Mib Walker, podremos ver con el analizador Wireshark como se mostraran las PDU de las primitivas GET-REQUEST, GET-NEXT-REQUEST, GET-BULK Y GET RESPONSE, véase Fig. 5.4.

Figura 70.4 Ejemplo de paquete SNMPv2 al realizar GET-NEXT-REQUEST al objeto dskPath

De todos los objetos disponibles, para nuestro proyecto realizaremos un monitoreo desde el Gestionador enviando la

primitiva GET-REQUEST sobre el objeto dskUsed de OID: 1.3.6.1.4.1.2021.9.1.8.1, se creara dentro del directorio "ArchivosTesis" un archivo de 1Mb y el aumento de espacio de disco se mostrara en un grafico 2D. Ayudándonos de Wireshark podremos realizar el análisis sobre el objeto al momento de aumentar el espacio utilizado en el disco.

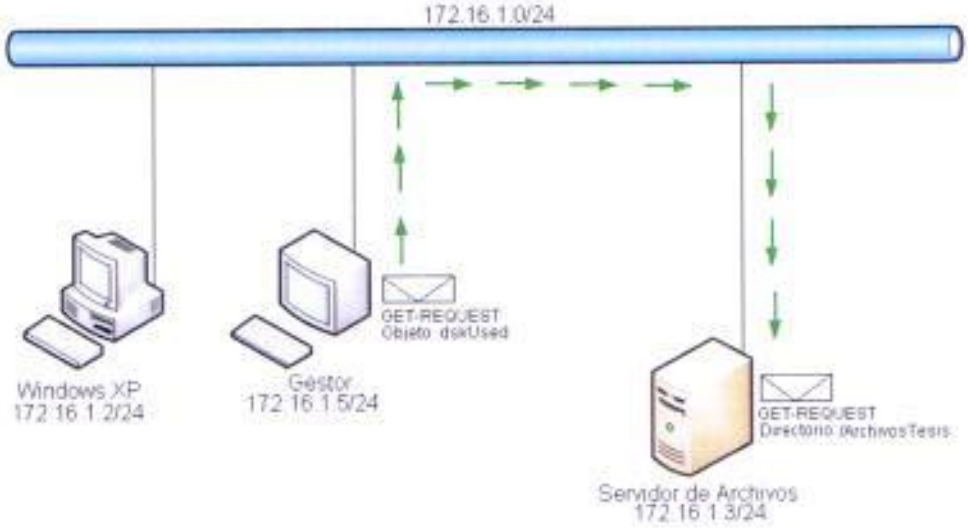


Figura 71.5 Simulación primitiva GET en Escenario 1

SIMULACIÓN DE LA PRIMITIVA SET

Para poder realizar la simulación de la primitiva SET vamos a utilizar la herramienta Action Library... del Gestionador, esta

nos permitirá configurar un SNMP Set Action para realizar SET-REQUEST.

Como se observa en la Fig. 5.6, deberemos llenar algunos parámetros correctamente:

- IP address or host name: 172.16.1.3
- Snmp v1/v2/v3 credentials: public_v2
- Object details: 1.3.6.1.2.1.1.4.0
- Value type: String
- Value to set: usuario@tesis.com

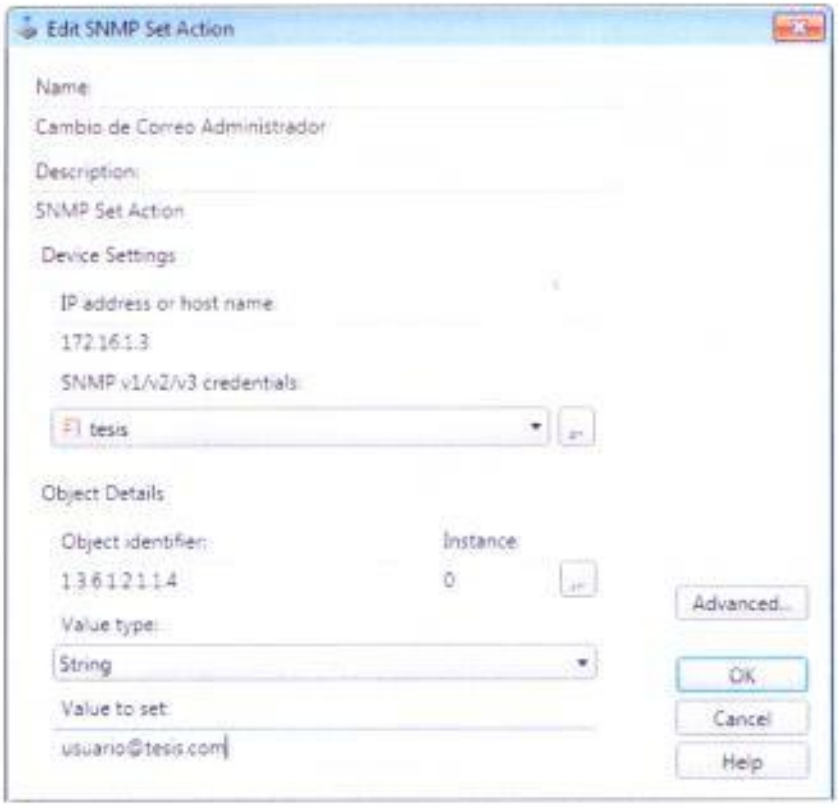


Figura 72.6 Configuración de SNMP Set Action

Los parámetros "Object details" y "Value to set" son los que indicaran el objeto y el nuevo valor en la primitiva SET-REQUEST.

Ahora realizaremos Walk con la herramienta SNMP Mib Walker para ver los objetos que muestran información de sistema del servidor de archivos, como se ve en la Fig. 5.7.

Figura 73.7 Objetos del servidor de archivos sobre el cual se realizara SET

Para nuestro proyecto realizaremos un cambio del valor en el objeto sysContact de OID: 1.3.6.1.2.1.1.4.0, el cual se realizara haciendo un test del SNMP Set Action que creara un SET-REQUEST al objeto sysContact, y al hacer nuevamente un Walk deberá ser visible el cambio. Ayudándonos de Wireshark podremos realizar el análisis sobre el objeto al momento del cambio.

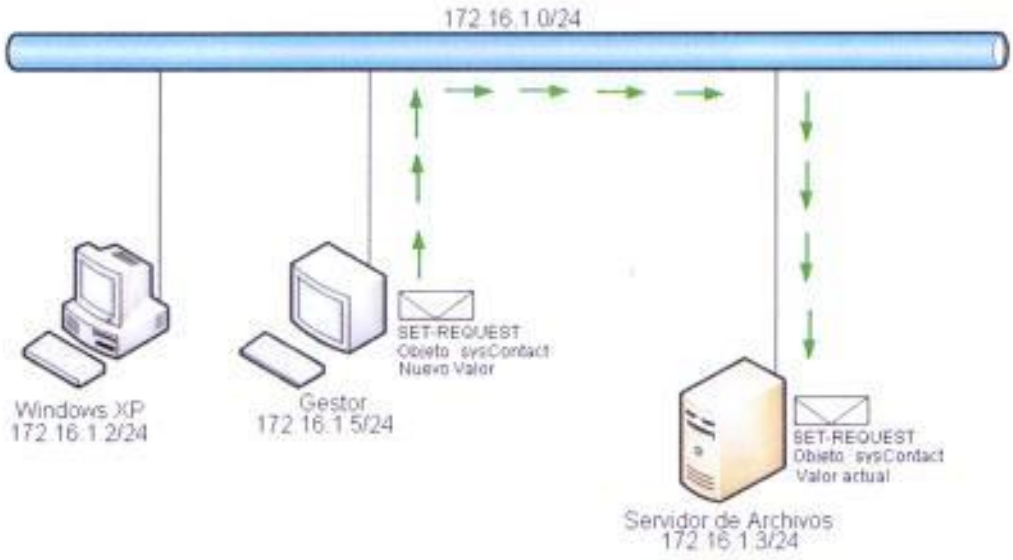


Figura 74.8 Simulación primitiva SET en Escenario 1

SIMULACIÓN DE LA PRIMITIVA TRAP

En la simulación de la primitiva TRAP primero dentro del archivo de configuración del agente del servidor de archivos se revisara que contenga los comandos que permitan la comunidad: rocommunity gestion 172.16.1.5, que permitan la comunidad para TRAP: trapcommunity gestion, y que permita activar las TRAPS para SNMPv2: trap2sink 172.16.1.5 gestion 162; en caso de no tenerlas configuradas se debe ingresarlas, guardarlasy reiniciar el servicio Snmpd.

```
rocommunity gestion 172.16.1.5
trapcommunity gestion
trap2sink 172.16.1.5 gestion 162
```

Figura 75.9 Configuración en Servidor para activar TRAP en Servidor de Archivos

Para la simulación de la primitiva TRAP en el escenario 1 vamos a proceder a detener el servicio Snmpd, esto hará que se envíe la TRAP correspondiente. Luego daremos inicio al servicio y se deberá generar otra TRAP correspondiente.

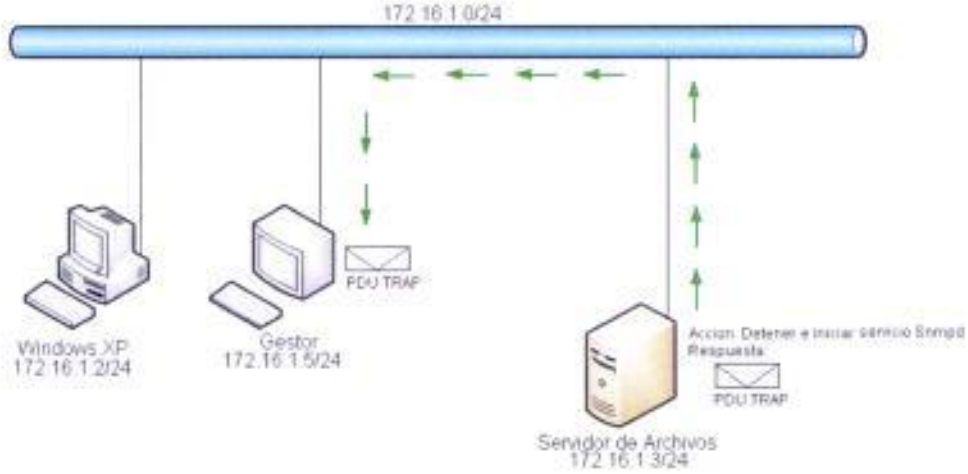


Figura 76.10 Simulación primitiva TRAP en Escenario 1

5.1.2. SIMULACION ESCENARIO2

En nuestro segundo escenario, vamos a realizar la simulación de las primitivas GET, SET y TRAP sobre el Servidor de Correos. Para lo cual realizaremos lo siguiente:

SIMULACIÓN DE LA PRIMITIVA GET

Para poder realizar la simulación de la primitiva GET deberemos configurar en el agente del Servidor la sentencia que nos permita tener gestión. En este escenario nos concentramos sobre el Servidor de Correos, se realizara GET-REQUEST relacionado al proceso Sendmail.

Para hacerlo se deberá ingresar la sentencia: proc sendmail 10, ya ingresada, guardamos el cambio y se reinicia el servicio Snmpd para poder visualizar el cambio, véase Fig. 5.11.

```
[root@tesis axib]# vim  etc/snmp/snmpd.conf

proc   0
proc sendmail 10
```

Figura 77.11 Configuración del proceso Sendmail para poder ser visto por SNMPv2

Dentro del Servidor de Correos con el comando: ps aux | grep sendmail, podremos ver la cantidad de procesos existentes de Sendmail, véase Fig. 5.12.

Figura 78.12 Procesos realizados por Sendmail

Con el cambio realizado en el agente del Servidor de Archivos podremos visualizar todas las OID relacionadas al proceso Sendmail utilizando la herramienta SNMP Mib Walker.

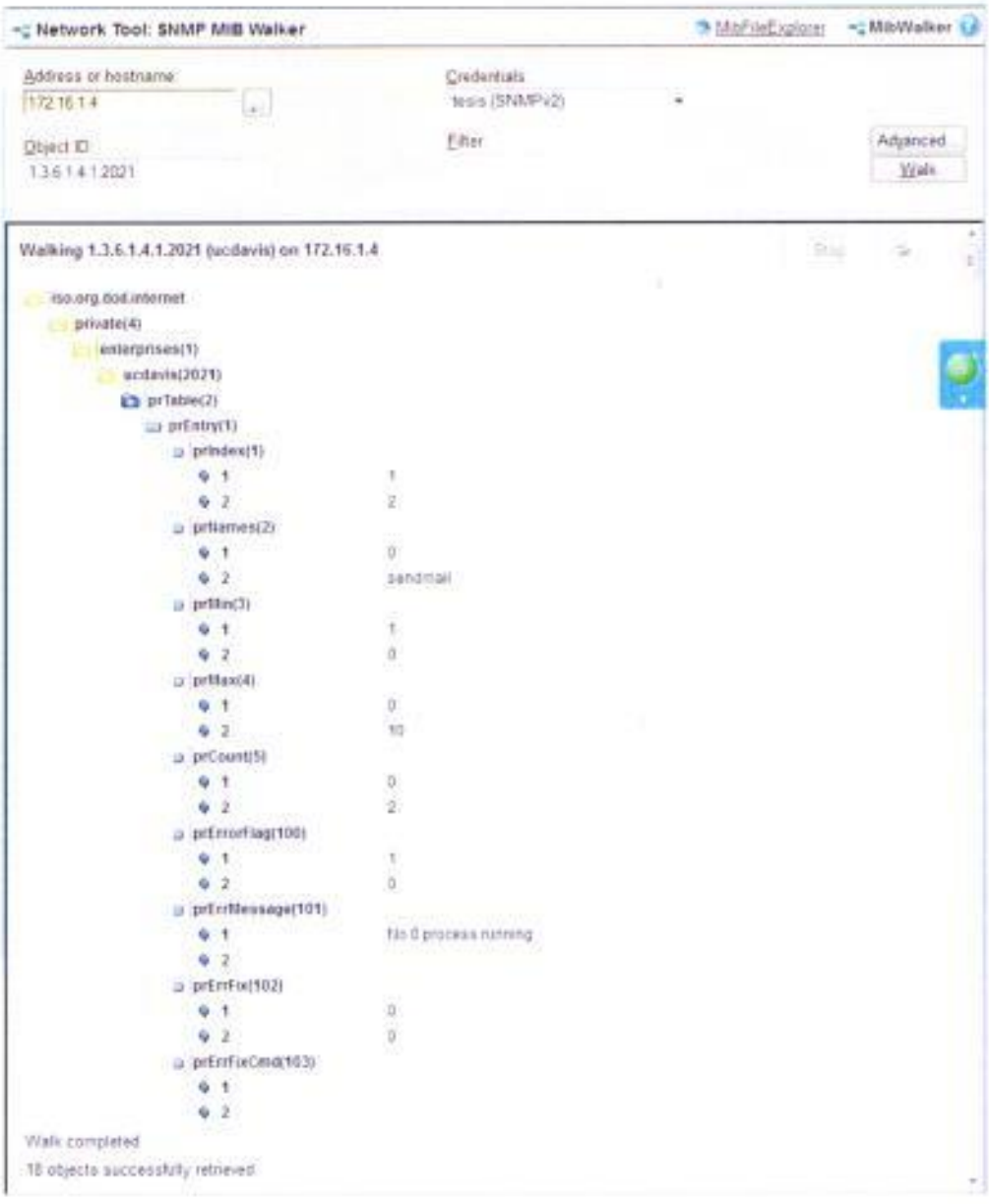


Figura 79.13 Atributos del proceso Sendmail visualizado por SNMPv2

En la Fig. 5.13, podremos ver los objetos correspondientes a las OID del proceso Sendmail. Entre los cuales los más importantes pueden ser:

- prName: Nombre del proceso.
- prMax: Número máximo de procesos
- prCount: Numero de procesos en curso.

Para nuestro proyecto realizaremos un monitoreo desde el Gestionador, el cual de entre todos los objetos disponibles solo realizara GET-REQUEST sobre el objeto prCount de OID: 1.3.6.1.4.1.2021.2.1.5.2,se enviara un correo electrónico para que aumente la cantidad de procesos y mostrarlo en un grafico 2D. Ayudándonos de Wireshark podremos realizar el análisis sobre el objetoy sunúmero de procesos.

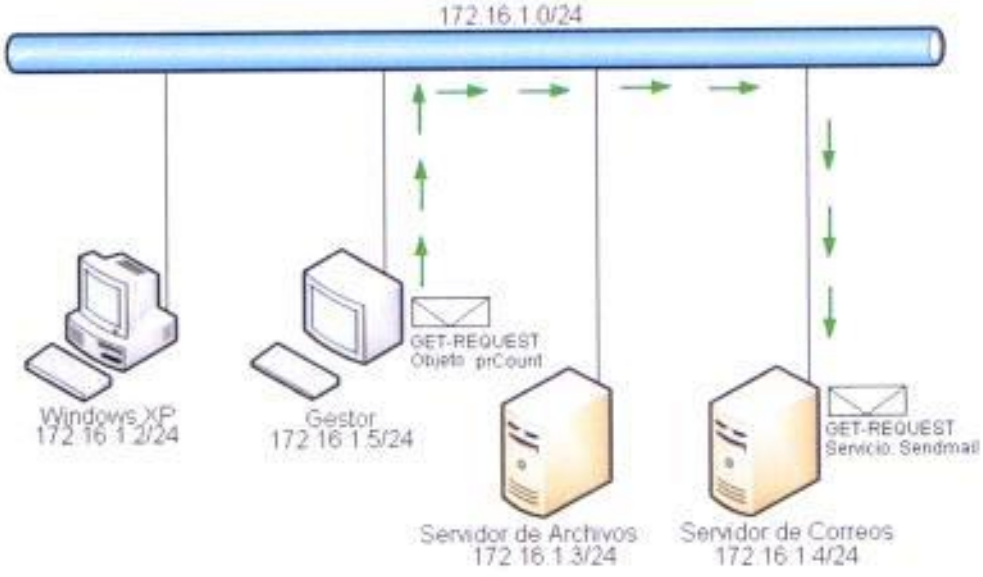


Figura 80.14 Simulación primitiva GET en Escenario 2

SIMULACIÓN DE LA PRIMITIVA SET

Para la simulación de la primitiva SET utilizaremos la herramienta Action Library..., con la que crearemos un SNMP Set Action.

Como se observa en la Fig. 5.15 deberemos llenar algunos parámetros correctamente:

- IP address or host name: 172.16.1.4
- Snmp v1/v2/v3 credentials: public_v2
- Object details: 1.3.6.1.2.1.1.5.0
- Value type: String
- Value to set: Ángel Ibarra

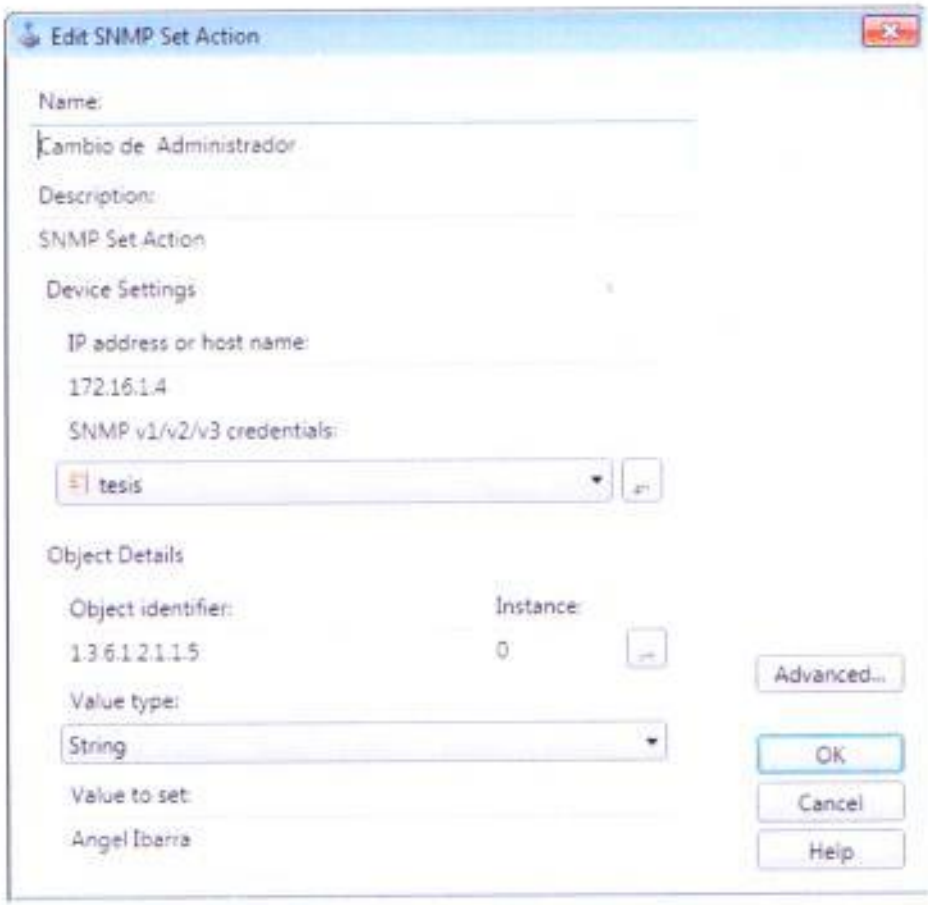


Figura 81.15 Configuración de SET

Los parámetros "Object details" y "Value to set" son los que indicaran el objeto y el nuevo valor en la primitiva SET-REQUEST.

Ahora realizaremos Walk con la herramienta SNMP Mib Walker para ver los objetos de información de sistema del Servidor de Correos.

Figura 82.16 Objetos del servidor de correos sobre el cual se realizara SET

Para nuestro proyecto realizaremos un cambio de valor en el objeto sysName de OID: 1.3.6.1.2.1.1.5.0, el cual al realizar un test del SNMP Set Action se enviara un SET-REQUEST al objeto sysName, al realizar nuevamente un Walk deberá ser visible el cambio. Ayudándonos de Wireshark podremos realizar el análisis sobre el objeto al momento del cambio.

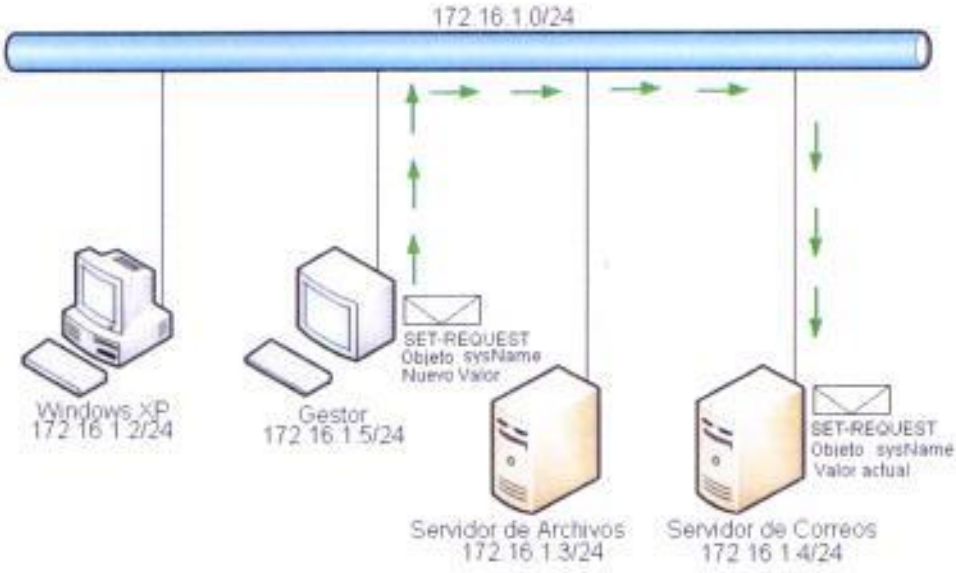


Figura 83.17 Simulación primitiva SET en Escenario 2

SIMULACIÓN DE LA PRIMITIVA TRAP

En la simulación de las primitivas TRAP primero revisaremos la configuración en el agente del servidor de correos para activar la TRAP, adicional se agregara: authtrapeneable 1, que nos ayudara en nuestra simulación, véase Fig. 5.18.

```
rocommunity gestion 172.16.1.5
trapcommunity gestion
trap2sink 172.16.1.5 gestion 162
authtrapenable 1
```

Figura 84.18 Configuración de agente SNMP en Servidor de Correos

Nuestro interés estará sobre: authtrapeneable 1, siendo colocada con el valor "1" estaremos activando la TRAP que corresponde aautenticación de la comunidad.

Para la simulación de la primitiva TRAP en el escenario 2 realizaremos el cambio de la comunidad en el agente, al momento que el gestionador realice alguna primitiva GET el Servidor de Correos deberá enviarcomo respuesta una TRAP.

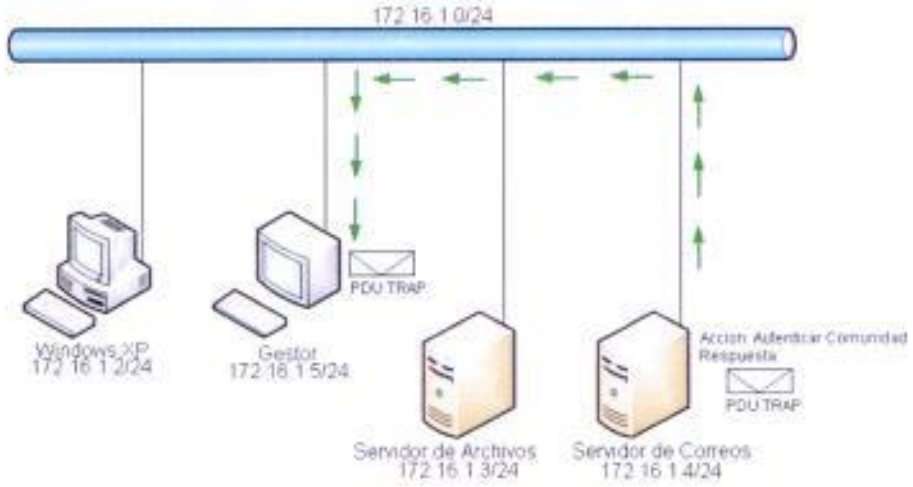


Figura 85.19 Simulación primitiva TRAP en Escenario 2

5.1.3. SIMULACION ESCENARIO3

En nuestro tercer escenario, vamos a realizar la simulación de las primitivas GET, SET y TRAP sobre el Servidor Web. Para lo cual realizaremos lo siguiente:

SIMULACIÓN DE LA PRIMITIVA GET

En este escenario realizaremos la simulación de la primitiva GET sobre el Servidor Web, nuestro eje de trabajo se hará sobre el uso de memoria RAM, un recurso muy importante para este tipo de servidores. Primero verificaremos en el Servidor Web la cantidad de memoria RAM con el comando: free –k –t, podremos ver que la descripción "Mem" se refiere a la memoria RAM, véase Fig. 5.20.

```
[root@localhost axib]# free -k -t
             total       used       free     shared    buffers     cached
Mem:        648392     499240     149152          0      55192     227960
-/+ buffers/cache:     216088     432304
Swap:      2064380       8064    2056316
Total:     2712772     507304    2205468
```

Figura 86.20 Espacio de memoria RAM en el Servidor Web

Como ya conocemos la cantidad de memoria RAM en uso, lo comprobaremos con la OID relacionadas a memoria RAM utilizando la herramienta SNMP Mib Walker, véase Fig. 5.21.

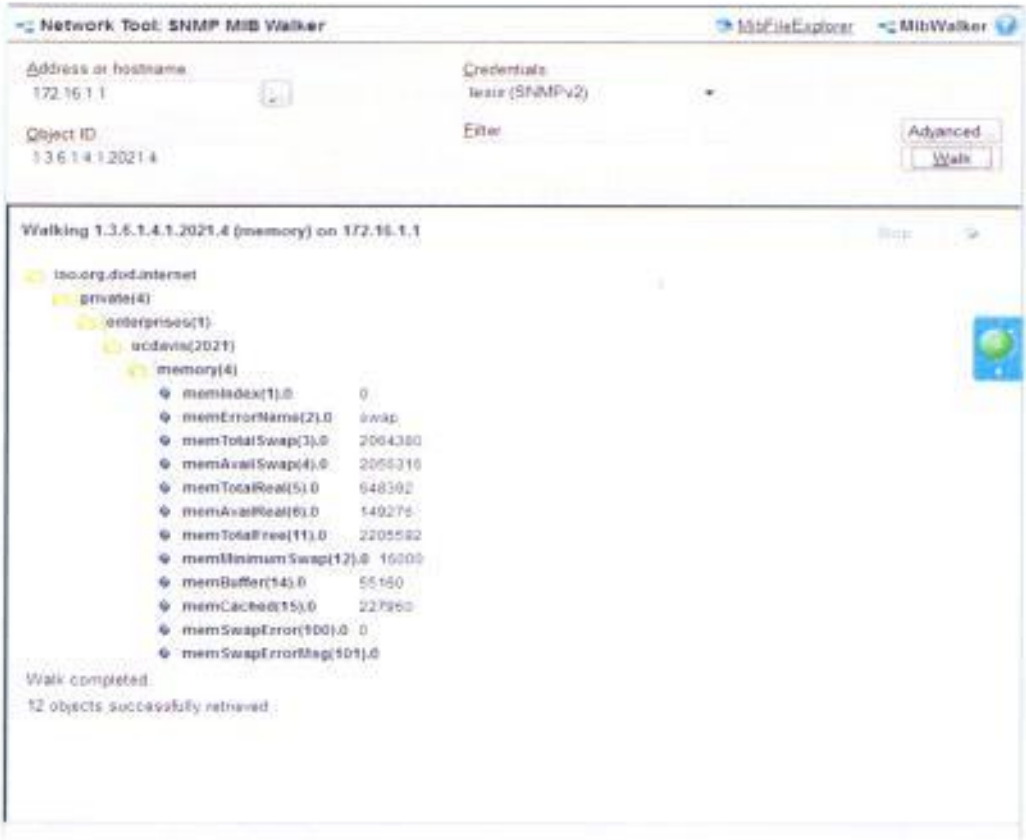


Figura 87.21 Objetos de memoria RAM

En la Fig. 5.22 podremos ver los objetos correspondientes a las OID de memoria RAM y Swap. Entre los cuales los más importantes pueden ser:

- memTotalReal: Memoria RAM total.
- memAvailReal: Memoria RAM disponible.

Entre todos los objetos disponibles, para nuestro proyecto realizaremos un monitoreo en el Gestionador lo que generara varios GET-REQUEST sobre el objeto memAvailReal de OID: 1.3.6.1.4.1.2021.4.6.0, y se irá mostrando en un grafico 2D. Ayudándonos de Wireshark podremos realizar el análisis sobre el objetomemAvailReal.

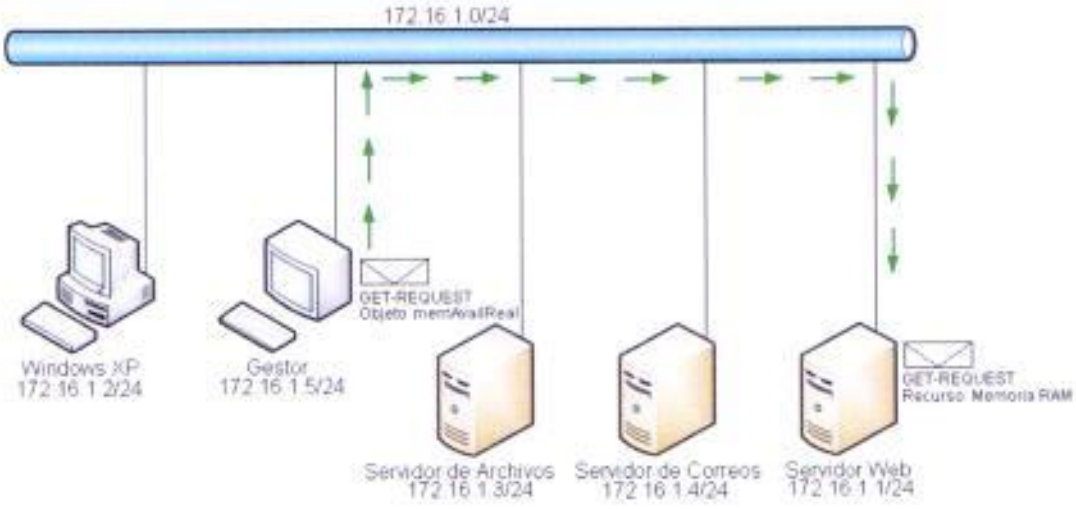


Figura 88.22 Simulación primitiva GET en Escenario 3

SIMULACIÓN DE LA PRIMITIVA SET

En la simulación de la primitiva SET utilizaremos la herramienta Action Library..., con la que crearemos un SNMP Set Action para poder realizar la primitiva SET.

Como se observa en la Fig. 5.23, deberemos llenar algunos parámetros correctamente:

- IP address or host name: 172.16.1.1
- Snmp v1/v2/v3 credentials: public_v2
- Object details: 1.3.6.1.2.1.1.6.0
- Value type: String
- Value to set: Espol

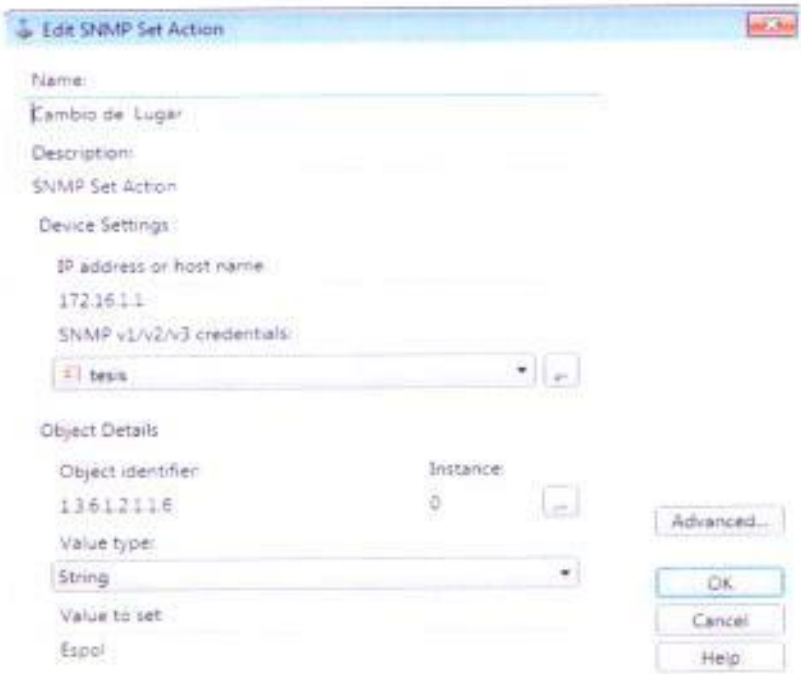


Figura 89.23 Configuración de SNMP Set Action

Los parámetros "Object details" y "Value to set" son los que indicaran el objeto y el nuevo valor en la primitiva SET-REQUEST.

Ahora realizaremos Walk con la herramienta SNMP Mib Walker para ver los objetos de información de sistema del Servidor Web.

Figura 90.24 Objetos del Servidor Web de información de sistema

Para nuestro proyecto realizaremos un cambio de valor en el objeto sysLocation de OID: 1.3.6.1.2.1.1.6.0, a lo quese realice un test del SNMP Set Action se enviara un SET-REQUEST al objeto sysLocation y al un Walk deberá ser visible el cambio. Ayudándonos de Wireshark podremos realizar el análisis sobre el objeto posterior al cambio.

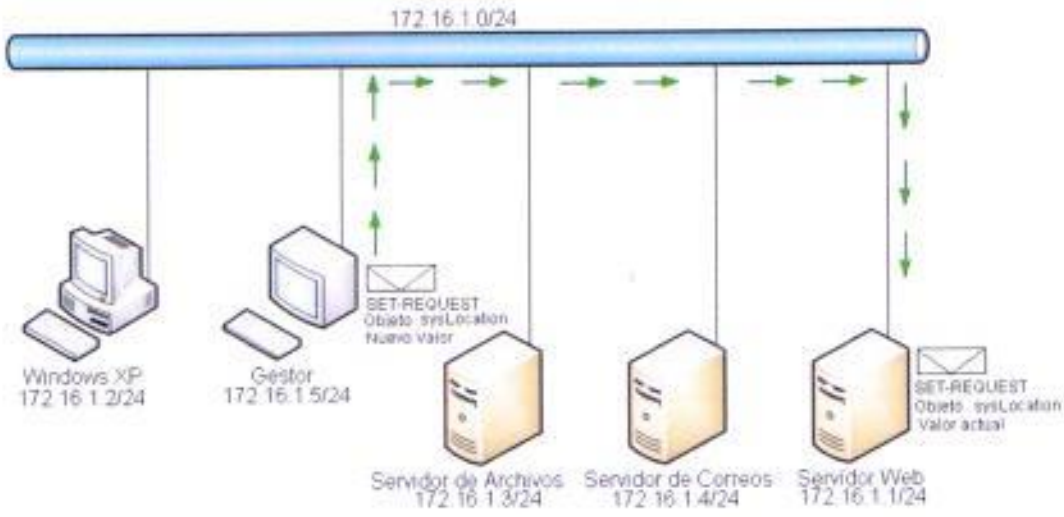


Figura 91.25 Simulación primitiva SET en Escenario 3

SIMULACIÓN DE LA PRIMITIVA TRAP

En la simulación de la primitiva TRAP deberemos comprobar la configuración, que al igual que en los otros servidores se debe tener dentro del agente del servidor. Adicional vamos a ingresar el comando: informsink 172.16.1.5 gestion 162, que nos permitirá enviar las primitiva INFORM.

```
rocommunity gestion 172.16.1.5

trapcommunity gestion
trap2sink 172.16.1.5 gestion 162
```

Figura 92.26 Configuración de TRAP en el agente del Servidor

Para la simulación de la primitiva TRAP y la primitiva INFOR vamos a realizar el apagado del Servidor Web y después de un tiempo prudente la encenderemos. Con lo que deberemos esperar recibir la TRAP e INFORM correspondiente tanto al evento de apagado y de encendido.

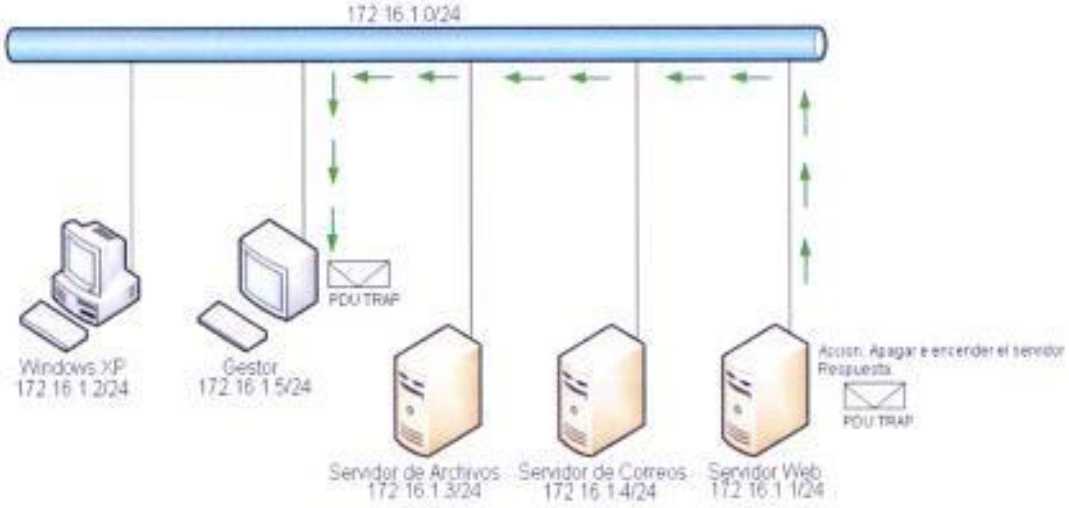


Figura 93.27 Simulación primitiva TRAP en Escenario 3

5.2. RESULTADOS DE LOS ESCENARIOS

5.2.1. RESULTADOS ESCENARIO1

RESULTADOS DE LA PRIMITIVA GET

Una vez configurado el monitoreo del objeto dskUsed para el Servidor de Archivos en el gestionador estaremos realizando constantes GET-REQUEST.

Ahora crearemos un archivo de 1Mb dentro del directorio con el comando: dd if=/dev/zero of=/ArchivosTesis/prueba.txt bs=1024 count=1000, véase Fig. 5.28.

```
[root@localhost axib]# dd if=/dev/zero of=/Archivos/prueba.txt bs=1024 count=2000
2000+0 records in
2000+0 records out
2048000 bytes (2.0 MB) copied, 0.00280073 s, 731 MB/s
```

Figura 94.28 Comando para aumentar tamaño del directorio "/ArchivosTesis"

Al momento de realizar GET-REQUEST, veremos que es solicitado desde el gestionador de IP: 172.16.1.5 hacia el servidor de archivos de IP: 172.16.1.3 solicitando el valor de dskUsed con la OID: 1.3.6.1.4.1.2021.9.1.8.1, véase Fig. 5.29.

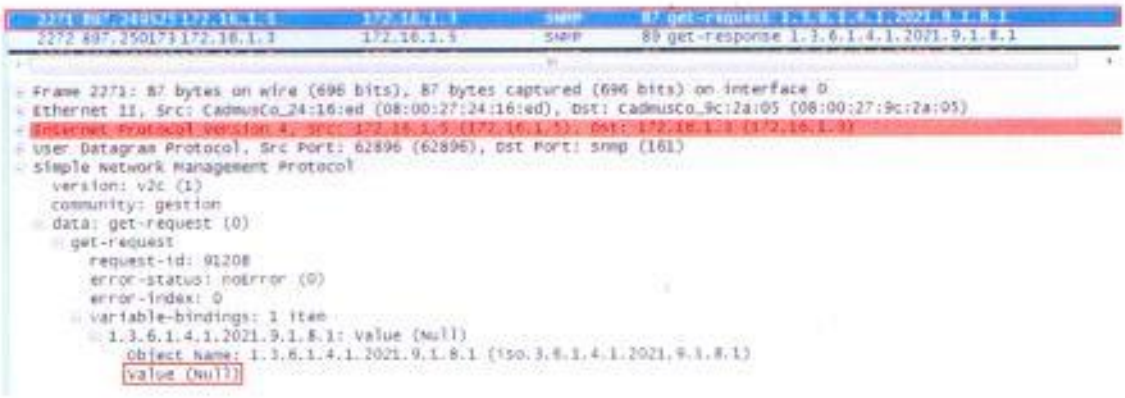


Figura 95.29 El paquete SNMPv2 al momento de consultar del tamaño de "ArchivosTesis"

Como respuesta obtenemos un GET-RESPONSE de parte del Servidor de Archivos hacia el gestionador devolviendo el valor: 7420 bytes, véase Fig. 5.30.

Figura 96.30 GET-RESPONSE de consulta de tamaño de "ArchivosTesis"

Como resultado en la Fig. 5.31, tenemos que en la grafica 2D una línea constante marcando el tamaño del directorio

"/ArchivosTesis" previo al aumento y luego el momento en que se creó el archivo, el tamaño del directorio "ArchivosTesis" ahora es 7420 bytes.

Figura 97.31 Grafica del Gestionador del tamaño de "ArchivosTesis"

RESULTADOS DE LA PRIMITIVA SET

Realizamos un test del SNMP Set Action configurado, será visible el cambio de valor en el objeto sysContact al realizar nuevamente un Walk, véase la Fig. 5.32.

Figura 98.32 Resultado al realizar SET sobre sysContact

Como podemos ver en la Fig. 5.33, al momento de realizar el SET-REQUEST, se envía el valor que se deberá colocar dentro del objeto sysContact siendo solicitado por el gestionador de IP: 172.16.1.5 al Servidor de Archivos de IP: 172.16.1.3 con la OID: 1.3.6.1.2.1.1.4.0.

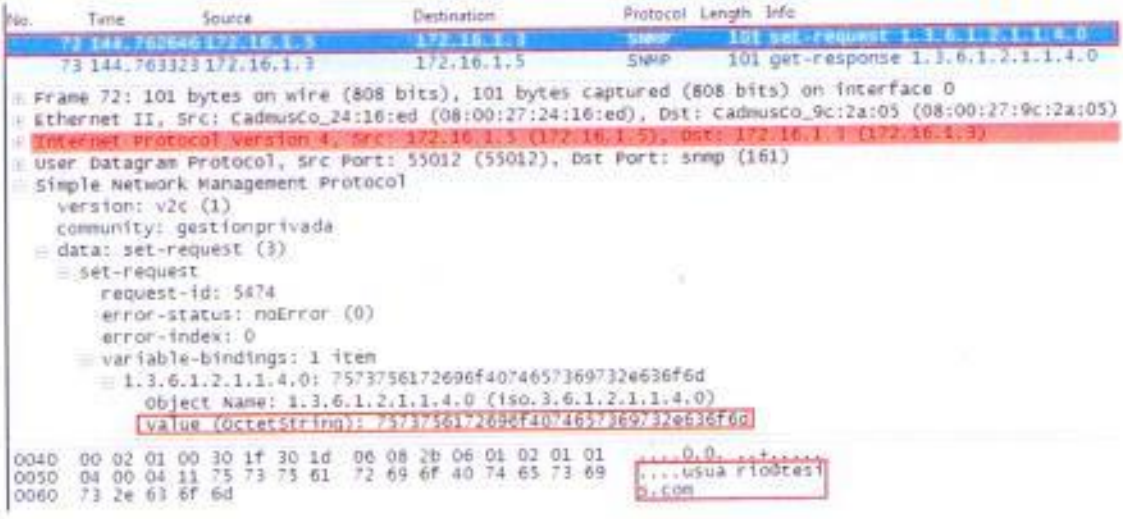


Figura 99.33 Posterior al SET sobre sysContact con Wireshark

Como respuesta se obtiene un GET-RESPONSE de parte del Servidor de Archivos hacia el gestionador mostrando el valor actual del objeto sysContact: usuario@tesis.com, véase Fig. 5.34.

Figura 100.34 Posterior al SET sobre sysContact

RESULTADOS DE LA PRIMITIVA TRAP

Al momento de detener el servicio Snmpd, tendremos que el Servidor de Archivos de IP: 172.16.1.3 enviara la primitiva SNMPv2-trap al gestionador de IP: 172.16.1.5 indicando que se detuvo el servicio dando como valor la siguiente OID: 1.3.6.1.4.1.8072.4.0.2, véase Fig. 5.35.

Figura 101.35 Resultado de la TRAP al detener el servicio Snmpd

Ahora vamos a volver a iniciar el servicio Snmpd, obtenemos la primitiva SNMPv2-trap desde el Servidor de Archivos hacia el gestionador dando como valor la OID: 1.3.6.1.6.3.1.1.5.1, véase Fig. 5.36.

Figura 102.36 Resultado de la TRAP al iniciar el servicio Snmpd

5.2.2. RESULTADOS ESCENARIO2

RESULTADOS DE LA PRIMITIVA GET

Con el monitoreo del objeto prCount se obtiene GET-REQUEST constantemente hacia el Servidor de Correos.

Al realizar un Walk con la herramienta SNMP Mib Walker podremos ver que el valor de prCount: 2y su correspondiente OID: 1.3.6.1.4.1.2021.2.1.5.2 como vemos en la Fig. 5.37.

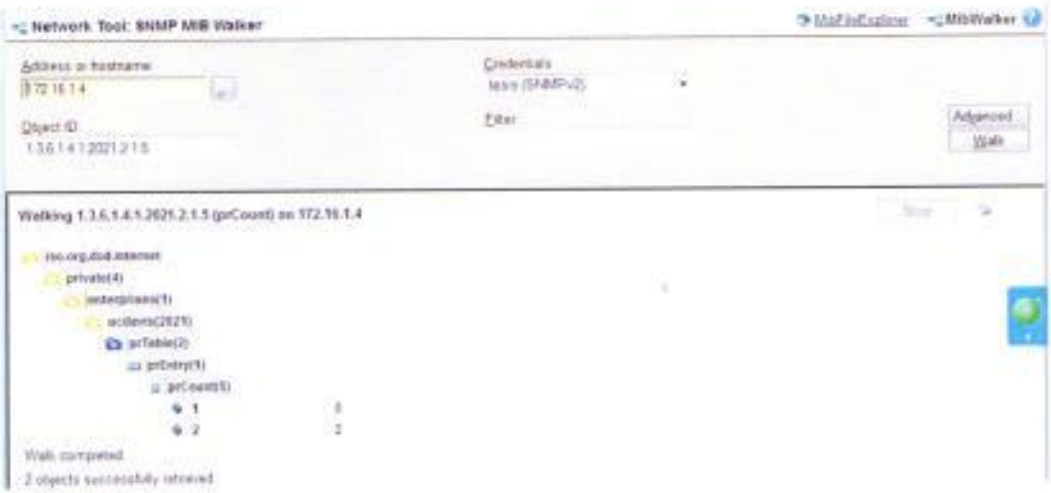


Figura 103.37 Numero de procesos de Sendmail

En la Fig. 5.38 vemos que se envía un correo desde el servidor y el cuerpo del mensaje, cambiando el resultado de prCount.

```
[root@tesis axib]# mail -v usuario@tesis.com
Subject: tesis
Esta es una prueba para la tesis.
.
EOT
usuario@tesis.com... Connecting to [127.0.0.1] via relay...
220 sara.com ESMTP Sendmail 8.14.4/8.14.4; Tue, 17 Sep 2013 19:58:57 -0500
>>> EHLO tesis.com
250-tesis.com Hello localhost [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH GSSAPI DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
>>> MAIL From:<axib@tesis.com> SIZE=240 AUTH=axib@tesis.com
250 2.1.0 <axib@tesis.com>... Sender ok
>>> RCPT To:<usuario@tesis.com>
>>> DATA
250 2.1.5 <usuario@tesis.com>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 r8I0wvbF002020 Message accepted for delivery
usuario@tesis.com... Sent (r8I0wvbF002020 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 tesis.com closing connection
```

Figura 104.38 Cuerpo de un correo electrónico desde el Servidor

Una vez enviado el correo nos damos cuenta en la Fig. 5.39, que efectivamente se cambio el valor de prCount que ahora será igual a: 3. En el momento que se realizo el GET-REQUEST, vemos que se solicita desde el gestionador de IP: 172.16.1.5 hacia el Servidor de correos de IP: 172.16.1.4 el valor de prCount con la OID: 1.3.6.1.4.1.2021.2.1.5.2.

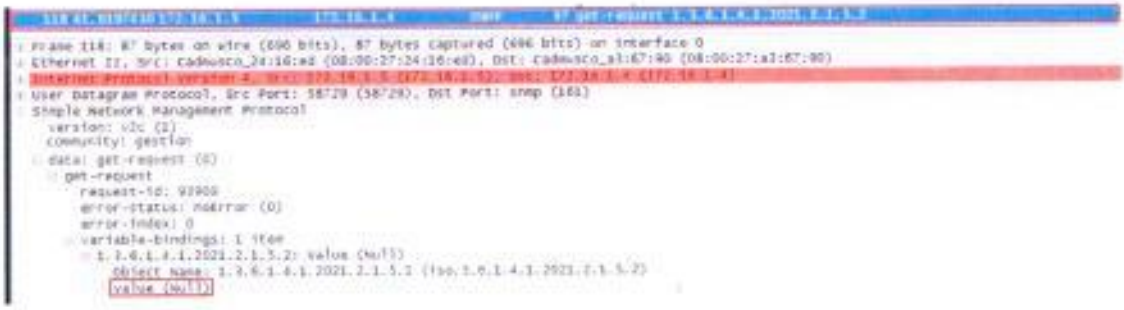


Figura 105.39 Realizando GET al número de procesos

Como respuesta se obtiene un GET-RESPONSE de parte del Servidor de Correos hacia el gestionador devolviendo el valor de prCount: 3, véase Fig. 5.40.

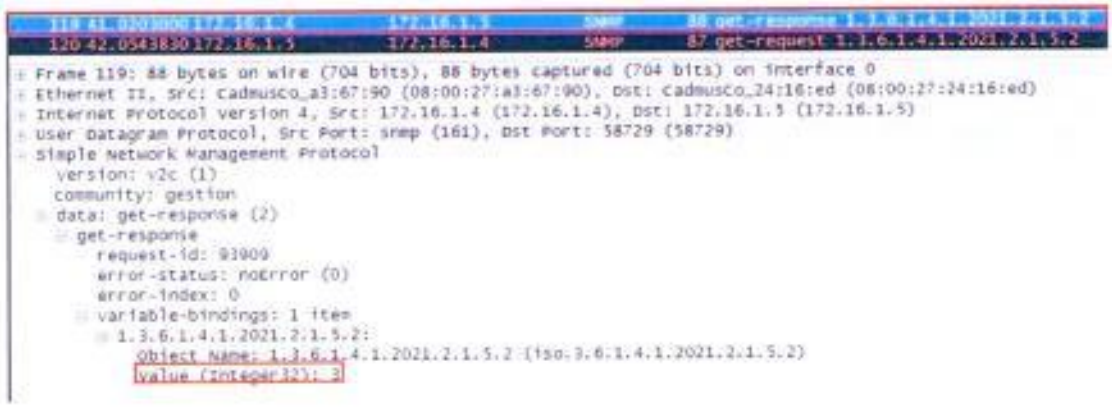


Figura 106.40 Resultado del número de procesos

Los valores como resultado del constantemente envío de GET-REQUEST, nos muestra una grafica de la cantidad de

procesos en ejecución y en el momento que se envió el correo se dio un aumento en la cantidad de proceso, véase Fig. 5.41.

Figura 107.41 Grafica mostrando el número de procesos

RESULTADOS DE LA PRIMITIVA SET

En el momento que realizamos el Test, se da por realizado el cambio de valor en el objeto sysName. El cual es visible al realizar un Walk, como se ve en la Fig. 5.42.

Figura 108.42 Grafica mostrando el número de procesos Posterior al SET al objeto sysName

Como podemos ver en la Fig. 5.43, al realizar SET-REQUEST, se envió el valor que se a cambiar dentro del objeto sysName solicitado por el gestionador de IP: 172.16.1.5 al Servidor de Correos de IP: 172.16.1.4 con la OID: 1.3.6.1.2.1.1.5.0.

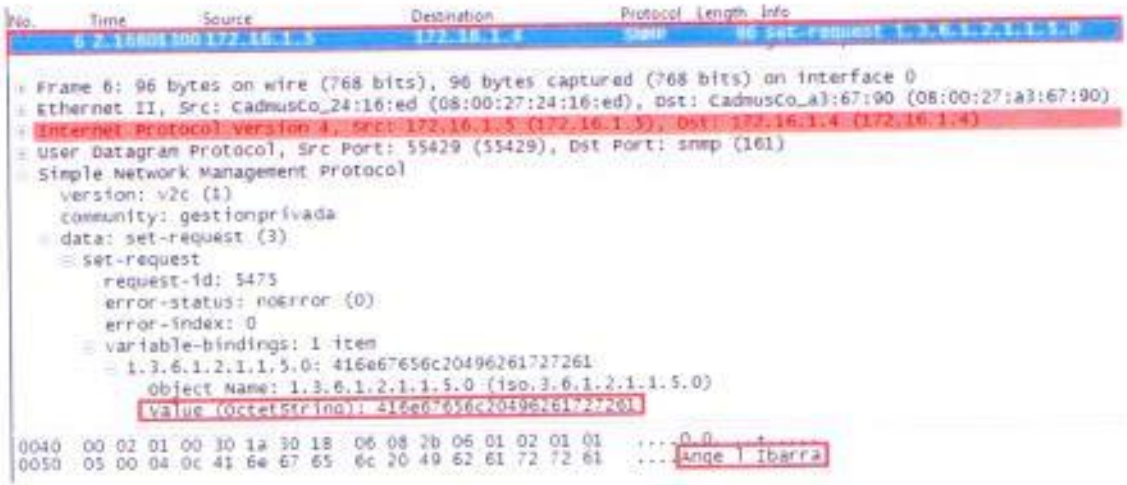


Figura 109.43 Primitiva SET-REQUEST

Como respuesta se obtiene un GET-RESPONSE de parte del Servidor de Correos hacia el gestionador indicando cual es el nuevo valor del objeto sysName: Angel Ibarra, véase Fig. 5.44.

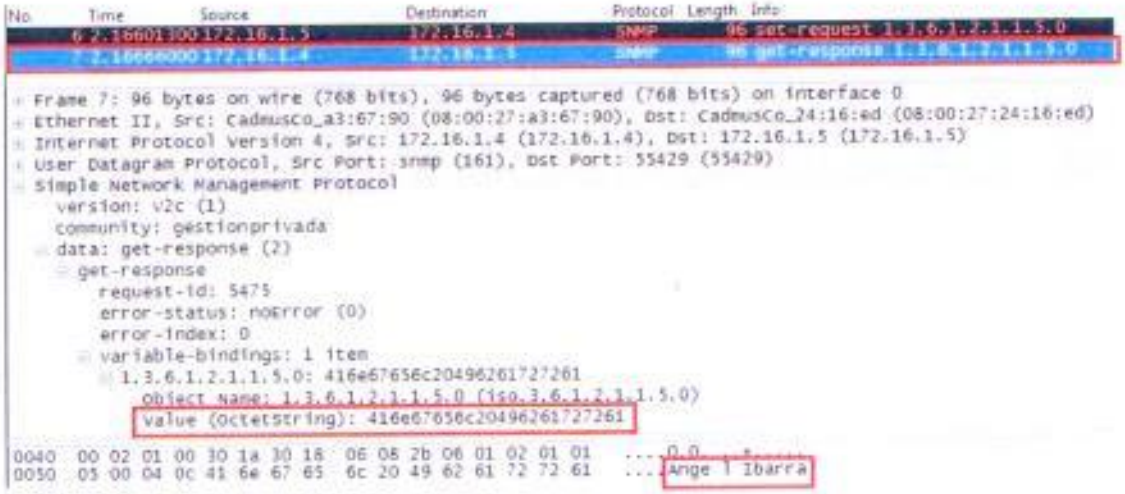


Figura 110.44 Primitiva GET-REQUEST posterior al SET-REQUEST

RESULTADOS DE LA PRIMITIVA TRAP

Se cambio la comunidad en el agente del Servidor de Correos y en su lugar se puso: tesis, como vemos en la Fig. 5.45. Guardamos los cambios y se reinicio el servicio Snmpd en el servidor.

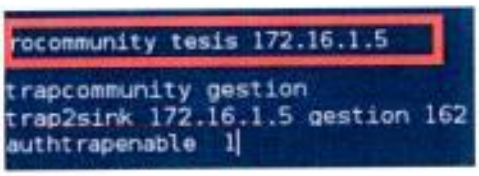


Figura 111.45 Cambio de Comunidad en Escenario 2

En el gestionador se activo el monitoreo realizando constantemente GET-REQUEST. El gestionador trata de

autenticar con la anterior comunidad: gestion, tal como lo observamos en la Fig.5.46.

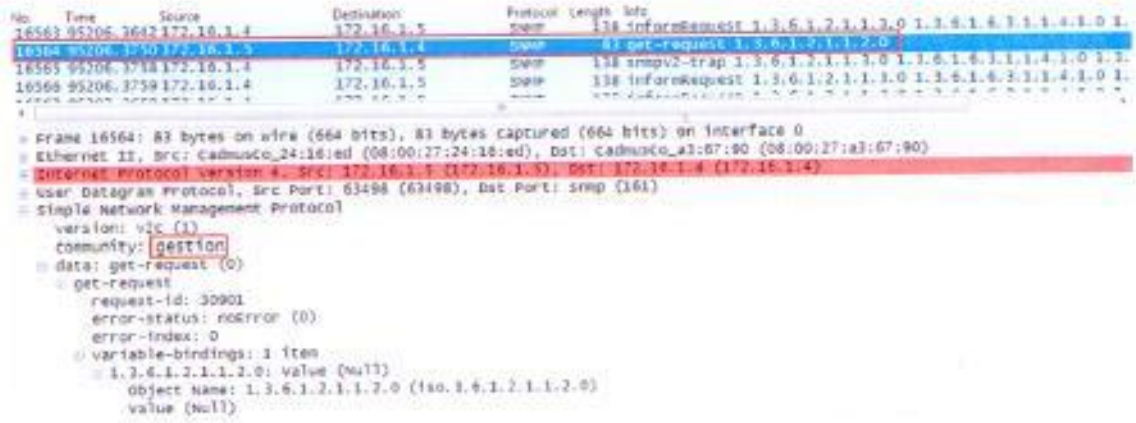


Figura 112.46 Solicitud GET-REQUEST con comunidad "gestion"

El Servidor de Correos de IP: 172.16.1.4 enviara la primitiva SNMPv2-trap al gestionador de IP: 172.16.1.5 indicando que la autenticación fallo dando como valor la siguiente OID: 1.3.6.1.6.3.1.1.5.5, véase Fig. 5.47.

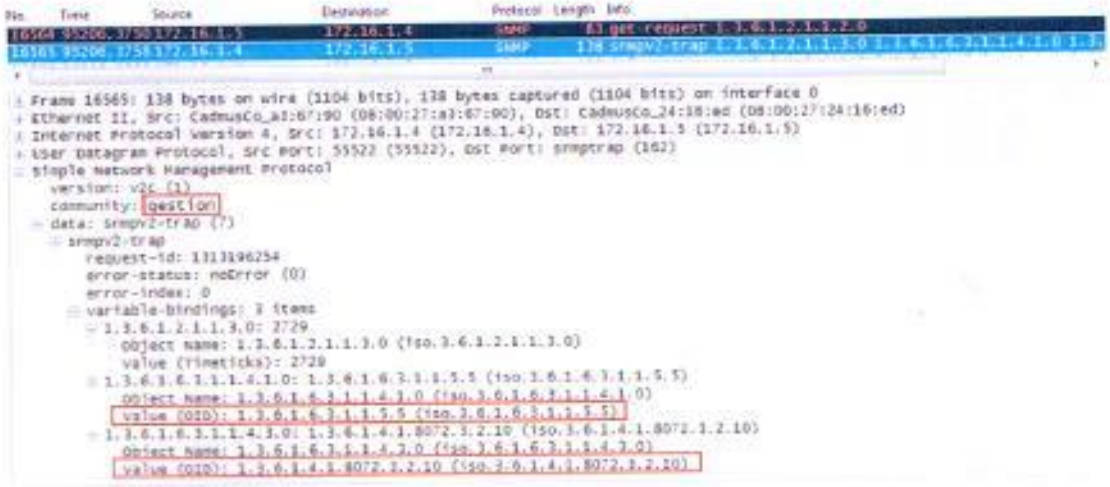


Figura 113.47 Mensaje TRAP resultante

5.2.3. RESULTADOS ESCENARIO3

RESULTADOS DE LA PRIMITIVA GET

Con el monitoreo del objeto memAvailReal se realizo GET-REQUEST constantemente hacia el Servidor Web.

Al realizar un Walk con la herramienta SNMP Mib Walker vemos la cantidad de memoria RAM disponible con el objetomemAvailReal:136064, ayudándonos por la OID:1.3.6.1.4.1.2021.4.6.0, véase Fig. 5.48.

Figura 114.48 Cantidad de memoria RAM disponible

Al momento de realizar GET-REQUEST, vemos que se solicita desde el gestionador de IP: 172.16.1.5 hacia el Servidor Web de IP: 172.16.1.5 solicitando el valor de memAvailReal con la OID: 1.3.6.1.4.1.2021.4.6.0, véase Fig. 5.49.

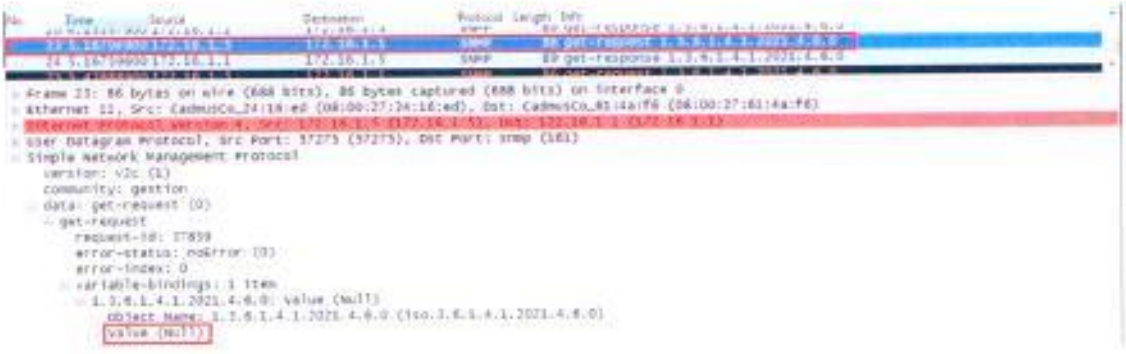


Figura 115.49 GET-REQUEST de cantidad de memoria RAM disponible

Como respuesta se obtiene un GET-RESPONSE de parte del Servidor Web: 172.16.1.5 hacia el gestionador: 172.16.1.5 devolviendo el valor de memAvailReal:134840.

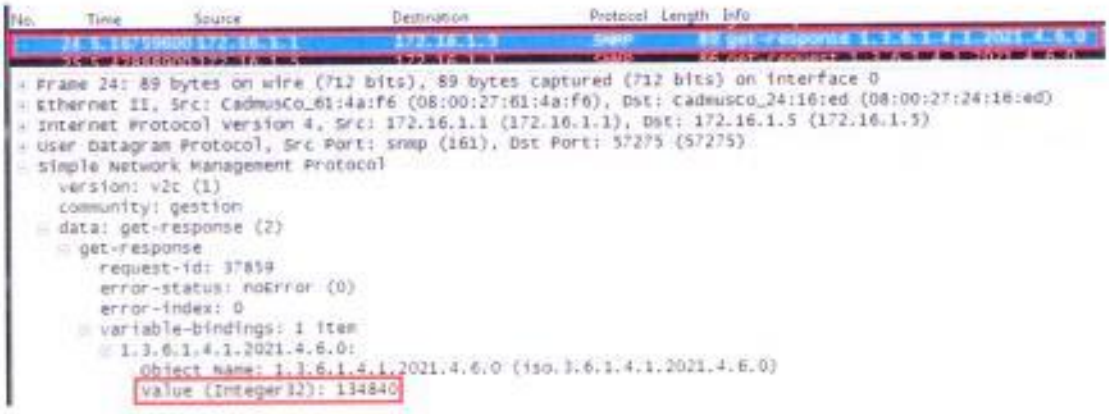


Figura 116.50 GET-RESPONSE de la cantidad de memoria RAM disponible

La cantidad de memoria RAM que tenemos disponible se estará graficando, como el monitoreo del gestionador se encuentra constantemente realizando GET-REQUEST, podremos ver que efectivamente el valor de memAvailReal es casi igual a 134840, véase Fig. 5.51.

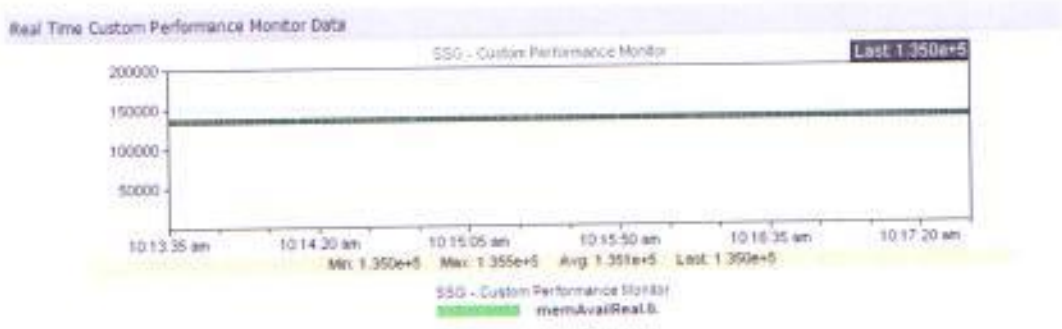


Figura 117.51 Grafico de memoria RAM disponible

RESULTADOS DE LA PRIMITIVA SET

Con SNMP Set Action realizamos el Test, cambiando de valor del objeto sysLocation. Al realizar nuevamente un Walk se podrá observar el cambio, véase Fig. 5.52.

Figura 118.52 Valor de objeto sysLocation antes de realizar SET

Como podemos ver en la Fig. 5.53, al realizar SET-REQUEST se envía el valor que se deberá colocar dentro del objeto sysLocation solicitado por el gestionador de IP: 172.16.1.5 hacia el Servidor Web de IP: 172.16.1.1 con la OID: 1.3.6.1.2.1.1.5.0.

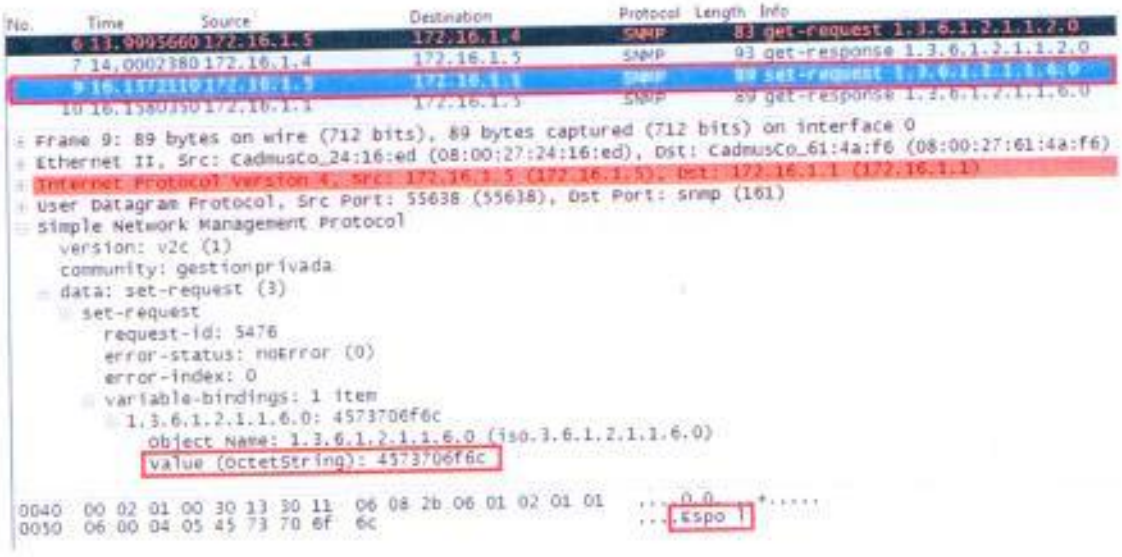


Figura 119.53 Primitiva SET-REQUEST al objeto sysLocation

Como respuesta se obtiene un GET-RESPONSE de parte del Servidor Web hacia el gestionador indicando el nuevo valor del objeto sysLocation: Espol, véase Fig. 5.54.

Figura 120.54 Primitiva GET-REQUEST posterior al SET-REQUEST

RESULTADOS DE LA PRIMITIVA TRAP

Al momento de apagar la máquina virtual se nos envío la primitiva SNMPv2-trap y la primitiva informRequest desde el Servidor Web de IP: 172.16.1.1 hacia el gestionador de IP: 172.16.1.5 dando de valor la siguiente OID: 1.3.6.1.4.1.8072.4.0.2, véase Fig. 5.55, 5.56.

Figura 121.55 TRAP al apagar máquina virtual

Figura 122.56 INFORM al apagar máquina virtual

Una vez que encendemos la máquina virtual se nos envío la primitiva SNMPv2-trap y la primitiva informRequest desde el servidor web de IP: 172.16.1.1 hacia el gestionador de IP: 172.16.1.5 dando como valor la siguiente OID: 1.3.6.1.6.3.1.1.5.1, véase Fig. 5.57, 5.58.

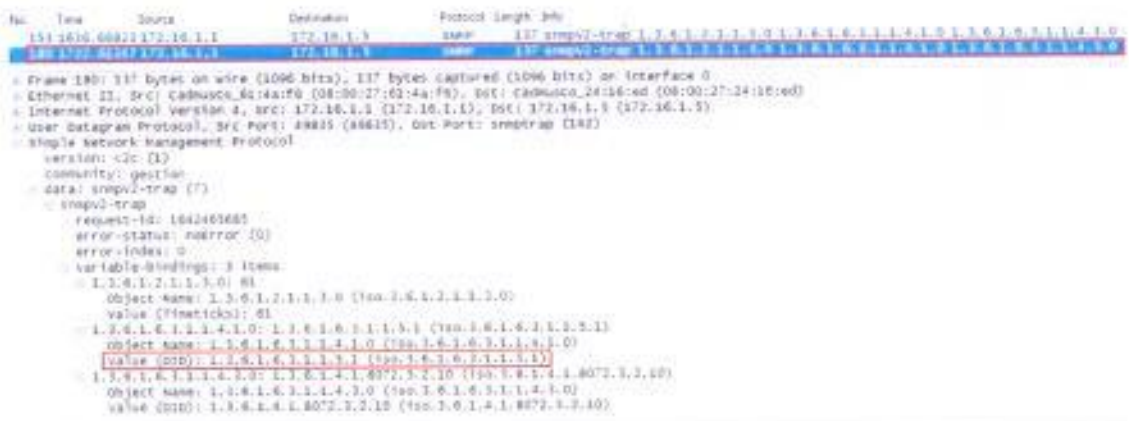


Figura 123.57 TRAP al encender máquina virtual

Figura 124.58 INFORM al encender máquina virtual

5.3. ANALISIS DE LOS RESULTADOS

Hemos podido constatar que en nuestro modelo de simulación de una Red LAN es posible realizar Gestión con un modelo Gestor-Agente y semejante a escenarios reales.

ANALISIS DE LA PRIMITIVA GET

En el caso de la primitiva GET la PDU que se obtiene al realizar GET-REQUEST, GET-NEXT-REQUEST, GET-BULK-REQUEST nos mostrara los mismos resultados para un mismo objeto, esto dependerá si está como instancia, un arreglo de instancias o en una tabla de instancias. La relación entre el objeto y su OID se encuentra dada por la MIB:UDP-SNMP-MIB la cual se encuentra contenida en el

Gestionador y los servidores. De entre las primitivas SNMPv2 las primitivas GET son con las que mas trabajaremos en la Gestion de la red.

En el escenario 1la primitiva GET es realizada al objeto dskUsed cuyo valor tiene el tipo de datoInteger32. Dentro de la figura vemos que en la PDU del GET-REQUEST el parámetro "data" tiene la id: 0, que se asocia a GET-REQUEST. Otro parámetro de importancia son los campos variables (variable-bindings) dentro vemos la OID: 1.3.6.1.4.1.2021.9.1.8.1que está asociado al objeto dskUsed y el valor de tipo de dato Null, en espera de la respuesta, véase Fig. 5.59.

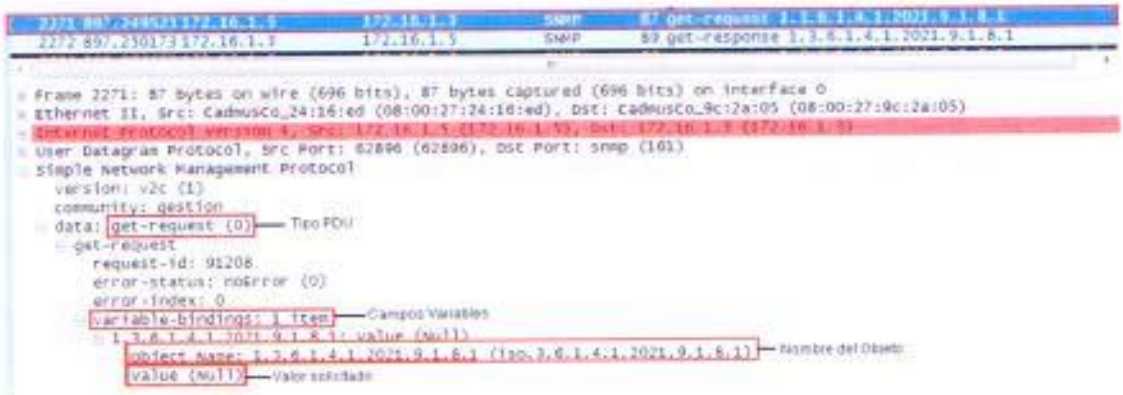


Figura 125.59 Análisis de PDU GET-REQUEST

Al recibircomo respuesta unGET-RESPONSE verificamos en su PDU que posea el mismo request-id: 91208, lo que indica que esta es la respuesta esperada. Ahora el parámetro "data"

tendra de id: 2, asociada a GET-RESPONSE. En este caso se obtuvo satisfactoriamente el valor: 7420 asociado a la OID:1.3.6.1.4.1.2021.9.1.8.1correspondiente al objeto dskUsed, vease Fig. 5.60.

Figura 126.60 Análisis de Resultados en PDU GET-RESPONSE

Cuando se realizo el aumento del espacio en el disco "ArchivosTesis" fue visible en la Fig. 5.31, y se comprobó que el protocolo UDP permite a SNMPv2 una rápida respuesta ante grandes cantidades de solicitudes.

En el escenario 2 vemos que la primitiva GET realizada al objeto prCount posee el tipo de dato Integer32. Dentro de los campos variables que contiene la OID:1.3.6.1.4.1.2021.2.1.5.2 asociado a prCount y el valor de tipo de dato Null en espera de la respuesta. El comportamiento entre GET-REQUEST y su

correspondiente GET-RESPONSE es similar al analizado dentro del escenario 1, véase Fig. 5.39.

Veremos como respuesta un GET-RESPONSE, este debera tener en su PDU el mismo request-id: 93909, lo que indicara que esta es la respuesta esperada. Ahora el parámetro "data" tendra de id: 2, asociado a GET-RESPONSE. En este caso se obtuvo satisfactoriamente el valor: 3 equivalente al numero de procesos del servicio Sendmail, asociado a la OID:1.3.6.1.4.1.2021.2.1.5.2 correspondiente al objeto prCount , vease Fig. 5.61.

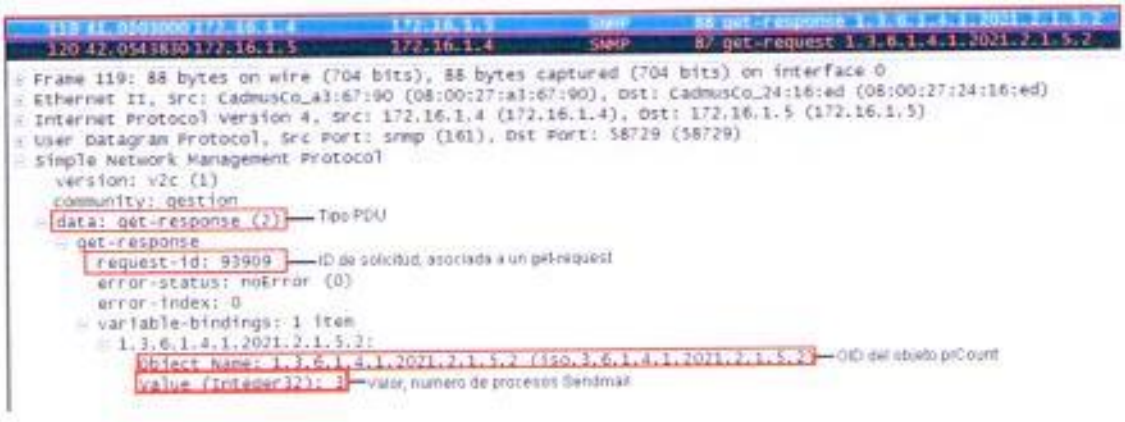


Figura 127.61 Análisis de Resultados en PDU GET-RESPONSE

Cuando se realizo el envio del correo electronico, el tiempo del que se dispone para visualizar el aumento de procesos es

corto como se ve en la Fig. 5.41 ,debido a que durara lo que demore el proceso de envio de correo.

En el escenario 3 la primitiva GET se realiza al objeto memAvailReal cuyotipo de dato es Integer32.Dentro de la PDU de GET-REQUEST veremos en los campos variables que contiene la OID: 1.3.6.1.4.1.2021.4.6.0 asociada al objeto memAvailReal y el valor de tipo de dato Null, en espera de la respuesta, véase Fig. 5.49.

Comprobamos que el PDU GET-RESPONSE posee la misma request-id: 37859, que la PDU de GET-REQUEST, y este sera nuestra respuesta esperada. Ahora el parámetro "data" tendra de id: 2, asociado a GET-RESPONSE. En este caso se obtuvo satisfactoriamente el valor: 134840, asociado a la OID:1.3.6.1.4.1.2021.4.6.0 correspondiente al objeto memAvailReal, vease Fig. 5.62.

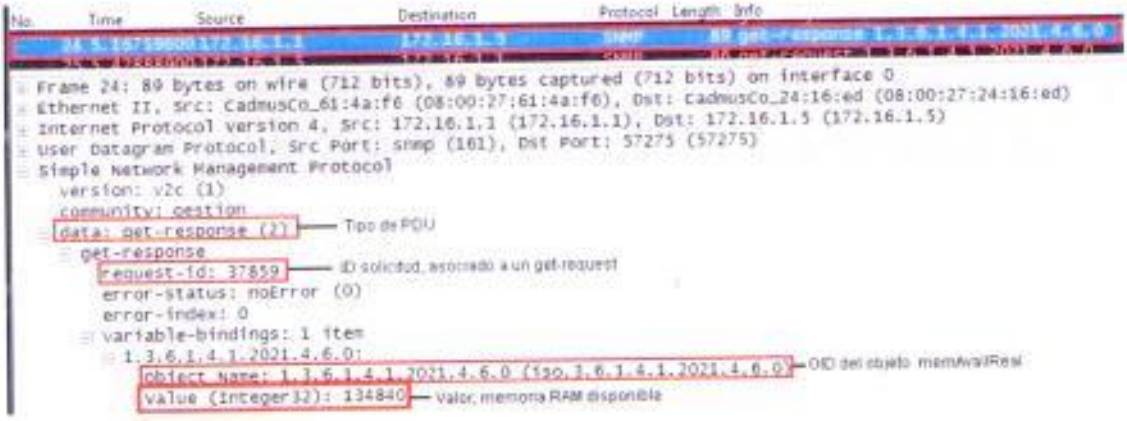


Figura 128.62 Análisis de Resultados en PDU GET-RESPONSE

ANALISIS DE LA PRIMITIVA SET

Para el caso de las primitivas SET nos hemos ayudado de la herramienta SNMP Set Action del Gestionador, que al realizar un Test se generaran los SET-REQUEST correspondiente por cada escenario.

En el escenario 1 se realizo un SET-REQUEST al objeto sysContact cuyo valor es de tipo de dato OctetString. En la figura vemos que dentro de la PDU de SET-REQUEST el parámetro "data" se le asigno la id: 3, correspondiente a SET-REQUEST. Dentro de los campos variables se enviara el objeto, utilizando su OID: 1.3.6.1.2.1.1.4.0 correspondiente al objeto sysContact y su valor:usuario@tesis.com, debido a

utilizar el tipo de dato OctetString se envía su equivalente en hexadecimal, por lo que tendrá de valor:7573756172696f4074657369732e636f6d, véase Fig. 5.63

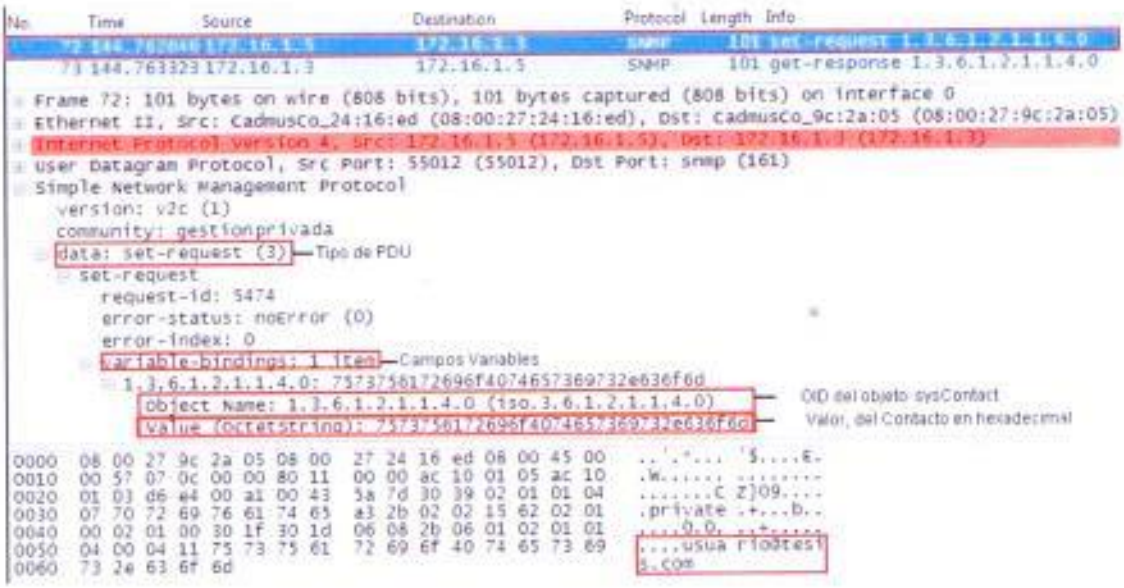


Figura 129.63 Análisis de PDU SET-REQUEST

Se identifica que GET-REQUEST tiene de request-id: 5474, cuando se reciba un GET-RESPONSE con request-id: 5474 este será la PDU que contendrá nuestra respuesta. Se comprueba que el cambio fue satisfactorio revisando los campos variables donde se mostrara el valor actual del objeto sysContact, véase Fig. 5.64

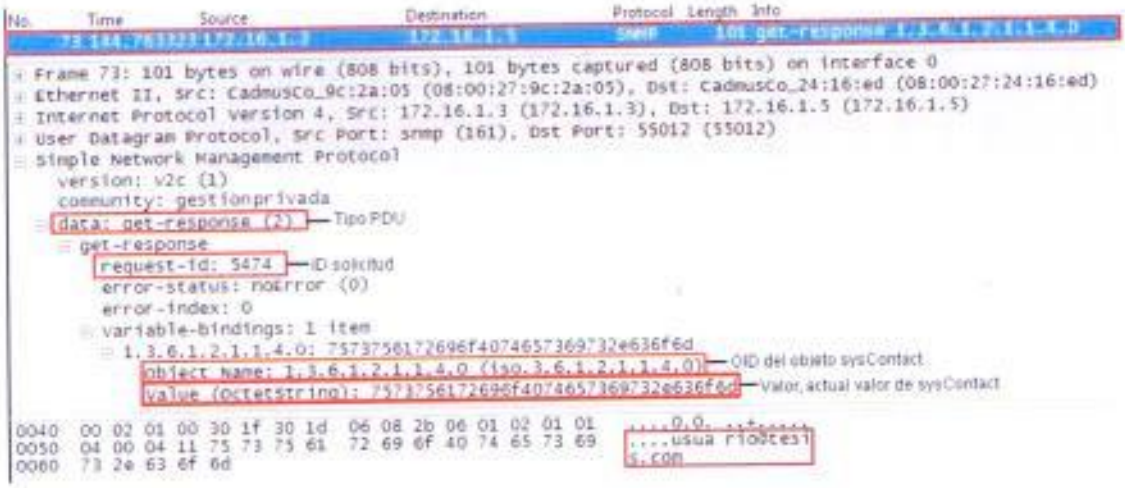


Figura 130.64 Análisis de PDU GET-RESPONSE de primitiva SET

En el escenario 2 al realizar la primitiva SET se realizo un SET-REQUEST al objeto sysName cuyo valor es de tipo de dato OctetString. En la figura vemos que dentro de la PDU de SET-REQUEST el parámetro "data" se le asigno la id: 3, correspondiente a SET-REQUEST. Dentro de los campos variables se enviara el objeto, utilizando su OID: 1.3.6.1.2.1.1.5.0 correspondiente al objeto sysName y su valor: Angel Ibarra, debido a utilizar el tipo de dato OctetString se envía su equivalente en hexadecimal, por lo que tendrá de valor: 416e67656c20496261727261, véase Fig. 5.65

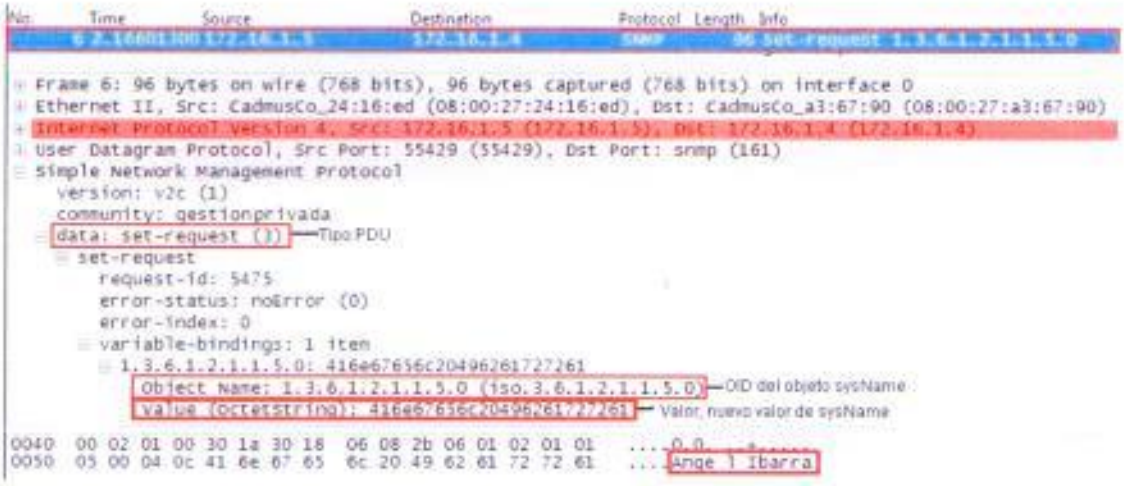


Figura 131.65 Análisis de PDU SET-REQUEST

Se identifica que GET-REQUEST tiene de request-id: 5475, cuando se reciba un GET-RESPONSE con request-id: 5475 este será la PDU que contendrá nuestra respuesta. Se comprueba que el cambio fue satisfactorio revisando los campos variables donde se mostrara el valor actual del objeto sysName, véase Fig. 5.66.

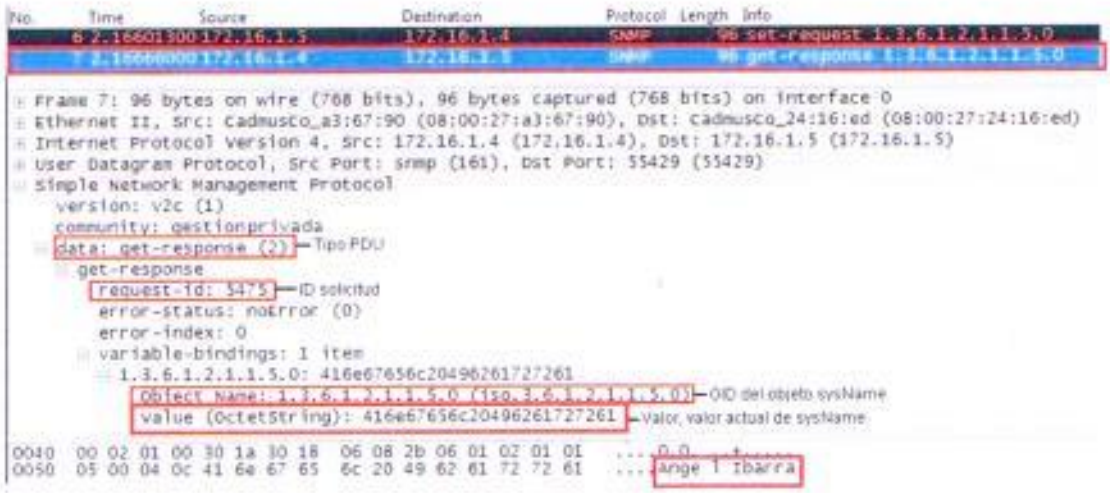


Figura 132.66 Análisis de PDU GET-RESPONSE de primitiva SET

En el escenario 3 al realizar la primitiva SET se realizo un SET-REQUEST al objeto sysLocation cuyo valor es de tipo de dato OctetString. En la figura vemos que dentro de la PDU de SET-REQUEST el parámetro "data" se le asigno la id: 3, correspondiente a SET-REQUEST. Dentro de los campos variables se enviara el objeto, utilizando su OID: 1.3.6.1.2.1.1.6.0 correspondiente al objeto sysName y su valor: Espol, debido a utilizar el tipo de dato OctetString se envía su equivalente en hexadecimal, por lo que tendrá de valor: 4573706f6c, véase Fig. 5.67.

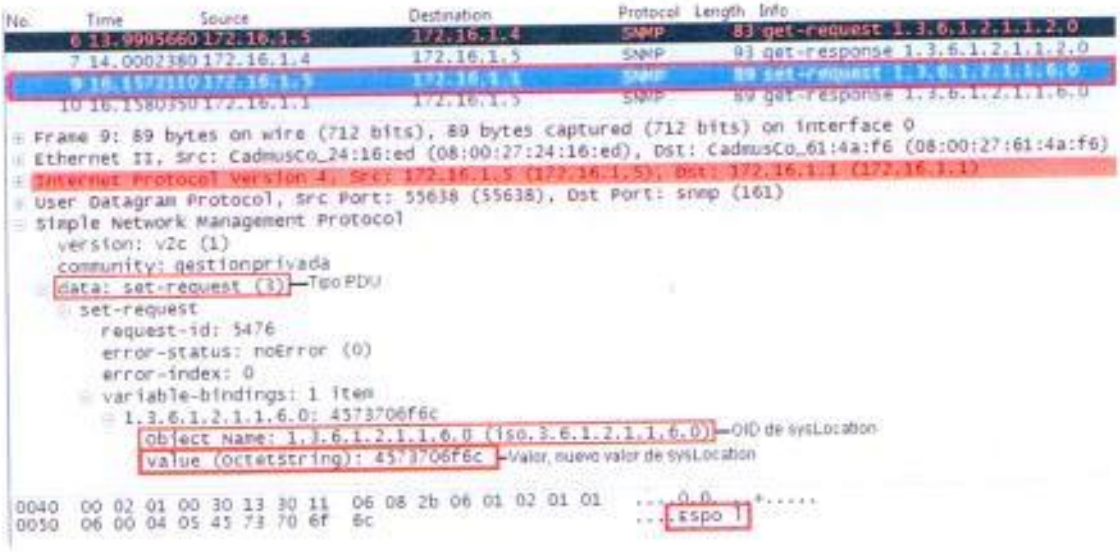


Figura 133.67 Análisis de PDU SET-REQUEST

Se identifica que GET-REQUEST tiene de request-id: 5476, cuando se reciba un GET-RESPONSE con request-id: 5476 este será la PDU que contendrá nuestra respuesta. Se comprueba que el cambio fue satisfactorio revisando los campos variables donde se mostrara el valor actual del objeto sysLocation, véase Fig. 5.68.

Figura 134.68 Análisis de PDU GET-RESPONSE de primitiva SET

ANALISIS DE LA PRIMITIVA TRAP

En el caso de las primitivas TRAP debemos recordar que son respuestas a eventos que suceden en el dispositivo y no se relaciona a ninguna acción realizada por el Gestionador. Por lo tanto solo se dispondrá de la PDU Snmpv2-trap cuyo id: 7 para el parámetro "data" correspondiente a Snmpv2-trap enviada por el dispositivo. Es diferente a las primitivas GET y SET que trabajaban con REQUEST y RESPONSE.

También están limitadas a la cantidad de TRAPS que se disponganen las MIBS que posea el dispositivo.

En el escenario 1 al momento de detener el servicio snmpd, tendremos que el Servidor de Archivos enviara la primitiva Snmpv2-trap al gestionador indicando que se detuvo el servicio, esto lo verificamos dentro del parámetro de campos variables dando como OID: 1.3.6.1.6.3.1.1.4.1.0 correspondiente al objeto snmpTrapOID y de valor la OID: 1.3.6.1.4.1.8072.4.0.2 que entre los objetos es llamada nsNotifyShutdown(Notifica que se detuvo). También provee adicional la OID: 1.3.6.1.6.3.1.1.4.3.0 correspondiente al objeto snmpTrapEnterprise y de valor la OID: 1.3.6.1.4.1.8072.4 que entre los objetos es llamado netSnmpNotificationPrefix (Notificación correspondiente a NET-SNMP), véase Fig. 5.69.

Figura 135.69 Análisis Snmpv2-trap al detener el servicio Snmpd

Al iniciar el servicio snmpd, obtenemos la PDU Snmpv2-trap desde el Servidor de Archivos donde observamos dentro del parámetro campos variables la OID: 1.3.6.1.6.3.1.1.4.1.0 correspondiente al objeto snmpTrapOID y de valor la OID: 1.3.6.1.6.3.1.1.5.1 que entre los objetos es llamado coldStart (Notifica que se inicio).También provee adicional la OID: 1.3.6.1.6.3.1.1.4.3.0 correspondiente al objeto snmpTrapEnterprise y de valor la OID: 1.3.6.1.4.1.8072.3.2.10que entre los objetos es llamado linux (Núcleo o kernel de Sistema Operativo sobre el que se encuentra el agente NET-SNMP), véase Fig. 5.70.

Figura 136.70 Análisis Snmpv2-trap al iniciar el servicio Snmpd

En el escenario 2 al momento de cambiar la comunidad en el agente, tendremos que el Servidor de Correos enviara la primitiva Snmpv2-trap al gestionador indicando que no se

logra autenticar la comunidad, esto lo verificamos dentro del parámetro de campos variables dando como OID: 1.3.6.1.6.3.1.1.4.1.0 correspondiente al objeto snmpTrapOID y de valor la OID: 1.3.6.1.6.3.1.1.5.5 que entre los objetos es llamada authenticationFailure (Notifica la falla en la autenticación). También provee adicional la OID: 1.3.6.1.6.3.1.1.4.3.0 correspondiente al objeto snmpTrapEnterprise y de valor la OID: 1.3.6.1.4.1.8072.3.2.10que entre los objetos es llamado linux (Núcleo o kernel de Sistema Operativo sobre el que se encuentra el agente NET-SNMP), véase Fig. 5.71.

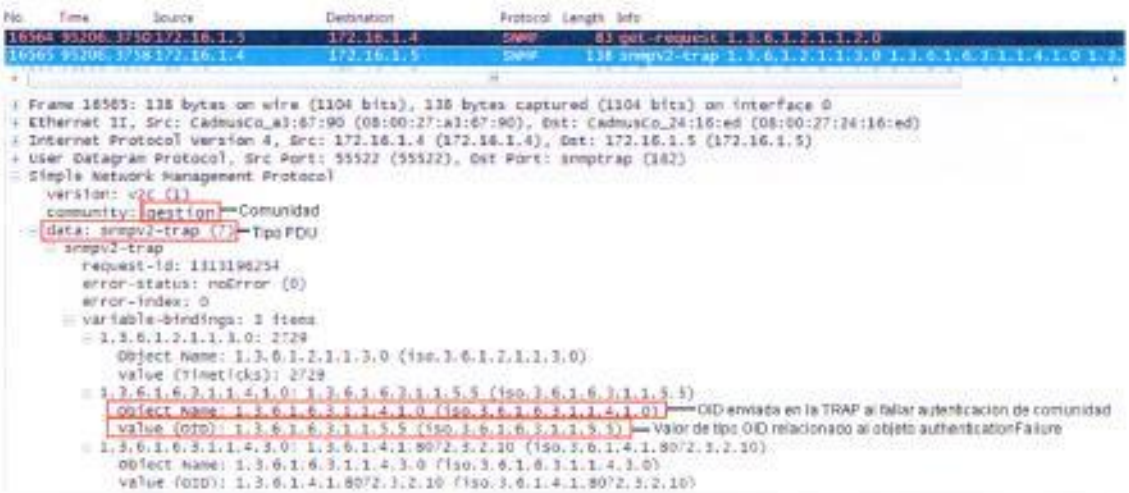


Figura 137.71 Análisis Snmpv2-trap al fallar autenticación de comunidad

En el escenario 3 al momento de apagar el Servidor Web seenviara la PDUSnmpv2-trap y la PDU informRequestal gestionador indicando que se apago el servidor. En la figura vemos la notificación de apagado del servidor, dentro de la PDU Snmpv2-trap en el parámetro de campos variables tenemos la OID: 1.3.6.1.6.3.1.1.4.1.0 correspondiente al objeto snmpTrapOID y de valor la OID: 1.3.6.1.4.1.8072.4.0.2 que entre los objetos es llamada nsNotifyShutdown. También provee adicional la OID: 1.3.6.1.6.3.1.1.4.3.0 correspondiente al objeto snmpTrapEnterprise y de valor la OID: 1.3.6.1.4.1.8072.4 que entre los objetos es llamado netSnmpNotificationPrefix (Notificación correspondiente a NET-SNMP), véase Fig. 5.72.

Figura 138.72 Análisis Snmpv2-trap al apagar el servidor

En este escenario también se dispondrá de la PDU inform-Request cuyo id: 6 para el parámetro "data" correspondiente a inform-Request enviada por el dispositivo. Dentro de la PDU inform-Request en el parámetro de campos variables tendremos las OID y valores que se encuentran en la PDU Snmpv2-trap, véase Fig. 5.73. El propósito de la primitiva INFORM está dado para comunicación entre gestores por motivo del evento o TRAP suscitado por lo tanto no exige mayor análisis adicional al previo.

Figura 139.73 Análisis InformRequest al apagar el servidor

Al encender el servidor, obtenemos la PDU Snmpv2-trap y la PDU inform-Request enviadas por el Servidor de Archivos. Observamos dentro de la PDU Snmpv2-trap que el parámetro campos variables contiene la OID: 1.3.6.1.6.3.1.1.4.1.0

correspondiente al objeto snmpTrapOID y de valor la OID: 1.3.6.1.6.3.1.1.5.1 que entre los objetos es llamado coldStart. También provee adicional la OID: 1.3.6.1.6.3.1.1.4.3.0 correspondiente al objeto snmpTrapEnterprise y de valor la OID: 1.3.6.1.4.1.8072.3.2.10 que entre los objetos es llamado Linux, véase Fig. 5.74.

Figura 140.74 Análisis Snmpv2-trap al encender el servidor

También se dispondrá de la PDU inform-Request cuyo propósito de la primitiva INFORM está dado para comunicación entre gestores por motivo del evento o TRAP suscitado al momento de encender el Servidor Web, véase Fig. 5.75.

Figura 141.75 Análisis InformRequest al encender el servidor

CONCLUSIONES

1. La simulación de la red nos permite una mejor comprensión de cómo trabajan las primitivas SNMPv2 sin la necesidad de poseer una red real para su aprendizaje.

2. Los escenarios utilizados nos permitieron aprender cómo se crean, configuran y gestionan los servidores en cada escenario, y que forman parte de una red LAN.

3. De las primitivas SNMPv2 las primitivas GET, GET-NEXT y GET-BULK están representadas por la primitiva GET en las simulaciones debido a que realizan la misma función.

4. En el manejo del programa VIRTUALBOX la creación de la red LAN es de fácil manejo y aprendiza, siendo el más óptimo para la simulación de la red.

5. La demostración de las primitivas ayudándonos de un Gestor nos permitió aprender más sobre cómo maneja la información obtenida de los objetos y las herramientas que proporciona para hacerlo.

RECOMENDACIONES

1. Es preferible para poder adquirir algunos softwares que son pagados, contactarse con soporte al cliente con el fin de obtener una demo para así probar si es o no el software que necesitamos.

2. En los servidores que poseen kernel o núcleo Linux, siempre dispondremos de MIBS que nos permitan obtener amplia información importante de los recursos físicos y lógicos.

3. Para entender los valores OctectString primero los llevamos al sistema de numeración decimal tomando cada dos valores hexadecimales, con el valor en decimal se lo compara con los Códigos ASCII y obtendremos así nuestra palabra.

4. Para poder hacer las primeras pruebas con las primitivas TRAPS deberemos comprobar que este permitido el puerto 162 entre los dos dispositivos (gestor y cliente), para evitarnos problemas podremos desactivar los firewall de ambos dispositivos.

BIBLIOGRAFÍA

[1] Barba A. (1999). Capitulo 7 Areas funcionales de gestión, pag. 94,95

[2] Universidad Industrial de Santander, Facultad de ingenierías Fisicomecánicas http://repositorio.uis.edu.co/jspui/bitstream/123456789/8095/2/116700.pdf

[3] SNMP Agent Simulator Datasheet, http://www.webnms.com/simulator/snmp-agent-simulator-ds.html

[4] Network Management Administration Guide for Routing Devices, http://www.juniper.net/techpubs/en_US/junos/information-products/pathway-pages /network-management/network-management.pdf

[5] SNMPv3 Overview, http://www.webnms.com/net-snmp/help/technology_over view/snmnpv3_overview. html

[6] Cisco Networking Academy (s.f.), Cisco Packet Tracer, https://www.netacad.com/web/about-us/cisco-packet-tracer

[7] GNS3,http://www.gns3.net/

[8] Virtualbox, https://www.virtualbox.org/

[9] Stallings w., SNMP, SNMPV2, SNMPV3, and RMON1 and 2, 3ra. Ed., Addison-Wesley,1999

[10] Douglas R., Kevin J., Essential SNMP, 2da. Ed., O´Reilly, 2005

[11] Barba A., Gestión de red, Ediciones UPC, 1999

[12] Perkins D., Mcginnis E., Understanding SNMP MIBs, Prentice Hall,1997