ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Implementación virtual de redes LAN, enfocadas en el análisis comparativo de las ventajas y desventajas del uso y aplicación de las diferentes versiones del protocolo SNMP"

TESINA DE SEMINARIO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:
Alisson Karina Lago Castillo
Daniel Marcelo Mera Moreano

GUAYAQUIL – ECUADOR
AÑO 2013

AGRADECIMIENTO

A nuestro director, el Ing. Washington Medina por su valiosa colaboración para poder desarrollar con éxito el presente proyecto de graduación.

Un agradecimiento especial a Dios, a nuestros padres, hermanos, amigos y a todas aquellas personas que siempre nos brindaron su apoyo y su ayuda incondicional.

DEDICATORIAS

Este éxito se lo dedico a Dios por haberme dado la fortaleza necesaria para culminar esta etapa de mi vida, a mi familia, por brindarme su apoyo moral y espiritual en cada una de mis decisiones tomadas, en especial a mi madre por ser mi pilar fundamental y haberme ayudado a no desfallecer en los momentos más difíciles.

Alisson Lago C.

Este logro se lo dedico a mis padres, Daniel y Magaly, a mi segundo padre, Jhonny, quienes con sus consejos y guías fueron el pilar principal de mi formación, a mis abuelos, tíos, primos, con los que he crecido y me han visto crecer, a mis amigos, y toda persona que me ha brindado su apoyo, no sería nada sin ustedes.

Daniel Mera M.

TRIBUNAL DE SUSTENTACIÓN

Mgs. Washington Medina M.

PROFESOR DEL SEMINARIO DE GRADUACIÓN

Ing. César Yepez Flores

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

DECLARACIÓN EXPRESA

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

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Alisson Karina Lago Castillo

Daniel Marcelo Mera Moreano

RESUMEN

El presente proyecto consiste en una investigación a fondo del Protocolo Simple de Administración de Red o SNMP, para captar las diferencias que existen entre las tres versiones expuestas a los usuarios. El proyecto no solo se basa en un análisis teórico, también se realizó una pequeña red LAN virtual compuesta por tres elementos de red, dos servidores y un Router, con el fin de no solo demostrar en la teoría sino también en la práctica las conclusiones obtenidas al final de la investigación.

El capítulo uno trata sobre la explicación general del proyecto, se menciona el porqué de la investigación, los objetivos, los alcances y las limitaciones a las que nos veremos expuestos.

El capítulo dos abarca todo el fundamento teórico recopilado de los diferentes RFC´s que hace mención al protocolo SNMP, mostrando los conceptos básicos, el principio operativo, las ventajas y desventajas de una versión frente a la otra, entre otras características.

El capítulo tres hace un resumen de los programas que se utilizarán para el desarrollo del proyecto, dando una breve explicación del uso y aplicación de cada uno de ellos e indicando como configurar los parámetros necesarios.

En el capítulo cuatro se definen los escenarios, es aquí donde se realizan las pruebas y simulaciones de algunas de las características expuestas en cada versión del protocolo.

Para finalizar en el capítulo cinco se presentan los resultados obtenidos donde se muestran nuestras respectivas observaciones luego de haber analizado las tres versiones, primero de manera individual y luego de manera general.

El objetivo del proyecto es brindarle al lector una explicación clara del protocolo y responder a la mayoría de sus dudas, mediante la comparación del análisis teórico y práctico de las tres versiones.

ÍNDICE GENERAL

ABREVIATURAS

CMIP	Common Management Information Protocol
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAN	Local Area Network
MA	Management Agent
MIB	Base de información de administración
NMA	Network Management Agent
NMS	Network Management Station
OSI	Open System Interconnection
PDU	Protocol Data Unit
RFC	Request For Comments
SMN	Self Managing Network
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
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Cada día, el mundo se ve enfrentado a cambios significativos en muchos ámbitos, pues la búsqueda del ser humano por satisfacer cada vez mejor sus necesidades, es el principal impulso a lo largo de toda la historia.

Las Redes de Telecomunicaciones no se quedan atrás, en la actualidad el uso de las redes se caracteriza por el constante incremento y complejidad en las estructuras de los recursos utilizados en ellas, pero a medida que se produce esta expansión se van presentando algunos hechos evidentes, pues las redes ya no pueden ser fácilmente gestionadas directamente por el hombre, se debe realizar una planificación estratégica de su crecimiento y utilizar herramientas que funcionen de manera automatizada para el control y la gestión de la red, debido a que cualquier tipo de error o falla en alguno de sus elementos pueden desencadenar una serie de problemas que afectará directa o indirectamente a los otros dispositivos conectados a ella y también a la empresa u organización que la maneja .

Es aquí donde nace la importancia de incluir en las empresas estas herramientas encargadas de gestionar de manera individual cada uno de los dispositivos y recursos pertenecientes a su red, con el fin de que ayuden al control, vigilancia y a la detección de fallas a tiempo.

En respuesta a esta necesidad se han desarrollado estándares que tratan sobre la gestión de red, los mismos que abarcan servicios, protocolos y

bases de datos de información de gestión. El enfoque de este proyecto investigativo será estudiar y analizar el estándar más utilizado, que es el SNMP.

SNMP se usa en un número de redes cada vez mayor y en entornos mucho más complejos. Razón por la cual se vio la necesidad de incluir nuevas funcionalidades que se adapten a la actual demanda, presentando tres versiones diferentes a los usuarios, dándole cada vez más la importancia a la seguridad como parte de la gestión de redes. Las mejoras de la seguridad fueron expuestas en la última versión.

Este proyecto describe el conjunto de características perteneciente a cada una de las versiones existentes del protocolo, realizando una comparación expuesta de manera sencilla con la ayuda de una red LAN.

CAPÍTULO 1

1. DESCRIPCIÓN GENERAL DEL PROYECTO

1.1 DESCRIPCIÓN

Desde que se creó el sistema de internet y de redes de comunicación, a la actualidad, estas han evolucionado y se han vuelto más complejas, por esta razón es importante mantener una correcta administración que no solo consista en un simple monitoreo de la red, si no que se involucre mucho más, realizando una gestión con herramientas que proporcionen una información más completa, amplia y eficiente que ayude en el correcto control, uso y desempeño de los equipos, para que de manera más sencilla se haga un reconocimiento del comportamiento y del estado de todo lo utilizado en la red y del estado de los mensajes. Es así como dentro de algunas herramientas existentes se encuentran ciertos protocolos que nos mantienen al tanto de este correcto funcionamiento, uno de estos es el protocolo “SNMP”.

Este se ha convertido en un protocolo bastante utilizado, porque brinda una forma simple de implementación y la funcionalidad que ofrece es variable.

Actualmente se presentan tres versiones disponibles de este protocolo; SNMPv1, SNMPv2 y SNMPv3. En las primeras dos versiones se encontraron algunos errores en lo que respecta a la seguridad del sistema, entre otras, por lo cual en la versión tres se implementaron grandes mejoras en este punto, dando una mejor seguridad, mejor autentificación y correcto control de acceso, sin embargo aunque esta es la última y mejorada versión no ha tenido tanta acogida, ni es muy aceptada como lo es la versión 2 del protocolo; es por esta razón que se ha decidido indagar en el tema realizando simulaciones y mostrando ciertas comparaciones a lo largo del proceso dentro de una red LAN virtual básica, indicando las características, las ventajas y las desventajas de cada una de las versiones disponibles, e incluyendo en la comparación la razón por la cual se emigró de la versión 1 a la versión 2 y por qué de la versión 2 no se ha emigrado por completo a la versión 3, tomando en cuenta todos los factores.

1.2 JUSTIFICACIÓN

La gestión de la Red toma una parte significativa dentro de todos los campos de las telecomunicaciones en una empresa u organización, puesto que a cada momento es importante saber la manera en que los equipos conectados a una red se están operando, si su funcionamiento

está correcto o hasta para anticiparse a daños o fallos que se puedan presentar.

Hay que tener claro que la gestión no solo está encargada de un monitoreo, se adentra mucho más buscando controlar los recursos y minimizar fallas, costos y problemas futuros, haciendo uso de varias herramientas. El SNMP es un protocolo que trabaja en la capa de aplicación del modelo OSI, facilitando el intercambio de información de administración entre los dispositivos pertenecientes a una red. Dentro de sus características generales está el permitir a los administradores supervisar en qué estado se encuentra el funcionamiento de la red, permite también buscar y resolver problemas existentes, y a planear su crecimiento.

Con el presente informe se quiere realizar un análisis específico basado en el estudio de las versiones existentes, mostrando las características de cada una de ellas, la variabilidad y las mejoras con respecto a la versión de la que proceden.

También se va a cuestionar, por qué pese a los cambios significativos de la última versión del protocolo, SNMPv3, con relación a sus predecesores, SNMPv1 y SNMPv2, sobre todo en aspectos de seguridad y control, esta no ha sido totalmente aceptada en el medio, y la versión 2 sigue ganando la mayor parte del terreno.

Se quiere abarcar el análisis de todas las características presentes, explicando no solo de manera teórica, sino también mediante procesos

que experimenten lo que sucede con cada una de las versiones con simulaciones y monitores dentro de la red.

1.3 OBJETIVOS

1.3.1 Objetivo General

Comparar mediante la simulación virtual de redes LAN las ventajas y desventajas de las tres versiones existentes del protocolo SNMP.

1.3.2 Objetivos Específicos

- Comprender los conceptos básicos del protocolo SNMP.
- Realizar un análisis teórico y establecer diferencias y semejanzas entre las versiones del SNMP.
- Analizar los Software a utilizarse, incluyendo la instalación y operación de los mismos.
- Simular virtualmente una pequeña red LAN con un Router y dos máquinas virtuales con diferentes sistemas operativos.
- Mostrar a través de simulaciones la operación del protocolo SNMPv1 dentro de la red LAN.
- Mostrar a través de simulaciones la operación del protocolo SNMPv2 dentro de la red LAN.
- Mostrar a través de simulaciones la operación del protocolo SNMPv3 dentro de la red LAN.

- Analizar y comparar los resultados obtenidos en las simulaciones.
- Explicar por qué la versión 2 tiene mayor acogida que la versión 3

1.4 METODOLOGÍA

Para lograr el resultado requerido se seguirá una serie de pasos que encierran el análisis teórico, análisis práctico, análisis de software y programas a utilizarse y análisis experimental.

Como primer punto, se realizará el análisis teórico general del protocolo SNMP, estableciendo cuáles son sus funciones, la arquitectura que maneja, la capa del modelo OSI en la que se desarrolla, su modo de operación, y lo que facilita al emplearla dentro de una red LAN, para luego pasar a detallar las características propias de cada una de las versiones de SNMP.

Como recursos se tiene un Router Mikrotik y dos máquinas virtuales con sistemas operativos correspondientes a Linux y Windows Server 2008, así como también dos Softwares Wireshark, y Net-SNMP de los cuales se aprenderá la configuración y el funcionamiento de cada uno, para luego poder mostrar detalladamente el comportamiento del sistema, el modo de seguridad brindado, el empaquetamiento.

Para el desarrollo del análisis experimental se implementarán tres pequeñas redes LAN iguales, las cuales serán configuradas bajo cada

una de las versiones existentes, las mismas que serán simuladas, para luego proceder a monitorearlas y gestionarlas.

Una vez que se recopile toda la información se continuará a detallar las características obtenidas y que marcarán las ventajas y desventajas de cada versión realizadas anteriormente en el análisis teórico.

Para finalizar, se explicarán y contestarán todas las interrogantes expuestas en la justificación del proyecto, usando como base todo lo analizado en el desarrollo.

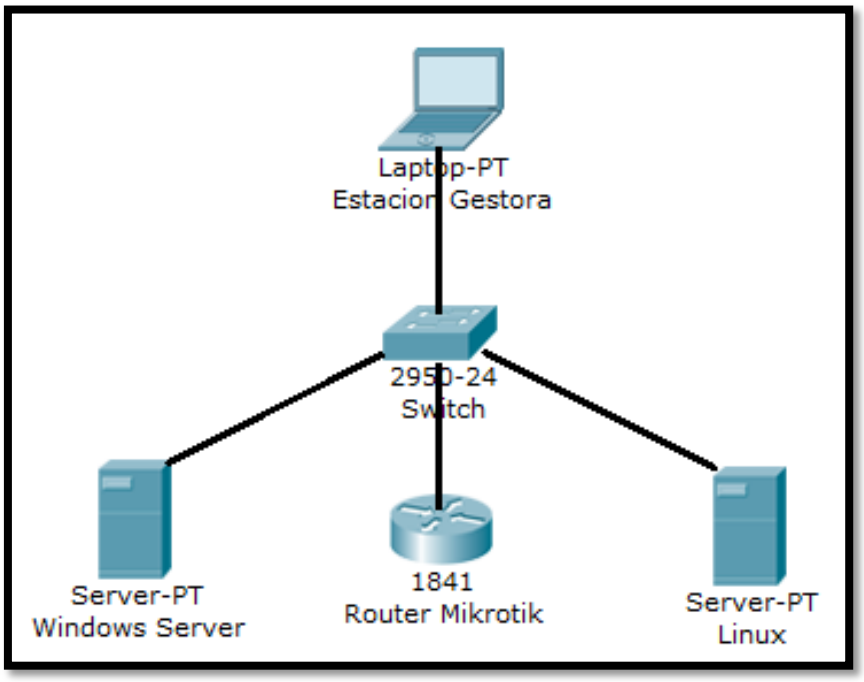


Figura 1.1: Topología a utilizarse

CAPÍTULO 2

2. FUNDAMENTO TEÓRICO

2.1 PRINCIPIO OPERATIVO DE SNMP

"Simple Network Management Protocol" o SNMP se originó en la comunidad de Internet como medida para administrar redes TCP/IP, este es un sistema de administración de red basado fundamentalmente en dos elementos principales: un administrador, el cual es el terminal que le va a permitir al administrador de la red realizar las diferentes solicitudes de administración, y los agentes, los cuales son entidades que se encuentran al nivel de cada una de las interfaces, permitiendo conectar a la red los dispositivos administrados y recopilar información sobre los diferentes objetos.

[3] SNMP funciona con el protocolo de transporte UDP (Unreliable Datagram Protocol). Para mandar un mensaje, una entidad SNMP serializa un mensaje SNMP y lo envía como un datagrama UDP a la dirección de la entidad que recibe. Los agentes SNMP están escuchando por el puerto 161.

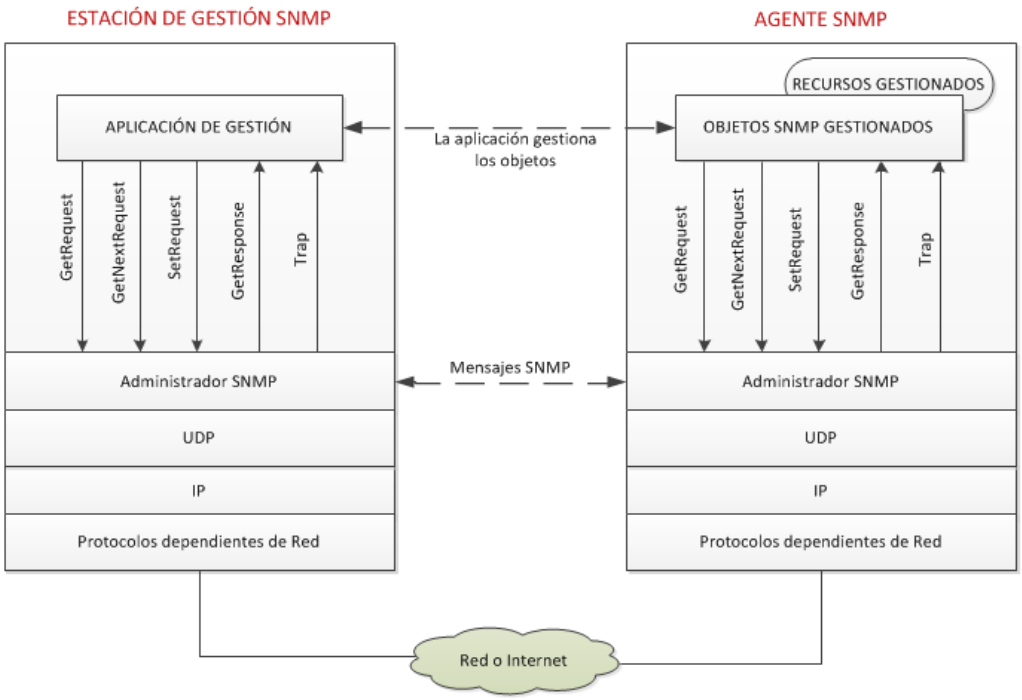
[11] SNMP se diseñó como protocolo del nivel de aplicación para formar parte de la suite de protocolos TCP/IP. Fue pensado para operar sobre UDP, así definido en la RFC 768, para una estación de gestión independiente, un proceso de administrador controla el acceso a la MIB central en la estación de gestión y proporciona una interfaz al administrador de red, es decir el proceso de administrador consigue la gestión de la red usando SNMP, que se implementa sobre UDP, IP y los protocolos dependientes de la red de que se trate (por ejemplo, Ethernet, FDDI, X.25).

Cada agente también debe implementar SNMP, UDP e IP. Además, hay un proceso agente que interpreta los mensajes SNMP y controla la MIB del agente. Para un dispositivo agente que de soporte a otras aplicaciones como FTP, se requiere TCP y UDP.

En la Figura 2.1 se ilustra el contexto del protocolo SNMP. Desde una estación de gestión se emiten tres tipos de mensajes SNMP en nombre de una aplicación de gestión: GetResquet, GetNextRequest y SetRequest. Los dos primeros son variaciones de la función Get, los tres mensajes son reconocidos por el agente mediante un mensaje GetResponse, que se entrega a la aplicación de gestión. Además, un

agente puede emitir un mensaje Trap, de interceptación, en respuesta a un hecho que afecta a la MIB y a los recursos gestionados implicados.

Debido a que SNMP se basa en UDP, que es un protocolo no orientado a conexión, SNMP es, en sí mismo, un protocolo no orientado a conexión, es decir no se mantiene conexiones entre una estación de gestión y sus agentes. En vez de ello, cada intercambio es una transacción separada entre una estación de gestión y un agente.



Fuente: Fundamentos de seguridad en redes: aplicaciones y estándares [10]

Figura 2.1: Principio Operativo SNMP

2.2 ARQUITECTURA DE ADMINISTRACIÓN DE RED

[4] La arquitectura de administración de la red propuesta por el protocolo SNMP es una colección de estaciones de gestión de redes y elementos de red, la misma que se basa en tres elementos principales: elementos de red, agentes y NMS.

- ✓ Los elementos de red son dispositivos, que serán administrados, tales como hosts, gateways, servidores terminales, entre otros, que tienen agentes de gestión responsables de realizar las funciones solicitadas por las estaciones de gestión de red.

- ✓ Los agentes o las estaciones de red ejecutan aplicaciones de gestión que monitorean y controlan los elementos de red, esas se encuentran en un periférico y son responsables de la transmisión de datos de administración local desde el periférico en formato SNMP.

- ✓ El sistema de administración de red (NMS), es un terminal a través del cual los administradores pueden llevar a cabo tareas de administración.

  El protocolo SNMP es utilizado para manejar comunicación con información de gestión entre las estaciones de gestión de red y los agentes dentro de los elementos de red.

[4] La arquitectura del protocolo SNMP articula una solución para el problema de gestión de redes en los siguientes términos:

1.- Los ámbitos de información de gestión comunicados por el protocolo
2.- La representación de la información de gestión comunicados por el protocolo
3.- Las operaciones de la información de gestión que soporta el protocolo
4.- La forma y significado de los cambios dentro de entidades de gestión
5.- La definición de relaciones administrativas dentro de entidades de gestión
6.- La forma y significado de las referencias de información de gestión.

2.2.1 **Metas de la Arquitectura**

[4] Explícitamente el protocolo SNMP minimiza el número y la complejidad de funciones de dirección realizadas por el propio agente de administración. Esta meta es atractiva en por lo menos cuatro aspectos.

1. El costo necesario para desarrollar el software que soporta el protocolo en el agente es reducido.
2. Aumenta el grado de función de administración remota, por esta razón admite un uso pleno de recursos de la internet en la tarea de administración
3. Aumenta el grado de función de administración remota, por esta razón impone menos restricciones posibles en la forma y sofisticación de herramientas de administración.
4. Simplifica conjunto de funciones de gestión fácilmente y es usado por diseñadores de herramientas de administración de red

[4] Una segunda meta del protocolo es que el paradigma funcional de monitoreo y control sea suficientemente extensible para ajustar parámetros futuros, posiblemente no anticipados en los aspectos de función y gestión de la red y una tercera meta es que sea, tanto como sea posible, independiente de la arquitectura y mecanismos de hosts o gateways particulares.

2.2.2 Elementos del protocolo SNMP

El protocolo SNMP está compuesto por 4 elementos:

1. Estación de gestión (Manager)
2. Agente administrador (Agente)
3. Base de información de administración (MIB)
4. Protocolo de administración de redes.

2.2.2.1 Estación de gestión (Manager)

[8] Se define al NMS (Network Management Station) como una interfaz entre el Administrador de red y el sistema de gestión de red, tiene una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades gestionadas en la red.

Dentro del grupo de elementos a gestionar tenemos a los hosts, pasarelas y servidores terminales. Estos elementos usan un agente de gestión, (MA), encargado de realizar estas funciones. El

protocolo SNMP es el encargado de llevar a cabo la correcta comunicación entre las NMS y los MA.

Las estaciones de red deben tener como mínimo los siguientes requisitos:

- Un conjunto de aplicaciones de gestión SNMP para analizar y recuperar datos, para la detección de las alarmas y fallas.
- Una interfaz mediante la cual se pueda realizar el monitoreo y control de la red
- La capacidad de trasladar los requerimientos del administrador a los dispositivos remotos que forman parte de la red
- Una base de datos de toda la información de gestión de la red, extraída a partir de las bases de datos de todas las entidades gestionadas en la red.

2.2.2.2 Agente administrador (Agente)

[8] El SNMP modela todas las funciones de agente de gestión como alteraciones o inspecciones de variables. Un agente responde a las solicitudes de acción desde la estación gestora y puede proporcionarle de una forma asíncrona información importante.
Es un módulo del software de gestión de red que reside en los dispositivos gestionados.

El agente, al recibir un GetRequest o GetNextRequest, emitirá un mensaje GetResponse a la estación gestora, ya sea con la información solicitada o una indicación de error indicando porqué la solicitud no pudo ser procesada.

Con un SetRequest, SNMP permite solicitar un cambio de valor a una variable específica en este caso, el agente SNMP responderá con un GetResponse que indicará que el cambio se ha hecho o en el caso de que este no pueda realizarse responderá con una indicación de error. Con el Trap, SNMP permitirá que el agente informe espontáneamente a la estación gestora de un evento "importante".

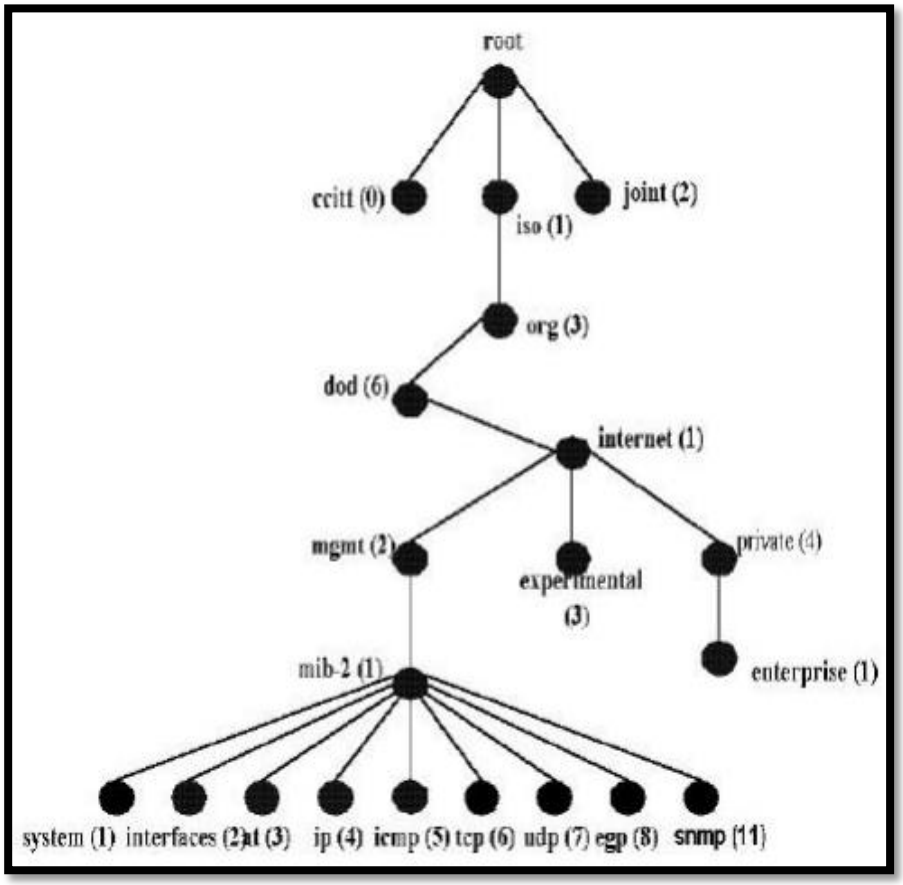
2.2.2.3 Base de información de administración (MIB)

[1] MIB es un tipo de base de datos definida en el modelo OSI, su función principal es definir las variables que utiliza el protocolo SNMP para la gestión control y supervisión de los dispositivos de red. Su formato de información está disponible en forma jerárquica que a diferencia de la forma relacional, los detalles de información se establecen siempre a nivel físico, es decir, mediante referencias a direcciones físicas del medio de almacenamiento. Es gracias a esta forma de relación que se define a la MIB como una estructura en forma de árbol conteniendo detalles de todos los elementos o dispositivos gestionados dentro de una red, pero las relaciones de este tipo son unidireccionales, es decir, para este caso, de nodos hijo a raíz, hacer una búsqueda de información en la otra dirección

requiere búsquedas secuenciales por todos los registros existentes, lo cual permite llegar a la conclusión de que para algunos casos obtener respuestas en este tipo de estructuración puede ser muy fácil, pero en otros casos puede ser muy complicado.

[4] Como existen diferentes tipos de objetos para representar los diferentes dispositivos de red, cada objeto manejado en el MIB tiene un identificador de objeto único, y a su vez incluye el tipo de objeto (Counter, Secuence, Gauge), el nivel de acceso (Read-Only, Write), limitación en tamaño y su información de rango.

- Cada elemento SNMP maneja objetos específicos con cada objeto teniendo características específicas.
- Cada objeto/característica tiene un único identificador de objeto (OID) el cual consiste de números separados por puntos decimales (ej. 1.3.6.1.4.1.2682.1).
- Estos identificadores de objetos forman un árbol.
- El MIB asocia cada OID con una etiqueta legible (ej., dpsRTUAState) y varios otros parámetros relacionados al objeto.
- En este caso el MIB sirve como un diccionario de datos o libro de códigos que es usado para ensamblar e interpretar mensajes SNMP.



Fuente: Barba Marti, A. Gestión de red, Ediciones OPC [1]

Figura 2.2: Esquema jerárquico de nombrado utilizado en la MIB

2.2.2.4 Protocolo de administración de redes.

[8] El protocolo de administración de red es un protocolo de aplicación por el cual pueden examinar o cambiar varias MIB de un agente. La comunicación de información de administración entre

las entidades de gestión (gestor-agente) es realizada en el SNMP a través del intercambio de mensajes protocolares.

El protocolo de administración es el encargado de enlazar la estación de gestión y los agentes La estrategia implícita en el protocolo SNMP es que el monitoreo de estado de red a cualquier nivel significante de detalle es llevado a cabo principalmente por el sondeo de información adecuada por parte de la central de monitoreo. Un número limitado de mensajes no solicitados denominados Traps mantiene el tiempo y la atención del sondeo. Limitar el número de mensajes no solicitados va acorde con la meta de simplicidad y de minimizar la cantidad de tráfico generado por las funciones de gestión de red.

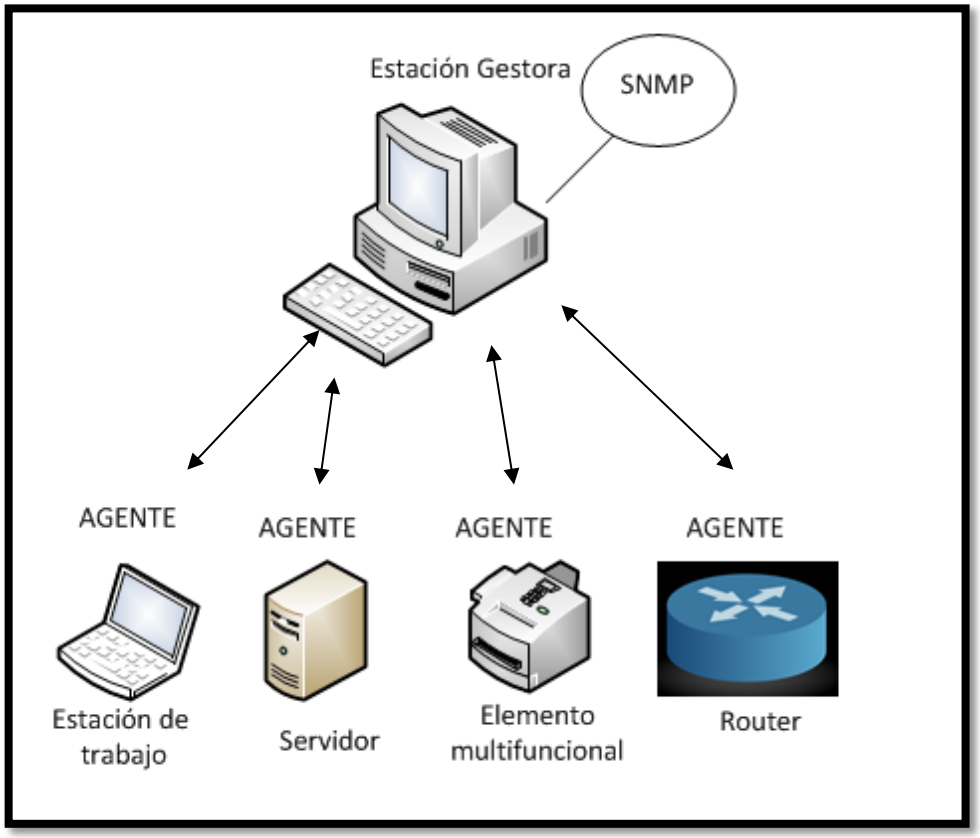


Figura 2.3: Elementos del protocolo de Gestión de SNMP

2.2.3 Estructura de la PDU

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

Todas las implementaciones del SNMP soportan 5 tipos de PDU:

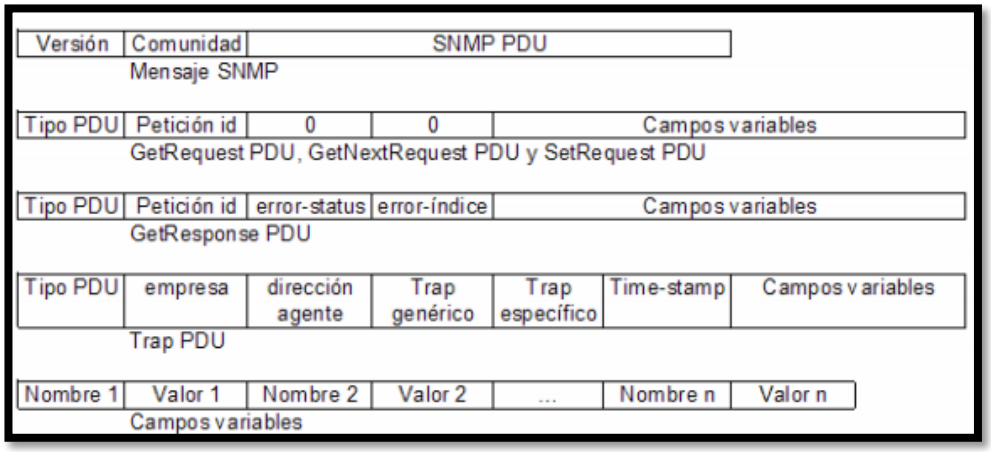
1. GetRequest
2. GetNextRequest
3. GetResponse
4. SetRequest
5. Trap

[7] Los datos que incluye una PDU genérica son los siguientes:

- Versión: Indica la versión del protocolo SNMP
- Comunity Name: Nombre de la comunidad para autentificar un mensaje SNMP
- RequestID: Entero que indica el orden de emisión de los datagramas. Este parámetro sirve también para identificar datagramas duplicados en los servicios de datagramas poco fiables.
- ErrorStatus: Entero que indica si ha existido un error. Puede tomar los siguientes valores, que se explicarán posteriormente:
  - noError (0)
  - tooBig (1)
  - noSuchName (2)
  - badValue (3)
  - readOnly (4)
  - genErr (5)
- ErrorIndex: Entero que en caso de error indica qué variable de una lista ha generado ese error.

- VarBindList: Lista de nombres de variables con su valor asociado.

  Algunas PDU quedan definidas sólo con los nombres, pero aún así deben llevar valores asociados. Se recomienda para estos casos la definición de un valor NULL.



Fuente: Barba Marti, A. Gestión de red, Ediciones OPC [1]

Figura 2.4: Estructura de la PDU

2.2.3.1 Get-Request

[4] Es una PDU que solicita a la entidad destino los valores de ciertas variables, las mismas que se encuentran en la lista VarBindList; en el de GetNextRequest

Esta PDU siempre tiene cero en los campos ErrorStatus y ErrorIndex y es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP.

El GetRequest siempre espera como respuesta una GetResponse.

2.2.3.2 Get-Next-Request

[4] Es una PDU que solicita a la entidad destino los valores de ciertas variables, estas son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista VarBindList, El GetNextRequest es útil para confeccionar tablas de información sobre una MIB.

Esta PDU al igual que el GetRequest siempre tiene cero en los campos ErrorStatus y ErrorIndex y es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP.

El GetNextRequest siempre espera como respuesta una GetResponse.

2.2.3.3 Get-Response

[4] La forma del GetResponse es idéntica a la del GetRequest a excepción de la indicación del tipo de PDU. El GetResponse se genera por una entidad de protocolo únicamente a la recepción de la GetRequest, GetNextRequest, o SetRequest.

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

1. Si algún nombre de la lista no coincide con el nombre de algún objeto en la vista del MIB al que se pueda realizar el tipo de operación requerido ("set" o "get"), la entidad envía al remitente del mensaje un GetResponse con un formato idéntico al recibido, pero con el campo ErrorStatus puesto a 2 (noSuchName), y con el campo ErrorIndex indicando el nombre de objeto en la lista recibida que ha originado el error.

2. De la misma manera actúa si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era un GetRequest.

3. Si se ha recibido un SetRequest y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente un GetResponse idéntico al recibido, salvo en que el campo ErrorStatus tendrá el valor 3 (badValue) y el campo ErrorIndex señalará el objeto de la lista que ha generado el error.

4. Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente un GetResponse con un formato idéntico al recibido, pero con el campo ErrorStatus puesto a 1 (tooBig).

5. Si el valor de algún objeto de la lista no puede ser obtenido por una razón no contemplada en las reglas anteriores, la

entidad envía al remitente un GetResponse con un formato idéntico al recibido, pero con el campo ErrorStatus puesto a 5 (genErr), y el campo ErrorIndex indicando el objeto de la lista que ha originado el error. Si no se llega a aplicar alguna de estas reglas, la entidad enviará al remitente una GetResponse-PDU de las siguientes características:

- Si es una respuesta a un GetRequest, tendrá la lista varBindList recibida, pero asignando a cada nombre de objeto el valor correspondiente.

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

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

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

2.2.3.4 Set-Request

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

2.2.3.5 Trap

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

2.3 ASPECTOS GENERALES DE CADA VERSIÓN

En la actualidad, existen tres versiones del protocolo SNMP definidas como: SNMPv1, SNMPv2 y SNMPv3. Las primeras dos versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras respecto a la versión 1, como las operaciones de protocolo adicionales.

Sin embargo a los pocos años se creó una nueva y mejorada versión, SNMP versión 3, la cual añade capacidades de configuración y mejor seguridad, autentificación, correcto control de acceso y mando a distancia para las versiones anteriores. Para resolver el problema de ediciones incompatibles entre diferentes versiones de SNMP, Se crea el RFC 3584 el cual define estrategias de coexistencia.

2.3.1 Protocolo de administración simple versión 1

[14] SNMPv1 constituye la primera definición e implementación del protocolo SNMP, estando descrito en las RFC 1155, 1157 y 1212 del IETF (Internet Engineering Task Force).Es un protocolo de petición y respuesta sencilla. Su comportamiento se implementa mediante el uso de una de las cuatro operaciones de protocolo: Get, GetNext, Set, y Trap. La operación Get se utiliza por el NMS para recuperar el valor de una o más instancias de objetos de un agente. La operación GetNext es utilizada por el NMS para recuperar el valor de la siguiente instancia de objeto de una tabla o una lista dentro de un agente. La operación Set es utilizada por el NMS para configurar los valores de instancias de objetos dentro de un agente. La operación Trap es utilizada por los agentes para informar de forma asíncrona el SMN de un hecho relevante.

2.3.2 Protocolo de administración simple versión 2

[14] SNMPv2 apareció en 1993, estando definido en las RFC 1441-1452. SNMPv1 y SNMPv2 tienen muchas características en común,

siendo la principal mejora la introducción de nuevas operaciones de protocolo:
GetBulk: para que el gestor recupere de una forma eficiente grandes bloques de datos, tales como las columnas de una tabla
Inform: para que un agente envíe información espontánea al gestor y reciba una confirmación
Report: para que el agente envíe de forma espontánea excepciones y errores de protocolo.

SNMPv2 también incorpora un conjunto mayor de códigos de error y más colecciones de datos. En 1995 apareció una revisión de SNMPv2, denominada SNMPv2c y descrita en las RFC 1901-1910, añadiendo como mejoras una configuración más sencilla y una mayor modularidad; pero manteniendo el sencillo e inseguro mecanismo de autentificación de SNMPv1 y SNMPv2 basado en la correspondencia del denominado nombre de comunidad.

2.3.3 Protocolo de administración simple versión 3

[14] La nueva y última versión de SNMP, SNMPv3, refuerza las prestaciones de seguridad, incluyendo autentificación, privacidad y control de acceso; y de administración de protocolo, con una mayor modularidad y la posibilidad de configuración remota. SNMPv3 apareció en 1997, estando descrito en las RFC 1902-1908 y 2271-2275.

Cabe destacar que SNMPv3 no se trata de un estándar que reemplaza a SNMPv1 y/o SNMPv2, sino que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunción con SNMPv2 (preferiblemente) o SNMPv1. Estas mejoras harán que SNMP se constituya en un protocolo de gestión susceptible de ser utilizado con altas prestaciones en todo tipo de redes, desplazando a mediano plazo a CMIP como estándar de gestión de las grandes redes de las operadoras de telecomunicación.

Fue diseñada para proteger contra las siguientes amenazas de seguridad, mediante el uso de algoritmos de autenticación y de encriptación, como lo especifica el RFC 2574

- ✓ Modificación de la información: una entidad podría alterar un mensaje generado por otra que esta autenticada y así lograr que haya una acción no autorizada en la entidad que recibe el mensaje. El problema aquí es que se podría modificar algún parámetro de configuración.

- ✓ Enmascaramiento (masquerade): Un usuario no autorizado puede intentar realizar operaciones asumiendo la identidad de otro usuario que si posee autorización para la operación deseada.

- ✓ Reenvío de mensajes: como SNMP opera sobre un protocolo de transporte sin conexión, existe el riesgo que un mensaje SNMP sea almacenado por algún tercero y luego, reenviado o

duplicado, para realizar operaciones de administración no autorizadas.

- ✓ Poca privacidad (disclosure): una entidad puede observar el intercambio de mensajes entre un agente y una consola de administración y así, aprender de los valores de los objetos.

2.4 VENTAJAS Y DESVENTAJAS GENERALES DE SNMP

2.4.1 Ventajas

- ✓ La ventaja fundamental de usar el protocolo SNMP es que su diseño es bastante simple lo que hace que su implementación sea sencilla en grandes redes.

- ✓ La operación de su gestión que se necesita para intercambiar información ocupa pocos recursos de la red.

- ✓ Permite al usuario elegir las variables que se desea monitorear sol definiendo
  - El título
  - El tipo de datos de las variables
  - Si la variable es solo de lectura o también de escritura
  - El valor de la variable

- ✓ Tiene la capacidad para recopilar información sobre muchos tipos de agentes Trap en la estación de administración de red y notificación de la ocurrencia de eventos específicos

- ✓ Puede generar relativamente poco tráfico mediante el uso de UDP

- ✓ Permite controlar la cantidad de datos enviados a la red y el tiempo de espera para los equipos de respuesta.

- ✓ Existe compatibilidad de las diferentes versiones de bases de datos con diferentes versiones de SNMP, con algunas excepciones

- ✓ Tiene un buen sistema de seguridad mediante el uso de algoritmos de cifrado conocido principalmente implementado en la versión 3

2.4.2 Desventajas

- ✓ En cuanto a sus desventajas la primera deficiencia de SNMP es que tiene grandes fallos de seguridad que pueden permitir el acceso a cualquier tipo de persona a la información que lleva la red, pudiendo bloquear o deshabilitar terminales, esto se ha solucionado en su mayor punto en la versión 3

- ✓ Por otro lado, se definió que no estaba diseñado para prevenir estos tipos de ataques:

- Denegación de servicio (DoS): prevenir que haya intercambio de mensajes entre agente y consola de administración.
- Análisis de tráfico: un atacante puede observar los patrones de tráfico entre estas dos entidades.

✓ No hay mecanismos adecuados para garantizar la seguridad en SNMPv1 y SNMPv2

✓ No es posible aceptar la recepción de un aviso enviado por el Agente. No hay confirmación durante la transmisión de datos.

CAPÍTULO 3

3. DESCRIPCIÓN E IMPLEMENTACIÓN VIRTUAL DEL PROYECTO

3.1 INTRODUCCIÓN

Para el desarrollo del proyecto se implementará una red LAN virtual, la cual consiste en la simulación de dos sistemas operativos, Windows y Linux, y un enrutador de red, con el fin de observar el intercambio de información en cada uno de estos tres dispositivos de red haciendo uso del protocolo SNMP.

Hay que tener en cuenta que los dispositivos y programas que se usen deben ser compatibles con las tres versiones existentes del protocolo, razón por la que se realizó un estudio previo de los software a utilizarse en el proyecto.

3.2 SOFTWARE

3.2.1 Sistemas Operativos

[11] Los Sistemas Operativos son el software básico de toda computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario.

Sus funciones son administrar los recursos de la máquina, coordinar el hardware y organizar archivos y directorios en dispositivos de almacenamiento.

Los sistemas operativos usados en el proyecto son Windows y Linux pero como todo el desarrollo se realizara dentro de una misma computadora se hará uso de máquinas virtuales, las mismas que simularan a las dos servidores y les permitirán ejecutar programas como si fueran computadoras reales.

3.2.1.1 Windows Server 2008

Este sistema operativo está diseñado para ofrecer a las organizaciones la plataforma más productiva para virtualización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Ofrece una plataforma segura y de fácil administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web. Del grupo de trabajo al centro de datos, Windows Server 2008 incluye nuevas funciones de gran valor y eficacia y mejoras impactantes en el sistema operativo base.

3.2.1.2 Linux CentOS

CentOS es una distribución del código fuente de Red Hat Enterprise Linux contando con las mismas características y funcionalidades, es de clase empresarial derivado de fuentes libremente ofrecidas al público y se compone de Software libre y código abierto.

CentOS es realizado por un equipo pequeño pero creciente grupo de desarrolladores del núcleo. A su vez los desarrolladores centrales son apoyados por una activa comunidad de usuarios como los administradores de sistemas, administradores de red, los usuarios empresariales, gerentes, principales contribuyentes de Linux y los entusiastas de Linux de todo el mundo.

3.2.2 Router

[10] Un Router es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un Router (mediante bridges), y que por tanto tienen prefijos de red distintos.

Para el desarrollo del proyecto se hará uso de un Mikrotik, este un sistema Operativo de Router, es decir que con él se podrá convertir cualquier computador en un poderoso Router y no necesita de un

sistema operativo previamente instalado, ya que la herramienta viene encapsulada dentro de un microkernel de Linux, lo que brinda flexibilidad y escalabilidad.

3.2.3 Programa Net-SNMP

[12] Net-snmp es un programa que provee herramientas y librerías relacionadas al protocolo SNMP que incluye: un agente extensible, esto quiere decir que el agente básico que viene con el programa puede ser extendido a manejar otras MIB's que uno puede desarrollar y estas pueden ser fácilmente introducidas al agente, por lo cual, éste puede monitorear lo que se le ha incorporado; una librería SNMP, provee una implementación del protocolo con la funcionalidad especificada en los RFC's que definen el funcionamiento de SNMPv1, SNMPv2 y SNMPv3; herramientas para obtener y modificar información de agentes SNMP; herramientas para generar y manejar Traps; un "compilador" de MIB's que se encarga de generar una plantilla de código en lenguaje C, y que implementa alguna de la funcionalidad final que tendría lo que uno está programando; entre otras cosas.

Por esta razón se decidió usar este programa en dos partes del proyecto: en la máquina de la estación gestora y en la maquina virtual que contiene al Windows Server.

3.2.4 Programa WireShark

[13] WireShark un analizador de paquetes de red, una utilidad que captura todo tipo de información que pasa a través de una conexión. Wireshark es gratis y de código abierto, y se puede usar para diagnosticar problemas de red, efectuar auditorías de seguridad y aprender más sobre redes informáticas.

Uno de los usos más principales de Wireshark es la captura de paquetes, cuyos contenidos (mensajes, código, o contraseñas) son visibles con un clic. Los datos se pueden filtrar, copiar al portapapeles o exportar.

Las capturas se inician y controlan desde el menú Capture; presiona Control+E para empezar o detener la recogida de paquetes. Las herramientas de análisis y estadísticas de Wireshark permiten estudiar a fondo los resultados.

Como muchas utilidades de su tipo, Wireshark puede usarse para toda clase de propósitos, y solo del usuario depende el uso correcto de sus funcionalidades.

3.3 INSTALACIÓN Y CONFIGURACIÓN

3.3.1 Instalación y Configuración de Sistemas Operativos

3.3.1.1 Instalación y Configuración de SNMP en Windows server 2008

Para el caso de Windows, como se mencionó al inicio del capítulo, no es posible activar el protocolo del sistema operativo de forma directa debido a que el sistema operativo no soporta las tres versiones existentes del protocolo SNMP lo cual nos genera inconvenientes para el desarrollo del proyecto debido a que es de suma importancia analizar el comportamiento de cada una de las versiones existentes. Como solución proponemos el uso de Net-Snmp. A continuación se muestra los pasos para la instalación:

1. Primero es necesario cambiar la Dirección IP asignada a nuestro equipo de trabajo con una perteneciente a la Red LAN que se utilizará.

Para realizarlo se deben seguir los siguientes pasos, Ingresar a:

"Panel de control"

"Network and Internet"

"Network and sharing center"

"Local Area Connection"

"Properties"

"Internet Protocol Version 4"

Se procederá a realizar estos cambios manualmente con los datos respectivos, la dirección Ip que se le ha asignado al Windows Server es 192.168.199.52, entonces su Máscara de Red será 255.255.255.0. Véase figura 3.1

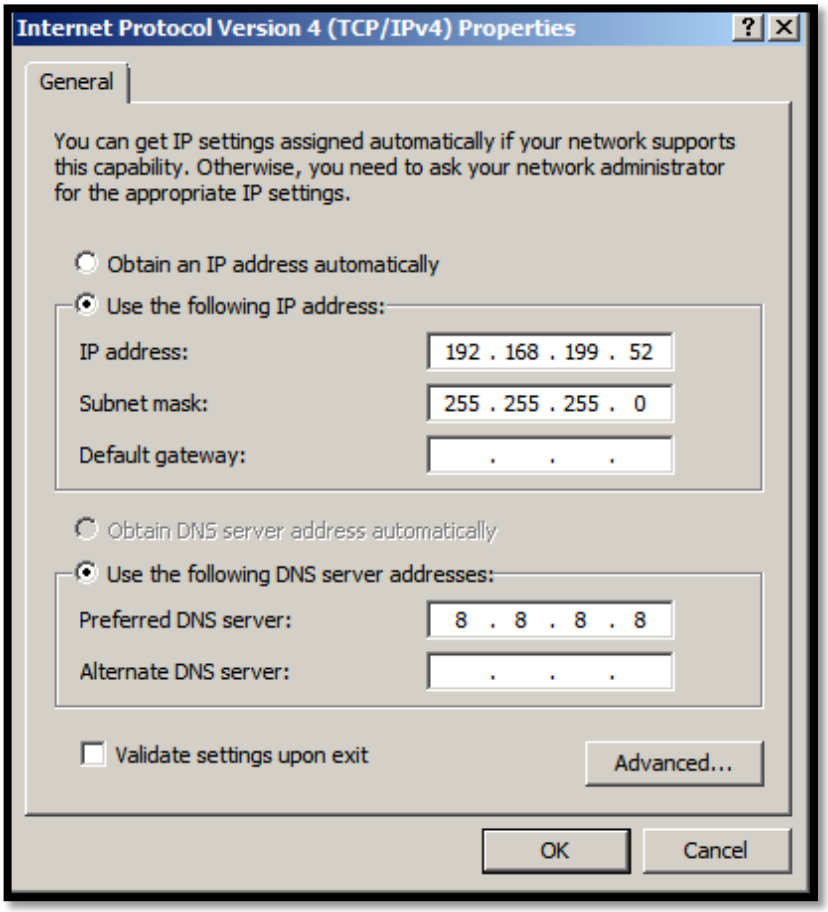


Figura 3.1: Configuración de Ip

2. Descargar el programa Net-SNMP desde el siguiente enlace, e instalarlo:

   http://sourceforge.net/projects/netsnmp/files/latest/download?source=files

3. Una vez instalado el agente NetSNMP, se debe copiar los siguientes archivos: el snmpd.conf y snmp.conf en el directorio c: \ usr \ etc \ snmp

El archivo snmpd.conf es el que contiene toda la información correspondiente a la configuración de las versiones, nombre de la comunidad, usuarios, grupos y contraseñas, respectivamente, un archivo muy similar se creará en Linux.

```
com2sec local 127.0.0.1 gestiondered
com2sec miredlocal 192.168.199.50 gestiondered
com2sec miredlocal 192.168.0.51 gestiondered
createUser version3 MD5 12345678 DES 12345678
#Se asigna ACL al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
#Se asigna ACL al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm version3
# Ramas MIB que se permiten ver
## name   incl/excl subtree   mask(optional)
view all  included  .1        80
# Establece permisos de lectura y escritura
## group         context  sec.model sec.level prefix read   write
notif
access MyROGroup ""       any       noauth    exact  all    none
none
access MyRWGroup ""       any       noauth    exact  all    all
all
# InformaciÃ³e Contacto del Sistema
syslocation Servidor Windows en red local
syscontact Administrador (alisson@lago.net)
rouser alisson
```

Figura 3.2: Archivo snmpd.conf

4. Luego de editar ese archivo, se debe registrar el agente mediante la ejecución del archivo registeragent.bat, el mismo que se encuentra en el directorio c: \ usr.

5. Para finalizar se debe iniciar el agente por medio de cmd con el siguiente comando: net start "agente net-snmp"

Si se hace algún cambio en el archivo snmpd.conf se debe restaurar el agente NetSNMP mediante los siguientes comandos y verificamos que este activo:

- net stop "agente net-snmp"
- net start "agente net-snmp"
- netstat -ano

Con la ejecución del último comando en la Figura 3.3 se puede observar que la IP y el puerto 161 ya están habilitados para trabajar con las operaciones de SNMP GetRequest, GetNextRequest, GetResponse y Set.

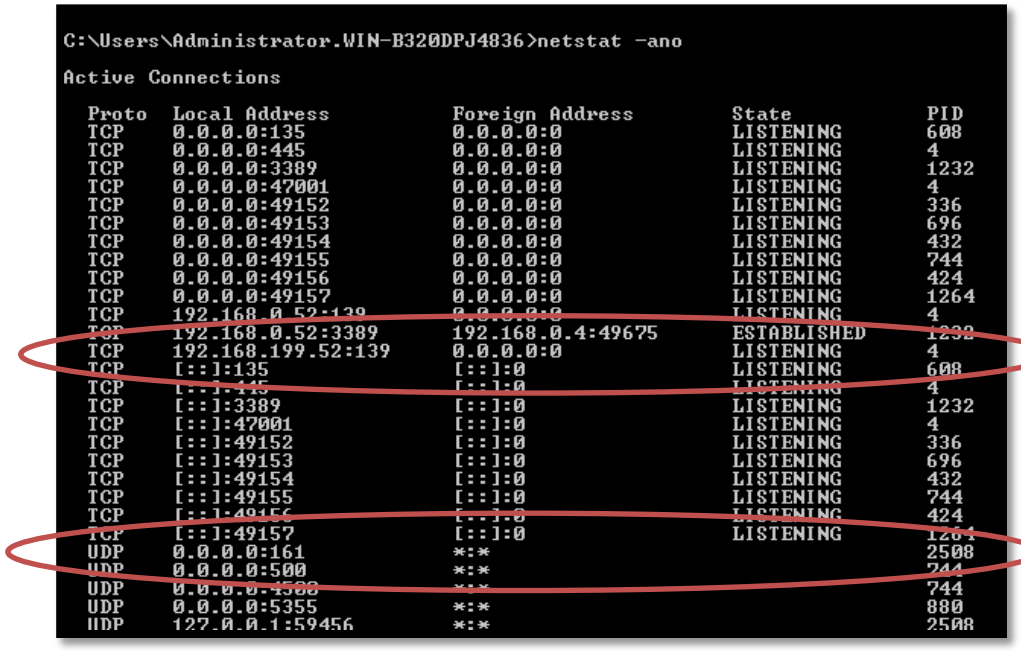


Figura 3.3: Comprobación de habilitación de puerto 161

En la Figura 3.4 se muestra que el puerto 162 está habilitado, por medio de este se generarán las Traps.

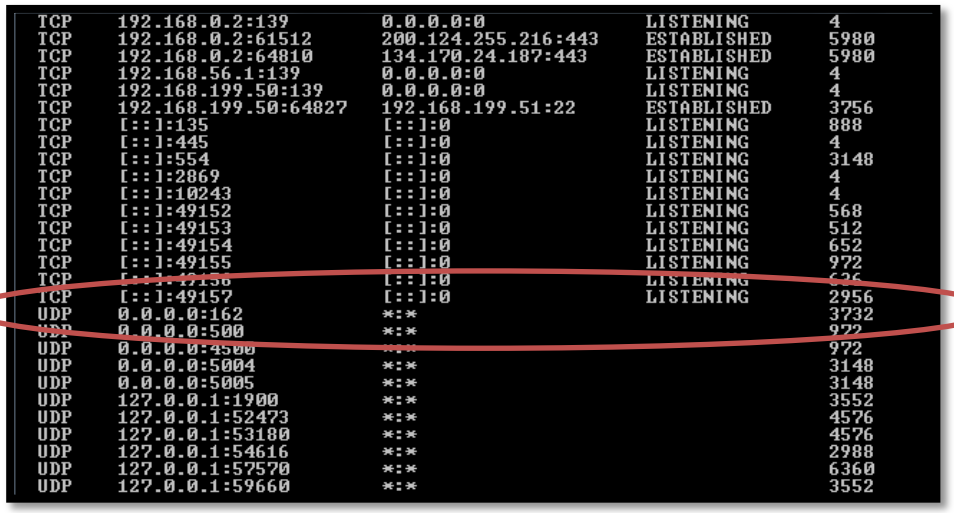


Figura 3.4: Comprobación de habilitación del puerto 162

3.3.1.2 Instalación y Configuración de SNMP en LINUX

1. Al igual que en Windows primero hay que cambiar la Dirección Ip, Mascara y Gateway con datos que pertenezcan a la Red LAN que se utilizara esto se lo realiza con los siguientes comandos:

   - ***Vi /etc/sysconfig/network-scripts***

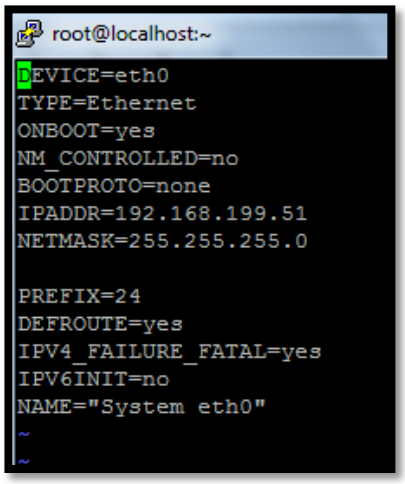


Figura 3.5: Archivo Network-Scripts para cambio de IP

Los siguientes comandos también son válidos, pero no los usamos porque estos tendrían que editarse cada vez que ingresemos al sistema operativo:

- ***ifconfig eth0 192.168.199.51 netmask 255.255.255.0 up***
- ***ip route add default via 192.168.0.1***

2. Una vez cambiada y verificada la dirección IP el siguiente paso será la configuración de SNMP, se lo realiza con el siguiente comando :

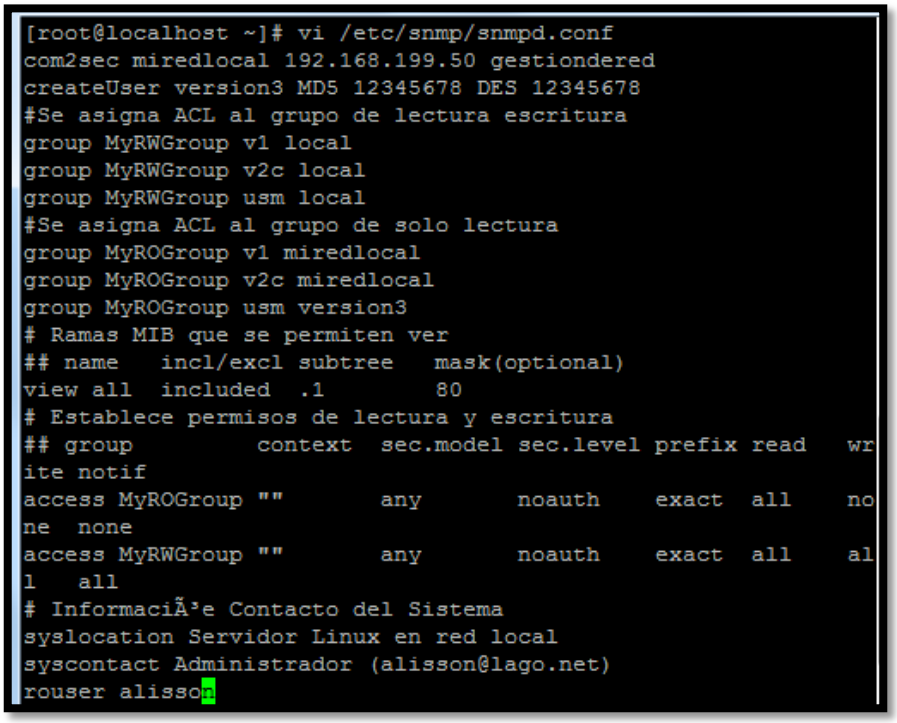
- ***yum -y install net-snmp net-snmp-utils***

3. Una vez finalizado se debe cambiar de directorio y respaldar el archivo snmpd.conf, debido a que este podrá ser editado más adelante, se usan los siguientes comandos:

   - ***cd /etc/snmp***
   - ***mv snmpd.conf snmpd.conf-OLD***
   - ***touch snmpd.conf***

4. una vez respaldado se ingresa al directorio para proceder a editarlo con el siguiente comando:
   - vi /etc/snmp/snmp.conf

Y se edita la ventana con los siguientes datos para hacer la configuración respectiva de las tres versiones del protocolo agregando el nombre de la comunidad y usuario contraseñas y grupo respectivamente. Véase Figura3.6



```
[root@localhost ~]# vi /etc/snmp/snmpd.conf
com2sec miredlocal 192.168.199.50 gestiondered
createUser version3 MD5 12345678 DES 12345678
#Se asigna ACL al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
#Se asigna ACL al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm version3
# Ramas MIB que se permiten ver
## name   incl/excl subtree   mask(optional)
view all  included  .1        80
# Establece permisos de lectura y escritura
## group         context  sec.model sec.level prefix read   wr
ite notif
access MyROGroup ""       any       noauth    exact  all    no
ne  none
access MyRWGroup ""       any       noauth    exact  all    al
l   all
# InformaciÃ³e Contacto del Sistema
syslocation Servidor Linux en red local
syscontact Administrador (alisson@lago.net)
rouser alisso
```

Figura 3.6: Archivo snmpd.conf de Linux

5. Se reinicia el servicio de SNMP y se añade éste al resto de los servicios que arrancan junto con el sistema:

   - ***service snmpd start***
   - ***chkconfig snmpd on***

3.3.2 Instalación y Configuración del Router

Como se mencionó anteriormente se hará uso de un Router Mikrotik, para poder realizar la configuración de una manera más sencilla nos

ayudaremos con el programa Winbox, esta es una herramienta para configurar la interfaz del equipo de Mikrotik.

Para obtener los programas hay que dirigirse a la página http://www.mikrotik.com/download, la cual los ofrece de manera gratuita, la instalación es bastante sencilla se crea una máquina virtual y en almacenamiento se dirige hacia el Archivo Iso del Mikrotik. Para Winbox simplemente se pone ejecutar y este funcionará inmediatamente.

1. Se debe indicar la dirección Ip con la que operará el Router dentro de la red, esta será 192.168.199.53. Se lo hace desde la máquina virtual.

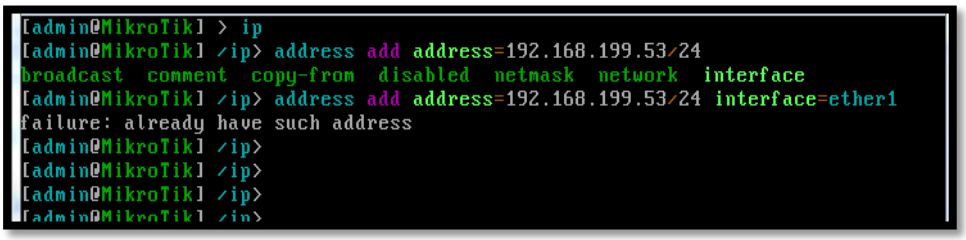


Figura 3.7: Configuración IP en Router Mikrotik

2. Se ingresa al programa Winbox, este pedirá la dirección Ip asignada al Router, se la ingresa y se hace click en “Connect”

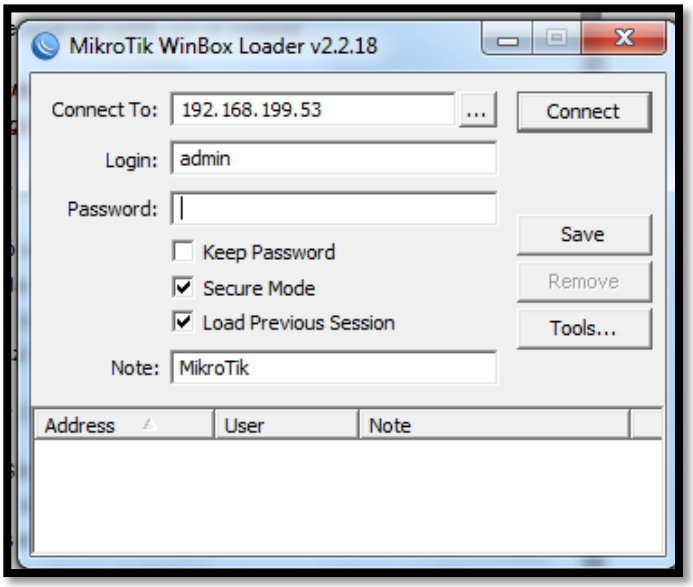


Figura 3.8: Inicialización del Programa Winbox

3. Una vez dentro, Ingresar a: IP y hacer click en SNMP. Se abrirá una nueva ventana donde se deben llenar los datos correspondientes, para SNMPv1 y SNMPv2 se ingresará el nombre de la comunidad y la dirección Ip del destino dónde llegarán los avisos de “TRAP”, luego se hace click en “Apply”. Véase Figura 3.9

   Para el caso de SNMPv3 al momento de especificar la versión 3, pedirá el nombre de usuario, las contraseñas respectivas y el nivel de seguridad que se le va a aplicar. Véase Figura 3.10

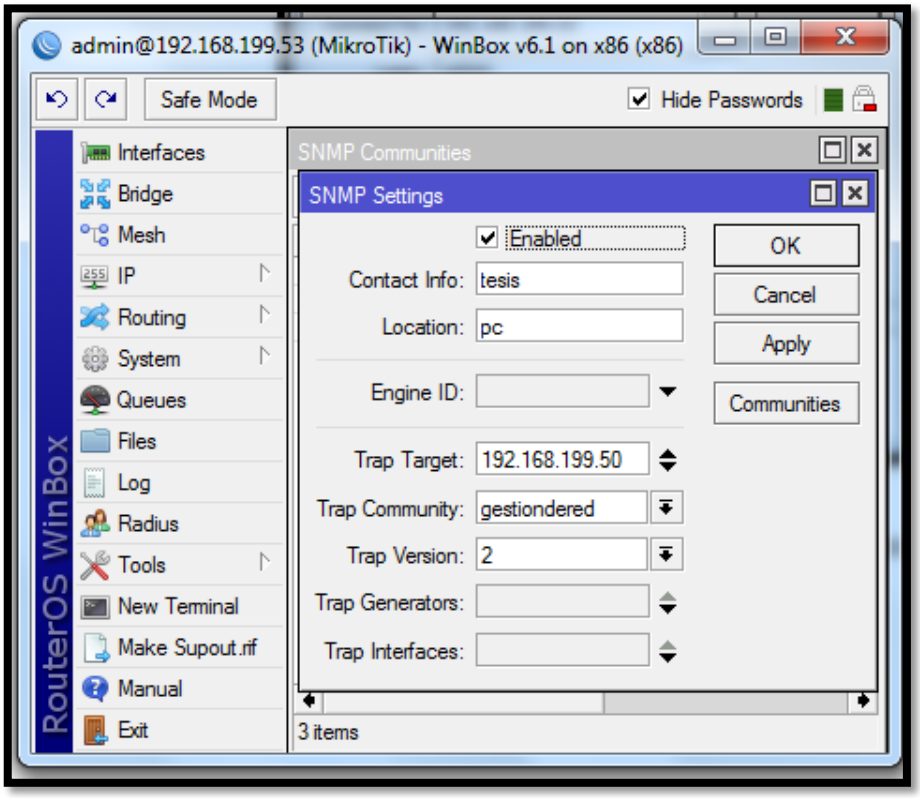


Figura 3.9: Configuración SNMPv2 en Router

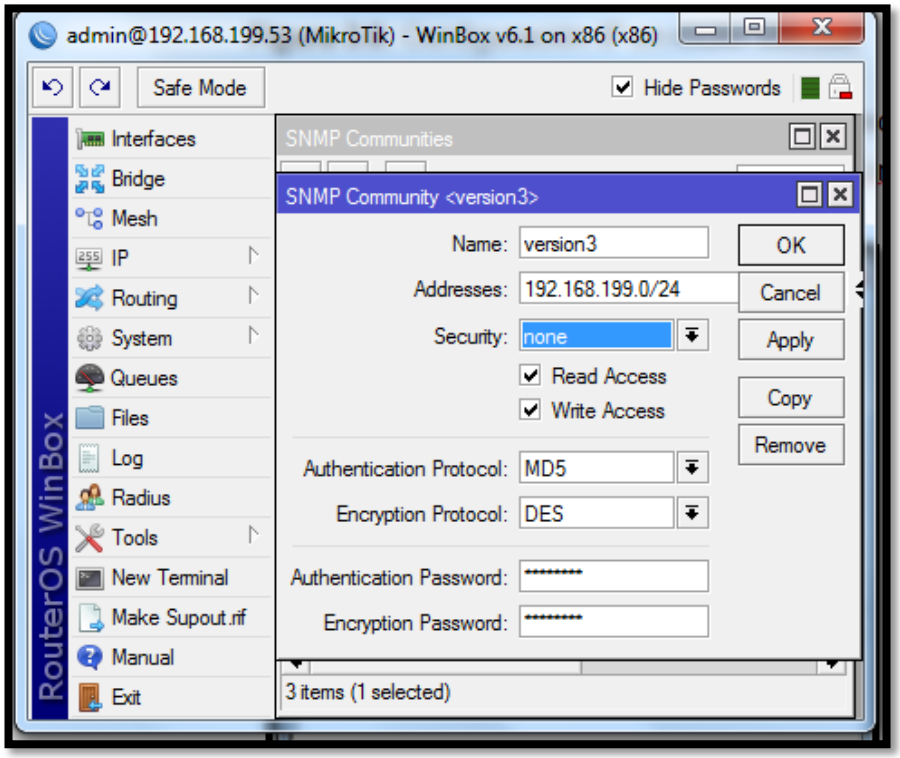


Figura 3.10: Configuración SNMPv3 en Router

4. Verificamos que todo esté en orden y que los cambios se hayan efectuado haciendo click en IP>SNMP>Communities.

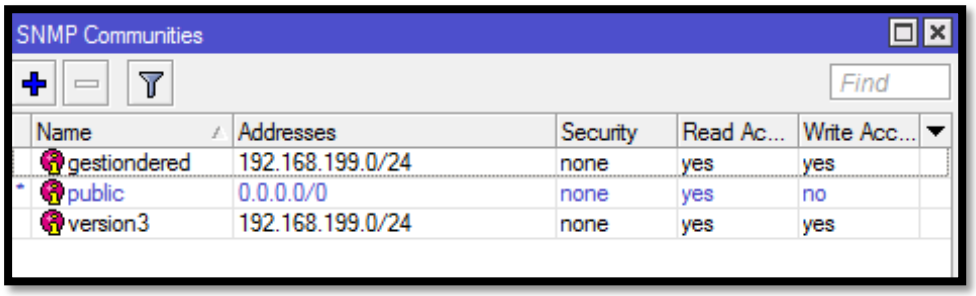


Figura 3.11: Verificación del protocolo SNMP en Router

3.3.3 Instalación y Configuración WireShark

WireShark es un programa de seguimiento y análisis de paquetes de datos de una red, su instalación es muy sencilla y se realiza siguiendo los pasos comunes de cualquier software básico, es decir el instalador realiza todos los pasos por el usuario y solo se deberá aceptar términos y condiciones de licencia y seleccionar las opciones necesarias para que no se realicen cambios en el navegador predeterminado.

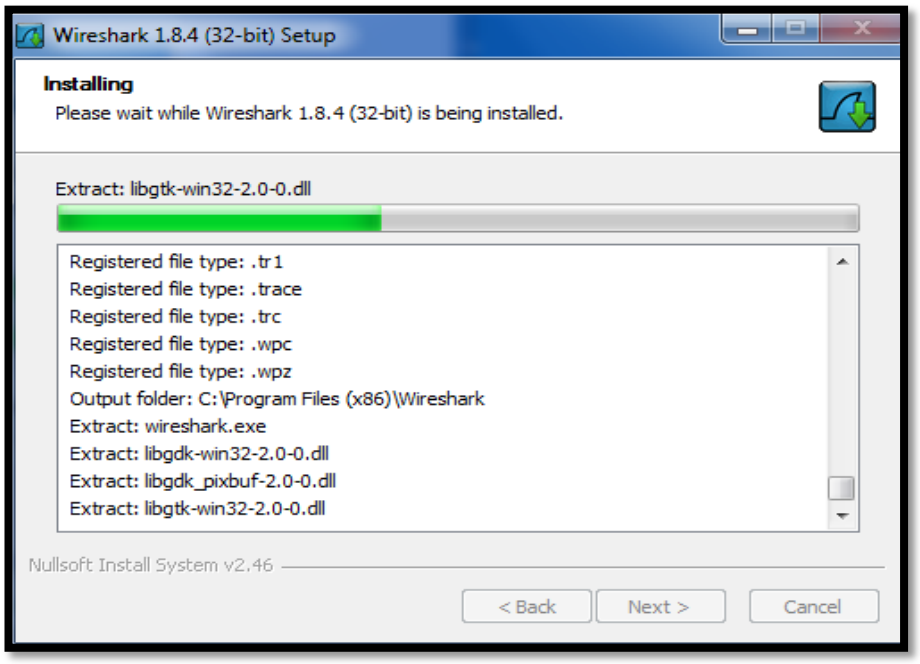


Figura 3.12: Instalación de WireShark

Una vez terminada la instalación el programa estará listo para usarse. Para realizar capturas de paquetes se siguen los siguientes pasos:

Iniciado el programa ir a la barra de herramientas a la opción “Capture”, se abrirá una ventana como la que se muestra en la Figura 3.13, en esta ventana se da click en “start”, de esta manera el programa automáticamente comenzará a capturar los paquetes de datos con sus descripciones tal y como se muestra a continuación. Véase Figura 3.14

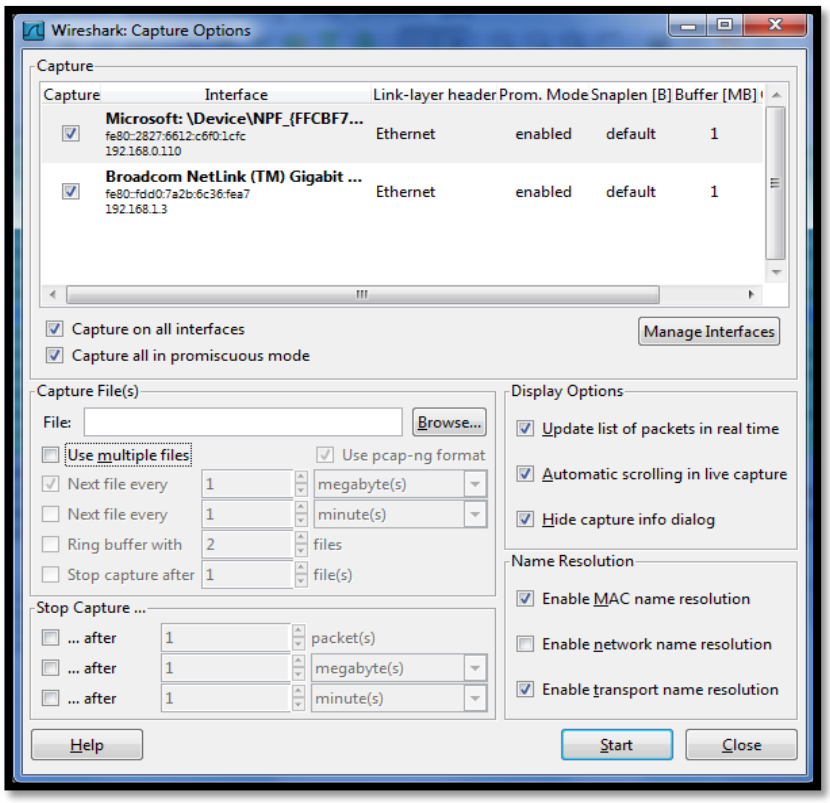


Figura 3.13: Wireshark Pantalla de Opción de Captura

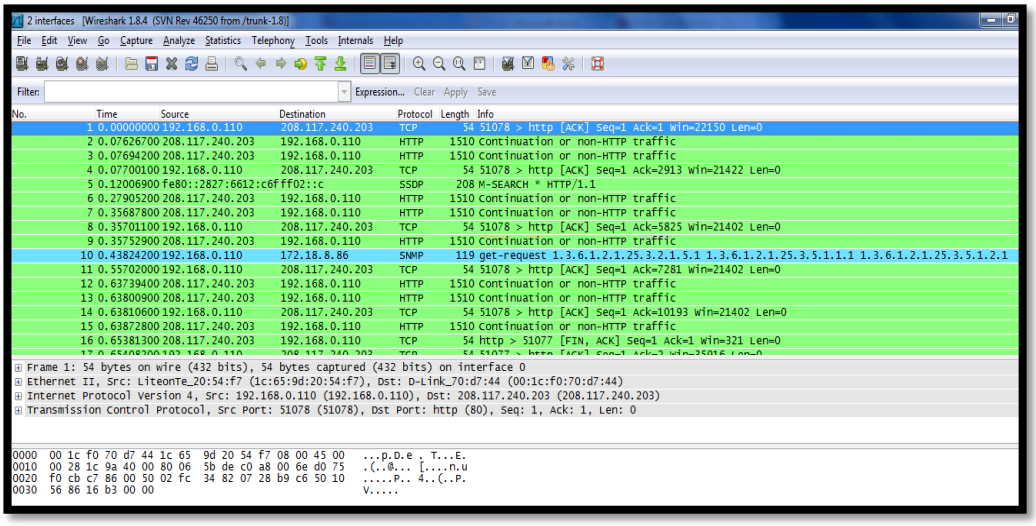


Figura 3.14: Captura de paquetes en Wireshark

Se pueden filtrar los paquetes obtenidos por el tipo de protocolo al que pertenecen, solo es necesario ingresar el tipo de protocolo que deseado.

3.3.4 Configuración de Estación Gestora

La estación gestora será la encargada de la administración de la gestión de todos los elementos conectados a la red, es desde aquí donde se ejecutarán todos los comandos para observar el funcionamiento del protocolo.

Para realizar lo antes mencionado, se instalará en la estación el programa Net-SNMP para de esta manera tener acceso a los

programas que ayudarán a realizar las distintas consultas por SNMP, estos son ejecutables y programados en C, pueden correr tranquilamente en el MS-DOS del Windows, que es el que se usará en el proyecto, algunos de ellos son: snmpget snmpgetnext, snmptrap, snmpwalk, snmpbulkget, snmpbulkwalk.

CAPÍTULO 4

4. SIMULACIÓN Y PRUEBAS

4.1 DESCRIPCIÓN DE LOS DIFERENTES ESCENARIOS A ANALIZAR

En este capítulo se muestran las pruebas y simulaciones que se realizaron para el desarrollo del proyecto, haciendo uso de todos los programas mencionados en el capítulo anterior y con sus configuraciones respectivas.

A continuación se mencionan los tres escenarios usados, todos mantienen la misma red LAN, pero muestran las diversas operaciones posibles de realizar en cada una de las versiones.

- Escenario A: Pruebas de la simulación de red virtual LAN con protocolo SNMPv1.

  En este escenario se trabajará únicamente con la versión 1, para una mejor comprensión se crearán Sub-escenarios, los mismos que son presentados a continuación:

  - Sub-escenario 1: Se simularán las operaciones: GetRequest y GetResponse.
  - Sub-escenario 2: Se mostrará un ejemplo de una comunidad ingresada de manera errónea, y la forma en que el protocolo responde ante este suceso.
  - Sub-escenario 3: Se hará uso de una Trap originada en el Windows server

- Escenario B: Pruebas de la simulación de red virtual LAN con protocolo SNMPv2.

  Al igual que en el caso anterior nos guiaremos por medios de Sub-escenarios.

  - Sub-escenario 1: Se simularán las operaciones: GetRequest y GetResponse, para la comparación con SNMPv1.
  - Sub-escenario 2: Se utilizará GetBulk con el fin de mostrar cómo opera una de las nuevas opciones implementadas en esta versión.

- Sub-escenario 3: También se ejecutará la operación Trap para comprobar si existen o no diferencias con el formato de la PDU expuesta en SNMPv1.

- Escenario C: Pruebas de la simulación de red virtual LAN con protocolo SNMPv3.

  Finalmente en este último escenario se dividirá en dos Sub-escenarios:

  - Sub-escenario 1: Se simularán las operaciones GetRequest, GetNextRequest y GetResponse desde el servidor Linux.
  - Sub-escenario 2: Aprovechando las nuevas características que ofrece SNMPv3 en cuanto a seguridad y teniendo en cuenta los tres niveles proporcionados, se harán las pruebas respectivas para ver qué tan factibles resultan ser y como responde el protocolo ante cualquier intento erróneo de contraseñas.

4.2 Escenario A: PRUEBAS DE LA SIMULACION DE RED VIRTUAL LAN CON PROTOCOLO SNMP VERSION 1

Sub-escenario 1: Una vez configurados todos los parámetros como se indicó en el Capítulo 3, se inicializa el CMD en la estación gestora, para que este pueda acceder a todos los programas para ejecutar los

respectivos comandos de SNMP hay que ingresar al directorio **cd\usr\bin**, una vez dentro se ingresan los comandos de los respectivos agentes, dentro de los parámetros se ingresa la Comunidad, la cual es la misma para todos los elementos de la red. Véase Figura 4.1, para luego proceder a revisar el resultado de los paquetes en WireShark.

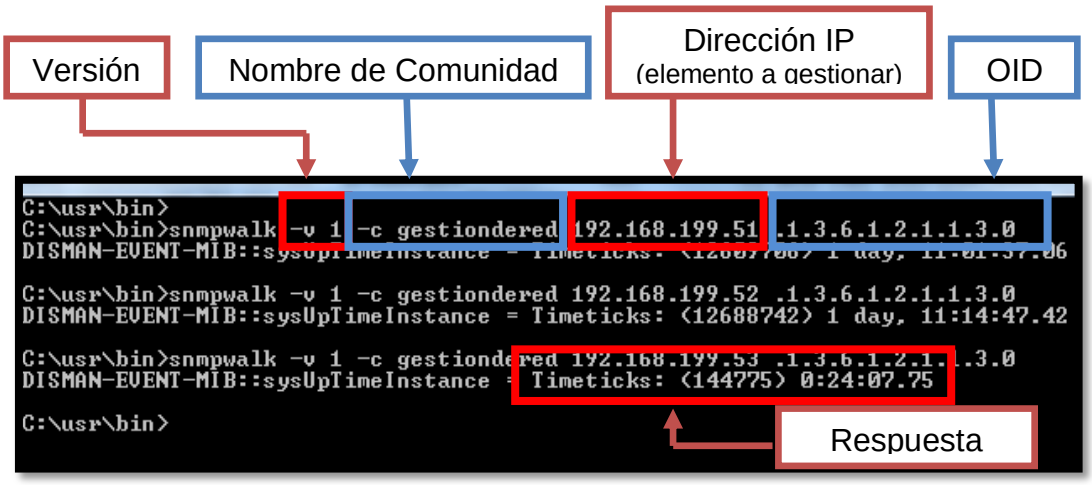


Figura 4.1: Consulta por SNMPv1uando el comando SnmpWalk en CMD

En Wireshark se encuentra en modo de paquetes el resultado de las consultas realizadas por el CMD, como se hizo uso de snmpWalk se observa un “GetNextRequest” y un “GetRequest” por parte de la estación gestora, Véase Figura 4.2, y un “GetResponse” que es enviado por el elemento gestionado, Véase Figura 4.3, en este caso se muestra un ejemplo del resultado que devuelve el Router.

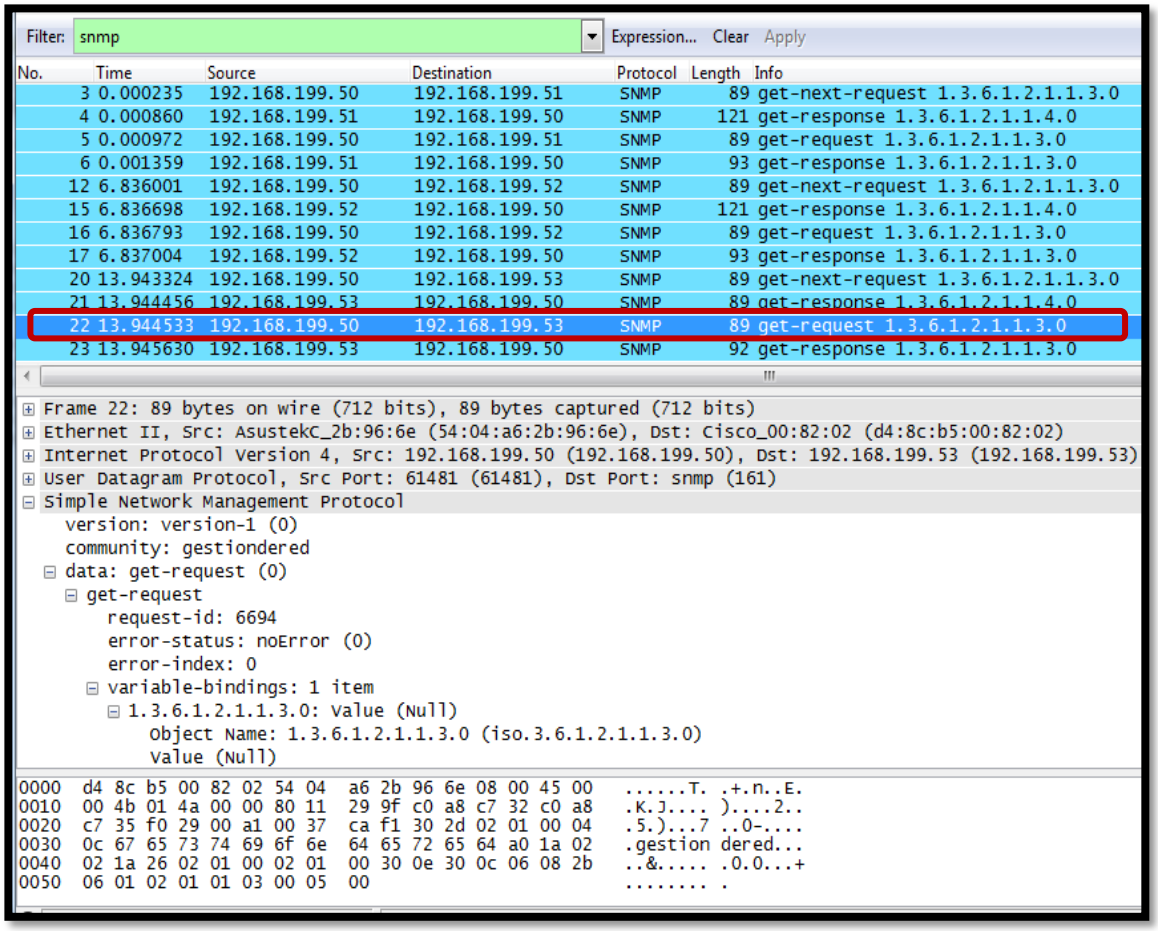


Figura 4.2: Get-Request SNMPv1 desde la PC al Router

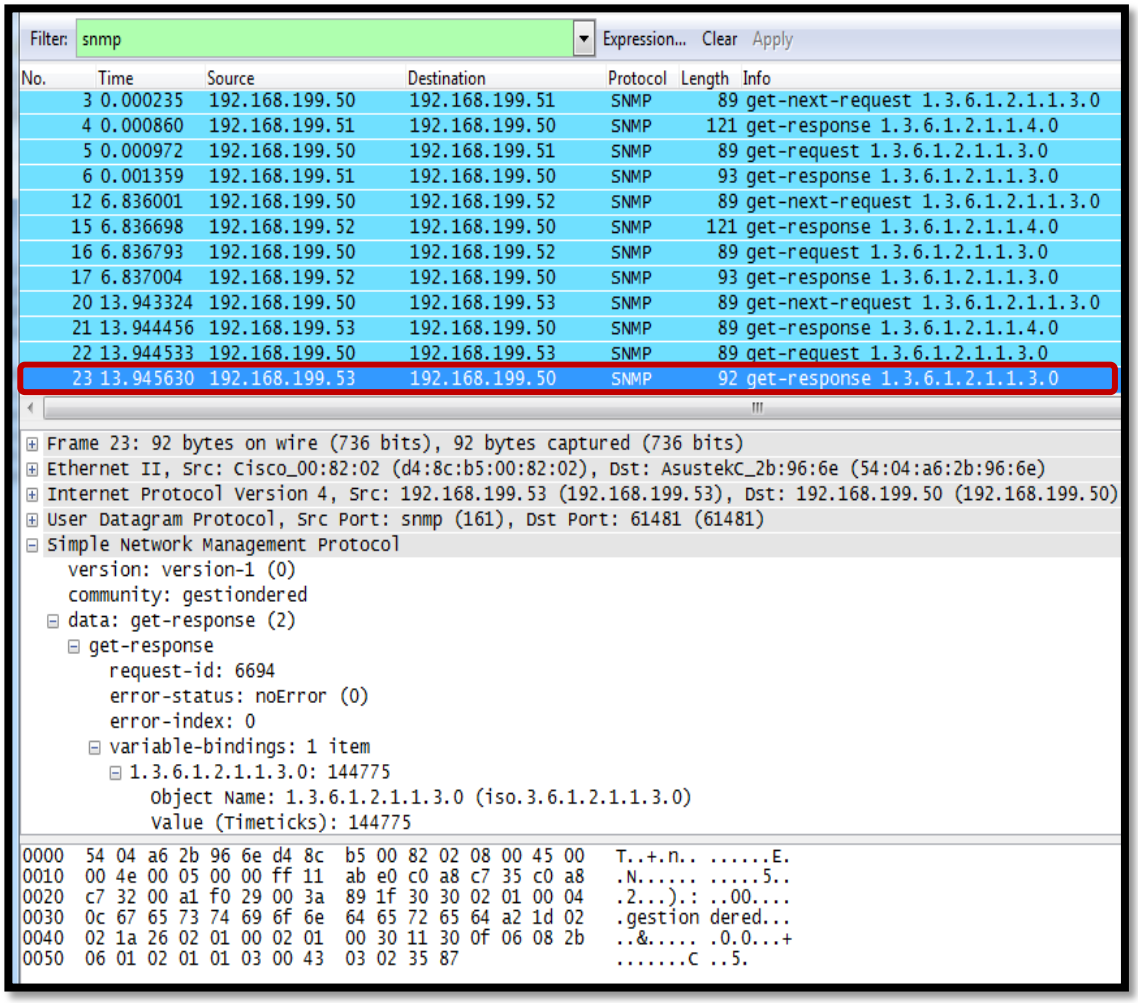


Figura 4.3: Get-Response SNMPv1 del Router

Sub-escenario 2: En este caso se busca la respuesta que se generará al ingresar el nombre de la comunidad de manera errónea, el nombre verdadero de la comunidad es “gestiondered”, pero en el comando fue ingresada la comunidad “gestionred”. Véase Figura 4.4

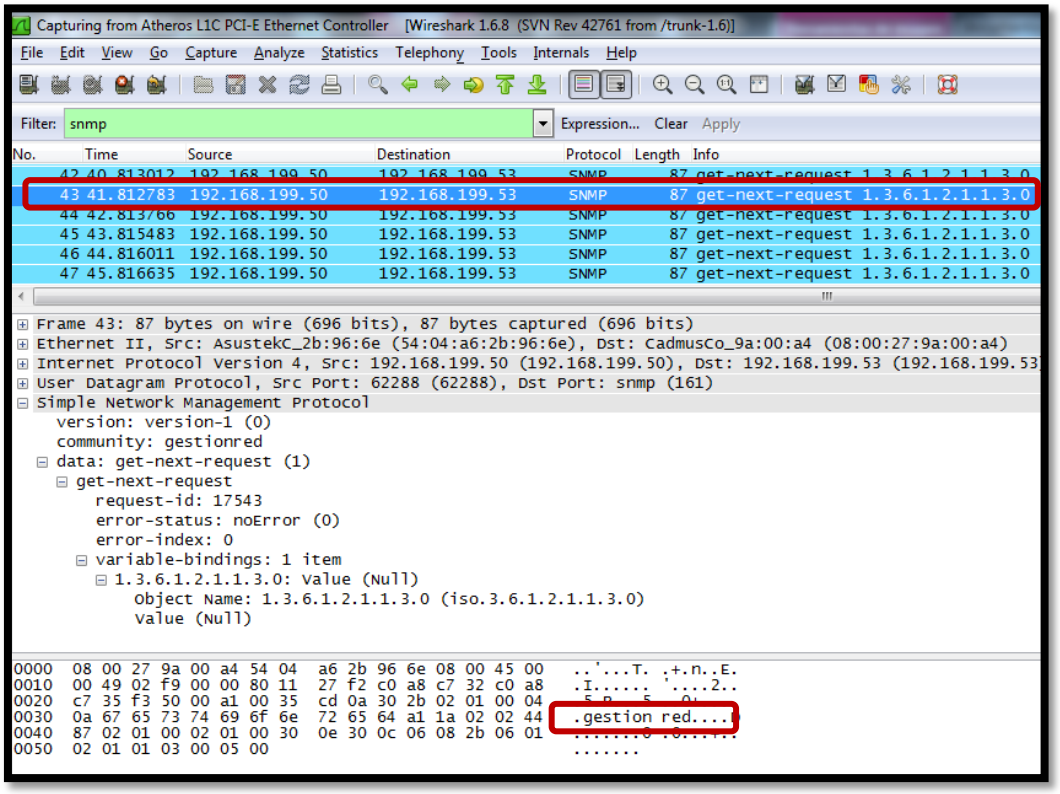


Figura 4.4: Resultado de ingresar una comunidad incorrecta desde la estación gestora o agente

Sub-escenario 3: Este hace referencia a las Traps, en el caso de esta versión se usa el siguiente comando el cual, a diferencia del snmpwalk debe ser ejecutado en el elemento de red que se vaya a usar. Para este ejemplo se ejecutará desde el Windows server:

snmptrap -v1-c gestiondered 192.168.199.50 1.2.3.4 192.168.199.52 4 0 '1'

este comando indica la versión, el nombre de la comunidad, la dirección Ip de la estación Gestora y el tipo de Trap que se va a generar.

Una vez realizado el comando, el siguiente paso será revisar Wireshark para ver el resultado del mismo. Véase Figura 4.5.

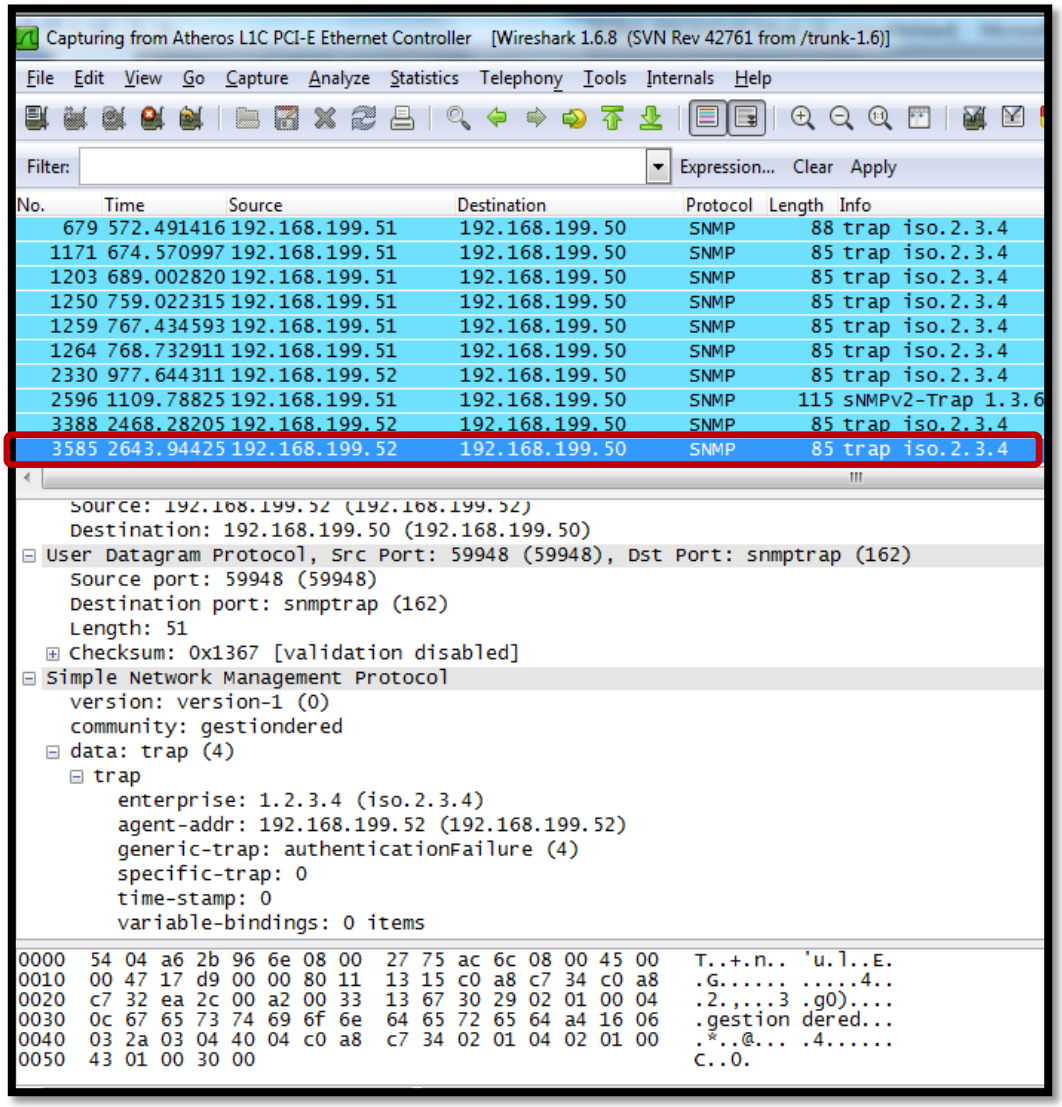


Figura 4.5: Trap SNMPv1 Del Windows Server en WireShark

4.3 Escenario B: PRUEBAS DE LA SIMULACION DE RED VIRTUAL LAN CON PROTOCOLO SNMP VERSION 2

Sub-escenario 1: El procedimiento a realizar en este caso no tiene mucha diferencia con el del primer sub-escenario del Escenario A, de igual manera se inicializa el CMD en la estación gestora y se ingresan los comandos de los agentes, dentro de los parámetros se ingresa la Comunidad, la cual es la misma para todos los elementos de la red. Véase Figura 4.6, para luego proceder a revisar el resultado de los paquetes en WireShark.

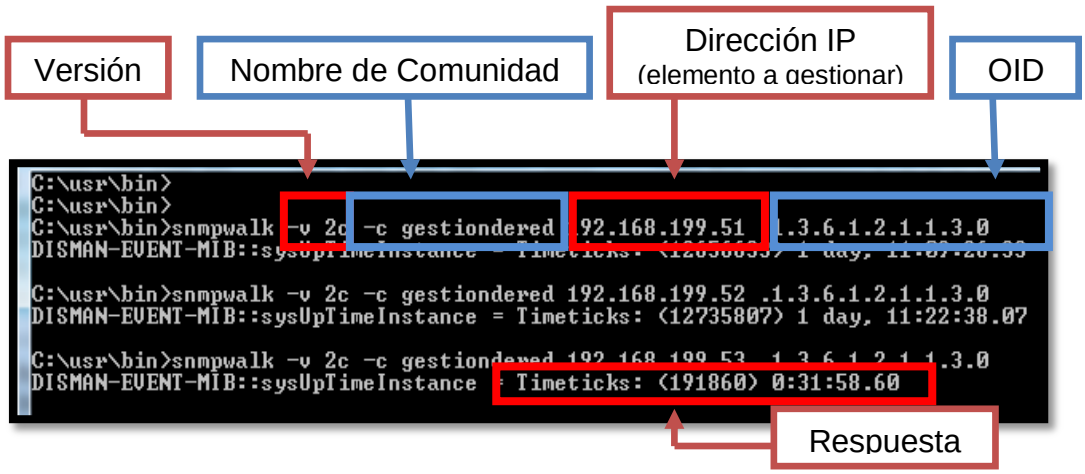


Figura 4.6: Consulta por SNMPv2 usando el comando SnmpWalk en CMD

En Wireshark se muestran los resultados en modo de paquetes de las consultas realizadas por el CMD, como se hizo uso de snmpWalk se observa un “GetNextRequest” y un “GetRequest” por parte de la estación gestora, Véase Figura 4.7, y un “GetResponse” que es enviado por el

agente gestionado, Véase Figura 4.8, en este caso se muestra un ejemplo del resultado que devuelve el Windows Server.

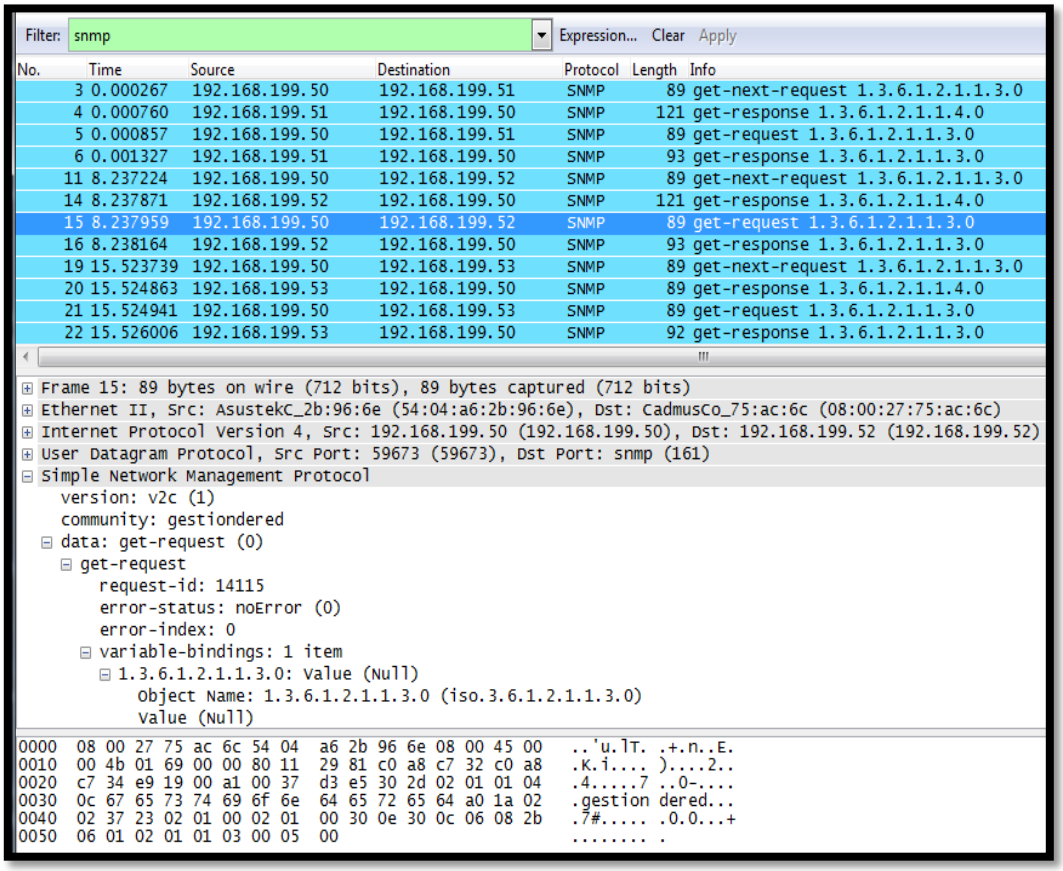


Figura 4.7: Get-Request SNMPv2 desde la PC al Windows Server

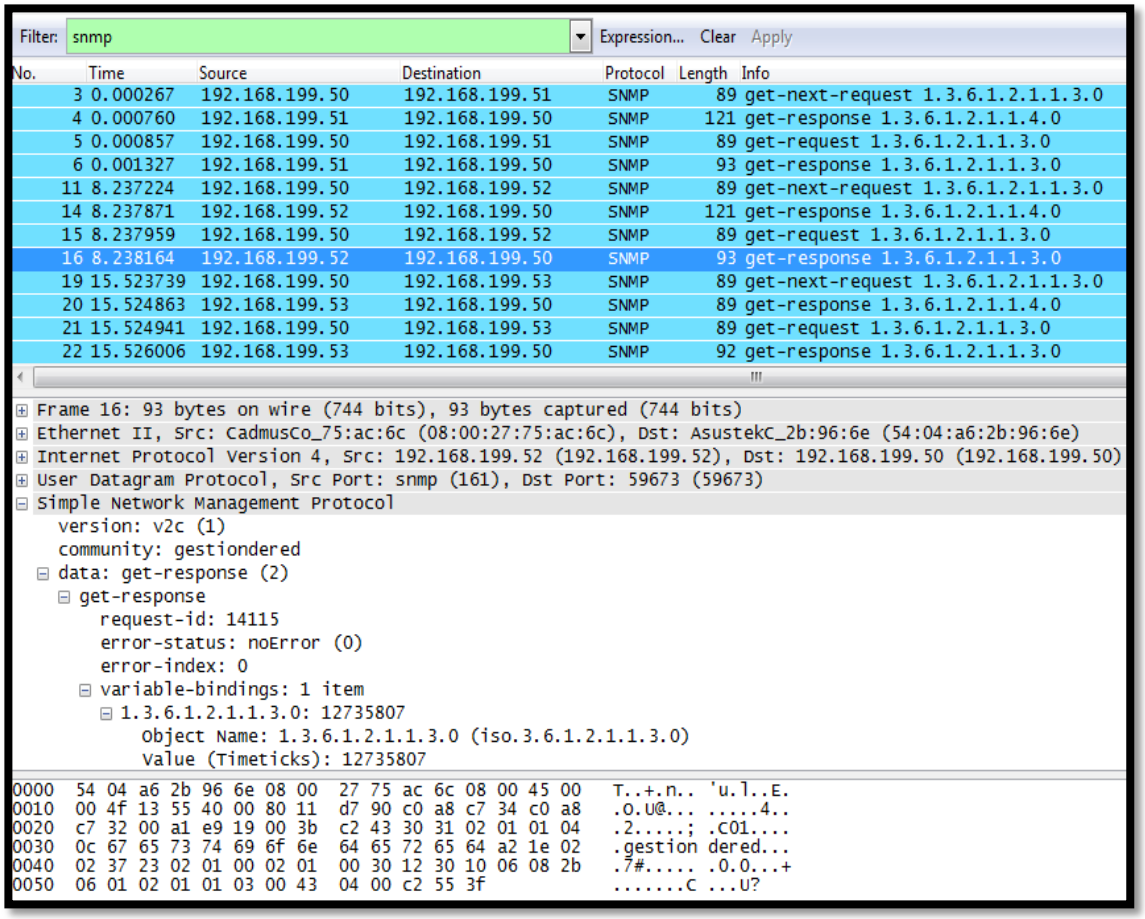


Figura 4.8: Get-Response SNMPv2 del Windows Server

Sub-escenario 2: En este caso se ejecutará un GetBulk, esta operación es añadida en esta versión del protocolo, la estructura de su comando es igual a la de “snmpwalk”, solo hay que sustituir esta palabra por “snmpbulkwalk”. Véase Figura 4.9.

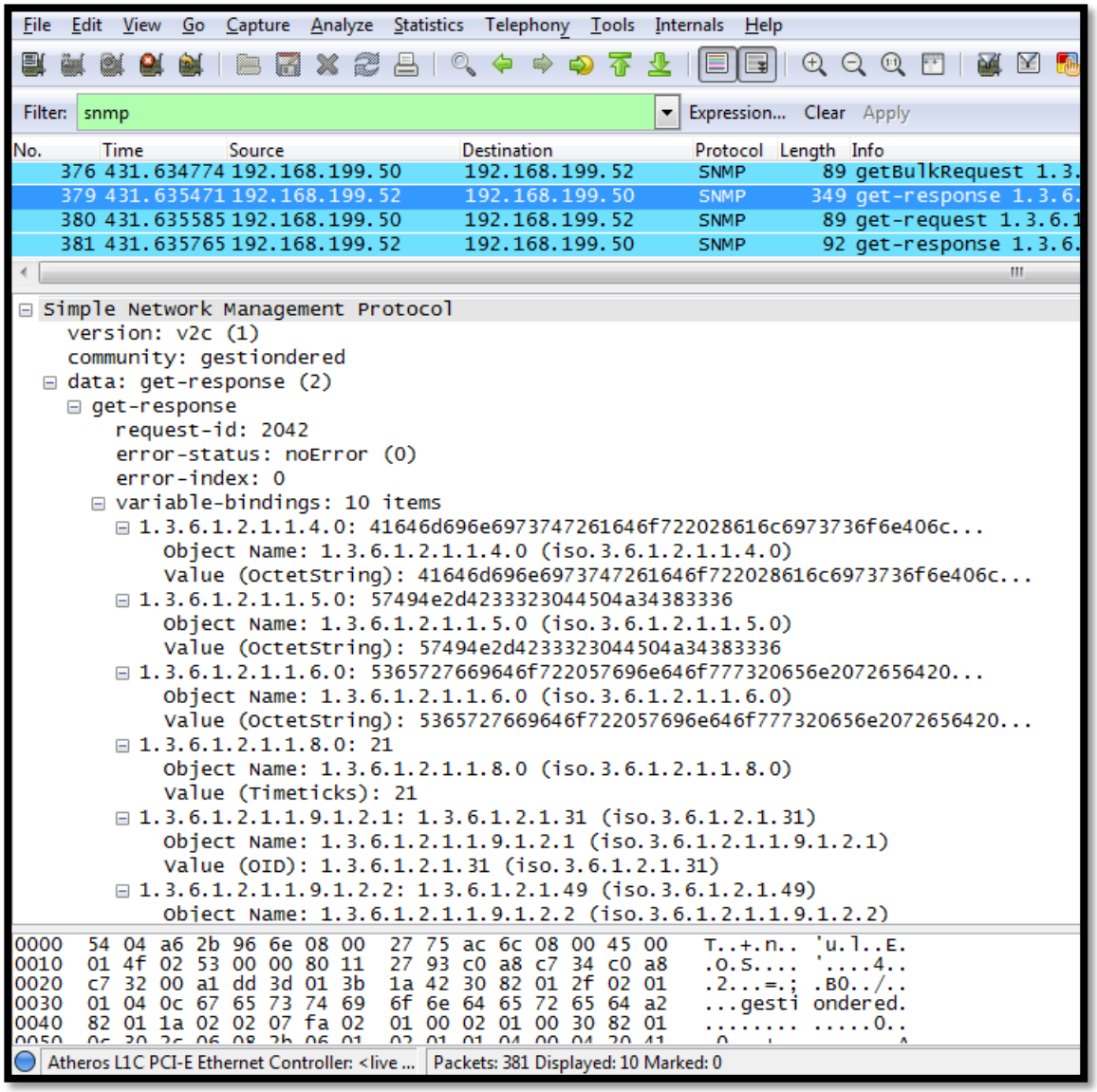


Figura 4.9: Respuesta del Get-Bulk en SNMPv2 del Windows Server

Sub-escenario 3: En el caso de las Traps en la SNMPv2 se usa el siguiente comando

snmptrap -v 2c -c gestiondered 192.168.199.50 "" 1.2.3.4.0

Este también debe ser ejecutado en el elemento de red que se vaya a usar. Para este ejemplo se ejecutará desde el Servidor Linux:

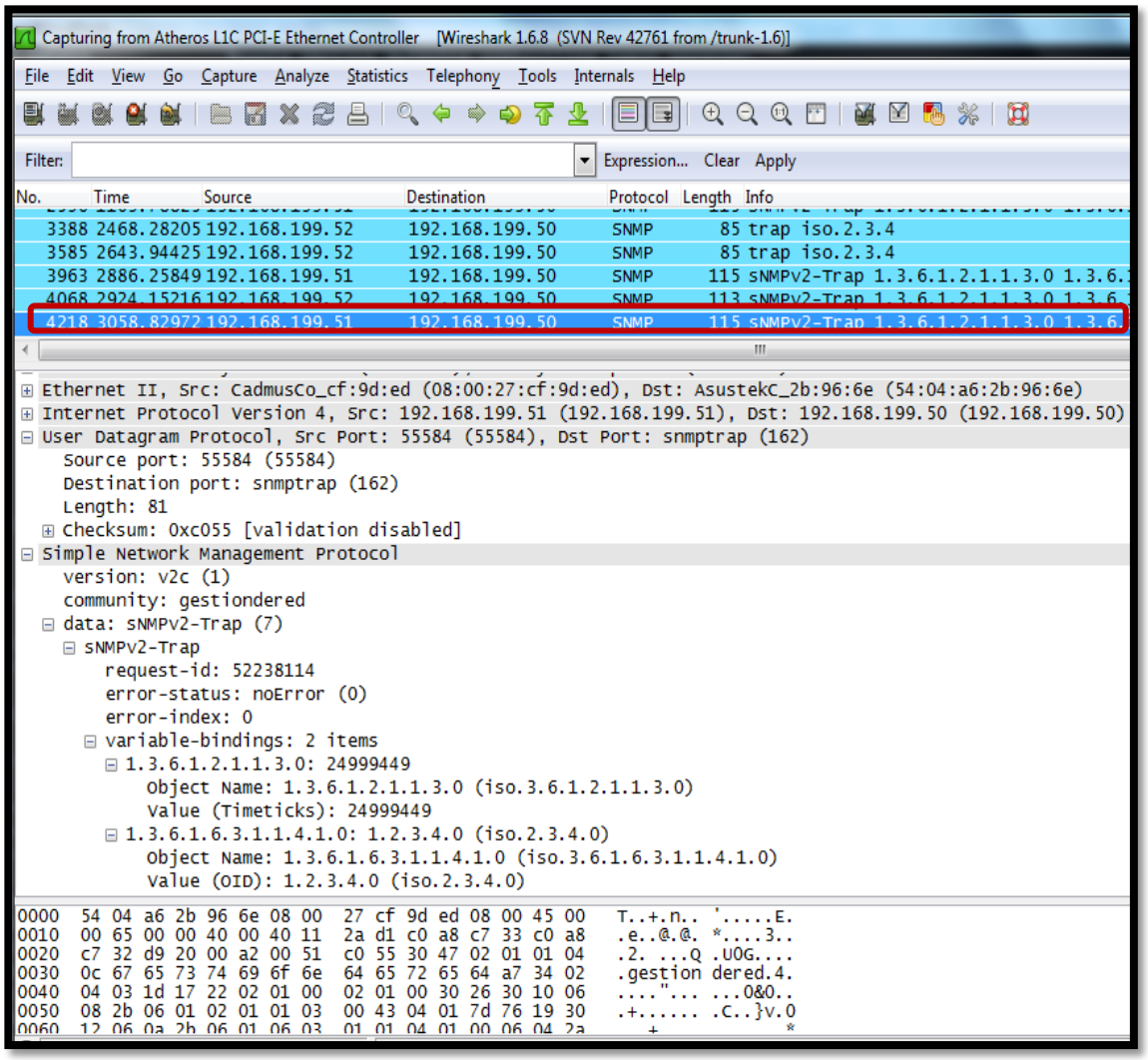


Figura 4.10: Trap SNMPv2 del Servidor Linux en WireShark

4.4 Escenario C: PRUEBAS DE LA SIMULACIÓN DE RED VIRTUAL LAN CON PROTOCOLO SNMP VERSION 3

Sub-escenario 1: Para realizar las pruebas en la versión 3 se inicializa el CMD en la estación gestora. Aquí se ingresan los comandos de los respectivos elementos pertenecientes a la red, dentro de los parámetros se ingresan las contraseñas y el nombre de Usuario, estos serán los mismos para todos los elementos de la red. Véase Figura 4.11, para luego proceder a revisar el resultado de los paquetes en WireShark.

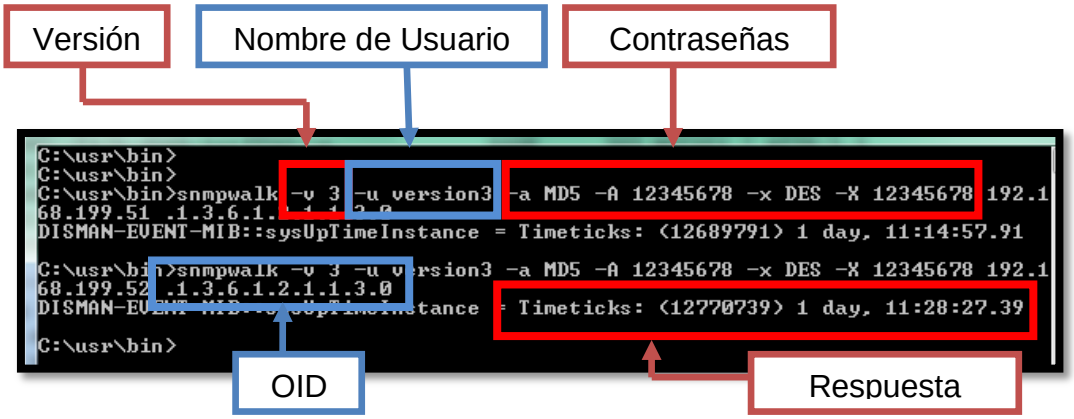


Figura 4.11: Consulta por SNMPv3 usando el comando SnmpWalk en CMD

En Wireshark se muestran los resultados en modo de paquetes de las consultas realizadas por el CMD, como se hizo uso de snmpWalk se observa un “GetRequest” por parte de la estación gestora, Véase Figura 4.14, y un “GetResponse” que es enviado por el agente gestionado, Véase Figura 4.15, en este caso se muestra un ejemplo del resultado que devuelve el Servidor Linux.

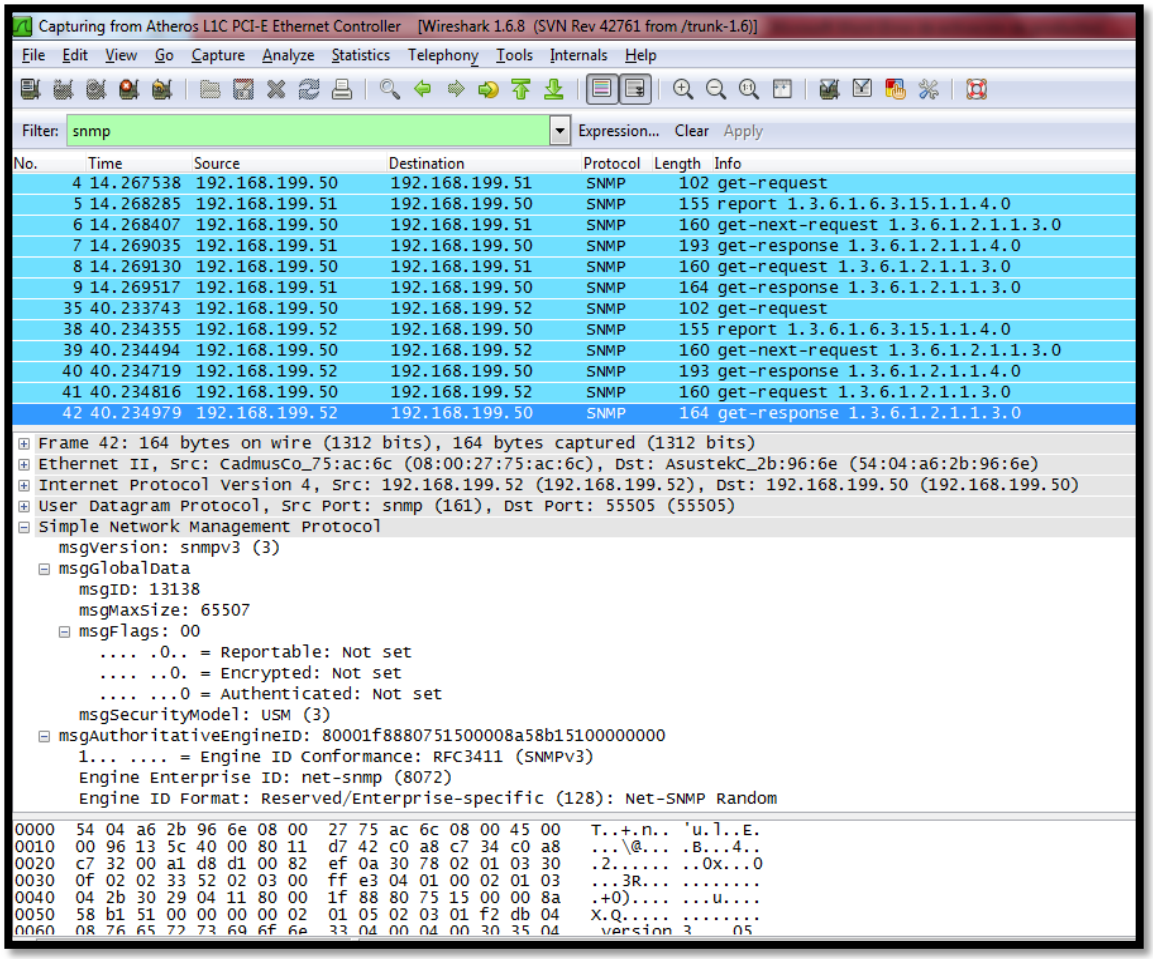


Figura 4.12: Captura de Paquetes SNMP en WireShark

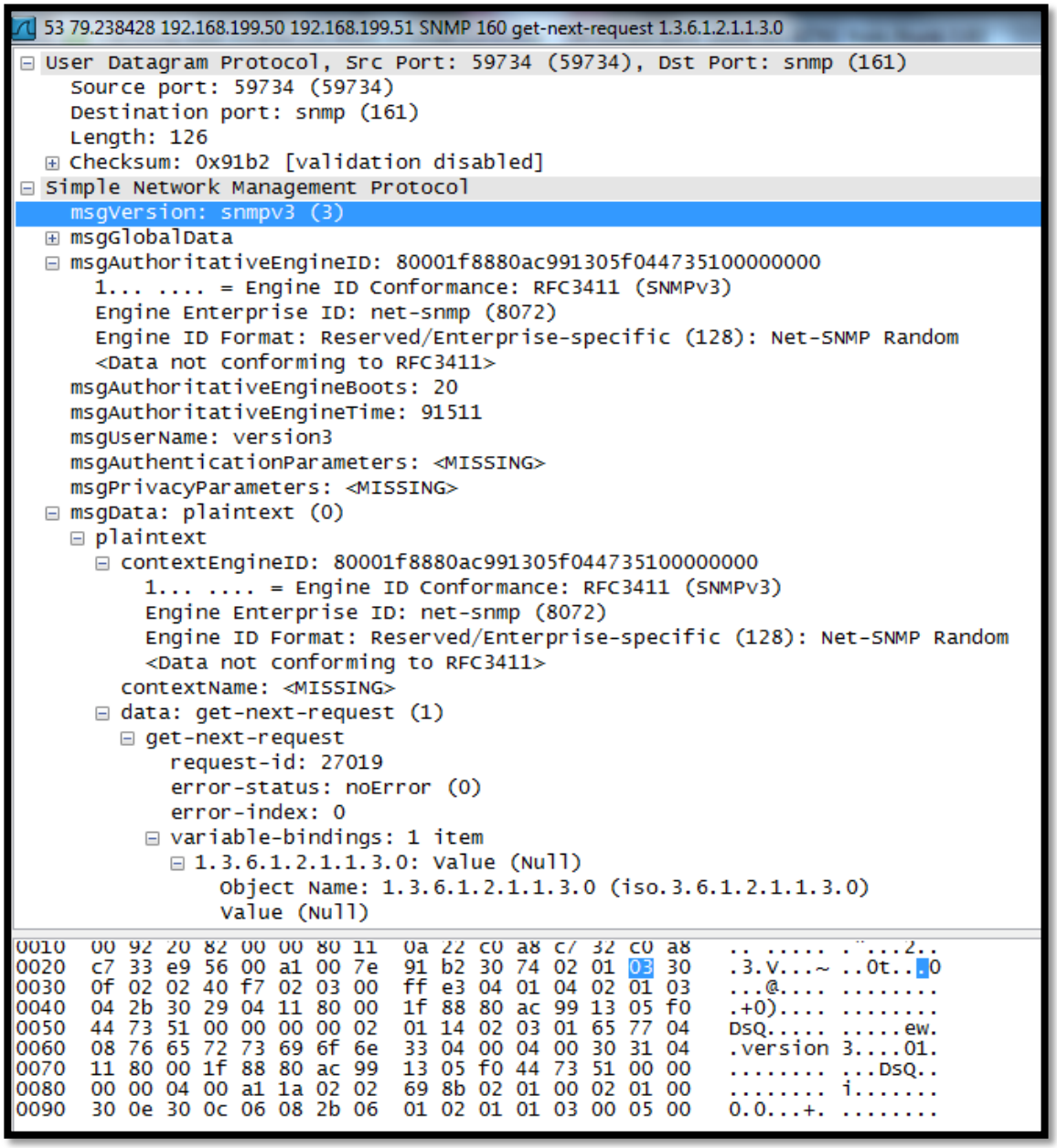


Figura 4.13: Get-NextRequest SNMPv3 desde la PC al Servidor Linux

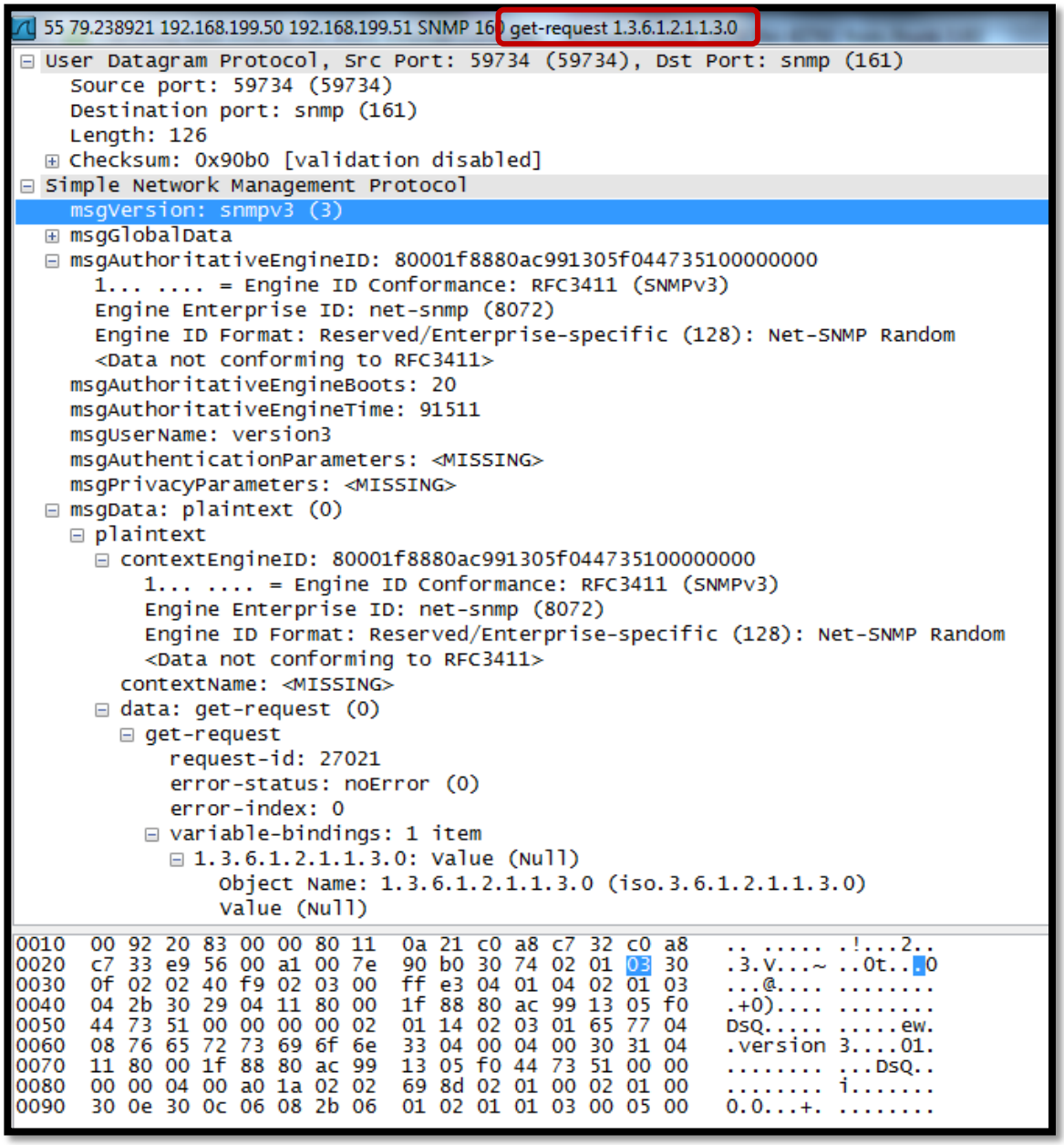


Figura 4.14: Get-Request SNMPv3 desde la PC al Servidor Linux

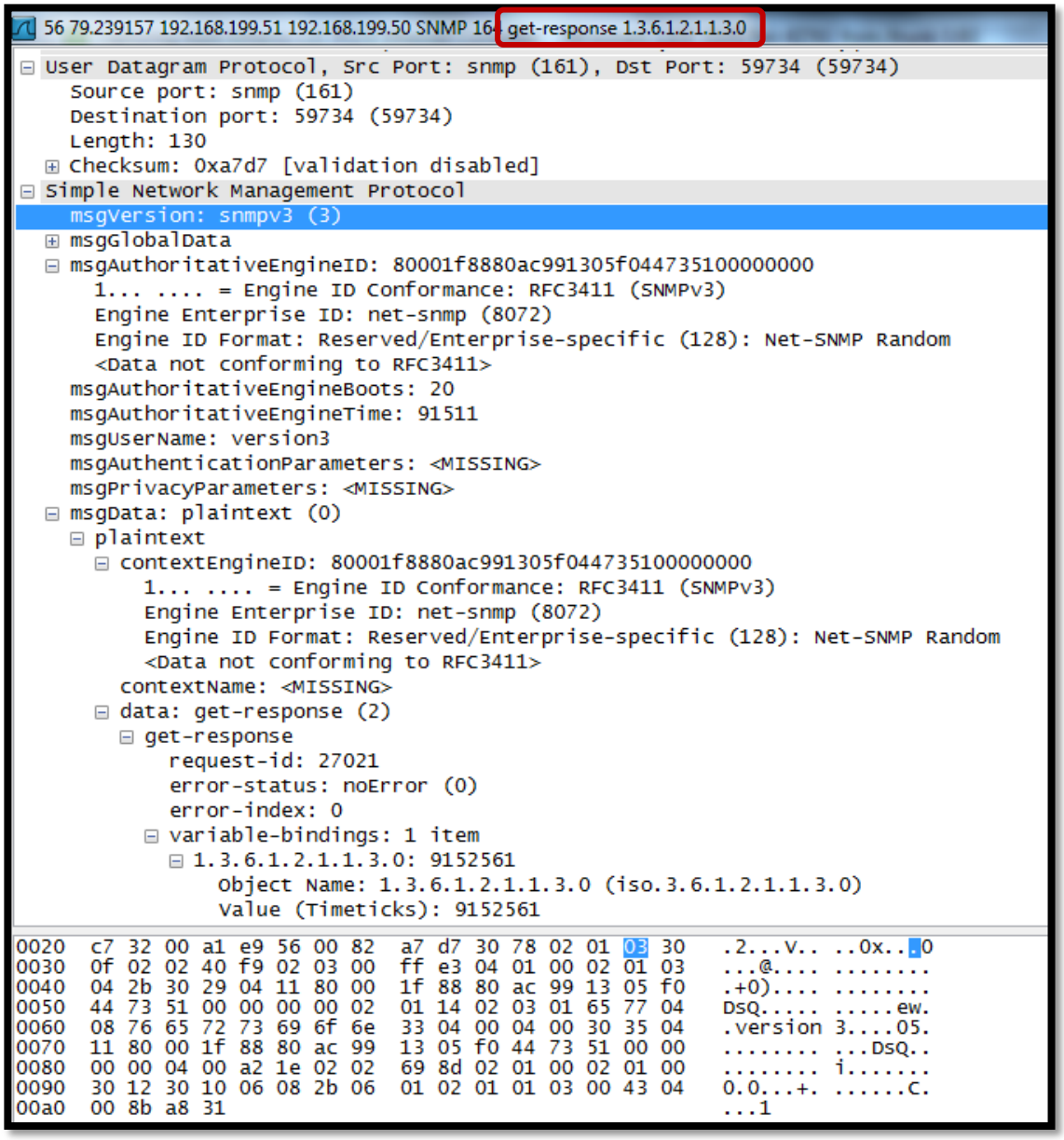


Figura 4.15: Get-Response SNMPv3 del Servidor Linux

Sub-escenario 2: En SNMPv3 se pueden usar tres tipos de seguridad, a continuación se muestra la ejecución del comando cuando las contraseñas son ingresadas incorrectamente y el comportamiento que toma el protocolo en cada uno de los casos mediante Wireshark

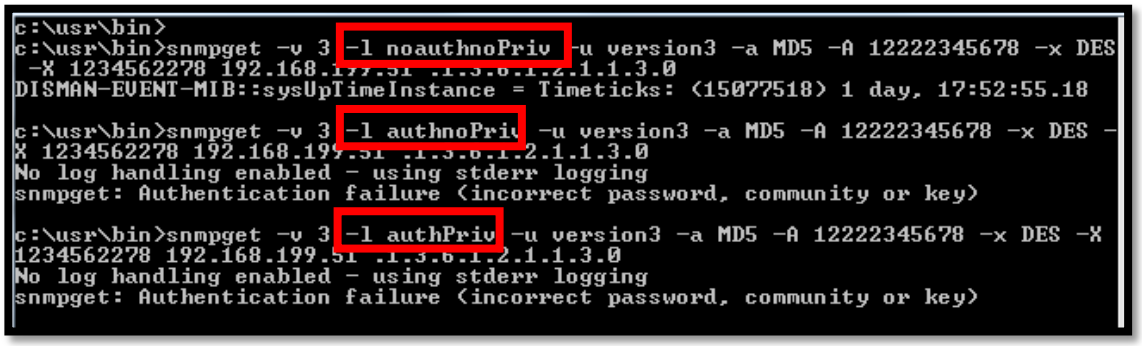


Figura 4.16: Ejecución de los comando en CMD desde la estación gestora

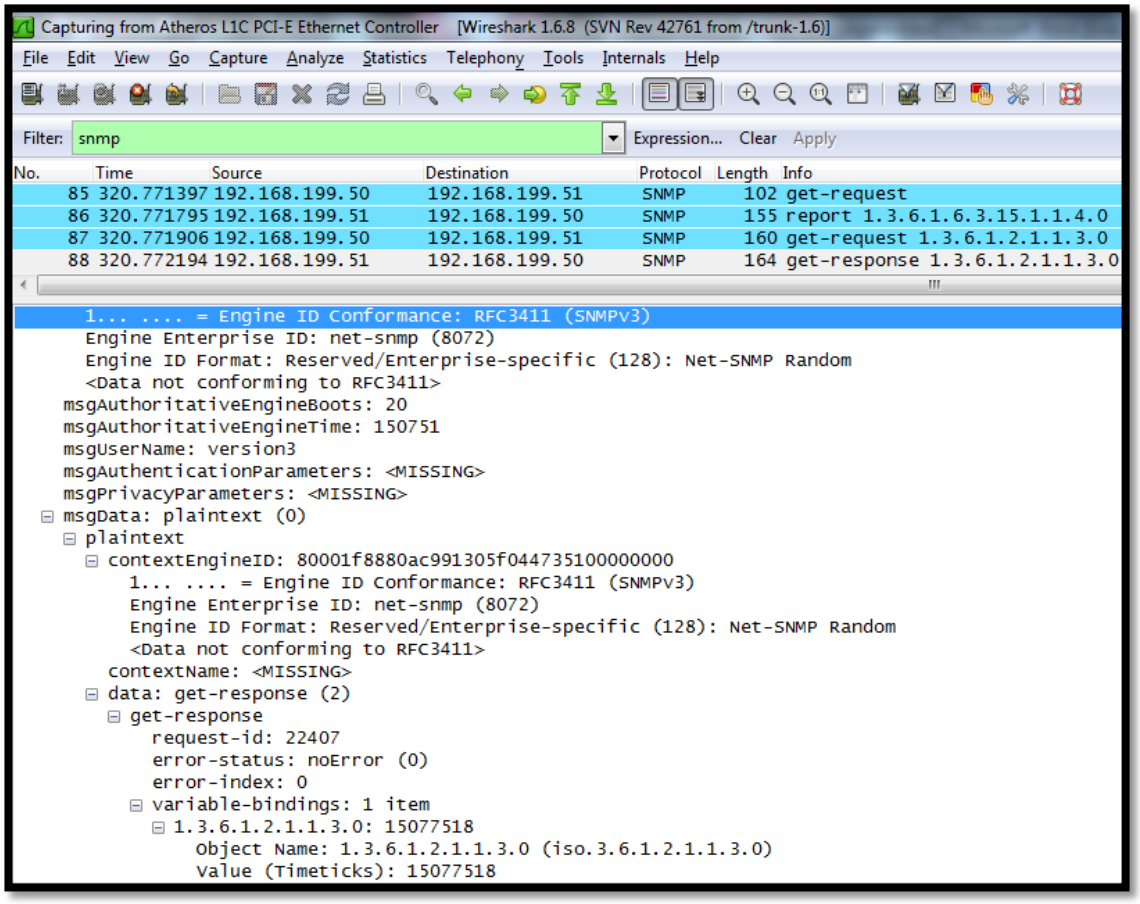


Figura 4.17: Reporte generado con el modo de seguridad “NoAuthNoPriv” al ingresar contraseñas incorrectas

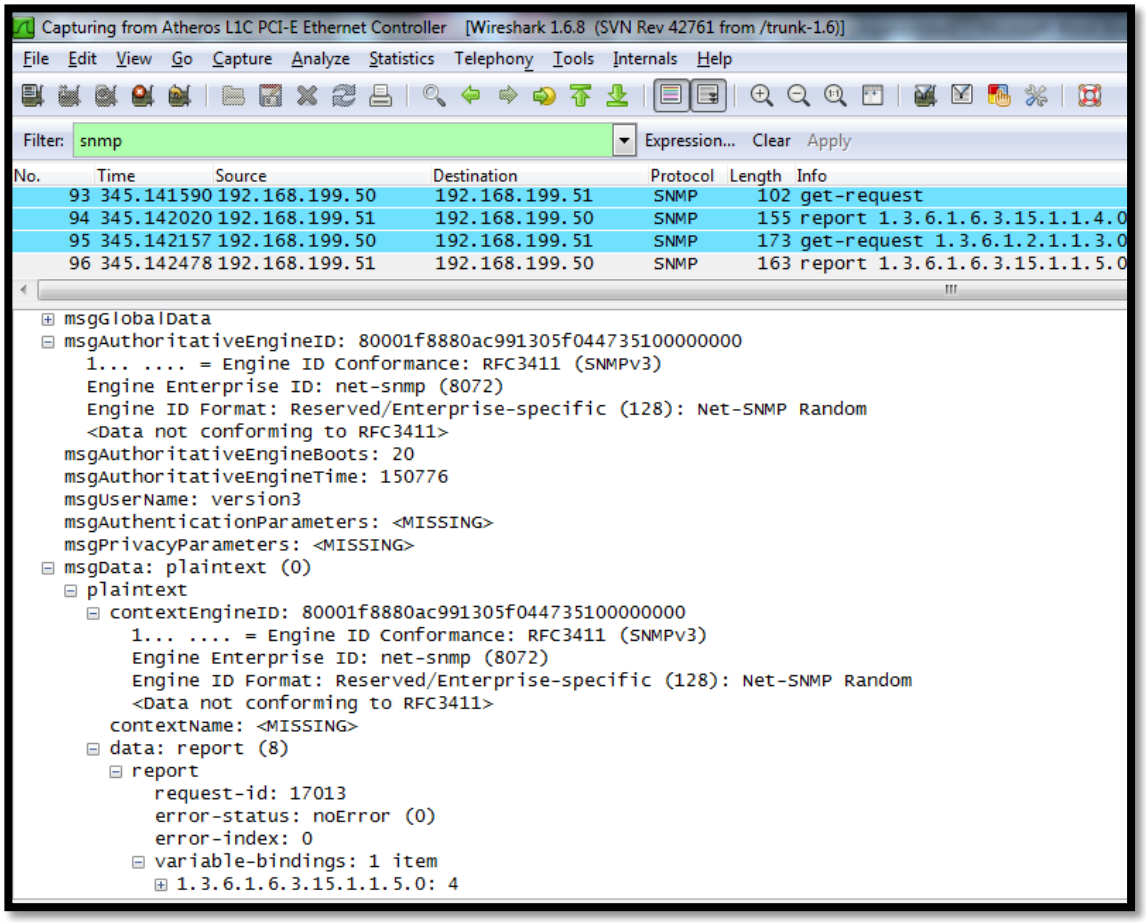


Figura 4.18: Reporte generado con el modo de seguridad “AuthNoPriv” al ingresar contraseñas incorrectas

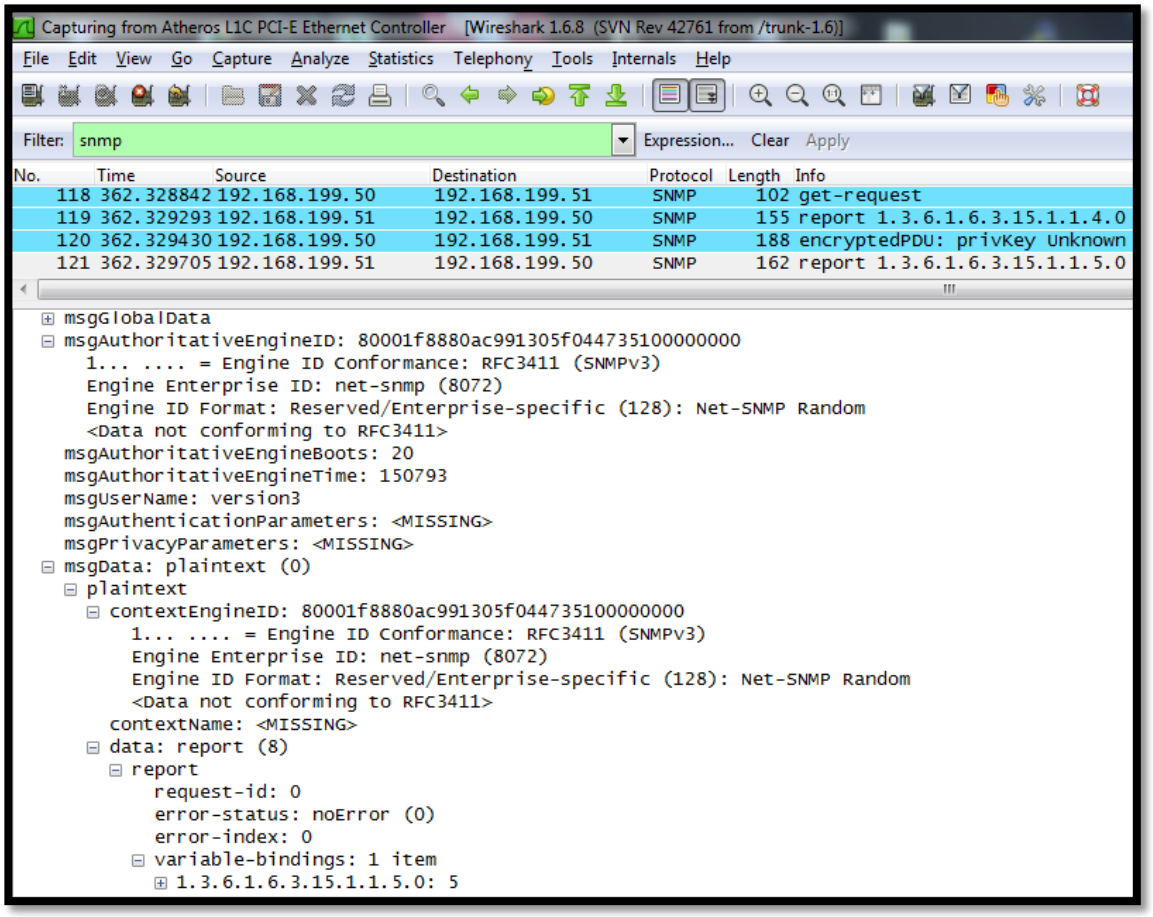


Figura 4.19: Reporte generado con el modo de seguridad “AuthPriv” al ingresar contraseñas incorrectas

CAPÍTULO 5

5. ANÁLISIS DE RESULTADOS

En este capítulo se exponen todas las observaciones obtenidas de cada una de las versiones del protocolo resultado de las pruebas realizadas en el capítulo anterior, las diferencias, las semejanzas, las ventajas y desventajas que tiene una versión respecto a la otra.

5.1 RESULTADOS GESTION DE RED LAN CON PROTOCOLO SNMP VERSIÓN 1

Snmpv1 es la primera implementación del protocolo dada a los usuarios encargados de monitorear y gestionar las redes, este al igual que todas las otras versiones opera a través de otros protocolos siendo uno de estos UDP.

Dentro de las operaciones que puede realizar en esta versión están: Get, GetNext, Set, y Trap.

Para el ejemplo en el Escenario A, se realiza un Snmpwalk desde el CMD de la estación Gestora hacia el Router perteneciente a la red, este contiene la siguiente OID .1.3.6.1.2.1.1.3.0, la misma que se refiere al tiempo que lleva el elemento de red inicializado. Este responde automáticamente luego de presionar un Enter, Pero no se muestra internamente como ha sido empaquetado.

Esto se puede observar mediante el programa Wireshark, el que automáticamente muestra un GetRequest, y un GetResponse por cada elemento de la red consultado, en este caso será un GetRequest desde la estación Gestora con IP:192.168.199.50 hasta el Router, véase Figura 4.2 y un Get Response desde el Router hasta la estación gestora, véase Figura 4.3.

En este programa se muestra la configuración realizada, dentro de los campos están:

- ✓ La versión: "1", la misma que fue ingresada en el comando a ejecutarse.
- ✓ El nombre de la comunidad: "gestiondered" que claramente se ve que esta sin encriptar, pues esta versión tiene poca seguridad.
- ✓ request-id: "6694", este número entero indica el orden de emisión de los datagramas, de ser el caso este informaría si hay presencia de datagramas duplicados.

- ✓ Error-status: noError(0), dentro de las seis opciones que tiene este campo envía esta respuesta, debido a que no se ha encontrado ningún tipo de error en el proceso.
- ✓ Error-index: 0, normalmente mostraría en que variable se ha encontrado un error, en este caso no se muestra ninguno por eso su respuesta es 0.
- ✓ VarBindList: 1 item, se muestran la lista de las variables analizadas en este caso es una, también muestra el nombre del objeto que ya fue mencionado al inicio, 1.3.6.1.2.1.1.3.0.

Como hay dos operaciones, pregunta, respuesta, con Get Request el valor muestra solo "NULL", y en el Get Response este parámetro ya incluye la respuesta correspondiente al OID solicitado.

En la Figura 4.4 se puede observar un ejemplo de cuando el nombre de la comunidad ejecutado en la estación gestora no coincide con el configurado en el elemento de red, cuando esto sucede el sistema no envía respuesta y continua buscando localizar esa comunidad dentro de la red hasta que su tiempo de ejecución máximo finaliza.

Para probar las traps se realizó la ejecución del comando desde el Windows Server hacia la estación gestora dándole el valor 4 el mismo que corresponde a "authenticationFailure" o "fallo de autentificación", véase Figura 4.5. Los campos que se muestran se nombran a continuación:

- ✓ entreprise: 1.2.3.4, esto indica el tipo de objeto que generó la trap.
- ✓ agent-addr: 192.168.199.52 muestra la dirección desde donde se ejecuta la trap.

- ✓ generic-trap: authenticationFailure (4) esto hace referencia a un mensaje de protocolo que no ha sido autentificado, fue el enviado por el Windows.
- ✓ specific-trap: "0" es un entero que muestra un evento especifico del fabricante que definió dicha trap, en este caso como está enviando un trap tipo genérico se define este valor en 0.
- ✓ time-stamp: "0" este es el tiempo desde la última inicialización de la entidad de red y la generación de la trampa.
- ✓ variable-bindings: lista tipo varBindList con información de posible interés, en este caso no lo hay por eso la respuesta es "0".

5.2 RESULTADOS GESTION DE RED LAN CON PROTOCOLO SNMP VERSIÓN 2

La versión 2 del protocolo SNMP es la actualización de la versión uno, aquí se añaden y mejoran algunas opciones de protocolo. Dentro de las operaciones que puede realizar en esta versión están: GetRequest, GetNextRequest, Set,Trap, GetBulk e Inform.

Para el ejemplo en el Escenario B, se realiza un Snmpwalk desde el CMD de la estación Gestora hacia el Windows Server perteneciente a la red, se lo trabaja con el mismo OID anterior, .1.3.6.1.2.1.1.3.0,

El empaquetado en Wireshark genera automáticamente un GetRequest y un GetResponse por cada elemento de la red consultado, en este caso será un GetRequest desde la estación Gestora con IP:192.168.199.50 hasta el Windows Server, véase Figura 4.7 y un Get Response desde el

Windows Server hasta la estación gestora, véase Figura 4.8, con los siguientes resultados,:

- ✓ La versión: "v2c" es la versión que se especificó al ejecutar el comando
- ✓ El nombre de la comunidad: "gestiondered" que también se muestra sin encriptar, pues esta versión aunque se mejoran algunos componentes la seguridad sigue siendo un problema.
- ✓ request-id: "14115", este número entero indica el orden de emisión de los datagramas.
- ✓ Error-status: noError(0), indica que no se encontró ningún tipo de error en el proceso.
- ✓ Error-index: 0, no se ha encontrado ningún error, por lo tanto su respuesta es 0.
- ✓ VarBindList: 1 ítem, se muestran que solo una variable fue analizada, también muestra el nombre del OID, 1.3.6.1.2.1.1.3.0.

Como hay dos operaciones, pregunta, respuesta, con Get Request la evaluación muestra solo "NULL", y en el Get Response este parámetro ya incluye la respuesta correspondiente al OID solicitado.

Como se ya fue mencionado SNMPv2 incorpora dos nuevas operaciones, en la imagen 4.9 Se observa el funcionamiento de Get Bulk, a diferencia del get request o get next request este tiene la habilidad de introducir algunas OIDs dentro de un mismo paquete, se trabajó con la misma OID usada en el SnmpWalk.

Para probar las traps se realizó la ejecución del comando desde el Servidor Linux hacia la estación gestora, este comando es diferente al

ejecutado en la versión 1, aquí ya no se especifica el tipo de Trap, véase Figura 4.10. Los campos que se muestran se nombran a continuación:

- ✓ request-id: "52238114", este número entero indica el orden de emisión de los datagramas.
- ✓ Error-status: noError(0), indica que no se encontró ningún tipo de error durante el proceso.
- ✓ Error-index: no se ha encontrado ningún error, por lo tanto su respuesta es 0.
- ✓ variable-bindings: 2 item, indica que dos variables fueron analizadas, una evalúa el tiempo y otra evalúa el OID.

5.3 RESULTADOS GESTION DE RED LAN CON PROTOCOLO SNMP VERSIÓN 3

La versión 3 del protocolo SNMP ofrece las características actualizadas de la versión dos, aquí se añaden mejoras bastante notorias en cuanto a la capacidad de configuración de la seguridad de la red. Dentro de las operaciones que puede realizar en esta versión están: Get, GetNext, Set, Trap, GetBulk e Inform.

Para el ejemplo en el Escenario C, se realiza un Snmpwalk desde el CMD de la estación Gestora hacia el Servidor Linux perteneciente a la red, se lo trabaja con el mismo OID anterior, .1.3.6.1.2.1.1.3.0,

El empaquetado en Wireshark muestra automáticamente un GetNextRequest, un GetRequest y un GetResponse por cada elemento

de la red consultado, en este caso será un GetNextRequest y un GetRequest, desde la estación Gestora con IP:192.168.199.50 hasta el Servidor Linux. Véase Figura 4.13 y Figura 4.14. Y un GetResponse desde el Servidor Linux hasta la estación gestora. Véase Figura 4.15. Dentro de los resultados se observa:

- ✓ la versión 3 y el nombre de usuario “version3”
- ✓ EngineID: encargado de identificar de forma exclusiva el agente en el dispositivo.
- ✓ Request-id: "27021", este número entero indica el orden de emisión de los datagramas.
- ✓ Error-status: noError(0), indica que no se encontró ningún tipo de error en el proceso.
- ✓ Error-index: 0, no se ha encontrado ningún error, por lo tanto su respuesta es 0.
- ✓ VarBindList: 1 ítem, se muestran que solo una variable fue analizada, también muestra el nombre del OID, 1.3.6.1.2.1.1.3.0.

En el Get Request y en el Get Next Request la evaluación muestra solo "NULL”, y en el Get Response este parámetro ya incluye la respuesta correspondiente al OID solicitado.

Seguidamente se muestran los tres casos de seguridad que ofrece esta versión del protocolo, podemos observar que en la Figura 4.17 se utiliza el tipo “NoAuthNoPriv”, y aunque las contraseñas ingresadas no son las correctas, este no lo detecta, pues este nivel no trabaja con ellas.

En la Figura 4.18 se utiliza el tipo “authNoPriv”, en este caso solo trabaja con una de las contraseñas es decir basta con que MD5 sea ingresada

correctamente para que se genere una respuesta, por ultimo con el tipo “AuthPriv” ambas contraseñas deberán ser ingresadas y de manera exitosa, pues si una de ellas está mal solo se generara un reporte mostrando el error como se observa en la Figura 4.19.

5.4 ANÁLISIS Y COMPARACIÓN DE RESULTADOS OBTENIDOS

Una vez realizadas todas las pruebas y obtenidos los resultados de manera independiente, se muestra un análisis en conjunto del protocolo SNMP en sus distintas versiones.

En SNMPv1, siendo la más básica de todas, se puede constatar con el sniffer (Wireshark), el formato de la PDU y todos sus campos definidos.

Se observa también que los traps en esta versión manejan otro tipo de formato que cambia a partir de la versión dos para estandarizarlo con el resto de las directivas.

En SNMPv2 se observa una gran similitud con la versión 1 y se aprecia que el formato de las traps ya se estandariza con el descrito en la PDU.

Se implementan nuevas directivas que optimizan las operaciones del protocolo, siendo una de estas el "GetBulk", que permite obtener múltiples OIDs en un solo paquete, lo cual es útil en una larga transmisión de datos.

SNMPv1 y SNMPv2 usan el campo de comunidad como método de seguridad y autenticación, el elemento de red compara el campo de

comunidad enviado por el agente con el definido en su configuración, si estos son iguales acepta el solicitud y envía la respuesta respectiva, caso contrario no responde nada, y el agente asume que su mensaje no fue recibido por lo que sigue intentando hasta llegar al límite de su tiempo máximo de conexión definido.

En SNMPv3 se emplean campos adicionales que se usan para la seguridad adicional implementada en esta versión. Ya no se utiliza la comunidad y en su lugar existe autenticación de usuarios. También se tiene la posibilidad de encriptar el contenido del paquete evitando que su contenido pueda ser leído usando un sniffer de red como se apreció en las pruebas. Estos dos parámetros de seguridad son opcionales y su uso se define en el elemento de red. El agente también puede especificar estos parámetros mediante tres niveles de seguridad:

- noAuthNoPriv: Sin autenticación y sin encriptación.

- authNoPriv: Autenticación y sin encriptación. Los protocolos permitidos para autenticación son MD5 y SHA.

- authPriv: Autenticación y encriptación. Los protocolos permitidos para autenticación son: MD5 y SHA. Los protocolos permitidos para encriptación son: DES y AES.

Se aprecia que en toda comunicación con SNMPv3, el primer mensaje es un Get-Request que se encarga de negociar los parámetros de seguridad con el elemento de red. En este proceso los dispositivos se ponen de acuerdo en los protocolos de autenticación y encriptación y se validan credenciales. En caso de existir errores de acceso o falla en la

negociación se retorna un mensaje SNMP de tipo REPORT definiendo el motivo del rechazo.

<table>
<tr><th colspan="3">Simple Network Management Protocol</th></tr>
<tr><td colspan="3">Permite y da la facilidad de monitorear y administrar la red</td></tr>
<tr><td colspan="3">Opera en el nivel de aplicación utilizando el protocolo de transporte TCP/IP</td></tr>
<tr><td colspan="3">Compuesto por dos elementos fundamentales el agente y el gestor</td></tr>
<tr><td colspan="3">Los mensajes son recibidos en el puerto UDP 161 y las Traps en el puerto 162</td></tr>
<tr><td colspan="3">Describe la información exacta y precisa de cada tipo de agente que tiene que administrar y el formato con que éste le proporciona los datos</td></tr>
<tr><td colspan="3">La operación de su gestión que se necesita para intercambiar información ocupa pocos recursos de la red</td></tr>
<tr><th>Versión 1</th><th>Versión 2</th><th>Versión 3</th></tr>
<tr><td colspan="2">Usan el campo de comunidad como método de seguridad y autenticación</td><td>Se emplean campos adicionales que se usan para la seguridad y la autenticación de usuarios</td></tr>
<tr><td>Operaciones que puede realizar: GetRequest, GetNextRequest, GetResponse, Set y Trap.</td><td colspan="2">Operaciones que pueden realizar: GetRequest, GetNextRequest, GetResponse, Set, Trap, GetBulk e Inform</td></tr>
<tr><td>Los traps tienen una estructura de PDU distinta a la de las versiones sucesoras</td><td>Estandariza la Versión 1 del protocolo en todas sus propiedades</td><td>Se puede encriptar el contenido de los paquetes evitando que su contenido pueda ser leído por otros usuarios</td></tr>
<tr><td>Permite el acceso a cualquier tipo de persona a la información que lleva la red</td><td>Tiene mejoras que optimizan las operaciones entre los agentes y los elementos de red</td><td>Tiene tres niveles de seguridad: 1.-"noAuthNoPriv" 2.-"AuthNoPriv" 3.-"AuthPriv"</td></tr>
</table>

Tabla5.1: Tabla sintetizada del protocolo SNMP con las principales diferencias reflejadas en las tres versiones

CONCLUSIONES

1. SNMP sirve para intercambiar y definir la estructura de una información mediante un mensaje entre una estación gestora y un agente

2. SNMP es un protocolo estándar que ayuda en la administración de redes utilizadas en Internet, se implementa de una manera fácil y sencilla, consume pocos recursos y poco tiempo del procesador, además posee la capacidad de unir distintos elementos de red sin importar marcas, modelos o fabricantes de los mismos, brinda también alarmas de alerta detectoras de fallas que se pueden observar mediante incidentes o gráficas.

3. Se pudo validar que todos los campos, del protocolo SNMP, aparecen en los paquetes capturados por el Sniffer de red tal como fueron definidos en los RFCs respectivos, para las distintas versiones del protocolo.

4. SNMPv2 definitivamente tiene mejoras que optimizan las operaciones entre los agentes y los elementos de red y además estandariza la versión 1 del protocolo.

5. En todos los escenarios se consultó el mismo OID para comprobar que la respuesta sea siempre la misma sin importar la aplicación,

sistema, o hardware de los distintos elementos de red utilizados en las pruebas y los resultados fueron satisfactorios.

6. Con el Wireshark se pudo confirmar la falencia en seguridad existente en las versiones 1 y 2 del protocolo SNMP, al poderse leer la comunidad usada en la red e incluso la información de los dispositivos. Si bien es cierto se cubre esta debilidad con controles de acceso por IP, se añade una capa más de administración que puede incluso llegar a ser vulnerada con ataques más sofisticados o incluso aprovechándose de descuidos en la configuración de accesos. Con la encriptación en la versión 3 se cubre esta vulnerabilidad y se puede apreciar en las capturas de paquetes.

7. Según lo investigado, a pesar de las mejoras en seguridad implementadas en SNMPv3 la versión 2 del protocolo aun es la opción preferida para el monitoreo de las redes actuales a tal punto que muchos sistemas incluso no soportan aun SNMPv3. Esto se debe a que las falencias de seguridad de las versiones anteriores a SNMPv3 pueden ser perfectamente controladas con políticas adecuadas de seguridad en la red. Si bien es cierto esto conlleva a una capa más de administración y configuración, el grado de complejidad es menor a la que involucraría una gestión de coexistencia entre diferentes versiones.

8. A pesar de que SNMPv3 soporta los protocolos DES y AES para encriptación, el procesamiento de los mismos tienen que ser gestionados por programas externos como por ejemplo openSSL.

RECOMENDACIONES

1. Para la implementación de SNMPv3 en Windows Server 2008 se tuvo que utilizar el paquete Net-SNMP debido a que el servicio de SNMP nativo de Windows no soporta esta versión.

2. Para poder hacer uso de la encriptación en SNMPv3, es necesario instalar el Net-SNMP con la característica de “EncryptionEnable”, esta opción se la define durante la instalación del programa.

3. Net-SNMP para Windows requiere de OpenSSL v0.9.8y, si se lo va a instalar con la característica de EncryptionEnable. Es importante tener en cuenta que Net-SNMP es una aplicación de 32 bits por lo que los binarios de OpenSSL también deben trabajar con la misma arquitectura.

4. Dado que Net-SNMP no es un servicio nativo de Windows, se deben ejecutar unos scripts adicionales que integran este paquete a los servicios de Windows.

5. Se recomienda comenzar a emplear SNMPv3, pues esta brinda mayor seguridad debido a la encriptación y evita que sea visible la información en texto plano, esto puede llegar a ser complicado de implementar en sistemas viejos que no dan soporte a esta versión, pero para redes actuales es preferible diseñar un plan que lleve versión 3.

BIBLIOGRAFÍA

[1] Barba Marti, A. Gestión de red, Ediciones OPC, Universita Politécnica de Catalunya, España 2001

[2] Barrios J. (2013). Cómo configurar SNMP. Extraído el 20 de abril de 2013, desde http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-linux-snmp

[3] Botero, N. (2005) Modelo de Gestión de seguridad con soporte SNMP. Extraído el 20 de abril de 2013, desde http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf

[4] Case J. (2001). Request for Comments: 1157, SNMP. Extraído el 18 de abril de 2013, desde http://www.ietf.org/rfc/rfc1157.txt

[5] Case J. (2002). Request for Comments: 3410, SNMPv3. Extraído el 18 de abril de 2013, desde http://tools.ietf.org/html/rfc3410

[6] Case J. (1993). Request for Comments: 3410, SNMPv3. Extraído el 19 de abril de 2013, desde http://tools.ietf.org/html/rfc1449

[7] García G. Desarrollo de plano de gestión para una red MPLS (2005). Extraído el 1 de Agosto del 2013, desde http://upcommons.upc.edu/pfc/bitstream/2099.1/3781/2/40628-2.pdf

[8] Edgar Pallo, Andrés Yajamin. “Escritura y compilación de una MIB para un transmisor de microondas” Extraído el 8 de abril de 2013, desde Repositorio Digital EPN: http://bibdigital.epn.edu.ec/bitstream/15000/5413/1/T2247.pdf

[9]Wikipedia. (n/d). Extraído el 22 de mayo de 2013, desde https://es.wikipedia.org/wiki/Router

[10] William Stallings, versión 2, 2003. Fundamentos de seguridad en redes: aplicaciones y estándares

[11] Botero, N. (2005). “Modelo de gestión de seguridad con soporte a SNMP”

[12] Wikipedia. (n/d). Extraído el 20 de mayo de 2013, desde http://es.wikipedia.org/wiki/Sistema_operativo

[13] Inteco Cert. “Análisis de Trafico con Wireshark”. Manual, 2011. http://openyourshell.files.wordpress.com/2011/02/analisis-de-trafico-con-wireshark.pdf

[14] Millan Ramon. (2003). “SNMPv3 (Simple Network Management Protocol version 3)” Extraído el 21 de mayo de 2013, desde http://www.ramonmillan.com/tutoriales/snmpv3.php

[15]Manage Engine. (n/d). Extraído el 16 de mayo de 2013, desde http://www.manageengine.com/products/mibbrowser-free-tool/