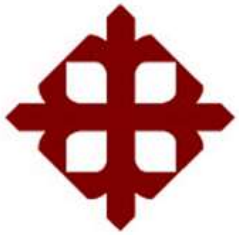

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TÍTULO:

ANÁLISIS Y PROBLEMAS DE LAS DIFERENTES VERSIONES DEL PROTOCOLO SNMP, IMPLEMENTACIÓN DE UNA RED CONECTADA CON 2 ROUTERS

AUTOR:

Viñan Carrillo, Diego Xavier

Previa la obtención del Título

INGENIERÍA EN TELECOMUNICACIONES

TUTOR:

ING. WASHINGTON MEDINA MOREIRA, MSc.

Guayaquil, Ecuador

2015

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por **Diego Xavier, Viñan Carrillo**, como requerimiento parcial para la obtención del Título de **Ingeniero en Telecomunicaciones.**

TUTOR (A)

_____

ING. WASHINGTON MEDINA MOREIRA, MSc.

DIRECTOR DE LA CARREAR

_____

ING. MIGUEL ARMANDO HERAS SÁNCHEZ

Guayaquil, 23 de septiembre del año 2015

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Diego Xavier Viñan Carrillo**

DECLARO QUE:

El Trabajo de Titulación **Análisis y Problemas de las Diferentes Versiones del Protocolo SNMP, Implementación de una Red conectada con 2 Routers** previa a la obtención del Título **de Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, 23 de septiembre del año 2015

EL AUTOR (A)

_____

Diego Xavier Viñan Carrillo

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Diego Xavier Viñan Carrillo**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Análisis y Problemas de las Diferentes Versiones del Protocolo SNMP, Implementación de una Red conectada con 2 Routers** previa a la obtención del Título **de Ingeniero en Telecomunicaciones**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 23 de septiembre del año 2015

EL AUTOR:

_____

Diego Xavier Viñan Carrillo

AGRADECIMIENTO

Agradezco todas las bendiciones que Dios me ha dado, la salud y la firmeza para lograr terminar una etapa de la vida que todos deseamos terminar.

Agradezco al esfuerzo día a día de mi madre María Enriqueta Carrillo Lluguay para darme lo que más necesitaba y terminar mi carrera, por ser el pilar más importante de mi vida y por ser la persona que me ha soportado.

Agradezco al Ing. Washington Medina por ser un buen amigo y un buen tutor por darme los conocimientos importantes para lograr comprender y terminar el proyecto.

Agradezco a todas las personas que me ayudaron desde el principio hasta el final de mi carrera, a las personas que me ayudaron con el proyecto y a las personas que confiaron en mí.

DEDICATORIA

A mi familia porque siempre estuvieron cuando comencé con mis sueños y siempre me ayudaron cuando lo necesitaba.

A mi sobrina Valentina Viñan Farías que fue la felicidad que Dios me pudo dar y para que pueda observar en un futuro los logros de su tío y nunca piense en retirarse o dejar sus sueños.

A mis amigos que siempre estuvieron conmigo.

GLOSARIO

CMD	Command prompt
IP	Internet Protocol
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
LAN	Local Area Network
MIB	Base de información de administración
NMS	Network Management Agent
OID	Object ID
RFC	Request For Comments
SNMP	Simple Network Management Protocol
SNMPv1	Simple Network Management Protocol versión 1
SNMPv2c	Simple Network Management Protocol versión 2
SNMPv3	Simple Network Management Protocol versión 3
TCP	Transmission Contrl Protocol
UDP	User Datagram Protocol

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Para las telecomunicaciones en el área de redes se han presentado muchos problemas ya sea por enviar o recibir información, equipos viejos, malas programaciones entre otros diversos temas; esto nos lleva a que las empresas presenten demasiados problemas y demandas en esta área.

En el área de redes hay diversos protocolos a usarse sea de seguridad o de monitoreo dependiendo de cómo se los utilice, para mejorar el funcionamiento de las redes. En este proyecto se estudiara sobre un protocolo muy conocido y muy usado en esta área y en muchas empresas; se trata del protocolo SNMP.

El capítulo 1, explicara de forma general el proyecto, tendremos el planteamiento del problema, los objetivos y diversas dudas que comenzamos al principio de este proyecto sea teórica y práctica.

Este proyecto consiste en estudiar todo sobre el protocolo SNMP, conoceremos la historia, concepto, características, clasificación de sus operaciones y sus versiones todo de manera teórica esto estará contenido en el capítulo 2, todo.

Para saber su funcionamiento real, realizamos una red conectada entre dos servidores y dos routers, sin antes enseñar los programas y las configuraciones que tenemos que realizar para que este proyecto en forma práctica se lleve con éxito, todo esto estará contenido en el capítulo 3.

Para el capítulo 4 tendremos configurados y conectados a todos nuestros equipos preparándose así para el respectivo análisis de cada versión del protocolo SNMP, tendremos los comandos a utilizarse para cada versión y para cada operación, tendremos las capturas de paquetes que son enviados desde un servidor a otro, en este caso de la maquina gestora hasta la máquina gestionada, diversos temas a tratar sobre dicho protocolo.

Finalmente en el capítulo 5 se verán los estudios de los informes obtenidos en el anterior capítulo, comparaciones entres versiones, beneficios, ventajas y desventajas, despejaremos las dudas que se tuvieron al principio de este proyecto teniendo en cuenta que se lo realizo en forma teórica y práctica con equipos reales.

ABSTRACT

For telecommunications networks in the area they have presented many problems send or receive information, old equipment, bad programming including various topics; this leads to companies to present too many problems and too much demand in this area. This brigns us to the companies to present too many problems and demands in this area.

In the area of networks there are differetn protocols to be used either security or monitoring depending on as in use, bad settings among other topics. In this project we study on a well-known and widely used protocol in this area and in many companies; it is SNMP.

Chapter 1, generally explain the project, we will have the problem statement, objectives and various doubts that started at the beginning of this project is theoretical and practical.

This project is to study all over the SNMP protocol, know the history, concept, characteristics, classification of their operations and their versions all theoretically this will be contained in Chapter 2, all.

To find out your actual operation, perform a network connected between two servers and two routers, without teaching programs and configurations we have to do this project in the forn practice be carried successful, this will be contained in Chapter 3.

For chapter 4 we configured and connected to all our teams and preparing to conduct an analysis of each version of the SNMP protocol, have the commands used for each version and each operation, we captures packets that are sent from a server another, in this case the manager machine to the managed machine, various topics on the protocol.

Finally in Chapter 5 studies the reports obtained in the previous chapter, enter comparisons versions, benefits, advantages and disadvantages we will be, will clear the doubts that were taken at the beginning of this project considering that it conducted theoretically and practice with real equipment.

CAPÍTULO 1

1 CONTENIDO DEL PROYECTO

1.1 INTRODUCCIÓN

En la actualidad se demanda tener un mayor control y administración en los dispositivos que integran las redes de telecomunicaciones; por tanto surge la necesidad de tener mejores herramientas y mejores controles para una buena gestión de red. Hay que tener mucho cuidado con las herramientas que se conectan porque una herramienta puede afectar directamente o indirectamente los otros equipos que están conectados a ella y esto trae problemas para los administradores.

El protocolo SNMP es una de las herramientas más usadas en las empresas por su costo ya que para tener una estación de trabajo se necesita personal para su mantenimiento y servicios técnicos; y esto a la larga generaba problemas financieros. Con el pasar de los tiempos y con una amplia demanda por este protocolo, se lo fue mejorando para que así su función se adapte a las empresas en sus requerimientos.

Este proyecto analiza el protocolo SNMP, su evolución, su mejoramiento y la comparación entre sus tres versiones existentes (SNMPv1, SNMPv2 y SNMPv3) para determinar sus problemas y el mejoramiento que tiene cada una de ellas en una pequeña red.

1.2 PLANTEAMIENTO DEL PROBLEMA

Las telecomunicaciones han logrado un gran crecimiento en el área de redes, por lo que es necesario saber las fallas o los problemas que se presentan, ya sea para vigilarla, para protegerla, por seguridad o simplemente darle un respectivo mantenimiento.

Existen varios protocolos que fueron creados para tener un buen manejo para las redes. Este proyecto se enfocara en desarrollar una simulación para conocer los problemas o el buen control que suceden en las redes con las diferentes versiones del protocolo SNMP; al enviar o recibir datos desarrollando su respectivo análisis y monitoreo.

1.3 JUSTIFICACIÓN

En las empresas surgen muchos problemas si los equipos están conectados a una red, que ocasionan daños o pérdidas, si su funcionamiento no es el correcto. En este proyecto nos enfocaremos en lo que es envíos o recepciones de paquetes o datos entre administradores, especificando el monitoreo de un solo protocolo, en este caso el protocolo SNMP donde se hará una comparación, análisis, problemas y funciones de cada versión de dicho protocolo.

Antes de escribir sobre el proyecto el protocolo SNMP es aquel que permite a los administradores supervisar en qué estado está el funcionamiento de la red, permite buscar y resolver los problemas que puedan presentarse en dicha red, es muy utilizado en las empresas por eso es que ha mejorado sus funcionamientos y procesos.

Utilizando una pequeña red con dos routers y dos servidores haremos el monitoreo y el análisis para cada versión del protocolo SNMP. Veremos el estudio y las diferencias en forma teórica del protocolo SNMP y sus diferentes versiones (SNMPv1, SNMPv2 y SNMPv3), se podrá indicar que versión es más utilizada y nos proporcione una mejor seguridad con un mejor control en las redes de las empresas. Este proyecto se lo explicara de manera teórica y práctica, con sus respectivos análisis y monitoreo dentro de esta pequeña red.

1.4 OBJETIVOS

1.4.1 Objetivo general

Analizar las diferencias de cada versión SNMP en diferentes escenarios de implementación.

1.4.2 Objetivos específicos

- Estudiar el Protocolo SNMP.
- Conocer las diferentes versiones del protocolo SNMP.
- Establecer las funciones y las diferencias de las versiones de SNMP.
- Establecer comunicación entre dos ordenadores con sistemas operativos Windows y dos routers Cisco.

- Implementar escenarios de simulación de las tres versiones de SNMP.
- Establecer las diferencias entre las versiones de SNMP mediantes análisis comparativos de los informes obtenidos.

1.5 TIPO DE INVESTIGACIÓN

El presente trabajo es de tipo descriptivo y explicativo.

- La investigación será de tipo descriptivo, la cual consiste en buscar y especificar características importantes del protocolo SNMP y de sus versiones.
- El tipo de investigación será explicativo, porque se explicará el funcionamiento de cada versión en su respectivo escenario.

1.6 HIPÓTESIS

En escenarios de simulación existe un SNMP que es más óptimo y brinda mayor seguridad.

1.7 METODOLOGÍA

Para poder entender sobre el protocolo SNMP y sus versiones se llegaran a realizarse pasos para así tener los conocimientos requeridos: tendremos el análisis teórico que serán las investigaciones y traducciones (libros, tesis de diferentes universidades, revistas, etc.), seguido de esto tendremos el análisis práctico (implementación de nuestra red) también constara los sistemas operativos con que trabajaran los ordenadores, los routers que se usaran para la conexión de nuestra red y los programas para el respectivo estudio, también de las configuraciones de cada uno.

Para comenzar con nuestro estudio tendemos el primer paso que será el análisis teórico tendremos todo lo investigado sobre que es el protocolo SNMP, historia, características, funciones y mucho más; también estarán las versiones de SNMP, que son SNMPv1, SNMPv2c y SNMPv3, características, diferencias, ventajas y desventajas; y todo lo que se necesario para nuestra red.

Tendremos nuestras herramientas que constaran de: dos ordenadores (laptops) con diferentes sistemas operativos en cada ordenador, tendremos dos routers CISCO cada

uno configurado para su respectiva función y los programas a usarse que son Net-SNMP que permite hacer la configuración de cada versión del protocolo SNMP; para así realizar su comparación y el programa Wireshark para tener las capturas de paquetes que son enviados para cada máquina virtual y así obtener nuestros informes.

Después de tener todo lo mencionado anteriormente nos queda lo último por realizar que es el análisis práctico; implementaremos nuestra respectiva red como se ve en la figura 1.1, pero por cada escenario se realizara una red que está configurada con su respectiva versión, para su respectivo análisis y para obtener la información que deseamos; para monitorear su manejo y forma de uso, así mismo los problemas que surgen y la perdida de los paquetes que se presentan.

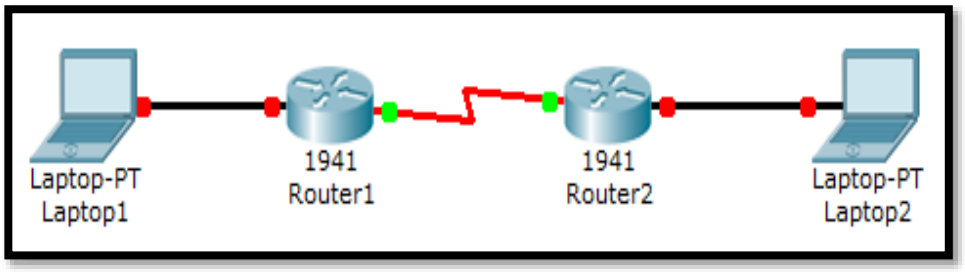

Figura 1.1 Topología de la red.
Elaborado por: Autor

CAPÍTULO 2

2 MARCO TEÓRICO

2.1 BREVE HISTORIA

En Internet, cada red individual tiene su propio conjunto de reglas y regulaciones. En 1993, para permitir la comunicación entre las diferentes redes, un comité independiente llamada la Junta Actividad de Internet (IAB) fue establecida para estandarizar las reglas de Internet entre los grupos de trabajo. El IAB cuenta con dos grupos de trabajo (Xerox, 2003).

- Internet Research Task Force (IRTF): miembros IRTF gestionar la búsqueda de protocolos de red como TCP / IP.
- Internet Engineering Task Force (IETF): Los miembros del IETF se reúnen tres veces al año y son responsables de mantener Internet operacional. Así, el IETF evolucionó y estandarizado el uso del protocolo SNMP para lo que es hoy.

El protocolo SNMP fue creado en 1988 debido a una gran necesidad de un estándar para administrar dispositivos sobre las redes IP, con el pasar de los años y viendo los problemas que daba el SNMPv1, en el año de 1993 se crea una nueva versión "SNMPv2"; mejorando así la gestión y problemas que presentaba la anterior versión del protocolo SNMP; con el pasar de los años deciden crear una nueva versión para mejorar más la gestión de red y es en 1998 que nace la nueva, mejorada y última versión del protocolo SNMPv3 para así mejorar con mayor capacidad la gestión de red, mayor capacidad y velocidad de envió de datos o paquetes y mayor control del usuario. Durante los últimos 20 años, SNMP ha evolucionado en un número de maneras. La especificación original SNMP tenía poco apoyo para la comunicación segura.

Figura 2.1 Historia del desarrollo del protocolo SNMP.
Fuente (Gutierrez, 2010)

2.2 SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

Un administrador necesita poder monitorear el estado de la red para ver qué sucede en ella, siempre desde el punto de vista de la administración. Los factores más importantes son el control y corrección de errores para poder ofrecer más fidelidad. SNMP es un protocolo que permite de una manera muy simple hacer esto. A pesar de que ha presentado pequeños problemas en cuanto a seguridad, es uno de los más populares desde sus inicios, hasta la actualidad, de hecho, es el protocolo que nos permite monitorear en internet (Doctors & Vecchiotti, 2012).

El protocolo SNMP forma parte de la capa de aplicación porque hace más fácil el intercambio de información entre las redes donde se maneja la administración. Trabaja con el protocolo TCP/IP para el control de transmisión. Con SNMP el administrador maneja las estructuras y los problemas que se presentan en las redes. Sin embargo, en SNMP hay operaciones que el protocolo TCP no puede realizar, por eso SNMP trabaja con el protocolo UDP (Datagrama), UDP es utilizado cuando la comunicación que no proporciona ningún reconocimiento, nos diga que no fue una transmisión exitosa (George, 2003).

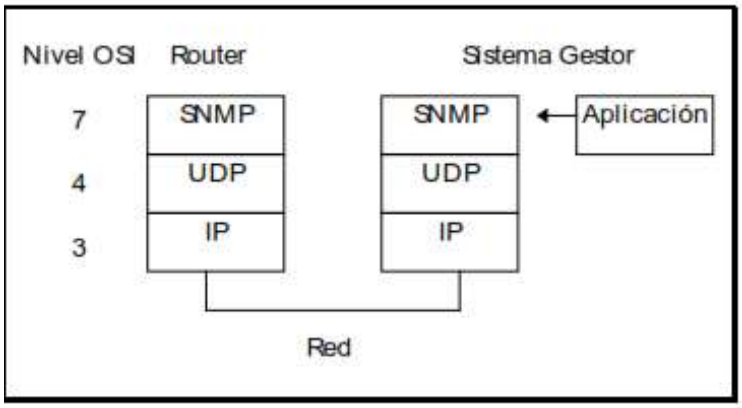

Figura 2.2 Niveles de protocolo del entorno de SNMP
Fuente: (Teldat, 2014)

SNMP es formalmente definido en la RFC 1157: "El modelo arquitectónico de SNMP es una colección de las estaciones de gestión y elementos de la red. Con las estaciones de gestión se ejecutan muchas aplicaciones que controlan y que supervisan los elementos de una red. En cambio para los elementos de la red serán dispositivos tales como ordenadores, puertas de enlace, servidores de terminales, y similares, que tienen los agentes de gestión encargados de llevar a cabo las funciones de gestión de red solicitados por las estaciones de gestión de red. SNMP se utiliza para enviar datos o información de gestión; entre las estaciones y los agentes de red." (CERT, 2002).

Según A. Telesyn Corporation, (2005); el marco de gestión de red estándar de Internet es el marco utilizado para gestión de la red en Internet. El marco se definió originalmente por tres documentos:

- RFC 1155, "Estructura e identificación de información de gestión para TCP / IP basados en internet " (conocidos como el SMI), detalla los mecanismos utilizados para describir y nombrar los objetos a ser gestionados.
- RFC 1212, "Gestión de base de información para la gestión de la red de TCP / IP basados en internet: MIB-II, define el conjunto básico de objetos administrados para la suite de protocolos de Internet. El conjunto de objetos administrados se puede ampliar mediante la adición de otra MIB específica a determinados protocolos, interfaces o dispositivos de red.

- RFC 1157, "Un protocolo simple de gestión de red (SNMP)", es el protocolo utilizado para la comunicación entre la gestión estaciones y dispositivos administrados.

Según A. Telesyn Corporation, (2005); los documentos posteriores que han definido SNMPv2c son:

- RFC 1901 → "Introducción de SNMPv2 basada en la comunidad entre los equipos"
- RFC 1902 → "Información de la estructura de gestión para la versión 2 (SNMPv2) "
- RFC 1903 → "Convenio textual para la versión 2 (SNMPv2) "
- RFC 1904 → "Declaraciones de conformidad para la versión 2 del protocolo de gestión de red simple "
- RFC 1905 → "Protocolo de operaciones para la versión 2 (SNMPv2) "
- RFC 1906 → "Asignaciones de transporte para la versión 2 (SNMPv2) "
- RFC 1907 → "Gestión de la base de información para la versión 2 del protocolo de gestión de red simple (SNMPv2) "
- RFC 2576 → "Relaciones entre la versión 1, versión 2 y la versión 3 del estándar de internet para la gestión de red del framework"
- RFC 2578 → "Estructura de gestión de información La versión 2 (SMIv2)"
- RFC 2579 → "Convenios textual para SMIv2"
- RFC 2580 → "Declaraciones de conformidad para SMIv2"

Según A. Telesyn Corporation, (2005); los documentos posteriores que han definido SNMPv3 son:

- RFC 3410 → "Introducción y aplicabilidad de las declaraciones de Internet estándar del marco de gestión "
- RFC 3411 → "Una arquitectura para la descripción del protocolo de gestión de red simple (SNMP) marcos de gestión "
- RFC 3412 → "Procesamiento de mensajes y envíos para el protocolo de gestión de red simple (SNMP) "

- RFC 3413 → "Protocolo de gestión de red simple (SNMP) Aplicaciones"
- RFC 3414 → "Utiliza el modelo de seguridad USM (User Security Model) para la versión 3 (SNMPv3) "
- RFC 3415 → "Utiliza el VACM (View Access Control Model) para la versión 3 (SNMPv3) "
- RFC 3417 → "Se asigna el transporte para el protocolo SNMPv3"
- RFC 3418 → "Base de información de gestión (MIB) para el protocolo de gestión de red simple (SNMP) "

2.3 ARQUITECTURA SNMP

Según Figueroa Arias, (1999); la arquitectura de SNMP contiene una gran colección de las estaciones de gestión y de los elementos de red. En las estaciones podemos ejecutar las aplicaciones que podrían permitir la observación y el control de los elementos de la red. En cambio los elementos de red son los dispositivos a utilizarse como: hosts, Gateway, servidores de terminal, etc., que contienen a los agentes para realizar las funciones de administración de red. Cuando se obtengan problemas, la arquitectura de SNMP desarrolla las siguientes soluciones:

- SNMP comunicara la información que se da en la gestión.
- SNMP representara la información de la gestión que se comunica.
- SNMP va a soportar las operaciones que se dan a través de la información de gestión.
- Se darán forma y significado a los intercambios entre entidades y a las referencias de las informaciones de las gestiones realizadas.

2.3.1 Propósito de la arquitectura

Para Figueroa Arias, (1999); el propósito será minimizar los números y las complejidades que dan las funciones de gestión que desarrollo el agente. Este propósito es atractivo por lo menos en tres aspectos que son:

- El costo, porque para el desarrollo de un software que SNMP soporte no tenga mucho valor financiero.

- Aumentaría el grado de las funciones de administración remota, porque se admitirá el uso de los recursos del internet para la administración
- Simplificara las funciones de gestión, son muy entendibles y son muy usados.

Otro propósito importante es que la herramienta para observar y controlar sea lo suficientemente fácil para los aspectos de gestión y operaciones de las redes. Y para el último propósito es que tenemos que dejar que la arquitectura sea independiente de los mecanismos de hosts o gateways (Figueroa Arias, 1999).

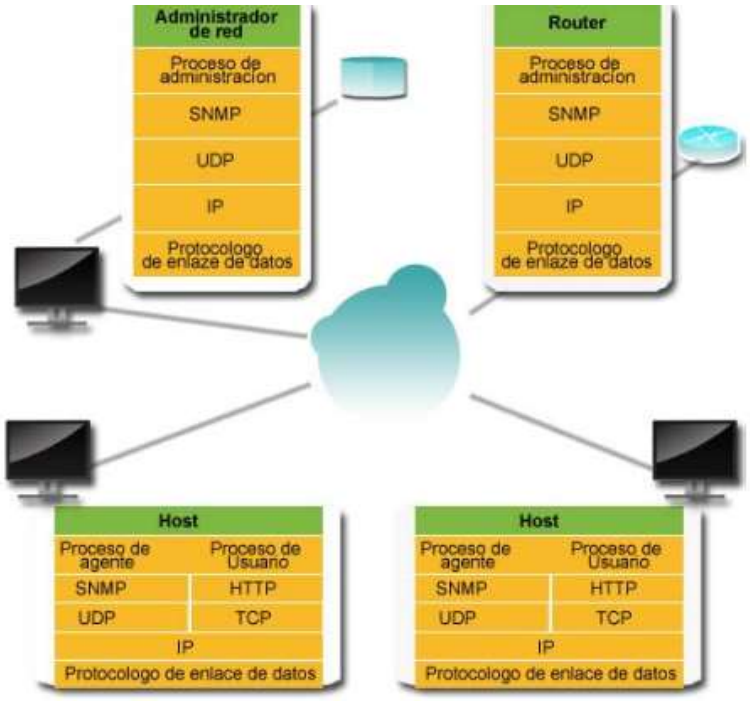

Figura 2.3 Elementos que intervienen en la arquitectura SNMP
Fuente: (Molero, Villaruel, Aguirre, & Martínez, 2010)

2.3.2 Elementos de SNMP

Para Lago & Mera, (2013); los elementos que conforman al protocolo SNMP son:

1. La estación de gestión (Manager-Administrador).
2. El agente de administrador (Agente).
3. La base de información de administración (MIB).
4. El protocolo de administración de redes.

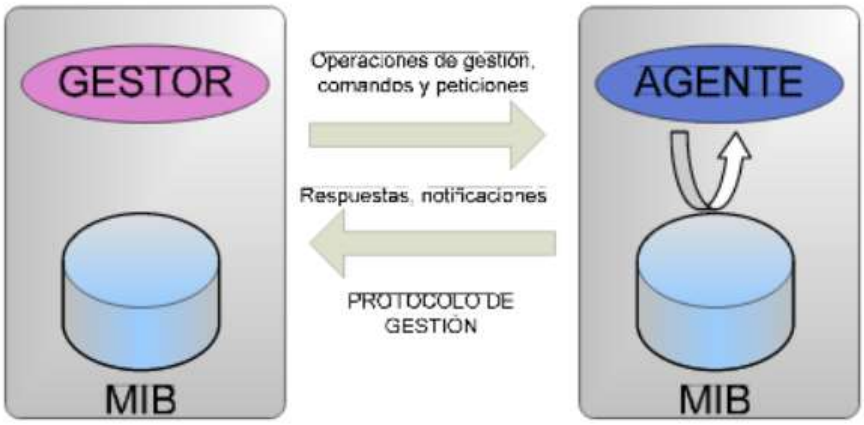

Figura 2.4 Protocolo de gestión
Fuente: (Ibarra & Ramos, 2014)

2.3.2.1 Estación de gestión (Manager-Administrador)

El administrador de SNMP es el software que se ejecuta en un ordenador central. El administrador del sistema utiliza el gestor de SNMP para comunicarse con el agente para gestionar la información almacenada en el elemento de red. El agente SNMP se ejecuta en cada elemento de red y es capaz de acceder a los elementos específicos en el MIB tal como se definen en ese dispositivo. La información de intercambios de agentes con el administrador utiliza unidades de datos de protocolo (PDU) (Xerox, 2003).

La función principal del administrador es sondear agentes para solicitar información específica. El administrado es configurado para escuchar pasivamente a la red para el tráfico específico (traps) y tomar la acción apropiada (Lorenzo, 2011). Los equipos o estaciones que son gestionados por el administrador son denominadas NMS, es aquel que ejecuta y muestra la información del estado de los dispositivos y de la red. Para que el administrador supervise y controle los dispositivos se ejecuta con el NMS (Lago & Mera, 2013).

Según Lago & Mera, (2013); el agente de gestión (MA), realiza la función de gestionar un grupo de elementos como hosts, pasarelas y servidores. SNMP es el que permite la comunicación entre las MA y los NMS. Los requisitos que deben cumplir las estaciones de red son:

- Para el análisis, la recuperación de información, la detección de alarmas y fallas, SNMP desarrolla un conjunto de aplicaciones en base a la gestión.
- Para el respectivo monitoreo y el control de red se desarrolla una interfaz.
- Desarrollar la capacidad de enviar los requerimientos que el administrador pide a los dispositivos remotos que conforman la red.

2.3.2.2 Agente del administrador (Agente)

Un agente es aquel que se encuentra en el dispositivo de una red, como un programa y escucha las peticiones del administrador, permite enviar los mensajes de respuesta PDU más convenientes a la red. Un agente también envía Traps no solicitados con el administrador. Las traps pueden indicar el uso incorrecto de la autenticación, la impresora se reinicia, estado del enlace, el cierre de una conexión TCP, o la pérdida de una conexión a un servidor de comunicaciones vecino (Xerox, 2003).

A los agentes también se los conoce como módulos software que van instalados en los dispositivos que deseamos gestionar. Es decir, al recibir un GetRequest o GetNextRequest, responderá con un mensaje GetResponse a la estación gestora, puede ser con la información solicitada o una indicación de error donde nos indique porque la solicitud deseada no es procesada. Con la operación SetRequest, SNMP pedirá el cambio de valor a una variable específica, el agente SNMP contestará con un GetResponse que nos dirá que el cambio se ha logrado, también indicar que si no se pudo realizar lo pedido emitirá un indicador de error. Con la operación Trap, SNMP permitirá que el agente informe a la estación gestora de cualquier evento importante (Lago & Mera, 2013).

Para los equipos que serán gestionados, obtendrán información del estado desde la base de información de administración (MIB). En este caso el agente se encargara de recoger y transmitir la respectiva información de los equipos ya administrados a los diferentes NMS, quien responderá las solicitudes o puede enviar alarmas o Traps cuando surjan los respectivos problemas. La función que pueden realizar las Trap es la de informar desde el agente hacia el NMS que algo no funciona bien como se fuera

una notificación. Ya que estas Trap son de alerta serán enviadas sin ninguna petición al NMS de manera asíncrona quien también puede hacer la ejecución de la respectiva información que ha recibido el agente. Un ejemplo sencillo será la caída del internet en un router, se podría enviar Trap hacia el NMS informando sobre la perdida de internet (Lorenzo, 2011).

2.3.2.3 Base de información de administración (MIB)

Un agente SNMP utiliza una base de datos de información cuando el administrador SNMP solicita los valores de la misma. Esta colección de datos se conoce como la base de información de gestión (MIB). La información de la MIB sigue la estructura de información de gestión (SMI). SMI es el estándar que define la estructura de una MIB de manera que cualquier proceso que consulta la recibe un resultado esperado. Se puede pensar en el MIB como un árbol. La base del árbol contiene la información más genérica. A medida que suben el árbol, la información más detallada sobre cada aspecto separado de un elemento se revela hasta que se exponen todas las piezas de información acerca de un dispositivo. Cada una de estas piezas es conocida como un identificador de objeto (OID). El nivel más bajo del árbol que normalmente se conoce como "Internet". Las principales ramas llevan el nombre de los tipos más específicos de dispositivos como anfitrión, impresora, datos privados, y el router (Xerox, 2003).

El MIB utiliza la notación de sintaxis abstracta 1 (ASN.1) convención de nombres para nombrar todas las variables. ASN.1 garantiza un espacio de nombres único y absoluto para acceder a las variables MIB. Por ejemplo, la convención de nombres para la variable MIB que cuenta datagrama IP entrante, ipInReceives, es: iso.org.dod.internet.mgmt.mib.ip.ipInReceices. MIB proporcionan las variables que se pueden **almacenar** (set) o **leer** (get), para cambiar los parámetros o proporcionar información sobre los dispositivos de red e interfaces. Es decir que el agente recolectara datos o información desde el MIB en respuesta a la solicitud pedida del administrador para obtener o almacenar datos importantes (Xerox, 2003).

2.3.2.3.1 Tipos de MIB

Según Xerox, (2003); hay tres tipos de MIB:

- **Público:** Las MIB públicas siguen las MIB estándar y se puede acceder a cualquier proveedor que utiliza SNMP como vehículo de comunicación.
- **Privado:** La aplicación MIB puede ampliarse para dar cabida a la adición de nuevos objetos. Esta flexibilidad permite que los diferentes proveedores puedan crear objetos para gestionar las entidades específicas y únicas de sus productos. MIB privadas pueden ser publicados y puestos a disposición del público si se desea. MIB privadas siguen las convenciones estándar SMI. Por lo tanto, cuando se concede un acceso adecuado, es posible que los diferentes proveedores para administrar las MIB privadas de otros proveedores.
- **Pública / experimental:** El público / MIB experimental es utilizado por los vendedores para desarrollar MIB.

Existen muchos tipos de objetos que se pueden representar en los dispositivos de la red, cada objeto que se maneje a través del MIB tendrá una identificación de objeto único, que también incluye el tipo de objeto, los niveles de acceso que so podrían dar que son “Read-Only” y “Read-Write” limitando la información y tamaño en rango (Lago & Mera, 2013).

- Cualquier elemento que sea manejado con SNMP tendrá su respectivo objeto específico como si fuera un cartón sellado.
- También cada característica tendrá su identificador de objeto (OID) el cual será dado por números separados por puntos decimales (así 1.3.6.1.4.1.2682.1).
- Se podrá colocar una etiqueta legible a los MIB que son asociados con los OID (ej. dpsRTUAState).
- Se podría decir que el MIB servirá como un diccionario pero que solo será en base a datos y códigos que es para los mensajes de SNMP.

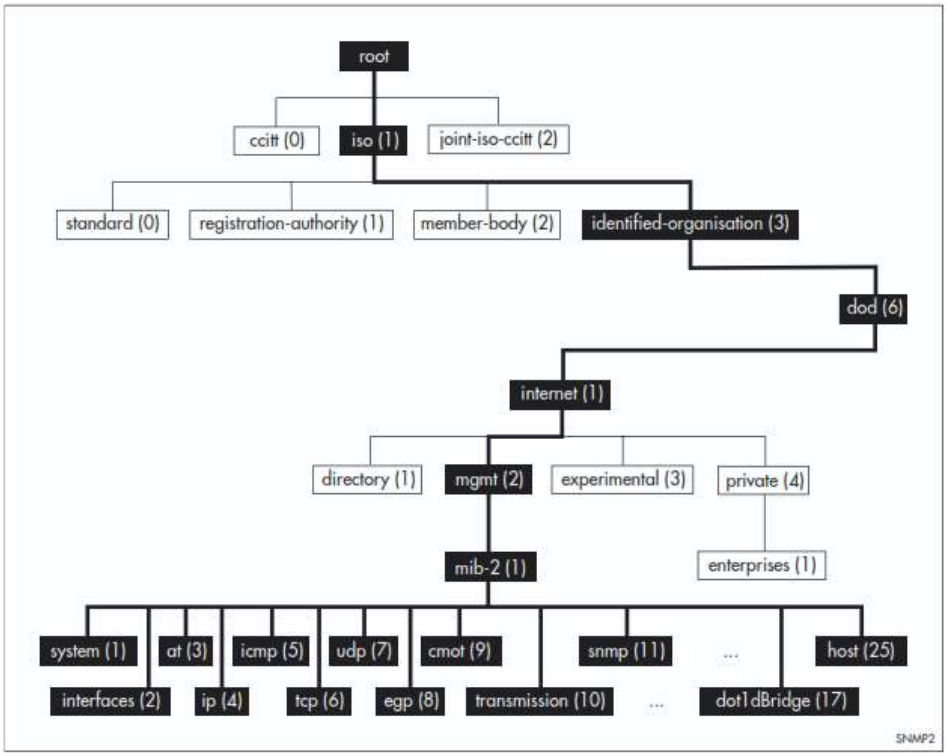

Figura 2.5 Esquema de árbol de una MIB
Fuente: (Lorenzo, 2011)

2.3.2.3.2 MIB-II

Los agentes son capaces de llevar o colocar muchos MIBs pero se implementa una muy en particular que es la del MIB-II. La característica principal del MIB-II es la de proporcionar una MIB pero estandarizada que pueda guardar los datos de la gestión que son la información del sistema, interfaces, protocolos, etc. Para poder definir una MIB-II para las redes de TCP/IP se lo puede hacer como iso.org.dod.internet.mgmt.1, o también con números como 1.3.6.1.2.1. A continuación se podrá observar el grupo system que es mib-2.system.0, o 1.3.6.1.2.1.1, y así continuamente (Lorenzo, 2011).

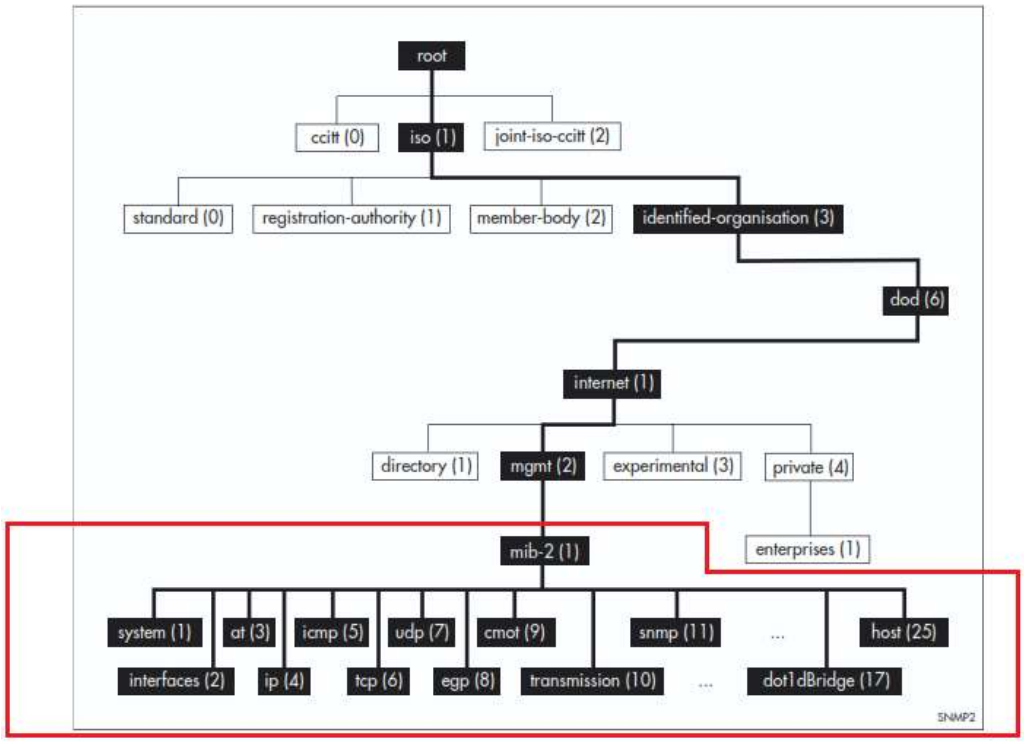

Figura 2.6 Subárbol MIB-II
Fuente: (Lorenzo, 2011)

2.3.2.4 Protocolo de administración de red

También es un protocolo de la capa de aplicación, es decir pueden examinar o cambiar todas las MIBs que desea del agente. Al realizar la comunicación para la información entre el administrador y el agente se la realiza a través del protocolo SNMP por donde se hará el intercambio de mensajes protocolares. Otra función que realiza el protocolo de administración de red es enlazar la estación de gestión con los agentes. La destreza que se maneja en SNMP es que al monitorear la red en cualquier nivel es llevado con éxito especialmente el sondeo de la información que se da desde el monitoreo. Los mensajes no solicitados llamados Traps son ordenados ya que mantienen el tiempo y mantienen la atención del sondeo que se da entre los dispositivos. Se establece un límite a los mensajes que no fueron solicitados y esto mejora la meta de simplicidad y mejora minimización de la mayor cantidad de tráfico generado por las respectivas funciones de la gestión (Lago & Mera, 2013).

Figura 2.7 Componentes de SNMP
Fuente: (Velásquez, 2009)

2.3.3 Estructura de PDU

Según Figueroa Arias, (1999); antes de mencionar las operaciones de PDU tenemos que tener claro cuáles son los datos que se incluyen en los paquetes al enviarse de la PDU y son:

- **RequestID:** Nos permite indicar el orden para él envió de los datagramas. Otra función importantes es que permite que no se envíen datagramas duplicados para los servicios de datagramas que son muy pocos confiables
- **ErrorStatus:** Nos permite saber si ha existido o no un error. Puede que tome cualquier valor:
    - noError (0)
    - tooBig (1)
    - noSuchName (2)
    - badValue (3)
    - readOnly (4)
    - genErr (5)
- **ErrorIndex:** Cuando se obtenga un error, nos indicara cual variable fue la que nos generó el problema.
- **VarBindList:** Nos da una lista con los nombres de las variables con su respectivo valor. Las pocas PDU son definidas solo con los nombres que se les dan. Es recomendable que cuando se tienen estos casos definir nuestros valores con NULL.

Para Xerox, (2003); las unidades de datos de protocolo (PDU) representan el vocabulario básico a través de los gestores SNMP y los agentes de comunicación de información. PDU son asíncronas en la naturaleza. Esto significa la comunicación entre el gestor y el agente se divide en dos mensajes, solicitud y la respuesta. Desde la versión 1 hasta la versión 3 manejaran siempre las mismas operaciones aunque aumentaran por cada versión y por cada mejoramiento; las operaciones son:

- Operación getRequest
- Operación GetNextRequest
- Operación getResponse
- Operación setRequest
- Operación Trap

Para Xerox, (2003); las operaciones PDU getRequest y GetNextRequest recuperar datos de elementos de red. La operación setRequest permite la modificación de los datos sobre el elemento de red. La respuesta a estas PDU se devuelve con el comando getResponse. La última PDU, Trap, permite que el elemento de red para transmitir datos bajo ciertas condiciones. Estas cinco operaciones cumplen tres tareas principales para el software de cliente:

- Un PC cliente puede leer un fragmento de información.
- Un cliente puede cambiar una pieza de información.
- Un dispositivo inicia la comunicación de información al cliente cuando se utiliza la trampa PDU.

2.3.3.1 Operación GetRequest y operación GetNextRequest

Las operaciones GetRequest y GetNextRequest solicitaran al destino los valores de algunas variables. Para la operación GetRequest estas variables estarán ubicadas en la lista VarBindList; y para el caso de la operación GetNextRequest los nombres que usan son lexicográficos para los nombres de las variables en las listas, esta operación es muy útil para poder manejar tablas de información sobre cualquier MIB. El campo ErrorStatus y el campo ErrorIndex siempre tendrán “0”. Cuando la aplicación SNMP requiere se podrá generar una entidad. Para saber que no hubo ningún problema las

PDU siempre tendrán que esperar una respuesta que en este caso será la operación GetResponse (Figueroa Arias, 1999).

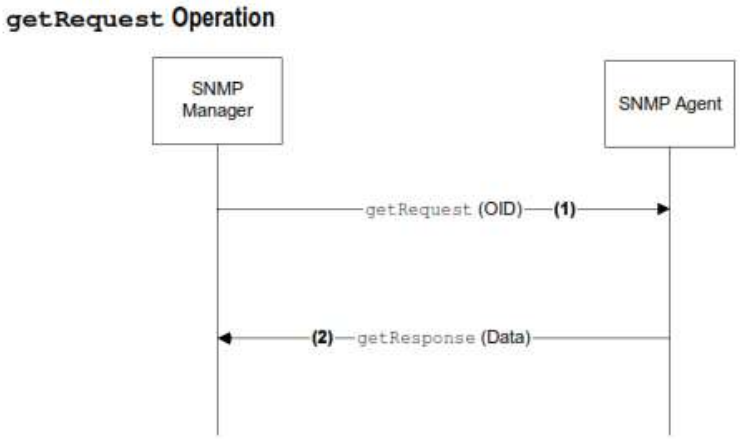

Figura 2.8 SNMP operación getRequest
Fuente: (Xerox, 2003)

- getRequest informa al agente SNMP para obtener el valor de un identificador de objeto (OID).
- getResponse devuelve el valor asociado con el OID de la MIB del SNMP-agente.

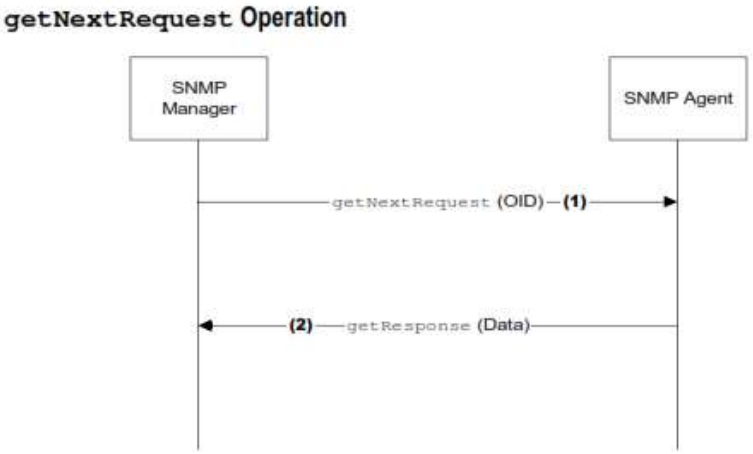

Figura 2.9 SNMP operación getNextRequest
Fuente: (Xerox, 2003)

- GetNextRequest informa al agente SNMP para obtener el valor de la siguiente OID raíz de la petición OID.

- getResponse devuelve el valor asociado con el siguiente OID del MIB del SNMP-agente.

Esta técnica se utiliza para "walk" (caminar) la MIB para permitir que un cliente pueda interrogar a cada valor contenido dentro de la MIB. Cuando no hay "next" (siguiente) OID, el agente SNMP devuelve un error (Figueroa Arias, 1999).

2.3.3.2 Operación SetRequest

Maneja el orden hacia la entidad de destino eso quiere decir que pone a cada objeto en la lista VarBlindList, con su respectivo valor que tiene asignado en la lista. La entidad de protocolo genera una entidad cuando se requiera la aplicación de SNMP. Para poder saber que se ejecutó con éxito tendrá que esperar la respuesta de la operación GetResponse (Figueroa Arias, 1999).

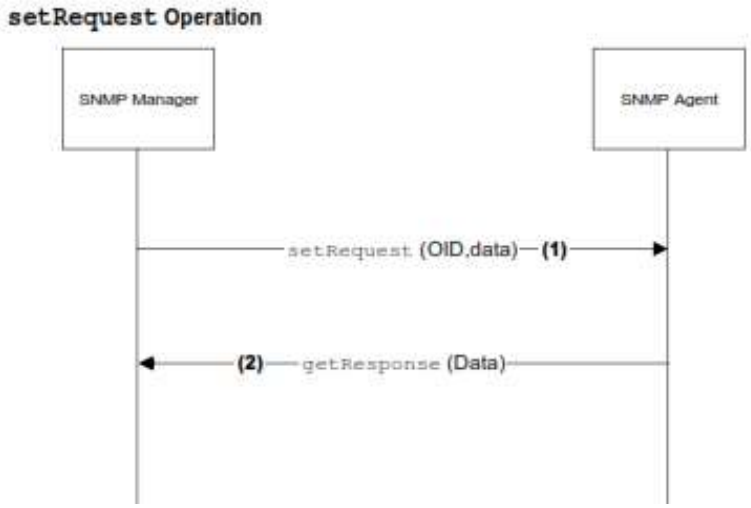

Figura 2.10 SNMP operación setRequest
Fuente: (Xerox, 2003)

- setRequest le dice al agente SNMP para modificar el valor de un OID a un valor específico.
- getResponse devuelve el valor que se estableció por el agente SNMP, o un error, si el administrador no tiene permisos suficientes, o el OID no es válido.

2.3.3.3 Operación GetResponse

Según Figueroa Arias, (1999); esta operación se genera para que cumpla el trabajo de responder a las operaciones GetRequest, GetNextrequest o setRequest. Esta operación está contenida por la información que se requiere de la entidad de destino o por la indicación de cualquier error; para que funcione correctamente y sin ningún problema lo mencionado anteriormente se sigue las siguientes reglas:

- Cuando no coincidan los nombres de las listas con los nombres de cualquier objeto del MIB donde se desea realizar la operación set/get, la entidad notificara con un GetResponse idéntica a la que se recibió, pero con el campo ErrorStatus en la sección "2" la del noSuchName, señalando el nombre del objeto que origino el error de la lista recibida.
- Con el mismo modo actúa si cualquier objeto de las listas que se recibieron es de tipo agregado (como se define en el SMI), siempre y cuando la PDU recibida sea de la operación GetRequest.
- En el caso que se reciba la operación SetRequest y el valor de la variable de la lista no está fuera del rango o no es de tipo correcto, se envía un GetResponse igual a la recibida pero con la excepción que el campo ErrorStatus ahora obtendrá el valor "3" que es la del badValue y el campo ErrorIndex cumplirá con la función de señalar los objetos de la lista donde se generó el error.
- Cuando se excede el tamaño de la PDU que se recibió, se enviara al remitente la operación GetResponse igualita a la que se recibió, pero esta vez el campo de ErrorStatus será puesto a "1" que será el tooBig.
- Cuando no se pueda obtener el valor de la lista por cualquier razón que se observó en las reglas anteriores, se enviara un Getresponse idéntica a la recibida, pero esta vez el campo ErrorStatus estará puesto al valor "5" que es el de genErr, y para el campo de ErrorIndex nos indicara el objeto donde se originó el error.

Según Figueroa Arias, (1999); cuando no se pueda aplicar las reglas anteriores, se lograra enviar un getResponse pero con las siguientes características:

- Al obtener una respuesta de la getResponse que se envió lograra tener la lista varBindList recibida, con los nombres de objetos que fueron asignados el valor que corresponde.
- Al obtener una respuesta GetNextResponse, se obtendrá la respectiva lista varBindList pero con los lexicográficos de cada objeto que se recibió, junto a cada nombre, se colocara su valor correspondiente.
- Al obtener una respuesta SetResponse, estarán iguales, lo primero que se hará es asignar a cada variable que se mencionan en la lista varBindList su valor correspondiente. Será considerado simultáneo para todas las variables.

Para finalizar sino cumplen estos casos el valor del ErrorStatus es "0" es decir pertenece al noError, igual funcionara con el ErrorIndex. Para el valor de requestID será el mismo que se recibió (Figueroa Arias, 1999).

2.3.3.4 Operación Trap

Según Figueroa Arias, (1999); la operación Trap es aquella que nos indicara si hay problemas. La aplicación SNMP generara una petición de entidad del protocolo. Cuando se recibe una Trap se presentara los contenidos a la entidad de aplicación que se solicitó; una operación Trap incluye los siguientes datos:

- Enterprise: Sera el tipo de objetivo que se generó en la Trap.
- Agent-addr: Sera la dirección del objeto que se generó en la Trap.
- Generic-trap: Seran los enteros que se indicara para el tipo de Trap; pueden ser:
    - ColdStart (0)
    - warmStart (1)
    - linkDown (2)
    - linkUp (3)
    - authenticationFailure (4)
    - egpNeighborLoss (5)
    - enterpriseSpecific (6)

- specific-trap: Sera el que contenga el entero con un código específico para la Trap.
- Time-stamp: Sera el tiempo donde fue la última inicialización de la entidad de red y la que generara la Trap.
- Variable-bindings: Contiene información de posible interés y su lista será del tipo varBindList.

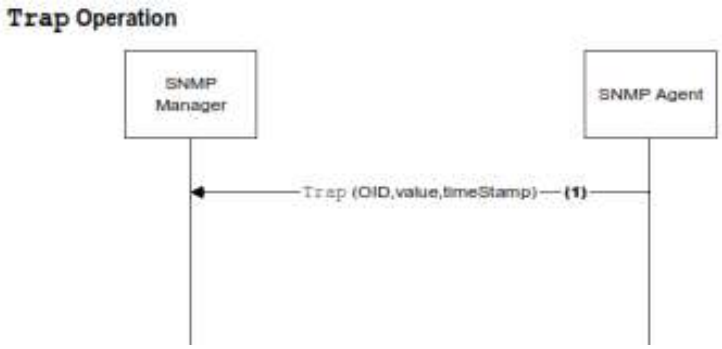

Figura 2.11 SNMP operación Trap
Fuente: (Xerox, 2003)

La trap permite que un agente SNMP comunique un valor modificado cuando el valor cruza un umbral pre-especificado. El agente SNMP se puede configurar para enviar información trap al administrador SNMP designado (Figueroa Arias, 1999).

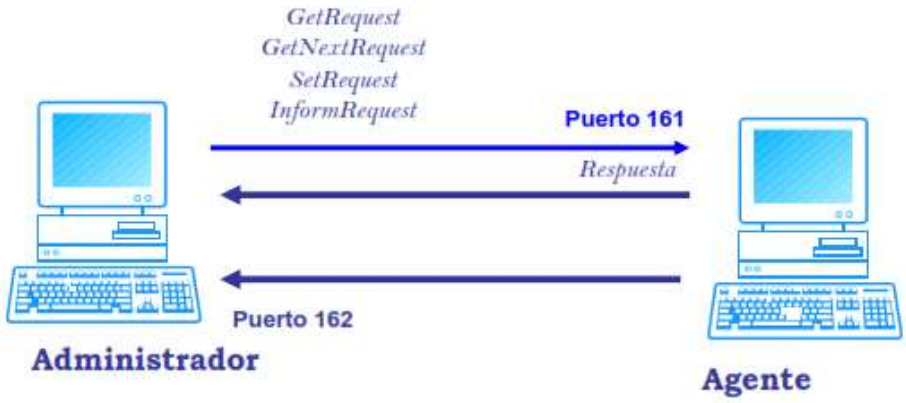

Figura 2.12 Funcionamiento de SNMP.
Fuente: (Sabal, 2006)

2.4 DESCRIPCIÓN GENERAL DE CADA VERSIÓN DEL PROTOCOLO SNMP

En estos tiempos existen tres tipos de versiones de SNMP que son: SNMPv1, SNMPv2c y SNMPv3. La versión 1 de SNMP (SNMPv1) fue la primera versión creada con operaciones que facilitaban al administrador, pero como la tecnología evolucionaba y esta versión daba problemas, se decide crear una nueva y mejorada versión (SNMPv2c) y esta versión consta con las antiguas operaciones de la versión 1 pero se integrarían nuevas versiones así mismo con el manejo de las Traps. Los administradores al ver que se necesitaba seguridad en este protocolo deciden crea la versión 3 (SNMPv3) esta contiene lo mismo que las antiguas versiones solo que se mejora en la seguridad al enviar los paquetes ya tendrían un código que solo los usuarios que están incluidos al enviar los paquetes pueden descifrar el código o sea tea versión mejora en lo que es seguridad.

2.4.1 Protocolo de administración simple versión 1

SNMP versión 1 contiene el modelo básico MIB, y Set / Get enfoque descrito anteriormente. También contenía un mecanismo de seguridad rudimentaria conocida como nombres de comunidad SNMP. El problema con los nombres de comunidad, sin embargo, es que la contraseña está en texto plano, y puede ser interceptada y utilizada por las personas que supervisan el tráfico SNMP entre el cliente y el dispositivo de red. Esta versión de SNMP es un estándar de internet establecido y es predominante en la industria (Xerox, 2003).

Para entender sobre el protocolo SNMPv1 estará descrito en las RFC 1155, 1157, y 1212 del IETF. Se podría decir que es un protocolo que hace una petición y obtiene una respuesta es muy sencillo de manejar. El trabajo de SNMPv1 sera por el uso de las operaciones del protocolo: Get, GetNext, Set, y Trap. Todas estas operaciones fueron descritas anteriormente pero se recordara lo más básico para la operación Get se lograra el uso del NMS para lograr la recuperación de los valores de los objetos del agente. Para la operación GetNext, cumplirá la función que es utilizada por el NMS para poder lograr recuperar los valores de los objetos de las tablas o que están dentro de un agente. Con la operación Set, el NMS lo utilizara para la configuración de los

valores del objeto que están dentro de la red. Para la última operación Trap, los agentes lo utilizan para informar de manera asíncrona el NMS de cualquier hecho relevante que se pida (Lago & Mera, 2013).

Según Moreno & Serna, (2013); el formato de mensajes para la versión SNMPv1 es idéntica a la versión 2, los mensajes que se usan para la respectiva comunicación entre el administrador y el agente contiene un formato con tres indicadores:

- ✓ Versión: es aquel que indica el número de versión del protocolo SNMP que se está utilizando en el ordenador.
- ✓ Nombre de comunidad: Es aquel que estará conformado con el conjunto de estaciones de red o de dispositivos que se lograran administrar y que serán utilizados para la respectiva autenticación.
- ✓ PDU: Es aquel donde estarán los diferentes tipos de PDU.

Figura 2.13 Formato de mensajes SNMPv1
Fuente: (Moreno & Serna, 2013)

Según Moreno & Serna, (2013); como se observó en la figura 2.13, nos indica la descripción del formato de las mensajes de la versión 1; las operaciones de cómo es enviada la PDU serán indicadas en la figura 2.14.

Figura 2.14 Formato de las PDU
Fuente: (Moreno & Serna, 2013)

Según Moreno & Serna, (2013); para la versión SNMPv1 también constara de la Trap y es por eso que en la figura 2.15 se puede observar como es el formato de la operación de la Trap.

Figura 2.15 Formato de la Trap versión SNMPv1
Fuente: (Moreno & Serna, 2013)

2.4.2 Protocolo de administración simple versión 2

Según Xerox, (2003); SNMP versión 2 (SNMPv2) además de mejorar su seguridad, incluye un mecanismo de recuperación mayor y el mensaje de error que nos detallara los informes a las estaciones del administrador. Para el trabajo de recuperación mayor constara con el gran apoyo de recuperar las grandes cantidades de información que se podrían haber perdido. Este mecanismo mejora el rendimiento de la red al acceder grande cantidades de datos. SNMP versión 2 tiene soporte mejorado de gestión de errores e incluye error ampliada de códigos que distinguen diferentes tipos de condiciones de error; estas condiciones de error son reportadas a través de un único código de error en SNMP versión 1. En la Versión 2, el código de error también informa del tipo de error. Además, también se reportan tres tipos de excepciones en SNMP Versión 2. Ellos son:

- ✓ No such object
- ✓ No such instance
- ✓ End of MIB

Según Lago & Mera, (2013); SNMPv2 está definido en las RFC's como ya lo hemos dicho anteriormente. SNMPv1 y SNMPv2 tienen muchas características en común, pero la versión 2 es mejor y se integran nuevas operaciones de protocolo que son:

- ✓ GetBulk: Sirve para la recuperación de grandes bloques de datos como lo son las columnas de una tabla, esta operación se realizara desde el gestor.
- ✓ Inform: Esta operación se desarrollara enviando la información del agente al gestor y así obtener la confirmación respectiva.
- ✓ Report: Sera la operación que el agente enviara de una manera espontánea las excepciones y los errores que se generaran en el protocolo.

En el año de 1995 apareció una versión de SNMPv2, que sería el mejoramiento de la versión 2 como que si fuera un plus denominada SNMPv2c, se lograron añadir mejoras en base a la configuración sencilla y con mayor modularidad, siempre y cuando se mantuvo el inseguro y sencillo mecanismo de autenticación de las versiones anteriores basado en los nombre de comunidad. Las operaciones que se integraron a SNMPv2 desarrollarían una mejor eficiencia en el intercambio de la información. Las operaciones que estaban contenidas en la versión 1, son las mismas que cumplirán el mismo funcionamiento con la versión 2; con la única diferencia que las 3 primeras operaciones ya no estarán trabajando en modo atómica, es decir si la operación falla con cualquier objeto, el resto de objetos solicitados seguirán ejecutándose y la única operación que lograr mantener este modo es el SetRequest (Lago & Mera, 2013).

Según Moreno & Serna, (2013); como se lo ha explicado el mismo formato que se maneja en la versión 1 también se lo hace en la versión 2 por eso en la figura 2.16 solo se explicara el formato de la nueva PDU integrada que es el GetBulkRequest.

Figura 2.16 Formato de la PDU GetBulkRequest
Fuente: (Moreno & Serna, 2013)

Según Moreno & Serna, (2013); las Traps de SNMPv2 realizan la misma función que la versión 1, a diferencia que el formato cambia para así poder facilitar el procesamiento en el receptor. En la figura podemos observar también el formato de la otras PDU que se integran a la versión 2 que es el InformRequest y el report, todas asociados en un mismo formato con las Traps.

Figura 2.17 Formato de las PDU informRequest, Report y Trap v2
Fuente: (Moreno & Serna, 2013)

2.4.3 Protocolo de administración simple versión 3

Según Lago & Mera, (2013); SNMP versión 3 fue aprobado como un estándar por el órgano de Internet Engineering Task Force (IETF) normas en 2002. Llegando a ser la última versión, los creadores decidieron reforzar la seguridad, incluyendo lo que es la autenticación, privacidad, control de acceso y de administración pero con una gran modularidad y con la posibilidad de una configuración muy remota. SNMPv3 no es el estándar que lograra reemplazar a las antiguas versiones sino que será aquel que tenga mayor capacidad de seguridad y de administración. Se logró diseñar esta versión para protegerla usando encriptación y autenticación para las siguientes amenazas:

- **Modificación de información**: Se podría cambiar el mensaje que se generó por otra que esta con la protección de la autenticación y así no permitir el acceso de una entidad no autorizada que recibió el mensaje, el único detalle es que se pueda modificar cualquier parámetro de cualquier configuración.
- **Enmascaramiento (masquerade):** Para los usuarios que no están autorizados podrán intentar operaciones logrando así asumir la entidad de otro usuario que si posee la autorización correspondiente para las operaciones deseadas.
- **Reenvió de mensajes**: Ya que SNMP trabaja sobre un protocolo de transporte sin ninguna conexión hay el riesgo de que un mensaje pueda ser almacenado por algún otro usuario y luego ser duplicado o reenviad; para así lograr realizar operaciones que no estén autorizadas.
- **Poca privacidad (disclosure):** Cualquier entidad puede observar el intercambio que hay entre los mensajes de un agente y un equipo de administración y lograr aprender todos los valores de los objetos que se encuentran.

Para Teldat, (2014); los niveles de seguridad que existen en la versión 3 de SNMP estarán clasificados en la tabla 2.1.

Tabla 2.1 Niveles de seguridad para SNMPv3

noAuthNoPriv	AuthNoPriv	AuthPriv
Los paquetes no usan autenticación ni cifrado. Este nivel solo es aplicado en los paquetes de la seguridad de las versiones 1 y 2 de SNMP	En este nivel los paquetes estarán usando la autenticación pero el problema es que los paquetes no van cifrados presentando un poco de inseguridad.	Este último nivel de seguridad permite que los paquetes usen autenticación y cifrado, mejorando con mayor fuerza la seguridad.

Fuente: (Teldat, 2014)

Según Moreno & Serna, (2013); en la versión 3 de SNMP no se añadirán ni se mejoraran las operaciones de PDU, constara con las mismas PDUs que estaban definidas en la versión 2 de SNMP, la función más importante es la de mejorar su seguridad. El formato de mensaje para esta versión lo dividiremos en tres campos: en el primer campo tendremos los que son generados por el modelo de procesamiento de mensajes:

- msgVersion: Contiene el número de versión del mensaje SNMP.
- msgID: Podrá identificar el mensaje se lo utiliza para la relación entre solicitud y respuesta de los mensajes.
- msgMaxSize: Nos permitirá lograr especificar el tamaño del mensaje donde soportara el emisor. El valor mínimo sera de 484.
- msgFlags: Para este octeto estarán contenidos las tres banderas en los bits menos significativos.
    - reportableFlag: determina si se envía o no un reporte.
    - privFlag: Es aquel que nos indica si se empleó o no una criptografía
    - authFlag: Nos indica si se emplea autenticación.
- msgSecurityModel: Nos especifica el modelo de seguridad que se maneja.

Según Moreno & Serna, (2013); en el siguiente campo tendremos el modelo de seguridad basado en lo que es el usuario:

- msgAuthoritativeEngineID: Lograra representar el motor autorizado del snmpEngineID.
- msgAuthoritativeEngineBoots: Este representa el motor autorizado del snmpEngineBoots.
- msgAuthoritativeEngineTime: Aquel que representara el motor autorizado del snmpEngineTime.
- msgUserName: Cuando nos envíen un mensaje es aquel que especificara el nombre del usuario.
- msgAuthenticationParameters: Son los parámetros definidos por el protocolo de autenticación.
- msgPrivacyParameters: Son los parámetros definidos por el protocolo de privacidad.

Según Moreno & Serna, (2013); en el último campo estarán aquellos que conforman un ScopedPDU, es decir puede lograr estar en texto plano o puede estar encriptado y es examinado con un subsistema de procesamiento de mensaje y pueden ser:

- contextEngineID: Permite la identificación de cualquier entidad de SNMP
- contextName: Permite Identificar el contexto que este contenido en un motor de SNMP.
- PDU: Este campo contendrá los datos de las operaciones de SNMP.

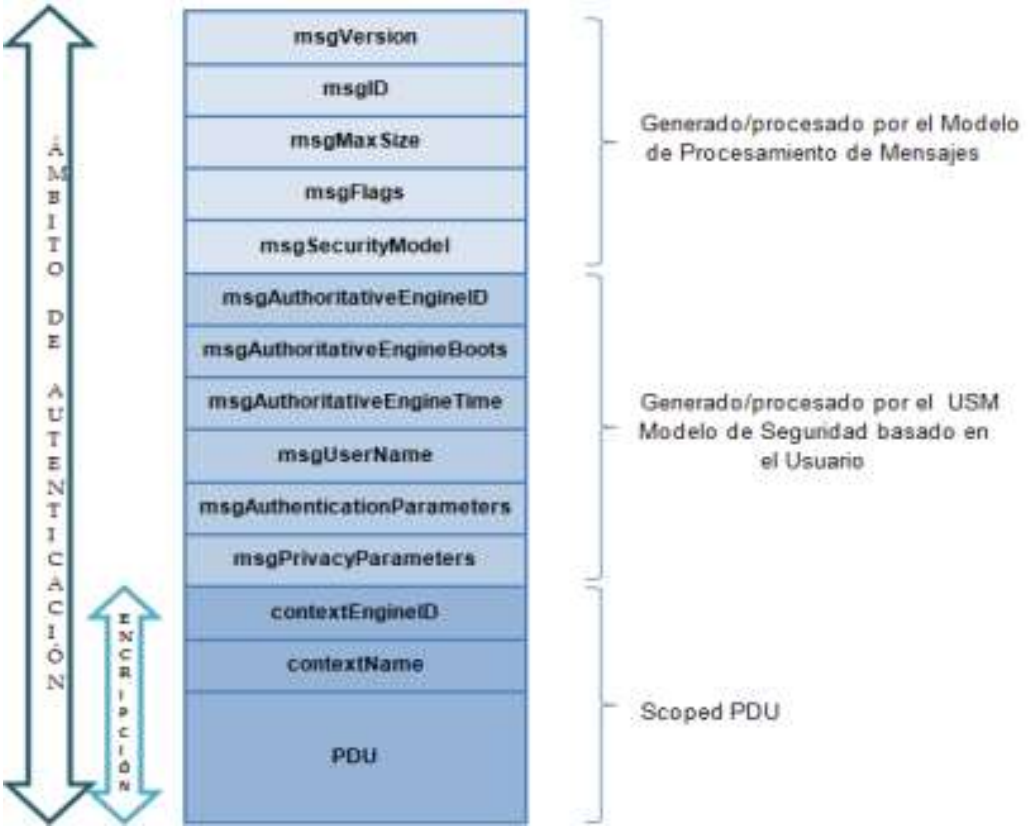

Figura 2.18 Formato del mensaje SNMPv3
Fuente: (Moreno & Serna, 2013)

2.5 VENTAJAS Y DESVENTAJAS DEL PROTOCOL SNMP

2.5.1 Ventajas del protocolo SNMP

- La ventaja principal de SNMP es que el diseño es demasiado simple lo que hace que su configuración sea sencilla en todas las redes.
- Cuando se vaya a gestionar necesitaremos intercambiar información, por eso se ocupara pocos recursos de cualquier red.
- El usuario podrá elegir las variables que se desea observar con solo definir: los títulos, los tipos de los datos de las variables, también si las variables serán solo de escritura o también de lectura y los valores que son de las variables.
- Permite recopilar información sobre la trap y los tipos de agentes en la estación de la administración de la red; lograra notificar de los eventos específicos que se desarrollaran.
- Se reduce mucho el tráfico mediante el uso del protocolo UDP.

- ❖ Controlará la mayor cantidad de datos que se envíen a la red y también el tiempo de espera para los dispositivos de respuesta.
- ❖ Contiene compatibilidad en las bases de datos de las con las diferentes versiones de SNMP, obteniendo también excepciones.
- ❖ Con la versión 3 se tiene una buena seguridad mediante el uso de algoritmos de cifrado.

2.5.2 Desventajas del protocolo SNMP

- ❖ La desventaja que presenta SNMP es que tiene mucha inseguridad con las dos primeras versiones ya que esto puede permitir el acceso a cualquier persona a las informaciones que son enviadas a la red, creando bloqueos o deshabilitando terminales; pero con la versión 3 se logró mejorar.
- ❖ SNMP no está diseñado para prevenir los siguientes tipos de ataques que se dan:
    - Denegación de servicios (DoS): Es aquel que intercambia los mensajes que se envían entre el agente y la consola de administración.
    - Análisis de tráfico: Cualquier atacante podra observar los patrones de tráfico que hay entre estas entidades.
- ❖ En la recepción no es posible el aviso de un mensaje enviado por el agente. No se puede ver la confirmación durante la transmisión de datos.

CAPÍTULO 3

3 DESCRIPCIÓN E IMPLEMENTACIÓN DEL PROYECTO

3.1 INTRODUCCIÓN

Este capítulo nos servirá para ver la descripción de los equipos que usaremos tanto routers como ordenadores, equipos conectados para el proyecto de la red que se ha descrito anteriormente; así mismo también conoceremos los programas que necesitaremos para la respectiva implementación, descripción de cada programa con sus respectivas instalaciones; también estará la programación de cada equipo y de cada programa todo tiene que estar relacionado con el protocolo SNMP.

3.2 SISTEMAS OPERATIVOS

Un sistema operativo es un programa que gestiona el hardware de la computadora. También proporciona una base para los programas de aplicación y actúa como intermediario entre el usuario de la computadora y el hardware del equipo. Un aspecto sorprendente de los sistemas operativos es la variedad que está en el cumplimiento de estas tareas. Sistemas operativos de mainframe están diseñados principalmente para optimizar la utilización de hardware. Sistemas operativos personales ordenador soportan juegos complejos, aplicaciones empresariales, y todo lo demás. Los sistemas operativos para ordenadores portátiles están diseñados para proporcionar un ambiente en el cual un usuario puede interactuar fácilmente con la computadora para ejecutar programas. Por lo tanto, algunos sistemas operativos están diseñados para ser conveniente, otros a ser eficiente, y otros para alguna combinación de los dos (Silberschatz, Baer, & Gagne, 2009).

3.2.1 Windows 8

Windows 8 cambia definitivamente su experiencia de Windows. Todavía viene con el escritorio tradicional de Windows, pero la nueva pantalla de inicio está creando toda la emoción. La Imagen inicial azulejos grandes, coloridas ofrecen peldaños rápidos para revisar el correo electrónico, ver vídeos, y el muestreo de tarifas de Internet. Lo nuevo de Windows 8 a diferencia de otras versiones es que lo aprendido en las anteriores versiones no nos servirá de mucho ya que el sistema operativo ha cambiado y mucho. Windows 8 comienza esencialmente a partir de cero, en un intento de

complacer a las dos formas de mercado de los propietarios de ordenadores. Algunas personas son en su mayoría consumidores. Ellos leen el correo electrónico, ver vídeos, escuchar música y navegar por la web, a menudo, mientras está lejos de su PC. Ya sea en el camino o en el sofá, están los medios de comunicación que consume. Otras personas son en su mayoría creadores. Ellos escriben papeles, preparan declaraciones de impuestos, actualizan blogs, editan videos, o, muy a menudo, lo que toque sus jefes les pidan. Las versiones anteriores de Windows permiten sesión tan pronto como se enciende el ordenador. Para la nueva versión de Windows 8, hace que se desbloquee una pantalla antes de pasar a la página de registro o al escritorio, donde primero se escribe su nombre y contraseña (Rathbone, 2013). En el siguiente enlace: http://windows.microsoft.com/es-ES/windows/downloads podemos descargar el sistema operativo Windows 8 e instalarlo ya que es muy fácil.

3.2.2 Windows 10

El lanzamiento de Windows 10 abarca una gama mucho más amplia de dispositivos, aunque todos estos dispositivos comparten una gran cantidad de código común. Es más fácil de manejar y muy segura. Un nuevo enfoque de las actualizaciones y mejoras Como ya he mencionado, el cambio más revolucionario en Windows 10 es el concepto de mejora continua. Las nuevas características se entregan a través de Windows Update. En un cambio importante de las mejores prácticas de larga data, Microsoft ahora recomienda que los clientes empresariales permiten de Windows Update para la mayoría de los usuarios, aunque la opción de utilizar Windows Server Update Services (WSUS) todavía puede estar disponible en algunas configuraciones. Para poder descargar este sistema operativo se tiene que reservar desde la página oficial de Windows con el correo del usuario (Bott, 2015).

Figura 3.1 Pantalla inicial de Windows
Elaborado por: Autor

3.3 ROUTER

Un router es un dispositivo que puede conectar y permitir la comunicación entre dos redes, es aquel que permite determinar el mejor camino a través de la red para que los datos lleguen sin problemas a su destino. Los archivos de configuración para controlar el tráfico generalmente tienen dos tipos de conexión: WAN (conexión al ISP) y LAN. Los datos se envían en forma de paquetes entre dos dispositivos finales, los routers se utilizan para dirigir los paquetes a su destino, al enviar estos paquetes lo primero es examinar la dirección IP y determinar el mejor camino mediante el uso de una tabla de enrutamiento (Bornhager, 2002).

3.3.1 Descripción router Linksys E900

El router Linksys e900 wireless propiedad de Cisco es aquel que fue construido con tecnología líder 802.11n, la de crear una red doméstica inalámbrica de gran alcance en cuestión de minutos. Conecta sus computadoras, televisores listos para Internet, consolas de videojuegos, teléfonos inteligentes y otros dispositivos Wi-Fi en las velocidades de transferencia rápidas para una experiencia sin igual (Cisco, 2012).

Figura 3.2 Router Linksys E900
Fuente: (Cisco, 2012)

Según Cisco, (2012); los componentes que están ubicados en la parte trasera:

- **Ethernet puertos.-** conectar los cables Ethernet (también llamados cables de red) a estos Fast Ethernet (10/100) puertos, un código de color azul, y para los dispositivos de red Ethernet con cable de la red.
- **Puerto de internet.-** conectar un cable Ethernet (también llamado cable de red o de Internet) a este puerto, un código de color amarillo, y al módem.
- **Wi-Fi Protected Setup™ botón.-** Pulse este botón para configurar fácilmente la seguridad inalámbrica en los dispositivos de red de configuración habilitado Wi-Fi Protegidas.
- **Indicador de potencia.-** Estancias en forma constante mientras que el poder está conectado y siguiendo una exitosa conexión Wi-Fi Protected Setup. Parpadea lentamente durante el arranque, durante las actualizaciones de firmware, y durante una conexión de Wi-fi Protected Setup, parpadeara rápidamente cuando hay un error de configuración Wi-fi Protected Setup.
- **Actividad Verde indicator.-** En puertos Ethernet, permanece encendida cuando un cable se conecta al puerto a otro puerto Ethernet. En el puerto de Internet, se queda encendida mientras está conectado a un módem. En ambos tipos de puertos, parpadea durante la transferencia de datos.
- **Reset button.-** Mantenga pulsado este botón durante 5 a 10 segundos (hasta que las luces del puerto parpadean al mismo tiempo) para reiniciar el router a sus valores de fábrica.

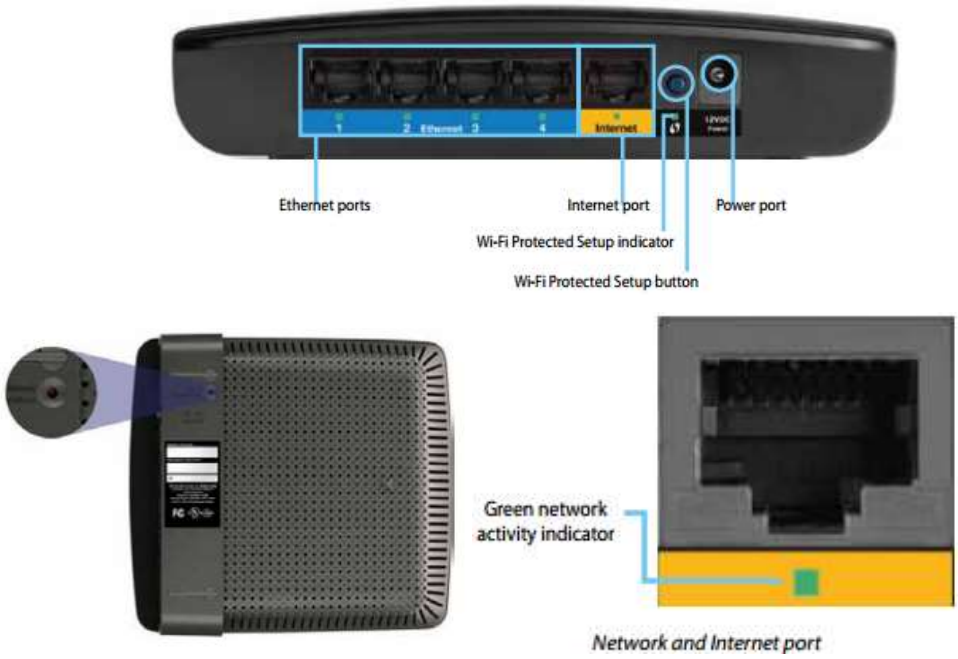

Figura 3.3 Descripción router Linksys
Fuente: (Cisco, 2012)

3.4 PROGRAMA NET-SNMP

Net-SNMP proporciona herramientas y bibliotecas relacionadas con el protocolo simple de administración de red, incluyendo: Un agente extensible, una biblioteca SNMP, herramientas a petición o establecer información de los agentes SNMP, herramientas para generar y manejar trampas SNMP, etc. Net-SNMP es un marco de código abierto: los cambios inesperados son posibles. Preste atención a las versiones compatibles de su plataforma Windows. Al querer instalar este programa para el sistema operativo Windows 8 se presentaran muchos problemas ya que no es fácil su instalación y para su funcionamiento necesitara otros métodos; pero con las respectivas búsquedas, análisis y experiencia en base a este proyecto daremos unas formas para el buen uso y una buena instalación, lo bueno de este programa es que trabaja con las tres versiones del protocolo SNMP y es muy fácil usar, este programa se instalara en los dos ordenadores para su respectivo análisis.

3.5 PROGRAMA WIRESHARK

Este programa nos ayuda mucho en lo que es el análisis de los paquetes transmitidos y recibidos. Este analizador de paquetes de red logra la captura de los paquetes y

lograra mostrar que los paquetes de datos estén muy detallados. Se podría decir que un analizador de paquetes examina lo que está pasando dentro de un cable de red, o dentro de los dispositivos o equipos; al igual que un voltímetro es manejado por un electricista para chequear lo que está pasando dentro de un cable eléctrico o cualquier equipo conectado, cabe decir que con un nivel más alto (Lamping, Sharpe, & Warnicke, 2014).

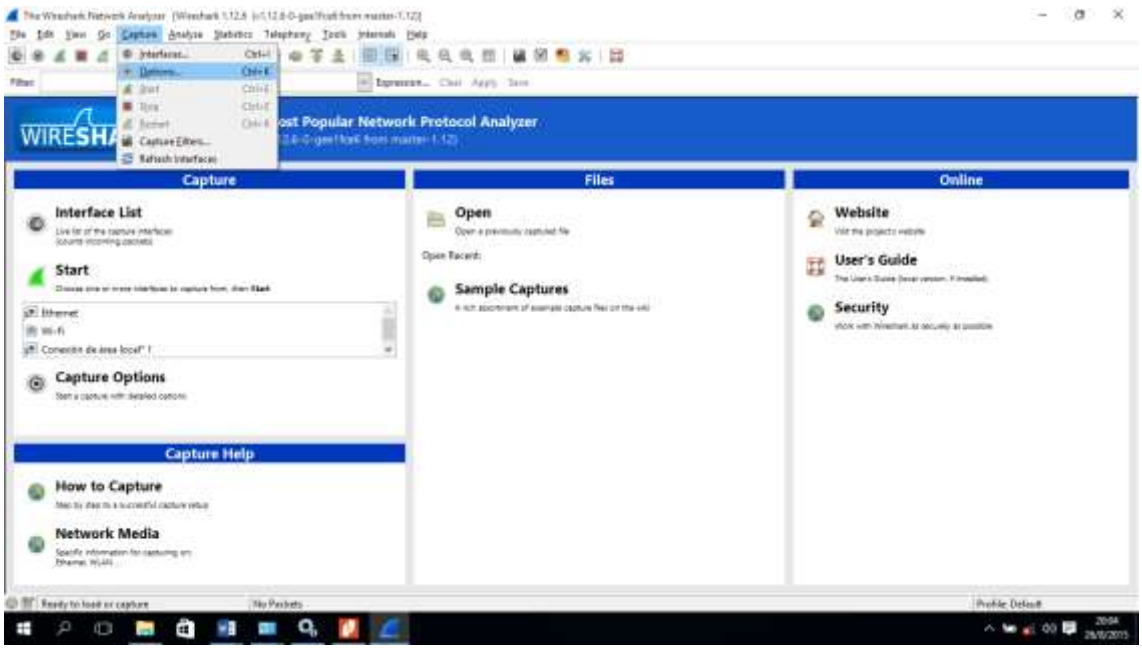

Figura 3.4 Programa WireShark
Elaborado por: Autor

3.6 INSTALACIÓN Y CONFIGURACIÓN

3.6.1 Instalación y configuración de NET-SNMP

Para poder descargar este programa nos dirigimos a la página oficial http://www.net-snmp.org/ después de descargarlo e instalarlo no bastara ya que cuando queremos entrar al modo de configuración en el CMD nos pedirá un programa más cómo podemos ver en la figura 3.5.

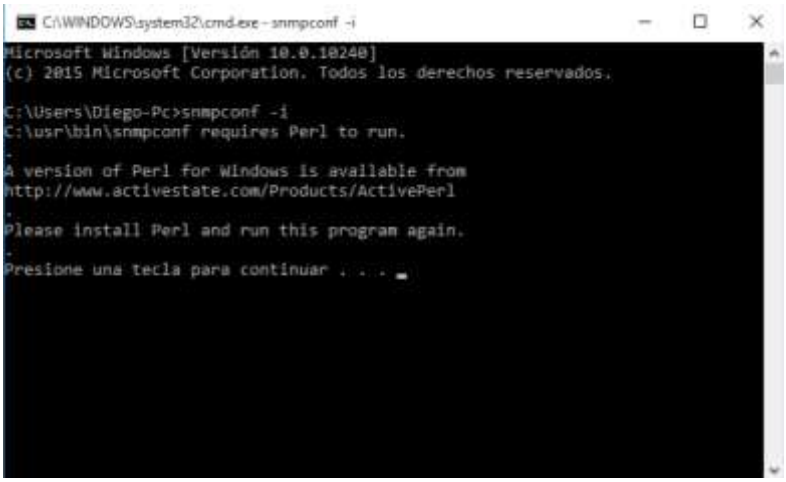

Figura 3.5 Problema en la configuración en Net-SNMP
Elaborado por: Autor

Después de descargar "Active Perl" en la página que nos indicaba, lo instalamos y una vez instalado ya podemos entrar al modo de configuración en CMD para el protocolo SNMP y sus versiones.

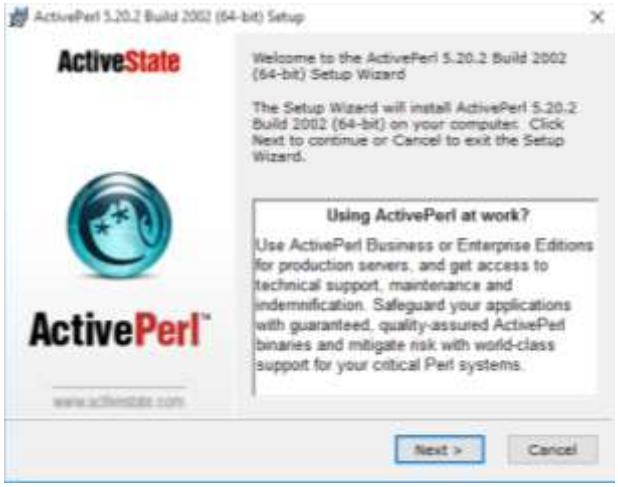

Figura 3.6 Instalación del programa ActivePerl
Elaborado por: Autor

3.6.2 Instalación y configuración de WireShark

Después de descargar este programa lo instalaremos dependiendo de la capacidad de nuestro ordenador ya sea de 32 bits o de 64 bits, en este caso será de 64 bits, lo instalamos y lo configuramos para que pueda analizar lo equipos que deseamos como veremos en la figura 3.7.

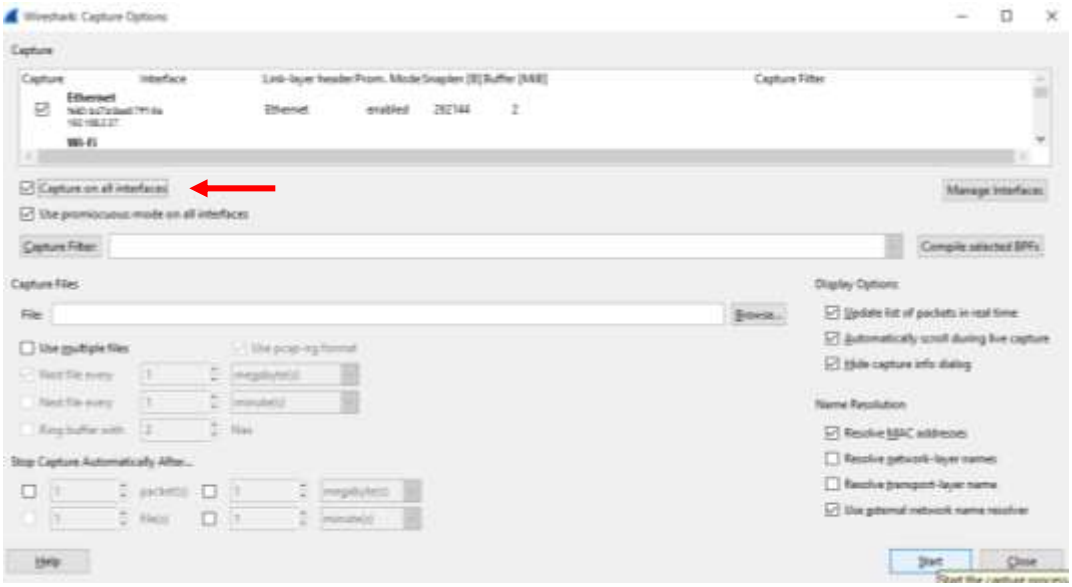

Figura 3.7 Configuración de WireShark
Elaborado por: Autor

3.6.3 Configuración de los routers Cisco

Como mencionamos anteriormente lo primero que debemos hacer es configurar los routers cisco, para que se pueda tener el enlace que queremos para la respectiva simulación y para obtener los respectivos informes. Se desactivan todas las redes conectadas a nuestro equipo, conectamos el router, para poder saber la dirección del router conectado abrimos el CMD programa que trabaja en lenguaje C (lo buscamos a través de las teclas Windows + R) y colocamos el comando "ipconfig" esto nos dará la dirección de los equipos conectados; después de saber nuestra dirección abrimos nuestro navegador favorito y en la barra de búsqueda colocamos la dirección IP en este caso 192.168.1.1 para el Router1 y 192.168.2.1 para el Router2; después saldrá una barra pidiendo usuario y clave para ingresar al router por lo general estos equipos cisco Linkysis son usados por la empresa NETLIFE así que para poder acceder a este router ponemos en usuario: **netlife** y la contraseña será: **ecua1220-(los últimos 5 dígitos de la serie del router)**; en caso de que no tenga este usuario y clave, por defecto será usuario: **admin** y contraseña: **admin.**

Al ingresar al router tendremos puras pestañas pero solo necesitaremos configurar pocas comenzaremos con la pestaña de "configuración"; ahí tendremos la "configuración básica" donde elegiremos el idioma a nuestra preferencia, después

tenemos la configuración de internet en donde colocaremos las direcciones que deseamos para tener el acceso punto a punto de nuestro enlace (a cada router se le colocan diferentes direcciones) como podemos ver en las figuras 3.8 y 3.9.

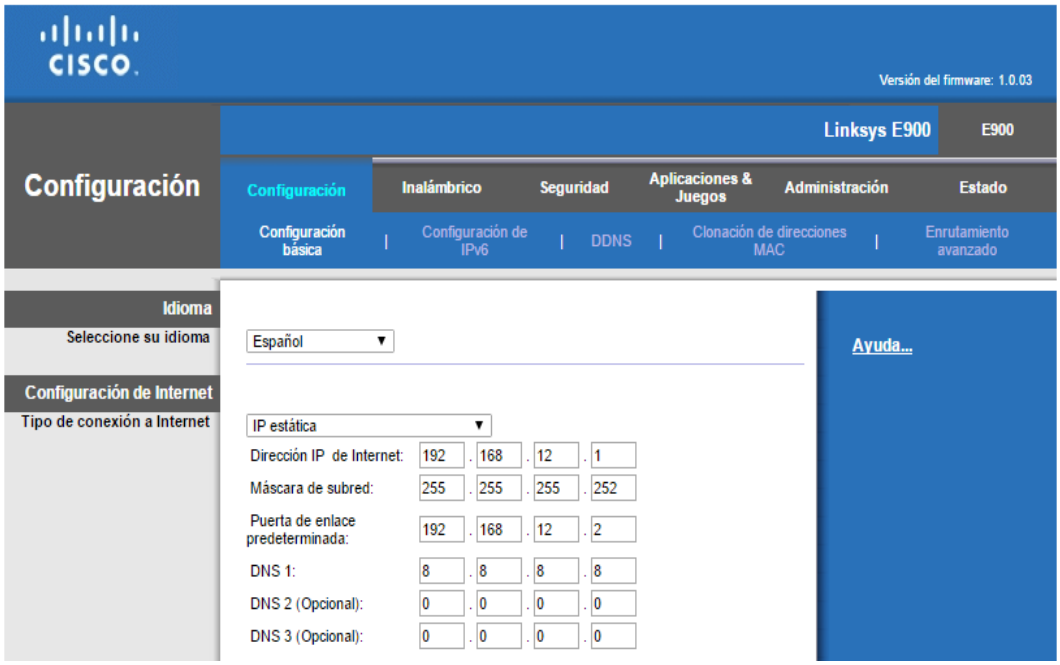

Figura 3.8 Configuración de internet-Router 1
Elaborado por: Autor

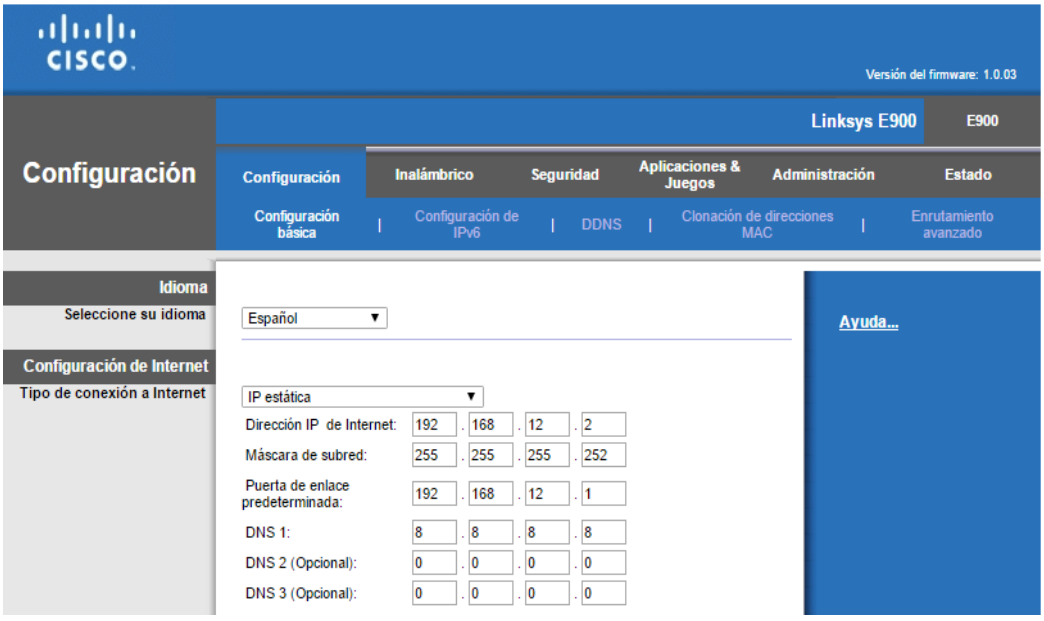

Figura 3.9 Configuración de internet-Router 2
Elaborado por: Autor

En la misma pestaña de configuración pero más abajo tenemos la configuración de red y es ahí en donde podemos configurar la dirección de nuestros routers cualquier dirección que deseamos y también el nombre del routers, después de configurar damos clic en guardar parámetros para no perder las configuraciones como podemos ver en las figuras 3.10 y 3.11.

Figura 3.10 Configuración de red del router 1
Elaborado por: Autor

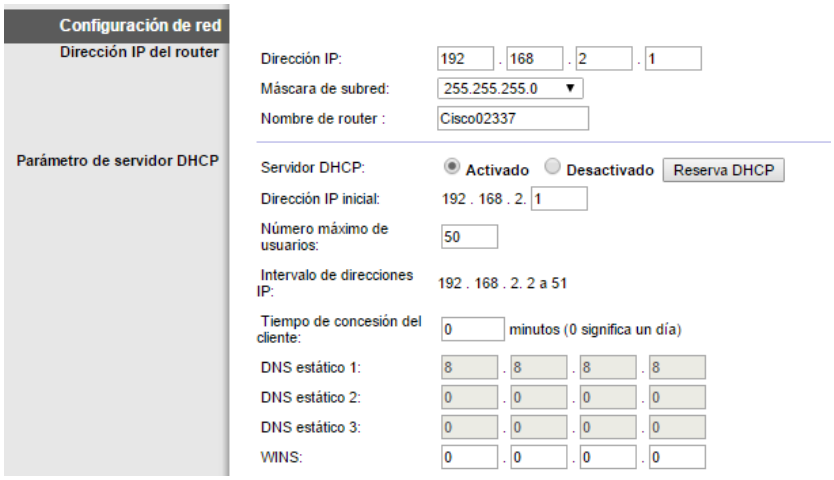

Figura 3.11 Configuración de red del router 2
Elaborado por: Autor

La siguiente pestaña en configurarse es la del “Enrutamiento avanzado” ya que con esta configuración podemos tener acceso de un ordenador a otro ordenador con las mismas direcciones que están configurados los dos routers, podemos verlo en las figuras 3.12 y 3.13; no olvidar guardar las configuraciones.

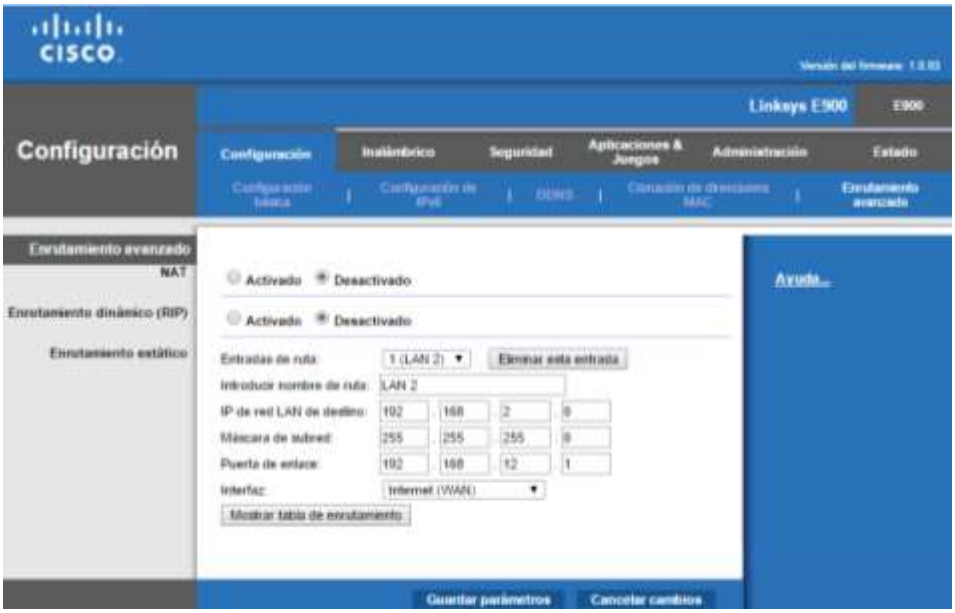

Figura 3.12 Configuración del enrutamiento del router 1
Elaborado por: Autor

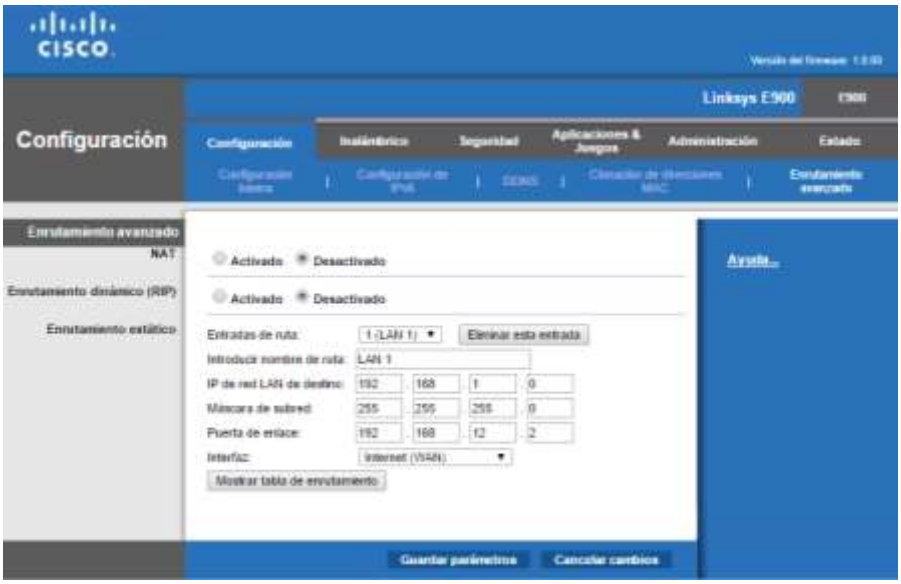

Figura 3.13 Configuración del enrutamiento del router 2
Elaborado por: Autor

Seguimos la configuración con la pestaña de “seguridad”, ya que aquí desactivaremos los firewall a los dos routers, porque no necesitamos establecer una conexión a internet sino una conexión a otro ordenador, lo podemos ver en la figura 3.14, sin olvidar guardar cada configuración que terminemos de desarrollar.

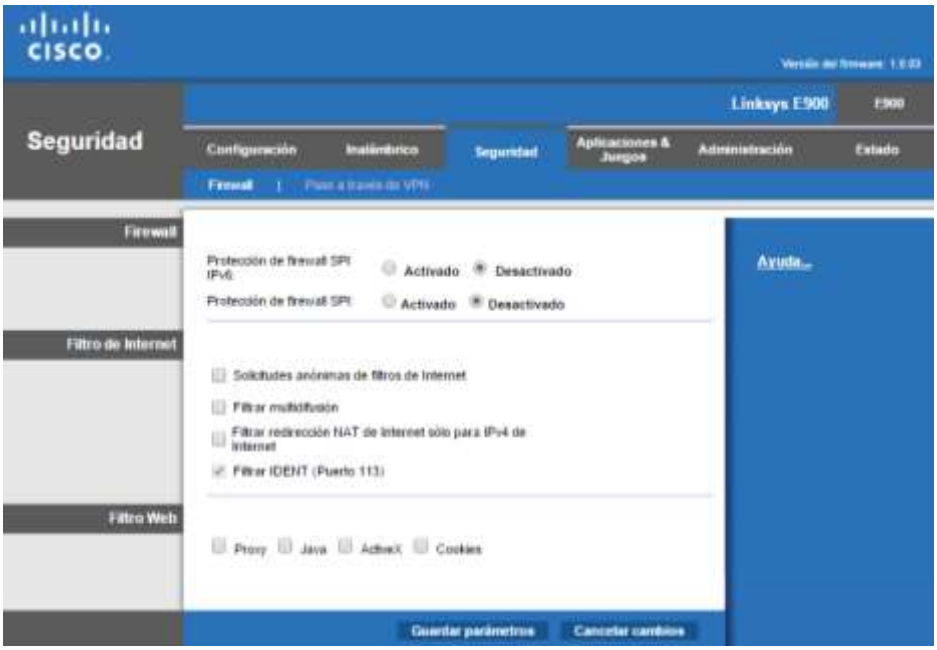

Figura 3.14 Desactivación del Firewall
Elaborado por: Autor

Para la última configuración de los routers, nos ubicaremos en la pestaña “Aplicaciones & juegos” en esta pestaña podemos configurar la salida de los puertos, como estamos investigando sobre el protocolo SNMP, elegiremos que los puertos a usarse trabajen solo con este protocolo, colocaremos la dirección que obtenemos con el comando “ipconfig” explicado anteriormente; no olvidar activarlo para que funcione correctamente esto se lo desarrollara en los dos routers como podemos ver en la figura 3.15 y se guardan los cambios que realizamos.

Figura 3.15 Configuración de los puertos
Elaborado por: Autor

3.6.4 Configuración de los ordenadores

Para que se establezca la comunicación entre los dos ordenadores con los dos routers conectados, se configura cada ordenador para que las direcciones de los routers se conecten sin ningún problema y se lo realiza así: Panel de control → Centro de redes y recursos → Seleccionamos donde dice Ethernet → Propiedades → Protocolo de internet versión 4 → y elegimos obtener la dirección IP y la dirección del servidor DNS automáticamente (ver figura 3.16).

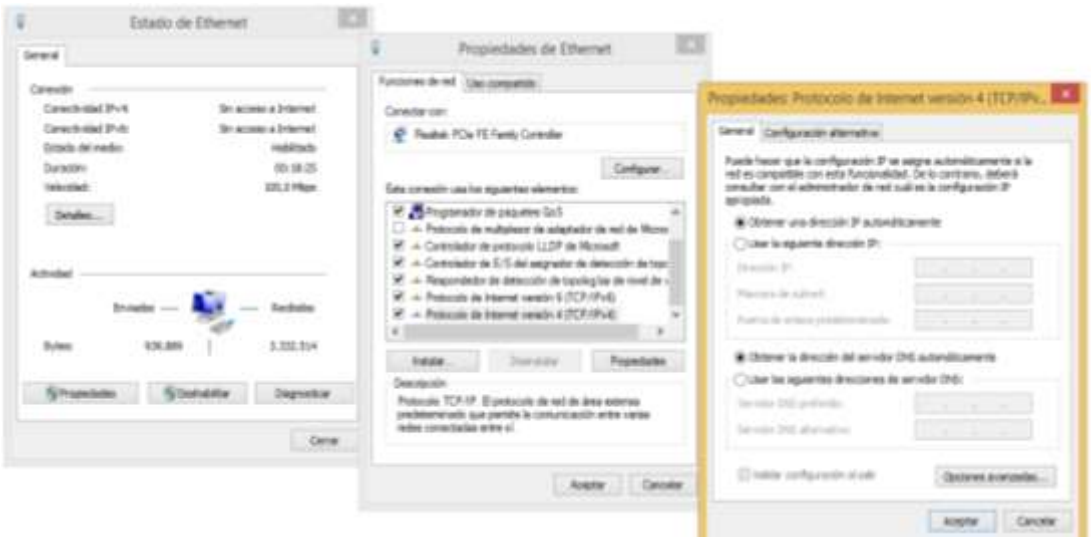

Figura 3.16 Configuración de las direcciones a los ordenadores
Elaborado por: Autor

3.6.5 Configuración de SNMP para Windows

En los ordenadores con el sistema operativo Windows para que el protocolo SNMP funcione lo primero que tenemos que realizar es instalar sus características, esto solo se lo realiza de esta forma: Panel de control → Programas y características → Activar o desactivar características de Windows; aquí seleccionaremos la casilla "Protocolo Simple De Administración De Redes (SNMP) y le damos aceptar,

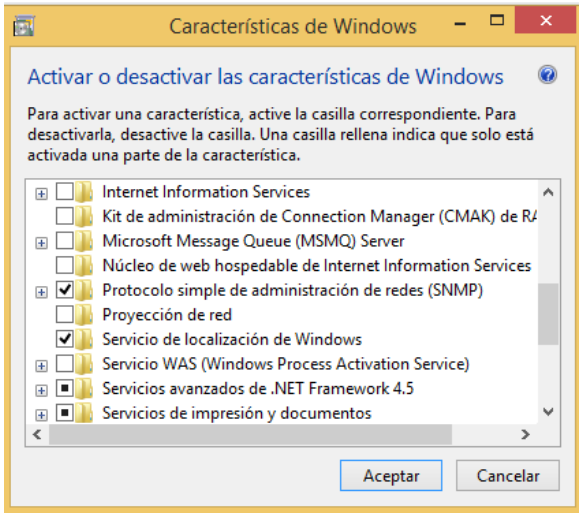

Figura 3.17 Características Windows
Elaborado por: Autor

Después de haber instalado las características SNMP, tenemos que configurar los servicios para las versiones a utilizarse, para realizarlo tenemos que dirigirnos así: Panel de control → Herramientas administrativas → Servicios → Servicio SNMP; en esta ventana tendremos muchas pestañas, nos colocamos a la pestaña "Agente" y aquí colocaremos cualquier nombre y cualquier lugar y activamos todas las casillas de servicio y le damos aceptar.

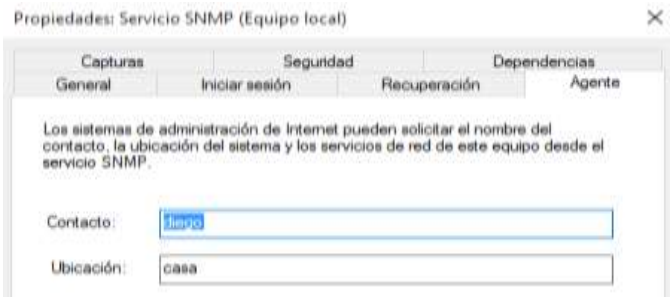

Figura 3.18 Configuración de Agente
Elaborado por: Autor

Después nos ubicaremos en la pestaña “Capturas”; aquí colocaremos el nombre a nuestra comunidad y también la dirección que vamos a gestionar o la dirección de destino; puede ser cualquiera que deseamos.

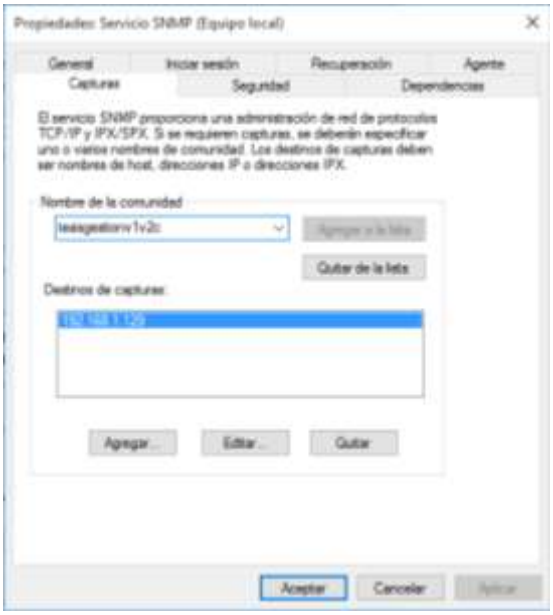

Figura 3.19 Configuración de Capturas
Elaborado por: Autor

Seguimos con la pestaña “Seguridad” aquí podemos seleccionar el nombre de la comunidad ingresada y podemos elegir si puede ser solo lectura, lectura y escritura o lectura y creación; dependiendo de lo que vayamos a realizar y más abajo podemos colocar la aceptación de los paquetes aquí se puede elegir si aceptamos cualquier paquete de cualquier host o solo paquetes de hosts elegidos.

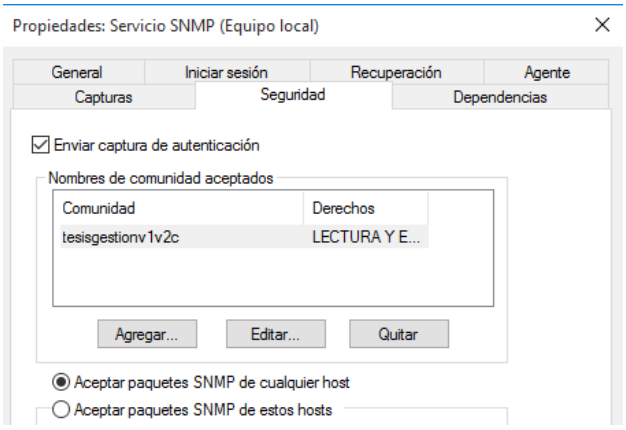

Figura 3.20 Configuración de seguridad
Elaborado por: Autor

Y la última pestaña será la “General” aquí una vez realizado los cambios que deseábamos le damos clic al botón iniciar y los servicios SNMP configurados ya están listos para usarse.

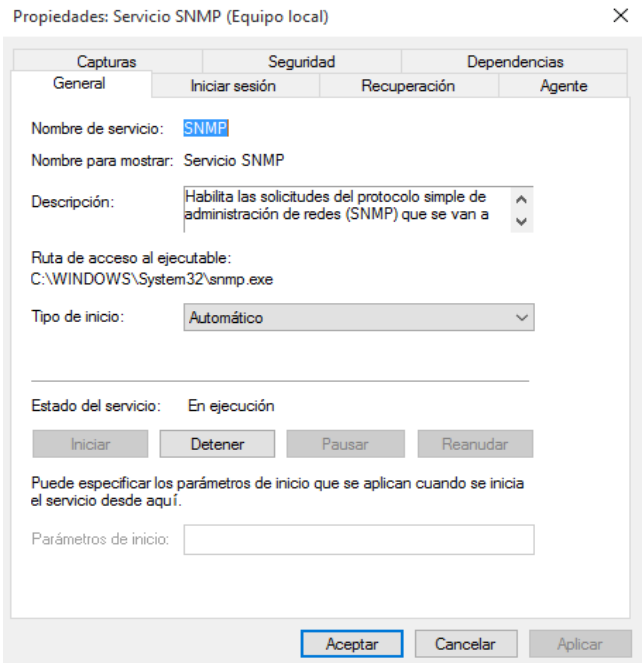

Figura 3.21 Activación de las configuraciones
Elaborado por: Autor

Lo mismo vamos a realizar con la configuración de las captura SNMP que se encuentran as arriba de los servicios SNMP, en esta ventana solo damos clic en iniciar ya que solo se activaran las Trap de SNMP.

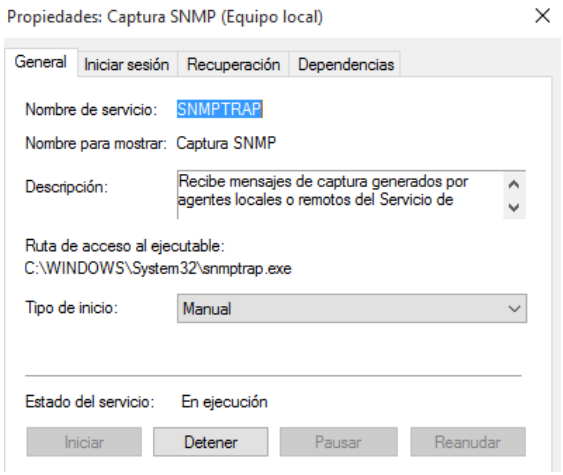

Figura 3.22 Activación de las SNMPTRAP
Elaborado por: Autor

Para activar las configuraciones hechas en CMD escribimos el comando “net start” y eso activara nuestras configuraciones, para poder ver los puertos activados de SNMP en CMD lo podemos hacer con el comando “netstat –ano” y veremos los puertos 161 y 162 que están activados en la figura 3.23.

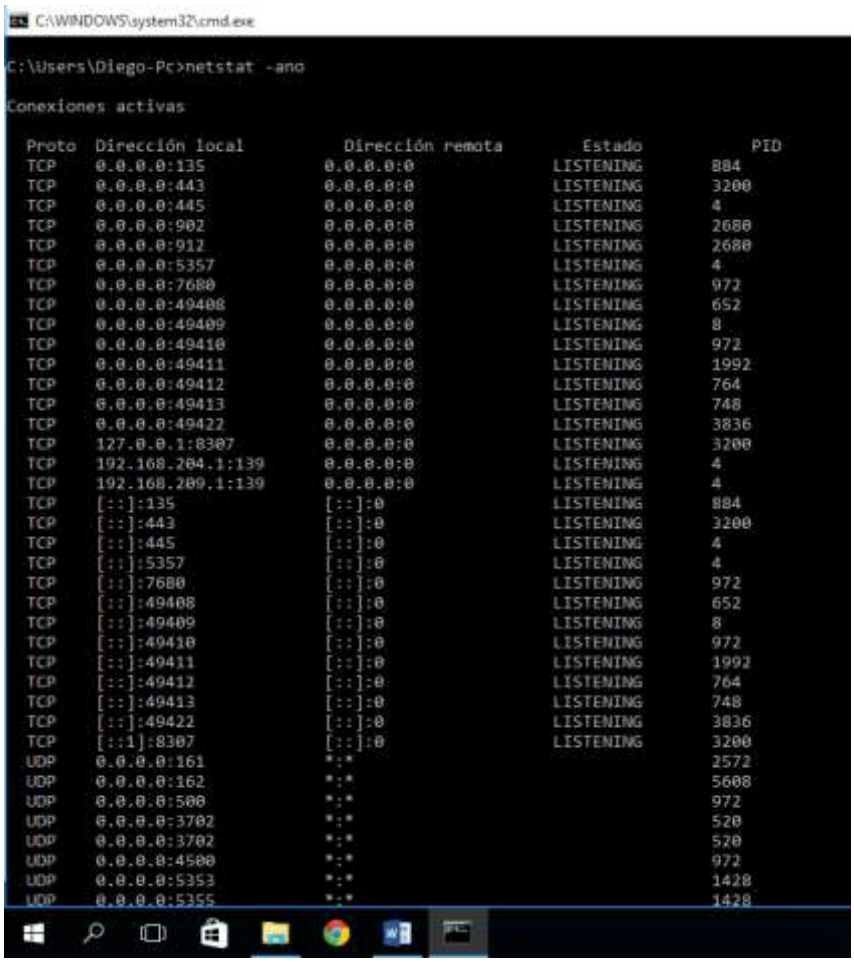

Figura 3.23 Puertos 161 y 162 activados
Elaborado por: Autor

Para que los ordenadores tengan acceso entre ellos y entre los routers se tienen que desactivar los firewall de Windows ya que esto nos impide la transmisión y recepción de datos entre ellos, para acceder a la ventana firewall lo hacemos así: Panel de control → Firewall de Windows → Activar o desactivar firewall de Windows; aquí elegimos las casillas de desactivación de red privada y de red pública y le damos aceptar para que se guarden las configuraciones.

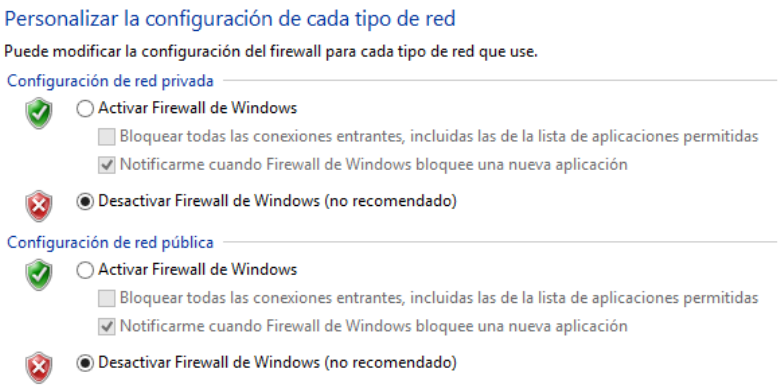

Figura 3.24 Configuración del Firewall de Windows
Elaborado por: Autor

3.7 PRUEBA DE COMUNICACIÓN ENTRE LOS EQUIPOS

Después de realizar todos estas configuraciones y tener conectado todos los equipos; para saber que hay una comunicación entre los equipos se lo realiza con el comando "PING", se abre el programa CMD y se escribe ping 192.168.2. *** (La dirección del otro equipo o de los routers) cómo podemos ver en la figura 3.25; es así que vemos que está bien establecida la conexión entre los equipos.

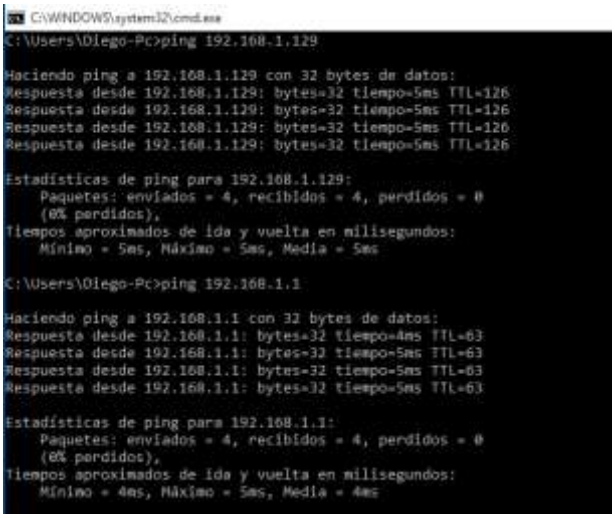

Figura 3.25 Prueba del ping para la conexión de los equipos
Elaborado por: Autor

CAPÍTULO 4

4 SIMULACIONES Y PRUEBAS

4.1 ESTUDIO DE LOS DIFERENTES ESCENARIOS

La finalidad de este capítulo es mostrar las simulaciones con sus respectivas pruebas que se desarrollaron para el estudio de este proyecto y con la ayuda de todos los equipos y programas que se mencionaron anteriormente en el capítulo 3 y con sus respectivas configuraciones establecidas de forma correcta. Siguiendo con este capítulo, ahora mencionaremos los escenarios a utilizarse todos ellos están conectados en la misma red que se lo menciono anteriormente pero mostrando en cada una las diferentes versiones estudiadas.

- Escenario 1: Versión 1 del protocolo SNMP (SNMPv1), equipos conectados a una red con sus respectivas simulaciones e informes.

  Con los equipos conectados y configurados correctamente, este escenario solo trabajara con la versión 1 del protocolo SNMP y para tener una buena presentación se manejaran con sub-escenarios que están conformados a continuación:

  - Sub-escenario 1: Se mostraran el uso de las operaciones que están conformadas en la versión 1 del protocolo SNMP que son: GetRequest y GetResponse.
  - Sub-escenario 2: Se manejaran el uso de una Trap que será enviada desde la maquina gestora para saber su función.

- Escenario 2: Versión 2 del protocolo SNMP (SNMPv2c), equipos conectados a una red con sus respectivas simulaciones e informes.
  Comparado con el escenario 1 no tendrá mucha diferencia, solo que se generara un sub-escenario más ya que las operaciones en este protocolo aumentan.

  - Sub-escenario 1: Se mostraran el uso de las operaciones que están conformadas en la versión 2 del protocolo SNMP que son: GetRequest y GetResponse y se compararan con la versión 1.

- ❖ Sub-escenario 2: Este escenario es importante ya que en el podemos ver porque se mejoraron las versiones, ya que se manejara el GetBulk y con esta operación veremos cómo funciona las nuevas opciones.
- ❖ Sub-escenario 3: Se desarrollara las mismas pruebas de Trap que en el escenario anterior, solo que con esta operación haremos la comparación con la versión 1.

- ➢ Escenario 3: Versión 3 del protocolo SNMP (SNMPv3), equipos conectados a una red con sus respectivas simulaciones e informes.

  Para finalizar con el estudio de los diferentes escenarios tendremos la de la versión 3 que se encontrara dividida en solo 2 sub-escenarios.

  - ❖ Sub-escenario 1: Se desarrollara la simulación de las operaciones correspondientes a la versión 3 desde la maquina gestora.
  - ❖ Sub-escenario 2: con las nuevas características que integran a la versión 3 en lo que es seguridad y con los tres niveles, se desarrollaran las respectivas pruebas para saber cuáles son los resultados de cada una y como se defiende ante cualquier intento de contraseñas mal escritas.

4.2 ESCENARIO 1: VERSIÓN DEL PROTOCOLO SNMP (SNMPv1), EQUIPOS CONECTADOS A UNA RED CON SUS RESPECTIVAS SIMULACIONES E INFORMES

4.2.1 Sub-escenario 1

Con las instalaciones y configuraciones que se desarrollaron en el capítulo anterior, desde la máquina gestora iniciamos el CMD para ejecutar los comandos que se necesitaran para esta versión, lo primero a realizar es la creación de la comunidad ya que en la versión 1 y 2 se manejan por comunidades, para crear esta comunidad podemos ver en las figuras (4.1, 4.2, 4.3, 4.4 y 4.5) y con los comandos requeridos paso a paso.

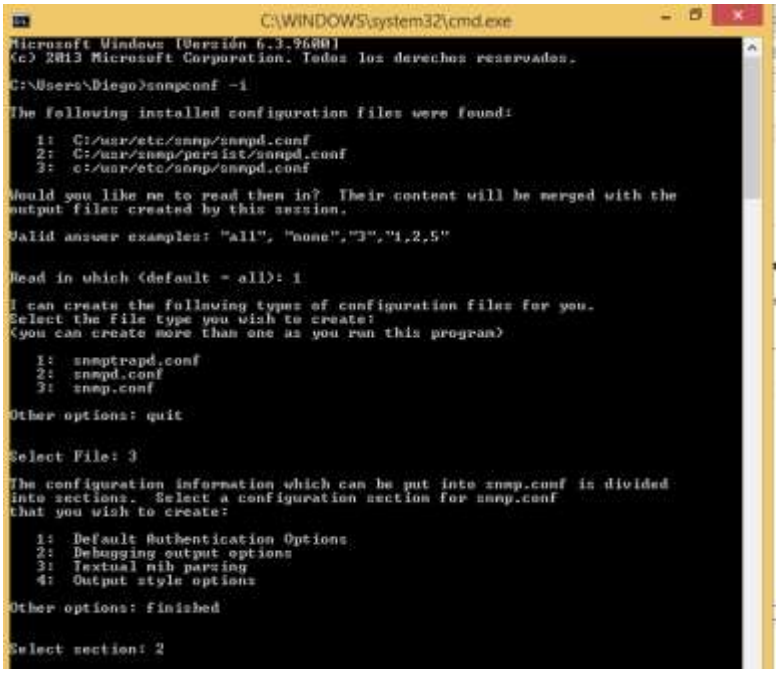

Figura 4.1 Creación de la comunidad-1
Elaborado por: Autor

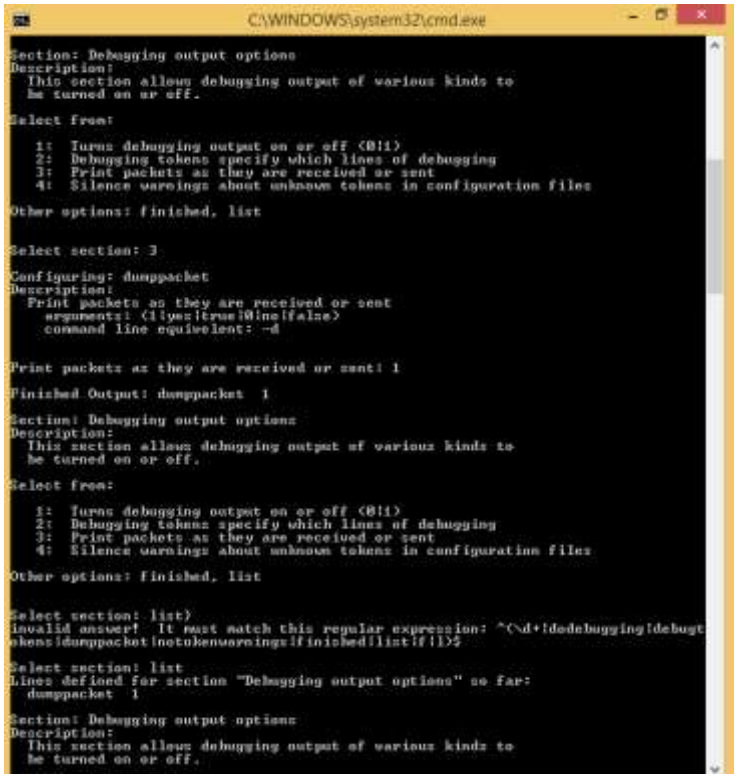

Figura 4.2 Creación de la comunidad-2
Elaborado por: Autor

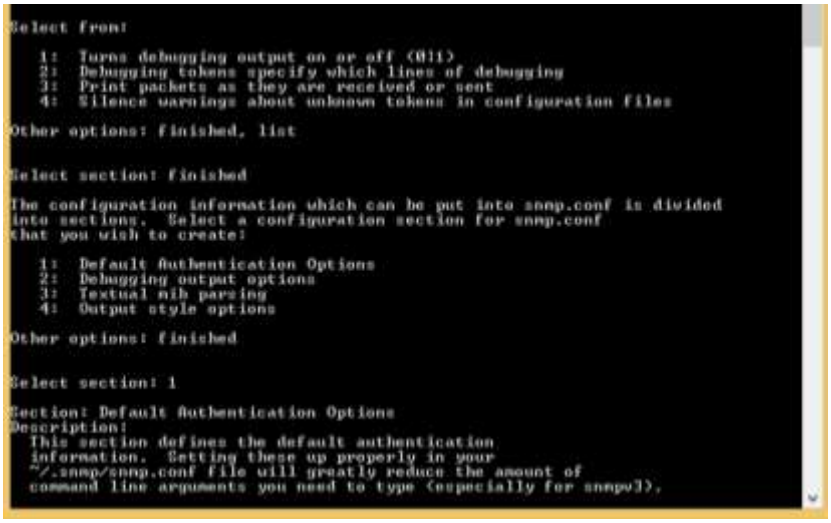

Figura 4.3 Creación de la comunidad-3
Elaborado por: Autor

Figura 4.4: Creación de la comunida-4
Elaborado por: Autor

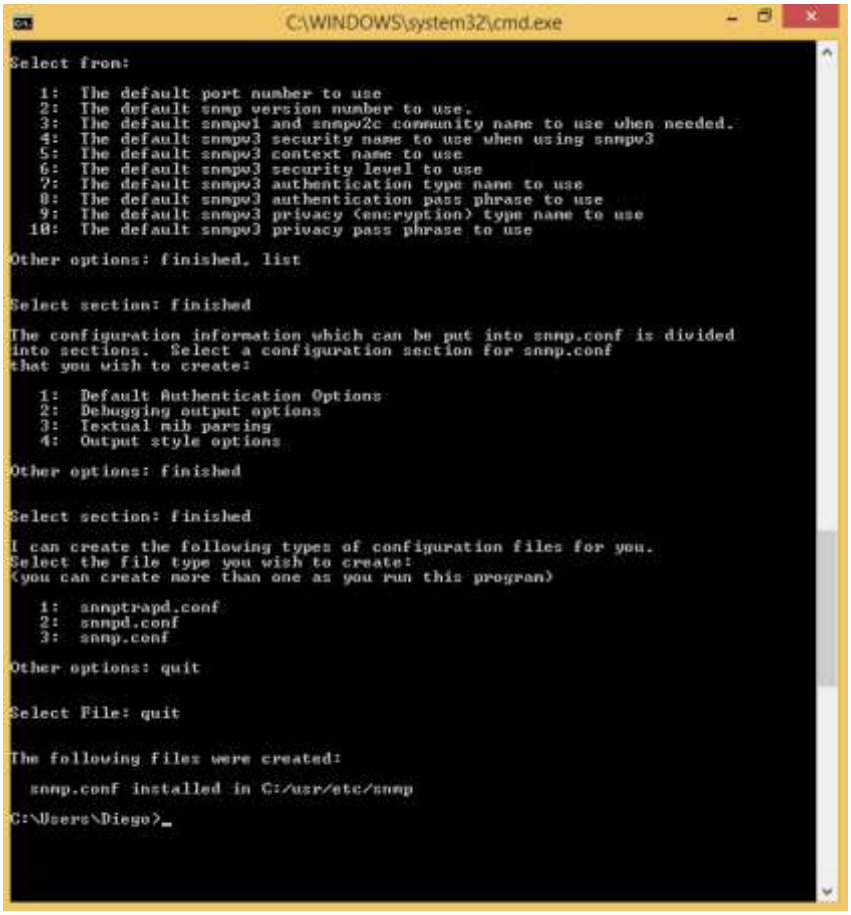

Figura 4.5 Creación de la comunidad-5
Elaborado por: Autor

Después de haber creado nuestra comunidad realizaremos en el mimo CMD la consulta de envió de paquetes desde la maquina gestora a la maquina gestionada para la primera versión, ingresamos los comandos que se necesitaran para ver la función en esta versión, la direcciones que se usaran son visualizadas desde el comando "ipconfig" y después se realizara la respectiva captura de paquetes con el WireShark.

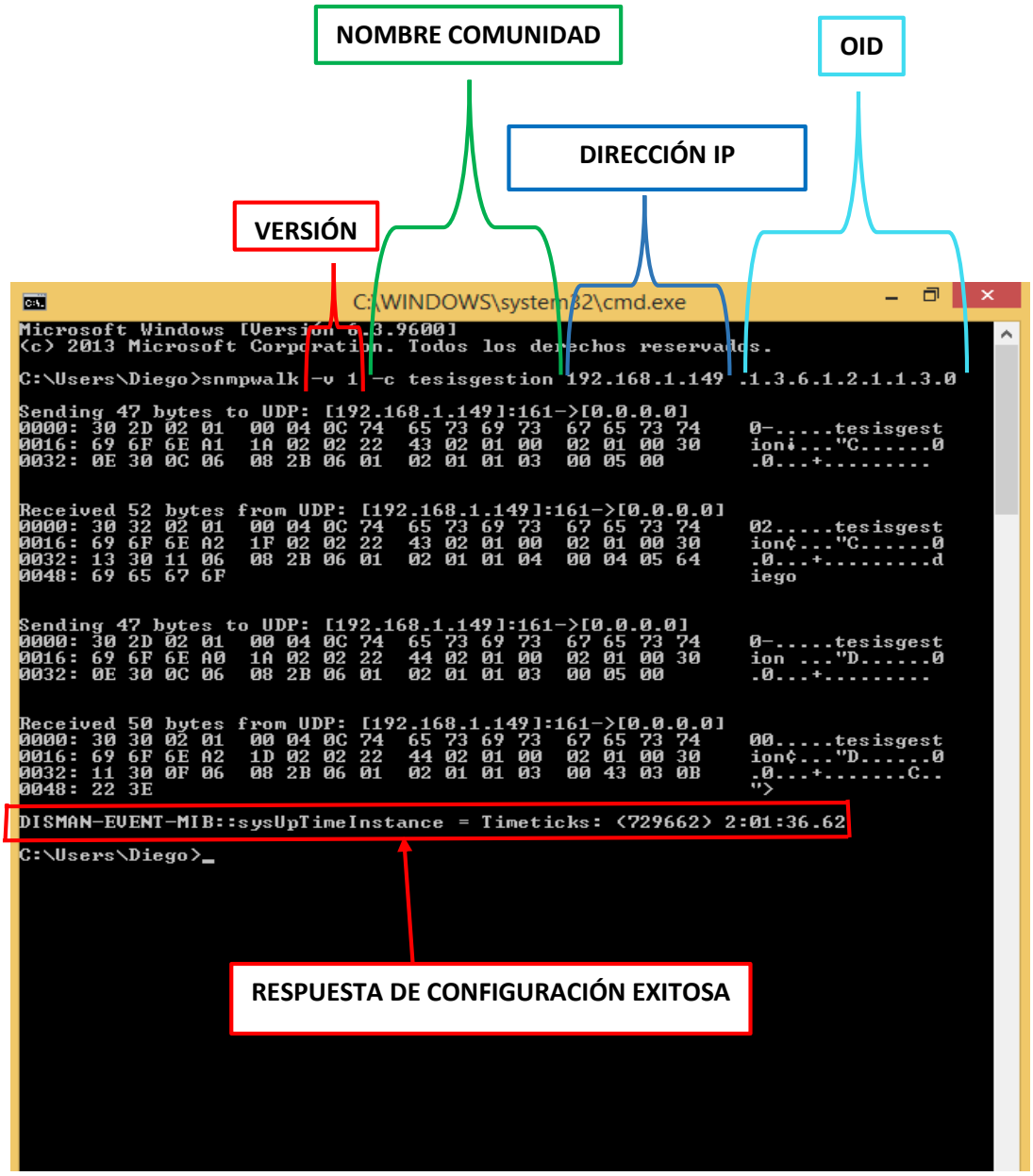

Figura 4.6 Desarrollo de las operaciones de la versión 1 del protocolo SNMP con el comando SNMPWALK.
Elaborado por: Autor

Ahora veremos la captura de paquetes en WireShark, lo que se realizó con el comando snmpWalk en CMD y vemos como tenemos un “GetNextRequest”, un “GetRequest” y un “GetResponse” las dos primeras operaciones son dadas de la maquina gestora y la última operación es la respuesta de la maquina gestionada, lo podremos ver en las figuras 4.7, 4.8 y 4.9.

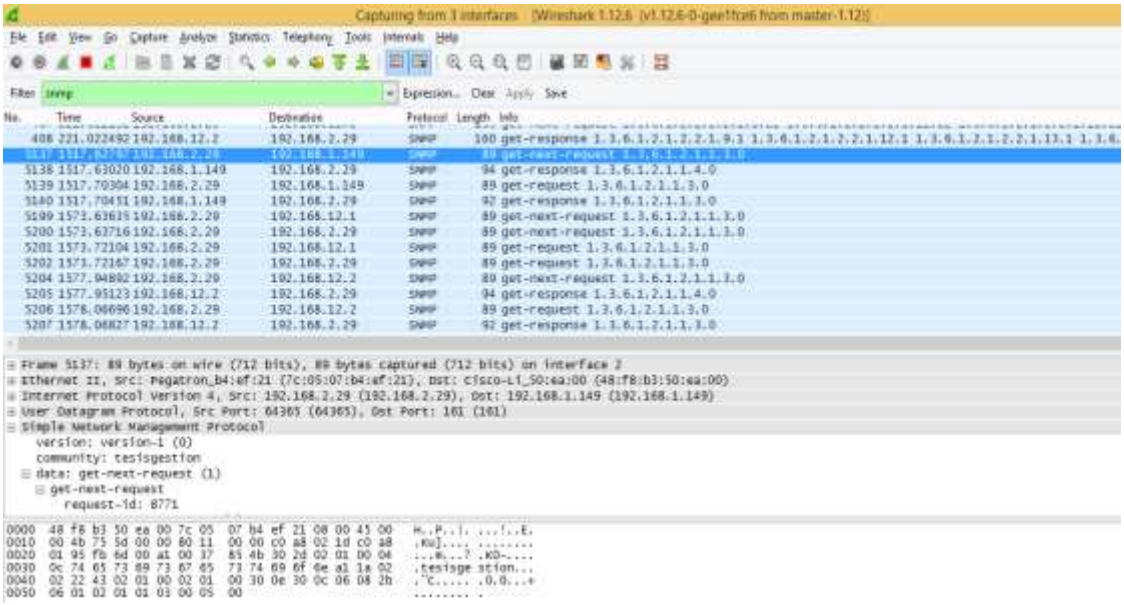

Figura 4.7 GetNextRequest enviado desde la maquina gestora a la máquina gestionada-se puede observar el nombre de la comunidad "tesisgestion".
Elaborado por: Autor

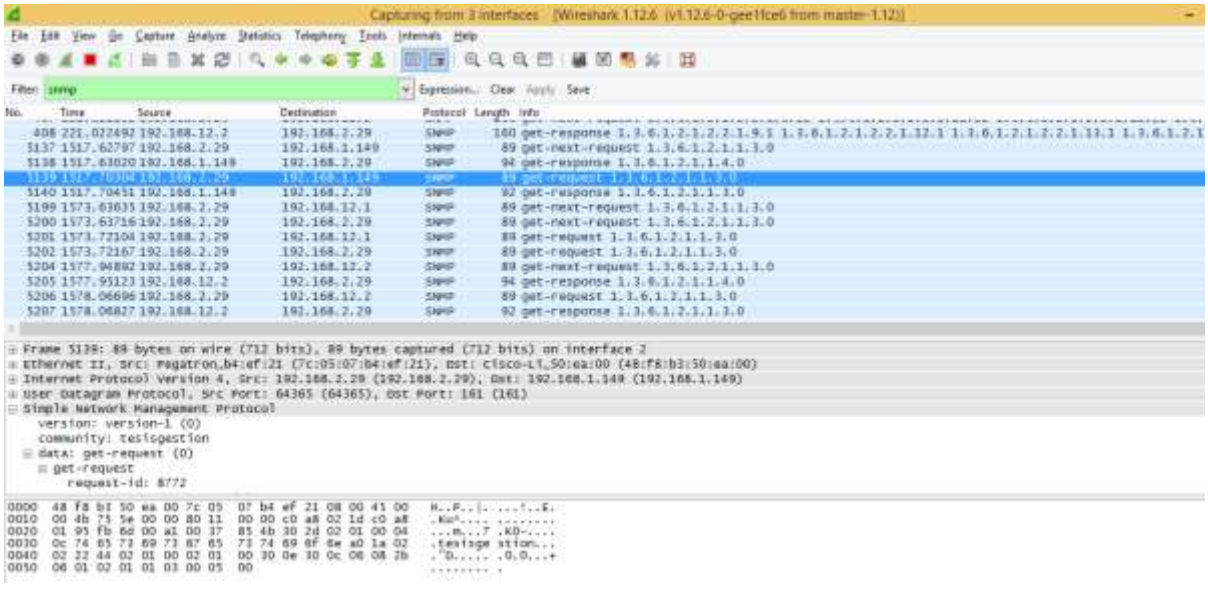

Figura 4.8 GetRequest enviado desde la máquina gestora a la maquina gestionada-se puede observar el nombre de la comunidad "tesisgestion".
Elaborado por: Autor

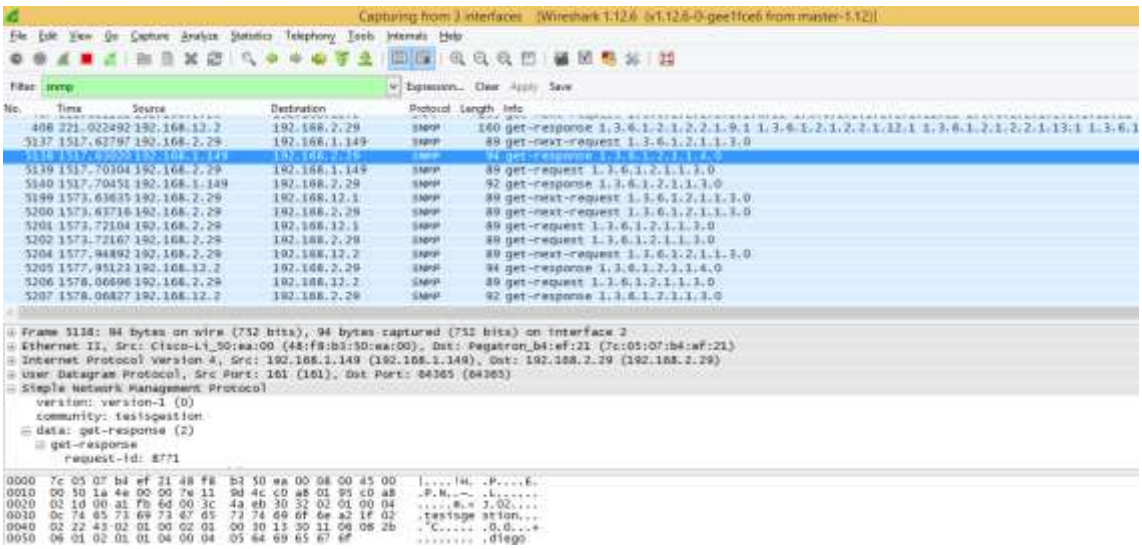

Figura 4.9 GetResponse enviado desde la máquina gestionada a la máquina gestora-se puede observar el nombre de la comunidad y el agente.
Elaborado por: Autor

4.2.2 Sub-escenario 2

Como lo mencionamos anteriormente este sub-escenario tratara sobre las captura de Traps, en CMD tenemos que ubicar la dirección de las carpetas ya que las traps se ubican en una carpeta diferente a los otros comandos lo podremos ver en la figura 4.10; y para poder utilizar las traps será con el comando snmptrap para que funcione en la red. El siguiente comando que configuraremos en CMD funciona:

Snmptrap –v1 –c tesisgestion 192.168.1.149 1.2.3.4 192.168.2.29 4 0 ‘1’

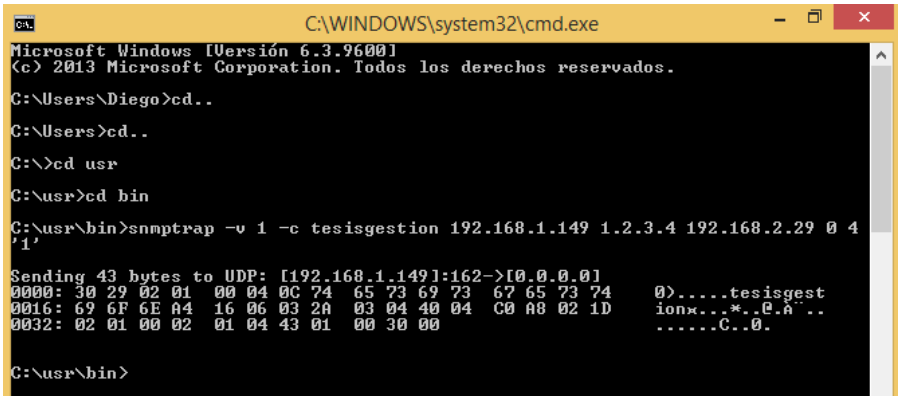

Figura 4.10 Configuración de acceso a las carpetas y configuración de las Traps para la versión 1.
Elaborado por: Autor

Después de haber realizado las traps con su respectivo comando y obteniendo la respectiva respuesta podemos ir a WireShark para comprobar que si hemos capturado las Traps.

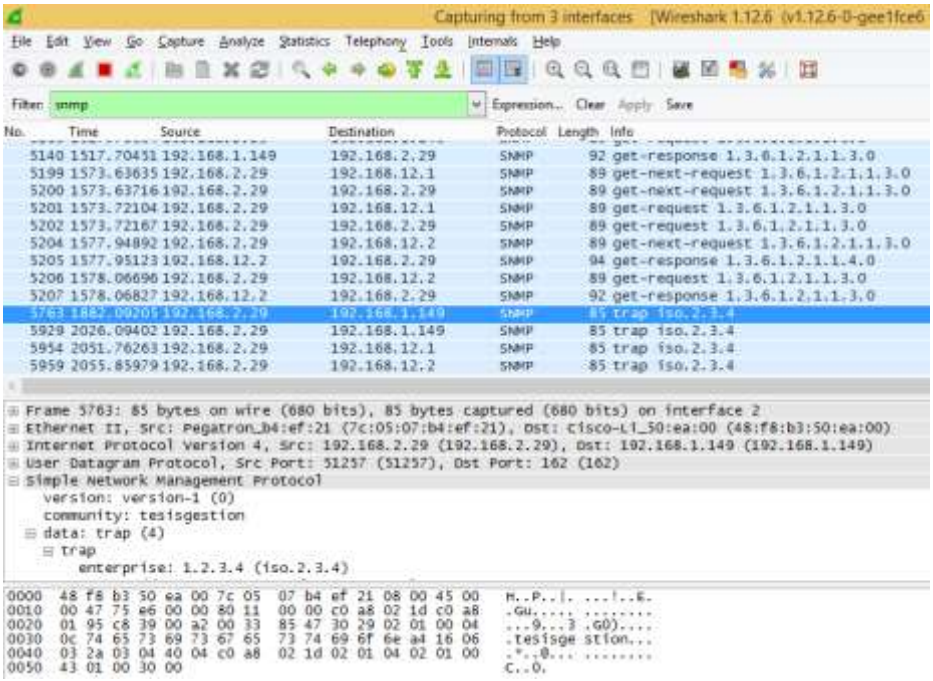

Figura 4.11 Capturas de Traps para la versión 1 de SNMP.
Elaborado por: Autor

4.3 ESCENARIO 2: VERSIÓN 2 DEL PROTOCOLO SNMP (SNMPv2c), EQUIPOS CONECTADOS A UNA RED CON SUS RESPECTIVAS SIMULACIONES E IFNFORMES

4.3.1 Sub-escenario 1

Para el análisis que se da en esta red con los equipos conectados, no tendrá mucha diferencia con el protocolo SNMPv1 ya que en esta versión solo se incluyen dos operaciones más que se verán respectivamente en los informes y capturas, lo que podríamos decir es que el comando para obtener las Traps cambiara un poco no mucha diferencia a la versión 1, todo lo realizaremos desde la maquina gestora como veremos en las figuras 4.12, y al final revisar todo lo que configuremos y programemos en los paquetes con WireShark para luego analizarla y comprarla.

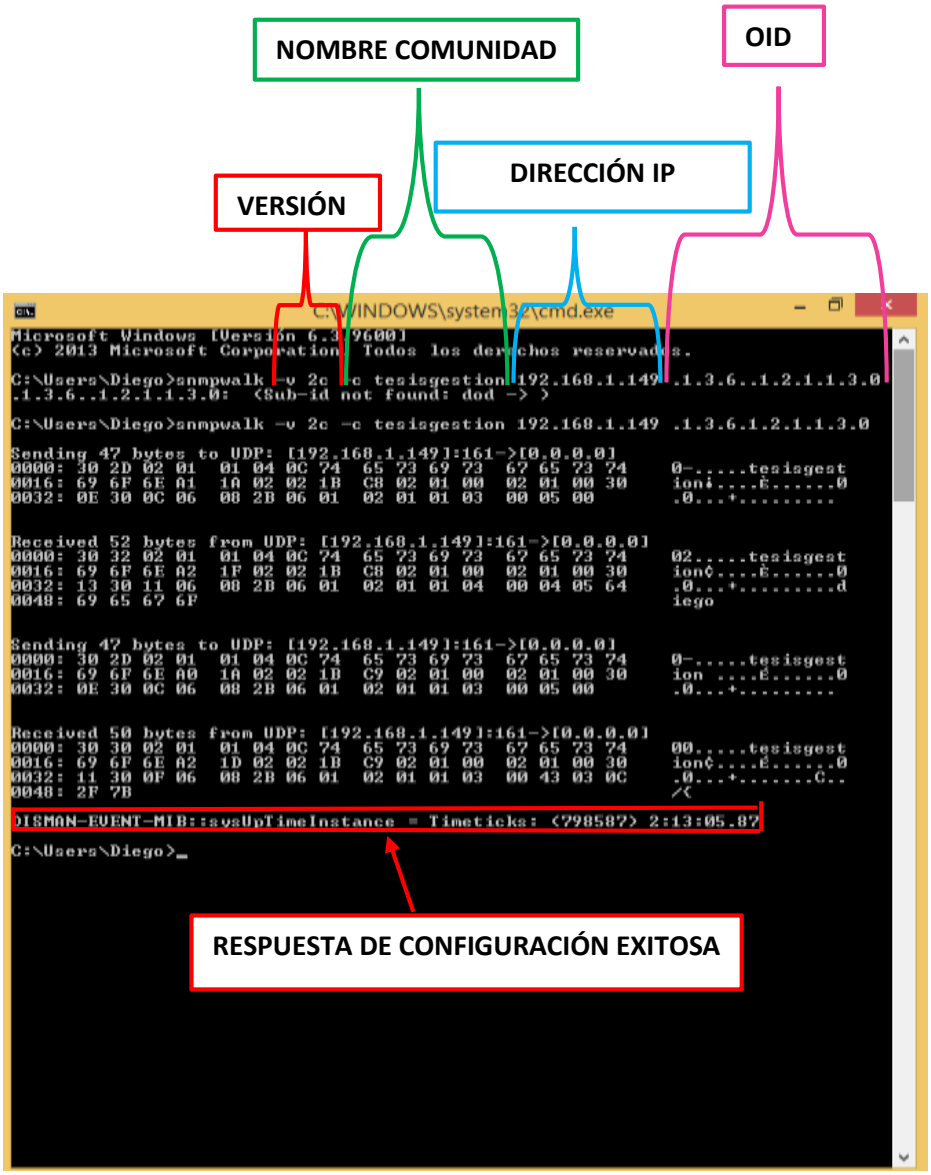

Figura 4.12 Configuración en CMD del comando SNMPWALK desde la máquina gestora.
Elaborado por: Autor

Después de haber usado el comando podemos dirigirnos a WireShrak para verlos resultados que obtuvimos, como se vio en la versión anterior tendremos las operaciones: “GetNextRequest”, “GetReques” y la del “GetResponse” que son enviados entre los equipos, como lo podemos ver en las figuras 4.13, 4.14 y 4.15.

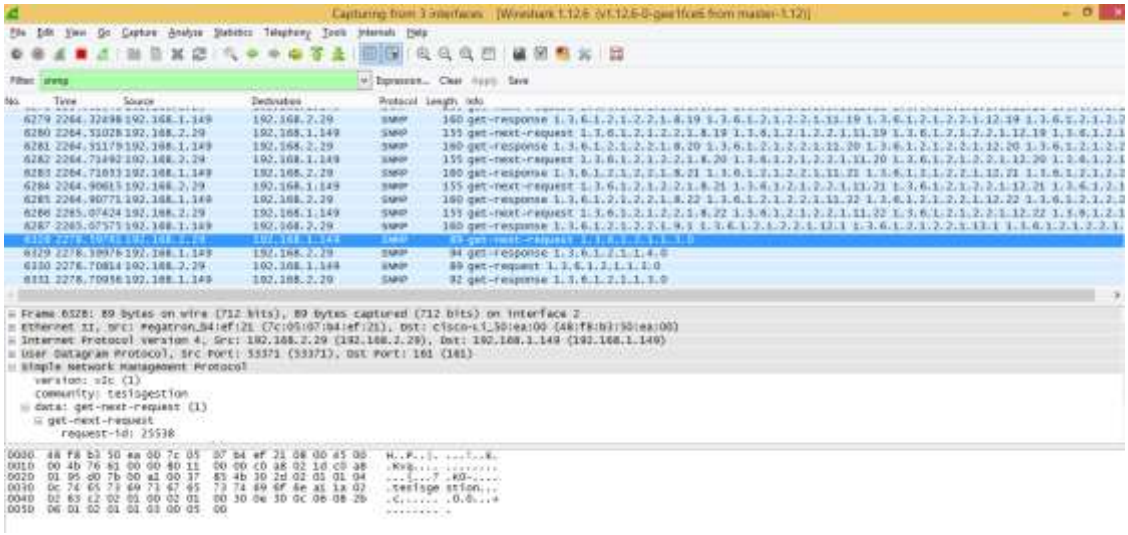

Figura 4.13 Captura de la operación "GetNextRequest" de la versión SNMPv2c.
Elaborado por: Autor

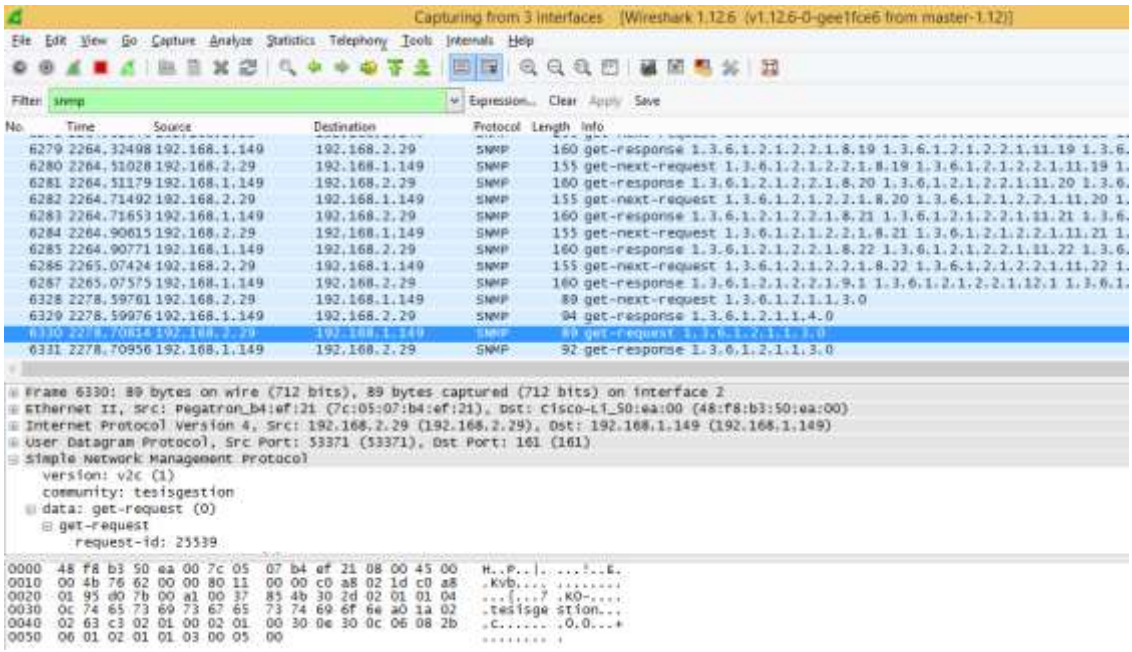

Figura 4.14 Captura de la operación "GetRequest" de SNMPv2c.
Elaborado por: Autor

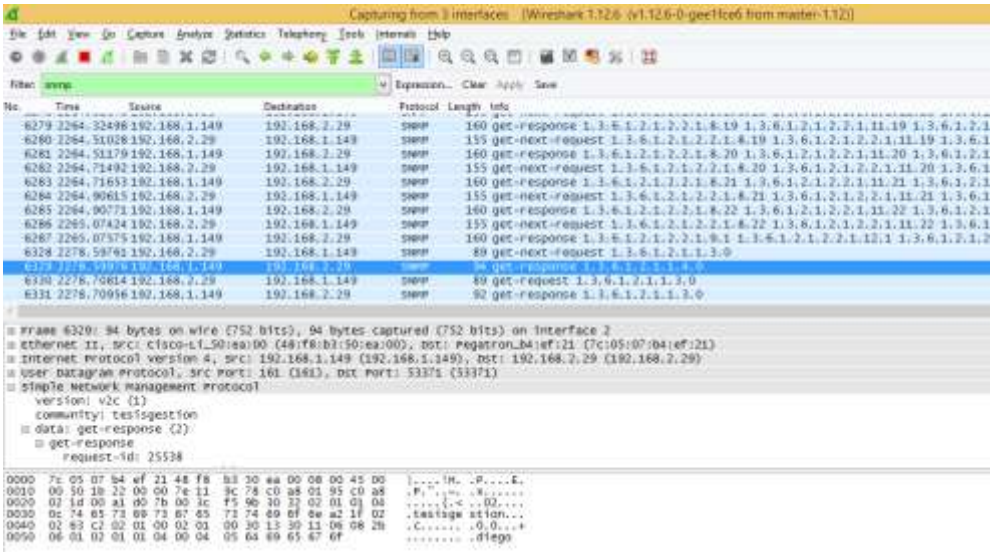

Figura 4.15 Captura de la operación "GetResponse" de la versión 2 (SNMPv2), podemos observar el agente del equipo.
Elaborado por: Autor

4.3.2 Sub-escenario 2

En este sub-escenario veremos las operaciones que fueron incluidas para esta versión, desde el CMD usamos el comando "SNMPBULKWALK" veamos en la figura 4.16.

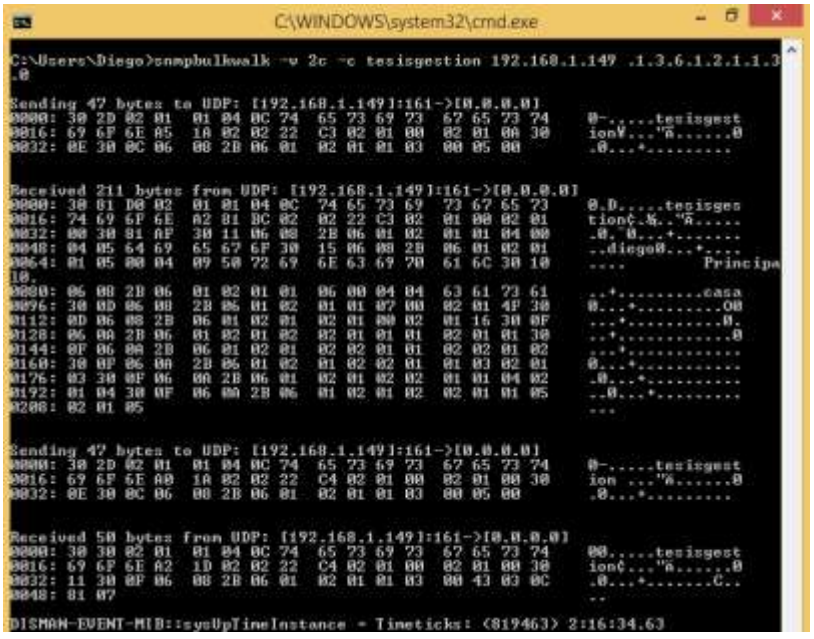

Figura 4.16 Configuración del comando SNMPWBULWALK, a diferencia del snmpwalk solo se cambia el comando.
Elaborado por: Autor

Después de haber usado SNMPBULKWALK nos dirigimos al WhireShark para poder observar lo que el comando proporciona, lo podemos ver en la figura 4.17.

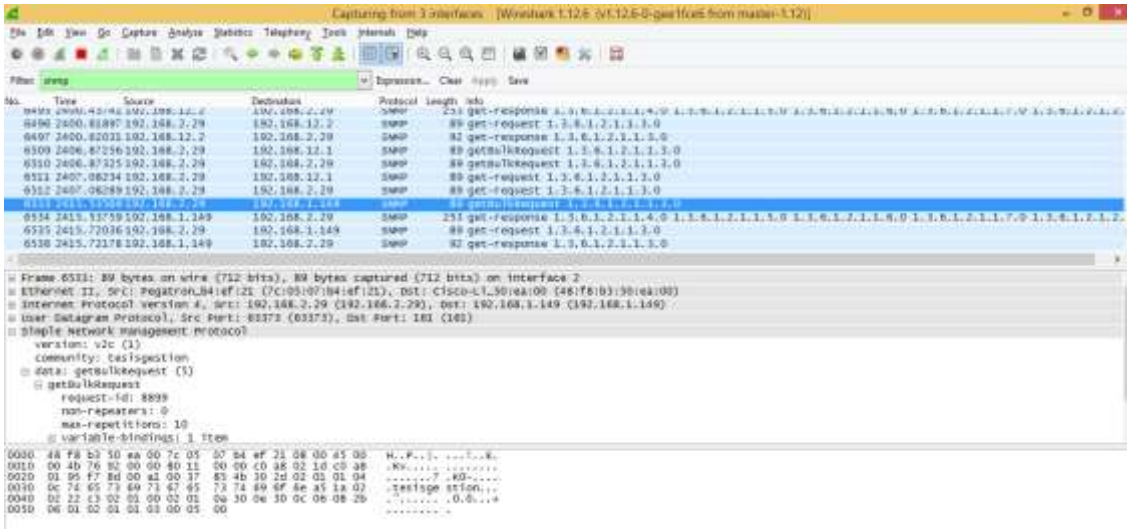

Figura 4.17 Captura de la operación "SNMPBULKWALK" en WireShark.
Elaborado por: Autor

4.3.3 Sub-escenario 3

Como lo hicimos en el escenario de la versión 1, haremos las capturas de las Traps para la SNMPv2c, entramos al CMD, buscamos la carpeta "bin" para poder acceder a las Traps como se lo explico en la versión 1 y escribimos el siguiente comando:

Snmptrap –v 2c –c tesisgestion 192.168.1.149 "" 1.2.3.4.0

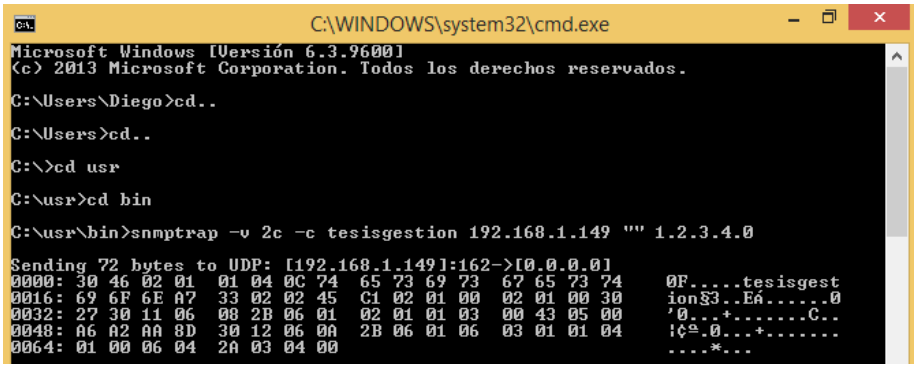

Figura 4.18 Uso del comando SNMPTrap para la versión 2 en CMD.
Elaborado por: Autor

Después de haber ejecutado el comando de las Traps, nos colocamos en WireShark para la respectiva captura, como podemos ver en la figura 4.19.

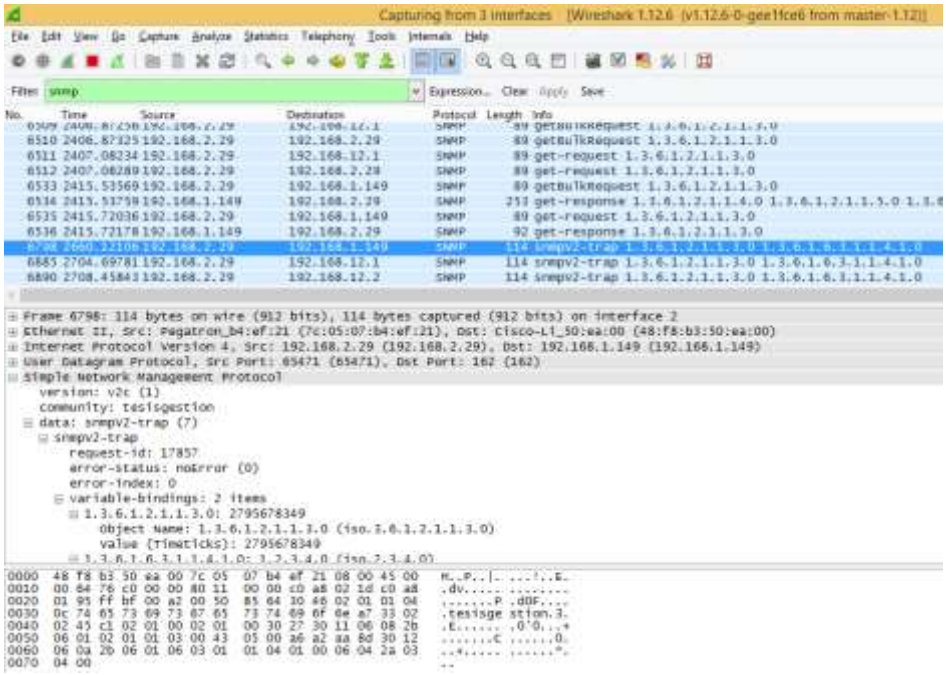

Figura 4.19 Captura de las Traps-SNMPv2c en WireShark.
Elaborado por: Autor

4.4 ESCENARIO 3: VERSIÓN 3 DEL PROTOCOLO SNMP (SNMPv3), EQUIPOS CONECTADOS A UNA RED CON SUS RESPECTIVAS SIMULACIONES E INFORMES

4.4.1 Sub-escenario 1

Para la configuración de la versión 3 de SNMP en sistemas operativos Windows será lo mismo que en las anteriores versiones, entraremos a modo configuración en el CMD pero elegimos las opciones que vemos en las figuras , toda la configuración ya no serán en modo de comunidad sino en modo de usuario; elegiremos nombre del usuario, nombre del contexto, el nivel de seguridad y las claves; después de haber configurado el "snmpconf" guardaremos el archivo para que funcione con los comandos que se utilizaran en la versión 3.

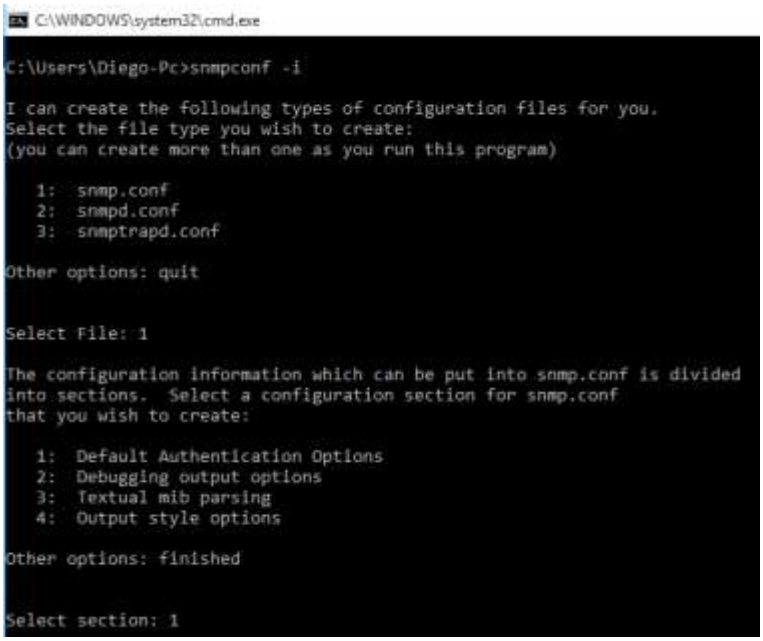

Figura 4.20 Configuración snmpconf para la versión 3.
Elaborado por: Autor

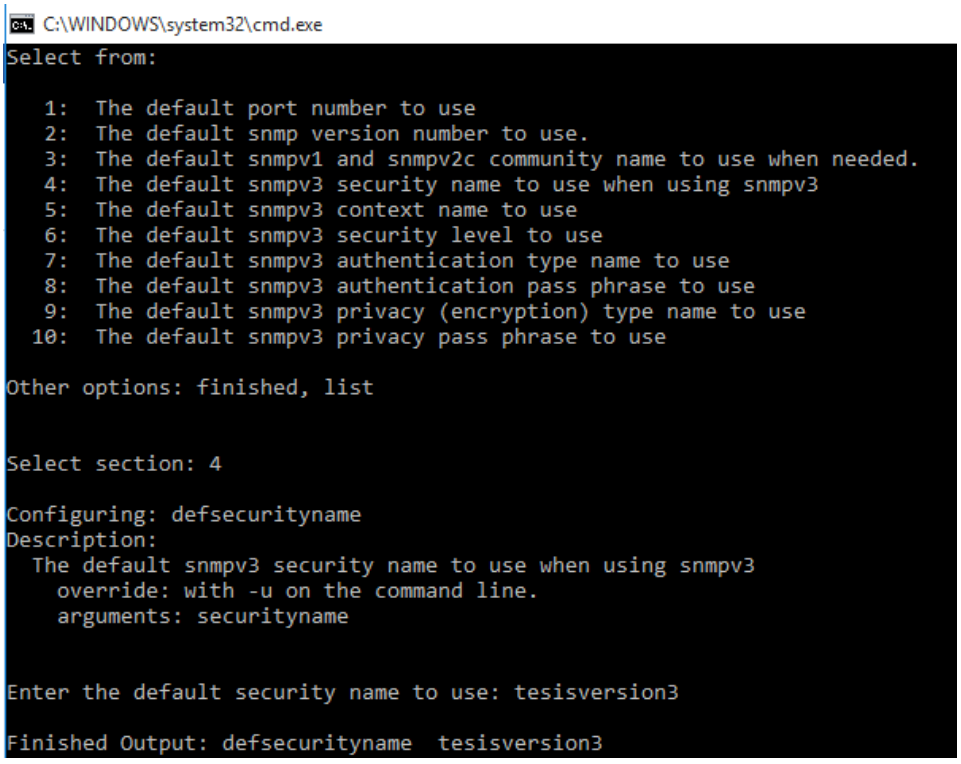

Figura 4.21 Configuración del nombre del usuario para SNMPv3.
Elaborado por: Autor

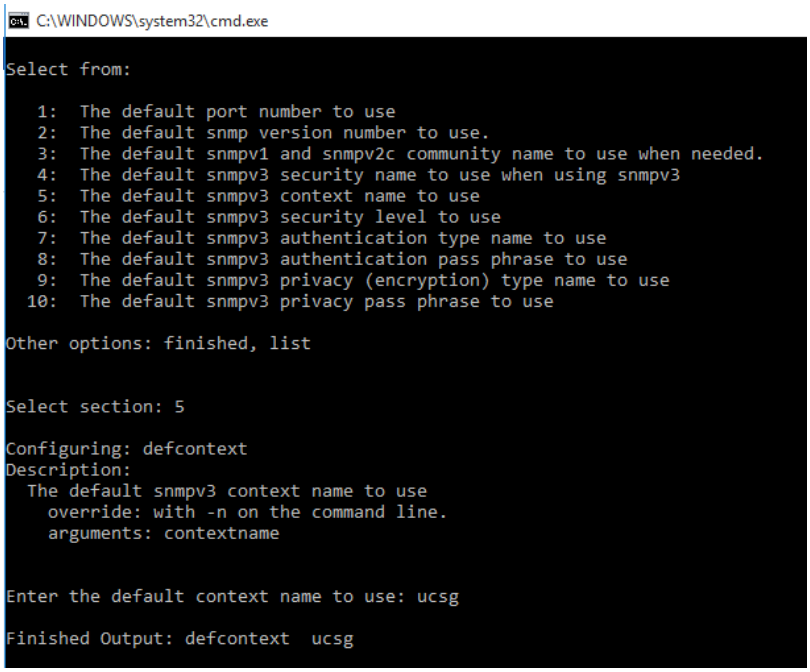

Figura 4.22 Configuración de nombre del contexto de SNMPv3.
Elaborado por: Autor

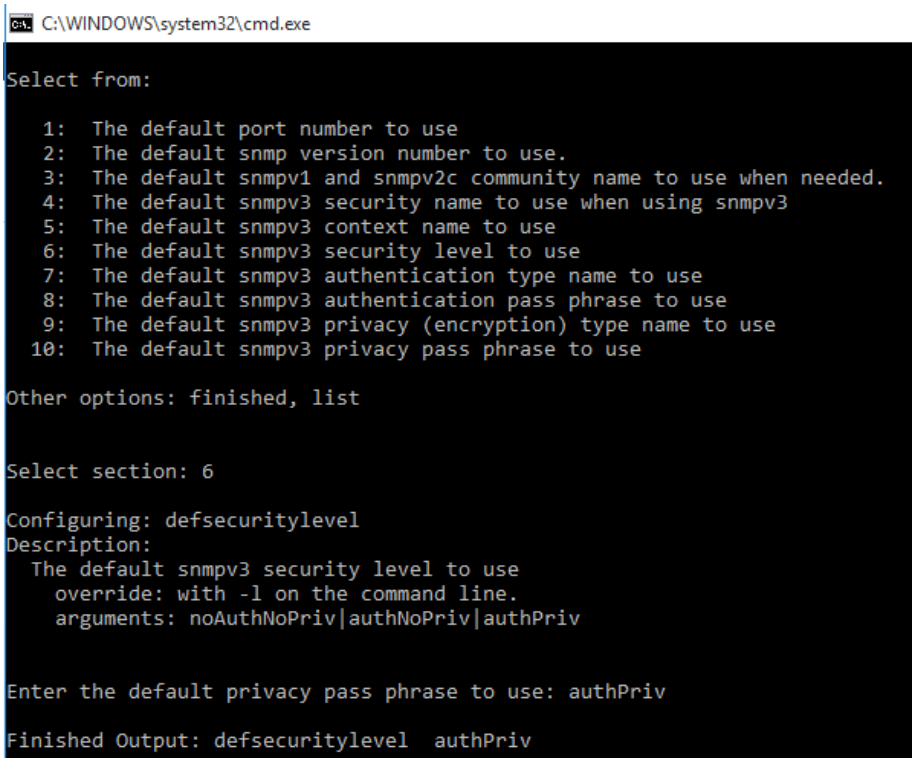

Figura 4.23 Configuración del nivel de seguridad a utilizarse.
Elaborado por: Autor

```
Select from:

   1:  The default port number to use
   2:  The default snmp version number to use.
   3:  The default snmpv1 and snmpv2c community name to use when needed.
   4:  The default snmpv3 security name to use when using snmpv3
   5:  The default snmpv3 context name to use
   6:  The default snmpv3 security level to use
   7:  The default snmpv3 authentication type name to use
   8:  The default snmpv3 authentication pass phrase to use
   9:  The default snmpv3 privacy (encryption) type name to use
  10:  The default snmpv3 privacy pass phrase to use

Other options: finished, list


Select section: 7

Configuring: defauthtype
Description:
  The default snmpv3 authentication type name to use
    override: with -a on the command line.
    arguments: authtype


Enter the default authentication type to use (MD5|SHA): MD5

Finished Output: defauthtype  MD5
```

Figura 4.24 Configuración del tipo de autenticación a utilizarse en SNMPv3.
Elaborado por: Autor

```
C:\WINDOWS\system32\cmd.exe
Select from:

   1:  The default port number to use
   2:  The default snmp version number to use.
   3:  The default snmpv1 and snmpv2c community name to use when needed.
   4:  The default snmpv3 security name to use when using snmpv3
   5:  The default snmpv3 context name to use
   6:  The default snmpv3 security level to use
   7:  The default snmpv3 authentication type name to use
   8:  The default snmpv3 authentication pass phrase to use
   9:  The default snmpv3 privacy (encryption) type name to use
  10:  The default snmpv3 privacy pass phrase to use

Other options: finished, list


Select section: 8

Configuring: defauthpassphrase
Description:
  The default snmpv3 authentication pass phrase to use
    Note: It must be at least 8 characters long.
    override: with -A on the command line.
    arguments: passphrase


Enter the default authentication pass phrase to use: 12345678

Finished Output: defauthpassphrase  12345678
```

Figura 4.25 Configuración de la clave para el ingreso a la autenticación.
Elaborado por: Autor

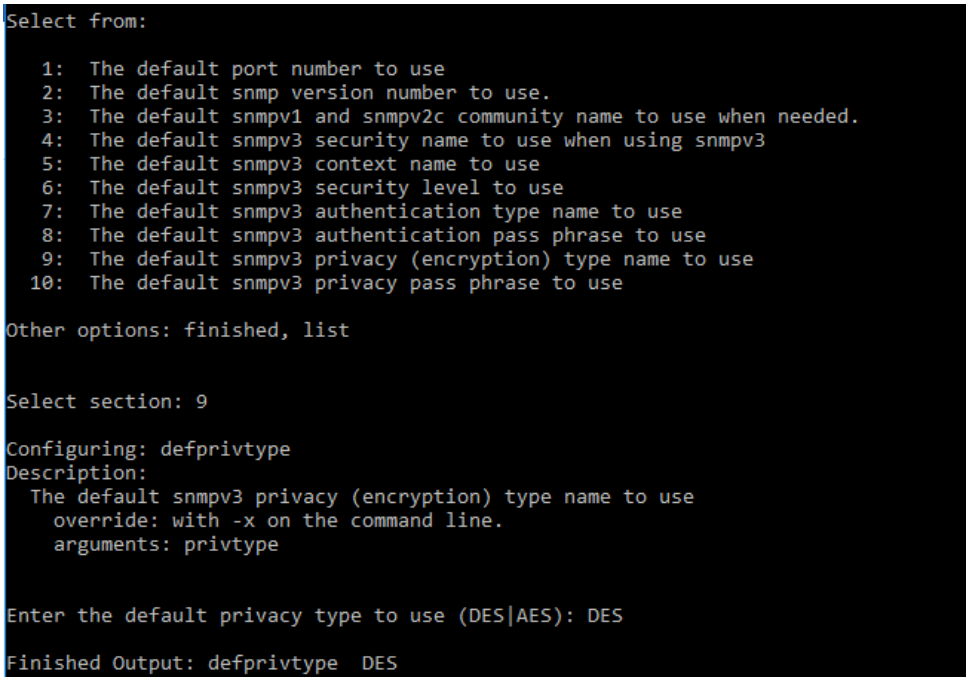

Figura 4.26 Configuración del tipo de privacidad a utilizarse en SNMPv3.
Elaborado por: Autor

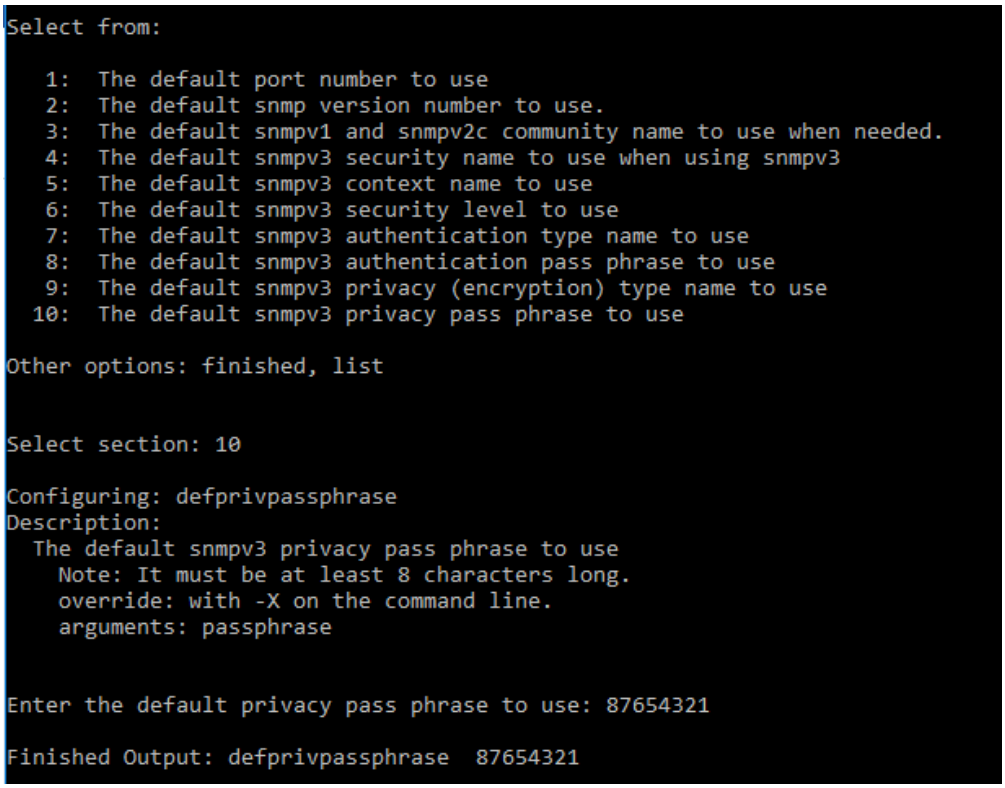

Figura 4.27 Configuración de la clave para ingresar a la privacidad.
Elaborado por: Autor

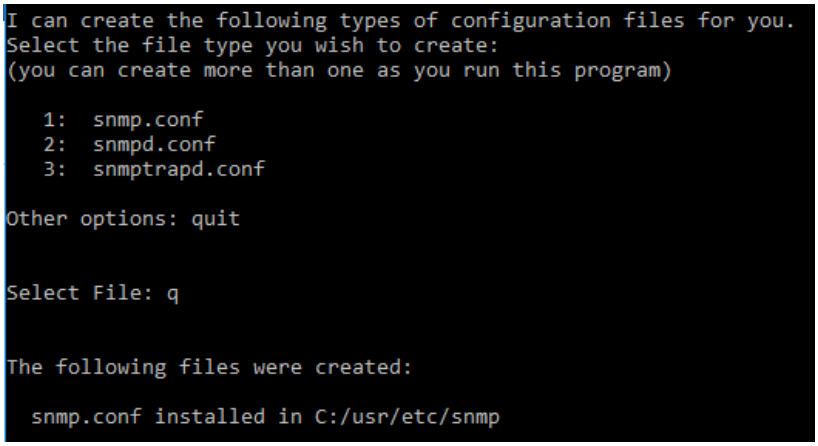

Figura 4.28 Creación del usuario en SNMPCONF para la versión 3.
Elaborado por: Autor

Después de haber creado el usuario, utilizaremos el comando que sirve para activar el usuario y los comandos que se usaran para que se cumplan las operaciones en SNMPv3 al enviar los paquetes, como podemos ver en la figura 4.20, 4.21, 4.22, 4.23, 4.24, 4.25 4.26, 4.27 y 4.28.

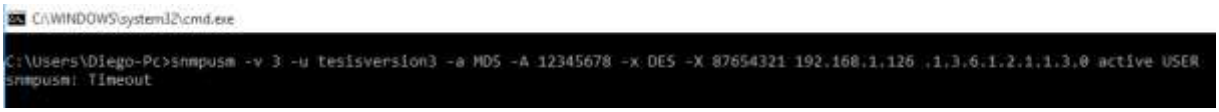

Figura 4.29 Comando SNMPUSM para activar el usuario en SNMPv3.
Elaborado por: Autor

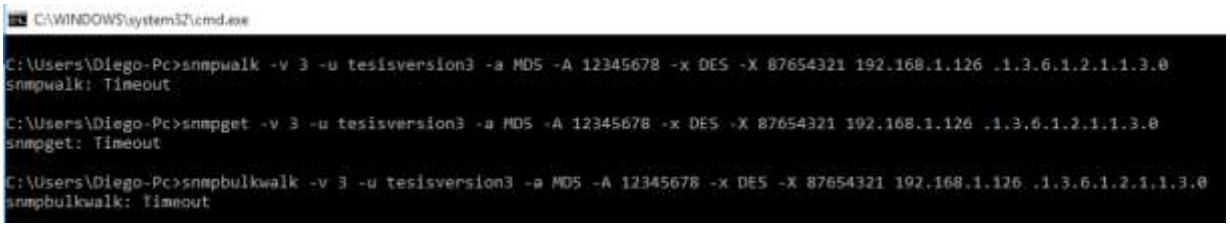

Figura 4.30 Comandos para el uso de las operaciones en SNMPv3.
Elaborado por: Autor

Al utilizar los comandos respectivos para la versión 3 de SNMP en el CMD de Windows, nos damos cuenta que se presentan problemas ya que como en las anteriores versiones obteníamos una respuesta de que se hizo la transmisión correcta, en esta versión la respuesta que nos da es de “TimeOut”, al ver la figura 4.31, que es la de captura d paquetes en el WireShark se observa que no hay una respuesta desde la máquina gestora a la máquina gestionada.

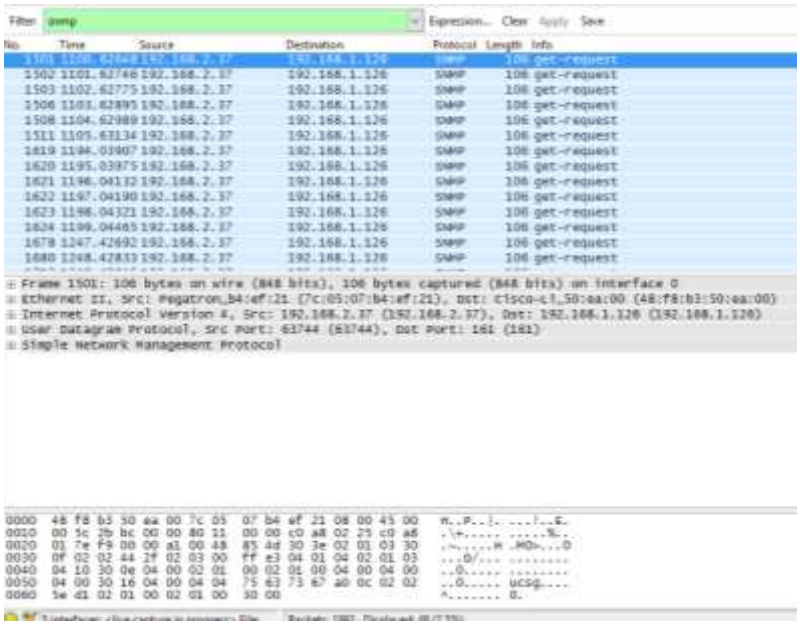

Figura 4.31 Captura de paquetes de SNMPv3.
Elaborado por: Autor

4.4.2 Sub-escenario 2

Existen tres niveles de seguridad para la versión 3, para definir la seguridad que se desea utilizar se lo configura como ya se lo observo anteriormente en el sub-escenario 1; los comandos que se utilizaran para cada nivel de seguridad se los observara en la figura 4.32.

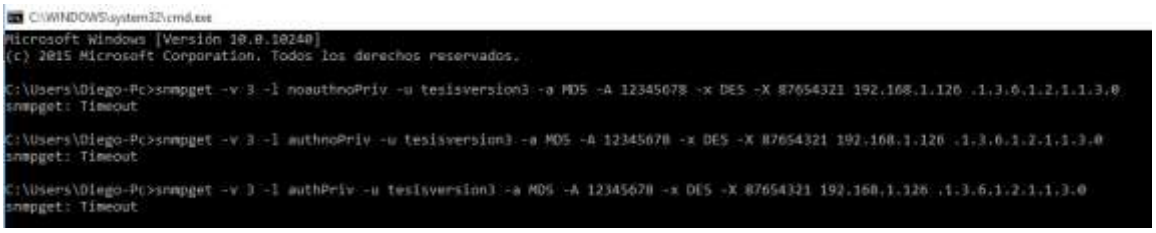

Figura 4.32 Comandos para los diferentes niveles de seguridad en SNMPv3.
Elaborado por: Autor

Como se observa en la figura 4.32, se presenta el mismo problema de programación con los anteriores comandos de SNMPV3; la misma respuesta obtenida "TimeOut" quiere decir que no se pudo comunicar los dos ordenadores.

CAPÍTULO 5

5 ANÁLISIS DE LOS RESPECTIVOS INFORMES OBTENIDOS

En este capítulo se presentarán los informes y resultados obtenidos de las simulaciones y pruebas que permiten determinar las diferencias, las ventajas, las desventajas, el que puede ser más rendidor y no presentar problemas y otras dudas de todas las versiones del protocolo SNMP, primero se describirá cada versión con los resultados obtenidos y después se realizara un cuadro comparativo de lo más importante de cada versión.

5.1 SNMP VERSIÓN 1

Con los informes obtenidos y las investigaciones hechas, el protocolo SNMPv1 trabaja con un rango de operaciones, que al desarrollar nuestra implementación y con sus respectivas capturas podemos ver cuáles son las operaciones UDP que se manejan en esta versión; dichas operaciones cumplen funciones diferentes al enviar los paquetes desde la máquina gestora hasta la máquina gestionada. En el escenario 1, usamos el comando snmpwalk para que así puedan funcionar las operaciones de la versión 1 desde la maquina gestora, se asigna la dirección correspondiente siempre con la OID que corresponde en este caso .1.3.6.1.2.1.1.3.0. En el programa WireShark podemos ver las operaciones que no podemos ver en el CMD, y vemos que hay un envío de paquetes desde la maquina gestora y una respuesta de que ha recibido con éxito en la máquina gestora, como se ven en las figuras del capítulo 4.

En la figura 4.7 podemos observar el Request-ID 8771, este número no indica el orden que son enviados los datagramas y también nos informa si se encuentran datagramas duplicados, como podemos ver que las capturas de la primera versión es demasiado extensa se encontraran más campos que aunque no se puedan observar se los explicara para que se tenga un concepto más apropiado los otros campos; tenemos el campo del Error-Status se encuentra más abajo del RequestID y es aquel que nos dice que si se encuentra o no un error en el proceso en este caso nuestro Error-Status nos dice noError(0). Otro campo a indicar es el Error-Index es el que nos indica si la variable presenta un error pero nuestra respuesta es “0” ósea que tampoco presentamos un error y el ultimo campo será la del VarBindList que nos mostrara la lista de las

variables analizadas en este caso nos dirá que es “1” la cual ya la hemos dicho que es la .1.3.6.1.2.1.1.3.0. Como se ve en la figura hay dos operaciones, pregunta y respuesta con el GetRequest el valor a mostrar será solo NULL y para el getResponse será la OID ingresada. En la figura 4.11 nos indica cómo es que funciona la ejecución del comando de las Traps, explicamos porque le damos el valor “4” y es porque este corresponde al “authenticationFailure” o también conocido como el “fallo de autenticación”, los campos que no podemos observar a partir del “entreprise” se los describirá. El campo entreprise es aquel que nos indica el objeto que genera la trap (en este caso el 1.2.3.4), seguimos y el campo que encontramos es el del “agen-addr” y es aquel en donde encontramos la dirección desde donde ejecutamos la trap como vemos en la figura 4.11 es la 192.l68.2.29, el campo del “generic-trap” es aquel que nos hace referencia de un mensaje que no ha sido autenticado en este caso está el authenticationFailure “4”. El campo ubicado más abajo es del “specific-Trap” y es el que nos muestra un evento especifico del fabricante en la trap enviada, pero como la trap enviada fue de tipo genérico se define con el valor “0”, el campo del “time-stamp” es el que nos indica el tiempo desde la última inicialización de la entidad de red y la generación de la trap pero como pudimos darnos cuenta es de “0” ósea que no hubo dicho tiempo y por ultimo tenemos el campo de “variable-bindings” es de la lista de tipo varBindList que contiene información de posible interés pero como no se programó así nos dará una respuesta de “0”.

5.2 SNMP VERSIÓN 2

SNMPv2c abarca nuevas operaciones; en el escenario 2 del capítulo 4 al igual que la primer versión se utiliza la misma programación, el mismo nombre de comunidad, la misma dirección IP de la máquina a gestionarse, el mismo OID y se utilizara el mismo comando snmpwalk para después ver los cambios que se efectuaron en el programa wireshark. Las primeras operaciones son iguales a la versión 1 pero mejora en su encapsulado, así que no tiene mucha diferencia se enviara el paquete y se obtendrá la debida respuesta de que se transmitió correctamente como lo observamos en la figura 4.13. Lo mismo que en la versión 1 se verán dos operaciones de pregunta y respuesta que estarán con el GetResponse pero se mostrara en su evaluación el NULL y en el GetResponse estará la OID asiganada.

Las nuevas operaciones que se incluyeron para la versión 2 serán expuestas por el nuevo comando "snmpBulkWalk" que a diferencia de las otras operaciones mencionadas pueden introducir más OID's dentro de un mismo paquete así que se trabajó con la misa OID usada en el snmpwalk. Aunque esta versión es mejor que la versión 1 aún se puede mostrar la comunidad sin encriptar que quiere decir que todavía presenta problemas en lo que es seguridad. Con respecto a las traps como podemos ver su configuración en la figura 4.18 ya no especificaremos el tipo de Trap a enviarse porque el comando que usaremos será diferente a la versión 1. Como podemos ver en la figura 4.19 tendremos más campos el primero es el de RequestID: "17857" como se dijo es aquel que nos indica el orden de envió de datagramas, tendremos el campo de Error-status que nos dice que es "0" ósea que no hay errores en el proceso, el siguiente campo es el de Error-Index que como vemos es "0" nos indica que no encontró ningún error y el ultimo campo que es el de "variable-bindings" que nos indica la variables que fueron analizadas como vemos dice "2" que son las variables que se usaron ya que una evalúa el tiempo y la otra el OID.

5.3 SNMP VERSION 3

Los resultados obtenidos en el capítulo 4 nos mostraban el mismo problema que se presentaba en todas nuestras ejecuciones de comandos para el funcionamiento de cada operación, "TimeOut" no es un problema común ya que después de muchas investigaciones y de buscar una solución a esta mala programación o mala configuración, se llegó a varios problemas que se pueden presentar en SNMPv3 para sistemas operativos Windows. Se investigó el problema y la posible solución que se podría dar, pero no se obtuvo solución alguna, los problemas que se investigaron fueron:

- En la configuración del usuario en CMD no es muy confiable, porque cuando creamos el usuario faltan más variables o más ítems que son necesarios para que el usuario sea creado con los propósitos que el administrador desea.
- Cuando se hizo una comparación de las programaciones que usaron en otros proyectos, se observó que los sistemas operativos que utilizan son

diferentes entre la máquina gestora y la máquina gestionada; es decir que no era de Windows a Windows sino que eran de diferentes sistemas operativos: Windows-Linux, Windows-Solaris, se podría decir que Windows no es muy confiable para la creación de usuarios de la versión 3 de SNMP.

- Se buscó otras soluciones para este proyecto, las investigaciones que se obtuvo fue la de utilizar un programa que ejecute directamente con SNMP sin programar; pero se obtuvo la misma respuesta no había la respectiva comunicación ya que los otros programas funcionaban con sistemas operativos diferentes a Windows.
- Otro problema es que como la configuración del usuario en otros sistemas operativos (LINUX-SOLARI); es más exacto ya que usa más comandos que en WINDOWS no hay.

En las capturas de paquetes de WireShark solo se observa que se envía la operación GET-REQUEST, o sea que no hay una respuesta desde la máquina gestionada ya que por la falta de variables en CMD no se podrán observar las demás operaciones.

5.4 ANÁLISIS Y COMPARACIÓN DE LOS INFORMES OBTENIDOS

Después de los resultados obtenidos en la respectiva implementación con la configuración de cada versión, se realizara el análisis y la comparación que hay entre las 3 versiones de SNMP.

Cada versión tiene su funcionamiento y su mejoramiento, aunque se obtuvo problemas para la obtención de los resultados de la versión 3 con lo que se ha investigado y con lo que se ha manejado en configuraciones daremos los conceptos más importantes de la versión 3; esto se lo demostrara en el siguiente cuadro que clasifica y compara sus funciones, operaciones y traps:

Tabla 5.1 Tabla de las importantes comparaciones y diferencias de las versiones de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Acceso a los paquetes	Trabaja con el acceso de comunidades.	Trabaja con el acceso de comunidades.	Trabaja con la autenticación de nombres de usuarios (USM)
Seguridad	La seguridad se mide con el nombre de la comunidad que el administrador desea ingresar	La seguridad se mide con el nombre de la comunidad que el administrador desea ingresar	Trabaja con los niveles de seguridad "noAuthNoPriv", "authNoPriv" y "atuhPriv".
Operaciones	GetNextRequest, GetRequest, GetResponse, Set y Trap.	GetNextRequest, GetRequest, GetResponse, GetBulk, Set, Trap e Inform.	GetNextRequest, GetRequest, GetResponse, GetBulk, Set, Trap e Inform.
Acceso a la información	Permite el acceso de cualquier persona a la información que es enviada en la red.	Permite el acceso de cualquier persona a la información que es enviada en la red.	La información es encriptada mediante el authprotocol (MD5-SHA) y el privprotocol (DES-AES)
O. Traps	Él envió de traps para esta versión es muy primitivo a diferencia de las otras versiones.	Las Traps son mejoradas en esta versión ya que mejora su estructura.	Las traps son mejoradas y trabajan con los niveles de seguridad y de encriptación.

Elaborado por: Autor

CONCLUSIONES

- El protocolo SNMP es de mucha utilidad cuando se desea intercambiar informaciones entre diferentes dispositivos y es muy útil para las empresas; los equipos que se usaron fueron configurados todos en base al protocolo SNMP.
- SNMP es un muy buen administrador de las redes que son utilizadas en internet, no utiliza muchos recursos, para procesar la información no requiere mucho tiempo y es muy fácil manejar este protocolo.
- En los escenarios que se implementaron, siempre se utilizó el mismo OID para que se vea la misma respuesta entre las versiones y que no se tenga problemas; y para obtener los resultados de los mismos paquetes en el WireShark.
- Entre las dos primeras versiones de SNMP, se puede observar las operaciones entre los elementos de la red y los agentes que son muy diferentes ya que la versión 2 es mejor que la versión 1.
- Con el programa Wireshark podemos ver la igualdad entre las dos primeras versiones de SNMP y es que trabajan con la misma comunidad; o sea que si ingresamos el nombre de otra comunidad no va a poder acceder al uso de los paquetes que son enviadas en la red. Pero la diferencia es que estas dos versiones son muy débiles en lo que es seguridad ya que el acceso lo puede hacer cualquier persona pero con la encriptación que tiene la versión 3 el nivel de seguridad aumenta y es por eso que la versión 3 es la más recomendaba para el trabajo con este protocolo.
- De acuerdo a las investigaciones que se han dado en este proyecto las empresas que manejan este protocolo tienen diferentes criterios ya que unos prefieren utilizar la versión 2 y otras empresas la versión 3 de SNMP y esto se debe a que la versión 2 es la más preferida para el monitoreo de redes y la versión 3 aún hay sistemas que no soportan esta versión, como lo pudimos ver en el escenario 3.
- Otro punto de lo que se investigo fue que para la versión 3 por la complejidad de su encriptación tiene que ser manejados con otros programas.
- Para finalizar se podría decir que la versión 2 es la que más opción tendría para el manejo en las empresas.

RECOMENDACIONES

- Se recomienda el uso de letras, número y signos para el nombre de las comunidades ya que ayudaría a mejorar en la seguridad de las versiones 1 y 2.
- Para la versión 3 se recomienda trabajar con un sistema operativo que al crear el usuario y la seguridad sean bien configurados y no presenten problemas.
- Es recomendable dejar de usar la versión 2 ya que con el tiempo surgirán problemas en la seguridad y es tiempo de comenzar a utilizar la versión 3 pues brinda mayor seguridad y es más confiable.

BIBLIOGRAFÍA

A. Telesyn Corporation. (2005). *http://www.alliedtelesis.com/media/fount/software_reference/271/ar400/400sr.pdf.* Obtenido de http://www.alliedtelesis.com/media/fount/software_reference/271/ar400/snmp.pdf: http://www.alliedtelesis.com/

Bornhager, M. (2002). *Router and routing Basics.*

Bott, E. (mayo de 2015). *microsoft press blog.* Obtenido de microsoft virtual academy: http://blogs.msdn.com/

CERT. (s.f.). *Software Engineering Institute.* Obtenido de Digital Library: https://resources.sei.cmu.edu

Cisco. (s.f.). Linksys E-serier Routers. *User Guide*, 92.

Doctors, A., & Vecchiotti, R. (2012). *Sistemas de gestió y monitorización de fallas para clientes de SANNET soluciones C.A.* Caracas.

Figueroa Arias, D. (1999). *Herramientas de Gestión basada en Web.* Argentina.

George, T. (2003). Introduction to SNMP. *The Extension*, 4.

Gutierrez, D. (Noviembre de 2010). *http://es.slideshare.net.* Obtenido de http://es.slideshare.net/danitxu/snmp-rmon.

Ibarra, Á., & Ramos, G. (2014). *Simulación de las primitivas SNMPv2 en un entorno de una red LAN.* Guayaquil.

Lago, A., & Daniel, M. (2013). *Implementación virtual de redes LAN, enfocadas en el análisis comparativo de las ventajas y desvetajas del uso y aplicación de las diferentes versiones del protocolo SNMP.* Guayaquil.

Lamping, U., Sharpe, R., & Warnicke, E. (2014). *Wireshark User's Guide*

Lorenzo, D. (2011). *Monitorización de red con SNMP y MRTG.*

Molero, L., Villaruel, M., Aguirre, E., & Martínez, A. (2010). *Planificación y Gestión de red.* Maracaibo.

Moreno, A., & Serna, S. (2013). *Diseño e implementación de un prototipo de software para la administracion de red usando SNMPv3 sobre el sistema operativo android.* Quito.

Rathbone, A. (2013). *Windows 8 for dummies.* New Jersey.

Release, S. (s.f.). *Allied Telesis.* Obtenido de http://www.alliedtelesis.com/

Sabal, M. (2006). *http://biblioteca2.ucab.edu.ve/.* Obtenido de *http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAQ8679.pdf.*

Silberschatz, A., Baer, P., & Gagne, G. (2009). *Operating System Concepts 8th Edition.*

Tapía, R., & Sánchez, D. (2009). *Propuesta de un sistema de monitoero para la red de esime zacatenco utilizando el protocolo SNMP y software libre.* Mexico.

Teldat. (2014). *Router Teldat Agente SNMP*.

Valarezo, G., & Julio, S. (2011). *Implementación de un sistema de gestión y administración de redes basados en el protocolo simple de monitoreo de redes SNMP en la red ESPOL-FIEC.* Guayaquil.

Velásquez, A. (2009). *Diseño e implementación de un módulo software para la monitorización de elementos de una red informática utilizando el protocolo SNMP y el lenguaje XML.* Quito.

Xerox. (2003). Simple Network Management Protocol (SNMP) Primer. *Customer Tips*, 10.