ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Diseño e Implementación del monitoreo desde una estación real hacia un entorno virtual utilizando el software de simulación GNS3, basado en el protocolo de gestión de redes SNMPv2"

TESINA DE SEMINARIO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

William Paúl Burbano Moreira

Rita Lissette Bonilla Zambrano

GUAYAQUIL – ECUADOR

AÑO 2014

AGRADECIMIENTO

Gracias Jehová por haberme ayudado durante estos años, el sacrifico fue grande pero tú me diste la fuerza necesaria para continuar; siempre tuve confianza en que lograría salir adelante, en que los retos se podían superar y que alcanzaría esta meta, todo eso se lo debo al más grande de todos, a Dios.

Quiero agradecer a mi mamá, por su incondicional apoyo, tanto al inicio como al final de mi carrera. Gracias Ma' por ser ejemplo de arduo trabajo y tenaz lucha en la vida.

A la ESPOL, y a mis estimados maestros, que, a lo largo de mi carrera, me han transmitido sus amplios conocimientos; especialmente al Ing. Washington Medina, quien, muy acertadamente, dirigió nuestra tesis.

William Paúl Burbano Moreira.

AGRADECIMIENTO

Mis más sinceros agradecimientos a todos quienes han hecho posible obtener mi título profesional; al alma mater de la ESCUELA SUPERIOR POLITECNICA DEL LITORAL (ESPOL), por brindarme las herramientas necesarias para mi aprendizaje; mi director, Washington Medina que con su sapiencia ayudó a forjarme como una profesional lista para representarlos como se lo merecen; mis amigos, que siempre me han tendido la mano cuando se las eh pedido, en especial a mi amigo William Burbano por estar a mi lado luchando constantemente en el trajinar de mis días; mis familiares en general, pero primordialmente a mis padres quienes velan por mi persona, por alentarme tanto en momentos ásperos como difíciles de mi vida y en especial a JEHOVA Dios que siempre está conmigo. A todos y cada uno de ustedes les estaré agradecido eternamente.

Rita Lissette Bonilla Zambrano.

DEDICATORIA

Este éxito se lo quiero dedicar a mis padres, especialmente a mi mamá porque si hay alguien que está detrás de todo este trabajo, eres tú mi Vieja, que has sido, eres y serás el pilar de mi vida.

A mis hermanas, porque juntos aprendimos a vivir, crecimos como cómplices día a día y somos amigos incondicionales de toda la vida, compartiendo triunfos y fracasos. Doy gracias a Dios porque somos hermanos.

A ti, amor; Angy, que has sido fiel amiga y compañera, que me has ayudado a continuar, haciéndome vivir los mejores momentos de mi vida. Gracias mi Gorda

A todos, mis amigos que me han brindado desinteresadamente su valiosa amistad, entre ellos a mis padrinos; gracias por ser la sal que condimenta mi vida.

William Paúl Burbano Moreira.

DEDICATORIA

Esta etapa de mi vida se la dedico humildemente a JEHOVA por poder confiar en sus caminos y no apoyarme en mis propios entendimientos como lo cita Proverbios 3:5,6; por darme la fortaleza para no dejarme desvanecer en obtener este logro; también a los mentores pilares así como motores de mi vida, como lo son mis padres, que día a día se esfuerzan por mi bienestar, por enseñarme a luchar y cursar obstáculos por muy difíciles que estos puedan ser; ya que sin ustedes no lo hubiera hecho tan ameno este logro obtenido, por eso este título se lo dedico a ellos con mucha algarabía en mi vida.

Rita Lissette Bonilla Zambrano.

TRIBUNAL DE SUSTENTACIÓN

M.Sc. Washington Medina M.

PROFESOR DEL SEMINARIO DE GRADUACIÓN

PH. D. Freddy Villao Quezada

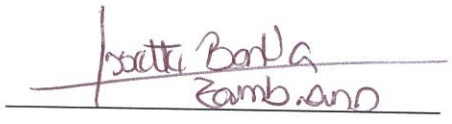
PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

DECLARACIÓN EXPRESA

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

(Reglamento de exámenes y títulos profesionales de la ESPOL)

William Paúl Burbano Moreira



Rita Lissette Bonilla Zambrano

RESUMEN

El presente proyecto consiste en diseñar e implementar una red para monitorear desde una estación real hacia un entorno virtual, basado en el protocolo de gestión SNMPv2; es decir, a través de las herramientas de monitoreo se demostrará la operación de las primitivas del protocolo SNMPv2, destacando las ventajas y desventajas de dicho protocolo. Para llevar a cabo este proyecto se realizó una profunda investigación del funcionamiento del Protocolo SNMP (Simple Network Managment Protocol). Cabe destacar que para el diseño de la red se utilizó el software de simulación de redes GNS3 que es una herramienta importante para el desarrollo de la misma, en vista que permite crear una conexión real lógica y a través de ella se procederá a monitorear toda la red.

El capítulo uno explica de forma sencilla y concisa el proyecto, mencionando y justificando el porqué de la investigación, los objetivos y la metodología del mismo.

El capítulo dos expone el fundamento teórico del protocolo SNMP siendo éste su arquitectura, especificaciones, la estructura de su PDU, la comunidad para enviar capturas SNMP y peticiones de su Gestor, así mismo su evolución, las opciones de seguridad y sus primitivas adicionales en la estructura del PDU del protocolo SNMPv2, siendo la fuente de información los diferentes RFC´s.

El capítulo tres explica detalladamente la instalación de las herramientas a utilizar y su respectiva configuración en base al protocolo SNMPv2, además describe la topología diseñada para este proyecto, la conexión virtual lógica establecida y el protocolo de enrutamiento a cada uno de los routers.

El capítulo cuatro muestra tres escenarios creados para dicho estudio, examinando el comportamiento del protocolo SNMPv2. A estos escenarios se les ha realizado las pruebas y simulaciones respectivas, destacando sus primitivas para posteriormente ser analizadas.

Y por último, en el capítulo cinco se expone los resultados de los tres escenarios mencionados anteriormente dando a conocer las debidas observaciones de cada uno de ellos.

ÍNDICE GENERAL

ABREVIATURAS

AS	Autonomous System
ASN	Autonomous System Number
CCIE	Cisco Certified Internetwork Expert
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CMIP	Common Management Information Protocol
CMIS	Content Management Interoperability Services
DNS	Domain Name System
DPI	Deep Packet Inspection
FTP	File Transfer Protocol
GNS3	Graphical Network Simulator
HMAC	Hash-based message authentication code
HTTP	Hypertext Transfer Protocol
IDLE	Integrated development environment
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IOS	Internet Operating System
JMX	Java Management Extensions
LAN	Local Area Network
LCD	Local configuration data
MA	Management Agent
MIB	Management Information Base

MD5	Message-Digest Algorithm 5
MCSE	Microsoft Certified Solutions Expert
NIO	Network Input/Output
NM-16 ESW	EtherSwitch Network Module PUERTO 16
NMA	Network Management Agent
NMS	Network Management Station
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PDU	Protocol Data Unit
RHCE	Red Hat Certified Engineer
RHCT	Red Hat Certified Technician
RFC	Request For Comments
SHA	Synology High Availability
SMI	Management Information Base
SNMP	Simple Network Management Protocol
SNMPv1	Simple Network Management Protocol version 1
SNMPv2	Simple Network Management Protocol version 2
SNMPv3	Simple Network Management Protocol version 3
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User Security Model
VACM	View-based Access Control Model
VTY	Virtual Teletype
XML	Extensible Markup Language

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo surge ante la necesidad de administrar una red, la misma que facilite al Administrador realizar tareas de gestión como planificar, organizar, mantener, supervisar, evaluar, y controlar los elementos de las redes de comunicaciones.

La Administración o Gestión basada en el protocolo SNMP (Simple Network Management Protocol o Protocolo Simple de Gestión de Red), permite a los administradores de red administrar dispositivos y diagnosticar problemas en la red.

Este trabajo plantea, por una parte, diseñar e implementar una red virtual, la misma que estará constituida de tres redes LAN con sus respectivos ruteadores ubicados en las ciudades Guayaquil, Quito y Cuenca, utilizando el software de simulación de redes GNS3; para luego proceder a monitorear toda la red a través del software OpenNMS y capturar los paquetes con Wireshark, de tal manera que permita al administrador inspeccionar el área de la gestión. Por otro lado, se planea realizar un seguimiento a las transmisiones de datos con la herramienta de monitoreo para supervisar el rendimiento de la red y reparar daños si es necesario.

La red está compuesta por varias estaciones, de las cuales una será la estación real; la misma que permitirá al administrador monitorear toda la red y mostrar las capacidades del protocolo de gestión SNMP.

También se implementará la configuración básica en cada uno de los ruteadores, entendiéndose como configuración básica: Nombre del host del router, desactivar la búsqueda DNS, contraseña de modo EXEC, contraseña para las conexiones de la consola y conexiones VTY, etc. Además se pondrá en funcionamiento el protocolo de enrutamiento OSPF.

Se hace énfasis en muchas características como seguridad, eficiencia, interfaz amigable, etc. Por otro lado, intenta integrar un conjunto de herramientas que sean rápidamente implementables y permitan al Administrador realizar algunas operaciones de administración en agentes del tipo pc/routers, ver estadísticas, estado y evolución de estos dispositivos.

CAPÍTULO 1

1. DESCRIPCIÓN GENERAL DEL PROYECTO

1.1 DESCRIPCIÓN

A medida que avanza los años, también el avance tecnológico se hace presente en la vida de los usuarios y la complejidad de la misma sin lugar a dudas, por eso se destaca la importancia que representa las plataformas tecnológicas con software necesarios para la administración, control y monitorización de redes mediante gestión de redes, que es la forma más fiel de representar configuración de red y poder seguir paso a paso la interconexión entre los equipos que la componen y ofrecer la visión real de las instalaciones.

Existen plataformas de gestión integradas con aplicaciones en común como el protocolo SNMP, para la administración de redes estándar utilizadas en Internet. Dicho protocolo, define la comunicación de un administrador con un agente a través de dispositivos administrados.

El protocolo SNMP tiene la capacidad de integrarse en productos de diferentes fabricantes que permite al administrador mantener una base de datos con todas las configuraciones de los ruteadores.

Hoy en día existen tres versiones disponibles de este protocolo; SNMPv1, SNMPv2 y SNMPv3, pero nos enfocaremos en SNMPv2 este protocolo fue la mejora de SNMPv1 perfeccionando la seguridad y funcionamiento y es el más usado, por eso se lo ha tomado en consideración para el proyecto presente, teniendo el respectivo monitoreo desde una estación real hacia un entorno virtual, mediante el uso del software de simulación GNS3 para dar a conocer las ventajas y las desventajas de dicho protocolo.

1.2 JUSTIFICACIÓN

Hasta la llegada de SNMP, la gestión de red había sido propietaria y los productos eran desarrollados por cada fabricante, lo que complicaba enormemente los centros de control de las redes heterogéneas. Además, dada la dificultad de desarrollar este tipo de productos y el mercado restringido al que iban dirigidos, los productos eran caros y complejos.

SNMP (Protocol Management Network Simple) apareció para añadir nuevos comandos y reducir el tráfico de red, especialmente en redes grandes; este protocolo habilita una estación de administración para que configure, monitoree y reciba mensajes trap (alarma) de equipos de la red.

La finalidad de realizar una administración de redes es dar un servicio para emplear una variedad de herramientas, aplicaciones y dispositivos que sirvan para ayudar en la supervisión y mantenimiento. Esta tarea recae en una persona (administrador de red) responsable de supervisar y controlar el hardware y software de la misma, trabajar en la detección y corrección de problemas que hacen ineficiente o imposible la comunicación.

Con el propósito de cubrir algunas falencias de este protocolo nace SNMPv2 (Versión 2), que es una actualización propuesta de la versión 1, la misma que provee estructura administrativa adicional, autenticación y privacidad.

El interés de este proyecto es la simulación de una estación real basada en la estructura del protocolo SNMPv2 como estación de gestión, para familiarizar al usuario con los dispositivos de la red con una interfaz amigable; creando un método de aprendizaje educativo para entidades que no poseen equipos en sus laboratorios, puesto que este sistema permite evaluar con simulación orientada a la realidad.

1.3 OBJETIVOS

1.3.1 Objetivo General

Diseñar e implementar una red LAN utilizando el protocolo SNMPv2 para monitorear la red desde una estación real hacia un entorno virtual, a través del software de simulación de redes GNS3.

1.3.2 Objetivos Específicos

- Interpretar los conceptos básicos del protocolo de gestión SNMP.
- Estudiar y comprender el software de simulación de redes GNS3 y las herramientas de administración.
- Diseñar una red LAN a través del software libre GNS3 en base a una estación real para la implementación virtual de la misma.
- Establecer la conexión de los ruteadores mediante el protocolo de enrutamiento OSPF.
- Simular de manera virtual la red LAN en el software GNS3.
- Mostrar las capacidades del protocolo de administración SNMPv2 a través de las herramientas de monitoreo.
- Realizar un seguimiento de la red y solucionar daños si es necesario.
- Analizar y comprender los resultados obtenidos en las simulaciones.

1.4 METODOLOGÍA

Como metodología de trabajo se realizará un análisis teórico general acerca del protocolo de gestión SNMP, estableciendo sus características (arquitectura, funciones, modo de operación, seguridad) dentro de una red.

Para el desarrollo de este proyecto se procederá a diseñar y simular una red LAN virtual basada en la arquitectura del protocolo SNMP, habilitando su estación de gestión, la misma que será una estación real mediante el software de simulación de redes GNS3. En esta estación real se podrá monitorear la red a través de la herramienta de monitoreo OpenNMS y capturar los paquetes con Wireshark para posteriormente mostrar detalladamente el comportamiento del sistema.

Por otra parte, a través de la estación real y de la herramienta de administración se obtendrá información detallada del protocolo SNMPv2, destacando sus capacidades las mismas que reflejarán las ventajas y desventajas de dicho protocolo.

Para finalizar, se pretende realizar un seguimiento de la red para supervisar el rendimiento de la misma y solucionar daños si es necesario, creando varios escenarios para fines de estudio explicando y contestando todas las inquietudes expuestas en el proyecto.

CAPÍTULO 2

2. FUNDAMENTO TEÓRICO

2.1 INTRODUCCIÓN A SNMP

SNMP (simple network management protocol) es un protocolo que nos permite recabar información y administrar un equipo en forma remota, como su nombre lo indica, en forma simple, muy útil para saber el estado de diferentes dispositivos como: ruteadores, conmutadores (switches), servidores, estaciones de trabajo, dispositivos móviles, hub, pc, impresoras, ups, etc. en una red, incluso es posible manipular a través de él cualquier dispositivo que maneje SNMP, como lo muestra a continuación la figura 2.1.

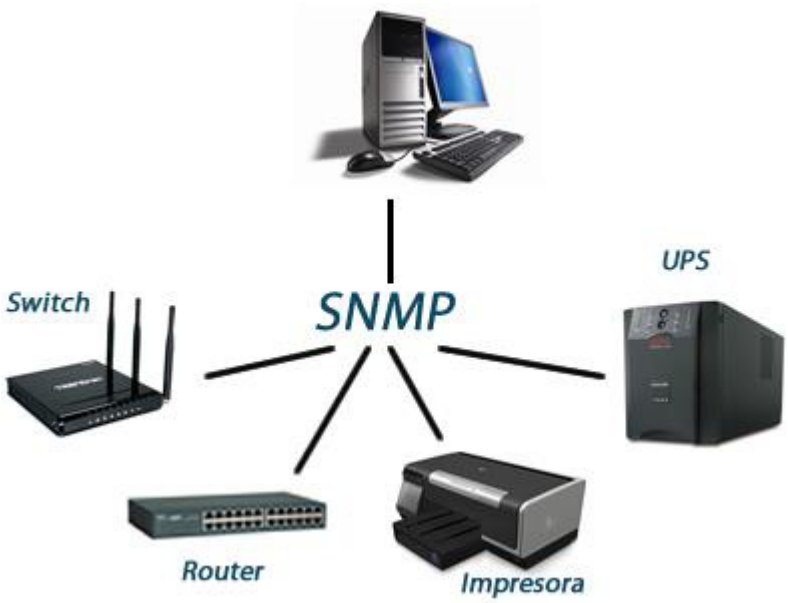


Figura 2.1: Protocolo SNMP [25]

Gestionar una red, es uno de los temas más controvertidos en teleinformática, ya que, prácticamente, no existe una solución única, aceptada por todos y que sea fácilmente implantable. Las soluciones existentes suelen ser propietarias -Netview de IBM, OpenView de HP, etc.- lo que hace que en una red compleja, formada por equipos multifabricante, no exista un único sistema capaz de realizar la gestión completa de la misma, necesitándose varias plataformas -una por cada fabricante-, lo que dificulta y complica enormemente la labor del gestor de red; con la idea de presentar una solución única, válida para cualquier tipo de red, varios grupos de normalización están trabajando en ello y, aunque hay dos tendencias claras (SNMP para redes de empresa y CMIS/CMIP para redes públicas), SNMP es la que está consiguiendo una aceptación e implantación amplia, por su sencillez y rapidez de desarrollo. [1]

2.2 ARQUITECTURA DE SNMP

SNMP es un protocolo que provee una comunicación amena entre la estación administradora y el agente de un dispositivo de red llamado también nodo administrativo, accediendo que los agentes transfieran datos estadísticos (variables), mediante una red a la estación de administración. [2]

2.2.1 Propósito de la Arquitectura

SNMP exclusivamente ayuda a la reducción de número y grado de dificultad de las funciones de gestión que son hechas por el mismo agente de gestión, que como sabemos va aumentando remotamente el soporte de funciones de gestión, facilitando en su totalidad los recursos del internet en la tarea de gestión, para la facilidad de entendimiento, usados por los autores de herramientas de gestión de red. [3]

2.2.2 Elementos de la arquitectura

La arquitectura SNMP expresa una solución al inconveniente de gestión de redes en términos de los siguientes puntos:

- Representación de la información de gestión comunicada por el protocolo.
- Importancia de la información de gestión comunicada por el protocolo.
- Forma y significado de los cambios entre entidades de gestión.

- Operaciones toleradas por el protocolo en la información de gestión.
- Forma y significado de las referencias a la información de gestión.

2.3 SNMP: ESPECIFICACIONES DEL PROTOCOLO

SNMP facilita un mecanismo para poder acceder a los objetos de MIB (Management Information Base) que es la base de datos donde se encuentra toda la información que se gestiona, y así ser consultados y hacer cambios, también hace que los dispositivos que están conectados a la red envíen mensajes que no han sido solicitados a una estación de gestión SNMP y así avisar que se ha producido alguna situación.

SNMP como tal define cinco tipos de mensajes de intercambio entre gestor y agente que se llaman PDU's (Unidad de datos de Protocolo). [4]

2.3.1 Elementos de procedimiento

A continuación daremos especificación a las acciones que se realizan en una entidad de protocolo de implementación SNMP, por lo tanto diremos que dirección de transporte es como una dirección IP seguida de un número de puerto UDP.

Cabe recalcar que el software que tiene el cargo de la gestión de la red en las estaciones de gestión pueda tener acceso a la información

de los elementos de la red, es preciso que estos elementos posean un software que permita su comunicación con la estación de gestión. Y por ende a este software se le denomina agente.

Por lo tanto, se pueden distinguir los siguientes elementos:

- Agente de gestión. (Agente)
- Gestor (Manager)
- Objeto gestionado
- Protocolo de gestión.

El agente de gestión: es el que supervisa a un elemento de la red; éste se comunica con el gestor para tener en cuenta sus peticiones e informarle de eventos acaecidos en el objeto gestionado. El agente de gestión puede estar físicamente en el elemento gestionado.

El gestor: es un software que está en una estación de gestión que se comunica con los agentes y que ofrece al usuario una interfaz para poder comunicarse con los agentes de gestión y así tener información de los recursos gestionados. Además recibirá las notificaciones enviadas por los agentes.

Los objetos gestionados: son las abstracciones de los elementos físicos de la red que se gestionan como por ejemplo tarjeta de red, concentrador, módem, router, etc. También se puede manipular los atributos y las operaciones que se pueden hacer sobre el objeto, de la misma manera, las notificaciones que el objeto pueda generar así

como las relaciones con otros objetos que también son susceptibles de ser controladas. Y algo muy importante que hay que tomar en cuenta es la base de datos de gestión (MIB) que está formada por todos los objetos gestionados, siendo un archivo de texto que nos describe toda la información que podemos obtener o manipular en determinado dispositivo; cada dispositivo debe de tener su propia MIB. La MIB describe toda esa información en una estructura jerárquica de árbol. [25]

Protocolo de gestión: es el protocolo que describe cómo se realizará la comunicación entre los agentes de gestión y el gestor. Para nuestra tesis seria el protocolo SNMP. La comunicación que se hace es por medio de requerimientos, respuestas y notificaciones. [5]

2.3.2 Definición de un Mensaje

Un mensaje tiene como elemento un identificador de versión, un nombre de comunidad y una PDU (Protocol Data Unit). SNMP define cinco tipos de mensajes:

- Get Request: Para leer el valor de una o varias variables del MIB.
- Get Next Request: Para realizar lecturas secuenciales a través del Mffi.
- Get Response: Es el mensaje de respuesta a un Set Request, Get Request o Get
- Set Request: Mensaje enviado para establecer el valor de una variable.

- Trap: A través de este mensaje se hacen notificaciones de eventos.

Estos cinco tipos de mensajes SNMP son encapsulados en datagramas UDP. Los mensajes de petición y respuesta son enviados al puerto 161, mientras que las notificaciones de eventos usan el puerto 162.

La definición de un mensaje SNMP en ASN.1 es la siguiente:

Message: = SEQUENCE {
Version INTEGER
Community OCTET STRING,
Data ANY
}[5]

2.3.2.1 Estructura de una PDU

PDU´s contiene un comando específico como: Get, Set, etc. así mismo operandos, los cuales detallan las instancias del objeto que están implicados en la transacción. Los campos PDU de SNMP son de longitud variable, según lo especificado por ASN.1. A continuación se muestra en la figura 2.2 la estructura de PDU.

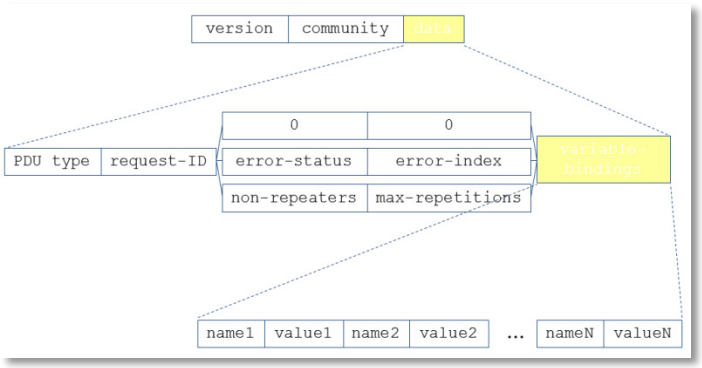


Figura 2.2: Explicación de estructura PDUs [6]

A continuación los componentes de una PDU:

PDU Type: Especifica el tipo de PDU transmisión

Request ID: Relaciona las solicitudes y respuestas SNMP; es decir es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes de manera simultánea.

Error Status: Muestran uno (1), de una serie de errores y los tipos de errores. Únicamente la operación de Respuesta fija o pone (SETS) este campo. Otras operaciones colocan (SET) este campo en Cero (0).

Error Index: Relaciona un error con una instancia de objeto en particular. Solamente la operación de respuesta pone (SETS) este campo, otras operaciones ponen este campo en Cero (0).

Estado e índice de error: Sólo se utilizan en los mensajes GetResponse (en las consultas siempre se utiliza cero). El campo "índice de error" sólo es usado cuando "estado de error" es diferente de 0 y tiene como objetivo de proporcionar información

adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:

- 0: No hay error;
- 1: Demasiado grande;
- 2: No existe esa variable;
- 3: Valor incorrecto;
- 4: El valor es de solo lectura;
- 5: Error genérico

Variable Bindings: Actúa como el campo de datos de la PDU SNMP, es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1), tal como se muestra a continuación en la figura 2.3.

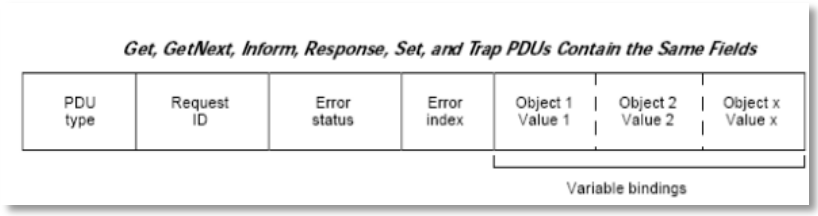


Figura 2.3: Descripción del campo de datos. [7]

2.3.2.1.1 GetRequest-PDU y GetNextRequest-PDU

Son PDU's que piden a la entidad destino los valores de ciertas variables. En el caso de GetRequest-PDU estas variables están ubicadas en la lista VarBindList; en el de GetNextRequest-PDU los nombres son sucesores lexicográficos de los nombres de las variables de la lista. Como notamos, GetNextRequest-PDU es ventajoso para la creación de tablas de información sobre un MIB.

Siempre tienen cero los campos ErrorStatus y ErrorIndex. Sólo cuando lo solicita su entidad de aplicación SNMP, son generadas por una entidad de protocolo.

Estas PDU's siempre esperan como respuesta una GetResponse-PDU.

GetRequest-PDU:

Con esta PDU se puede requerir el valor sea de una o más variables. Dichas variables que se desea conocer su valor se listan en variable-bindings. Como respuesta se recibe una PDU de tipo GetResponse, con los valores de las variables requeridas, que están establecidos en variable-bindings o si hubiera algún error, éste se identificaría con error-index y asi identificar qué variable falló, y error-status para saber cuál fue el fallo o error. El campo request-id de la PDU GetResponse tendrá el mismo valor que en GetRequest, para que la aplicación puede asociar la respuesta con la petición.

Suelen pasar los siguientes errores:

- Cuando se hace una petición en la que la referencia a un nombre de variable no conoce el receptor, este o sea el receptor indicara en error-index qué variable causó el error, mostrando en error-status "noSuchName".
- Cuando se recibe una respuesta que es demasiado grande para el sistema local, se devolverá el mensaje de respuesta con error-index puesto a 0 y error-status establecido a "tooBig".
- Si el agente no puede obtener el valor de una variable por alguna razón distinta a las previstas por el protocolo, enviará el mensaje de respuesta con el campo errorindex apuntando a la variable que causó el error y el campo error-status establecido a "genErr".

GetNextRequest-PDU:

Con esta PDU se solicita el valor de la siguiente variable a la indicada o indicadas, suponiendo un orden léxico.

Pueden darse las siguientes situaciones de error:

- Cuando no hay un sucesor léxico para alguna variable de las indicadas en variable-bindings, se devuelve en error-status el valor "noSuchName" y error-index que indicará qué nombre de variable falló.
- Si la respuesta recibida es demasiado grande, como en el caso de la PDU anterior se devolverá la respuesta con

el campo error-status indicando "tooBig" y error-index a 0.

- No se puede obtener el valor de la variable sucesora a alguna de las indicadas en variablebindings, este se enviará la respuesta con error-index indicando qué variable fallo.

2.3.2.1.2 SetRequest-PDU

Con esta PDU se pide el establecimiento del valor de la variable o variables que digamos en variable-bindings. Si no llega a ver errores el receptor devuelve una PDU de tipo Response con el campo error-status establecido a NoError y error- index a 0.

Existen diferentes tipos de errores:

- Si el receptor no haya alguna variable de las dichas en variable-bindings, indicara en la respuesta el error "noSuchName" en el campo error-status, y mostrara qué variable falló en error-index.

- Si se intenta establecer un valor que no es acorde al tipo de la variable, entonces el receptor devolverá en la PDU de respuesta el error "badValue" en error-status y mostrara qué variable falló en error-index. "

- Cuando reciba alguna respuesta que es demasiado grande y que no se puede tratar, entonces se devolverá con el error "tooBig" en error-status y error-index a 0.

- Al haber algún error no especificado en el protocolo se devolverá una PDU de respuesta con el valor "genErr" en el campo error-status y un 0 en error-index.

2.3.2.1.3 GetResponse-PDU

Esta PDU se genera como respuesta a las PDUs de tipo GetRequest, GetNextRequest y SetRequest.

2.3.2.1.4 Trap-PDU

Las PDU de tipo Trap admiten a los agentes comunicar de manera asíncrona a los gestores cualquier evento que le esté pasando al objeto gestionado y en el cual el gestor tiene interés de ser informado. El campo generic-trap indica que un evento ha ocurrido, como lo describe la figura 2.4.

Evento	Significado
coldStart	El dispositivo se ha reiniciado, con lo que que la configuración del agente ha podido cambiar
WarmStart	El dispositivo se ha reiniciado, pero el agente sigue intacto
LinkDown	El dispositivo ha detectado un fallo en uno de sus enlaces de red. El enlace que falla es especificado en el campo variable-bindings
LinkUp	El dispositivo ha detectado que uno de sus enlaces con la red se ha activado. El nombre del enlace y el valor de la variable ifIndex aparecen en el campo variable-bindings
AuthenticationFailure	El agente ha detectado un fallo en la autenticación del mensaje
EgpNeighborLoss	Uno de los nodos colaboradores EGP se ha caido. El primer elemento del campo variable-bindings es el nombre y valor de la variable egpNeighAddr del nodo afectado
EnterprisesSpecific	Evento de un fabricante particular. El evento se identifica con el campo specific-trap

Figura 2.4: Eventos relacionados a SNMP [5]

Los únicos campos que permanecen sin comentar son agent-addr, que aclara cual es la dirección de red del objeto que está diciendo la notificación, y time-stamp que indica el tiempo transcurrido desde la última inicialización de la entidad de red y la generación de la notificación.

2.3.3 Definición de Comunidad

Se denomina comunidad (community) a un conjunto de gestores y a los objetos gestionados. A las comunidades se les asignan nombres, de tal forma que este nombre junto con cierta información adicional sirva para validar un mensaje SNMP y al emisor del mismo.

Así, por ejemplo, si se tienen dos identificadores de comunidad "total" y "parcial", se podría definir que el gestor que use el identificador "total" tenga acceso de lectura y escritura a todas las variables de la base de administración de información, MIB (Management Information

Base), mientras que el gestor con nombre de comunidad "parcial" sólo pueda acceder para lectura a ciertas variables del MIB. [5]

2.4 GESTION INTERNET- PROTOCOLO SNMPV2

2.4.1 Antecedentes

Surge la necesidad de cubrir algunas deficiencias del SNMP original, conocido como SNMPv1. Para esto SNMPv2 se compone de dos iniciativas las cuales fueron terminadas a mediados de 1992 como lo son: “Secure SNMP” y “Simple Management Protocol (SMP)”, es decir, mejorar la seguridad de SNMPv1 y adquirir nuevos aspectos de gestión respectivamente, mostrado en la figura 2.5. Evidenciando así un nuevo y útil protocolo en donde no posee características de seguridad pero que sí potencia en funcionalidad y rendimiento de SNMP. Por tal motivo es que SNMPv2 es la evolución natural de SNMPv1 ya que por su grado de complejidad la hace más difícil de implementarla y que su uso se extienda rápidamente, pero hace que los usuarios trabajen en una versión mejorada. Adicionalmente, para poder cubrir los mismos aspectos que intentaba abarcar SMP, y así mejorar SNMP, se hace presente RMON (Remote Network Management) que es una herramienta que brinda la capacidad para observar la red como un todo. [8]

Finalmente SNMPv2 es presentado en Marzo de 1992 en las RFCs1441-1452 (actualmente obsoletas), en donde se proporcionan nuevas PDU(Protocol Data Unit), la cual es el medio para enviar

peticiones y recibir respuestas, es así como esta nueva versión ofrece mejoras modestas de seguridad a través del cifrado DES (Data Encryption Standard). [9]

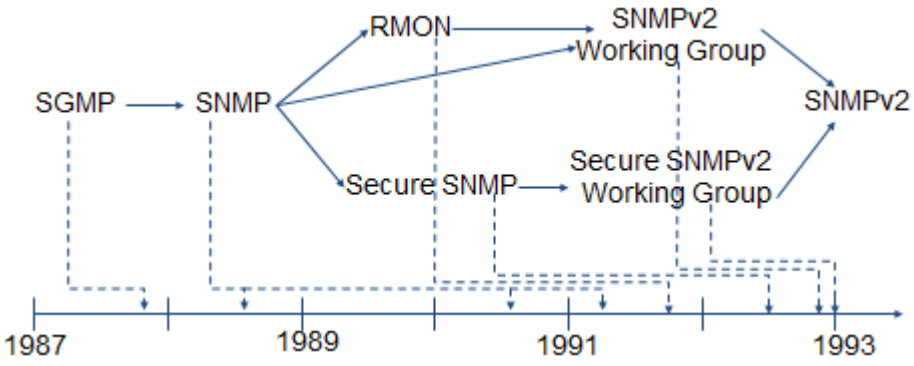


Figura 2.5: Resumen de la evolución histórica de SNMPv2 [6]

2.4.2 Arquitectura

2.4.2.1 Características

Entre las características sobre el protocolo SNMPv2 tenemos detalles sobre capacidades, ya sea sobre los sistemas en el modo de operar tanto como agente o como gestores y la capacidad de comunicación conocida como gestor-gestor la cual es posible jerarquizar la gestión.

SNMPv2 posee una mejora en los PDU's ya que al momento de entregar los mensajes se entregan con mayor facilidad, sin tener comandos extras como lo tenía la versión 1 (SNMPv1), también

esta versión soporta una señalización extendida de errores y permite el uso de varios transportes, a esto es lo que denominamos mayor eficiencia en la transferencia de la información. [8]

En base a esta información sacamos tres categorías claves de características, como lo son:

Estructura de la información de Gestión (SMI), Capacidad de interacción Gestor-Gestor y Operaciones de Protocolo.

- **Estructura de la información de Gestión (SMI)**

  SNMPv2 recoge toda la estructura de formación de gestión proveniente del SNMPv1, con documentación más elaborada y especificaciones de los objetos gestionados y MIBs. Entre las principales mejoras tenemos las nuevas definiciones de objetos a las cuales se le añaden nuevas síntesis, como lo son Integer32 que es usada para un complemento de 2 a 32 bits, UInteger32 empleada para números naturales hasta 32 bits, BitString con numeración de bits en octetos, Counter32 con un contador más amplio, NSAPAddress la cual tiene direcciones OSI y finalmente Counter64 si el que de 32 bits se llena en menos de una hora.

  A todas estas se le añade una cláusula adicional UNITS la cual indica la unidad de medida asociada con un objeto de medida, para esto tenemos 4 tipos de acceso:

- Not-accesible
- Read-only
- Read-write
- Read-creat
- Accesible-for-notify

Por otro lado tenemos las nuevas características de semántica bien conocida como Macros, ésta permite añadir información semántica a una MIB y no afecta a la interoperabilidad (véase figura 2.6), es decir, SNMPv2 es incompatible con SNMPv1 en dos áreas clave: el formato de los mensajes y las operaciones de protocolo, los mensajes SNMPV2 hacen uso de encabezados (header) y formatos PDU´s muy diferentes a los mensajes del protocolo SNMPV1. [7]

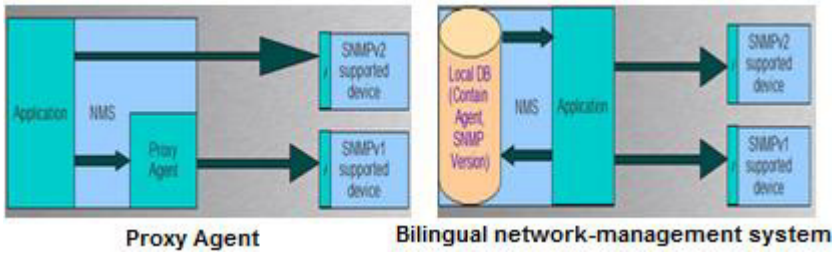


Figura 2.6: Interoperabilidad entre SNMPv1/v2 [10]

Por otra parte, RFC 1908 define dos posibles estrategias de coexistencia SNMPv1/v2: Proxy Agents y Bilingual

network management systems, como se muestra en la figura 2.6 [7]

A esto es lo que se denomina una nueva definición de una Macro para las notificaciones que incluye información adicional de referencia a otros elementos de la MIB (NOTIFICATION-TYPE macro).

Finalmente los módulos de información, definiciones y funciones para el manejo específico de tablas son otras de las mejoras que posee este nuevo sistema de información de gestión de SNMPv2.

- **Operaciones de Protocolo**

  Para el protocolo de SNMPv2, se conoce que las PDU van encapsuladas en un mensaje. En la cabecera de dicho mensaje se determinan cuáles serán las políticas de autenticación y autorización.

  Los mensajes de SNMPv2 proporciona la funcionalidad limitada para las características de seguridad. El protocolo SNMPv2 provee tres tipos de acceso a la información de gestión:

  - Gestor-Agente Request-Response
  - Gestor-Gestor Request-Response
  - Agente-Gestor unconfirmed

Para esto SNMPv2 añade algunos cambios (véase figura 2.7) con respecto a SNMPv1.

Figura 2.7: Características dirigido a SNMPv2 [13]

A continuación tres nuevos tipos de PDU:

GetBulkRequest: Es la que permite la recuperación de tablas de una manera más eficiente, es decir, minimiza el número de intercambios. Actúa de forma parecida a GetNextRequest, solo que esta nueva mejora hace posible indicar varios sucesores a uno dado. Para esto añadimos dos nuevos parámetros de PDU dentro de la misma.

- non-repeaters: Numero de variables de la lista a la cual se le realizara una recuperación simple.
- max-repetitions: Es el número de veces que equivale de las recuperaciones múltiples [11]

SNMPv2-Trap: Este tipo de PDU reemplaza al trap de la versión 1, a pesar de que su función es la misma existen una ligera variación en los campos del PDU:

- Este tipo de mensaje no posee ningún tipo de confirmación asociada.
- Con respecto a los campos Generic Trap Type y Specific Trap Type ya no son utilizados en esta nueva versión ya que aparece uno nuevo llamado TrapOID, el cual consiste en la unión de los dos anteriores.
- La lista variable-binding posee dos variables llamadas sysUpTime y snmpTrapOID. Después de esto se puede añadir las VariableBindings que se deseen envía, como se lo solicitaba en el Trap-PDU de SNMPv1.

    - ✓ SnmpTrapOID: Es de tipo OBJECT IDENTIFIER el mismo que ha sido definido en el RFC 3418 [21]. Es una secuencia de enteros que codifica un algoritmo, tipo de atributo o tipo definido procedente de una autoridad de registro (registration authority), el mismo que se lo utiliza como una identificación de la notificación actual que se envía.
    - ✓ SysUpTime: Este proviene de un tipo de timeTicks, definido en el RFC 3418[21]. Es una

medida del tiempo transcurrido (cada unidad representa la centésima parte de un segundo) desde que la región de la red, en la que está el proceso que genera un valor, fue reinicializada por última vez [12]

InformRequest: Establece comunicaciones entre gestores las cuales se configuran mediante la M2M MIB. Para esto tenemos dos tipos de comunicaciones, la que es por la ocurrencia de algún evento y la que es a petición de algún gestor.

- **Capacidad de interacción Gestor-Gestor**
  Este tipo de acceso radica en un incorporado conjunto de objetos que describen el comportamiento de una entidad SNMPv2 que funciona como gestor. Mediante esta capacidad de interacción, la MIB establece comunicaciones entre gestores SNMPv2. [11]

2.4.2.2 Clasificación

El protocolo de SNMPv2, el mismo que no trabaja bajo ningún estándar en cuanto a seguridad, se ve la necesidad de asociarse con otros modelos administrativos bajo el concepto de objetos, los mismos que se agrupan en MIBs, a lo que tenemos la clasificación de tres nuevas versiones del protocolo: SNMPv2c, SNMPv2*, SNMPv2u.

La versión SNMPv2c (Community-based SNMPv2), es la única mejora introducida ya que posee una mayor flexibilidad de los mecanismo de control de acceso, la misma que permite la definición de política de acceso consistente en relacionar un nombre de comunidad con un perfil de comunidad realizado por una vista MIB y unos derechos de acceso a dicha vista (read-only o read-write), es aquí donde aparece las denominadas view, ya que esta nos puede dar acceso a una community concreta.

La versión SNMPv2* realiza cambios en su modelo administrativo, para poder introducir los conceptos de integridad y privacidad, dando hincapié a un sistema de seguridad la cual consiste en mejorar el control de acceso a la información. Esta versión posee niveles de seguridad adecuado, pero no alcanzo el nivel necesario de estandarización, por ende no fue expuesta a los usuarios a manera de uso.

La versión SNMPv2u (User-based SNMPv2) es la que introduce la noción de usuario, inclusive ha sido una de las versiones más usadas, ya que ha llevado a un avance en la remodelación de este protocolo y que dio lugar finalmente a la versión tres de este protocolo (SNMPv3). [1]

2.4.3 Aplicaciones de SNMPv2

Cuando un usuario requiere una aplicación del protocolo SNMPv2, puede ser conveniente para el usuario ya que puede especificar la cantidad mínima de información a utilizarse en el momento que requiera establecer y mantener comunicaciones SNMPv2. El modelo asumido en la presente nota hace referencia a que el usuario tendrá un mejor control de lo que está ingresando y el resultado del mismo.

Por otra parte, SNMPv2 introduce algunas nuevas posibilidades a la versión de SNMPv1, de las cuales la que más resalta a manera de uso a los servidores es la muy conocida operación **Get-bulk.** Esta permite que se envíe un gran número de entradas MIB en tan solo un mensaje, en vez de necesitar múltiples consultas **Get-next** para SNMPv1. Por consiguiente SNMPv2 posee mayor seguridad que SNMPv1 ya que es capaz de detener intrusos que quieran observar el estado o condición de los dispositivos administrados, de manera que la encriptación y la autentificación están soportadas por SNMPv2, a esto surge la idea de decir que SNMPv2 es un protocolo más complejo y no es tan fácil el uso para los usuarios como lo es SNMPv1. [14]

2.4.4 Coexistencia entre SNMPV1 y SNMPV2

Cuatro unidades de datos de protocolo (PDU) son los que se comparten entre SNMPv1 y SNMPv2, es decir el establecer valores de los datos en los dispositivos gestionados y recuperarlos.

Las PDU del protocolo SNMP como GetRequest, GetNextRequest o GetResponse sirven para obtener datos desde un dispositivo gestionado, mientras que la PDU SetRequest establece el valor en un dispositivo dado. Cuando hablamos de la recuperación respectiva de SNMPv1 es un tanto complejo, ya que solo se basa en las iteraciones repetidas del GetNextRequest. Mientras que SNMPv2 agiliza este proceso ya que posee su PDU “GetBulkRequest”, el mismo que puede recuperar una cantidad grande de datos con tan solo una iteración.

Es importante hablar de la seguridad existente entre ambas versiones. Por un lado tenemos que en SNMPv1 los nombres de comunidad están encriptados, por lo que el acceso completo a la red puede obtenerse con facilidad por cualquier entidad o persona capaz de jaquear el sistema. Por otro lado SNMPv2 utiliza la tal denominada Data Encryption Standard, que es la que proporciona una mayor seguridad de paquetes y cada cabecera de PDU posee los datos de autenticación que confirman que los dispositivos, que participan en un intercambio que es cuando el PDU solicita una red legitima.

Finalmente se tiene que SNMPv1 no es compatible con las nuevas PDU de SNMPv2, pero los administradores de red tienen nuevos métodos para evitar estos problemas ya que existen redes que usan ambas versiones. A la ayuda de los PDU, un agente proxi v2 traduce PDUv2 en mensajes de un agente PDUv1 para poder entenderlo y ejecutarlo. La instalación también puede utilizar un NMS bilingüe, esta mantiene una base de dato indicando que la versión SNMP está

utilizando un dispositivo y las cuestiones de las comunicaciones SNMP oportunas a cada nodo de la red. [15]

2.5 SEGURIDAD

2.5.1 SNMP Seguro (S-SNMP)

SNMP no proporciona mecanismos de seguridad, es decir, no es capaz de identificar y autentificar la fuente de un mensaje de gestión para prevenir posibles alteraciones.

Un intruso puede observar un mensaje y leer su nombre de comunidad para posteriormente enviar mensajes modificando parámetros de configuración de un dispositivo. Por ello, muchos fabricantes no implementan el comando SetRequest.

Existen cuatro requerimientos básicos de un sistema seguro:

- Confidencialidad: Acceso a información no autorizada.
- Autenticidad: Identificación correcta del origen de un mensaje.
- Integridad: Modificación de datos no autorizados.
- Disponibilidad: Interrupción del correcto funcionamiento de los dispositivos.

Existen a su vez cuatro tipos de amenazas:

- Interrupción: Se interrumpe o destruye la disponibilidad de un recurso.

- Intercepción: Una entidad no autorizada accede a un recurso.
- Modificación: Se modifican los parámetros o datos de un recurso.
- Enmascaramiento: Una entidad se hace pasar por otra.

Estas amenazas la podemos clasificar, a su vez, en pasivas (observación del contenido de un mensaje y análisis del tráfico) y activas (enmascaramiento, replicación, modificación de mensajes y denegación de servicios). Las pasivas son más difíciles de detectar pero menos malignas. [16]

2.5.2 Seguridad con SNMPv2

Este es el campo en donde SNMPv2 se ha esmerado con respecto a SNMPv1 es decir es el mayor cambio que éste ha realizado, ya que el usuario tiene la opción de poder dotar de privacidad y autentificarse. Además introduce el concepto de grupo proveniente de S-SNMP (Security SNMP), ésta se ubica en la cabecera del mensaje de información del contexto (vista MIB) sobre el que actuara el mensaje.

En la figura 2.8, encontraremos un formato del mensaje en SNMPv2, visualizando los campos del mismo mensaje que son norma dentro del formato.

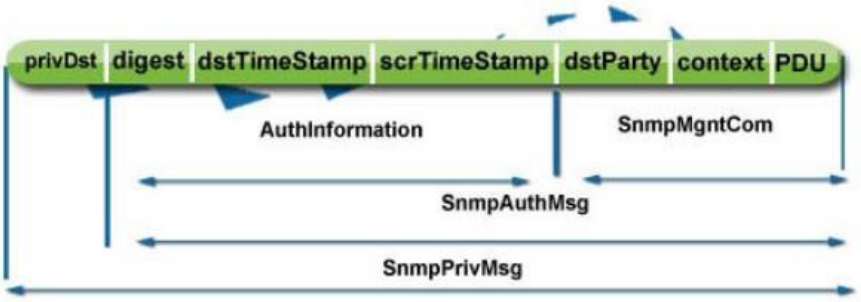


Figura 2.8: Formato del mensaje SNMPv2 [17]

Cabe destacar que en este sentido de seguridad, los efectos de poder mostrar los esquemas provistos por la versión dos de SNMP, es necesario implementar el proceso para generar un mensaje SNMP que se describe a continuación.

2.5.2.1.1 Proceso para generar un mensaje SNMP v2

Para realizar un mensaje SNMP v2 se lleva el siguiente proceso:

1. Se construye el valor del SnmpMgmtCom donde:
   - PDU: representa la operación de gestión deseada.
   - context: indica la vista MIB sobre la que se actuará.
   - dstParty: identifica al destino.
   - srcParty: identifica la parte origen.

2. Se construye el valor de SnmpAuthMsg donde:
   - authDigest: resumen generado por MD-5 en la parte origen.

- authSrcTimestamp: indica el clock del origen.
- authDstTimestamp: indica el clock del destino.

3. Se encripta el SnmpAuthMsg.

4. Se coloca en el campo privDst de SnmpPrivMsg el identificador de la parte destino.

2.5.2.1.2 Proceso de recepción de un mensaje SNMP v2

Para realizar el proceso de recepción de un mensaje SNMP v2 se deben contemplar los siguientes pasos:

1. Si el privDst no es válido, se rechaza el mensaje.
2. Se desencripta el privData para obtener el SnmpAuthMsg.
3. Se rechaza el mensaje si no casa el privDst con dstParty o se desconoce el srcParty.
4. Se rechaza el mensaje si no cuadran los Timestamp dentro del margen.
5. Se extrae el valor del authDigest y se compara con el nuevo cálculo.
6. Se consulta el contexto para ver si la operación solicitada es posible [17]

CAPÍTULO 3

3. DESARROLLO E IMPLEMENTACIÓN VIRTUAL DEL PROYECTO

3.1 DESCRIPCIÓN

Para el desarrollo de este proyecto se procederá a diseñar, implementar y simular una red virtual basada en la arquitectura del protocolo SNMPv2, habilitando su estación de gestión, la misma que será una estación real lógica (PC anfitrión) mediante el software de simulación de redes GNS3.

En esta estación real lógica se podrá monitorear toda la red a través del software OpenNMS y posteriormente mostrar detalladamente el comportamiento del sistema. Además utilizaremos el capturador de

paquetes Wireshark para analizar el protocolo de administración SNMPv2.

Con este proyecto se pretende obtener un método de aprendizaje para entidades educativas que no poseen equipos, puesto que son muy costosos, además este sistema permite evaluar con simulación orientada a la realidad. Es por ello que el diseño de la red estará constituido de tres redes LAN, denominadas Guayaquil, Quito, Cuenca con sus respectivas direcciones IP; es decir tendremos tres ruteadores encargados de operar el sistema.

También se realizará subnetting para crear subredes de las redes principales y poder configurar los elementos de la red, asignando las direcciones IP a cada dispositivo de la red.

Se implementará el protocolo de enrutamiento OSPF para establecer la conexión de los ruteadores. A diferencia de otros sistemas de enrutamiento, OSPF puede operar dentro de una jerarquía. La entidad más grande dentro de una jerarquía es lo que llamamos sistema autónomo (AS). El AS es un grupo de redes bajo una administración común que comparte una estrategia de enrutamiento. El protocolo OSPF es interno en el AS, aunque es capaz de recibir y enviar rutas a otros sistemas autónomos.

Por otra parte, a través de la estación real, la herramienta de monitoreo y el analizador de paquetes se obtendrá información detallada del protocolo

SNMPv2 y del estado de la Red, destacando sus capacidades las mismas que reflejarán las ventajas y desventajas de dicho protocolo.

3.2 SOFTWARE DE SIMULACION

3.2.1 GNS3 (Graphical Network Simulator)

GNS3 es un software de código abierto que permite simular redes complejas, además brinda servicio orientado al funcionamiento de las redes reales, todo esto sin necesidad de hardware de red, como routers y switches. [18]

Este software proporciona una interfaz gráfica de usuario intuitiva para diseñar y configurar redes virtuales, que se ejecuta en hardware de PC tradicionales y se puede utilizar en múltiples sistemas operativos, incluyendo Windows, Linux y MacOS X.

GNS3 es una excelente alternativa y una herramienta complementaria a los laboratorios reales para ingenieros en redes, administradores y personas que estudian para certificaciones como Cisco CCNA, CCNP y CCIE.

Por último, gracias al apoyo VirtualBox, incluso los administradores de sistemas e ingenieros pueden aprovechar GNS3 para hacer los laboratorios, las características de la red de ensayos y estudios para Redhat (RHCE, RHCT) y certificaciones de Microsoft (MCSE, ACEM).

A fin de proporcionar simulaciones completas y precisas, GNS3 utiliza los siguientes emuladores para ejecutar los mismos sistemas operativos como en redes reales:

- **Dynamips,** programa que permite la emulación de Cisco IOS.
- **Dynagen,** es un texto basado en front-end para Dynamips.
- **Qemu,** máquina emuladora y virtualizadora de código abierto.

En la Figura 3.1, se muestra la unión de Dynamips-Dynagen-GNS3, que crea una plataforma, permitiendo el fácil diseño de topologías de red complejas, puesto que se realizan tan sólo arrastrando los componentes y dibujando líneas entre routers de forma intuitiva. Por lo tanto, GNS3 es idóneo para el entrenamiento de estudiantes que desean familiarizarse con dispositivos de red.

Figura 3.1: Plataforma GNS3 [13]

Debido a la importancia de sus componentes es necesario detallar los emuladores antes mencionados que utiliza el software GNS3.

3.2.1.1 Dynamips

Dynamips, fue realizado por Christophe Fillot que comenzó su labor en agosto de 2005. La última versión oficial de Dynamips soporta Cisco 7200, 3600 series (3620, 3640 y 3660), serie 3700 (3725, 3745), serie 2600 (2610 a 2650XM, 2691) y la serie 1700. [18]

Según Christophe Fillot el emulador GNS3 será útil:

- Para utilizarlo como una plataforma de entrenamiento, utilizando software del mundo real. Esto permitiría que la gente se familiarice con los dispositivos de Cisco, debido a que Cisco es el líder mundial en tecnologías de redes.
- Probar y experimentar las características de Cisco IOS.
- Comprobar y verificar configuraciones que en lo posterior se pueden implementar en equipos reales.

Aunque Dynamips no emula switches Catalyst, provee una versión limitada de un switch virtual, cuyas limitaciones pueden ser resueltas usando métodos alternativos como es la emulación de NM-16ESW (Módulo de switch Ethernet de 16 puertos), es decir es una tarjeta “EthernetSwitch” emulada por GNS3.

Inicialmente Dynamips consume grandes rendimiento dl CPU de la PC en la que se está trabajando, esto se debe a que se está emulando entornos virtuales y no se puede saber cuándo un router virtual está inactivo, de modo que ejecuta instrucciones como si la

imagen del IOS estuviera realizando algún trabajo útil; para resolver el problema del excesivo uso de CPU se crea un proceso llamado IDLE-PC.

El proceso IDLE-PC se trata de una herramienta que realiza un análisis en el código de una imagen IOS para determinar los puntos más probables que representen un bucle de inactividad, de modo que, cuando se detecten, haga que los routers virtuales *duerman* durante ese instante. Es decir, ayuda a Dynamips a emular el estado inactivo de la CPU virtual de un router.

3.2.1.2 Dynagen

Dynagen, fue desarrollado en Python, y es por lo tanto compatible con cualquier plataforma para la que hay un intérprete Python. El diseño es modular, con una API de programación orientada a objetos por separado para la interfaz con Dynamips. [18]

Dynagen, es un front-end utilizada por GNS3 para interactuar con Dynamips. Utiliza un archivo de configuración INI, como un medio de almacenamiento de las configuraciones realizadas de todos los dispositivos emulados. Se encarga de especificar los adaptadores correctos de los puertos, generando y haciendo coincidir los descriptores NIO, que se encargan de la conexión con equipos reales o los puertos en los que trabaja los adaptadores de red.
De igual forma Dynagen permite a los usuarios listar los dispositivos, ejecutar, suspender, reiniciar, determinar y

administrar los valores de idle-pc para realizar captura de paquetes.

3.2.1.3 Qemu

Qemu, es una máquina genérica emuladora y virtualizadora de código libre la misma que puede ejecutar Sistemas Operativos y programas hechos por una máquina sobre una diferente, usando una transferencia dinámica, se consigue un buen rendimiento. [18]

3.2.2 OpenNMS

OpenNMS es una herramienta que permite monitorear y gestionar la red, además es la primera plataforma de aplicaciones de gestión de red de nivel empresarial en el mundo. El Proyecto OpenNMS se inició en julio de 1999 y registrado en marzo de 2000 en SourceForge. Tiene años de experiencia en las alternativas. [19]

Debido a las necesidades requeridas por las empresas y compañías, openNMS fue diseñado desde el primer día para controlar a decenas de miles de dispositivos de última instancia, brindando capacidad, escalabilidad y flexibilidad a la red.

OpenNMS es útil, puesto que está diseñado para ser totalmente personalizable; es decir, poder trabajar en una amplia variedad de entornos de red y a su vez crear una solución única e integrada de gestión. Además, es un software de código abierto y libre, sin pago de

licencias, suscripciones de software o versiones especiales y actualizaciones.

OpenNMS está escrito en Java , por lo que se puede ejecutar en cualquier plataforma con soporte para Java SDK versión 1.6 o superior. Está disponible para los sistemas operativos Windows, Solaris, OS X y para algunas distribuciones de Linux. OpenNMS también requiere del software PostgreSQL para la base de datos.

A OpenNMS se accede a través de una interfaz de usuario basada en web construida en Jetty (Servidor Web). Una integración con JasperReports crea informes de alto nivel de la base de datos y los datos de rendimiento recopilados.

Existen 4 principales áreas funcionales de OpenNMS:

- **Descubrimiento directo y automatizado**; es decir, contiene un sistema de aprovisionamiento avanzado para agregar dispositivos de la red al sistema de gestión.

- **Gestión de eventos y notificaciones**, se basa en una publicación y suscripción de bus de mensajes. Los eventos pueden ser configurados para generar alarmas, los mismos representan un historial de información de la red.

- **Servicio de Monitoreo**, es una de las características de OpenNMS que permite la disponibilidad de los servicios basados en red que se determine.

- **Recolección de Datos**, es la recopilación de datos de rendimiento para una serie de protocolos de red incluyendo SNMP, HTTP, JMX, XML, NSClient, etc. Los datos pueden ser recolectados, graficados y almacenados a través de la base de datos.

3.2.3 VirtualBox

VirtualBox es un software que permite crear máquinas virtuales (VM); es decir admite virtualizar otros sistemas operativos en el sistema operativo anfitrión. Además es un excelente gestor de máquinas virtuales de código libre que permite la ejecución simultánea de varias instancias de máquinas virtuales, albergando diferentes o similares sistemas operativos en cada una de ellas. [20]

Este software es realmente interesante por su versatilidad; es decir, podemos activar los puertos USB e imprimir desde las máquinas virtuales. Al instalar las aplicaciones *Guest Aditions* podemos pasar de un Sistema Operativo a otro, solo con mover el mouse entre las ventanas de cada sistema, también podemos compartir información y documentos entre ambos Sistemas.

3.2.4 Software Wireshark

WireShark es un analizador de paquetes de red, una utilidad que captura todo tipo de información que pasa a través de una conexión. Wireshark es gratis y de código abierto, y se puede usar para diagnosticar problemas de red, efectuar auditorías de seguridad y aprender más sobre redes informáticas. [21]

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

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

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

3.2.5 Sistema Operativo

Los Sistemas Operativos (OS) son el software básico de toda computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario. [22]

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

Windows 7 es el sistema operativo usado en el proyecto a través de VirtualBox, es decir; para la simulación se hará uso de máquinas virtuales y a su vez nos permitirá ejecutar programas como si fueran computadoras reales.

Windows 7 Professional es un sistema operativo desarrollado por Microsoft Corporation, es una de las ediciones de Windows 7. Esta versión está diseñada para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, tablet PC, netbooks y equipos media center que cumplan con el requerimiento de hardware: procesador de 1GHz, 1GB de memoria RAM, dispositivos de gráficos DirectX 9 y 20 GB de espacio libre en el disco duro. [23]

La interfaz que presenta este OS es más accesible al usuario e incluyen nuevas características que permiten hacer tareas de una manera más fácil y rápida, al mismo tiempo realiza menos esfuerzos para lograr un sistema más ligero, estable y rápido.

3.3 ELEMENTOS DE LA RED

Nube.- El elemento “Nube” sirve para enlazar la red virtual con cualquier interfaz de red real lógica de la máquina donde se ejecuta GNS3. Para

que la interfaz real lógica funcione correctamente se debe agregar el adaptador de red para que exista la conexión.

Switch Ethernet.- GNS3 posee integrada la capacidad de emulación de simples switches Ethernet con funcionalidades básicas como la creación de Vlans o el funcionamiento del trunking 802.1q. Por defecto, un switch emulado con GNS3 tiene 8 puertos access configurados en la Vlan1 pero se puede añadir hasta 10.000 puertos, pudiendo ser cada uno de ellos, un puerto de acceso o uno troncal. [24]

En este sentido, si se desea trabajar con switches que poseen más funcionalidades, GNS3 puede emular una tarjeta "EtherSwitch" que pude ser soportada sólo por determinadas plataformas CISCO.

Router c2691.- Este router cuenta con las características que necesitamos para el desarrollo de este proyecto, además cuenta con una memoria RAM de 64MB suficiente para que no se cuelgue el software ya que requiere de muchos recursos de la memoria y procesador de la PC. La Tabla 3.1 muestra las características del Router c2691.

Tabla 3.1Características del Router c2691 [26]

CARACTERÍSTICAS DE MANEJO	
Administración a distancia	RMON
CONDICIONES AMBIENTALES	
Alcance de temperatura operativa	0 - 40 °C
Humedad relativa	5 - 95 %
PROCESADOR	
Built-in processor	1 x 160 MHz
REQUISITOS DEL SISTEMA	
Compatibilidad	IEEE 802.3-LAN, IEEE 802.3U-LAN

Requerimientos mínimos sistema	Cisco IOS 12.2(8)T
PESO Y DIMENSIONES	
Dimensiones: (Anchura x Profundidad x Alto)	454 x 285 x 88 mm
Montaje en bastidor	Opcional
Tipo de forma	Rack-mount
ETHERNET LAN FEATURES	
Full dúplex	✔
ILUMINACIÓN/ALARMAS	
Indicadores LED	Port status, link activity, power, 100M device connected
SEGURIDAD	
Método de autenticación	RADIUS
MEMORIA	
Memoria RAM	64 MB
Número de ranuras disponibles para expansión	5
PROTOCOLOS	
Protocolo de routing	OSPF, BGP
Protocolo de trasmisión de datos	Ethernet, Fast Ethernet
CONECTIVIDAD	
Puertos de entrada y salida (E/S)	2 x network - Ethernet 10Base-T/100Base-TX - RJ-45 - 2 1 x management - console - RJ-45 - 1 1 x serial - auxiliary - RJ-45 - 1
CONTRO DE ENERGÍA	
Requisitos de energía	AC 100/240 V (50/60 Hz)
TRANSMISIÓN DE DATOS	
Tasa de transferencia (máx)	0.1 Gbit/s

VirtualBox guest.- Este dispositivo proporcionado por el simulador GNS3 permite la interacción de máquinas virtuales con los dispositivos de la red, este elemento es el sistema contenido; es decir la máquina virtualizada propiamente dicha que se ejecuta dentro de la plataforma de virtualización del host.

El host o anfitrión es el que contiene la máquina que ejecutará el sistema de virtualización y sobre el que se ejecutarán las máquinas virtuales. Generalmente es una máquina física que funciona directamente sobre el hardware.

3.4 INSTALACIÓN Y CONFIGURACIÓN

Para este proyecto se ha diseñado e implementado una red virtual para el monitoreo desde una estación real hacia un entorno virtual, utilizando el software de simulación de redes GNS3 basado en el protocolo de gestión SNMP y para ello se ha realizado la topología como se muestra en la Figura 3.2; cabe recalcar que la topología es opcional; es decir podrá utilizar y diseñar cualquier topología de red que el usuario crea propicia.

Como se ha mencionado anteriormente se ha diseñado una topología dinámica que sirva como caso de estudio para entidades educativas que por motivos de costo, sus laboratorios no cuenten con quipos CISCO.

La topología ésta diseñada para poner en marcha varios conocimientos de redes como enrutamiento estático y dinámico, subnetting, configuración básica de los routers, configuración de la interfaces, configuración de seguridad etc.

Además implementaremos con una estación real lógica denominada ADMINISTRADOR, como se muestra en la Figura 3.2. Esta estación real lógica es la PC anfitrión es decir la máquina donde se ha diseñado la red virtual, Gracias al software GNS3 decidimos aprovechar y evaluar una

característica muy importante que ofrece dicho emulador que es adaptar una interfaz lógica a través de una tarjeta de red; es decir incluiremos la máquina anfitrión para monitorear todo el sistema. Se explicará detalladamente el proceso para crear la conexión virtual real lógica en el apartado 3.4.1.5

Es importante destacar que nuestra estación real; es decir nuestro Gestor (PC ADMINISTRADOR) será el encargado de ejecutar openNMS a través del Procesador de Comandos de Windows en modo administrador.

A continuación se detallada cuidadosamente el proceso de instalación y configuración.

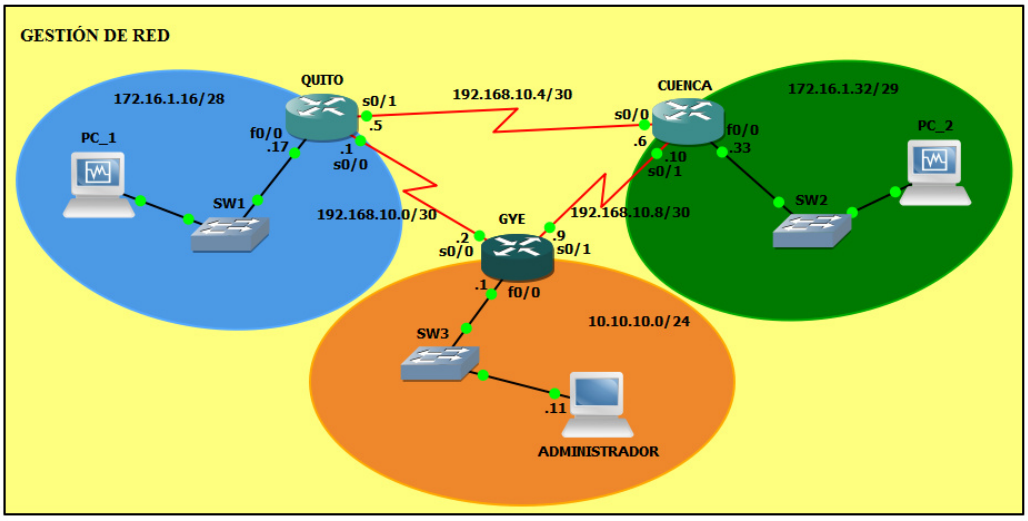


Figura 3.2: Topología de la Red a utilizarse

3.4.1 Instalación y configuración de GNS3

El primer paso para la instalación es descargar el archivo, GNS3-0.8.6-all-in-one.exe (ocupa aproximadamente 59.40MB), que se encuentra en la página web http://www.gns3.net/download. El archivo anterior contendrá la versión binaria de los siguientes programas:

Dynamips 0.2.8 – Dynagen 0.11.0: Ambos programas son la base para el funcionamiento de GNS3.

Pemu 0.2.3: Es un emulador de firewalls PIX de Cisco basado en QEMU que no es más que una máquina emuladora y virtualizadora de código libre.

WinPcap 4.1.3: Permite la comunicación de redes virtuales con redes reales, ya que se encarga de detectar las interfaces reales del PC de trabajo para que el simulador pueda asignarlas como extremo de un enlace hacia un router virtual.

3.4.1.1 Instalar GNS3

Una vez descargado el software GNS3 se procede a dar doble clic en el archivo ejecutable de instalación, se sigue el proceso de instalación de forma habitual; es decir, los valores por defecto de instalación son los que aceptaremos en la misma, a no ser que desee cambiar la ruta de dirección donde se instalará el simulador GNS3. Los pasos para la instalación son:

1) Dar *doble clic* al archivo de instalación .exe. Aparecerá una ventana como la que se muestra en la Figura 3.3. Hacer clic en "*Next*".

Figura 3.3: Proceso de instalación GNS3: Inicio de la instalación.

2) Aceptar la licencia haciendo clic en el botón "*I Agree*" como se observa en la Figura 3.4.

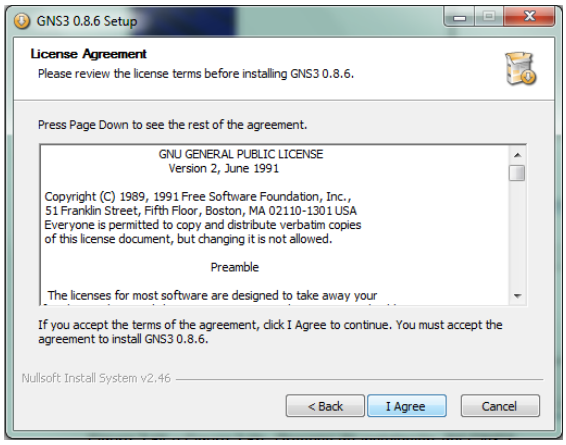


Figura 3.4: Proceso de instalación GNS3: Aceptar licencia.

3) Indicar el nombre del directorio de inicio de GNS3. Seguidamente hacer clic en "*Next*". Ver Figura 3.5.

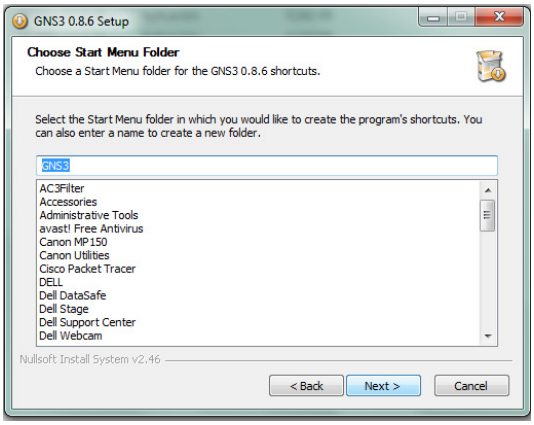


Figura 3.5: Proceso de instalación GNS3: Indicar directorio de inicio.

4) Aceptar todos los componentes que se instalarán por defecto. Hacer clic en "*Next*". Ver Figura 3.6.

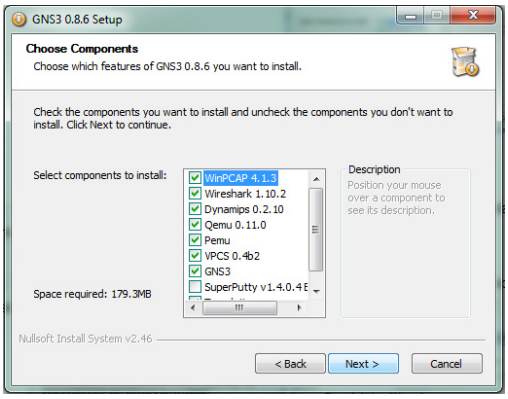


Figura 3.6: Proceso de instalación GNS3: Escoger componentes.

5) Indicar la ubicación del directorio donde se instalará al simulador. Seguidamente hacer clic en "*install*". Ver Figura 3.7.

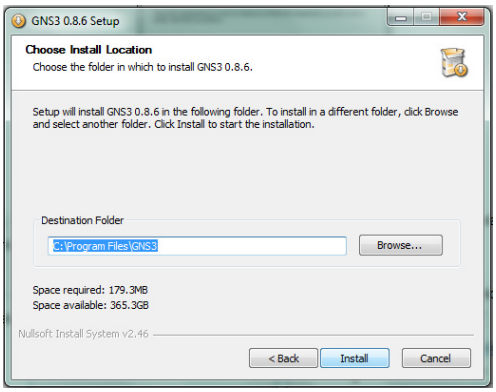


Figura 3.7: Proceso de instalación GNS3: Indicar ubicación de directorio.

6) Antes de concluir la instalación de GNS3, aparecerá la ventana que da inicio a la instalación de WinPcap como se muestra en la Figura 3.8. Hacer clic en "*Next*".

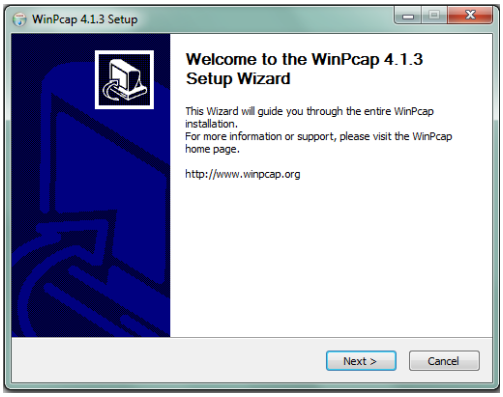


Figura 3.8: Proceso de instalación GNS3: Instalar WinPcap.

7) Aceptar la licencia de WinPcap haciendo clic en "*I Agree*". Ver Figura 3.9.

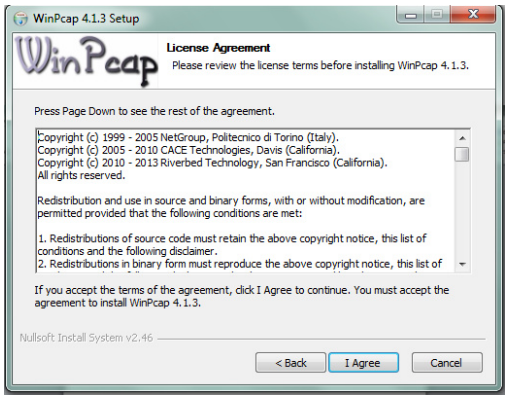


Figura 3.9: Proceso de instalación GNS3: Aceptar licencia de WinPcap.

8) Después de aceptar la licencia de WinPcap, aparecerá una ventana "*Instalation options*" seleccionamos "*Automatically start the WinPcap driver at boot time*" y clic en *"Instal"* como se muestra en la Figura 3.10. Hacer clic en "*Instal*" para proceder con la instalación y esperamos hasta que finalice la misma.

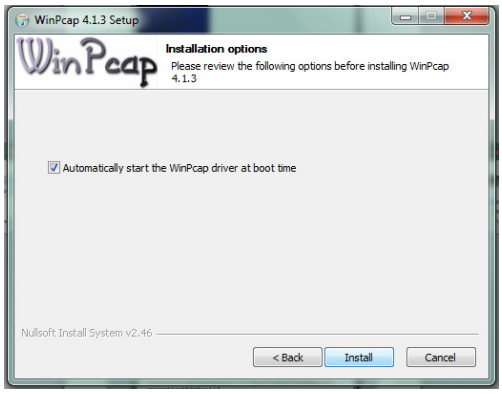


Figura 3.10: Proceso de instalación GNS3: Finalización de la instalación.

9) Tras la finalización de la instalación, se puede ejecutar la aplicación desde "Programas" en el menú de *"Inicio"* o haciendo doble clic en el icono correspondiente del escritorio, y aparecerá la pantalla de la Figura 3.11.

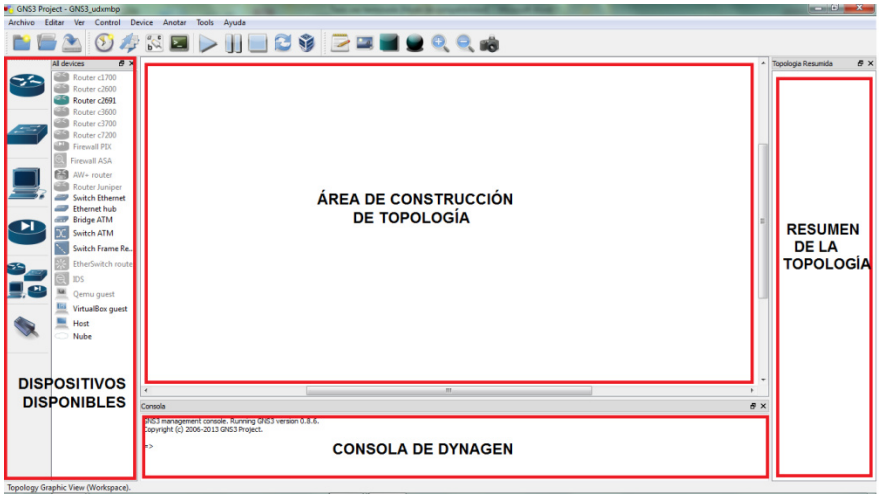


Figura 3.11: Ventana del software GNS3.

Al momento de ejecutar el programa aparecerá una ventana como la que se muestra en la figura 3.12.

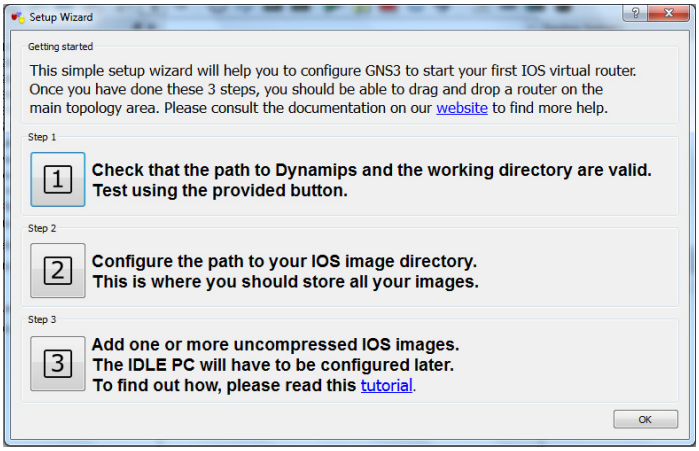


Figura 3.12: Complemento de instalación del GNS3

3.4.1.2 Comprobar el path hacia Dynamips

Una vez instalado GNS3 es importante comprobar si el simulador ha podido reconocer de forma eficaz el *path* donde se encuentra instalado Dynamips para que pueda usarlo correctamente [04]. Los pasos para realizar esta tarea son los siguientes:

En el complemento de instalación de GNS3 dar clic en *Step 1* (Figura 3.12) o en la aplicación, seleccionar la opción "*Preferencias*" del menú Editar, como se muestra en la Figura 3.13.

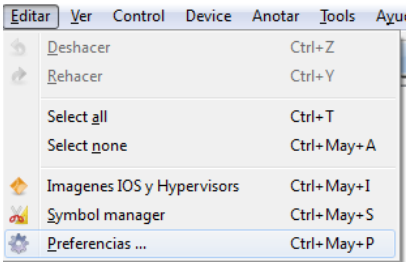


Figura 3.13: Inicio para la comprobación del path del Dynamips

En la ventana que aparece hacer un clic en la opción "*Dynamips*", comprobar que el *path* se encuentra en la ruta indicada haciendo clic en "*Test Settings*" como se muestra en la Figura 3.14, si obtenemos algún error buscar la verdadera ubicación donde se encuentre Dynamips.

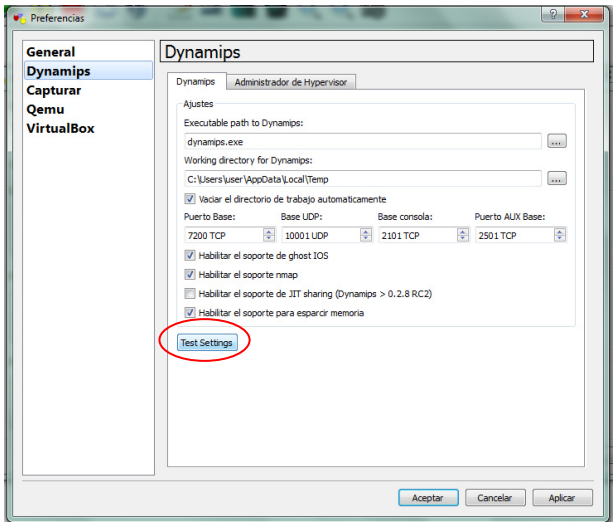


Figura 3.14 Comprobación del path del Dynamips

Luego se debe hacer clic en "*Aplicar*" y luego "*Aceptar"* para guardar los cambios. Después debemos verificar que la comprobación ha sido exitosa mostrando un mensaje *"successfully started",* como se muestra en la Figura 3.15.

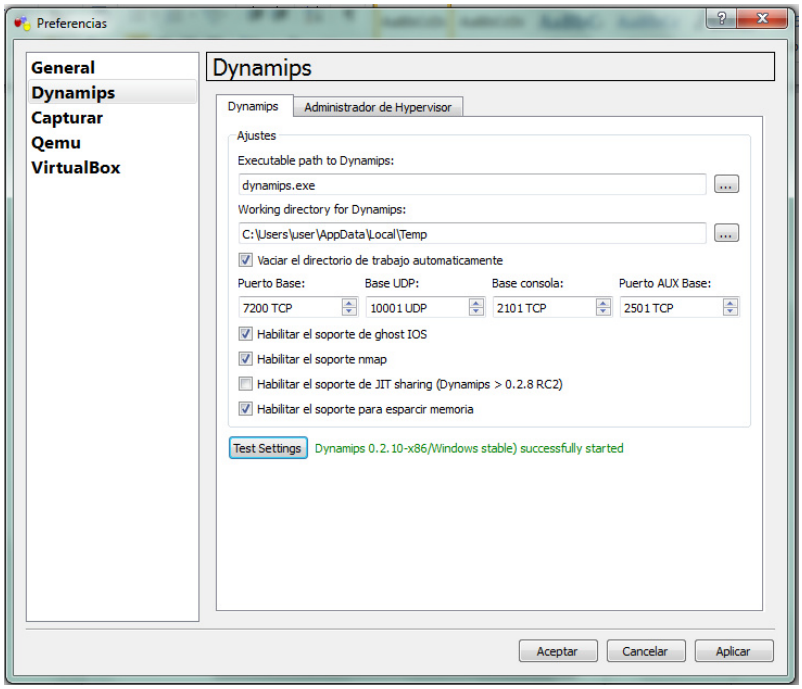


Figura 3.15: Comprobación exitosa del path en Dynamips

3.4.1.3 Configuración General (Idioma, directorio de almacenamiento)

El siguiente paso es la configuración general de la aplicación como por ejemplo el idioma, la dirección donde guardar las imágenes del IOS, los proyectos, las topologías, etc., para lo cual realizaremos los siguientes pasos:

En el complemento de instalación de GNS3 dar clic en *Step 2* (Figura 3.12) o en la aplicación, seleccionar la opción "*Preferencias*" del menú Editar, como se muestra en la Figura 3.16.

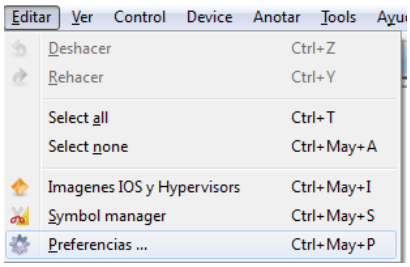


Figura 3.16: Inicio para configuración general GNS3

En la ventana que aparece hacer un clic sobre "*General*" para obtener la pestaña donde se muestra el idioma de la aplicación "*Language*". Seleccionamos el idioma a convenir y así mismo los directorios de almacenamiento. Figura 3.17

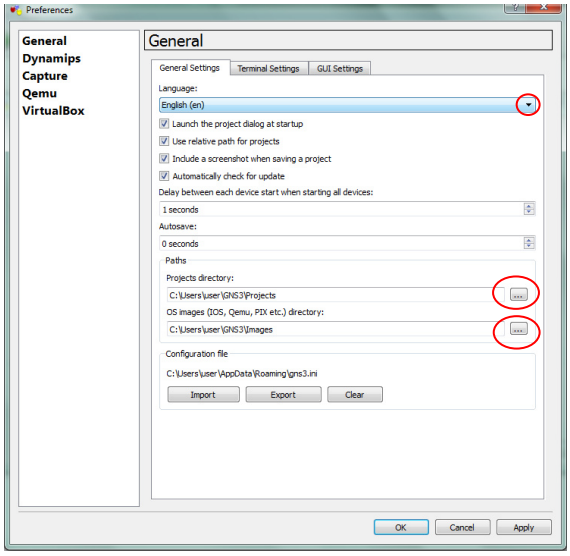


Figura 3.17: Selección de idioma y almacenamiento.

Luego procedemos a hacer clic en "*Aplicar*" y luego "*OK*" para guardar los cambios. Figura 3.18.

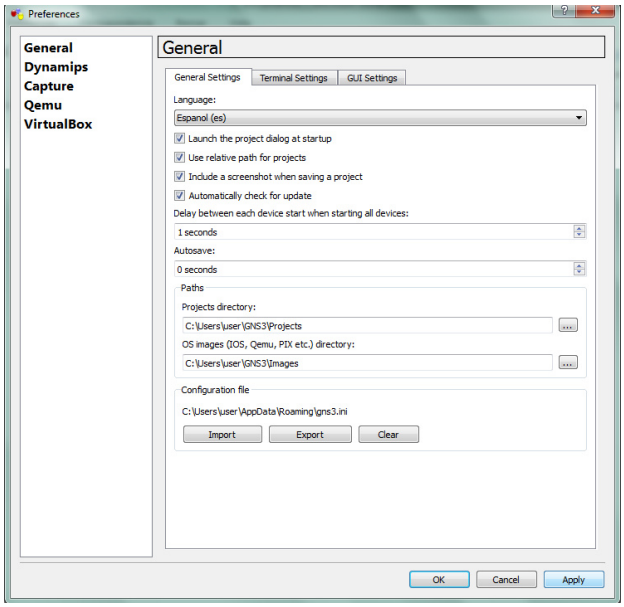


Figura 3.18: Configuración de idioma y almacenamiento guardado.

3.4.1.4 Carga de los CISCO IOS

El siguiente paso es la carga de la imagen IOS que usarán los routers virtuales de nuestra topología, que previamente debe estar descargado. La imagen del IOS que se hará uso para el presente proyecto se denomina "c2691-adventerprisek9_sna-mz.124-13b", para que sea posible ejecutarlo. Se encuentra ubicado en: "*http://certs4u.info/ciscoios/Cisco%202600%20Series%20Routers%20IOS/c2691".*

Una vez descargado realizaremos los siguientes pasos:

En el complemento de instalación de GNS3 dar clic en Step 3 (Figura 3.12) o en la aplicación y seleccionar “IOS images and hypervisors” en el menú Edit, como se muestra en la Figura 3.19.

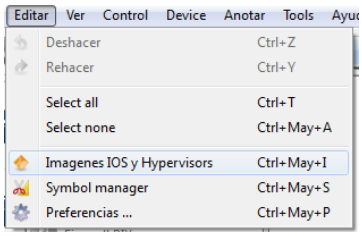


Figura 3.19: Carga de los CISCO IOS en el GNS3

En la ventana que aparece, se debe buscar la ubicación de la imagen IOS en el PC y cargarla. Ver Figura 3.20.

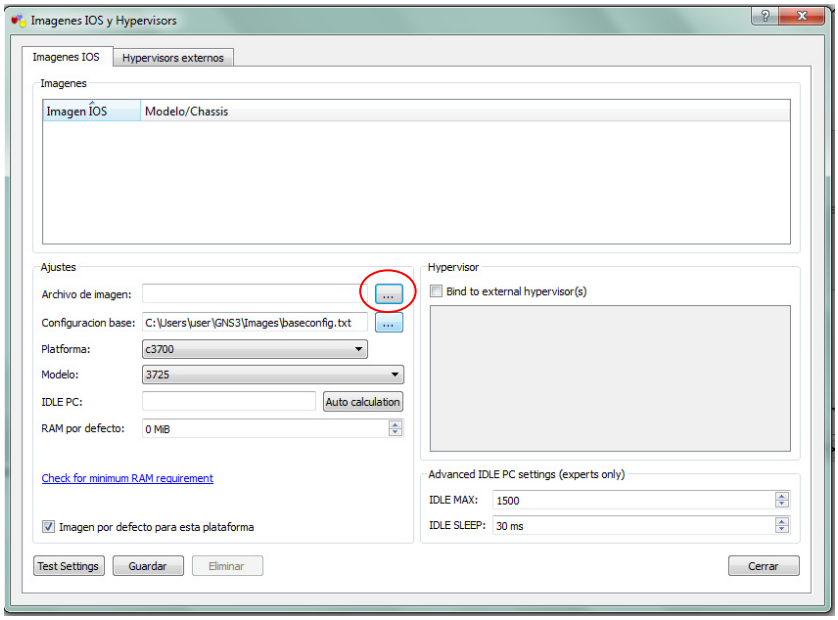


Figura 3.20: Ubicación de CISCO IOS en el GNS3

Seguidamente se elegirá la plataforma y el modelo que corresponde con la imagen IOS que usaremos para simular. Ver Figura 3.21.

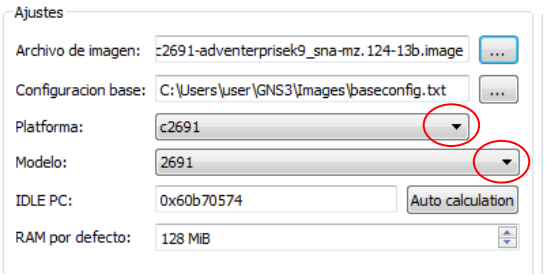


Figura 3.21: Selección de CISCO IOS en el GNS3

Después procedemos hacer clic sobre “Test Settings” para calcular los valores de IDLE PC al router. Ver Figura 3.22.

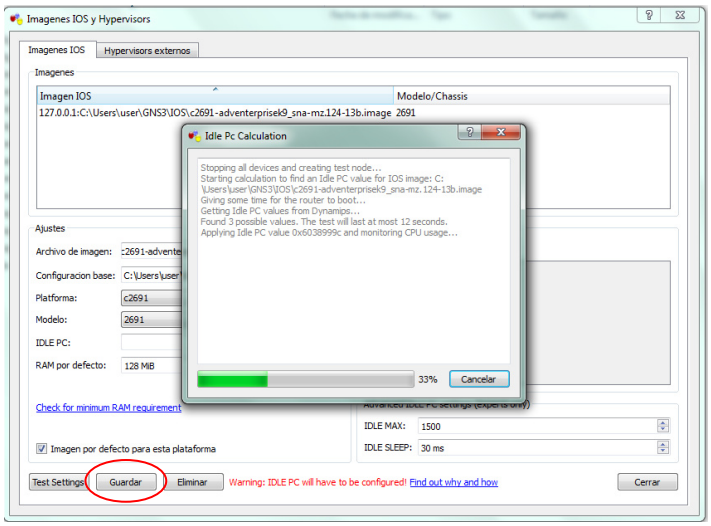


Figura 3.22: Proceso del cálculo del valor de IDLE PC

Finalmente guardamos los cambios haciendo clic en “Guardar”. Ver Figura 3.23

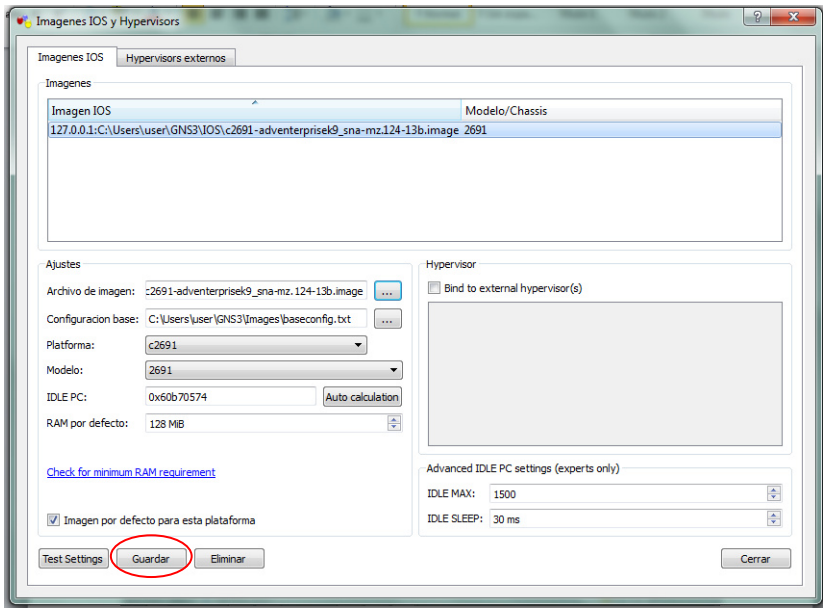


Figura 3.23: Almacenamiento de CISCO IOS en el GNS3

3.4.1.5 Establecer conexión virtual lógica

Para este proyecto se ha establecido cuatro computadoras de las cuales una de ellas será la PC anfitrión denominada ADMINISTRADOR, en la misma que se va a monitorear mediante OpenNMS.

Para establecer la conexión virtual lógica se creará un adaptador de red virtual, para ello primero debemos ingresar al cmd de la máquina y escribimos el comando “*hdwwiz.exe*”. Ver Figura 3.24.

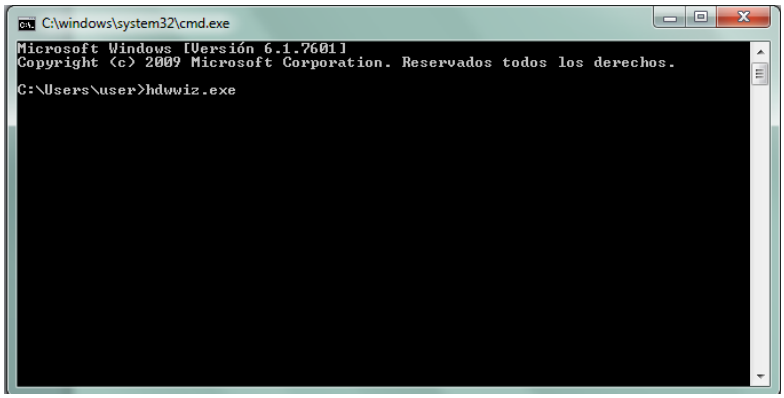


Figura 3.24: Establecer Conexión Virtual Lógica

Este comando direcciona al asistente para agregar hardware y damos clic en siguiente. Ver Figura 3.25

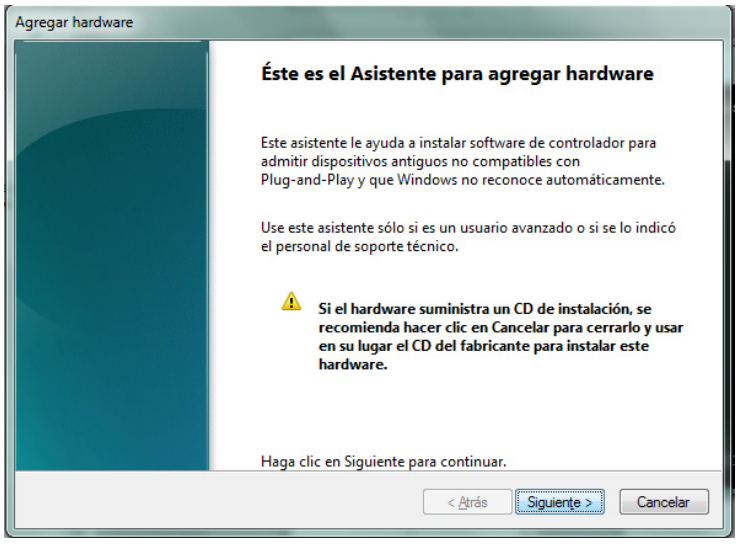


Figura 3.25: Asistente para Agregar Hardware

Para agregar el hardware lo realizamos manualmente, es decir; damos clic en la opción "*Instalar el hardware seleccionado manualmente de una lista (avanzado)*". Ver Figura 3.26.

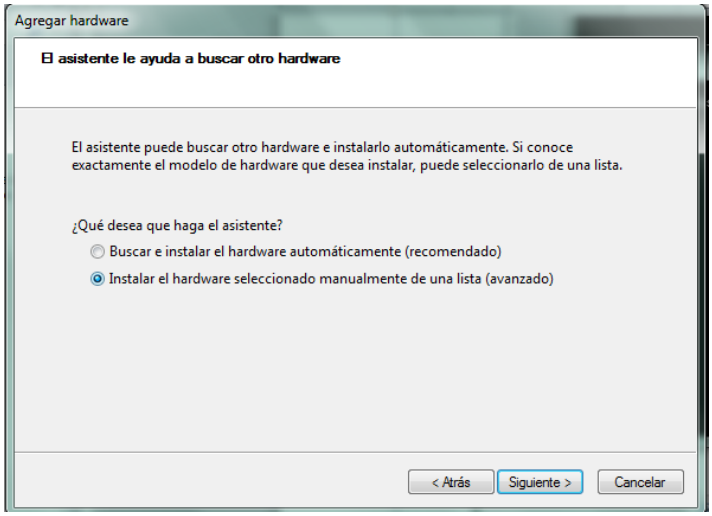


Figura 3.26: Asistente para Agregar Hardware Manualmente

Seleccionamos en la siguiente ventana "*Adaptadores de red*" como tipo de hardware que estamos instalando. Ver Figura 3.27

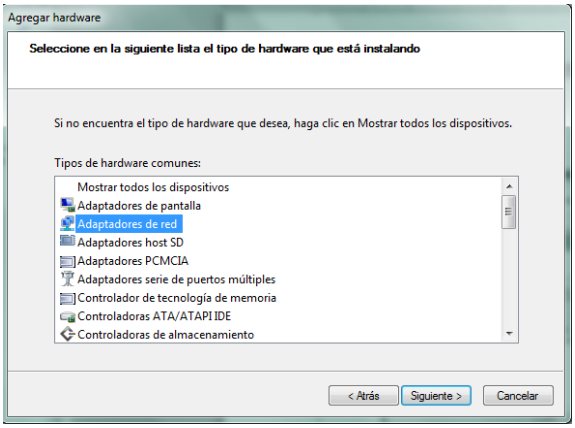


Figura 3.27: Instalación del Adaptador de Red

Esperamos a que cargue los adaptadores de red, una vez presente dichos adaptadores elegimos como fabricante "*Microsoft*" donde automáticamente se despliega los adaptadores de red y seleccionamos "*Adaptador de bucle invertido de Microsoft o Microsoft Loopback Adapter*", como se muestra en la Figura 3.28.

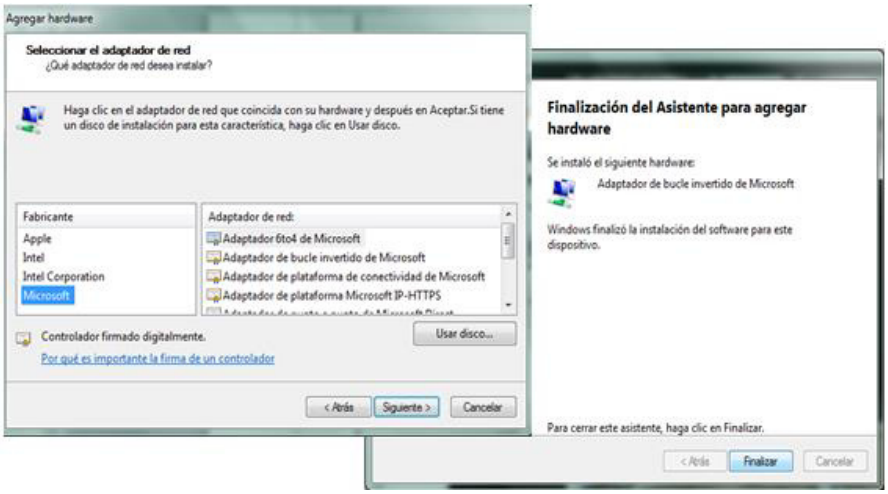


Figura 3.28: Selección del Adaptador de Red

Una vez agregado el hardware del asistente para el adaptador de red, verificamos en centro de redes y recursos compartidos de Windows que se encuentre el adaptador de red de bucle invertido o loopback. Ver Figura 3.29.

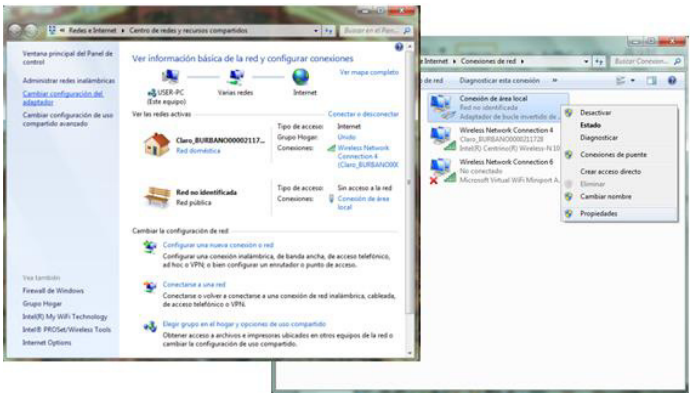


Figura 3.29: Verificación del Adaptador de Red

Después de la verificación se procede a dar clic derecho en el adaptador y seleccionamos "*Propiedades*" para asignarle una dirección IP que debe ser subred de la red de Administración de la configuración de la Red LAN virtual, para nuestro caso dirección IP: 10.10.10.11/24, puerta de enlace 10.10.10.1. Ver Figura 3.30

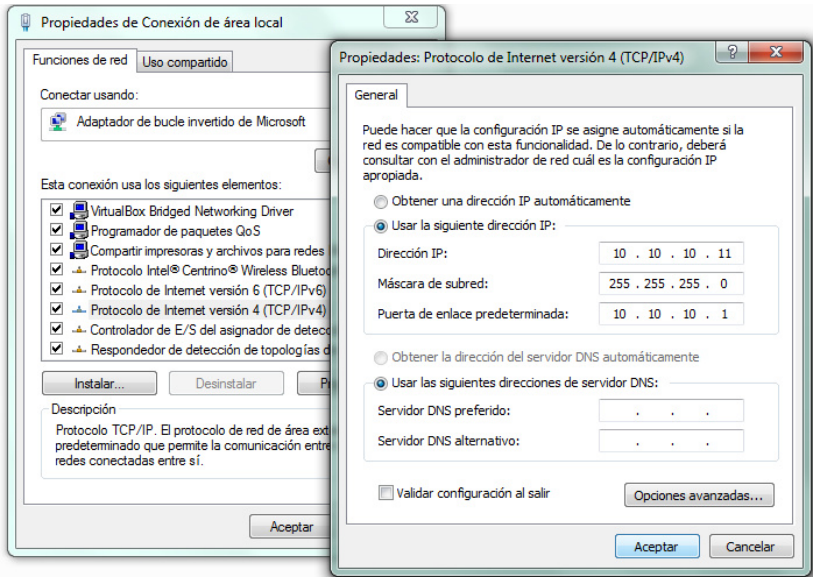


Figura 3.30: Configuración IP de la PC ADMINISTRADOR

Para establecer la conexión virtual lógica se debe abrir el software GNS3 para configurar el puerto que va a ir asignado el adaptador de red. Cabe recalcar que el software GNS3 debe ejecutarse como administrador para que detecte los adaptadores de red.

Luego se asigna un nombre al nuevo proyecto. Para la interfaz real incluimos el elemento “Nube”. El elemento nube sirve para enlazar la red virtual con cualquier interfaz de red real de la máquina donde se ejecuta GNS3. Ver figura 3.31.

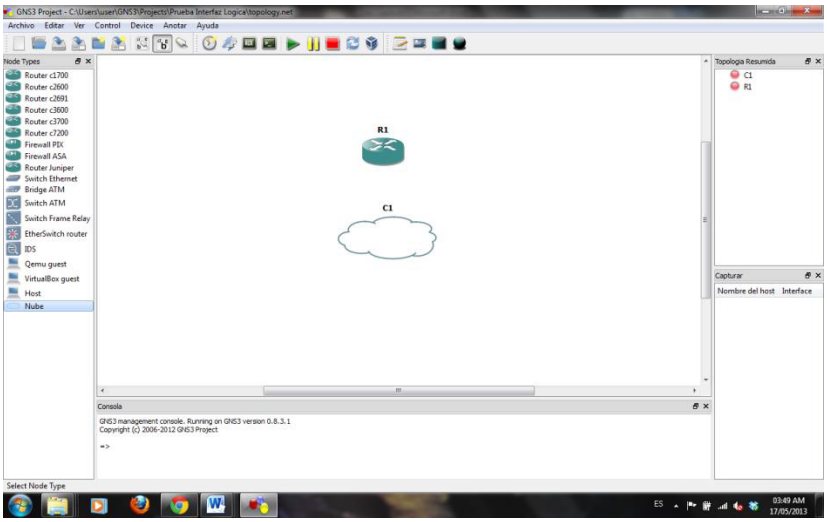


Figura 3.31: Configuración de la Conexión Virtual Lógica en GNS3

A continuación dar doble clic o clic derecho en la “Nube” para configurar, Primero se debe agregar el adaptador de red creado de bucle invertido o loopback y luego establecer la conexión creando un enlace con el router c2691. Ver Figua 3.32

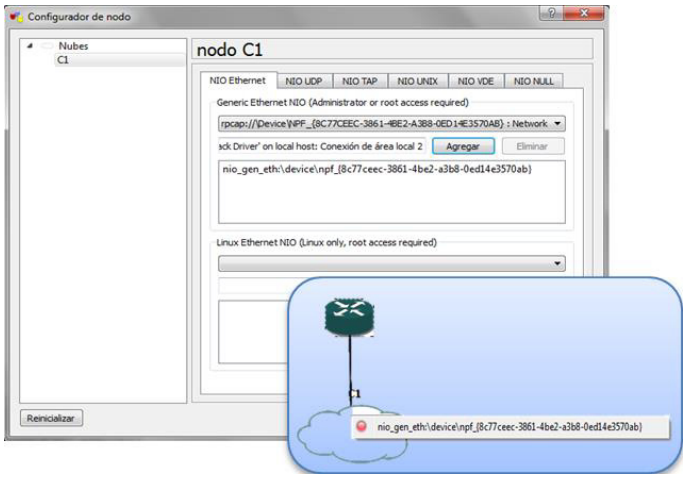


Figura 3.32: Asignación del Adaptador de Red en la PC ADMINISTRADOR en GNS3

Para verificar que haya conexión con la interfaz real necesitamos configurar el router dándole clic derecho y seleccionamos la opción "*Consola*", el router empezará arrancar y debemos asignarle una dirección IP que se encuentre dentro de la red del adaptador de red creado como se muestra en la Figura 3.33, con los siguientes comandos:

- GYE#configure terminal
- GYE(config)#int fa0/0
- GYE(config-if)#ip address 10.10.10.1 255.255.255.0
- GYE(config-if)#no shutdown
- GYE(config-if)#exit

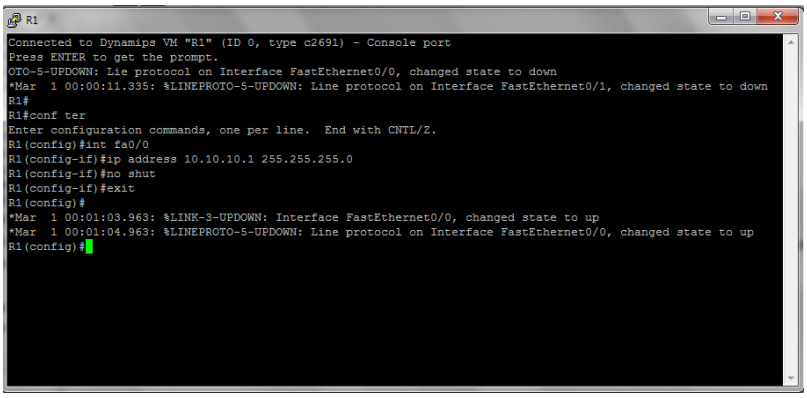


Figura 3.33: Configuración IP del Router GYE

Antes de verificar que la conexión ha sido exitosa, debemos desactivar el Firewall de Windows a través de los siguientes pasos: *Inicio/ Panel de Control/ Sistema y seguridad/ Firewall de Windows/ Activar o desactivar Firewall de Windows.* Una vez desactivado el Firewall de Windows procedemos hacer ping tanto desde la PC a través de cmd (Figura 3.34) como del router GYE (Figura 3.35).

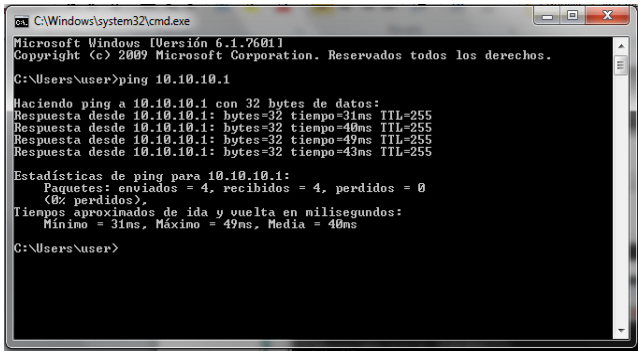


Figura 3.34: Verificación de la conexión virtual lógica de la PC a Router GYE.

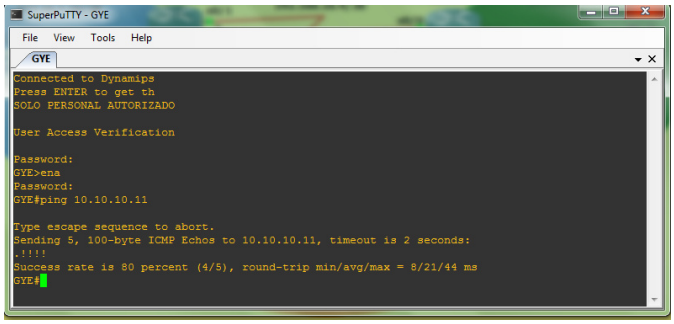


Figura 3.35: Verificación de la conexión virtual lógica del Router GYE a la PC.

3.4.1.6 Comunicación VirtualBox y GNS3

Para ingresar una máquina virtual en el software GNS3, debe tener instalado el software VirtualBox instalado se explicará con detalle en el apartado 3.4.2; una vez instalado VirtualBox, debemos crear las máquinas virtuales, asignarles una tarjeta de red y enlazar con GNS3.

Para comunicar una máquina virtual con GNS3 se debe realizar los siguientes pasos:

1) Primero debemos asegurarnos que el Path de trabajo a VBoxwrapper se encuentre en el directorio de trabajo, haciendo clic en "*Test Settings*" (Ver Figura 3.36). para la confirmación se observará un mensaje que indica "*VBoxwrapper y VirtualBox API 4.2.18 have successfully started*".

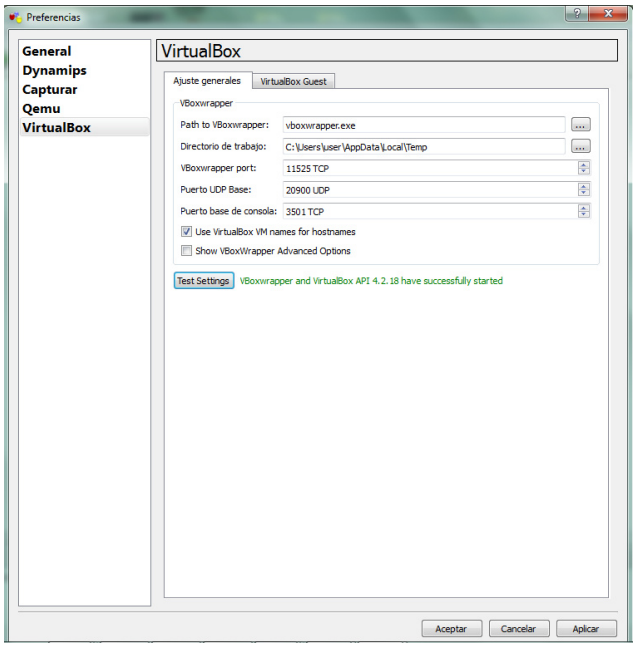


Figura 3.36: Confirmación del Path de trabajo a VBoxwrapper.

2) Una vez creada las máquinas virtuales (se explicará detalladamente en el apartado 3.4.3.2), damos clic en "*Virtual Guest*" e ingresamos las máquinas virtuales creadas. Ver Figura 3.37

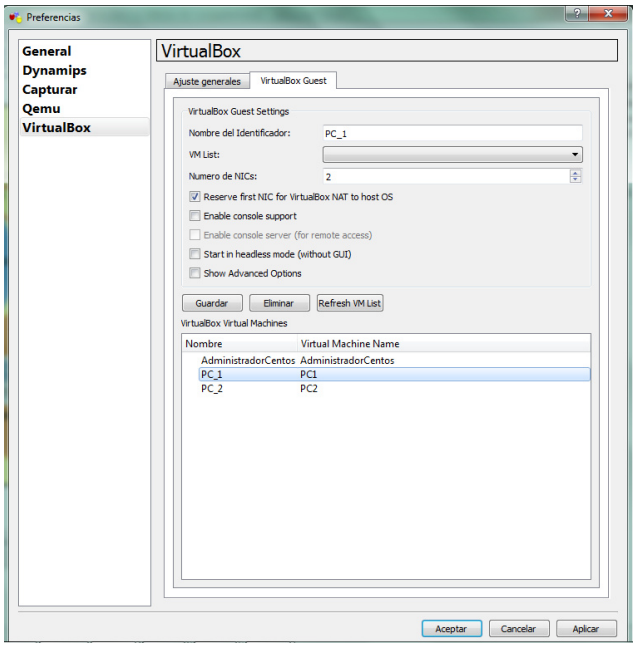


Figura 3.37: Inclusión de Máquinas Virtuales a GNS3.

3.4.2 Instalación y configuración de VirtualBox

Como se observa en la diagrama de la topología Figura 3.2, se ha hecho uso de dos máquinas virtuales PC_1 y PC_2. A continuación se detalla el proceso de instalación y configuración de VirtualBox.

El primer paso para la instalación es descargar el archivo, VirtualBox-4.2.18-88781-Win.exe (ocupa aproximadamente 97.28MB), que se encuentra en la página web *https://www.virtualbox.org/wiki/Downloads.*

3.4.2.1 Instalación VirtualBox

Una vez descargado el software VirtualBox, proceder a dar doble clic en el archivo ejecutable de instalación, seguir el proceso de instalación de forma habitual; es decir, los valores por defecto de instalación son los que aceptaremos en la misma, a no ser que desee cambiar la ruta de dirección donde se instalará el software VirtualBox.

Los pasos de instalación son:

1) Dar doble clic al archivo de instalación .exe. Nos aparecerá una ventana como la que se muestra en la Figura 3.38. Hacer clic en "*Next*".

Figura 3.38: Proceso de instalación VirtualBox: Inicio de la instalación.

2) Indicar la ubicación del directorio donde se instalará VirtualBox. Como se observa en la Figura 3.39. Seguidamente hacer clic en "*next*".

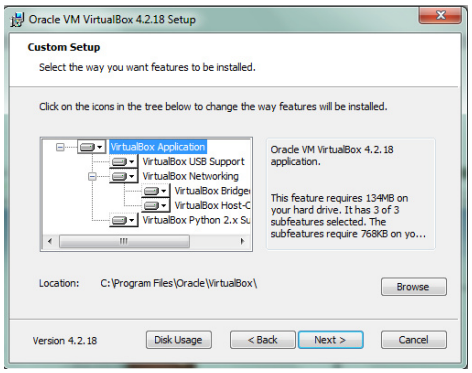


Figura 3.39: Proceso de instalación VirtualBox: Indicar dirección de directorio.

3) La siguiente ventana que se muestra es un aviso de las interfaces de red que indica que se hará un reset en las conexiones de red. Procedemos a dar clic en “Next”. Ver Figura 3.40.

Figura 3.40: Proceso de instalación VirtualBox: Configuración Conexiones de Red.

4) Antes de concluir la instalación de VirtualBox, aparecerá la ventana que da inicio a la instalación del software. Hacer clic en “*Instal*” después del proceso de instalación aparecerá

una ventana dar clic en la opción "*Finish*" para empezar a utilizar VirtualBox. Ver Figura 3.41.

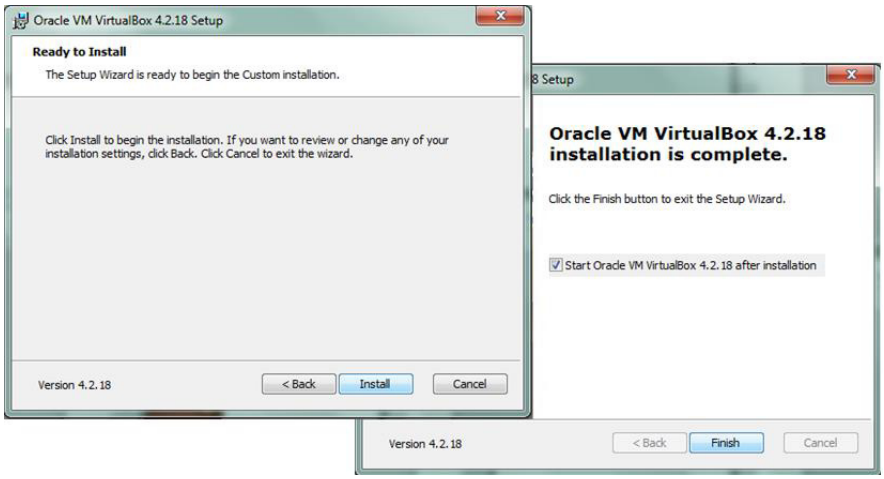


Figura 3.41: Proceso de instalación VirtualBox: Finalización de la Instalación

3.4.2.2 Configuración de VirtualBox

Para este proyecto utilizaremos dos máquinas virtuales PC_1, PC_2; es decir, necesitamos crear dos PC virtuales donde PC_1 y PC_2 se les ha asignado como sistema operativo Microsoft Windows 7 Professional, en vista que la interfaz es más accesible al usuario y es un sistema operativo más ligero, estable y rápido.

A continuación se detalla el proceso para crear una máquina virtual con VirtualBox:

1) Como primer paso, dar clic en la opción "*Nueva*", rápidamente se desplegará una ventana la cual nos permitirá escribir el nombre de la máquina virtual y seleccionar el sistema operativo y la versión. Ver figura 3.42.

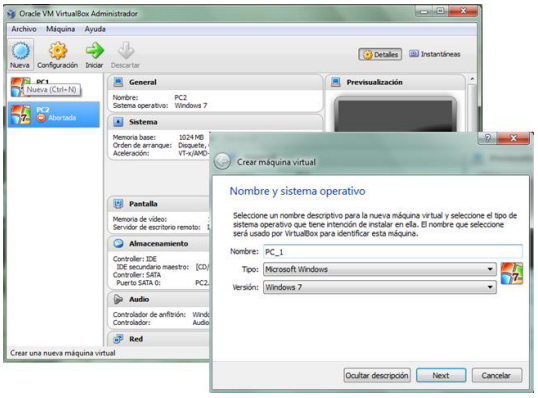


Figura 3.42: Creación Máquina Virtual PC_1

2) Asignar el tamaño de memoria de nuestra PC_1. Como podemos apreciar en la Figura 3.43, le daremos 1GB (1024MB) de memoria RAM.

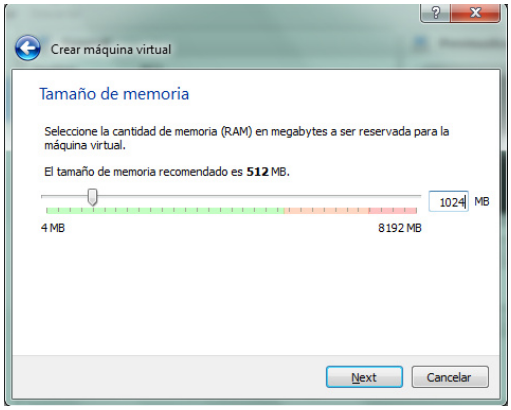


Figura 3.43: Asignación del tamaño de memoria de la Máquina Virtual PC_1

3) Crear disco duro virtual y elegir el tipo de archivo de unidad de disco duro dando clic en la opción "*Next*", es preferible dejar las opciones por default. Ver figura 3.44.

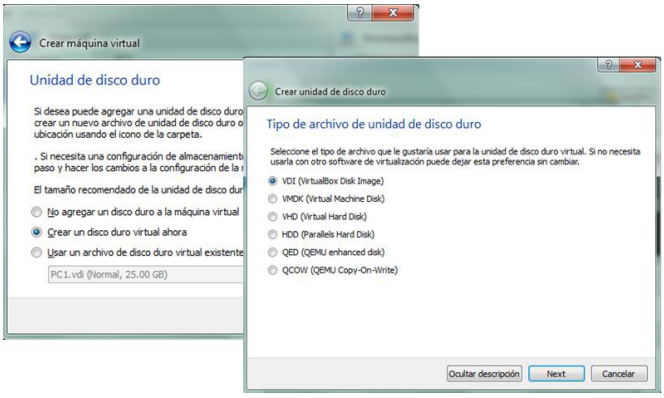


Figura 3.44: Creación virtual de Unidad de Disco Duro de la Máquina Virtual PC_1.

4) Elegir el tipo de almacenamiento y asignar nombre de la máquina virtual (PC_1), ubicación del archivo y tamaño del disco duro virtual. Ver Figura 3.45.

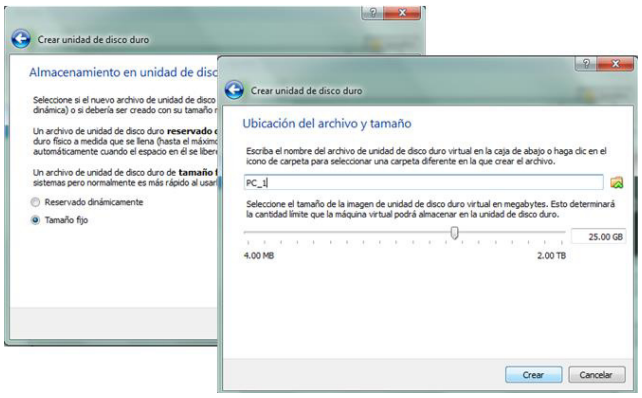


Figura 3.45: Asignación de la Ubicación del Archivo y Tamaño de Disco Duro de la Máquina Virtual PC_1.

5) Por último debemos esperar a que VirtualBox cree la máquina virtual, este procedimiento puede durar algunos minutos. Ver Figura 3.46.

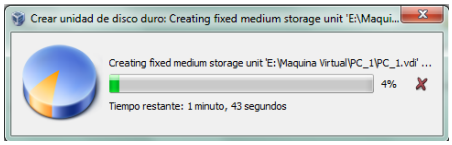


Figura 3.46: Finalización en la creación de la Máquina Virtual PC_1.

Una vez realizado este procedimiento se debe repetir los mismos pasos para crear la máquina virtual PC_2. Cabe recalcar que las máquinas virtuales han sido creadas pero aún les falta asignar el sistema operativo a cada una ellas.

Para instalar el sistema operativo en las máquinas virtuales creadas, se debe dar doble clic o clic derecho, opción "*Iniciar*". Automáticamente se iniciará la máquina virtual y solicitará el sistema operativo desde un archivo de disco óptico virtual o una unidad óptica física como se observa en la Figura 3.47.

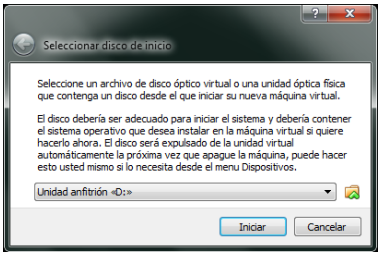


Figura 3.47: Instalación del Sistema Operativo en Máquina Virtual.

El proceso de instalación de Sistema Operativo es similar como instalar el OS en la máquina anfitrión, por ello omitiremos dicho procedimiento. Pero es importante destacar que una vez que las máquinas virtuales han sido asignados sus OS, debemos instalar "*Guest Additions*", que es un software proporcionado por Virtual Box que brinda mejor integración entre el sistema anfitrión y el invitado, el cual está ubicado en la barra de herramientas de la máquina virtual inicializada, opción "*dispositivos*", dar clic en "Instalar <<*Guest Additions*>>". Ver Figura 3.48.

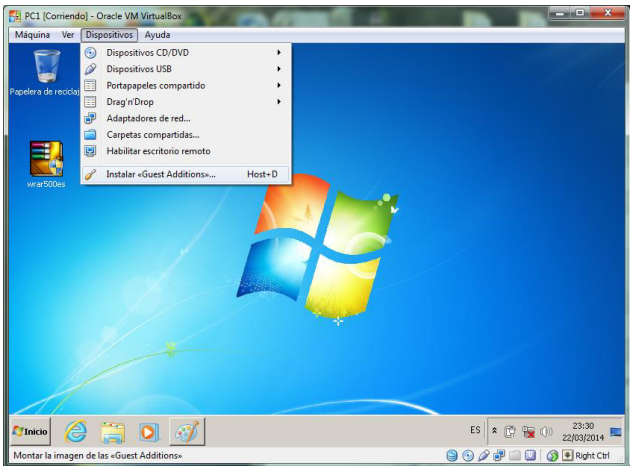


Figura 3.48: Instalación Guest Additions de la Máquina Virtual.

De acuerdo a nuestra topología se debe crear rutas estáticas, es decir, cambiar manualmente los datos respectivos en los adaptadores de red de cada una de las máquinas virtuales.

La Figura 3.49, muestra la configuración para asignar la ruta estática de la PC_1. La dirección IP que se la ha asignado a la

PC_1 es 172.16.1.18, con Máscara de Red 255.255.255.240, Puerta de Enlace 172.16.1.17. Para configurar la IP se debe ingresar a: *Inicio/ Panel de control/ Redes e Internet/ Centro de redes y recursos compartidos/ Cambiar configuración del adaptador/ Conexión de área local 2/ Propiedades/ Protocolo de Internet versión 4 (TCP/IPv4)*.

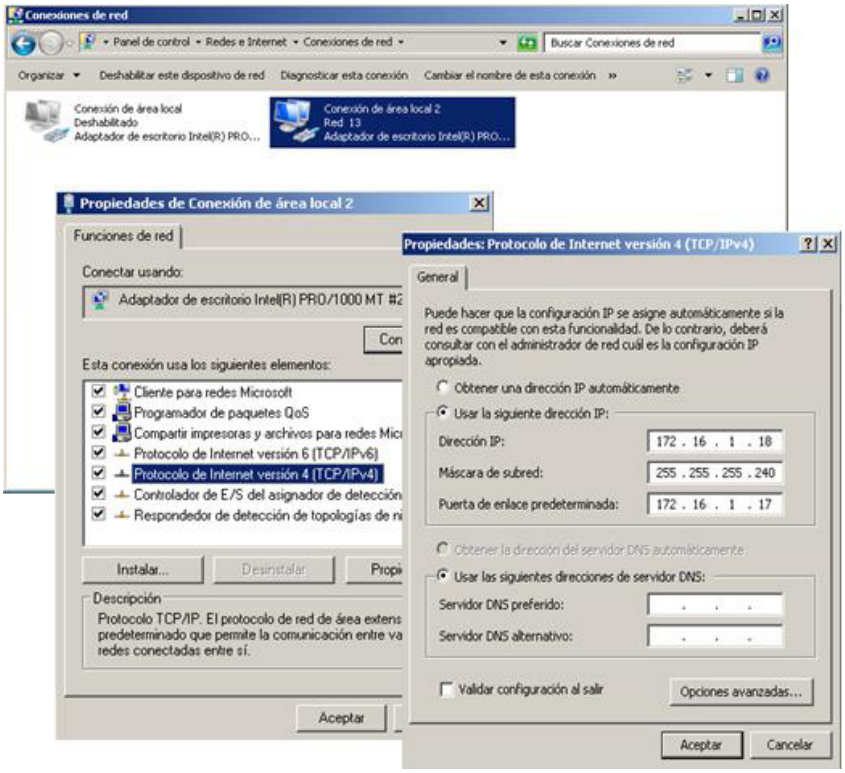


Figura 3.49: Configuración IP de la PC_1.

La Figura 3.50, muestra la configuración para asignar la ruta estática de la PC_2. La dirección IP que se la ha asignado a la PC_2 es 172.16.1.34, con Máscara de Red 255.255.255.248, Puerta de Enlace 172.16.1.33. Para configurar la IP se debe

ingresar a: *Inicio/ Panel de control/ Redes e Internet/ Centro de redes y recursos compartidos/ Cambiar configuración del adaptador/ Conexión de área local 2/ Propiedades/ Protocolo de Internet versión 4 (TCP/IPv4)*.

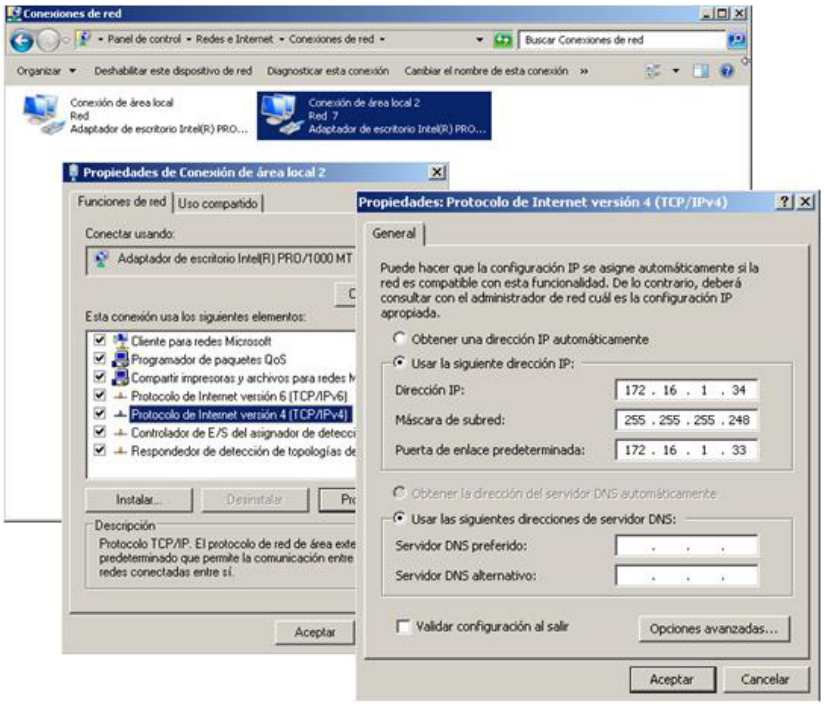


Figura 3.50: Configuración IP de la PC_2.

Antes de verificar que la conexión ha sido exitosa, se debe desactivar el Firewall de Windows en las máquinas virtuales; es decir, PC_1 y PC_2 a través de los siguientes pasos: *Inicio/ Panel de Control/ Sistema y seguridad/ Firewall de Windows/ Activar o desactivar Firewall de Windows* (Ver Figura 3.51). Además debemos configurar el protocolo de enrutamiento en cada router (se explicará en el apartado 3.4.5).

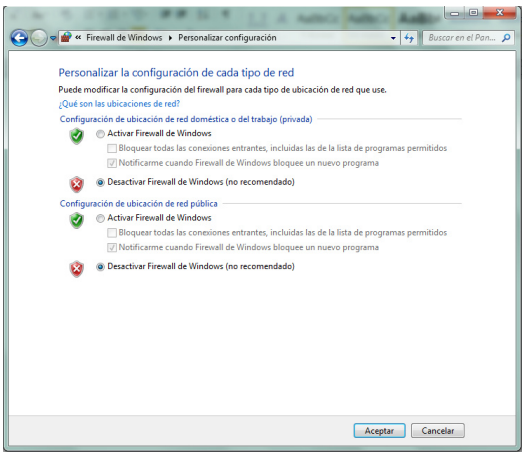


Figura 3.51: Desactivar Firewall de Windows.

3.4.3 Instalación y configuración de OpenNMS.

OpenNMS es el software que permitirá administrar y monitorear toda la red. Este software es fácil descargarlo en su página web (*http://www.opennms.org/wiki/Installation:Windows*) se encuentra todos los archivos necesarios para el proceso de instalación, además proporciona un tutorial donde explica detalladamente como instalar y configurar OpenNMS.

Para hacer uso del programa como tal, necesita de PostgreSQL para la base de datos, un motor basado en Java que realiza todo el trabajo pesado (monitorización, alertas, etc.) y una interfaz web basada en Java para la administración y la gestión del sistema.

No se explicarán todos los detalles de instalación, puesto que OpenNMS dispone de una guía de instalación muy completa que cubre todo el proceso a profundidad.

Una vez descargado el software OpenNMS e instalado Java y PostgreSQL, proceder a dar doble clic en el archivo ejecutable de instalación, seguir el proceso de instalación de forma habitual; es decir, los valores por defecto de instalación son los que aceptaremos en la misma, a no ser que desee cambiar la ruta de dirección donde se instalará el software OpenNMS.

Los pasos de instalación son:

1. Dar doble clic al archivo de instalación .exe de OpenNMS. Nos aparecerá una ventana como la que se muestra en la Figura 3.52. Hacer clic en "*Next*".

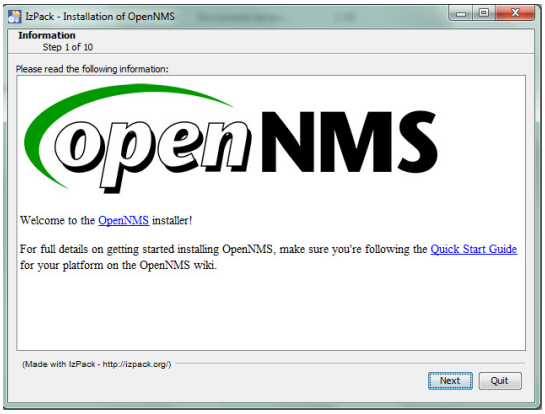


Figura 3.52: Proceso de instalación OpenNMS: Inicio de la instalación.

2. Aceptar los términos de licencia de OpenNMS como se observa en la Figura 3.53. Seguidamente hacer clic en "*next*".

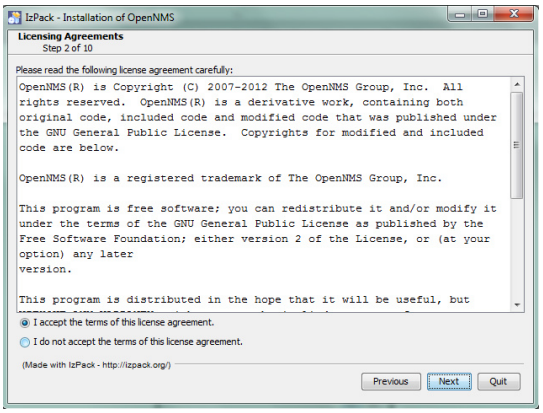


Figura 3.53: Proceso de instalación OpenNMS: Aceptar los términos de licencia.

3. La siguiente ventana que se muestra nos permitirá buscar el archivo de Java jdk1.8.0 previamente instalado. Una vez localizado el archivo dar clic en "Next". Ver Figura 3.54.

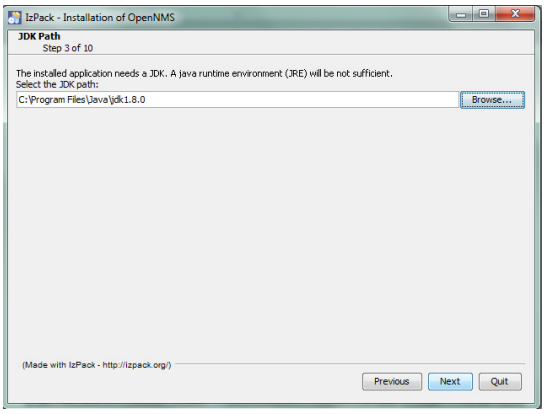


Figura 3.54: Proceso de instalación OpenNMS: Seleccionar el archivo de Java jdk1.8.0.

4. Indicar la ubicación de directorio donde se instalará OpenNMS como se muestra en la Figura 3.55. Seguidamente hacer clic en "*Next*".

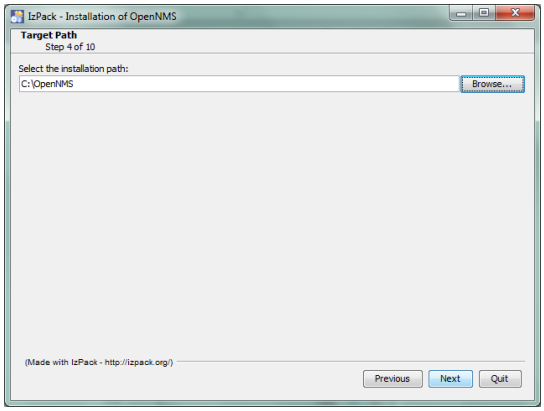


Figura 3.55: Proceso de instalación OpenNMS: Indicar la ubicación de directorio

5. Seleccionar todos los paquetes de instalación de OpenNMS como se muestra en la Figura 3.56. Seguidamente hacer clic en "*Next*".

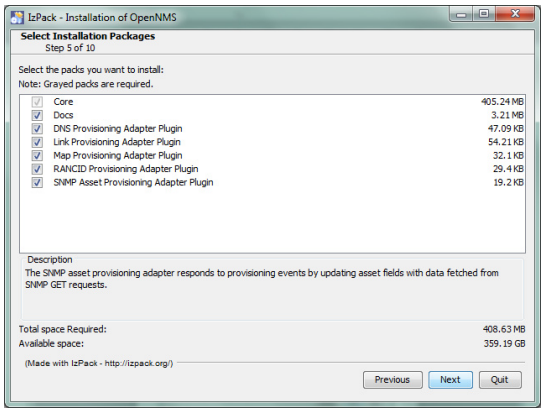


Figura 3.56: Proceso de instalación OpenNMS: Seleccionar los paquetes de instalación.

6. Configurar el password de la Base de Datos como se muestra en la Figura 3.57. Nuestro caso *password*: administrador. Seguidamente hacer clic en "*Next*".

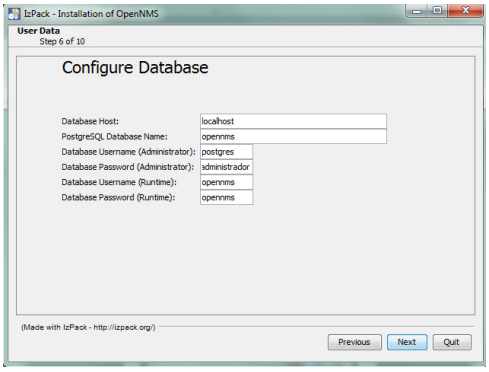


Figura 3.57: Proceso de instalación OpenNMS: Configuración de la Base de Datos.

7. Los siguientes pasos de instalación de OpenNMS son proceso de carga e instalación como tal. Por ello excluiremos los siguientes pasos. La Figura 3.58, muestra la ventana de finalización de la instalación de OpenNMS. Dar clic en "*Done*".

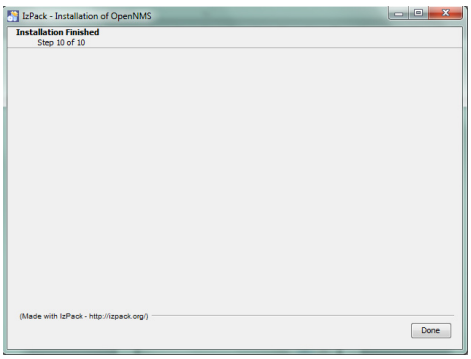


Figura 3.58: Proceso de instalación OpenNMS: Finalización de la instalación.

Para dar inicio a openNMS nos dirigimos al cmd de la PC y encontramos la ruta donde ha instalado el programa; es decir, abrir Opennms/bin y ejecutar el archivo opennms.bat con el comando "*start*" (opennms/ bin/ opennms.bat start) como se muestra en la Figura 3.59.

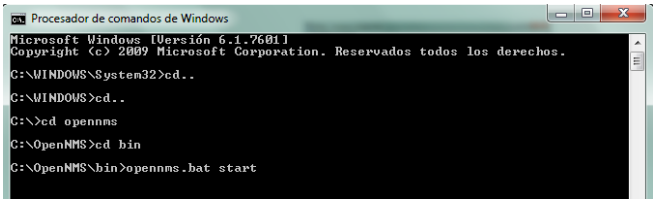


Figura 3.59: Proceso de inicialización de OpenNMS.

Una vez ejecutado este comando procedemos a ir a cualquier servidor web (Google Chrome). El link que ejecutaremos es: *http://10.10.10.11:8980/opennms*, rápidamente se despliega la página de presentación de OpenNMS como se muestra en la Figura 3.60. Cabe recalcar que en el link de enlace a OpenNMS la dirección IP que visualizamos es la dirección IP del Gestor, también es posible entrar con localhost como muestra el tutorial de OpenNMS. Por defecto el user y el password es "*admin*".

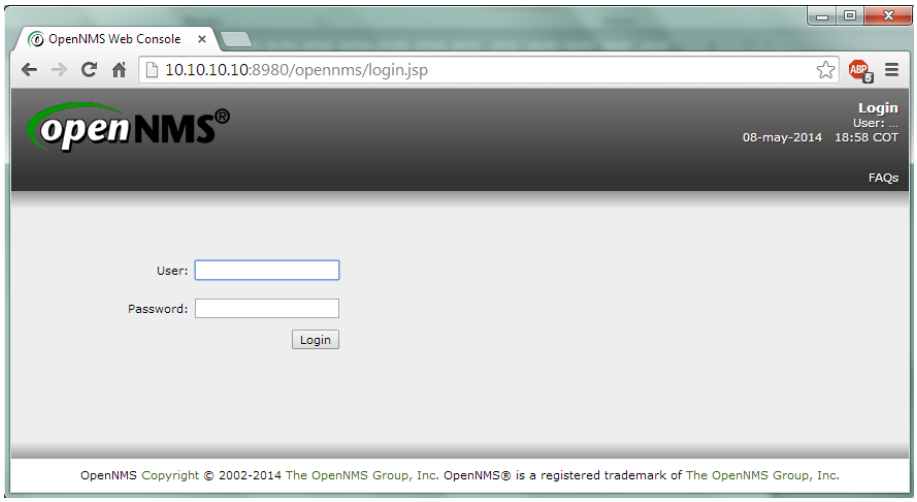


Figura 3.60: Página de inicio de OpenNMS.

3.4.4 Instalación y configuración de Wireshark

WireShark es un software que permite el seguimiento y análisis de paquetes de datos de una red, su instalación es sencilla por lo que se explicará de manera breve su proceso de instalación. A través de su página web (http://www.wireshark.org/) podrá encontrar tutoriales, guía de instalación y los archivos ejecutables para diferentes sistemas operativos.

Los pasos de instalación son:

1. Dar doble clic al archivo de instalación .exe de Wireshark. Nos aparecerá una ventana como la que se muestra en la Figura 3.61. Hacer clic en "*Next*".

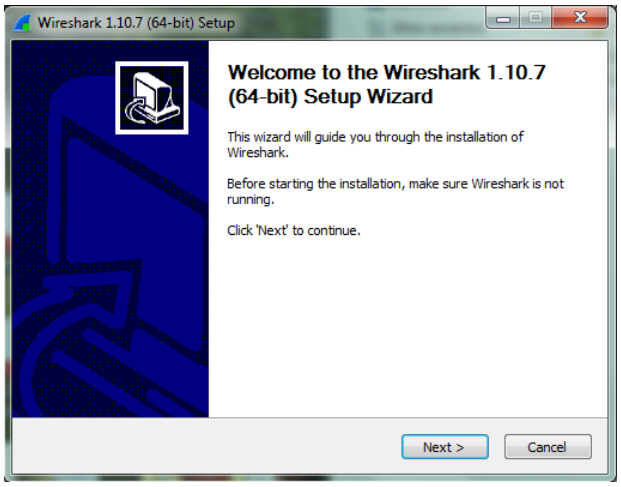


Figura 3.61: Proceso de instalación Wireshark: Inicio de la instalación.

2. Aceptar los términos de licencia de Wireshark como se observa en la Figura 3.62. Dar clic en "*I Agree*".

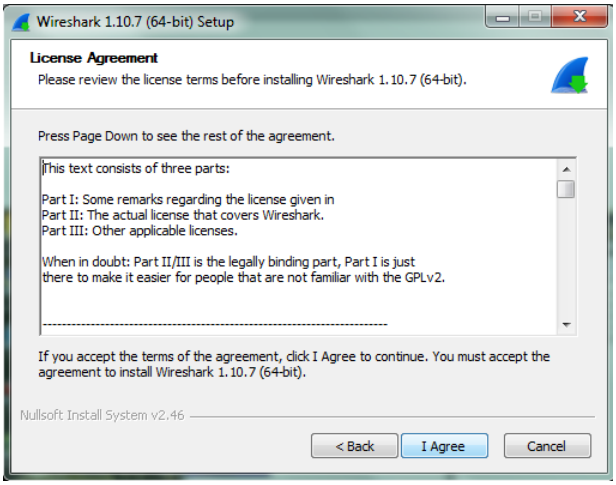


Figura 3.62: Proceso de instalación Wireshark: Aceptar los términos de licencia.

3. La siguiente Figura 3.63, muestra opciones a elegir en el proceso de instalación de Wireshark. Damos clic en “Next”.

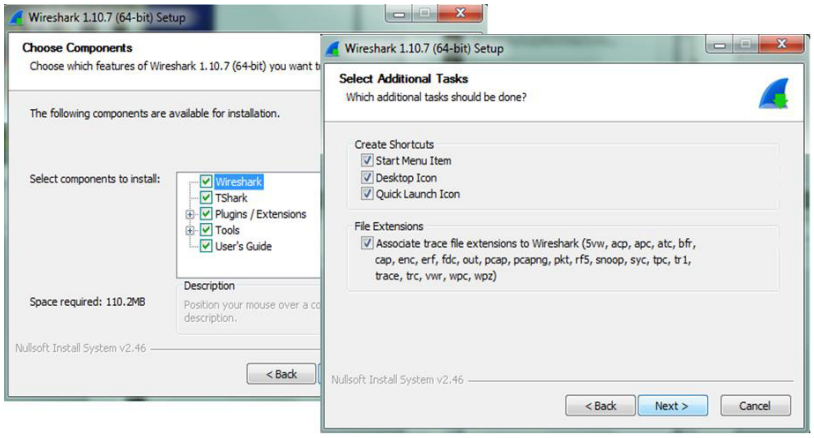


Figura 3.63: Proceso de instalación Wireshark: Seleccionar componentes de la instalación.

4. Indicar la ubicación de directorio donde se instalará Wireshark como se muestra en la Figura 3.64. Seguidamente hacer clic en “*Next*”.

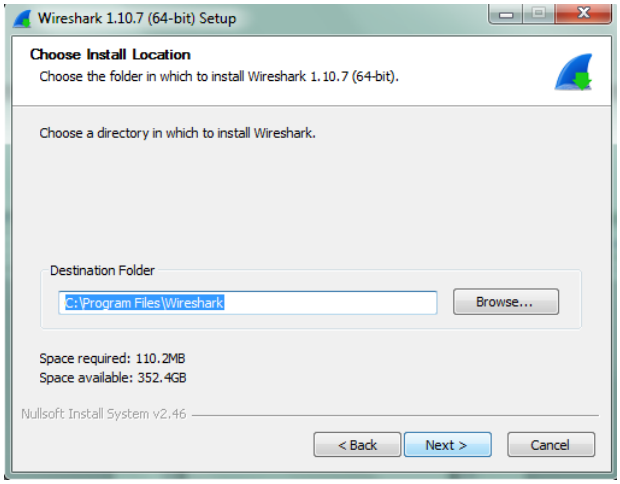


Figura 3.64: Proceso de instalación Wireshark: Indicar la ubicación de directorio

5. Damos clic en "*Next*" y automáticamente comienza a instalarse, después se presentará una ventana para finalizar la instalación como se muestra en la Figura 3.65. Seguidamente hacer clic en "*Finish*".

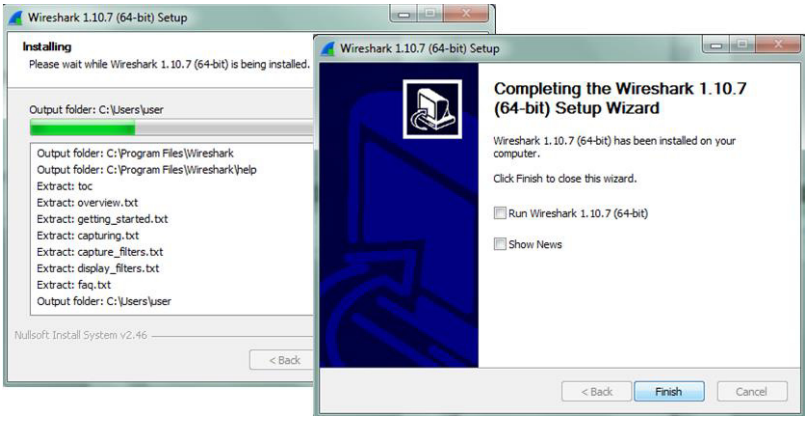


Figura 3.65: Proceso de instalación Wireshark: Finalización de la instalación.

Una vez instalado el programa estará listo para usarse. Para realizar capturas de paquetes de la red, se procede a seguir los siguientes pasos:

Primero debemos seleccionar la interfaz que queremos capturar para analizar lo deseado, recordemos que por defecto debemos tener en nuestra PC varias conexiones de red por ello debemos seleccionar "*Conexión de área local de bucle invertido o LoopBack*" como se muestra en la Figura 3.66. Para configurar debemos dirigirnos a la barra de herramientas a la opción "*Capture*", y seleccionar "*Interfaces*".

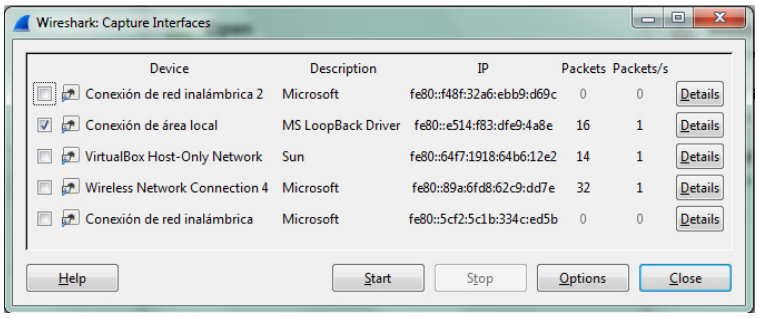


Figura 3.66: Pantalla de selección de Interfaz de Wireshark

Después que seleccionemos la interfaz a capturar debemos dar clic en "*start*", de esta manera el programa automáticamente comenzará a capturar los paquetes de datos con sus descripciones tal y como se muestra en la Figura 3.67

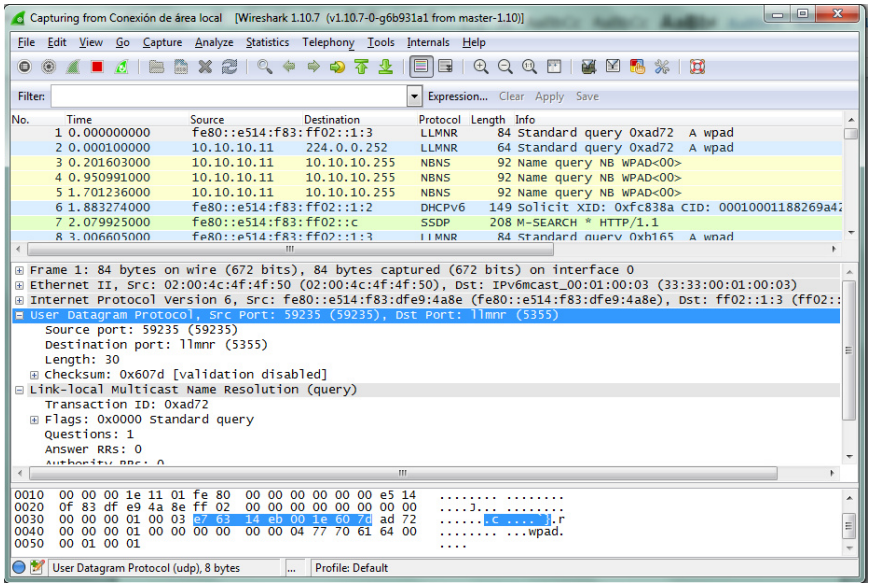


Figura 3.67: Captura de paquetes en Wireshark

3.4.5 Configuración de Servicios SNMP

3.4.5.1 Configuración de SNMP en las PC

Para detectar tráfico SNMP, primero es necesario habilitar dicho el protocolo a través de la siguiente configuración: *Inicio/ Panel de control/ Programas/ Activar o desactivar características de Windows.* Activar la opción "Protocolo Simple de Administración de Redes (SNMP)". Ver Figura 3.68.

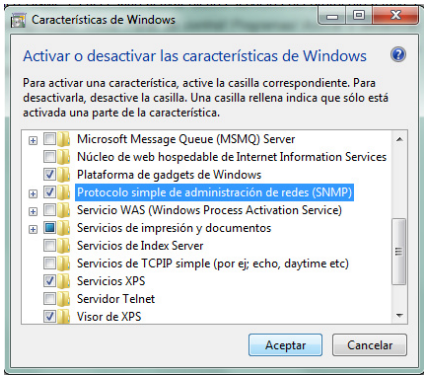


Figura 3.68: Activación de SNMP en la PC.

Una vez activado el protocolo SNMP en Windows de las máquinas PC_1, PC_2 y ADMINISTRADOR, procedemos a configurar los servicios de SNMP a través de la siguiente configuración de dichas máquinas:

1. Primero se debe ingresar a los Servicios (locales) de Windows: escribimos "*servicios*" en "*Buscar programas y archivos"* en Inicio/ Servicio SNMP, clic derecho

"Propiedades". Ver Figura 3.69. Cuando se haya realizado todas las configuraciones dar clic en *Reiniciar*.

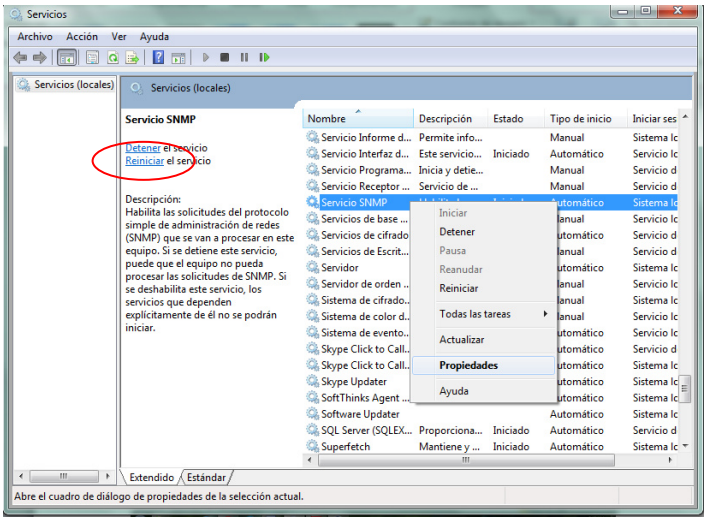


Figura 3.69: Procedimiento para configurar el Servicio SNMP en la PC.

2. Debemos agregar comunidades desde la opción "*Seguridad*". Las comunidades se crean para que los agentes puedan enviar capturas al administrador y además puedan responder las solicitudes del administrador. Para nuestro proyecto hemos creado la comunidad denominada "private" se le ha asignado derechos de lectura y escritura. Además se debe incluir la dirección IP de nuestro Gestor es decir la IP 10.10.10.11, que es la máquina que va a aceptar paquetes SNMP de estos host que se les ha configurado la comunidad. Ver Figura 3.70.

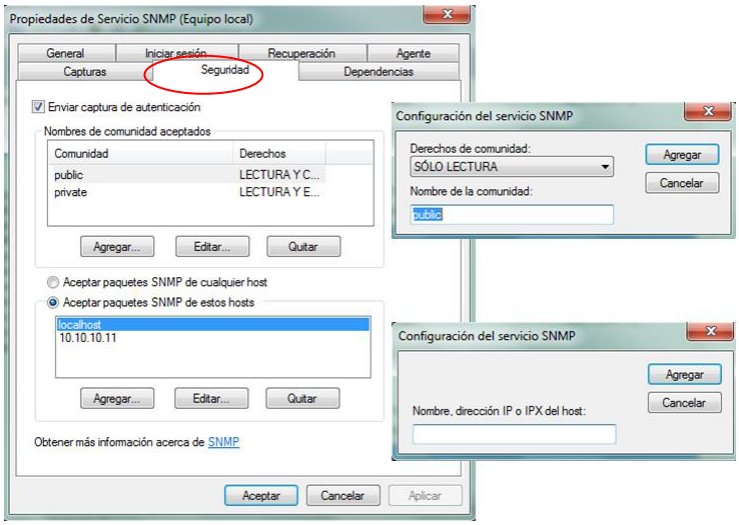


Figura 3.70: Configuración de Seguridad del Servicio SNMP en la PC.

3. El servicio SNMP proporciona una administración de red de protocolos TCP/IP y IPX/SPX si se requiere recibir capturas añadir a la lista las comunidades creadas. Ver Figura 3.71

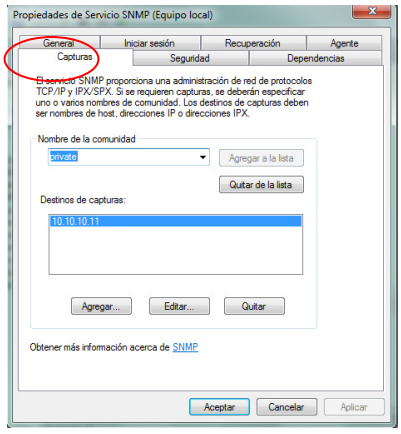


Figura 3.71: Configuración de Capturas del Servicio SNMP en la PC.

4. En vista que los sistemas de administración de internet suelen solicitar información de contacto, es necesario configurar el Agente, describiendo el nombre de contacto, ubicación del sistema y los servicios de red del equipo. Ver Figura 3.72

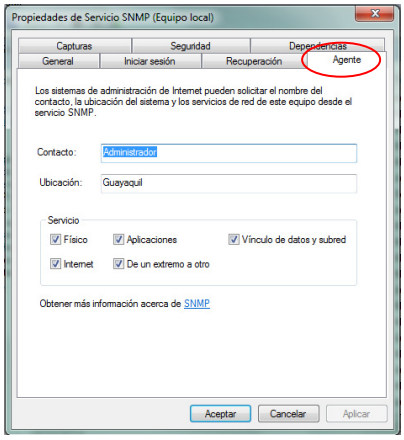


Figura 3.72: Configuración de Agente del Servicio SNMP en la PC.

3.4.5.2 Configuración de SNMP en OpenNMS

Para configurar SNMP en OpenNMS debemos entrar en el servidor web, seleccionar la opción "*Admin*". Seguidamente damos clic en la opción "*Configure SNMP by IP*". Configuramos SNMP a través de una dirección IP específica o por rangos, la comunidad y la versión. Véase en la Figura 3.73.

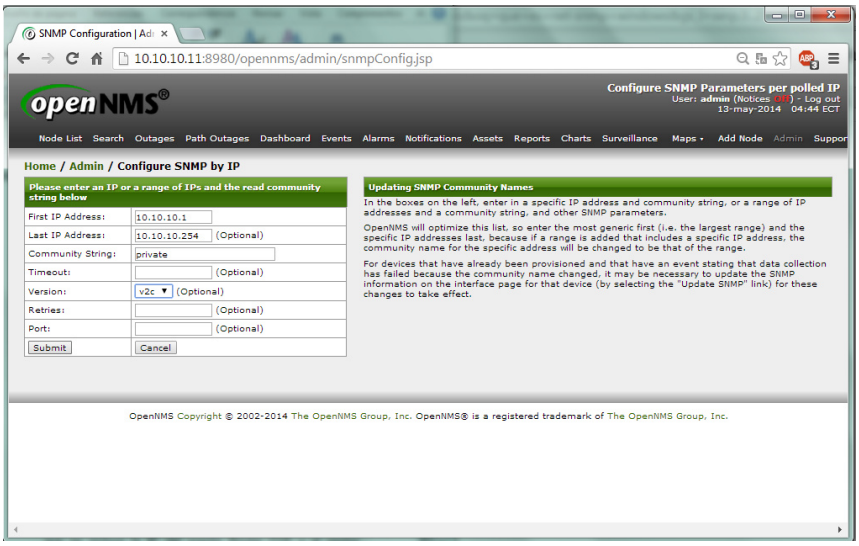


Figura 3.73: Configuración de SNMP en OpenNMS

Se ha configurado SNMPv2 con un rango de dirección IP, La IP de la Red 10.10.10.0; es decir de 10.10.10.1 – 10.10.10.254, nótese que se incluye la IP del agente Router GYE y el gestor ADMINISTRADOR. El nombre de la comunidad correspondiente “private” y la versión de SNMP “v2c”.

Se repite el procedimiento para todas las direcciones IP de los elementos de la red, también puede ingresar a través de rangos de IP para que detecte automáticamente las IP de los agentes. Véase en la Figura 3.74

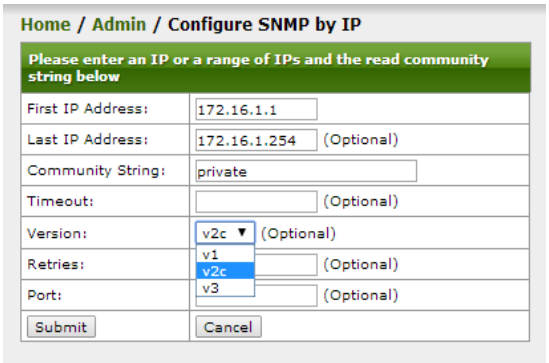


Figura 3.74: Configuración de SNMP en OpenNMS

Se ha configurado SNMPv2 con un rango de dirección IP, La IP de la Red 172.16.1.0; es decir de 172.16.1.1 – 172.16.1.254, nótese que se incluye la IP del agente Router QUITO, Router CUENCA, PC_1 y PC_2. El nombre de la comunidad correspondiente "private" y la versión de SNMP "v2c".

3.4.5.3 Configuración de SNMP en Routers

Para configurar SNMP en los routers QUITO, CUENCA y GYE se deben escribir los siguientes comandos, estos comandos permitirán que los agentes envíen capturas al administrador y puedan responder las solicitudes del Gestor.

Configuración SNMP en Router QUITO

```
QUITO#conf ter
QUITO(config)#snmp-server community private RW
QUITO(config)#snmp-server location Quito
QUITO(config)#snmp-server contact William Burbano
QUITO(config)#snmp-server enable traps
```

```
QUITO(config)#snmp-server host 10.10.10.11 version 2c private
QUITO(config)#snmp-server host 10.10.10.11 inform version 2c private
```

Configuración SNMP en Router CUENCA

```
CUENCA#conf ter
CUENCA(config)#snmp-server community private RW
CUENCA(config)#snmp-server location Cuenca
CUENCA(config)#snmp-server contact Liss
CUENCA(config)#snmp-server enable traps
CUENCA(config)#snmp-server host 10.10.10.11 version 2c private
CUENCA(config)#snmp-server host 10.10.10.11 inform version 2c private
```

Configuración SNMP en Router GYE

```
GYE#conf ter
GYE(config)#snmp-server community private RW
GYE(config)#snmp-server location Guayaquil
GYE(config)#snmp-server contact Administrador
GYE(config)#snmp-server enable traps
GYE(config)#snmp-server host 10.10.10.11 version 2c private
GYE(config)#snmp-server host 10.10.10.11 inform version 2c private
```

3.4.6 Configuración Básica de los Routers

En este proyecto se ha diseñado una red con consta de tres routers, el router QUITO se encuentra en la red LAN con dirección IP: 172.16.1.16/28, el router CUENCA se encuentra ubicado en la red LAN 172.16.1.32/29 y el router GYE se encuentra en la red LAN con dirección IP: 10.10.10.0/24. Ver Figura 3.2.

También se ha realizado subnetting para direccionar y proporcionar las direcciones IP a cada una de las interfaces de los elementos de la

red. La Tabla 3.2, muestra el cuadro de direccionamiento de cada elemento de red.

Tabla 3.2: Tabla de Direccionamiento de la Red

Dispositivo	Interfaz	Dirección IP	Máscara	Gateway
R1: QUITO	Fa0/0	172.16.1.17	255.255.255.240	N/C
	S0/0	192.168.10.1	255.255.255.252	N/C
	S0/1	192.168.10.5	255.255.255.252	N/C
R2: CUENCA	Fa0/0	172.16.1.33	255.255.255.248	N/C
	S0/0	192.168.10.6	255.255.255.252	N/C
	S0/1	192.168.10.10	255.255.255.252	N/C
R3: GYE	Fa0/0	10.10.10.1	255.255.255.0	N/C
	S0/0	192.168.10.2	255.255.255.252	N/C
	S0/1	192.168.10.9	255.255.255.252	N/C
ADMINISTRADOR	NIC	10.10.10.11	255.255.255.0	10.10.10.1
PC_1	NIC	172.16.1.18	255.255.255.240	172.16.1.17
PC_2	NIC	172.16.1.34	255.255.255.248	172.16.1.33

Se considerará como configuración básica de los ruteadores los siguientes puntos:

1. Configuración de los nombres de los hosts de los routers (R1, R2, R3)
2. Des habilitación de la búsqueda DNS.
3. Configuración de contraseña de modo EXEC privilegiado.
4. Configuración de contraseña para la conexión de las consolas.
5. Configuración de contraseña para las conexiones VTY.
6. Configuración de los puertos seriales y fast-ethernet con sus respectivas direcciones IP mostradas en la tabla de direccionamiento.
7. Configuración del Protocolo de Enrutamiento OSPF.

Configuración R1

- **Configuración básica**

```
router(config)#hostname QUITO
QUITO(config)#no ip domain-lookup
QUITO(config)#enable secret cisco
QUITO(config)#banner motd #SOLO PERSONAL AUTORIZADO#
QUITO(config)#line console 0
QUITO(config-line)#password cisco
QUITO(config-line)#logging synchronous
QUITO(config-line)#login
QUITO(config-line)#exit
QUITO(config)#line vty 0 4
QUITO(config-line)#password cisco
QUITO(config-line)#logging synchronous
QUITO(config-line)#login
QUITO(config-line)#exit
```

- **Configuración de interfaces**

```
QUITO(config)#int fa0/0
QUITO(config-if)#ip address 172.16.1.17 255.255.255.240
QUITO(config-if)#no shutdown
QUITO(config-if)#exit
QUITO(config)#int s0/0
QUITO(config-if)#ip address 192.168.10.1 255.255.255.252
QUITO(config-if)#clock rate 64000
QUITO(config-if)#no shutdown
QUITO(config-if)#exit
QUITO(config)#int s0/1
QUITO(config-if)#ip address 192.168.10.5 255.255.255.252
QUITO(config-if)#no shutdown
QUITO(config-if)#exit
```

- **Configuración del protocolo de enrutamiento OSPF**

```
QUITO(config)#router ospf  1
QUITO(config-router)#network 172.16.1.16 0.0.0.15 area 0
QUITO(config-router)#network 192.168.10.0 0.0.0.3 area 0
QUITO(config-router)#network 192.168.10.4 0.0.0.3 area 0
QUITO(config-router)#default-information originate
QUITO(config-router)#passive-interface FastEthernet0/0
QUITO(config-router)#exit
```

Configuración R2

- **Configuración básica**

```
router(config)#hostname CUENCA
CUENCA(config)#no ip domain-lookup
CUENCA(config)#enable secret class
CUENCA(config)#banner motd #SOLO PERSONAL AUTORIZADO#
CUENCA(config)#line console 0
CUENCA(config-line)#password cisco
CUENCA(config-line)#logging synchronous
CUENCA(config-line)#login
CUENCA(config-line)#exit
CUENCA(config)#line vty 0 4
CUENCA(config-line)#password cisco
CUENCA(config-line)#logging synchronous
CUENCA(config-line)#login
CUENCA(config-line)#exit
```

- **Configuración de interfaces**

```
CUENCA(config)#int fa0/0
CUENCA(config-if)#ip address 172.16.1.33 255.255.255.248
```

```
CUENCA(config-if)#no shutdown
CUENCA(config-if)#exit
CUENCA(config)#int s0/0
CUENCA(config-if)#ip address 192.168.10.6 255.255.255.252
CUENCA(config-if)#no shutdown
CUENCA(config-if)#exit
CUENCA(config)#int s0/1
CUENCA(config-if)#ip address 192.168.10.10 255.255.255.252
CUENCA(config-if)#clock rate 64000
CUENCA(config-if)#no shutdown
CUENCA(config-if)#exit
```

- **Configuración de interfaces**

```
CUENCA(config)#router ospf 1
CUENCA(config-router)#network 172.16.1.32 0.0.0.7 area 0
CUENCA(config-router)#network 192.168.10.4 0.0.0.3 area 0
CUENCA(config-router)#network 192.168.10.8 0.0.0.3 area 0
CUENCA(config-router)#default-information originate
CUENCA(config-router)#passive-interface FastEthernet0/0
CUENCA(config-router)#exit
```

Configuración R3

- **Configuración básica**

```
router(config)#hostname GYE
GYE(config)#no ip domain-lookup
GYE(config)#enable secret class
GYE(config)#banner motd #SOLO PERSONAL AUTORIZADO#
GYE(config)#line console 0
GYE(config-line)#password cisco
GYE(config-line)#logging synchronous
```

```
GYE(config-line)#login
GYE(config-line)#exit
GYE(config)#line vty 0 4
GYE(config-line)#password cisco
GYE(config-line)#logging synchronous
GYE(config-line)#login
GYE(config-line)#exit
```

- **Configuración de interfaces**

```
GYE(config)#int fa0/0
GYE(config-if)#ip address 10.10.10.1 255.255.255.0
GYE(config-if)#no shutdown
GYE(config-if)#exit
GYE(config)#int s0/0
GYE(config-if)#ip address 192.168.10.2 255.255.255.252
GYE(config-if)#no shutdown
GYE(config-if)#exit
GYE(config)#int s0/1
GYE(config-if)#ip address 192.168.10.9 255.255.255.252
GYE(config-if)#no shutdown
GYE(config-if)#exit
```

- **Configuración de interfaces**

```
GYE(config)#router ospf 1
GYE(config-router)#network 10.10.10.0 0.0.0.255 area 0
GYE(config-router)#network 192.168.10.0 0.0.0.3 area 0
GYE(config-router)#network 192.168.10.8 0.0.0.3 area 0
GYE(config-router)#default-information originate
GYE(config-router)#passive-interface FastEthernet0/0
GYE(config-router)#exit
```

CAPÍTULO 4

4. SIMULACIÓN Y PRUEBAS

4.1 DESCRIPCIÓN

En este capítulo se emplearán todas las herramientas mencionadas en el capítulo anterior con sus respectivas configuraciones para analizar y demostrar las primitivas del protocolo SNMPv2.

Para un mejor estudio del protocolo SNMPv2, se han creado tres escenarios en base a la misma topología pero con diferentes operaciones para analizar los paquetes y capturas tráfico SNMPv2.

OpenNMS mostrará el comportamiento de cada dispositivo y su funcionamiento en tiempo real.

4.2 PRUEBAS DE LA SIMULACIÓN DE RED VIRTUAL BASADA EN EL PROTOCOLO SNMPv2

Para realizar las pruebas de la simulación de la red virtual basada en el protocolo SNMPv2 se han creado tres escenarios, manteniendo la misma topología de red pero realizando algunas acciones para observar las primitivas del protocolo SNMPv2.

A continuación se detalla los escenarios creados:

- Escenario 1: Se mostrará las primitivas GetRequest y GetResponse a través de la comunicación de los agentes a la estación gestora, la PC denominado ADMINISTRADOR.
- Escenario 2: Se mostrará la primitiva GetBultRequest modificando el nombre de la comunidad del Router QUITO, para observar el comportamiento del protocolo SNMPv2 ante este suceso.
- Escenario 3: Se mostrará la operación de las primitivas InformRequest y SNMPv2-Trap apagando la interfaz fastethernet del Router GYE.

4.2.1 Escenario 1: Primitiva GetRequest y GetResponse

Una vez configurados todos los parámetros en todo el software, como se indicó en el capítulo anterior, se inicia GNS3, se simula la red

creada para activar todos los dispositivos previamente configurados. La red debe estar operando sin ningún problema; es decir los agentes deben enviar capturas y recibir las solicitudes del gestor.

En la estación real (ADMINISTRADOR) iniciamos el servidor web (Google Chrome) y entramos a OpenNMS como se indicó anteriormente, una vez que entremos a OpenNMS se puede monitorear, analizar las interfaces y los dispositivos configurados con SNMPv2.

OpenNMS mostrará si tiene algún fallo o corte con cualquier dispositivo, para este escenario se mostrará todo en funcionamiento es decir sin ningún corte y enviando capturas SNMPv2. Véase Figura 4.1.

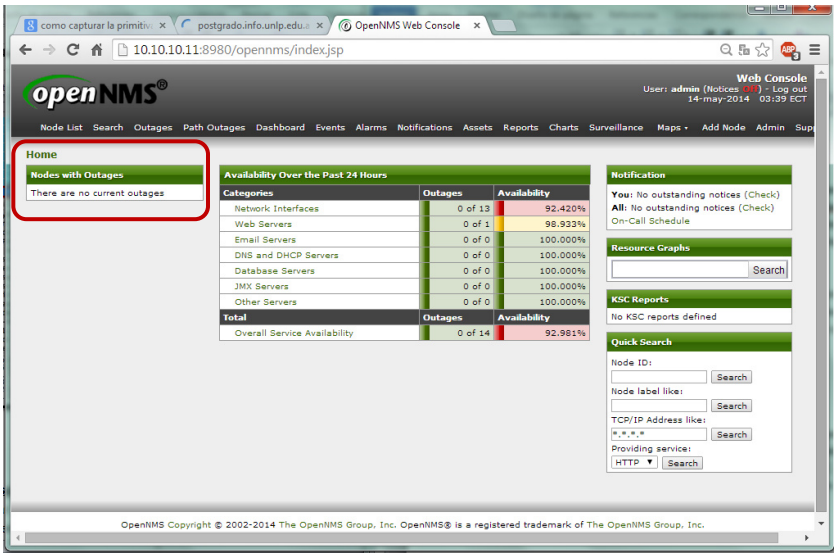


Figura 4.1: Monitoreo de la Red Virtual operando, Nodos sin Cortes

Al iniciar Wireshark desde el ADMINISTRADOR se puede apreciar que la estación gestora intenta comunicarse con los agentes; es decir les envía un “GetRequest”, Véase Figuras 4.2, 4.4, 4.6, y un “GetResponse” que es enviado por el elemento gestionado, Véase Figuras 4.3, 4.5, 4.7.

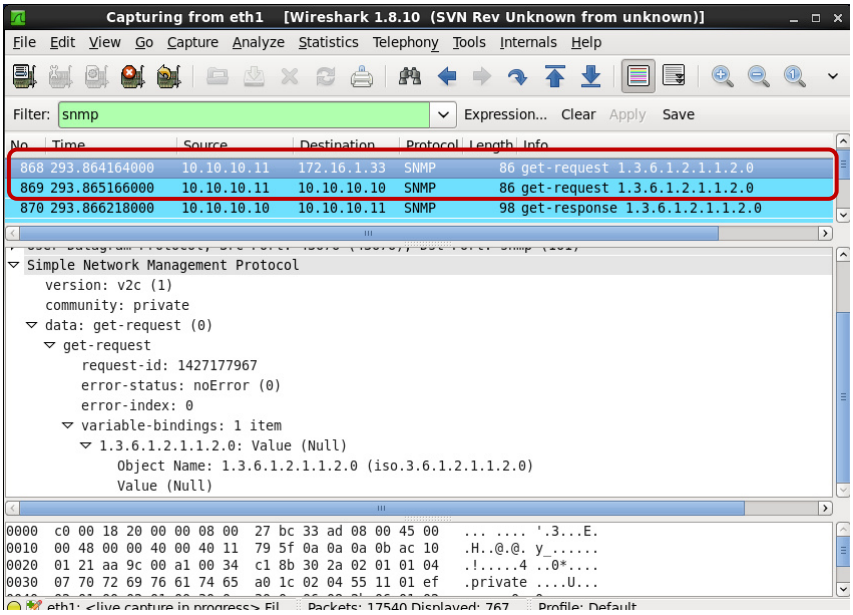


Figura 4.2: Get-Request SNMPv2 desde el ADMINISTRADOR al Router CUENCA

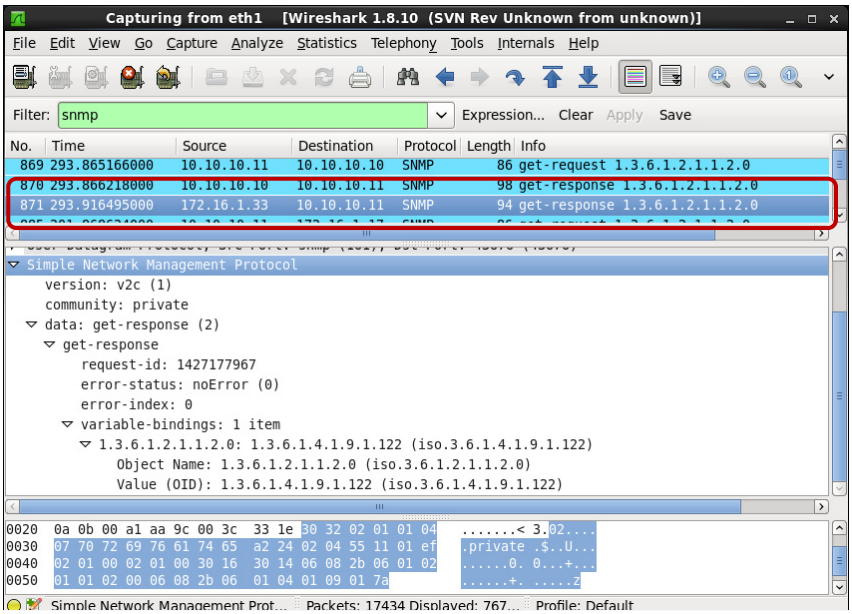


Figura 4.3: Get-Response SNMPv2 del Router CUENCA

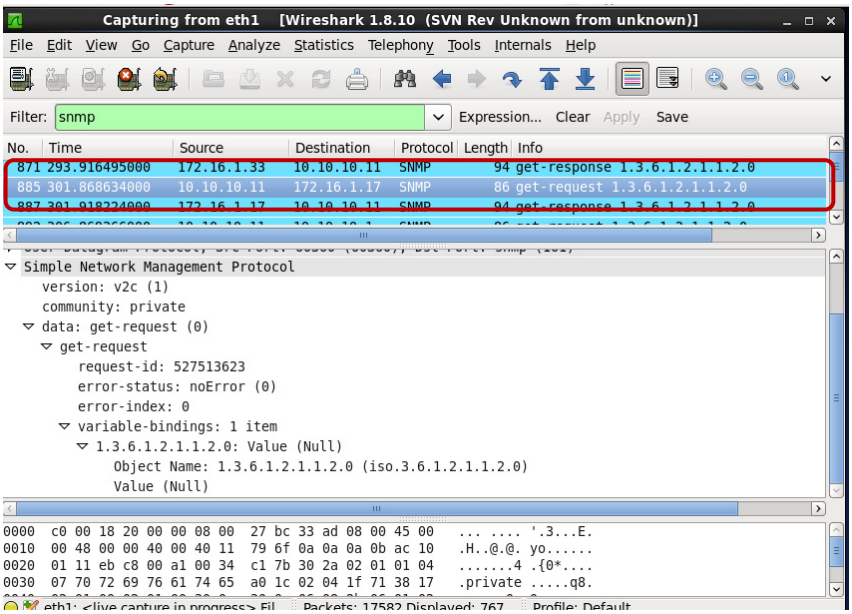


Figura 4.4: Get-Request SNMPv2 desde el ADMINITSRADOR al Router QUITO

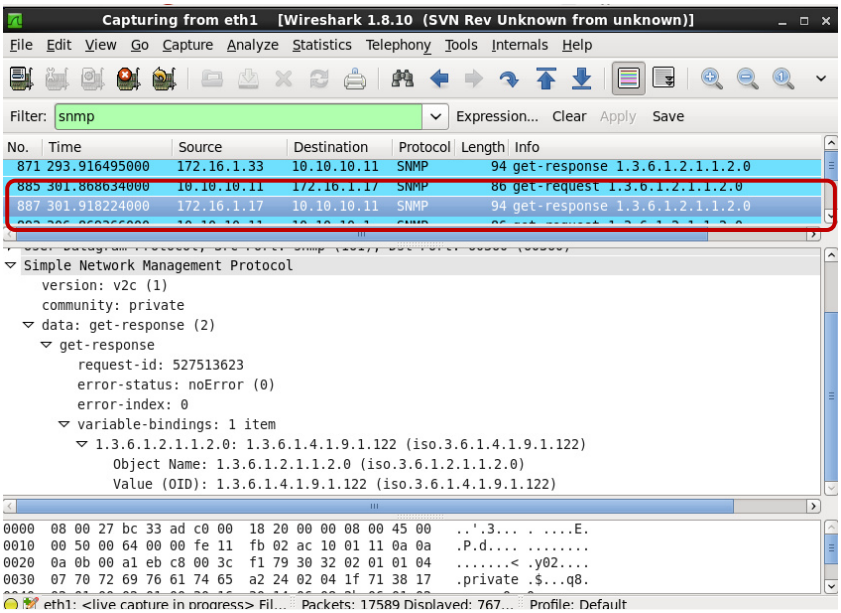


Figura 4.5: Get-Response SNMPv2 del Router QUITO

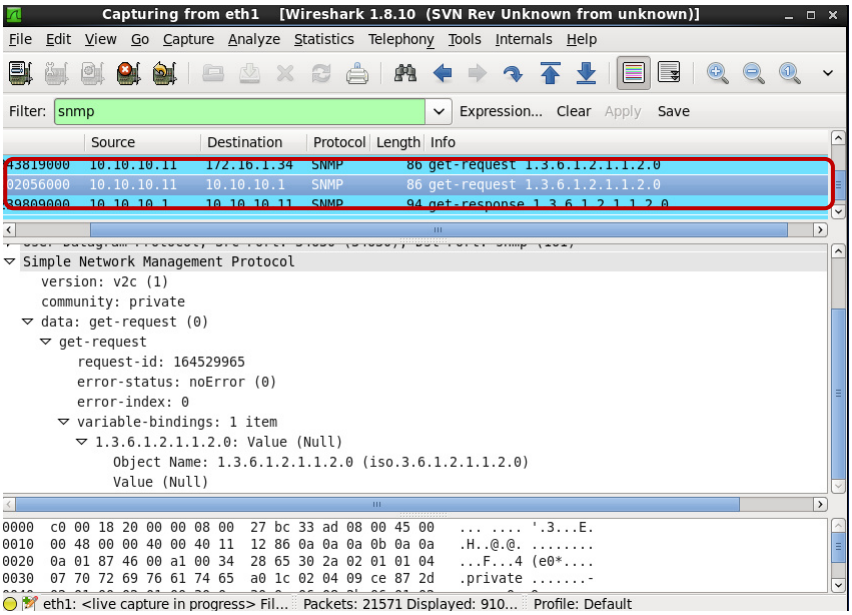


Figura 4.6: Get-Request SNMPv2 desde el ADMINISTRADOR al Router GYE

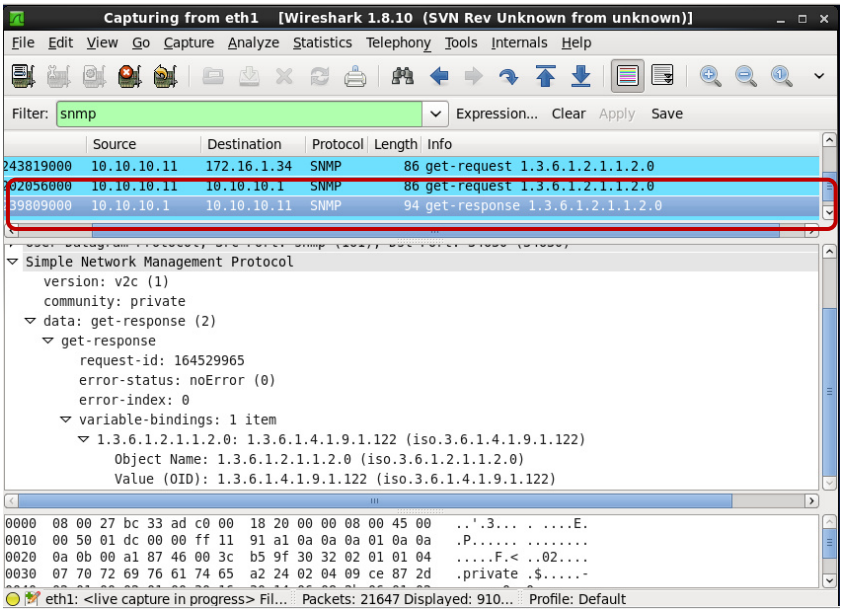


Figura 4.7: Get-Response SNMPv2 del Router GYE

4.2.2 Escenario 2: Primitiva GetBulkRequest

Se modificará el nombre de la comunidad del Router QUITO, para observar el comportamiento del protocolo SNMPv2 ante este suceso. Una vez iniciado, operando y en proceso de monitoreo como el escenario anterior, se procede a abrir la consola del Router QUITO, Véase Figura 4.8 y configurar el cambio de comunidad; es decir, primero se debe quitar la comunidad “private” y sustituir por “privado”, con los siguientes comandos:

```
QUITO#conf ter
QUITO(config)#no snmp-server community private RW
QUITO(config)#snmp-server community privado RW
QUITO(config)#end
QUITO#copy running-config startup-config
```

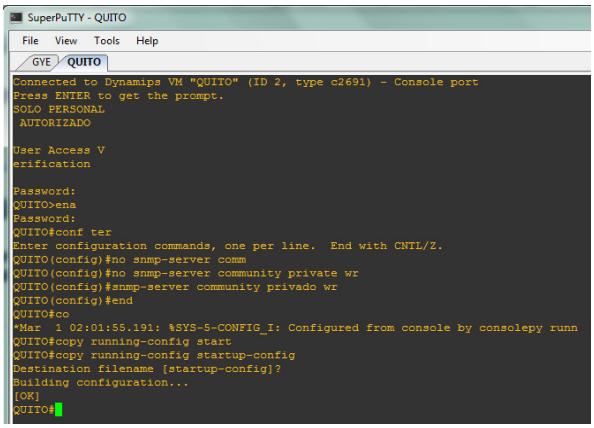


Figura 4.8: Configuración cambio de comunidad del Router QUITO

OpenNMS mostrará que ha existido en evento reciente, este evento denota que ha ocurrido una configuración de administración en el Router QUITO; cuya configuración impide el tráfico SNMP a los dispositivos. Véase Figura 4.9.

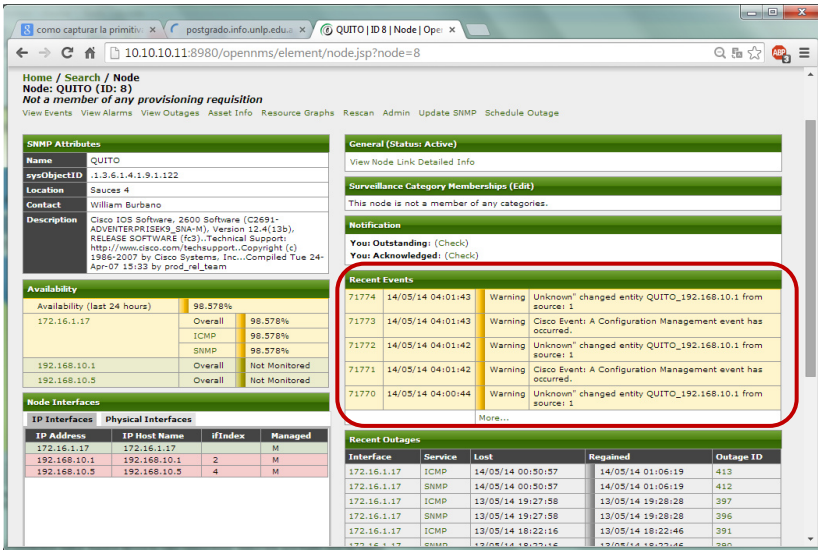


Figura 4.9: Notificación de un evento reciente en el Router QUITO

En Wireshark se muestra como el gestor intenta solicitar un “GetBulkRequest” al Router QUITO, Véase Figura 4.10, y un “SNMPv2-trap” es enviado por el dispositivo gestionado, Véase Figura 4.11. En cambio el Router GYE y CUENCA responde con un “GetResponse” a la solicitud del Gestor. Véase Figura 4.12, 4.13, 4.14, 4.15.

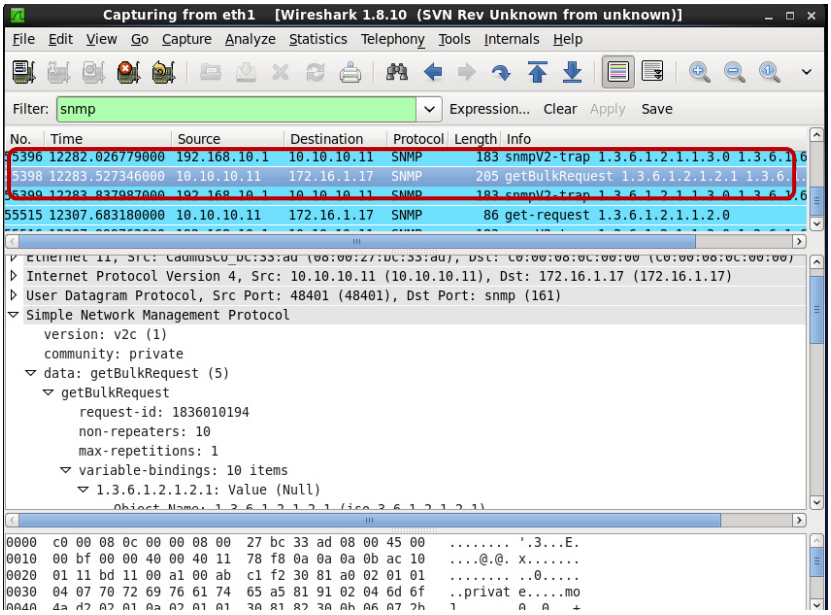


Figura 4.10: GetBulkRequest SNMPv2 desde el ADMINISTRADOR al Router QUITO

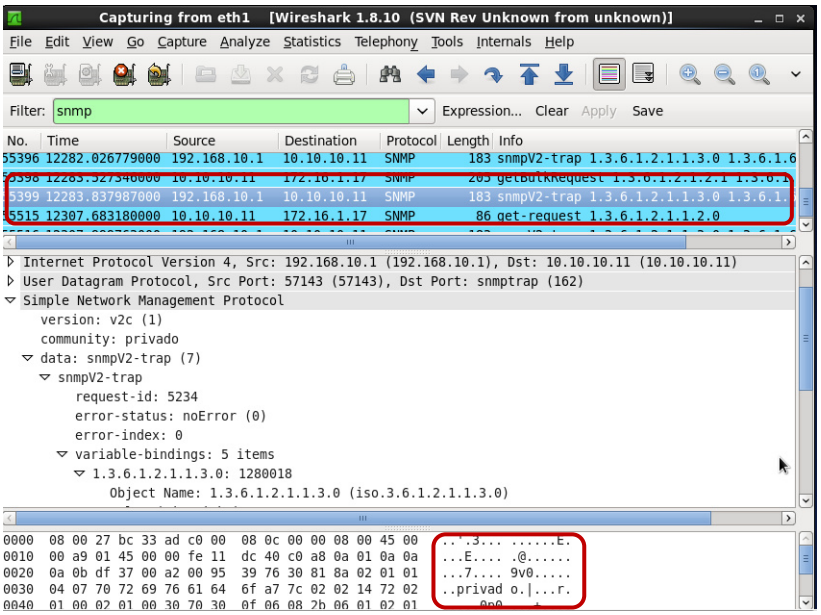


Figura 4.11: SNMPv2-Trap del Router QUITO

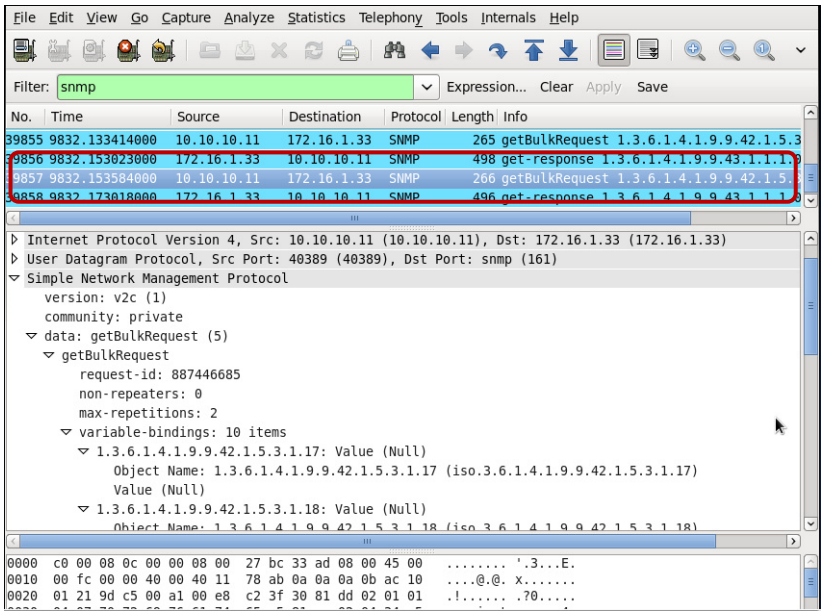


Figura 4.12: GetBulkRequest SNMPv2 desde el ADMINISTRADOR al Router CUENCA

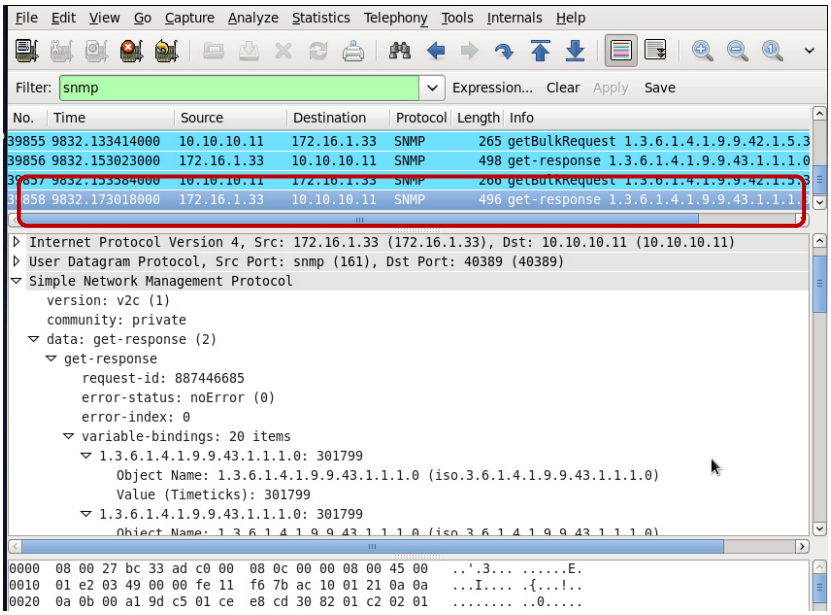


Figura 4.13: GetResponse SNMPv2 del Router CUENCA

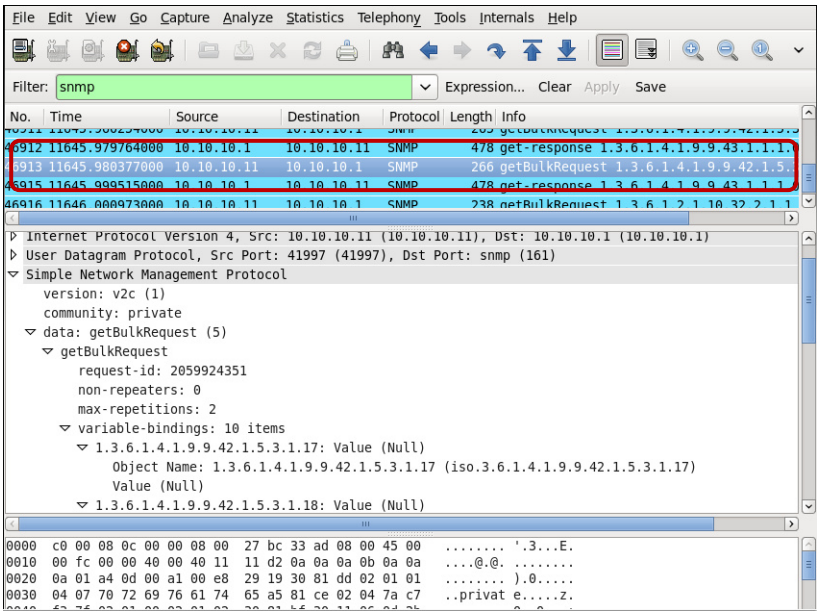


Figura 4.14: GetBulkRequest SNMPv2 desde el ADMINISTRADOR al Router GYE

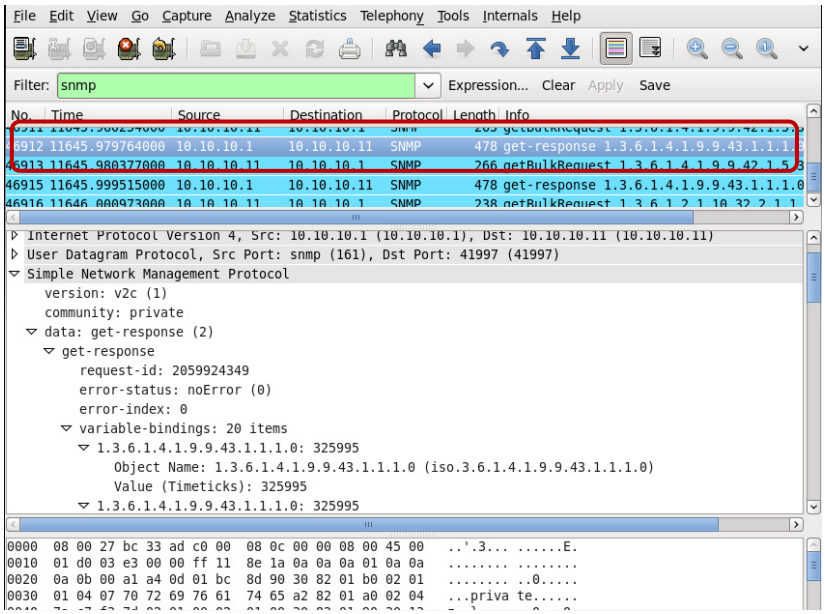


Figura 4.15: GetResponse SNMPv2 del Router GYE

4.2.3 Escenario 3: Primitiva InformRequest y SNMPv2-Trap

Para este escenario se repite el inicio de los demás escenarios para que la red se encuentre operando y en proceso de monitoreo, se procede a abrir la consola del Router GYE, Véase Figura 4.16 y realizamos los cambios respectivos; es decir, para activar las primitivas “InformRequest” y “SNMPv2-Trap” vamos a bajar la interfaz fastethernet 0/0 del Router GYE.

Para bajar la interfaz fastethernet 0/0 con dirección IP: 10.10.10.1/24, debemos ingresar los siguientes comandos:

```
GYE#conf ter
GYE(config)#interface fastethernet0/0
GYE(config)#shutdown
```

QUITO(config)#end
QUITO#copy running-config startup-config

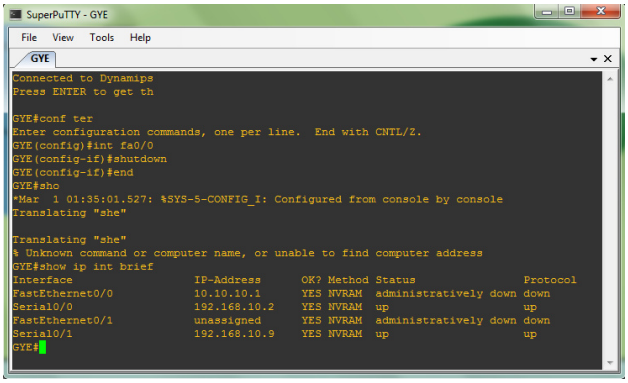


Figura 4.16: Configuración bajar interfaz 0/0 del Router GYE

OpenNMS nos mostrará que ha existido en evento reciente, este evento denota que han ocurrido cortes en los nodos y que el nodo GYE está down. Cuya configuración impide el tráfico SNMP a los dispositivos. Véase las Figura 4.17 y 4.18.

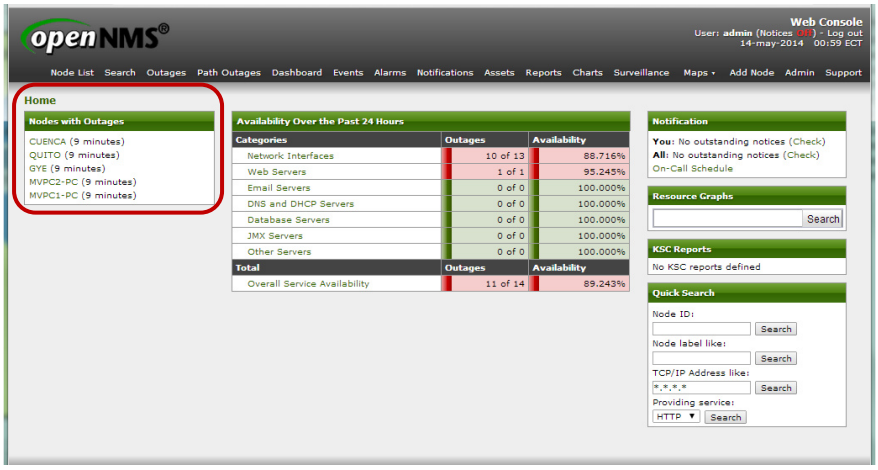


Figura 4.17: Notificación de un evento ocurrido: Corte en los Nodos.

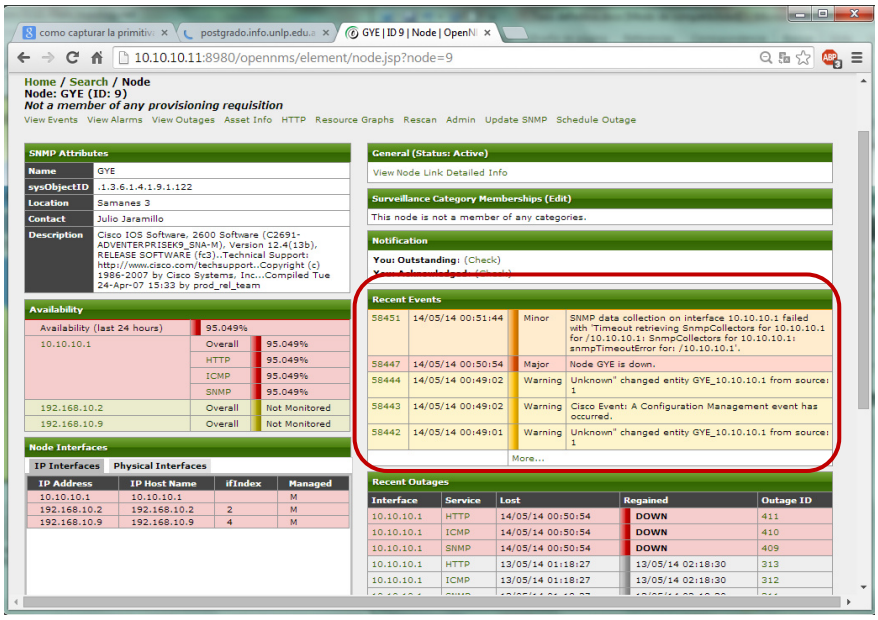


Figura 4.18: Notificación de un evento ocurrido: Nodo de GYE está down.

En Wireshark se muestra como el Router GYE al bajar la iinterfaz envía al gestor un “InformRequest”, Véase Figura 4.19, un “GetResponse” emite el Gestor, Véase Figura 4.20, y un “SNMPv2-trap” es enviado por el dispositivo gestionado, Véase Figura 4.21.

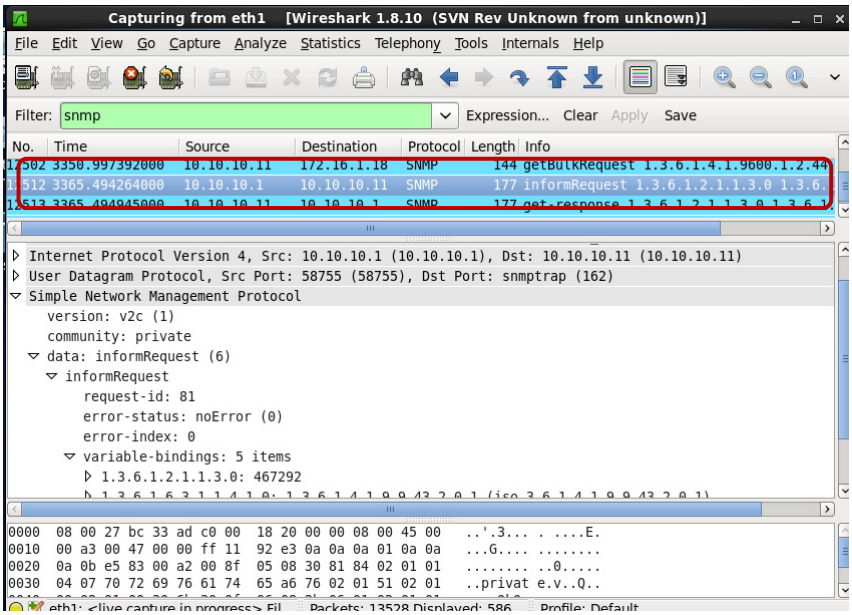


Figura 4.19: InformRequest SNMPv2 del Router GYE

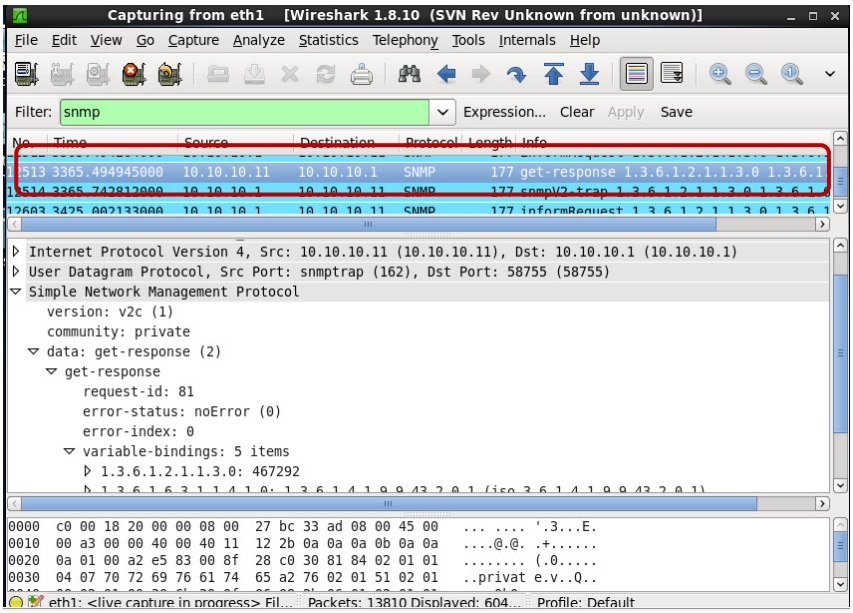


Figura 4.20: GetResponse SNMPv2 desde el ADMINISTRADOR al Router GYE

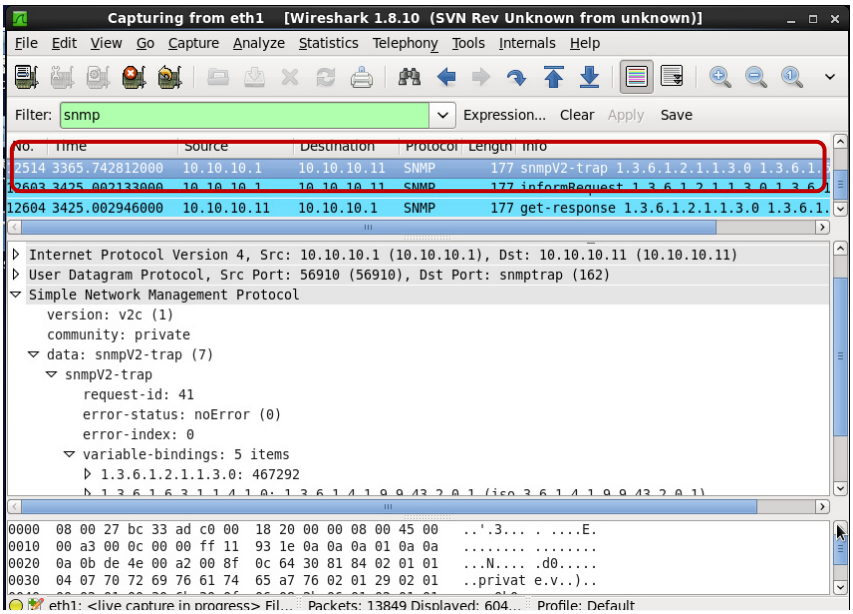


Figura 4.21: SNMPv2-Trap del Router GYE

CAPÍTULO 5

5. ANÁLISIS DE RESULTADOS

En este capítulo se describe todas las observaciones de los resultados obtenidos de cada uno de los escenarios, destacando las capacidades del protocolo SNMPv2, las mismas que reflejarán las ventajas y desventajas de dicho protocolo.

5.1 RESULTADOS ESCENARIO 1: Primitivas GetRequest y GetResponse.

Una vez configurado todos los equipos (agentes) con el protocolo SNMPv2 en la Red, automáticamente estos envían capturas SNMPv2 y responden solicitudes al Gestor.

Como se puede observar en la Figura 4.1 no existe ningún corte en los nodos y estos estando previamente configurados, envían tráfico SNMP. Es decir; para el Administrador, la Red opera correctamente.

Para ver internamente como los mensajes SNMPv2 son empaquetados y observar las primitivas se utilizará la herramienta Wireshark. La estación Gestora contiene la siguiente OID .1.3.6.1.2.1.1.2.0, la misma que se refiere al tiempo que lleva el elemento de red inicializado y automáticamente muestra un GetRequest y un GetResponse por cada elemento consultado, en este caso será:

- GetRequest desde la estación Gestora con IP 10.10.10.11 hasta el Router CUENCA con IP 172.16.1.33, véase Figura 4.2, y un GetResponse desde el Router CUENCA hasta la estación Gestora, véase Figura 4.3.
- GetRequest desde la estación Gestora con IP 10.10.10.11 hasta el Router QUITO con IP 172.16.1.17, véase Figura 4.4, y un GetResponse desde el Router QUITO hasta la estación Gestora, véase Figura 4.5.
- GetRequest desde la estación Gestora con IP 10.10.10.11 hasta el Router GYE con IP 10.10.10.1, véase Figura 4.6, y un GetResponse desde el Router GYE hasta la estación Gestora, véase Figura 4.7.

En Wireshark se muestra la captura SNMP de la configuración realizada, dentro de los campos están:

- La versión: "v2c" es la versión con la que se ha configurado los equipos; es decir muestra la versión del mensaje SNMP.
- community: "private" que como se pudo observar se muestra el nombre de la comunidad sin encriptar, pues la versión 2 del protocolo SNMP a pesar de que se mejoraron algunos componentes la seguridad sigue siendo un problema.
- request-id: "1427177967", este número entero indica el orden de emisión de los datagramas.
- Error-status: noError(0), indica que no se encontró ningún tipo de error en el proceso.
- Error-index: 0, no se ha encontrado ningún error, por lo tanto su respuesta es 0.
- variable-bindings: 1 item, indica que solo una variable fue analizada, además muestra el nombre del OID.

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

5.2 RESULTADOS ESCENARIO 2: Primitiva GetBulkRequest.

Así mismo como en el Escenario 1, una vez configurado todos los equipos (agentes) con el protocolo SNMPv2 en la Red, automáticamente estos envían capturas SNMPv2 y responden solicitudes al Gestor.

Para este escenario se ha modificado el nombre de la comunidad de “private” a “privado” en el Router QUITO, como se puede observar en la Figura 4.8. Recordemos que el nombre de la comunidad en el protocolo SNMP es muy importante para capturar mensaje SNMP, es decir el Gestor puede recibir las capturas SNMP cuando tienen el nombre de la misma comunidad.

OpenNMS muestra que ha existido un evento, puesto que esta herramienta detecta cualquier configuración en tiempo real; el evento indica que una configuración de administración ha ocurrido en el Router QUITO. Véase Figura 4.9.

Para ver internamente como los mensajes SNMPv2 son empaquetados y observar las primitivas, se empleará la herramienta Wireshark. La estación Gestora muestra un “GetBulkRequest” y cuando se ha cambiado el nombre a la comunidad responde un “SNMPv2-Trap” por el elemento consultado, en este caso será:

GetBulkRequest desde la estación Gestora con IP 10.10.10.11 hasta el Router QUITO con IP 172.16.1.37, véase Figura 4.10, y como respuesta un SNMPv2-Trap desde el Router QUITO hasta la estación Gestora, cabe destacar que en el “Trap” indica el nombre de la comunidad “privado”, es decir no llegará un “GetResponse” por parte de este Router. véase Figura 4.11.

Cuando tienen el mismo nombre de comunidad los agentes responden al Gestor de la siguiente manera:

- GetBulkRequest desde la estación Gestora con IP 10.10.10.11 hasta el Router CUENCA con IP 172.16.1.33, véase Figura 4.12, y como respuesta un GetResponse desde el Router CUENCA hasta la estación Gestora, véase Figura 4.13.
- GetBulkRequest desde la estación Gestora con IP 10.10.10.11 hasta el Router GYE con IP 10.10.10.1, véase Figura 4.14, y como respuesta un GetResponse desde el Router GYE hasta la estación Gestora, véase Figura 4.15.

En Wireshark se muestra la captura SNMP de la configuración realizada en el Router CUENCA, véase Figura 4.11, dentro de los campos están:

- La versión: "v2c" es la versión con la que se ha configurado los equipos; es decir muestra la versión del mensaje SNMP.
- community: "privado" que como se pudo observar se muestra el nombre de la comunidad sin encriptar, claramente se puede determinar que no está enviando capturas SNMP en vista que no tiene el mismo nombre de comunidad que el Gestor (private es el nombre de la comunidad del Gestor).
- request-id: "5234", este número entero indica el orden de emisión de los datagramas.
- Error-status: noError(0), indica que no se encontró ningún tipo de error en el proceso.
- Error-index: 0, no se ha encontrado ningún error, por lo tanto su respuesta es 0.

- variable-bindings: 5 item, indica que cinco variables fueron analizadas, además muestra el nombre del OID.

5.3 RESULTADOS ESCENARIO 3: Primitivas Inform y SNMPv2-Trap.

Así mismo, como en el Escenario 1, una vez configurado todos los equipos (agentes) con el protocolo SNMPv2 en la Red, automáticamente estos envían capturas SNMPv2 y responden solicitudes al Gestor.
Para este escenario se ha apagado la interfaz fastethernet 0/0 del Router GYE; es decir, la interfaz fastethernet 0/0 con IP 10.10.10.1 estará en estado “down”, Véase Figura 4.16. Esta interfaz es la conexión directa del administrador a toda la Red.

OpenNMS muestra que ha existido un evento, puesto que esta herramienta detecta cualquier configuración en tiempo real; el evento indica que una configuración de administración ha ocurrido en el Router GYE. Además informa que un Nodo en el Router GYE está “down”, Véase Figura 4.17.

Para ver internamente como los mensajes SNMPv2 son empaquetados y observar las primitivas, se utilizará la herramienta Wireshark. El Router GYE envía un “InformRequest” espontáneamente a la estación Gestora, y la estación Gestora responde una confirmación con un “GetResponse”, entonces el Router GYE envía un “SNMPv2-Trap” como alarma, en este caso será:

InformRequest desde el Router GYE con IP 10.10.10.1 hasta el Gestor con IP 10.10.10.11, véase Figura 4.18, y un GetResponse como mensaje de confirmación desde la estación Gestora al Router GYE, véase Figura 4.19, luego el Router GYE envía a la estación Gestora un “SNMPv2-Trap” como alarma, véase Figura 4.20.

En Wireshark se muestra la captura SNMP de la configuración realizada en el Router GYE:

1. Mensaje “InformRequest” del Router GYE a la estación Gestora, Véase Figura 4.18, dentro de los campos están:

    - La versión: "v2c" es la versión con la que se ha configurado los equipos; es decir muestra la versión del mensaje SNMP.
    - community: "private" que como se pudo observar se muestra el nombre de la comunidad sin encriptar, pues la versión 2 del protocolo SNMP a pesar de que se mejoraron algunos componentes la seguridad sigue siendo un problema.
    - request-id: "81", este número entero indica el orden de emisión de los datagramas.
    - Error-status: noError(0), indica que no se encontró ningún tipo de error en el proceso.
    - Error-index: 0, no se ha encontrado ningún error, por lo tanto su respuesta es 0.
    - variable-bindings: 5 item, indica que cinco variables fueron analizadas, además muestra el nombre del OID.

2. Mensaje “GetResponse” de la estación Gestora como mensaje de confirmación al Router GYE, Véase Figura 4.19, dentro de los campos están:

   - La versión: "v2c" es la versión con la que se ha configurado los equipos; es decir muestra la versión del mensaje SNMP.
   - community: "private" que como se pudo observar se muestra el nombre de la comunidad sin encriptar, pues la versión 2 del protocolo SNMP a pesar de que se mejoraron algunos componentes la seguridad sigue siendo un problema.
   - request-id: "81", este número entero indica el orden de emisión de los datagramas.
   - Error-status: noError(0), indica que no se encontró ningún tipo de error en el proceso.
   - Error-index: 0, no se ha encontrado ningún error, por lo tanto su respuesta es 0.
   - variable-bindings: 5 item, indica que cinco variables fueron analizadas, además muestra el nombre del OID.

3. Mensaje “SNMPv2-Trap” del Router GYE a la estación Gestora como alerta, Véase Figura 4.20, dentro de los campos están:

   - La versión: "v2c" es la versión con la que se ha configurado los equipos; es decir muestra la versión del mensaje SNMP.
   - community: "private" que como se pudo observar se muestra el nombre de la comunidad sin encriptar, pues la versión 2 del

protocolo SNMP a pesar de que se mejoraron algunos componentes la seguridad sigue siendo un problema.

- request-id: "41", este número entero indica el orden de emisión de los datagramas.
- Error-status: noError(0), indica que no se encontró ningún tipo de error en el proceso.
- Error-index: 0, no se ha encontrado ningún error, por lo tanto su respuesta es 0.
- variable-bindings: 5 item, indica que cinco variables fueron analizadas, además muestra el nombre del OID.

CONCLUSIONES

1. SNMP es un protocolo de administración de red que facilita el intercambio de información a través de una estación de gestora y un agente.

2. SNMP se compone de dispositivos administrados, que es un nodo en la red y contiene al agente SNMP, además son controlados por los agentes y los sistemas que administran la red.

3. GNS3 es una excelente alternativa para simular redes, puesto que brinda servicio orientado al funcionamiento de redes reales, sin necesidad de hardward. Es de mucha utilidad en el mundo empresarial, puesto que reduce el costo de implementación de redes; como en el mundo académico, debido a que trabaja con herramientas que permiten emular las imágenes del IOS y configurar a través de su interfaz de texto y su interfaz gráfica, esto hace más accesible el estudio del networking.

4. Se demostró que GNS3 proporciona una interfaz gráfica que permite configurar redes virtuales, implementar máquinas virtuales e incluso establecer conexiones físicas con equipos reales externos hacia el entorno virtual de la red. Además permite realizar captura de los paquetes que pasan por sus enlaces virtuales

5. OpenNMS es una herramienta útil de monitoreo y administración de una red, puesto que está diseñado para ser totalmente personalizable; es decir, poder trabajar en una amplia variedad de entornos de red y a su vez crear una solución única e integrada de administración.

6. Los escenarios creados permitieron apreciar la operación y la gestión de las primitivas del protocolo SNMPv2 (GetRequest, GetResponse, GetBulkRequest, InformRequest y SNMPv2-Trap).

7. Se comprobó que SNMPv2 agrega dos operaciones GetBulk e Inform. La operación “GetBulk” recupera información de administración de gran tamaño usando pocos recursos de red e “Inform” permite que un dispositivo administrado envíe Traps hacia otro dispositivo administrado y luego reciba una respuesta por el sistema de administración de la red.

8. A través de la herramienta Wireshark se pudo comprobar la teoría del protocolo SNMPv2, puesto que muestra el empaquetamiento del mensaje SNMP. El protocolo SNMPv2 es una versión mejorada del SNMPv1 que incluye mejores políticas de autenticación y seguridad, pero como se pudo apreciar en la captura, no encripta al cambiar el nombre de la comunidad de un dispositivo administrado, tiene algunas falencias que en teoría lo cubriría la versión 3.

RECOMENDACIONES

1. Para evitar el consumo excesivo de recursos del equipo en el que se ejecuta GNS3, se debe tener una IOS que tenga las funciones necesarias de cada elemento de la red y elegir un buen valor IDLE-PC para la optimización del uso del CPU y la memoria.

2. Para un mejor rendimiento de la red simulada, es necesario que el software GNS3 se ejecute en un equipo con buenas características; puesto que las capacidades de procesamiento óptimas del emulador GNS3 dependen de la cantidad de routers que se desean emular; es decir, se requerirán más recursos del sistema si se quieren emular topologías con varios routers.

3. Se recomienda que para la elaboración de este proyecto se utilice un equipo aproximadamente con las siguientes características: un procesador Intel Core i3 2.1 GHz y 4 GB de Memoria RAM, en vista que requiere de varias herramientas para instalar los software. Este proyecto fue realizado en un computador con las siguientes características: Procesador Intel Core i7 de 2.20 GHz y 8 GB de Memoria RAM.

4. Se aconseja desactivar y eliminar todas las interfaces de red que no se desea monitorear, puesto que OpenNMS posee una característica que descubre los nodos y las direcciones IP. En

caso que detecte también es posible eliminar la dirección IP del proceso de monitoreo.

5. En Wireshark se recomienda filtrar los paquetes obtenidos por el tipo de protocolo al que pertenecen; es decir, sólo es necesario capturar el tipo de protocolo que se desea estudiar.

6. Se recomienda ejecutar el Procesador de Comandos de Windows en modo “Administrador” cuando se inicie OpenNMS, en vista que este software opera en un servidor web y necesitará los privilegios del administrador para que se ejecute correctamente.

BIBLIOGRAFÍA

[1] Principia Technologica (2013 Abril 7). *Introducción a SNMP – Protocolo de Gestión de Red "¿Simple?"*. Obtenido el 15 de abril de 2013, de http://principiatechnologica.wordpress.com/2013/04/07/introduccion-a-snmp-protocolo-de-gestion-de-red-simple/

[2] Universitat de València (2008). *Asignatura de Arquitectura de Redes y Servicios*. Recuperado el 15 de Abril de 2013, de http://informatica.uv.es/it3guia/ARS/transparencias_1c/snmp-santi.ppt

[3] Escuela Superior Politécnica del Litoral (2002*). Implementación de Funciones de Gestión a la Red LAN de la compañía MAINT usando HP OpenviewNode Manager*. Recuperado el 25 de Abril de 2013, de http://www.dspace.espol.edu.ec/bitstream/123456789/3085/1/5602.pdf

[4] Unai Estébanez Sevilla (1999). *Introducción a SNMP*. Recuperado el 26 de Abril de 2013, de "http://www.unainet.net/documents/SNMP.pdf" no se encontró

[5] Universidad Autónoma Metropolitana (2005). *Una Herramienta de Gestión deRedes Virtuales*. Recuperado el 25 de Abril de 2013, de http://newton.azc.uam.mx/mcc/02_ingles/11_tesis/tesis/terminada/Abraham%20Jimenez/08%20Cap2.-SNMP.pdf

[6] Asensio, Juan (1995). *SNMPv2 y SNMPv3.* Recuperado el 25 de Abril de 2013, de

https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCYQFjAA&url=http%3A%2F%2Fdesa.tel.uva.es%2Fdescargar.htm%3Bjsessionid%3DCC738A79B365BCD55C6EC0EB8D332EFC%3Fid%3D367&ei=e30rU6P7DIS7kQfG_IHwCw&usg=AFQjCNE3X72p-jNZhbSFITO20u74OUOpNQ&bvm=bv.62922401,d.eW0&cad=rja

[7] Informática y Telecomunicaciones (2010). *SNMP Protocol*. Recuperado el 26 de Abril de 2013, de http://infotelecommil.webcindario.com/librostelecom/SNMP.pdf

[8] Universidad de Jaén departamento de ingeniería electrónica de telecomunicación y automática (2007). *SNMPv2.* Recuperado el 18 de abril de 2014, de http://www4.ujaen.es/~mdmolina/grr/Tema%203.pdf.

[9] Jim Orrill. (S.F.). *SNMPv2 y v3*. Obtenido el 21 de abril de 2014, de http://www.ehowenespanol.com/snmp-v2-v3-info_307979/

[10] Adhirudran. (2010 Octubre 29). Simple Network Management Protocol Version 2-SNMPv2. Obtenido el 5 de mayo de 2014, de http://adhirudran.blogspot.com/

[11] Paula Montoto Castelao. (2009). *Gestión Internet.* Recuperado el 28 de abril de 2014, de http://quegrande.org/apuntes/EI/OPT/XR/teoria/08-09/08_-_gestion_internet_5.pdf

[12] Gamarra, Rodríguez R.; Villacastin Candil L. (2011). *Proyecto de sistemas informáticos.* Recuperado el 30 de abril de 2014, de http://eprints.ucm.es/13093/1/memQuaggaSNMP.pdf

[13] Cisco CertificationKits. (S. F.). *Implementing a High Avaliable Network*. Obtenido el 1 de mayo de 2014, de http://www.certificationkits.com/cisco-certification/Cisco-CCNP-SWITCH-642-813-Exam-Study-Guide/cisco-ccnp-switch-high-availability-a-redundancy.html

[14] Lucas Morea. (2001). *Aplicaciones del protocolo TCP/IP.* Obtenido el 30 de abril de 2014, de http://www.monografias.com/trabajos7/tcp/tcp.shtml#SNMP

[15] Computer Informacion. (S. F.). *SNMP V1 Vs V2.* Obtenido el 3 de mayo de 2014, de http://ordenador.wingwit.com/Redes/local-networks/71460.html

[16] Red Iris. (2007). *La seguridad en la familia de protocolos SNMP.* Recuperado el 21 de Marzo de 2014, de https://www.rediris.es/difusion/publicaciones/boletin/50-51/ponencia16.html.

[17] González, L. (2012). *Planificación y Gestión de la Red.* Recuperado el 3 de Febrero de 2014, de http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-II.pdf

[18] Escuela Superior Politécnica de Chimborazo (2013*). Interconectividad de routers emulados mediante GNS3 con routers emulados físicos.* Recuperado el 06 de Febrero de 2014, de http://dspace.espoch.edu.ec/bitstream/123456789/2714/1/18T00533.pdf.

[19] The OpenNMS Group. (2002). *OpenNMS.* Recuperado el 10 de Enero de 2014, de http://www.opennms.org/about/

[20] Oracle Corporation (2004). *Oracle VM VirtualBox.* Recuperado el 08 de Diciembre de 2013, de http://www.virtualbox.org/manual/UserManual.html

[21] Descargas De Internet (2012). *Descargar Wireshark 1.6.6 (64 bits)*. Recuperado el 16 de Diciembre de 2013, de http://descargas-de-internet.blogspot.com/2012/08/descargar-wireshark-166-64-bits.html

[22] Wikipedia. (n/d). *Sistema Operativo*. Extraído el 27 de octubre de 2013, desde http://es.wikipedia.org/wiki/Sistema_operativo

[23] Wikipedia. (n/d). *Microsoft Windows*. Extraído el 27 de octubre de 2013, desde http://en.wikipedia.org/wiki/Microsoft_Windows

[24] Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona. *Evaluación de la herramienta de GNS3 con conectividad a enrutadores reales. Obtenido el 27 de junio de 2013, desde http://upcommons.upc.edu/pfc/bitstream/2099.1/9989/1/PFC_Lisset_D%C3%ADaz.pdf*

[25] Pharalax Blog (S.F.). *Introduccion al Protocolo SNMP.* Obtenido el 18 de mayo de 2014, de http://pharalax.com/blog/introduccion-al-protocolo-snmp/.

[26] Cisco System (2008). *Cisco 2600 Series Modular Access Routers.* Obtenido el 18 de mayo de 2014, desde http://www.cisco.com/c/en/us/products/collateral/routers/2600-series-multiservice-platforms/product_data_sheet0900aecd800fa5be.pdf.