UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

TESIS PARA TITULO PROFESIONAL

"ALTERNATIVAS DE CONFIGURACIÓN CON EL USO DE LOS PROTOCOLOS SYSLOG Y SNMP PARA LA GESTIÓN DE RED DE REDES AVANZADAS"

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO EN INFORMÁTICA Y SISTEMAS

Elaborado por:

RAMIREZ DIAZ, EFLL YOVANKA

Asesores:

MG. WILLIAM ROGELIO MARCHAND NIÑO

M. EN C. JOSÉ IGNACIO CASTILLO VELÁZQUEZ

Tingo María – Perú

Agosto, 2019

Universidad Nacional Agraria de la Selva Facultad de Ingeniería en Informática y Sistemas	ACTA DE SUSTENTACIÓN DE TESIS N.º 05-2019	COMISION DE GRADOS Y TITULOS Fecha: 25/Octubre/2019

PARTE 1. FASE INICIAL

Siendo las 10:10 horas del día 25 de OCTUBRE de 2019; en la Sala de Grados de la FIIS, se instala el jurado calificador conformado por:

Jurado 1: Ing. Gregorio VASQUEZ PINEDO (Presidente)

Jurado 2: M.Sc. Nilton CHUCOS BAQUERIZO

Jurado 3: Ing. José Martín SANTILLAN RUIZ

Oficializado mediante **Resolución N.º 134-2019-D-FIIS-UNAS** del 11 de setiembre de 2019, para el proceso de sustentación del informe final de Tesis de la bachiller **Efl Yovanka RAMIREZ DIAZ,** titulado: **"ALTERNATIVAS DE CONFIGURACIÓN CON EL USO DE LOS PROTOCOLOS SYSLOG Y SNMP PARA LA GESTIÓN DE REDES AVANZADAS".** ASESOR: **Mg. William Rogelio MARCHAND NIÑO,** y CO-ASESOR **M. EN C. José Ignacio CASTILLO VELÁZQUEZ.**
Se manifiesta que la bachiller cumple con los requisitos exigidos de Ley y se le invita a disertar su Tesis por espacio de 30 minutos, asimismo se dispondrá de igual tiempo para la absolver preguntas y sugerencias.

PARTE 2. FASE DE PREGUNTAS Y RESULTADO

Culminada la exposición se inicia la fase de preguntas por parte del jurado calificador; también se invita a los asistentes a formular preguntas sobre el tema de Tesis.
Absueltas todas las peticiones, el jurado calificador procede a deliberar en privado la calificación y resultado.
Concluida la deliberación y en presencia del público asistente, el jurado calificador anuncia que el resultado de la Sustentación de Tesis es: APROBADO POR UNANIMIDAD
(NOTA: consignar una de la siguientes: DESAPROBADO, APROBADO POR MAYORIA o APROBADO POR UNANIMIDAD)
Con calificativo de: EXCELENTE
(NOTA: consignar una de la siguientes: EXCELENTE, MUY BUENO, BUENO, DEFICIENTE, MUY DEFICIENTE)
Por lo que se comunicará a las instancias correspondientes para el trámite respectivo.

PARTE 3. CONFORMIDAD

De todo lo mencionado se firma al pie en señal de conformidad, siendo las 11:20 horas se da por finalizada la ceremonia de Sustentación de Tesis.

Firma:	Firma:	Firma:
Jurado 1: GREGORIO VASQUEZ	Jurado 2: NILTON CHUCOS B.	Jurado 3: JOSE SANTILLAN R.
Firma:		
Sustentante: EFLL YOVANKA RAMIREZ DIAZ	Asesor: William R. Marchand Niño	

DEDICATORIA

A mi Madre, mi mayor fuente de inspiración para superarme cada día, como persona y profesional. Por sus valores y principios que me inculco a lo largo de mi vida, además del gran esfuerzo que hizo para poder forjar mi educación, aquella a la cual le debo más que la vida y a quien viviré eternamente agradecida.

A mi Hermana Yovi Flor, quien es mi mayor adoración, a la que deseo sea un ejemplo para tantos logros que ella desee alcanzar.

A mis Abuelos; Mi mamá Etelvina y desde el cielo Mi Papá Roberto, que siempre me brindaron sus consejos, amor y comprensión. Gracias por haber inculcado en mí siempre un espíritu de superación.

AGRADECIMIENTO

A Dios por brindarme la sabiduría necesaria, guiar mis pasos y ponerme a personas extraordinarias que me encaminaron y ayudaron a culminar esta etapa académica muy importante.

A mi asesor Mg. William Rogelio Marchand Niño, quien tiene todo mi admiración y respeto como profesional y ser humano; por todo lo inculcado a lo largo de mi carrera profesional, y el compromiso depositado en esta investigación, sin su orientación y conocimientos, no hubiese sido posible cimentar este proyecto.

Al M. en C. José Ignacio Castillo Velázquez, asesor del trabajo de investigación, por haber aceptado ser parte de esta investigación, dedicándole tiempo necesario para impartir sus conocimientos para lograr con éxito esta investigación.

A Víctor Raúl Cobos P., mi compañero entrañable desde el inicio académico; por permanecer a mi lado en esta etapa brindándome su cariño, paciencia y gran apoyo; alentándome siempre a culminar este trabajo de investigación.

A mi Familia, amigos y compañeros de clase, quienes de algún modo me brindaron siempre palabras de aliento y consejos.

Agradecer también, a la Universidad Nacional Agraria de la Selva, mi Alma Mater, y profesores de la Facultad de Informática y Sistemas, por sus conocimientos impartidos.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación denominada “Alternativas de Configuración con el uso de los protocolos Syslog y SNMP para la Gestión de Redes Avanzadas”, se basa en la evaluación de los protocolos para aprovechar así sus capacidades. Este estudio identifica a dos protocolos comúnmente utilizados para la gestión de red, con amplia difusión y disponibilidad en los dispositivos propios de una red avanzada; con el objetivo de determinar la mejor alternativa de configuración en un entorno emulado de la gestión de una red avanzada considerando la configuración de los protocolos en los equipos, el uso de recursos, la seguridad que presentan y los servicios disponibles.

Debido a que la Red Académica Peruana se encuentra inactiva, como primera fase de este trabajo de investigación se realizó la propuesta de una topología con el fin de reinsertar a la Red Académica Peruana a la Red CLARA, además de usarlo como escenario para la emulación que es parte del estudio.

La segunda fase consistió en la emulación de los protocolos Syslog, SNMP v2c y 3 cada uno configurado en la misma topología, pero en escenarios distintos para realizar pruebas independientes de cada protocolo. Las pruebas realizadas demostraron que Syslog y SNMPv3 poseen capacidades propias cada una de ellas, pero que pueden complementarse configurándose de forma paralela; SNMPv3 se cataloga como una configuración “compleja” frente a SNMPv2c y Syslog que se considera entre “regular” y “simple”; además de presentar mayor consumo de recursos computacionales sobreponiéndose en el uso del CPU, memoria y ancho de banda (3.10%, 0.6KB, 0.23kbps) versus un Syslog más ligero consumiendo CPU, memoria y ancho de banda (0.5%, 0.3 KB,

0.07kbps); pero también se determinó que el nivel de seguridad *authpriv* del protocolo SNMPv3 presenta un nivel de seguridad “alto” por encima de SNMPv2c y Syslog, esto explica el mayor consumo de recursos e incluso el nivel de complejidad en la configuración. El protocolo que presenta mayores indicios favorables de los servicios disponibles para cada mensaje es Syslog, porque aporta mayor disponibilidad de información.

INTRODUCCIÓN

Las Redes Avanzadas conocidas como redes académicas son redes específicas para la investigación y educación, el tipo de infraestructura que presentan son robustas y de alta demanda por mantener un servicio fluido en la red. Por otro lado, la gestión de redes se encarga justamente de mitigar posibles fallos que expongan a la red a cortes de operatividad, siendo fundamental el uso de los protocolos que se configuran para este fin.

Actualmente en el mercado existe una diversidad de protocolos desde los propietarios hasta los denominados *open source*, pero este estudio se basó en determinar la mejor alternativa de configuración con el uso de Syslog y SNMP, proponiendo una nueva topología de la red troncal integral para la red avanzada del Perú, con el fin de emular sobre esta las pruebas correspondientes que nos lleven alcanzar nuestro objetivo.

En este punto es importante clarificar que al hablar de “redes avanzadas” no nos referimos a la “Internet comercial”, sino a aquella red de Interrnet 2 la cual es completamente independiente.

El capítulo I “Diagnóstico”, describe la importancia de la gestión de Redes Avanzadas abordando los protocolos SNMP y Syslog, además se propuso crear una topología para la RAAP, ya que actualmente en el Perú está inactiva.

El capítulo II “Revisión de Literatura”, describe los antecedentes de emulación y gestión de Redes Avanzadas; además del Marco Teórico y Marco Conceptual, donde se incluye las definiciones de Redes Avanzadas, Gestión de

Redes, los protocolos SNMPv2c, SNMPv3 y Syslog; además de direcciones IPv6.

El capítulo III “Diseño de la RAAP”, describe el diseño de la nueva topología para la Red Académica Peruana (RAAP), teniendo en cuenta las principales características que se consideraron para lograr este fin; además, se evalúan las herramientas de gestión de red comercial y *open source*, siendo seleccionado la herramienta de gestión de red PRTG.

El capítulo IV “Emulación de Redes Avanzadas con protocolos Syslog y SNMP: caso RAAP” describe detalladamente la emulación de la RAAP que se realizó en el software emulador GNS3, donde se hizo uso de la herramienta de gestión PRTG.

El capítulo V “Materiales y Métodos”, describe las pruebas realizadas de la evaluación de los protocolos Syslog y SNMP; además de los instrumentos utilizados, medición de las variables, indicadores y validación de Hipótesis.

I. DIAGNÓSTICO

1.1. Marco referencial del problema

Las redes de datos son un ámbito de constante desarrollo e innovación, en esta época ha comenzado a sumar importancia el manejo de la información y el uso de la red, debido a que empresas y entidades educativas brindar sus servicios y cimientan sus comunicaciones a través de las redes de datos.

El inicio de la red de datos surge con la creación de la primera WAN en 1969, cuando ARPANET *(Advanced Research Projects Agency Network)* logra conectar a universidades de Estados Unidos, uniendo inicialmente 4 nodos que fueron distribuidos en el instituto de Investigación de Stanford (SRI) ubicado en California, a la vez dos campus de la Universidad de California ubicados en los Ángeles (UCLA) y Santa Bárbara (UCSB), y la Universidad de UTAH, sumándose más nodos con el tiempo (Bolt, Beranek y Newman, 1981); al comenzar este proyecto se optó por módems conectados a líneas dedicadas de 50 Kbps con equipos denominados *Interface Message Processor.*

La evolución de esta red se dio de manera inminente, según el último reporte de la Central Intelligence Agency (2016) en *The World Factbook*, al 2016 han superado los 3 billones de usuarios, de manera que los intereses comerciales han trascendido mucho más que los académicos. A raíz de esto, surge el interés de crear redes exclusivas para el entorno académico; debido a la necesidad por inculcar la investigación e incentivar el intercambio de conocimientos, se crea las generalmente denominadas, NREN *(Nacional Research and Education Network) o* Redes Avanzadas*.*

La intención de contar con una red avanzada que permita conectar a centros de investigación y entidades educativas se replicó a nivel mundial, es así, que estás redes están interconectadas a nivel de continentes, distribuidas por Europa, Asia-Pacífico, Estados Unidos y América Latina. Con relación a América Latina existe la red avanzada CLARA (Cooperación Latino Americana de Redes Avanzadas), que nace gracias a ALICE (América Latina Interconectada con Europa), proyecto que fue valorizado en 1.2 millones de euros para la primera etapa, con la finalidad que se permita la conexión con Europa y el resto del mundo; Actualmente conecta 9 países en Latinoamérica: Argentina, Brasil, Chile, Perú, Ecuador, Colombia, Panamá, El Salvador y México. Perú no fue ajeno a pertenecer a esta red; la proyección inicio desde el 2004, concretando su integración unos años después, la Red Académica Peruana (RAAP) tuvo participación por aproximadamente 11 años interconectando entidades educativas como se evidencia en la figura 1, sin embargo, en la actualidad no tiene actividad eminente puesto a que el 2017 se desconectó; dado que uno de los factores que impide muchas veces el desarrollo y disponibilidad de una Red Académica, es el costo, tal fue el caso de la RAAP.

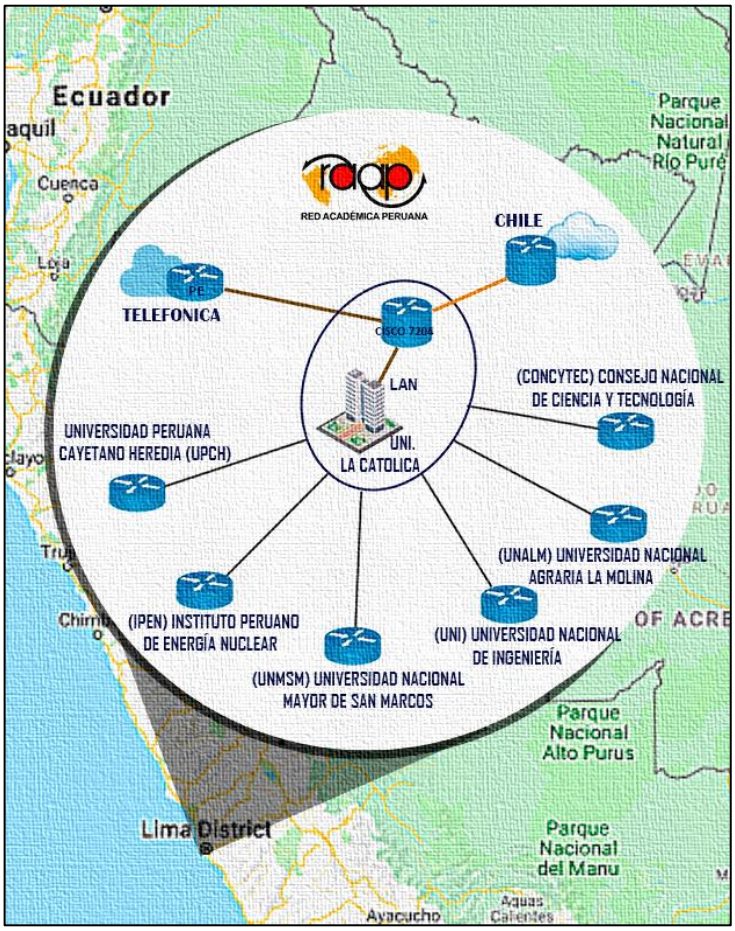


Figura 1: Topología RAAP
Fuente: Elaboración Propia

El fin de las Redes Académicas es actuar como base para intercambiar proyectos de carácter científicos y brindar servicios de colaboración; permitiendo la interconexión de entidades a nivel nacional e internacional, en consecuencia, aumenta las exigencias para satisfacer las demandas de los servicios. Debido a esto un administrador de red ejerce varias funciones, entre ellas el de velar por la gestión de la red. Esta actividad ha tenido un amplio uso en las infraestructuras, existiendo distintas herramientas hoy en día en el mercado; algunos son de uso libre *(open source)* y otras de licencia comercial. Lo usual es que estas herramientas se manejen en un entorno visual para interactuar; la información es extraída de los mensajes que son capaz de generar los

dispositivos, procesos y sistemas operativos sobre su propio estado u ocurrencia de eventos.

Uno de los elementos fundamentales para la gestión de red son los protocolos comúnmente utilizados para este fin desde estándares propietarios como *Network Based Application Recognition* (NBAR) de Cisco y por otro lado protocolos completamente abiertos como el SNMP *(Simple Network Management Protocol)* y Syslog. Al ser protocolos accesibles a cualquier persona u organización son más conocidos y fácil de encontrar en cualquier equipo. Syslog es un protocolo libre muy utilizado, diseñado originalmente por la universidad de California para su sistema BSD Unix, pero debido a la versatilidad se estableció en versiones actuales de Unix, y en sistemas basados en TCP/IP; el otro protocolo que se utiliza frecuentemente para realizar la misma función de notificación basados en *traps* y del conjunto de TCP/IP, llamado SNMP *(Simple Network Management Protocol)* documentado en el RFC 1157.

En efecto es importante la gestión de red continua de componentes de la infraestructura para hacer frente a posibles incidentes; uno de los factores más importantes es identificar problemas proactivamente y solucionarlo antes de que impacte en el usuario final, a fin de evitar degradaciones en la operatividad de la Red Académica. Otro factor es la información emitida del desempeño de la infraestructura para poder garantizar la optimización del rendimiento, debido a que las redes académicas garantizan un servicio fluido de la red.

1.2. Planteamiento del problema

El ámbito de las redes de avanzadas es área de constante crecimiento y evolución, actualmente centros de investigación y entidades educativas son

participes de estas redes de datos, como plataformas para potenciar el trabajo colaborativo e individual, con el fin de contribuir al avance de la investigación y la ciencia, así como otras ventajas; la proyección hacia nuevos miembros y la continua demanda por cubrir un servicio ininterrumpido a los usuarios finales, enfocan la atención a aspectos relacionados con el funcionamiento de los dispositivos.

Las Redes Académicas están permanentemente expuestas a incidentes de seguridad, sobrecarga de recursos, o errores, que hace difícil asegurar un funcionamiento efectivo, ya que la red se encuentra propenso a la caída o detención de servicios que en estos casos sería perjudicial.

Debido al nivel de sistematización de las redes académicas surge la necesidad de saber qué pasa con los equipos de la red. Es así, que la gestión de red pretende abarcar este tema con la finalidad de minimizar los riesgos frente a una posible falla, con el fin de evitar algún suceso que genere problemas y mantener el funcionamiento de los servicios sin inconvenientes.

Para ello es importante mencionar a uno de los elementos más importante en la gestión de red, que son los protocolos capaces de monitorear los elementos de la red. Existe más de un protocolo en el mercado para este fin, desde estándares propietarios, hasta los conocidos *open source* como SNMP y Syslog, quienes al ser accesibles a cualquier persona o empresa son mucho más difundidos y utilizados. Estos protocolos realizan un trabajo de recopilar la información a través de *traps o logs*, proporcionando un medio para gestionar los dispositivos de la red a través de la emisión de reporte de fallas y la información que proporcionan de los eventos ocurridos en los dispositivos.

Estos protocolos presentan fortalezas y debilidades independientemente en su uso, por ende, en este trabajo de investigación se evaluará alternativas de configuración con el uso de los protocolos Syslog y SNMP para la gestión de Redes Avanzadas con el fin de exponer su complejidad de configuración, el uso de recursos para efectuar su trabajo, la seguridad que presentan estos protocolos, y los servicios que se encuentran disponibles ofrecidos por cada protocolo.

Considerando que el Perú, no fue ajeno a la implementación de una red avanzada, como la Red Académica Peruana (RAAP), sin embargo, en la actualidad se desconoce su estado (el sitio web asociado se encuentra fuera de línea); surge la idea de tomar el ejemplo de aquellos países que aún mantienen sus Redes Avanzadas; con tecnologías, tales como: *multicast*, protocolos de enrutamiento para IPv6, entre otras características, para formular una nueva topología de una red avanzada para el Perú, sobre la cual se realiza la evaluación de protocolos de gestión de red.

1.3. Formulación del problema

1.3.1. Problema general

¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP para la Gestión de Redes Avanzadas?

1.3.2. Problemas específicos

1. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de complejidad para la Gestión de Redes Avanzadas?

2. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de uso de recursos computacionales para la Gestión de Redes Avanzadas?

3. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de seguridad de protocolo para la Gestión de Redes Avanzadas?

4. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de servicios disponibles para la Gestión de Redes Avanzadas?

5. ¿Cuál es la alternativa de diseño de topología para la Red Avanzada del Perú (RAAP) para la Gestión eficiente?

1.4. Justificación

Debido al avance de la investigación en el entorno educativo y científico, se emana el interés por explorar en el ámbito las Redes Avanzadas, el cual se ha expandido a nivel mundial conectando a instituciones educativas y centros de investigación; una de las características que tiene, es de poseer una infraestructura robusta, capaz de proveer y mantener un espacio para el desarrollo de pruebas y nuevas tecnologías. Por ende, la exigencia por mantener una operatividad contínua sin interrupciones de la red es cada vez más demándate; en consecuencia, la gestión de red se convierte en una labor muy importante, con características proactivas para evitar posibles fallos.

En el tiempo actual es crítica la necesidad de saber qué está pasando con los dispositivos de la red, es así, como la gestión de red cobra relevancia puesto a que implica la utilización de herramientas para ayudar conocer el

comportamiento de cada dispositivo (Mauro D; Schmidt k, 2005). Un aspecto importante de la gestión de red, son los protocolos que se utilizan para monitorear los elementos de la red; es aquí donde nace el interés de investigar SNMP y Syslog, que son protocolos libres comúnmente utilizados para este fin; este objeto de estudio es accesible a cualquier entidad o empresa, además puede ser encontrados en todo tipo de equipos por ser protocolos abiertos.

Es por ello, este trabajo de investigación pretende ayudar a conocer a profesionales y universitarios la mejor alternativa de configuración con el uso de Syslog y SNMP, considerando los factores de: Nivel de Complejidad de la configuración, consumo de recursos, seguridad y servicios. Con el objetivo de infundir la capacidad de realizar una configuración de equipos intermediarios para lograr una eficiente gestión de red en Redes Avanzadas.

1.5. Objetivos

1.5.1. Objetivo general

Evaluar las alternativas de configuración con el uso de los protocolos Syslog y SNMP para la gestión de Redes Avanzadas para la formulación de una guía de configuración general.

1.5.2. Objetivos específicos

1. Determinar la mejor alternativa de configuración respecto al nivel de complejidad para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP

2. Determinar la mejor alternativa de configuración respecto al nivel de uso de recursos computacionales para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP.

3. Determinar la mejor alternativa de configuración respecto al nivel de seguridad de protocolo para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP.

4. Determinar la mejor alternativa de configuración respecto al nivel de servicios disponibles para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP.

5. Diseñar una alternativa de topología de la Red Avanzada del Perú (RAAP) para la gestión de red eficiente.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

Según July Hernández, 2012 en su trabajo de investigación de pregrado **“Evaluación de los mecanismos de seguridad en los sistemas de notificación y registro de eventos para la gestión de redes**", indica que los equipos que componen las redes proveen condiciones para alertar sobre condiciones críticas, por ende, equipos y sistemas operativos son susceptibles a ser para ser monitoreado y registrado, detectando el uso de recursos o actividades poco convencionales. Apoyado de los protocolos Syslog y SNMP, este trabajo de investigación pretende estudiar y evaluar las carencias de seguridad en dichos protocolos desde las notificaciones y registro de eventos, debido a que la información que se maneja tiende a poder ser utilizados de manera desventajosa para la red. En este sentido se realizan pruebas con protocolos y tecnologías de código abierto, que permitieron evaluar un canal seguro (Túnel) entre la partida y destino, tecnologías también llamadas VPN, para a notificación de eventos, originados por Syslog y *traps* SNMP. Al evaluar las a las soluciones: *Kiwi Syslog Tunnel*, Protocolo de Túnel de Punto a Punto (PPTP), Protocolo de Túnel de Punto a Punto (PPTP). Se determina en conclusión que el Protocolo de Túnel de Punto a Punto (PPTP), resulta como la mejor opción para una mejora de seguridad por facilidad de uso y portar trasparencia a los protocolos que se trasladó.

Según Avila Gonzales (2014) en el trabajo de tesis titulada **“Diseño e implementación de un sistema de monitoreo basado en SNMP para la red nacional académica de tecnología avanzada”** donde se propone la

corporación de la Red Nacional Académica de Tecnología Avanzada (RENATA) la implementación de un sistema de monitoreo de la red y servicios orientados a la verificación de enlaces y atención al cliente apoyados en tiempos de respuesta y tráfico. Se presenta la descripción de RENATA, cuyo crecimiento abarca la deterioración de la red, pero con el fin de cumplir los Acuerdo de Nivel de servicio, y garantizar a las instituciones que hacen uso de esta conexión se propone realizar implementación, realizando un diseño de la solución de monitoreo, teniendo en cuenta la topología de la red, determinan por medio de una comparación la herramienta más favorable para la implementación de acorde a los requerimientos y funcionalidades de cada uno. Se pretende monitorear toda la infraestructura de red, a través del envío y recepción de *traps* SNMP hacia los equipos que constituyen a RENATA, priorizando el servidor local y seguido por los equipos adyacentes. Del resultado de la evaluación sobre los sistemas de monitoreo más prominentes del mercado, se estableció la implementación de la aplicación *PRTG NETWORK MONITOR*, este permite la configuración por medio de sensores, dependiendo del mismo para la configuración sobre los cambios de estado de los sensores, primando para esta selección la adaptabilidad, estabilidad y funcionalidad de la aplicación según las necesidades presentadas para mejorar la red, consiguiendo una configuración de las notificaciones que alertan de manera rápida sobre el estado de los dispositivos.

Según Tsunoda & Keeni, (2014) en el artículo titulado ***"Managing Syslog"*** señala que el crecimiento de las aplicaciones de TI es importante para un administrador de red, inspeccionar los registros para detectar eventos y diagnosticar fallas. A su vez, estos registros deben recopilase de manera

confiable y sin interrupción, por ende, lo mecanismos de seguridad deben garantizar la autenticidad e integrada de los mensajes. Syslog es uno de los mecanismos de recopilación de mensajes de registro, más utilizados desde los inicios del internet, dentro de su arquitectura, los dispositivos que comprenden desde sistemas operativos hasta procesos son capaces de generar registro sobre su propio estado u ocurrencia de eventos, entre otros. Sin embargo, aún se presenta la carencia de estandarización para la supervisión de Syslog, Sin un marco estándar para monitoreo y supervisión, poco se puede decir acerca de las operaciones del sistema Syslog. En consecuencia, este artículo, tiene como objetivo discutir requisitos básicos para supervisar aplicaciones Syslog y presentar el esquema de diseño de un módulo Base de información de gestión (MIB), que consiente monitorear un sistema Syslog utilizando protocolos de administración estándar, seguido de una propuesta para implementación de un prototipo de MIB, este sistema prototipo supervisa cada host y obtiene información de configuración de las aplicaciones Syslog, a su vez se hace presente la discusión de una implementación de prototipo de MIB. Dentro de los requisitos básicos a discutirse para el monitoreo de Syslog, refiere a que los objetos deben servir para acceder a: Estado operativo y estadísticas: Syslog provee información relevante sobre el comportamiento de una aplicación, y la dinámica en la red, El uso de recursos: *Host Resources MIB* proporciona información genérica sobre el uso de recursos en un host, Información de configuración: Una configuración de manera correcta en cada dispositivo puede garantizar la integridad de la recopilación de registros. Cuya información relacionada responde a la supervisión de Syslog. Así mismo se toma en cuenta

la notificación de eventos primando el siguiente conjunto de notificaciones: Notificación para indicar que los mensajes se eliminan, notificación para indicar que el estado de la operación ha cambiado, notificación para indicar que el recurso ha alcanzado el umbral, notificación para indicar que la configuración ha cambiado. Del prototipo se concluye que supervisa a cada *host*, y extrae información de configuración de las aplicaciones Syslog, utilizando. SNMP, al procesar la información supervisada, el sistema visualiza la ruta de recolección de mensajes de registro en un mapa de red. En consecuencia, se cree que el prototipo ilustra ampliamente el potencial y la importancia de la supervisión y administración de Syslog.

Según Tsunoda Hiroshi; Maruyama Takafumi; Oht Kohei; Waizumi Yuji; Glenn Mansfield (2009) en el artículo titulado **"*A Prioritized Retransmission Mechanism for Reliable and Efficient Delivery of Syslog Messages"*** la información que contienen los registros de red, son relevantes para un administrador de red, así como para monitorear los componentes de la red donde se espera que un sistema de registro proporcione un mayor grado de disponibilidad, confiabilidad y escalabilidad. El protocolo Syslog gracias a su facilidad es uno de los más utilizados como mecanismo de registro de red, pero presenta problemas en cuanto a seguridad. Este protocolo carece de mecanismos retransmisión, existiendo siempre el riesgo de una pérdida de mensajes en los sistemas de registros actuales, sumando a ello que usa como medio de transmisión UDP, además de no contar con mecanismos de protección contra el espionaje y manipulación. La comunidad de internet contribuye a mejorar el protocolo y su implementación, sin embargo, hasta donde se indica

en este documento la confiabilidad de la transmisión depende únicamente del uso de TCP en las propuestas actuales. Bajo esas circunstancias, se realiza en una red real una evaluación con problemas prácticos en los sistemas de registro de Syslog, donde uno de los experimentos tuvo como resultado una variación en la cantidad de mensajes Syslog, puesto a que presentaban días donde excedía al rango normal, pero quedando demostrado que no específicamente aumentaba la cantidad de mensajes por un ataque, siendo estas ocasionados por fracasos de inicio de sesión de SSH o malas configuración de host, entre otros, posteriormente en otro experimento se demostró que se tenía presencia de mensajes perdidos durante la transición producidos a partir de generase múltiples mensajes a la vez. Dado que el uso de TCP para un sistema de registro garantizaría una entrega confiable de los mensajes Syslog, en este artículo también contempla algunos puntos al respecto, evidenciándose que TCP no garantiza la confiabilidad, finalizada la conexión, asimismo tiene un efecto adverso a la puntualidad de los mensajes importantes. Proponiéndose así un mecanismo para la retrasmisión priorizado para un sistema confiable y eficiente entrega de mensajes Syslog, tal que este mecanismo está basado en el acuse de recibo simple en la capa de aplicación y bajo la trasmisión de UDP, este método categoriza los mensajes en dos tipos: importante y normal, debido a esto, se manejan dos acuses de recibido, donde retorna un mensaje de confirmación para cada recepción de un mensaje importante. Y para mensajes normales, el método propuesto adopta el algoritmo de reconocimiento selectivo diferido, diferenciando el mecanismo de retrasmisión de los distintos tipos de mensajes.

Demostrándose a través de simulaciones mayor eficiencia frente a TCP proporcionando a su vez, mensajes confiables de Syslog.

Según Castillo Velazquez , Cobos Panduro, & Marchand Niño, (2018) en el artículo titulado "*IPV6 Connectivity and Management Emulation for REUNA, the Chilean Advanced Network*"; RAAP es la red avanzada para Perú, pero la falta de uso de esta empujó a RAAP a salir de América Latina y las Redes Avanzadas del mundo en 2018. Por lo tanto, para promover dentro de las universidades peruanas la importancia de este tipo de redes de investigación, se analizó REUNA, la red avanzada de Chile. Por lo tanto, la conectividad y la administración de la red troncal de REUNA se emularon utilizando IPV6 como lo hacen las compañías ISP comerciales. Los resultados muestran las capacidades y limitaciones del emulador al acercarse a la infraestructura de la red troncal real. Este trabajo está bajo un proyecto de colaboración de transferencia de tecnología.

2.2. Bases Teóricas

2.2.1. Gestión de Red

La gestión de red es un concepto bastante amplio, que involucra la utilización de herramientas para apoyar el manejo de dispositivos o sistemas.

Según Castillo Velázquez (2009) gestionar una red implica *"controlar y alterar la configuración de dispositivos de red, y todo dispositivo gestionado tiene como huésped un agente tal que las tareas del agente son; a) suministrar información de gestión (MI) respecto del dispositivo y b) aceptar instrucciones para configurar un dispositivo*". Además, indica que la gestión de red consiste en

realizar 4 actividades básicas que son: El monitoreo, configuración, actualización y resolución de problemas de los recursos de la red. (Castillo Velazquez , 2017).

Para Tuncay Saydam (1996) la gestión de red consiste en la integración y condonación de elementos como hardware, software y elementos humanos con la finalidad de monitorizar, configurar, analizar y controlar los recursos de la red.

2.2.2. Redes Avanzadas

Las Redes Avanzadas o Redes Nacionales de Investigación y Educación (*National Research and Education Network*, NREN), surge con la finalidad de intercambiar conocimiento evocadas al desarrollo de la investigación científica y tecnología, conectando a investigadores de todo el mundo; es preciso señalar que el origen de estas redes se dio en el año 1969 con la creación de ARPANET *(Advanced Research Projects Agency Network),* cuya finalidad era conectar diferentes entidades de Estados Unidos, por esta razón se unió al Instituto de Investigación de Stanford (SRI), dos campus de la Universidad California: Santa Bárbara (UCSB) y Los Ángeles (UCLA) y la Universidad de UTAH, sumándose a estos centros de investigación más miembros al pasar el tiempo, como se indica en la figura 2 (Heart, McKenzie, & McQuillan, 1981); esta red dio inicio a la que posteriormente fueran denominada NREN, conectadas a nivel de todo el mundo.

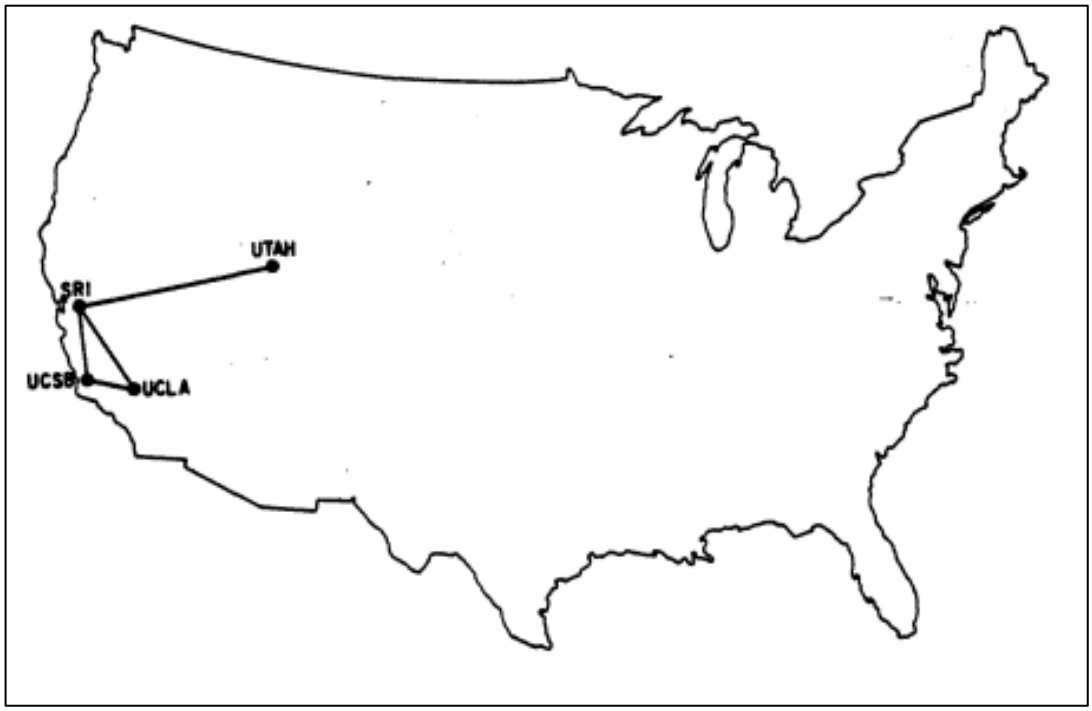


Figura 2. Mapa ARPANET - Primeros Centros Interconectados
Fuente: Heart, McKenzie, & McQuillan (1981)

Para Avila Gonzales (2014) las Redes Avanzadas son de suma importancia para el desarrollo de la investigación, ciencia y tecnología a nivel mundial a continuación, debido a estas razones:

- Sobre esta plataforma se desarrollan de nuevos servicios y aplicaciones que favorecen el crecimiento y el progreso del internet.
- La red opera como una plataforma experimental para probar protocolos de comunicación, fortalecer la calidad de servicio y brinda velocidades de comunicación de la información, no disponibles en el internet comercial.
- Accesible por el bajo costo de servicio para las instituciones que desean sumarse.
- Capaz de ofrecer una infraestructura robusta para una colaboración, educación y acceso a recursos para la comunidad científica.

Entre las redes más destacadas a citar:

- **ABILENE,** en Norte América: Formada por el consorcio de Internet2, une a más de 220 entidades y universidades, con enlaces de hasta 100 gigabit. Su topología se ilustra en la figura 3.

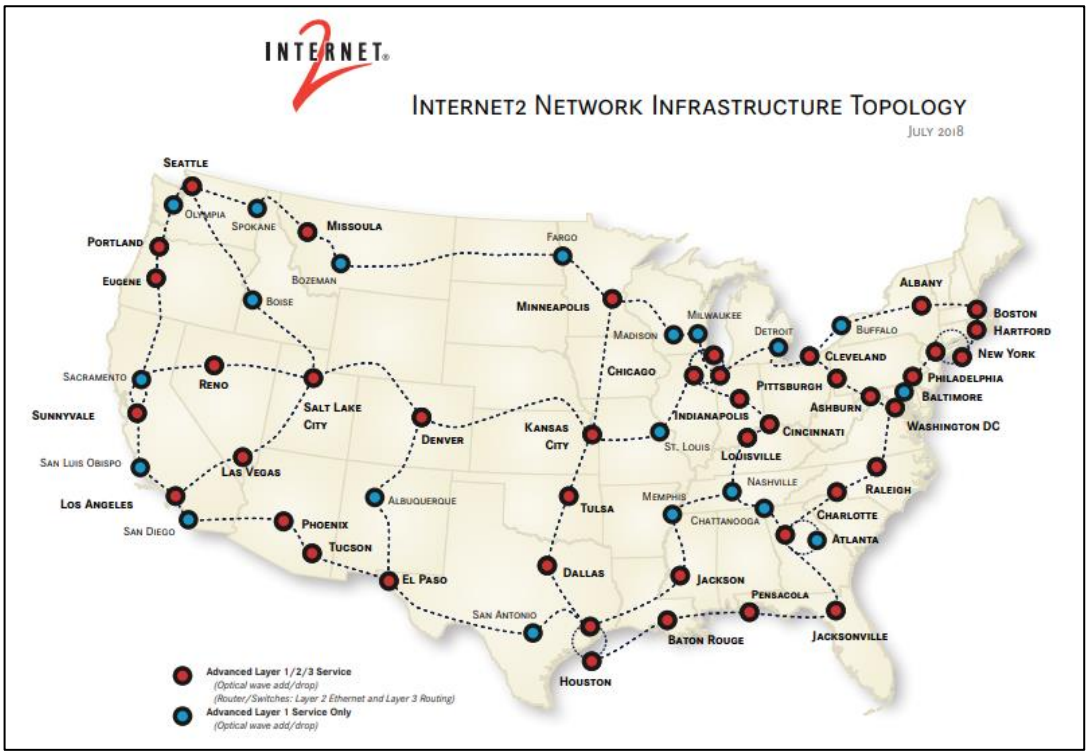


Figura 3. Backbone de Abilene
Fuente: (Abilene Home)

- **GÉANT** en Europa: Construida por socio gerente y coordinador del proyecto *Delivery of Advance Network Technology to Europe* (DANTE), uniendo entre 40 socios donde 37 son RNIE europeas, Dante, TERENA y NORDUnet, cuya topología se muestra en la figura 4.

Figura 4. Mapa de Conectividad Global GÉANT
Fuente: (GÉANT, 2015)

- **RedClara** en Latinoamérica: Los países latinoamericanos no son ajenos a contar con Redes Avanzadas, por tal motivo se creó la Cooperación Latino Americana de Redes Avanzadas (RedCLARA) como parte de una estrategia de unificación, teniendo como miembros colaboradores a países latinoamericanos como Argentina, Bolivia, Brasil, Colombia, Costa Rica entre otros, Clara nace gracias al proyecto ALICE (América Latina Interconectada con Europa) pensada para la conexión con Europa y resto del mundo, cuya topología se muestra en la figura 5.

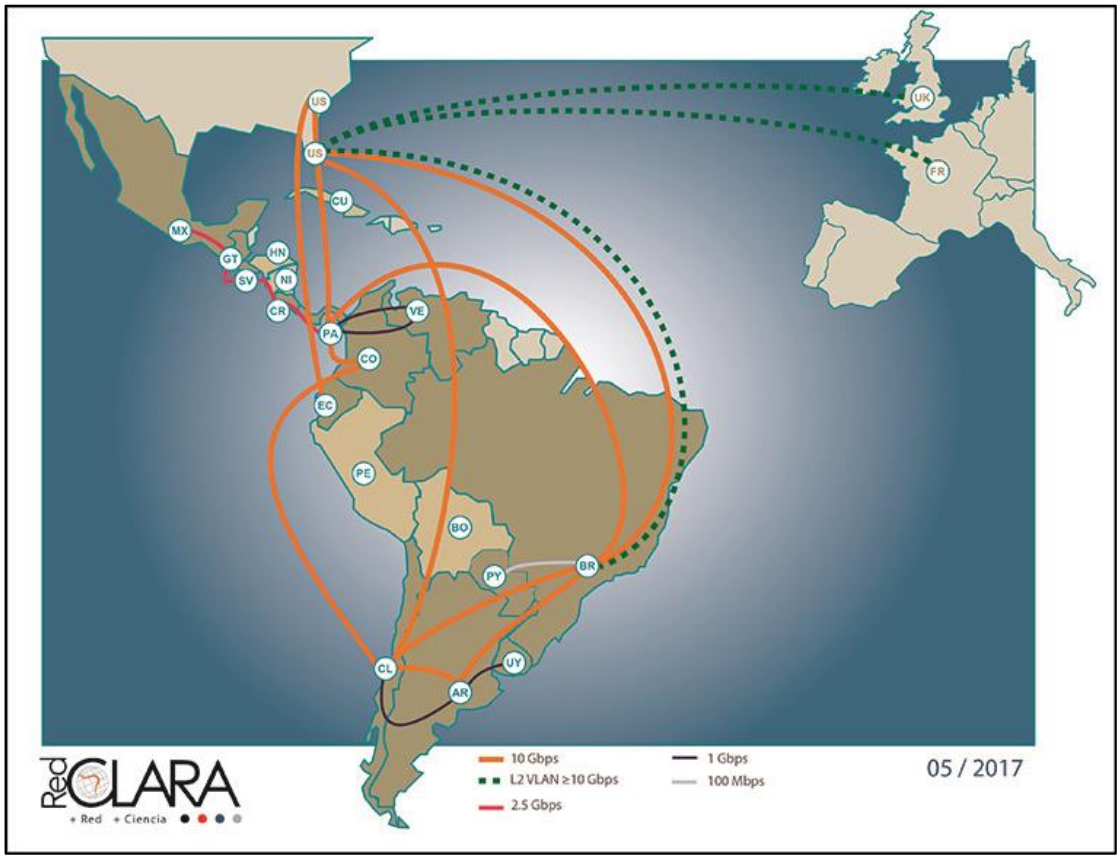


Figura 5. Topología de la Red Clara
Fuente: (REDCLARA, 2017)

2.2.3. *The Simple Network Management Protocol* (SNMP)

La comunidad de internet originó el desarrollo de SNMP, como medida para supervisar redes TCP/IP; El predecesor y base de SNMP, SGMP (*Simple Gateway Management Protocol)* pretendía supervisar puertas de enlace de *router,* siendo más limitado a comparación de SNMP, que es admitible a cualquier dispositivo, siendo posible obtener información e incluso modificarla (Avila Gonzales, 2014).

Por lo tanto, SNMP es un protocolo estándar para monitorear y supervisar los componentes de una red; funciona a través de UDP *(Unreliable Datagram Protocol);* una entidad SNMP serializa un mensaje y lo envía como un datagrama UDP al destino de la entidad que recibe. Un sistema de registro debe ser

manejable con la utilización de SNMP, para este propósito, los objetos administrados deben definirse como Base de información de administración (MIB).

A. Componentes de SNMP

Existen tres elementos que forman parte del protocolo de aplicación SNMP, como desglose de los componentes determinados por la RFC 1157 son: Consola de Administración de SNMP, Base de Información de administración de (MIB) y los agentes SNMP especificados (docwiki.cisco, 2012). La figura 6 intenta clarificar la relación entre estos conceptos.

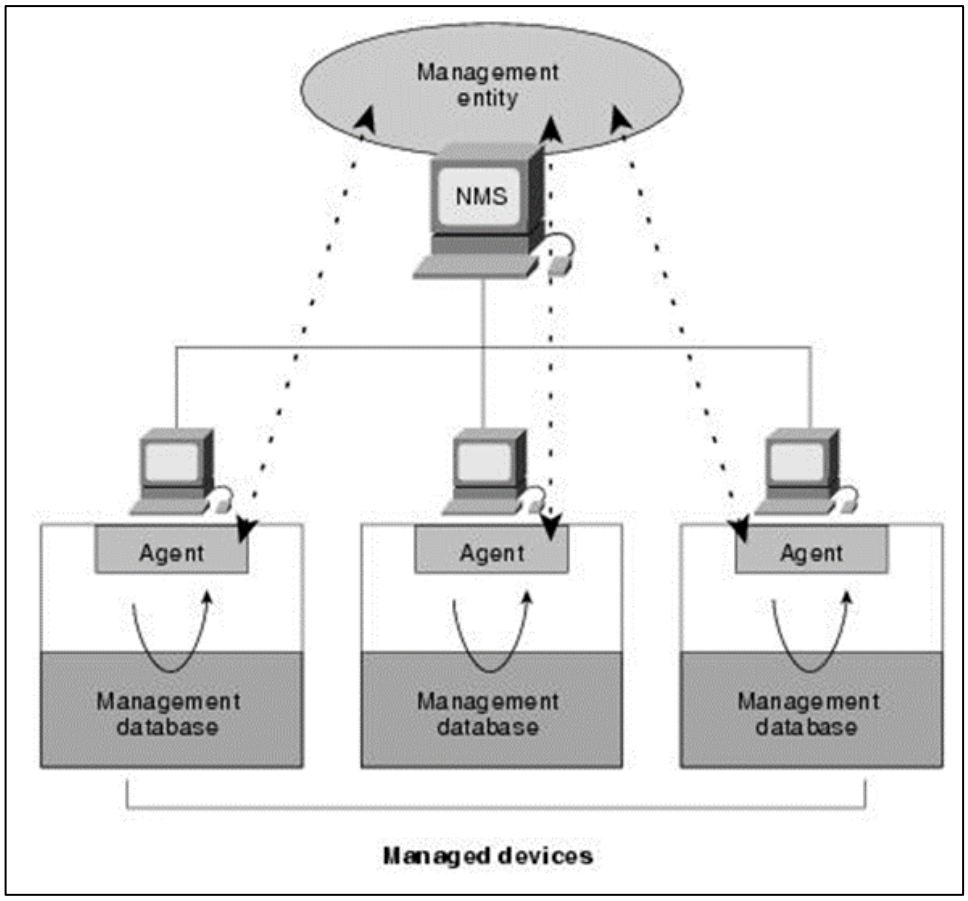


Figura 6. Elementos SNMP
Fuente: *(docwiki.cisco, 2012)*

Según Terplan (1992) las responsabilidades más importantes de cada uno de estos componentes son:

- Agente: Es un programa encontrado en un dispositivo de red, ya sea un *switch*, *router* o cualquier estación.
- Consola de Administración (NMS): Es una aplicación encontrado en un equipo, que cumple la función de sondear los agentes utilizando SNMP, ayudando a analiza el funcionamiento de la red; habitualmente utiliza una interfaz gráfica.
- Base de Información de administración de (MIB): Es una estructura de datos de objetos administrados que son accesibles y manipulables vía SNMP; se encuentran divididas en cuatro áreas: Atributos del Sistema, privados, experimentales y de directorio.

B. Operaciones del Protocolo

SNMP cuenta con 6 comandos básicos:

- *GetRequest:* encargado de traer el valor de ciertos objetos indicados como parámetros.
- *GetNextRequest:* Aunque es ligeramente similar al comando especificado anteriormente, la diferencia radica en regresar el siguiente valor del objeto según el orden lexicográfico.
- *GetResponse*: este comando devuelve los datos que se ha recolectado, del comando *GetRequest* o *GetNextRequest.*

Por lo tanto, al recibir un comando PDU (*Protocol Data Unit*) desde la consola de administración (NMS), sean *GetReques*t o *NextRequest,* el agente

inspecciona el valor de las variables que tiene la MIB, y devuelve los datos que ha recolectado del comando recibido mediante un *GetResponse.*

Obsérvese las figuras del 7 a 10, las cuales explican algunos de los 6 comandos.

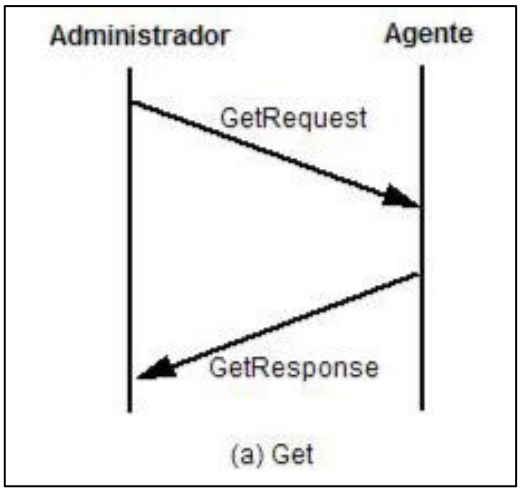


Figura 7. Intercambio de mensajes para el comando Get
Fuente: Stalling (1999)

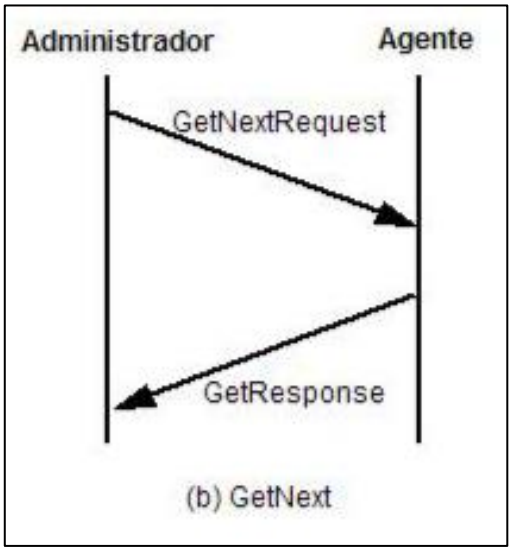


Figura 8. Intercambio de mensajes para el comando GetNext
Fuente: Stalling (1999)

- *SetRequest:* utilizado para modificar variables de la MIB, es similar al GetRequest, pero la diferencia radica que este comando es utilizado para escribir un valor y no de leerlo. En la figura 9 se

muestra el intercambio de mensaje SNMP; El agente responde con un *GetResponse* que contiene el mismo ID de identificación.

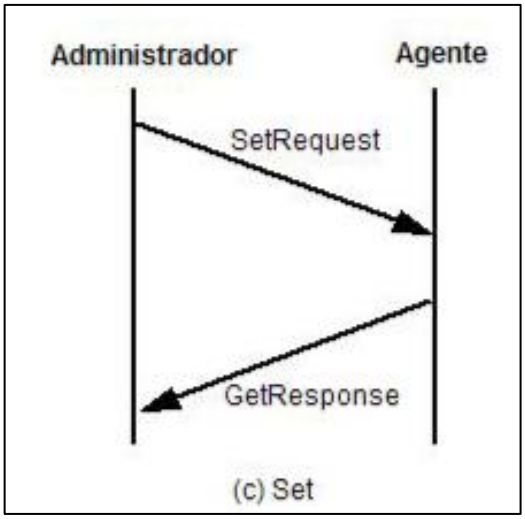


Figura 9. Intercambio de mensajes para el comando GetNext
Fuente: Stalling (1999)

- *Traps*: utilizado por el agente para enviar datos a la consola de administración tras un suceso inusual; de naturaleza asíncrona.

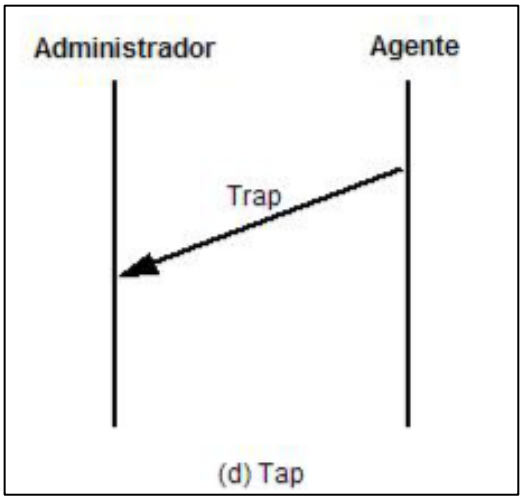


Figura 10. Intercambio de mensajes para el comando GetNext
Fuente: Stalling (1999)

- *GetBulkRequest:* comando utilizado para solicitar transferencia de datos, pero en gran cantidad, minimizando así las solicitudes que tocaría realizar para traer filas de tablas.

C. Datagrama SNMP

Los datagramas SNMP se transportan a través de UDP, usando por defecto el puerto 161 para las diversas consultas GET que envía el administrador SNMP a los agentes (incluyendo las respuestas), y el 162 para enviar las *traps* del agente al administrador SNMP, debido al uso de UDP, no se realiza una verificación de inicio de sesión entre los agentes y MIB, pero se realiza una verificación tal sea el caso del sondeo de NMS, se pone tiempo límite de respuesta para la recepción del mensaje, de caso contrario el paquete será reenviado, por otra parte si se trata de un *traps*, puede perderse o no llegar a ser notificado ni el agente ni el NMS (Rosemberg Diaz , 2007).

La entidad SNMP manda una entidad de autenticación que consta de:

- Nombre de la comunidad.
- Dirección del origen.
- Los Datos.

La entidad de autenticación que conoce el tipo de permiso que se puede hacer, es decir ya sea lectura o escritura, o solo lectura, devuelve dos de las siguientes opciones (Arana Boreto, 2005).

- Una instancia del tipo de dato y la identificación de la entidad que manda.
- Una excepción.

D. Estructura de PDU

La estructura del formato del PDU del mensaje SNMP, consta de los siguientes campos indicados en la figura 11 (Marti Baiba, 2001).

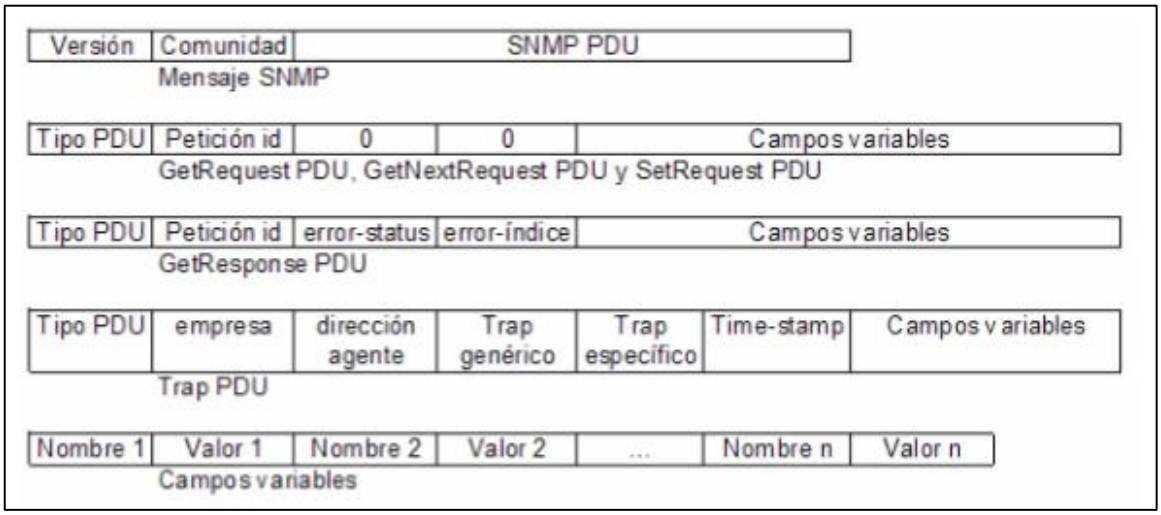


Figura 11. Estructura de PDU v2
Fuente: Marti Baiba (2001)

A continuación, se detalla cada término mencionado:

- Versión: Versión de SNMP utilizada.
- Comunidad.
- Tipo PDU: varía según el tipo, que puede ser de tipo *Request,* (como *GetRequest, GetNextRequest y SetRequest*), un *trap* o un *GetResponse.*
- Petición ID: usado para distinguir de entre otras solicitudes, cada id es único.
- Error-status: indica si ha existido un error cuando se procesaba una solicitud.
- Error-índice: cuando existe un error proporciona información adicional indicando la variable que causo la excepción.
- Campos variables: una lista de nombre de variables con sus correspondientes valores, que responden a una operación solicitada por un *Get*, o un *trap.*
- Empresa: Tipo de objeto que genera un *trap*.

- Dirección agente: origen del objeto generado del *trap*.
- *Trap* genérico: Tipo genérico del *trap.*
- Trap específico: código específico del *trap.*
- Time-*stamp:* tiempo transcurrido entra la última vez que se reinició. el dispositivo de red y la generación del *trap.*

2.2.4. *The Simple Network Management Protocol* (SNMP) versión 3

SNMPv3 definido por RFC 3410, en esta versión, tiende a resaltar los modelos de seguridad como el nivel seguridad del mensaje, teniendo características que promueven la autenticación y encriptación de los paquetes a través de la red (Cuchala Vásquez, 2017). La autenticación de SNMP v3, es dada a través de la función criptográfica *Hash.*

SNMPv3 fue diseñado para proteger contra las siguientes amenazas de seguridad, mediante el uso de algoritmos de autenticación y de inscripción como lo especifica el RFC 2574.

- Modificación de la información
- Enmascaramiento (*masquerade)*
- Reenvió de mensajes
- Poca privacidad *(disclosure)*

A. Arquitectura SNMPv3

SNMP se compone de entidades, donde cada entidad corresponde una parte de la funcionalidad de SNMPv3 y así, puede actuar como nodo administrador o nodo agente (RFC 2271).

En la figura 12, se muestra el diagrama general de bloques de una entidad SNMPv3.

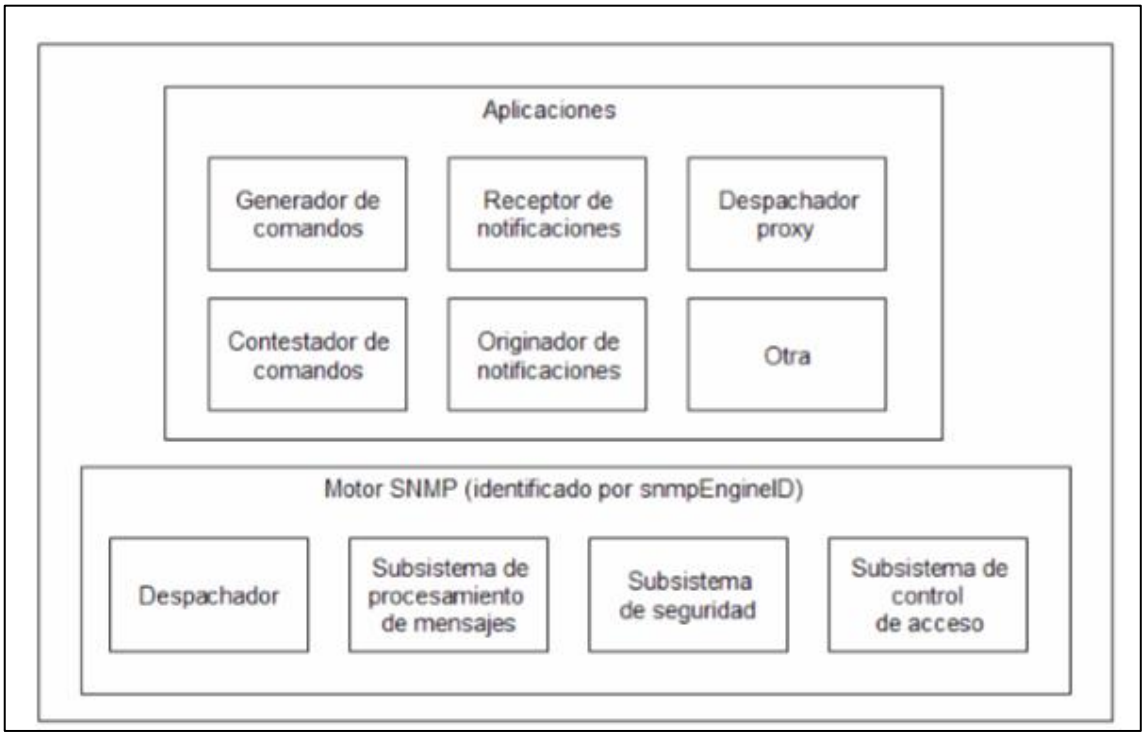


Figura 12. Arquitectura de una entidad SNMPv3
Fuente: Stalling (1999)

Solo un motor SNMP por entidad, implementa funcionalidades para enviar, recibir mensajes, poder autenticar, encriptar mensaje y realizar un control de acceso; estas funciones están a cargo de ciertos módulos, que a su vez pueden ser utilizados por otras aplicaciones conocidas como entidad SNMP.

B. Formato del Mensaje

En la figura 13, se muestra el formato del mensaje de SNMPv3; cada mensaje contiene un encabezado y un PDU.

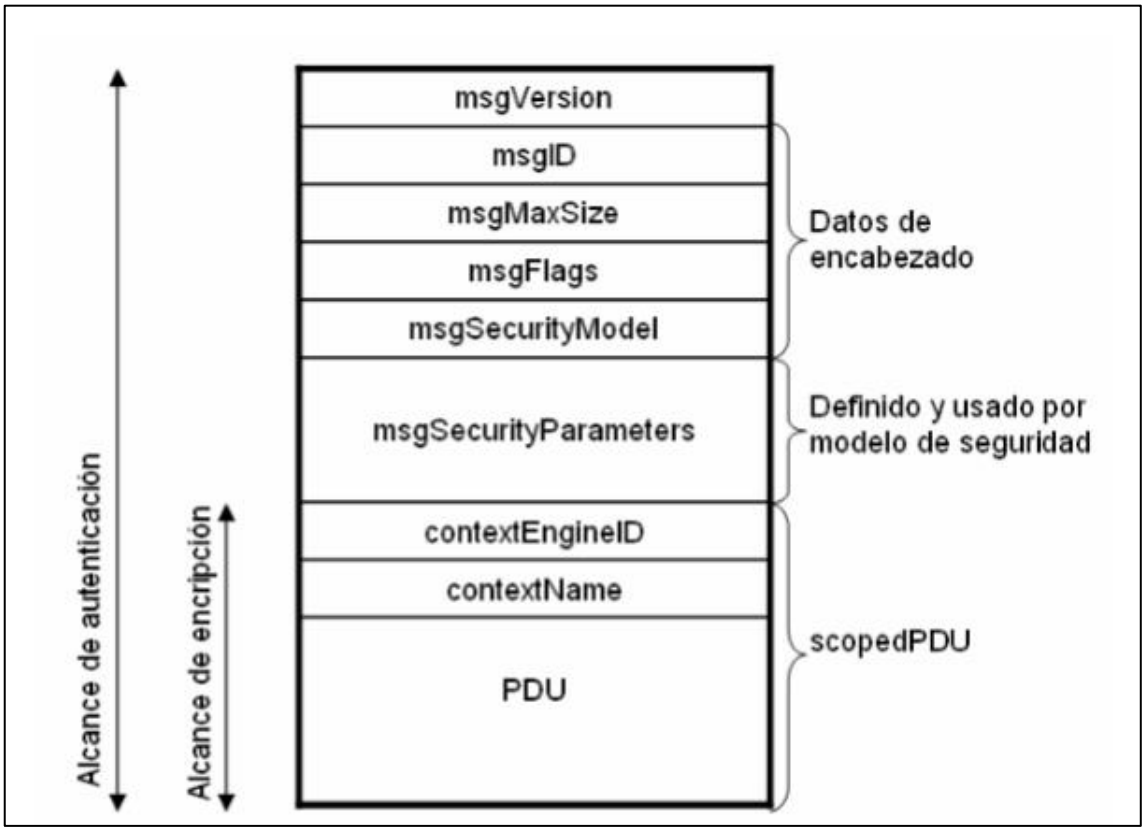


Figura 13. Formato del mensaje SNMPv3
Fuente: Stalling (1999)

A continuación, se detalla cada término:

- *msgVersion:* su valor por defecto es SNMPv3
- *msgID:* identificador único usado entre dos entidades para establecer mensajes de solicitud y respuesta.
- *msgMaxSize:* tamaño máximo del mensaje que un remitente puede aceptar.
- *msgFlags:* cadena que contiene: *reportableFlag, privFlag y authFlag.*
- *msgSecurityModel:* identificador para indicar modelo de seguridad usado por el remitente.

- *msgSecurityParameters:* cadena de parámetros generados por el subsistema de seguridad en la entidad de origen, y procesadas por la entidad de destino.
- *contextEngineID:* identificador único de una entidad SNMP.
- *contextName:* identificador de manera única, particularmente dentro del contexto del motor SNMP

2.2.5. *Management Information Base* (MIB)

La Management Information Base (MIB) almacenan datos de los dispositivos que se pueden administrar cuya estructura jerárquica está definida en forma de árbol. Según Avila Gonzales (2014), definido en primera instancia por el RFC 1156, y actualizada en el RFC 1213.

La estructura proporciona ramas con variables conocidas a distintos dispositivos de red y otras con variables determinadas ya sea por tipo o proveedor, para un dispositivo. Para que un SNMP trabaje correctamente, es necesario tener acceso a al MIB, ya que estas definen cada variable como un ID de objeto. La figura 14 muestra el árbol de internet de acuerdo con su OID.

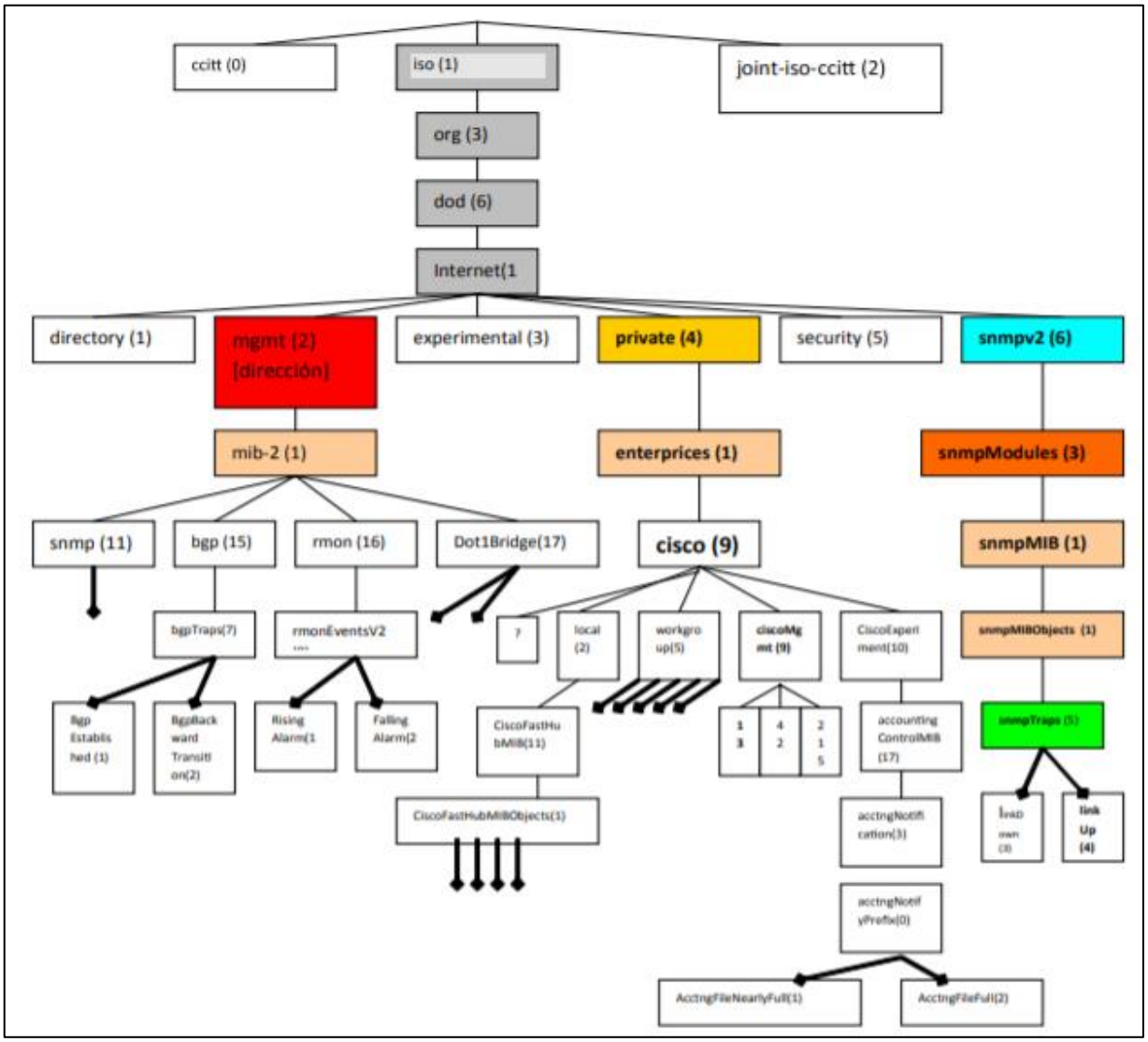


Figura 14. Árbol de internet de acuerdo con su OID
Fuente: Velázquez Castillo (2009)

A. *Structure of Management Information* (SMI)

La Structure of Management Information (SMI), define el nombre y la sintaxis de los objetos que van a ser monitoreados, es decir, especifica los tipos de datos que pueden usar en la MIB y la forma en que los recursos de una MIB son identificados, este tiene dos versiones, SMIv1 definido en la RFC 1155 y completado en la RFC 1215 y la SMIv2 ampliando la primera versión en el RFC 2578. Cada tipo de objeto tiene tres atributos:

- **El nombre o OID (*Object Identifier*),** representado con un identificador preciso.
- **Sintaxis**, el cual establece el tipo de dato de un objeto, o su estructura de datos abstracta.
- **Codificación**, instancia del valor del objeto, considerando como se codifican o decodifican los objetos de forma que no pueda surgir errores en la transmisión.

B. El *Abstract Syntax Notation One* (ASN.1)

ASN.1 es un lenguaje formal estandarizado por ITU-T y la ISO; para definir sintaxis sobre datos intercambiado entre aplicaciones. SNMP utiliza un subconjunto de reglas especificadas por este estándar, para definir la estructura y representación de las PDU (*Protocol Data Unit).*

C. *Object IDentifier* (OID)

Los OIDs (*Object IDentifier*), definidas por números enteros positivos, que indican donde los objetos se determinan en jerarquía de su estructura de MIB. Cada OID pueden identificarse en cuanto a la ruta y su posición en el árbol; desde una forma absoluta o de forma relativa.

Un OID se puede reconocer de las siguientes formas:

- Solo números: Secuencia de números enteros positivos separados por puntos. Por ejemplo .1.3.6.1.2.1.1 que identifica al nodo *system*
- Solo Texto: solo se utiliza el nombre de los nodos separados por puntos. Por ejemplo: *mgmt.mib-2. system.sysContact* que identifica al nodo *sysContact.*

- Combinación entre números y texto: se pueden utilizar tanto números como texto, separados por puntos.

2.2.6. Syslog

Syslog es un sistema de *logs*, encargados principalmente del manejo de *logs*, generados por eventos del sistema, procesos o por el *kernel.* Desarrollado inicialmente por la Universidad de California, para sistemas UNIX, pero IETF lo registro inicialmente en la RFC 3164. Este protocolo de red proporciona un medio de transporte donde un equipo remita mensajes de notificación de eventos, los equipos que admitan este protocolo permiten que se envié los mensajes del sistema a otro equipo donde este configurado el Syslog como servidor.

Entre sus funciones principales también destacan la capacidad de seleccionar el tipo de información que se recopila, además de especificar los destinos de los mensajes (docwiki.cisco, 2012).

A. Formato de Mensajes

Los mensajes Syslog utilizan en UDP (*User Datagram Protocol*) el puerto 514, no se puede exceder de 1024 octetos y contiene 3 campos.

- **Prioridad:** Este campo está conformado de 8 bits, se representa a través de la multiplicación del valor del código numérico de funcionalidades por ocho, y sumando a este resultado el valor del código numérico de severidad, por causas de que originalmente fue creado para sistemas Unix, los nombres descrito para el nivel de funcionalidades reflejan nombres de procesos y *Daemon* (demonios)

de Unix (July Hernández, 2012). La tabla 1 muestra las facilidades y su código numérico respectivo.

Tabla 1: Facilidades y su código numérico respectivo

Código Numérico	Funcionalidades
0	*kernel messages*
1	*user-level messages*
2	*mail system*
3	*system daemons*
4	*security/authorization messages*
5	*messages generated internally by Syslogd*
6	*line printer subsystem*
7	*network news subsystem*
8	*UUCP subsystem*
9	*clock Daemon*
10	*security/authorization messages*
11	*FTP Daemon*
12	*NTP subsystem*
13	*log Audit*
14	*log alert*
15	*clock Daemon*
16	*local use 0 (local0)*
17	*local use 1 (local1)*
18	*local use 2 (local2)*
19	*local use 3 (local3)*
20	*local use 4 (local4)*
21	*local use 5 (local5)*
22	*local use 6 (local6)*
23	*local use 7 (local7)*

Fuente: July Hernández (2012)

Además, en la tabla 2 se describen los indicadores de severidad decimal:

Tabla 2: Severidades y su código numérico respectivo

Código numérico	Severidad	Descripción
0	*Emergency*	El sistema esta caída
1	*Alert*	Se debe tomar de inmediato una acción
2	*Critical*	Condiciones Críticas.
3	*Error*	Condiciones de Error
4	*Warning*	Condiciones de Alerta
5	*Notice*	Condición Normal, pero significativa
6	*Informational*	Mensajes Informativo
7	*Debug*	Mensaje de depuración

Fuente: July Hernández (2012)

- **Cabecera:** Está contenida de dos campos: *Timestap* que corresponde a la hora y fecha local en formato “Mmm dd hh:mm:ss” ubicado posteriormente al campo de prioridad, y el segundo campo que ya está compuesto, es el *Hostname*, correspondiente al nombre del dispositivo o dirección IP (July Hernández, 2012).
- **Mensaje:** Está contenida de dos campos: *TAG* (Etiqueta), que corresponde al proceso o nombre del programa que genera el evento, y *CONTENT* que corresponde un texto que explica los detalles del mensaje (July Hernández, 2012).

2.2.7. IPV6

Esta nueva versión del protocolo de internet, también conocido como IPv6, fue proyectado como sucesor de la versión anterior IPv4 (RFC 2460, 1998). Dentro de los cambios se categoriza en lo siguiente:

- **Capacidades de direccionamiento expandido**

A diferencia de la versión anterior (IPv4) con 32 bits, IPv6 amplía a 128 bits el tamaño, cubriendo mayores necesidades de asignación de direcciones IP, además se define un nuevo tipo de dirección llamada “dirección *anycas*t”, utilizada para enviar un paquete a cualquiera de un grupo de nodos.

- **Formato de encabezado**

Pensando en una reducción del coste de procesamiento y la limitación del coste de ancho de banda del encabezado IPv6, algunos campos del encabezado IPv4 han sido eliminados o determinados opcionales.

La figura 15, muestra el formato de encabezado del protocolo de internet versión 6 (IPv6).

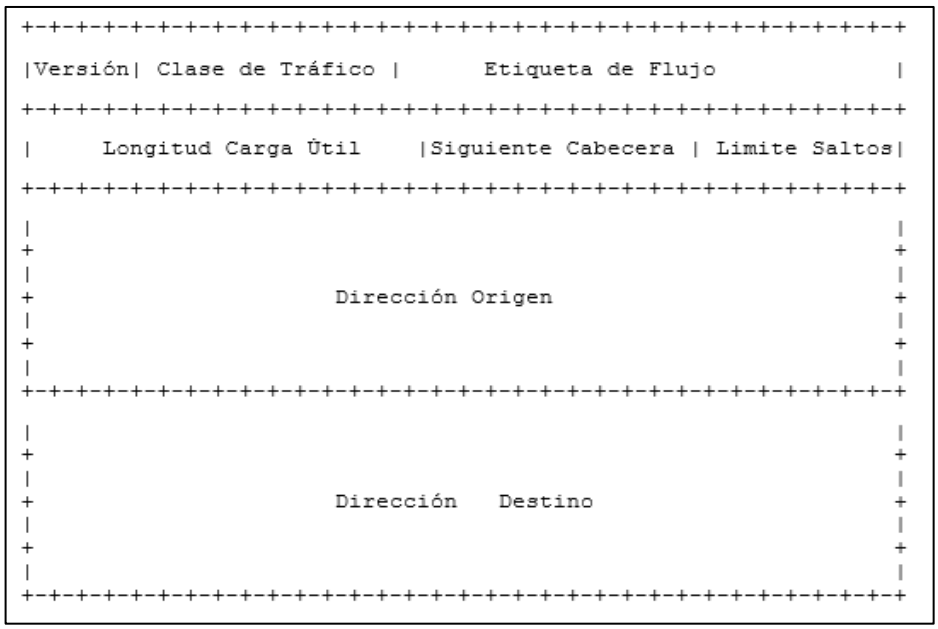


Figura 15. Formato de Encabezado IPv6
Fuente: RFC 2460 (1998)

- **Capacidad de etiquetado de flujo**

En IPv6 se adiciona una solicitud hecha por el emisor por un manejo especial el cual permite etiquetas de paquete pertenecientes a flujos de tráfico en particular.

- **Autenticación y privacidad**

En esta versión, se adicionan extensiones para admitir autenticación, integridad de datos y la confidencialidad de los datos.

2.3. Marco Conceptual

2.3.1. Protocolos Syslog y SNMP

A. Complejidad de configuración

La complejidad de configuración de protocolos como una de las dimensiones, de la variable independiente trata de explicar el contexto y limitaciones funcionales para SNMP y Syslog. La configuración de protocolos se refiere a plasmar a conveniencia los comandos de los protocolos con el fin recabar la mayor información de cada uno de ellos.

Indicadores

- Nivel de complejidad de configuración de SNMP
- Nivel de complejidad de configuración de Syslog

B. Uso de recursos computacionales

El uso de recursos computacionales como una de las dimensiones de la variable independiente, trata de explicar la cantidad de recursos disponibles del *router* que utiliza Syslog y SNMP al realizar sus funciones de reportar eventos.

Por ende, se realiza una evaluación sobre quien consume más recursos, Syslog o SNMP.

Indicadores

- Nivel de uso de CPU de Syslog
- Nivel de uso de memoria en Syslog
- Nivel de uso de ancho de banda para Syslog
- Nivel de uso de CPU de SNMP
- Nivel de uso de memoria en SNMP
- Nivel de uso de ancho de banda para SNMP

C. Seguridad de protocolos

La seguridad de protocolos como una de las dimensiones de la variable independiente, trata de explicar el nivel de seguridad para que tiene cada protocolo al ser vulnerados de su configuración por defecto.

Indicadores

- Nivel de integridad de Syslog
- Nivel de confidencialidad de Syslog
- Nivel de integridad de SNMP
- Nivel de confidencialidad de SNMP

D. Servicios Disponibles

Los servicios disponibles como una de las dimensiones de la variable independiente, trata, de explicar el grado de detalle que emite cada servicio para recopilar los mensajes de Syslog y SNMP.

2.3.2. Gestión de red

A. Eficacia

La eficacia de la gestión de red como una de las dimensiones de la variable dependiente, trata de constatar el cumplimiento de los objetivos de la gestión de red, a través del reporte de los eventos suscitados al permitir la conexión, comunicación y transferencia de datos.

Indicadores

- Información de eventos reportados

B. Eficiencia

La eficiencia de la gestión de red, como una de las dimensiones de la variable dependiente, trata de explicar el consumo del tiempo y recursos para cumplir los objetivos de la gestión de red.

Indicadores

- Tiempo invertido en gestión de la red

2.4. Hipótesis

2.4.1. Hipótesis general

La mejor alternativa para la gestión de Redes Avanzadas es la configuración de Syslog y SNMPv3 de forma complementaria.

2.4.2. Hipótesis Específicas

1. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de complejidad de configuración es Syslog y SNMPv3 de forma complementaria.

2. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de uso de recursos computacionales es Syslog.

3. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de seguridad de protocolo es la configuración de SNMPv3

4. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de servicios disponibles es la configuración de Syslog.

5. La alternativa de diseño de una topología para la Red Avanzada del Perú (RAAP) para la gestión eficiente estará basada en la ubicación de los nodos respecto los tipos y relevancia de instituciones científicas.

III. DISEÑO PROPUESTO DE LA RAAP

La Topología propuesta para la Red Avanzada del Perú, fue elaborada teniendo a universidades públicas y privadas licenciadas por SUNEDU a enero del 2018; desde que se aprobó la nueva ley universitaria el 2014, el proceso de acreditación está aún en marcha por lo que algunas universidades incorporadas a partir de enero del 2018 no fueron contempladas, sin embargo, si hubiera alguna universidad que pueda clasificar para ser añadida, tendría que evaluarse la ubicación para considerar si es factible o no, el acoplamiento de algún nodo dentro de la topología.

También se tomó en cuenta los principales centros de investigación a nivel nacional. De la información recopilada se destacó lo relevante de cada universidad, considerando:

- Cantidad de programas según nivel de enseñanza.

Se consideró una característica relevante para este estudio la cantidad de programas que posee cada universidad, debido a que se considera mayor la amplitud por abordar temas de investigación. Los departamentos considerados a continuación, son los más relevantes por poseer en algunas de sus instituciones un número significativo de programas de enseñanza: Lima, Arequipa, La libertad, Puno, Tacna, Ayacucho, Cusco, Piura, Huancavelica, Apurímac.

- Último registro de número de estudiantes.

Se consideró una característica relevante para este estudio, el tener en cuenta el último registro de número de estudiantes que posee cada universidad,

debido a que a mayor amplitud existe mayor posibilidad de aprovechar el intercambio de conocimientos dentro de una red avanzada, los departamentos considerados relevantes se detallan a continuación, son los más relevantes por poseer en algunas de sus instituciones un número significativo de estudiantes: Lima, La libertad, Puno, Junín, Cusco, Arequipa, Ayacucho, Cajamarca, Amazonas, Piura, Huancavelica, Apurímac.

- Recursos destinados para la investigación

Considerado como un aspecto resaltable, debido a ser uno de los factores para que las Redes Avanzadas se mantengan en vigencia; para este estudio se tomó como referencia las fichas técnicas de cada universidad, obteniendo universidades que tienen más fortalecida la inversión en aspectos de investigación. Los departamentos detallados a continuación son considerados relevantes para este estudio, por poseer en algunas de sus instituciones un número significativo de inversión: Tacna, Arequipa, La libertad, Lima, Cusco, Puno, Lambayeque, Ucayali, Cajamarca, Junín

- Centros de investigación

Loreto, San Martin fueron considerados por los centros de investigación, que posee, además de poseer, un número significativo de publicaciones.

Se analizó los datos recabados; del total de universidades se pudo corroborar un alto porcentaje de universidades se concentran en Lima. Los detalles de la recopilación e ilustración de estas entidades educativas se pueden apreciar en el Anexo 2.

El diseño propuesto de la topología es una red WAN, desarrollada en base a la Red Dorsal Nacional de Fibra óptica. Esta otra característica se tomó en cuenta debido a requerimientos presentes de interconexión con cada entidad educativa y centros de investigación.

3.1. Ubicación de Nodos

Para la identificación de los nodos se tiene en cuenta la distribución de la red dorsal en el país. La elaboración del diseño consta de una combinación de topología punto a punto con malla extendida.

El diseño de red estará conformado por nodos conformados en las siguientes ciudades, proponiendo tener una cobertura con dieciocho departamentos, como se indica en la tabla 3.

Tabla 3: Distribución de Nodos

Nodo	Numero de Nodos
Lima	3
Piura	1
Lambayeque	1
Cajamarca	1
La Libertad	1
Arequipa	1
Moquegua	1
Tacna	1
Puno	1
Cusco	1
Apurímac	1
Ayacucho	1
Huancavelica	1
Junín	1
Ucayali	1
San Martín	1
Amazonas	1
Loreto	1

Fuente: Elaboración Propia

Realizando un análisis de la cantidad de instituciones contempladas por departamento, Lima contiene el mayor número de instituciones que existen actualmente, por ende, se propone tener en esta ciudad una distribución de tres nodos agrupados, siendo uno de estos el nodo principal, el cual deberá tener comunicación hacia la actual internet y será el mismo que permita la salida hacia los nodos de CLARA.

Para la red dorsal pretende desplegar fibra óptica a un número considerable de sectores a nivel nacional, bajo este prospecto la propuesta de la red considera usar enlaces de fibra óptica para establecer conexión entre nodos de cada cuidad con canales de 1Gbps y 10 Gbps, que son capacidades especificadas en los términos de referencia del proyecto de la Red Dorsal. Además, se tomó como referencia la forma de comunicación de REUNA, quien utiliza diferentes tecnologías entre ellas la comunicación de enlaces de fibra óptica, pero ha incorporado en los últimos años la tecnología DWDM, que le permite habilitar sobre fibra óptica múltiples circuitos ampliando así el ancho de banda; cuenta con canales de 500 Mbps, 1 Gbps, 10 Gbps y 100Gbps. A partir de esto, se pretende proyectar a una Red Académica Peruana operativa utilizando este tipo de tecnologías.

En la figura 16 se puede apreciar el diseño de la topología propuesta para la red avanzada, seguido de la tabla 4, donde se especifican los anchos de banda pensada para la realización de transmisiones paralelas bajo una arquitectura abierta.

Figura 16. Propuesta de Diseño de Topología para la Red Académica Peruana
Fuente. Elaboración Propia

Tabla 4: Ancho de Banda de los enlaces

Ruta	Ancho de Banda (BW)
Tacna - Moquegua	10 Gbps
Moquegua - Arequipa	10 Gbps
Arequipa – Puno	10 Gbps
Arequipa – Lima (2)	10 Gbps
Lima (2) – Lima (1)	10 Gbps
Lima (1) – Junín	10 Gbps
Lima (1) - Lima (3)	10 Gbps
Lima (3) – La Libertad	10 Gbps
La Libertad – Lambayeque	10 Gbps
Lambayeque – Cajamarca	10 Gbps
Lambayeque – Piura	10 Gbps
Apurímac – Cusco	10 Gbps
Apurímac – Ayacucho	10 Gbps
Ayacucho – Huancavelica	10 Gbps
Huancavelica – Junín	10 Gbps
Junín – Ucayali	10 Gbps
Junín – San Martin	10 Gbps
San Martin – Loreto	1 Gbps
San Martin – Amazonas	10 Gbps

Fuente: Elaboración Propia

3.2. Opciones de Herramientas de Gestión de red

3.2.1. Nagios

Nagios es una herramienta de gestión de red basada en Linux para controlar la infraestructura de red. Puede monitorear dispositivos de red, Windows, Linux / Unix / BSD, Netware. El monitoreo se realiza mediante SNMP y scripts. Cuenta con un gran número de *plugins*.

Además, puede ser configurado para realizar alarmas frente a acciones que generan alguna falla, como notificar a correos electrónico al equipo técnico de la empresa o mensajes de texto, además de realizar acciones concretas como reiniciar un demonio. En la figura 17 se muestra la interfaz de Nagios.

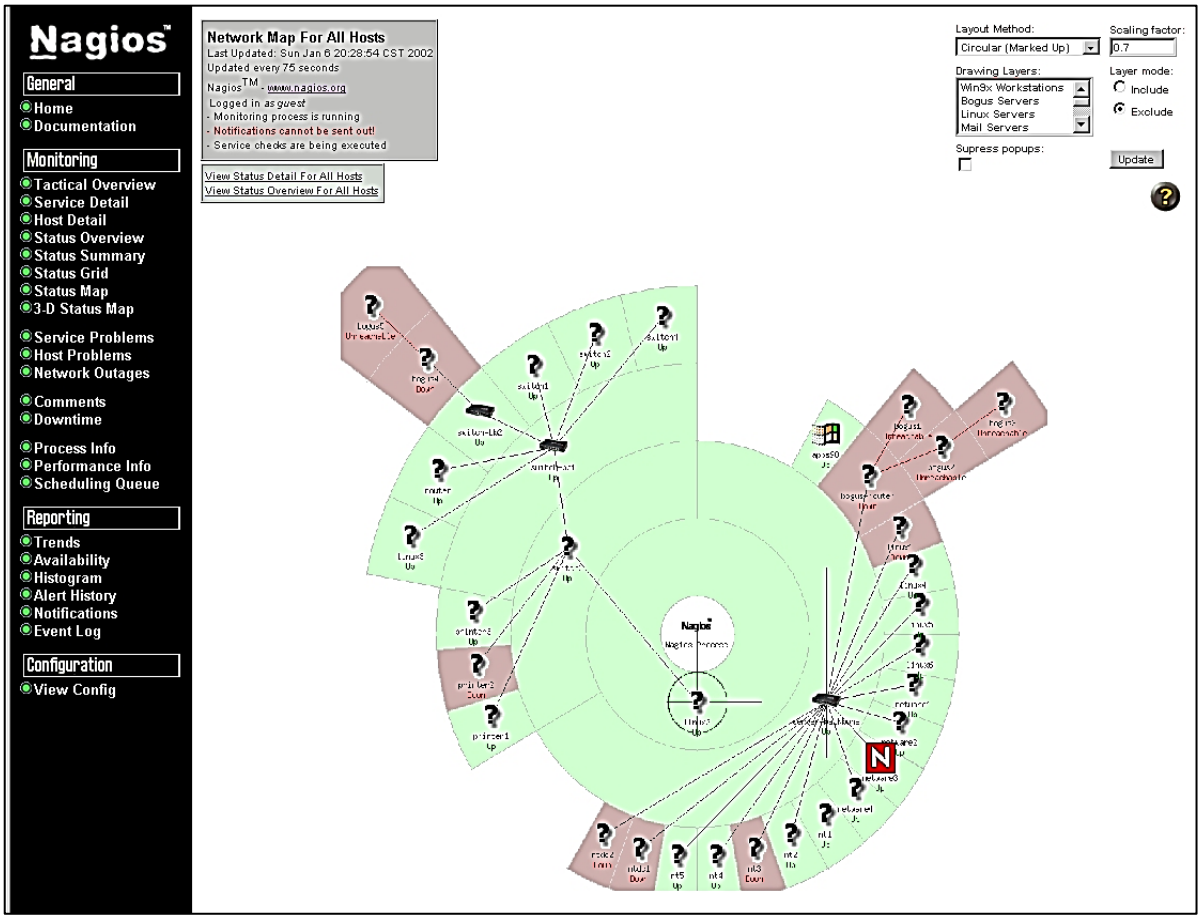


Figura 17. Interfaz Nagios.
Fuente: Documentación de la Página Oficial de Nagios

3.2.2. Zabbix

Zabbix herramienta de gestión de red creada en código abierto; ofrece un monitoreo avanzado, alertas y características de visualización y otras descritas a continuación:

- Detección automática de servidores y dispositivos de red
- Monitorización sin agentes
- Autenticación de usuarios
- Interfaz web
- Notificación de correo electrónico flexible de los eventos predefinidos
- Registro de *logs*
- Vista de recursos

3.2.3. Cacti

Cacti es una herramienta de monitoreo que almacena información en MySQL para crear gráficos. La interfaz está escrita en PHP, hace uso de RRDTools, y además permite utilizar scripts. Es posible implantarlo en Linux, solaris, BSD y Windows. Tiene una arquitectura de *plugins* que se instala de manera opcional para añadir algunas funcionalidades adicionales como mostrar mapas de red, definir límites y alertas, entre otros. La interfaz por defecto se muestra en la figura 18. En la Parte superior se aprecia los botones de navegación y en la parte izquierda las opciones de configuración.

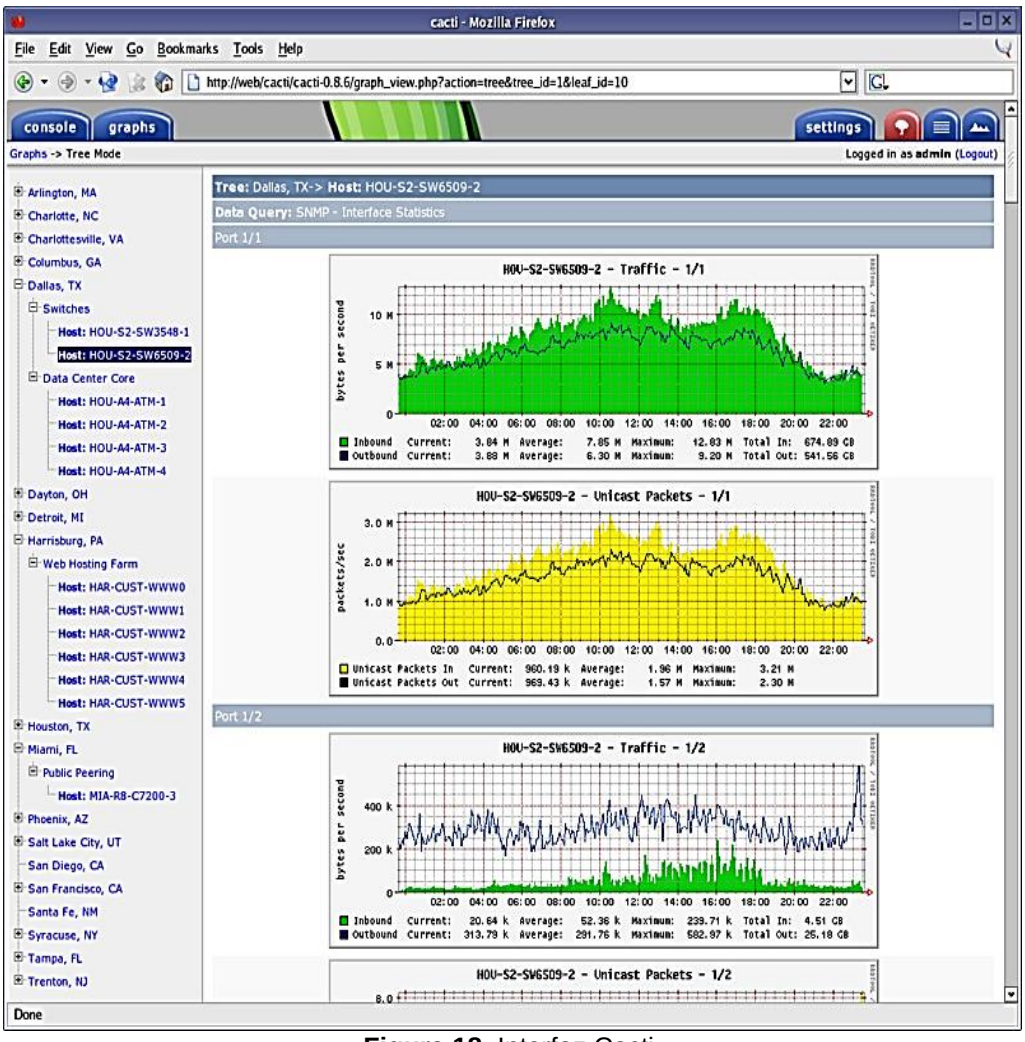


Figura 18. Interfaz Cacti.
Fuente: www.cacti.net

3.2.4. *Paessler Router Traffic Grapher*

PRTG es una herramienta de gestión en Windows, diseñada para ser ejecutada sobre la red durante las 24 horas al día, registra los parámetros de la red y envía datos detallados referentes a la está.

PRTG tiene una interfaz web sencillo de utilizar y con configuración *point-and-clic;* graficas en tiempo real, además de soporte de múltiples protocolos.

3.3. Selección de la herramienta

Para la selección de la herramienta se tomaron en cuenta características básicas para contar con la alternativa que mejor se ajuste para recopilar datos de los protocolos a evaluar

Una característica importante es que la herramienta sea configurable para IPv6, ya que toda Red Académica lo soporta y ademas promueven activamente su utilización.

Además, debe de contar con reportes de los *traps* generados por SNMP y a su vez la recopilación de *logs*, de forma que nos permita tener acceso a los reportes generados por los dispositivos en respuesta de ciertos eventos.

Finalmente, la herramienta que se utilizará debe tener la documentación detallada con la información del uso y configuración de la herramienta para recrear el escenario de pruebas.

A. Escenario de Pruebas

Para la evaluación de las herramientas se llevó a cabo en un escenario de pruebas se contempló solo 3 *routers* dentro de la topología.

Inicialmente se contempló la idea de usar unas herramientas *open source,* por ende, se propuso adicionar a los 3 *routers,* integrar a la topología Ubuntu Server y un Ubuntu Cliente para la visualización de la herramienta web, como se muestra en la figura 19.

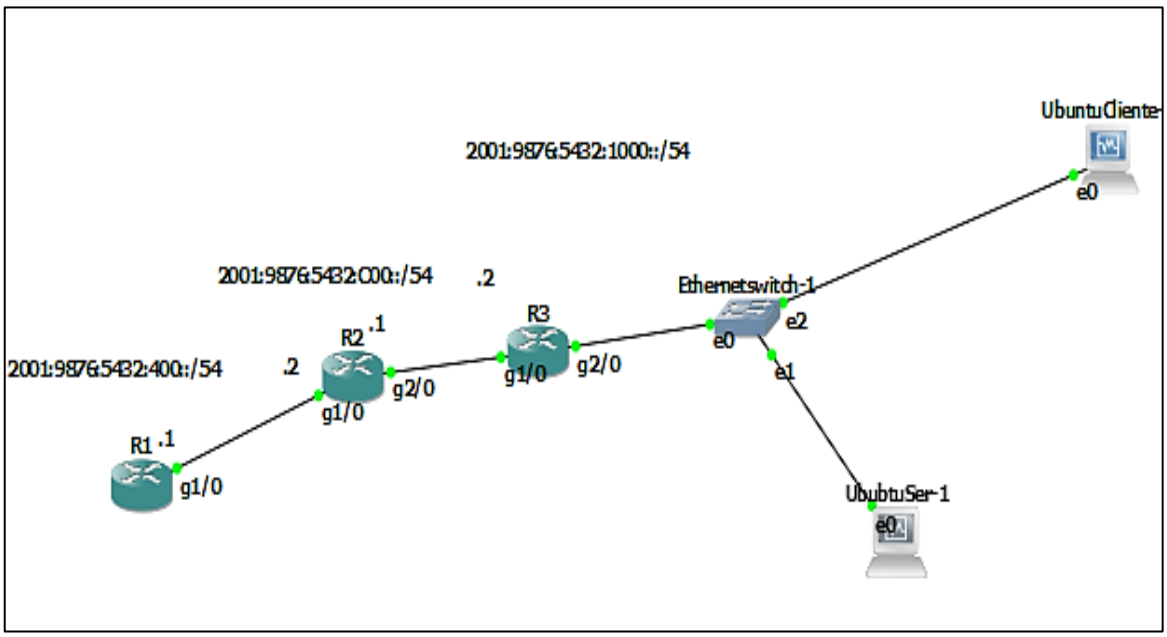


Figura 19. Escenario de Pruebas para *Open Source*
Fuente: Elaboración Propia

Debido a que las herramientas consultadas no contemplaban información detallada del soporte en IPv6, dificultó la culminación de un entorno de pruebas en el escenario detallado en la figura 19; por ende, se pasó a probar con alternativas comerciales en su versión *trial* como es el caso de la herramienta PRTG cuyo escenario se puede observar en la figura 20.

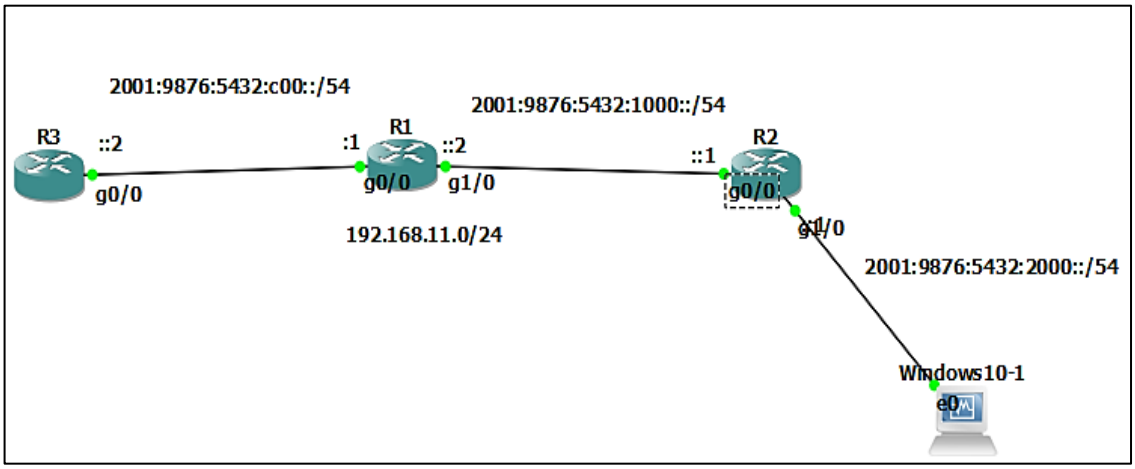


Figura 20. Escenario de Pruebas de Herramienta PRTG
Fuente: Elaboración Propia

B. Comparación entre herramientas

En concordancia con lo señalado de las características principales, la determinación de la herramienta más adecuada se tomó con base en las pruebas realizadas y haciendo un análisis de las funciones mínimas que debe tener la herramienta desde el punto de vista operativo. A continuación, en la tabla 5 se describen los resultados de la comparación de herramientas.

Tabla 5. Comparación de Herramientas de Gestión de Red.

Nombre		Cacti	Nagios	Zabbix	PRTG
Funcionalidades	Licencia	GLP	GLP (versión core)	GLP	Versión libre (100 sensores)
	Gráficos	Si	Si	Si	Si
	Estadísticas	Si	Si	Si	Si
	Mapeo de Red automático	SI A través de Plugin	SI A través de Plugin	Si	Si
Características Obligatorias	Soporte Ipv6	Última Versión (No especifica)	A través de Plugin	Si (escasa información de configuración)	Si
	SNMP	SI A través de Plugin	SI A través de Plugin	SI	Si
	Syslog	SI A través de Plugin	Solo uso Comercial	No	Si

Fuente: Elaboración Propia

Inicialmente se contempló la idea de trabajar con herramientas *open source,* pero presenta escasa información del soporte en IPv6, debido a esto no fue posible contar con un escenario de pruebas. Además, existen herramientas *open source* como Nagios, pandora y otros, cuya versión comercial supera en características funcionales a la versión GLP, quedando así desfasadas en el mercado actual. Sin embargo, el software PRTG presenta una propuesta de trabajo completa, cuya documentación fue accesible, aunque no es una herramienta GLP, es gratis para un máximo de 100 sensores.

PRTG fue elegido herramienta base, dado que contempla características necesarias para apoyar nuestro trabajo de investigación, además de poder encontrar en su página web información necesaria para recrear el escenario de pruebas, como el de emulación.

IV. EMULACIÓN DE REDES AVANZADAS CON PROTOCOLOS SYSLOG Y SNMP: CASO PROPUESTA RAAP

4.1. Escenario de Emulación

4.1.1. Especificaciones Técnicas de Hardware y Software

Para la emulación se ha trabajado con dos equipos físicos con las mismas características técnicas y en ambos instalados el software emulador, como se describe en la tabla 6.

Tabla 6: Especificaciones Técnicas de equipos físicos y hardware para emulación

Nombre	Características
Sistema Operativo	Ubuntu 18.04
Procesador	Intel® Core™ i7-3770k CPU @ 3.50 GHz
Memoria Instalada (RAM)	8 GB
Tipo de Sistema	Sistema operativo de 64 bits
Software Emulador	GNS3 versión 2.1.16

Fuente: Elaboración Propia

4.1.2. Instalación de Software Emulador GNS3 en Ubuntu

Se procedió a instalar la versión más actualizada y estable del emulador, donde:

1. En primer lugar, se procedió a agregar el repositorio de GNS3.

   ```
   root@cisco-desktop: add-apt-repository ppa:gns3/ppa
   ```

2. Actualizar nuestras fuentes

   ```
   root@cisco-desktop: apt-get update
   ```

3. Por último, instalar el GUI con la última versión del GNS3

   ```
   root@cisco-desktop: apt-get install gns3-gui
   ```

Una de las configuraciones adicionales que se realizo es añadir el soporte para IOU, con los siguientes comandos:

```
1. root@cisco-desktop: dpkg –add architecture i386
2. root@cisco-desktop: apt-get update
3. root@cisco-desktop: apt install dynamips:i386
```

Por último, para evitar problemas de permisos al agregar algún nodo, realizamos la siguiente configuración:

```
4. root@cisco-desktop: apt-get update
5. root@cisco-desktop: apt install sudo
6. root@cisco-desktop: usermod –aG sudo cisco
7. root@cisco-desktop: reboot -f
8. root@cisco-desktop: sudo dpkd-reconfigure ubridge
```

Todos los pasos fueron desarrollados en los dos equipos escogidos para la emulación.

4.1.3. *Router* de *Backbone* IOS Cisco C7200

Para el desarrollo de la emulación se utilizó un IOS *Router* C7200 con características detalladas a continuación:

- Cisco IOS Software
- 7200 Sofware (C7200-ADVIPSERVICESK9-M)
- Versión 15.2(4) S5
- *Release software* (fc1)
- 1 *Ethernet interface*

- 7 *gigabit Ethernet interfaces*
- 512 MiB de RAM
- 512 KiB DE NVRAM

A continuación, se detalla los pasos para agregar el IOS *Router* C7200:

a. Se Ingresa a *Preferences*

b. Seleccionamos *Dynamips -> IOS router*

c. Clic en *New*

d. Seguidamente se mostrará una ventana, donde se debe ingresar la imagen.

Los pasos mencionados se detallan a continuación en la figura 21.

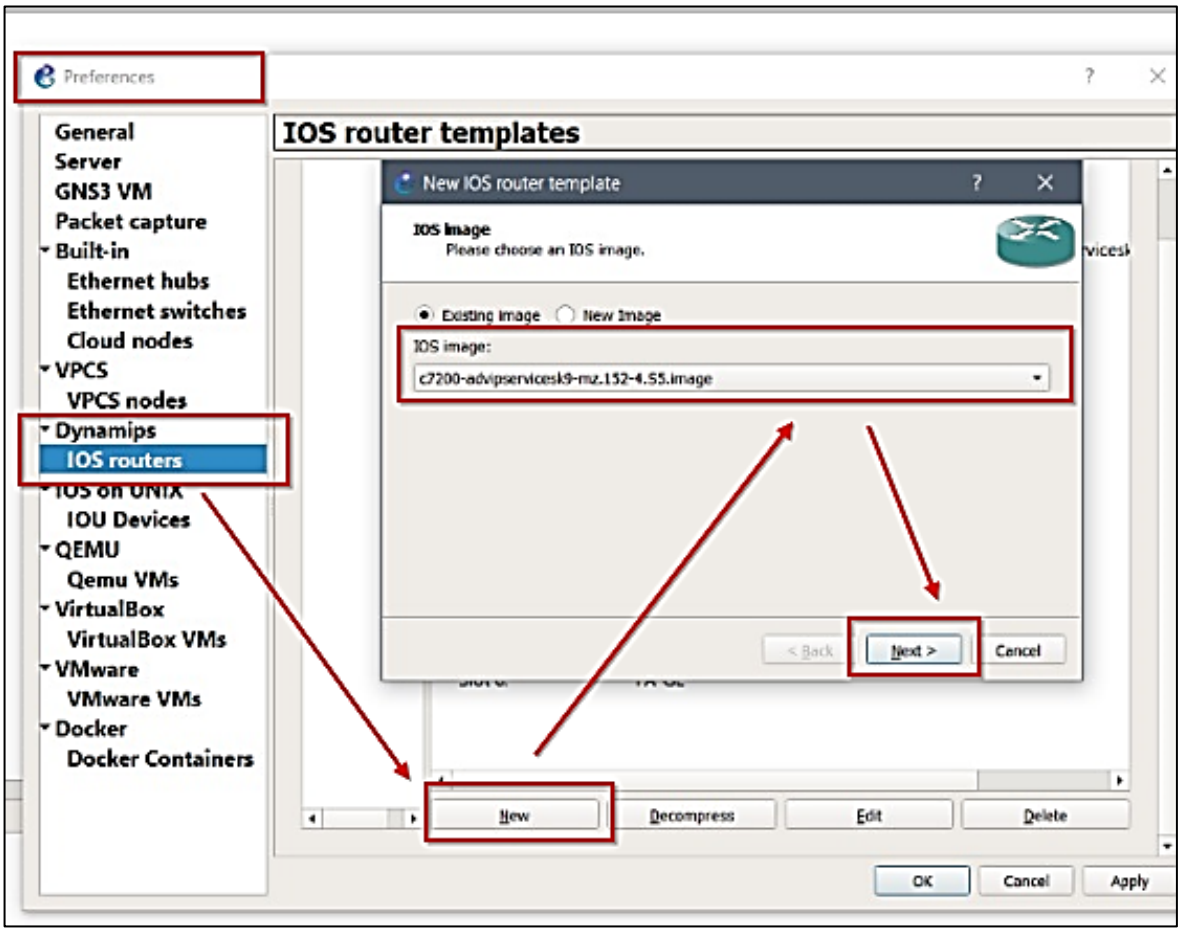


Figura 21. Agregar IOS *Router* C7200
Fuente: Elaboración Propia

4.1.4. Máquinas Virtuales

Para el presente trabajo de investigación se utilizaron dos máquinas virtuales dentro de le emulación, una con SO Windows Server 2012, que se utilizó como Servidor SNMP, Syslog y tftp y otra con SO Ubuntu 18.04, que se utilizaba como cliente se realizó con máquinas virtuales. Se utilizó para esto el software, Oracle VM VirtualBox versión 6.0.

En Windows Server 2012, se realizó la instalación de la herramienta con PRTG, la que a continuación se describe el proceso de implementación de la herramienta:

a. Ingreso a la Página web de la herramienta *Paessler.*
b. Descargar la versión prueba.
c. Instalación de la Herramienta.
d. Configuración del certificado digital SSL.
e. Configuración de usuarios.

4.2. Topología propuesta para la RAAP en GNS3

Para el desarrollo de la emulación en GNS3, principalmente se pensó en la capacidad del equipo físico, puesto a que el IOS r*outer* consume un porcentaje considerable de memoria RAM física; por lo que se optó por plasmar la mitad del número total del *routers* planteados en la topología, en dos máquinas físicas, conectadas por la red del Laboratorio de Redes y Seguridad cada una con 8 GB de RAM.

A continuación, en las figuras 22 y 23 se observa el diseño de la topología para la Red Académica Peruana construido en GNS3, que será el

escenario para trabajar los protocolos SNMPv2c y SNMPv3, además de Syslog, **de forma independiente**.

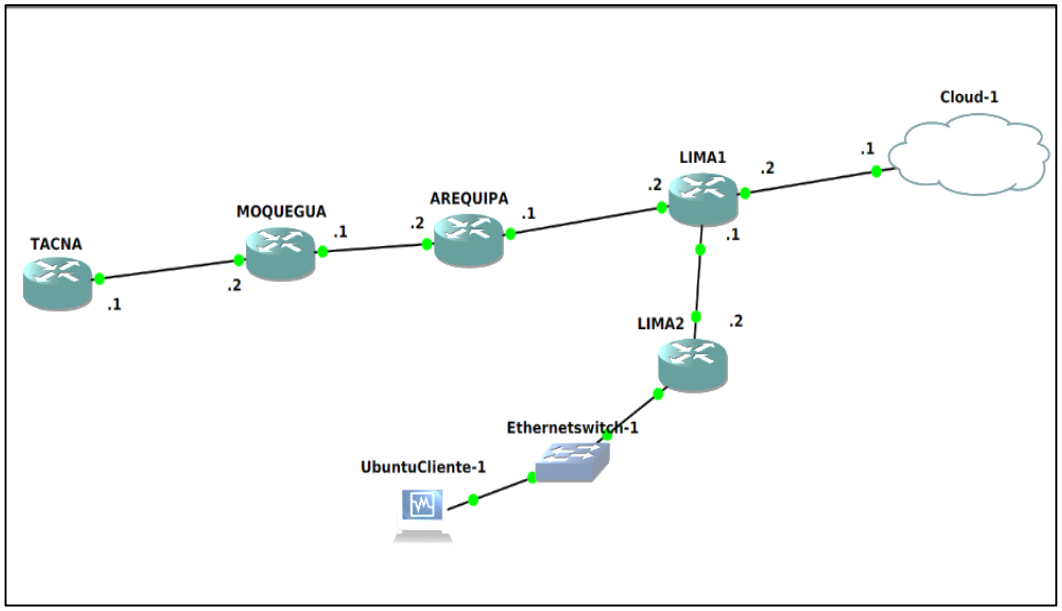


Figura 22. Propuesta de Topología de Red Académica Peruana en GNS3– Equipo 1
Fuente: Elaboración Propia

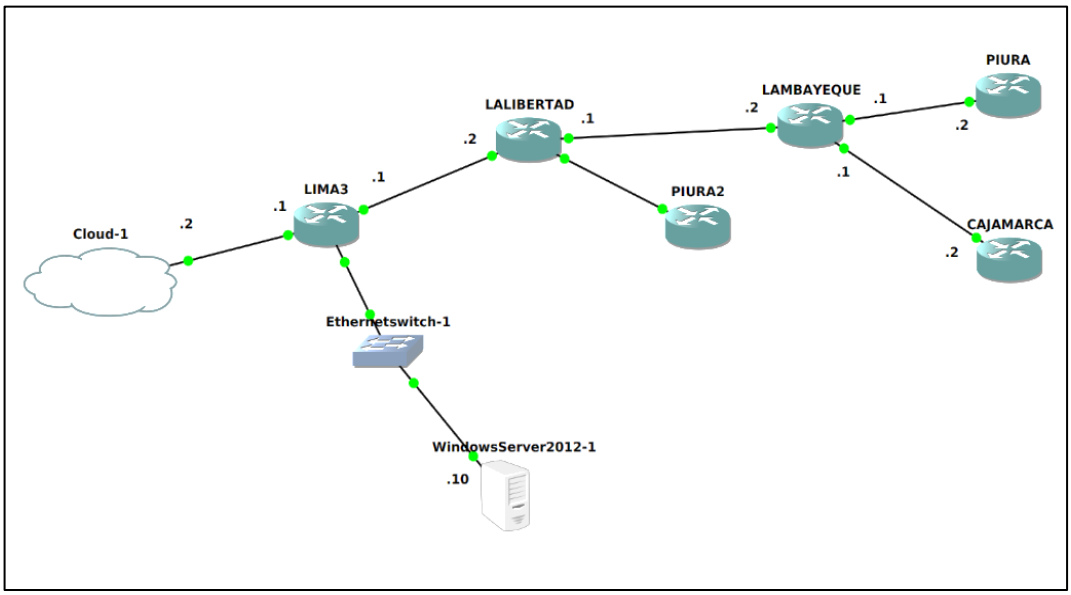


Figura 23. Propuesta de Topología de Red Académica Peruana en GNS3 – Equipo 2
Fuente: Elaboración Propia

Para la creación de la topología en gns3 se tuvo las siguientes consideraciones:

- Se optó por tener en cuenta los nodos contemplados en costa y sierra, debido a que se buscaba economizar los recursos del equipo optando solo por emular la mitad del número total de nodos.
- Se tomó en cuenta el nodo central Lima, puesto a que se concentra el mayor porcentaje de universidades y centros de investigación.
- El servidor encargado de recopilar información de los protocolos se encuentra ubicado en el nodo 2 de la región LIMA.
- Los enlaces utilizados en la emulación de la Topología son Gigabit Ethernet; por lo que se limita a solo 1 Gbps comparado a lo que se plantea en la topología real que lo muestra la tabla 4. En la tabla 7, se muestran las diferencias del ancho de banda (BW) de los enlaces utilizados en la emulación de los enlaces planteados.

Tabla 7. Ancho de Banda de los enlaces Propuestos y enlaces de emulación

Ruta	Emulación GNS3	Real
Tacna - Moquegua	1 Gbps	10 Gbps
Moquegua - Arequipa	1 Gbps	10 Gbps
Arequipa – Puno	1 Gbps	10 Gbps
Arequipa – Lima (2)	1 Gbps	10 Gbps
Lima (2) – Lima (1)	1 Gbps	10 Gbps
Lima (1) – Junín	1 Gbps	10 Gbps
Lima (1) - Lima (3)	1 Gbps	10 Gbps
Lima (3) – La Libertad	1 Gbps	10 Gbps
La Libertad – Lambayeque	1 Gbps	10 Gbps
Lambayeque – Cajamarca	1 Gbps	10 Gbps
Lambayeque – Piura	1 Gbps	10 Gbps
Apurímac – Cusco	1 Gbps	10 Gbps
Apurímac – Ayacucho	1 Gbps	10 Gbps

Ayacucho – Huancavelica	1 Gbps	10 Gbps
Huancavelica – Junín	1 Gbps	10 Gbps
Junín – Ucayali	1 Gbps	10 Gbps
Junín – San Martin	1 Gbps	10 Gbps
San Martin – Loreto	1 Gbps	1 Gbps
San Martin – Amazonas	1 Gbps	10 Gbps

Fuente: Elaboración propia

En la topología planteada para la Red Académica Peruana lo enlaces planteados en su mayoría son de 10Gbps, pero debido a la limitación del IOS *Router* y del software GNS3, los enlaces utilizados fueron solo de 1 Gbps, como se detalla en la tabla 7.

4.3. Desarrollo de Emulación de Redes Avanzadas con SNMPv2c – Escenario 1

Para desarrollar la emulación se utilizó la topología indicada en el punto anterior; en sección se detallará la configuración realizada para el escenario 1, el que se basa únicamente en SNMPv2c.

4.3.1. Configuración del r*outer* C7200

A. Para realizar cualquier acción sobre el *router* es necesario encenderlo por ello, nos ubicamos en *router*, clic derecho *"Start".*

B. Realizado la acción anterior, sobre el *router* clic derecho "*Console".*

C. A continuación, aparecerá una ventada de configuración del *router,* tal como se muestra a continuación.

D. Seguidamente se procedió a realizar la configuración de las direcciones IPv6 en las interfaces de cada *router*. En la tabla 8 se muestra las direcciones IPv6 utilizadas dentro de la topología.

Tabla 8: Direcciones IPv6 en GNS3 para Escenario SNMP v2c

Ruta	Dirección
Tacna -Moquegua	2001:9876:5432:400::/54
Moquegua - Arequipa	2001:9876:5432:c00::/54
Arequipa - Puno	2001:9876:5432:1400::/54
Arequipa -Lima1	2001:9876:5432:1c00::/54
Lima 2	2001:9876:5432:2800::/54
Lima 1 - Lima 3	2001:9876:5432:2c00::/54
Lima 3	2001:9876:5432:3000::/54
Lima 3 - La Libertad	2001:9876:5432:7C00::/54
La libertad - Lambayeque	2001:9876:5432:8400::/54
Lambayeque - Cajamarca	2001:9876:5432:8C00::/54
Lambayeque - Piura	2001:9876:5432:9400::/54

Fuente: Elaboración propia

E. Posterior a las configuraciones de IPv6, se configuró los *router* ID en cada configuración del protocolo OSPF. En la tabla 9, se muestran las direcciones utilizadas para cada *router* ID.

Tabla 9: Direcciones para r*outer* ID en GNS3 para SNMPv2c

Nodo	Dirección
Tacna	1.1.1.1
Moquegua	2.2.2.2
Arequipa	3.3.3.3
Lima 1	4.4.4.4
Lima 2	5.5.5.5
Lima 3	15.15.15.15
La libertad	9.9.9.9
Lambayeque	8.8.8.8
Piura	6.6.6.6
Cajamarca	7.7.7.7

Fuente: Elaboración propia

F. Finalmente se realiza las siguientes configuraciones en cada *router.*

- **Habilitar IPv6 y el protocolo de enrutamiento OSPF**

1. Habilitamos IPv6
   ```
   ROUTER(config)#ipv6 unicast-routing
   ```
2. Se asigna un “id” al protocol OSPF
   ```
   ROUTER(config)#ipv6 router ospf 1
   ```
3. Se asigna la dirección al id del *router*
   ```
   ROUTER(config-rtr)#router-id 1.1.1.1
   ```
4. Se asigna el OSPF a la interface Gig 1/0
   ```
   ROUTER(config)#interface gigabitEthernet 1/0
   ROUTER(config-if)#ipv6 ospf 1 area 0
   ```
5.
   ```
   ROUTER(config-if)#end
   ```

- **Habilitar SNMPv2c**

1. Configuración la comunidad “raap” con los permisos de Solo lectura
   ```
   Router(config)# snmp-server community "raap"
   ```
2. Comandos de información descriptiva
   ```
   Router(config)# snmp-server location "snmp_admin"
   Router(config)# snmp-server contact "raap_admin"
   ```
3. Se especifica la dirección IPV6 del server
   ```
   Router(config)#snmp-server host
   2001:9876:5432:3000::10
    version 2c "raap"
   ```
4. Habilitamos todas las *traps* predeterminadas disponibles
   ```
   Router(config)# snmp-server enable traps
   ```

4.3.2. Configuración del *Cloud*

Debido a que la topología se encuentra distribuido en dos equipos físicos, se configuro un *Cloud* en cada escenario con la finalidad de conectar ambas partes de la topología; los equipos físicos se encuentran conectados a través de la red del laboratorio de Redes y Seguridad. A continuación, se detalla la configuración realizada:

A. Primeramente, se revisa la configuración de red cableada de cada equipo, con la finalidad de identificar la interfaz física, lo cual se muestra en la figura 24.

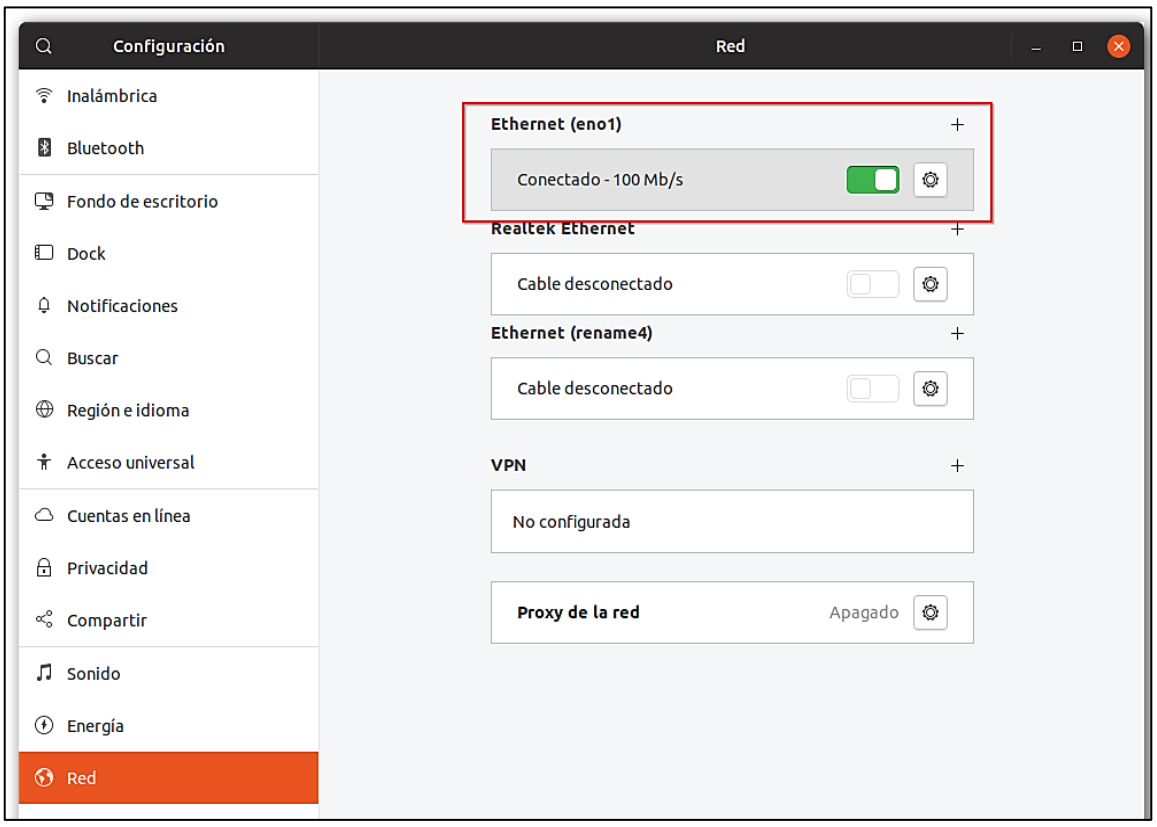


Figura 24. Configuración de red cableada
Fuente: Elaboración Propia

B. Dentro de la Topología se agrega el *cloud,* lo cual se muestra en la figura 25.

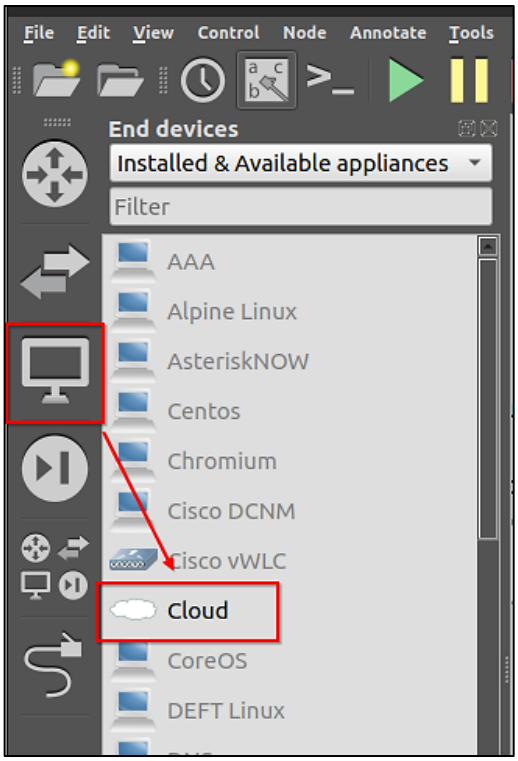


Figura 25. Insertar un *Cloud*
Fuente: Elaboración Propia

C. Clic derecho, "*configure*"

D. Posteriormente al paso anterior, se mostrará una ventana como muestra la figura 26. En esta Seleccionaremos el tipo de interfaz física activa.

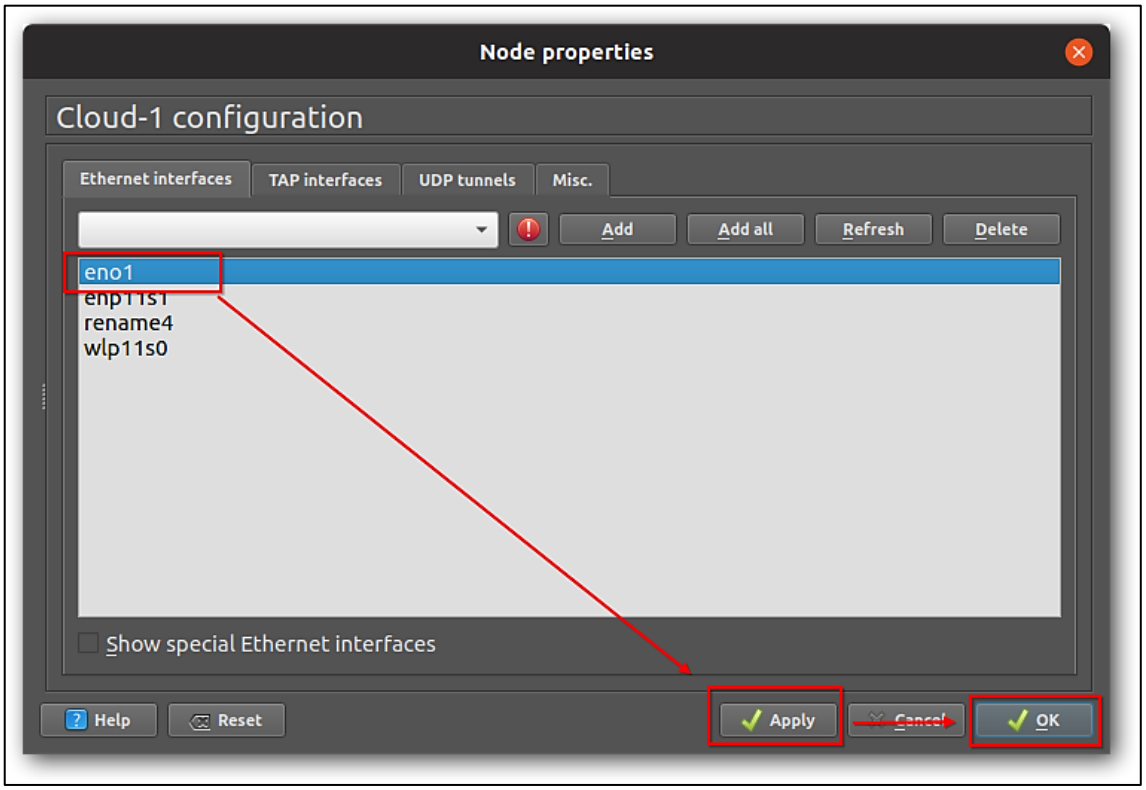


Figura 26. Configuración del *Cloud*
Fuente: Elaboración Propia

E. Por último, hacemos la conexión del *router* al *cloud.*

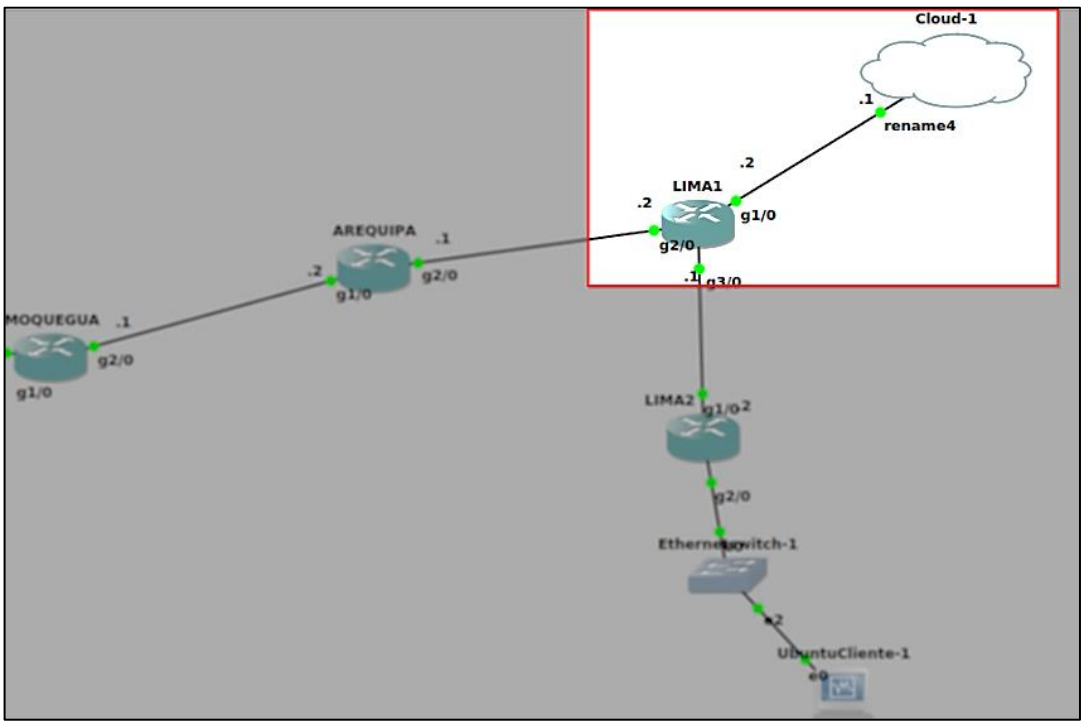


Figura 27. Conexión del *router* al *cloud*
Fuente: Elaboración Propia

Los pasos fueron repetidos para ambos equipos físicos, Asimismo, este punto fue repetitivo para los escenarios con SNMPv3 y Syslog.

4.3.3. Pruebas de Conectividad

Para comprobar la conectividad de la topología distribuida en dos equipos físicos, se realizó las pruebas utilizando el *router* PIURA, hacia el *router* TACNA ubicado en extremo del otro equipo. En las figuras 28 y 29 se muestra la ubicación de ambos *routers.*

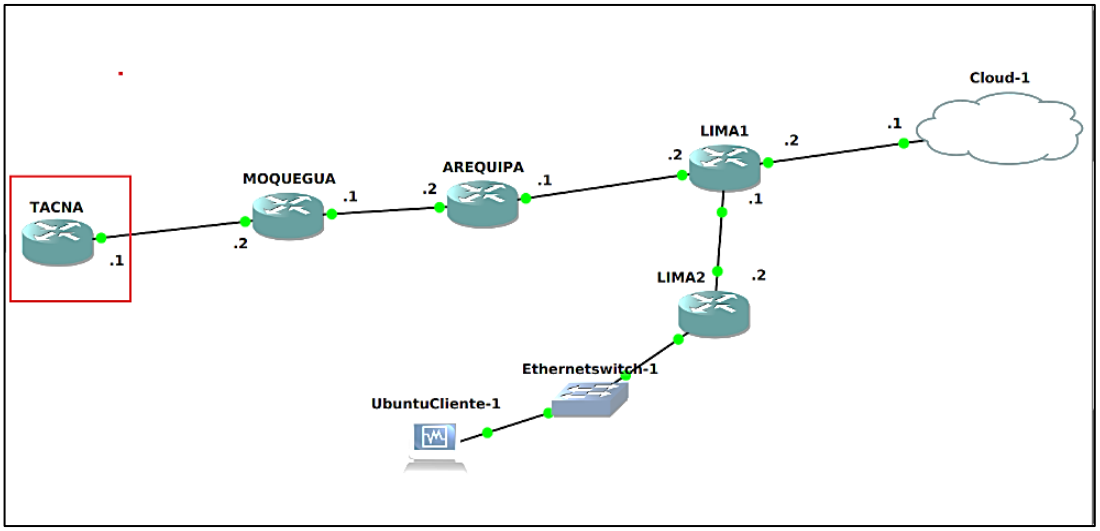


Figura 28. Ubicación de *router* TACNA
Fuente: Elaboración Propia

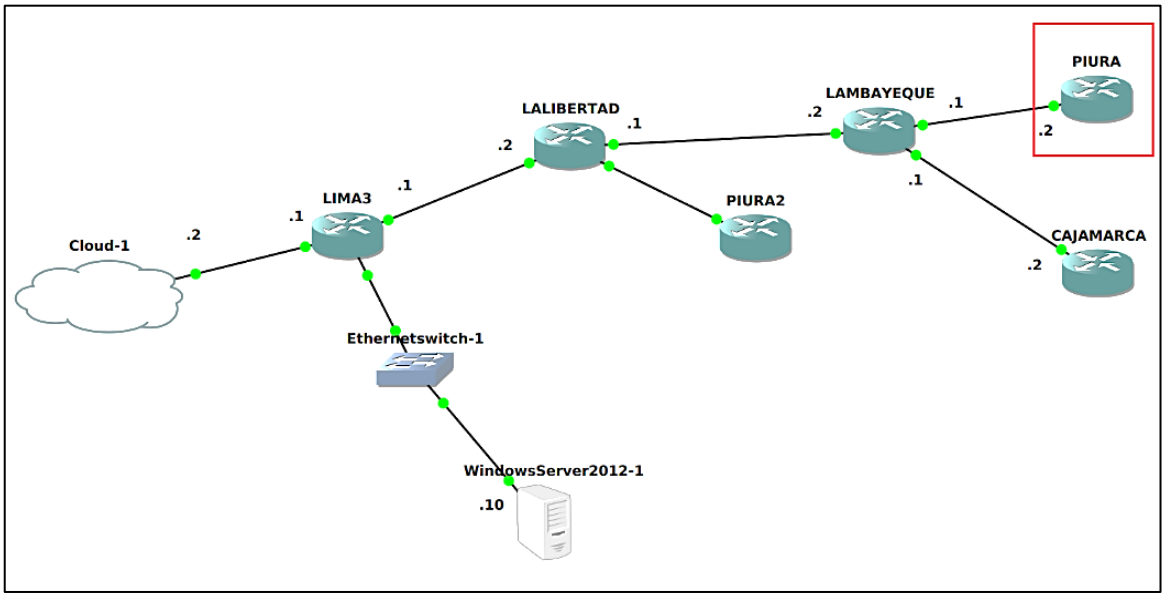


Figura 29. Ubicación del r*outer* TACNA
Fuente: Elaboración Propia

Para corroborar la conectividad se lanzó un ping desde el *router* PIURA hacia el *router* TACNA, lográndose satisfactoriamente comprobar la conectividad entre ambos *routers* de diferentes maquinas como se muestra en la figura 30.

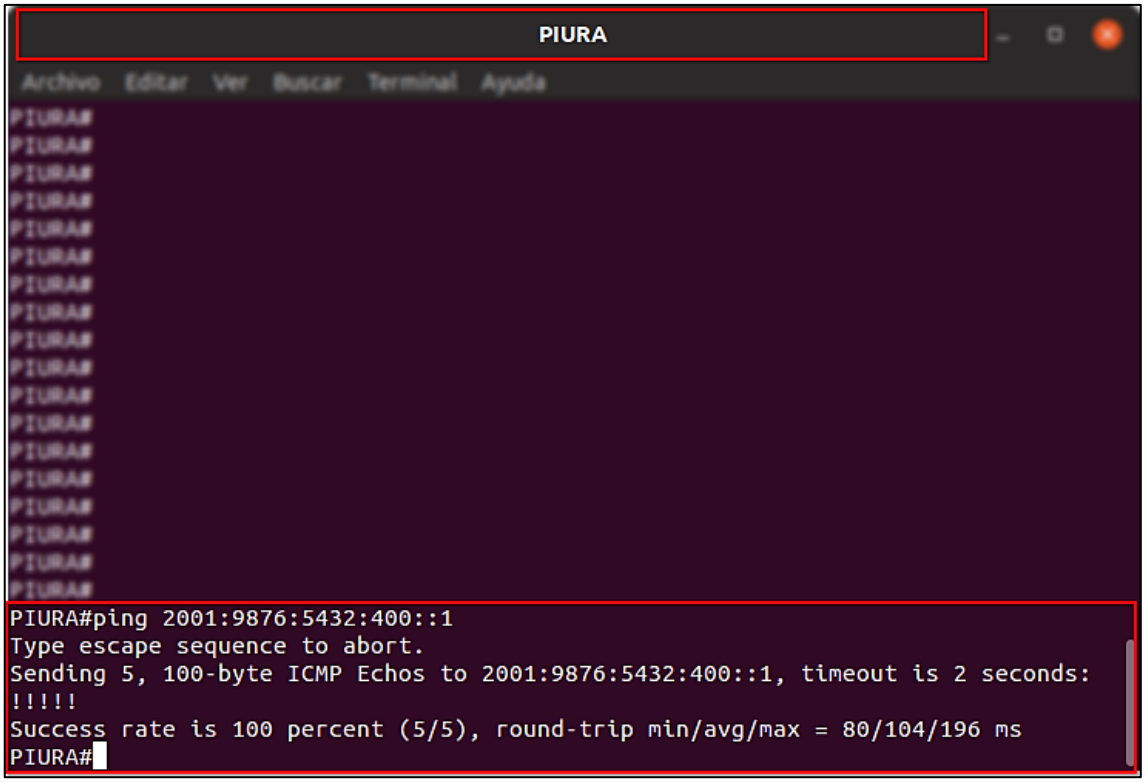


Figura 30. Ping satisfactorio desde el *router* PIURA hacia el *router* TACNA
Fuente: Elaboración Propia

4.3.4. Configuración del Servidor

Una vez realizados los pasos de instalación, se puede ingresar a la interfaz de herramienta, donde realizaremos la configuración de los equipos a monitorear.

A. Acceso al panel principal, en este paso nos identificamos con el usuario y contraseña de administrador, antes configurado. Como se muestra a continuación en la figura 31

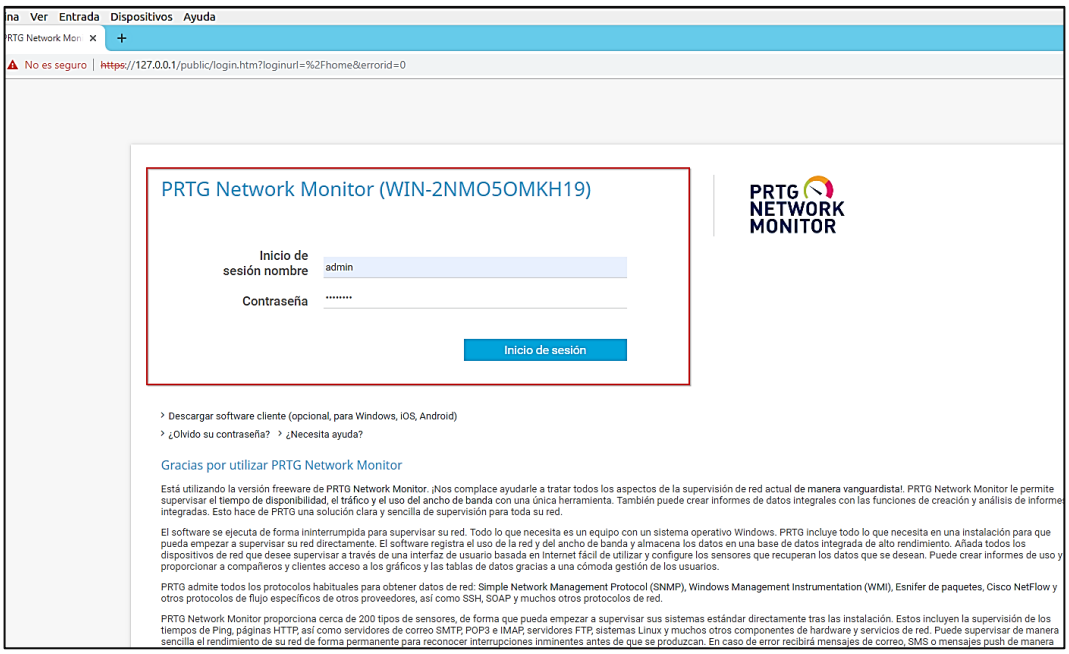


Figura 31. Interfaz de acceso de la herramienta PRTG
Fuente: Elaboración Propia

B. Luego de acceder al panel principal, la herramienta muestra los sensores correspondientes a las variables del servidor y las conexiones activas. Es decir, en este proceso se agrega por defecto el servidor y las interfaces de esta.

C. Se procedió a configurar el monitoreo para la Red Académica en la herramienta. Para ello se debe dar clic derecho sobre el primer grupo creado por defecto en la herramienta y cambien el nombre.

D. Posteriormente se procedió a realizar la configuración de los dispositivos, considerando que debe haber conexión total dentro de la topología.

- Nos ubicamos en dispositivo > “Agregar Dispositivo”, como se muestra en la figura 32.

Figura 32. Agregar dispositivo
Fuente: Elaboración Propia

- Seleccionamos al grupo creado específicamente para la Red Académica > “continuar”; como se muestra en la figura 33.

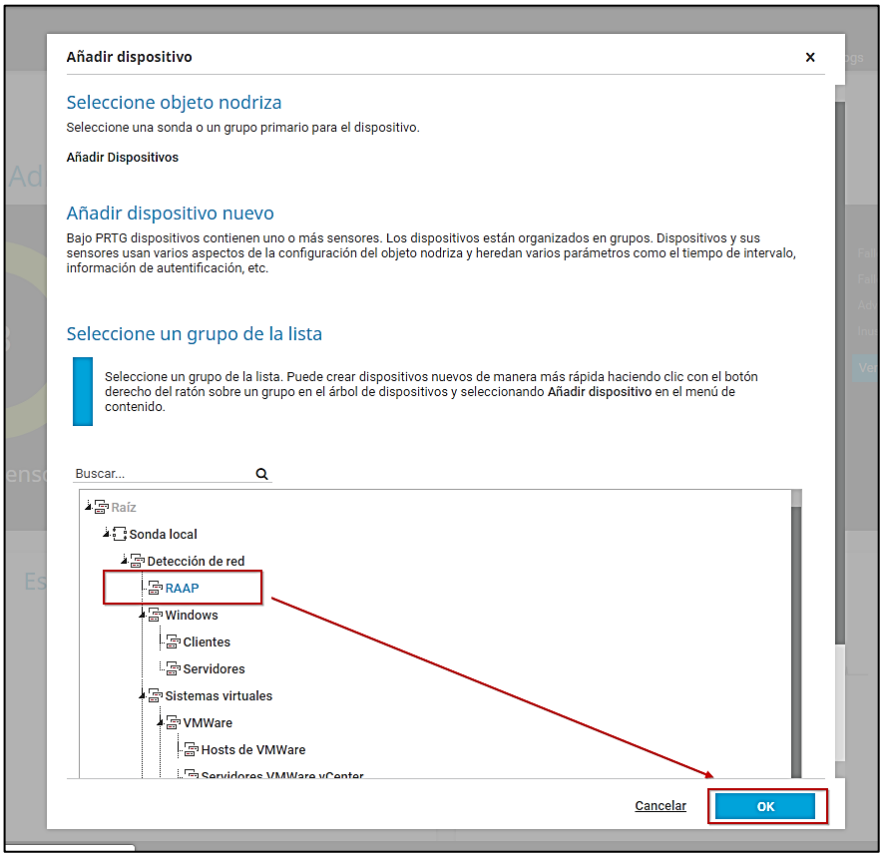


Figura 33. Detallar dispositivo al Grupo RAAP
Fuente: Elaboración Propia

- Seguidamente, nos mostrara una ventana para detallar las características del dispositivo. A continuación, en las figuras 34 y 35 se detalla las especificaciones que se tuvo para agregar cada dispositivo de la Red Académica.

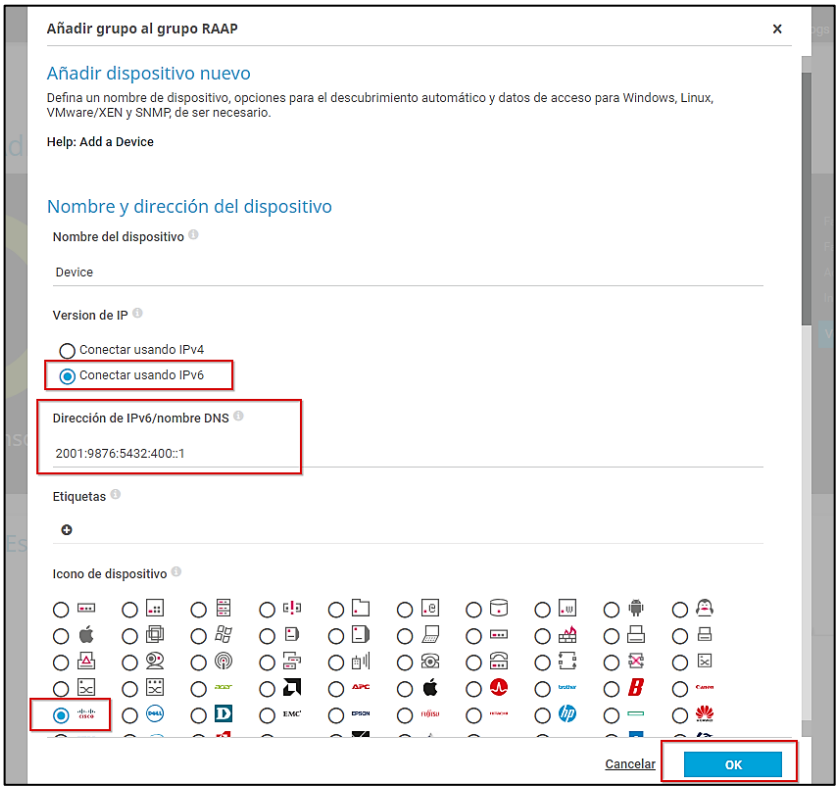


Figura 34. Características del r*outer* a Agregar
Fuente: Elaboración Propia

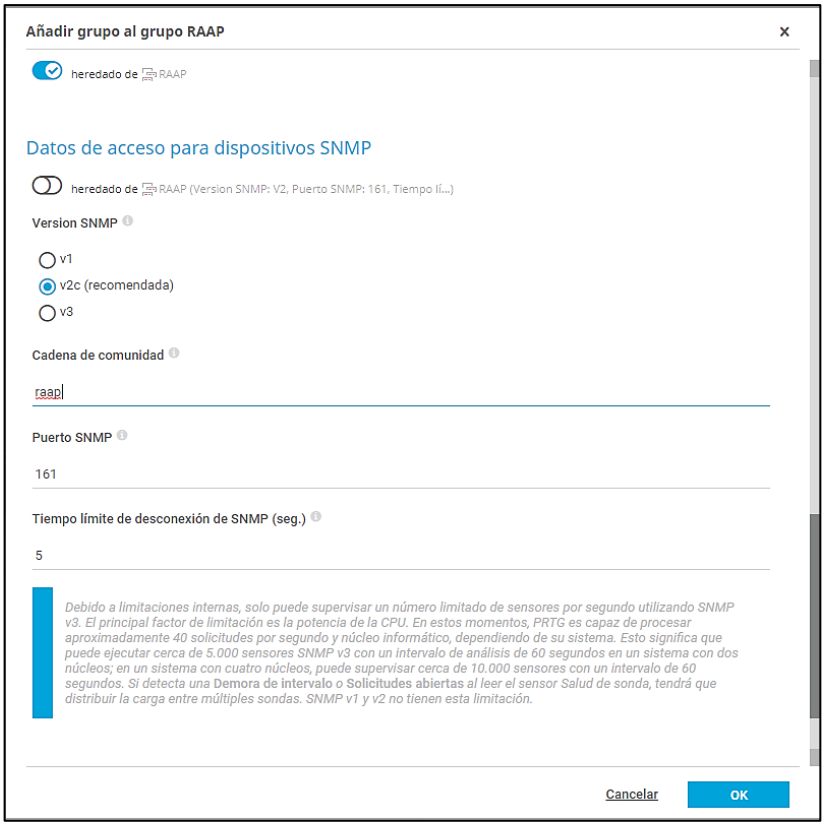


Figura 35. Características SNMPv2c
Fuente: Elaboración Propia

Esta acción se llevó a cabo para cada *router* que contiene la topología. En la figura 36 se muestra el resultado de la configuración de los diez *routers* de la topología.

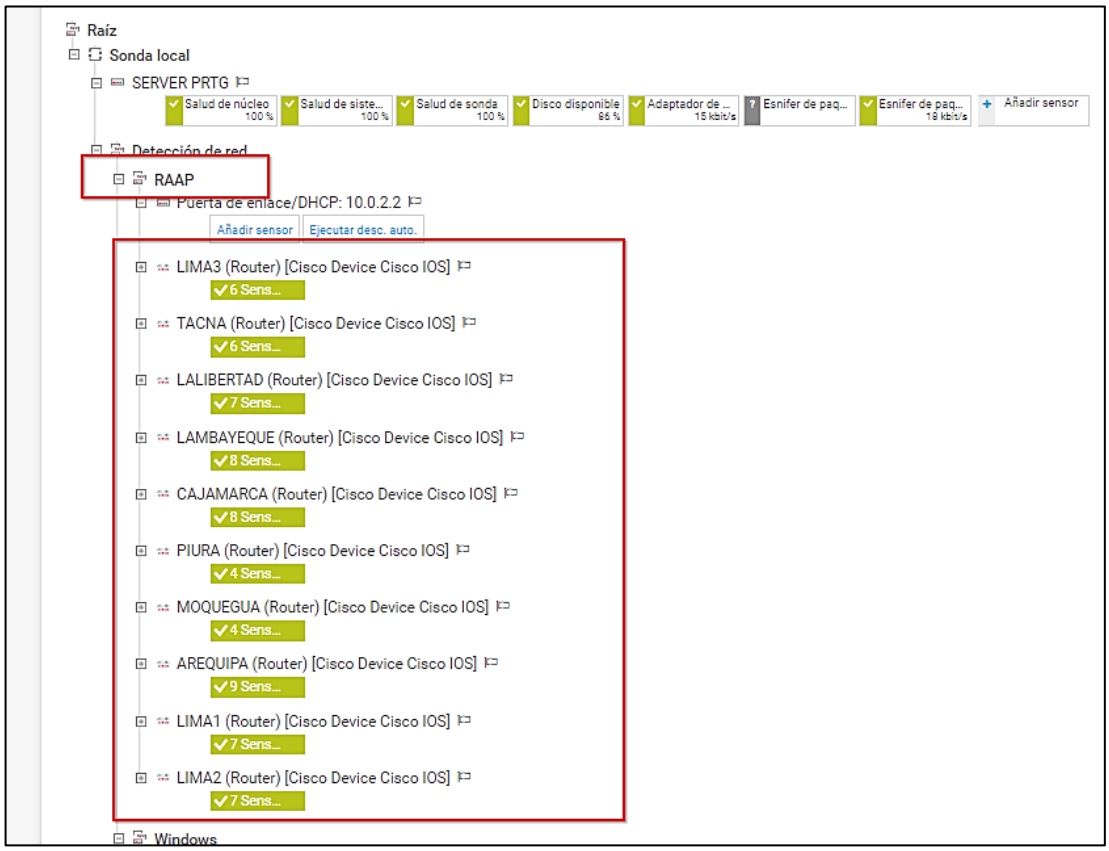


Figura 36. Interfaz de información del total *routers* agregados
Fuente: Elaboración Propia

Una vez ingresado los *routers* a la herramienta, se debe procedió a añadir los sensores, quienes nos servirán para recolectar los datos en las pruebas de este trabajo de investigación, los sensores varían de acuerdo con lo que se esté buscando obtener por cada *router*. A continuación, realizaremos los pasos para añadir un sensor, como ejemplo se optó por el sensor "*Receptor SNMP Traps*", que uno de los sensores utilizados en las pruebas realizadas.

E. Se procedió a localizar sensores, *clic* en "Añadir sensor", como se muestra en la figura 37.

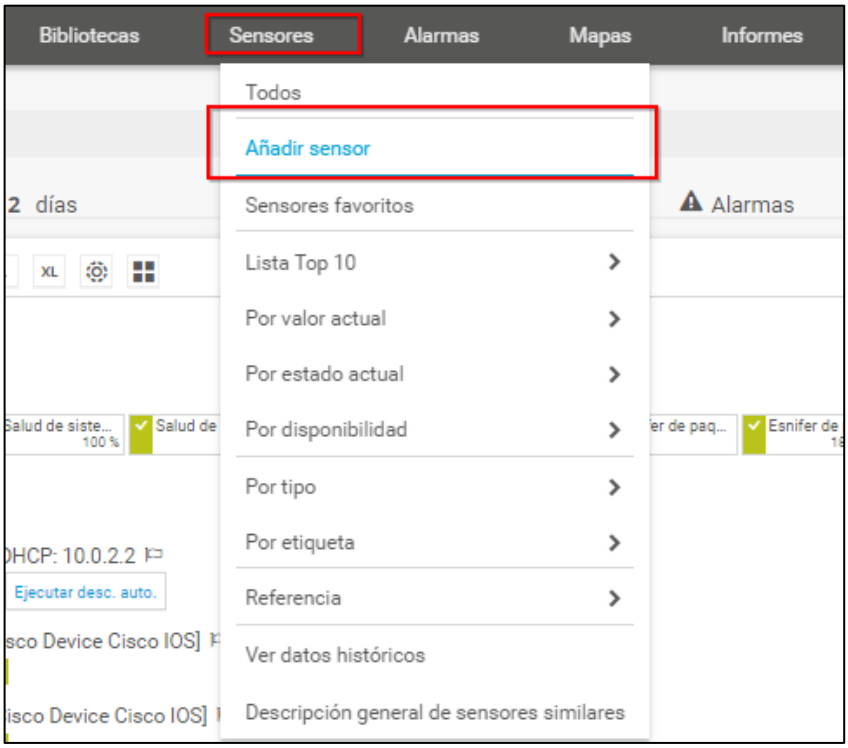


Figura 37. Añadir Sensor
Fuente: Elaboración Propia

F. Seleccionamos el *router* en que se añadirá el sensor, que nos facilitará a observar los *traps* emitidos por SNMPv2c, para ello seleccionamos: "añadir sensor a dispositivo existente" seguidamente, seleccionamos el *router*, y luego le damos clic en "guardar, como se muestra en la figura 38.

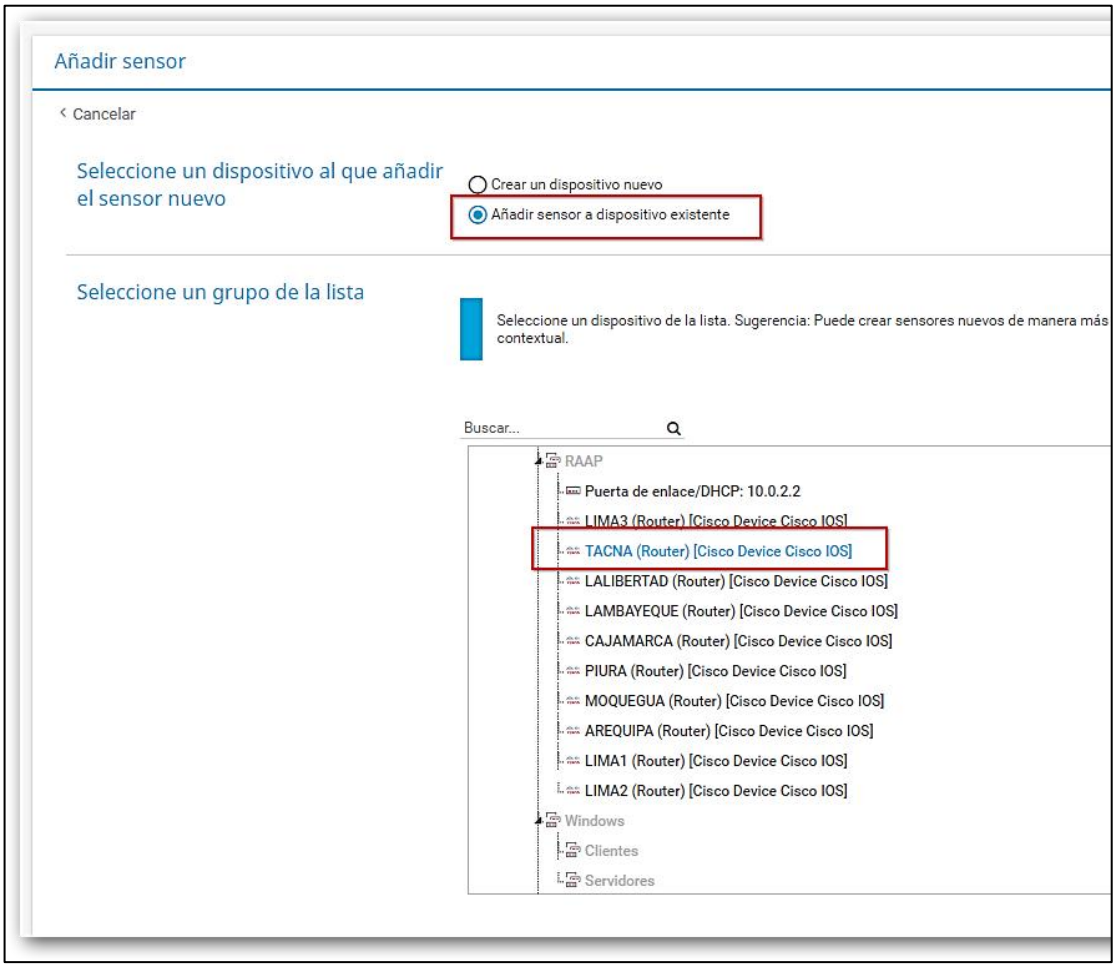


Figura 38. Seleccionar el *router* que será Agregado el Sensor
Fuente: Elaboración Propia

G. En el siguiente cuadro de Dialogo, seleccionaremos el sensor, para esto digitamos el nombre del sensor "*Receptor* SNMP *Traps*", como se muestra en la figura 39.

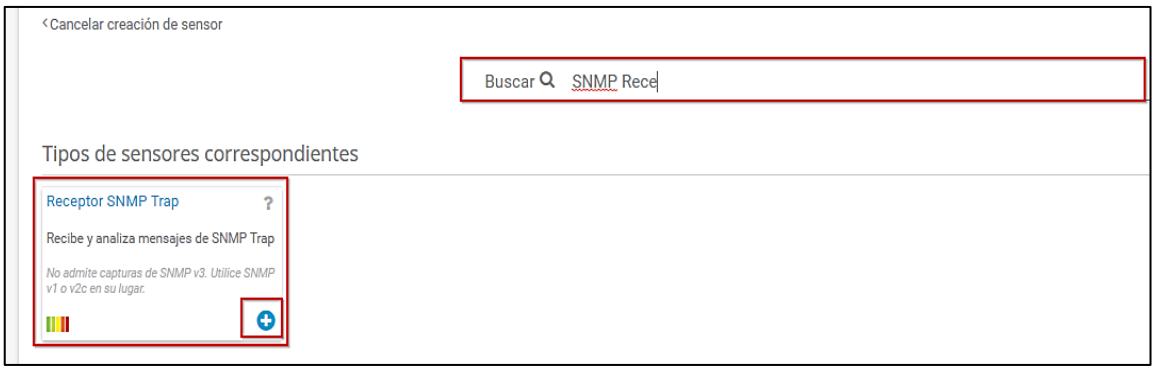


Figura 39. Añadiendo Sensor *"Receptor SNMP Traps"*
Fuente: Elaboración Propia

H. Nos aparecerá una interfaz para poner los parámetros de SNMPv2c. Como se muestra en la figura 40. Esta secuencia de pasos fue repetida para cada uno de los *routers* considerados dentro de la emulación.

Figura 40. Configuración del sensor *"Receptor SNMP Traps"*
Fuente: Elaboración Propia

4.4. Desarrollo de Emulación de Redes Avanzadas con SNMPv3 – Escenario 2

4.4.1. Configuración de *Router C7200*

Se detalla a continuación los pasos que se tomó en cuenta para la configuración del *router* C7200

A. Para realizar cualquier acción sobre el *router* es necesario encenderlo por ello, nos ubicamos en *router*, clic derecho *"Start"*

B. Realizado la acción anterior, sobre el *router* clic derecho "*Console"*

C. A continuación, aparecerá una ventada de configuración del *router.*

D. Seguidamente se procedió a realizar la configuración de las direcciones IPv6 en las interfaces de cada *router*. En la tabla 10 se muestra las direcciones IPv6 utilizadas dentro de la topología.

Tabla 10: Direcciones IPv6 utilizadas para SNMPv3 – Escenario 2

Ruta	Dirección
Tacna -Moquegua	2001:9876:5432:400::/54
Moquegua - Arequipa	2001:9876:5432:c00::/54
Arequipa - Puno	2001:9876:5432:1400::/54
Arequipa -Lima1	2001:9876:5432:1c00::/54
Lima 2	2001:9876:5432:2800::/54
Lima 1 - Lima 3	2001:9876:5432:2c00::/54
Lima 3	2001:9876:5432:3000::/54
Lima 3 - La Libertad	2001:9876:5432:7C00::/54
La libertad - Lambayeque	2001:9876:5432:8400::/54
Lambayeque - Cajamarca	2001:9876:5432:8C00::/54
Lambayeque - Piura	2001:9876:5432:9400::/54

Fuente: Elaboración propia

E. Posterior a las configuraciones de IPv6, se configuro los *router* ID en cada configuración del protocolo OSPF. En el tabla 11, se muestran las direcciones utilizadas para cada *router* ID.

Tabla 11*:* Direcciones para *router* ID en GNS3 para escenario de SNMPv3

Nodo	**Dirección**
Tacna	1.1.1.1
Moquegua	2.2.2.2
Arequipa	3.3.3.3
Lima 1	4.4.4.4
Lima 2	5.5.5.5
Lima 3	15.15.15.15
La libertad	9.9.9.9
Lambayeque	8.8.8.8
Piura	6.6.6.6
Cajamarca	7.7.7.7

Fuente: Elaboración propia

F. Finalmente se realiza las siguientes configuraciones en cada *router.*

- **Habilitar IPv6 y el protocolo de enrutamiento OSPF**

1. Habilitamos IPv6

```
ROUTER(config)#ipv6 unicast-routing
```

2. Se asigna un “id” al protocol OSPF

```
ROUTER(config)#ipv6 router ospf 1
```

3. Se asigna la dirección al id del *router*

```
ROUTER(config-rtr)#router-id 1.1.1.1
```

4. Se asigna el OSPF a la interface Gig 1/0

```
ROUTER(config)#interface gigabitEthernet 1/0
ROUTER(config-if)#ipv6 ospf 1 area 0
```

5.
```
ROUTER(config-if)#end
```

- **Habilitar SNMPv3**

Para este trabajo de investigación se procedió a configurar el tipo de seguridad "*AuthPriv"* pues tiene autenticación de usuario y además privacidad/cifrado.

Se configura la dirección del host donde se enviará las *traps,* además se habilita la versión 3 de SNMP y el tipo de seguridad que tiene el usuario que en este caso es "pri"

1. Se configura el nombre del grupo y el tipo de seguridad
   ```
   Router(config)# snmp-server groupraap v3 priv
   ```
2. Se especifica el nombre de usuario, el grupo al que pertenece, la autenticación que para este caso es md5 y el tipo de cifrado "des"
   ```
   Router(config)# snmp-server user usuarioraap gruporaap
   v3 auth md5 raap12345 priv des raap12345
   ```
3. Se configura la dirección del host donde se enviará las *traps*, además se habilita la versión 3 de snmp y el tipo de seguridad que tiene el usuario que en este caso "priv"
   ```
   Router(config)#snmp-server host 2001:9876:5432:3000::10
   version 3 priv usuarioraap
   ```
4. Habilitamos todas las *traps* predeterminadas disponibles
   ```
   Router(config)# snmp-server enable traps
   ```

4.4.2. Configuración del Servidor

Una vez realizados los pasos de instalación, se puede ingresar a la interfaz de herramienta, donde realizaremos la configuración de los equipos a monitorear.

A. Acceso al panel principal, en este paso nos identificamos con el usuario y contraseña de administrador, antes configurado.

B. Luego de acceder al panel principal, la herramienta muestra los sensores correspondientes a las variables del servidor y las conexiones activas. Es decir, en este proceso se agrega por defecto el servidor y las interfaces de esta.

C. Se procedió a configurar el monitoreo para la Red Académica en la herramienta. Para ello se debe dar clic derecho sobre el primer grupo creado por defecto en la herramienta y cambien el nombre.

D. Posteriormente se procedió a realizar la configuración de los dispositivos, considerando que debe haber conexión total dentro de la topología.

E. Nos ubicamos en dispositivo > “Agregar Dispositivo”

F. Seleccionamos al grupo creado específicamente para la Red Académica > “continuar”

G. Seguidamente, nos mostrara una ventana para detallar las características del dispositivo. A continuación, en las figuras 41 y 42 se detalla las especificaciones que se tuvo para agregar cada dispositivo de la Red Académica.

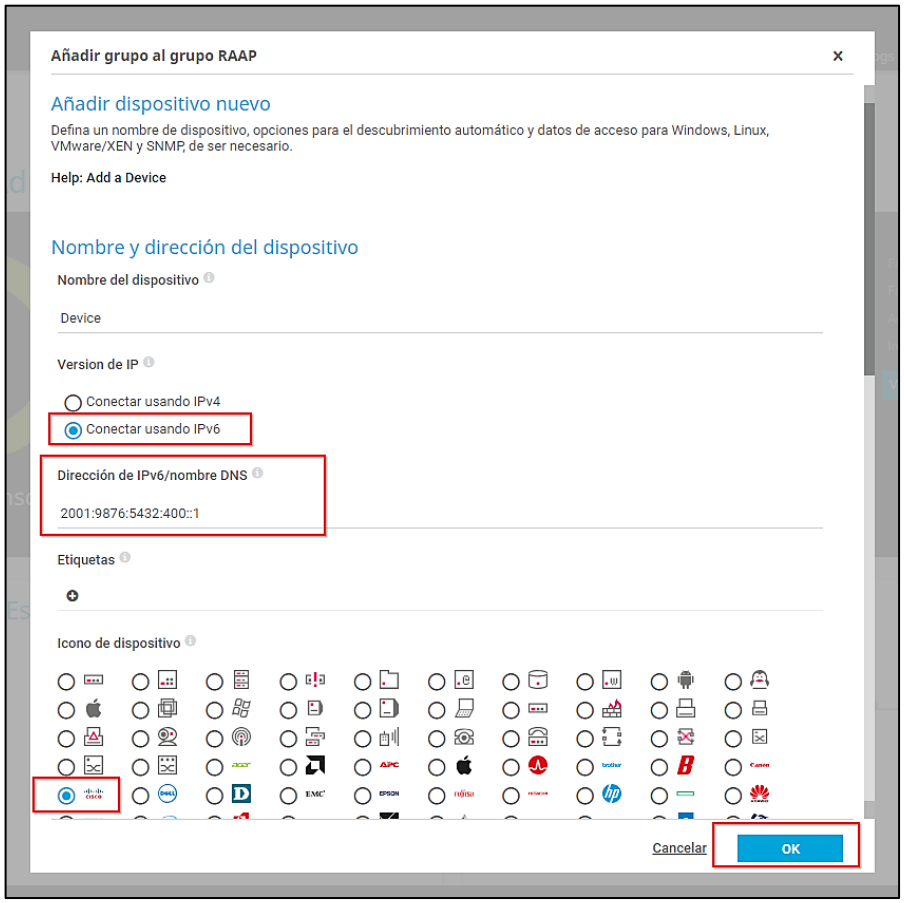


Figura 41. Configuración de características del *router*
Fuente: Elaboración Propia

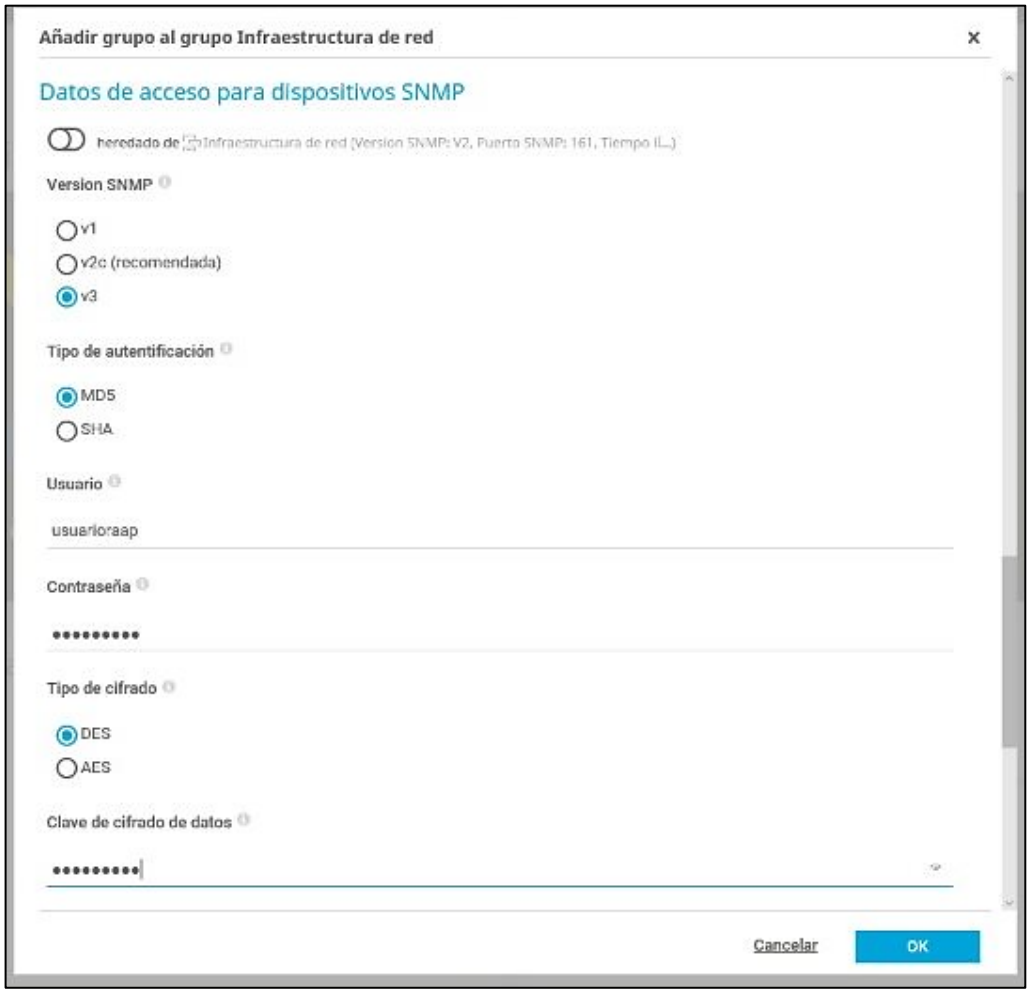


Figura 42. Características SNMPv3
Fuente: Elaboración Propia

El punto detallado anteriormente, es lo que diferencia a la configuración realizada en cada *router* de SNMPv2c con SNMPv3; se puede evidenciar las diferencias en los parámetros configurados para cada versión.

Para la emulación de Redes Avanzadas con SNMPv3, también se utilizaron sensores para recolectar los datos en las pruebas de este trabajo de investigación, los sensores fueron añadidos con el mismo procedimiento que se utilizaron en la versión 2c.

4.4.3. Configuración del *Cloud*

Debido a que la topología se encuentra distribuido en dos equipos físicos, se configuro un *Cloud* en cada escenario con la finalidad de conectar ambas partes de la topología; el procedimiento utilizado es el antes especificado en el punto 4.3.2.

4.5. Desarrollo de Emulación de Redes Avanzadas con Syslog – Escenario 3

4.5.1. Configuración de *Router* C7200

Se detalla a continuación los pasos que se tomó en cuenta para la configuración del *router* C7200.

A. Para realizar cualquier acción sobre el *router* es necesario encenderlo por ello, nos ubicamos en *router*, clic derecho *"Start"*

B. Realizado la acción anterior, sobre el *router* clic derecho *"Console"*

C. A continuación, aparecerá una ventana de configuración del *router*, tal como se muestra a continuación.

D. Seguidamente se procedió a realizar la configuración de las direcciones IPv6 en las interfaces de cada *router*. La tabla 12 muestra las direcciones IPv6 utilizadas dentro de la topología.

Tabla 12: Direcciones IPv6 utilizadas para Syslog – Escenario 3

Ruta	Dirección
Tacna -Moquegua	2001:9876:5432:400::/54
Moquegua - Arequipa	2001:9876:5432:c00::/54
Arequipa - Puno	2001:9876:5432:1400::/54
Arequipa -Lima1	2001:9876:5432:1c00::/54
Lima 2	2001:9876:5432:2800::/54
Lima 1 - Lima 3	2001:9876:5432:2c00::/54
Lima 3	2001:9876:5432:3000::/54
Lima 3 - La Libertad	2001:9876:5432:7C00::/54
La libertad - Lambayeque	2001:9876:5432:8400::/54
Lambayeque - Cajamarca	2001:9876:5432:8C00::/54
Lambayeque - Piura	2001:9876:5432:9400::/54

Fuente: Elaboración propia

E. Posterior a las configuraciones de IPv6, se configuro los *router* ID en cada configuración del protocolo OSPF. En la tabla 13, se muestran las direcciones utilizadas para cada *router* ID.

Tabla 13: Direcciones para *router* ID en GNS3 para escenario de SNMPv3

Nodo	Dirección
Tacna	1.1.1.1
Moquegua	2.2.2.2
Arequipa	3.3.3.3
Lima 1	4.4.4.4
Lima 2	5.5.5.5
Lima 3	15.15.15.15
La libertad	9.9.9.9
Lambayeque	8.8.8.8
Piura	6.6.6.6
Cajamarca	7.7.7.7

Fuente: Elaboración propia

F. Finalmente se realiza las siguientes configuraciones en cada *router.*

- **Habilitar IPv6 y el protocolo de enrutamiento OSPF**

1. Habilitamos IPv6
   ```
   ROUTER(config)#ipv6 unicast-routing
   ```
2. Se asigna un “id” al protocol OSPF
   ```
   ROUTER(config)#ipv6 router ospf 1
   ```
3. Se asigna la dirección al id del *router*
   ```
   ROUTER(config-rtr)#router-id 1.1.1.1
   ```
4. Se asigna el OSPF a la interface Gig 1/0
   ```
   ROUTER(config)#interface gigabitEthernet 1/0
   ROUTER(config-if)#ipv6 ospf 1 area 0
   ```
5. ```
   ROUTER(config-if)#end
   ```

- **Habilitar Syslog**

1. Configuración la comunidad “raap” con los permisos de Solo lectura
   ```
   Router(config)# logging host ipv6
   2001:9876:5432:3000::10
   ```
2. Especificamos el *nivel de detalle de la información que será registrada en el log*
   ```
   Router(config)# logging trap 7
   ```

4.5.2. Configuración del *Cloud*

Debido a que la topología se encuentra distribuido en dos equipos físicos, se configuro un *Cloud* en cada escenario con la finalidad de conectar ambas partes de la topología; el procedimiento utilizado es el antes especificado en el punto 4.3.2.
   ```

4.5.3. Configuración del Servidor

La herramienta PRTG tiene la capacidad de poder recopilar los *logs* y mostrar la información que se obtiene de cada *router*; Este protocolo puede emitir el reporte de sus *logs* desde un entorno configurado con SNMP en cualquier versión, sin hacer conflicto puesto a que este protocolo trabaja a través de otro puerto. Para el escenario de emulación se optó por agregar la funcionalidad de Syslog en un entorno antes configurados para aprovechar los *routers* agregados; Pero al existir pruebas donde solo se debía extraer información del consumo de recursos se procedió a quitar cualquier configuración SNMP, tanto de *routers* como del PRTG, para obtener netamente la información del consumo de recursos de Syslog a través de la herramienta, lo cual se muestra en la figura 43.

Figura 43. Dispositivos Agregados en el Servidor
Fuente: Elaboración Propia

A continuación, se detalla los pasos realizados para añadir un sensor que nos muestra la información de *logs*.

A. El acceso al panel principal nos muestra la configuración ya realizada en la nodriza y los *routers* añadidos para la configuración realizada a SNMP. Como se muestra en la figura 44. Dado que la herramienta tiene la capacidad de recopilar información de Syslog paralelamente.

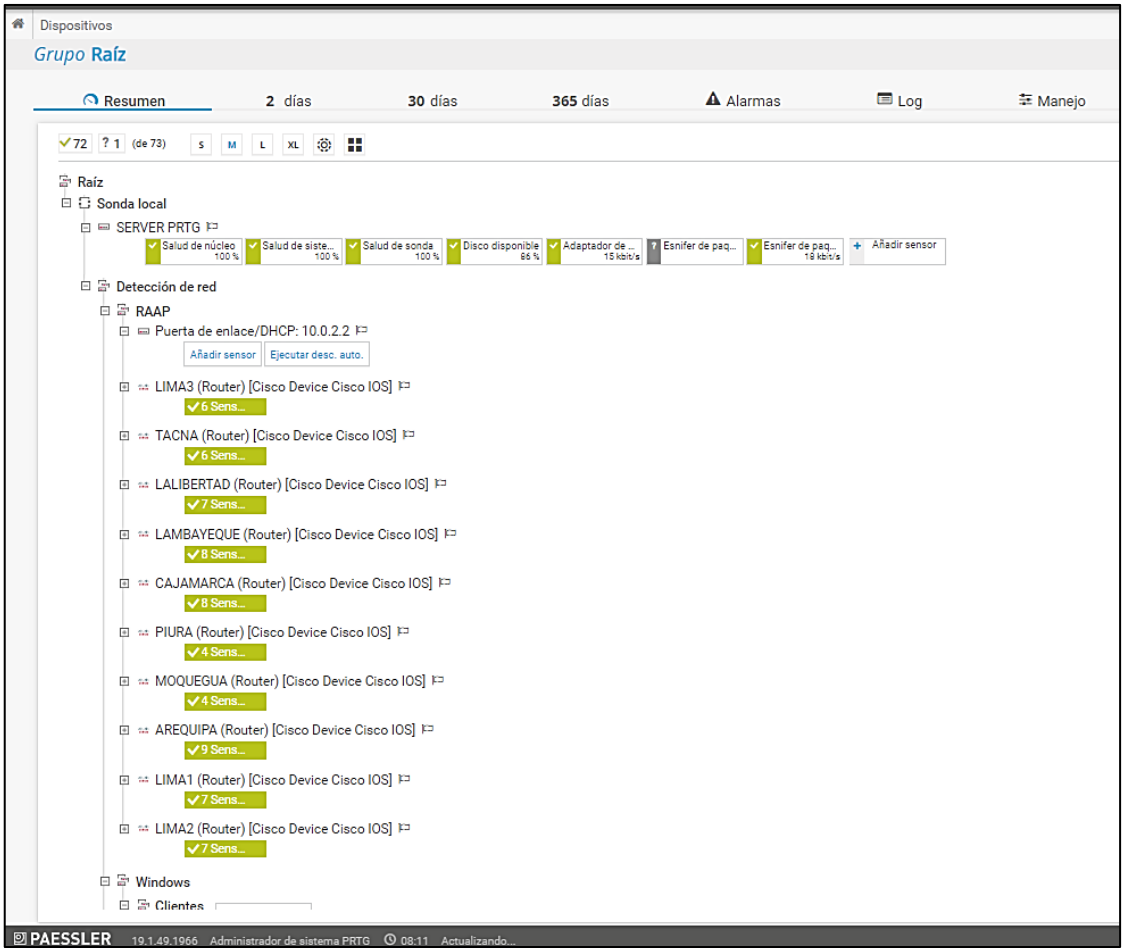


Figura 44. Panel Principal
Fuente: Elaboración Propia

B. Nos ubicamos en sensores, clic en “Añadir sensor”

C. Digitamos el nombre del sensor "*Receptor Syslog*", como se muestra en la figura 45.

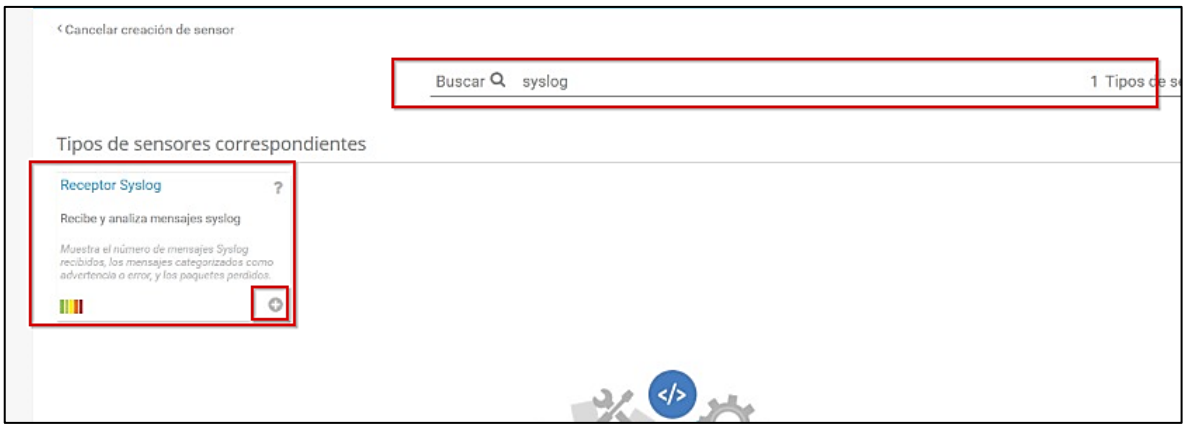


Figura 45. Añadiendo Sensor Syslog
Fuente: Elaboración Propia

D. Nos aparecerá una interfaz para poner los parámetros de Syslog Como se muestra en la figura 46.

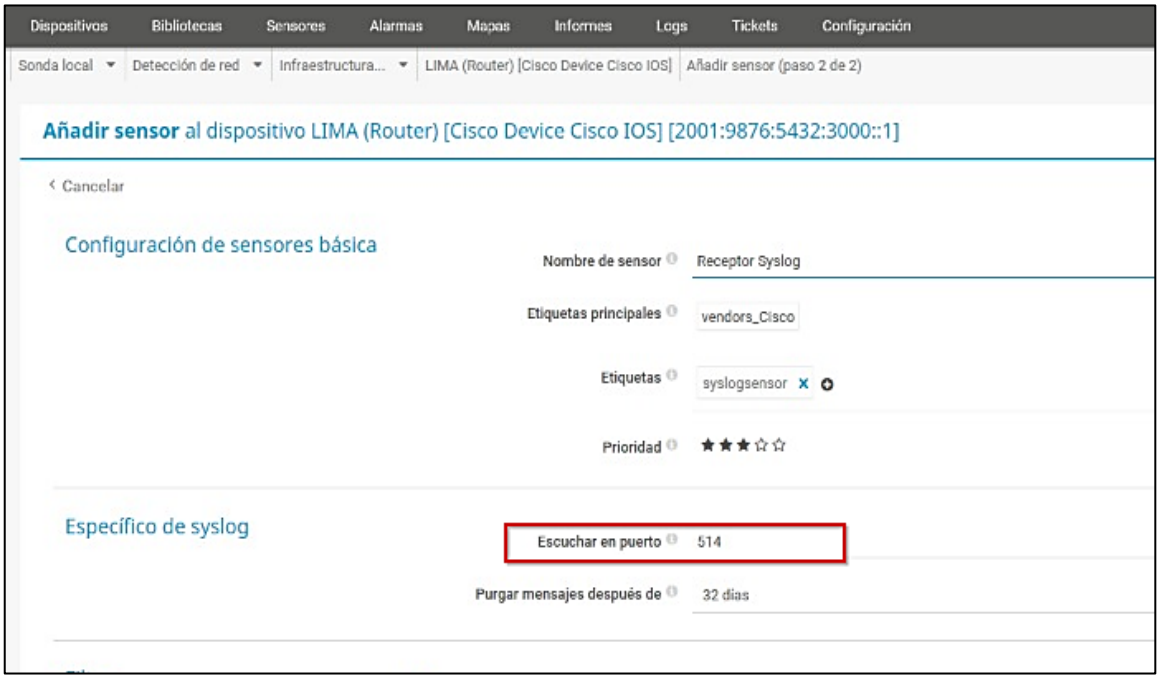


Figura 46. *Configuración de Parámetros Syslog*
Fuente: Elaboración Propia

V. MATERIALES Y MÉTODOS

5.1. Tipo de investigación

El tipo de investigación es aplicada y el nivel de investigación es cuantitativo, ya que según (Sampieri Hernández, 2014) los planteamientos cualitativos de refieren a una amplia gama de propósitos de investigación como la descripción de tendencias y patrones, la evaluación de variaciones además de identificar diferencias y medir resultados; por lo que este tipo de investigación se ajusta al proyecto de investigación, ya que los indicadores fueron medidos en términos de cantidad.

5.2. Diseño de investigación

El diseño de investigación es cuasi-experimental, que según, (Sampieri Hernández, 2014) este tipo de investigación identifica la manipulación de la variable independiente para ver el efecto con la variable dependiente y se aplica grupos constituidos. Se busca considerar el grado de características que puedan estar relacionadas con la variable de un objeto de investigación; además, consiste en recolectar conjunto de datos que no se asignan al azar. Por lo que este tipo de investigación se ajusta al proyecto de investigación ya que busca registrar las variaciones de las características para determinar mejor alternativa en base a Syslog y SNMP (X) en la gestión de la red (Y).

5.3. Operacionalización de Variables

Tabla 14: Matriz de operacionalización de variables

Variable	Tipo de Variable	Dimensión	Definición Conceptual	Definición Operacional	Indicador	Nivel de medición	Valor
Protocolos Syslog y SNMP (VI)	Cuantitativa	Complejidad de configuración	La complejidad de la configuración como una de las dimensiones de variable independiente trata de explicar en el contexto de las configuraciones técnicas y limitaciones de los protocolos Syslog y SNMP	La configuración de protocolos se refiere a plasmar a conveniencia los comandos de los protocolos con el fin recabar la mayor información de cada uno de ellos	• Nivel de complejidad de configuración de SNMP	Ordinal	•Muy Alto, Alto, Medio, Bajo, Muy Bajo
					• Nivel de complejidad de configuración de Syslog	Ordinal	•Muy Alto, Alto, Medio, Bajo, Muy Bajo
		Uso de recursos computacionales	Un recurso computacional representa cualquier elemento físico o virtual en un dispositivo o sistema, además incluyen medios de almacenamiento, procesamiento y producción (Jhaky, 2018) El consumo de recursos como una de las dimensiones de la variable independiente trata de explicar la cantidad de utilización de los recursos, como el nivel de utilización CPU, el consumo de ancho de banda, que los protocolos Syslog y SNMP consume para realizar sus funciones	Se refiere al consumo de recursos computacionales producidos por cada protocolo, para lograr saber quién genera mayor consumo.	• Nivel de uso de CPU de Syslog	Intervalo	•(0 % - 100 %)
					• Nivel de uso de memoria en Syslog	Intervalo	•(0 % – 100 %)
					• Nivel de uso de ancho de banda para Syslog	Intervalo	•(0 %-100 %)
					• Nivel de uso de CPU de SNMP	Intervalo	•(0 % - 100 %)
					• Nivel de uso de memoria en SNMP	Intervalo	•(0 % – 100%)
					• Nivel de uso de ancho de banda para SNMP	Intervalo	•(0 % - 100%)
		Seguridad de protocolos	Los mecanismos de seguridad deberían estar disponibles para garantizar privacidad e integridad de los mensajes Por seguridad de protocolos como una de las dimensiones de variable independiente, se refiere a evaluar falencias o fortalezas de seguridad que refieren los protocolos Syslog y SNMP, contemplando para ello el nivel de integridad y confidencialidad de cada protocolo.	Se refiere al grado de seguridad que se tiene al hacer uso de cada protocolo, para este proyecto de investigación se tomara en cuenta la integración y a confidencialidad	• Nivel de integridad de Syslog	Ordinal	•Si •No
					• Nivel de confidencialidad de Syslog	Ordinal	• Muy Alto, Alto, Medio, Bajo, Muy Bajo
					• Nivel de integridad de SNMP	Ordinal l	• Si • No
					•Nivel de confidencialidad de SNMP	Ordinal	• Muy Alto, Alto, Medio,

Variable	Tipo de Variable	Dimensión	Definición Conceptual	Definición Operacional	Indicador	Nivel de medición	Valor
							Bajo, Muy Bajo
		Servicios disponibles (ofrecidos)	Por servicios disponibles se refiere a evaluar a detalle el nivel de servicios que se admiten en cada uno de los protocolos Syslog y SNMP, considerando te proveen,	Los servicios disponibles como una de las dimensiones de la variable independiente, trata, de explicar el grado de detalle que emite cada servicio para recopilar los mensajes de Syslog y SNMP.	• Cantidad de Servicios ofrecidos por Syslog	Nominal	>0
					• Cantidad de servicios ofrecidos por SNMP	Nominal	>0
Gestión de red (VD)	Cuantitativa	Eficacia	La eficacia de la gestión de red como una de las dimensiones de la variable dependiente, trata de constatar el cumplimiento de los objetivos de la gestión de red, a través del reporte de los eventos suscitados al permitir la conexión, comunicación y transferencia de datos.	La eficacia como una de las variables dependientes trata de explicar a través de la información de los eventos reportados como contribuye al control dispositivos de la red, asegurando la operatividad de estos.	• Información de eventos reportados	Nominal	>0
		Eficiencia	Las medidas orientadas a la eficiencia de la gestión de red son las medidas de tiempo para detectar puntos probables de problemas de prestaciones, además se considera como la capacidad teórica de un recurso que se está utilizando y es empleado para ubicar posibles caídas de flujo de la operatividad. (Quispe Bustincio, 2018)	La eficiencia como una de las dimensiones de la variable dependiente trata de determinar cuánto tiempo invierten en la detección de eventos.	• Tiempo invertido en la gestión de red	Ordinal	•Muy Rápido, Rápido, ni rápido ni lento, lento, Muy lento
VI: Cuantitativa: La variable independiente “Protocolos Syslog y SNMP” es una variable **Cuantitativa** ya que los indicadores se miden en términos de cantidad.							
VD: Cuantitativa: La variable dependiente “Monitorización y Supervisión de red” es una variable **Cuantitativa** ya que los indicadores se miden en términos de cantidad.							

5.4. Validación de Hipótesis

La validación de Hipótesis se realizó a través de pruebas ejecutadas en el entorno de emulación en el laboratorio de Redes y Seguridad, utilizando como instrumento de recolección de resultados la herramienta PRTG y como un medio de contrastar la información también se utilizó la herramienta Wireshark.

A continuación, se detallan el proceso de cada prueba realizada.

5.4.1. Información de Eventos Reportados

La realización de esta prueba consistió en obtener la mayor información que recaba cada protocolo, por ende, era indispensable saber en caso de SNMP los *traps* y *logs* en caso de syslog, que se obtenían por eventos generados en los *routers* para saber si eran reportados o no por los protocolos. Para ello, se usó el Servidor PRTG configurado para cada protocolo, con la finalidad de obtener estos datos a través de los sensores que este posee. Los sensores utilizados para esta prueba se especifican en la tabla 15:

Tabla 15: Sensores Utilizados en cada PRTG Server para Prueba de Información de Eventos

Nombre	Sensor Utilizado	Descripción
SNMPv2c	"*Receptor SNMP Traps*"	Recolecta *traps* emitidos por los dispositivos.
SNMP v3	"*Receptor SNMP Traps*"	Recolecta *traps* emitidos por los dispositivos.
Syslog	"*Receptor* Syslog"	Muestra capturas de *logs* emitidos por el dispositivo.

Fuente: Elaboración propia

A causa de ser un entorno de emulación, los eventos fueron generados para poder recopilar la información; se contemplaron los eventos detallados a continuación por ser básicos para un entorno de producción en Redes Avanzadas.

- **Acceso al *router* vía telnet**

En esta prueba se accedió vía telnet desde la PC LIMA1, ubicado en la red del *router* LIMA1, a todos los *routers.* Pero para exponer el funcionamiento de las pruebas se utilizó el *router* CAJAMARCA como punto de destino. En las figuras 47 y 48 se muestra la ubicación de la PC LIMA1 y el *router* CAJAMARCA.

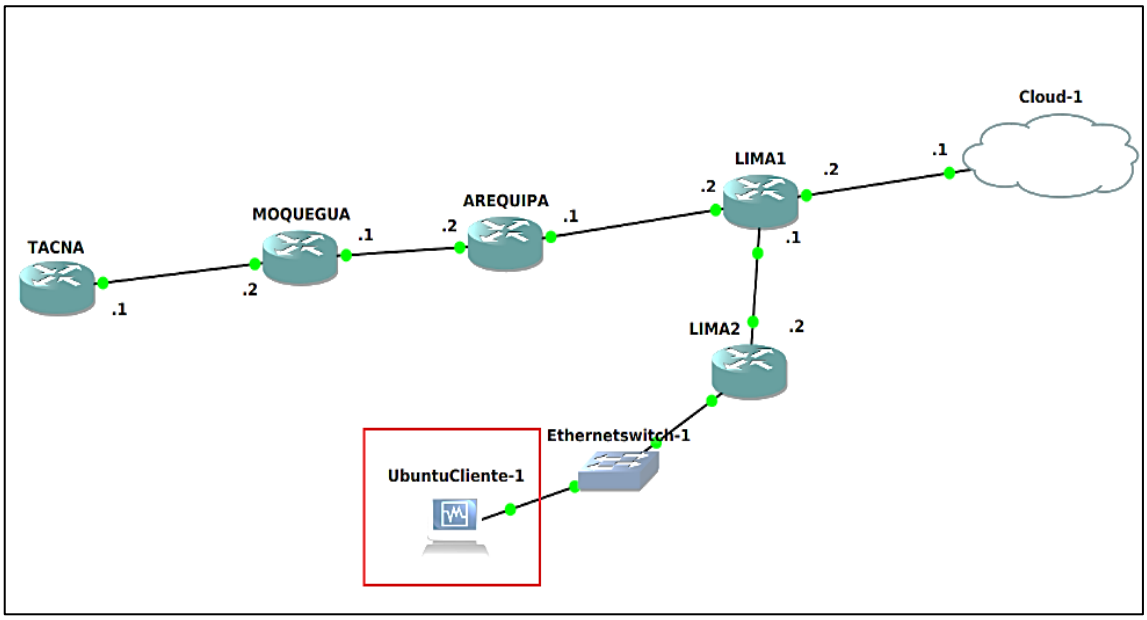


Figura 47. Ubicación de PC LIMA2
Fuente: Elaboración Propia

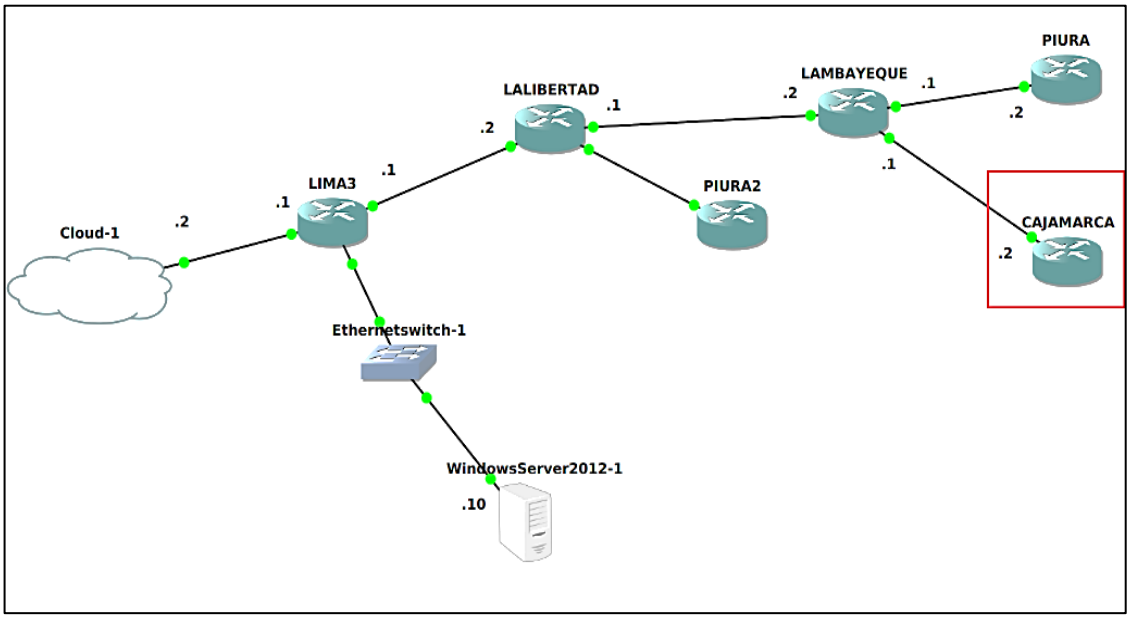


Figura 48. Ubicación del *router* CAJAMARCA
Fuente: Elaboración Propia

Comando utilizado en la PC LIMA1 con SO Ubuntu 18.04 con IP 2001:9876:5432:2800::10

```
root@LIMA1-desktop: telnet 2001:9876:5432:8C00::2
```

A. Reporte de Pruebas Información de eventos Syslog

De acuerdo con el reporte de capturas de *logs* que emite PRTG, Syslog no captura mensajes al iniciar una sesión al *router* vía telnet.

B. Reporte de Pruebas Información de eventos SNMPv2c

Según el reporte de capturas de *traps* que emite PRTG, SNMPv2c captura las *traps* generadas por el *router*. En la figura 49 se muestra la captura las *traps* emitido por el evento generado.

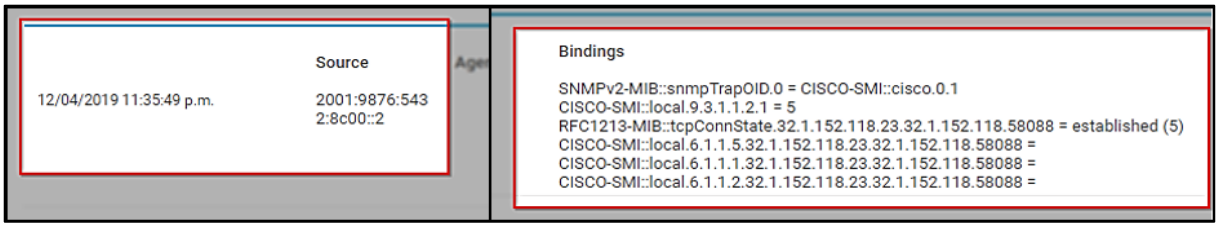


Figura 49. Reporte de SNMPv2c realizar un acceso al *router* vía telnet
Fuente: Elaboración Propia

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de SNMPv3 se pudo visualizar que los *traps* son encriptados de manera que no existe una lectura de *traps* por la herramienta. Para contrastar que las *traps* están viajando encriptadas se utilizó la herramienta Wireshark para poder visualizar los paquetes como se muestra en la figura 50.

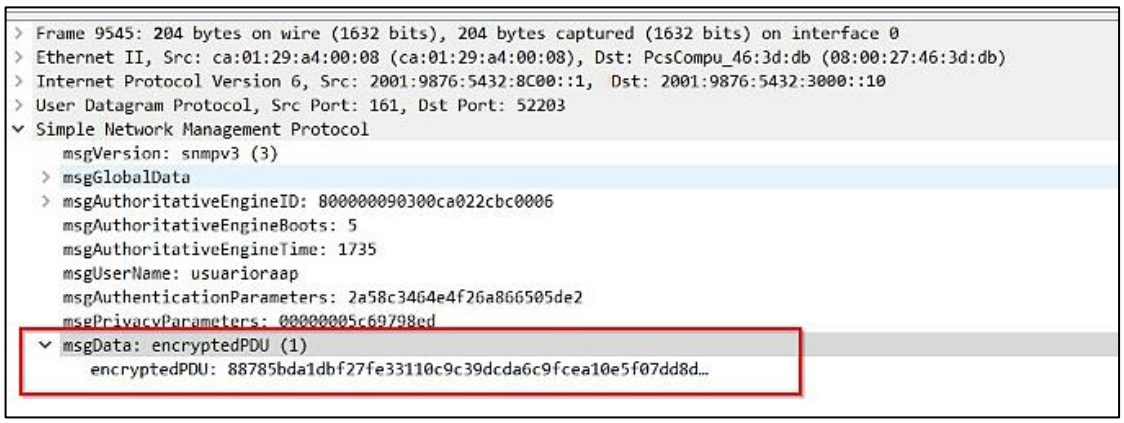


Figura 50. Captura de mensaje SNMPv3
Fuente: Elaboración Propia

- **Ingreso al modo de configuración global vía telnet**

Este evento se generó posterior al evento anterior, utilizando la misma PC LIMA1 como punto de acceso hacia el *router* PIURA como punto accedido.

A. Reporte de Pruebas Información de eventos Syslog

Para este evento, Syslog emitió un mensaje de notificación, donde indicaba la configuración por consola vía *tty*, como se puede observar en la figura 51.

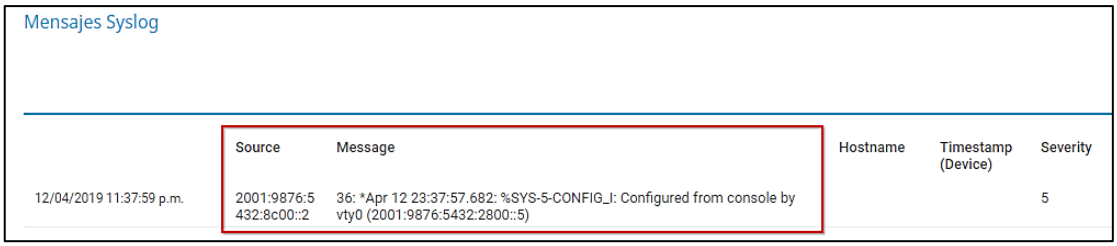


Figura 51. Reporte de Syslog al realizar un acceso configuración global vía telnet
Fuente: Elaboración Propia

B. Reporte de Pruebas Información de eventos SNMPv2c

El reporte de capturas de *traps* arrojo la información visualizada en la figura 52. Este *traps* contiene un OID donde notifica un evento de administración de configuración.

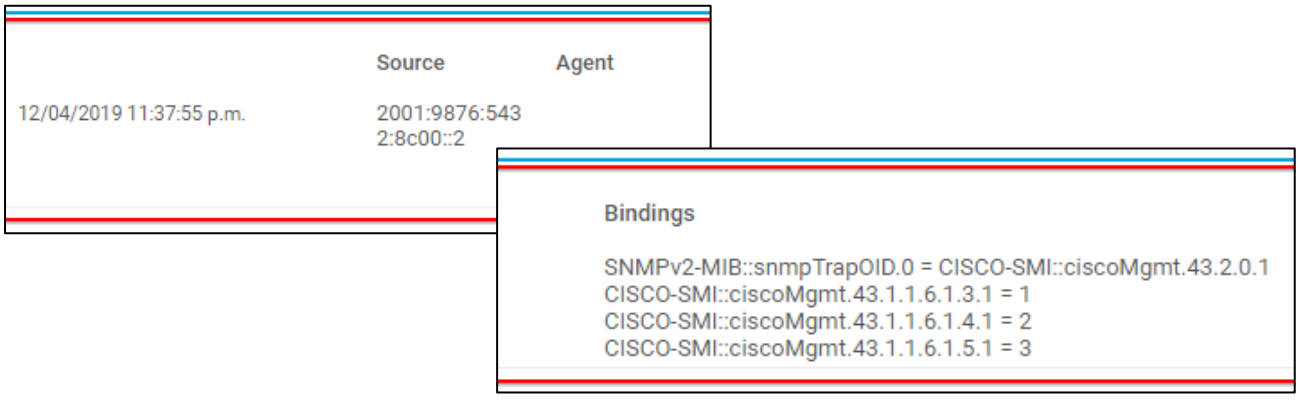


Figura 52. Reporte de SNMPv2c al realizar un acceso configuración global vía telnet
Fuente: Elaboración Propia

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de SNMPv3, no es accesible de visualizar las *traps* recepcionadas puesto a que son encriptados por la seguridad que poseen.

- **Ingreso al modo de configuración global vía SSH**

Este evento se generó posterior al evento anterior, utilizando la misma PC LIMA1 como punto de acceso hacia el *router* TACNA como punto accedido.

A. Reporte de Pruebas Información de eventos Syslog

Para este evento, Syslog emitió un mensaje de notificación, donde indicaba la configuración por consola vía *tty*, además de identificar con que usuario SSH (raap) con quien se realizó el ingreso a modo de configuración global, en la figura 53 se puede observar este registro.

Figura 53. Reporte de Syslog al realizar un acceso configuración global vía telnet
Fuente: Elaboración Propia

B. Reporte de Pruebas Información de eventos SNMPv2c

El reporte de capturas de *traps* arrojó la información visualizada en la figura 54. Este *traps* contiene un OID donde notifica un evento de administración de configuración.

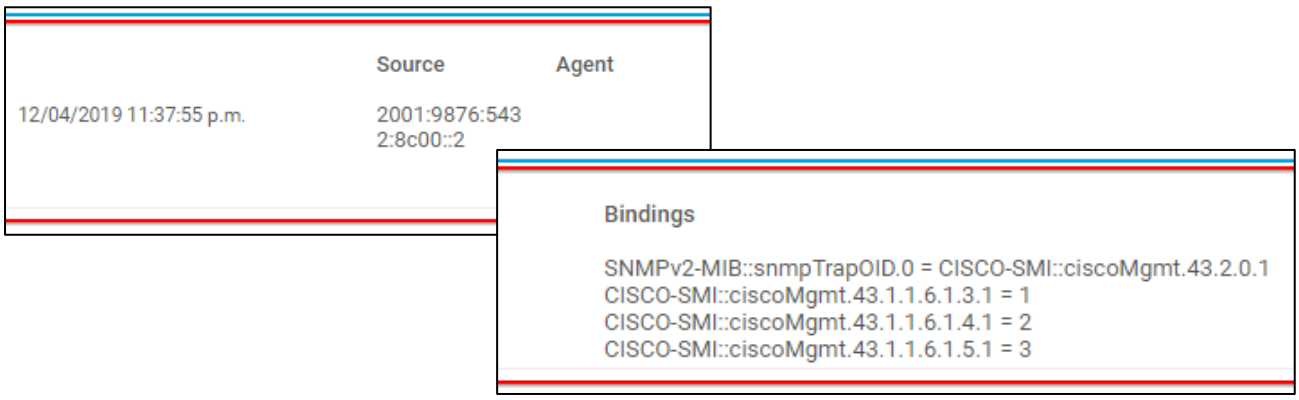


Figura 54. Reporte de SNMPv2c al realizar un acceso configuración global vía telnet
Fuente: Elaboración Propia

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de sNMPv3, no es accesible de visualizar los *traps* recepcionados puesto a que son encriptados por la seguridad que poseen.

- **Acceso al *router* vía consola**

En esta prueba se realizó accediendo desde el *router* CAJAMARCA, así como en los demás *routers,* pero para la exposición de funcionalidades se usa el *router* CAJAMARCA cuya ubicación muestra la figura 55.

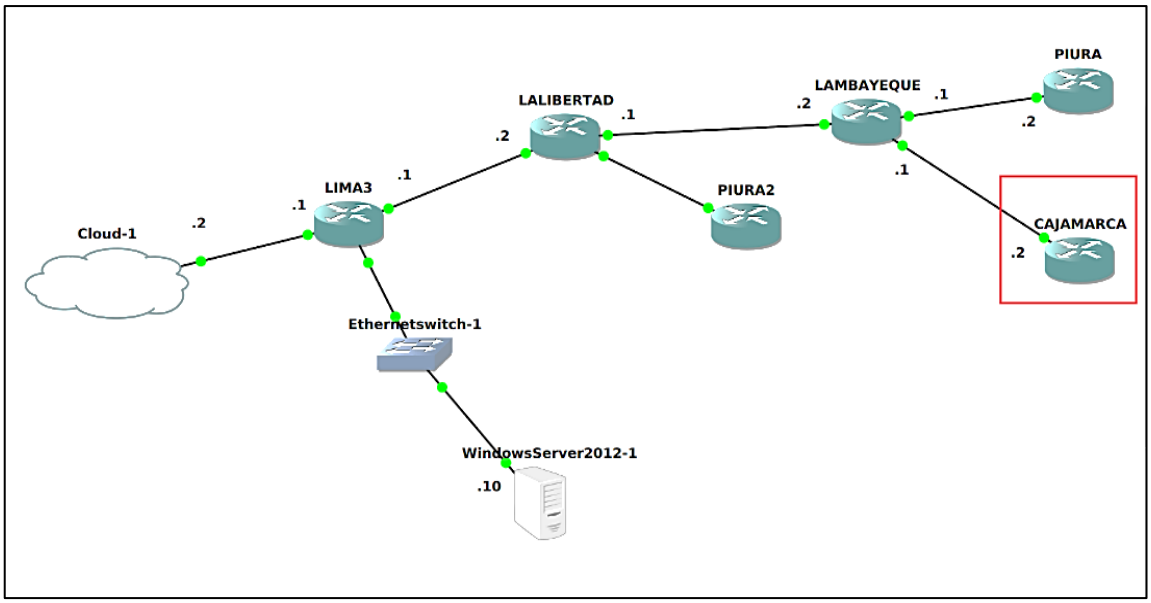


Figura 55. Ubicación del *Router* Cajamarca
Fuente: Elaboración Propia

A. Reporte de Pruebas Información de eventos Syslog

En la figura 56 muestra la vista de la captura del mensaje generado a través de Syslog, este mensaje es clasificado un mensaje de notificación.

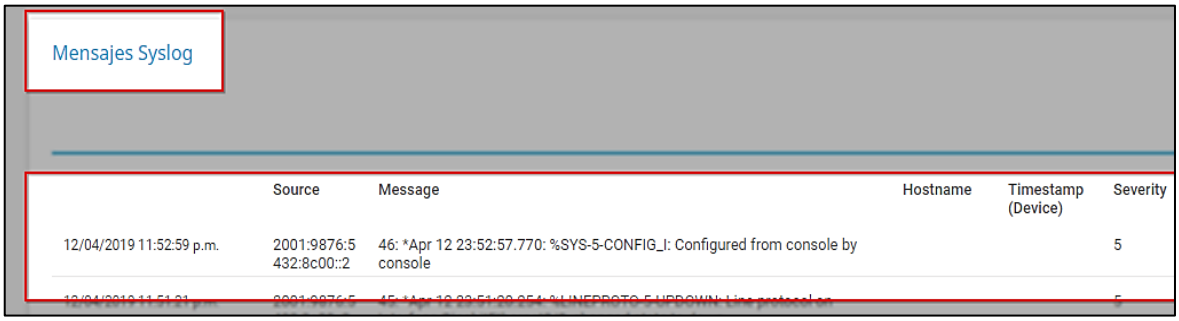


Figura 56. Reporte de Syslog al realizar un acceso configuración global
Fuente: Elaboración Propia

B. Reporte de Pruebas Información de eventos SNMPv2c

El reporte de capturas de *traps* produjo la información visualizada en la figura 57. Este *traps* contiene un OID donde notifica un evento de administración de configuración.

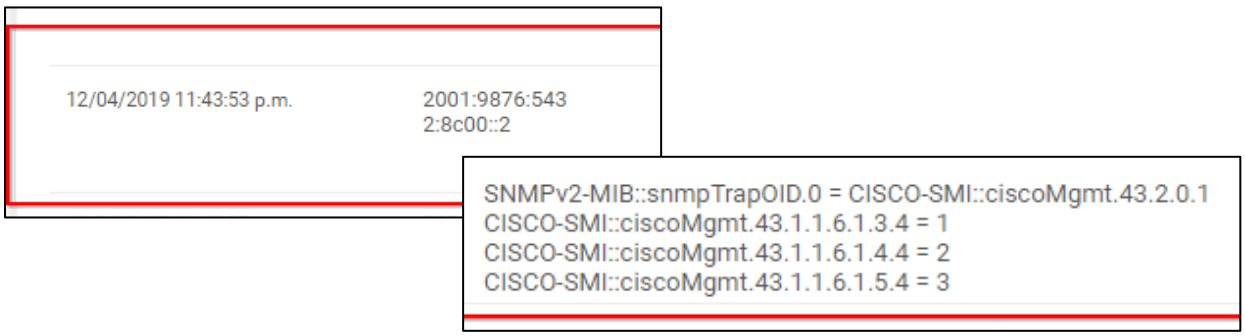


Figura 57. Reporte de SNMPv2c al realizar un acceso configuración global
Fuente: Elaboración Propia

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de sNMPv3, no es accesible de visualizar los *traps* recepcionados puesto a que son encriptados por la seguridad que poseen.

- **Encendido de una interfaz**

Esta prueba consistía en encender una interfaz del *router*, al emitir el comando *"no shutsown"* se genera también mensajes reportados por consola del encendido de la interfaz.

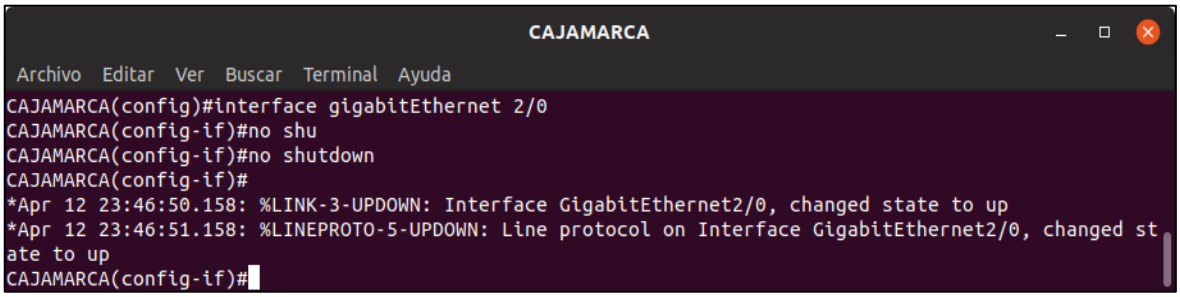
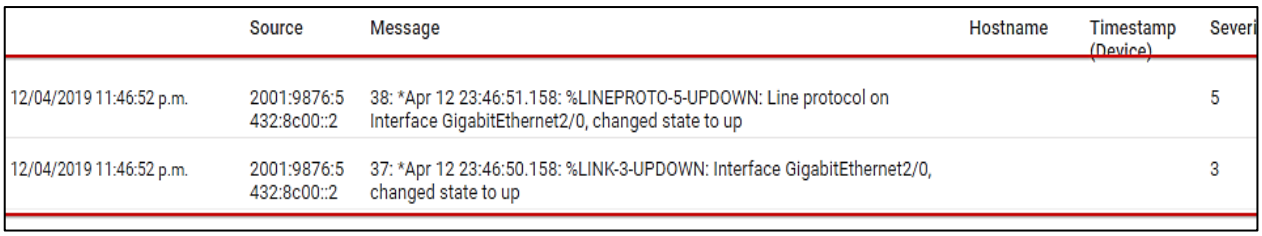


Figura 58. Encendido de una interfaz
Fuente: Elaboración Propia

A. Reporte de Pruebas Información de eventos Syslog

En este evento Syslog reporta dos *logs*, con diferentes niveles de severidad, para Syslog pasar de un estado inactivo a activo es considerado como nivel de "error" y nivel de "notificación". En la figura 59 se muestra el contenido de los *logs*.



	Source	Message	Hostname	Timestamp (Device)	Severi
12/04/2019 11:46:52 p.m.	2001:9876:5 432:8c00::2	38: *Apr 12 23:46:51.158: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up			5
12/04/2019 11:46:52 p.m.	2001:9876:5 432:8c00::2	37: *Apr 12 23:46:50.158: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up			3

Figura 59. Reporte de Syslog al realizar el encendido de una interfaz
Fuente: Elaboración Propia

B. Reporte de Pruebas Información de eventos SNMPv2c

Según el reporte de capturas de *traps* que emite PRTG, el evento generado emite 3 *traps*, pero solo el primero corresponde al encendido de la interfaz el cual se encuentra enmarcado de color rojo en la figura 60.

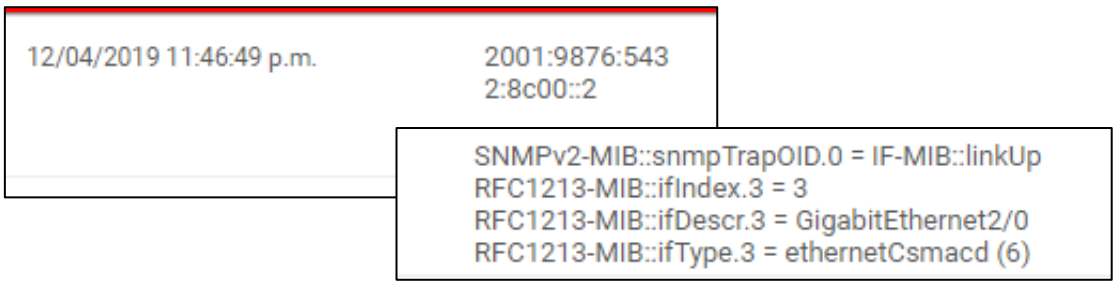


Figura 60. Reporte de SNMPv2c al realizar el encendido de una interfaz
Fuente: Elaboración Propia

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de SNMPv3, no es accesible de visualizar los *traps* recepcionados puesto a que son encriptados por la seguridad que poseen.

- **Caída de una interfaz (Apagado)**

En esta prueba se generó el evento de la caída de una interfaz del *router*, para este caso se forzó el apagado de una interfaz vía comando como se muestra en la figura 61.

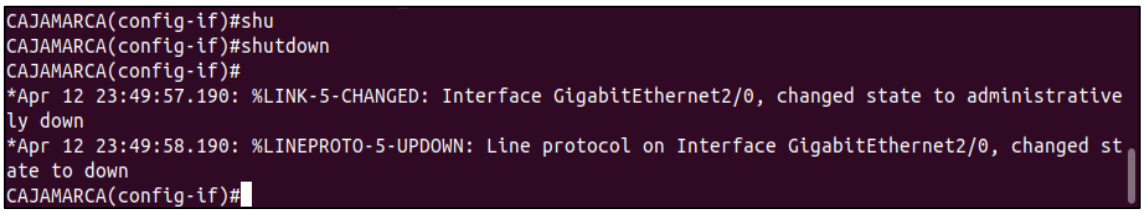


Figura 61. Apagado de una interfaz
Fuente: Elaboración Propia

A. Reporte de Pruebas Información de eventos Syslog

Para Syslog pasar de un estado activo a inactivo es considerado como nivel “notificación”. En la figura 62 se muestra el contenido de los *logs* en la herramienta PRTG.

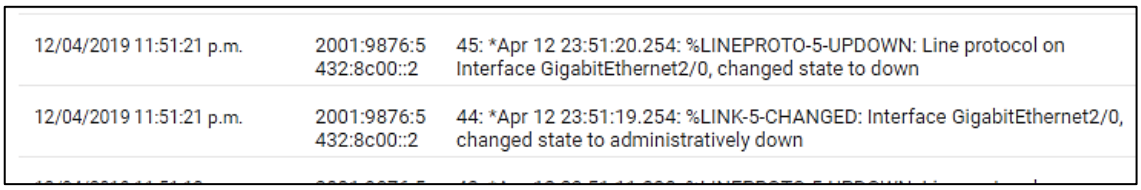


Figura 62. Reporte de Syslog al apagarse una interfaz
Fuente: Elaboración Propia

B. Reporte de Pruebas Información de eventos SNMPv2c

Según el reporte de capturas de *traps* que emite PRTG, el evento generado emite dos *traps* como se muestra en la figura 63; Un *trap* es generado

por que uno de los enlaces de comunicación está a ingresando al estado inactivo, y el siguiente *traps* se origina a raíz de la alarma emitida por la entidad física.

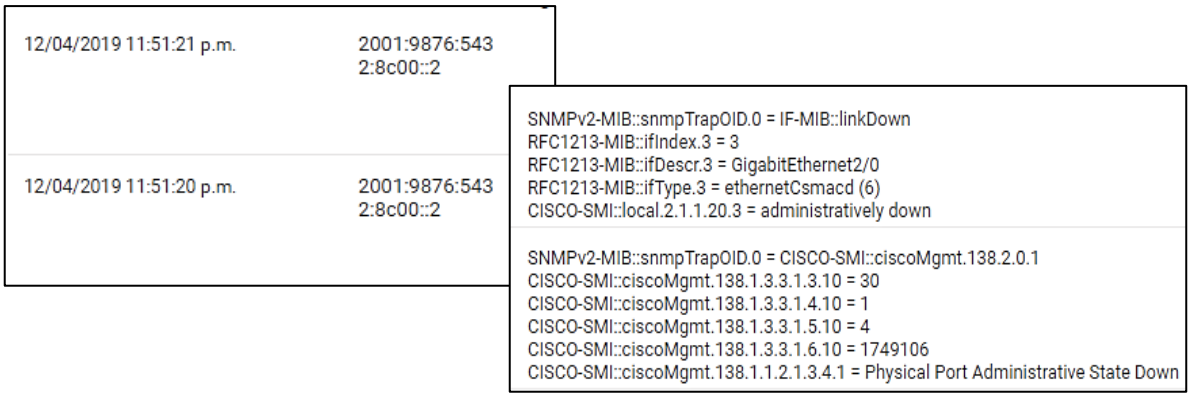


Figura 63. Reporte de SNMP v2c al apagarse una interfaz.
Fuente: Elaboración Propia

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de SNMPv3, no es accesible de visualizar los *traps* recepcionados puesto a que son encriptados por la seguridad que poseen.

- **Cambios de configuración**

En este evento se consideró los cambios de configuración, para lo cual se realizó el guardado de una configuración del *router* mediante los comandos descritos en la figura 64.

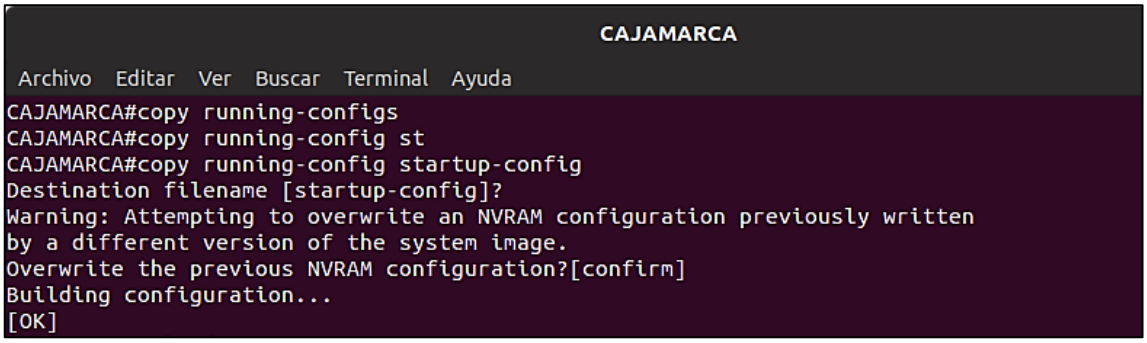


Figura 64. Cambios de configuración.
Fuente: Elaboración Propia.

A. Reporte de Pruebas Información de eventos Syslog

Según el reporte de capturas de *logs* que emite PRTG, el evento generado emite un log como se muestra en la figura 65; donde el nivel que es considerado es el de “notificación”.

	Source	Message
12/04/2019 11:52:59 p.m.	2001:9876:5432:8c00::2	46: *Apr 12 23:52:57.770: %SYS-5-CONFIG_I: Configured from console by console

Figura 65. Reporte de Syslog, al realizar cambios en la configuración.
Fuente: Elaboración Propia

B. Reporte de Pruebas Información de eventos SNMPv2c

El evento generado reporta en la herramienta PRTG, un *trap* emitido por el *router,* como se muestra en la figura 66. Este *trap* describe Notificación de un evento de administración de configuración

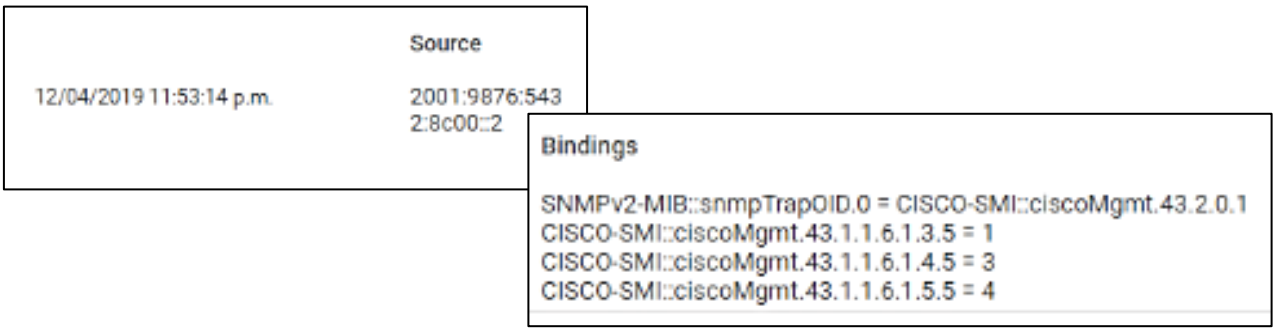


Figura 66. Reporte de SNMPv2c, al realizar cambios en la configuración.
Fuente: Elaboración Propia

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de sNMPv3, no es accesible de visualizar los *traps* recepcionados puesto a que son encriptados por la seguridad que poseen.

- **Reinicio del *router***

En este evento se procedió a forzar el reinicio de un *router* como se muestra en la figura 67.

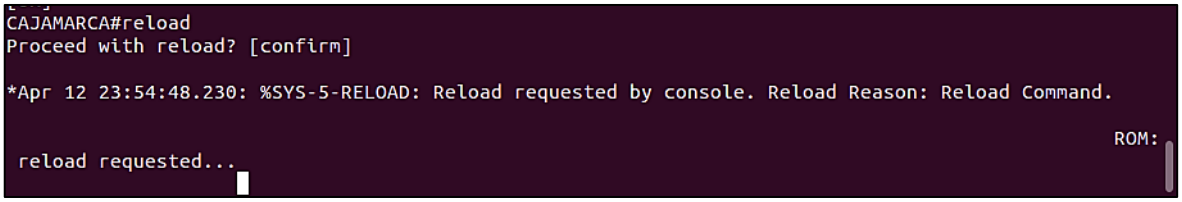


Figura 67. Reinicio del *Router*
Fuente: Elaboración Propia

A. Reporte de Pruebas Información de eventos Syslog

Según el reporte de capturas de logs que emite PRTG, el evento generado emite *log* como muestra en la figura 68; el cual se considera un "Mensaje de Notificacion" que indica el reinicio de *router.*

12/04/2019 11:54:50 p.m.	2001:9876:5 432:8c00::2	47: *Apr 12 23:54:48.230: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

Figura 68. Reporte de Syslog, al realizar el reinicio del *router*.
Fuente: Elaboración Propia.

B. Reporte de Pruebas Información de eventos SNMPv2c

Según el reporte de capturas de *traps* que emite PRTG que se muestra en la figura 69, el evento generado emite un *traps,* describe una captura de reinicio, es decir la entidad de envió se está reinicializando.

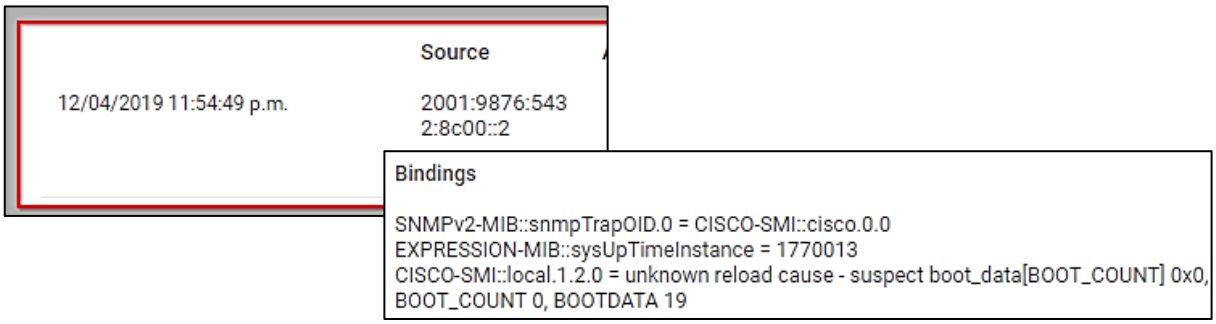


Figura 69. Reporte de SNMPv2c, al realizar el reinicio del *router*.
Fuente: Elaboración Propia.

C. Reporte de Pruebas Información de eventos SNMPv3

Debido a la configuración de sNMPv3, no es accesible de visualizar los *traps* recepcionados puesto a que son encriptados por la seguridad que poseen.

- **Guardar archivo de configuración en servidor TFTP**

Para esta prueba se tuvo implementado el TFTP en el Windows Server 2012, y este sirvió para guardar el archivo de configuración, el proceso realizado se visualiza en la figura 70.

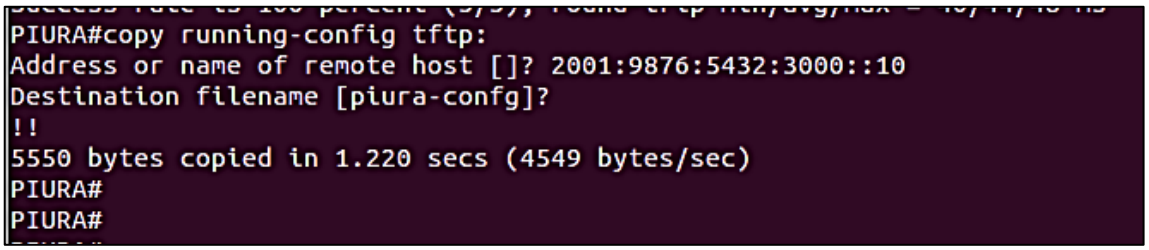


Figura 70. Comando para guardar el archivo de configuración en servidor.
Fuente: Elaboración Propia

A. Reporte de Pruebas Información de eventos Syslog

El procedimiento de guardar el archivo de configuración en el TFTP, no reporto ningún log en el reporte de Syslog en PRTG.

B. Reporte de Pruebas Información de eventos SNMPv2c

El procedimiento de guardar el archivo de configuración en el TFTP, según el reporte de capturas de *traps* que emite PRTG emitió una *traps* que describe Notificación de un evento de administración de configuración como se muestra en la figura 71.

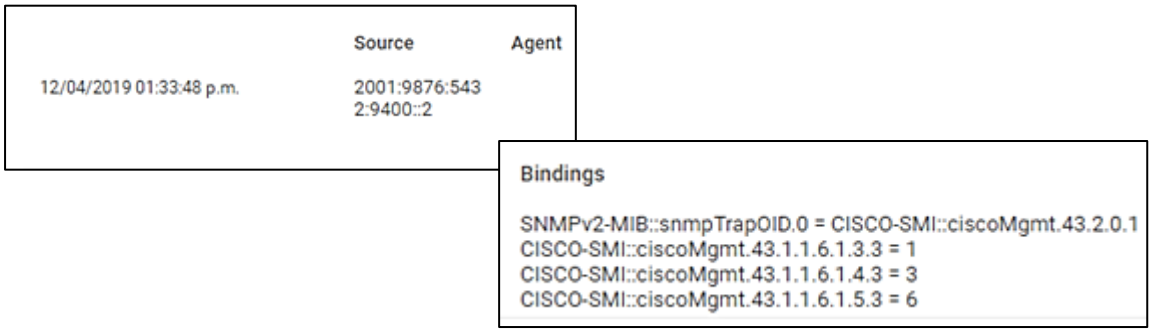


Figura 71. Reporte de SNMPv2c, al guardar un archivo de configuración en el TFTP.
Fuente: Elaboración Propia.

- **Resumen de la información de eventos reportados por protocolo**

De los eventos generados en cada escenario se tiene distintos reportes para los protocolos, donde, dos eventos no fueron reportados por Syslog, además por el nivel de seguridad configurado en SNMPv3, no fue posible traducir los OIDs emitidos por evento realizado; El extracto las pruebas realizadas se describen en la tabla 16.

Tabla 16: Resumen de la información de eventos reportados por protocolos

Evento	Nombre		Reporta Evento	Descripción
Acceso al *Router* Vía Telnet	Syslog		No	
	SNMP	Versión 2c	Si	Esta *traps* describe una captura tty, que significa que una conexión TCP, previamente establecida con la entidad
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID
Acceso al Modo configuración global vía telnet	Syslog		Si	Mensaje de Notificación Describe el ingreso a consola via tty
	SNMP	Versión 2c	Si	Objeto: *ciscoConfigManEvent* Esta *traps* describe Notificación de un evento de administración de configuración
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID
Acceso al Modo	Syslog		Si	Mensaje de Notificación Describe el ingreso a consola

configuración global vía consola	SNMP	Versión 2c	Si	Objeto: *ciscoConfigManEvent* Esta *traps* describe Notificación de un evento de administración de configuración
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID
Encendido de una interfaz	Syslog		Si	Mensaje de Error Describe el encendido de la interfaz GigabitEthernet2/0
				Mensaje de Notificación Describe el encendido de la interfaz por comando.
	SNMP	Versión 2c	Si	Objeto: *linkUp* Esta *traps* describe que uno de sus enlaces de comunicación deje el estado inactivo y pasó a otro estado.
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID
Caída de interfaz (apagado)	Syslog		Si	Mensaje de Notificación Describe el cambio de estado administrativo a apagado de la interfaz GigabitEthernet2/0
				Mensaje de Notificación Describe el apagado por consola
	SNMP	Versión 2c	Si	Objeto: *linkDown* Esta *traps* describe que uno de sus enlaces de comunicación está ingresando al estado inactivo desde otro estado.
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID
Cambios de Configuración	Syslog		Si	Mensaje de Notificación Describe la configuración de la consola
	SNMP	Versión 2c	Si	Objeto: *ciscoConfigManEvent* Describe la Notificación de un evento de administración de configuración
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID
Reinicio del *Router*	Syslog		Si	Mensaje de Notificación Describe el reinicio remitido por consola
	SNMP	Versión 2c	Si	Objeto: *reload* Esta *traps* describe una captura de reinicio, es decir la entidad de envió se está reinicializando
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID

Guardar archivo de configuración en servidor TFTP	Syslog		No	
	SNMP	Versión 2c	Si	Objeto: *ciscoConfigManEvent* Notificación de un evento de administración de configuración como se registró en *ccmHistoryEventTable*
		Versión 3	Si	Mensaje encriptado, no se puede traducir OID

Fuente: Elaboración propia

- **Registros adicionales de *traps* recopilados al generar de eventos**

En el proceso de la generación de eventos para ser reportados por los protocolos, existieron reportes adicionales dentro de la herramienta que se explicarán en la tabla 17.

Tabla 17. Detalle *traps* adicionales recopilados al generar eventos

Descripción del suceso que lo genero	**OID**	**Descripción del *traps*.**
Este *traps* fue generado al realizar el encendido y apagado de la interfaz, a raíz de que el dispositivo genera una alarma por consola en consecuencia a este evento	1.3.6.1.4.1.9.9.138.2.0.1	Objeto: *ceAlarmCleared* El agente genera esta *traps* cuando una entidad física emite una alarma
El evento generado fue un encendido de una interfaz, el *router* donde se suscitó el evento tenía configurado a medida de prueba el Syslog. Al emitirse este evento Syslog reporto un log con nivel 3, el cual género que SNMP notificará con un *trap* este reporte.	1.3.6.1.4.1.9.9.41.2.0.1	Objeto: *clogMessageGenerated* SNMP reporta que se ha generado un mensaje de Syslog

Fuente: Elaboración propia

- **Registros adicionales de *logs* recopilados al generar de eventos**

En el proceso de la generación de eventos para ser reportados por los protocolos, existieron reportes adicionales que se registraron en la herramienta que se explicaran a continuación.

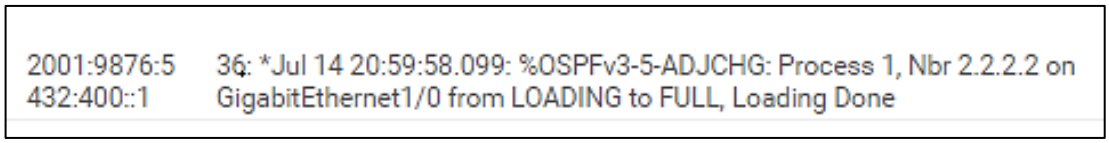


Figura 72. Reporte de *logs* adicional – Adyacencia de vecino OSPFv3
Fuente: Elaboración Propia

La figura 72, reporta un mensaje de OSPFv3 al producirse una adyacencia entre *routers*.

Cuando ocurre un reinicio del *router* o encendido de este, los servicios también son inicializados, tal es el caso descrito en la figura 73, que indica la inicialización de Syslog por el puerto 514.

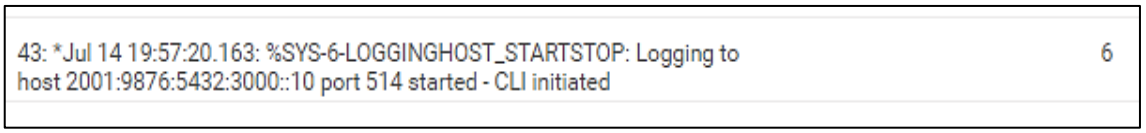


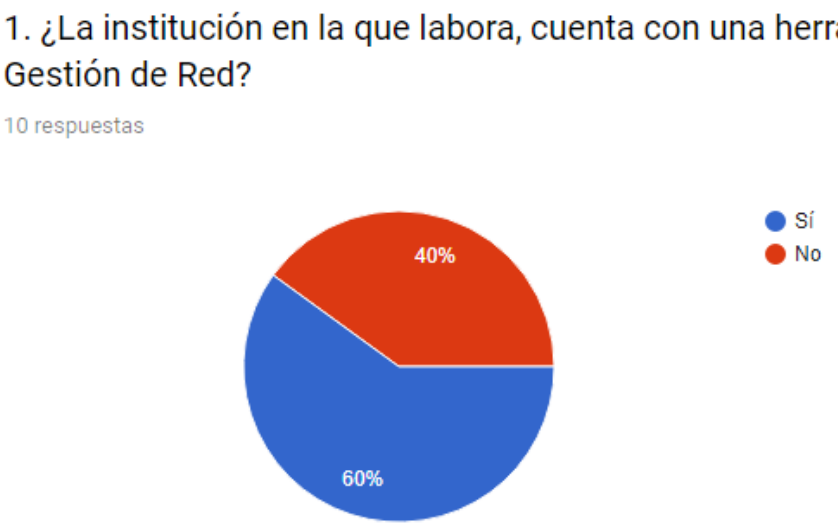
Figura 73. Reporte de *logs* adicional – inicialización de Syslog
Fuente: Elaboración Propia

Además, en la herramienta también se pudo visualizar los logs emitido tras configurar la habilitación de SSH, en la figura 74 se adjunta el suceso de este evento.

Figura 74. Reporte de *logs* adicional – habilitación de SSH
Fuente: Elaboración Propia

5.4.2. Tiempo invertido en la gestión de red

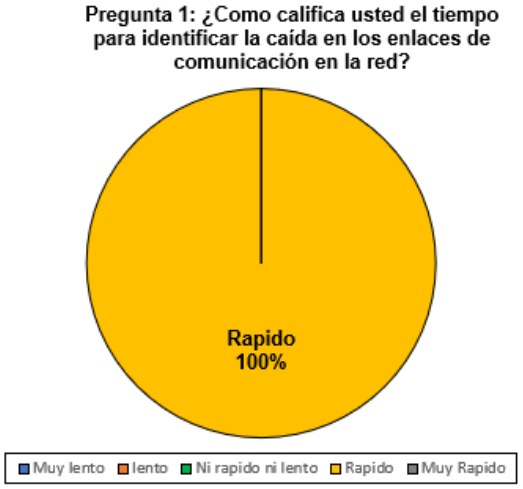
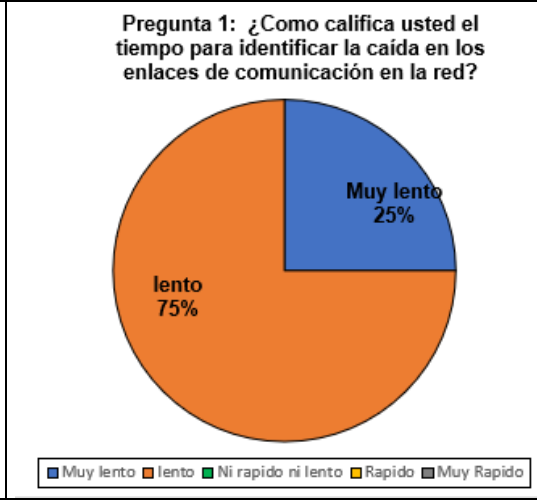
Se realizó una encuesta a expertos que pertenecen a instituciones nacionales como Telefónica, OSINFOR, PEAH, y por la ciudad de México existieron respuestas de personal informático del SICAP, TeCT Mx, CCTV seguridad, INFOTEC con el fin de determinar cuento tiempo invierten en los procedimientos u obtención de datos que los protocolos planteados a través de una herramienta de red ayudarían hacerlo más rápido.



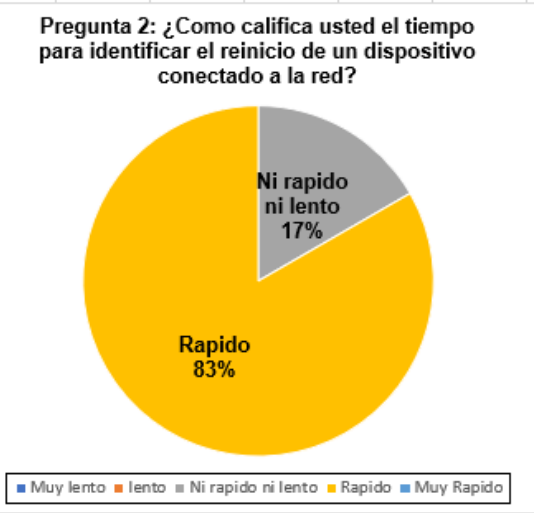
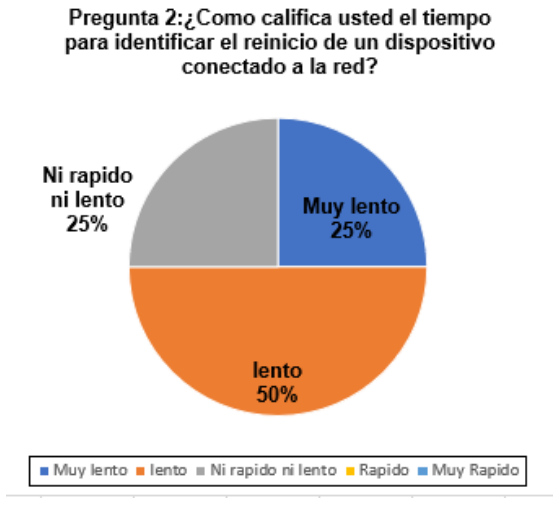
Interpretación: El 60% de expertos afirmo tener una herramienta de gestión de red en su centro de labores, y un 40 % no cuenta con una de herramienta.

Para lograr distinguir mejor los resultados se realizó comparaciones de las encuestas de los que afirmaron tener una herramienta de gestión de red y los que no.

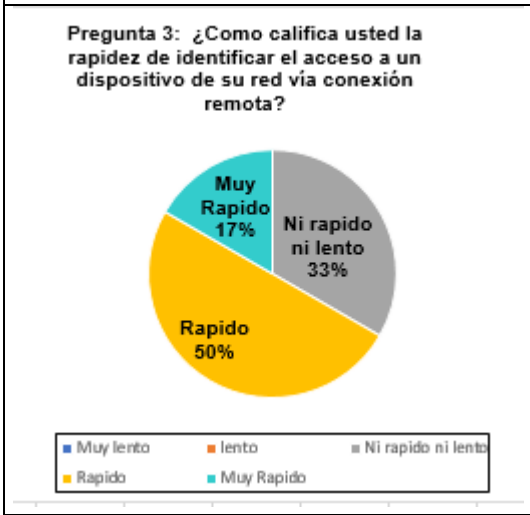
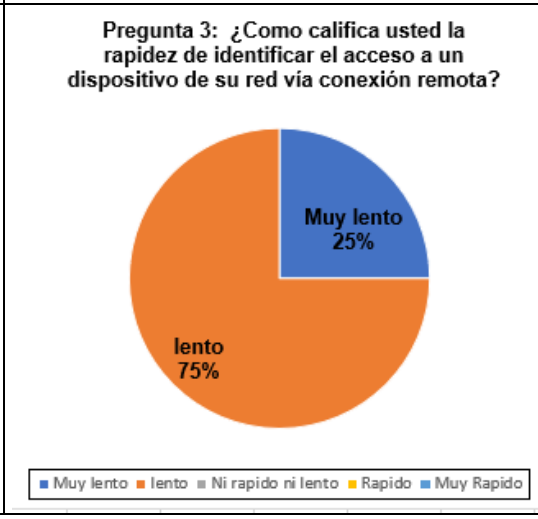
- Comparación realizada para la pregunta 1.

CON HERRAMIENTA DE GESTION DE RED.	CON HERRAMIENTAS DE SIMULACIÓN Y EMULACIÓN
	
INTERPRETACIÓN: En el gráfico de la izquierda se observa claramente que el 100% considera “rápida” la identificación de la caída en los enlaces de la comunicación de red; mientras que el gráfico de la derecha un 75% considera de “lenta” la identificación de caída de enlaces.	

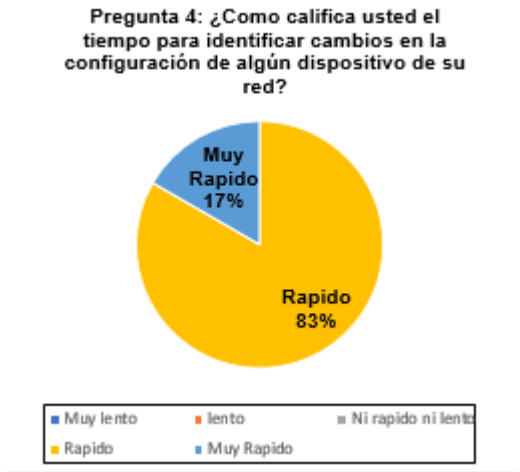
- Comparación realizada para la pregunta 2.

CON HERRAMIENTA DE GESTION DE RED.	CON HERRAMIENTAS DE SIMULACIÓN Y EMULACIÓN
	
INTERPRETACIÓN: En el gráfico de la izquierda se observa claramente que el 83% considera “rápida” la identificación de un reinicio de un dispositivo conectado a su red; mientras que en el gráfico de la derecha un 50% lo considera lento a la identificación de un reinicio de algún dispositivo.	

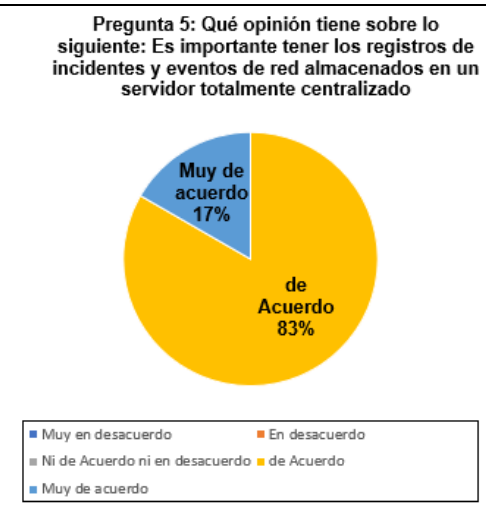
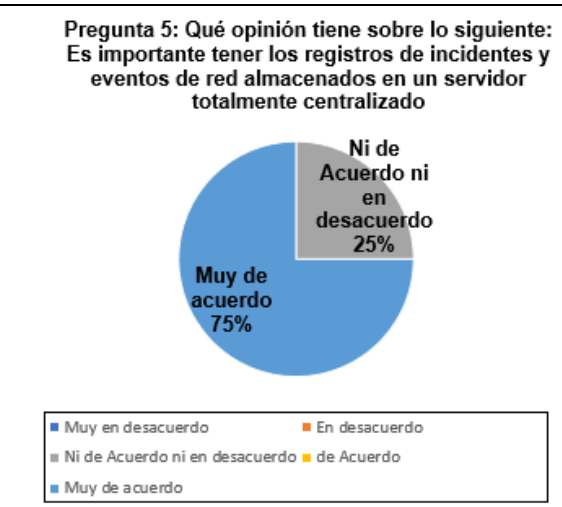
- Comparación realizada para la pregunta 3.

CON HERRAMIENTA DE GESTION DE RED.	CON HERRAMIENTAS DE SIMULACIÓN Y EMULACIÓN
	
INTERPRETACIÓN: En el gráfico de la izquierda se observa claramente que un 50% considera de rápida; mientras que en el gráfico de la derecha un 75 % lo considera lento,	

- Comparación realizada para la pregunta 4.

CON HERRAMIENTA DE GESTION DE RED.	CON HERRAMIENTAS DE SIMULACIÓN Y EMULACIÓN
	
INTERPRETACIÓN: En el gráfico de la izquierda se observa claramente que el 100% considera “rápida” la identificación de cambios en la configuración de algún dispositivo; mientras que en el gráfico de la derecha un 50% considera lento a una identificación de la configuración de algún dispositivo.	

- Comparación realizada para la pregunta 5.

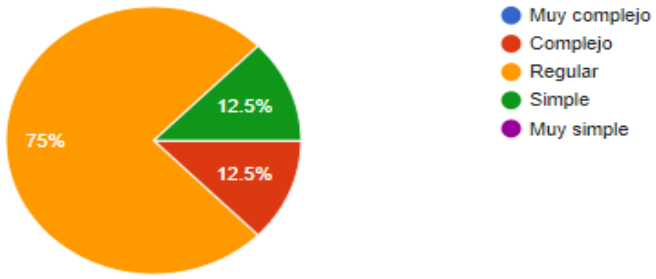
<table>
<tr><th>CON HERRAMIENTA DE GESTION DE RED.</th><th>CON HERRAMIENTAS DE SIMULACIÓN Y EMULACIÓN</th></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td colspan="2">INTERPRETACIÓN: En el gráfico de la izquierda se observa la consideración profesional de los encuestados, en el que un 83% considera de acuerdo con la importancia de tener los registros de incidentes y eventos de red almacenados en un servidor centralizado; frente a un 75 % que respalda la afirmación, respondiendo “Muy de acuerdo”.</td></tr>
</table>

5.4.3. Complejidad de Configuración

Se realizó una encuesta a expertos de Perú, México y Ecuador para conocer el nivel de complejidad de configuración de los protocolos SNMP v2c, SNMP v3 y Syslog. Los resultados obtenidos se muestran continuación.

1. De acuerdo a su experiencia, el nivel de complejidad de configuración del servicio/protocolo SNMP versión 2c es:

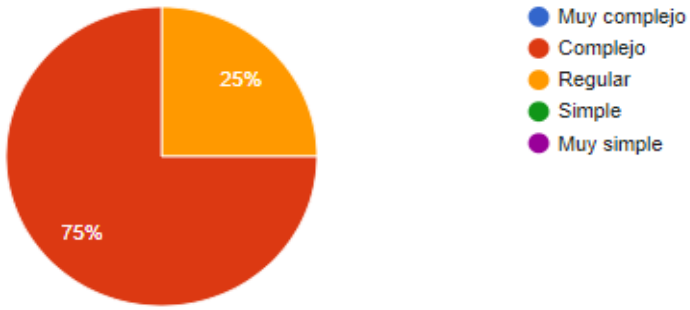
8 respuestas



Interpretación: El 75% de los expertos respondió “Regular”, el 12.5% respondió “Simple”, y el 12.5% restante respondió “Complejo”.

2. De acuerdo a su experiencia, el nivel de complejidad de configuración del servicio/protocolo SNMP versión 3 es:

8 respuestas



Interpretación: El 75% de los expertos respondió “Complejo”, y el 25% restante respondió “Regular”.

Interpretación: El 37.5% de los expertos respondió “Regular”, el 37.5% respondió “Simple”, y el 25% restante respondió “Complejo”

5.4.4. Uso de Recursos computacionales.

Para ejecutar esta prueba, se recopilo información de los tres escenarios de emulación.

A. <u>Nivel del uso del CPU.</u>

En esta prueba se realizó con todos los *routers* activos en cada escenario de emulación. La herramienta PRTG tiene la capacidad de medir el nivel del uso del CPU a través del sensor “CPU *load*” por ende, en cada escenario de emulación se tuvo añadido este sensor dentro del servidor, es preciso indicar que en cada escenario de emulación fueron configurados el protocolo que se designó únicamente. Posteriormente, se procedió a realizar 4 pruebas de consumo de CPU a cada protocolo (Anexo 3), con la finalidad de obtener un valor promedio del consumo para mayor precisión, en esta prueba se tuvo en cuenta los siguientes eventos, capaces de ser reportados por cada protocolo:

- Ingreso a modo de configuración vía consola
- Ingreso a modo de configuración vía telnet
- Ingreso a modo de configuración vía SSH.
- Reinicio del router
- Convergencia OSPF
- Encendido de la interfaz
- Apagado de la interfaz
- Cambios de configuración
- Inicialización de un servicio

Para realizar las pruebas, se ha hecho uso de los eventos mencionados de forma aleatoria, el resumen de estas cuatro pruebas se detalla en la tabla 18.

Tabla 18. Resumen de Pruebas para determinar el Consumo de CPU

Característica	Escenario 1 - SNMPv2c	Escenario 2 - SNMPv3	Escenario 3 - Syslog
Prueba 1	1%	3%	0.5%
Prueba 2	1%	3%	0.5%
Prueba 3	1.2%	3.2%	0.6%
Prueba 4	1%	3%	0.4%
Nro. de eventos	6	6	6
Máx. Promedio Carga	**0.5%**	**1.05%**	**3.10%**

Fuente: Elaboración propia

En la tabla anterior, se muestra un resumen generado por la herramienta PRTG, indicando el tipo de protocolo empleado en diferentes pruebas de eventos, así también el consumo que tiene cada uno de ellos en cada prueba. La generación de eventos para estas pruebas, fueron realizadas sin complicaciones, no existiendo error en el registro de *traps* ni *logs*, cada evento

generado fue reportado también en la herramienta, determinando así una igualdad de consumo para cada prueba realizada.

Así mismo se puede distinguir la diferencia de los valores de consumo de las pruebas en la figura 75, cuando se realiza eventos corriendo SNMPv3 existe un promedio de 3.10% de consumo, que es mayor a Syslog y SNMPv2c que son mucho más ligeros.

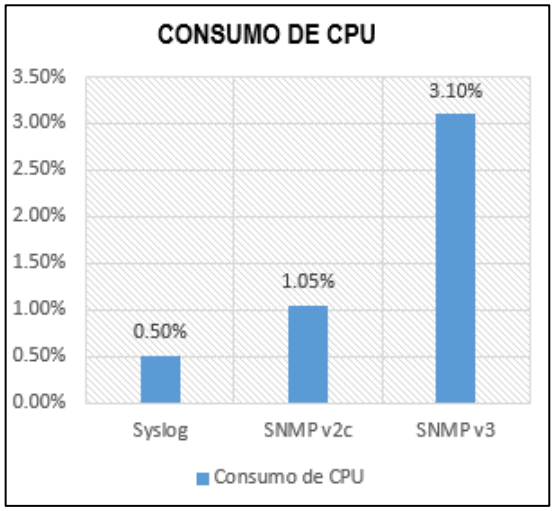


Figura 75. Resumen de consumo de CPU
Fuente: Elaboración Propia

B. Nivel de uso de Memoria

El uso de memoria de cada protocolo ha sido analizado con la herramienta *Wireshark* con la finalidad de obtener el tamaño consumido por paquete de cada protocolo. La idea de identificar el tamaño aproximado de cada paquete es para evidenciar que protocolo consume mayo número de bytes, a partir de ello deducir cual consume mayor uso de memoria. Se realizaron 4 pruebas para cada protocolo (Anexo 4), para ello se generó un número mínimo de eventos con la finalidad de verificar tamaño de paquetes en un tiempo de 4 min por prueba, así como se detalla en la tabla 19.

Tabla 19. Consumo de Memoria

Característica	Eventos Generados	Escenario 1-SNMPv2c	Escenario 2-SNMPv3	Escenario 3-Syslog
Prueba 1	•Inicio del servicio Syslog. •Configuración global	2284 bytes	2695 bytes	215 bytes
Prueba 2	•Configuracion global via ssh •Apagado de un interfaz por ssh	3148 bytes	8108 bytes	368 bytes
Prueba 3	•convergencia ospf •encendido de interfaz	2679 bytes	2925 bytes	296 bytes
Prueba 4	•Apagado de interfaz •reinicio de router	3695 bytes	6994 bytes	236 bytes
Promedio		301.25 bytes	2701.50 bytes	5180.50 bytes
%Consumo promedio de memoria		0.001%	0.002%	0.0001%

Fuente: Elaboración Propia

En la tabla anterior, se puede observar las diferencias del consumo de la memoria de cada escenario, para llegar a estos resultados se tomó en cuenta la cantidad de paquetes que se generaba y el tamaño que este acumulaba por escenario. La duración de la prueba de consumo de memoria fue generada sin complicaciones.

Así mismo se observa la diferencia que existe entre el tamaño de paquete que genera cada protocolo, siendo el protocolo SNMPv3 el que genera un paquete más pesado que Syslog y SNMPv2c, esto debido a la forma de comunicación que posee, además SNMPv2c también se sobrepone a Syslog en el peso del paquete, esto debido a la forma de entablar la comunicación para este protocolo. En las figuras 76, 77 y 78, se puede observar el diagrama de comunicación de los protocolos.

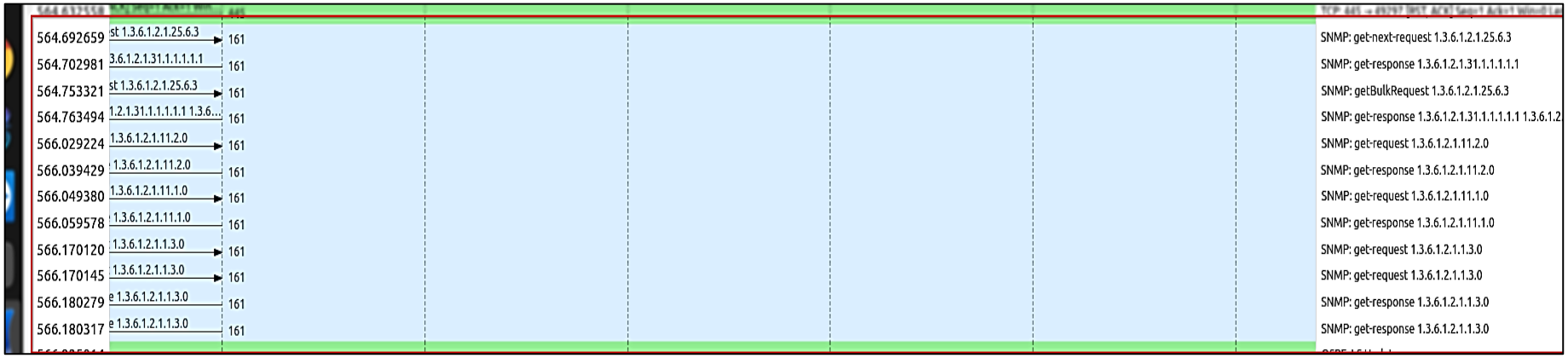


Figura 76. Diagrama de envío y recepción de paquetes de SNMP v2c – Escenario 1
Fuente: *Wireshark*

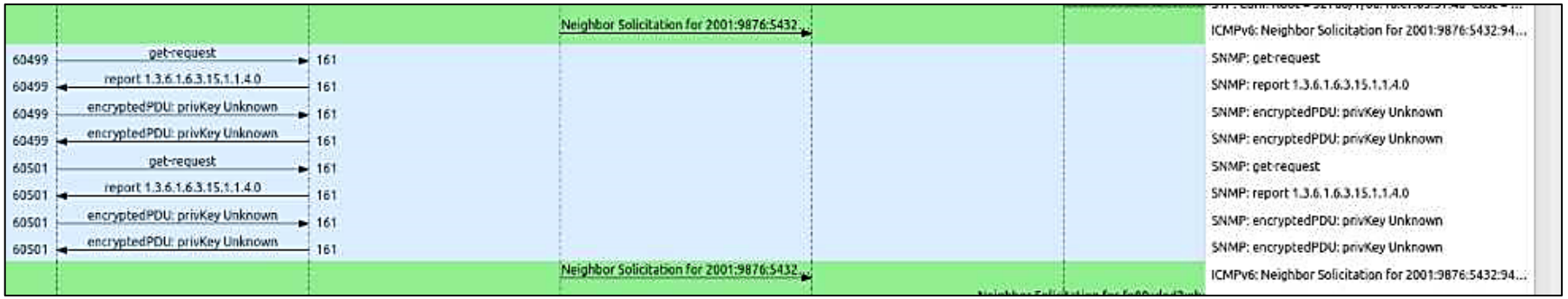


Figura 77. Diagrama de envío y recepción de paquetes de SNMP v3 – Escenario 2
Fuente: *Wireshark*

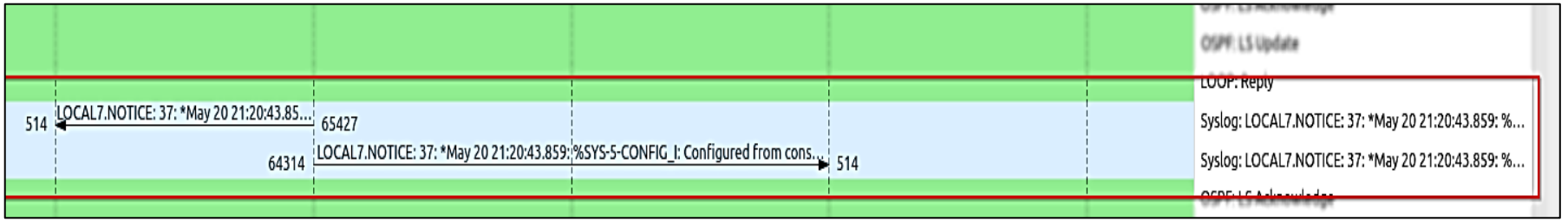


Figura 78. Diagrama de envío y recepción de paquetes de Syslog – Escenario 3
Fuente: *Wireshark*

C. Nivel de ancho de banda

En esta prueba se realizó con todos los *routers* activos. La herramienta PRTG tiene la capacidad de medir el nivel del consumo de ancho de banda de protocolos, el sensor utilizado es el *Packet Sniffer* que cumple de función de monitorear los encabezados de los paquetes de datos, por defecto este sensor solo funciona en el dispositivo de sonda es decir solo se podrá monitorear el ancho de banda consumido por los paquetes que ingresan al servidor y tiene agrupado a distintos protocolos para mostrar el tráfico en kbps como se muestra en la figura 79.

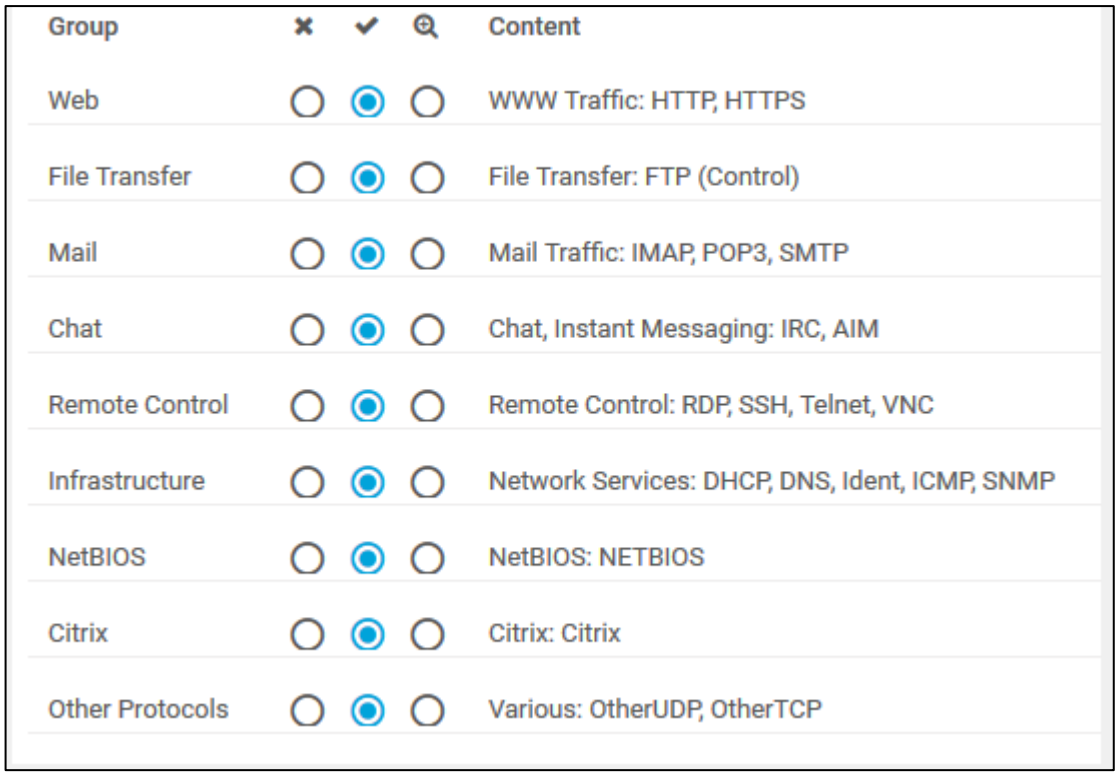


Figura 79. Agrupación de protocolos por defecto
Fuente: Elaboración Propia

Debido a nuestro estudio se basa únicamente en los protocolos Syslog y SNMP, se procedió a cambiar los grupos y canales predeterminados para el *Packet Sniffer*. El cual detallamos a continuación

- ✓ Ingresamos a la carpeta de instalación del PRTG
- ✓ Creamos una copia del archivo *lowrules.osr* y cambie el nombre de la copia a *customflowrules.osr*
- ✓ Abrimos el archivo *customflowrules.osr* en un editor de texto.
- ✓ Estructuramos las nuevas reglas de flujo.

```
      <caption>SNMP</caption>
      <help>Network Services</help>
      <defaultvalue>1</defaultvalue>
      <channels>
        <channel id="3009" name="SNMP">
          <rule>
            Protocol[UDP] and (SourcePort[161-162] or
 destinationPort[161-162])
           </rule>
        </channel>
      </channels>
  <caption>Syslog</caption>
      <help>Network BW</help>
      <defaultvalue>1</defaultvalue>
      <channels>
        <channel id="3007" name="Syslog">
          <rule>
             Protocol[UDP] and (SourcePort[514] or
  destinationPort[514] )
           </rule>
        </channel>
      </channels>
```

Para determinar el nivel de consumo de ancho de banda, se realizaron cuatro puedas con la finalidad de obtener un dato promedio, para esto fue necesario tener los *router* encendidos y generando eventos para que puedan ser reportados, para no saturar los recursos de las maquinas físicas se generó eventos en solo dos los *routers* encendidos por prueba.

- **Reporte de Uso de Ancho de Banda en Syslog y SNMPv2c**

Dado a que este monitoreo se llevara a cabo por puerto de protocolo, se tiene configurado en el *router* como en el servidor parámetros para ambos protocolos, esto no afectara a los resultados puesto a que cada protocolo se emite por diferentes puertos.

Se realizaron cuatro pruebas para medir el consumo de ancho de banda (Anexo 5) para ambos protocolos, el cual se detalla en la tabla 20.

Tabla 20: Consumo de Ancho de Banda

Característica	SNMPv2c	SNMPv3	Syslog
Prueba 1	0.11kbps	0.17kbps	0.05kbps
Prueba 2	0.12kbps	0.24kbps	0.07kbps
Prueba 3	0.12kbps	0.25kbps	0.07kbps
Prueba 4	0.13kbps	0.25kbps	0.07kbps
Promedio del Max Consumo	0.12kbps	0.23kbps	0.07kbps

Fuente: Elaboración propia

En la tabla anterior, se obtuvo el promedio del consumo de ancho de banda para los protocolos Syslog y SNMP; el cual representa los kibts que genera cada protocolo al generarse algún evento ocasional dentro del *router*. Para Syslog se obtiene un consumo de ancho de banda menor que SNMP en sus dos versiones evaluadas como se observa en la comparación en la figura 80.

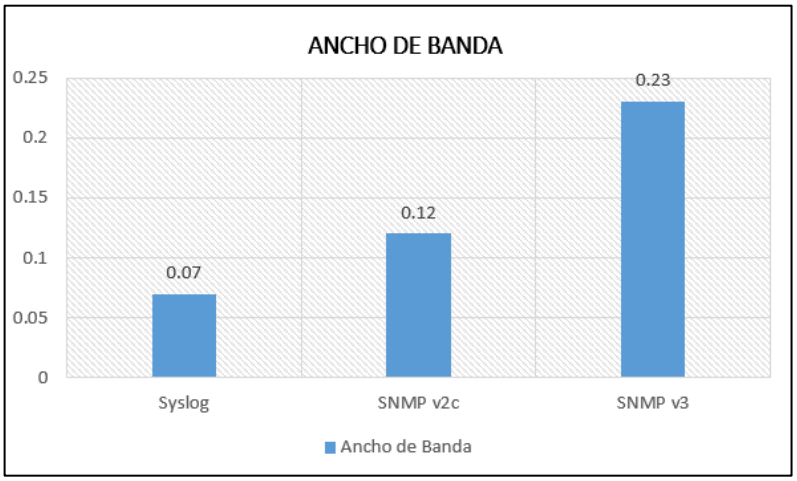


Figura 80. Resumen de Ancho de Banda en Kbps
Fuente: Elaboración propia

5.4.5. Seguridad de Protocolo

Lo que se pretende conocer a través de las pruebas realizadas es determinar el nivel de seguridad de cada protocolo, en la tabla 21 se muestra la forma de autenticación y privacidad por protocolo, en este trabajo de investigación se pretende evidenciar la información que se expone en el transporte además de ver si pueden ser vulnerados.

Tabla 21. Autenticación y privacidad de los protocolos Syslog y SNMP

Característica	Syslog	SNMPv2c	SNMPv3		
			noAuthNoPriv	authNoPriv	authPriv
Autenticación	-	Community String	Username	MD5 or SHA	MD5 or SHA
Privacidad	-	-	-	-	CBC-DES AES-128

Fuente: Elaboración propia

A. Sniffer Capture

En esta prueba fue realizada a través de un *sniffer,* cuyo propósito fue recabar todos los datos que se pueda obtener del tránsito que realiza desde el enrutador al NMS en cada uno de los tres escenarios.

Los resultados se detallan en los siguientes puntos.

- **SNMPv2c**

El dispositivo emite un *traps* de un evento generado. La captura de Sniffer que se muestra en la figura 81, revela direcciones IP, numero de puertos; además el detalle de SNMP muestra la versión, la comunidad que es la forma de autenticarse de esta versión y el OID en texto plano

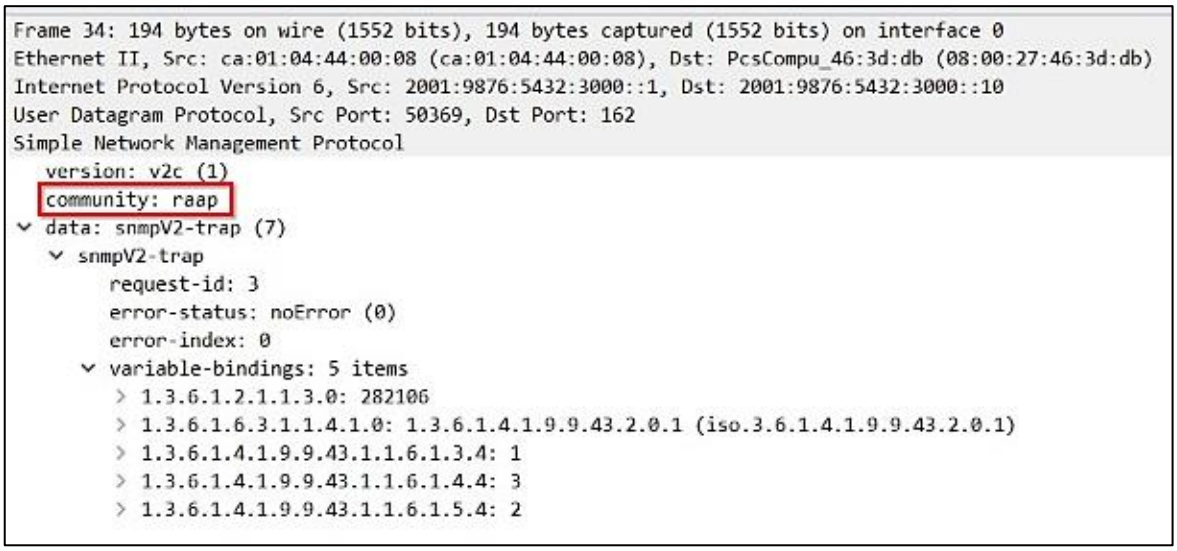


Figura 81. Captura de paquete SNMPv2c – Escenario 1
Fuente: Elaboración propia

- **SNMPv3**

Dado los distintos niveles de seguridad para esta versión, se ha capturado los paquetes de cada nivel como se detalla a continuación:

- ✓ ***noAuthNoPriv***

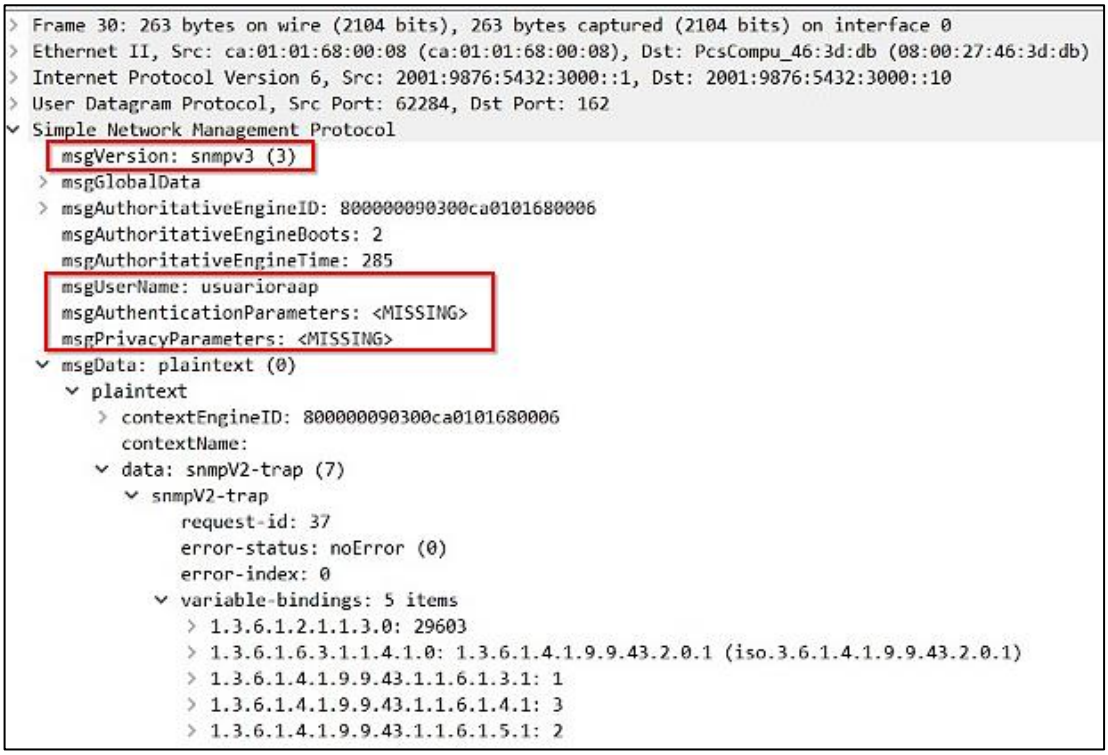


Figura 82. Captura de paquete SNMPv3, nivel: *noAuthNoPri*
Fuente: Elaboración propia

La figura 82 se puede observar la captura de *Sniffer*, del resultado de la emisión de un *traps* en el dispositivo por un evento generado; esta captura revela direcciones IP, número de puertos; además el detalle de SNMP muestra: la versión, el nombre del usuario usado para la autenticación, así como también la ausencia de contraseñas de autenticación y privacidad. Dentro del detalle de *data* podemos conocer los OID del evento que se suscitó.

- ✓ ***authNoPriv***

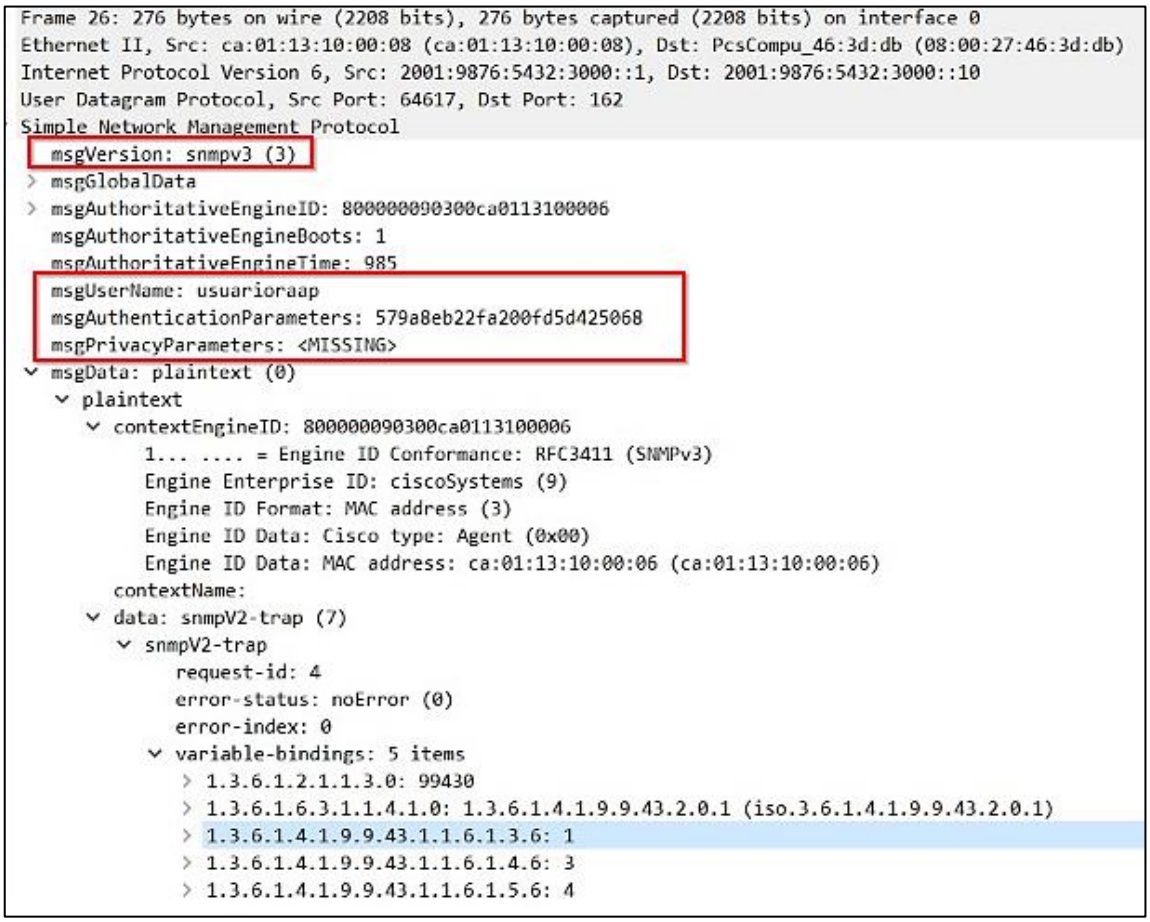


Figura 83. Captura de paquete SNMPv3, nivel: *AuthNoPri*
Fuente: Elaboración propia

La figura 83 se pude observar la captura de *Sniffer* el cual revela direcciones IP, numero de puertos; además el detalle de SNMP muestra: la versión, el nombre del usuario y la contraseña cifrada usada para la autenticación, en *msgPrivacyParameters* se puede observar la ausencia de la contraseña del cifrado/privacidad; Dentro del detalle de *data* podemos conocer los OID del evento que se suscitó.

- ✓ ***authPriv***

Este nivel de seguridad de SNMPv3 incorpora una contraseña para cada usuario para la autenticación y cifrado/privacidad; en la figura 84 se muestra la captura de un *traps* con nivel *authPriv*. El *Sniffe*r revela la versión, así como el usuario, no pudiendo visualizar en texto plano la contraseña de autenticación ni privacidad, además de encontrarse en la sección *msgData* donde usualmente en los niveles anteriores de seguridad encontrábamos el desglose del OID del evento suscitado, en este nivel de seguridad se encuentra totalmente cifrado, no pudiendo obtener la información del OID.

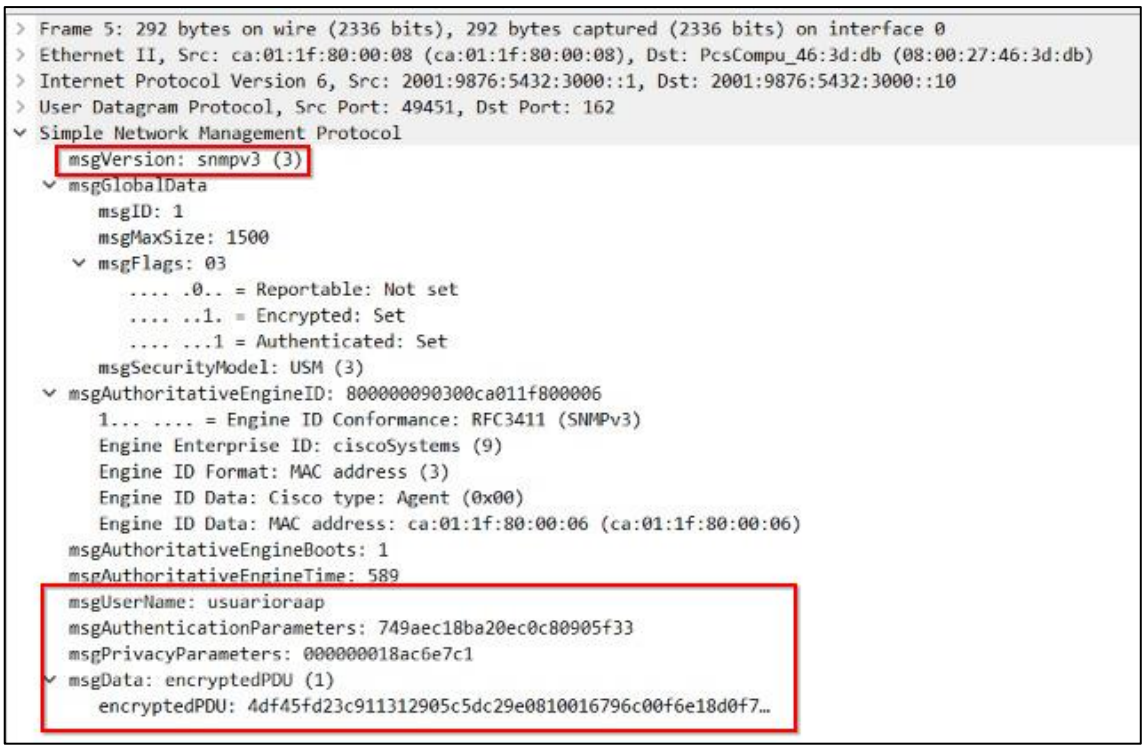


Figura 84. Captura de paquete SNMPv3, nivel: *AuthPri*
Fuente: Elaboración propia

B. Ataque con la herramienta SNMPwn

Debido a la exposición de datos revelados por el *Sniffer* en la prueba anterior, se corroboro que SNMPv3 con el nivel de seguridad *AuthPriv*, fue el que menos datos de importancia se pudo obtener. Por ende, se pensó en utilizar una herramienta de ataque para exponer que, aun configurado con el mayor nivel de seguridad *(authPriv)* las contraseñas se pueden encontrar vulnerables.

Center for Internet Security (CIS) Controls V7.1 especifica en el control 5 acerca de la Configuración segura para hardware y software en dispositivos, que las cuentas o contraseñas predeterminadas o no seguras, pueden convertirse en puntos vulnerables para cualquier atacante. Desarrollar cuentas o contraseñas con buenas propiedades de seguridad es una tarea compleja, el sub control 5.1 considera mantener estándares de configuración para establecer configuraciones seguras.

Para exponer las vulnerabilidades que pueden tener las configuraciones débiles, se propuso un escenario con contraseñas conocidas y fáciles de recordar para los usuarios.

Se configuró un *router* con SNMPv3 con el tercer nivel de seguridad *"AuthPriv";* para la autenticación y la privacidad se puso contraseñas fáciles de identificar.

Para descubrir la vulnerabilidad de las contraseñas de autenticidad y privacidad de SNMPv3 se utilizó una herramienta de enumeración y ataque de usuarios SNMPv3 denominado **SNMPwn**, cuyo objetivo es atacar el servidor con las cuentas enumeradas y su lista de contraseñas y contraseñas de cifrado,

ataca los 3 niveles de seguridad que tiene SNMPv3; para el uso de esta herramienta se utilizó el Sistema Operativo Kali Linux, dicha herramienta contiene 2 archivos de texto denominados “users.txt” y “passwords.txt” respectivamente, el primero incluye una lista de usuarios y el segundo una lista de contraseñas, las 2 listas son muy conocidas y muy utilizadas por los usuarios.

El proceso de la instalación de la herramienta **SNMPwn** se muestra en la figura 85.

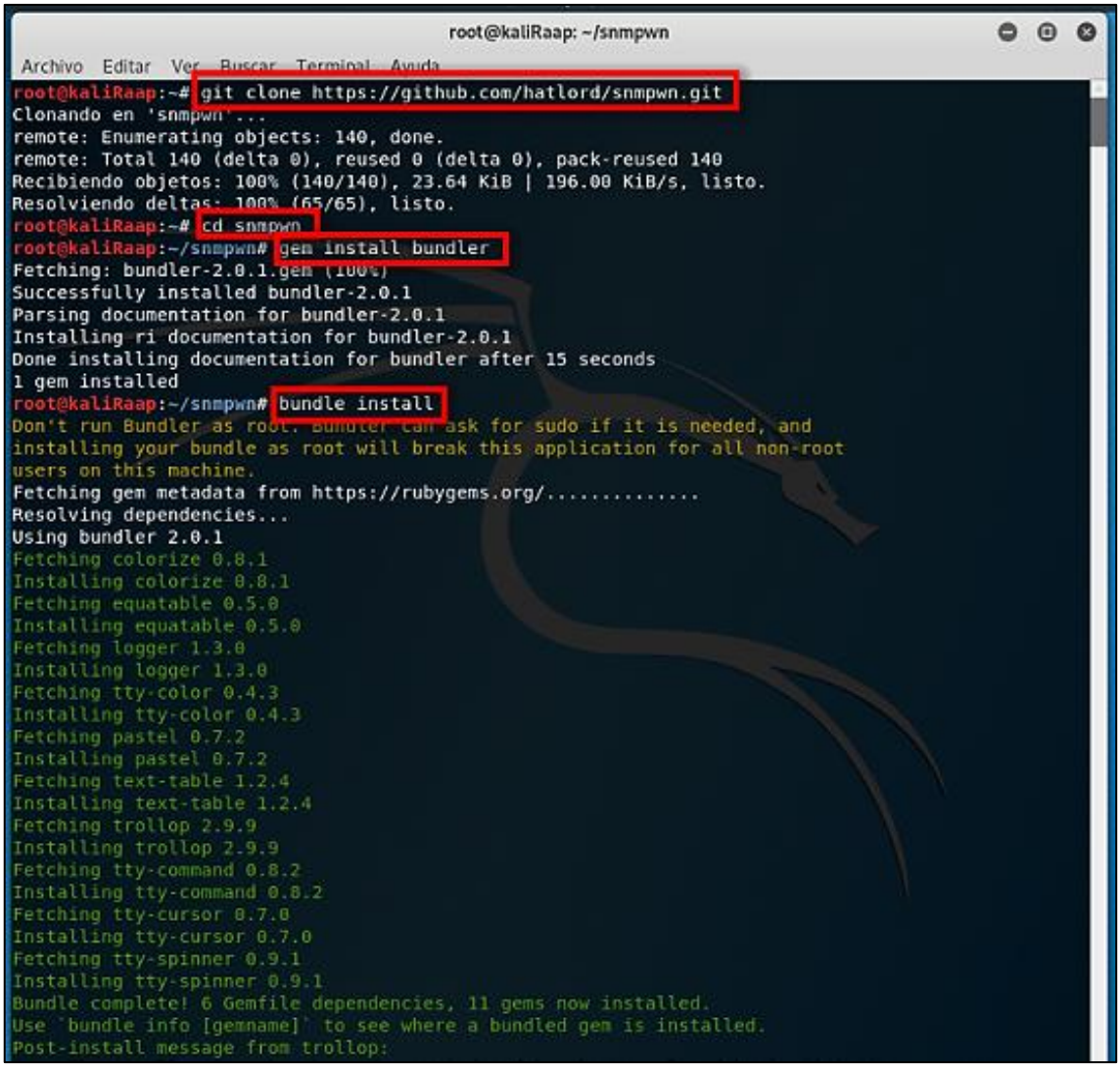


Figura 85. *Proceso de Instalación de la herramienta SNMPwn*
Fuente: Elaboración propia

Las figuras 86 y 87 muestran los archivos de texto “users.txt” y “passwords.txt” respectivamente.

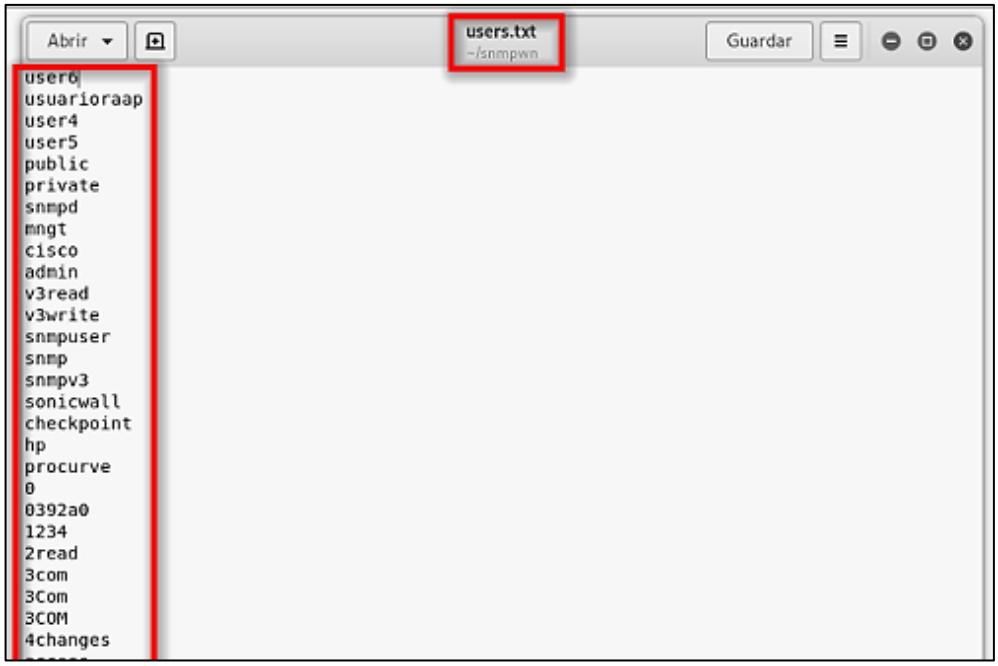


Figura 86. Archivo de texto “users.txt”
Fuente: Elaboración propia

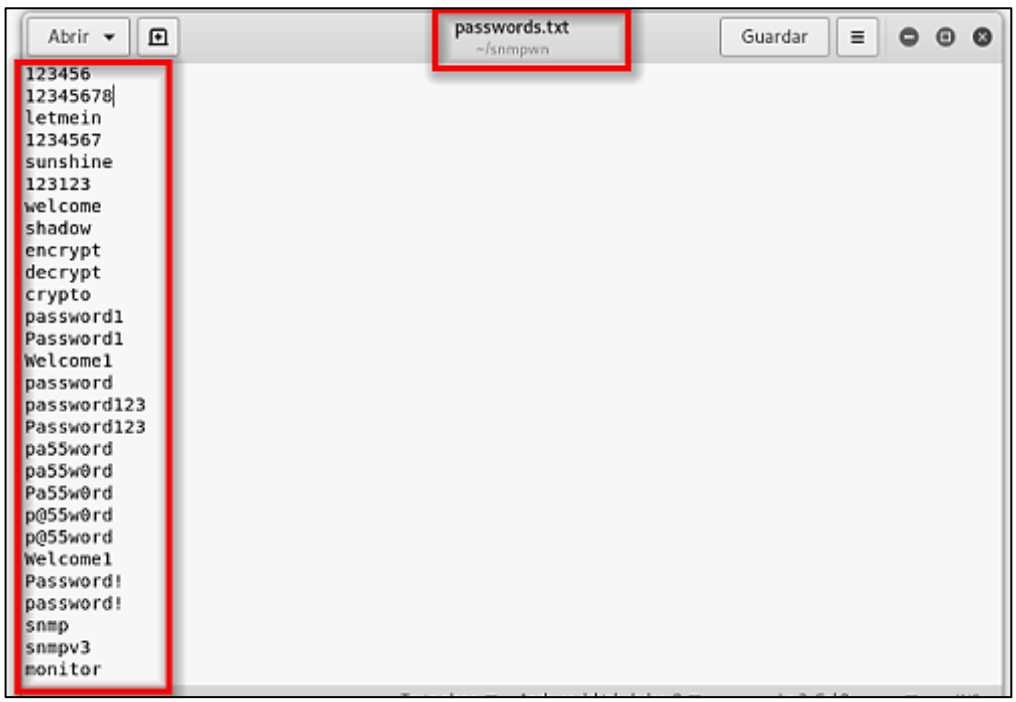


Figura 87. Archivo de texto *“passwords.txt”*
Fuente: Elaboración propia

Debido a que se debe proporcionar al script **snmpwn** una lista de *hosts*, se procedió a crear un archivo de texto denominado “hosts.txt” que contenía la IPv6 del *router* a ser atacado, lo cual se muestra en la figura 88.

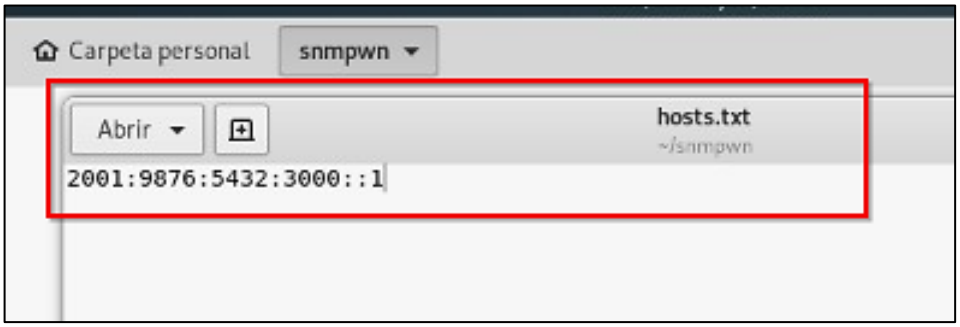


Figura 88. Archivo de texto “*hosts.txt”*
Fuente: Elaboración propia

Luego se procedió a editar el archivo “users.txt” y se añadió el usuario que se configuró en el *router* snmp-server para facilitar el descubrimiento, lo cual se muestra en la figura 89.

Figura 89. Archivo de texto “*users.txt”* editado
Fuente: Elaboración propia

La línea de comandos para lograr el ataque y comprobar las vulnerabilidades de las contraseñas de autenticidad y privacidad del usuario snmp-server se muestra en la figura 90; donde se visualiza al script snmpwn, y los archivos con las listas de hosts, usuarios, contraseñas y contraseñas cifradas.

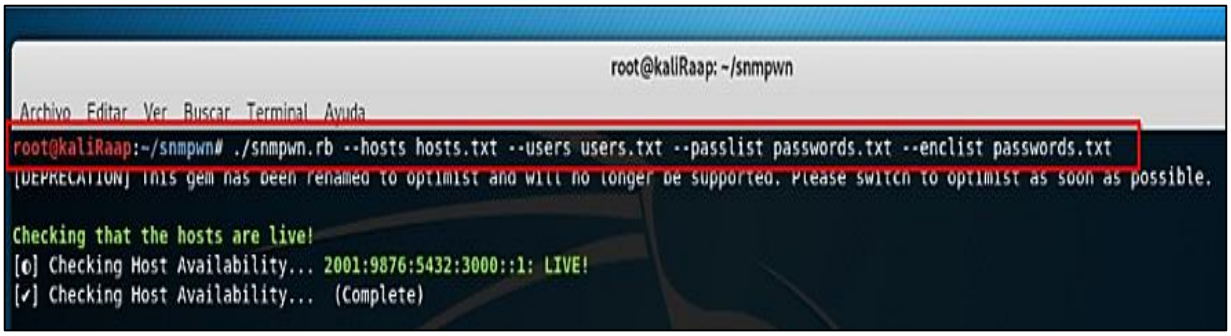


Figura 90. Línea de comandos del script “snmpwn”
Fuente: Elaboración propia

La figura 91 muestra que se logró con éxito la enumeración de usuarios, donde se puede visualizar que el usuario “usuarioraap” pertenece a la IPv6 “2001:9876:5432:3000::1” del *router* snmp-server.

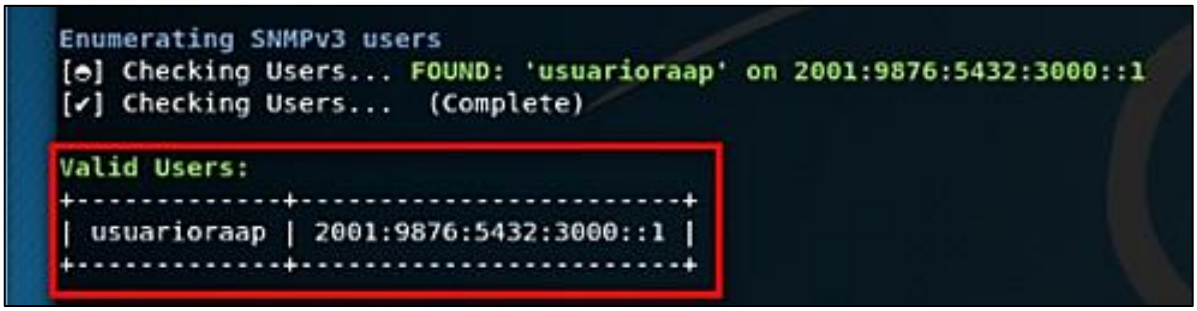


Figura 91. Enumeración de usuarios
Fuente: Elaboración propia

Por último, la figura 92 muestra que se logró descubrir con éxito las contraseñas de autenticidad y privacidad del usuario snmp-server, donde se visualiza que del usuario “usuarioraap” las contraseñas de autenticidad y privacidad son “12345678”, por tanto, se logró exponer las vulnerabilidades de las configuraciones débiles.

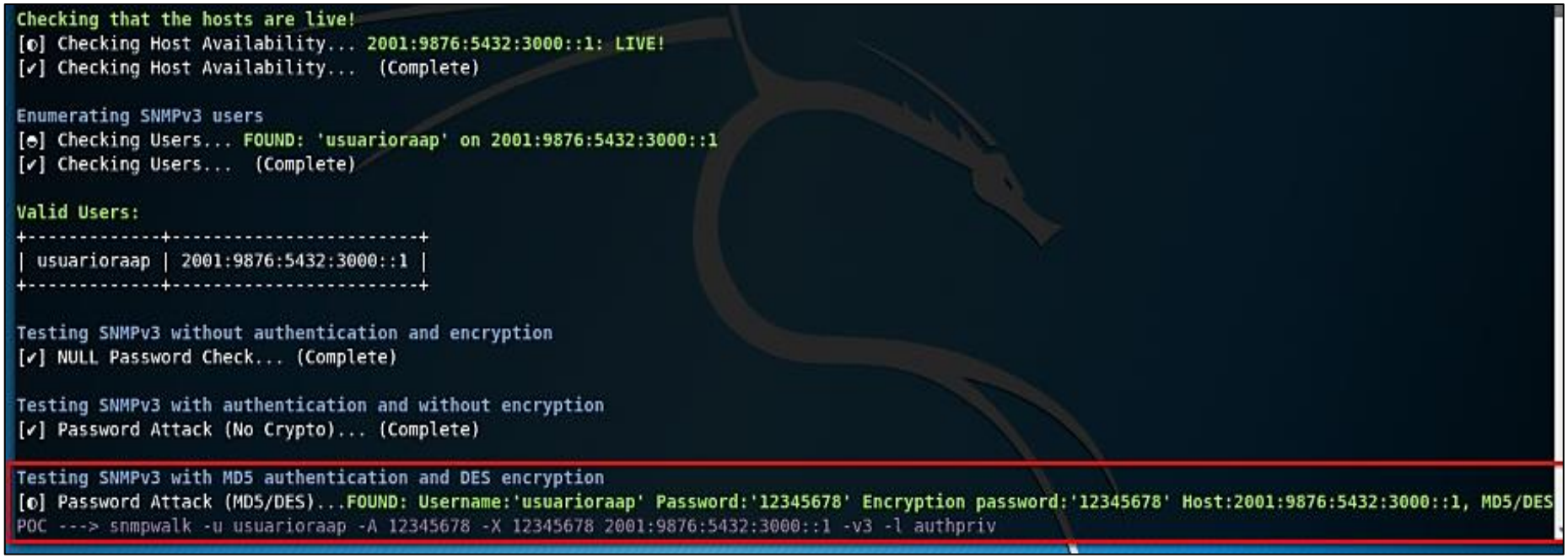


Figura 92. Descubrimiento de contraseñas de autenticidad y privacidad
Fuente: Elaboración propia

VI. ANÁLISIS DE RESULTADOS Y DISCUSIÓN

6.1. Análisis de resultados

A. Interpretación de Resultados de la variable independiente

- **Complejidad de Configuración**

Syslog	SNMP	
	Versión 2	Versión 3
El nivel de complejidad según las respuestas obtenidas de los expertos existe una coincidencia de un 35% que considera de “Regular” y de otro 35% que considera de “Simple” la configuración por encima del 25% calificaron de “complejo”. Este escenario se debe a las propias conclusiones de los expertos según la experiencia que adquirieron en el campo profesional.	El nivel de complejidad según las respuestas obtenidas de los expertos, indica que un 75% considera de “Regular” la complejidad de configuración muy por encima del 12.5% calificaron de “simple” y de otro 12.5% de “complejo”. Este escenario se debe a las propias conclusiones de los expertos según la experiencia que adquirieron en el campo profesional.	El nivel de complejidad según las respuestas obtenidas de los expertos, indica que un 75% considera de “complejo” la configuración de SNMPv3 muy por encima del 25% calificaron de “Regular”. Este escenario se debe a las propias conclusiones de los expertos según la experiencia que adquirieron en el campo profesional. Además, el poder interactuar en este trabajo de investigación con esta versión del protocolo se requirió conocimientos previos para comprender el funcionamiento de SNMP v3 y sus niveles de seguridad para realizar la configuración.

- **Uso de Recursos Computacionales**

Syslog	SNMP	
	Versión 2	**Versión 3**
El nivel de consumo de recursos por parte del protocolo fue considerado “bajo” frente al otro protocolo, ya que la evaluación que se realizó por protocolo arrojó promedios muy reducidos frente a SNMP. En el CPU consumió solo un 0.5%, en el ancho de banda 0.7kbps y por último el consumo de la memoria en 0.3KB, el cual usa solo un 0.0001% del total de la memoria	El nivel de consumo de recursos por parte del protocolo fue considerado “medio” frente al otro protocolo, ya que la evaluación que se realizó por protocolo arrojó promedios más bajos que SNMP v3 y más altos que Syslog. En el CPU arrojo un promedio de un consumo de un 1.05%, en el ancho de banda un promedio máximo del consumo fue de 0.12kbps y por último el consumo de la memoria en 3KB, el cual usa solo un 0.001% del total de la memoria.	El nivel de consumo de recursos por parte del protocolo fue considerado “alto”, ya que la evaluación que se realizó por protocolo arrojó promedios más altos que SNMP v2 y Syslog. En el CPU arrojó un promedio de un consumo de un 3.10%, en el ancho de banda un promedio máximo del consumo fue de 0.23kbps y por último el consumo de la memoria en 6KB, el cual usa solo un 0.002% del total de la memoria.

- **Seguridad de protocolo**

Indicador	Syslog	SNMP	
		Versión 2	**Versión 3**
Nivel de integridad	El nivel de integridad del protocolo fue “bajo” puesto a que carece de integridad ya que la información se transporta en texto plano.	El nivel de integridad del protocolo fue “bajo” puesto a que carece de integridad ya que la información es transportada en texto plano.	En este caso el nivel de integridad es “alto” para el nivel de seguridad *authpriv,* ya que la información se trasporta de manera cifrada sea por des o md5

Nivel de confidencialidad	El nivel de integridad del protocolo fue “bajo” puesto a que carece de autenticación previa.	El nivel de integridad del protocolo fue “medio” puesto a que se atentica por medio de la comunidad.	En este caso el nivel de integridad es “alto” para el nivel de seguridad *authpriv,* ya que la autenticación se realiza mediante un usuario y una contraseña.

- **Servicios Disponibles**

Las pruebas realizadas en el punto 5.3.1 empleadas para obtener la información de eventos reportados por protocolo favorecieron para que este trabajo de investigación pueda corroborar a través de los diferentes reportes obtenidos los diferentes servicios de cada protocolo al emitir un mensaje.

La tabla 22 está conformada por los servicios considerados para este estudio, los que sirvieron para recabar información de cuantos servicios disponibles cuenta cada protocolo.

Tabla 22. Servicios disponibles por protocolo.

Característica del Servicio	**Syslog**	**SNMPv2c**	**SNMPv3**
Envió de mensaje de ocurrencia (eventos) de cualquier tipo.	Según las pruebas realizadas, Syslog omite algunos reportes de evento generados para este estudio, como se evidenció en el punto 5.3.1. Por ende, **No** envía cualquier tipo de mensaje.	Según las pruebas realizadas, SNMPv2c reporta cualquier evento generado en este estudio como se evidenció en el punto 5.3.1. Por ende, **Si** envía cualquier tipo de mensaje.	Según las pruebas realizadas, SNMPv3 emite un *traps* encriptado, para cualquier evento generado en este estudio como se evidenció en el punto 5.3.1. Por ende, **Si** envía cualquier tipo de mensaje.
Envió de Mensaje en tiempo real	Si	Si	Si
Envío de Mensaje en formato estandarizado	Si	Si	Si
Puede Clasificar el tipo de mensaje	Si.	No	No
Puede recopilar información de diferentes dispositivos	Si	Si	Si
Gestión de Seguridad	No	No	Si
Registro de eventos o incidentes de manera detallada	Si	No	No
Cantidad de Servicios	5	4	5

6.2. Discusión.

Antecedente: “Evaluación de los mecanismos de seguridad en los sistemas de notificación y registro de eventos para la gestión de redes”

Interpretación: Este antecedente de investigación pretende conocer carencias de seguridad de los protocolos Syslog y SNMP, realizando la implementación pos pruebas de un canal Seguro para él envió de información; Pero el enfoque de esta tesis es distinto puesto a que si bien es cierto en el antecedente se evalúa ambos protocolos, no se hace referencia más que a seguridad; sin embargo en este trabajo de investigación se evalúan otros indicadores de este protocolo, como el nivel de complejidad de configuración, uso de recursos y los servicios que presentan los mensajes.

Antecedente: “Diseño e implementación de un sistema de monitoreo basado en SNMP para la red nacional académica de tecnología avanzada”

Interpretación: En este antecedente de investigación tiene ciertas similitudes con el presente estudio; ya que se logró implementar el sistema PRTG en la Red Avanzada de Colombia, pero solo abarcaron SNMP y la investigación concluía con la implementación de la solución; no realizaron un estudio más profundo acerca del protocolo

Antecedente: *“Managing Syslog”*

Interpretación: Este antecedente de investigación propone un prototipo para la supervisión y administración de Syslog a través considerando el estado operativo y estadísticas del dispositivo, el prototipo supervisa cada host y extrae la información de configuración de las aplicaciones de Syslog utilizando SNMP,

con el fin de trabajar de forma complementaria, lo cual tiene cierta similitud con el estudio de los protocolos de estudio. Ya que en la presente tesis se resalta la fortalezas y debilidades de cada protocolo y como se pueden complementar teniendo configurado ambos protocolos.

Antecedente: "*A Prioritized Retransmission Mechanism for Reliable and Efficient Delivery of Syslog Messages"*

Interpretación: Este antecedente de investigación se enfoca en el estudio de seguridad de Syslog además de proponer un mecanismo para la retrasmisión priorizado para un sistema confiable y eficiente entrega de mensajes Syslog, pero no realizan ningún estudio con respecto a Syslog. La presente tesis de investigación tiene como estudio la seguridad del protocolo Syslog, pero además también abarca a SNMP como parte de este estudio.

Antecedente: *"IPV6 Connectivity and Management Emulation for REUNA, the Chilean Advanced Network"*

Interpretación: Este antecedente de investigación tiene como finalidad promover en las universidades peruanas la importancia de las Redes Avanzadas, para ello se realizó la emulación de la red troncal de REUNA, la red avanzada de Chile; lo cual tiene cierta similitud con el presente estudio de investigación, ya que se realizó la emulación de RAAP, la red avanzada de Perú; teniendo en cuenta la red dorsal de fibra óptica, aplicando IPV6, el protocolo de enrutamiento OSPFv3, y para la gestión el protocolo Syslog y SNMP, tal como lo hacen las compañías ISP comerciales

CONCLUSIONES

Al evaluar la eficacia y eficiencia de la Gestión de Redes, teniendo configurado las alternativas de configuración se ha podido determinar que brinda una reducción de tiempo a los administradores de red que invierten en los procedimientos u detención de eventos, considerando la información que brinda cada registro gracias a la notificación por parte de los protocolos, un aporte para cumplir los objetivos de la Gestión de Red; por lo cual la presente tesis se enfocó en evaluar las fortalezas y debilidades de los protocolos Syslog y SNMP como caso de estudio; con base en las pruebas y análisis de resultados alineados al objetivo general y objetivos específicos de la investigación, se llegó a las siguientes conclusiones:

1. La evaluación de las dimensiones de la variable independiente (Syslog y SNMP) determinaron la mejor alternativa para la gestión de Redes Avanzadas es la configuración de Syslog y SNMPv3 de forma complementaria; la complejidad de la configuración se determinó más “compleja” para SNMPv3, frente a SNMPv2c, ya que para realizarla se tiene que tener conocimientos de la funcionalidad de SNMPv3 y sus niveles de seguridad en esta versión, frente a Syslog que para ser configurados los conocimientos previos son básicos. Los resultados de las pruebas realizadas muestran que el SNMPv3 utiliza más recursos (Ancho de Banda, CPU y RAM) que SNMPv2c y más que Syslog, debido a la seguridad “*authpriv”* con el que fue configurado para esta investigación todos los paquetes son transportados cifrados; Sin embargo, este nivel de seguridad en SNMPv3, destacó con el nivel más “alto”, esto debido al proceso de autenticación y cifrado que posee. El nivel de servicios del mensaje

el que más aporta indicios de disponibilidad de la información de cada evento fue Syslog frente a SNMP en ambas versiones, ya que en SNMPv2c se logró descifrar cada *traps* con la ayuda de *browser OID* y los *traps* SNMPv3 no fueron percibidas por las herramientas debido al nivel de encriptación que funciona esta versión de protocolo, pero este protocolo no dejo de notificar, pero teniendo la capacidad dentro de la herramienta de ser auto configurables OIDs específicas para determinar ciertos eventos anormales dentro de la red. Por lo tanto, se determinó la mejor forma de la mejor alternativa de para la gestión de Redes Avanzadas es la complementación de las capacidades de SNMPv3 con Syslog.

2. Syslog y SNMPv3 puede maximizar sus capacidades para gestionar Redes Avanzadas, siendo configuradas de forma complementaria; SNMPv3 puede ser más seguro pero implica un mayor consumo de recursos, la ventaja de este protocolo es que tiene la capacidad de acoplarse a cualquier herramienta de gestión de forma automática, solo sería necesario la configuración en los dispositivos, sin embargo Syslog muestra un formato de mensaje más detallado con mayor disponibilidad de información.

3. Las pruebas realizadas muestran que Syslog es la mejor alternativa para el consumo de recursos computacionales, porque presenta menor consumo en el CPU, RAM y Ancho de Banda (0.5%, 0.3 KB, 0.07Kbps) frente a SNMPv3 con (3.10%, 0.6KB, 0.23kbps) y el SNMPv2c (1%, 3KB, 0.12kbps)

4. Las pruebas muestran que SNMPv3 en su nivel de seguridad *authpriv* contempla un nivel de seguridad alto frente a Syslog y SNMPv2c por presentar la confidencialidad e integridad en cada uno de sus paquetes trasmitidos a través de la autenticación y cifrado que posee.

5. Las pruebas que Syslog presentan mayor características de servicios, ofreciendo mayor disponibilidad de información en sus mensajes frente a SNMPv2c y 3 quienes no presentan características como la clasificación del mensaje y registro de estos de manera detallada.

6. La propuesta de una red Backbone para la Red Académica Avanzada del Perú (RAAP) fue elaborada con el criterio de reincorporar la Red Académica Peruana a CLARA, conectando distintos nodos que representan a entidades científicas de las Regiones del Perú, además de ser el escenario principal para la emulación de la gestión de Redes Avanzadas en esta investigación.

RECOMENDACIONES

Para el uso del protocolo SNMPv3, se debe realizar una configuración segura, descartando para esto contraseñas predeterminadas por el sistema, o que sean fáciles de descifrar, puesto a que el protocolo puede verse vulnerado, no por que carezca de seguridad si no por llevar una “configuración débil”.

Como trabajo futuro se recomienda utilizar los protocolos de configuración para un análisis de rendimiento en *routers* físicos, puesto que en esta investigación se realizó un análisis preliminar en un emulador, teniendo limitaciones para recopilar reportes de eventos que propiamente de equipos físicos.

ABSTRACT

This research called "Configuration Alternatives with the use of Syslog and SNMP protocols for Advanced Network Management", is based on the evaluation of protocols to take advantage of their capabilities. This study identifies two protocols commonly used for network management, with wide dissemination and availability in the devices of an advanced network; with the objective of determining the best configuration alternative in an emulated environment of the management of an advanced network considering the configuration of the protocols in the equipment, the use of resources, the security they present and the available services.

Because the Peruvian Academic Network is inactive, as a first phase of this research work the proposal of a topology was made in order to reinsert the Peruvian Academic Network to the CLARA Network, in addition to using it as a scenario for the emulation that It is part of the study.

The second phase consisted of the emulation of the Syslog, SNMP v2c and 3 protocols each configured in the same topology, but in different scenarios to perform independent tests of each protocol. The tests carried out showed that Syslog and SNMPv3 have their own capabilities, but that they can complement each other by configuring in parallel; SNMPv3 is cataloged as a "complex" configuration versus SNMPv2c and Syslog that is considered between "regular" and "simple"; in addition to presenting greater consumption of computing resources overlapping in the use of CPU, memory and bandwidth (3.10%, 0.6KB, 0.23kbps) versus a lighter Syslog consuming CPU, memory and bandwidth (0.5%, 0.3 KB, 0.07kbps); but it was also determined that the authpriv security

level of the SNMPv3 protocol has a "high" security level above SNMPv2c and Syslog, this explains the greater resource consumption and even the level of complexity in the configuration. The protocol that presents the most favorable indications of the services available for each message is Syslog, because it provides greater information availability

REFERENCIAS BIBLIOGRÁFICAS

Central Intelligence Agency. (Julio de 2016). *CIA.* Obtenido de The Word Factbook: https://www.cia.gov/library/publications/resources/the-world-factbook/fields/204rank.html

Quispe Bustincio, J. w. (2018). *Implementacion de un sistema de monitore y control de red para un canal de televisión basado en Open Source.* Puno: UNA-PUNO.

Abilene Home. (s.f.). *ADVANCED NETWORKING*. Obtenido de About Abilene: https://www.internet2.edu/products-services/advanced-networking/

Arana Boreto, N. (2005). *Modelo de gestión de seguridad con soporte a SNMP.* Pontificia Universidad Javeriana, Facultad de Ingenieria, Bogota D.C.

Avila Gonzales, V. R. (2014). *Diseño e Implementacion de un sistema de monitoreo Basado en SNMP para la ren nacional academica de Tecnología avanzada.* Bogotá: Universidad Santo Tomas.

Bolt, Beranek y Newman. (1981). *ARPANET COMPLETION REPORT.*

Castillo Velazquez , J. I. (2017). *Redes de Datos.* Mexico: SAMSARA.

Castillo Velazquez , J. I., Cobos Panduro, V. R., & Marchand Niño, W. R. (2018). IPV6 Connectivity and Management Emulation for REUNA, the Chilean Advanced Network . *IEEE*.

Castillo Velázquez, J. I. (2009). *"El árbol de Internet y la estructura de la información de la gestión de una red".* pp. 15-17: Rev. IEEE Latinoamérica-NoticIEEEro.

Cuchala Vásquez, S. (2017). *Gestión y monitoreo de la red interna del Gobierno Provincial de Imbabura mediante el modelo de gestión y software libre.* Ibarra, Ecuador: Universidad Técnica del Norte.

docwiki.cisco. (16 de 10 de 2012). *docwiki.cisco*. Obtenido de Simple Network Management Protocol: http://docwiki.cisco.com/w/index.php?oldid=49113&title=Simple_Network_Management_Protocol&dtid=osscdc000283#SNMP_Basic_Components

docwiki.cisco. (16 de 10 de 2012). *Simple Network Management Protocol*. Obtenido de Simple Network Management Protocol: http://docwiki.cisco.com/w/index.php?oldid=49113&title=Simple_Network_Management_Protocol&dtid=osscdc000283#SNMP_Basic_Components

GÉANT. (2015). *GÉANT*. Obtenido de GÉANT: https://www.geant.net

Heart, F., McKenzie, A., & McQuillan, J. (1981). *ARPANET Completion Report.* ARPA Network Development.

Jhaky, C. S. (08 de 2018). *Recursos Informaticos.* Obtenido de Recursos Informaticos: https://es.slideshare.net/Gamajal/recursos-informaticos-1-55763655

Josh Whitford; Andrew Schrank. (2011). *The Anatomy of Network Failure.* Washington: American Sociological Association.

July Hernández, M. (2012). *Evaluación de Mecanismos de Seguridad en los Sistemas de Notificación y Registro de Eventos para la Gestión De Redes.* Tesis, Universidad Central de Venezuela, Caracas.

Marti Baiba, A. (2001). *Gestión de red.* Universidad Politécnica de Catalunya. España: Edicions OPC.

Mauro D; Schmidt k. (2005). *Essential SNMP.* Estados Unidos: 2nd Edition O'Reilly.

REDCLARA. (Mayo de 2017). *REDCLARA*. Obtenido de REDCLARA: http://www.redclara.net/index.php/es/red/redclara/topologia-actual-de-la-red

RFC 2271. (s.f.).

RFC 2460. (1998). *Internet Protocol, Version 6 (IPv6).* -: The Internet Society.

RFC 2574. (s.f.).

Rosemberg Diaz , A. (2007). *Diseño e implementación de un centro de operación red académica peruana en software libre.* Lima: FACULTAD DE CIENCIAS E INGENIERÍA.

Sampieri, R. H. (10 de Junio de 2014). *Metodología de investigación 6ta Edición.* Mexico: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. Obtenido de DEFINICIÓN DE COMPRENSIÓN: http://definicion.de/comprension/

Stalling, W. (1999). *SNMP, SNMPv2, SNMPv3 and RMON .* Addison Wesley.

Terplan, K. (1992). *Communication Networks Management* (Vol. 702 pag.). New Jersey: Prentice Hall.

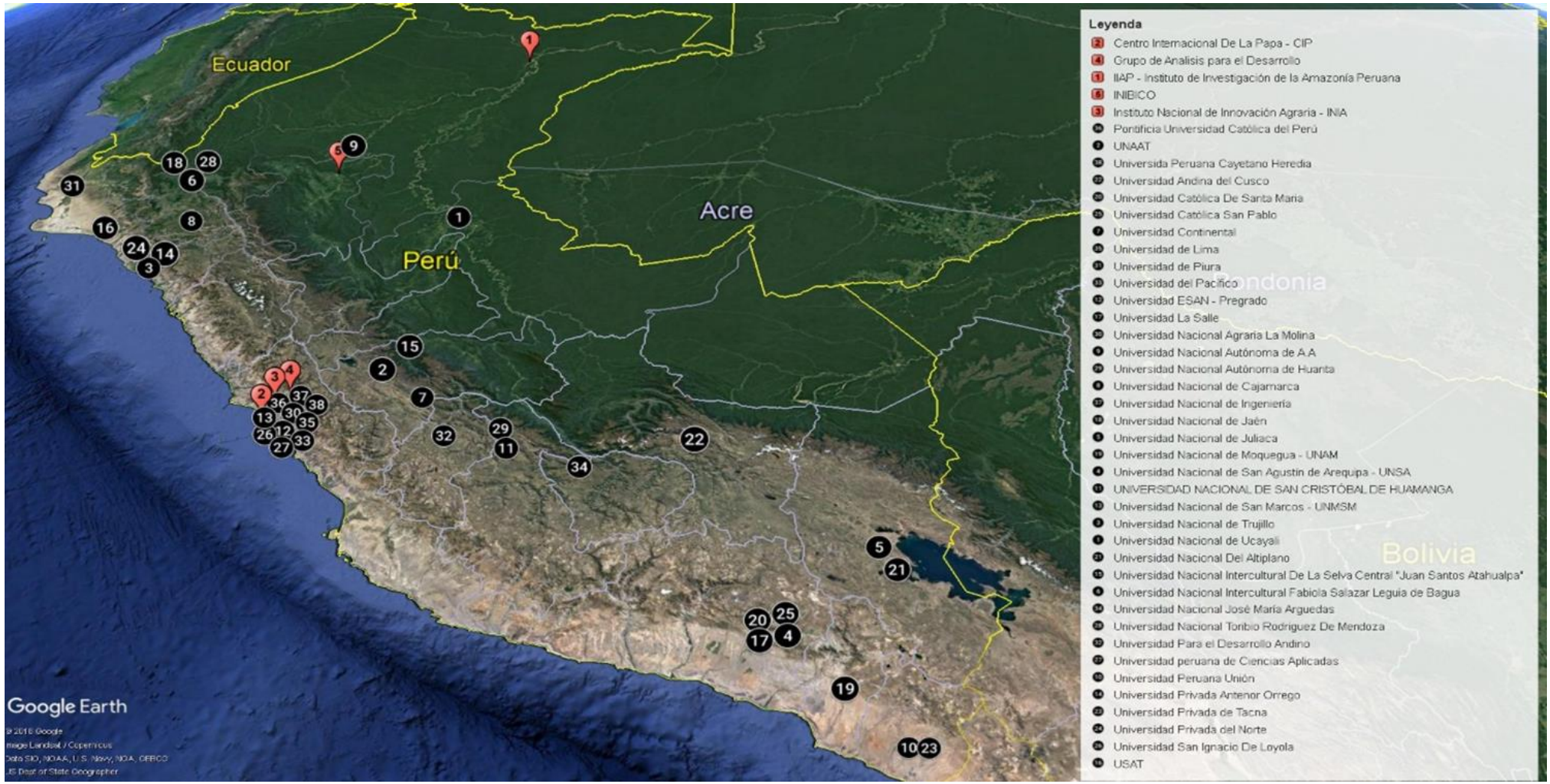
Tuncay Saydam, T. M. (1996). From Networks and Network Management into Services and Services Management. *Journal of Networks and System Management*, vol 4 No 4.

ANEXOS

ANEXO 1.

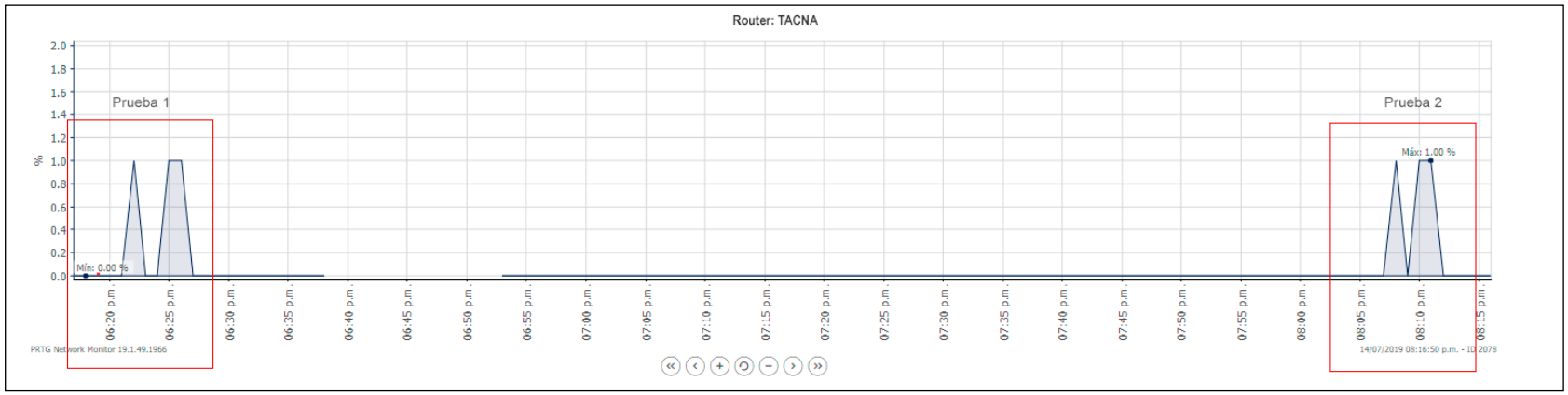
FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	MÉTODOS Y TÉCNICAS
General: ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP para la gestión de Redes Avanzadas? **ESPECÍFICOS:** 1. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de complejidad para la gestión de Redes Avanzadas? 2. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de uso de recursos computacionales para la gestión de Redes Avanzadas? 3. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de seguridad de protocolo para la gestión de Redes Avanzadas? 4. ¿Cuál es la mejor alternativa de configuración con el uso de los protocolos Syslog y SNMP, respecto al nivel de servicios disponibles para la gestión de Redes Avanzadas? 5. ¿Cuál es la alternativa de diseño de topología para la Red Avanzada del Perú (RAAP) para la gestión eficiente?	**General:** Evaluar las alternativas de configuración con el uso de los protocolos Syslog y SNMP para la gestión de Redes Avanzadas para la formulación de una guía de configuración general. **ESPECÍFICOS:** 1. Determinar la mejor alternativa de configuración respecto al nivel de complejidad para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP 2. Determinar la mejor alternativa de configuración respecto al nivel de uso de recursos computacionales para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP. 3. Determinar la mejor alternativa de configuración respecto al nivel de seguridad de protocolo para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP. 4. Determinar la mejor alternativa de configuración respecto al nivel de servicios disponibles para la gestión de Redes Avanzadas con el uso de los protocolos Syslog y SNMP. 5. Diseñar una alternativa de topología de la Red Avanzada del Perú (RAAP) para la gestión de red eficiente.	**General:** La mejor alternativa para la gestión de redes avanzadas es la configuración de Syslog y SNMPv3 de forma complementaria. **ESPECÍFICOS:** 1. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de complejidad de configuración es Syslog y SNMPv3 de forma complementaria 2. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de uso de recursos computacionales es Syslog. 3. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de seguridad de protocolo es la configuración de SNMPv3 4. La mejor alternativa para la gestión de Redes Avanzadas respecto al nivel de servicios disponibles es la configuración de Syslog. 5. La alternativa de diseño de una topología para la Red Avanzada del Perú (RAAP) para la gestión eficiente estará basada en la ubicación de los nodos respecto los tipos y relevancia de instituciones científicas. .	**Independiente:** Protocolos Syslog y SNMP (X)	Complejidad de configuración	• Nivel de complejidad de configuración de SNMP • Nivel de complejidad de configuración de Syslog	**Tipo de Investigación:** Aplicada **Nivel de Investigación:** Cuantitativo **Diseño de Investigación:** Causi-Experimental **Herramientas de recolección de datos:** •Revisión de tesis, libros, internet y publicaciones. •Informes oficiales de la evolución de las topologías de la red avanzada. •Informes y publicaciones de redes avanzadas •Encuestas •Sniffer (wireshark) •Herramienta de Gestión de Red (PRTG) **Software de Emulación:** GNS3.
				Uso de recursos computacionales	• Nivel de uso de CPU de Syslog • Nivel de uso de memoria en Syslog • Nivel de uso de ancho de banda para Syslog • Nivel de uso de CPU de SNMP • Nivel de uso de memoria en SNMP • Nivel de uso de ancho de banda para SNMP	
				Seguridad de protocolos	• Nivel de integridad de Syslog • Nivel de confidencialidad de Syslog • Nivel de integridad de SNMP • Nivel de confidencialidad de SNMP	
				Servicios Disponibles	• Cantidad de Servicios ofrecidos por Syslog. • Cantidad de Servicios ofrecidos por SNMP.	
			Dependiente: Gestión de red (Y)	Eficacia	Información de eventos reportados	
				Eficiencia	Tiempo invertido en gestión de la red	

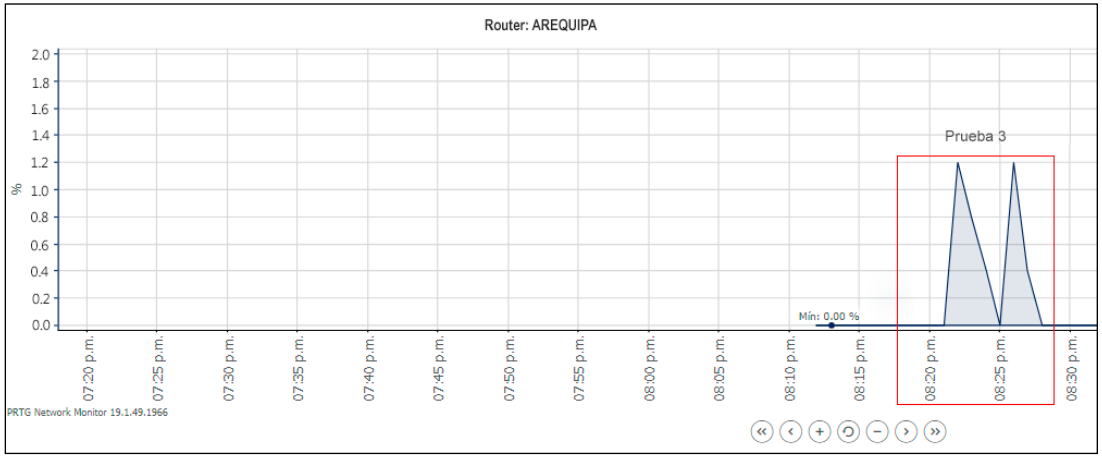
ANEXO 2.

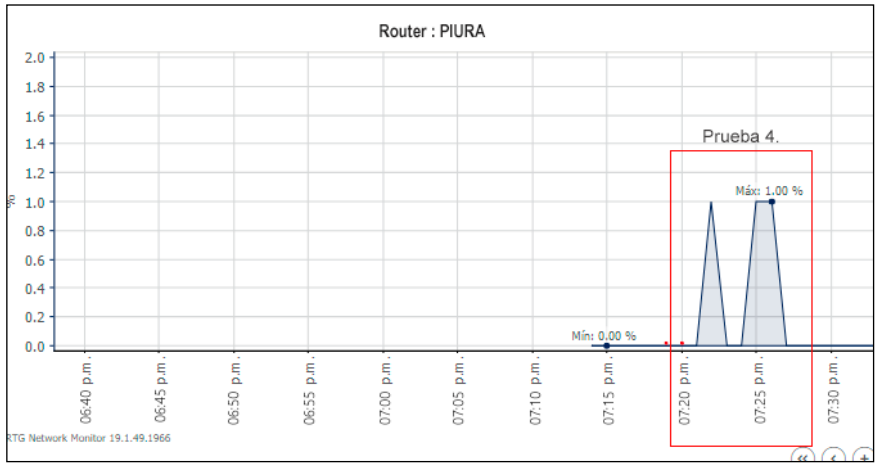

Ecuador
Perú
Acre
Bolivia
Google Earth
Leyenda
Centro Internacional De La Papa - CIP
Grupo de Analisis para el Desarrollo
IIAP - Instituto de Investigación de la Amazonía Peruana
INIBICO
Instituto Nacional de Innovación Agraria - INIA
Pontificia Universidad Católica del Perú
UNAAT
Universida Peruana Cayetano Heredia
Universidad Andina del Cusco
Universidad Católica De Santa Maria
Universidad Católica San Pablo
Universidad Continental
Universidad de Lima
Universidad de Piura
Universidad del Pacífico
Universidad ESAN - Pregrado
Universidad La Salle
Universidad Nacional Agraria La Molina
Universidad Nacional Autónoma de A.A
Universidad Nacional Autónoma de Huanta
Universidad Nacional de Cajamarca
Universidad Nacional de Ingeniería
Universidad Nacional de Jaén
Universidad Nacional de Juliaca
Universidad Nacional de Moquegua - UNAM
Universidad Nacional de San Agustin de Arequipa - UNSA
UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
Universidad Nacional de San Marcos - UNMSM
Universidad Nacional de Trujillo
Universidad Nacional de Ucayali
Universidad Nacional Del Altiplano
Universidad Nacional Intercultural De La Selva Central "Juan Santos Atahualpa"
Universidad Nacional Intercultural Fabiola Salazar Leguia de Bagua
Universidad Nacional José María Arguedas
Universidad Nacional Toribio Rodriguez De Mendoza
Universidad Para el Desarrollo Andino
Universidad peruana de Ciencias Aplicadas
Universidad Peruana Unión
Universidad Privada Antenor Orrego
Universidad Privada de Tacna
Universidad Privada del Norte
Universidad San Ignacio De Loyola
USAT

ANEXO 3.

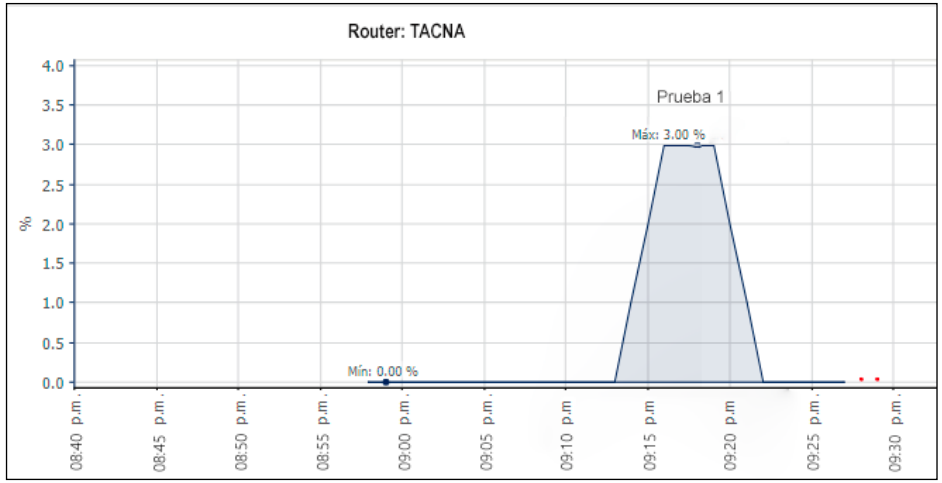
- **Pruebas de consumo de CPU SNMPv2c**

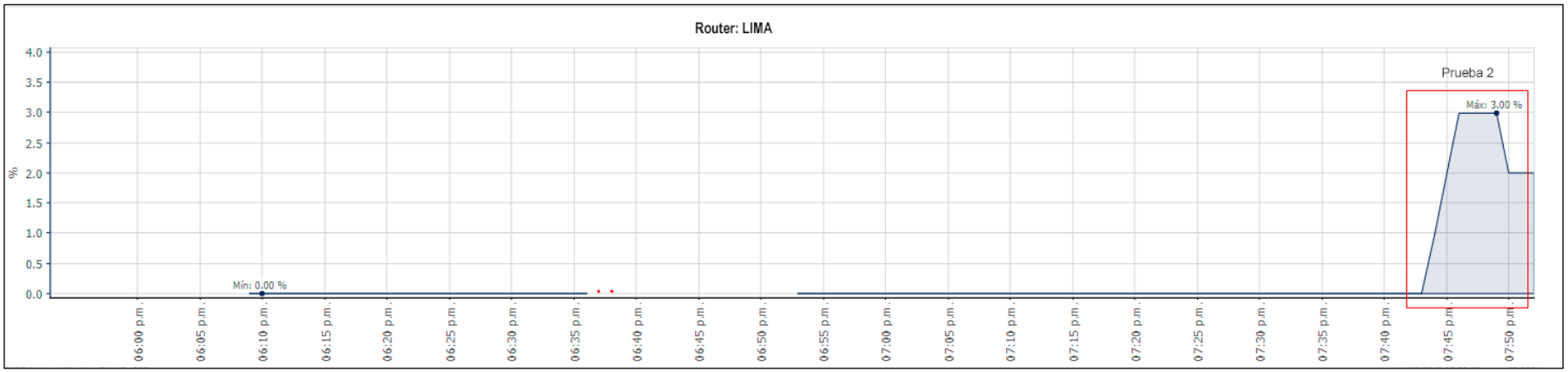


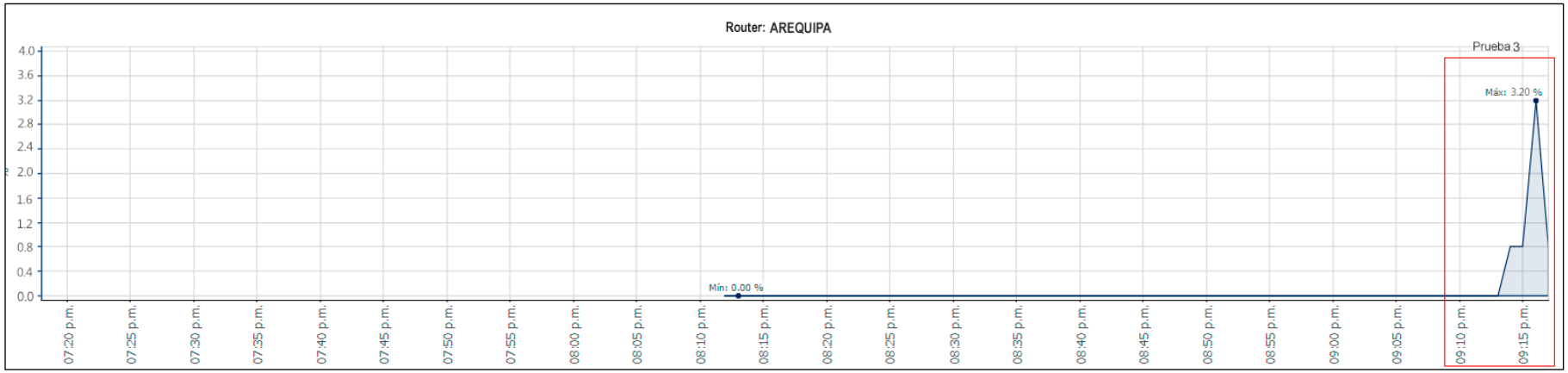


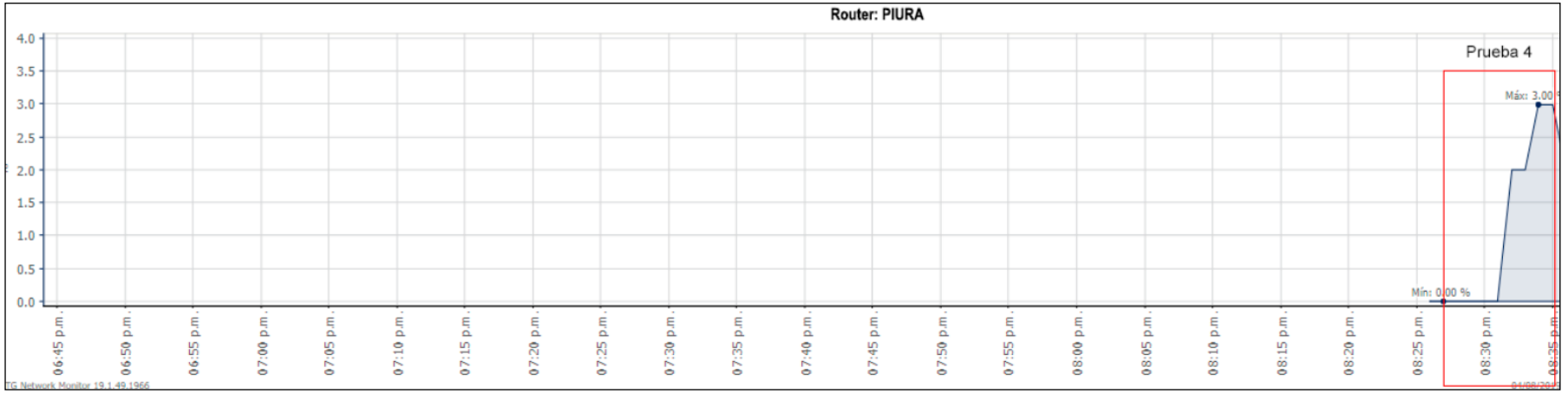


- **Pruebas de consumo de CPU SNMPv3**

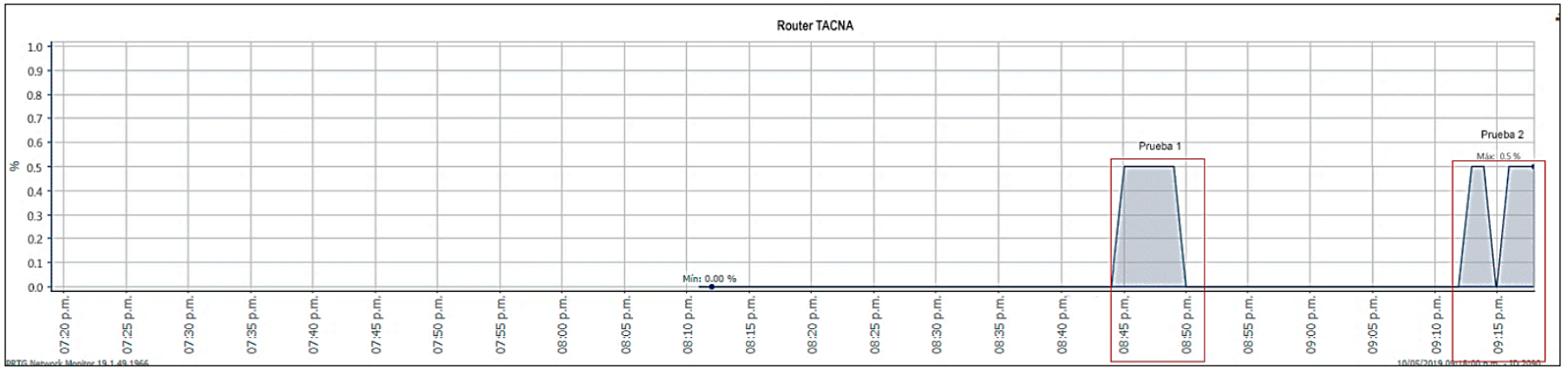


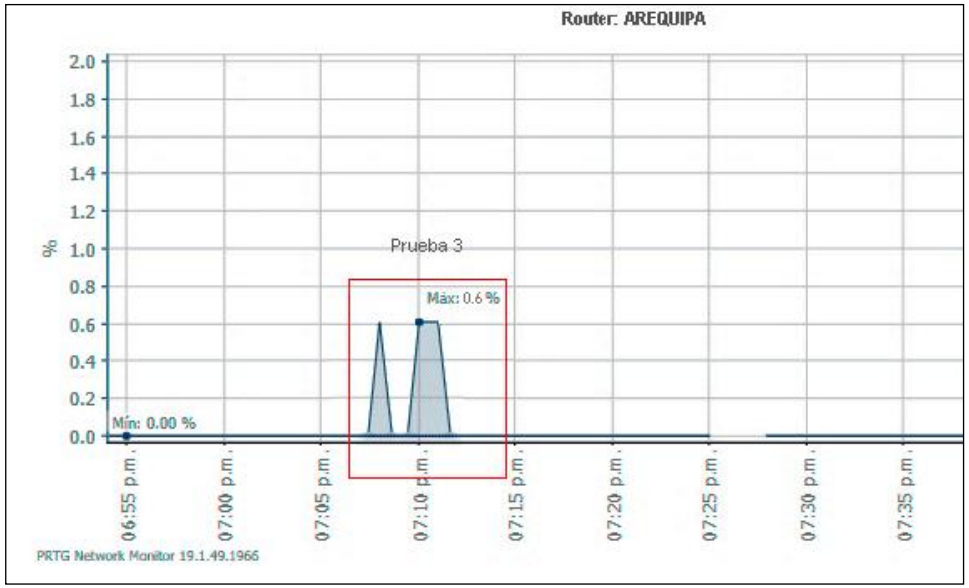


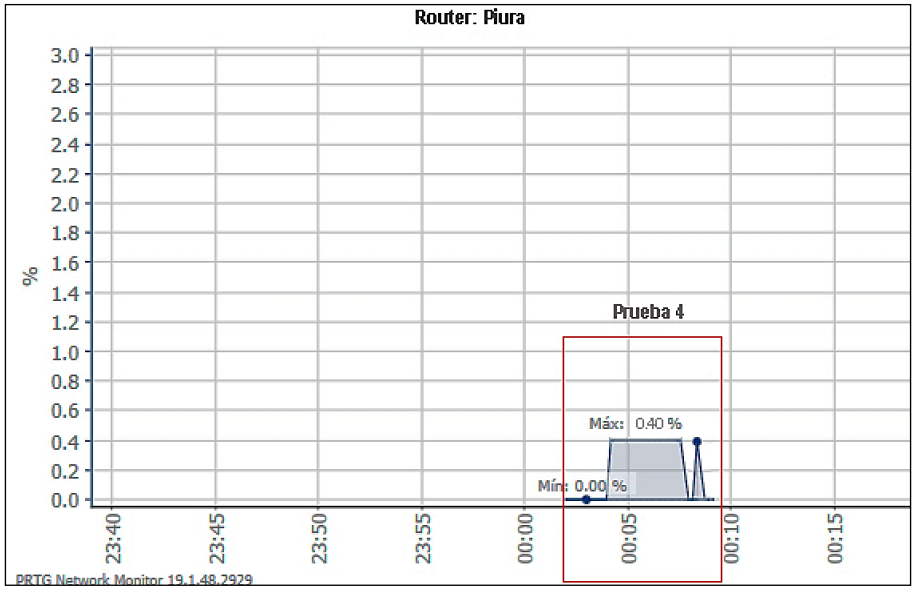

Router: AREQUIPA
Prueba 3
Máx: 3.20 %
Mín: 0.00 %
4.0
3.6
3.2
2.8
2.4
2.0
1.6
1.2
0.8
0.4
0.0
07:20 p.m.
07:25 p.m.
07:30 p.m.
07:35 p.m.
07:40 p.m.
07:45 p.m.
07:50 p.m.
07:55 p.m.
08:00 p.m.
08:05 p.m.
08:10 p.m.
08:15 p.m.
08:20 p.m.
08:25 p.m.
08:30 p.m.
08:35 p.m.
08:40 p.m.
08:45 p.m.
08:50 p.m.
08:55 p.m.
09:00 p.m.
09:05 p.m.
09:10 p.m.
09:15 p.m.


Router: PIURA
Prueba 4
Máx: 3.00
Mín: 0.00 %
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
06:45 p.m.
06:50 p.m.
06:55 p.m.
07:00 p.m.
07:05 p.m.
07:10 p.m.
07:15 p.m.
07:20 p.m.
07:25 p.m.
07:30 p.m.
07:35 p.m.
07:40 p.m.
07:45 p.m.
07:50 p.m.
07:55 p.m.
08:00 p.m.
08:05 p.m.
08:10 p.m.
08:15 p.m.
08:20 p.m.
08:25 p.m.
08:30 p.m.
08:35 p.m.
PG Network Monitor 19.1.49.1966

- **Pruebas consumo de Syslog**

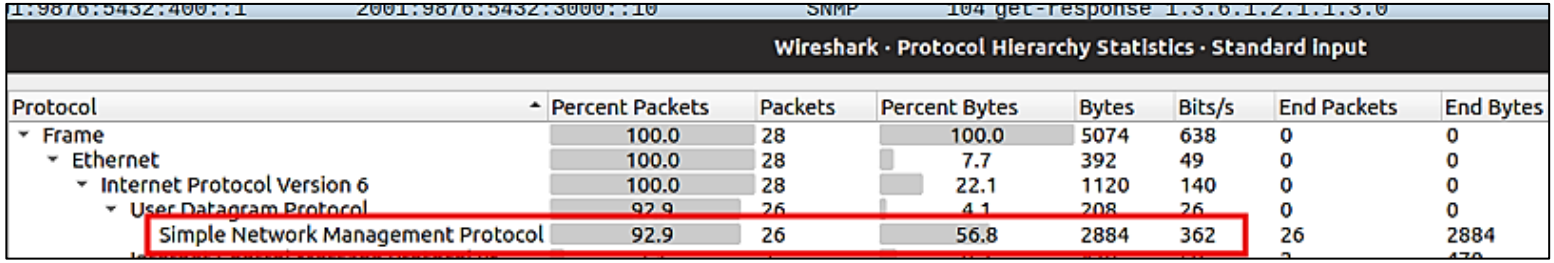


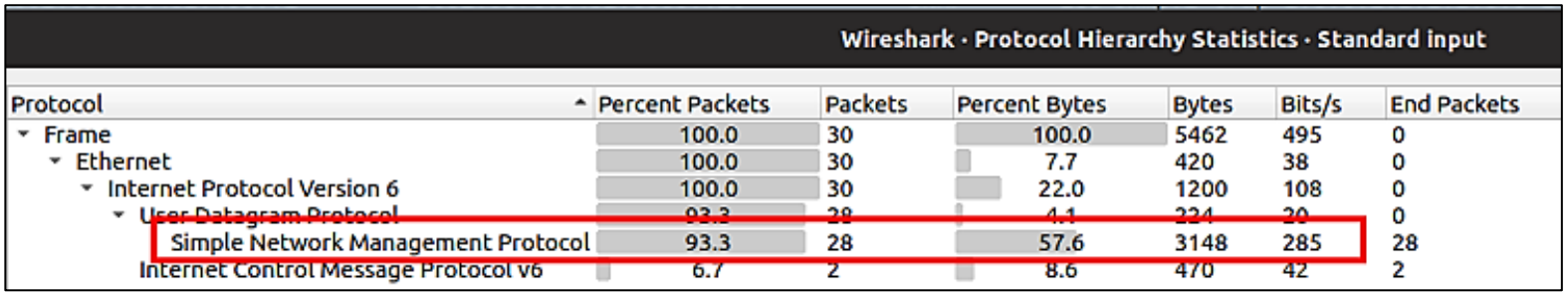


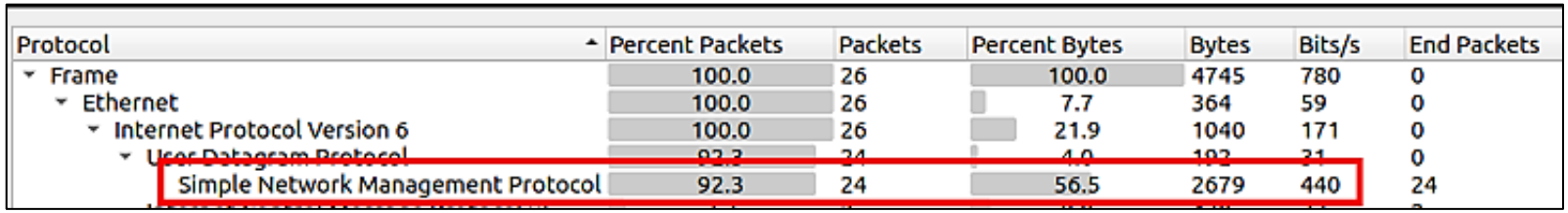


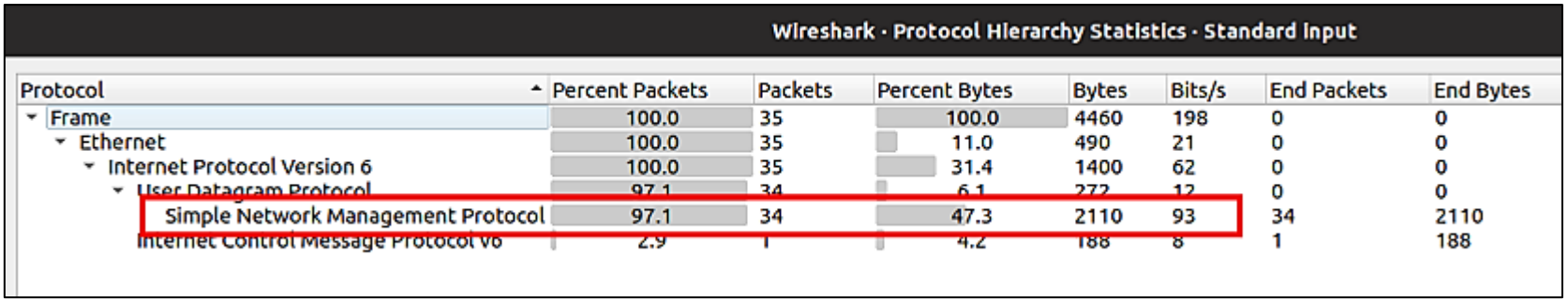
ANEXO 4.

- **Pruebas de uso de memoria SNMPv2c**

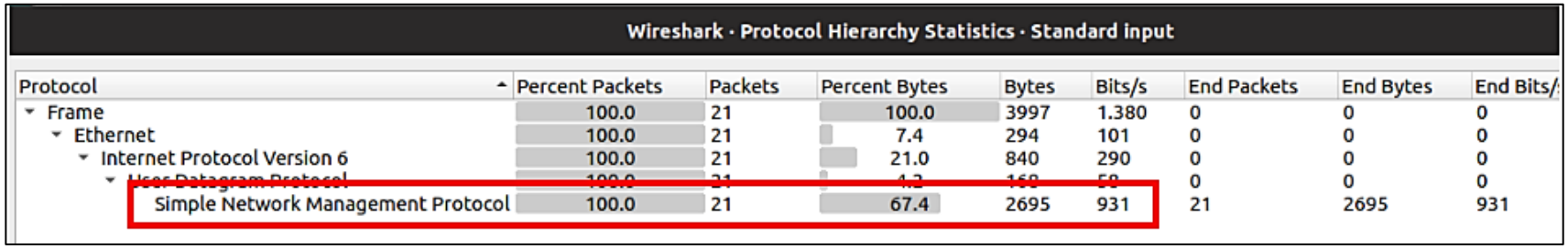








- **Pruebas de uso de memoria SNMPv3**



Wireshark · Protocol Hierarchy Statistics · Standard input

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	46	100.0	10960	751	0	0	0
Ethernet	100.0	46	5.9	644	44	0	0	0
Internet Protocol Version 6	100.0	46	16.8	1840	126	0	0	0
User Datagram Protocol	100.0	46	3.4	368	25	0	0	0
Simple Network Management Protocol	100.0	46	74.0	8108	556	46	8108	556

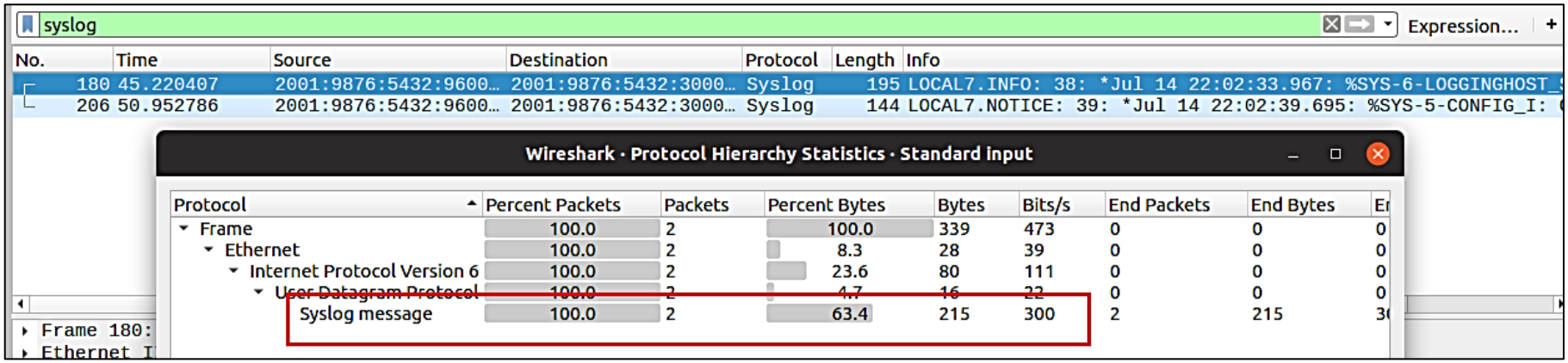
Wireshark · Protocol Hierarchy Statistics · Standard input

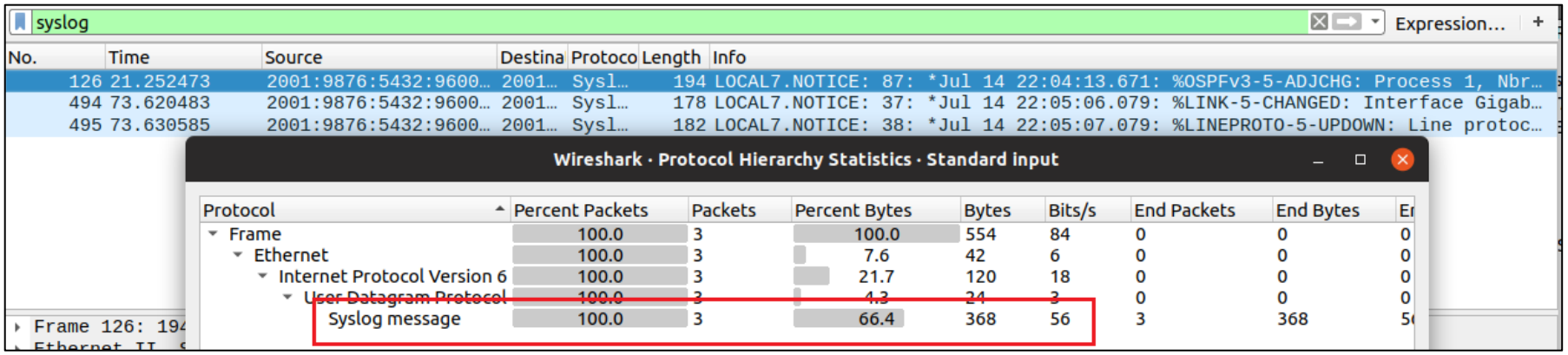
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	22	100.0	4289	851	0	0	0
Ethernet	100.0	22	7.2	308	61	0	0	0
Internet Protocol Version 6	100.0	22	20.5	880	174	0	0	0
User Datagram Protocol	100.0	22	4.1	176	34	0	0	0
Simple Network Management Protocol	100.0	22	68.2	2925	580	22	2925	580

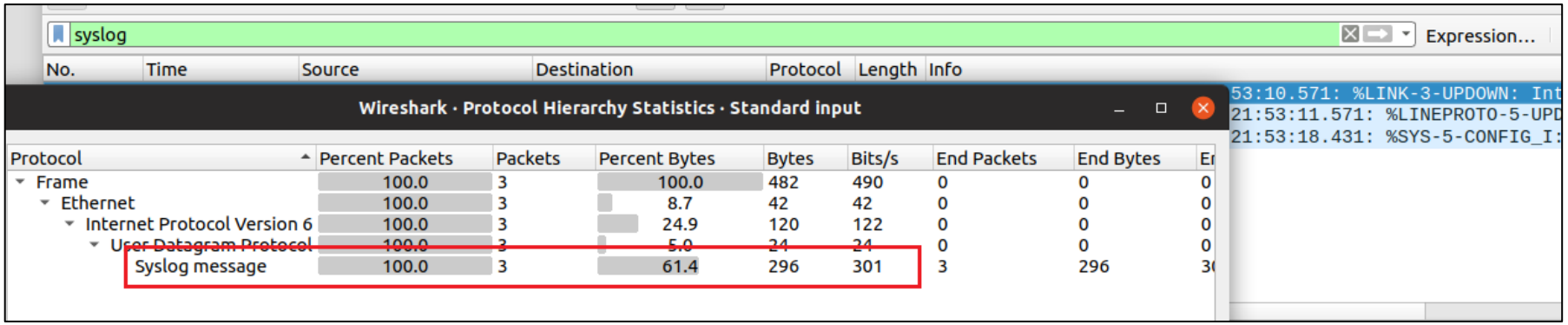
Wireshark · Protocol Hierarchy Statistics · Standard input

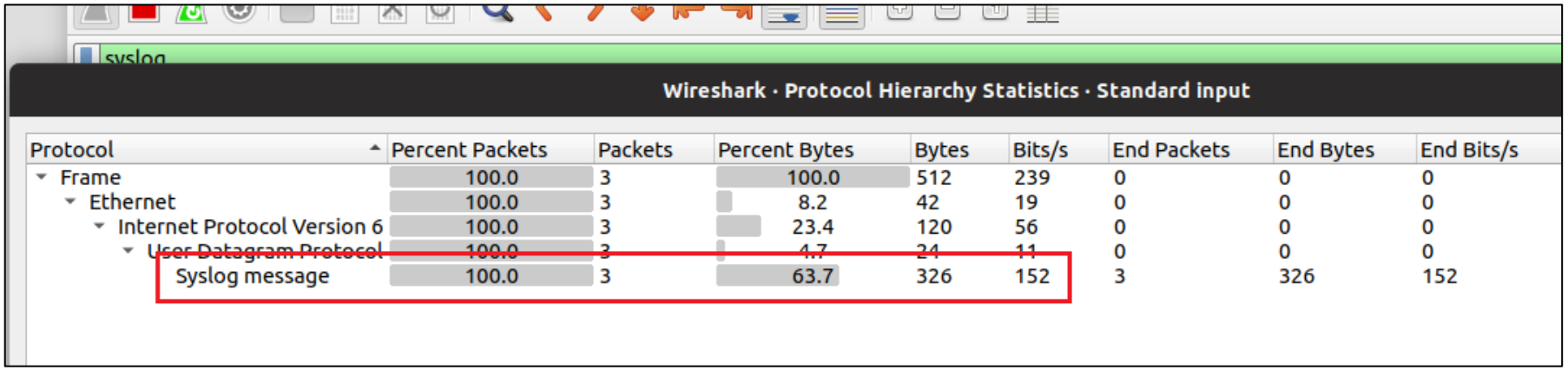
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	42	100.0	9598	927	0	0	0
Ethernet	100.0	42	6.1	588	56	0	0	0
Internet Protocol Version 6	100.0	42	17.5	1680	162	0	0	0
User Datagram Protocol	100.0	42	3.5	336	32	0	0	0
Simple Network Management Protocol	100.0	42	72.9	6994	675	42	6994	675

- **Pruebas de uso de memoria Syslog**






syslog
Expression...
No. Time Source Destination Protocol Length Info
Wireshark · Protocol Hierarchy Statistics · Standard input
53:10.571: %LINK-3-UPDOWN: Int
21:53:11.571: %LINEPROTO-5-UPD
21:53:18.431: %SYS-5-CONFIG_I:
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes
Frame 100.0 3 100.0 482 490 0 0
Ethernet 100.0 3 8.7 42 42 0 0
Internet Protocol Version 6 100.0 3 24.9 120 122 0 0
User Datagram Protocol 100.0 3 5.0 24 24 0 0
Syslog message 100.0 3 61.4 296 301 3 296


syslog
Wireshark · Protocol Hierarchy Statistics · Standard input
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes End Bits/s
Frame 100.0 3 100.0 512 239 0 0 0
Ethernet 100.0 3 8.2 42 19 0 0 0
Internet Protocol Version 6 100.0 3 23.4 120 56 0 0 0
User Datagram Protocol 100.0 3 4.7 24 11 0 0 0
Syslog message 100.0 3 63.7 326 152 3 326 152

ANEXO 5.

- **Pruebas de ancho de banda para SNMPv2c y Syslog**

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
NetBIOS	3008	0 KByte	0 kbit/s	0 kbit/s	0.39 kbit/s
Otros	0	89 KByte	12 kbit/s	0 kbit/s	28 kbit/s
Remote Control	3005	0 KByte	0 kbit/s	0 kbit/s	0.06 kbit/s
SNMP	3007	0.29 KByte	0.09 kbit/s	0 kbit/s	0.11 kbit/s
Syslog	3009	0.14 KByte	0.03 kbit/s	0 kbit/s	0.05 kbit/s

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
NetBIOS	3008	0 KByte	0 kbit/s	0 kbit/s	0.39 kbit/s
Otros	0	89 KByte	12 kbit/s	0 kbit/s	28 kbit/s
Remote Control	3005	0 KByte	0 kbit/s	0 kbit/s	0.06 kbit/s
SNMP	3007	0.30 KByte	0.09 kbit/s	0 kbit/s	0.12 kbit/s
Syslog	3009	0.19 KByte	0.05 kbit/s	0 kbit/s	0.07 kbit/s

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
NetBIOS	3008	0 KByte	0 kbit/s	0 kbit/s	0.39 kbit/s
Otros	0	89 KByte	12 kbit/s	0 kbit/s	28 kbit/s
Remote Control	3005	0 KByte	0 kbit/s	0 kbit/s	0.06 kbit/s
SNMP	3007	0.24 KByte	0.08 kbit/s	0 kbit/s	0.12 kbit/s
Syslog	3009	0.18 KByte	0.04 kbit/s	0 kbit/s	0.07 kbit/s
Tiempo de inactividad	-4				

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
NetBIOS	3008	0 KByte	0 kbit/s	0 kbit/s	0.39 kbit/s
Otros	0	89 KByte	12 kbit/s	0 kbit/s	28 kbit/s
Remote Control	3005	0 KByte	0 kbit/s	0 kbit/s	0.06 kbit/s
SNMP	3007	0.30 KByte	0.11 kbit/s	0 kbit/s	0.13 kbit/s
Syslog	3009	0.19 KByte	0.06 kbit/s	0 kbit/s	0.07 kbit/s
Tiempo de inactividad	-4				

- **Pruebas de ancho de banda para SNMPv3**

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
SNMPv3	0	0.33 KByte	0.17 kbit/s	0 kbit/s	0.17 kbit/s
Tiempo de inactividad	-4				
Total	-1	0.33 KByte	0.17 kbit/s	0 kbit/s	0.17 kbit/s

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
SNMPv3	0	0.40 KByte	0.24 kbit/s	0 kbit/s	0.24 kbit/s
Tiempo de inactividad	-4				
Total	-1	0.40 KByte	0.24 kbit/s	0 kbit/s	0.24 kbit/s

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
SNMPv3	0	0.38 KByte	0.21 kbit/s	0 kbit/s	0.25 kbit/s
Tiempo de inactividad	-4				
Total	-1	0.38 KByte	0.21 kbit/s	0 kbit/s	0.25 kbit/s

Canal	ID	Último valor (volumen)	Último valor (velocidad)	Mínimo	Máximo
SNMPv3	0	0.44 KByte	0.25 kbit/s	0 kbit/s	0.25 kbit/s
Tiempo de inactividad	-4				
Total	-1	0.44 KByte	0.25 kbit/s	0 kbit/s	0.25 kbit/s

ANEXO 6.

GUÍA DE CONFIGURACIÓN BÁSICA DE SNMP

DESCRIPCIÓN GENERAL DE SNMP

SOBRE SNMP

El protocolo simple de administración de red (SNMP) es un protocolo de capa de red que realiza operaciones de gestión de red mediante una conexión de Ethernet utilizando protocolo de datagramas de usuario/protocolo de Internet (UDP/IP).

El protocolo simple de administración de redes permite:

- Que se informe de los problemas posibles al administrador de sistemas.
- Que los administradores de sistemas consulten información sobre configuración, funcionamiento y estadísticas.

AGENTES DE GESTIÓN Y CONTROL DE PUERTOS

SNMP usa datagrama de usuario (UDP) con los siguientes puertos:

- 161 para el agente
- 162 para el host

El host puede enviar solicitudes desde cualquier puerto disponible al agente en el puerto 161. Luego, el agente responde al host solicitante a ese puerto de origen.

El agente genera capturas o notificaciones y las envía desde cualquier puerto disponible al gestor en el puerto 162.

CONFIGURACIÓN DE SNMPV2C PARA DISPOSITIVOS DE RED

VARIABLES DE SNMPV2C

ARGUMENTO	VARIABLE	DESCRIPCIÓN
Community	*communitystring*	Cadena de comunidad de agente. Cuando se define como pública, se aceptarán las solicitudes que provienen de cualquier cadena.
Contact	*contactString*	Nombre de contacto para servicio
Host	*host*	Dirección IP de host

HABILITAR SNMPV2C

① CONFIGURACIÓN DE LA COMUNIDAD

Con permiso de lectura:

```
Router(config)# snmp-server community “communitystring” ro
```

Con permiso de escritura (Opcional):

```
Router(config)# snmp-server community “communitystring” rw
```

② COMANDOS DE INFORMACIÓN DESCRIPTIVA

```
Router(config)# snmp-server location "locationstring"
```

```
Router(config)# snmp-server contact "contactstring"
```

③ ESPECIFICA LA DIRECCIÓN IPV6 DEL SERVIDOR

```
Router(config)#snmp-server host “host” version 2c "communitystring"
```

④ HABILITAMOS TODAS LAS TRAPS PREDETERMINADAS DISPONIBLES

```
Router(config)# snmp-server enable traps
```

CONFIGURACIÓN DE SNMPV3 PARA DISPOSITIVOS DE RED

VARIABLES DE SNMPV3

ARGUMENTO	VARIABLE	DESCRIPCIÓN
name	*name*	Nombre asignado al usuario de SNMP.
auth	*auth_protocol*	Protocolo de autenticación para usuarios y hosts que reciben capturas. MD5 o SHA.
authPass	*auth_password*	Contraseña de autorización.
priv	*privacy_protocol*	Tipo de protocolo de privacidad: DES o AES.
privPass	*priv_password*	Contraseña de cifrado que es la clave privada para cifrado.
Host	host	Dirección IP de host

PROCEDIMIENTO DE CONFIGURACIÓN DE SNMPV3 NIVEL "*AUTHPRIV*"

① CONFIGURACIÓN DEL GRUPO Y TIPO DE SEGURIDAD

En modo de configuración global, ingrese:

```
Router(config)# snmp-server groupraap v3 priv
```

② AÑADIENDO USUARIO

Al especificar el nombre de usuario también definimos la autenticación y el tipo de cifrado:

```
Router(config)# snmp-server user "name" "username" v3 auth md5 "auth_password" priv des "priv_password"
```

③ ESPECIFICA LA DIRECCIÓN IPV6 DEL SERVIDOR

Además de especificar el host, también se habilita la versión 3 de SNMP y el tipo de seguridad que tiene el usuario que en este caso "priv":

```
Router(config)#snmp-server host "host" version 3 priv "priv_password"
```

④ HABILITAMOS TODAS LAS *TRAPS* PREDETERMINADAS DISPONIBLES

```
Router(config)# snmp-server enable traps
```

GUÍA DE CONFIGURACIÓN BÁSICA DE SYSLOG

CONFIGURACIÓN DE SYSLOG PARA DISPOSITIVOS DE RED

SOBRE SYSLOG

El protocolo Syslog envía mensajes del sistema y el resultado del comando *debug* a un proceso de registro local interno del dispositivo. La forma en que el proceso de registro administra estos mensajes y resultados se basa en las configuraciones del dispositivo. Los destinos comunes para los mensajes de Syslog incluyen lo siguiente:

- Búfer de registro (RAM dentro de un router o switch)
- Línea de consola
- Línea de terminal
- Servidor de syslog

Esta guía de configuración se basa únicamente en el proceso para que los mensajes de Syslog puedan enviar a través de la red a un servidor de Syslog.

INFORMACIÓN SOBRE LA CONFIGURACIÓN

Para mejorar la depuración y la administración de eventos se haga en tiempo real, los mensajes de Syslog deben de ser registrados con la hora y la dirección de origen de los mensajes Syslog. Para lograr tener actualizado la hora y fecha puede lograr de dos maneras:

- Configuración manual mediante el comando clock set
- Configuración automática mediante el protocolo NTP

CONFIGURACIÓN DE *ROUTER* Y *SWITCH* PARA LOS CLIENTES SYSLOG

① CONFIGURACIÓN DEL HOST DE DESTINO.

El comando *logging* establecerá la dirección IP que recepcionara el *log* del dispositivo; En modo de configuración global, ingrese:

- Comando para IPv6

```
Router(config)# logging host IPv6 “host”
```

- Comando para IPv4

```
Router(config)# logging host IPv6 “host”
```

② ESTABLECER NIVEL DE DETALLE DEL LOG

Establecer el nivel de detalle, dependerá si desea que la información registrada del log sea limitada algún nivel; de no ser el caso, podría omitir este comando y ser notificado hasta el nivel 7, que es el nivel más alto. En el siguiente comando a manera de ejemplo se establecerá el nivel 7 *(debugging).*

```
Router(config)# logging trap 7
```

③ CONFIGURACIÓN DE LA INTERFAZ (OPCIONAL)

De manera opcional, configure la interfaz de origen con el comando del modo de configuración global.

```
Router(config)# logging source-interface “interface-type interface number”
```