Universidad Zaragoza
1542

Trabajo Fin de Grado

IMPLEMENTACIÓN DE SERVIDOR SNMP EN LOS NODOS V4.5 DE SC2NET-D PARA SU UTILIZACIÓN EN EJERCICIOS

Javier Sánchez Siles

Dr. D. Alejandro Mosteo Chagoyen

Tte. D. Miguel Castiblanque Manzaneque

Centro Universitario de la Defensa-Academia General Militar

2022

Agradecimientos

En primer lugar, me gustaría dar gracias al Director Académico, D. Alejandro Mosteo Chagoyen, que, gracias a su esfuerzo y dedicación, me ha aportado todas las correcciones y directrices necesarias en este trabajo, facilitando así mi trabajo y esfuerzo, y siendo la figura principal para poder llevar a cabo todo este proyecto.

A su vez, me gustaría agradecer también a la Brigada Extremadura XI. Dar gracias tanto a cuadros de mandos como personal de tropa, gracias a los cuales he tenido la oportunidad de aprender tanto en el ámbito militar como a nivel personal durante el periodo de prácticas externas en el cual he estado en dicha unidad. Así mismo, agradecer por la atención y dedicación que me han dado, proporcionándome todas las facilidades necesarias para la realización de este proyecto.

Por último, me gustaría dar especial gracias a toda mi familia y conocidos más cercanos, los cuales me han prestado todo su apoyo y ánimos no solo de cara a la realización de este proyecto, si no también, durante todo el curso académico, desde que tuve la oportunidad de iniciarlo hace más de cuatro años.

RESUMEN

El siguiente trabajo surge tras observar la necesidad de las unidades de poder determinar cuáles son los causantes de que, durante la realización de cualquier tipo de ejercicio, la red se encuentre colapsada, no pudiendo funcionar adecuadamente.

Como solución a este problema se ha contemplado la implementación de un sistema de monitorización en los nodos de SC2NET, los cuales gestionan y coordinan toda la red y servicios de la unidad militar.

Así, gracias a la implementación de un sistema de monitorización, se podrá detectar, analizar y proporcionar posibles soluciones a aquellos dispositivos o áreas que hacen un uso ineficaz de la red, provocando un tráfico excesivo en esta o con un elevado uso de los recursos, de forma que la red no pueda soportar esta carga, llegando en ocasiones a colapsar.

Dicho sistema de monitorización consistirá en la implementación de un servidor utilizando el protocolo SNMP, el cual está diseñado específicamente para la monitorización y permitirá poner solución a este problema.

Para llevar a cabo este proyecto, ha sido necesaria la división de este en dos partes. La primera parte se basa en comprender el funcionamiento a nivel usuario de todos los elementos implicados. Es decir, es necesario conocer en qué consiste la monitorización, cómo funciona el protocolo SNMP y para qué lo vamos a emplear, y como es la estructura de los nodos de SC2NET.

La segunda parte consiste en la realización de las pruebas necesarias para poder implementar dicho protocolo como servidor de SNMP y utilizar ese servidor para monitorizar todos los dispositivos que comparten la red y poder programar alertas ante cualquier incidencia, como puede ser el caso de que un dispositivo sature la red o simplemente que esta se encuentre caída.

En resumen, este trabajo pretende fomentar la creación de un sistema de monitorización que, sumado a alguna aplicación de ámbito civil o militar, permita la detección y prevención de los dispositivos y recursos que dificultan el buen funcionamiento de la red, lo que conlleva a la paralización o suspensión de los ejercicios que se llevan a cabo, no solo por las unidades de transmisiones, si no también por el resto de unidades implicadas durante la maniobra.

PALABRAS CLAVE

Sistema de monitorización, protocolo SNMP, Nagios, nodo SC2NET, redes.

ABSTRACT

The following work arises after observing the need of the units to be able to determine which are the causes that, during the realization of any type of exercise, the network collapsed, not being able to function properly.

As a solution to this problem, the implementation of a monitoring system has been contemplated in the SC2NET nodes, which manage and coordinate the entire network and services of the military unit.

As a result, thanks to the implementation of a monitoring system, it will be possible to detect, analyze and provide possible solutions to those devices or areas that make ineffective use of the network, causing excessive traffic in it or with a high use of resources, so that the network cannot support this load, sometimes collapsing.

This monitoring system will consist of the implementation of a server that uses the SNMP protocol, which is specifically designed for monitoring, and that will allow to solve this problem.

To carry out this project, it has been necessary to divide it into two parts. The first part is based on understanding the operation at the user level of all the elements involved. That is, it is necessary to know what monitoring consists of, how the SNMP protocol works and what we are going to use it for, and how is the structure of the SC2NET nodes.

The second part consists of carrying out the necessary tests to be able to implement this protocol as an SNMP server and use that server to monitor all the devices that share the network and be able to program alerts in the event of any incident, such as the case that a device saturates the network or simply that it is down.

In summary, this work is intended to promote the creation of a monitoring system that, added to civilian or military applications, allows the detection and prevention of the devices and resources that hinder the proper functioning of the network, which leads to the paralysis or suspension of the exercises that are carried out, not only for the transmission units, but also for the rest of the units involved during the military exercises.

KEYWORDS

Monitoring system, SNMP protocol, Nagios, SC2NET node, networks.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

Acrónimo	Significado en español	Significado en inglés
APP	Área de Panes y Políticas	-
BDT	Base de Datos Táctica	-
C2IS	Sistemas de Información de Mando y Control	Command and Control Information System
CCNA	-	Cisco Certified Network Associate
CDO	Director de Datos	-
CECOM	Centro de Comunicaciones	-
CESTIC	Centro de Sistemas y Tecnologías de la Información y Comunicaciones	-
CTO	Director de Tecnología	-
COO	-	Chief Operating Office
DAFO	Debilidades, Amenazas, Fortalezas y Oportunidades	Strengths, Weaknesses, Opportunities and Threats
DISEVAR	División Diseño y Evaluación de Arquitecturas	-
DISEGINFO	División Seguridad de la Información	-
DIVINDES	División Infraestructuras y Desarrollo	-
DIVOPER	División Operación de RED	-
DNS	Sistema de Nombres de Dominio	Domain Name System
ICMP	Protocolo de mensajes de control de Internet	Internet Control Message Protocol
IPV4	Protocolo de Internet versión 4	Internet Protocol version 4
MAC	Control de Acceso a Medios	Media Access Control
MDEF	Ministerio de Defensa	-

MIB	Bases de Información de Gestión	Management Information Base
NetBIOS	Sistema de Entrada Salida Básica de Red	Network Basic Input/ Output System
NMS	Sistemas Administradores de Red	Network Management Systems
OCCP	Oficina Central de Control de Procesos	-
OCIO	Oficina del Director de Información	-
OID	Identificador de Objeto	Object Identifier
OTAN	Organización del Tratado Atlántico Norte	North Atlantic Treaty Organization
RFC	-	Request for Comments
SAI	Sistema de Alimentación Ininterrumpida	Uninterruptible Power Supply
SAAS	Software como Servicio	Software as a Service
SC2NET	Sistema de Mando y Control Nacional del Ejército Tierra	-
SC2NET-D	Sistema de Mando y Control Nacional del Ejército Tierra Desplegable	-
SC2NET-CGP	Sistema de Mando y Control Nacional del Ejército Tierra de Cuartel General Permanente	-
SEGER	Secretaría General	-
SIMACET	Sistema de Información para el Mando y Control del Ejército Tierra	-
SNMP	Protocolo Simple de Administración de Red	Simple Network Management Protocol
SYLOG	Protocolo de Registro del Sistema	System Logging Protocol
UEDEC	Unidad de Estrategia, Demanda y Calidad	-
UGE	Unidad Gestión Económico-Financiera	-

UPERLOG	Unidad de Personal, Logística e Infraestructura	-
WAN-PG	Red de área amplia de propósito general	-

1. INTRODUCCIÓN

Las unidades de transmisiones del Ejército de Tierra son aquellas que tienen como objetivo establecer, gestionar y mantener los sistemas de información y telecomunicación necesarios, con el objetivo de proporcionar al jefe una herramienta adecuada para que este pueda ejercer la función del mando.

El Sistema de Mando y Control del Ejército de Tierra (SIMACET) facilita al jefe militar la herramienta necesaria para la dirección, planeamiento y conducción de las operaciones, además de proporcionarle una visión clara y concisa del escenario de operaciones.

Recientemente, la denominación de SIMACET ha cambiado a SC2NET, aunque todavía es muy frecuente emplear el término SIMACET.

El SIMACET se materializa físicamente mediante una serie de nodos interconectados entre sí a través de los sistemas de telecomunicación necesarios, formando una amplia red, que permite el intercambio de información entre los diferentes puestos de mando.

Durante la realización de las maniobras o cualquier ejercicio de ámbito militar, se ha detectado un problema en relación a un tráfico excesivo en la red o uso elevado de los recursos, por lo cual la red se satura, haciendo que no funcione como es debido, llegando en ocasiones a hacer que toda esta se encuentre inutilizable.

Como consecuencia, para la restauración del normal funcionamiento de la red, se requiere de personal y tiempo para poder solventar las incidencias ocurridas. Es por ello, que este exceso de tiempo y personal implica la suspensión temporal de cualquier tipo de actividad que se vea involucrada con el uso de la red.

La principal solución que se contempla y ha sido el objeto de estudio de este trabajo, es la implementación de un sistema de monitorización. Estos sistemas permiten la rápida localización y prevención de cualquier tipo de incidencia en la red.

De hecho, es tal su importancia, que no solo llegan a utilizarse en el ámbito militar. También en muchas empresas o redes domésticas se utilizan sistemas de monitorización, ya que proporcionan una gran ventaja de cara a solucionar cualquier mal funcionamiento en la red.

Con el objetivo de proponer una solución más rápida y eficaz para evitar todos los problemas que conlleva la falta de un servicio o la caída de la red, se pretende abordar este problema mediante el uso de un sistema de monitorización que, no solo sea utilizado durante la realización de ejercicios de las unidades, si no, también durante el desarrollo de todo tipo de misiones de carácter internacional.

1.1. Contexto y justificación

El siguiente proyecto ha sido realizado durante el transcurso de las prácticas externas de quinto curso de la Academia General Militar.

Estas prácticas han sido realizadas en la Compañía de Transmisiones encuadrada en el Batallón de Cuartel General de la Brigada Extremadura XI.

El motivo de este proyecto radica en la necesidad de implementar un sistema de monitorización de redes y recursos capaz de localizar, detectar y prevenir los principales causantes que conllevan al colapso de la estructura de la red, con el objetivo de restaurar su normal funcionamiento a la mayor brevedad posible.

1.2. Estructura de la memoria

La memoria de este proyecto comienza con una introducción con ayuda del manual del Mando de Adiestramiento y Doctrina sobre el establecimiento y empleo de SIMACET. Además, en esta parte se muestra el contexto y justificación de este proyecto.

Posteriormente, en el capítulo 2, se muestran tanto los objetivos y alcance del proyecto, como las herramientas utilizadas, es decir, la metodología.

A continuación, en el capítulo 3, se recogen los antecedentes y marco teórico del proyecto. Debido al carácter técnico de este proyecto, en este apartado se hace un primer acercamiento a los sistemas de monitorización y al empleo del protocolo SNMP (Protocolo Simple de Administración de Red).

Tras todo ello, en el capítulo 4, se realiza un desarrollo del proyecto, mostrando los resultados obtenidos. Para ello, se explica brevemente la utilidad del proyecto aplicado al ámbito militar, para posteriormente proceder a la realización de pruebas y muestra de resultados obtenidos.

Por último, en el capítulo 5, se recogen las conclusiones obtenidas de este proyecto y se plantean las líneas futuras del proyecto.

2. OBJETIVOS Y METODOLOGÍA

El objetivo general de este proyecto es la implementación de un sistema de monitorización en los nodos de SC2NET, por el cual se pretende abordar el problema de falta de medios y recursos para la detección y prevención de fallos en la red, gracias a la facilidad que suponen los sistemas de monitorización de cara a localizar el foco del mal funcionamiento de cualquier dispositivo.

2.1. OBJETIVOS Y ALCANCE

Para la obtención del objetivo general de este proyecto se han fijado los siguientes objetivos específicos.

- Comprender en qué consiste la monitorización y qué ventajas nos aporta.
- Conocer el funcionamiento del protocolo SNMP, el principio de funcionamiento de la mayoría de los sistemas de monitorización.
- Analizar la estructura del nodo de SC2NET, donde se va a implementar el sistema de monitorización.
- Aprender a instalar el protocolo SNMP en el nodo de SC2NET, para poder proceder posteriormente a la monitorización mediante el empleo de algún tipo de aplicación al efecto.
- Realizar un breve estudio de posibles aplicaciones para el ámbito de la monitorización.

El alcance de este proyecto llega hasta el uso de una aplicación para la monitorización, mostrando sus principales características y funciones. Para ello, se establecen los siguientes hitos: implementación de una máquina virtual con las características de SNMP en el nodo; incluir la propia máquina virtual en la red, lo cual es necesario para que la máquina conozca todos los dispositivos de la red; y, por último, uso de una aplicación para la monitorización y muestra de resultados en el nodo.

Uno de los hitos que no se ha podido alcanzar del modo previsto ha sido la verificación de resultados mediante una aplicación en el nodo. Esto se debe a que una vez que se instaló en el servidor, se necesitaba de una aplicación externa que notificase de las incidencias producidas. Pese a que existe una gran variedad de aplicaciones con esta función, muchas de ellas son de pago, mientras que otras no podíamos contar con ellas debido a las políticas de seguridad impuestas por el Parque y Centro de Hardware y Software. Pese a ello, como alternativa se ha procedido a verificar los resultados de la misma forma, pero independiente del nodo, es decir, desde un ordenador personal.

Para la realización de estas tareas es necesario disponer de mínimo un ordenador, ya sea personal o normalizado, de un nodo de SC2NET y de la licencia o prueba gratuita de la aplicación que se va a emplear.

2.2. METODOLOGÍA

Dentro de la metodología empleada para el desarrollo de este proyecto, destacan dos herramientas cualitativas, ya que permiten obtener datos que no se pueden medir, pero permiten llegar a una conclusión. A su vez, también se han empleado herramientas cuantitativas, gracias

a las cuales se realiza una comparación de valores medibles en diferentes aspectos.

Las herramientas cualitativas utilizadas han sido, la realización de entrevistas personales y el desarrollo de un análisis DAFO.

La entrevista personal ha sido una herramienta que ha permitido conocer las necesidades de la unidad en lo que respecta a la monitorización. Para ello, se ha realizado una entrevista personal al personal más experimentado del área de SIMACET de la unidad para conocer los motivos por los que es necesario la implementación de un sistema de monitorización.

Además, gracias a otra entrevista personal realizada (ver anexo III), he podido contrastar el uso de la aplicación Nagios, en su versión militar, con las aplicaciones civiles de monitorización. Ya que el uso de Nagios estaba limitado, tal cual se indica más adelante, he podido realizar un breve acercamiento a este, gracias al uso que sí han podido realizar el personal entrevistado durante su participación en una operación militar de carácter internacional, en concreto en Mali.

Es por ello, que, gracias a la realización de entrevistas personales, se ha llegado a la conclusión de la vital importancia de este proyecto ya que todo el personal entrevistado coincide en que, debido a los constantes fallos e interrupciones en los servicios, es necesario la implementación de un servidor que permita conocer dónde se encuentran los principales causantes de estos fallos.

Además, esta herramienta nos ha permitido tener una idea sobre la experiencia previa y conocimiento de la unidad en lo que respecta a la monitorización.

Por otro lado, previa a las pruebas de implementación de SNMP, se ha realizado un análisis DAFO, con el objetivo de conocer las debilidades, amenazas, fortalezas y oportunidades que suponen la implementación de un servidor SNMP en un nodo SIMACET.

Esta herramienta no solo proporciona un análisis interno y externo sobre las características de este proyecto. También, permite que todos los miembros del área de SIMACET puedan conocer principalmente las amenazas y debilidades que suponen la implementación de este proyecto, para que así, resulte más fácil el desarrollo de posibles mejoras de cara a un futuro.

El análisis DAFO, junto con las entrevistas personales, permiten conocer los principales motivos por los cuales es necesario un sistema de monitorización, no solo en esta unidad, sino también, en la mayoría de unidades militares de España.

Por otro lado, dentro de las herramientas cuantitativas, se ha realizado un cuadro comparativo donde se han comparado diferentes aplicaciones para la monitorización de redes.

Así, gracias a esta herramienta, se puede llegar a realizar un estudio más en profundidad acerca de la adquisición de una de estas aplicaciones, pudiendo comparar entre estas, los diferentes precios en su adquisición, el número máximo de dispositivos que son capaces de monitorizar o hasta si disponen de una versión gratuita de cara a hacer pruebas.

Por último, también se ha utilizado como herramienta referencias bibliográficas. En concreto, la principal referencia bibliográfica se observa en la información adquirida acerca del protocolo SNMP.

Esta información procede del curso *Cisco Certified Networking Associate* (CCNA), el cuál es una empresa que proporciona gran variedad de certificaciones dentro del ámbito de las tecnologías y de la información. Además, CCNA es una de las principales fuentes en el ámbito militar de cara a la realización de cursos orientados a la enseñanza y perfeccionamiento, especialmente en las unidades de transmisiones.

También, destaca como referencia bibliográfica los manuales del Mando de Adiestramiento

y Doctrina empleados para la obtención de la información acerca de la estructura y uso del nodo de SIMACET.

3. ANTECEDENTES Y MARCO TEÓRICO

La monitorización es el conjunto de sistemas, cuya función consiste en comprobar constantemente si en una red de sistemas hay un mal funcionamiento, ya sea porque el sistema no trabaja a la velocidad adecuada o por algún tipo de fallo en el normal funcionamiento de este. El objetivo no se queda solamente ahí, pues tratan de informar al administrador a la mayor brevedad posible para que este tome acción en la detección y resolución de cualquier tipo de anomalía (Cisco, 2022).

Su funcionamiento se basa en el uso de protocolos. Estos son el conjunto de todas las instrucciones necesarias para que los dispositivos de la red se puedan comunicar entre ellos. Así, el hardware de red no puede transmitir datos sin estos protocolos (Cisco, 2022).

Los sistemas de monitorización de redes utilizan diferentes protocolos para la detección, informe y prevención de los errores en la red. Hay diferentes protocolos (ver tabla 1).

SNMP (Simple Network Management Protocol)	*Este protocolo usa un sistema de llamada y respuesta para comprobar el estado de los dispositivos. SNMP se puede usar para monitorear el estado y la configuración de los sistemas.*
ICMP (Internet Control Message Protocol)	*Este protocolo permite enviar información de operaciones por IP para posteriormente generar mensajes de error ante fallas de dispositivos.*
Cisco Discovery Protocol	*Este protocolo facilita la administración de dispositivos de Cisco al detectar estos dispositivos, determinar su configuración y permitir que los sistemas usen diferentes protocolos de capa de red para obtener información el uno del otro.*

Tabla 1: Protocolos de monitorización (Cisco, 2022)

SNMP es el protocolo empleado para la monitorización de redes universalmente conocido gracias a la simplicidad de su uso y estructura, además de su buena organización.

La primera versión del protocolo SNMP surge a finales de la década de los 80, llegando esta versión a utilizarse hasta el día de hoy.

Aunque existen diferentes protocolos, SNMP es el utilizado por un mayor número de usuarios ya que permite proporcionar más información sobre el estado de la red, a diferencia de otros protocolos que solo nos indican si la red está activa o no.

El servidor SNMP o Protocolo Simple de Administración de Red es aquel que permite a los

usuarios administradores monitorizar las redes que cuelgan[1] de un nodo. Gracias a la monitorización y con este protocolo, se les permite a los administradores el control del rendimiento de la red, la detección y resolución de problemas de red, así como la planificación del crecimiento de la red.

3.1. Sistemas de monitorización

Debido a la complejidad de las redes que se usan hoy en día, en cualquier organización y en diferentes ámbitos, las tareas que se realizan sobre ellas son cada vez más exigentes para garantizar el correcto y continuo funcionamiento de estas.

Como consecuencia, la monitorización de redes está tomando hoy en día un papel fundamental, tanto para la detección de problemas en la red, como para la solución de estos.

Entre las principales ventajas que aporta el hecho de que un administrador de la red pueda monitorizarla, se encuentran entre otras, una visión conjunta y global de todos los dispositivos que cuelgan de la red, reducción de la carga de trabajo gracias a la posibilidad de anticipación ante los posibles errores que ofrecen los sistemas de monitorización o la visión genérica del rendimiento y eficacia de la organización.

3.1.1. Sistemas de monitoreo de red

Los sistemas de monitoreo de red son el conjunto de herramientas de software y hardware que permiten hacer un seguimiento del estado y funcionamiento de la red y sus dispositivos, como el tráfico, el uso de ancho de banda o el tiempo de actividad.

De esta forma, los sistemas de monitoreo de red permiten detectar rápidamente los fallos en el normal funcionamiento de los dispositivos o conexiones, generando si es necesario, las alertas correspondientes para informar al usuario sobre el estado de la red.

En la monitorización se emplean diferentes protocolos, entre los que se encuentra el protocolo SNMP. Además, existen diferentes tipos de aplicaciones para la monitorización de servidores, aplicaciones o redes. Una de ellas es Nagios, la cual es utilizada en el ámbito de defensa. Esta aplicación la podemos encontrar tanto en su versión civil como militar, pero siendo las dos completamente diferentes en cuanto a su funcionalidad (Cisco, 2022).

La monitorización facilita a los administradores el control de los sistemas, con el objetivo de conservar y almacenar datos de los sistemas analizados para generar reportes, poder comparar un sistema con otro gracias a esos reportes y justificar las necesidades de actuación de los sistemas monitorizados (Cisco, 2022).

Si realizásemos un aprovechamiento eficaz y eficiente de todos los recursos disponibles, no necesitaríamos de ningún sistema de monitorización; sin embargo, esto es más difícil de lo que parece, por lo que, a día de hoy, la implementación de un sistema de monitorización sobre el uso

[1] Término empleado para denominar a las redes a las que un determinado nodo monitor tiene acceso.

de una red puede facilitarnos la gestión de esta.

3.2. Servidor SNMP

A continuación, se muestra una guía a nivel usuario sobre las principales funciones y características de dicho servidor, la cual ha sido elaborada a raíz del curso CCNA (Cisco, 2022), de *Cisco Networking Academy* (CCNA desde cero, 2018) y de la guía del manual *SNMP User´s Guide* (Tekelec, 2012) para sintetizar la información.

3.2.1. Introducción a SNMP

Este protocolo de la capa de aplicación permite el intercambio de información entre los dispositivos conectados a la red. Está constituido por los siguientes elementos:

- Administrador de SNMP.
- Agentes de SNMP (nodo administrado).
- Base de información de administración (MIB, *management information base*).

El administrador de SNMP puede consultar a los dispositivos cliente para obtener información, o puede recibir un tipo de mensaje trampa o *Trap*, los cuales son mensajes de agentes que se envían sin el requerimiento de la estación del administrador en caso de que se produzca algún imprevisto.

3.2.2. Estructura de SNMP

Antes de empezar a configurar el protocolo de SNMP, es necesario establecer la relación que existe entre el administrador y el cliente (ver figura 1).

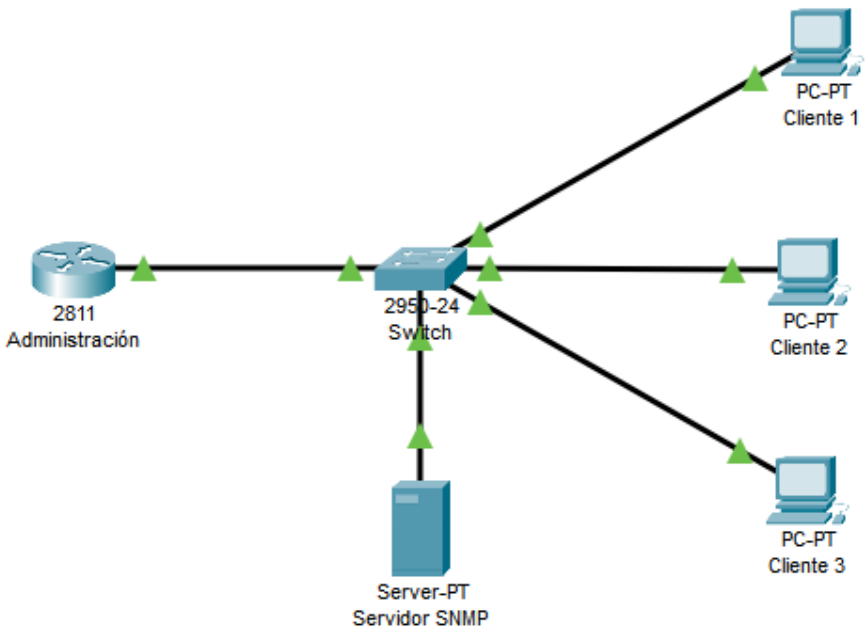

Figura 1: Esquema de red de un administrador SNMP y los diferentes agentes (elaboración propia)

El administrador de SNMP forma parte de un sistema de administración de red (NMS, *Network Management System*) y ejecuta el software de administración SNMP. Este puede obtener información y cambiar la configuración de un agente de SNMP.

El agente de SNMP y la MIB se encuentran en los clientes de los dispositivos que cuelgan de la red que incorporan un módulo de software de SNMP. Por un lado, la MIB se encarga de almacenar los datos sobre el funcionamiento del dispositivo, mientras que, por otro lado, el agente de SNMP proporciona el acceso a la MIB.

Existen dos tipos de solicitudes principales del administrador que son *get* y *set*. Mediante la solicitud *get* se solicitan datos al dispositivo, mientras que con la solicitud *set* se pueden cambiar las variables de configuración en el dispositivo del agente.

En resumen, los agentes SNMP que residen en los clientes, recopilan y almacenan información sobre los dispositivos y su funcionamiento. Esta información es almacenada en la MIB. El administrador SNMP utiliza el agente SNMP para tener acceso a la información dentro de la MIB.

3.2.3. Operaciones de SNMP

A continuación, se muestran las diferentes operaciones que utiliza el administrador bajo las solicitudes *get* y *set* en la tabla 2.

get- request	*Recupera el valor de una variable específica.*
get-next-request	*Recupera el valor de una variable dentro de una tabla; el administrador de SNMP no necesita saber el nombre exacto de la variable.*
get-bulk-request	*Recupera grandes bloques de datos, como varias filas en una tabla, que de otra manera requerirían la transmisión de muchos bloques pequeños de datos.*
get-response	*Responde a una operación get-request, get-next-request y set-request que envió NMS.*
set-request	*Almacena un valor en una variable específica.*

Tabla 2: Tipos de operaciones utilizadas por el administrador (CCNA desde cero, 2018)

La secuencia de estas operaciones sería la siguiente: (ver figura 2)

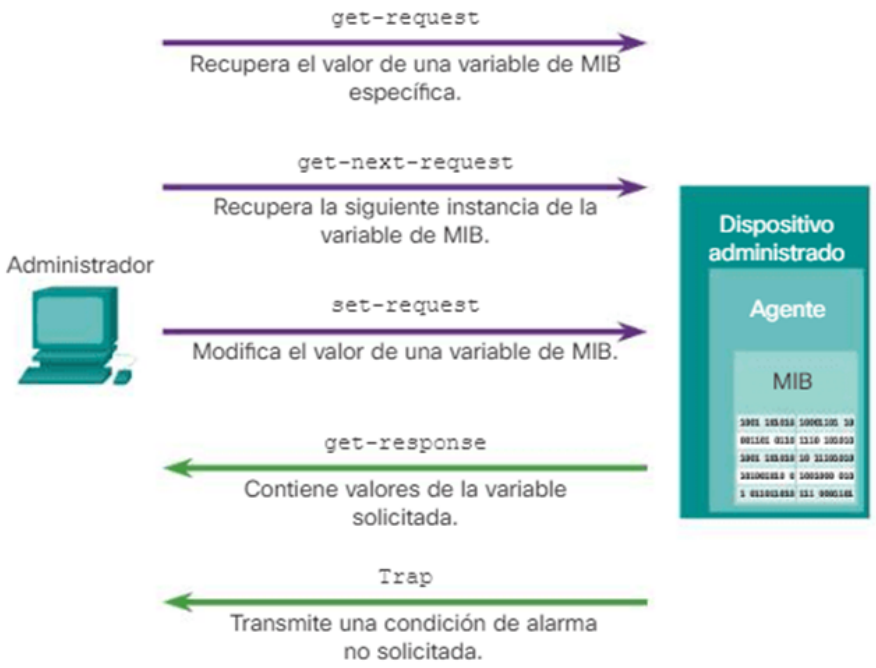

Figura 2: Secuencia de las operaciones de SNMP (CCNA desde cero, 2018)

Tras estas operaciones, el agente responde al administrador de la siguiente forma:

- Si el administrador ha enviado una solicitud de *get*, el agente recuperará el valor de la variable de MIB solicitada y responderá al administrador con ese valor.
- Si el administrador ha enviado una solicitud de *set*, el agente SNMP cambiará el valor de la variable de MIB por el valor que especifica el administrador. Dentro de la respuesta del agente SNMP ante este tipo de solicitudes se encuentra incluir la nueva configuración en el cliente.

3.2.4. Uso de las *traps* de SNMP

El NMS analiza constantemente a los agentes SNMP que se encuentran en los dispositivos clientes y les solicita información mediante la solicitud *get*. Gracias a esto, mediante las aplicaciones de monitorización y las de administración de redes, se puede recopilar información sobre la propia red para una gestión y control de las cargas de tráfico o la verificación de la configuración de cada dispositivo de la red que es administrado.

Esta información permite calcular los promedios, los mínimos o los máximos, representar los datos gráficamente o establecer umbrales para activar un proceso de notificación cuando se exceden los umbrales.

Sin embargo, este análisis periódico de SNMP presenta las siguientes desventajas:

- Existe un retraso entre el momento en el que ocurre un evento y el momento en el que NMS lo advierte.
- Existe cierta diferencia entre la frecuencia del sondeo y el uso del ancho de banda.

Para solucionar estas desventajas, los administradores de SNMP utilizan un tipo de mensajes denominados *traps*.

Las *traps* son mensajes no solicitados que alertan al administrador de SNMP sobre cualquier incidencia o acontecimiento en la red. Estos pueden ser enviados por diferentes motivos como que el usuario no se haya autenticado correctamente, que el enlace se encuentre en un estado inactivo, seguimiento de una dirección MAC o por la pérdida de conexión con otros agentes vecinos.

3.2.5. Versiones de SNMP

Existen las siguientes versiones de SNMP:

SNMPv1: el protocolo simple de administración de red, un estándar de Internet completo, definido en RFC[2] 1157.

SNMPv2c: definido en las RFC 1901 a 1908; utiliza el marco administrativo basado en cadenas de comunidad.

SNMPv3: protocolo interoperable basado en estándares, definido originalmente en las RFC 2273 a 2275; proporciona acceso seguro gracias a la autenticación y el cifrado de paquetes a través de la red.

Pese a que son versiones diferentes, todas ellas utilizan administradores de SNMP, agentes SNMP y MIB.

La diferencia entre SNMPv1 y SNMPv2c radica en que SNMPv2c incluye un mecanismo de recuperación masiva e informes de mensajes de error más detallados para las estaciones de administración. Ambos proporcionan características de seguridad mínima, sin embargo, no pudiendo autenticar el origen de un mensaje de administración ni proporcionar cifrado.

SNMPv3 es una versión más actualizada a las citadas previamente. Esta incluye métodos para garantizar la transmisión segura de datos importantes entre los diferentes dispositivos administrados. Además, proporciona tanto modelos como niveles de seguridad.

Un modelo de seguridad queda definido como una estrategia de autenticación configurada para un usuario y el grupo dentro del que reside el usuario, mientras que el nivel de seguridad queda definido como la seguridad dentro de ese modelo de seguridad.

La combinación de ambas, tanto el nivel de seguridad y el modelo de seguridad determina qué mecanismo de seguridad se utiliza al manejar un paquete SNMP.

3.2.6. Comunidad de SNMP

Principalmente para que SNMP funcione, NMS debe tener acceso a la MIB. Además, debe existir cierta forma de autenticación, para que las solicitudes de acceso sean válidas.

Una cadena de comunidad (*community string*) es una cadena de texto que controla el

[2] Conjunto de documentos que se emplean para la estandarización de las normas, tecnologías y protocolos relacionados con las redes e Internet.

acceso a la MIB. Tanto SNMPv1 como SNMPv2c usan cadenas de comunidad. Estas son simplemente contraseñas de texto no cifrado que autentican el acceso a los objetos MIB.

Existen dos tipos de cadenas de comunidad. Por un lado, se encuentran las de solo lectura (ro, *read-only*), las cuales proporcionan acceso a las variables de MIB, pero no permite realizar cambios a estas variables, solamente leerlas. Por otro lado, se encuentran las de lectura y escritura (rw, *read-write*), que como su nombre indica, proporcionan acceso de lectura y escritura a todos los objetos de la MIB.

Para poder ver o establecer variables de MIB, el usuario debe especificar la cadena de comunidad correspondiente para el acceso de lectura o escritura.

3.2.7. Recomendaciones

Aunque SNMP proporciona múltiples ventajas en la monitorización de redes y la resolución de incidencias, también puede proporcionar desventajas sobre todo en cuestiones de seguridad.

SNMPv1 y SNMPv2c dependen de las cadenas de comunidad SNMP en texto no cifrado para autenticar el acceso a los objetos de la MIB. Estas cadenas de comunidad, actúan igual que cualquier tipo de contraseña, por lo que deben elegirse cautelosamente para que no puedan ser descifradas con facilidad.

Además, conforme a las políticas de seguridad de la red, las cadenas de comunidad deben ser cambiadas cada cierto tiempo de forma regular.

Si SNMP se utiliza solo para monitorear los dispositivos, es recomendable utilizar comunidades de solo lectura.

Es conveniente que los mensajes de SNMP no se propaguen más allá de las consolas de administración.

Es recomendable SNMPv3 porque proporciona autenticación y cifrado de seguridad. Existen otros comandos del modo de configuración global que puede implementar un administrador de red para aprovechar la autenticación y el cifrado en SNMPv3.

4. DESARROLLO: ANÁLISIS Y RESULTADOS

Previamente a la implementación de un sistema de monitorización en el nodo, se ha realizado un estudio, mediante un análisis DAFO (ver anexo I) con el objetivo de conocer los principales riesgos y debilidades que pueden afectar a la estructura de la red, además de conocer los aspectos positivos de cara a la implantación de mejoras en un futuro.

Una vez realizado este análisis, para la implementación de un sistema de monitorización en el nodo de SIMACET, se han hecho pruebas en base a una máquina virtual capaz de realizar la monitorización de cualquier dispositivo que se encuentre en la misma red.

Se ha creado una máquina virtual, con las características necesarias para soportar el protocolo SNMP, así como, la versión del nodo, para que no dé problemas de compatibilidad. La activación del protocolo de SNMP permite que el servidor donde se encuentre la máquina virtual sea capaz de llevar a cabo las tareas de monitorización.

Tras crear la máquina virtual con el protocolo de SNMP, es necesario implementarla en el nodo. Para ello, es necesario conocer los pasos involucrados, entre los que se incluyen, asignación de direcciones IP y máscaras de red y puesta en dominio entre otros. Además, es necesario conocer los pasos para activar el protocolo SNMP una vez que la máquina virtual se encuentre implementada en el nodo.

Por último, para obtener resultados gráficos, se muestra el funcionamiento de una aplicación mientras está monitorizando, además de realizar un análisis sobre la viabilidad de la adquisición de alguna de las principales aplicaciones de monitorización.

Todo esto se ha realizado de forma independiente al nodo, ya que, para poder usar una de estas aplicaciones, se necesitan permisos por parte del administrador del nodo, a los cuales no ha sido posible su acceso.

Así, si dispusiéramos de esos permisos, solo bastaría instalar la aplicación que permita la monitorización en la máquina virtual, para posteriormente, implementarla en el nodo y proceder a su uso tal y como se explica.

4.1. Monitorización en el ámbito Defensa

Gracias a la monitorización, el Mando militar puede tener una visión completa de los sistemas que tiene bajo su responsabilidad. Los sistemas de monitorización le facilitan el conocimiento de si un sistema se encuentra caído, si presenta algún tipo de fallo o cualquier tipo de incidencia, si hay un consumo de memoria ineficaz, etc (Mando de Adiestramiento y Doctrina, 2009).

La División de Operaciones de Red, también conocida como DIVOPER (ver anexo II), es el principal órgano encargado de la provisión de servicios CIS/TIC (sistemas de información y telecomunicaciones/ tecnologías de la información y la comunicación) del Sistema de Mando y Control Nacional (SC2N), siendo una de sus principales funciones el garantizar la monitorización necesaria para asegurar el correcto funcionamiento de los servicios, gestionando a su vez las incidencias, peticiones y accesos a los mismos (Ministerio de Defensa de España, s.f.).

A través de la DIVOPER se proporciona una herramienta de monitorización para la monitorización, pero cabe recalcar que desde DIVOPER no se monitoriza, simplemente DIVOPER proporciona la herramienta habilitada para ello. Esto implica que el departamento de monitorización no lleva a cabo medidas correctoras sobre los sistemas que no se encuentren a

su cargo (Ministerio de Defensa de España, s.f.).

4.1.1. Sistemas a monitorizar

La monitorización ha ido ampliando sus horizontes, enfocándose originalmente en los servidores de la WAN-PG hasta otros dispositivos de hoy en día como puede ser cualquier dispositivo conectado a la red, como podría darse en el caso de impresoras. Aunque la monitorización es una herramienta que facilita la supervisión de cualquier sistema, no todos pueden ser gestionados, especialmente aquellos que se encuentran desfasados o con un firmware desactualizado.

Para ello, no es necesario que los sistemas estén en el dominio de MDEF, a excepción de aquellos que se encuentren en redes aisladas o protegidas y no podamos acceder a ellos mediante la WAN-PG por razones de seguridad (Mando de Adiestramiento y Doctrina, 2009).

4.2. Sistema de Mando y Control del Ejército de Tierra

La información obtenida para este apartado ha sido obtenida del manual PD3-602 sobre el establecimiento y empleo de SIMACET (Mando de Adiestramiento y Doctrina, 2009).

4.2.1. Introducción a SC2NET

Mediante la función de combate mando y control, el Mando militar ejerce la autoridad que le ha sido conferida sobre sus unidades subordinadas, con el fin de conducir las operaciones, dirigiendo y coordinando las fuerzas y medios asignados para el cumplimiento de la misión.

Los sistemas de información para mando y control son los que mejor contribuyen al conocimiento y comprensión de la situación, reduciendo los tiempos necesarios para la toma de decisiones y facilitando la sincronización de elementos y acciones.

Para ello, el jefe militar dispone de una serie de Sistemas de Información y Comunicación que le apoyan en la toma de decisiones. Uno de estos es el Sistema para el Mando y Control del Ejército de Tierra.

En el ámbito militar, se consideran dos tipos genéricos de sistemas de información

- Sistemas de información para el mando y control (C2IS)
- Sistemas de información de propósito general

El Sistema para Mando y Control del Ejército Tierra ofrece al usuario aplicaciones de diferentes tipos, donde se pueden destacar las siguientes:

- Aplicaciones de gestión táctica
- Aplicaciones de información geográfica
- Aplicaciones de mensajería

El núcleo principal del sistema es la base de datos táctica (BDT). Esta puede definirse como el conjunto de datos base de iconografía, plantillas, grupos y perfiles de usuario y de datos planeados de usuarios, de red del sistema y de información táctica. Los datos mencionados son cargados en los nodos que van a intervenir en la maniobra, consiguiendo con esto que todos dispongan de la misma información inicial.

Una vez la maniobra ha dado inicio, los cambios que se produzcan en la BDT son actualizados en todos los nodos del sistema. Para que dichos cambios sean transferidos a todos los usuarios se utiliza un mecanismo de réplica.

4.2.2. Composición del sistema

La composición de SIMACET se basa en tres elementos

- Nodos: Un nodo está definido como el conjunto de medios, *hardware* y *software*, capacidades, personal y procedimientos que realizan todas o algunas de las funciones del sistema. Cada nodo dispone de la BDT que intercambia información con la de otros nodos. El conjunto de varios nodos junto con los procedimientos adecuados conforma la red de SIMACET.
- Redes lógicas de réplica: Con el fin de difundir y actualizar la información táctica, agrupada en la BDT, los nodos se agrupan en redes lógicas de réplica, consiguiendo de esta manera que los nodos integrados en esta red posean idéntica información. Para interconectar diferentes redes lógicas de réplica se utilizan los nodos pasarela, consiguiendo además la aplicación de filtros para la información táctica que discurra entre redes distintas. Además, existen tres tipos de redes lógicas diferentes, atendiendo al procedimiento utilizado para la transmisión de la información táctica.
- Usuarios: responsables de introducir y gestionar la información dentro del sistema. Para el establecimiento de los usuarios se crean una serie de perfiles, los cuales se asignan a cada grupo de usuarios. Dichos perfiles permiten dar acceso o denegarlo a ciertos recursos y/o servicios disponibles en el sistema. Hay dos tipos de usuarios en SIMACET. Por un lado, se encuentran los usuarios técnicos, estos serían los administradores del nodo. Estos normalmente corresponderían con el personal perteneciente a las unidades de transmisiones. Por otro lado, se encontrarían los usuarios de los Cuarteles Generales y de la Plana Mayor de Mando, los cuales corresponderían a los clientes con acceso a la gestión de la información táctica y la mensajería oficial, además de la información interpersonal, como el correo electrónico tanto interno como externo.

4.2.3. Estructura del nodo

Hay diferentes tipos de nodos. Estos son:

- Nodos fijos: son aquellos que permiten al Mando llevar a cabo el planeamiento y el seguimiento de las operaciones mediante la instalación fija de estos en los cuarteles generales de las unidades. A su vez, su uso también puede estar destinado a la enseñanza y a la instrucción y adiestramiento.
- Nodos desplegables: son empleados por los puestos de mando, en situaciones de paz, crisis o guerra y en conflicto armado. Estos se pueden clasificar como nodos de gran unidad o de pequeña unidad. Estos se diferencian por la entidad de los puestos de mando a los que proporcionan servicio, además, de la movilidad, equipamiento y número de usuarios a los que dan servicio.

Para la realización de este proyecto, el nodo que se ha utilizado correspondería a un nodo desplegable de gran unidad, ya que este pertenece a la Brigada y da servicio a esta.

Además, resulta de vital importancia conocer la estructura del nodo ya que este es el

elemento principal a la hora de implementar el servidor SNMP físicamente y la pieza fundamental para el desarrollo de este proyecto.

La estructura del nodo sería la siguiente (ver figura 3)

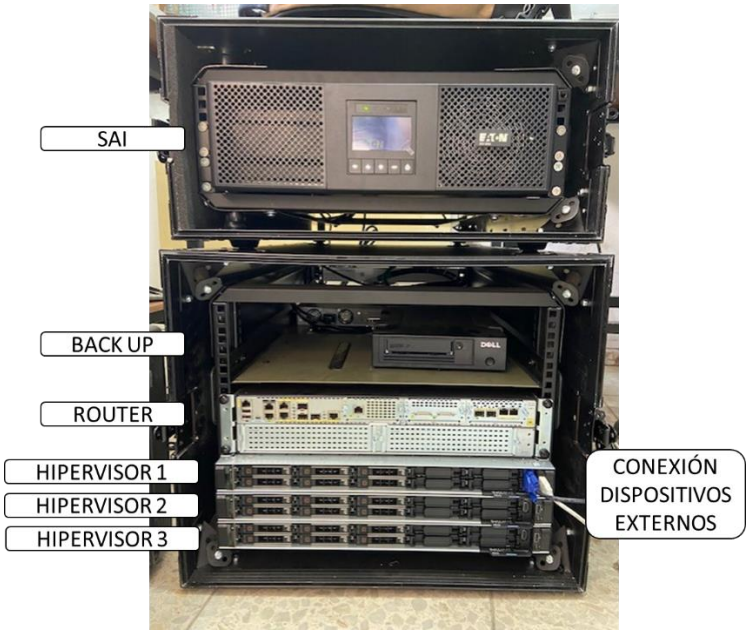

Figura 3: Estructura física de un nodo de SC2NET (elaboración propia)

Como podemos observar, hay dos cofres separados el uno del otro. El primer cofre se trataría de la SAI (Sistema de Alimentación Ininterrumpida), mientras que el segundo incluye los servidores, los cuales se explicarán a continuación.

La SAI se trata de una fuente de alimentación alternativa que actúa en caso de que se interrumpa el suministro eléctrico, evitando que no se apague el nodo y se pierdan todas sus funciones. Así, se puede garantizar la continuidad del nodo y sus servicios el tiempo necesario hasta que se restauren las condiciones iniciales.

En la siguiente imagen podemos ver qué es lo que nos indicaría esta. Esto sería principalmente la batería disponible y tiempo de uso (ver figura 4).

Figura 4: Parámetros que nos indica la SAI (elaboración propia).

Por otro lado, tenemos el cofre de abajo, el cual incluye el back up, un router, un switch y en este caso 3 hipervisores. Estos hipervisores son los servidores físicos, los cuales contienen cada uno diferentes máquinas virtuales, que proporcionan diferentes servicios o funciones. Estas funciones serían provistas por los servidores virtualizados.

En el caso del hipervisor 1, se incluyen las aplicaciones de controlador de dominio, SIMACET y OT1, este último incluye las aplicaciones OTAN como son *JChat*, *JEMM* y *Exchange*.

El hipervisor 2 incluye otro controlador de dominio de respaldo al primero, SIMACET y un servidor de impresión y archivos.

Por último, el hipervisor 3, incluye un servicio de copia de seguridad, el cual va conectado al back up y el SASS (Software como Servicio), el cual incluye las actualizaciones.

4.2.4. Versiones de SC2NET

Actualmente, se distinguen dos tipos de nodos: SC2NET-D (Desplegable) y SC2NET-CGP (Cuarteles Generales Permanentes).

Los servicios principales que ofrece SC2NET a los usuarios son información táctica (mapa de situación con la ubicación de las unidades), mensajería oficial y mensajería interpersonal, aunque hay más aplicaciones a parte de estas. El sistema comenzó a implementarse en las unidades de transmisiones en el año 2001 y actualmente, las versiones que se están utilizando son:

- SIMACET v4.2: en esta versión, los nodos están compuestos por una serie de servidores físicos (controlador de dominio, SIMACET, exchange y share point).
- SIMACET v5: el software es esencialmente el mismo que en la versión 4.2. Sin embargo, hay cambios en el hardware ya que existen únicamente dos servidores físicos, en los cuales se encuentran virtualizados todos los servidores. Ambos servidores son redundantes, para poder garantizar el servicio en caso de que uno de ellos falle.
- SIMACET v6 “PROMETEO”: aún no se ha implementado en las unidades, en esta versión se modifican las aplicaciones del sistema para adecuarse al modelo de datos de OTAN. El hardware es similar al de la versión 5.

Debido a que la versión 4.2 se encuentra algo obsoleta, resulta muy difícil el despliegue y la compatibilidad con otro tipo de unidades que utilizan la versión 5. Es por ello, que a la versión 4.2 se le está aplicando actualizaciones para que los nodos con esta versión puedan comunicarse con su versión más avanzada. Esta actualización se conoce como versión 4.5 y es la que se va a analiza en este proyecto.

Esta versión surge por la necesidad de cambios en los servidores actuales por obsolescencia, falta de mantenimiento y de capacidad de almacenamiento y virtualización. Es por ello que se pretende incorporar mejoras tanto en los medios hardware como software.

4.3. Comandos de configuración de SNMP

En este apartado, se detallan los comandos básicos para la configuración de SNMP, para

tener una idea general de cara a su configuración, la cual se explica en el apartado posterior. Estos comandos son válidos para aplicaciones que permitan la simulación de redes como *Cisco Packet Tracer*, donde podemos realizar la simulación de todo el esquema de red, a la vez que activamos protocolos o probamos la conectividad y enlace de los diferentes dispositivos de la red.

Para que un administrador de red pueda configurar SNMP y así obtener información de red debe seguir los siguientes pasos. Todos estos pasos se ejecutan en el modo de configuración global.

- Lo primero es configurar la cadena de comunidad y el nivel de acceso (solo lectura o lectura y escritura). Utilizaremos el comando 1 (ver figura 5). En este caso, se ha configurado SNMPv2 con cadenas de comunidad en vez de SNMPv3. El motivo de esto, se debe a que ambas versiones son muy similares, y aunque SNMPv3 es mas segura por su tecnología criptográfica, SNMPv2 utiliza un sistema de seguridad basado en el intercambio de contraseñas, lo que la hace más compleja en ese aspecto.
- Registrar la ubicación del dispositivo mediante el *comando snmp-server location text*.
- Registrar el contacto del sistema mediante el comando *snmp-server contact text*.
- En función de la versión utilizada, tanto el comando de *location* o de *contact* puede no ser reconocido por el administrador. En este utilizaremos el comando 2 (ver figura 5). En este comando se muestra la dirección IP del dispositivo al que vamos a registrar la ubicación, además de mostrar las *traps*.

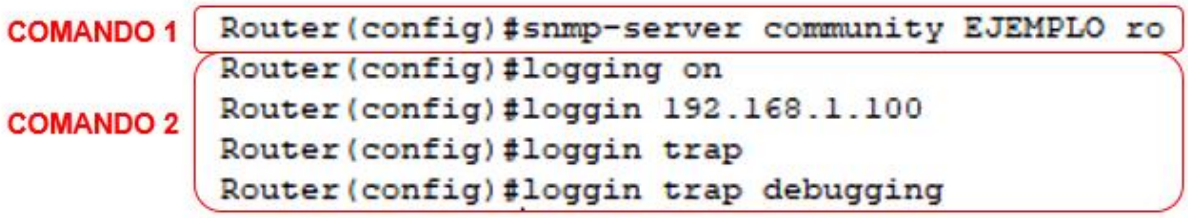

Figura 5: Lista de comandos en el administrador (elaboración propia)

- El siguiente paso será especificar el destinatario de las operaciones de *trap* de SNMP en cada dispositivo y las operaciones que se van a llevar a cabo en este (ver figura 6). Esta información se guardará en la OID, la cual define las características de un dispositivo que es gestionado.

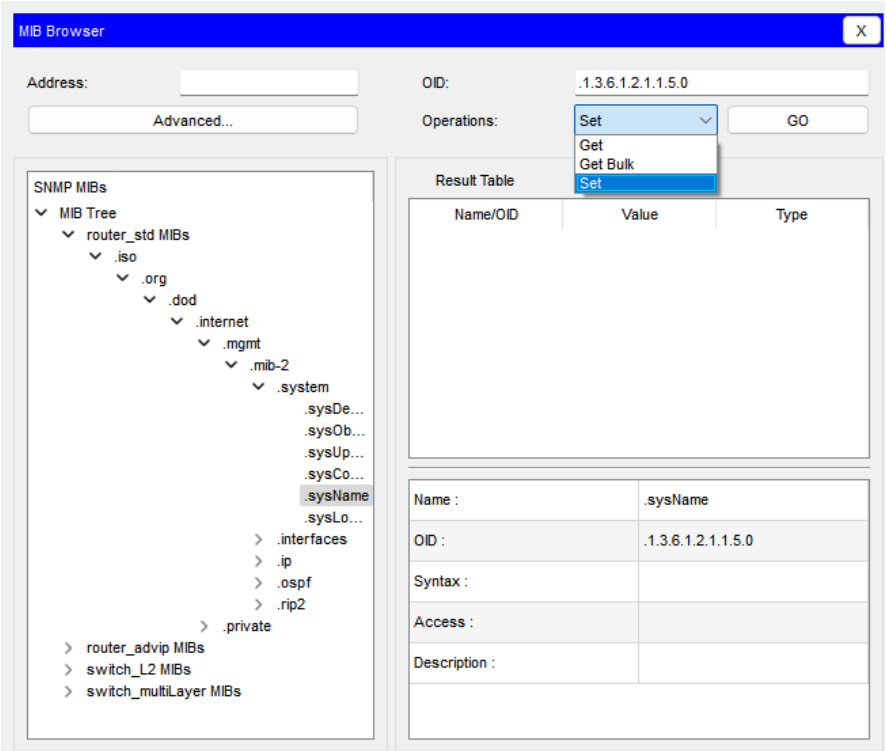

Figura 6: Asignación de operaciones SNMP a un dispositivo (elaboración propia)

- Toda la configuración de SNMP la podemos verificar en el protocolo de registro del sistema (SYSLOG) del servidor que está conectado en la red (ver figura 6). Este protocolo permite al servidor comunicarse con los dispositivos de la red. Este se usa principalmente, para facilitar el monitoreo de dispositivos de red (Cisco, 2022).

4.4. Implementación del servidor SNMP en el nodo SC2NET

Todos los ordenadores de Windows proporcionan el servicio de SNMP, lo cual quiere decir que llevan implementada esa característica en su configuración y nosotros podemos decidir si queremos activarla o no.

Sin embargo, el hecho de tener activa esta característica no quiere decir que podamos utilizarla con total libertad, ya que no podemos visualizar los datos que nos proporciona SNMP si no disponemos de una herramienta adecuada para su visualización.

Así, tras implementar el protocolo de SNMP, necesitaremos de alguna aplicación que nos muestre los resultados y utilidades de este protocolo de forma gráfica.

Uno de los problemas del uso de este tipo de aplicaciones es que la mayoría de ellas son de uso civil y, además, muchas de ellas son de pago, o su versión gratuita no incluye todas las funciones necesarias. Una de las aplicaciones de uso militar es *Nagios.* Esta presenta la ventaja de que puede ser utilizada directamente desde una intranet, sin necesidad de pago, tal cual se ha podido contrastar gracias a una de las múltiples entrevistas realizadas al personal encargado

del área de SC2NET (ver anexo III).

Nagios es un sistema de monitorización de redes que es ampliamente utilizado por múltiples empresas y organizaciones, ya que permite consultar prácticamente casi cualquier parámetro de un sistema o red, además de generar alertas en caso de cualquier tipo de incidencias. Se trata de una aplicación muy útil ya que proporciona gran variedad de herramientas que facilitan una visión detallada del estado de los servicios, así como la detección de errores (Nagios, 2019).

Sin embargo, para poder acceder a Nagios se requiere de usuario y contraseña el cual necesita ser previamente autorizado por el Centro de Comunicaciones (CECOM), por lo que, por esta forma, esto resultaba inviable para llevar a cabo el proyecto.

No obstante, previamente a la monitorización es necesario la instalación y configuración del protocolo SNMP en el administrador. Por eso, se ha llevado a cabo experimentos en base a una máquina virtual que cuenta con la característica de SNMP y una vez vinculada al nodo y en el dominio correspondiente, esta podría monitorizar todos los dispositivos que se encuentren en ese dominio.

4.4.1. Instalación del servidor

Para llevar a cabo la implementación del servidor SNMP en el nodo, utilizaremos el hipervisor 3. Podríamos haber utilizado cualquier otro, pero la elección de este se debe a que, en este caso, contaba con menos máquinas virtuales y de esa forma podíamos aprovechar los recursos de una forma más eficaz y obtener una mayor velocidad de respuesta por parte del servidor.

Lo primero que necesitamos es que los dispositivos externos como el monitor, teclado y ratón se encuentren conectados al nodo para que nos permitan gestionar todo el proceso.

Cada nodo es gestionado por dos personas, por lo que tenemos dos dispositivos administradores. De estos, uno está conectado al hipervisor 1 y 3, mientras que el otro solo está conectado al hipervisor 2. Es por ello que utilizaremos el dispositivo conectado a los hipervisores 1 y 3, ya que la máquina virtual la vamos a conectar en el hipervisor 3.

A continuación, necesitaremos tener creado en ese ordenador una máquina virtual (ver anexo IV) con la característica de SNMP. Esta máquina virtual se puede crear desde un ordenador personal y después exportarla al dispositivo que se utilizaría como administrador.

Una vez que hayamos pasado la máquina virtual al hipervisor, lo siguiente que vamos a hacer es activar la característica de SNMP.

Nada más iniciar la máquina virtual, se nos abrirá la ventana de administrador del servidor, donde podemos indicar todos los roles y características que queremos activar en esta máquina virtual (ver figura 7).

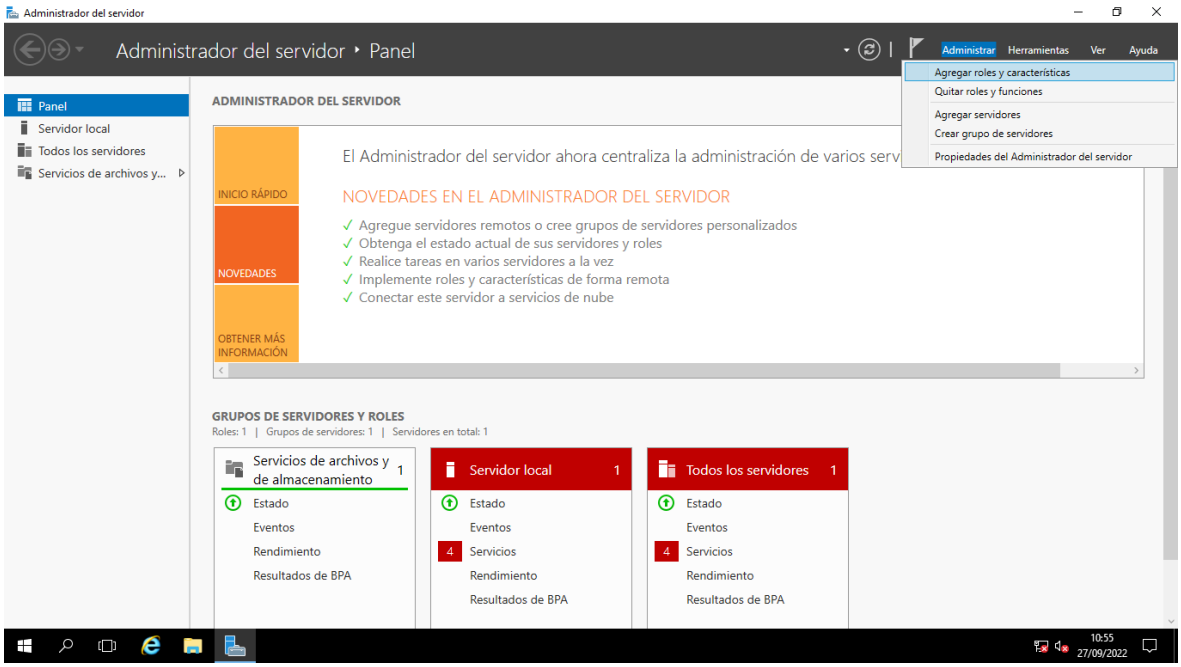

Figura 7: Panel para agregar la característica de SNMP (elaboración propia)

A continuación, al pinchar en *Agregar roles y características* se nos abrirá un cuadro donde debemos seleccionar el protocolo SNMP como característica de esta máquina virtual, para de esta forma activarlo (ver figura 8).

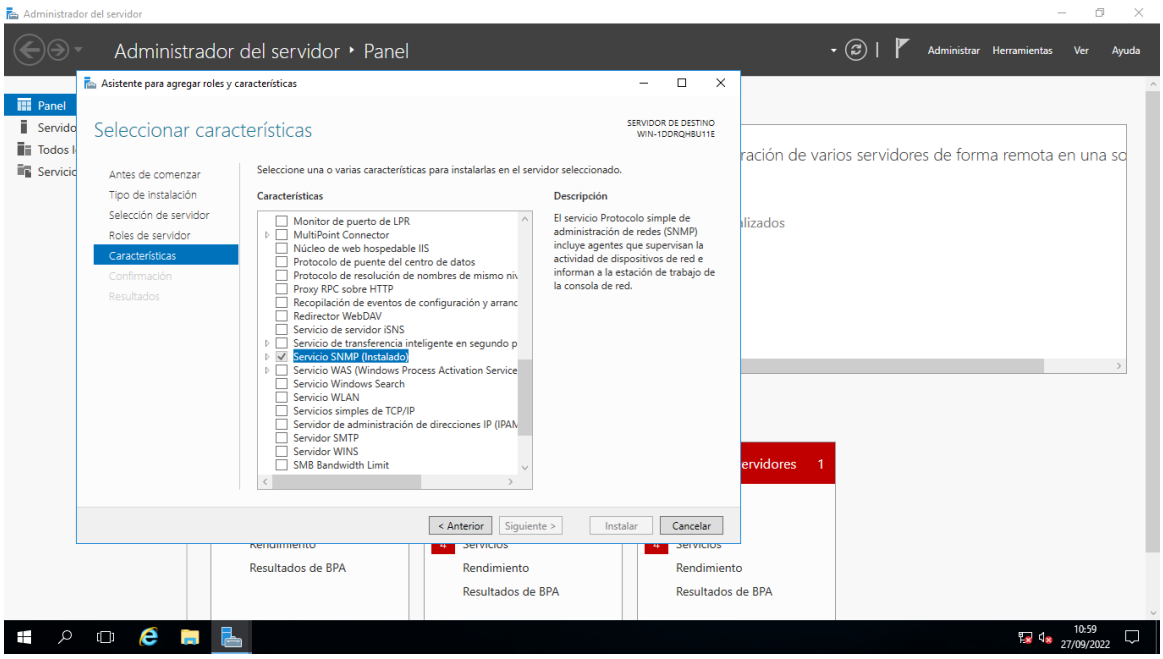

Figura 8: Selección del protocolo SNMP (elaboración propia)

Tras ello, y tras un proceso de instalación, ya tendríamos una máquina virtual con el

protocolo de SNMP.

Igualmente, este proceso se puede realizar directamente en el ordenador administrador, sin la necesidad de crear una máquina virtual. Sin embargo, esto lo hacemos así porque los hipervisores del nodo de SIMACET están pensados para tener una máquina virtual por cada servicio que queramos dar, ya que así, en caso de que la máquina virtual se encuentre inoperativa, solo se interrumpa el servicio que proporciona.

Una vez que tenemos la máquina virtual en el hipervisor y con la característica activa de SNMP, necesitamos que esta se encuentre en la red, para que así conozca los dispositivos que cuelgan de esta y para su futura monitorización.

Para ello, lo primero a realizar sería incluir esta máquina virtual en el dominio del servidor. A continuación, lo que tenemos que hacer es darle una dirección IP a nuestra máquina virtual. Esto se hace directamente desde la configuración de red del protocolo IPV4 de la propia máquina (ver figura 9).

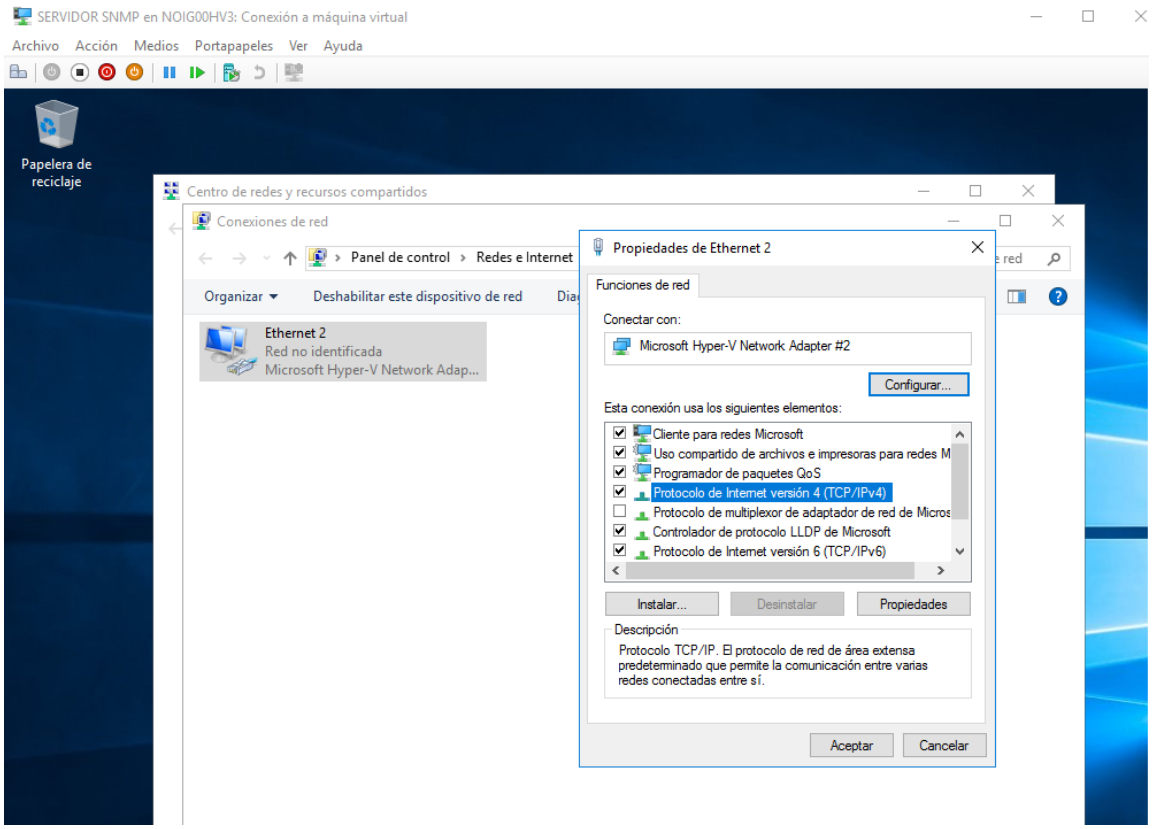

Figura 9: entrada al protocolo IPV4 (elaboración propia)

Aunque la máquina virtual se encuentre dentro del domino del nodo, esta no podrá hacer *ping* a los demás dispositivos que se encuentren en dominio, ya que no los reconocerá. Esto impedirá que podamos monitorizar estos dispositivos, por lo que, para cambiarlo, lo haremos mediante la configuración avanzada del protocolo IPv4.

Tendremos que incluir el sufijo DNS (ver figura 10) y desactivar la *NetBIOS*, la cual habilita un cortafuegos de Windows (ver figura 11).

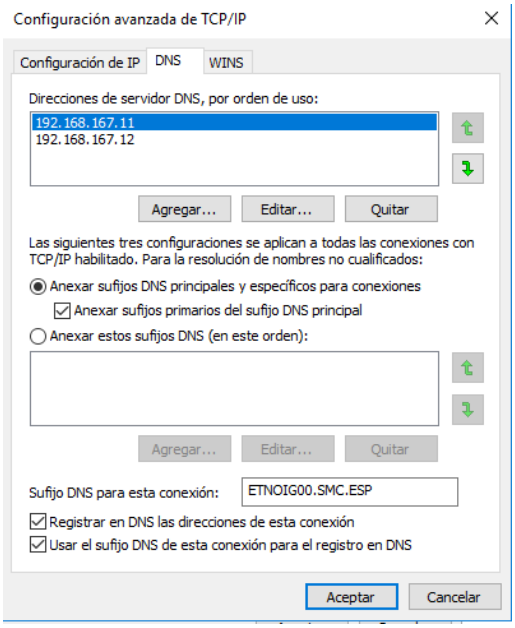

Figura 10: cambio en el sufijo en DNS (elaboración propia)

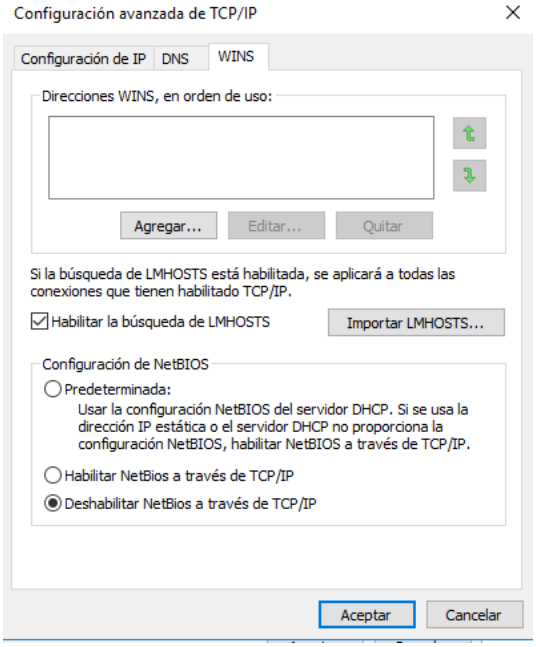

Figura 11: como deshabilitar la NetBIOS (elaboración propia)

El cortafuegos es un programa que actúa como un antivirus, evitando que un *malware*[3] se

[3] Programa o código malicioso que es dañino para los ordenadores

expanda por la red y entre en nuestro sistema.

La desactivación del cortafuegos no supone ningún riesgo para la seguridad de nuestro dispositivo si se realiza de forma prudente, sin embargo, somos más susceptibles de que nuestro ordenador sea infectado por esos *malwares* si desactivamos el cortafuegos durante un largo periodo de tiempo, ya que los cortafuegos permiten y bloquean las conexiones entrantes y salientes a nuestro ordenador. Otra alternativa sería abrir en el cortafuegos únicamente los puertos utilizados por el protocolo SNMP.

El siguiente paso será indicar los parámetros que se nos piden. La dirección IP y la máscara vienen fijadas de forma predeterminada por el Parque y Centro de Mantenimiento de Sistemas de Hardware y Software.

Este es el órgano del Ejército encargado del mantenimiento de todos los sistemas, principalmente de mando y control, así, como el mantenimiento correctivo adaptativo del software, por lo que estas entrarían dentro de sus competencias y no podemos modificarlas (Ejército de Tierra, s.f.).

Como estos parámetros vienen con una configuración predeterminada, es necesario conocerlos, ya que no podemos cambiar los parámetros por nuestra propia voluntad.

Así, la dirección IP es 192.168.167.37 y la máscara de red es 255.255.255.0.

La puerta de enlace predeterminada correspondería a la boca del router del nodo, que en este caso hemos utilizado 192.168.167.1.

Por último, el servidor DNS principal sería la dirección del controlador de dominio 1, es decir, 192.168.167.11, mientras que el alternativo sería el controlador de dominio 2, 192.168.167.12, ya que este sería el respaldo al 1 en caso de fallo (ver figura 12).

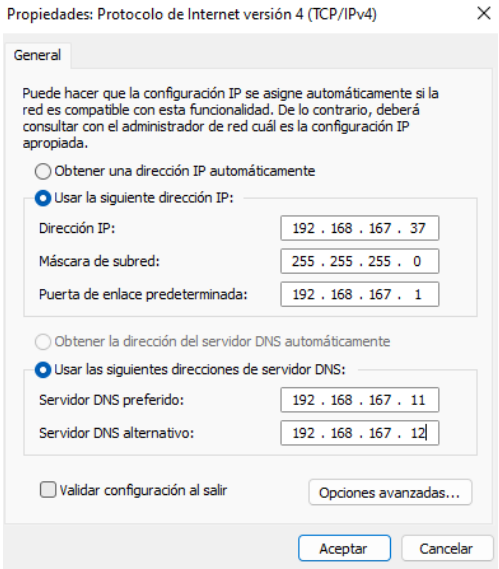

Figura 12: Direcciones utilizadas para la máquina virtual (elaboración propia)

Esta dirección IP se encuentra ya dentro del rango del dominio, por lo que lo siguiente sería meterlo en el dominio. Esto lo podemos hacer desde la configuración del sistema y seguridad,

en el cual, si nos metemos en este apartado, podremos introducir el nombre del dominio en el que se encuentra el servidor (ver figura 13), que en este caso es *ETNOIG00.SMC.ESP.*

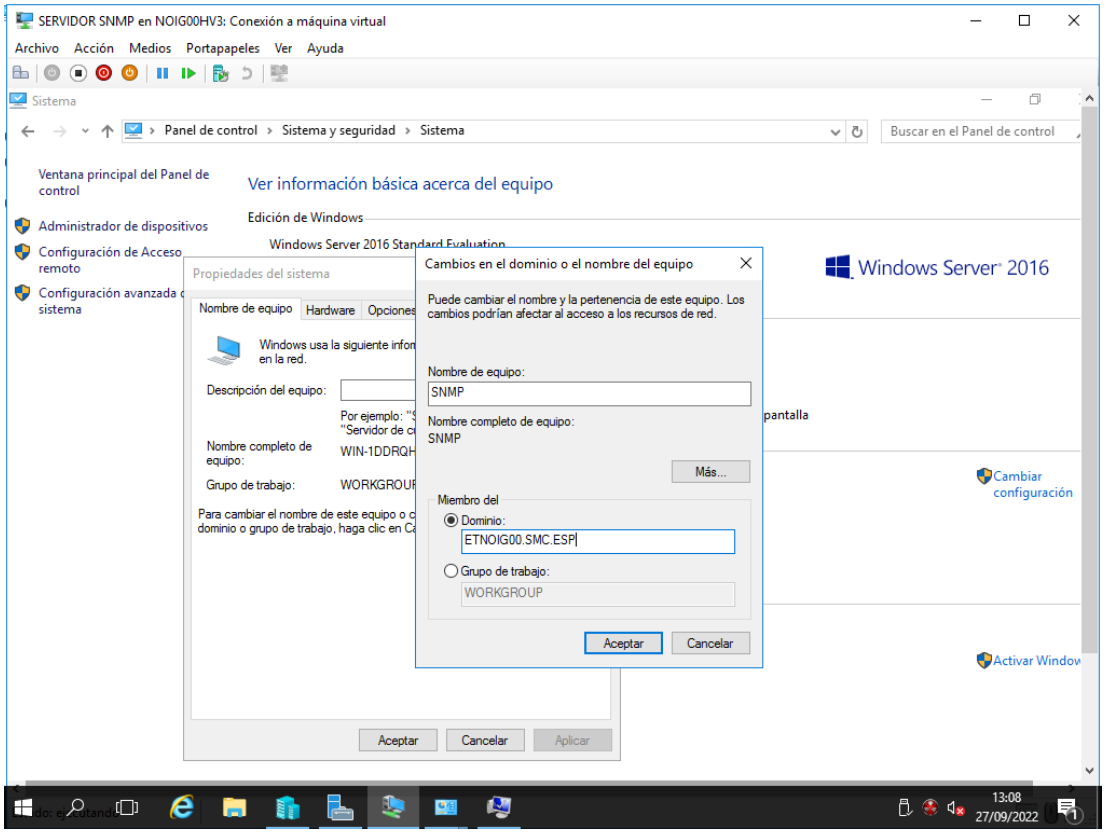

Figura 13: configuración del nombre de dominio (elaboración propia)

Antes de terminar este proceso, se nos pedirá indicar un usuario y contraseña que ya esté creado en ese dominio y posteriormente el equipo se reiniciará.

Por último, un aspecto a tener en cuenta es que la hora de nuestro servidor tiene que coincidir con la del controlador del dominio. Esto realmente no nos influye en la realización del proyecto; sin embargo, de cara a la realización de ejercicios más complejos con más servicios, puede conllevar a problemas de conflictos en la sincronización con otros servidores. Este ajuste de la hora podemos hacerlo mediante el protocolo NTP, a través del cual, podemos sincronizar la hora de los routers conectados a un servidor. Otra alternativa sería directamente desde el centro de control mediante el comando *net time* (ver figura 14).

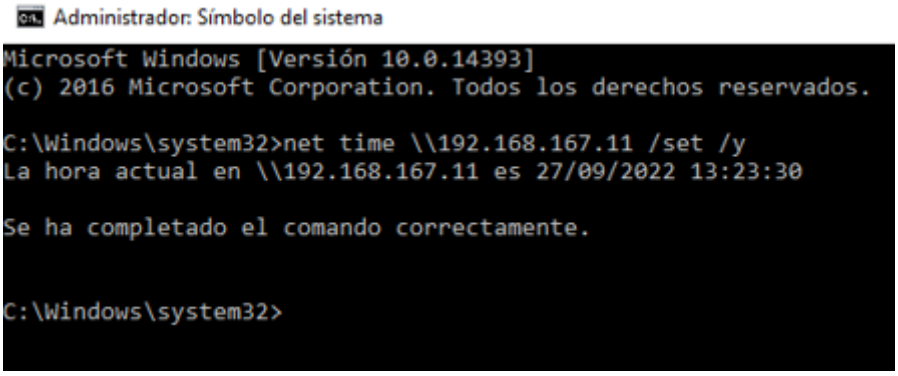

Figura 14: comando de configuración de la hora (elaboración propia)

Finalmente, ya tendríamos nuestra máquina virtual implementada en el servidor del nodo, con el protocolo SNMP, metida en dominio y lista para funcionar. Esto podemos comprobarlo y revisarlo desde las características de configuración del nodo (ver imagen 15).

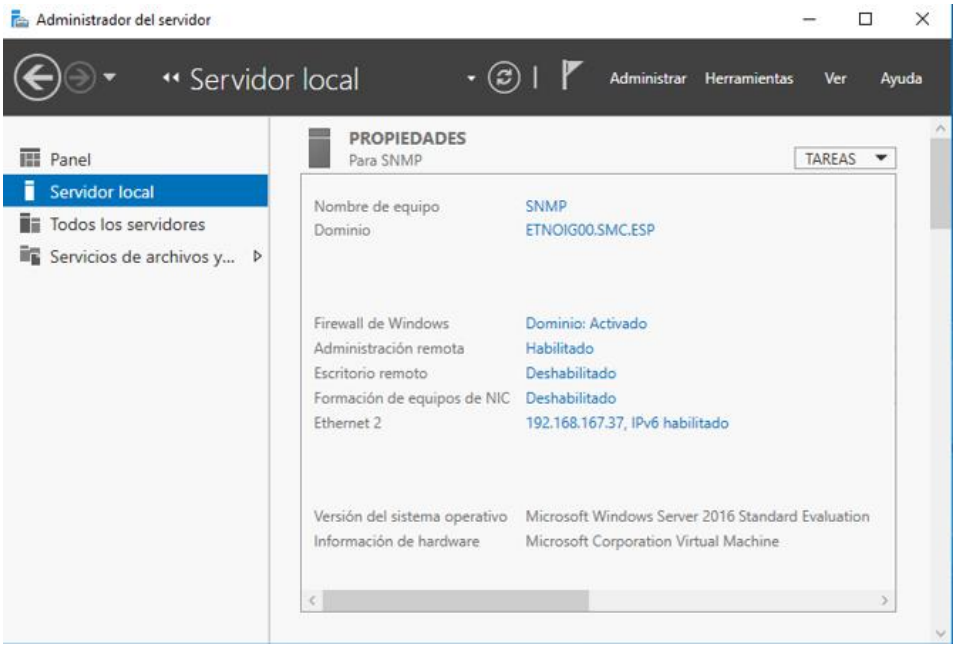

Figura 15: resumen de los parámetros de la máquina virtual ya implementada en el servidor (elaboración propia)

4.4.2. Utilidades del servidor

Tras instalar el protocolo SNMP en nuestro servidor, lo siguiente que vamos a hacer es configurarlo en todos los dispositivos que se encuentran en el mismo dominio. Para ello, utilizaremos lo visto previamente sobre el protocolo SNMP.

Lo primero que vamos a hacer será acceder a este protocolo. Para ello, nos vamos a los *Servicios de Windows* y buscamos el *Servicio de SNMP* y entramos en este (ver figura 16).

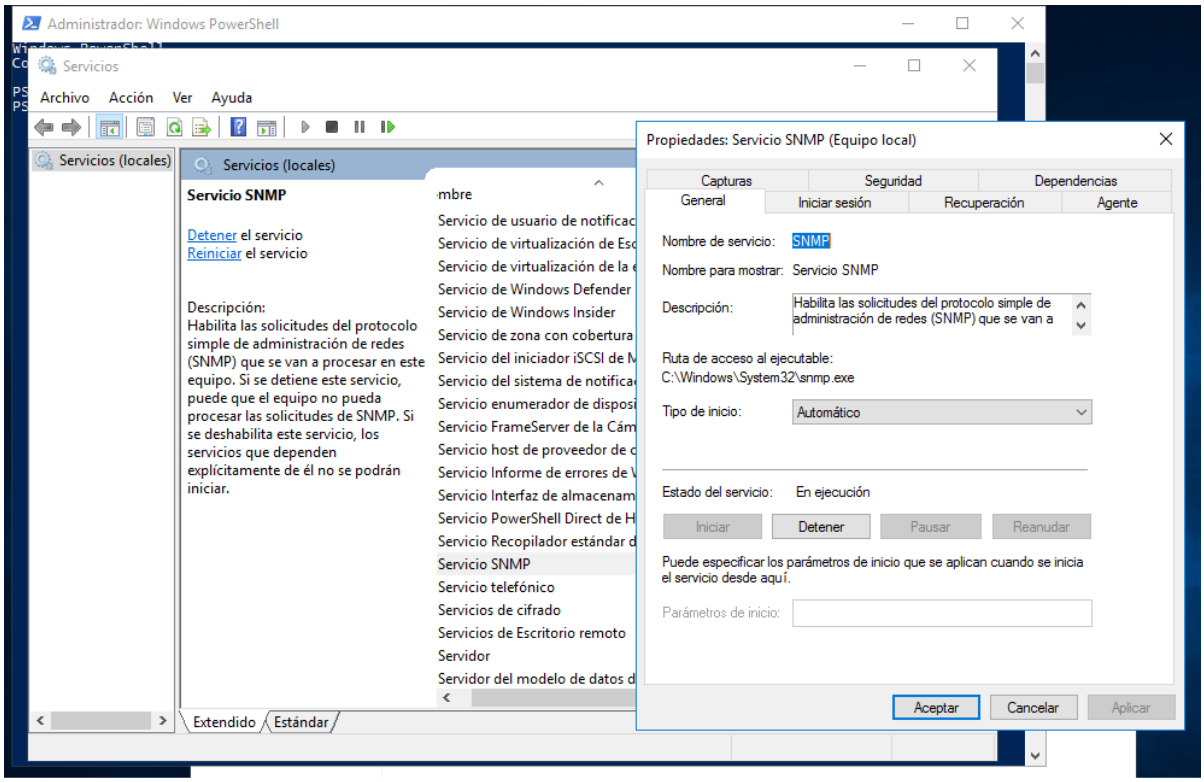

Figura 16: parámetros básicos del servicio SNMP (elaboración propia)

De esta ventana que se nos ha abierto, nos interesa principalmente el apartado *Seguridad*, donde especificaremos el tipo de comunidad SNMP, y el apartado *Capturas*, donde se configurarían las *traps* de los dispositivos monitorizados.

En la ventana de *Seguridad*, podremos crear diferentes tipos de comunidad, en este caso la comunidad es de solo lectura. Además, podemos especificar si queremos incluir todos los dispositivos de la red o solo los que indiquemos. En este último caso, necesitaríamos decir cuál es su dirección IP (ver figura 17).

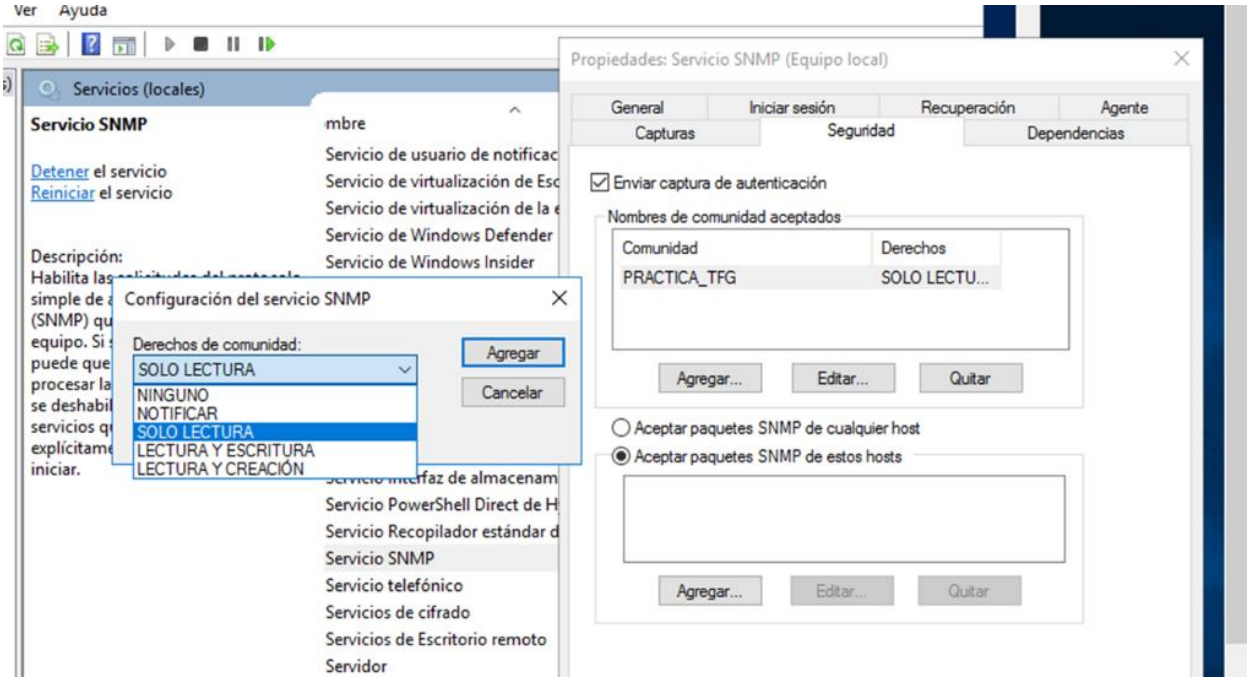

Figura 17: configuración de las comunidades de SNMP (elaboración propia)

En este caso, hemos creado una comunidad de solo lectura y hemos incluido la dirección IP del controlador de dominio del hipervisor 2 para monitorizar este, pero podríamos haber incluido todas las direcciones IP que quisiéramos siempre y cuando se encuentren en el mismo dominio.

Por último, hemos configurado las trampas o capturas desde el apartado de C*apturas*. En este apartado se incluye la comunidad y los dispositivos de los que queremos recibir esas capturas (ver figura 18).

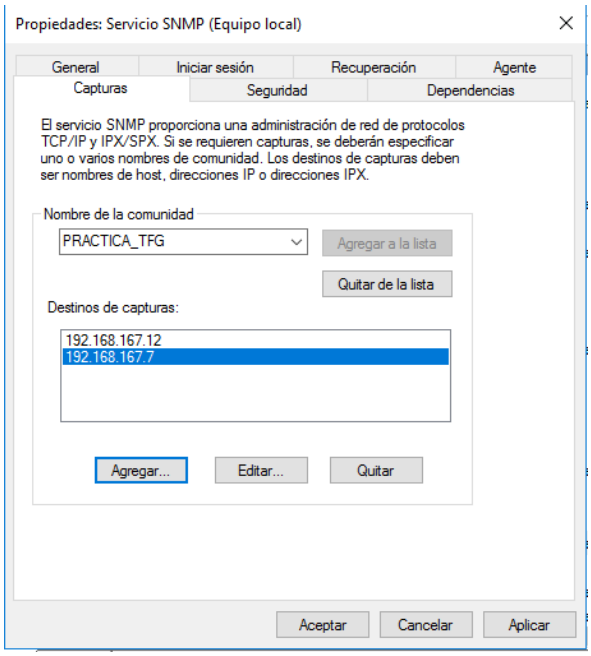

Figura 18: configuración de las trampas de SNMP (elaboración propia)

Además, la gestión de estas capturas se puede realizar aparte como otro servicio diferente al *Servicio SNMP* del administrador, desde el apartado *Captura SNMP* (ver figura 19).

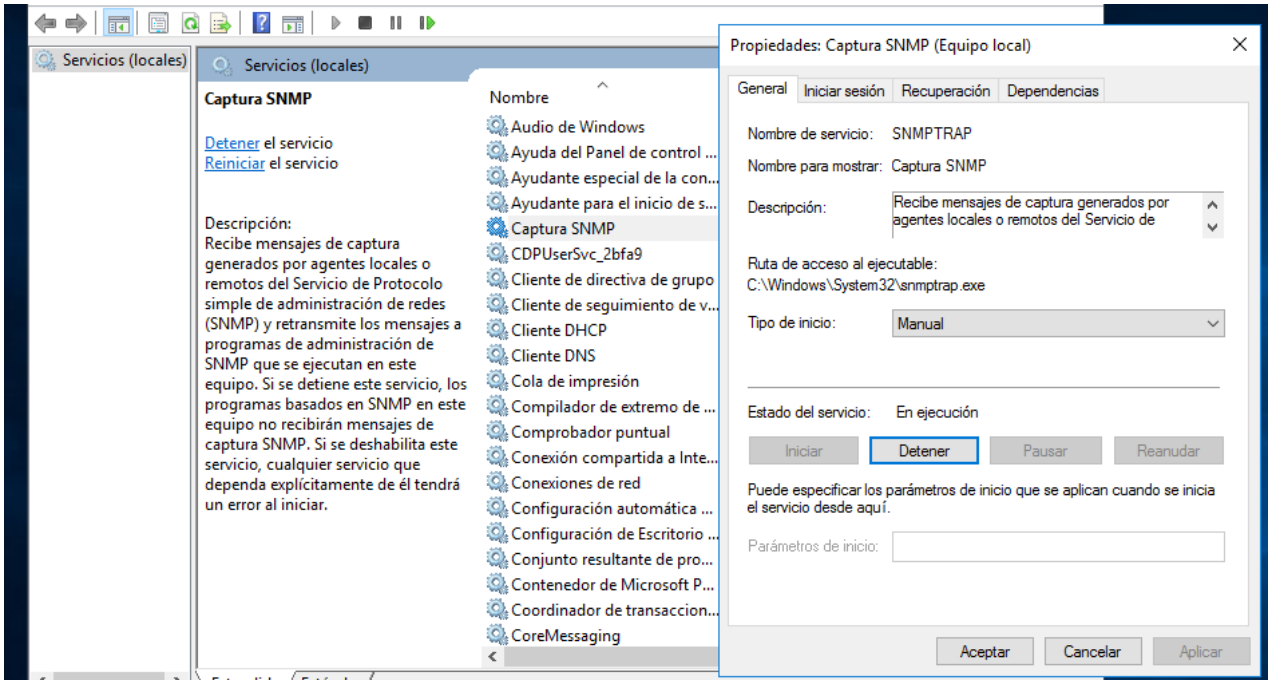

Figura 19: servicio de capturas de SNMP (elaboración propia)

4.4.3. Resultados obtenidos. Ventajas e inconvenientes

Actualmente, el Ejército de Tierra no cuenta con ninguna licencia de cualquier tipo de aplicación empleada para la monitorización a excepción de Nagios, cuyo uso está muy limitado a operaciones militares internacionales. Como consecuencia, si queremos verificar el funcionamiento del protocolo SNMP y monitorizar una red en cualquier escenario de operaciones, necesitaremos hacerlo de forma externa al nodo.

Para ello, hemos utilizado la aplicación *Network Inventory Adviser*. Esta aplicación es utilizada para la detección de redes y seguimiento de hardware y software. Basándose en el funcionamiento del protocolo SNMP, permite realizar un escaneo sobre la situación en la que se encuentran la CPU, la memoria, sistemas, audio y video, sistemas periféricos y, lo más importante para este trabajo, los recursos de la red (Network Inventory Advisor, s.f.).

Esta aplicación es de pago, pero disponemos de una prueba gratuita de 14 días donde podemos monitorizar todas estas funciones de hasta 25 dispositivos diferentes, aunque podríamos haber optado por cualquier otra aplicación, ya que disponemos de multitud de estas con similitud de funciones. Es por ello que se ha realizado una comparativa entre las principales aplicaciones empleadas en la monitorización, donde se reflejan los costes y principales características (ver anexo V).

Tras haberla instalado e iniciado, disponemos de muchas funciones, pero la más simple consiste en comprobar que en nuestro ordenador todo funcione correctamente (ver figura 20).

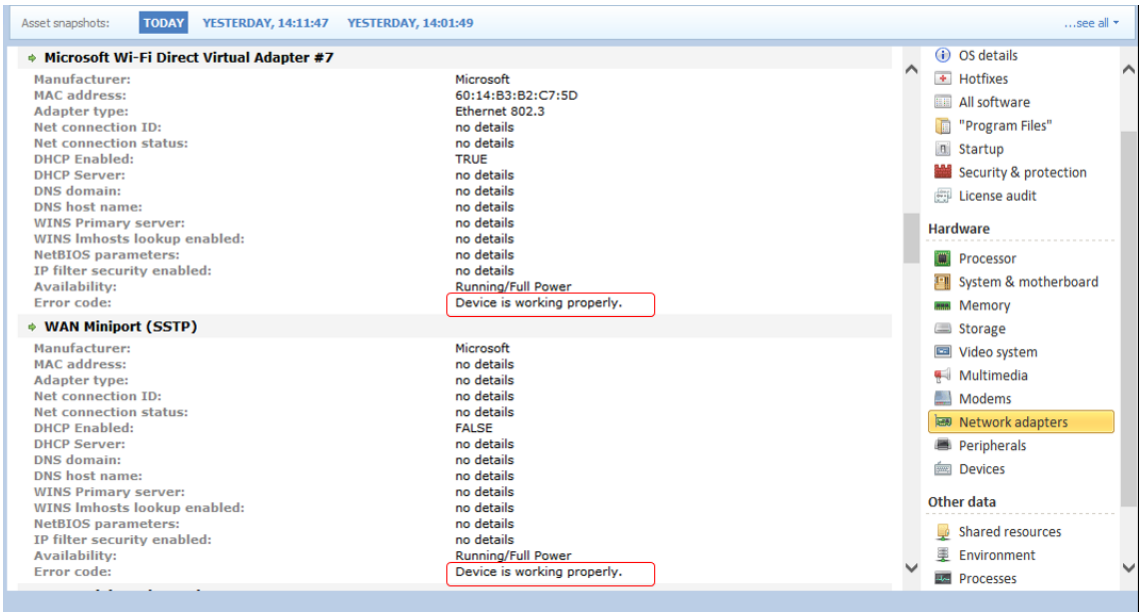

Figura 20: Análisis de los adaptadores de red de un ordenador personal con Network Inventory Adviser (elaboración propia)

En esta figura se muestra como gracias a esta aplicación se ha realizado un escaneo de todos los adaptadores de red, aunque solo se muestren dos, indicando que estos funcionan correctamente.

Además, podemos observar a la derecha de la figura, como aparte del análisis y escaneo de los adaptadores de red, tenemos una multitud de funciones como el escaneo de periféricos o

de los programas instalados.

También, podemos realizar un análisis de la red mediante el protocolo SNMP, donde se nos pedirá todo lo visto anteriormente, desde especificar el tipo de comunidad, hasta indicar el direccionamiento de los dispositivos que cuelgan del nodo (ver figura 21 y 22).

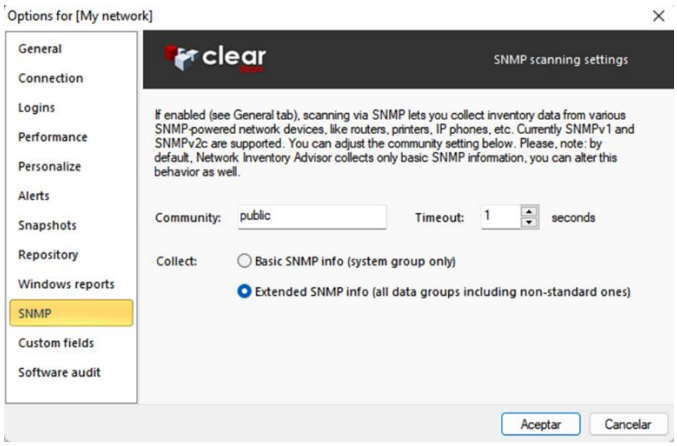

Figura 21: Especificación de las comunidades SNMP (elaboración propia)

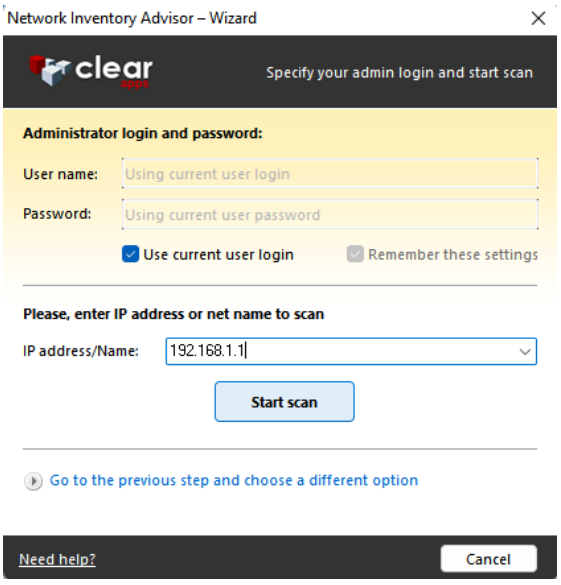

Figura 22: Especificación del escaneo de la IP de un dispositivo (elaboración propia)

De la misma forma que cuando se ha realizado el escaneo del ordenador personal, si hemos indicado correctamente la comunidad SNMP y los dispositivos de esta, podremos hacer un análisis de estos, además de tener acceso a un informe de alertas, donde se nos muestran todos los parámetros que se han analizado más al detalle.

En este informe, podemos seleccionar qué es lo que realmente queremos que aparezca, de cara para eliminar la información menos relevante y poder ir directamente a aquellos aspectos que tomen mayor protagonismo en el colapso de la red (ver figura 23).

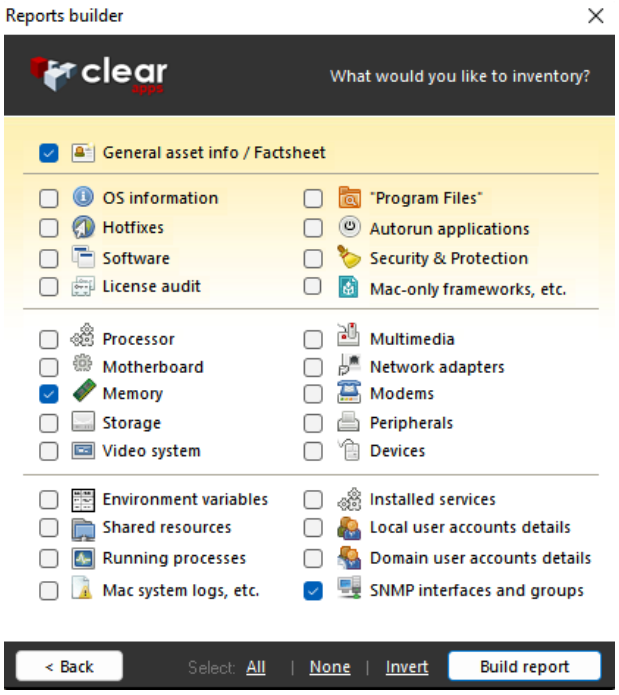

Figura 23: parámetros objeto de análisis (elaboración propia)

En esta figura, se puede observar todos los parámetros a analizar, de los cuales se ha seleccionado la memoria y las interfaces y grupos SNMP. Una vez aceptado el reporte, se nos muestra un informe de todos los dispositivos que hayamos incluido similar a la figura 20.

Este análisis ha sido realizado en base a las características de un ordenador personal; sin embargo, también podemos incluir la dirección IP de cualquier dispositivo de la misma forma que se muestra en la figura 22, pudiendo realizar de la misma forma la monitorización de todos los parámetros que especifiquemos, siempre y cuando este dispositivo se encuentre en la misma red que el ordenador desde el cual se realiza la monitorización.

Así, gracias a esta aplicación, la cual se basa en el uso de SNMP, podemos realizar un escaneo y análisis de todos los dispositivos que cuelgan de la red que hayamos configurado previamente. Gracias a esto, podemos visualizar de forma gráfica donde se encuentran los principales problemas causantes del colapso de la red.

5. CONCLUSIONES

Gracias a este proyecto, se ha estudiado la implementación del protocolo SNMP en un nodo de SC2NET, para su posterior uso, además del análisis de algunas aplicaciones diseñadas para el uso de este.

Para ello, se ha seguido una serie de pasos, empezando por la creación de una máquina virtual compatible a la versión del nodo.

Posteriormente, se llevó a cabo la implementación de esta en el nodo y la habilitación del protocolo SNMP. Este ha sido el paso más importante, no solo porque implica entender el funcionamiento del nodo de SIMACET, si no también, porque implica la implementación de una

máquina virtual en el nodo, a partir del cual, se proporcionó el servicio de monitorización para toda la maniobra.

Por último, se realizaron pruebas en base al protocolo SNMP, pero de forma independiente al nodo. Gracias a esto, se pudo verificar el funcionamiento de un protocolo de monitorización en un ordenador personal.

Como resultado de todo este proyecto, tanto yo como muchos de los sargentos con los que he podido contar, hemos llegado a la conclusión de que sería necesario la implementación de un servidor SNMP en todas o en la mayor parte de las unidades.

Un servidor con estas características facilita mucho la gestión y resolución de incidencias en las transmisiones y puede garantizar que en cuestión de minutos podamos conocer las causas de un mal funcionamiento en la red, en vez de tener que revisar cada dispositivo uno por uno en caso de incidencia.

La falta de este, sumado a la carga laboral que implica la realización de unas maniobras supone que en numerosas ocasiones no se disponga del tiempo necesario para poder gestionar las incidencias una por una.

De hecho, hoy en día gracias al creciente uso de las tecnologías, este protocolo proporciona tantas ventajas por las cuales también puede ser empleado en muchos más ámbitos, desde poder gestionar todos los dispositivos en red de una empresa, hasta los diferentes dispositivos que se encuentran en una red doméstica.

Pese a todas las ventajas que facilita, hay un gran inconveniente, al cual he hecho mención en diferentes ocasiones en este proyecto. SNMP necesita una aplicación para poder ver los resultados gráficamente, por lo que podemos llegar a configurar SNMP y sin esta aplicación no podemos sacarle una utilidad práctica.

La mejor alternativa que se ha contemplado para este proyecto consistía en la adquisición de la licencia de alguna de estas aplicaciones, como *Network Inventory Adviser*, cuyo funcionamiento es muy sencillo a la par de eficaz. Una vez adquirida la licencia y permisos de esta, es necesario la instalación de esta en una máquina virtual con la característica de SNMP para posteriormente poder implementarla en el nodo y proceder a su uso.

5.1. Líneas futuras

Tal y como se ha explicado anteriormente, para la visualización de resultados gráficos es necesario la adquisición de una aplicación apta para ello.

A día de hoy el Ejército de Tierra no cuenta con las licencias o permisos necesarios para poder implementar la mayoría de estas aplicaciones, a excepción de Nagios, pero como se ha indicado anteriormente, su uso está muy limitado a operaciones militares de carácter internacional.

Por consiguiente, resulta de vital importancia realizar un estudio sobre la viabilidad que supone la adquisición de una aplicación apta para la monitorización de redes.

Aunque existe una gran variedad de aplicaciones destinadas para la monitorización de redes, es necesario realizar un estudio en profundidad con el objetivo de poder seleccionar aquellas que nos proporcionen mayor tiempo de disponibilidad, mayor cantidad de nodos a monitorizar y por supuesto, que supongan un menor coste posible, a la vez que sean más fiables y seguras, con el objetivo de que no pongan en riesgo la información personal y más relevante

de nuestros ordenadores.

Referencias

CCNA desde cero, 2018. *SNMP: Funcionamiento y Configuración.* [En línea] Disponible en: https://ccnadesdecero.es/snmp-funcionamiento-configuracion/ [Último acceso: 24 Octubre 2022].

Cisco, 2022. *¿Qué es el monitoreo de red?.* [En línea] Disponible en: https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html [Último acceso: 24 Octubre 2022].

Ejército de Tierra, 2022. *Parque y Centro de Mantenimiento de Material de Transmisiones.* [En línea] Disponible en: https://ejercito.defensa.gob.es/unidades/Madrid/pcmmt/Organizacion/index.html [Último acceso: 24 Octubre 2022].

Mando de Adiestramiento y Doctrina, 2009. *Establecimiento y empleo de SIMACET.* PD3-602 ed. Granada.

Ministerio de Defensa de España, 2022. *División Operación de Red (DIVOPER).* [En línea] Disponible en: https://www.defensa.gob.es/cestic/mas/organizacion_cestic/divoper/ [Último acceso: 24 Octubre 2022].

Nagios, 2019. *SNMP Monitoring.* [En línea] Disponible en: https://www.nagios.com/solutions/snmp-monitoring/ [Último acceso: 24 Octubre 2022].

Network Inventory Advisor, 2022. *Asequible y Rentable Software de Inventario de la Red.* [En línea] Disponible en: https://www.network-inventory-advisor.com/es/ [Último acceso: 24 Octubre 2022].

Tekelec, 2012. *SNMP User´s Guide,* EE.UU.

ANEXOS

Anexo I. Análisis DAFO

Con el objetivo de realizar un análisis sobre las debilidades, amenazas, fortalezas y oportunidades, se ha realizado un análisis DAFO (ver tabla 3), donde se muestran todas estas en detalle.

Debilidades *Falta de medios necesarios para la monitorización de redes y dispositivos.*	***Amenazas*** *Coste adicional que supondría la adquisición de esta herramienta, además del personal necesario para su uso y el coste que supondría el aprendizaje de esta herramienta.*
Fortalezas *Permitiría que las redes y dispositivos puedan ser supervisados con mayor facilidad, lo que conlleva a una mejor respuesta ante incidencias, reduciendo los tiempos necesarios para solventarlas.*	***Oportunidades*** *Poder llegar a la implementación de esta herramienta, tanto en el ámbito nacional, como en las operaciones militares internacionales.*

Tabla 3: Análisis DAFO (elaboración propia)

Este análisis DAFO se ha realizado en base a la implementación de una aplicación apta para monitorizar desde el propio nodo de SIMACET.

Dentro de las debilidades, nos encontramos en la situación actual de no disponer de ninguna de estas aplicaciones para monitorizar, lo cual conlleva al gasto de todos los medios necesarios y tiempo para poder solucionar las incidencias asociadas al empleo de la red.

Si nos decidimos por adquirir una aplicación para la monitorización, nos encontramos con el problema de necesitar gente especializada en poder manejar esta, lo cual se traduce en un gasto en adquisición y enseñanza.

No obstante, como aspectos positivos se encontrarían el hecho de que puede facilitar la supervisión de redes y dispositivos, permitiendo un ahorro del tiempo durante los ejercicios, además de un aprovechamiento más eficaz de los recursos. Así, de cara a un futuro, podría implementarse y experimentar mejoras, no solo para ser utilizado en el ámbito nacional, si no también, durante el desarrollo de operaciones militares en el extranjero.

Anexo II. Estructura orgánica de la DIVOPER

El CESTIC es el Centro de Sistemas y Tecnologías de la Información. Entre sus funciones principales se encuentran: la planificación y desarrollo de políticas y estrategias para el Departamento, dirigir el diseño, obtención y configuración de las tecnologías, información y comunicaciones, coordinar la gestión de la información y conocimiento, gestionar los recursos en el marco de I3D, controlar la operación y mantenimiento de los sistemas y tecnologías, impulsar la transformación digital y dirigir y supervisar la integración de las redes y sistemas de información.

La DIVOPER forma parte de la estructura orgánica del CESTIC (ver figura 24), siendo el principal órgano encargado de la monitorización necesaria para garantizar el correcto funcionamiento de los servicios.

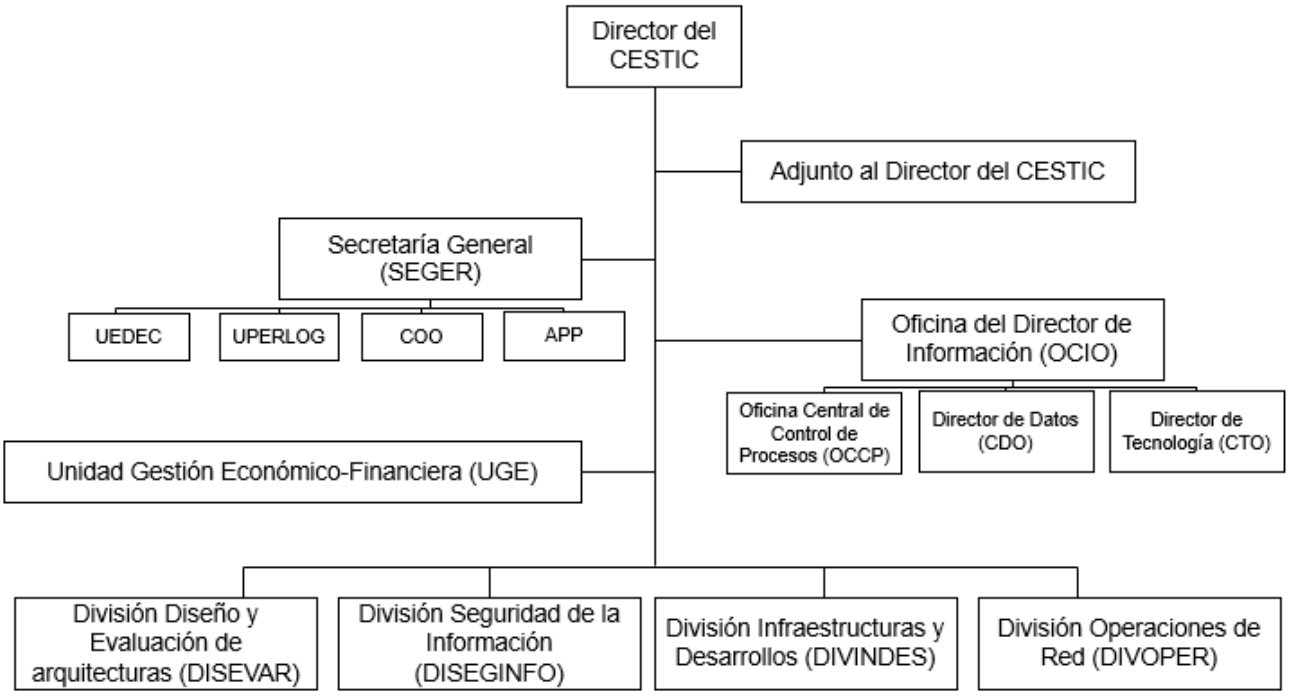

Figura 24: Estructura orgánica del CESTIC (elaboración propia)

Anexo III. Personal entrevistado del área de SIMACET

En el siguiente anexo anexo se muestra el personal entrevistado y su expediente laboral, por el cual han tomado importancia en este proyecto (ver tabla 4).

	PERSONAL 1	PERSONAL 2
NOMBRE	PACHECO MURTULA, ISMAEL	ANDRADE GARCÍA, JOSE MARÍA
SITUACIÓN	SERVICIO ACTIVO	SERVICIO ACTIVO
EMPLEO	SARGENTO	SARGENTO
TIEMPO DE SERVICIO EN EL ÚLTIMO EMPLEO	7 AÑOS	6 AÑOS
DESTINO	BRIGADA EXTREMADURA XI	BRIGADA EXTREMADURA XI
TÍTULOS	TÉCNICO SUPERIOR EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS DE RED	TÉCNICO SUPERIOR EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS DE RED
MISIONES	2021 EFP LETONIA 2017 LIBRE HIDALGO-LIBANO	2021 EUTM MALI 2019 APOYO IRAQ

Tabla 4: Personal entrevistado de SIMACET (Fuente: SIPERDEF)

Anexo IV. Cómo crear una máquina virtual

En el siguiente anexo se muestra cómo crear una máquina virtual con Hyper-v.

El primer paso sería abrir la aplicación y seleccionar la opción de crear nueva máquina virtual.

A continuación, se nos abrirá una pestaña, donde se nos pedirá indicar el nombre de nuestra máquina virtual, donde queremos almacenar esta, el tipo de generación que vamos usar, la memoria RAM de inicio y el tamaño de la propia máquina virtual. Por último y antes de instalar, se nos pedirá si queremos incluir un sistema operativo o si queremos añadirlo más adelante.

Dentro del tipo de generación a asignar, podemos elegir entre la 1 o 2, siendo la 2 una versión más moderna, incluyendo más características y con un sistema operativo de 64 bits, a diferencia de la primera generación que es solo de 32 bits.

La memoria RAM indica la propia memoria que esta máquina virtual va a consumir del propio ordenador físico desde donde se crea la propia máquina.

Para el sistema operativo, en este proyecto se ha utilizado Windows Server 2016; sin embargo, podemos seleccionar el que más nos convenga según la finalidad que queramos obtener de la máquina virtual.

Tras esto, ya estaría creada la máquina virtual, pero no instalada. Para ello, abrimos esta, mediante la opción de conectar y a continuación, se abrirá la máquina. Al ser la primera vez que nos conectamos a esta, y que todavía no hemos instalado, se nos abrirán algunas pestañas donde nos darán unas instrucciones previas para la instalación de esta. Tras ello y un tiempo de instalación, ya tendremos nuestra máquina virtual creada y lista para poder ser utilizada.

Actualmente, tenemos diferentes tipos de aplicaciones para crear máquinas virtuales, como por ejemplo VirtualBox; sin embargo, la utilización de Hyper-v se debe a que, si hubiésemos creado la máquina virtual con otra aplicación, hubiera dado problemas de compatibilidad de cara a implementar esta máquina en el servidor.

Anexo V. Aplicaciones para la monitorización

En la tabla 4 se pueden observar las principales aplicaciones civiles para la monitorización de redes y recursos, además de mostrar el precio por la adquisición de la licencia para un nodo. Cabe destacar que se puede monitorizar gran cantidad de dispositivos, en algunas aplicaciones hasta 1500 dispositivos, pero el precio es variable en función de la cantidad de dispositivos.

Para la mayoría de estas aplicaciones, estas ofrecen diferentes planes de compra, en función del tiempo de adquisición de la licencia y de los dispositivos a monitorizar. Se ha realizado una comparación para una cantidad de dispositivos y tiempo similar en todas las aplicaciones, pero siendo esta, un valor aproximado y variable en función de las necesidades del cliente.

Aplicación	***Coste por la adquisición de la licencia (en €)***	***Condiciones de compra***	***Prueba gratuita***
Network Inventory Adviser	*1.200,00*	*Se requiere mínimo la compra de la licencia para 25 dispositivos. Por este precio podemos monitorizar hasta 1500 dispositivos*	*15 días*
Pandora FMS	*1.000,00*	*Permite monitorizar hasta 200 dispositivos durante un año*	*30 días*
Solar winds	*1.175,00*	*Permite la monitorización de hasta 6000 dispositivos*	*30 días*
WhatsUp*Gold	*1.800,00*	*La licencia implica mínimo 1 año, pudiendo monitorizar desde 100 a 1000 dispositivos.*	*12 meses*
Logic Monitor	*1.750,00*	*Es compatible con más de 1000 tecnologías diferentes, ofreciendo una gran variedad de recursos de software*	*14 días*

Tabla 5: Tabla comparativa de las principales aplicaciones para la monitorización (elaboración propia)