**Monitoreo y análisis de trafico de la topología en Zabbix de los elementos de red y ESP32**

# Contenido

[Introducción 3](#_bookmark0)

[Objetivos 3](#_bookmark1)

[Objetivo General 3](#_bookmark2)

[Objetivos Específicos 3](#_bookmark3)

[Marco Teórico 4](#_bookmark4)

[Desarrollo 5](#_bookmark5)

[Instalación de Zabbix 5](#_bookmark6)

[Instalación del Servicio SNMP en el Host 14](#_bookmark7)

[Configuración de Mikrotik para Zabbix 17](#_bookmark8)

[Añadir equipos PC 20](#_bookmark9)

[Creación del mapa de la topología en el servidor Zabbix 21](#_bookmark10)

[Agregar ESP32 a Zabbix 24](#_bookmark11)

[Resultados 29](#_bookmark12)

[Conclusiones 40](#_bookmark13)

[Recomendaciones 41](#_bookmark14)

[Referencias 42](#_bookmark15)

# Introducción

El presente informe documenta el desarrollo y análisis de un sistema de monitoreo basado en Zabbix para una infraestructura compuesta por un punto de acceso (AP), cinco computadoras y cinco nodos implementados con placas ESP32. Cada nodo está equipado con sensores capaces de recolectar datos ambientales en tiempo real. El protocolo utilizado para la comunicación entre los nodos y el servidor de monitoreo es el Simple Network Management Protocol (SNMP), bajo el estándar MIB-II definido por la ISO.

El monitoreo abarca desde la capa de red (IP) hasta la capa de aplicación, enfocándose en las interacciones propias del protocolo SNMP, incluyendo operaciones como Get, Response, y Set, así como el análisis de los cambios efectuados mediante comandos SNMP. Adicionalmente, se estudian los valores obtenidos a través de las Management Information Bases (MIB), los cuales permiten estructurar la información recolectada por los sensores.

El objetivo principal de este proyecto es evaluar la funcionalidad y desempeño del monitoreo SNMP en Zabbix, destacando la forma en que se gestionan las solicitudes y respuestas dentro de la red, y su impacto en el análisis de datos provenientes de sensores distribuidos.

# Objetivos:

# Objetivo General:

Diseñar, implementar y analizar un sistema de monitoreo basado en Zabbix utilizando el protocolo SNMP para la gestión de datos recolectados por sensores en una red de nodos ESP32.

# Objetivos Específicos:

* Configurar el protocolo SNMP en los nodos ESP32 para habilitar operaciones de monitoreo remoto mediante Zabbix.
* Implementar las funciones principales del protocolo SNMP, incluyendo las operaciones Get, Response, Set, y la evaluación de los cambios efectuados con comandos SNMP.
* Analizar el modelo MIB-II en el contexto del monitoreo de sensores, comprendiendo su estructura jerárquica y el manejo de valores en las capas de red y aplicación.
* Evaluar la capacidad de Zabbix para gestionar datos en tiempo real provenientes de los nodos, asegurando la confiabilidad en la adquisición y presentación de los datos recolectados.
* Documentar el flujo de datos desde las capas más bajas (IP) hasta la aplicación, resaltando la interacción entre los elementos de la red y el servidor de monitoreo.

# Marco Teórico Monitoreo de zabbix

Mikrotik, conocido por su versatilidad y eficiencia en la gestión de redes, ofrece funcionalidades que permiten una supervisión efectiva mediante el protocolo SNMP (Protocolo Simple de Administración de Red). Este protocolo permite la recolección de información sobre el estado y el rendimiento de los dispositivos, incluyendo métricas como el uso de CPU, el tráfico de red, las interfaces activas, y el estado de las conexiones. Zabbix utiliza estos datos para generar gráficos, informes y alertas, facilitando la detección temprana de problemas (Zabbix LLC. (2023)).

La configuración de Zabbix para monitorear dispositivos Mikrotik implica varios pasos clave. En primer lugar, es necesario habilitar SNMP en el dispositivo Mikrotik, asegurando que las interfaces y el acceso a los datos estén correctamente configurados. Esto incluye establecer una comunidad SNMP que permita a Zabbix recopilar información de manera segura.

# Ventajas de utilizar Zabbix con dispositivos de red

Radica en la capacidad de obtener información en tiempo real sobre el rendimiento de la red. Los administradores pueden recibir alertas inmediatas ante condiciones anormales, como un uso elevado de CPU o una caída en el tráfico de red, lo que les permite actuar rápidamente para resolver problemas antes de que afecten a los usuarios finales.

# Protocolo SNMP

Es un estándar utilizado para la comunicación y gestión de dispositivos en redes IP. Permite monitorear parámetros críticos mediante objetos identificados por OIDs (Object Identifiers), facilitando tanto la consulta de información (get-request) como la modificación de configuraciones (set-request) SNMP Research International. (2020). En el contexto de Zabbix, SNMP asegura una interacción eficiente entre el servidor de monitoreo y los dispositivos supervisados, permitiendo un control granular y seguro.

# Get-request: Solicitud de datos

El comando get-request es utilizado por el gestor SNMP (como Zabbix) para obtener información específica de un agente (por ejemplo, un sensor o un dispositivo de red). Se basa en identificar un parámetro particular mediante su OID (Object Identifier) Espressif Systems. (2021).

# Set-request: Modificación de datos

El comando set-request permite al gestor SNMP modificar la configuración o el estado de un dispositivo supervisado Forouzan, B. A. (2021). Este comando también utiliza el OID para identificar el parámetro que debe ser modificado.

Estos comandos son esenciales en el protocolo SNMP porque:

* **get-request** permite recopilar datos para monitoreo y análisis.
* **set-request** habilita el control remoto de dispositivos.

# Desarrollo

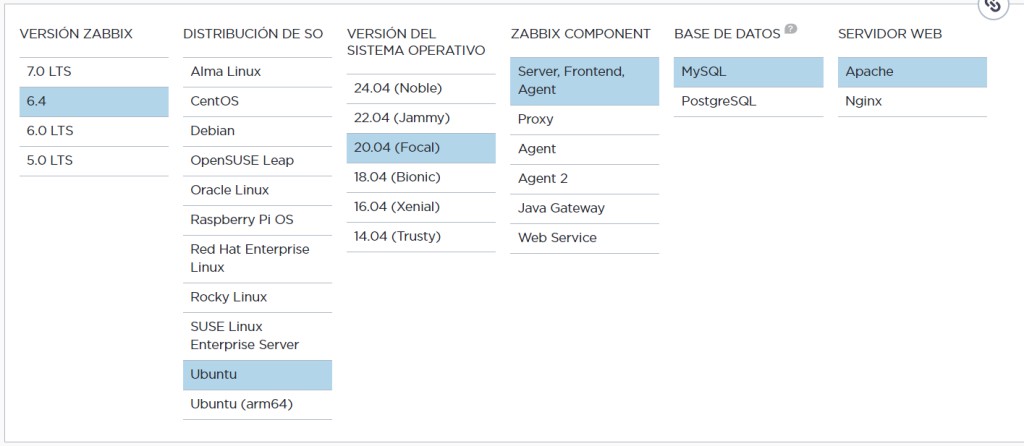
# Instalación de Zabbix

Como primer paso se debe dirigir a la pagina oficial de Zabbix para descargar este software de monitoreo mediante el siguiente enlace: <https://www.zabbix.com/la/download>

Porteriormente se debe elegir la plataforma en la que se va a trabajar que en este caso es Ubuntu de version 20.04, la versión de zabbix 6.4 debido a ser la mas estable, y servicios de MySQL y servidor Apache.

# Figura 1

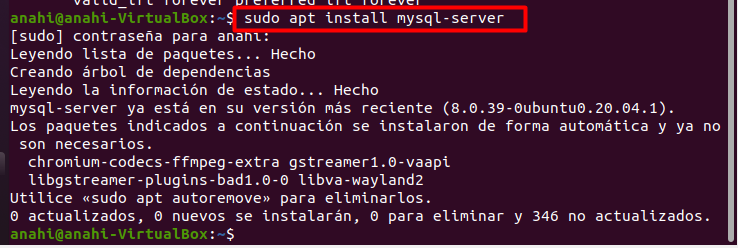
*Elegir la plataforma Zabbix*

**

Se necesita instalar el servicio de MySQL, ya que se va a crear la base de datos con este sistema de gestión.

# Figura 2

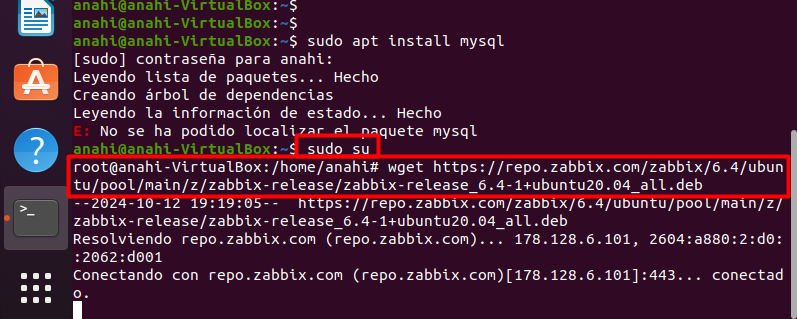
*Instalar servidor de MySQL*

**

El siguiente paso es iniciar sesión con privilegios de root, y posteriormente descargar e instalar los paquetes de zabbix para configurar en el repositorio.

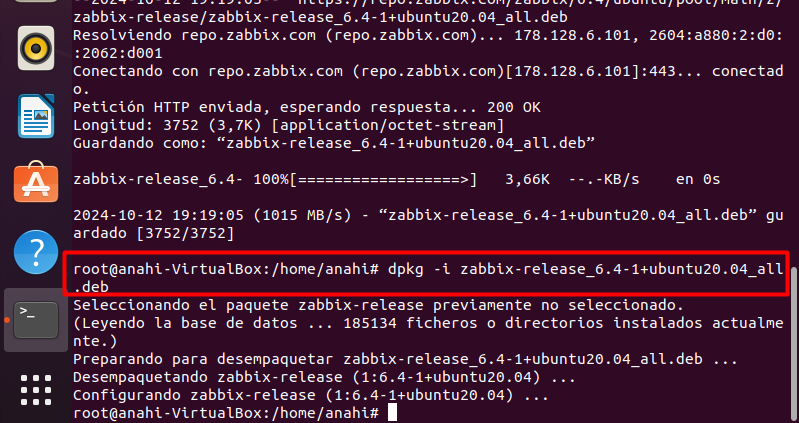
# Figura 3

*Descargar el paquete de Zabbix*

**

# Figura 4

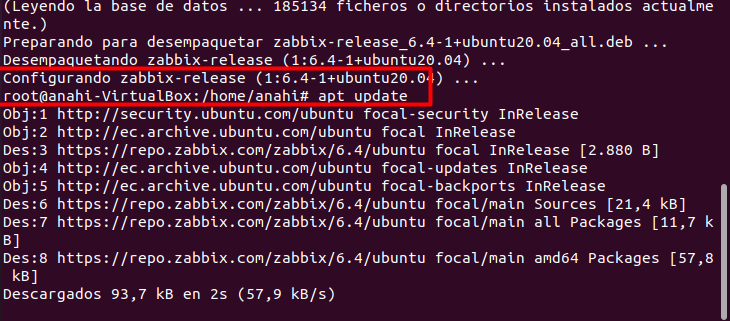
*Instalar el repositorio de Zabbix*

**

Una vez instalado el repositorio, se debe actualizar los paquetes con el comando apt update

# Figura 5

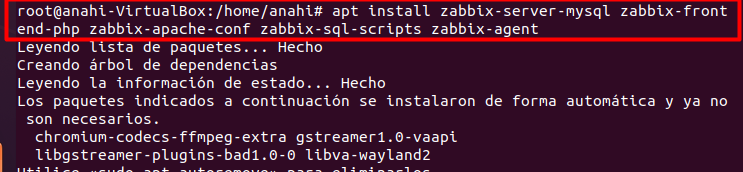
*Actualizar los paquetes*

**

Posteriormente se debe instalar zabbix y sus componentes, ya que se va usar zabbix como servidor y configurar para utilizar mysql como base de datos, tambien se instala los archivos para integrar el servidor web apache, además se instala el agente de zabbix para el monitorio de los datos.

# Figura 6

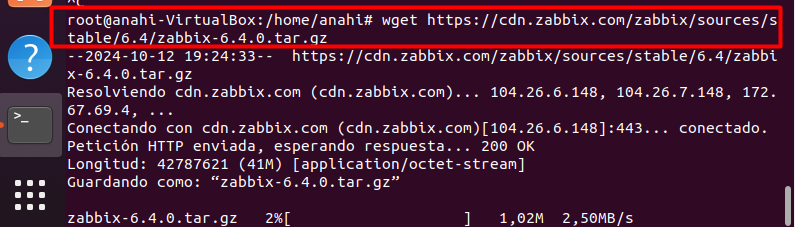
*Instalación de Zabbix*

**

El código fuente debe ser descargado, el cual es un archivo comprimido .tar de la versión seleccionada 6.4 de Zabbix.

# Figura 7

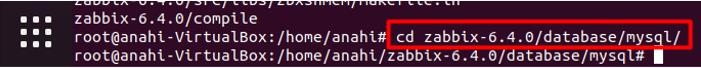
*Descargar el código fuente*

**

A continuación, se debe ingresar a la carpeta de la base de datos ya que contiene los scripts SQL para ser configurado el software zabbix con la base de datos y se puede añadir datos predeterminados.

# Figura 8

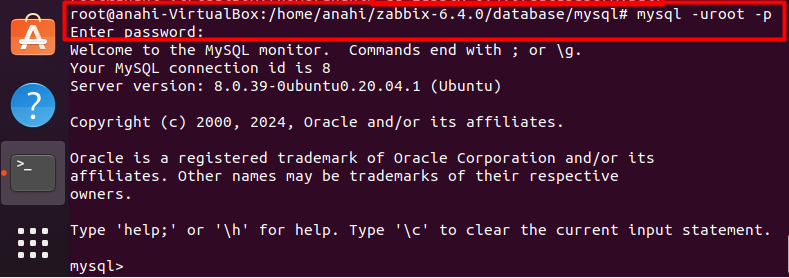
*Cambiar de directorio para configurar mysql*

**

Mediante el usuario root se va a iniciar sesión con mysql, el cual solicitara la contraseña respectiva.

# Figura 9

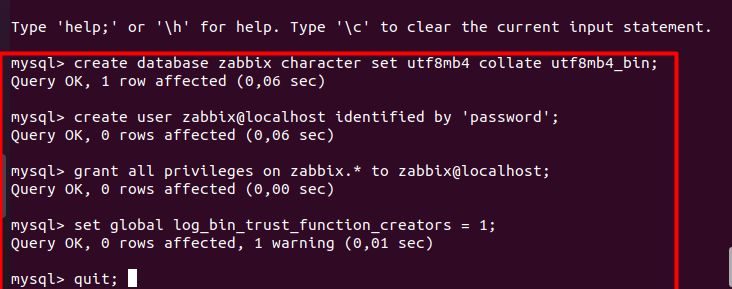
*Configuración de la base de datos*

**

Después de ingresar con root a mysql, se debe realizar configuraciones para crear base de datos, crear usuario, y que dicho usuario creado tenga privilegios.

**Figura 10**

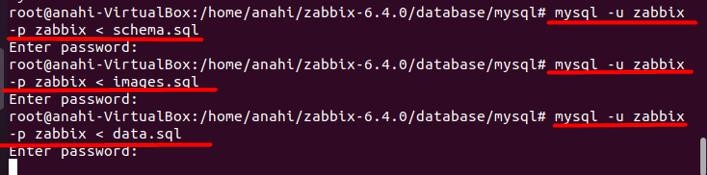
*Configuraciones dentro de MySQL*

**

Posteriormente se debe salir de la base de datos y dentro de la carpeta de zabbix ejecutar los siguientes comandos para importar los esquemas, imágenes y datos para la respectiva base de datos del software Zabbix.

# Figura 11

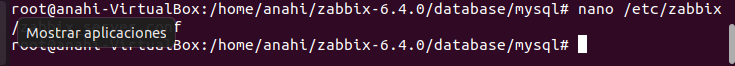
*Importar datos a la base de datos*

**

Mediante el comando nano se procede a ingresar al archivo de configuración de Zabbix, para que sea editado en la parte de BDPassword para agregar la contraseña para el acceso y conexión entre zabbix y la base de datos mysql.

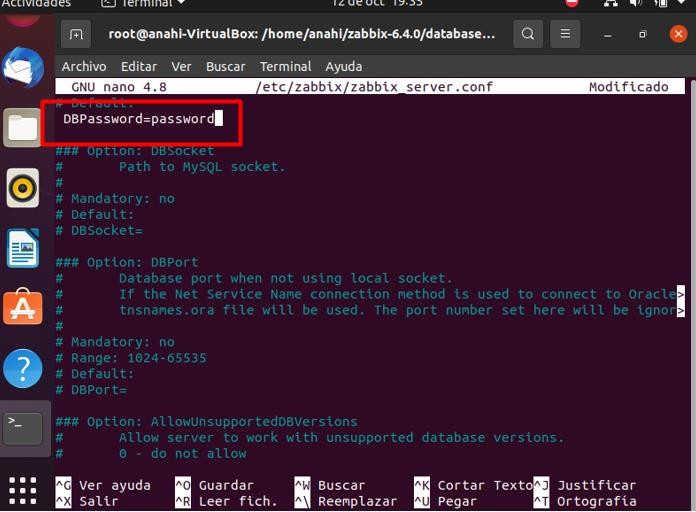
# Figura 12

*Edición de archivo de configuración*

**

# Figura 13

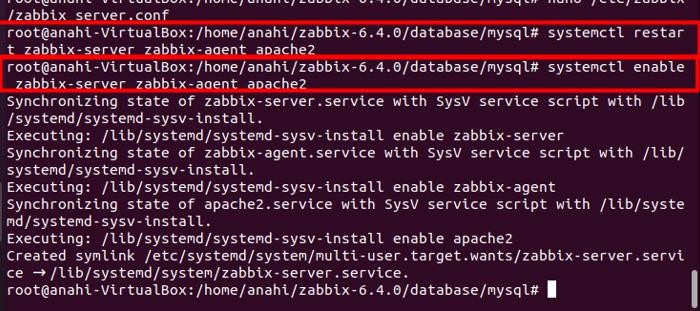
*Agregar la contraseña de base de datos*

**

Al terminar las configuraciones, se necesita reiniciar y habilitar los servicios de Zabbix para que los cambios sean aplicados, además para que sean iniciados automáticamente cuando el servidor se reinicie.

# Figura 14

*Reiniciar servicios Zabbix*

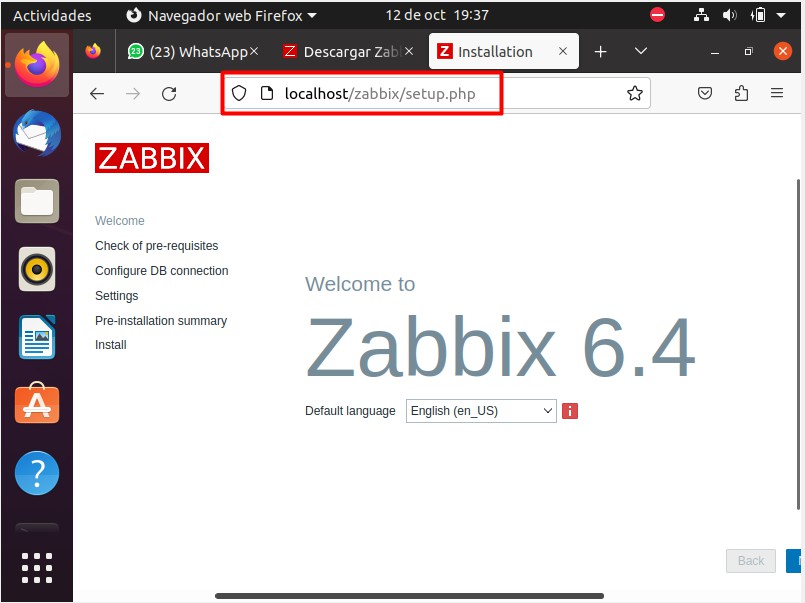
**

Para comprobar que el servicio esté funcionando y activado, se debe colocar

**localhost/zabbix** en el navegador para su posterior instalación.

# Figura 15

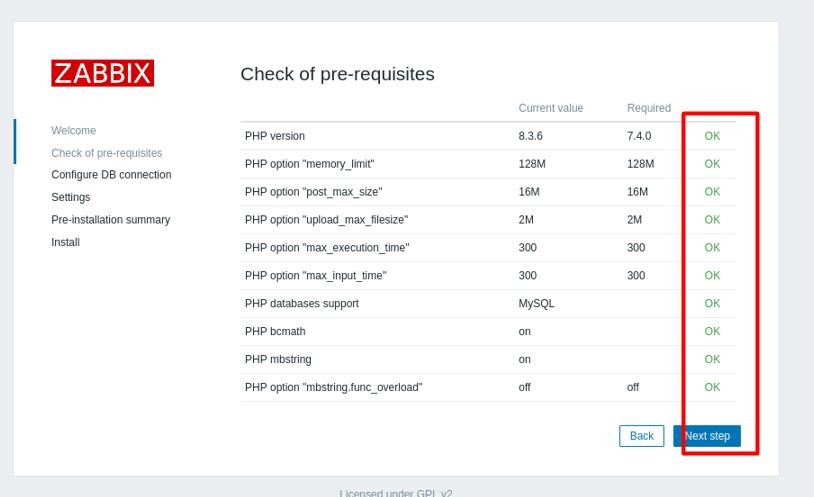
*Servidor Zabbix activo*

**

A continuación, se puede observar los requisitos que debe cumplir para la instalación del software para el monitoreo con el servidor, los cuales están todos correctamente establecidos.

# Figura 16

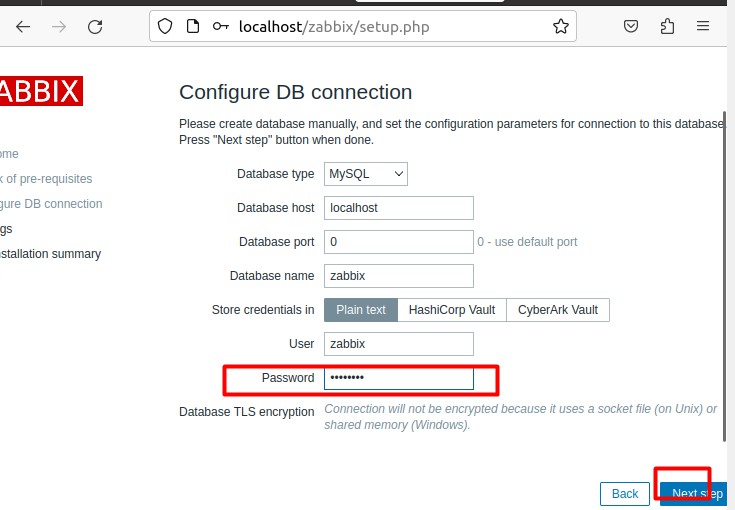
*Revisión de prerequisitos de zabbix*

**

El siguiente paso es asginar una contraseña para el ingreso por su interfaz gráfica del servidor zabbix.

# Figura 17

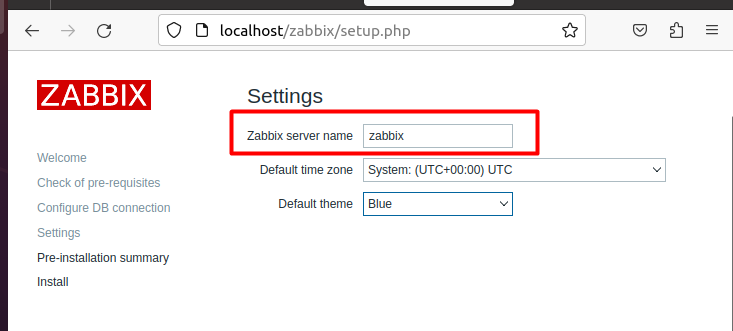
*Asignar contraseña para zabbix*

**

Luego se colocar un nombre con el que se va a conocer al servidor zabbix, y se puede configurar la zona horaria y color de tema predeterminado.

# Figura 18

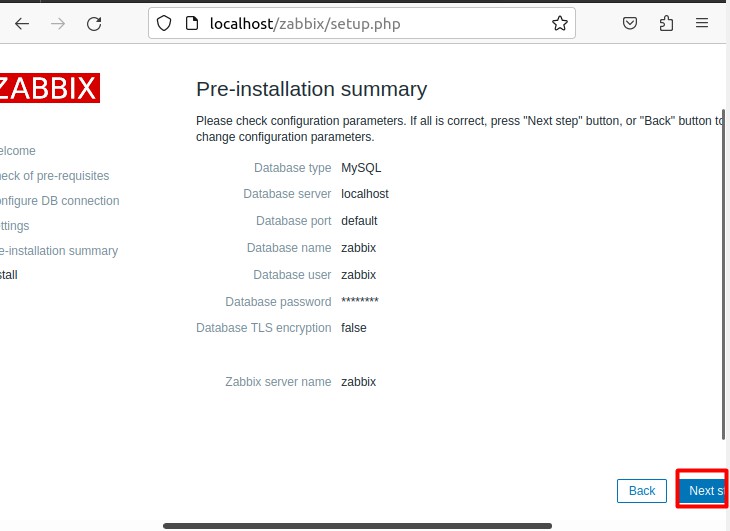
*Configuraciones del servidor Zabbix*

**

Al terminar de configurar el servidor zabbix, indica un resumen de las configuraciones asignadas en la preinstalación.

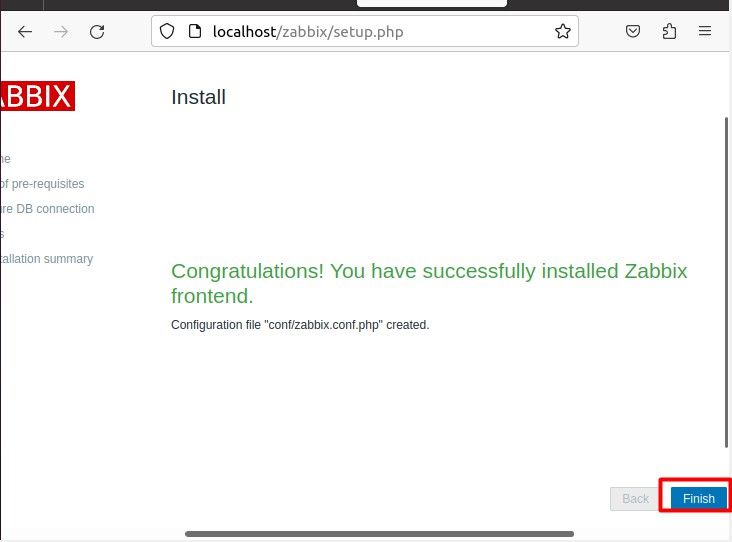
# Figura 19

*Resumen de las configuraciones del servidor Zabbix*

**

# Figura 20

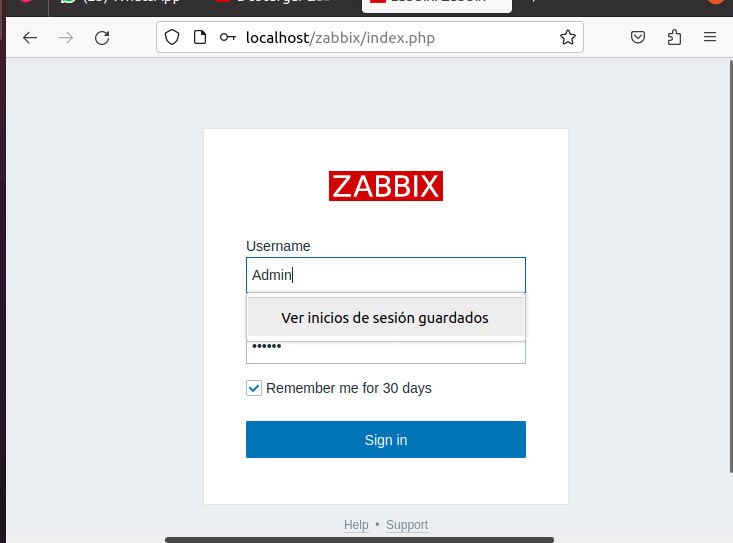
*Instalación completada del servidor Zabbix*

**

Al terminar la instalación, se procede a ingresar las credenciales para acceder al centro de monitoreo del servidor zabbix.

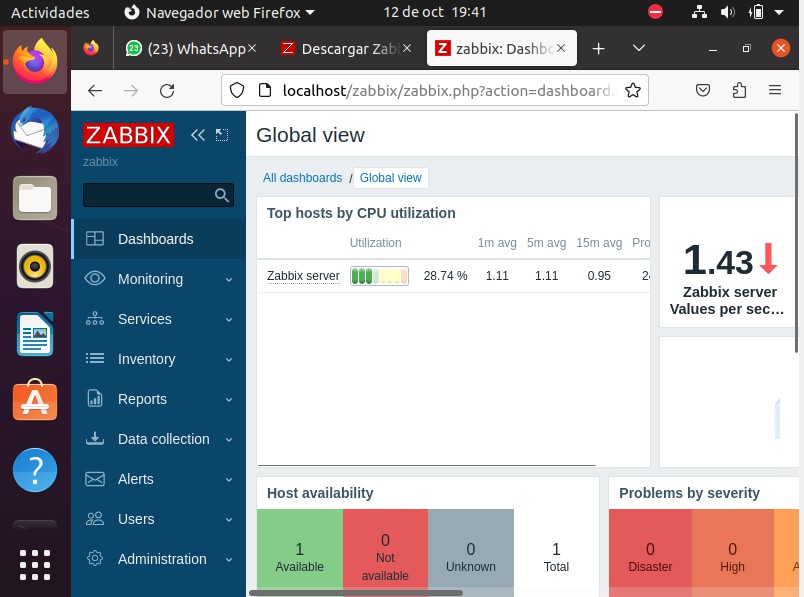
# Figura 21

*Inicio de sesión de zabbix*

**

# Figura 22

*Acceso al panel de control de Zabbix*

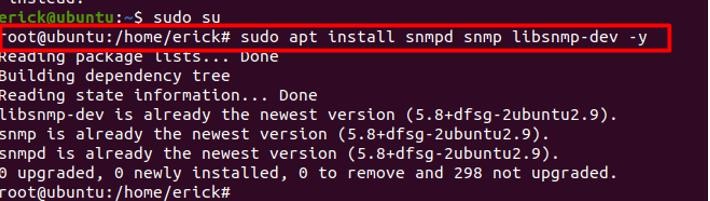
**

# Instalación del Servicio SNMP en el Host

Se instala el servicio SNMP, tanto como las librerías que ayudaran a conectar con el servidor de Zabbix.

# Figura 23

*Instalación SNMP en host*

**

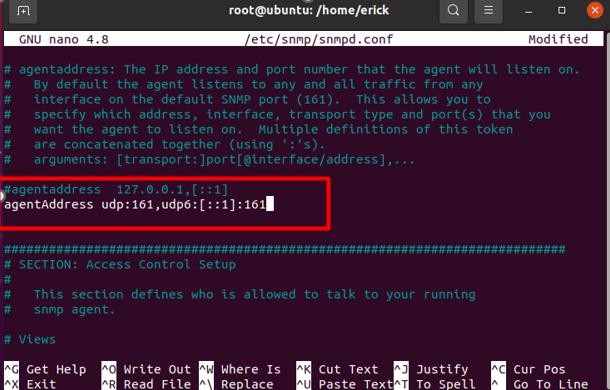
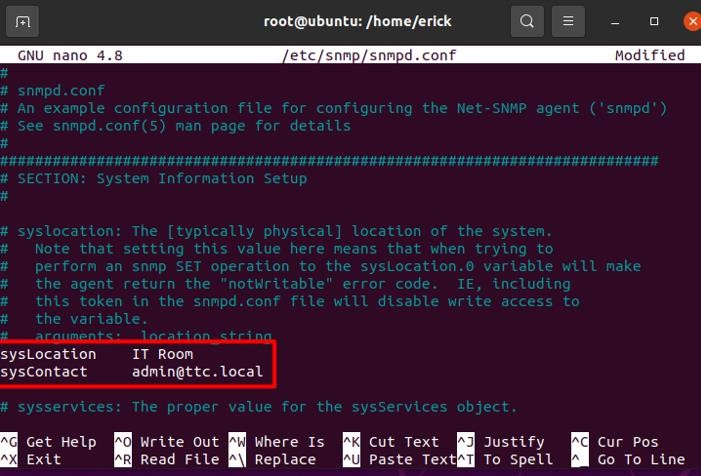
Una vez instalado se configura en el SNMP, accediendo a su archivo de configuración

/etc/snmp/snmpd.conf, para editar tanto el puerto y la ip.

Además, se edita el lugar y contacto que estará asociado al equipo para que el agente de Zabbix pueda supervisar, una vez configurada se guarda la configuración.

# Figura 24

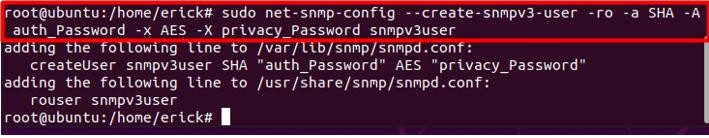
*Configuración del SNMP*

**

A continuación, se crea el usuario y la contraseña, con un formato de la contraseña y su encriptación para el SNMP.

# Figura 25

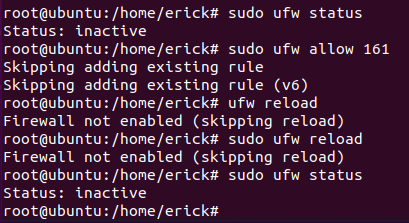
*Creación de usuario y contraseña del SNMP del Host*

**

Una vez establecido el tanto la instalación y la configuración del SNMP, establecen las reglas del firewall para que permita la administración del host.

# Figura 26

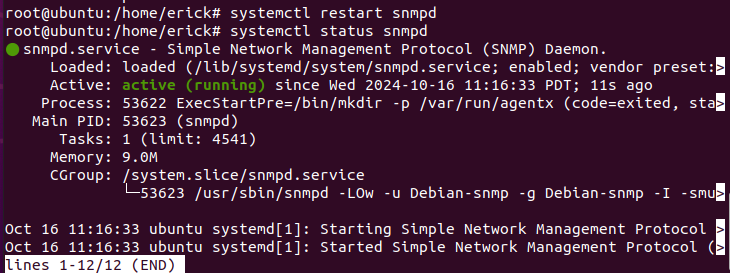
*Reglas del Firewall*

**

Luego, se resetea el servicio SNMP para verificar que las configuraciones estén correctas.

# Figura 27

*Verificación del estado del SNMP.*

**

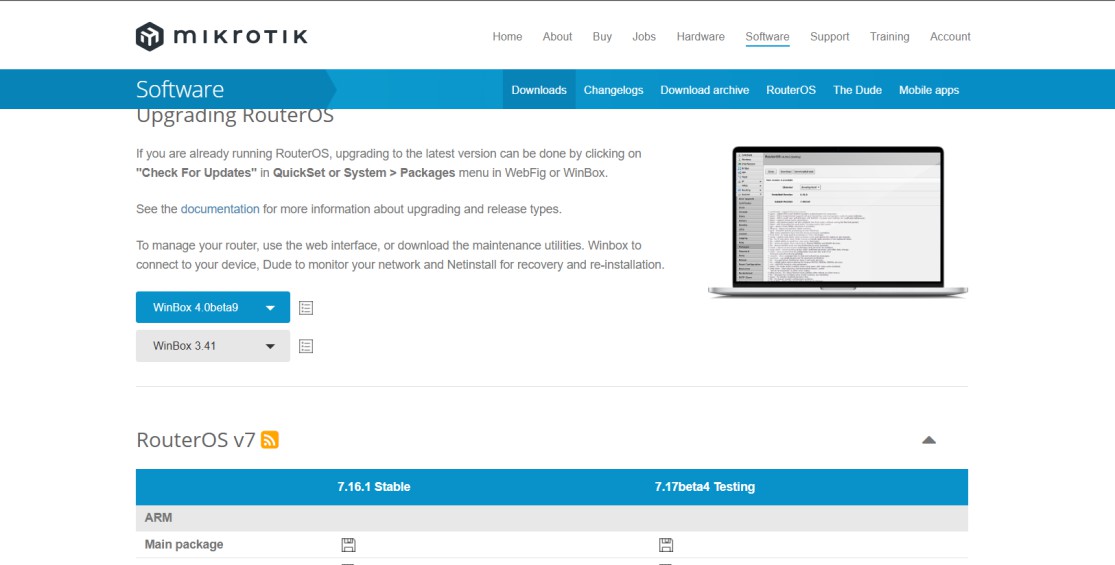
A continuación, se dará a conocer la forma entre la conexión de la red usando SNMP en todos los extremos de la red realizada, para ellos se han colocado el protocolo SNMP en el Mikrotik como en los demás usuarios, una vez hecha la conexión se realiza la prueba de rendimiento, usando para estos casos la herramienta de “Iperf” para esta prueba.

# Configuración de Mikrotik para Zabbix

Primeramente, el hardware debe ser conectado a la computadora para que lo reconozca, donde se descarga la versión correspondiente al software de Router que es WinBox el cual, es compatible con el Mikrotik, para administrar y habilitar el dispositivo.

# Figura 28

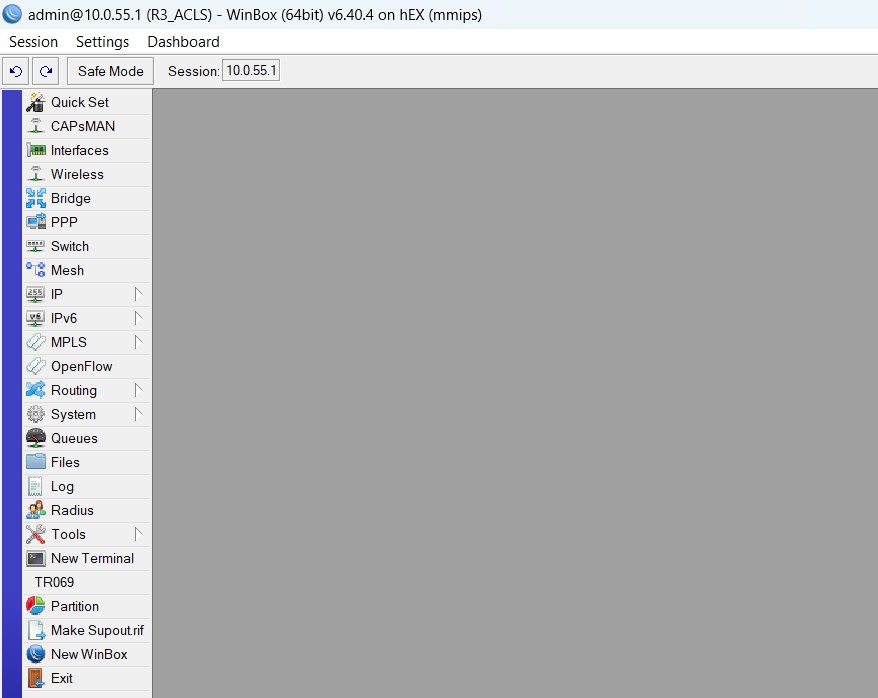
*Descargar paquete del Router compatible con el Mikrotik*

**

# Figura 29

*Interfaz de WinBox activa para conectar a los dispositivos*

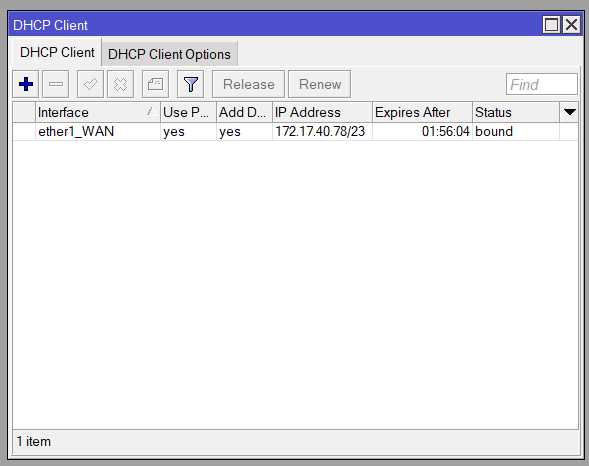
WinBox tiene una interfaz gráfica para la gestión, y se permita agregar mediante la configuración hosts clientes al dispositivo Mikrotik, por tanto, se debe habilitar cada puerto que tiene diferentes direcciones IP cada uno.



# Figura 30

*Configuración del cliente DHCP en WinBox*

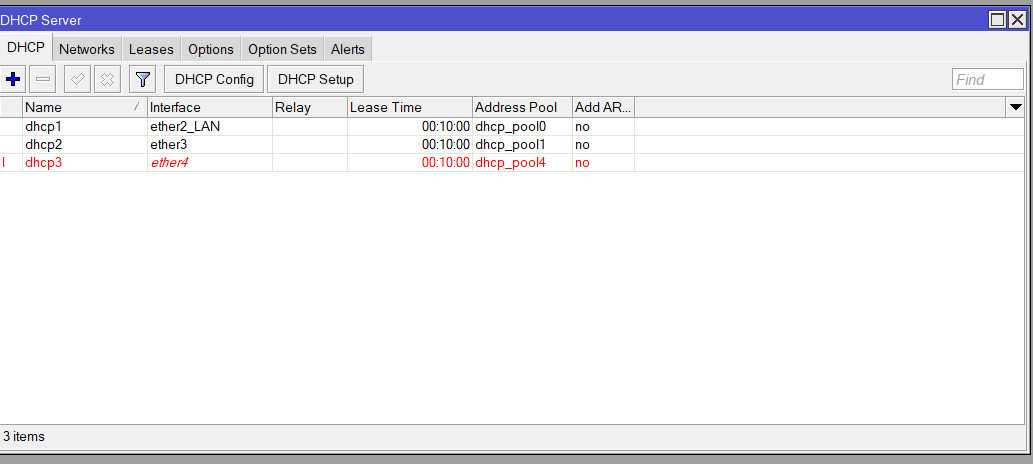
Se procede a configurar DHCP del cliente para la interfaz ethernet1\_WAN que corresponde a la PC que está siendo el administrador del Mikrotik, Esta interfaz tiene una dirección dinámica que se encuentra activa, pero con un tiempo de expiración de 1 hora y 56 minutos.



# Figura 31

*Configuración de interfaces de los clientes en servidor DHCP*

Configuración de los servidores DHCP designados a las distintas interfaces para que estén habilitadas y cada una tiene un grupo de direcciones IP específicas que distribuirá a los clientes de cada interfaz.



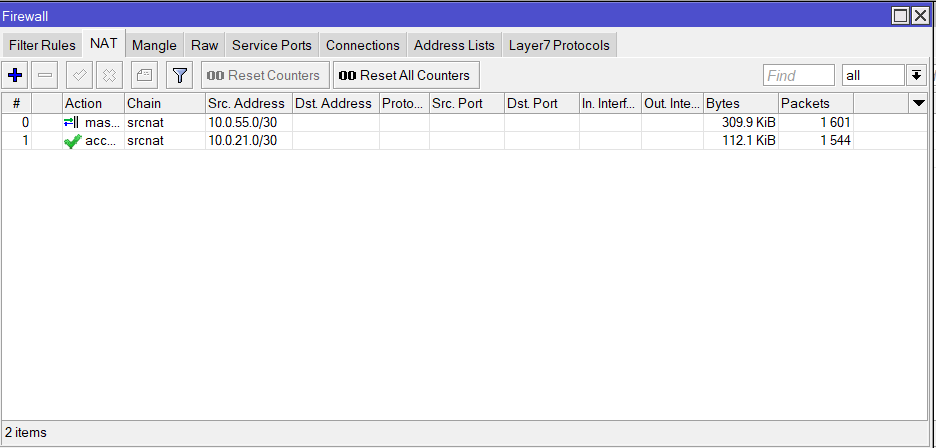
# Figura 32

*Configuración de reglas de Firewall*

Se configuran reglas de firewall para la NAT, con la finalidad de permitir la salida de la red privada a la pública con la subred 10.0.55.0/30.

Y la segunda regla permite tráfico desde la subred 10.0.21.0/30 con acción de ‘srcnat’ lo que cambia la dirección de origen de los paquetes.

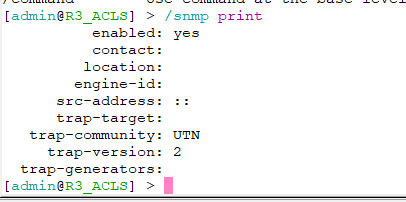
Estas reglas aseguran la salida de tráfico de subredes privadas, facilitando la comunicación con redes externas y el monitoreo de tráfico en Zabbix.



# Figura 33

*Configuración de SNMP en Mikrotik*

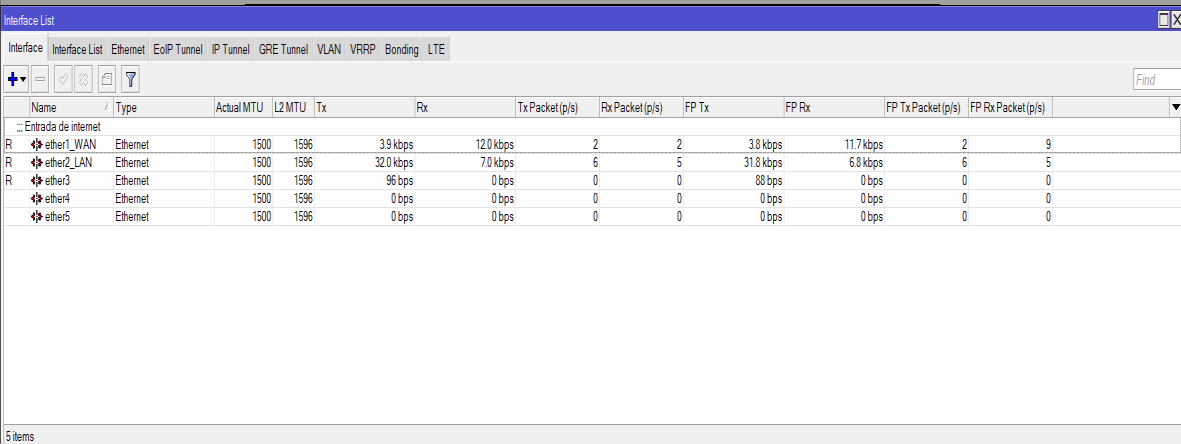
Luego, se configura el SNMP con la comunidad "UTN" creada y habilitada, ya que las notificaciones de los dispositivos estarán con esta etiqueta, además se especifica la versión del SNMP que se trabajará.



# Figura 34

*Lista de interfaces configuradas*

Cada interfaz está configurada en el dispositivo de Mikrotik, donde indica el tipo de conexión, tráfico entrante y saliente, además su estado de actividad.



# Figura 35

*Añadir dispositivo Mikrotik en servidor Zabbix*

Se edita algunos parámetros como nombre de equipo de la máquina que se va a analizar el tráfico, la plantilla que contiene configuraciones para recolectar datos de dispositivos a través de SNMP, también se asigna un grupo de equipos para que sean gestionados de manera centralizada y finalmente se considera la interfaz de red del SNMP correspondiente a la IP del puerto que está conectado el Mikrotik con un puerto 161 que es el estándar para este protocolo para tener la comunicación entre el servidor y el Mikrotik.

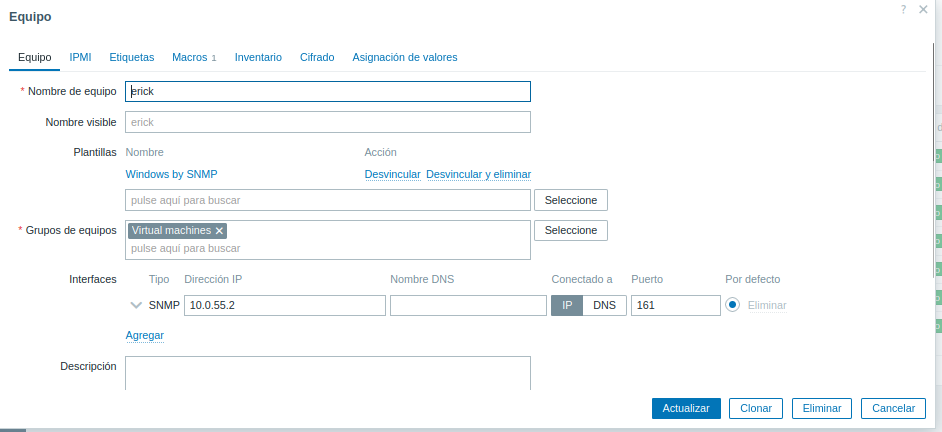


# Añadir equipos PC Figura 36

*Añadir equipo en Zabbix*

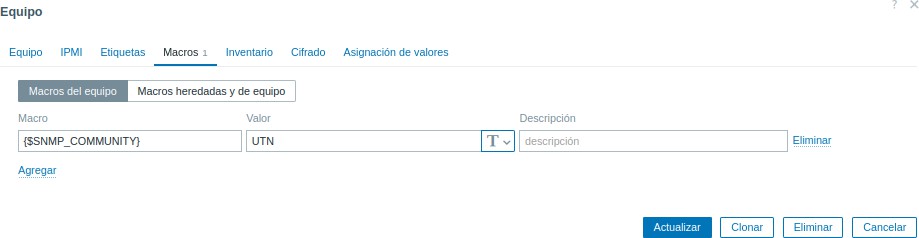
Para que sea posible monitorear el equipo, se agrega el nombre del equipo, la plantilla que en este caso es Windows, por tanto, monitoreará este equipo con parámetros específicos para sistemas Windows a través de SNMP.

El grupo de equipos pertenece a máquina virtual, ya que se encuentra la configuración allí, y con una interfaz SNMP con IP 10.0.55.2 que es del puerto de donde se está conectado el Mikrotik con cable ethernet y el puerto es por defecto.



# Figura 37

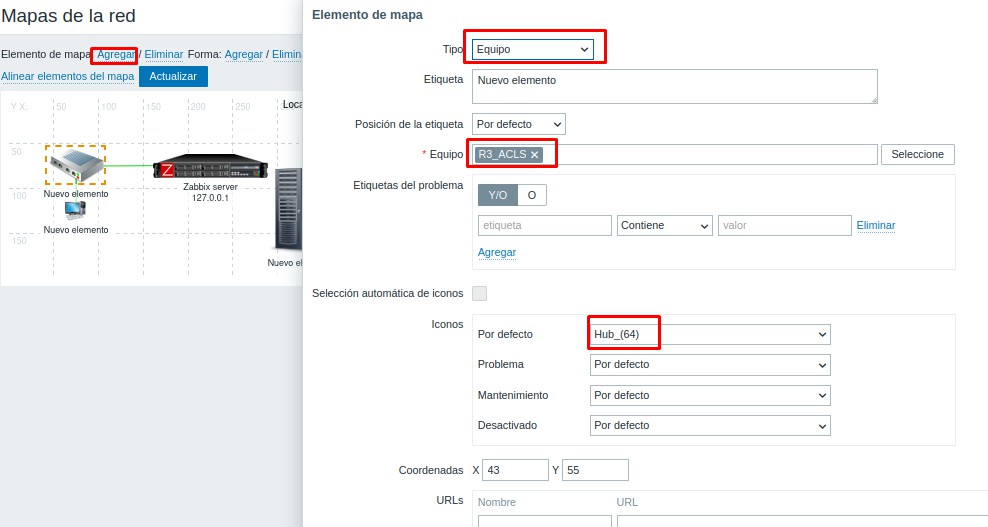
*Configuración de comunidad*

En cada equipo que es agregado se debe editar en la sección macros, para añadir la comunidad SNMP que es previamente creada en los equipos a ser administrados en Zabbix, en este caso se llamó a la comunidad UTN, por tanto, todos los equipos deben pertenecer a la misma comunidad

# Creación del mapa de la topología en el servidor Zabbix Figura 38

*Crear mapa de la red Zabbix*

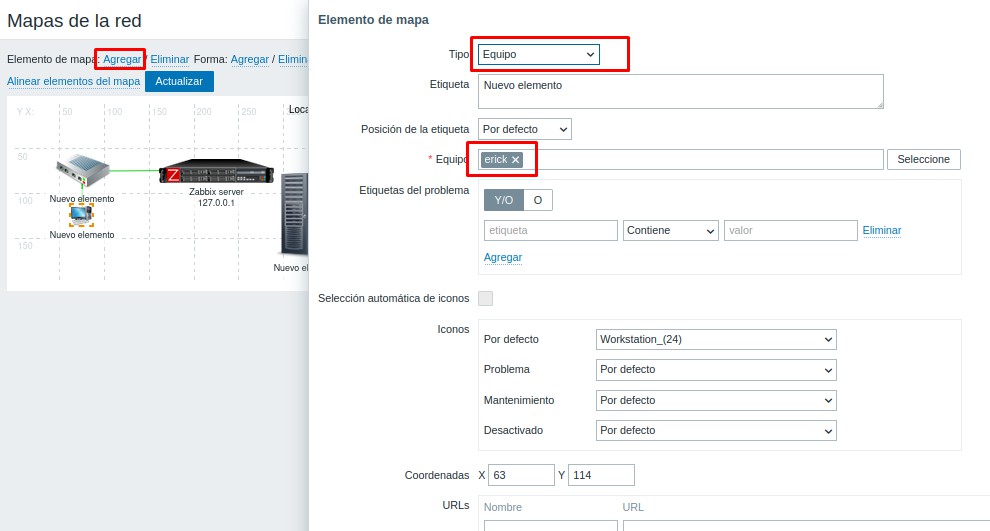
Para crear el mapa se debe agregar cada elemento como tipo ‘equipo’, que fueron los ya añadidos anteriormente, en este caso se está agregando el Mikrotik con icono de Hub para representar al dispositivo. Además, se puede agregarlas coordenadas para visualizarlos en una cierta posición de la infraestructura.



# Figura 39

*Agregar equipo para crear mapa de la red Zabbix*

De la misma forma se agrega el otro equipo correspondiente a la máquina que será monitoreada, el tipo de icono es Workstation, y las coordenadas son opcionales, ya que se puede arrastrar al equipo en el mapa de la red.

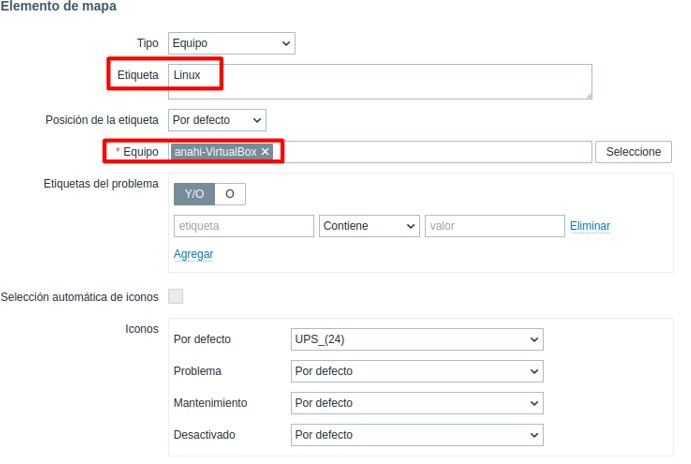


# Figura 40

*Agregar equipo para crear mapa de la red Zabbix*

Previamente se añadió otro equipo al servidor Zabbix para el monitorearlo, con la diferencia de que tiene una plantilla Linux, perteneciendo al grupo de equipos de máquina virtual con interfaz SNMP con IP 10.0.21.2.

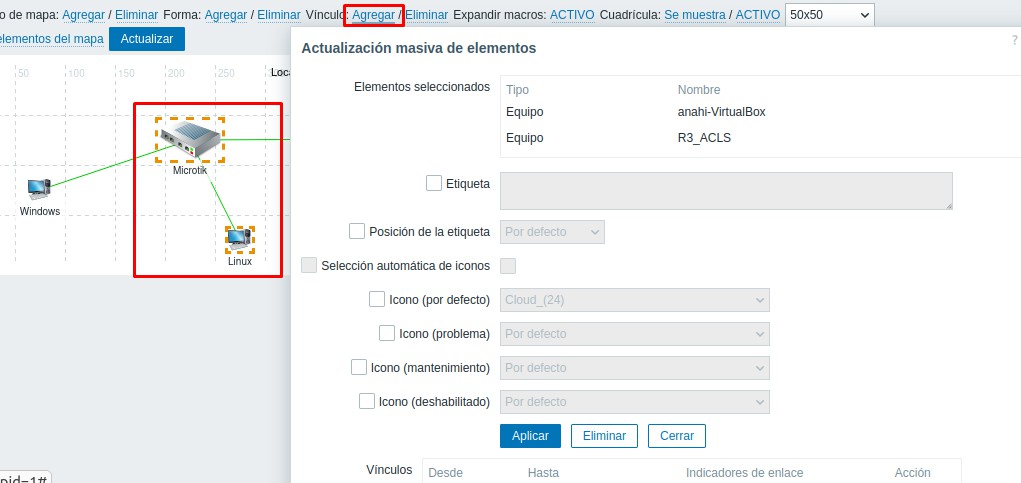
Entonces al agregar el elemento para el mapa de red, se considera las características mencionadas, siendo otra máquina que será monitoreada.



Para que los dispositivos se enlacen, se debe seleccionar en conjuntos los dos dispositivos que desea conectar y dar click a la opción agregar. Los parámetros que se visualizan en la ventana no son necesarios editarlos, solo se debe aplicar para conectarlos.

# Figura 41

*Enlazar los equipos en el mapa de red*

**

En el apartado de monitoreo, se observa que fueron agregados y configurados adecuadamente los equipos teniendo un estado activo con la disponibilidad de SNMP.

# Figura 42

*Estado de los equipos activo*

**

# Agregar ESP32 a Zabbix

En la siguiente figura en la parte de equipo se pone el nombre del equipo en este caso ESP32 Dev module.

# Figura 43

*Configuración del módulo ESP32*

**

Continuando con las configuraciones deslizando hacia abajo se elige snmp ahí se debe configurar la ip 192.168.88.239 y el puerto 161 (el puerto que se vaya a utilizar), el cual esta conectado un sensor de temperatura.

# Figura 44

*Agregación de parámetros para snmp*

**

De la misma forma se agrega el resto de los elementos ESP32 como equipos colocando su respectivo nombre, identificando el protocolo SNMP que se va usar para la recolección de datos de los elementos, y por ultimo se le asigna la dirección IP y el puerto para el esp32 agregado por donde se establecerá la conexión para la administración.

# Figura 45

*Añadir dispositivo esp32*

**

# Figura 46

*Añadir dispositivo esp32*

**

# Añadir monitores de los sensores de cada ESP32 a Zabbix

Como siguiente paso en la configuración de cada esp añadido, se agrega la monitorización del sensor que está conectado a este elemento en monitorización, con la finalidad de observar las gráficas de monitoreo de cada uno de ellos.

# Figura 47

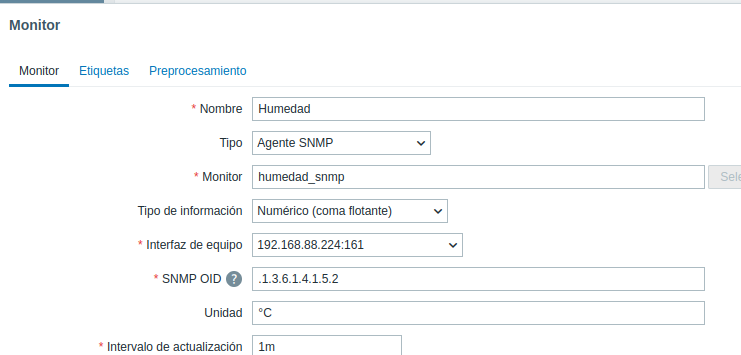
*Configuración del monitor ESP32*



Se debe llenar los espacios del monitor como el nombre para identificación del elemento en este caso corresponde al sensor de temperatura, el nombre de monitor, tipo de información SNMPIOD que es el valor único con el que se va a identificar el objeto y finamente en dar clic en probar.

# Figura 48

*Configuración de métricas del sensor temperatura*

**

# Figura 49

*Configuración de métricas del sensor nivel de agua*

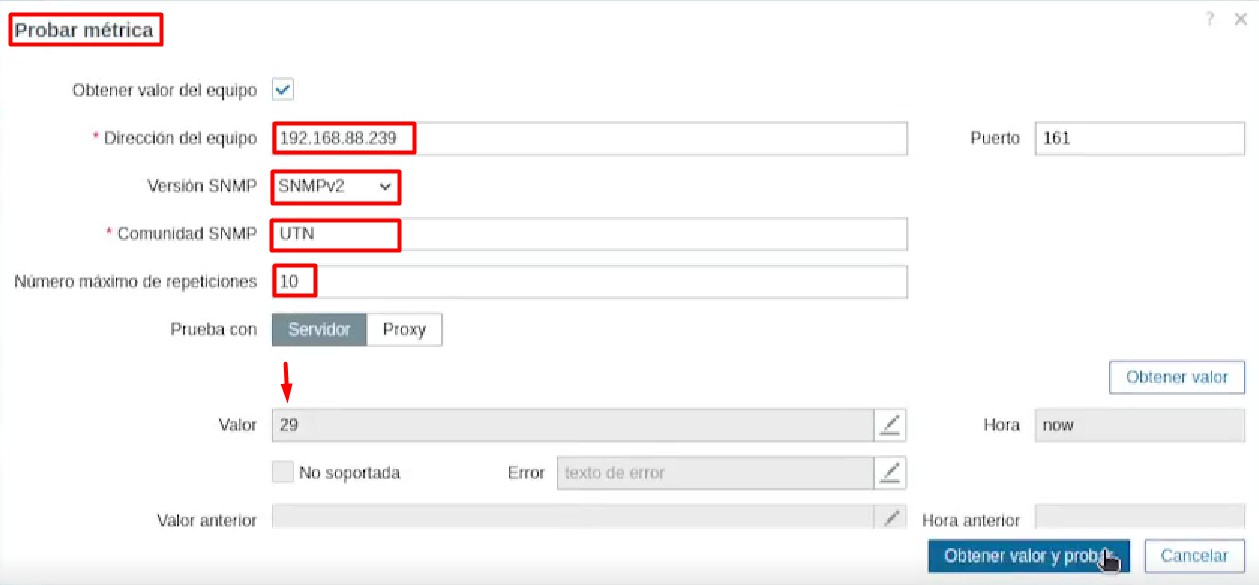


En la siguiente figura se válida la métrica, el mismo programa refleja la dirección ip del equipo la versión snmp, la comunidad snmp y el número máximo de repeticiones y al

dar clic en obtener valor y probar genera el valor 29.

# Figura 50

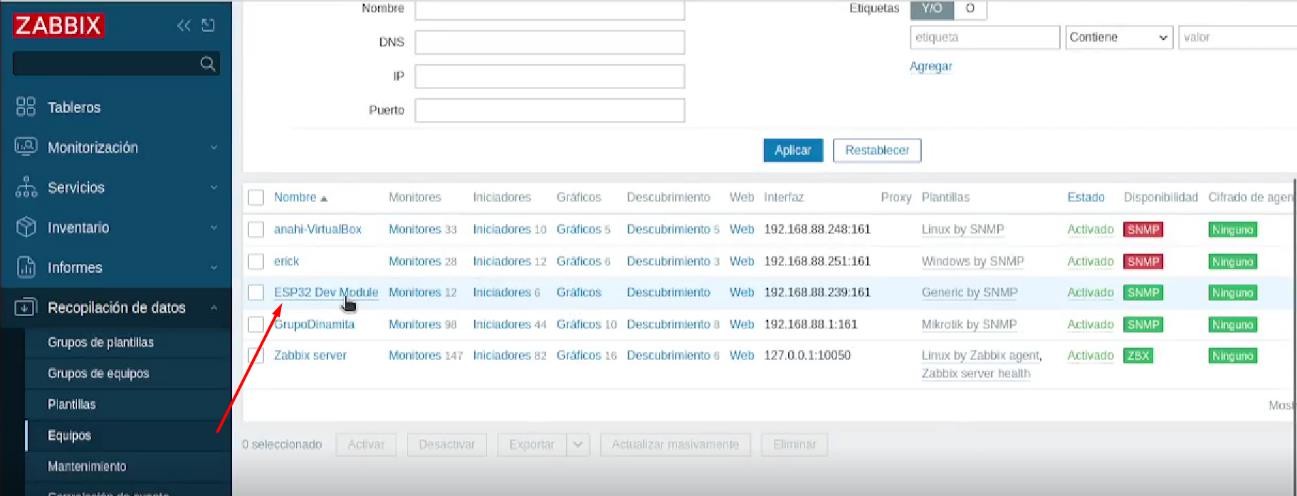
*Configuración de métricas*

**

En la siguiente figura se puede ver la disponibilidad del protocolo snmp como activa de cada elemento que se agrega

# Figura 51

*Elemento esp32 activo en el servidor zabbix*

**

# Código de ESP32 en Arduino IDE

Se considera el software Arduino IDE para la configuración del dispositivo esp32, el cual estará conectado a una red WIFI, correspondiente a la misma que se encuentran todos los hosts conectados por cable ethernet al router. Además, el esp32 lee los datos de los sensores, los cuales serán expuestos esos datos a través de SNMP.

* En las primeras líneas se coloca las bibliotecas importadas para conexión WIFI, usar UDP para SNMP, gestión del agente SNMP, y para la lectura de los datos de los sensores.
* En la línea 6, se configura la red wifi, especificando SSID y la contraseña a la que se conectará el dispositivo.
* En la línea 6 se configura SNMP, creando un objeto para manejar conexiones UDP, e se inicia con el nombre de la comunidad creada que es “UTN”
* En la línea 14, se agrega al código variables SNMP para OIDs, uno para almacenar el valor leído del sensor, y adicional el valor que puede ser modificado mediante solicitud SNMP SET.
* Linea 18 ya se considera las configuraciones del sensor en este caso se puede seguir añadiendo más, aquí se define el pin al que se conecta y el tipo de sensor.
* Desde la línea 23, se considera la función setup para el inicio de comunicación, inicio del sensor, configuración y arranque del agente SNMP, asignando las variables SNMP a sus respectivos OIDs.
* Desde la línea 53 empieza la función loop para la lectura de los datos del sensor, manejo de solicitudes SNMP entrantes.



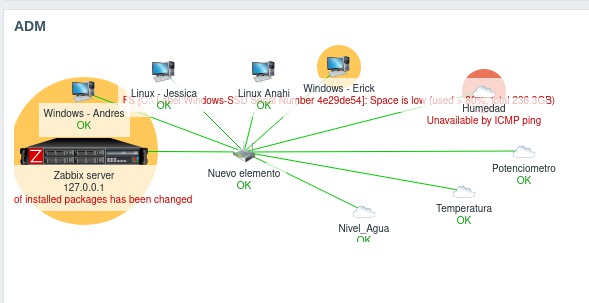
# Resultados

El mapa de Zabbix muestra un estado mayormente positivo en el monitoreo de los dispositivos, destacando la conectividad y funcionalidad correcta de varios hosts. Los dispositivos basados en Lora32 o ESP32, como Nuevo elemento, Potenciómetro,

Temperatura y Nivel\_Agua, están operando de manera óptima, lo que demuestra una integración exitosa con el sistema de monitoreo. Asimismo, los equipos como Linux – Jessica y Linux – Anahí también están funcionando correctamente, sin problemas reportados, lo que refleja estabilidad en los sistemas supervisados. Este panorama general resalta la efectividad del monitoreo y la conectividad en la mayoría de los dispositivos configurados.

# Figura 52

*Mapa de Monitoreo de Dispositivos en Zabbix*

**

En la parte de monitorización en ultima hora, seleccionar grupo de equipos en aplicaciones y aplicar elegir en equipos el equipo Esp32 Dev Module para mostrar los resultados.

# Figura 53

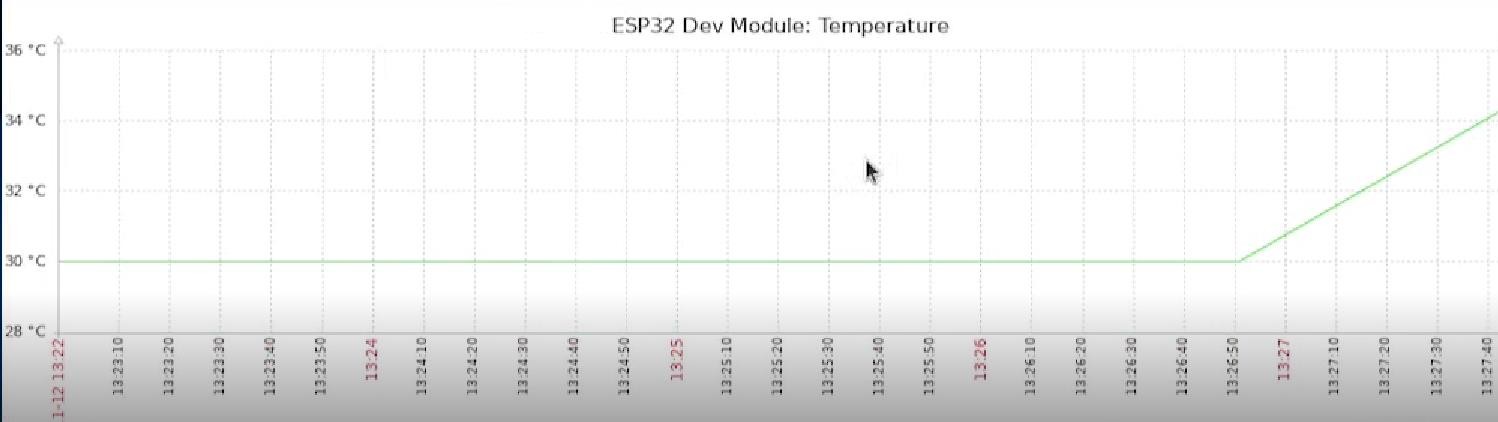
*Grupos de equipos y aplicaciones*

**

El gráfico titulado ESP32 Dev Module: Temperature muestra el monitoreo de la temperatura registrada por un módulo ESP32 en grados Celsius (°C) a lo largo del tiempo. En el eje vertical se representan los valores de temperatura, mientras que en el eje horizontal se muestran las marcas de tiempo. Inicialmente, la temperatura se mantiene estable alrededor de los 30 °C entre las marcas de tiempo 13:23:42 y 13:25:50. Sin embargo, a partir de las 13:26:00, se observa un aumento progresivo de la temperatura, alcanzando aproximadamente los 36 °C en la marca final, 13:27:40.

# Figura 54

*Monitoreo de temperatura*

**

El comando ejecutado muestra la utilización de snmpset para modificar un valor en el ESP32 mediante el protocolo SNMP v2c. Se especifica la dirección IP del dispositivo (192.168.1.37), la comunidad "private", la OID 1.3.6.1.4.1.5.3, y el valor a establecer, que en este caso es el número entero 42. El resultado confirma que la operación fue exitosa, indicando que el valor de la OID fue cambiado correctamente a 42. Esto demuestra que el cliente ESP32 está configurado para aceptar y procesar comandos SNMP de manera funcional.

# Figura 55

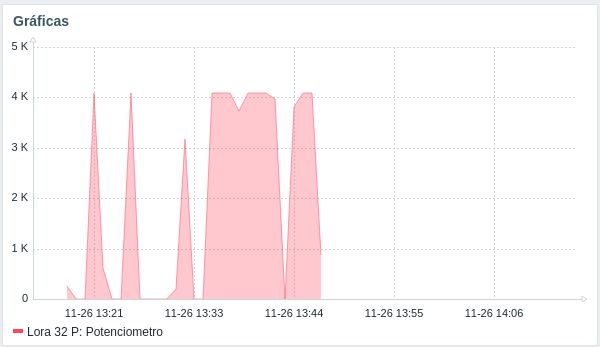
*Ejecución de comando snmpset para establecer valores en el ESP32 mediante SNMP*

**

El monitoreo del ESP32 en el servidor Zabbix muestra un gráfico de temperatura en tiempo real. Según los datos representados, la manipulación del potenciómetro registrada se mantiene constante en un valor del movimiento, tanto en su última lectura como en los valores mínimo, promedio y máximo. El gráfico permite visualizar un rango de tiempo de los últimos 5 minutos, con la posibilidad de ajustar el periodo para un análisis más amplio.

# Figura 56

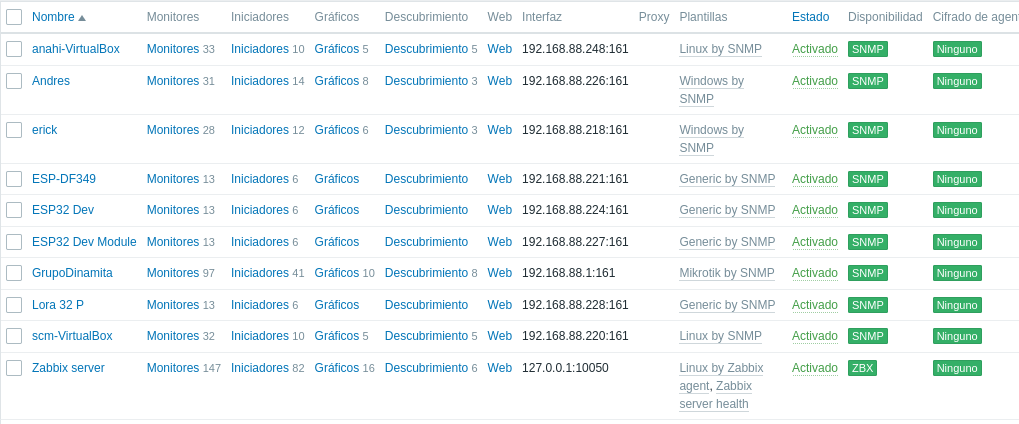
*Monitoreo en Zabbix del módulo Lora32: Registro del Potenciómetro*

**

El listado de dispositivos monitoreados en Zabbix muestra que todos están en estado activo y correctamente configurados, utilizando principalmente el protocolo SNMP para la recolección de datos. Los dispositivos virtuales, como anahi-VirtualBox y scm- VirtualBox, así como los equipos físicos como Andres y erick, están reportando datos mediante SNMP sin problemas. Los dispositivos basados en ESP32 y Lora32 también están activos y configurados como genéricos por SNMP, lo que indica que la integración ha sido exitosa. El servidor Zabbix, con 147 monitores y utilizando el agente Zabbix, también está en perfecto funcionamiento. La disponibilidad de todos los dispositivos es positiva, lo que demuestra una conectividad estable en la infraestructura. Además, no se observa ningún cifrado de agente configurado, lo cual es aceptable en entornos de red controlados, pero podría ser una oportunidad para mejorar la seguridad en el futuro. Tal como se muestra en la siguiente figura.

# Figura 57

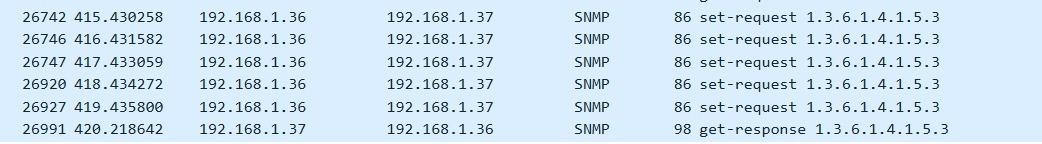
*Activo el SNMP en el ESP32*

**

El tráfico de red capturado muestra una interacción constante entre dos direcciones IP, específicamente entre el ESP32 (192.168.1.37) y otro dispositivo (192.168.1.36), utilizando el protocolo SNMP. Se observan múltiples solicitudes de tipo `set-request` hacia la misma OID `1.3.6.1.4.1.5.3`, lo que indica que el servidor está intentando establecer o modificar valores en el ESP32. Finalmente, el dispositivo ESP32 responde con un paquete `get-response`, confirmando que el valor solicitado fue recibido o procesado. Este flujo de comunicación demuestra que la conexión SNMP está activa y operativa, permitiendo el intercambio de información y control entre el servidor y el ESP32, tal como está en la siguiente figura.

# Figura 58

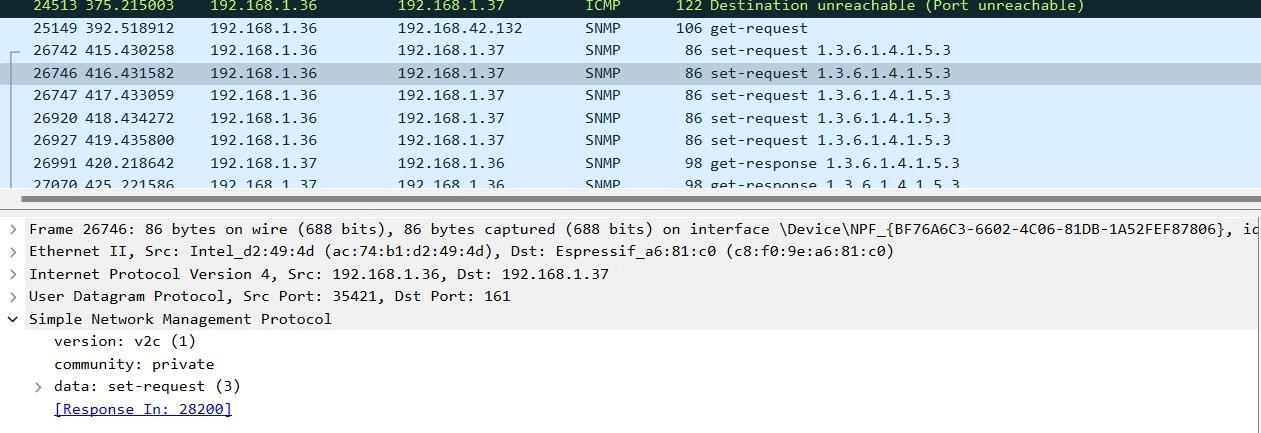
*Captura de tráfico SNMP entre servidor y cliente ESP32 entre set-request y el get- response*

**

El análisis del tráfico capturado refleja una comunicación establecida mediante el protocolo SNMP, en su versión 2c, entre un cliente (ESP32 con dirección 192.168.1.37) y un servidor (192.168.1.36). Los paquetes capturados incluyen solicitudes `set-request` hacia la OID especificada, lo que indica intentos de modificar datos en el ESP32. La comunidad SNMP configurada es "private", lo cual asegura que solo dispositivos autorizados puedan interactuar con el nodo. La respuesta asociada confirma que las operaciones son exitosas y que el ESP32 está procesando las solicitudes adecuadamente, validando la correcta implementación del protocolo, así como la figura siguiente.

# Figura 59

*Captura de paquete SNMP detallada en Wireshark entre servidor y cliente ESP32del set request*

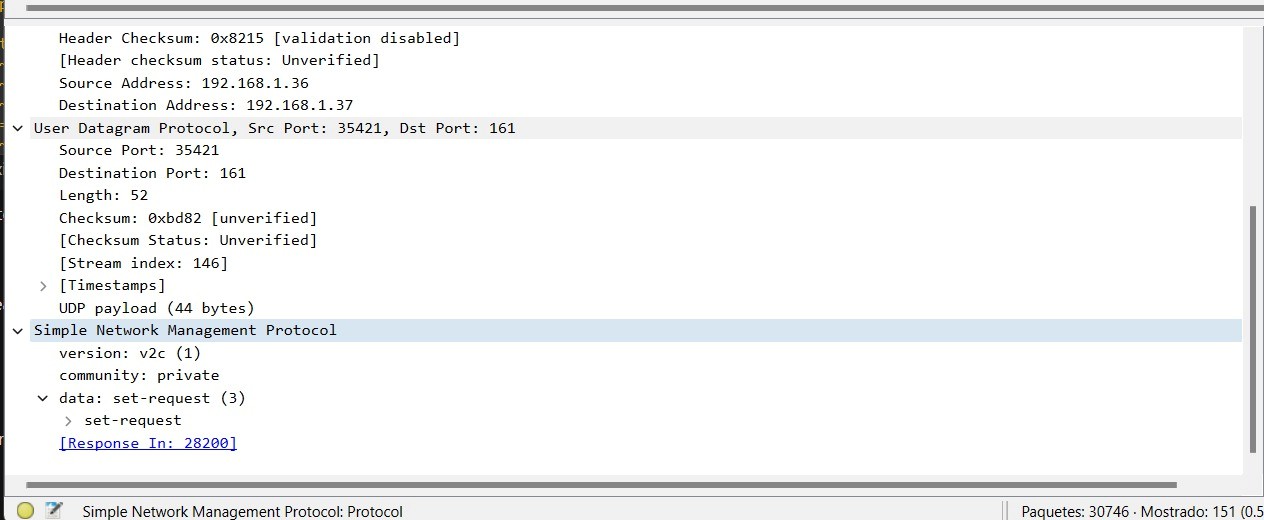
**

El paquete capturado muestra una solicitud set-request en el protocolo SNMP v2c enviada desde la dirección 192.168.1.36 al ESP32 (192.168.1.37) utilizando el puerto 161, que es el estándar para SNMP. La comunidad configurada es "private", y el intercambio ocurre mediante UDP, con un tamaño de carga útil de 44 bytes. Se incluye una respuesta

asociada, confirmando que la operación fue procesada correctamente por el ESP32, lo que valida la correcta configuración y comunicación entre ambos dispositivos.

# Figura 60

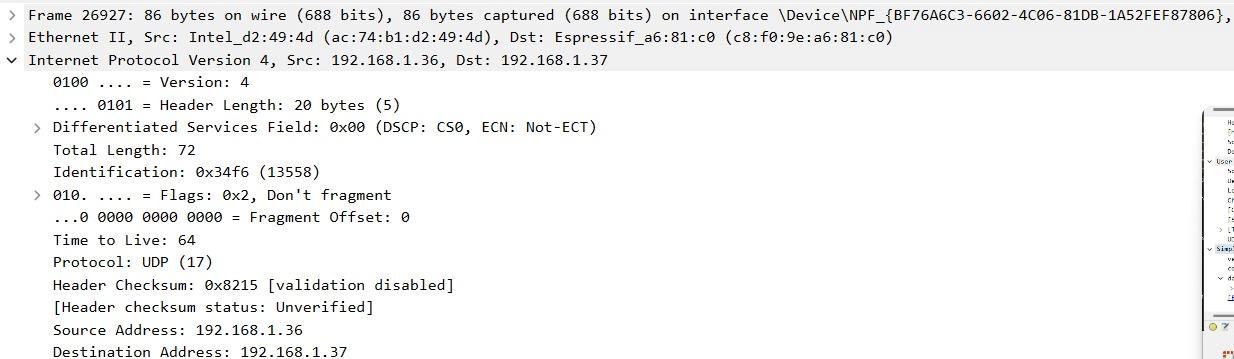
*Detalle del paquete SNMP v2c con solicitud set-request capturado en Wireshark*

**

El paquete capturado corresponde a una comunicación entre la dirección IP 192.168.1.36 (servidor) y 192.168.1.37 (ESP32) utilizando el protocolo UDP en IPv4. El encabezado del paquete muestra una longitud total de 72 bytes, sin fragmentación, con un TTL de 64, lo que indica que el paquete puede atravesar hasta 64 nodos antes de ser descartado. Además, el checksum del encabezado no fue verificado, pero esto no afecta la transmisión del paquete. La interacción se realiza sobre un canal de 86 bytes en la capa de enlace de datos, con el dispositivo destino identificado como "Espressif", lo que confirma la correcta recepción en el ESP32.

# Figura 61

*Detalles del paquete UDP capturado en Wireshark entre servidor y ESP32*

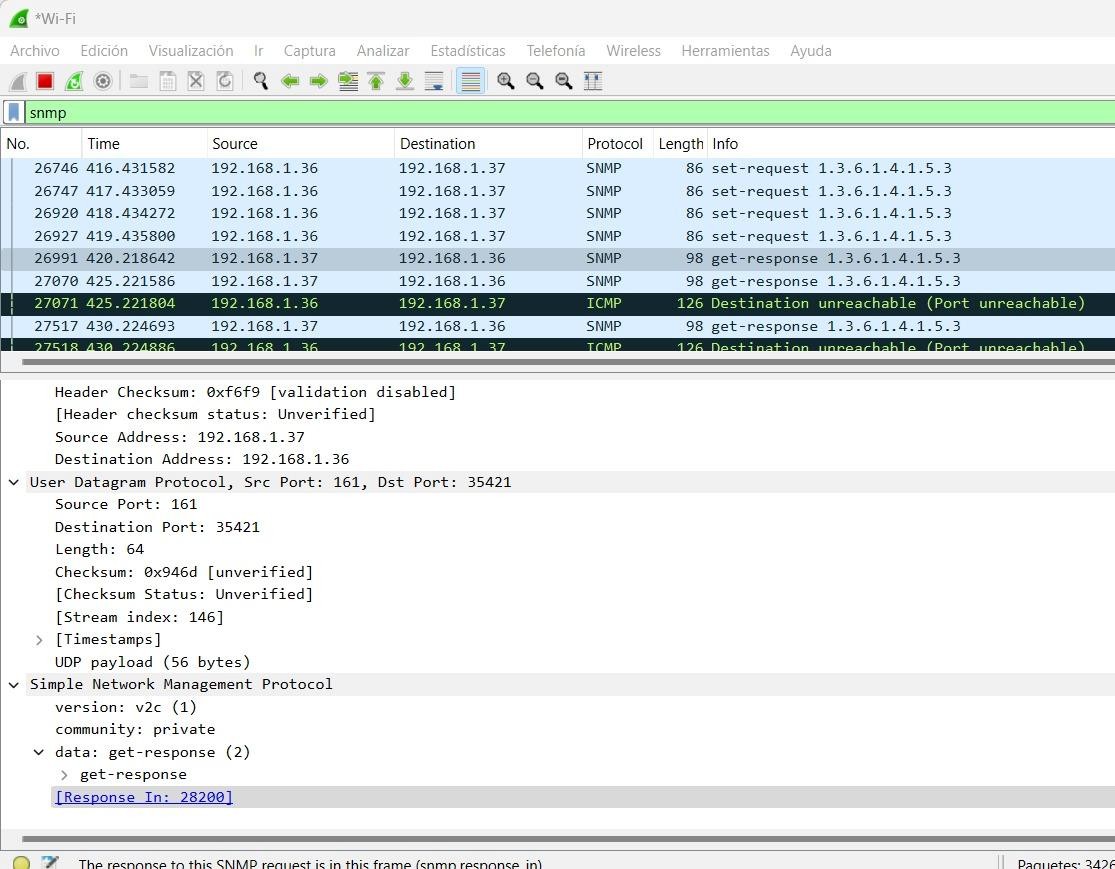
**

El análisis del tráfico muestra una interacción activa entre las direcciones IP 192.168.1.36 y 192.168.1.37 utilizando el protocolo SNMP v2c. Se registran múltiples solicitudes set- request seguidas de respuestas get-response, confirmando que el cliente (ESP32) está procesando las peticiones enviadas por el servidor de manera exitosa. Los paquetes se transmiten mediante UDP, con un puerto de origen 35421 y destino 161, que es estándar para SNMP. Además, se registran mensajes ICMP indicando "Destination unreachable", posiblemente por configuraciones de red incompletas o puertos cerrados en algunos

momentos específicos. Sin embargo, la comunicación SNMP principal funciona correctamente y asegura la transmisión de datos entre los dispositivos.

# Figura 62

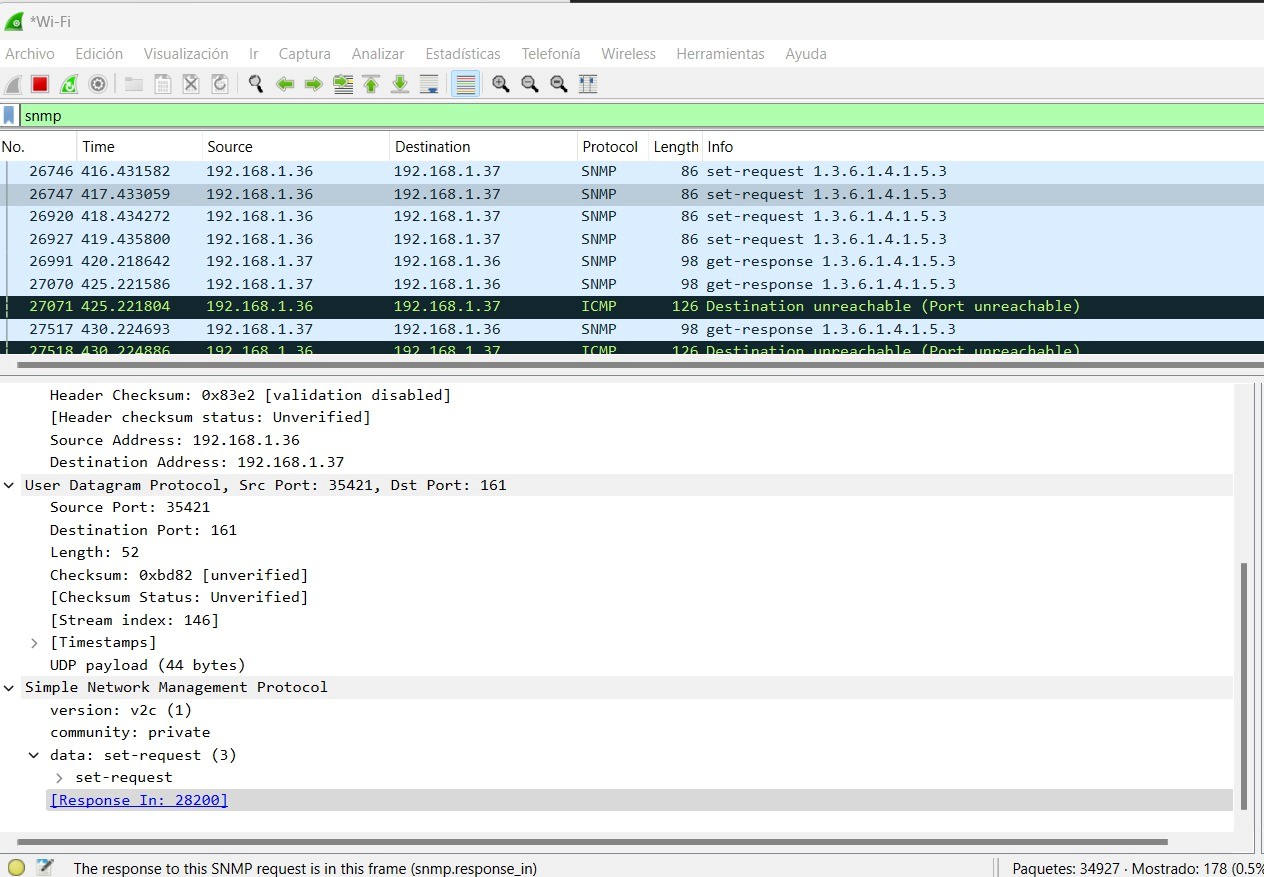
*Monitoreo de paquetes SNMP y respuesta de conexión en Wireshark del get-response*

**

El monitoreo muestra una interacción activa entre el servidor (192.168.1.36) y el cliente ESP32 (192.168.1.37) utilizando el protocolo SNMP v2c. Se observa un flujo constante de solicitudes set-request hacia el ESP32, seguido de respuestas get-response, indicando que las configuraciones enviadas por el servidor están siendo correctamente procesadas. Los paquetes se transmiten a través de UDP, con el puerto destino 161. También se registran mensajes ICMP con el estado "Destination unreachable", que podrían indicar intentos de comunicación hacia un servicio no disponible en ciertos momentos, aunque no afecta el funcionamiento principal del protocolo SNMP. La comunidad configurada es "private", asegurando un acceso restringido al intercambio de datos.

# Figura 63

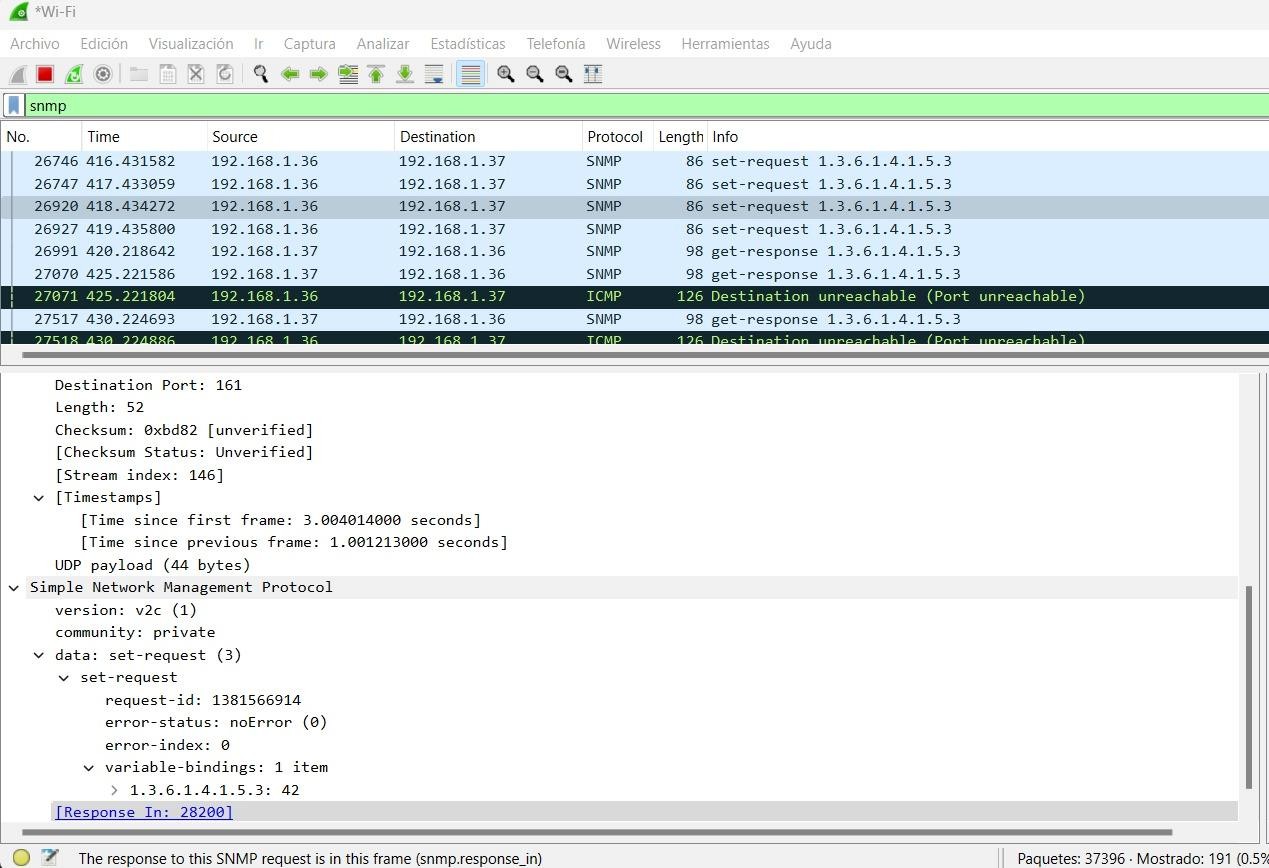
*Análisis de tráfico SNMP y estado de conexión en red mediante Wiresharkdel set request*

**

El análisis del tráfico muestra una interacción consistente entre el servidor y el ESP32 mediante el protocolo SNMP v2c. Las solicitudes set-request enviadas incluyen la OID 1.3.6.1.4.1.5.3 con un valor asignado de 42, lo que evidencia un intento de modificar o establecer un parámetro en el cliente. Cada solicitud incluye un request-id único, y el estado de error reportado es "noError", confirmando que la operación se está ejecutando correctamente. Además, las respuestas correspondientes son procesadas por el ESP32 sin errores. Los tiempos entre paquetes indican un flujo continuo, mientras que algunos mensajes ICMP reflejan "Destination unreachable", posiblemente debido a configuraciones específicas de puertos o dispositivos.

# Figura 64

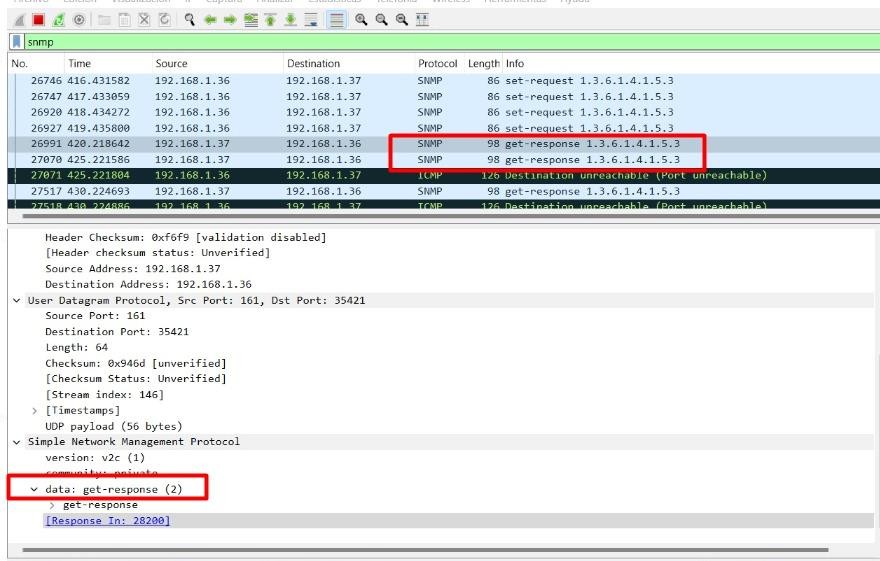
*Tráfico SNMP con solicitudes y respuestas detalladas capturadas en Wiresharkdel set- request*

**

El análisis refleja una interacción SNMP exitosa centrada en el **get-response**, el cual es la respuesta del dispositivo gestionado a una solicitud previa **get-request**. Este **get- response** confirma que el agente SNMP del dispositivo pudo interpretar el OID solicitado (`1.3.6.1.4.1.5.3`) y devolver el valor asociado correctamente, lo que valida tanto la comunicación como la configuración del agente. El hecho de recibir un \*\*get-response\*\* indica que el dispositivo está operativo, accesible y que el protocolo SNMP está funcionando adecuadamente para gestionar y consultar la información requerida en la MIB correspondiente.

# Figura 65

*Tráfico SNMP con solicitudes y respuestas detalladas capturadas en Wiresharkdel get- response*

**

# Análisis de OIDs:

El resultado muestra una interacción SNMP mediante una solicitud getBulkRequest, que es común en SNMPv2c y se utiliza para obtener información de múltiples OIDs consecutivos en una única operación, optimizando el intercambio de datos entre el cliente y el agente. En este caso, el cliente envía una solicitud para obtener valores desde el OID

`1.3.6.1.2.1.2.2.1.13` y continúa con el OID siguiente, `1.3.6.1.2.1.2.2.1.14`. La respuesta del dispositivo gestionado proporciona un valor para el primer OID, pero muestra un valor vacío (Null) para el segundo, lo que indica que no tiene información que reportar para ese parámetro.

El OID `1.3.6.1.2.1.2.2.1.13` pertenece a la MIB estándar IF-MIB y corresponde al contador `ifInDiscards`, que mide la cantidad de paquetes descartados al ser recibidos por una interfaz de red. Este parámetro es útil para detectar problemas relacionados con la calidad o capacidad de las interfaces, como buffers insuficientes o paquetes malformados. Por esta razón, los sistemas de monitoreo suelen incluirlo en las consultas SNMP como parte de un diagnóstico integral del rendimiento de la red.

Por otro lado, el OID `1.3.6.1.2.1.2.2.1.14`, también de la IF-MIB, representa el contador

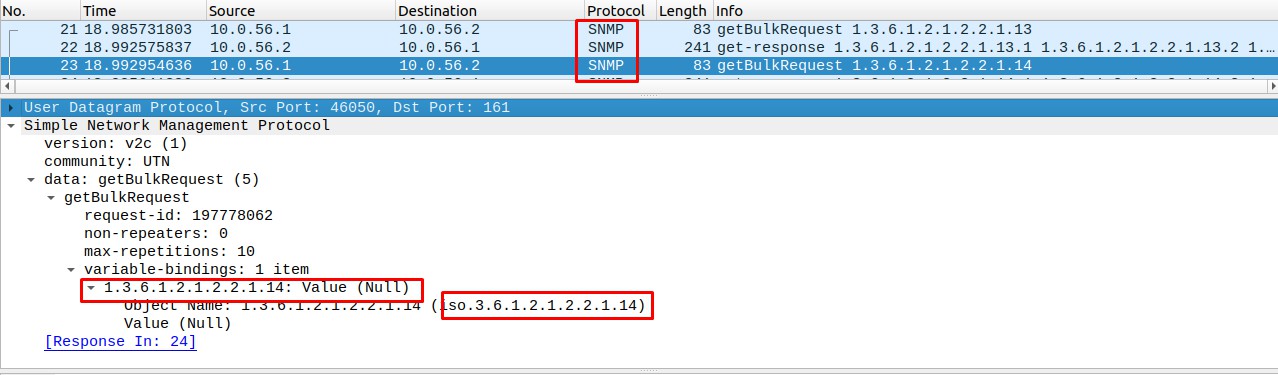
`ifOutErrors`, que mide los errores registrados al enviar paquetes desde una interfaz. Aunque esta métrica es clave para identificar problemas de transmisión o colisiones, en este caso, el agente SNMP devuelve un valor vacío, lo que podría deberse a la falta de

soporte para este parámetro en el dispositivo, a que no se han registrado errores, o a una configuración limitada de su MIB.

Estos OIDs forman parte de la MIB estándar porque son métricas fundamentales para evaluar la salud y el rendimiento de las interfaces de red. Al utilizar `getBulkRequest`, el cliente intenta optimizar las consultas al obtener múltiples valores consecutivos, minimizando el tráfico de red y el tiempo de respuesta. El valor Null no necesariamente indica un problema, pero sí sugiere que se podría verificar si el agente SNMP tiene configurados correctamente estos parámetros en su MIB para asegurar que la información esté disponible.

# Figura 66

*Interacción SNMP con Solicitud getBulkRequest y Respuesta de OIDs*

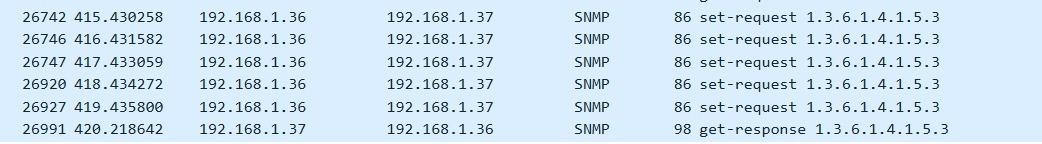
**

Los números de los OIDs (Object Identifiers) en el protocolo SNMP, como 1.3.6.1.4.1.5.3, tienen un significado jerárquico y estructurado que identifica una propiedad o recurso específico dentro de la MIB (Management Information Base) de un dispositivo gestionado. Aquí está el desglose de los componentes:

1. 1.3: Indica que pertenece a la familia de identificadores gestionados por la Organización Internacional de Normalización (ISO). En este caso, 1.3 se refiere a los estándares definidos por el Departamento de Internet.
2. 6: Se refiere al nodo "management", que abarca elementos relacionados con la administración de redes.
3. 1: Representa el nodo MIB-II (Management Information Base versión 2), una colección de parámetros estándares definidos para dispositivos de red.
4. 4: Este nivel indica el nodo "private", que contiene objetos definidos por fabricantes específicos o implementaciones personalizadas.
5. 1: Representa el subnodo "enterprises", utilizado para identificar objetos creados y gestionados por una empresa específica. Este nodo permite a los fabricantes agregar objetos únicos dentro de sus propios productos.
6. 5: Es un identificador único asignado a una empresa dentro del espacio "enterprises". En este caso, el "5" podría ser una empresa o dispositivo específico según el fabricante registrado.
7. 3: Representa un objeto específico dentro de los OIDs definidos por la empresa o fabricante. Este número identifica una propiedad particular o métrica monitoreada del dispositivo.

# Figura 67

*Tráfico SNMP*

**

# Conclusiones

* Con el protocolo SNMP para la gestión y monitoreo de variables en los dispositivos de red usa OIDs que son identificadores únicos y jerárquicos, en caso del código de Arduino los OIDs permiten la lectura y modificación de datos del sensor, con la finalidad de permitir una gestión de datos estandarizada y estructurada de variables en lo dispositivos de la red.
* La comunicación entre los elementos de la topología y el servidor Zabbix mediante SNMP v2c y v3c es funcional, ya que se lograron establecer y modificar valores en el dispositivo de manera exitosa, lo cual, valida la correcta configuración del protocolo, sim embargo tiene mejoras de autenticación la versión 3 aportando mayor seguridad.
* La integración de elementos como equipos PC y ESP32 con Zabbix junto con el uso del protocolo SNMP permiten una gestión remota eficiente mediante la recolección de datos de los elementos, esto permite evidencia la robustez del sistema al procesar comandos set-request y generar respuestas adecuadas, las cuales son operaciones específicas del protocolo SNMP.
* Las operaciones set-request y get-response, incluye el OID del elemento ya que, el set es usado por el cliente como una solicitud que se envía al agente SNMP para consultar o modificar el valor de alguna variable gestionada, mientras que el get es la respuesta del agente SNMP hacia la solicitud que puede ser tanto positiva como negativa, en caso de ser exitosa incluye el valor actualizado con el OID del objeto.
* La funcionalidad gráfica de Zabbix no solo facilita el monitoreo en tiempo real, sino que también ofrece un historial de datos detallado que puede ser usado para análisis predictivo y toma de decisiones, los cuales deben ser validados. Esto resalta la capacidad del sistema para identificar patrones de comportamiento y posibles anomalías en los dispositivos supervisados.
* La implementación del protocolo SNMP en dispositivos como el ESP32 permite la gestión centralizada y eficiente de datos, facilitando la estandarización en la monitorización y control de variables críticas en la red. Esto asegura un flujo de datos confiable y estructurado.

# Recomendaciones

* + Es recomendable instalar Zabbix una versión anterior a la última o asegurarse de que la versión actual sea estable, ya que las versiones más recientes pueden contener errores o problemas de compatibilidad que aún no han sido solucionados.
* Se recomienda personalizar los iconos y nombres de los equipos en el mapa de red en Zabbix para tener mejor visualización de la topología y en caso de requerir se puede agregar alguna descripción para identificar el dispositivo y su función.
* En caso de alta monitorización de varios hosts, puede ser necesario optimizar los parámetros de rendimiento, como el límite de monitoreo simultáneos de Zabbix para evitar que se vea afectado el rendimiento.
* Es recomendable implementar un sistema de copias de seguridad periódicas de la base de datos de Zabbix, para asegurar la integridad de la información monitoreada y evitar la pérdida de datos ante cualquier fallo del sistema.
* Configura gráficos y paneles en Zabbix para visualizar en tiempo real las métricas más relevantes de los dispositivos. Esto te permitirá obtener una vista rápida del rendimiento de la red y detectar problemas de inmediato.
* Revisar la configuración de la OID asociadas a los sensores para confirmar que los datos enviados por el ESP32 están correctamente vinculados al parámetro monitorizado en Zabbix.
* Se recomienda revisar y ajustar las configuraciones de red, incluyendo reglas de firewall y parámetros SNMP, para minimizar errores de conectividad, como los mensajes.
* Configurar notificaciones o alertas personalizadas en Zabbix basadas en umbrales predefinidos que permitirá una respuesta proactiva ante posibles anomalías, mejorando así la capacidad de reacción ante fallos críticos en el sistema.

# Referencias

softonic. (1 de abril de 2023). *App gratis para gestión de MikroTik*. Obtenido de App gratis para gestión de MikroTik: https://winbox.softonic.com/

XPERTS. (12 de septiembre de 2020). *Capítulo 2.1 – Configuración de un router MikroTik*. Obtenido de Configuración de un router MikroTik:

https://abcxperts.com/docs/capitulo-2-1-configuracion-de-un-router-mikrotik/

ZABBIX. (26 de julio de 2023). *Monitorear redes*. Obtenido de Realizar un

seguimiento del estado y el desempeño de tu red: https://[www.zabbix.com/](http://www.zabbix.com/)

Forouzan, B. A. (2021). Data Communications and Networking (5th ed.). McGraw-Hill RFC Editor. (2002). *RFC 3411: An Architecture for Describing Simple Network.*

Stallings, W. (2018). *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2 (3rd ed.)*. Addison.