



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO



Administración de Servicios en Red

Proyecto Final:

Sistema de Monitorización de Agentes dentro de una Red

Profesora: Leticia Henestrosa Carrasco

Alumnos: Hernández Oseguera Mayra Sofía
Martínez San Román Aarón Hazel
Nolasco Cid Víctor Iván

Grupo: 4CV3

Introducción

El núcleo de SNMP es un conjunto simple de operaciones (y la información que recopilan estas operaciones) que brinda a los administradores la capacidad de cambiar el estado de algunos dispositivos basados en SNMP. Por ejemplo, puede usar SNMP para apagar una interfaz en su enrutador o verificar la velocidad a la que está funcionando su entrelazado Ethernet. SNMP puede incluso controlar la temperatura de su interruptor y advertirle cuando es demasiado alto.

SNMP generalmente está asociado con la administración de enrutadores, pero es importante comprender que se puede utilizar para administrar muchos tipos de dispositivos. Mientras que el predecesor de SNMP, el Simple Gateway Management Protocol (SGMP), fue desarrollado para administrar enrutadores de Internet, SNMP se puede utilizar para administrar sistemas Unix, sistemas Windows, impresoras, bastidores de módems, fuentes de alimentación y más. Cualquier dispositivo que ejecute software que permite gestionar la recuperación de información SNMP. Esto incluye no solo dispositivos físicos sino también software, como servidores web y bases de datos.

Otro aspecto de la administración de la red es el monitoreo de la red; es decir, monitorear una red completa en lugar de enrutadores individuales, hosts y otros dispositivos. Remote Network Monitoring (RMON) se desarrolló para ayudarnos a comprender cómo funciona la red en sí, así como cómo los dispositivos individuales de la red están afectando a la red en su conjunto. Se puede usar para monitorear no solo el tráfico LAN.

SNMP es realmente sobre la gestión de la red. La administración de la red es una disciplina propia, pero antes de conocer los detalles de SNMP, es útil tener una visión general de la administración de la red.

¿Qué es la gestión de red? La administración de redes es un concepto general que emplea el uso de varias herramientas, técnicas y sistemas para ayudar a los seres humanos a administrar varios dispositivos, sistemas o redes. Eliminemos SNMP de la imagen en este momento y observemos un modelo para la administración de red llamado FCAPS, o Administración de fallas, Administración de configuración, Administración de contabilidad, Administración de rendimiento y Administración de seguridad. Estas áreas conceptuales fueron creadas por la Organización Internacional de Normalización (ISO) para ayudar a comprender las principales funciones de los sistemas de gestión de redes. Veamos brevemente cada uno de estos ahora.

El objetivo de la gestión de fallas es detectar, registrar y notificar a los usuarios de los sistemas o redes de problemas. En muchos entornos, el tiempo de inactividad de cualquier tipo no es aceptable. [1]

Objetivo

General

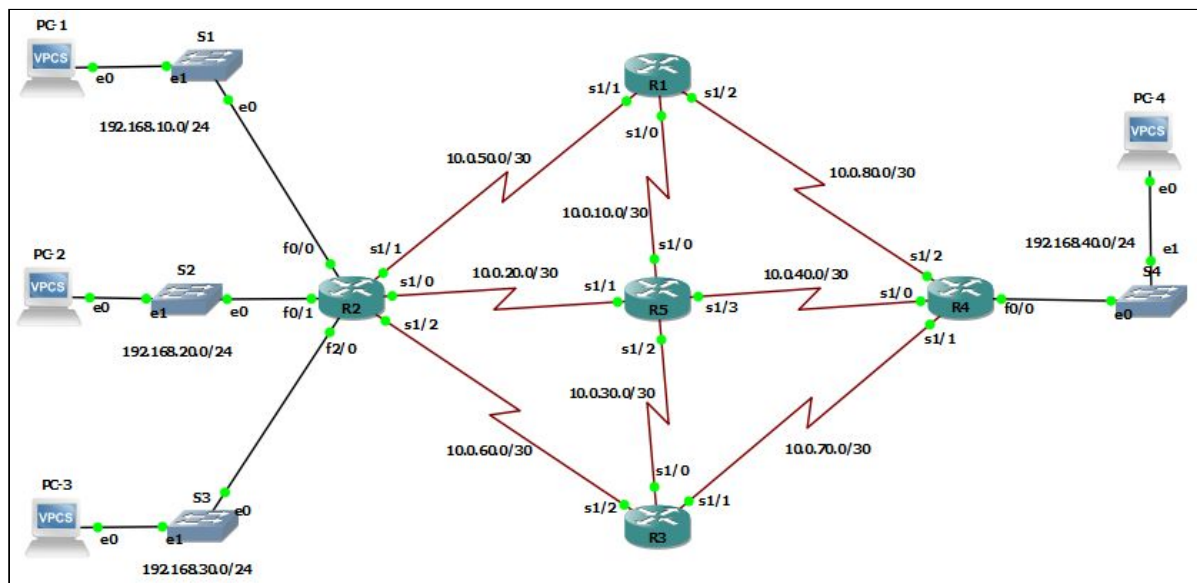
Desarrollar un sistema que monitoree el rendimiento de los componentes de hardware de los routers de una red.

Específicos

1. Monitorear el uso de la CPU de los routers de una red.
2. Monitorear la capacidad de la memoria de los routers en una red.
3. Monitorear el nivel de temperatura de los routers en una red.
4. Alertar al administrador cuando el rendimiento de un router no sea óptimo.

Desarrollo

Topología en GNS3



Topología de la red en GNS3 antes de conectar con nuestra PC

Tabla de Direcccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	Se1/0	10.0.10.1	255.255.255.252	NA
R1	Se1/1	10.0.50.1	255.255.255.252	NA
R1	Se1/2	10.0.80.1	255.255.255.252	NA
R2	Se1/0	10.0.20.1	255.255.255.252	NA
R2	Se1/1	10.0.50.2	255.255.255.252	NA
R2	Se1/2	10.0.60.1	255.255.255.252	NA
R2	Fa0/0	192.168.10.1	255.255.255.0	NA
R2	Fa0/1	192.168.20.1	255.255.255.0	NA
R2	Fa2/0	192.168.30.1	255.255.255.0	NA
R3	Se1/0	10.0.30.1	255.255.255.252	NA
R3	Se1/1	10.0.70.1	255.255.255.252	NA
R3	Se1/2	10.0.60.2	255.255.255.252	NA
R4	Se1/0	10.0.40.1	255.255.255.252	NA
R4	Se1/1	10.0.70.2	255.255.255.252	NA
R4	Se1/2	10.0.80.2	255.255.255.252	NA
R4	Fa0/0	192.168.40.1	255.255.255.0	NA

R5	Se1/0	10.0.10.2	255.255.255.252	NA
R5	Se1/1	10.0.20.2	255.255.255.252	NA
R5	Se1/2	10.0.30.2	255.255.255.252	NA
R5	Se1/3	10.0.40.2	255.255.255.252	NA
PC1	E0	DHCP	DHCP	DHCP
PC2	E0	DHCP	DHCP	DHCP
PC3	E0	DHCP	DHCP	DHCP
PC4	E0	DHCP	DHCP	DHCP

Configuración de la red

Se hizo la siguiente configuración en la red:

- Configuración de interfaces
- Configuración de protocolo de enrutamiento RIPv2
- Configuración de R5 como servidor DHCP para R2 Y R4
- Configuración de DHCP en todas las PCs
- Configuración de la comunidad de SNMP en los routers

* Para ver la configuración completa de cada dispositivo de clic en: [Configuración](#)

Conectar nuestra PC a GNS3

Para poder desarrollar y probar software en GNS3 es necesario configurar ciertos aspectos tanto en nuestra PC como en GNS3. A continuación se describen los pasos para conectar una PC con Windows a nuestra topología en GNS3. [2]

1. Primeramente se necesita crear una **interfaz Loopback** en nuestra PC.
Para crearla en Windows puede ejecutar en la línea de comandos: **hddwwiz.exe**
IMPORTANTE: debe ejecutar la línea de comandos como **ADMINISTRADOR**
Después de ejecutar el comando se despliega un wizard para crear la interfaz.

Add Hardware

The wizard can help you install other hardware

The wizard can search for other hardware and automatically install it for you. Or, if you know exactly which hardware model you want to install, you can select it from a list.

What do you want the wizard to do?

- ☐ Search for and install the hardware automatically (Recommended)
- ☒ Install the hardware that I manually select from a list (Advanced)

< Back

Next >










Cancel

Add Hardware

From the list below, select the type of hardware you are installing

If you do not see the hardware category you want, click Show All Devices.

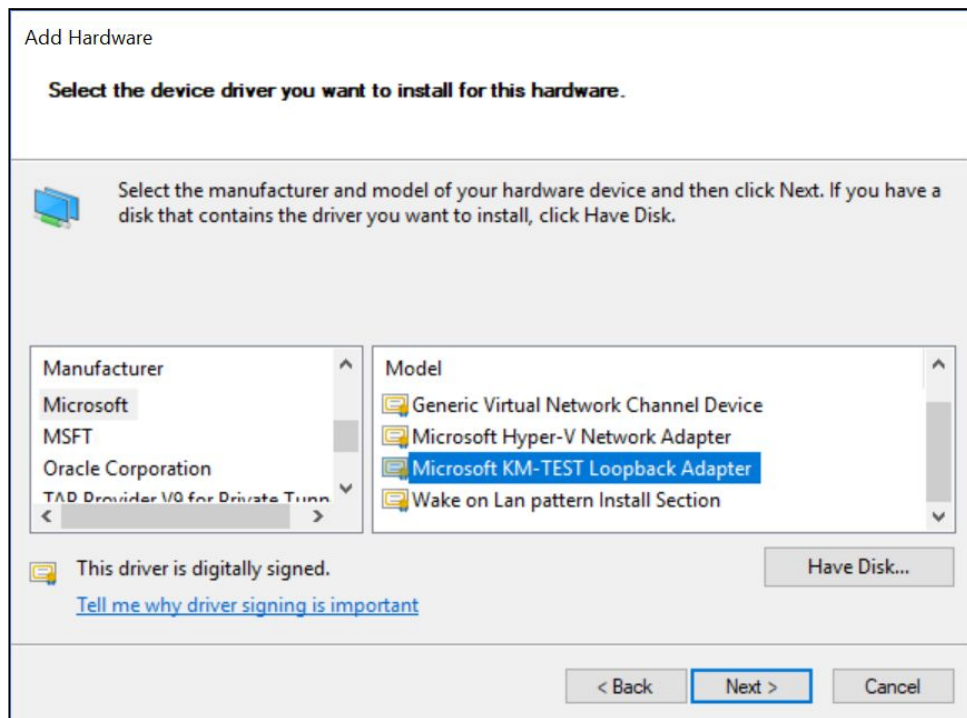
Common hardware types:

-  Modems
-  Multi-port serial adapters
-  Network adapters
-  OPOS Legacy Device
-  PCMCIA adapters
-  Ports (COM & LPT)
-  POS Barcode Scanner
-  POS Cash Drawer
-  POS HID Magnetic Stripe Reader

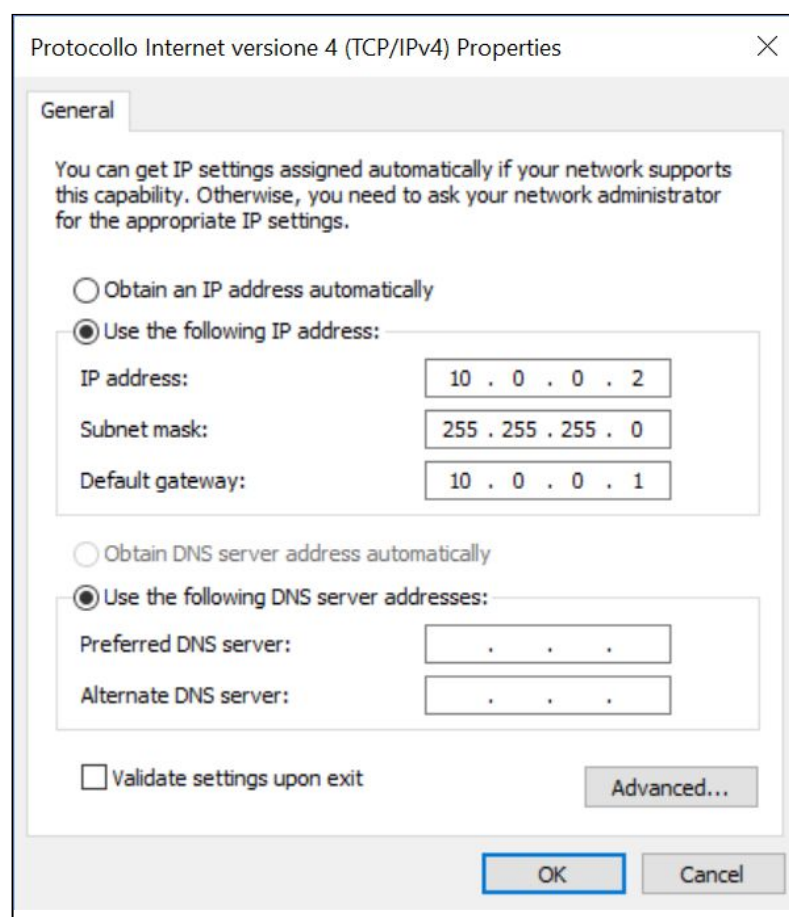
< Back

Next >

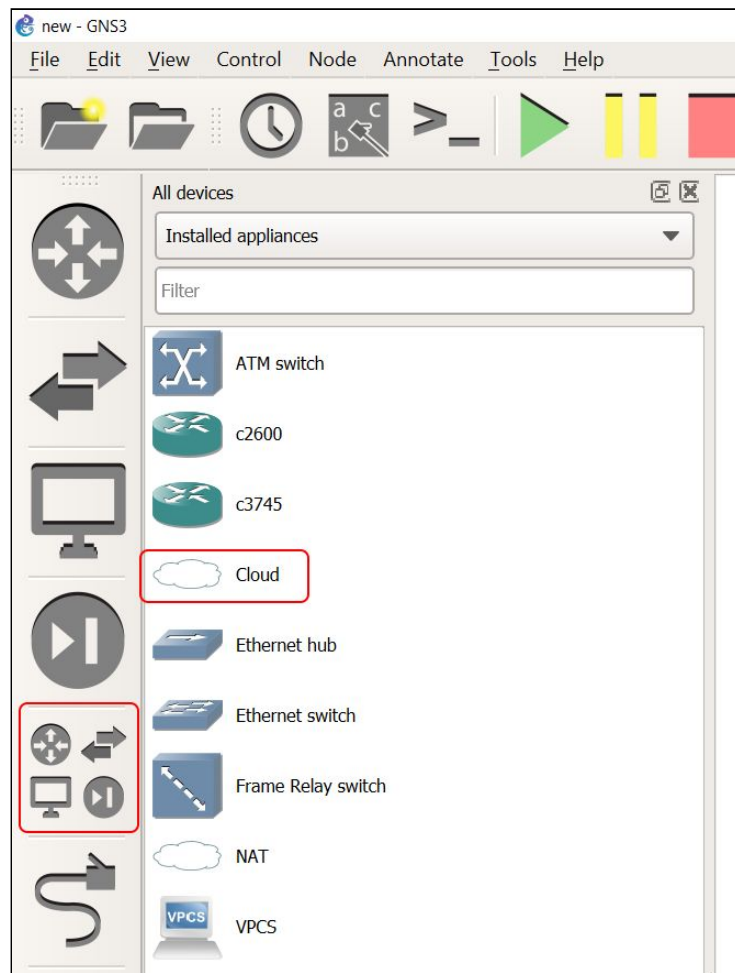
Cancel



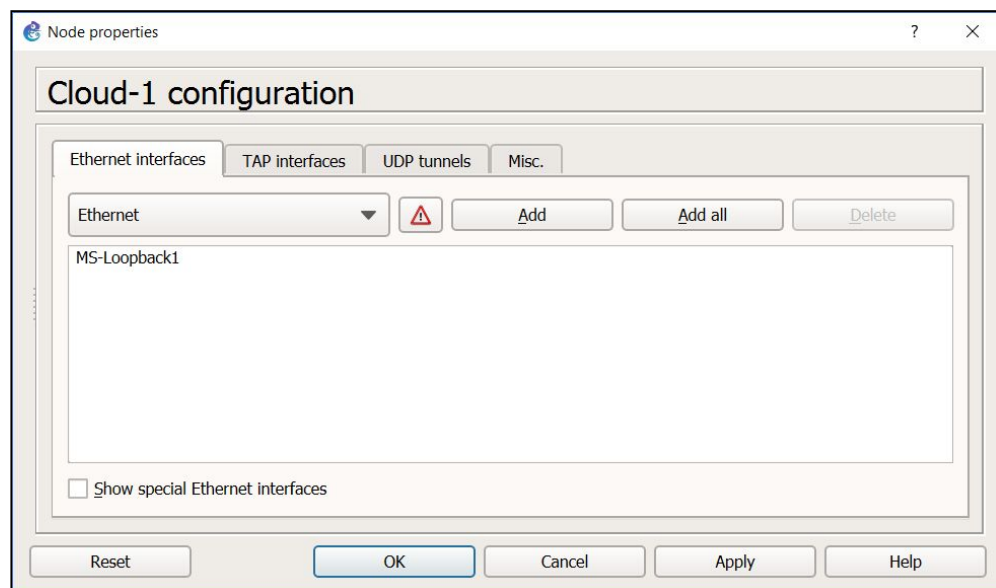
2. Una vez creada la interfaz se debe asignar la configuración IP. (Esta configuración es la misma que tendrá dentro de GNS3)



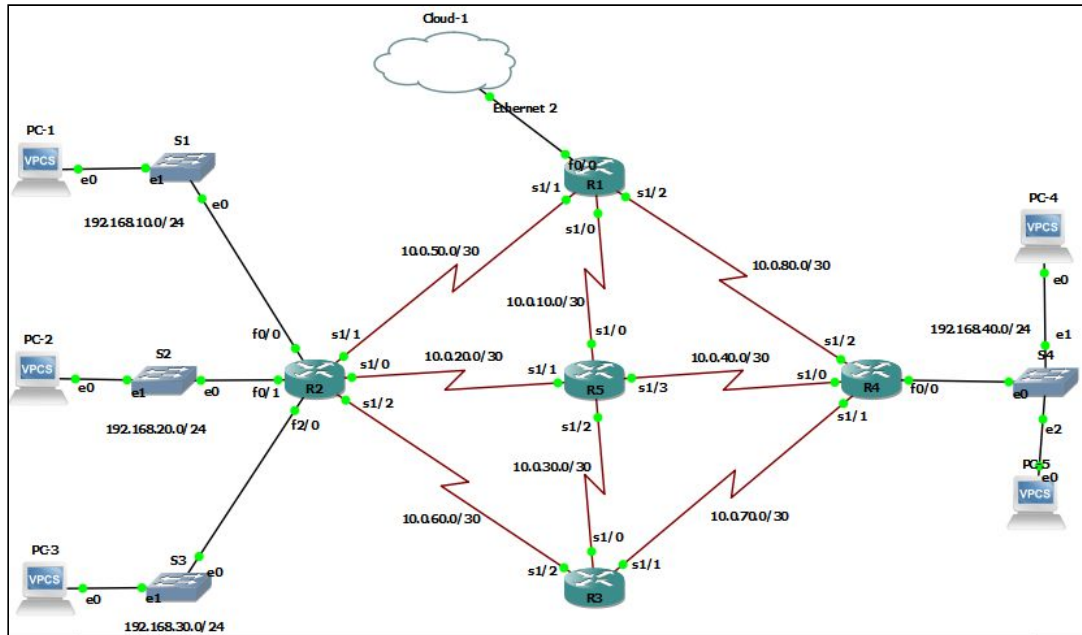
3. Para traer nuestra PC a GNS3 se debe agregar una **Cloud** a la topología.



4. Entrar a la configuración de la Cloud y agregar la interfaz Loopback que creamos previamente.



5. Agregar la configuración necesaria, para que la Cloud pueda comunicarse con el resto de la red (por ejemplo: el enrutamiento).



6. Finalmente tenemos “una instancia de nuestra PC” en GNS3 y de esta manera podemos interactuar con los elementos de nuestra red (en nuestro caso, nos interesa interactuar con los routers de la red).

* Para una descripción más detallada visite el tutorial en línea: [Tutorial Completo](#)

Monitoreo de routers

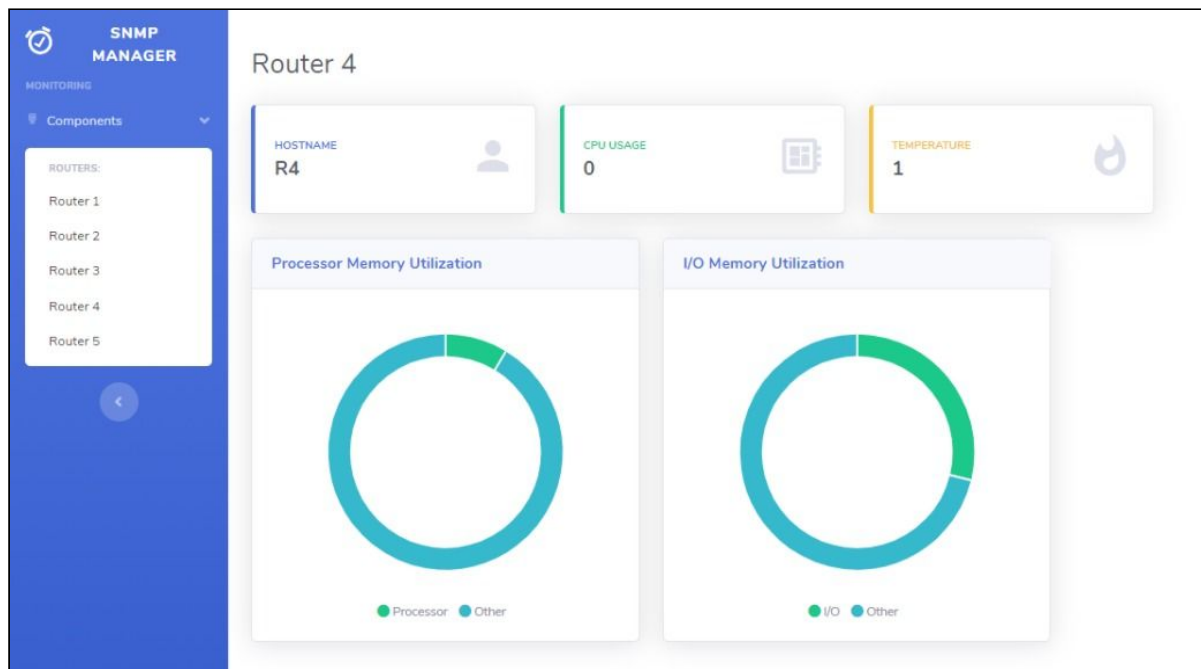
Desarrollamos con **Python** haciendo uso del paquete **pysnmp** un gestor de **SNMP**, que se comunica con los routers de nuestra red y a través de **OIDs** obtiene información de estos, tales como: su hostname, uso del CPU, uso de memoria del procesador, uso de memoria I/O y temperatura.

```
def get(target, oids, credentials, port=161, engine=hlapi.SnmpEngine(),
context=hlapi.ContextData()):
    handler = hlapi.getCmd(
        engine,
        credentials,
        hlapi.UdpTransportTarget((target, port)),
        context,
        *construct_object_types(oids)
    )
    return fetch(handler, 1)[0]
```

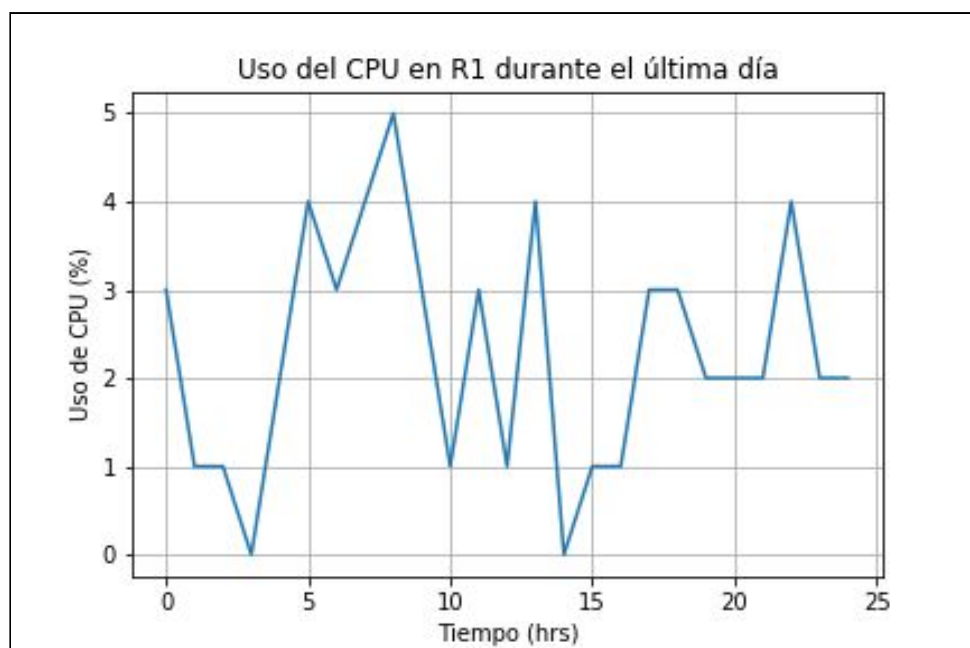
Función “get” obtiene los OIDs de los routers

Creación de aplicación web

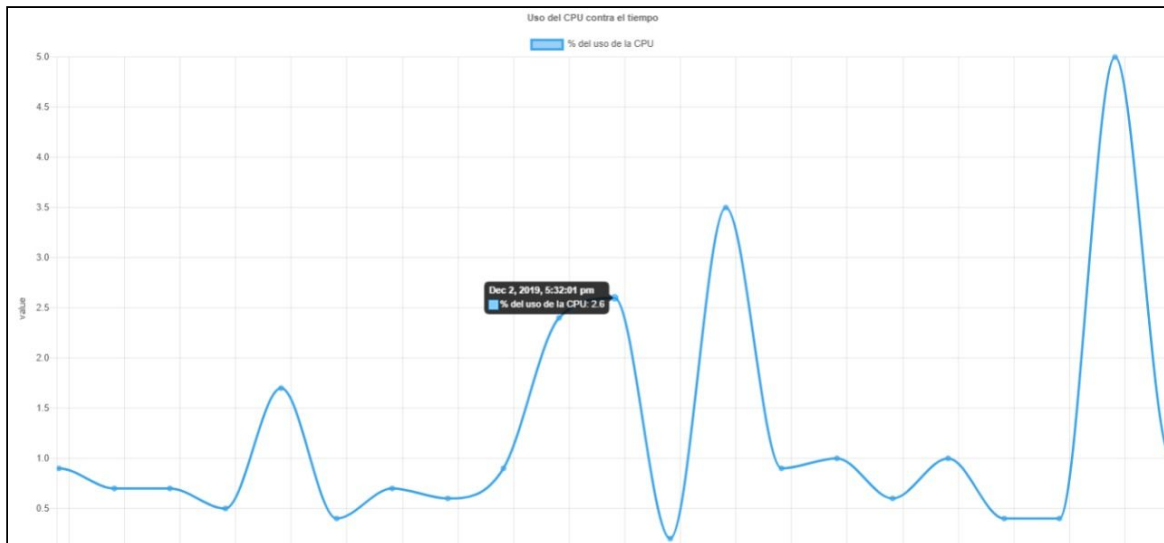
Para el despliegue de nuestro sistema de monitoreo se desarrolló una aplicación web con **Django**, que proporciona interfaces para la visualización de los aspectos que se monitorean en los routers de nuestra red, además de implementar más funcionalidades, tales como gráficas en tiempo real sobre el estado de los routers y generación de reportes sobre el rendimiento de estos.



Captura de la aplicación web: monitoreo de R4

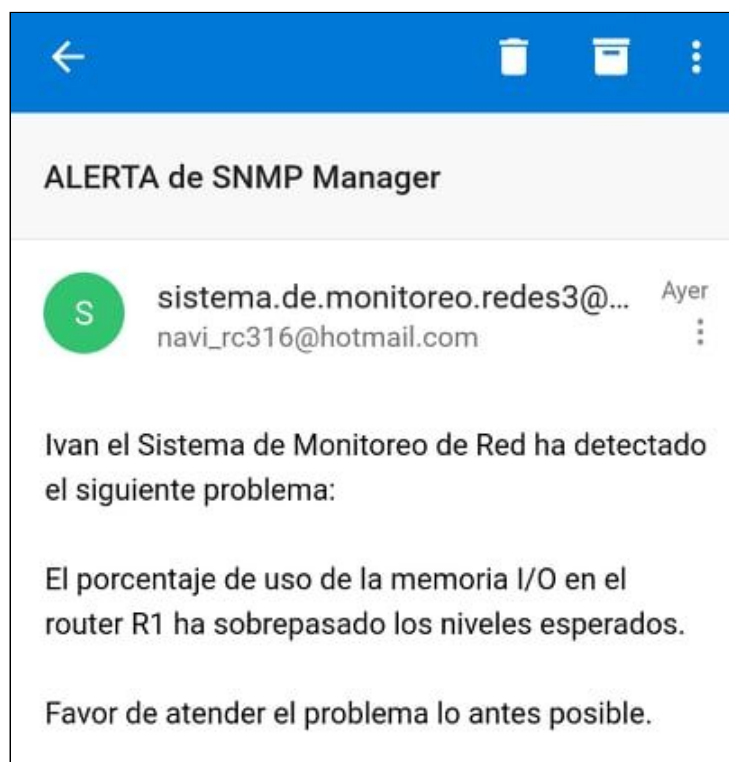


Gráfica sobre el uso del CPU de R1 en las últimas 24 hrs



Gráfica en tiempo real del uso del CPU de un router

El sistema de monitoreo tiene también la función de enviar a los una **ALERTA** mediante correo electrónico, cuando se detecta que el rendimiento de los routers no es óptimo, por ejemplo, cuando el % de uso CPU es muy alto.



Ejemplo del correo de ALERTA que envía el sistema

Para ver el código fuente de todo el proyecto puede visitar el [Repositorio de Github](#).

Conclusiones

El cometido principal del proyecto era realizar un monitoreo de los agentes (routers), que en éste caso son los routers. Que nos permitiera una mejor gestión de la red a través del rendimiento; sin embargo, nos dimos cuenta que no sólo sirve para ésta rama de la gestión de redes, incluso sirve para las demás.

Para la gestión de fallos sirve para prevenir al administrador de posibles fallos, ya que éste puede verificar el estado del hardware de los routers. Sabemos que la gestión de fallos es más reactivo, sin embargo, se puede utilizar para verificar el estado de éstos después del fallo también.

Para la gestión de rendimiento sirve para hacer un análisis del rendimiento de los componentes de hardware del agente. Si el desempeño de algún componente supera el umbral establecido por el administrador, el sistema enviará una alerta para que tome un comportamiento preventivo o en todo caso reactivo.

Para la gestión de configuración sirve para poder visualizar de manera más sencilla el estado de los routers, así como la cantidad de éstos. Así como también ver el estado de su memoria y del CPU.

Aunque éste proyecto se hizo de manera específica terminó siendo holístico e incluso podría serlo aún más si se invierte más tiempo y esfuerzo en él.

Referencias Bibliográficas.

[1] Essential SNMP. 2005. (2nd ed.). O'Reilly Media, Inc.