



PERÍODO 2020



II PAO 2020 ASSR – PROYECTO
DESARROLLO DE ALERTAS EN UNA RED DE DATOS
BASADO EN NETCONF/YANG

DOCENTE: ADRIANA ELISA COLLAGUAZO JARAMILLO MATERIA:
ADMINISTRACIÓN DE SISTEMAS Y SERVICIOS EN RED
CARRERA DE INGENIERÍA EN TELEMÁTICA

FIEC-ESPOL



Contenido

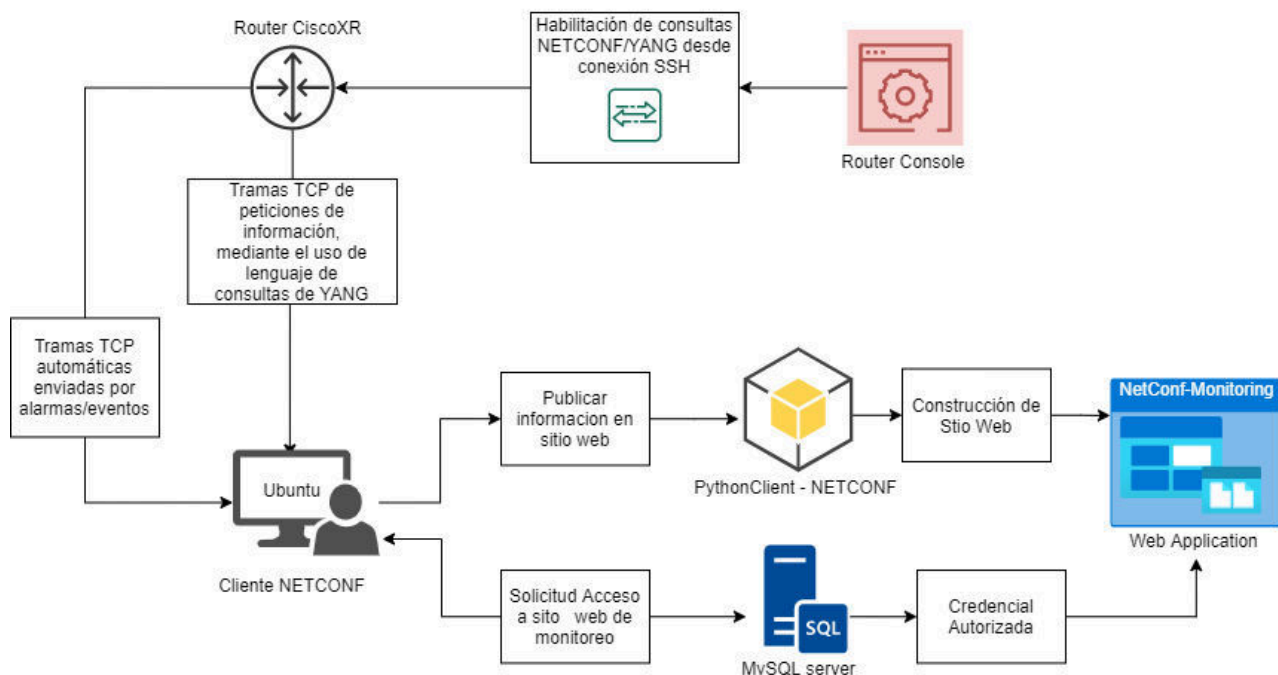
1.	Introducción.....	3
2.	Diagrama de Proyecto	3
3.	Diagrama de Despliegue	4
4.	Diagrama de Entidad-Relación	4
5.	Topología de Red	5
6.	Habilitación del Protocolo NETCONF:.....	10
7.	Instalación de paquete k9Sec del Protocolo NETCONF:	10
7.1	Prueba de Conectividad:.....	11
8.	Resultados:.....	11
8.1	Servidor Web	11
8.2	Registros en Consola Cisco	14
9.	Presupuesto	14
10.	Conclusiones	15
11.	Referencias:	15

1. Introducción

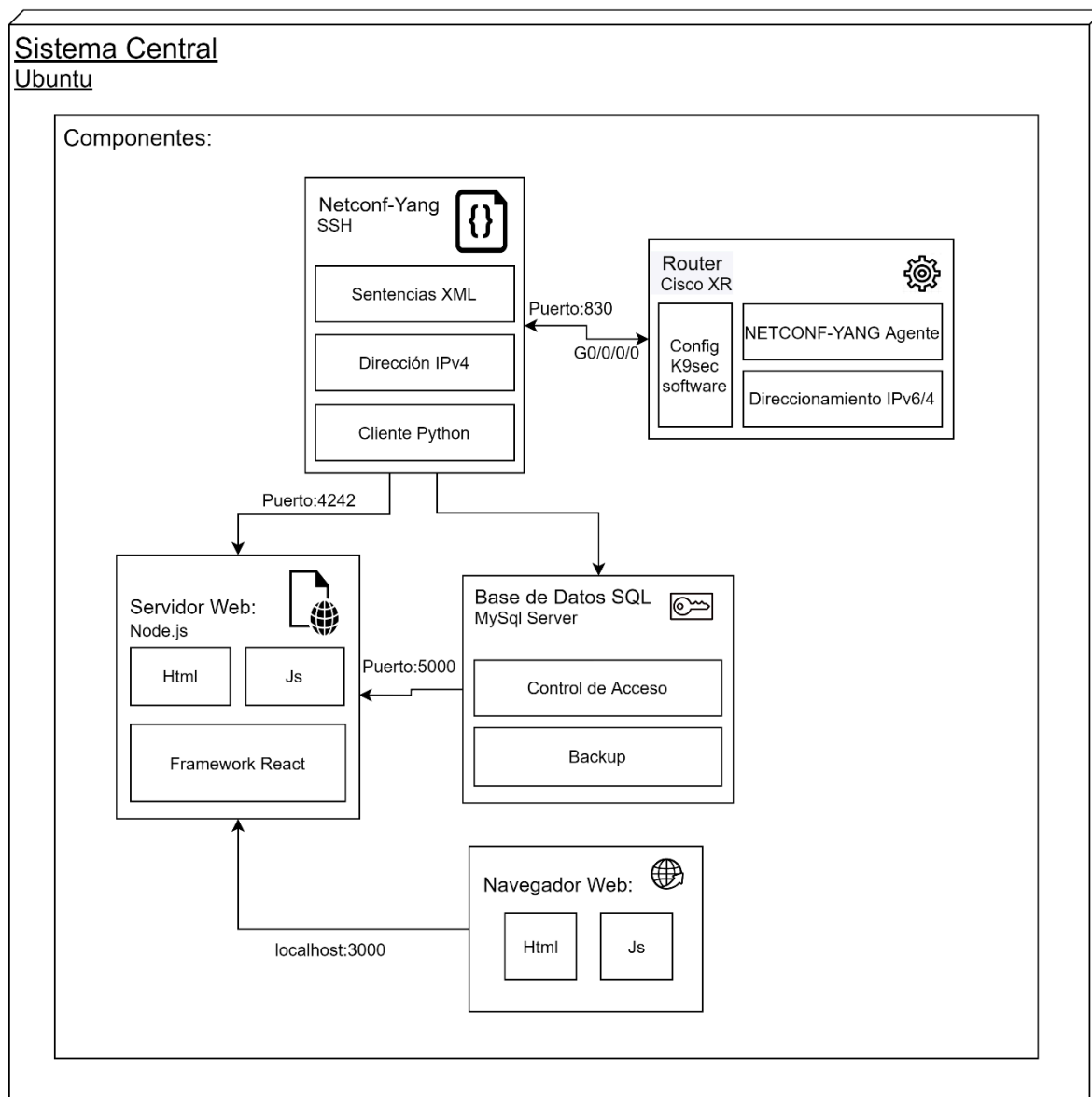
En el presente proyecto se busca diseñar un sitio web que permita monitorizar las actividades y alertas de un Router Cisco de la serie XR en una red de datos. Para ello se utilizará el protocolo NETCONF que permite entre otras cosas, obtener información del tráfico y configuraciones de dispositivos en red como router, switch, etc. Este protocolo es de gran importancia ya que nos permite obtener los logs del sistema y a su vez generar eventos o alarmas que permitan detectar comportamientos raros en la red o el nivel de tráfico en las interfaces de un router. Para configurar este protocolo es necesario tener presente tres elementos claves:

- Cliente NETCONF: Es el encargado de solicitar y recibir las peticiones y alarmas solicitadas del router, para establecer el enlace se establece una conexión SSH por el puerto 830, puerto que espera un mensaje de saludo del cliente en formato XML.
- Agente NETCONF: Dirigido por el Router, este necesita además de habilitar las conexiones SSH permitir que el protocolo NETCONF reciba y envíe consultas/respuestas mediante YANG, el cuál es un lenguaje de consultas que utiliza sintaxis XML
- Instalación de paquete de Software k9sec Pie y habilitación de la generación de Crypto-clave pública RSA en el sistema del Router XR.

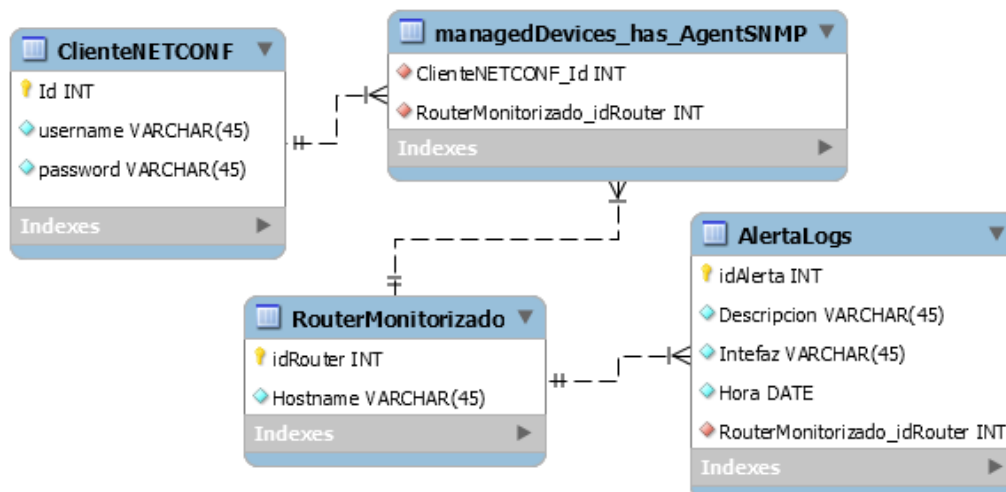
2. Diagrama de Proyecto



3. Diagrama de Despliegue



4. Diagrama de Entidad-Relación



5. Topología de Red

En la topología solicitada se debe implementar una red segmentada por un router Cisco de la serie XR, para ello, es necesario que previamente se preparen e instalen las herramientas necesarias para añadir la imagen del modelo respectivo al entorno de simulación GNS3:

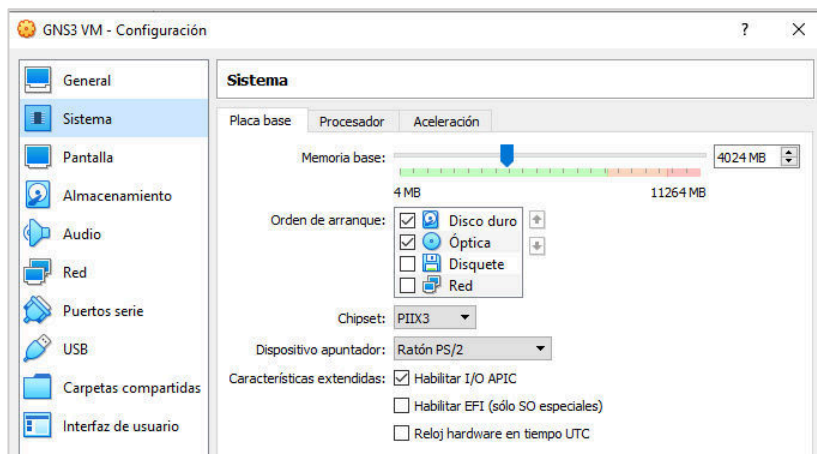
A continuación se detallan los recursos necesarios para replicar el proceso de adición del router Cisco XR utilizado en este proyecto:

- Software de Virtualización: para el desarrollo del presente proyecto se utilizó el software de VirtualBox, sin embargo, puede elegir el de su preferencia.
- Software de simulación de redes: se usó el software GNS3, es aquí donde se construirá de manera virtual la topología de la red que incluirá el router Cisco XR que será monitorizado.
- Máquina Virtual GNS3 VM: servidor de la topología sobre donde el sistema de router Cisco XR se ejecutará.
- Máquina Virtual Ubuntu 20.04 LTS
- Imagen de IOS Cisco XR.

Pasos para la implementación:

1. En primer lugar se deben preparar las máquinas virtuales que se utilizarán en la simulación:

Para el caso de GNS3 VM, la podrá descargar desde el siguiente enlace <https://www.gns3.com/software/download-vm>. Dentro de las configuraciones de la VM deberá asignar mínimo 4Gb de memoria RAM, ya que parte de esta será utilizada por el Router Cisco XR.



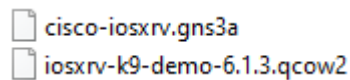
Para la segunda máquina virtual deberá instalar el S.O. de Ubuntu 20.04 LTS siguiendo el proceso ya conocido de instalación, dentro de los requerimientos mínimos más importantes tenemos:

- 2 núcleos de procesamiento
 - 1024 MB de Memoria RAM
 - 1 adaptador de Red
2. Lo siguiente que debe realizar es importar el Router XR, para ello deberá seleccionar y descargar el modelo a utilizar, esto dependerá de la cantidad de memoria base que disponga el dispositivo Host, ya que dependiendo del modelo el consumo aumenta.

Paralelo 1 - Grupo 4:

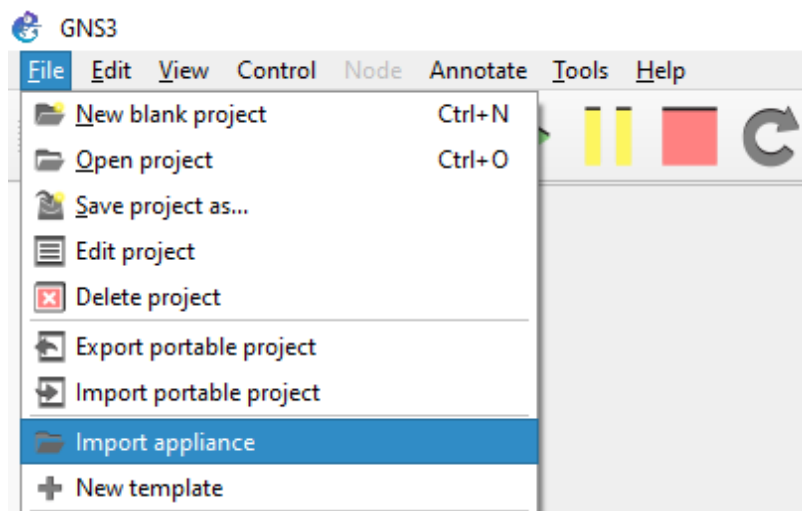
- García Erick

Para este proyecto se utilizó el modelo: “Cisco Router XRv6.1.3” el cual requiere un mínimo de 3Gb de RAM que serán tomados del GNS3 VM, para ello se descargaron los siguientes ficheros:

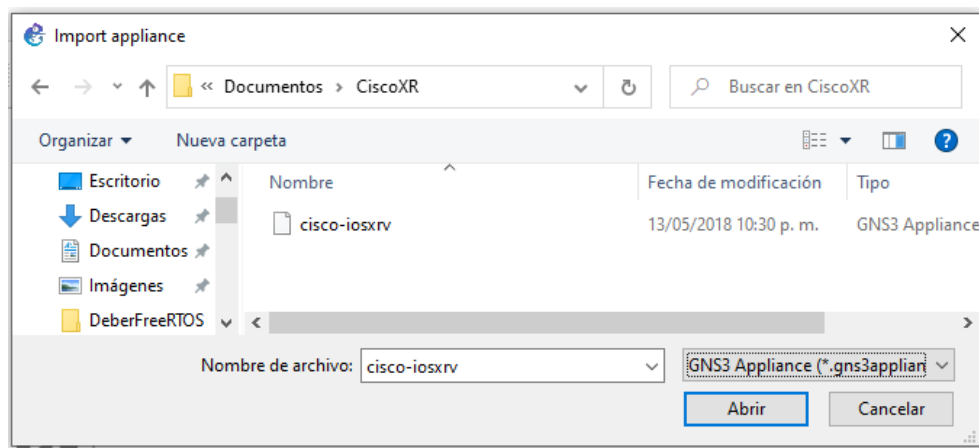


- Cisco-iosxrv.gns3a que contiene la configuración y diseño del template del router del gns3.
- iosxrve-k9-demo-6.1.3.qcow2, el cual es una imagen de prueba del modelo xrv6.1.3 del router Cisco y que será añadida al template previamente descrito.

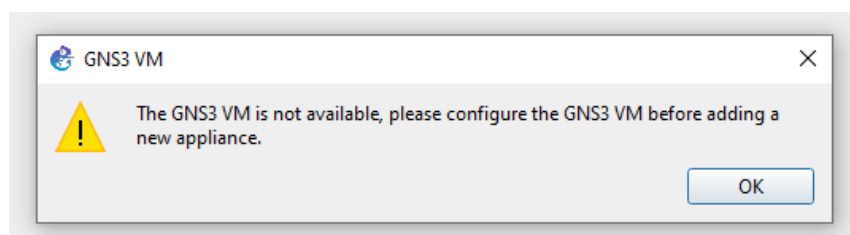
Para agregar la imagen al sistema de GNS3 primero hacemos clic en la opción **Import appliance**, ubicado en el menú de Files:



Se abrirá un cuadro de búsqueda donde deberá indicar la ruta del template del router:



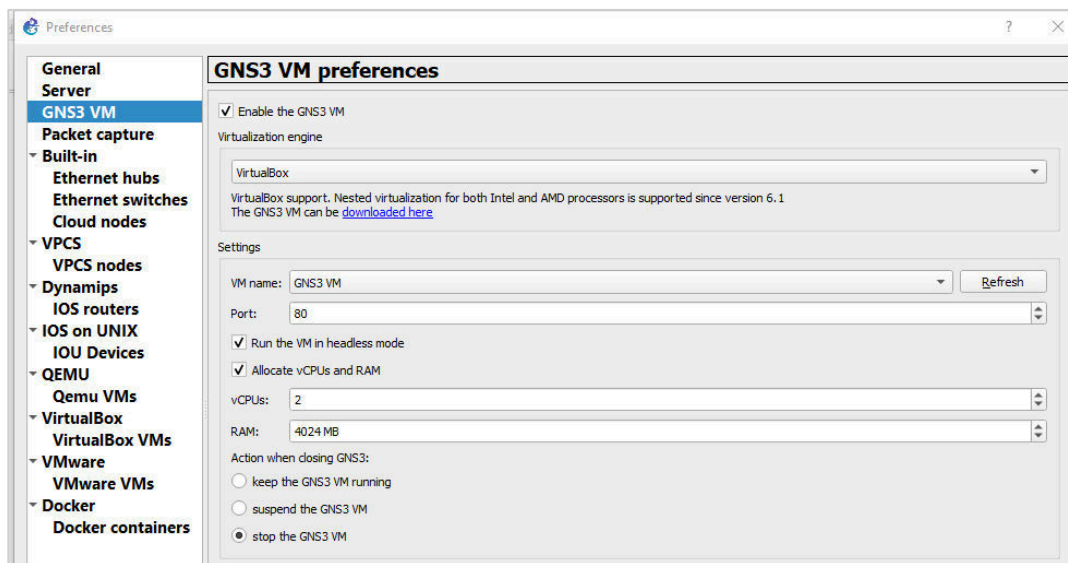
En caso de recibir una alerta como esta:



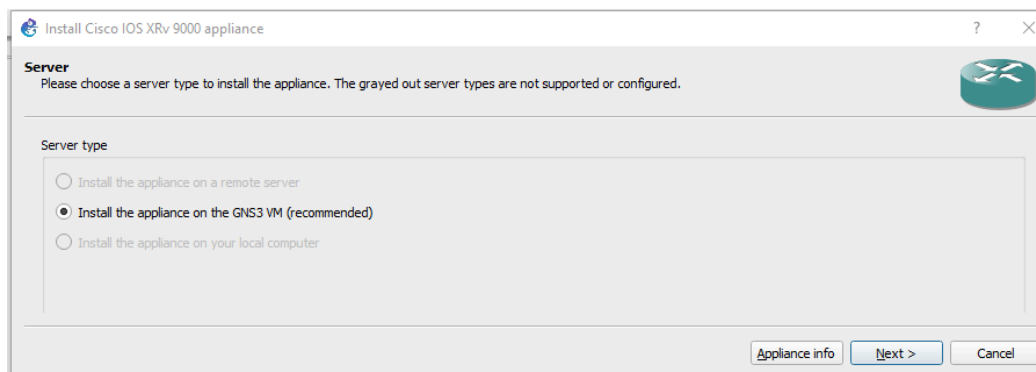
Paralelo 1 - Grupo 4:

- García Erick

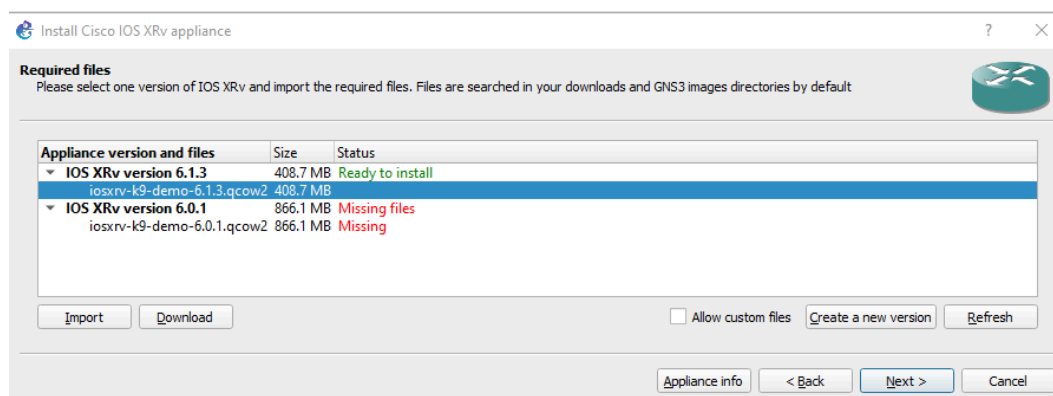
Deberá activar y configurar el servidor GNS3 VM, configurado en el paso 1, como se muestra a continuación:



Ya configurado el servidor, se nos mostrará la siguiente ventana luego de seleccionar el template:



Damos clic en Next, hasta llegar la ventana que se muestra:

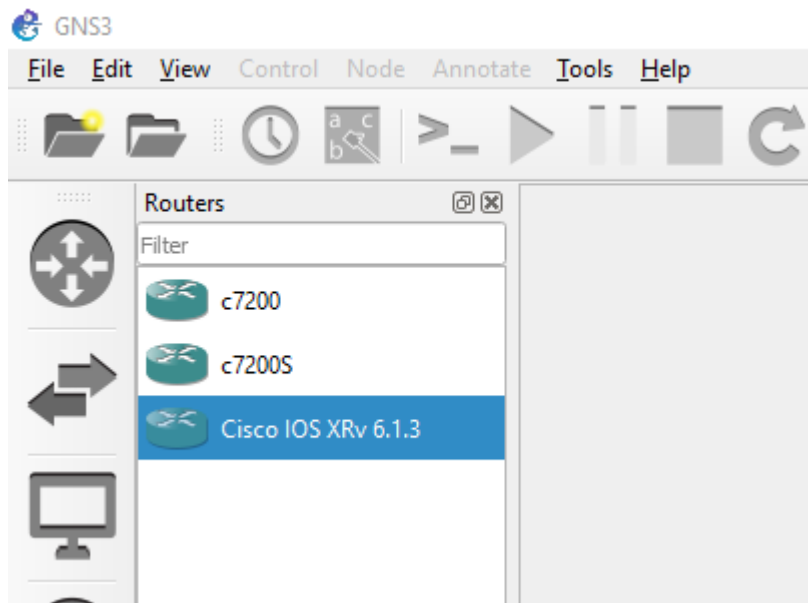


En esta ventana seleccionamos el archivo .qcow2 que descargamos anteriormente y damos clic en importar. Finalizada la importación presionamos el botón Next y luego Finish.

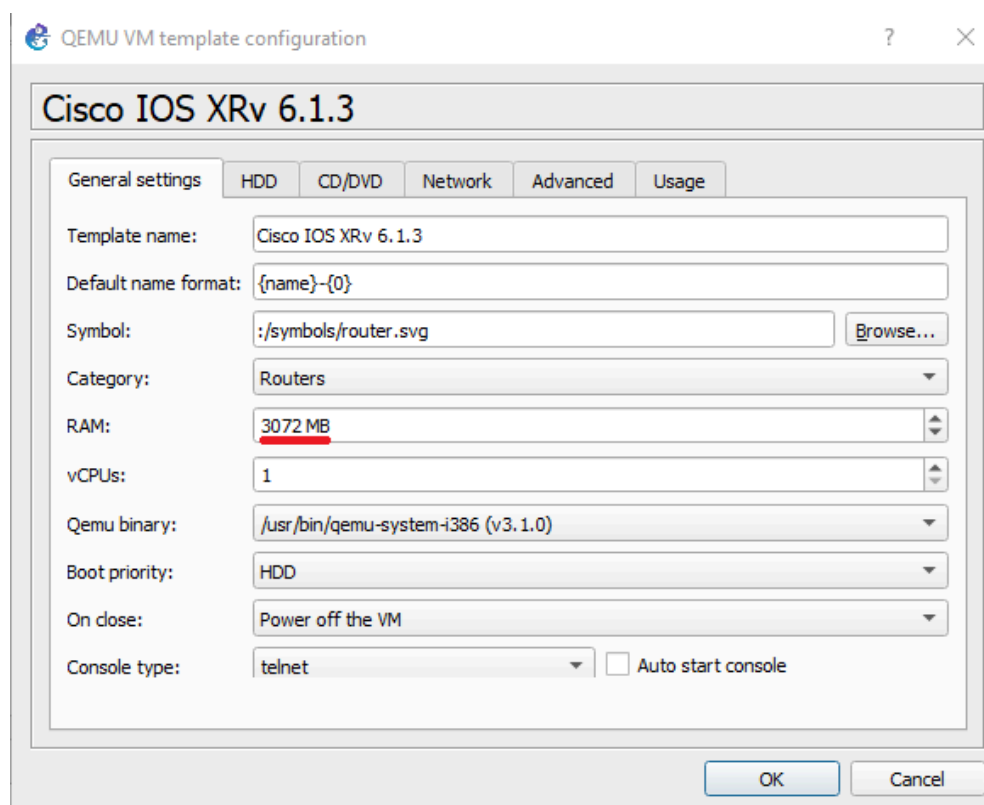
Paralelo 1 - Grupo 4:

- García Erick

Podremos verificar que el router fue importado correctamente buscándolo en la pestaña de los Templates:



Como último paso deberá asignar la cantidad de memoria mínima dentro de las configuraciones del router, para ello de clic derecho sobre el template del router y seleccionar la opción de **Configure terminal**



Como se mencionó anteriormente este modelo necesita un mínimo de 3GB de memoria RAM, de tener los recursos necesarios se recomienda aumentar el número de vCPUs ya que esto permitirá que el S.O. de Cisco XR inicie en menor tiempo.

Finalizado el proceso de instalación de la imagen del router Cisco XR ya podemos diseñar la topología de nuestra Red de tal forma que se implemente al menos un router de la serie XR.

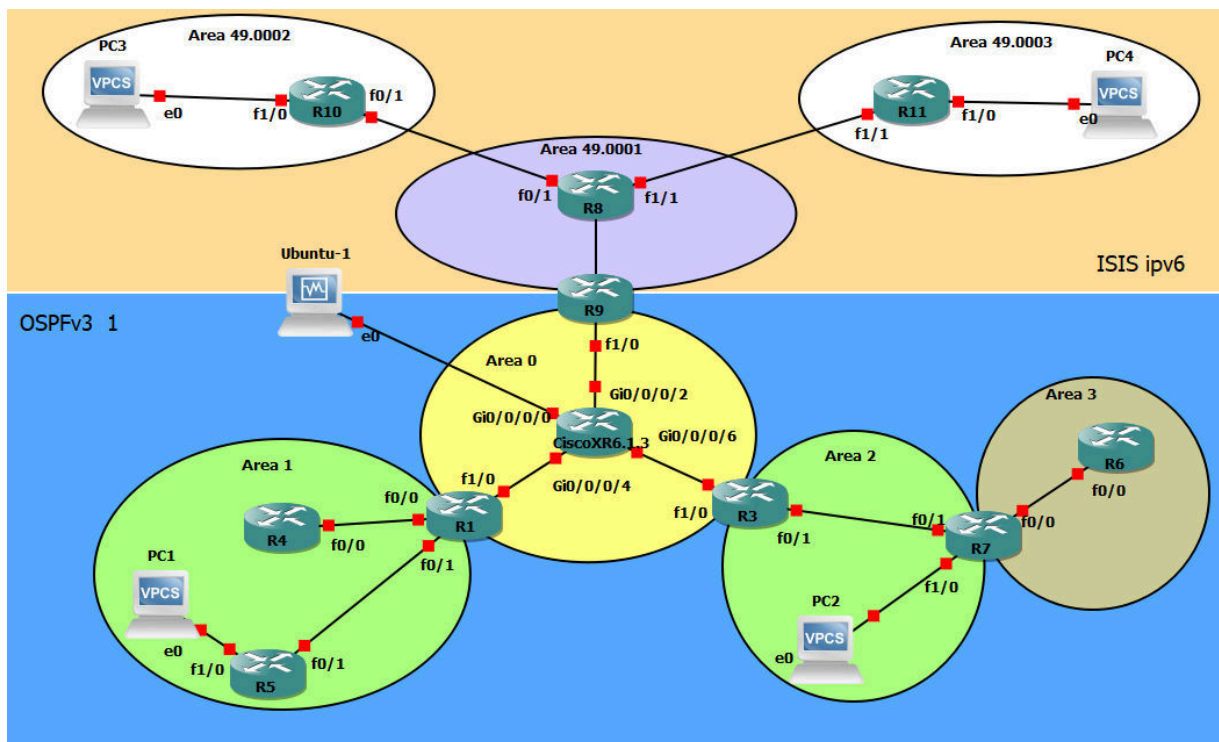


Figura 1. Diseño de Topología de Red

El diseño de esta topología puede realizarse a criterio personal, en este caso la red construida está formada por varios grupos de redes distribuidas en dos zonas, la primera ubicada en la parte superior utiliza el protocolo de enrutamiento ISIS en sus routers y cuenta con 3 áreas distintas. En la parte inferior se configuró el protocolo OSPFv3, esta segmentada en 3 áreas conectadas al backbone o área 0.

La red se encuentra direccionada con el protocolo IPv6, a excepción de la interfaz conectada a la máquina de Ubuntu que cumple con la función de Gestor SNMP, y sigue el siguiente direccionamiento:

Dispositivo	Interfaz	Dirección IPv6	Gateway
R1	F1/0	2001:DB8:ACAD:12::1/64	N/A
	F0/0	2001:DB8:ACAD:1::1/64	N/A
	F0/1	2001:DB8:ACAD:2::1/64	N/A
CiscoXRv6.1.3	G0/0/0/4	2001:DB8:ACAD:12::2/64	N/A
	G0/0/0/6	2001:DB8:ACAD:23::2/64	N/A
	G0/0/0/2	2001:DB8:ACAD:30::2/64	N/A
	G0/0/0/0	192.168.1.1/24 (Ipv4)	N/A
R3	F1/0	2001:DB8:ACAD:23::3/64	N/A
	F0/1	2001:DB8:ACAD:6::1/64	N/A
R4	F0/0	2001:DB8:ACAD:1::2/64	N/A
R5	F0/1	2001:DB8:ACAD:2::2/64	N/A
	F1/0	2001:DB8:ACAD:7::1/64	N/A
R6	F0/0	2001:DB8:ACAD:5::2/64	N/A

R7	F0/0	2001:DB8:ACAD:5::1/64	N/A
	F0/1	2001:DB8:ACAD:6::2/64	N/A
	F1/0	2001:DB8:ACAD:8::1/64	N/A
R9	F1/0	2001:DB8:ACAD:30::2/64	N/A
	F0/1	2001:DB8:ACAD:2::1/64	N/A
R8	F0/0	2001:DB8:ACAD:34::1/64	N/A
	F0/1	2001:DB8:ACAD:35::2/64	N/A
	F1/1	2001:DB8:ACAD:37::2/64	N/A
R10	F0/0	2001:DB8:ACAD:36::2/64	N/A
	F1/0	2001:DB8:ACAD:40::1/64	N/A
R11	F1/1	2001:DB8:ACAD:38::2/64	N/A
	F1/0	2001:DB8:ACAD:39::1/64	N/A
PC1	E0	2001:DB8:ACAD:7::2/64	2001:DB8:ACAD:7::1
PC2	E0	2001:DB8:ACAD:8::2/64	2001:DB8:ACAD:8::1
PC3	E0	2001:DB8:ACAD:40::2/64	2001:DB8:ACAD:40:1
PC4	E0	2001:DB8:ACAD:39::2/64	2001:DB8:ACAD:39:1

6. Habilitación del Protocolo NETCONF:

Como vemos en la Figura 1, El Router XR se encuentra ubicado en el backbone de la red OSPF y se encarga de redistribuir el tráfico de su red hacia la red ISIS. Para el monitoreo de este, es necesario realizar la configuración del protocolo NETCONF mediante la consola del router a monitorizar, para ello realizamos la siguiente configuración

Código:

```
CiscoXR6 # configure terminal
CiscoXR6 (config)# netconf-yang agent ssh port 830
CiscoXR6 (config)# ssh server v2
CiscoXR6 (config)# ssh server netconf
CiscoXR6 (config)# netconf agent tty
CiscoXR6 (config)# commit
```

7. Instalación de paquete k9Sec del Protocolo NETCONF:

K9sec es un paquete de seguridad que da soporte para:

- Secure Sockets Layer (SSL)
- Encriptación, Decipatación
- IPSec, SSH, PKI
- Certificados y otras herramientas de seguridad.

Para añadirlo se debe ingresar el siguiente comando:

```
CiscoXR6 # admin
CiscoXR6 (admin)# install add xrvr-fullk9-x-6.1.3
```

Para comprobar su instalación:

```
RP/0/0/CPU0:ios(admin)#sh install | in k9
Wed Jan 27 03:42:50.284 UTC
disk0:xrvr-fullk9-x-6.1.3
```

7.1 Prueba de Conectividad:

```
PC1> trace 2001:DB8:ACAD:39::2

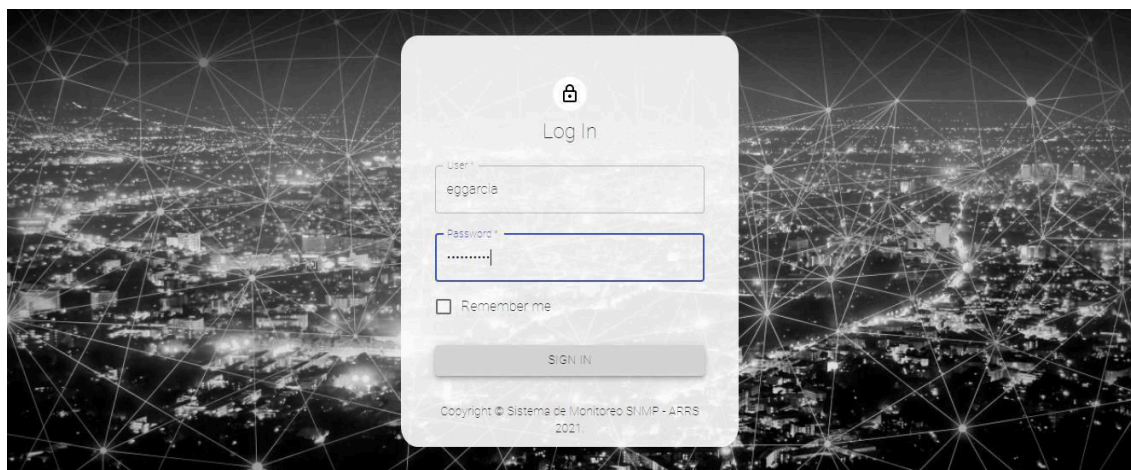
trace to 2001:DB8:ACAD:39::2, 64 hops max
 1 2001:db8:acad:7::1    31.785 ms  14.913 ms  12.087 ms
 2 2001:db8:acad:2::1    45.866 ms  46.404 ms  47.559 ms
 3 2001:db8:acad:12::2   76.739 ms  61.700 ms  62.555 ms
 4 2001:db8:acad:30::3   107.544 ms 89.992 ms  92.204 ms
 5 2001:db8:acad:34::1   121.767 ms 139.875 ms 124.062 ms
 6 2001:db8:acad:38::2   168.213 ms 127.674 ms 174.366 ms
 7 2001:db8:acad:39::2   170.160 ms 184.397 ms 171.027 ms
```

Ping PC1 -> PC4:

8. Resultados:

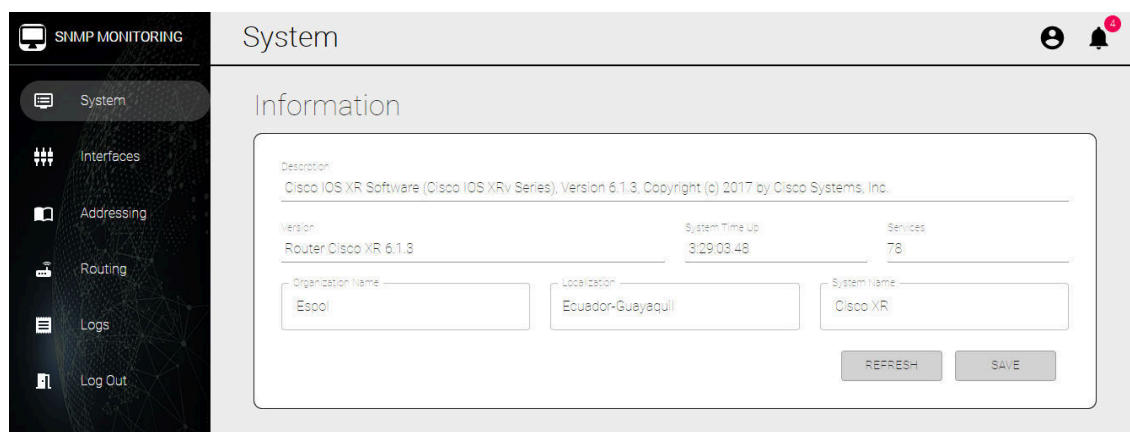
8.1 Servidor Web

LogIn



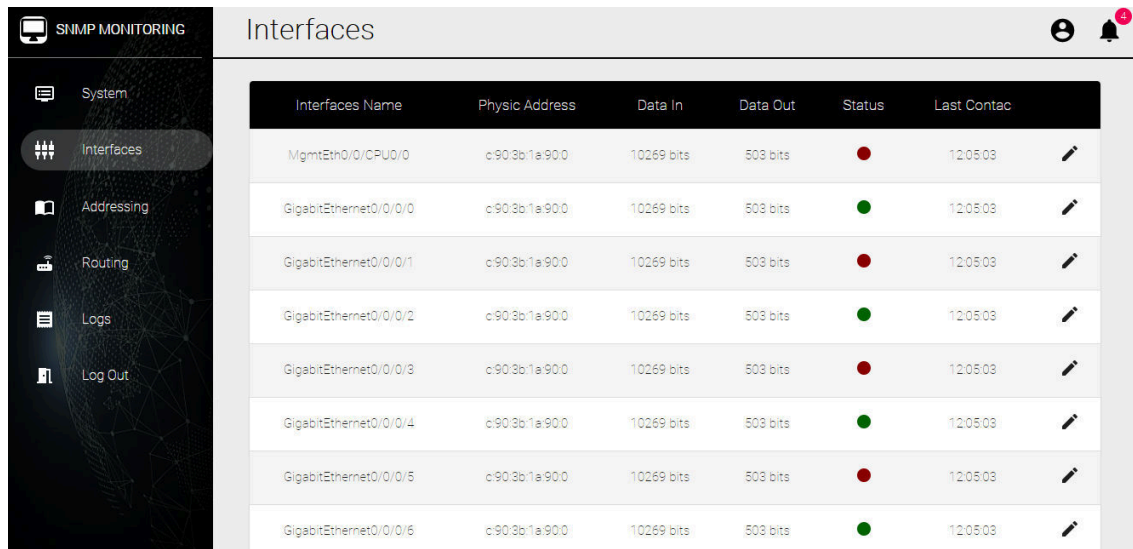
La interfaz LogIn permitirá a los gestores designados ingresar al sistema de monitoreo mediante su usuario y contraseña, que serán validados mediante el uso de la base de datos.









System



En la interfaz System, encontraremos la información básica del Sistema Operativo del router y otras características más comunes que podrán ser editadas desde la interfaz.

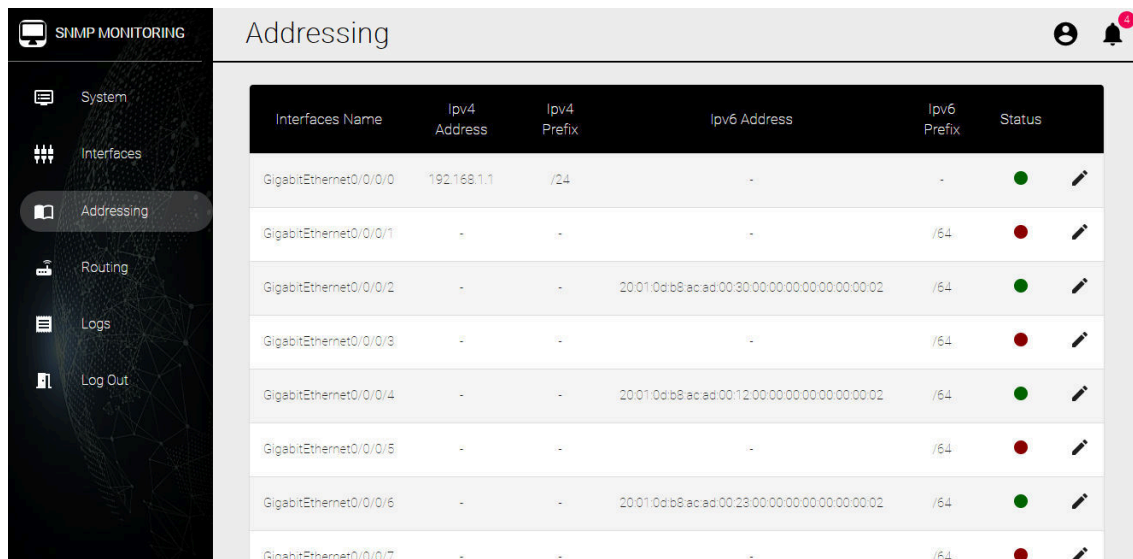
Interfaces











Interfaces Name	Physic Address	Data In	Data Out	Status	Last Contac
MgmtEth0/0/CPU0/0	c903b1a900	10269 bits	503 bits	●	12:05:03 
GigabitEthernet0/0/0	c903b1a900	10269 bits	503 bits	●	12:05:03 
GigabitEthernet0/0/1	c903b1a900	10269 bits	503 bits	●	12:05:03 
GigabitEthernet0/0/2	c903b1a900	10269 bits	503 bits	●	12:05:03 
GigabitEthernet0/0/3	c903b1a900	10269 bits	503 bits	●	12:05:03 
GigabitEthernet0/0/4	c903b1a900	10269 bits	503 bits	●	12:05:03 
GigabitEthernet0/0/5	c903b1a900	10269 bits	503 bits	●	12:05:03 
GigabitEthernet0/0/6	c903b1a900	10269 bits	503 bits	●	12:05:03 

En esta interfaz se presentará información sobre las interfaces del router como dirección física, cantidad de datos enviados y recibidos, estado, entre otros.

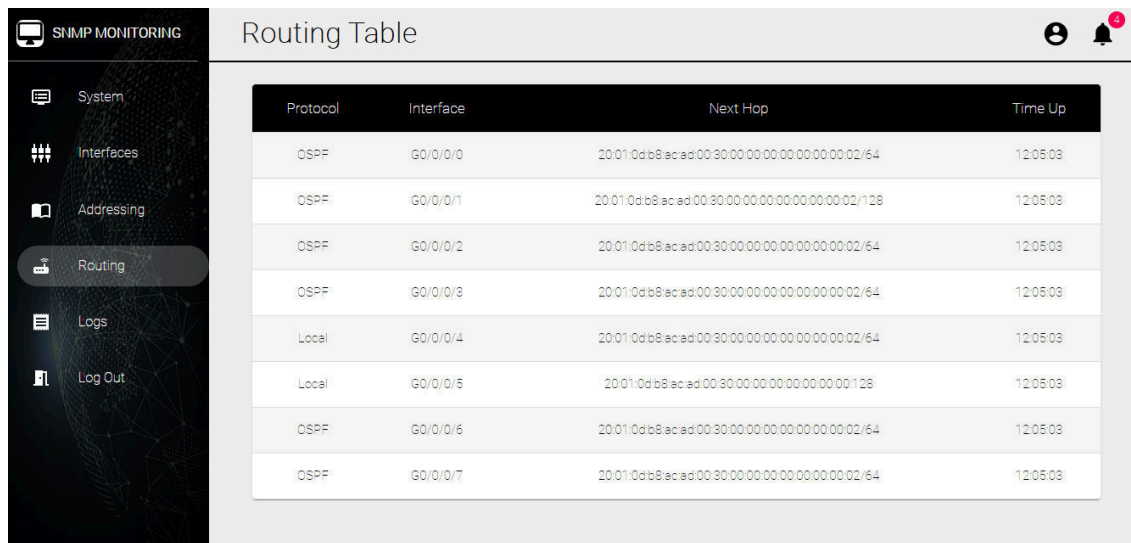
Addressing



Interfaces Name	Ipv4 Address	Ipv4 Prefix	Ipv6 Address	Ipv6 Prefix	Status
GigabitEthernet0/0/0	192.168.1.1	/24	-	-	● 
GigabitEthernet0/0/1	-	-	-	/64	● 
GigabitEthernet0/0/2	-	-	2001:0db8:acad:00:30:00:00:00:00:00:00:02	/64	● 
GigabitEthernet0/0/3	-	-	-	/64	● 
GigabitEthernet0/0/4	-	-	2001:0db8:acad:00:12:00:00:00:00:00:00:00:02	/64	● 
GigabitEthernet0/0/5	-	-	-	/64	● 
GigabitEthernet0/0/6	-	-	2001:0db8:acad:00:23:00:00:00:00:00:00:00:02	/64	● 
GigabitEthernet0/0/7	-	-	-	/64	● 

En esta sección se nos mostrara la tabla de direccionamiento de las interfaces, así como su estado administrativo de las mismas, en este caso tenemos tanto direccionamiento Ipv4 como Ipv6, los cuales podrán ser configurados presionando el icono ubicado a la derecha.

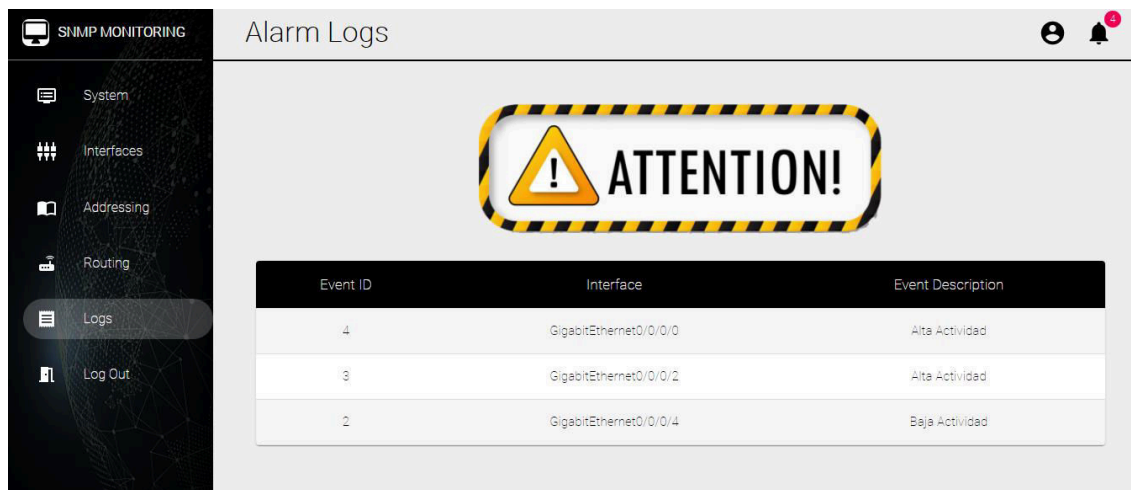
Routing Table



Protocol	Interface	Next Hop	Time Up
OSPF	G0/0/0/0	2001:0db8:acad:00:30:00:00:00:00:00:00:02/64	12:05:03
OSPF	G0/0/0/1	2001:0db8:acad:00:30:00:00:00:00:00:00:02/128	12:05:03
OSPF	G0/0/0/2	2001:0db8:acad:00:30:00:00:00:00:00:00:02/64	12:05:03
OSPF	G0/0/0/3	2001:0db8:acad:00:30:00:00:00:00:00:00:02/64	12:05:03
Local	G0/0/0/4	2001:0db8:acad:00:30:00:00:00:00:00:00:02/64	12:05:03
Local	G0/0/0/5	2001:0db8:acad:00:30:00:00:00:00:00:00:02/128	12:05:03
OSPF	G0/0/0/6	2001:0db8:acad:00:30:00:00:00:00:00:00:02/64	12:05:03
OSPF	G0/0/0/7	2001:0db8:acad:00:30:00:00:00:00:00:00:02/64	12:05:03

La interfaz Routing Table, proporciona información sobre el enrutamiento a cada interfaz a cada siguiente salto de la red, además indicará el protocolo utilizado para el descubrimiento de dicha red y el tiempo activo de la ruta.

Logs



Event ID	Interface	Event Description
4	GigabitEthernet0/0/0/0	Alta Actividad
3	GigabitEthernet0/0/0/2	Alta Actividad
2	GigabitEthernet0/0/0/4	Baja Actividad

En esta ultima interfaz se notificarán las alarmas más recientes detectadas por los agentes configurados en el router, mostrando en el sitio web la descripción del evento detectado como un alto tráfico por una de las interfaces.

8.2 Registros en Consola Cisco

A través de los siguientes comandos podemos verificar que se ha establecido una conexión ssh por medio de la línea NETCONF:

CiscoXR6 (config)# do show netconf-yang clients

```
RP/0/0/CPU0:ios(config)#do show netconf-yang client
Tue Feb  2 00:13:04.683 UTC
Netconf clients
client session ID|      NC version|      client connect time|      last OP time|      last OP type|      <lock>|
4085377167|      unknown|      0d 0h 13m 5s|      |      |      No|
RP/0/0/CPU0:ios(config)#do show netconf-yang
```

En este caso vemos que cada sesión se le establece un ID y se registra el tiempo en el que se ha mantenido la sesión.

CiscoXR6 (config)# do show netconf-yang statistics

```
RP/0/0/CPU0:ios(config)#do show netconf-yang statistics
Tue Feb  2 00:13:15.682 UTC
Summary statistics
request|      # requests|      total time|      min time per request|      max time per request|      avg time per
other|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
close-session|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
kill-session|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
get-schema|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
get|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
get-config|      2|      0h 0m 0s 59ms|      0h 0m 0s 0ms|      0h 0m 0s 59ms|      0h 0m 0
s 29ms|
commit|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
cancel-commit|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
lock|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
unlock|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
discard-changes|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
validate|      0|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0s 0ms|      0h 0m 0
s 0ms|
```

Por otro lado con la opción “statistics” obtenemos las solicitudes o peticiones que se han hecho a cada comando, en este caso podemos observar que se ha ejecutado en dos ocasiones la función de “get-config”.

Otra forma de verificar la conexión es revisando los registros de login, al revisar estos registros podemos ver que el usuario “assr” efectivamente se conectó al router de manera remota.

```
RP/0/0/CPU0:Feb  2 00:10:41 : exec[65724]: %SECURITY-LOGIN-6-CLOSE : User 'assr' logged out
RP/0/0/CPU0:Feb  2 00:12:39 : exec[65724]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'assr' from 'c
onsole' on 'con0_0_CPU0'
RP/0/0/CPU0:Feb  2 00:23:18 : exec[65724]: %SECURITY-LOGIN-6-CLOSE : User 'assr' logged out
RP/0/0/CPU0:Feb  2 00:24:25 : exec[65724]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'assr' from 'c
onsole' on 'con0_0_CPU0'
RP/0/0/CPU0:ios#
RP/0/0/CPU0:ios#
```

9. Presupuesto

Servicio	Precio
Cisco IOS XRv 9000 License	\$10 000,00

Servicio	Costo Mensual	Costo Anual
Web Hosting	\$65	\$780
Amazon RDBS (1TB)	\$17,60	\$211,20

Esto nos genera un gasto fijo de \$ 10 000 por la compra de la licencia del dispositivo Cisco con IOS XRv9000 y anualmente se requeriría un gasto de \$991,20 por servicios prestados de Hosteo del servidor web y de almacenamiento en la plataforma de Amazon Web Services.

10. Conclusiones

- La integración de varios sistemas y protocolos permiten desarrollar aplicaciones que permitirán ofrecer acceso y control a sistemas importantes de una organización de manera sencilla, ya que de otra forma se requeriría un profundo estudio del funcionamiento de cada uno de los componentes y protocolos que estén involucrados en el sistema de una organización.
- Hay que considerar que para el desarrollo de una aplicación web es muy importante asegurar la seguridad de los datos que transitan por el sistema, ya que estos detalles son los que permiten destacarte frente a otros desarrollos que siguen el mismo objetivo que la aplicación desarrollada. A su vez que este sistema debe ser escalable de forma que se encuentre listo y no se presenten dificultades al momento de querer expandir el alcance del sistema, ya sea en capacidad de almacenamiento o de velocidad de procesamiento.

11. Referencias:

- https://www.cisco.com/c/es_mx/support/docs/storage-networking/management/200933-YANG-NETCONF-Configuration-Validation.html
- https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/data-models/guide/b-data-models-config-guide-asr9000/b-data-odels-config-guide-asr9000_chapter_01.html#id_20899
- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-deploy-rsa-pki.html#GUID-44796FDC-72A0-4240-895A-CCA9DB62CAE6
- https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/system_management/command/reference/yr40crs_chapter15.html#wp460865614
- <http://www.paramiko.org/installing.html>
- <https://netconf-client.readthedocs.io/en/latest/quickstart.html>
- <https://github.com/darylturner/node-netconf>
- <https://www.iteramos.com/pregunta/29289/combinando-nodejs-y-python>
- <https://itprice.com/es/cisco-gpl/ios%20xrv%209000>
- <https://tools.ietf.org/html/rfc4741>
- <https://jsonformatter.org/xml-viewer>