



UNIVERSIDAD TECNOLÓGICA DEL NORTE DE GUANAJUATO

Tecnologías de la Información y Comunicación
Programa educativo:

TSU en Infraestructura de Redes Digitales
Área académica:

Programación de Redes
Asignatura:

Unidad III: Programación de Redes

Grupo: GIR0441

Raw NETCONF
Laboratorio 6:

Venado Soria German Emiliano
Alumno:

Gabriel Barrón Rodríguez
Docente:

Dolores Hidalgo, C.I.N., Gto., Miércoles 14 de Diciembre de 2022
Lugar y fecha:

Lab – raw NETCONF

Objectives

Part 1: Verify that NETCONF is Running on the IOS XE

Background / Scenario

In this lab, you will learn how to verify that the NETCONF service is running on the device by directly connecting to its port using an SSH client. You will be sending raw NETCONF Remote Procedure Calls encoded in XML structures.

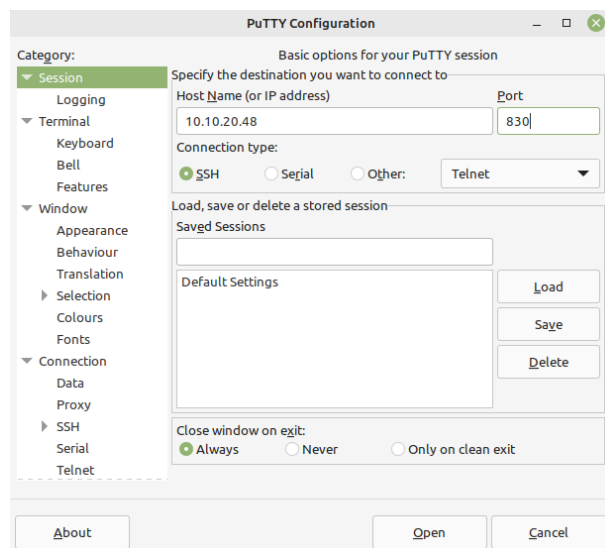
Required Resources

- Access to a router with the IOS XE operating system version 16.6 or higher
- Putty

Part 1: Verify that NETCONF is Running on the IOS XE

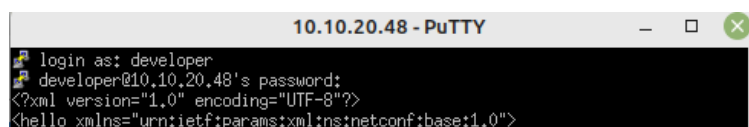
Step 1: Use Putty as an SSH client to connect to the NETCONF service.

- Start Putty.
- Using Putty, connect to host “192.168.56.101” (Adjust the IP address to match the router’s current address.) and port “830”.



En esta práctica nos pide interactuar con Putty, el cual ya hemos venido trabajando desde primer o segundo cuatrimestre, pues consta de una conexión remota, el cual solicita la dirección IP del dispositivo al que queremos acceder, el número de puerto y el protocolo por el cual queremos conectarnos.

- Login as “cisco” with the password “cisco123!” that was configured in IOS XE VM.



Una vez tuvimos acceso al Router nos solicita la autenticación, nos pide un usuario y una contraseña, los cuales vienen en las especificaciones del Router del sandbox que solicitamos.

- d. After a successful login to the NETCONF server, you should see a server “hello” message with an XML formatted list of supported YANG models (capabilities).
- e. The end of the message is identified with “]]>]]>”.
- f. To start a NETCONF session, the client needs to send its own hello message in a response:

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
]]>]]>
```



```
<capability>urn:ietf:params:xml:ns:yang:ietf-netconf-with-defaults?module=ietf-n
etconf-with-defaults&revision=2011-06-01</capability>
<capability>
  urn:ietf:params:netconf:capability:notification:1.1
</capability>
</capabilities>
<session-id>22</session-id></hello>]]>]]>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
]]>]]>
```

Para poder iniciar sesión de NETCONF y posteriormente procesar mensajes RPC, primeramente, debemos enviar nuestro propio mensaje de saludo en respuesta, el cual esta práctica nos orienta a elaborarlo.

- g. After the client hello message has been sent, the NETCONF session is ready to process RPC messages. For example, the following XML formatted RPC message will return the ietf-interfaces model data. Please note that the returned XML data are designed to be consumed by an application. By default, this data might be difficult to for humans to read.

```
<rpc message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces"/>
    </filter>
  </get>
</rpc>
]]>]]>
```

```
<rpc message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces"/>
    </filter>
  </get>
</rpc>
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="103"><data><interfaces xmlns="urn:ietf:
params:xml:ns:yang:ietf-interfaces"><interface><name>GigabitEthernet1</name><description>MANAGEMENT INTERFACE -
DON'T TOUCH ME</description><type xmlns:ianaift="urn:ietf:params:xml:ns:yang:iana-if-type">ianaift:ethernetCsmac
cd</type><enabled>true</enabled><ipv4 xmlns="urn:ietf:params:xml:ns:yang:ietf-ip"><address><ip>10.10.20.48</ip>
<netmask>255.255.255.0</netmask></address></ipv4><ipv6 xmlns="urn:ietf:params:xml:ns:yang:ietf-ip"></ipv6></int
erface><interface><name>GigabitEthernet2</name><description>Network Interface</description><type xmlns:ianaift=
"urn:ietf:params:xml:ns:yang:iana-if-type">ianaift:ethernetCsmacd</type><enabled>false</enabled><ipv4 xmlns="ur
n:ietf:params:xml:ns:yang:ietf-ip"></ipv4><ipv6 xmlns="urn:ietf:params:xml:ns:yang:ietf-ip"></ipv6></interface>
<interface><name>GigabitEthernet3</name><description>Network Interface</description><type xmlns:ianaift="urn:ie
tf:params:xml:ns:yang:iana-if-type">ianaift:ethernetCsmacd</type><enabled>false</enabled><ipv4 xmlns="urn:ietf:
params:xml:ns:yang:ietf-ip"></ipv4><ipv6 xmlns="urn:ietf:params:xml:ns:yang:ietf-ip"></ipv6></interface><interf
ace><name>Loopback99</name><description>Venado-Lab_2.5</description><type xmlns:ianaift="urn:ietf:params:xml:ns
:yang:iana-if-type">ianaift:softwareLoopback</type><enabled>true</enabled><ipv4 xmlns="urn:ietf:params:xml:ns:y
ang:ietf-ip"><address><ip>192.168.20.210</ip><netmask>255.255.255.0</netmask></address></ipv4><ipv6 xmlns="urn:
ietf:params:xml:ns:yang:ietf-ip"></ipv6></interface></interfaces></data></rpc-reply>]]>]]>
```

Se solicita asignar el siguiente mensaje RPC en formato XML, el cual regresará los datos del modelo de interfaces ietf. Pero los datos XML devueltos están diseñados para ser consumidos por una aplicación, y la salida de estos datos pueden ser un poco difíciles de leer.

- h. To close the NETCONF session, the client needs to send the following message:

```
<rpc message-id="99999999" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session />
</rpc>
]]>]]>
```

Finalmente, agregando este pequeño código, podremos finalizar y cerrar la conexión remota.

Investigaciones

- **¿Qué es Putty?**

En general, Putty no es más que una terminal de simulación open source que fue desarrollado para actuar como cliente de conexiones seguras a través de protocolos raw TCP, Telnet, rlogin y portal serial.

Por lo tanto, este software se indica para establecer conexiones seguras de acceso remoto a servidores a través de Shell Seguro (SSH) y para construir canales encriptados entre servidores.

- **¿Qué es NETCONF?**

NETCONF cuyas siglas significan network configuration es un protocolo de administración de red basado en XML que proporciona un método programable para configurar y administrar dispositivos de red, utilizado con modelos de datos YANG. Los mensajes enviados con NETCONF utilizan llamadas a procedimiento remoto (RPC), basado en la comunicación cliente-servidor.

- **¿Qué son los mensajes RPC?**

La llamada a procedimiento remoto es un protocolo de comunicación de software que un programa puede usar para solicitar un servicio de un programa ubicado en otra computadora en una red sin tener que comprender los detalles de la red. RPC se utiliza para llamar a otros procesos en los sistemas remotos como un sistema local.

RPC utiliza el modelo cliente-servidor. El programa solicitante es un cliente y el programa proveedor de servicios es el servidor. Al igual que una llamada a procedimiento local, un RPC es una operación síncrona que requiere que el programa solicitante se suspenda hasta que se devuelvan los resultados del procedimiento remoto. Sin embargo, el uso de procesos ligeros o subprocesos que comparten el mismo espacio de direcciones permite que se realicen múltiples RPC al mismo tiempo.

Conclusiones

Como conclusión puedo decir que esta práctica como algunas de las demás ha sido sencilla, pues nos otorga el proceso y script de configuración que se debe hacer en cada paso. Ya había trabajado con la conexión remota pero no con el formato xml, el cual es indispensable para el protocolo de configuración de red, para poder compartir mensajes RPC.