

UNIVERSIDAD TECNOLÓGICA
DEL NORTE DE GUANAJUATO



Área de TSU Infraestructura de Redes

Grupo:

GIR0441

Materia:

Programación de redes

Unidad:

III programación de redes

Actividad:

2.6 Raw NETCONF

Profesor:

Ing. Gabriel Barrón

No. Control:

1221100727

Alumna:

Sandra Dania Gonzalez Manzano

Lugar y Fecha:

Dolores Hidalgo C.I.N a diciembre del 2022

Investigación

Como en cada uno del laboratorio iniciaremos a conectarnos a la VPN con ayuda de la Sandbox.

Posterior iniciare la practica con saber que es NETCONF y para que sirve, este es un protocolo de la capa de aplicación, capa 7 (según modelo OSI) que debe trabajar sobre una capa de transporte que tiene que cumplir ciertos requisitos. NETCONF delega el transporte y la seguridad a las capas inferiores. También es un protocolo basado en Lenguaje de marcado extensible XML que las aplicaciones cliente utilizan para administrar la configuración en enrutamiento, conmutación y dispositivos de seguridad.

Proporcionados mecanismos para instalar, manipular y eliminar la configuración de dispositivos de red. Además de dar estándares a través de los cuales los administradores de red y los desarrolladores de aplicaciones pueden administrar configuraciones de dispositivos de red y obtener el estado del dispositivo de red rápidamente.

Practica

1.Lo primero que realice fue la reservación como lo realizamos en los otros laboratorios en sandbox, utilizando la sandbox 16.11.



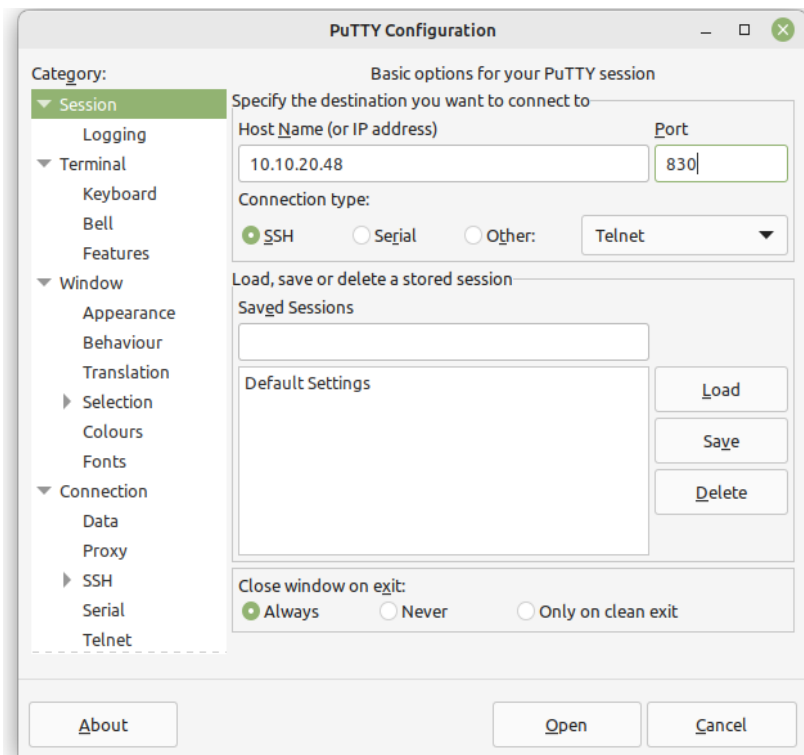
2.Lo siguiente que realice fue la conexión VPN con el usuario y contraseña otorgados por la reservación de sandbox cisco.



En el paso 3 inicia la practica donde solo existe un parte

3.1 Este laboratorio se realizará la practica en putty donde en otro de los laboratorio realizaba una explicación clara y concisa de lo que es este simulador. Por medio de conexión SSH

Donde usando la dirección 10.10.20.48 en el puerto 830, donde inicie sesión como cisco con la contraseña cisco123!



Después de iniciar sesión correctamente en el servidor NETCONF, debería ver un mensaje de "hola" del servidor con una lista con formato XML de modelos YANG compatibles (capacidades).

El final del mensaje se identifica con "]]>]]>".

Para iniciar una sesión de NETCONF, el cliente debe enviar su propio mensaje de saludo en una respuesta

```

10.10.20.48 - PuTTY
&revision=1994-10-23</capability>
<capability>urn:ietf:params:xml:ns:yang:smiv2:TUNNEL-MIB&revision=2005-05-16</capability>
<capability>urn:ietf:params:xml:ns:yang:smiv2:UDP-MIB&revision=2005-05-20</capability>
<capability>urn:ietf:params:xml:ns:yang:smiv2:VPN-TC-STD-MIB&revision=2005-11-15</capability>
<capability>urn:ietf:params:xml:ns:netconf:base:1.0?module=ietf-netconf&revision=2011-06-01</capability>
<capability>urn:ietf:params:xml:ns:yang:ietf-netconf-with-defaults?module=ietf-netconf-with-defaults&revision=2011-06-01</capability>
<capability>urn:ietf:params:netconf:capability:notification:1.1</capability>
</capabilities>
<session-id>23</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>
]]>]]>

```

Una vez enviado el mensaje hola del cliente, la sesión de NETCONF está lista para procesar los mensajes RPC. Por ejemplo, el siguiente mensaje RPC con formato XML devolverá los datos del modelo ietf-interfaces. Tenga en cuenta que los datos XML devueltos

están diseñados para ser consumidos por una aplicación. De forma predeterminada, estos datos pueden ser difíciles de leer para los humanos.

Para cerrar la sesión de NETCONF, el cliente debe enviar el siguiente mensaje:

```
<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>GigabitEthernet0/0</name><description>MANAGEMENT INTERFACE - DON'T TOUCH ME</description><type xmlns:ianaif="urn:ietf:params:xml:ns:yang:iana-if-type">ianaif:ethernetCsmacd</type><enabled>true</enabled><ietf-ip xmlns="urn:ietf:params:xml:ns:yang:ietf-ip"><address><ip>10.10.20.48</ip><netmask>255.255.255.0</netmask></address></ietf-ip></interface><interface><name>GigabitEthernet2</name><description>Network Interface</description><type xmlns:ianaif="urn:ietf:params:xml:ns:yang:iana-if-type">ianaif:ethernetCsmacd</type><enabled>false</enabled><ietf-ip xmlns="urn:ietf:params:xml:ns:yang:ietf-ip"><address><ip>1.1.1.1</ip><netmask>255.255.255.0</netmask></address></ietf-ip></interface><interface><name>Loopback0</name><description>Laboratorio 2.5 prueba</description><type xmlns:ianaif="urn:ietf:params:xml:ns:yang:iana-if-type">ianaif:softwareLoopback</type><enabled>true</enabled><ietf-ip xmlns="urn:ietf:params:xml:ns:yang:ietf-ip"><address><ip>99.99.99.99</ip><netmask>255.255.255.0</netmask></address></ietf-ip></interface></interfaces></data></rpc-reply>]]>]]
```

Conclusiones

Finalmente, esta práctica me sirvió conocer acerca de Netconf se esta ajustando en el dispositivo conectandose directamente a su puerto mediante un cliente SSH. Realizando la practica por medio de PUTTY