

Lab – raw NETCONF

Nombre:	Montserrat Orduña Basaldua
Num Control:	1222100895

Objectives

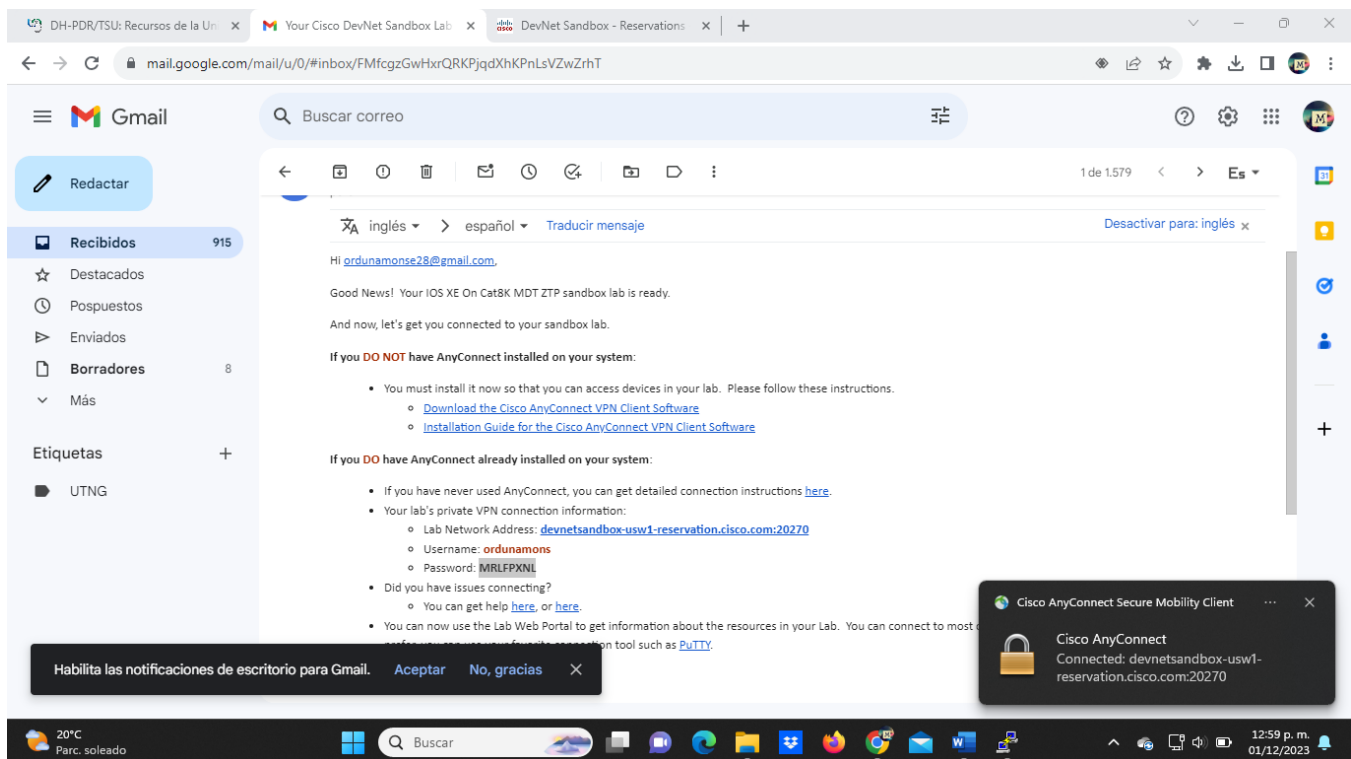
Part 1: Verify that NETCONF is Running on the IOS XE

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



The screenshot shows a Gmail interface with an email from 'Your Cisco DevNet Sandbox Lab'. The email content includes:

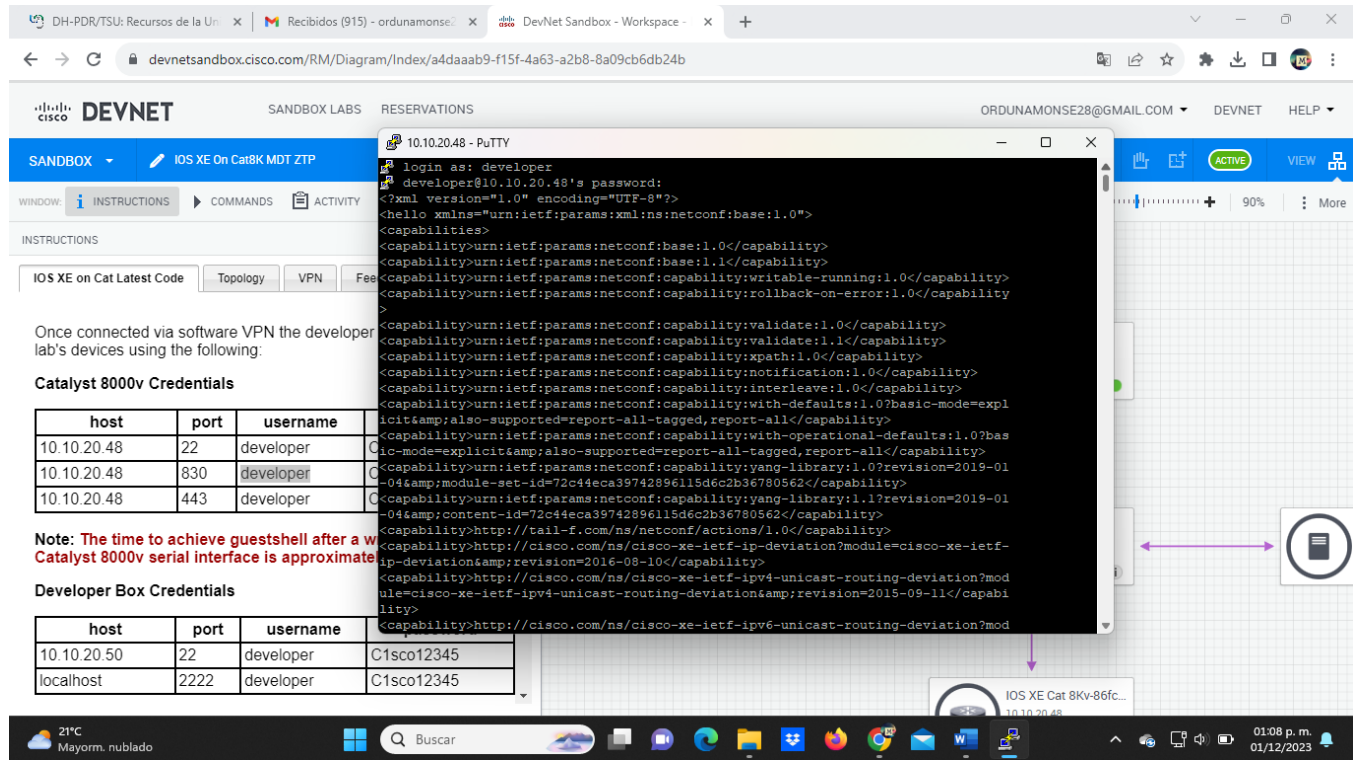
- Greeting: Hi ordunamonse28@gmail.com.
- Good News! Your IOS XE On Cat8K MDT ZTP sandbox lab is ready.
- And now, let's get you connected to your sandbox lab.
- If you DO NOT have AnyConnect installed on your system:**
 - You must install it now so that you can access devices in your lab. Please follow these instructions.
 - [Download the Cisco AnyConnect VPN Client Software](#)
 - [Installation Guide for the Cisco AnyConnect VPN Client Software](#)
- If you DO have AnyConnect already installed on your system:**
 - If you have never used AnyConnect, you can get detailed connection instructions [here](#).
 - Your lab's private VPN connection information:
 - Lab Network Address: devnetsandbox-usw1-reservation.cisco.com:20270
 - Username: **ordunamons**
 - Password: **MRLFPXNL**
 - Did you have issues connecting?
 - You can get help [here](#), or [here](#).
 - You can now use the Lab Web Portal to get information about the resources in your Lab. You can connect to most of the resources using a network management tool such as [PuTTY](#).

At the bottom of the screen, there is a Windows taskbar showing the time as 12:59 p.m. on 01/12/2023. A Cisco AnyConnect Secure Mobility Client notification is visible, stating 'Connected: devnetsandbox-usw1-reservation.cisco.com:20270'.

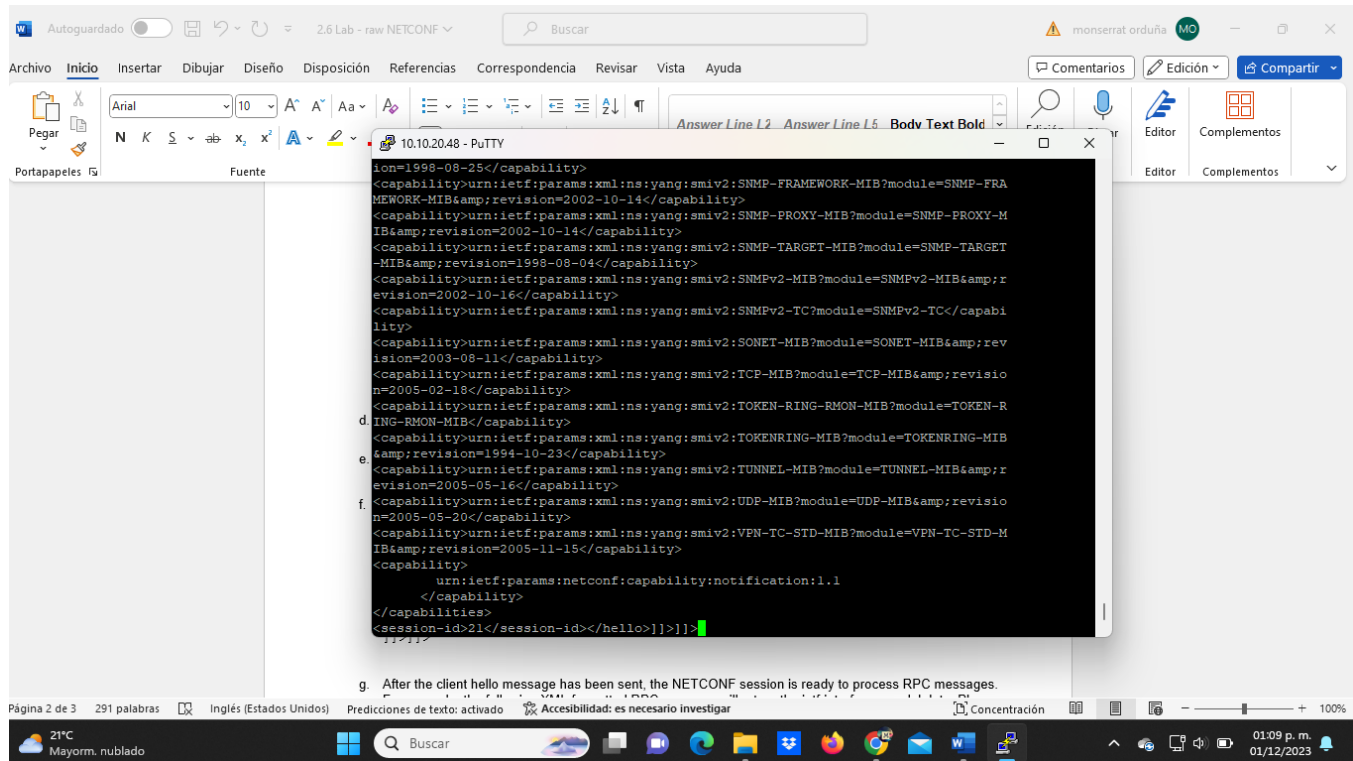
Part 1: Verify that NETCONF is Running on the IOS XE

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



- 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>
]]>]]>
```

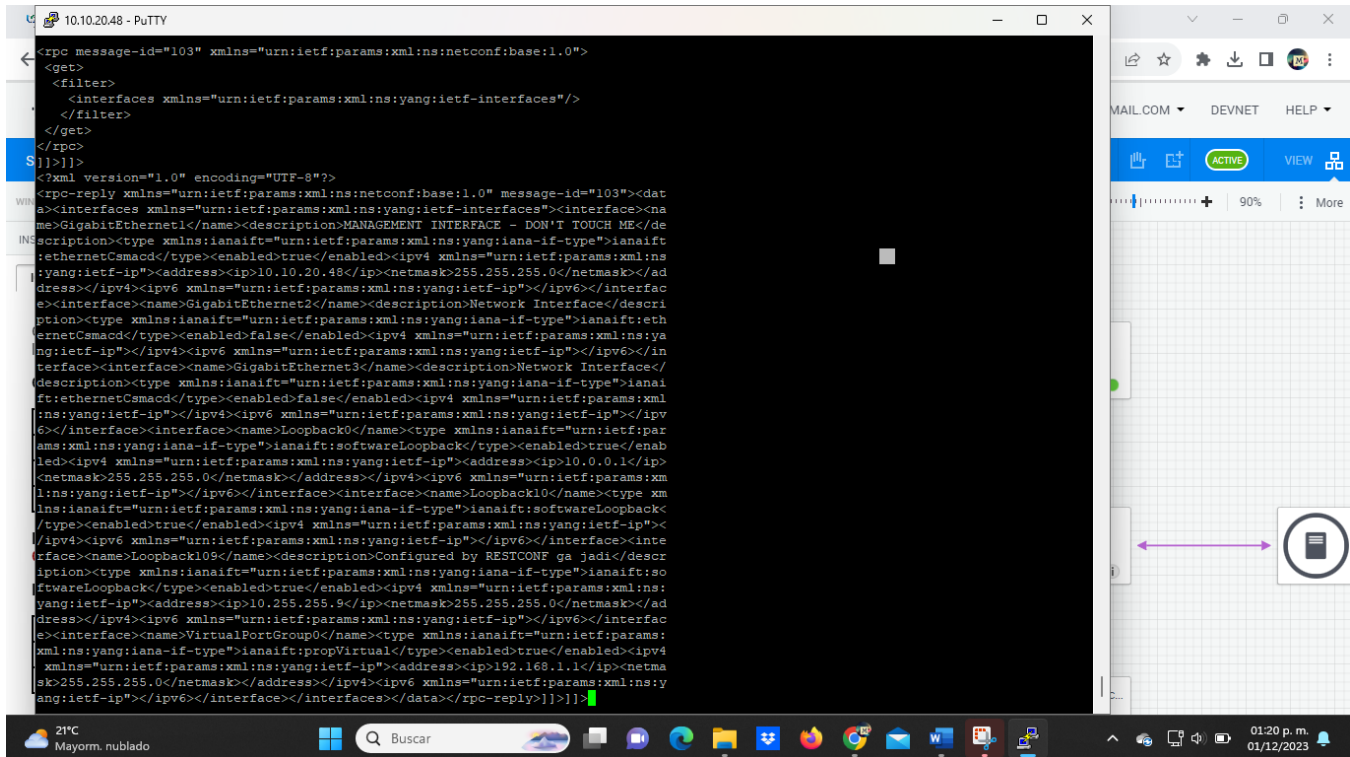
The screenshot shows the DevNet Sandbox interface. A PuTTY terminal window is open, displaying NETCONF XML data. Below the terminal, there is a table of Catalyst 8000v credentials.

host	port	username	password
10.10.20.48	22	developer	C1sco12345
10.10.20.48	830	developer	C1sco12345
10.10.20.48	443	developer	C1sco12345

Note: The time to achieve guestshell after a wr mem/reload Catalyst 8000v serial interface is approximately 6 minutes.

- 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 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>
]]>]]>
```



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

```
<rpc message-id="9999999" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session />
</rpc>
]]>]]>
```