# Laboratory Worksheet -3

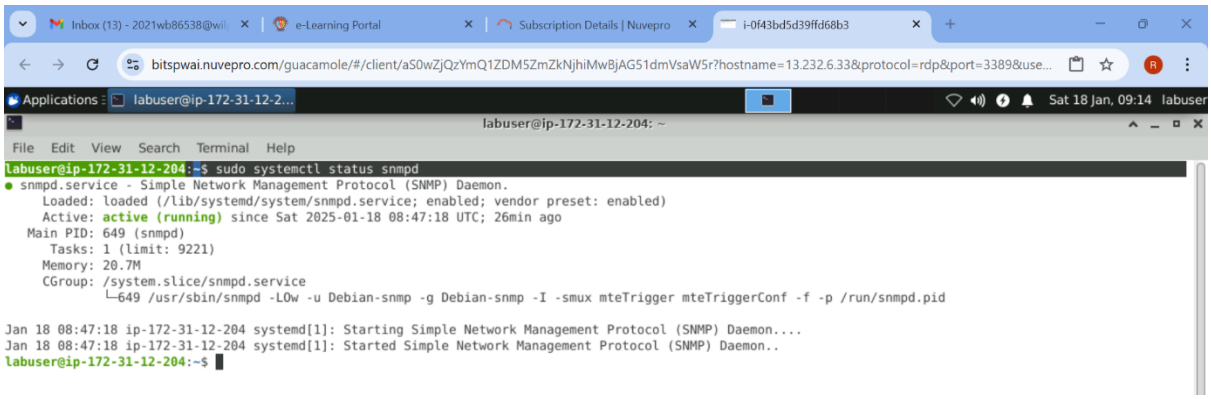
## 4. Lab Exercise:

**Problem Statement:**

Open the linux terminal and execute the following basic networking tools and utilities. Make your observations and record the output of each command.

**Steps to be followed: Open the terminal in Linux and execute the following commands:**

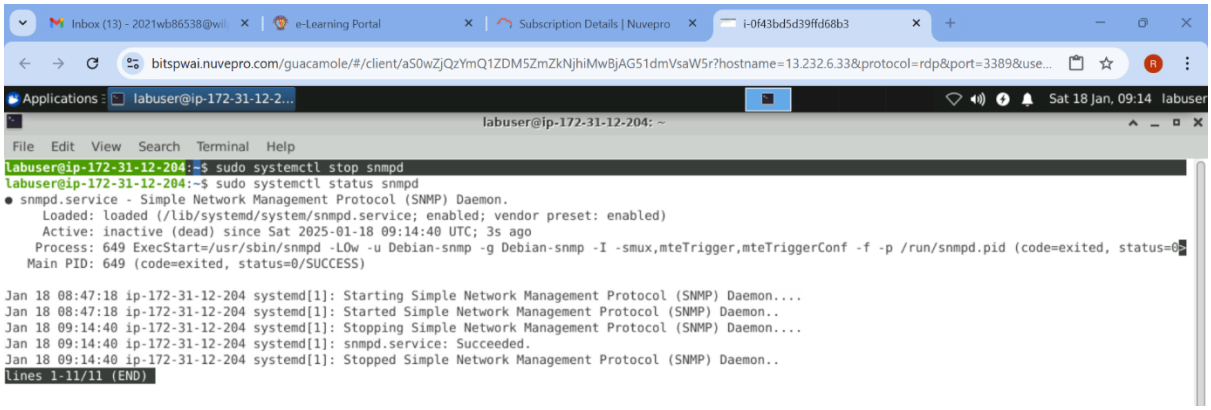
- Verify that snmp daemon status run the below command and record the output of each command.
    - `sudo systemctl status snmpd`




**Observation:**

This command checks whether the SNMP daemon (snmpd) is active. If it is running, the output shows a green "active (running)" status. If not, it displays "inactive" or "dead."

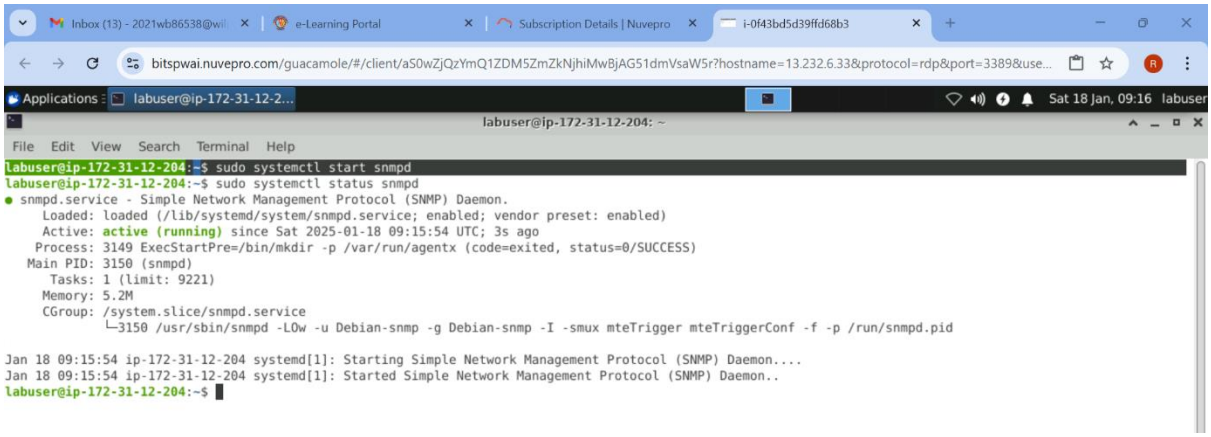
- **sudo systemctl stop snmpd**




**Observation:**

This stops the SNMP service. Running status snmpd afterward confirms the service has stopped, with the output showing "inactive" or "dead."

- **sudo systemctl start snmpd**




**Observation:**

After executing start command, as the system is re-initating daemon services,running sudo systemctl status snmpd should show that the daemon is active and running.

(Make sure that SNMP services are running always)

**Note: Write your comments on observation of each command output**

- Update SNMP Configuration
    - **`sudo vi /etc/snmp/snmpd.conf`**


**Modify the "*`agentaddress`*" to your machine in the config file**

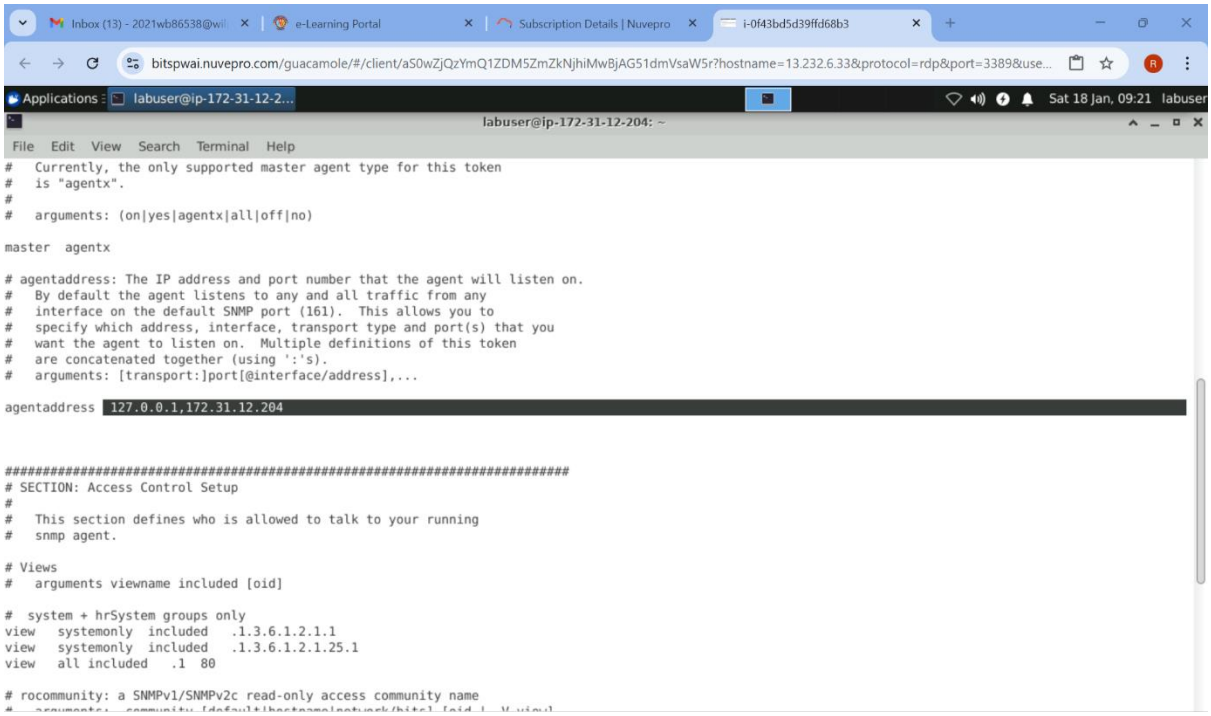
```
# agentaddress: The IP address and port number that the agent will listen on.
#   By default the agent listens to any and all traffic from any
#   interface on the default SNMP port (161).  This allows you to
#   specify which address, interface, transport type and port(s) that you
#   want the agent to listen on.  Multiple definitions of this token
#   are concatenated together (using ':'s).
#   arguments: [transport:]port[@interface/address],...

agentaddress  127.0.0.1,[::1]
```

**Make sure to have both <loopback IP address> and <Your_machine_IP_Address> in the configuration file as shown below**

```
# agentaddress: The IP address and port number that the agent will listen on.
#   By default the agent listens to any and all traffic from any
#   interface on the default SNMP port (161).  This allows you to
#   specify which address, interface, transport type and port(s) that you
#   want the agent to listen on.  Multiple definitions of this token
#   are concatenated together (using ':'s).
#   arguments: [transport:]port[@interface/address],...

agentaddress  127.0.0.1,172.31.20.139
```

- **Earlier:** agentaddress 127.0.0.1, [::1]
- We have changed the agentaddress line with our system IP address.

  127.0.0.1,172.31.12.204

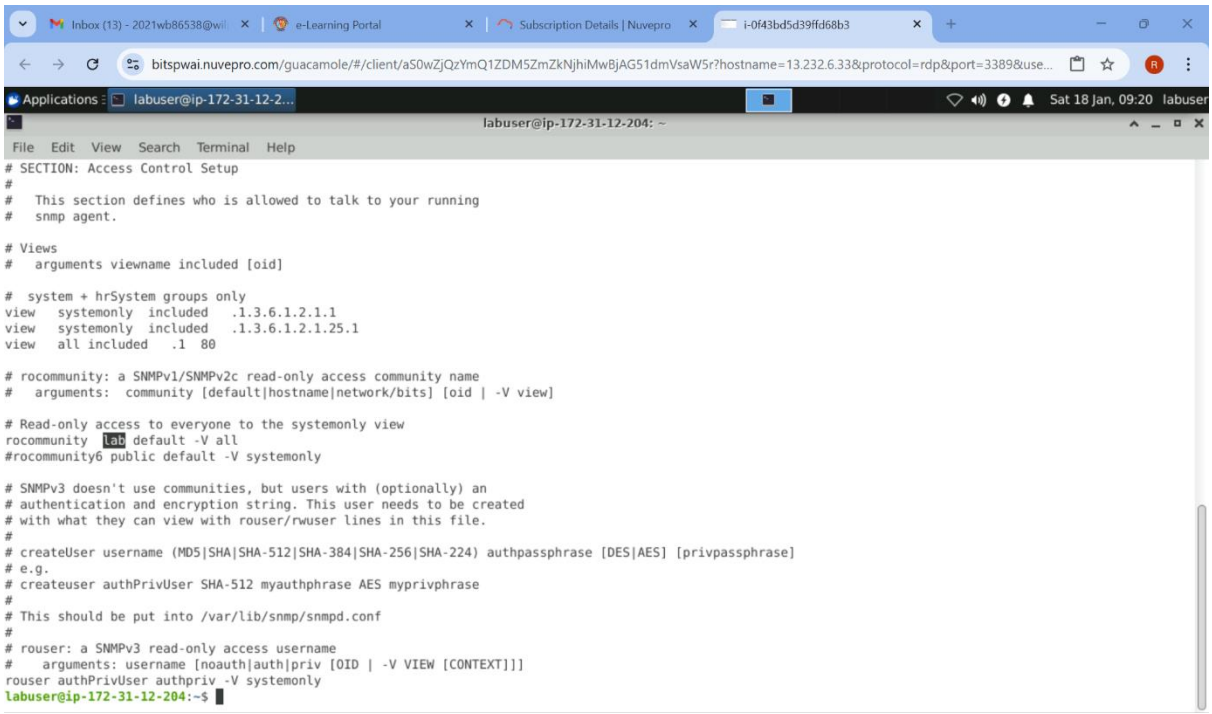



**Modify SNMP community name to your desired community name (replace public) name and comment IPv6 Community**

```
# rocommunity: a SNMPv1/SNMPv2c read-only access community name
#   arguments:  community [default|hostname|network/bits] [oid | -V view]

# Read-only access to everyone to the systemonly view
rocommunity  public default -V systemonly
rocommunity6 public default -V systemonly

# SNMPv3 doesn't use communities, but users with (optionally) an
```

**In the below *system* is the SNMP community name (You can use any community name)**

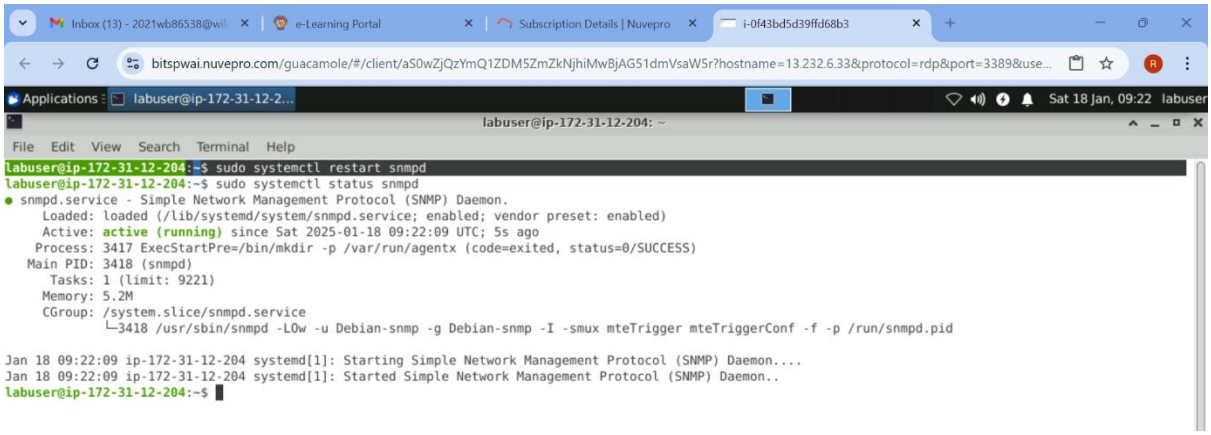
```
# rocommunity: a SNMPv1/SNMPv2c read-only access community name
#   arguments:  community [default|hostname|network/bits] [oid | -V v

# Read-only access to everyone to the systemonly view
rocommunity  system  default -V systemonly
#rocommunity6 public default -V systemonly

# SNMPv3 doesn't use communities, but users with (optionally) an
# authentication and encryption string. This user needs to be created
# with what they can view with rouser/rwuser lines in this file.
```



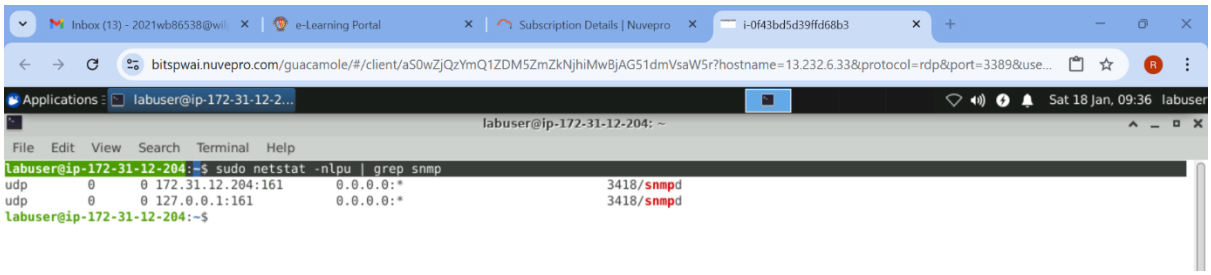

- Update the SNMP community name by replacing public with lab and comment out IPv6 configurations by adding a # at the beginning of the relevant lines.
- We have changed the name to lab and also commented the IPv6 configuration line.

- **On modifying SNMP config file, you need to Restart the SNMP Services with the commands used in beginning.**

  Restarted the SNMP services and now it's up and running.



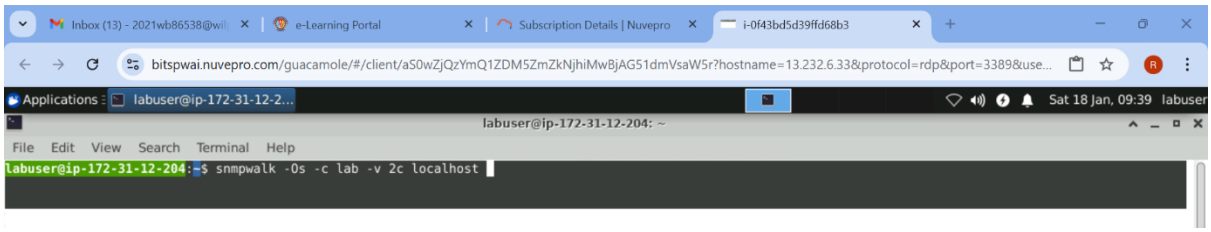

1. **Run the below command and record the output and also explain the usage of the command.**
   - `sudo netstat -nlpu | grep snmp`

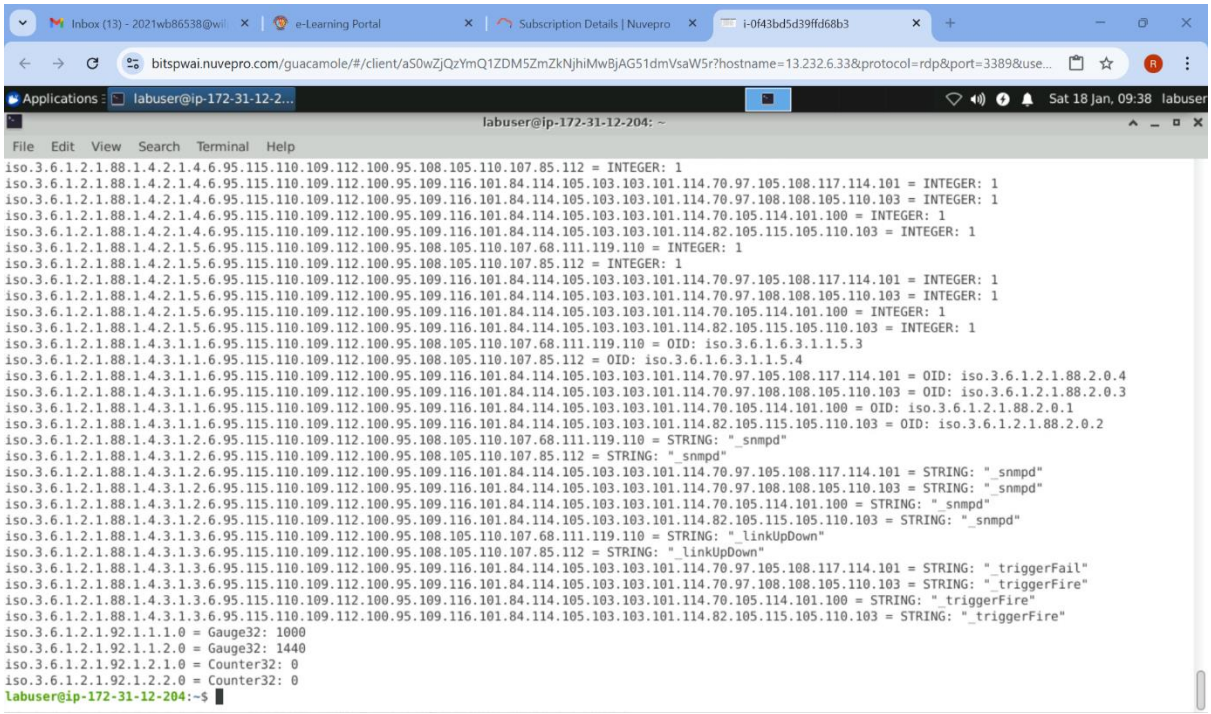



**Observation:**

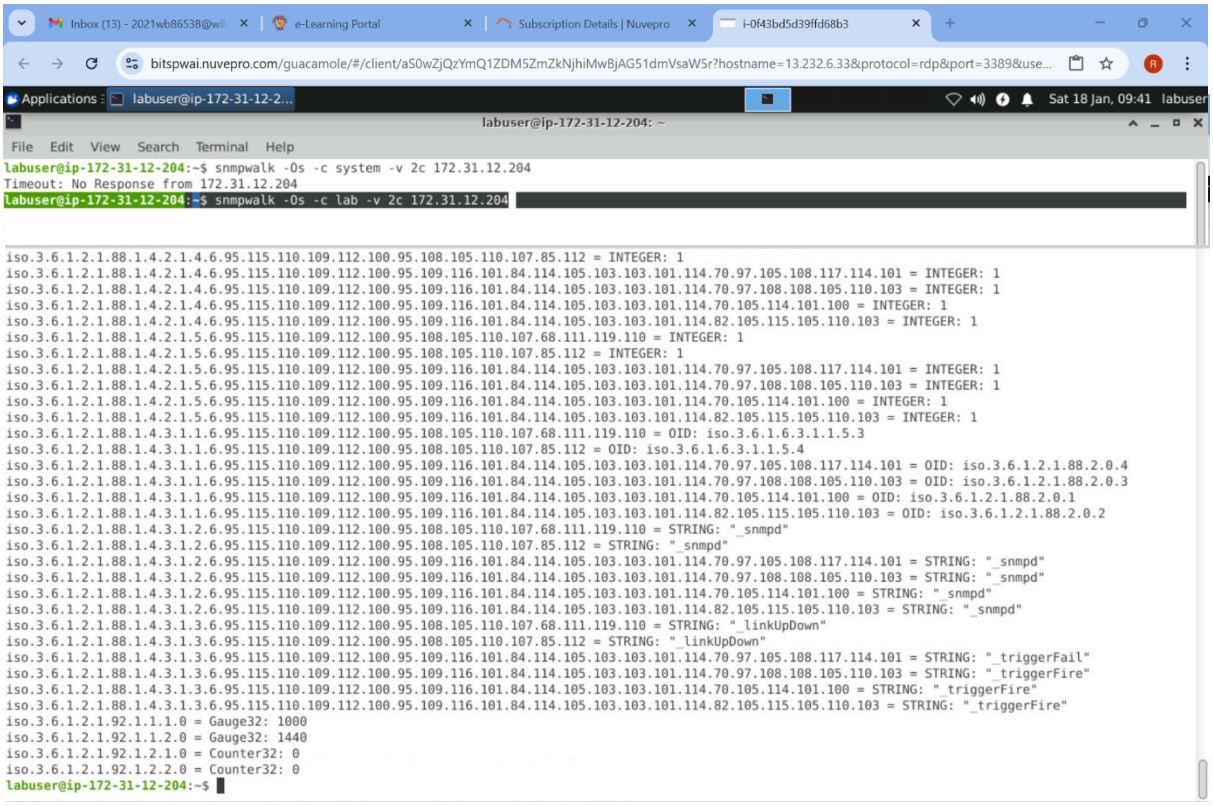
This command displays all listening UDP ports and filters for SNMP. The output includes the SNMP service's bound addresses (127.0.0.1:161 & 172.31.12.204:161), indicating it is listening on the configured addresses.

2. **Explore the usage of `snmpwalk` command**
   - **`snmpwalk -Os -c lab -v 2c localhost`**



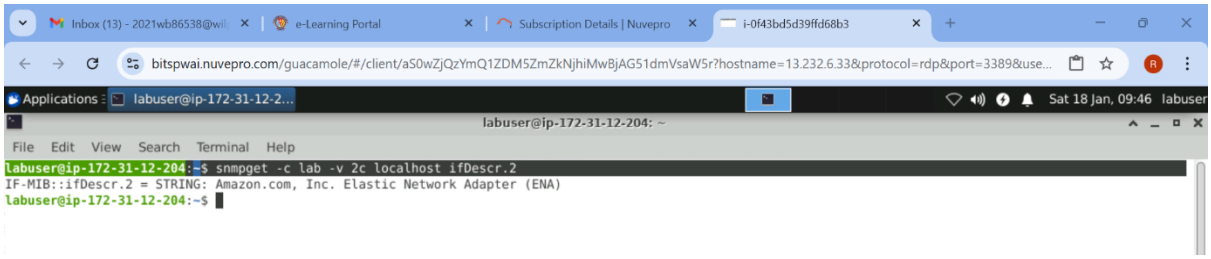



- **snmpwalk -Os -c lab -v 2c 172.31.12.204**



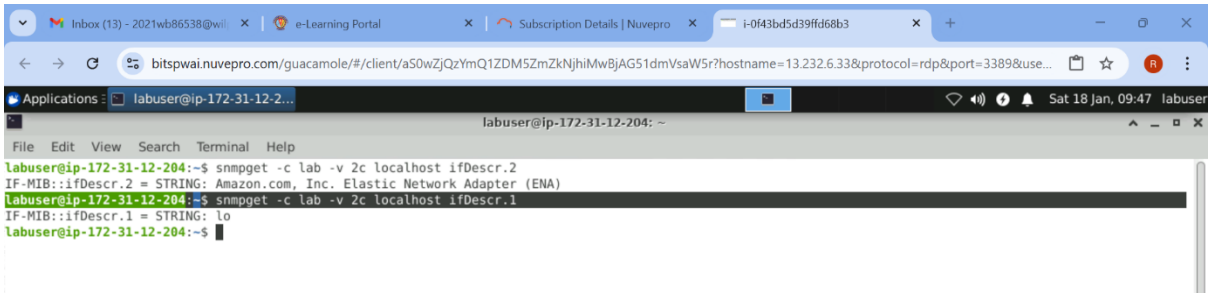

**Observation:**
The snmpwalk command retrieves a tree of SNMP objects. Using localhost fetches data for the local machine. The 172.31.12.204 query ensures SNMP is accessible via the configured IP.

3. **Run the below snmpget command to get the OID's of the following from your machine/snmp agent and record the output**
   - **OID of Ethernet interface (ens5)**
   - snmpget -c lab -v 2c localhost ifDescr.2



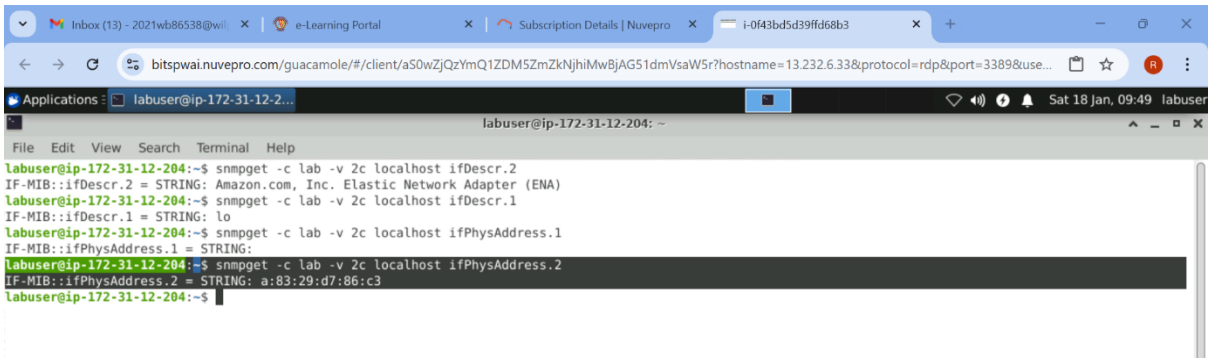

**Observation:** Retrieves the OID of the Ethernet interface.

- **OID of Loopback interface(lo)**
- `snmpget -c lab -v 2c localhost ifDescr.1`



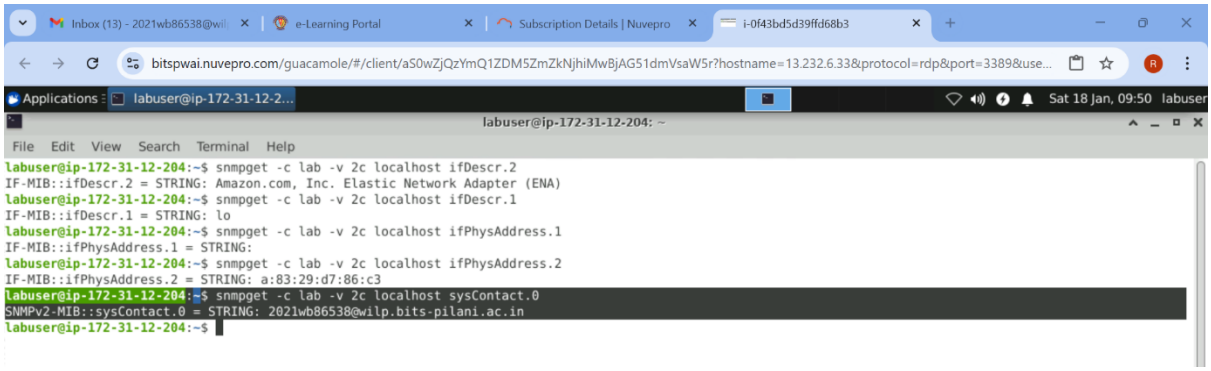

**Observation:** Retrieves the OID for the loopback interface.

- **OID of MAC Address**
- `snmpget -c lab -v 2c localhost ifPhysAddress.1`
- `snmpget -c lab -v 2c localhost ifPhysAddress.2`



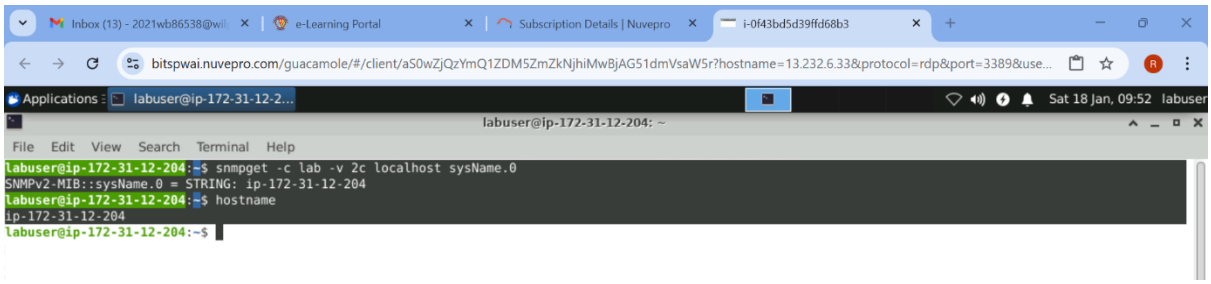

**Observation:** Displays the MAC address for the specified interface.

- **OID of sysContact**
- `snmpget -c lab -v 2c localhost sysContact.0`

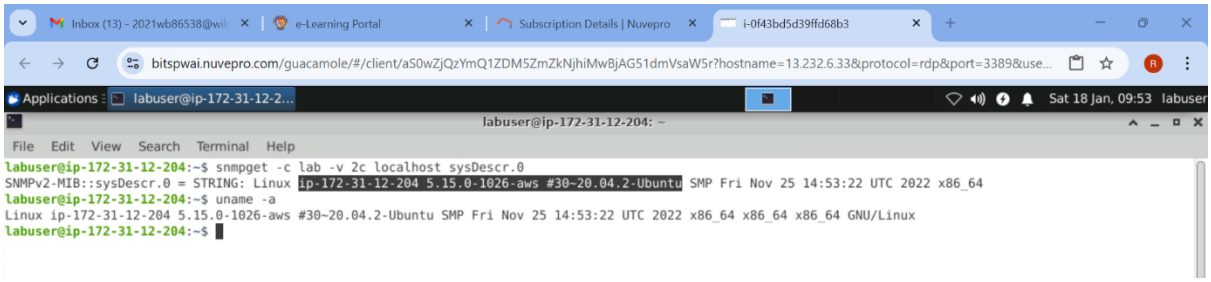


**Observation:** Displays the contact information configured in the SNMP settings.

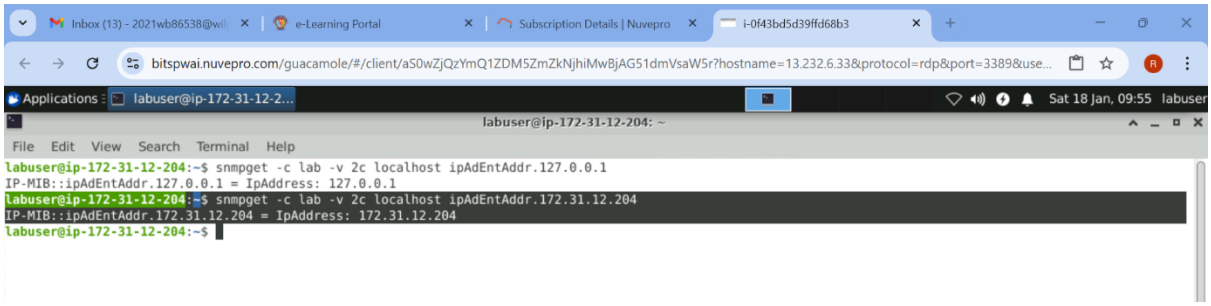
4. **Get the following system Information with the help of snmpget command**
   - **Host Name**
     - snmpget -c lab -v 2c localhost sysName.0
     - **Equivalent:** hostname




   - **Hostname with kernel version**
     - snmpget -c lab -v 2c localhost sysDescr.0
     - **Equivalent:** uname -a




   - **IP Address of the Host**
     - snmpget -c lab -v 2c localhost ipAdEntAddr.127.0.0.1
     - snmpget -c lab -v 2c localhost ipAdEntAddr.172.31.12.204
     - **Equivalent:** hostname -i




**(Note: Verify the ouput of each snmpget command with equivalent Linux command)**

# Thank you !