PES UNIVERSITY

Department of Computer Science and Engineering

Advanced Computer Networks

UE16CS346

Lab Assignment 4

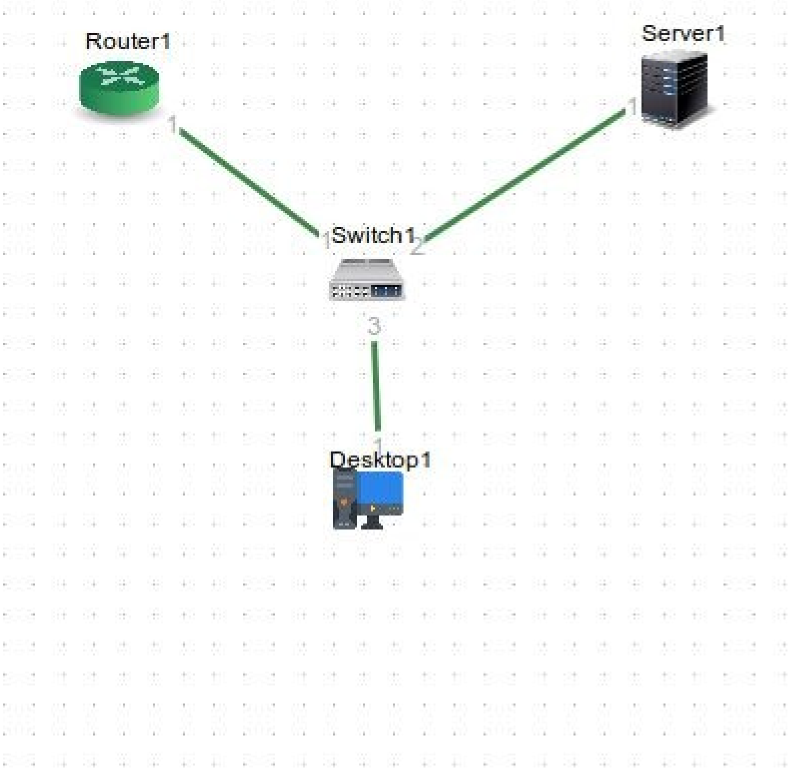
Dweepa Prasad	01FB16ECS138
Ishita Bhandari	01FB16ECS143
Shashank Prabhakar	01FB16ECS356
Shrey Tiwari	01FB16ECS368

Problem Statement

Connect an end system (host) to a server and fetch a webpage. Connect the host and the server using two routers. Display the results.

Procedure

1. Create topology as shown below. Ensure that the correct IP addresses are specified
at the port of the router. Make sure that the systems are chosen are Ubuntu 16.04. Save and deploy topology.
Add the ip addresses for the server and the snmp-managing entity.



2. Configure the router to enable snmp-agent. To configure according to the required version

1. Right click on the routers and select console access.
2. To login, use “test” as the login and “test@12345” as the password.
3. Change from operational mode to configure mode by entering “configure”
4. Enter the following commands (For version 2c) :

```
> modify parameter-group router data
> set enable yes
> add allowed-versions snmp-version-2c
> save
> show snmp summary (To verify if SNMP is enabled)
> create parameter-group snmp-context
> set name data configure
> set instance data
> save
```

<u>To create the snmp-community:</u>

```
> create parameter-group snmp-community public
> set enable yes
> set password public
> set context data
> add access v2c
> enter access v2c
> set access-control-group acg-1
> save
```

To create the snmp-user Parameter group for snmp v3

```
> create parameter-group snmp-user snmp-lab-user
> show draft -e
> set enable yes
> set authentication-protocol md5
> set authentication-password snmp
> set authentication-password snmp@12345
> set privacy-protocol des
> set privacy-password des@12345
> set access-control-group acg-1
> save
> show draft -e
```

Create the snmp-access-control-group Parameter Group with name acg-1

```
> create parameter-group snmp-access-control-group acg-1
> set enable yes
> add context data
> enter context data
> set security sec-1> save
```

Create the snmp-security-group Parameter Group

```
> create parameter-group snmp-security-group sec-1
> add security v2c
> enter security v2c
> add views no-authentication
> enter views no-authentication
> set read-view ace-1
> set write-view ace-1
> leave
> leave
> add security usm
> enter security usm
> add views authentication-privacy
> enter views authentication-privacy
> set read-view ace-1
> set write-view ace-1
> set write-view ace-1
> save
> show draft -e
```

Create the snmp-access-control-entry

```
> create parameter-group snmp-access-control-entry
> add mib-subtree .1
> save
```

3. SNMP configuration Ubuntu Server:

1. Edit file /etc/snmp/snmpd.conf
2. Add the following lines to the file

```
agentAddress udp:192.168.1.3:161
view systemonlyincluded .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1
rocommunity public default -V systemonly
rocommunity6 public default -V systemonly
rouser authOnlyUser
```

3. Save the file and restart the SNMP service.

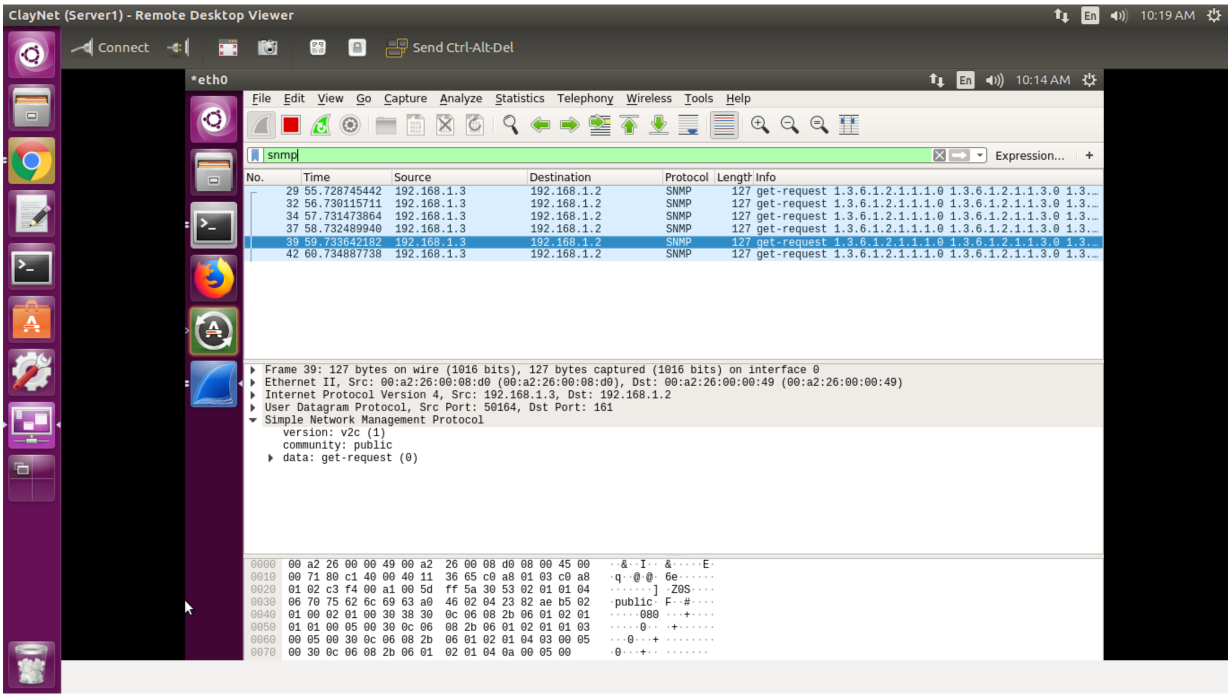
Observation and Output:

> snmpstatus -c public -v 2c 192.168.1.3

The output shows the status of the server.

> snmpget -v 2c -c public 192.168.1.3 sysName.0

> snmpwalk -v 2c -c public 192.168.1.2 .1 SNMPv2

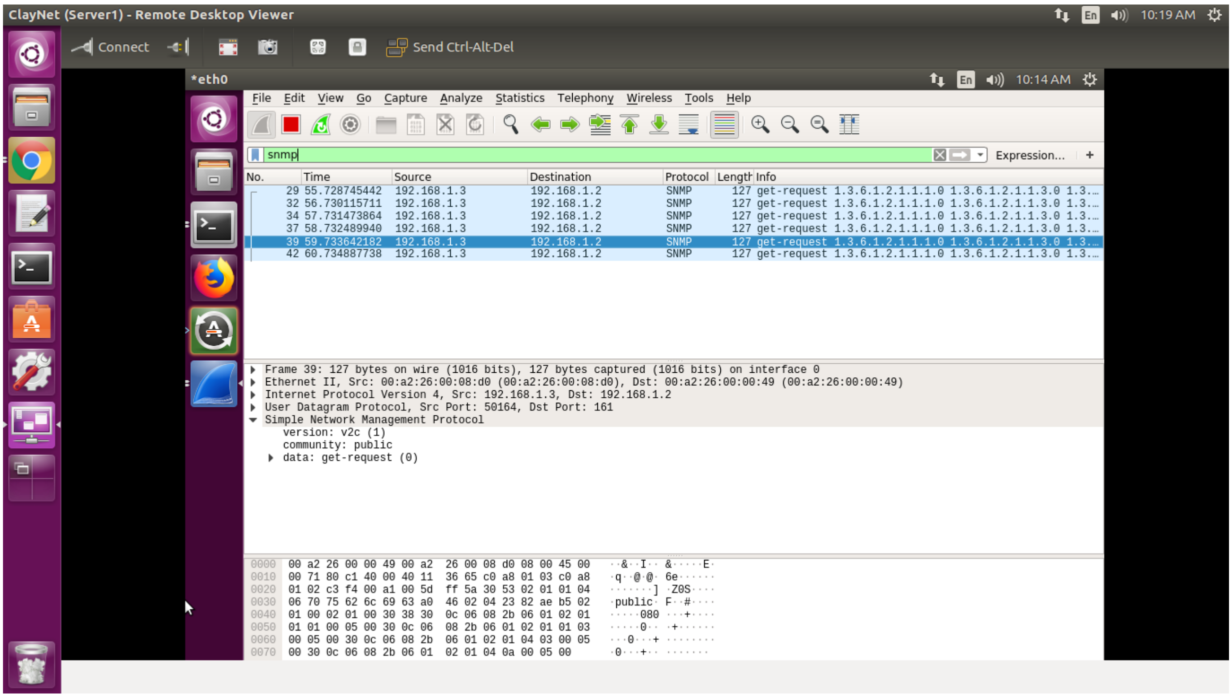

ClayNet (Server1) - Remote Desktop Viewer
Connect
Send Ctrl-Alt-Del
10:19 AM
*eth0
10:14 AM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
snmp

No.  Time          Source        Destination   Protocol Length Info
  29 55.728745442  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3…
  32 56.730115711  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3…
  34 57.731473864  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3…
  37 58.732489940  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3…
  39 59.733642182  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3…
  42 60.734887738  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3…

▶ Frame 39: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
▶ Ethernet II, Src: 00:a2:26:00:08:d0 (00:a2:26:00:08:d0), Dst: 00:a2:26:00:00:49 (00:a2:26:00:00:49)
▶ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.2
▶ User Datagram Protocol, Src Port: 50164, Dst Port: 161
▼ Simple Network Management Protocol
    version: v2c (1)
    community: public
  ▶ data: get-request (0)

0000  00 a2 26 00 00 49 00 a2  26 00 08 d0 08 00 45 00   ··&··I·· &·····E·
0010  00 71 80 c1 40 00 40 11  36 65 c0 a8 01 03 c0 a8   ·q··@·@· 6e······
0020  01 02 c3 f4 00 a1 00 5d  ff 5a 30 53 02 01 01 04   ·······] ·Z0S····
0030  06 70 75 62 6c 69 63 a0  46 02 04 23 82 ae b5 02   ·public· F··#····
0040  01 00 02 01 00 30 38 30  0c 06 08 2b 06 01 02 01   ·····080 ···+····
0050  01 01 00 05 00 30 0c 06  08 2b 06 01 02 01 01 03   ·····0·· ·+······
0060  00 05 00 30 0c 06 08 2b  06 01 02 01 04 03 00 05   ···0···+ ········
0070  00 30 0c 06 08 2b 06 01  02 01 04 0a 00 05 00      ·0···+·· ·······
```

-As we know that SNMPv2 has encryption, this can be observed from the packet captured in wireshark. All the packet data is cleartext since SNMPv2 provides no encryption making it less secure.> snmpwalk -v 3 -l authPriv -n data -u snmp-lab-user -a MD5 -A

snmp@12345 -x DES -X des@12345 192.168.1.2 .1

From the command it can be observed that the user needs to authenticate in order to iterate through the MIBs, and the data received is encrypted as was expected from SNMPv3.


ClayNet (Server1) - Remote Desktop Viewer
Connect
Send Ctrl-Alt-Del
10:19 AM
*eth0
10:14 AM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

snmp

```
No.   Time          Source        Destination   Protocol Length Info
   29 55.728745442  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3...
   32 56.730115711  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3...
   34 57.731473864  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3...
   37 58.732489940  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3...
   39 59.733642182  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3...
   42 60.734887738  192.168.1.3   192.168.1.2   SNMP     127 get-request 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.3.0 1.3...
```

```
▸ Frame 39: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
▸ Ethernet II, Src: 00:a2:26:00:08:d0 (00:a2:26:00:08:d0), Dst: 00:a2:26:00:00:49 (00:a2:26:00:00:49)
▸ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.2
▸ User Datagram Protocol, Src Port: 50164, Dst Port: 161
▾ Simple Network Management Protocol
     version: v2c (1)
     community: public
   ▸ data: get-request (0)
```

```
0000  00 a2 26 00 00 49 00 a2  26 00 08 d0 08 00 45 00   ··&··I·· &·····E·
0010  00 71 80 c1 40 00 40 11  36 65 c0 a8 01 03 c0 a8   ·q··@·@· 6e······
0020  01 02 c3 f4 00 a1 00 5d  ff 5a 30 53 02 01 01 04   ·······] ·Z0S····
0030  06 70 75 62 6c 69 63 a0  46 02 04 23 82 ae b5 02   ·public· F··#····
0040  01 00 02 01 00 30 38 30  0c 06 08 2b 06 01 02 01   ·····080 ···+····
0050  01 01 00 05 00 30 0c 06  08 2b 06 01 02 01 01 03   ·····0·· ·+······
0060  00 05 00 30 0c 06 08 2b  06 01 02 01 04 03 00 05   ···0···+ ········
0070  00 30 0c 06 08 2b 06 01  02 01 04 0a 00 05 00      ·0···+·· ·······
```

From this experiment we observe that:

1. The device UIDs are set in the configuration files providing every device its own identity for the managing entity to contact.

2. Both SNMPv2 and SNMPv3 packets travel over the Transport layer using UDP, for faster access times and reduced network traffic.

3. SNMPv3 requires authentication for both get and set requests and returns encrypted data making it more secure.

4. SNMPv2 returns cleartext data and requires no authentication.

5. The various MIBs can be altered to change the device status in both versions, showing what really goes on at the heart of network management.