Name: Repani, Justin Jello J.	**Date Performed: August 17, 2023**
Course/Section: CPE31S6	**Date Submitted: August 17, 2023**
Instructor: Dr. Jonathan V, Taylar	**Semester and SY: 1st, SY 2023-2023**

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

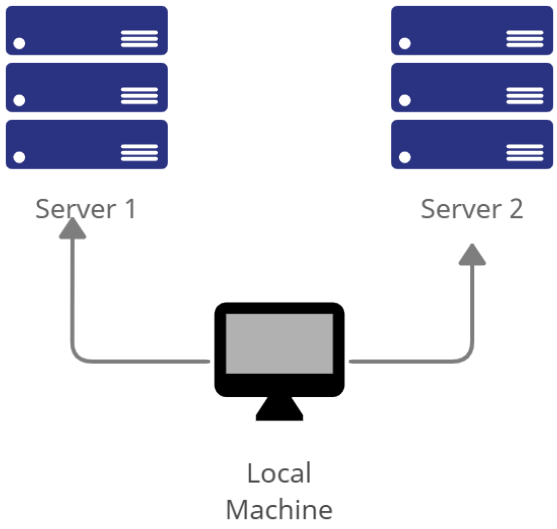
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

1.2. Set-up a Virtual Network and Test Connectivity of VMs

2. **Discussion:**

Network Topology:

Assume that you have created the following network topology in Virtual Machines, *provide screenshots for each task*. (Note: *it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine*).

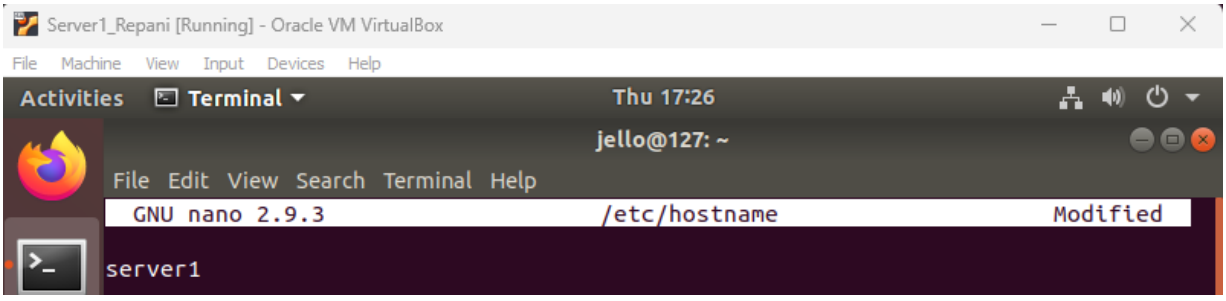


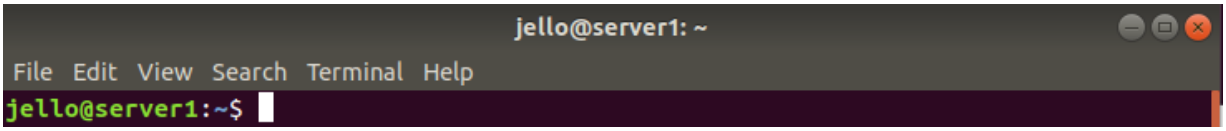
Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

1. Change the hostname using the command *sudo nano /etc/hostname*

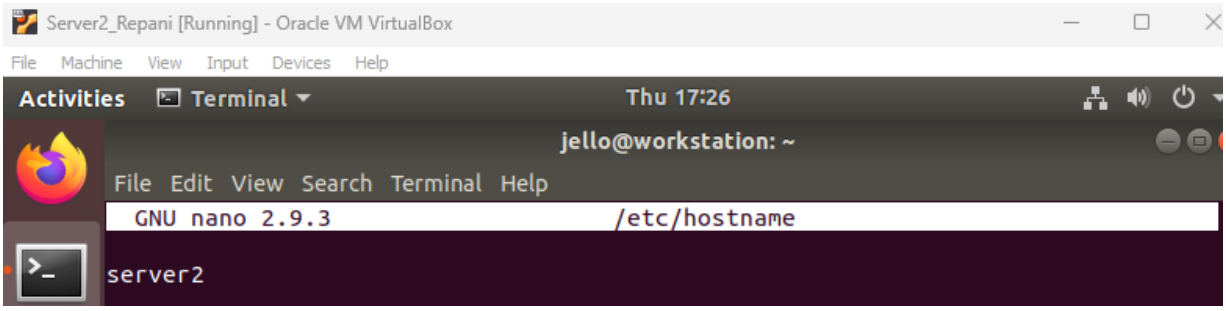
   1.1 Use server1 for Server 1

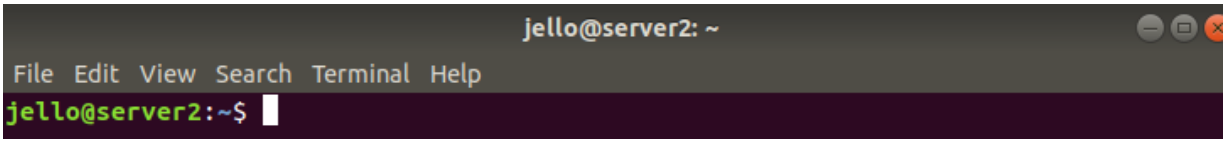
Name: Repani, Justin Jello J.	Date Performed: August 17, 2023



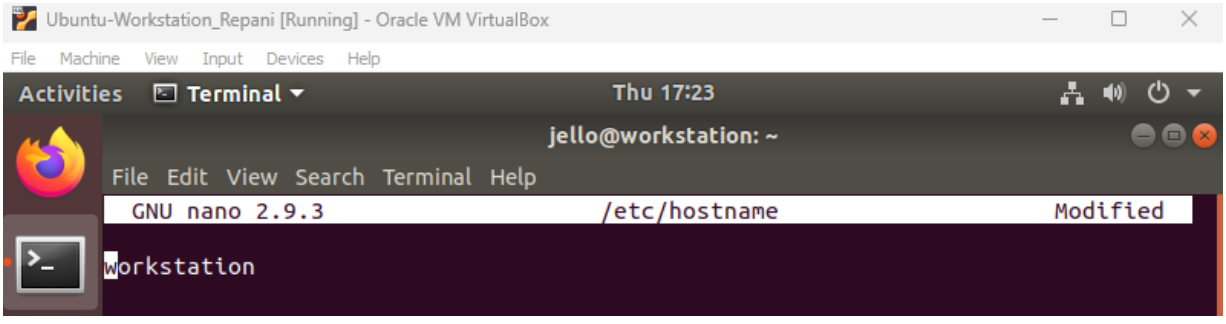


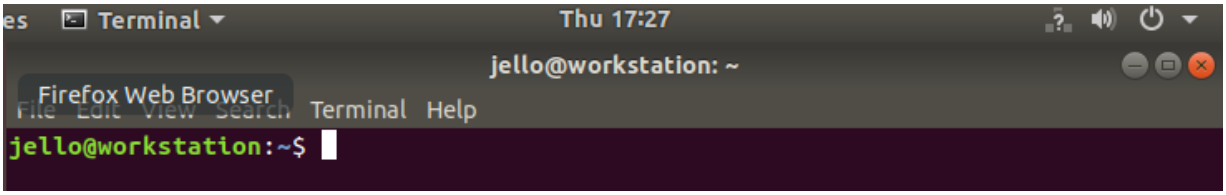
1.2 Use server2 for Server 2





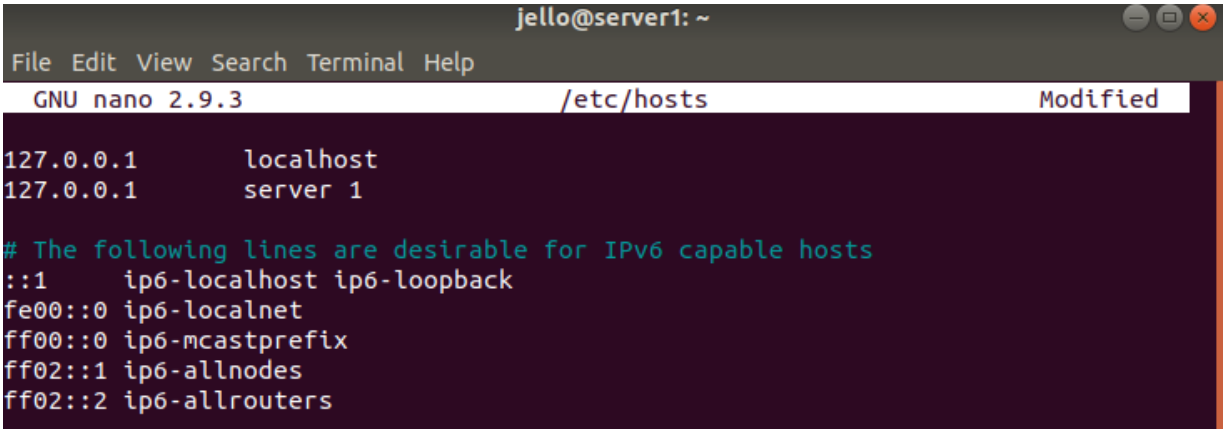
1.3 Use workstation for the Local Machine



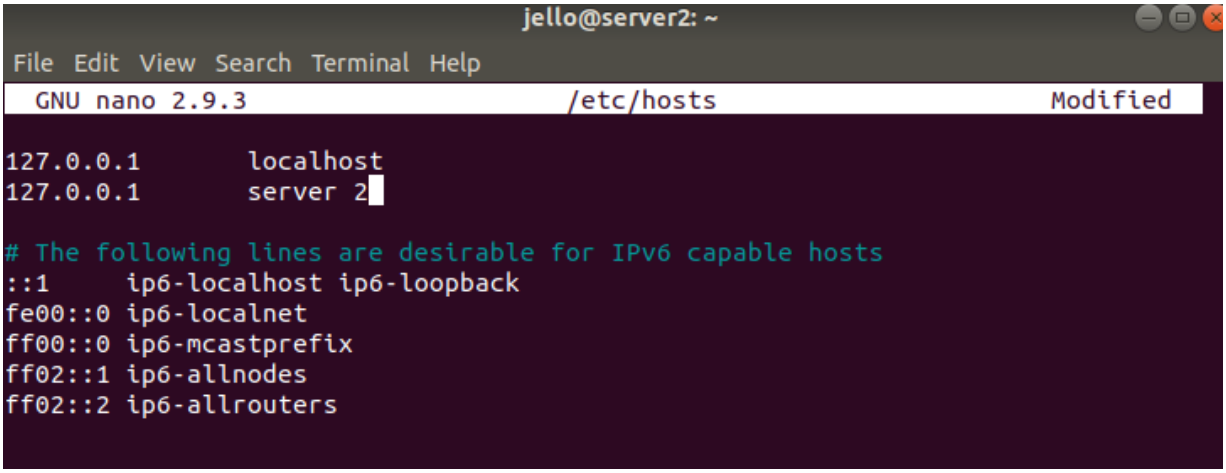


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.
   2.1 Type 127.0.0.1 server 1 for Server 1

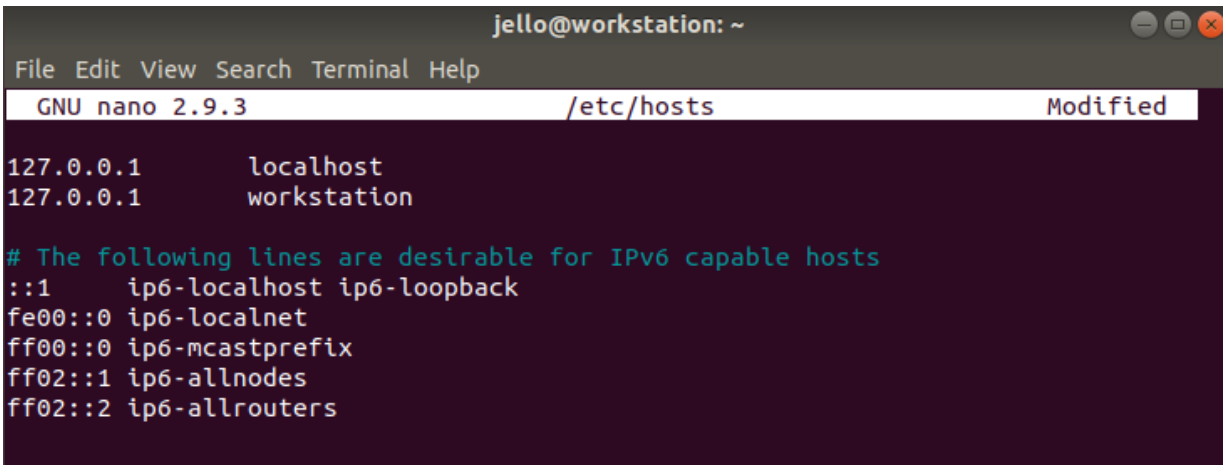
Name: Repani, Justin Jello J.	Date Performed: August 17, 2023



2.2 Type 127.0.0.1 server 2 for Server 2



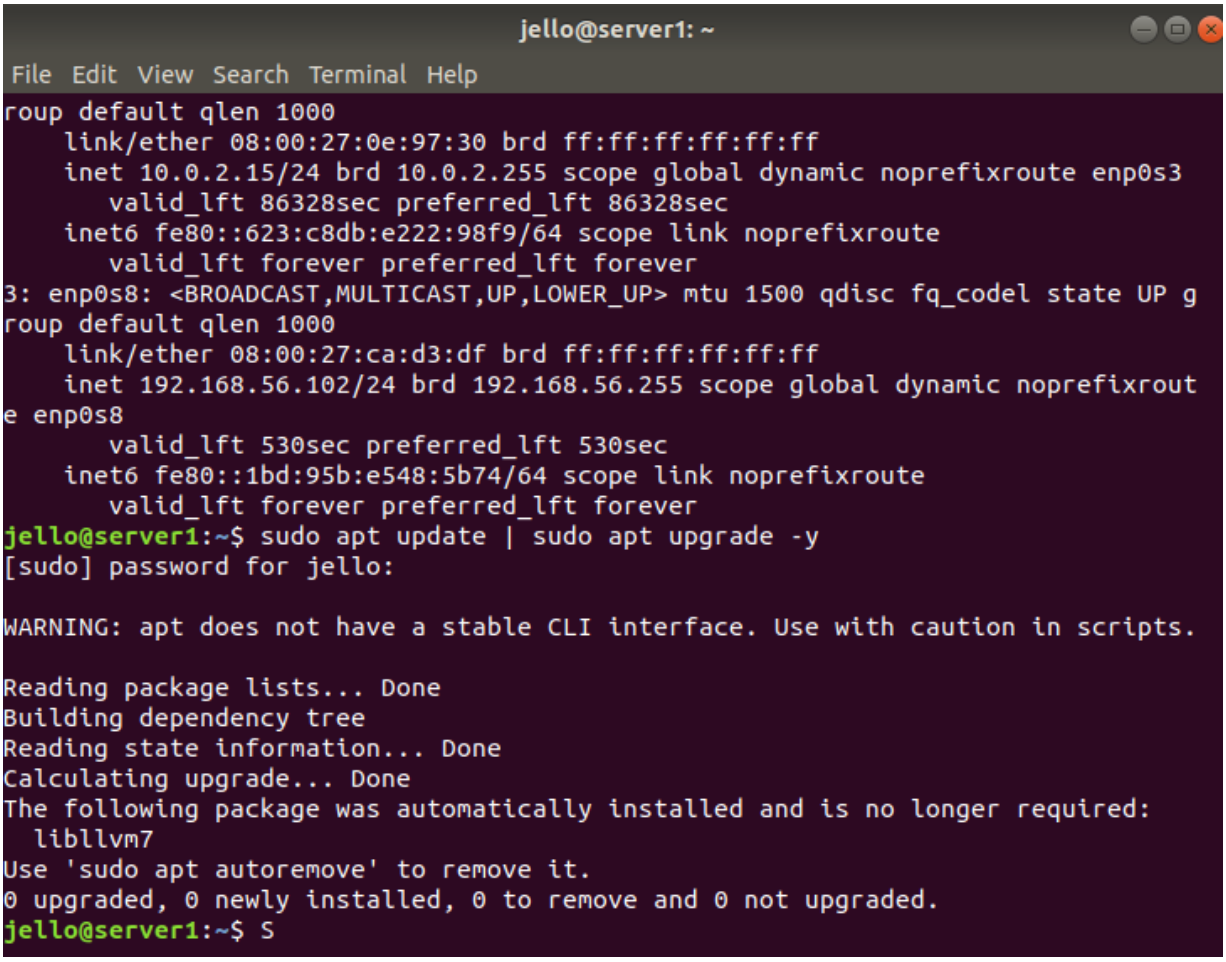
2.3 Type 127.0.0.1 workstation for the Local Machine



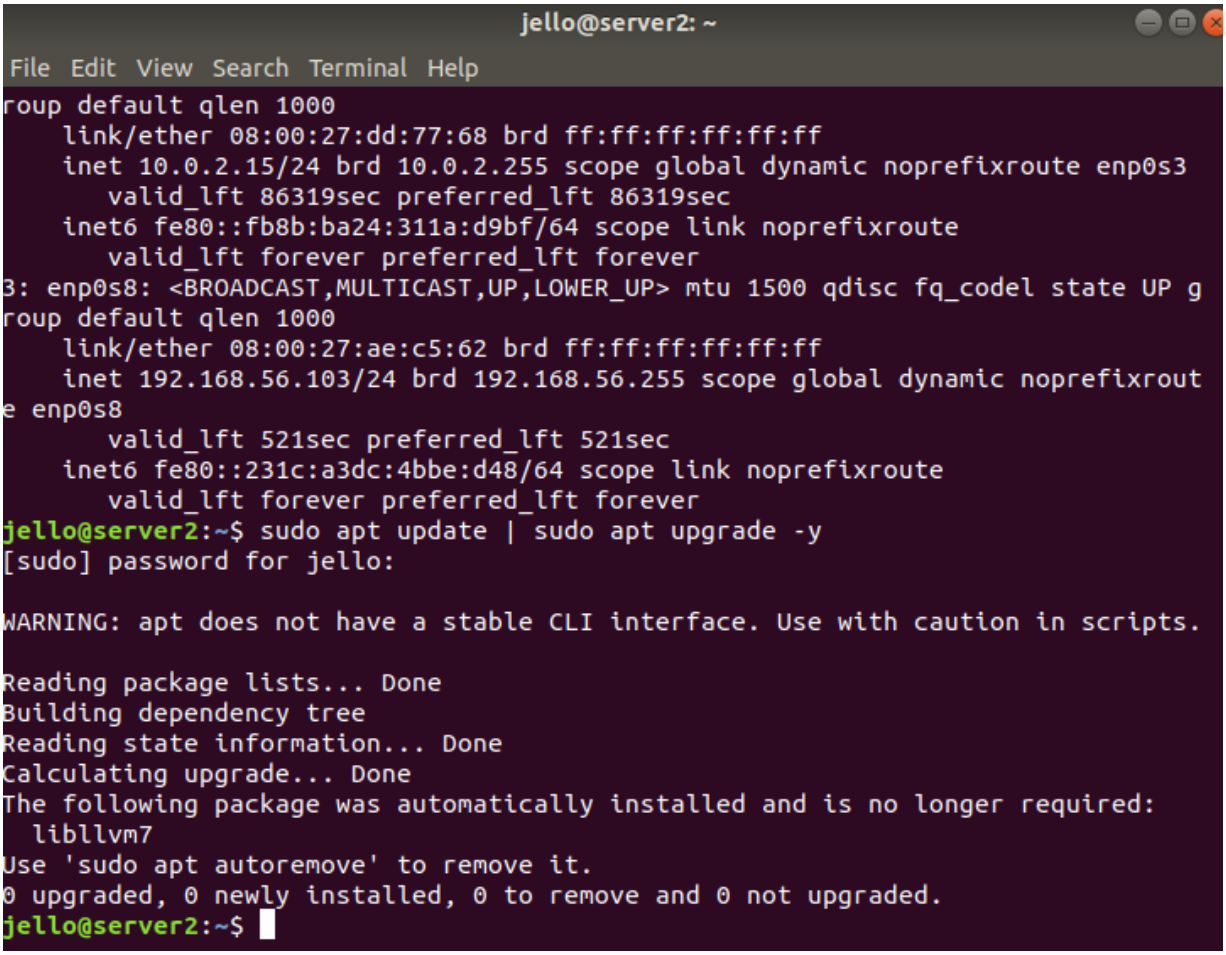
Task 2: Configure SSH on Server 1, Server 2, and Local Machine. Do the following:

1. Upgrade the packages by issuing the command *sudo apt update* and *sudo apt upgrade* respectively.

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023

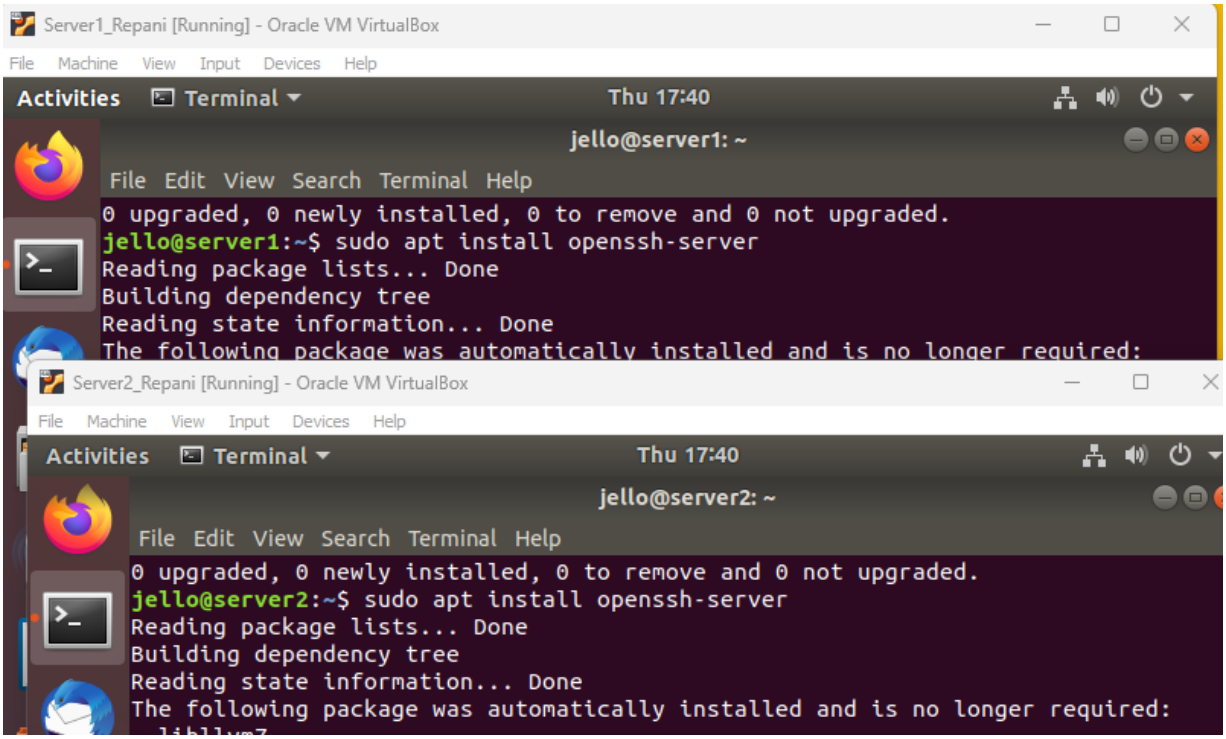


Name: Repani, Justin Jello J.	Date Performed: August 17, 2023



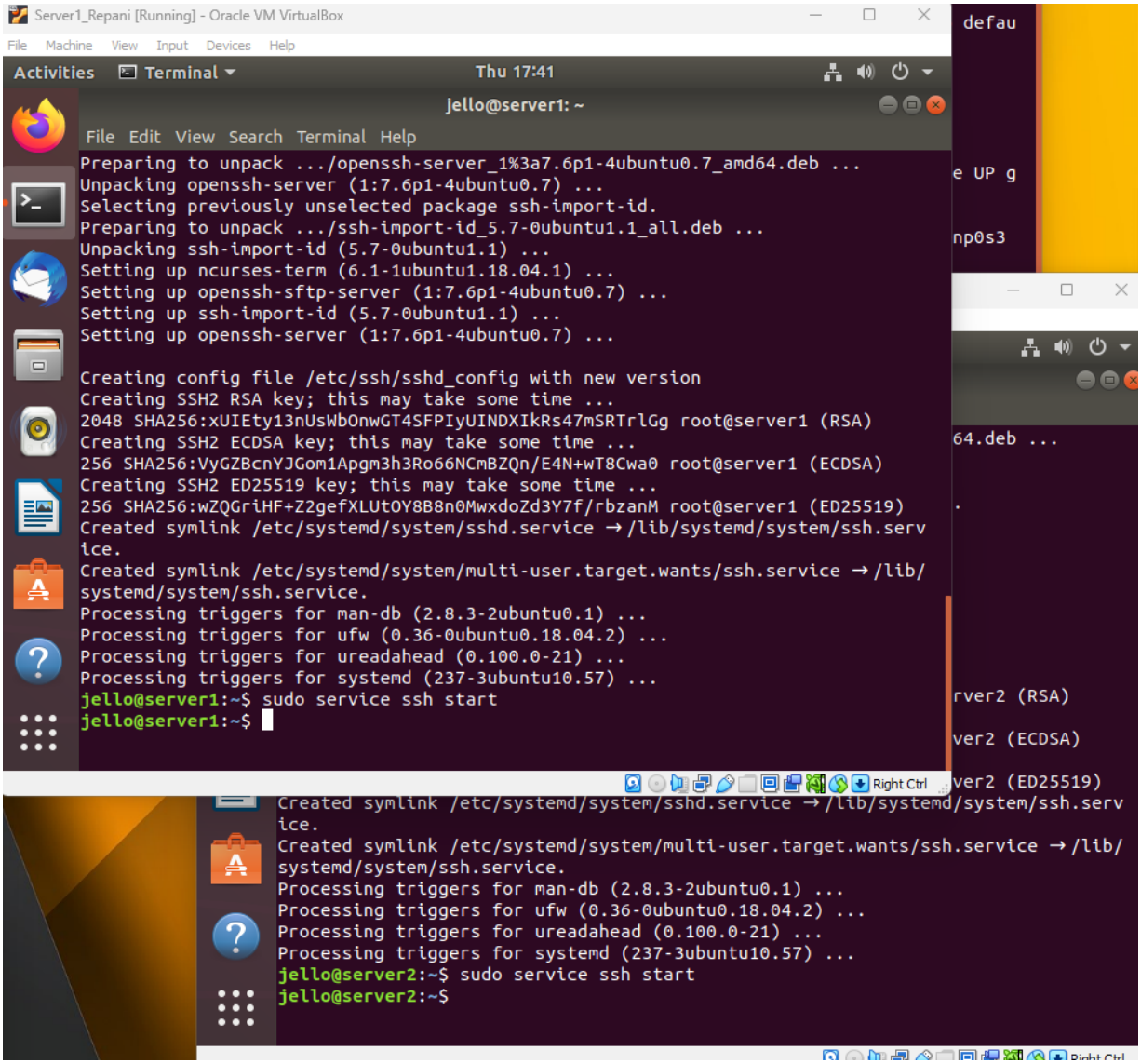
2. Install the SSH server using the command *sudo apt install openssh-server*.

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023



3. Verify if the SSH service has started by issuing the following commands:
   3.1 sudo service ssh start

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023



3.2 sudo systemctl status ssh

```
jello@server1:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Thu 2023-08-17 17:39:57 PST; 1min 33s ago
 Main PID: 2548 (sshd)
    Tasks: 1 (limit: 4656)
   CGroup: /system.slice/ssh.service
           └─2548 /usr/sbin/sshd -D

Aug 17 17:39:56 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:39:57 server1 sshd[2548]: Server listening on 0.0.0.0 port 22.
Aug 17 17:39:57 server1 sshd[2548]: Server listening on :: port 22.
Aug 17 17:39:57 server1 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023

```
jello@server2:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Thu 2023-08-17 17:39:51 PST; 1min 46s ago
 Main PID: 2558 (sshd)
    Tasks: 1 (limit: 4656)
   CGroup: /system.slice/ssh.service
           └─2558 /usr/sbin/sshd -D

Aug 17 17:39:51 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:39:51 server2 sshd[2558]: Server listening on 0.0.0.0 port 22.
Aug 17 17:39:51 server2 sshd[2558]: Server listening on :: port 22.
Aug 17 17:39:51 server2 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

4. Configure the firewall to all port 22 by issuing the following commands:

4.1 sudo ufw allow ssh

```
[1]+  Stopped                 sudo systemctl status ssh
jello@server1:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
jello@server1:~$
```

Right Ctrl

```
jello@server2:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
jello@server2:~$
```

4.2 sudo ufw enable

```
jello@server1:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
jello@server1:~$ sudo ufw enable
Firewall is active and enabled on system startup
jello@server1:~$
```

Right

```
Rules updated (v6)
jello@server2:~$ sudo ufw enable
Firewall is active and enabled on system startup
jello@server2:~$
```

4.3 sudo ufw status

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023

```
jello@server1:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

jello@server1:~$
```

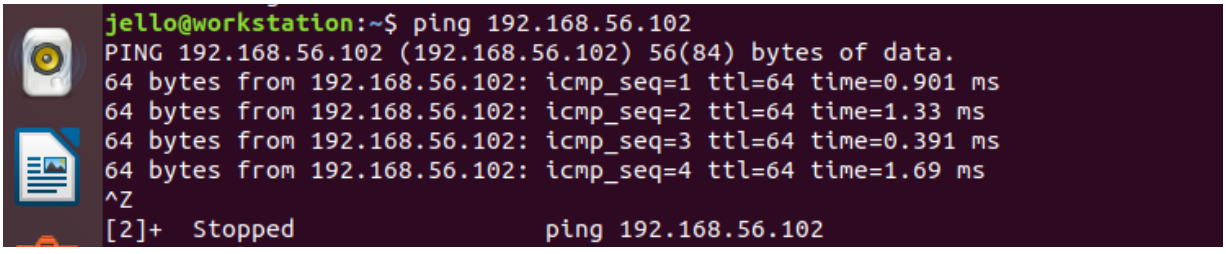
```
jello@server2:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

jello@server2:~$
```

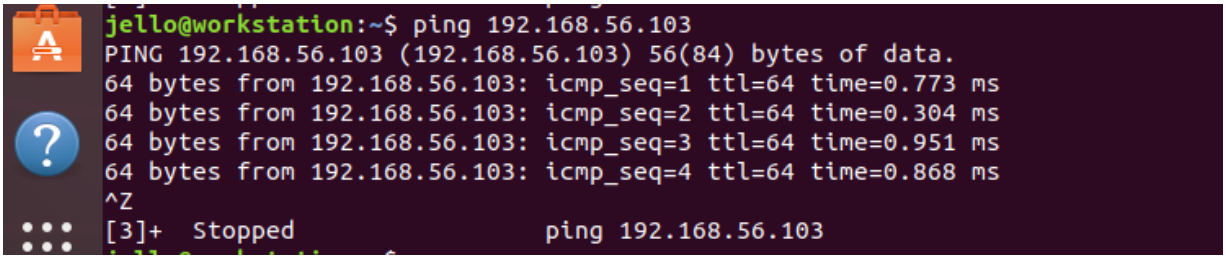
Task 3: Verify network settings on Server 1, Server 2, and Local Machine. On each device, do the following:

1. Record the ip address of Server 1, Server 2, and Local Machine. Issue the command *ifconfig* and check network settings. Note that the ip addresses of all the machines are in this network 192.168.56.XX.
   1.1 Server 1 IP address: 192.168.56.102
   1.2 Server 2 IP address: 192.168.56.103
   1.3 Server 3 IP address: 192.168.56.101
2. Make sure that they can ping each other.
   2.1 Connectivity test for Local Machine 1 to Server 1: ☐ Successful ☐ Not Successful

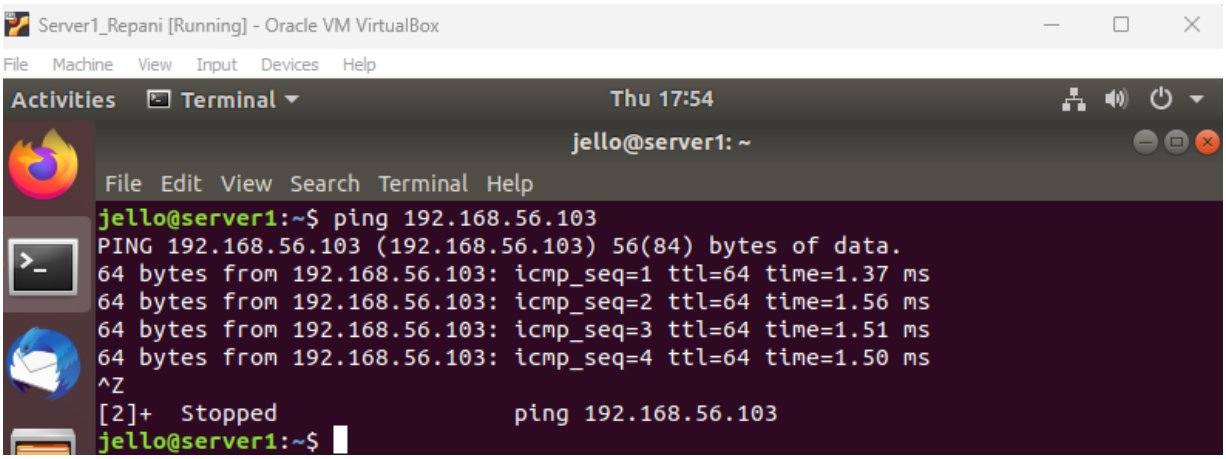


   2.2 Connectivity test for Local Machine 1 to Server 2: ☐ Successful ☐ Not Successful

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023



2.3 Connectivity test for Server 1 to Server 2: ☐ Successful ☐ Not Successful\



Task 4: Verify SSH connectivity on Server 1, Server 2, and Local Machine.

1. On the Local Machine, issue the following commands:

1.1 ssh username@ip_address_server1 for example, *ssh jvtaylar@192.168.56.120*

```
jello@workstation:~$ ssh jello@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established
.
ECDSA key fingerprint is SHA256:VyGZBcnYJGom1Apgm3h3Ro66NCmBZQn/E4N+wT8Cwa0.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
jello@192.168.56.102's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)
```

1.2 Enter the password for server 1 when prompted

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jello@server1:~$
```

1.3 Verify that you are in server 1. The user should be in this format user@server1. For example, *jvtaylar@server1*

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jello@server1:~$
```

2. Logout of Server 1 by issuing the command *control + D.*

```
jello@server1:~$ logout
Connection to 192.168.56.102 closed.
jello@workstation:~$
```

3. Do the same for Server 2.

```
jello@workstation:~$ ssh jello@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established
.
ECDSA key fingerprint is SHA256:7BrewEemwrzk/jFucX235tXhbYUu9o1M+iQ/8cv5I0M.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.103' (ECDSA) to the list of known hosts.
jello@192.168.56.103's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Infrastructure is not enabled.
```

```
jello@server2:~$ logout
Connection to 192.168.56.103 closed.
jello@workstation:~$
```

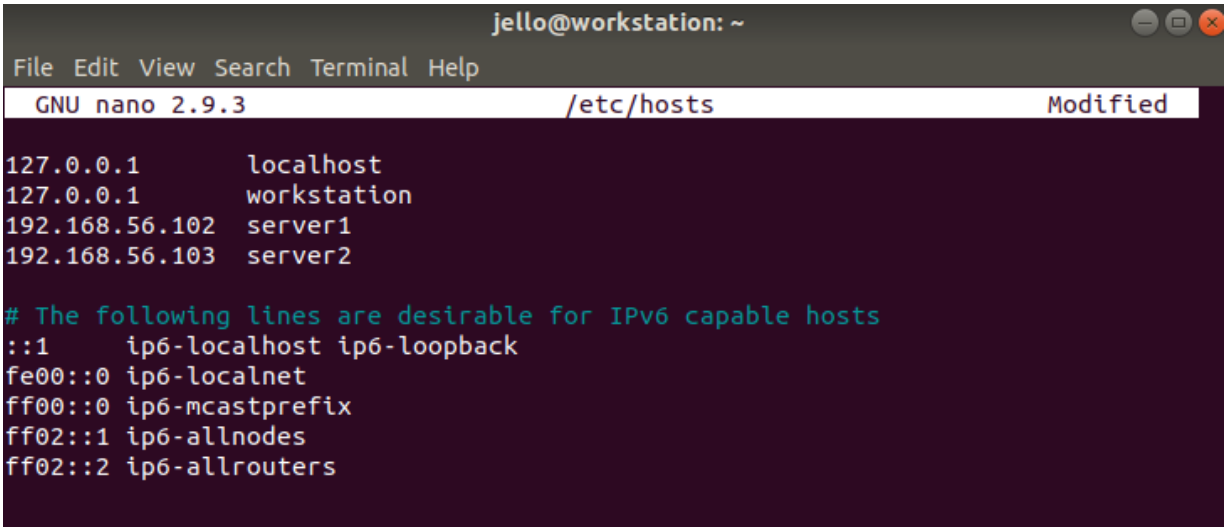
4. Edit the hosts of the Local Machine by issuing the command *sudo nano /etc/hosts.* Below all texts type the following:

4.1 IP_address server 1 (provide the ip address of server 1 followed by the hostname)

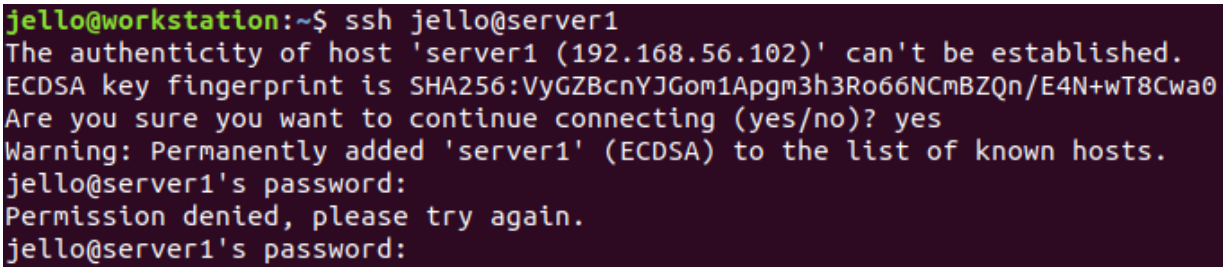
4.2 IP_address server 2 (provide the ip address of server 2 followed by the hostname)

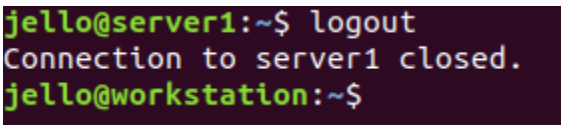
4.3 Save the file and exit.

Name: Repani, Justin Jello J.	Date Performed: August 17, 2023



5. On the local machine, verify that you can do the SSH command but this time, use the hostname instead of typing the IP address of the servers. For example, try to do *ssh jvtaylar@server1*. Enter the password when prompted. Verify that you have entered Server 1. Do the same for Server 2.





Name: Repani, Justin Jello J.	Date Performed: August 17, 2023

```
jello@workstation:~$ ssh jello@server2
The authenticity of host 'server2 (192.168.56.103)' can't be established.
ECDSA key fingerprint is SHA256:7BrewEemwrzk/jFucX235tXhbYUu9o1M+iQ/8cv5I0M.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
jello@server2's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Thu Aug 17 18:02:22 2023 from 192.168.56.101
jello@server2:~$ logout
Connection to server2 closed.
jello@workstation:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
   We are able to use the hostname instead of the IP address in SSH commands because we edited the /etc/hosts file and added the ip address to the list with its corresponding hostname, specifically 192.168.56.102 for server1 and 192.168.56.102 for server2. By doing this we can now use the command ssh jello@server1 instead of jello@192.168.56.102 since the ip address is now attached to the specific hostname.
2. How secured is SSH?

   Based on what we learned on Computer Networking 1, SSH is a secure type of login because it makes use of a username and password just like telnet, but this one on SSH also makes use of encryption so that the information about the hostname and password are encrypted instead of being in plain text file.

Conclusion

In this first hands-on activity for the course Managing Enterprise Server, we first created new Linux Ubuntu profiles in order to start the workstation and servers. We

Name: Repani, Justin Jello J.	**Date Performed: August 17, 2023**
first created the workstation profile and setup the Linux, after this the profile is cloned with different MAC addresses in order to create the new servers 1 and 2. After this the SSH was set up in order to make a connection between the different devices from workstation, server1, and server2. The basic commands in order to setup the ssh, firewall, and test the connections of the different machines are performed.	

“I affirm that I have not given or received any unauthorized help on this assignment, and that this work is my own.”