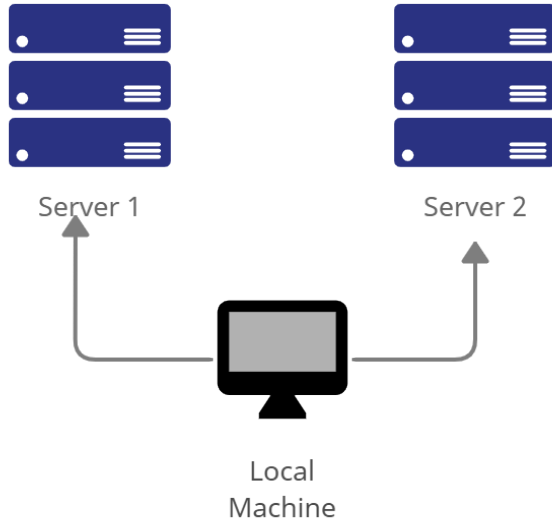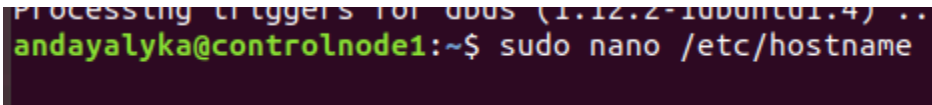| Name: Andaya, Lyka C	Date Performed: August 14, 2023
Course/Section: CPE 31S4	Date Submitted: August 15, 2023
Instructor: Engr. Taylar	Semester and SY:

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*).

Server 1   Server 2

Local
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

```
Processing triggers for dbus (1.12.2-1ubuntu1.4) ..
andayalyka@controlnode1:~$ sudo nano /etc/hostname
```

```
  GNU nano 2.9.3                          /etc/hostname

 controlnode1
```

      1.2 Use server2 for Server 2

```
andayalyka@controlnode2:~$ sudo nano /etc/hostname
```

```
  GNU nano 2.9.3                          /etc/hostname

 controlnode2
```

      1.3 Use workstation for the Local Machine

```
andayalyka@managenode:~$ sudo nano /etc/hostname
```

```
  GNU nano 2.9.3              /etc/hostname              Modified

 managenode
```

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

```
  GNU nano 2.9.3                          /etc/hosts

 127.0.0.1          controlnode1
 127.0.1.1          andayalyka-VirtualBox
```

      2.2 Type 127.0.0.1 server 2 for Server 2

```
  GNU nano 2.9.3                          /etc/hosts

 127.0.0.1          controlnode2
 127.0.1.1          andayalyka-VirtualBox
```

      2.3 Type 127.0.0.1 workstation for the Local Machine

```
  GNU nano 2.9.3                          /etc/hosts

 127.0.0.1          managenode
 127.0.1.1          andayalyka-VirtualBox
```

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.

```
andayalyka@managenode:~$ sudo apt  update | sudo apt upgrade -y

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  distro-info fwupd-signed gstreamer1.0-gtk3 libllvm10 libnetplan0 libxmlb1
  linux-headers-5.4.0-150-generic linux-hwe-5.4-headers-5.4.0-150
  linux-image-5.4.0-150-generic linux-modules-5.4.0-150-generic
  linux-modules-extra-5.4.0-150-generic python3-click python3-colorama
  python3-dateutil ubuntu-advantage-desktop-daemon xdg-desktop-portal
  xdg-desktop-portal-gtk
The following packages will be upgraded:
  accountsservice amd64-microcode apparmor apport apport-gtk apt apt-utils
  aptdaemon aptdaemon-data aspell avahi-autoipd avahi-daemon avahi-utils
  base-files bash bind9-host binutils binutils-common
  binutils-x86-64-linux-gnu bluez bluez-cups bluez-obexd bsdutils
  busybox-initramfs busybox-static bzip2 ca-certificates command-not-found
  command-not-found-data console-setup console-setup-linux cpio cpp cpp-7
```

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

```
andayalyka@managenode:~$ sudo apt install openssh-server
[sudo] password for andayalyka:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 39s (16.4 kB/s)
```

3. Verify if the SSH service has started by issuing the following commands:

3.1 *sudo service ssh start*

```
andayalyka@managenode:~$ sudo service ssh start
```

3.2 *sudo systemctl status ssh*

```
andayalyka@managenode:~$ 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 Tue 2023-08-15 16:43:49 PST; 1min 21s ago
 Main PID: 20736 (sshd)
    Tasks: 1 (limit: 2377)
   CGroup: /system.slice/ssh.service
           └─20736 /usr/sbin/sshd -D

Aug 15 16:43:49 managenode systemd[1]: Starting OpenBSD Secure Shell server...
Aug 15 16:43:49 managenode sshd[20736]: Server listening on 0.0.0.0 port 22.
Aug 15 16:43:49 managenode sshd[20736]: Server listening on :: port 22.
Aug 15 16:43:49 managenode systemd[1]: Started OpenBSD Secure Shell server.
```

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

4.1 *sudo ufw allow ssh*

```
andayalyka@managenode:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

4.2 *sudo ufw enable*

```
andayalyka@managenode:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

4.3 *sudo ufw status*

```
andayalyka@managenode:~$ sudo ufw status
Status: active

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

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.<u>102</u>

   1.2 Server 2 IP address: 192.168.56.<u>103</u>

   1.3 Server 3 IP address: 192.168.56.<u>101</u>

2. Make sure that they can ping each other.

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

```
andayalyka@managenode:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.58 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.43 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=1.34 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.764 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=1.83 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.840 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=0.393 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=0.384 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=0.417 ms
64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=1.14 ms
64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=1.27 ms
64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=1.77 ms
64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=0.442 ms
64 bytes from 192.168.56.102: icmp_seq=15 ttl=64 time=0.405 ms
64 bytes from 192.168.56.102: icmp_seq=16 ttl=64 time=0.383 ms
64 bytes from 192.168.56.102: icmp_seq=17 ttl=64 time=0.513 ms
64 bytes from 192.168.56.102: icmp_seq=18 ttl=64 time=0.776 ms
64 bytes from 192.168.56.102: icmp_seq=19 ttl=64 time=0.408 ms
64 bytes from 192.168.56.102: icmp_seq=20 ttl=64 time=0.442 ms
64 bytes from 192.168.56.102: icmp_seq=21 ttl=64 time=0.440 ms
64 bytes from 192.168.56.102: icmp_seq=22 ttl=64 time=0.582 ms
64 bytes from 192.168.56.102: icmp_seq=23 ttl=64 time=1.41 ms
```

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

```
andayalyka@managenode:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.961 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.765 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.725 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=1.55 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=1.57 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=0.891 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=0.544 ms
```

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

```
                vacca_crc rorcvcr prcrcrrca_crc rorcvcr
andayalyka@controlnode1:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.841 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.62 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.507 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.398 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.924 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=0.601 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=1.05 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=64 time=0.434 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=64 time=0.403 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=64 time=0.917 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=64 time=0.413 ms
64 bytes from 192.168.56.103: icmp_seq=12 ttl=64 time=0.489 ms
64 bytes from 192.168.56.103: icmp_seq=13 ttl=64 time=0.364 ms
64 bytes from 192.168.56.103: icmp_seq=14 ttl=64 time=0.450 ms
64 bytes from 192.168.56.103: icmp_seq=15 ttl=64 time=0.875 ms
64 bytes from 192.168.56.103: icmp_seq=16 ttl=64 time=0.807 ms
64 bytes from 192.168.56.103: icmp_seq=17 ttl=64 time=1.41 ms
64 bytes from 192.168.56.103: icmp_seq=18 ttl=64 time=0.442 ms
64 bytes from 192.168.56.103: icmp_seq=19 ttl=64 time=0.971 ms
64 bytes from 192.168.56.103: icmp_seq=20 ttl=64 time=0.960 ms
64 bytes from 192.168.56.103: icmp_seq=21 ttl=64 time=0.659 ms
64 bytes from 192.168.56.103: icmp_seq=22 ttl=64 time=1.07 ms
64 bytes from 192.168.56.103: icmp_seq=23 ttl=64 time=1.13 ms
64 bytes from 192.168.56.103: icmp_seq=24 ttl=64 time=1.35 ms
64 bytes from 192.168.56.103: icmp_seq=25 ttl=64 time=0.815 ms
```

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*

    1.2 Enter the password for server 1 when prompted

```
andayalyka@managenode:~$ ssh andayalyka@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:PTkRPjygx7JARtan/nDkOSfZ0qiZlpdLV86Ftf+WGI8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
andayalyka@192.168.56.102's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.18.0-15-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.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Your Hardware Enablement Stack (HWE) is supported until April 2023.
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

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

```
andayalyka@controlnode1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:de:f7:2e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 82741sec preferred_lft 82741sec
    inet6 fe80::ab35:714e:7ac0:a964/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:81:e8:3b brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixrout
e enp0s8
       valid_lft 420sec preferred_lft 420sec
    inet6 fe80::66c4:821c:4a0a:a418/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

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

```
andayalyka@controlnode1:~$ logout
Connection to 192.168.56.102 closed.
```

3. Do the same for Server 2.

```
andayalyka@controlnode2:~$ ssh andayalyka@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:PTkRPjygx7JARtan/nDkOSfZ0qiZlpdLV86Ftf+WGI8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
andayalyka@192.168.56.102's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.18.0-15-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.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

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.
*** System restart required ***
Last login: Tue Aug 15 17:38:28 2023 from 192.168.56.101
```

```
andayalyka@controlnode1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:de:f7:2e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 82639sec preferred_lft 82639sec
    inet6 fe80::ab35:714e:7ac0:a964/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:81:e8:3b brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixrout
e enp0s8
       valid_lft 546sec preferred_lft 546sec
    inet6 fe80::66c4:821c:4a0a:a418/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

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)

```
  GNU nano 2.9.3                        /etc/hosts

127.0.0.1          managenode
127.0.1.1          andayalyka-VirtualBox

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.56.102 server 1
```

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

```
  GNU nano 2.9.3                        /etc/hosts

127.0.0.1          managenode
127.0.1.1          andayalyka-VirtualBox

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.56.102 server 1
192.168.56.103 server 2
```

4.3 Save the file and exit.

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.

```
andayalyka@managenode:~$ ssh andayalyka@controlnode1
andayalyka@controlnode1's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.18.0-15-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.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

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.
*** System restart required ***
Last login: Tue Aug 15 17:41:56 2023 from 192.168.56.103
andayalyka@controlnode1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
```

```
andayalyka@controlnode2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:de:f7:2e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86122sec preferred_lft 86122sec
    inet6 fe80::ab35:714e:7ac0:a964/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:81:e8:3b brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixrout
e enp0s8
       valid_lft 588sec preferred_lft 588sec
    inet6 fe80::66c4:821c:4a0a:a418/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
   - When a host name is defined, you can specify a machine by host name instead of IP address. The host names vary depending on the network environment. Use the host name set to the data file on the DNS server. Use the machine name on the configuration page as the host name.

2. How secured is SSH?

   - SSH is encrypted. Whether users are transferring a file, browsing the web or running a command, their actions are private. While it is possible to use SSH with an ordinary user ID and password as credentials, SSH relies more often on public key pairs to authenticate hosts to each other.