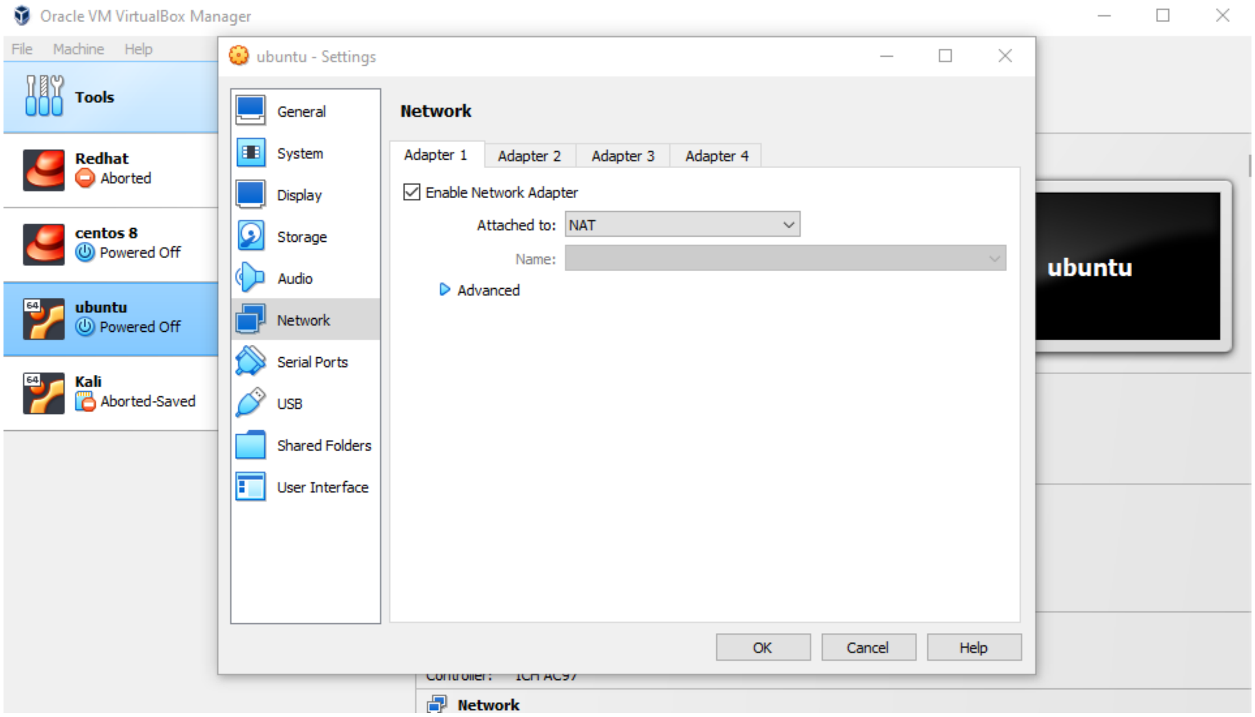
CYSE 270: Linux System for Cybersecurity

Lab 11 – Basic Network Configurations

You can use either Ubuntu VM or Kali Linux VM to complete the following tasks.

Task A – Explore Network Configurations (8 * 5 = 40 Points)

{{{{{{{{Connect your VM in the NAT mode}}}}}}}}

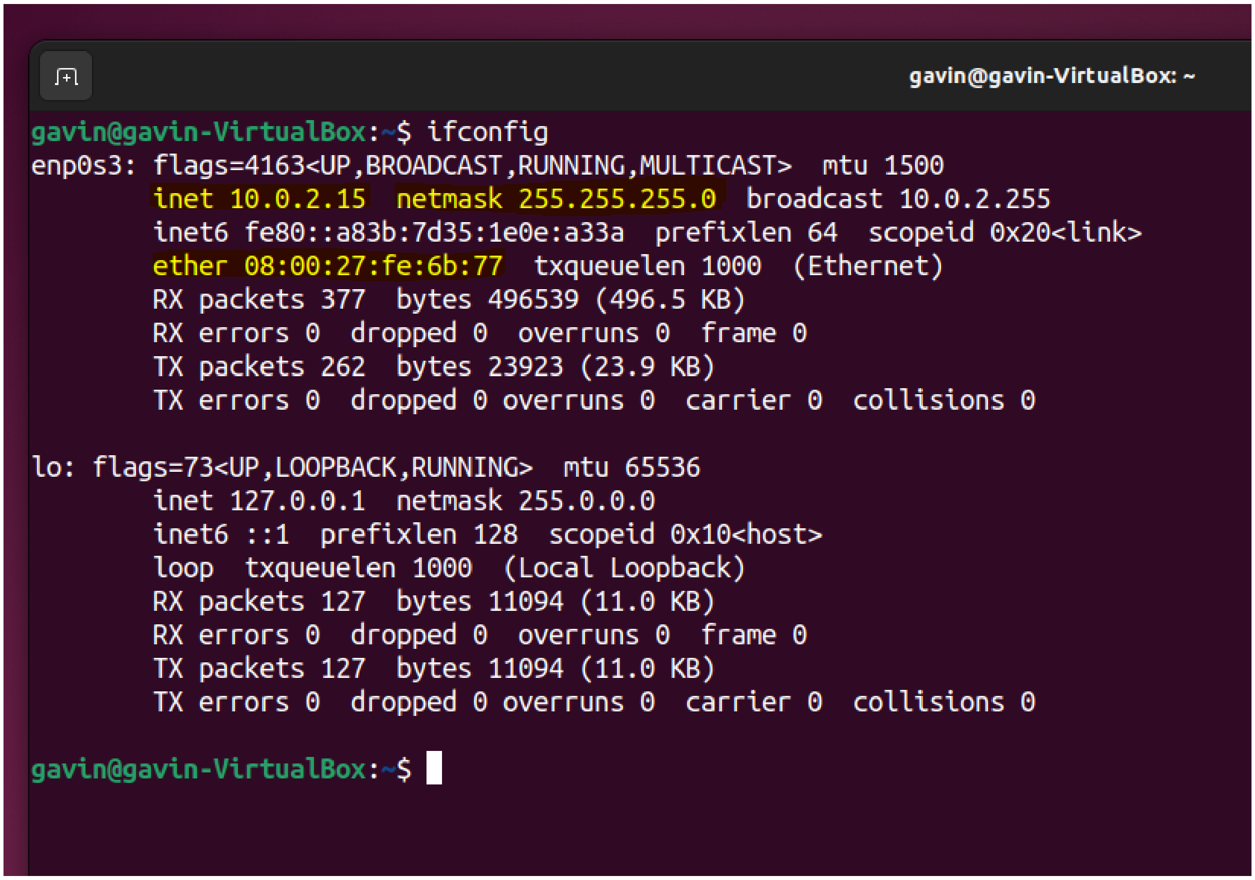


☑ Enable Network Adapter

Attached to: NAT

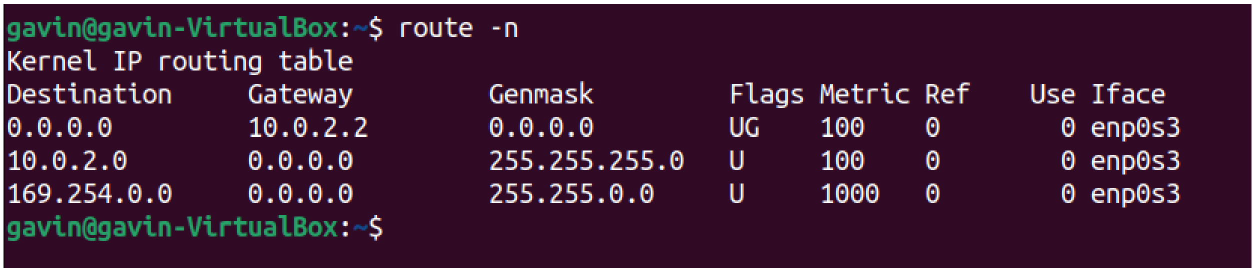
Name:

1. Use the correct **ifconfig** command to display the current network configuration. **Highlight your IP address, MAC address, and the network mask.**



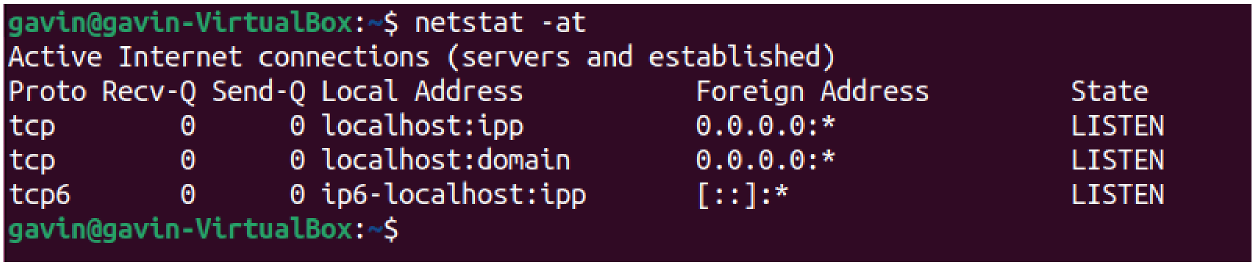
```
gavin@gavin-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a83b:7d35:1e0e:a33a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fe:6b:77  txqueuelen 1000  (Ethernet)
        RX packets 377  bytes 496539 (496.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 262  bytes 23923 (23.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 127  bytes 11094 (11.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 127  bytes 11094 (11.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

gavin@gavin-VirtualBox:~$ 
```

2. Use the correct **route** command to display the current routing table.



```
gavin@gavin-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
gavin@gavin-VirtualBox:~$
```

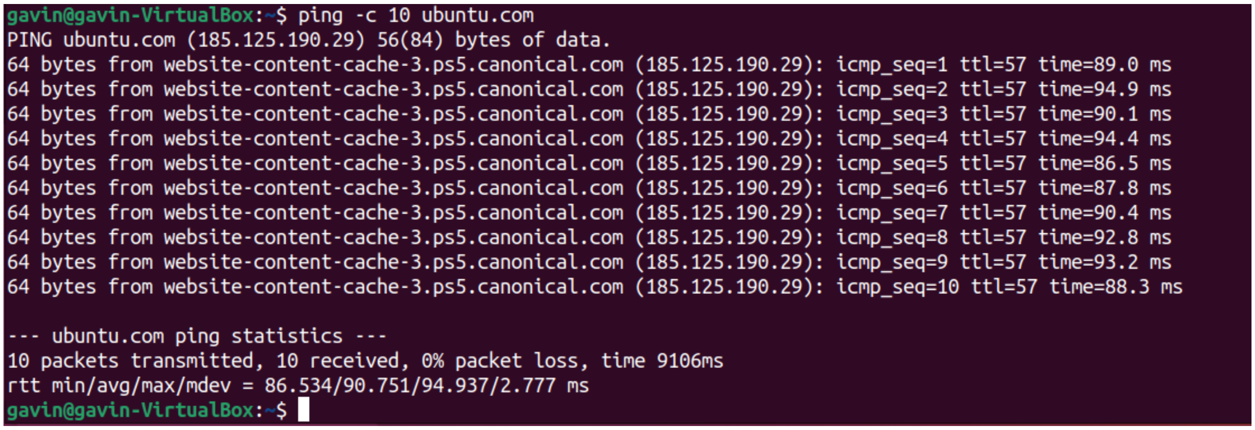
3. Use the **netstat** command to list current TCP connections.



```
gavin@gavin-VirtualBox:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
gavin@gavin-VirtualBox:~$
```

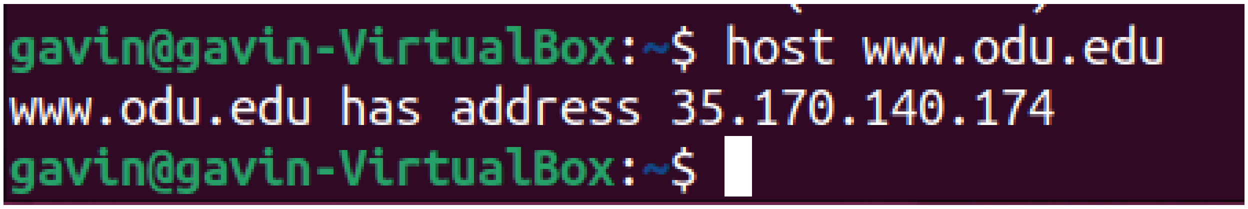
4. Use the **ping** command to determine if the ubuntu.com system is accessible via the network.

(Use the correct option to send 10 ping requests only.)



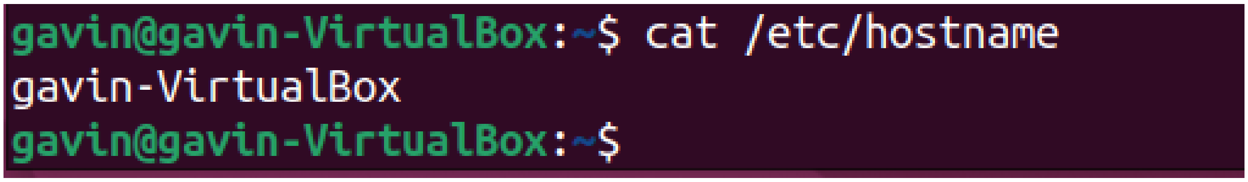
```
gavin@gavin-VirtualBox:~$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.29) 56(84) bytes of data.
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=1 ttl=57 time=89.0 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=2 ttl=57 time=94.9 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=3 ttl=57 time=90.1 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=4 ttl=57 time=94.4 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=5 ttl=57 time=86.5 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=6 ttl=57 time=87.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=7 ttl=57 time=90.4 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=8 ttl=57 time=92.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=9 ttl=57 time=93.2 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=10 ttl=57 time=88.3 ms

--- ubuntu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9106ms
rtt min/avg/max/mdev = 86.534/90.751/94.937/2.777 ms
gavin@gavin-VirtualBox:~$
```

5. Use the **host** command to perform a DNS query on www.odu.edu



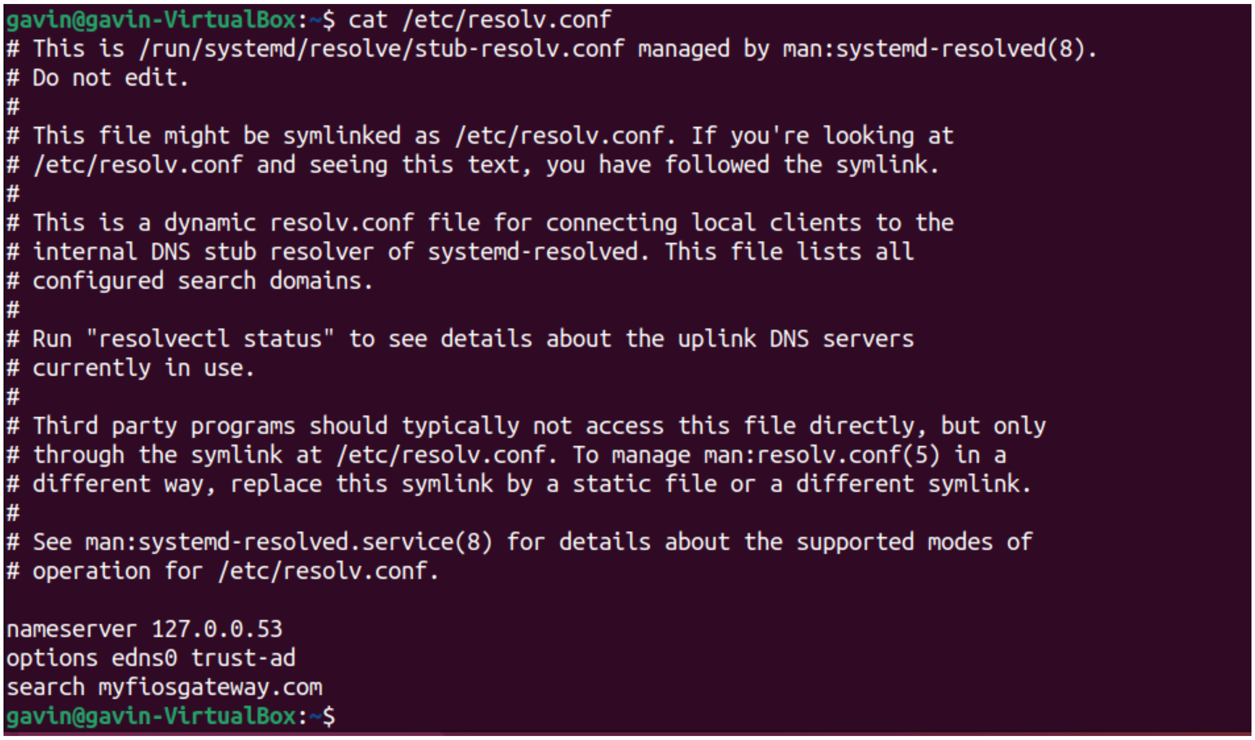
```
gavin@gavin-VirtualBox:~$ host www.odu.edu
www.odu.edu has address 35.170.140.174
gavin@gavin-VirtualBox:~$
```

6. Use the **cat** command to display the contents of the file that contains the system's hostname.



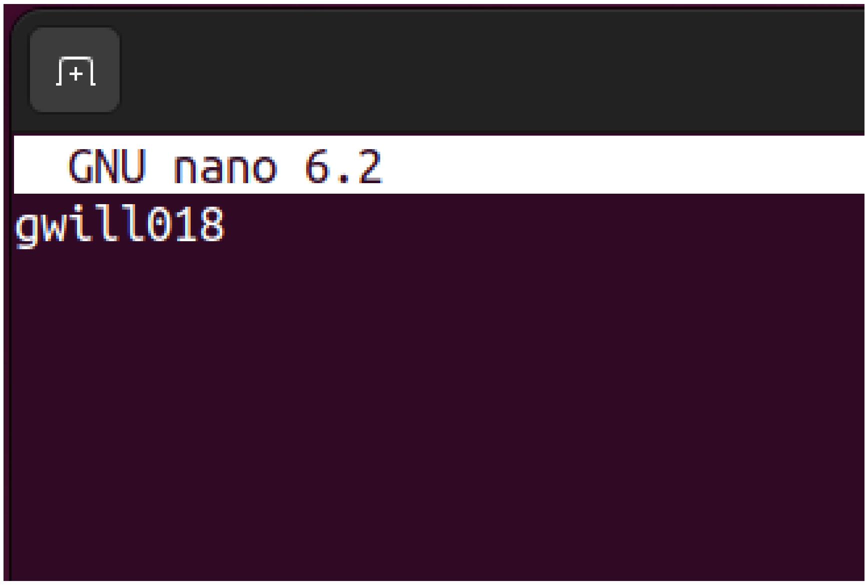
```
gavin@gavin-VirtualBox:~$ cat /etc/hostname
gavin-VirtualBox
gavin@gavin-VirtualBox:~$
```

7. Use the **cat** command to display the contents of the file that contains the DNS servers for this system.

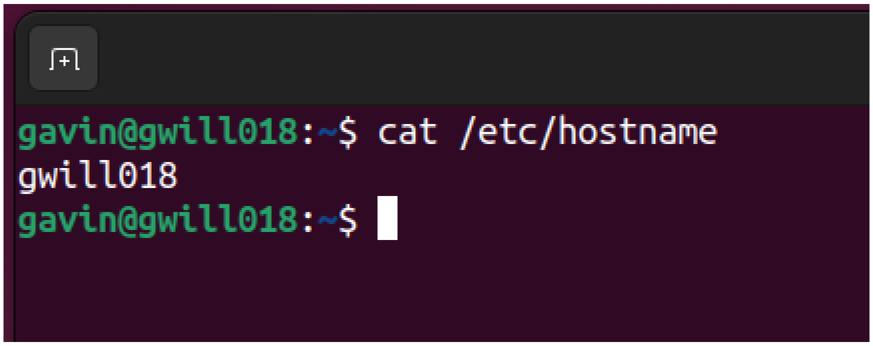


```
gavin@gavin-VirtualBox:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search myfiosgateway.com
gavin@gavin-VirtualBox:~$
```

8. Edit the same file you display in the previous step, set the system’s hostname to your MIDAS ID permanently. Reboot system and **repeat step 6**.



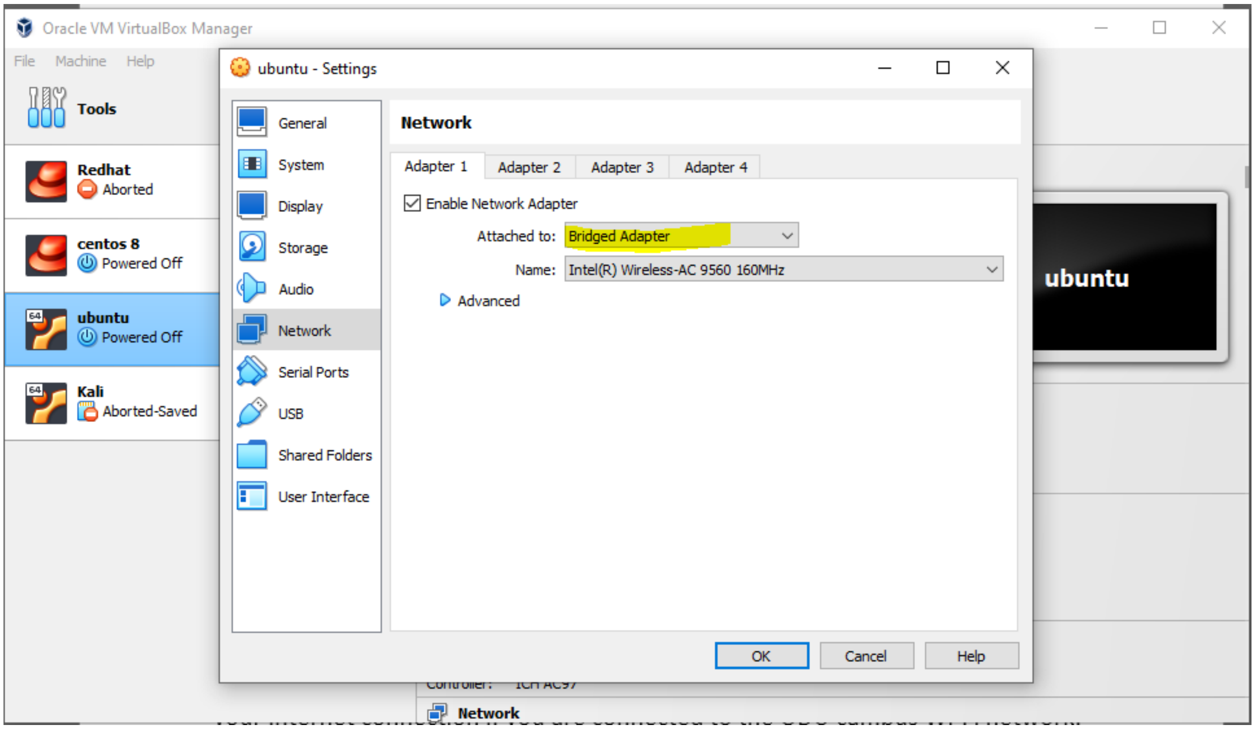
```
  GNU nano 6.2
gwill018
```



```
gavin@gwill018:~$ cat /etc/hostname
gwill018
gavin@gwill018:~$ 
```

Task B – A Different Network Setting (3 * 20 = 60 Points)

1. Change the VM network connection from NAT to bridge mode (you will lose your Internet connection if you are connected to the ODU campus Wi-Fi network, but it is okay).



Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

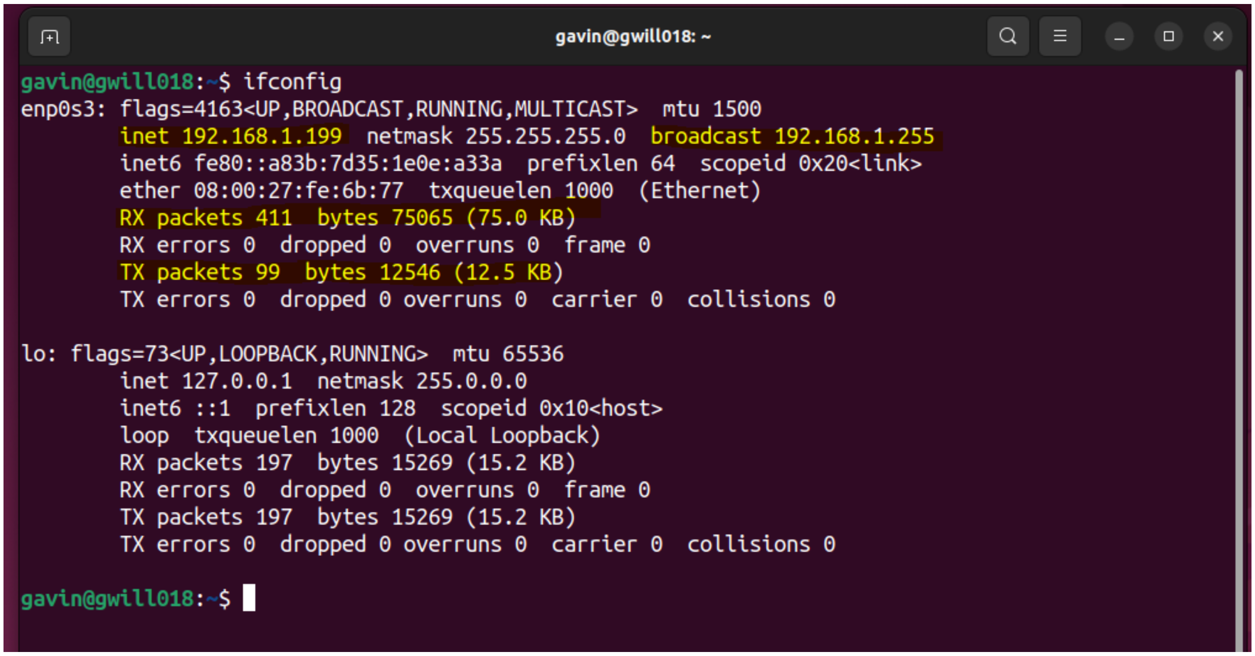
Name: Intel(R) Wireless-AC 9560 160MHz

2. Reboot your system, then repeat Steps 1 – 7 in Task A.

3. Highlight the differences at the end of each step and discuss what do you find.

*** screenshots for both step 2B and 3B ***

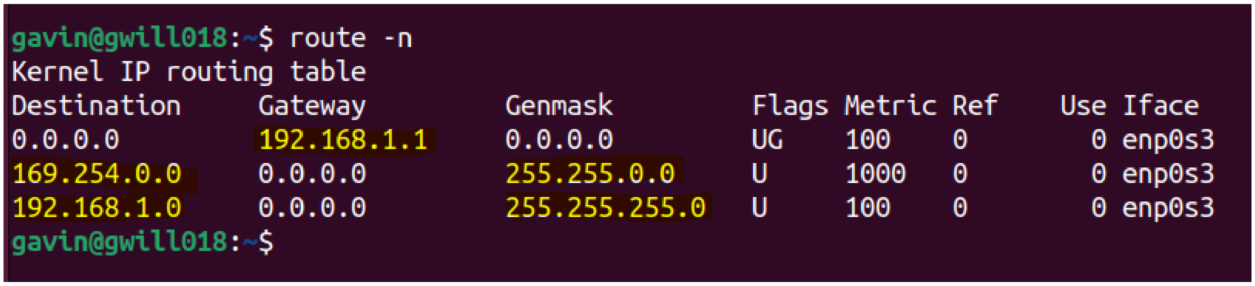
STEP 1



```
gavin@gwill018:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.199  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a83b:7d35:1e0e:a33a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fe:6b:77  txqueuelen 1000  (Ethernet)
        RX packets 411  bytes 75065 (75.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99  bytes 12546 (12.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 197  bytes 15269 (15.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 197  bytes 15269 (15.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

gavin@gwill018:~$ 
```

A couple of fields have changed, but more importantly the IP address and broadcast address are different.

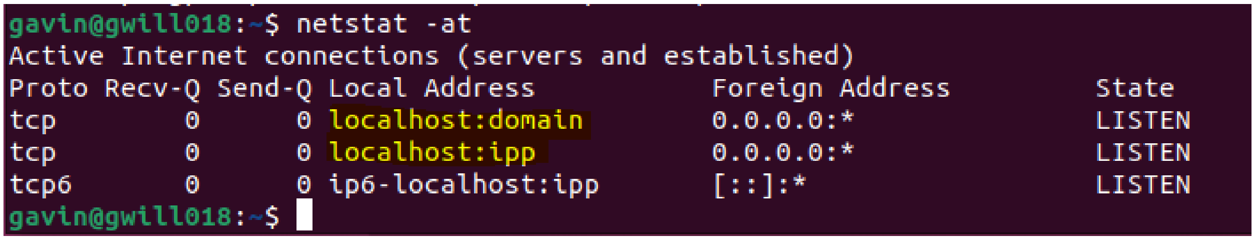
STEP 2



```
gavin@gwill018:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
gavin@gwill018:~$
```

The gateway address is different along with two destination addresses.

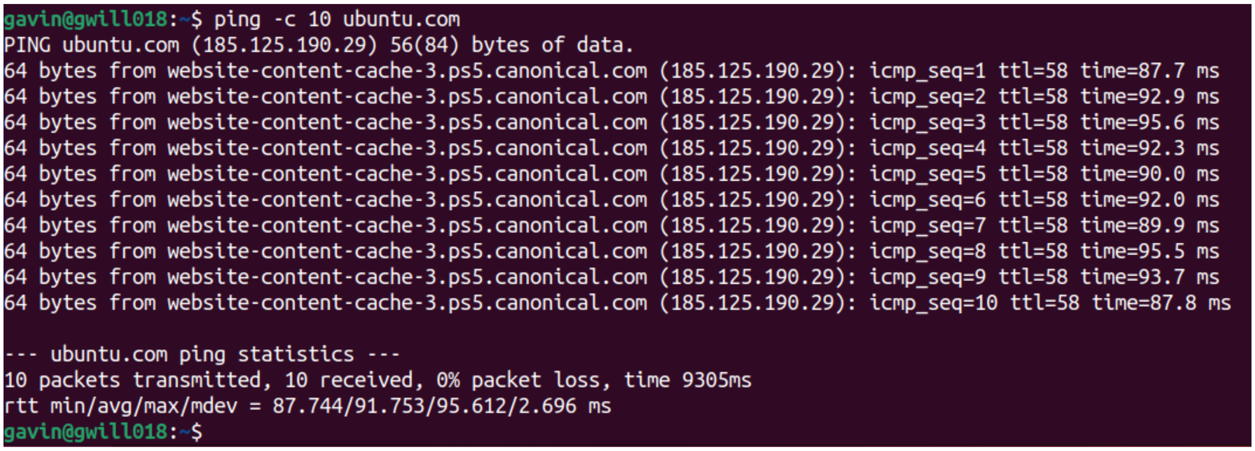
STEP 3



```
gavin@gwill018:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
gavin@gwill018:~$ 
```

There isn’t much change with the netstat -at command; however, the “localhost:Ipp” and “localhost:domain” switched order in the list.

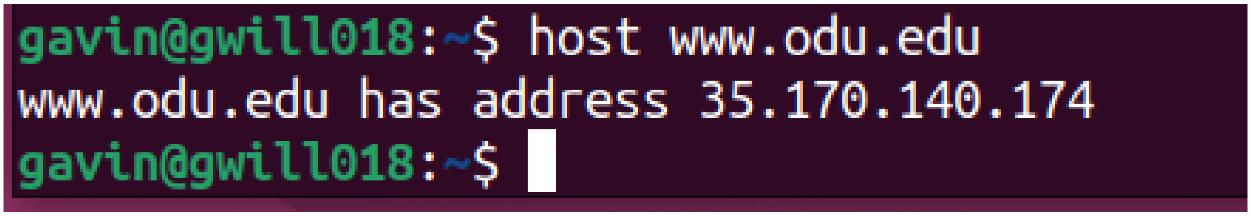
STEP 4



```
gavin@gwill018:~$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.29) 56(84) bytes of data.
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=1 ttl=58 time=87.7 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=2 ttl=58 time=92.9 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=3 ttl=58 time=95.6 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=4 ttl=58 time=92.3 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=5 ttl=58 time=90.0 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=6 ttl=58 time=92.0 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=7 ttl=58 time=89.9 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=8 ttl=58 time=95.5 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=9 ttl=58 time=93.7 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=10 ttl=58 time=87.8 ms

--- ubuntu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9305ms
rtt min/avg/max/mdev = 87.744/91.753/95.612/2.696 ms
gavin@gwill018:~$
```

I am still able to ping ubuntu.com.

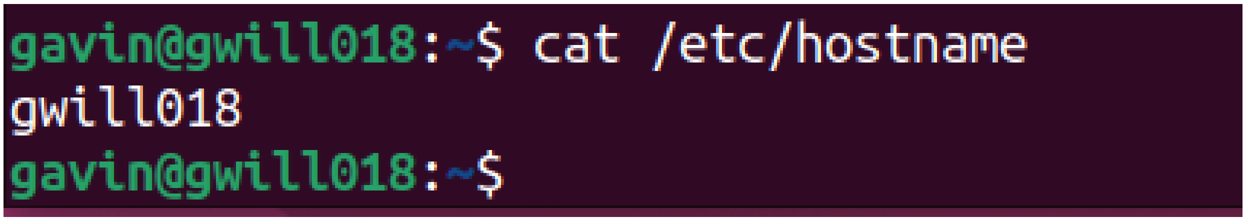
STEP 5



```
gavin@gwill018:~$ host www.odu.edu
www.odu.edu has address 35.170.140.174
gavin@gwill018:~$
```

There isn’t any change with the host command.

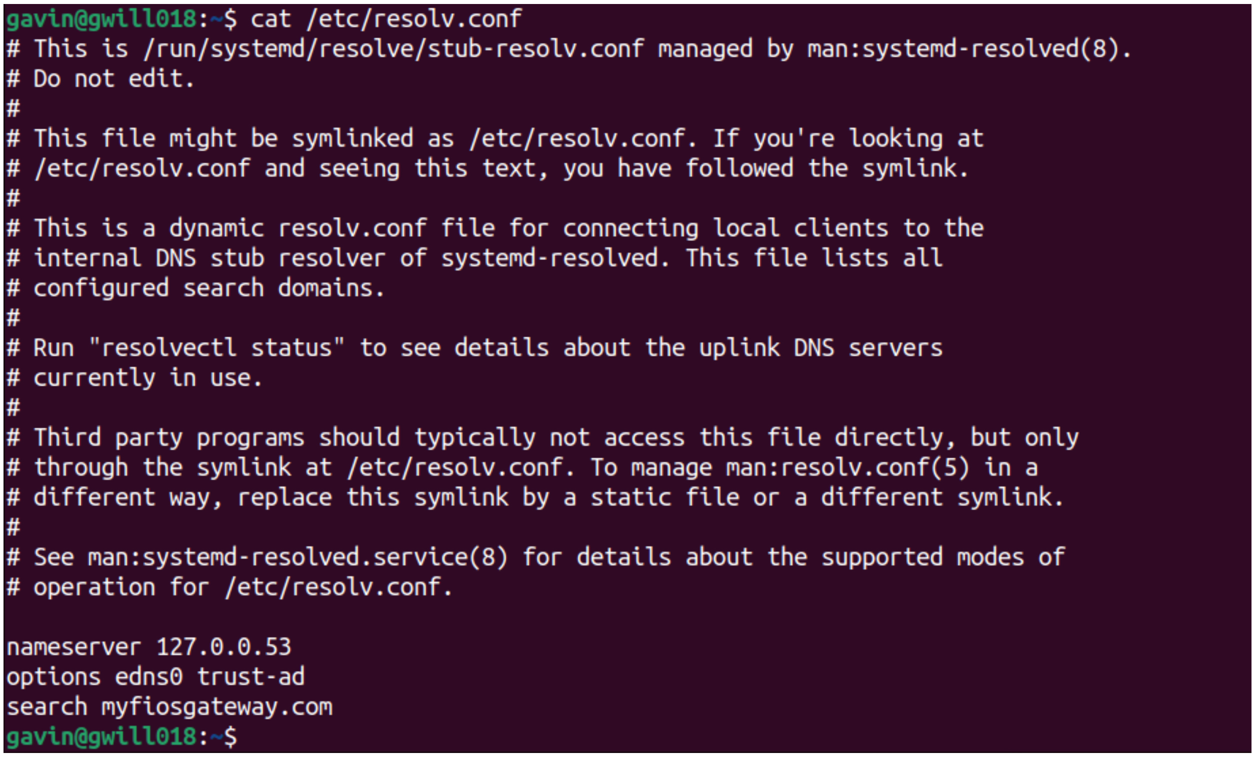
STEP 6



```
gavin@gwill018:~$ cat /etc/hostname
gwill018
gavin@gwill018:~$
```

There is no change when looking at the hostname file.

STEP 7



```
gavin@gwill018:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search myfiosgateway.com
gavin@gwill018:~$
```

Lastly there is no change when looking at the resolve config file.