

jta

CYSE 270: Linux System for Cybersecurity

Lab 11 – Basic Network Configurations

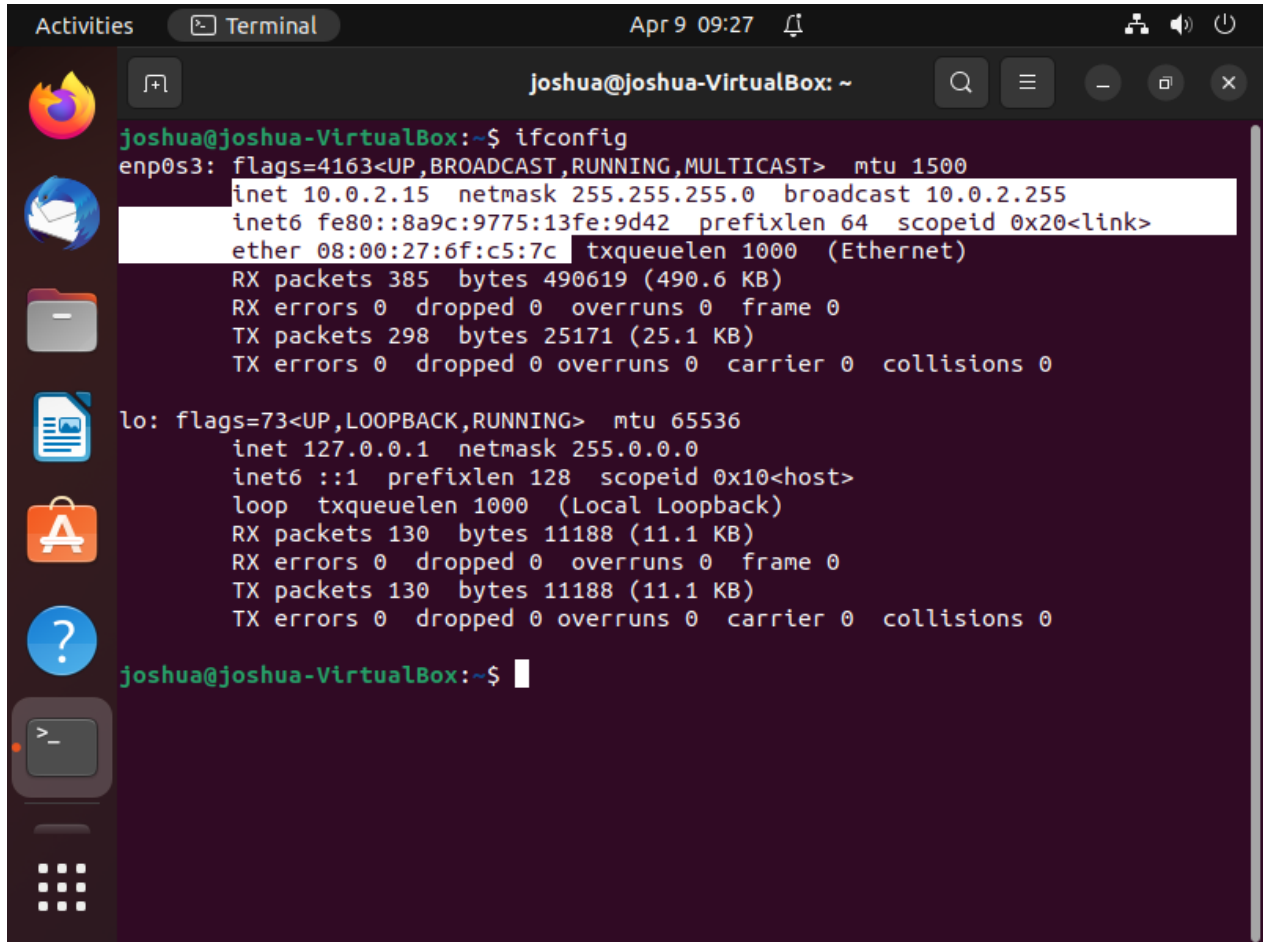
CYSE 270: Linux System for Cybersecurity

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}}}}}}}}

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



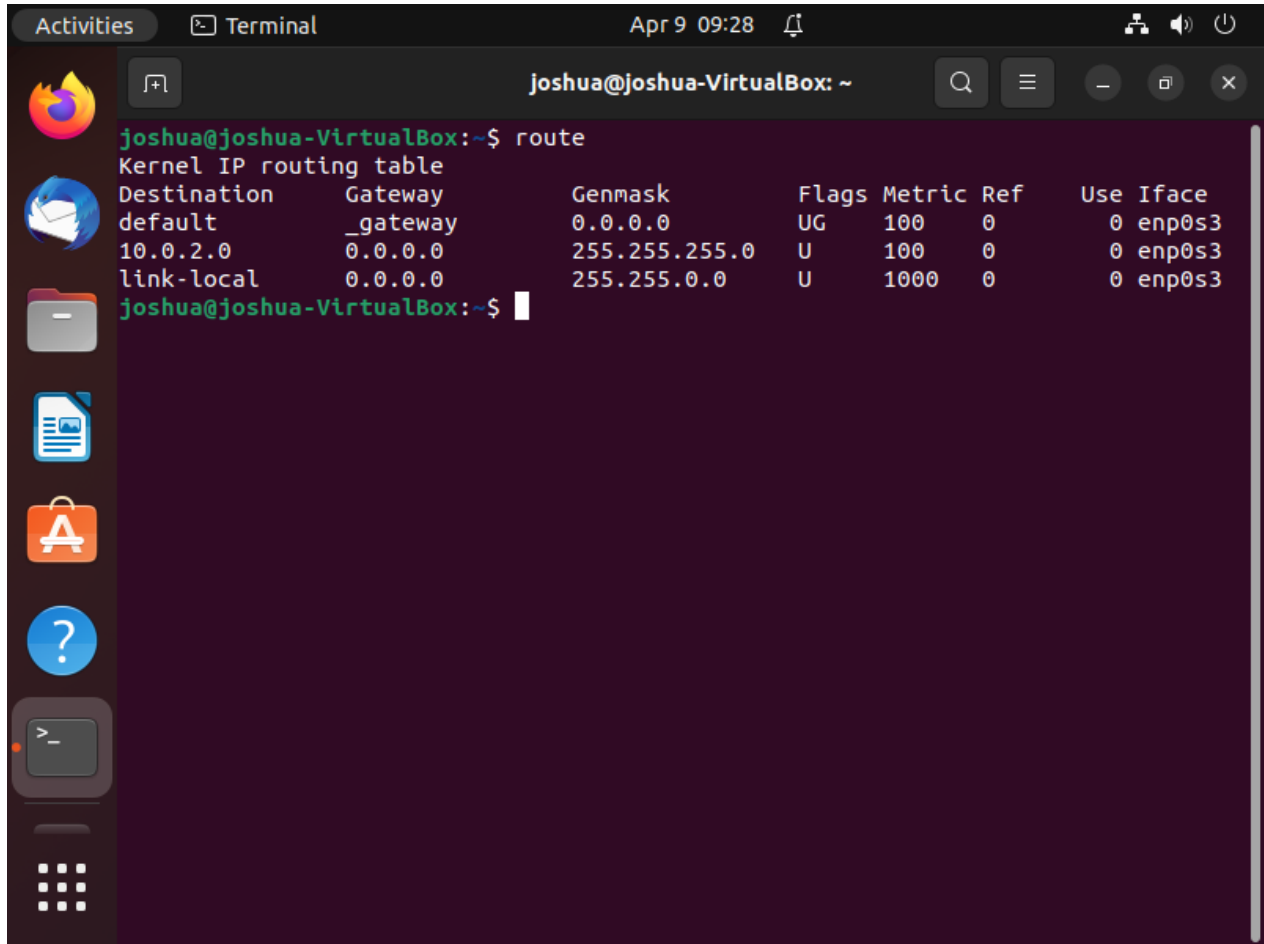
The image shows a terminal window titled "Terminal" with the user "joshua@joshua-VirtualBox: ~". The terminal displays the output of the command "ifconfig". The output is as follows:

```
joshua@joshua-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::8a9c:9775:13fe:9d42 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:6f:c5:7c txqueuelen 1000 (Ethernet)
    RX packets 385 bytes 490619 (490.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 298 bytes 25171 (25.1 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 130 bytes 11188 (11.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 130 bytes 11188 (11.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

joshua@joshua-VirtualBox:~$
```

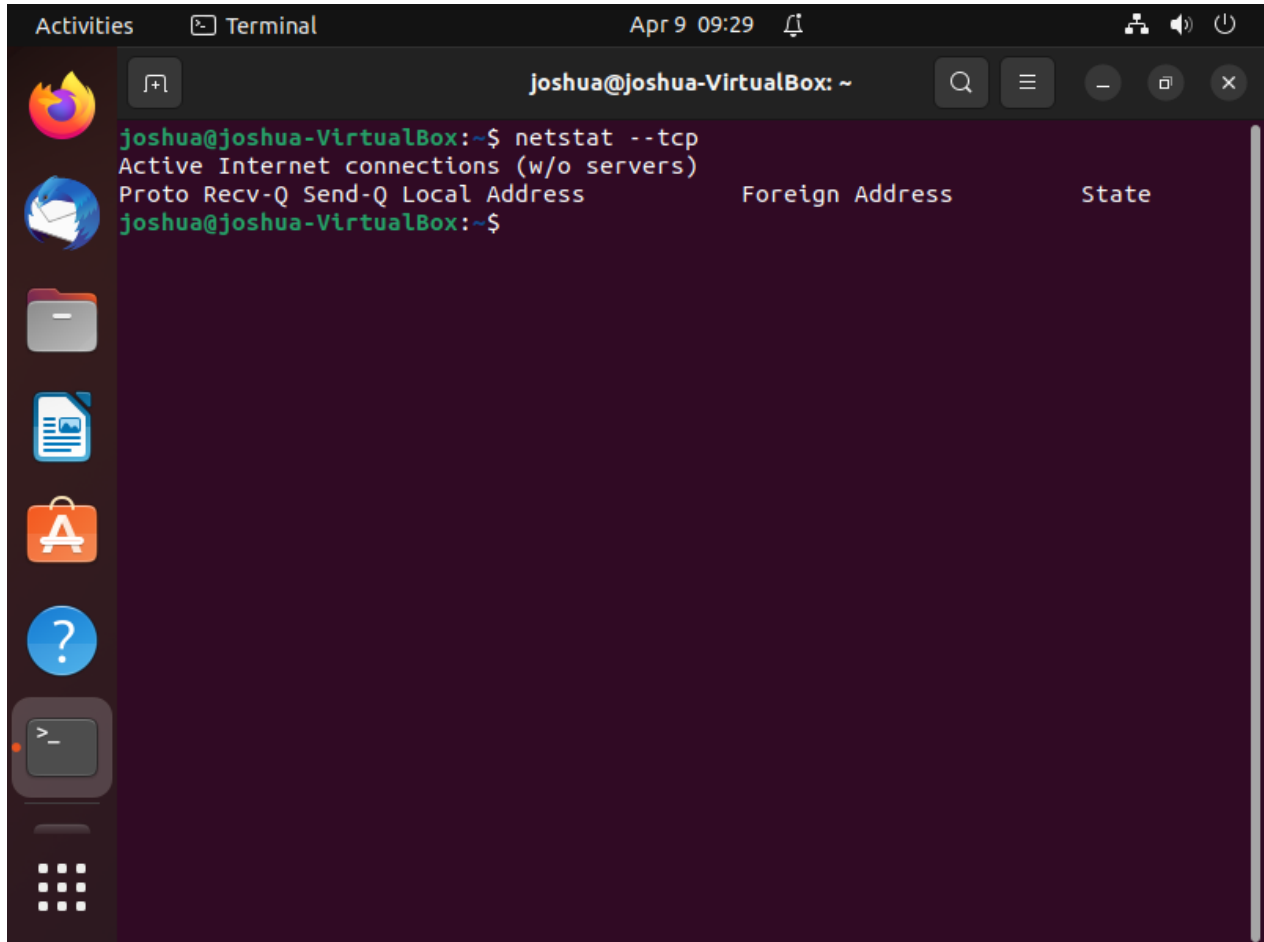
2. Use the correct **route** command to display the current routing table.



The image shows a terminal window titled "Terminal" with the user "joshua@joshua-VirtualBox: ~". The user has executed the command "route", which displays the kernel IP routing table. The output is as follows:

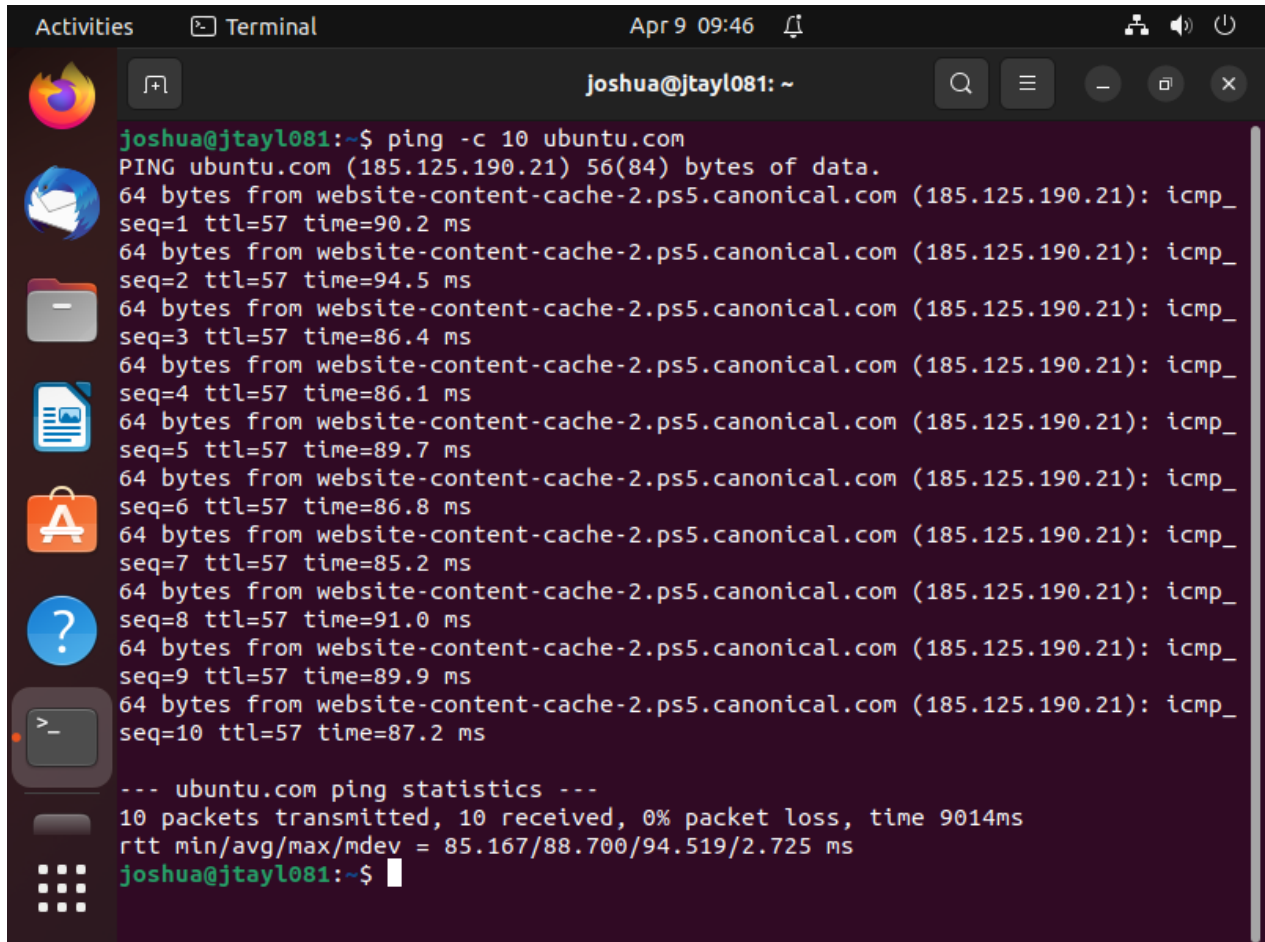
```
joshua@joshua-VirtualBox:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 100 0 0 enp0s3
10.0.2.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3
link-local 0.0.0.0 255.255.0.0 U 1000 0 0 enp0s3
joshua@joshua-VirtualBox:~$
```

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



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

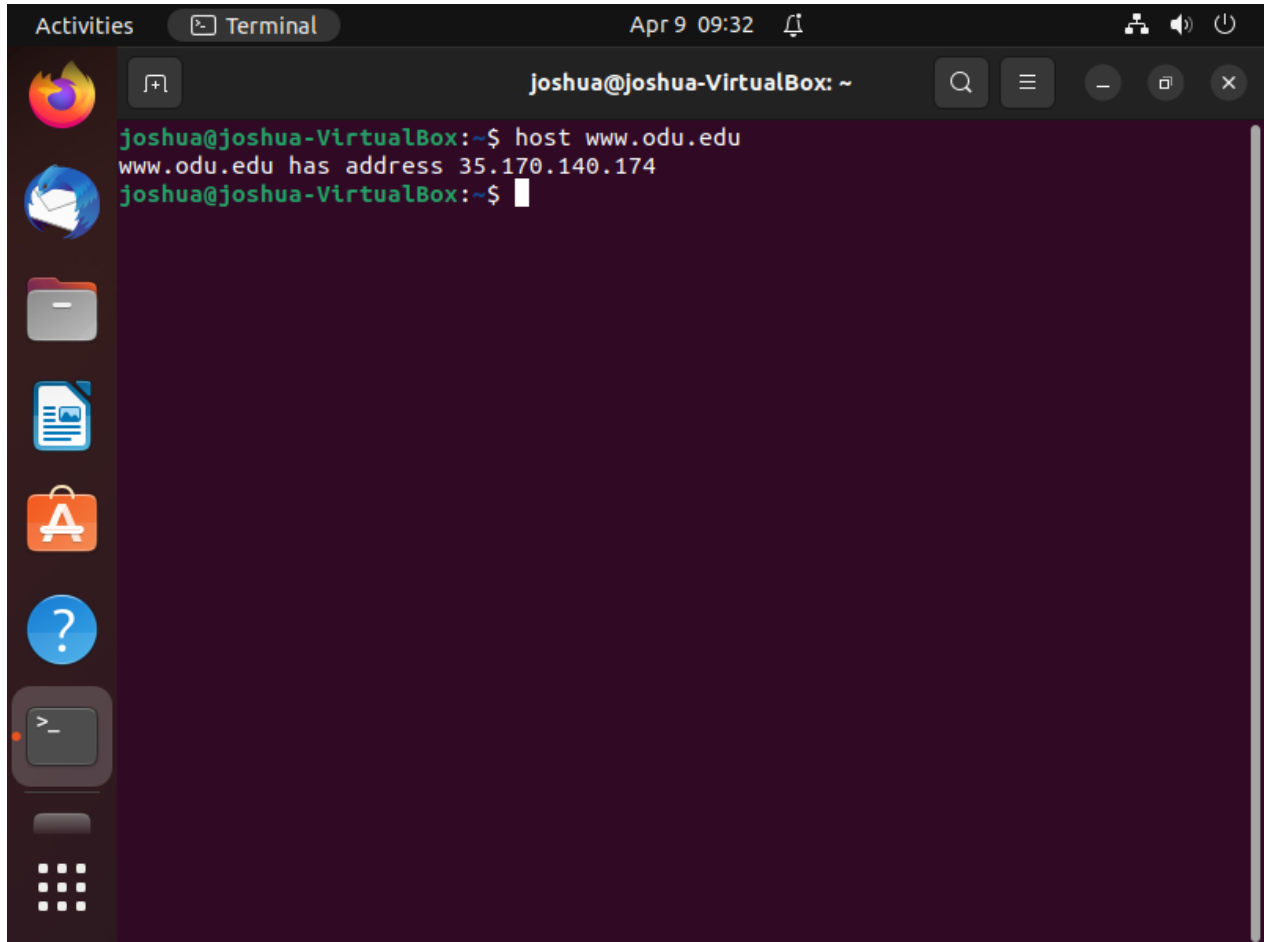
(Use the correct option to send 10 ping requests only.)

A terminal window titled "Terminal" with the user "joshua@jtayl081: ~". The terminal shows the execution of the command "ping -c 10 ubuntu.com". The output displays 10 successful ping requests to the IP address 185.125.190.21, each receiving 64 bytes of data. The response times for each request are: 90.2 ms, 94.5 ms, 86.4 ms, 86.1 ms, 89.7 ms, 86.8 ms, 85.2 ms, 91.0 ms, 89.9 ms, and 87.2 ms. At the end, it shows "ping statistics" for 10 packets transmitted and received with 0% packet loss and a total time of 9014ms. The round-trip times (rtt) are listed as min/avg/max/mdev = 85.167/88.700/94.519/2.725 ms.

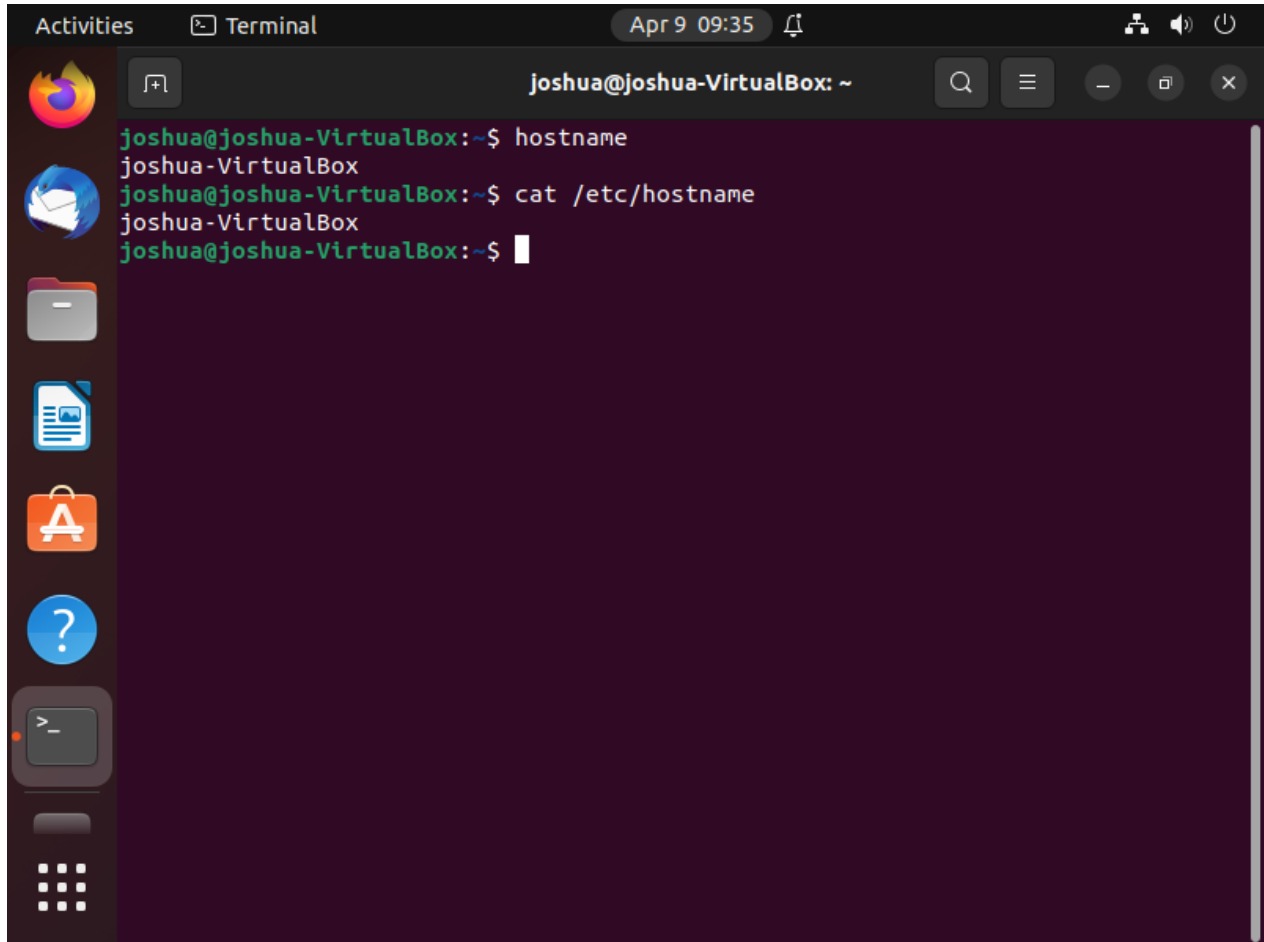
```
joshua@jtayl081:~$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.21) 56(84) bytes of data.
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=1 ttl=57 time=90.2 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=2 ttl=57 time=94.5 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=3 ttl=57 time=86.4 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=4 ttl=57 time=86.1 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=5 ttl=57 time=89.7 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=6 ttl=57 time=86.8 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=7 ttl=57 time=85.2 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=8 ttl=57 time=91.0 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=9 ttl=57 time=89.9 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_
seq=10 ttl=57 time=87.2 ms

--- ubuntu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 85.167/88.700/94.519/2.725 ms
joshua@jtayl081:~$
```

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



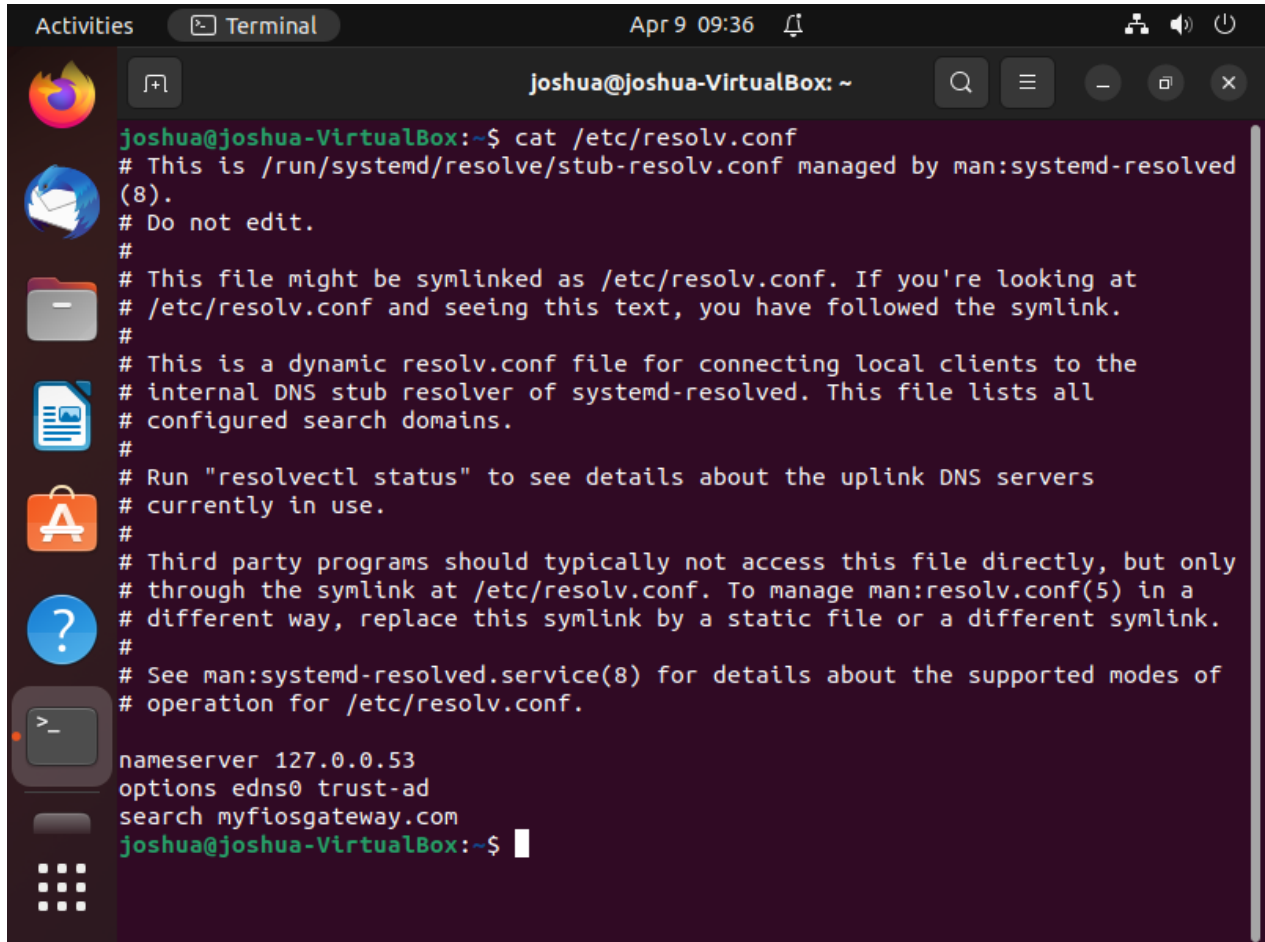
6. Use the **cat** command to display the contents of the file that contains the system's hostname.

A terminal window titled "Terminal" with a dark background. The window shows the following commands and output:

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

The terminal window is part of a desktop environment with a sidebar on the left containing icons for Firefox, Mail, Files, LibreOffice Writer, LibreOffice Impress, a question mark, and a terminal icon. The top of the window shows the system tray with the date "Apr 9 09:35" and system icons for network, volume, and power.

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

A terminal window titled "Terminal" with the user "joshua@joshua-VirtualBox: ~". The terminal shows the command "cat /etc/resolv.conf" and its output. The output consists of several lines of comments and configuration. The comments explain that the file is managed by systemd-resolved, should not be edited, and is a dynamic file for connecting local clients to the internal DNS stub resolver. The configuration lines are: "nameserver 127.0.0.53", "options edns0 trust-ad", and "search myfiosgateway.com".

```
joshua@joshua-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
joshua@joshua-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**.

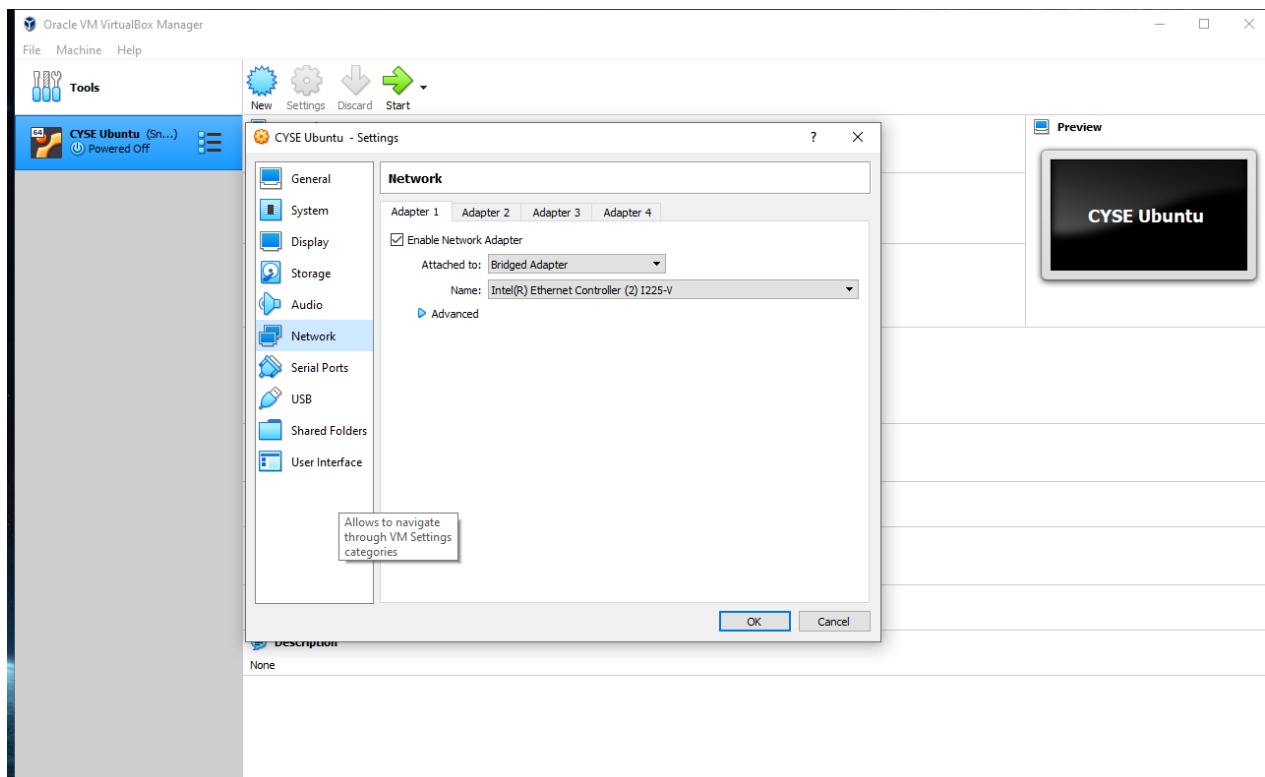
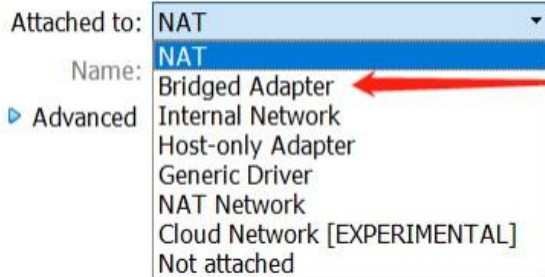
```
Activities Terminal Apr 9 09:42
joshua@joshua-VirtualBox: ~
joshua@joshua-VirtualBox:~$ hostnamectl
Static hostname: joshua-VirtualBox
Icon name: computer
Machine ID: 772f5c885cfe40ee8a8683e72278ea39
Boot ID: 84faaaca6c584d4f98139468b4a70ee4
Virtualization: oracle
Operating System: Ubuntu 22.10
Kernel: Linux 5.19.0-31-generic
Architecture: x86_64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
joshua@joshua-VirtualBox:~$ hostnamectl set-hostname jtayl081
joshua@joshua-VirtualBox:~$ sudo reboot
```

```
Activities Terminal Apr 9 09:43
joshua@jtayl081: ~
joshua@jtayl081:~$
```

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

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

Enable Network Adapter



```
Activities Terminal Apr 9 09:50
joshua@jtayl081: ~
joshua@jtayl081:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.191 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::8a9c:9775:13fe:9d42 prefixlen 64 scopeid 0x20<link>
    inet6 2600:4040:163a:7400:e8e9:446f:58d6:6faa prefixlen 64 scopeid 0x
0<global>
    inet6 2600:4040:163a:7400:c9e3:861a:eb8f:9665 prefixlen 64 scopeid 0x
0<global>
    ether 08:00:27:6f:c5:7c txqueuelen 1000 (Ethernet)
    RX packets 80 bytes 26954 (26.9 KB)
    RX errors 0 dropped 8 overruns 0 frame 0
    TX packets 124 bytes 32790 (32.7 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 113 bytes 10500 (10.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 113 bytes 10500 (10.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

joshua@jtayl081:~$
```

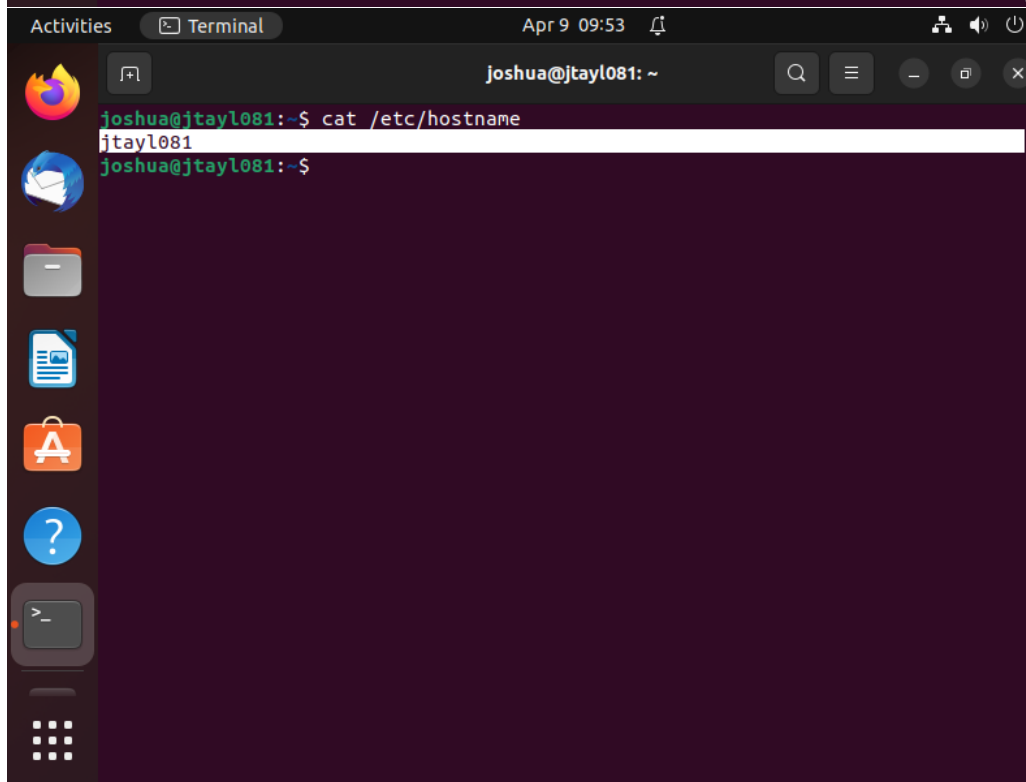
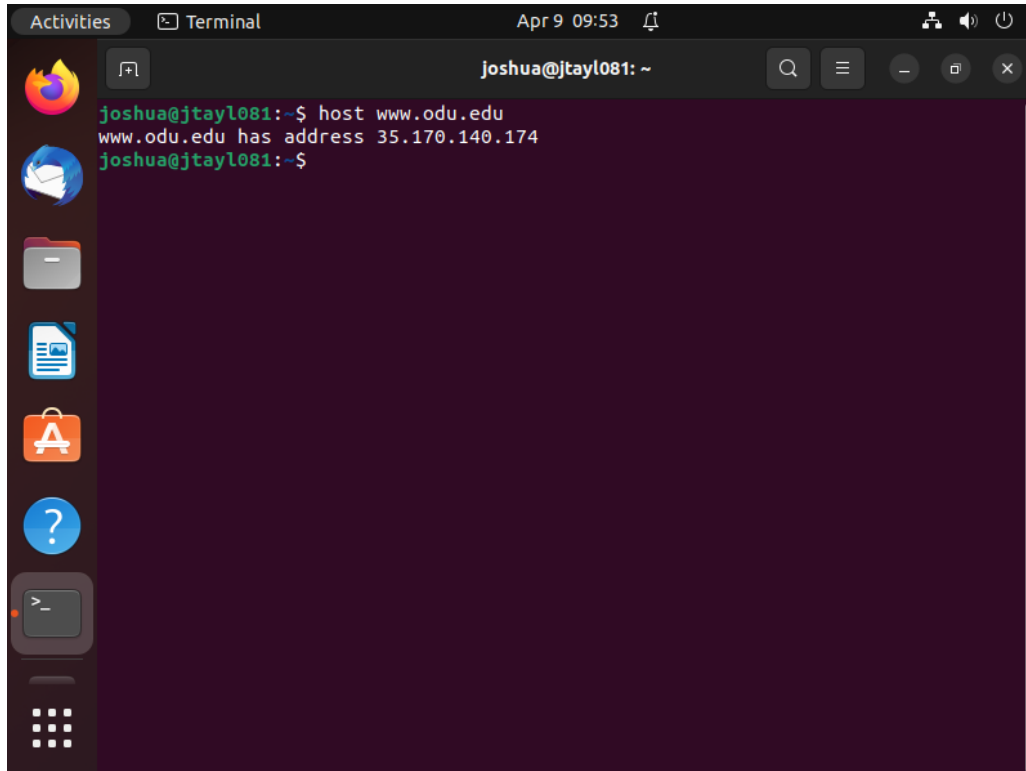
```
Activities Terminal Apr 9 09:51
joshua@jtayl081: ~
joshua@jtayl081:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default G3100.myfiosgat 0.0.0.0 UG 100 0 0 enp0s3
link-local 0.0.0.0 255.255.0.0 U 1000 0 0 enp0s3
192.168.1.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3

joshua@jtayl081:~$
```

```
Activities Terminal Apr 9 09:51
joshua@jtayl081: ~
joshua@jtayl081:~$ netstat --tcp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
joshua@jtayl081:~$
```

```
Activities Terminal Apr 9 09:52
joshua@jtayl081: ~
joshua@jtayl081:~$ 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=56 time=87.6 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=2 ttl=56 time=86.3 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=3 ttl=56 time=85.3 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=4 ttl=56 time=82.3 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=5 ttl=56 time=86.3 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=6 ttl=56 time=84.0 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=7 ttl=56 time=85.4 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=8 ttl=56 time=82.4 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=9 ttl=56 time=85.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_
seq=10 ttl=56 time=84.5 ms

--- ubuntu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 82.336/84.998/87.573/1.620 ms
joshua@jtayl081:~$
```



Activities Terminal Apr 9 09:54

Terminal window: joshua@jtayl081: ~

```
joshua@jtayl081:~$ 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
joshua@jtayl081:~$
```