M5 Lab: Network Layer (Part 2)

CITA 220: DATA COMM & NETWORK TECH

Gonzalez, Marco A.
SUNY CANTON | 34 CORNELL DRIVE, CANTON, NEW YORK 13617

TABLE OF CONTENTS

1 TABLE OF FIGURES

2 PREPARATION

If you do not have access to a Windows computer but can run a virtual machine on your computer, you can download a Windows 10 virtual machine from here. Set the VM network setting to **Bridged Adapter**. Launch a Windows command prompt. Start CITA 220 VM. Log in and launch a Terminal program.

3 WINDOWS

3.1 IP ADDRESS/SUBNET MASK/DEFAULT GATEWAY

The ipconfig command with the /all switch displays the IP address, subnet mask, and default gateway information. See Figure 1.

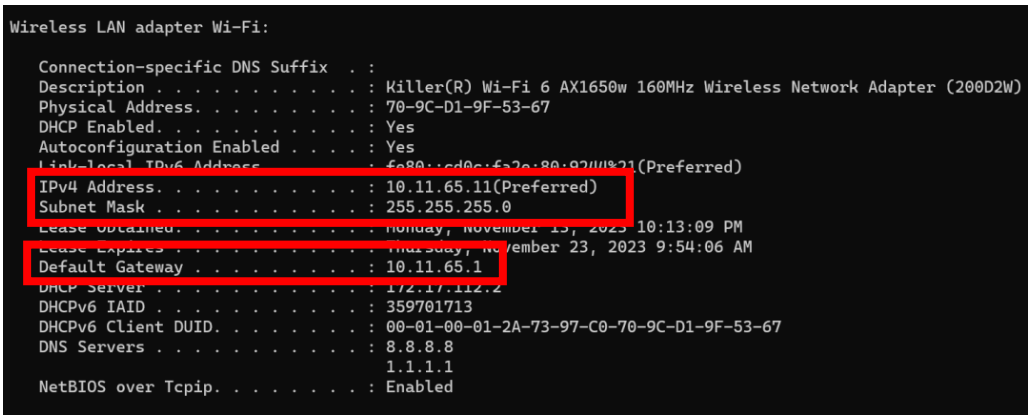

Figure 1. IP Address, Subnet Mask, and Default Gateway

The IP address and the subnet mask are used to identify the network ID of the IP (logical) network on which the computer resides. The default gateway IP address is the network interface address of one of the router ports with the same network ID as the computer's network ID. The router is the entry and exit points into and out of the IP network on which the computer resides. Without the default gateway address configured, the computer cannot communicate with other devices on other IP networks. (The computer can still communicate with other devices that reside on the same IP network.)

3.2 Domain Name System (DNS)

The domain name system is a mechanism to translate (convert) network device names into IP addresses and vice versa. The ipconfig command with the /all switch is used to display the current DNS information. See Figure 2.

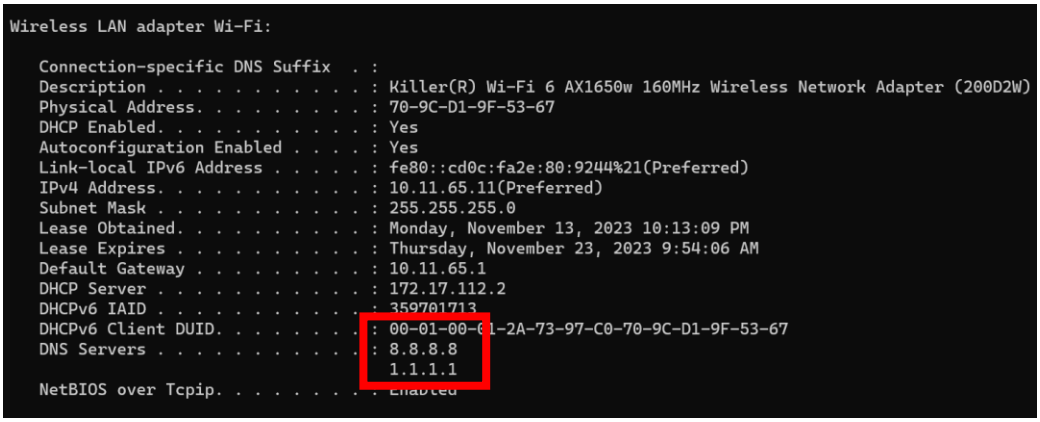

Figure 2. DNS Server Addresses

The annotated IP addresses are the DNS servers' IP addresses that the computer queries (asks) to translate device names into the corresponding IP addresses. Usually, more than one IP address is defined for redundancy since the computer cannot communicate with other devices if it cannot access at least one of the DNS servers.

3.2.1 Manually Querying a DNS Server

Although the computer queries the DNS server without the user's intervention, the user can manually query a DNS server. Manually querying is useful to test whether the computer can access the DNS server. The **nslookup** command is used to perform the query. In this example, the user wants to know the IP address of www.amazon.com. See Figure 3. The command output always has two sections. The first section shows which DNS server was queried. The second section shows the IP address of www.amazon.com. When a DNS server translates a device name into an IP address, it is said to be a DNS **forward resolution** (lookup).

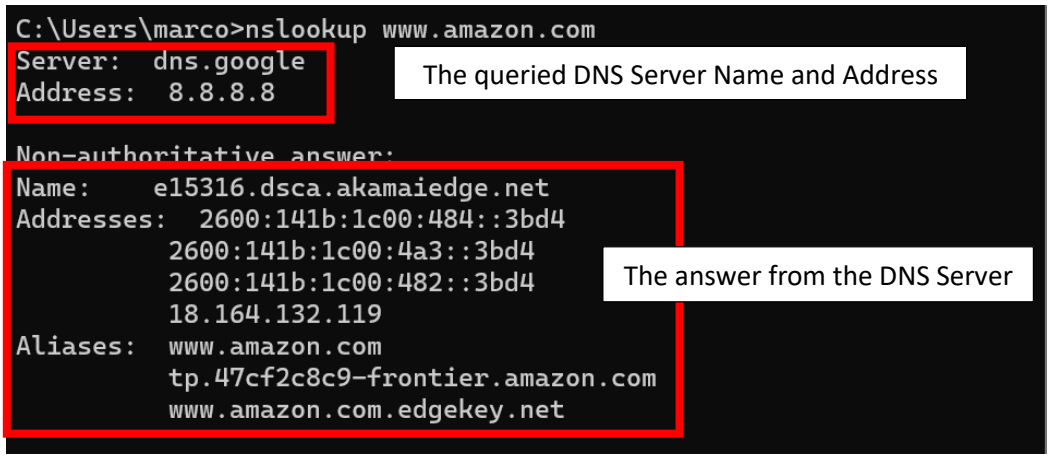

Figure 3. DNS Forward Resolution Query

The nslookup command can be used to query the name of the device from its IP address. This query type is called a DNS reverse resolution (lookup). See Figure 4. In this example, the IP address obtained in Figure 3 is used to query the device name. Notice that the returned name is not www.amazon.com. This is because a network device can have more than one name, and the DNS reverse resolution record on the DNS may not be up-to-date. Therefore, reverse resolutions may be unreliable. Forward resolutions are usually reliable.

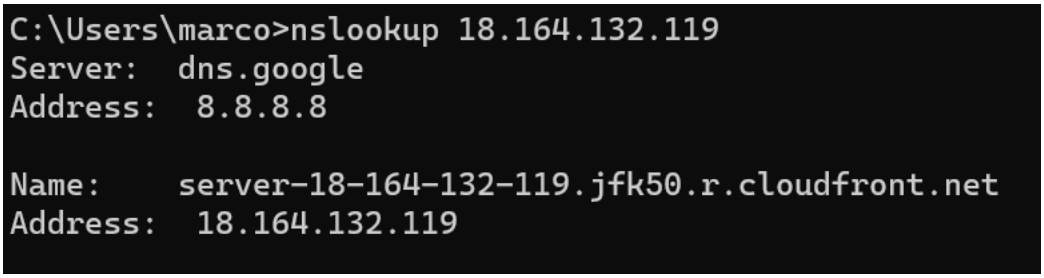

Figure 4. DNS Reverse Resolution Query

3.3 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a mechanism to manage network settings such as IP addresses, subnet masks, default gateway address, and DNS server addresses on multiple computers remotely to reduce the amount of manual system administration work. The ipconfig command with the /all switch is used to display if the computer is using DHCP to configure its network settings. See Figure 5. There is three DHCP information:

1. Whether the DHCP is enabled or not.
2. DHCP lease date information
3. DHCP server address

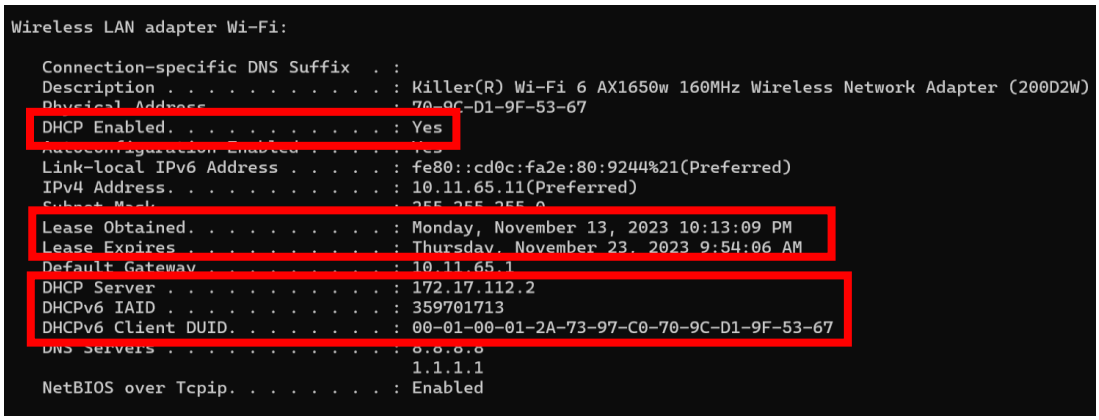

Figure 5. DHCP Configuration Information

A **DHCP server** provides network settings to computers (**DHCP clients**). The settings are provided temporarily (**leased**); therefore, the settings expire after a time duration set by the system administrator.

The DHCP network settings can be returned to the DHCP server manually. They can also be obtained from the DHCP server manually. The ipconfig command with the **/release** switch returns the settings to the DHCP server. See Figure 6. Notice IPv4 address disappeared.

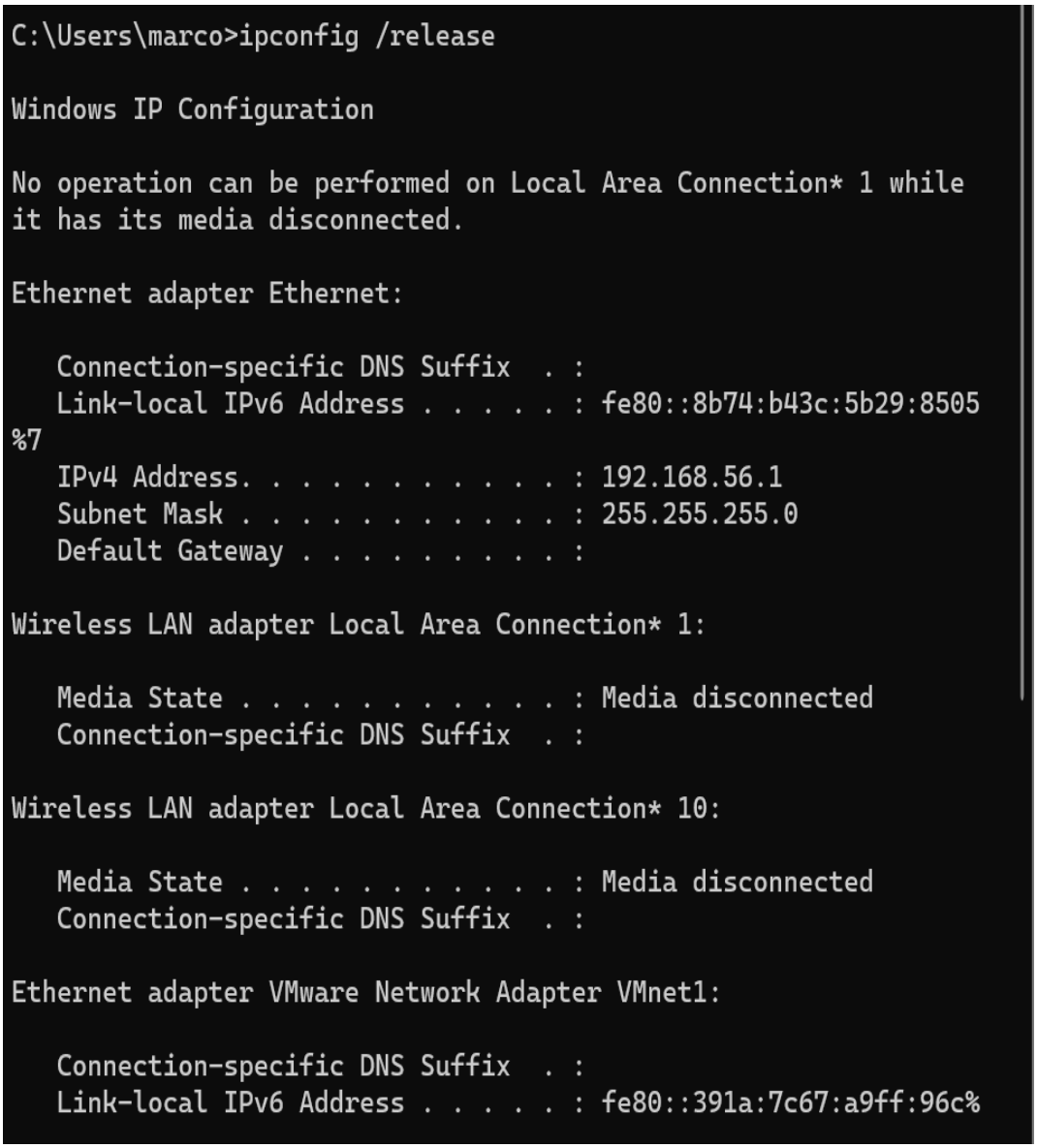

Figure 6. The ipconfig /release Command

The ipconfig command with the **/renew** switch is used to obtain network settings from a DHCP server. See Figure 7. Notice that the IPv4 address is restored.

```
C:\Users\marco>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its
media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its
 media disconnected.

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8b74:b43c:5b29:8505%7
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::391a:7c67:a9ff:96c%10
   IPv4 Address. . . . . . . . . . . : 192.168.29.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:
```

Figure 7. The ipconfig /renew Command

3.4 PING

The **ping** command is used to check the logical network connectivity between two network devices. If the device that has executed the ping command receives *Reply* messages, then the connectivity is established. See Figure 8. If *Request time out* messages are received instead, then the result is inconclusive. See Figure 9.

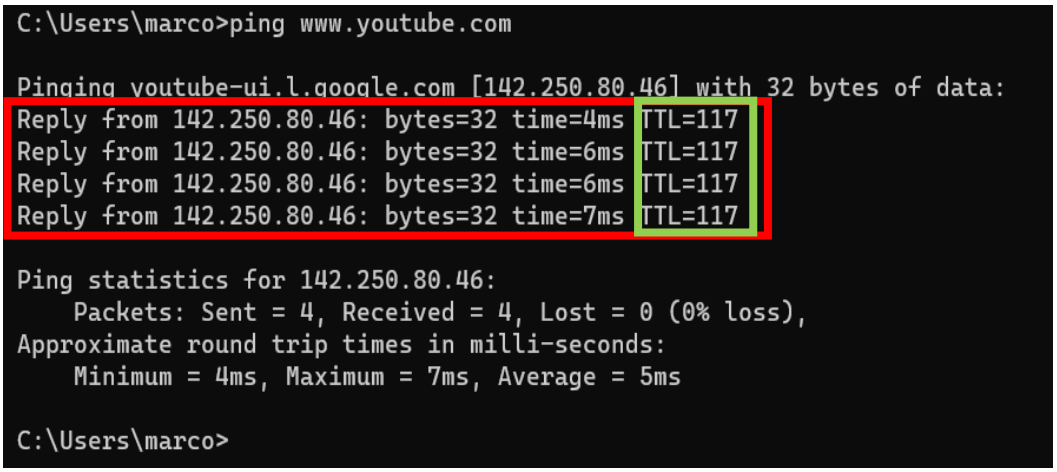

Figure 8. The ping Command is Successful

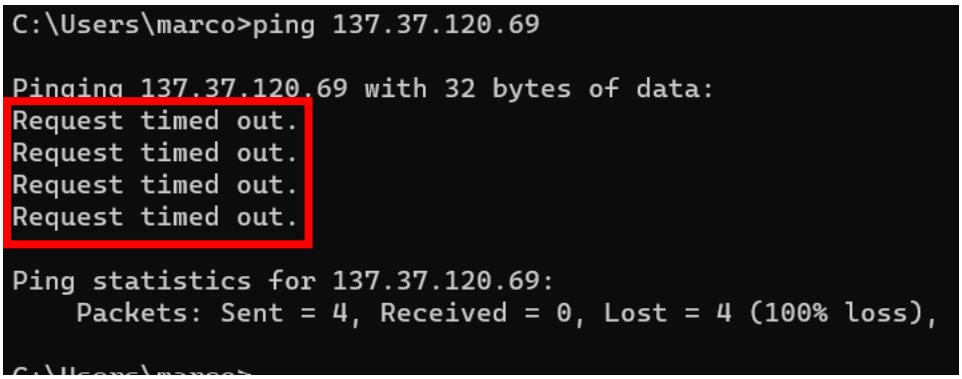

Figure 9. The ping Command is Unsuccessful

3.5 TRACERT

The **tracert** (trace route) command is used to identify routers (hops) that are between the network devices. See Figure 10. Notice ten routers are identified.

```
C:\Users\marco>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.250.80.46]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  10.11.65.1
  2     5 ms     2 ms     2 ms  454ad511.cst.lightpath.net [69.74.213.17]
  3     6 ms     3 ms     3 ms  10.193.204.199
  4     5 ms     3 ms     3 ms  10.249.88.100
  5     6 ms     5 ms     4 ms  64.15.3.144
  6     6 ms     4 ms     4 ms  rtr3-tg10-1.wan.whplny.cv.net [64.15.0.42]
  7     8 ms    16 ms     6 ms  72.14.215.203
  8     7 ms     4 ms     4 ms  142.251.67.163
  9     7 ms     4 ms     4 ms  142.251.65.99
 10     6 ms     4 ms     4 ms  lga34s34-in-f14.1e100.net [142.250.80.46]

Trace complete.
```

Figure 10. The tracert Command

3.6 ROUTING

Every network device has a **routing table** in its RAM to determine the best path to the destination network. The route command with the print switch displays the routing table. See Figure 11. Notice that the destination network ID 0.0.0.0 and the subnet mask 0.0.0.0 mean the default gateway.

```
C:\Users\marco>route print
===========================================================================
Interface List
  7...0a 00 27 00 00 07 ......VirtualBox Host-Only Ethernet Adapter
 17...70 9c d1 9f 53 68 ......Microsoft Wi-Fi Direct Virtual Adapter
  4...72 9c d1 9f 53 67 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 13...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 21...70 9c d1 9f 53 67 ......Killer(R) Wi-Fi 6 AX1650w 160MHz Wireless Net
work Adapter (200D2W)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.11.65.1      10.11.65.11     35
       10.11.65.0    255.255.255.0         On-link      10.11.65.11    291
      10.11.65.11  255.255.255.255         On-link      10.11.65.11    291
     10.11.65.255  255.255.255.255         On-link      10.11.65.11    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.29.0    255.255.255.0         On-link      192.168.29.1    291
     192.168.29.1  255.255.255.255         On-link      192.168.29.1    291
   192.168.29.255  255.255.255.255         On-link      192.168.29.1    291
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
    192.168.245.0    255.255.255.0         On-link     192.168.245.1    291
    192.168.245.1  255.255.255.255         On-link     192.168.245.1    291
  192.168.245.255  255.255.255.255         On-link     192.168.245.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link       10.11.65.11    291
        224.0.0.0        240.0.0.0         On-link     192.168.245.1    291
```

Figure 11. The route Command

4 LINUX

4.1 ADDRESS/SUBNET MASK/DEFAULT GATEWAY

The **ifconfig** and **ip address** commands are used to display the IP address, subnet mask, and default gateway information. See Figure 12 and Figure 13. Unlike the Windows ipconfig command, they do not display the default gateway, DNS servers, or DHCP information.

```
$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.11.65.141  netmask 255.255.255.0  broadcast 10.11.65.255
        inet6 fe80::8d2b:1d51:9e04:e378  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b9:82:41  txqueuelen 1000  (Ethernet)
        RX packets 9156  bytes 13397115 (13.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1270  bytes 119131 (119.1 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 296  bytes 26604 (26.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 296  bytes 26604 (26.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 12. The ifconfig Command

```
$ ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 10.11.65.141/24 brd 10.11.65.255 scope global dynamic noprefixroute enp0s3
       valid_lft 1581sec preferred_lft 1581sec
```

Figure 13. The ip Command

4.2 Domain Name System (DNS)

The DNS servers' IP addresses are stored in the **/etc/resolv.conf**. See Figure 14.

```
$ 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 .
```

Figure 14. The /etc/resolv.conf File

The **nslookup** and **dig** commands are used to query a DNS server. See Figure 15 and Figure 16.

```
$ nslookup www.amazon.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.amazon.com  canonical name = tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com        canonical name = d3ag4hukkh62yn.cloudfront.net.
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 18.238.58.131
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:f200:7:49a5:5fd2:8621
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:e200:7:49a5:5fd2:8621
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:7400:7:49a5:5fd2:8621
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:d000:7:49a5:5fd2:8621
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:f000:7:49a5:5fd2:8621
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:f400:7:49a5:5fd2:8621
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:e600:7:49a5:5fd2:8621
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:2511:d600:7:49a5:5fd2:8621
```

Figure 15. The nslookup Command

```
$ dig www.amazon.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> www.amazon.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35696
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.amazon.com.                        IN      A

;; ANSWER SECTION:
www.amazon.com.         91      IN      CNAME   tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com. 58 IN CNAME   d3ag4hukkh62yn.cloudfront.net.
d3ag4hukkh62yn.cloudfront.net. 60 IN    A       18.164.132.119

;; Query time: 23 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Nov 17 22:58:41 EST 2023
;; MSG SIZE  rcvd: 138
```

Figure 16. The dig Command

4.3 Dynamic Host Configuration Protocol (DHCP)

On the Linux system, there is no standard method to display the DHCP server information. The **dhclient** command with the **-r** option is used to release the current network settings to the DHCP server. See Figure 17.

```
$ ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 10.11.65.141/24 brd 10.11.65.255 scope global dynamic noprefixroute enp0s3
       valid_lft 767sec preferred_lft 767sec
(11/17 23:02:20) student@cita220-vm: ~
$ sudo dhclient -r
[sudo] password for student:
(11/17 23:02:32) student@cita220-vm: ~
$ ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
```

The enp0s3 interface is gone.

Figure 17. The dhclient -r Command

The dhclient command is used again without arguments to renew the settings from a DHCP server. See Figure 18.

```
$ ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
(11/17 23:08:15) student@cita220-vm: ~
$ sudo dhclient
(11/17 23:08:24) student@cita220-vm: ~
$ ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 10.11.65.20/24 brd 10.11.65.255 scope global dynamic enp0s3
       valid_lft 1794sec preferred_lft 1794sec
```

Figure 18. The dhclient Command

4.4 PING

The ping command is used to check the logical connectivity between two network devices. Unlike the Windows ping command, the Linux ping command does not stop automatically. To stop after a few responses, press the Control+C to terminate the command or use the **-c** option to limit the number of tests. See Figure 19. In this example the ping command stops after receiving four responses.

```
$ ping -c 4 www.youtube.com
PING youtube-ui.l.google.com (142.250.80.46) 56(84) bytes of data.
64 bytes from lga34s34-in-f14.1e100.net (142.250.80.46): icmp_seq=1 ttl=117 time=5.22 ms
64 bytes from lga34s34-in-f14.1e100.net (142.250.80.46): icmp_seq=2 ttl=117 time=5.91 ms
64 bytes from lga34s34-in-f14.1e100.net (142.250.80.46): icmp_seq=3 ttl=117 time=6.80 ms
64 bytes from lga34s34-in-f14.1e100.net (142.250.80.46): icmp_seq=4 ttl=117 time=7.12 ms

--- youtube-ui.l.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 5.215/6.262/7.120/0.748 ms
```

Figure 19. The ping Command

4.5 TRACEROUTE

The traceroute command is used to display the routers between two network devices. Notice the spelling difference between Window's tracert and this command. See Figure 20.

```
$ traceroute www.youtube.com
traceroute to youtube-ui.l.google.com (142.250.80.46), 64 hops max
  1   10.11.65.1  1.443ms  11.468ms  1.403ms
  2   69.74.213.17  2.727ms  2.717ms  2.385ms
  3   10.193.204.199  3.770ms  5.757ms  10.751ms
  4   10.249.88.100  4.372ms  4.295ms  4.385ms
  5   64.15.3.144  5.235ms  4.964ms  6.346ms
  6   64.15.5.70  4.921ms  4.355ms  5.524ms
  7   24.157.15.179  4.893ms  4.661ms  4.469ms
  8   *  *  *
  9   142.250.80.46  7.910ms  5.039ms  5.378ms
```

Figure 20. The traceroute Command

4.6 ROUTING

The **route** and **ip route** commands are used to display the routing table. See Figure 21.

```
$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.11.65.0      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
```

Figure 21. The route and ip route Commands