Study of Basic Networking Commands

Lab Exercises on October 15, 2020

Department of Electronics and Computer Engineering
Pulchowk Campus, Lalitpur

Ashlesh Pandey

PUL074BEX007

Contents

Listings

List of Figures

1 Objectives

- Familiarization with basic networking commands and their uses

2 Requirements

- Computer with internet connectivity

This lab report is prepared based on the networking commands for a Windows OS, more specifically the Windows 10 Home Edition. A list of all the commands used during the lab experiment is presented below:

- ipconfig
- ping
- getmac
- tracert
- arp
- hostname
- netstat
- route

3 Exercises

Problem 1
Explain the following commands briefly with their functions and few syntaxes.

The syntax and options listed in Listing 1 to Listing 8 have been extracted from the command line help with minor changes in the formatting and grammar for ease of understanding.

a. ipconfig

The *ipconfig* command is used to display the IP address, default gateway and the subnet mask of the different adapters on a device that are bound to TCP/IP. Listing 1 shows the syntax along with the options for the *ipconfig* command.

```
Usage:
ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]
where
    adapter             Connection name
                       (wildcard characters * and ? allowed)
```

```
Options:
       /all              Display all the configuration information.
       /release          Release the IPv4 address.
       /release6         Release the IPv6 address.
       /renew            Renew the IPv4 address.
       /renew6           Renew the IPv6 address.
       /flushdns         Flushes the DNS Resolver cache.
       /registerdns      Refreshes all DHCP leases and re-registers DNS names.
       /displaydns       Display the contents of the DNS Resolver Cache.
       /showclassid      Displays all the DHCP class IDs.
       /showclassid6     Displays all the IPv6 DHCP class IDs.
       /setclassid       Modifies the DHCP class id.
       /setclassid6      Modifies the IPv6 DHCP class id.
```

Listing 1: Syntax for ipconfig

b. ping

The *ping* command is used to check the ability of the source system to reach a destination. It works by sending out an ICMP echo request to the destination and waits for a response. Listing 2 shows the syntax along with the options for the *ping* command.

```
Usage:
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
    -a             Resolve addresses to hostnames.
    -n count       Specifies number of echo requests to transmit.
    -l size        Transmit buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force system to use IPv4.
    -6             Force system to use IPv6.
```

Listing 2: Syntax for ping

c. getmac

The *getmac* command is used to display the MAC address, also known as the physical address of the different network adapters on a device. Listing 3 shows the syntax along with the options for the *getmac* command.

```
Usage:
getmac [/S system [/U username [/P [password]]]] [/FO format] [/NH] [/V]

Options:
    /S      system              Specifies the remote system to connect to.

    /U      [domain\]user       Specifies the user context under
                                which the command should execute.

    /P      [password]          Specifies the password for the given
                                user context. Prompts for input if omitted.

    /FO     format              Specifies the format in which the output
                                is to be displayed.
                                Valid values: "TABLE", "LIST", "CSV".

    /NH                         Specifies that the "Column Header" should
                                not be displayed in the output.
                                Valid only for TABLE and CSV formats.

    /V                          Specifies that verbose output is displayed.
```

Listing 3: Syntax for getmac

d. tracert

The *tracert* command is used to display the details of the path taken by a packet to complete a connection to specified destination. In short, it traces the route of a packet from source to destination. Listing 4 shows the syntax along with the options for the *tracert* command.

```
Usage:
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for requested target.
    -j host-list        Loose source route along host-list (IPv4-only).
    -w timeout          Timeout in millisecond to wait for each reply.
    -R                  Trace round-trip path (IPv6-only).
    -S srcaddr          Source address to use (IPv6-only).
    -4                  Force system to use IPv4.
    -6                  Force system to use IPv6.
```

Listing 4: Syntax for tracert

e. arp

The *arp* command is used to display and change the ARP(Address Resolution Protocol) cache. ARP uses an IP-to-Physical address translation table to map IP addresses to the corresponding MAC addresses. This command is particularly used to know the MAC addresses of various devices that the system has interacted with based on their IP address and hence is useful in locating duplicate IP addresses. Listing 5 shows the syntax along with the options for the *arp* command.

```
Usage:
arp -s inet_addr eth_addr [if_addr]
arp -d inet_addr [if_addr]
arp -a [inet_addr] [-N if_addr] [-v]

Options:
  -a              Displays current ARP entries by interrogating the current
                  protocol data. If inet_addr is specified, the IP and Physical
                  addresses for only the specified computer are displayed. If
                  more than one network interface uses ARP, entries for each ARP
                  table are displayed.
  -v              Displays current ARP entries in verbose mode. All invalid
                  entries and entries on the loop-back interface will be shown.
  inet_addr       Specifies an internet address.
  eth_addr        Specifies a physical address.
  if_addr         If present, this specifies the Internet address of the
                  interface whose address translation table should be modified.
                  If not present, the first applicable interface will be used.
  -N if_addr      Displays the ARP entries for the network interface specified
                  by if_addr.
  -d              Deletes the host specified by inet_addr. inet_addr may be
                  wildcarded with * to delete all hosts.
  -s              Adds the host and associates the Internet address inet_addr
                  with the Physical address eth_addr. The Physical address is
                  given as 6 hexadecimal bytes separated by hyphens. The entry
                  is permanent.
```

Listing 5: Syntax for arp

f. hostname

The *hostname* command is used to display the host name of the device. Listing 6 shows the syntax for the *hostname* command. The command doesn't have any additional options for a Windows environment

```
Usage:
hostname
```

Listing 6: Syntax for hostname

g. netstat

The *netstat* command is used to display the active TCP network connections, protocol statistics for both IPv4 and IPv6 along with the IP routing table and the listening ports. Listing 7 shows the syntax along with the options for the *netstat* command.

```
Usage:
netstat [-a] [-b] [-e] [-f] [-n] [-o]
        [-p proto] [-r] [-s] [-x] [-t] [interval]

Options:
  -a              Displays all connections and listening ports.
  -b              Displays the executable involved in creating each connection
                  or listening port.
  -e              Displays Ethernet statistics. This may be combined with the -s
                  option.
  -f              Displays Fully Qualified Domain Names (FQDN) for foreign
                  addresses.
  -n              Displays addresses and port numbers in numerical form.
  -o              Displays the owning process ID associated with each
                  connection.
  -p proto        Shows connections for the protocol specified by proto; proto
                  may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                  option to display per-protocol statistics, proto may be any
                  of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q              Displays all connections, listening ports, and bound
                  nonlistening TCP ports.
  -r              Displays the routing table.
  -s              Displays per-protocol statistics.  By default, statistics are
                  shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                  the -p option may be used to specify a subset of the default.
  -t              Displays the current connection offload state.
  -x              Displays NetworkDirect connections, listeners, and shared
                  endpoints.
  -y              Displays the TCP connection template for all connections.
                  Cannot be combined with the other options.
  interval        Redisplays selected statistics, pausing interval seconds
                  between each display.
```

Listing 7: Syntax for netstat

h. route

The *route* command is used to display and manipulate the route informatons on a device. Printing, adding, deleting, or modifying a route is possible using the various command options for *route* command. Listing 8 shows the syntax along with the options for the *route* command.

```
Usage:
route [-f] [-p] [-4|-6] command [destination]
      [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

Options:
  -f              Clears the routing tables of all gateway entries.
  -p              When used with the ADD command, makes a route persistent across
                  boots of the system. By default, routes are not preserved
                  when the system is restarted. Ignored for all other commands,
```

```
                which always affect the appropriate persistent routes.
-4              Force system to use IPv4.
-6              Force system to use IPv6.
command         One of these:
                  PRINT     Prints a route
                  ADD       Adds   a route
                  DELETE    Deletes a route
                  CHANGE    Modifies an existing route
destination     Specifies the host.
netmask         Specifies a subnet mask value for this route entry.
                If not specified, it defaults to 255.255.255.255.
gateway         Specifies gateway.
interface       The interface number for the specified route.
METRIC          Specifies that the next parameter is the 'metric' value.
MASK            Specifies that the next parameter is the 'netmask' value.
```

Listing 8: Syntax for route

Problem 2

Note down the observation of each steps performed during the experiment along with necessary commands and also comment on it.

a. Using ipconfig

```
Windows IP Configuration


Unknown adapter VPN - VPN Client:

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

Ethernet adapter Ethernet 3:

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

Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d94a:5427:b7ca:594a%6
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network #3:

   Connection-specific DNS Suffix  . :
```

```
   Link-local IPv6 Address . . . . . : fe80::c8fa:6525:b46c:39db%13
   IPv4 Address. . . . . . . . . . . : 192.168.99.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : domain.name
   Link-local IPv6 Address . . . . . : fe80::509d:f9df:2bd5:9ab%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.19
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%9
                                       192.168.1.1
```

Listing 9: Observation for ipconfig

Listing 9 shows the observation for *ipconfig*. The IP addresses, subnet mask, and default gateways are displayed when the command is executed. There are multiple network adapters on the system, all of which are seen in the listing. The wireless LAN adapter is the one of concern in this observation since the system is connected to the internet via the Wi-Fi adapter. The IPv4 address of the adapter is 192.168.1.19 with the default gateway 192.168.1.1, which will be useful in further observations.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-QLRVLCUC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : domain.name

Unknown adapter VPN - VPN Client:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VPN Client Adapter - VPN
   Physical Address. . . . . . . . . : 5E-58-40-0A-AB-E1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-NordVPN Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-80-4F-8A-C2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

```
Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet
   Adapter #2
   Physical Address. . . . . . . . . : 0A-00-27-00-00-06
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d94a:5427:b7ca:594a%6(
   Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 772407335
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-A2-DC-F7-00-E1-8C
   -85-84-D2
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VirtualBox Host-Only Network #3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet
   Adapter #3
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c8fa:6525:b46c:39db%13(
   Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.99.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 906625063
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-A2-DC-F7-00-E1-8C
   -85-84-D2
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : domain.name
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC
   7265
```

```
   Physical Address. . . . . . . . . : 6E-76-04-C6-70-57
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::509d:f9df:2bd5:9ab%9(
   Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.19(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, October 31, 2020
   11:03:18 AM
   Lease Expires . . . . . . . . . . : Sunday, November 1, 2020
   11:03:16 AM
   Default Gateway . . . . . . . . . : fe80::1%9
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 158234116
   DHCPv6 Client DUID. . . . . . . . : 00-03-00-01-6E-76-04-C6-70-57
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
                                       fe80::1%9
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Listing 10: Observation for ipconfig/all

Listing 10 shows the observation for *ipconfig/all*. The */all* option for the *ipconfig* command displays additional informations about the various network adapters on the system. For instance, the descriptive name, physical address, DHCP status, autoconfiguration status, DNS servers and more for each adapter are displayed in addition to the original observation in Listing 9.

b. Using ping

```


Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

Listing 11: Observation for ping to default gateway

As discussed earlier, the *ping* command tests the ability of a source to reach a destination. In Listing 11 the system is pinging the default gateway, i.e. 192.168.1.1 which was previously observed in Listing 9. The statistics such as number of packets sent and received before timeout, approximate round trip time in milliseconds for the packet to reach from the source address to the default gateway address is displayed. It is obvious that this link will have less RTT, which can also be observed in the Listing 11.

```
Pinging vianet.com.np [110.44.112.54] with 32 bytes of data:
Reply from 110.44.112.54: bytes=32 time=4ms TTL=61
Reply from 110.44.112.54: bytes=32 time=3ms TTL=61
Reply from 110.44.112.54: bytes=32 time=5ms TTL=61
Reply from 110.44.112.54: bytes=32 time=2ms TTL=61

Ping statistics for 110.44.112.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

Listing 12: Observation for ping to vianet.com.np

The ISP subscribed while performing this experiment is Vianet Communications Pvt. Ltd. So, pinging their website vianet.com.np gives the observation shown in Listing 12. This link generally takes less RTT since the system has a faster link to the subscribed ISP, which can be verified from the observation.

```
Pinging google.com [172.217.166.46] with 32 bytes of data:
Reply from 172.217.166.46: bytes=32 time=64ms TTL=116
Reply from 172.217.166.46: bytes=32 time=62ms TTL=116
Reply from 172.217.166.46: bytes=32 time=63ms TTL=116
Reply from 172.217.166.46: bytes=32 time=63ms TTL=116

Ping statistics for 172.217.166.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 64ms, Average = 63ms
```

Listing 13: Observation for ping to google.com

Listing 13 shows the observation for pinging google.com website. The number of packets sent, received and lost along with the estimated RTT is shown in the observation, and clearly the RTT is higher than that with the default gateway and ISP.

```
Pinging 103.5.150.3 with 32 bytes of data:
Reply from 103.5.150.3: bytes=32 time=10ms TTL=59
Reply from 103.5.150.3: bytes=32 time=4ms TTL=59
Reply from 103.5.150.3: bytes=32 time=2ms TTL=59
Reply from 103.5.150.3: bytes=32 time=2ms TTL=59

Ping statistics for 103.5.150.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 4ms
```

Listing 14: Observation for ping to 103.5.150.3

Listing 14 shows the observation for pinging an IP 103.5.150.3, which is one of the multiple IP addressess owned by Pulchowk Campus. A notable observation here can be made in comparision to Listing 12 and Listing 13, where domain names were used to ping the server. But in fact, the server's IP address was being resolved which was truly being pinged. So, a ping to either the actual server IP or a domain name is possible and it is due to the DNS resolution technique used by the process.

c. Using getmac

```
Physical Address    Transport Name
=================   ==========================================
5E-58-40-0A-AB-E1   Media disconnected
6E-76-04-C6-70-57   \Device\Tcpip_{561610EB-9FD5-4441-8D90-A6CE9C6F241D}
00-FF-80-4F-8A-C2   Media disconnected
0A-00-27-00-00-06   \Device\Tcpip_{414ABB4C-7E20-48AE-B9D8-7AB94388A80D}
0A-00-27-00-00-0D   \Device\Tcpip_{72FDE6F9-BA30-482F-8241-9CB2F75E3045}
```

Listing 15: Observation for getmac

Listing 15 shows the observation for *getmac* command. The physical addressess for the various network adapters are displayed. The same addresses are also observed in the Listing 10 under individual adapter section.

d. Using tracert

```
Tracing route to 192.168.1.1 over a maximum of 30 hops

  1     7 ms     3 ms     2 ms  192.168.1.1

Trace complete.
```

Listing 16: Observation for tracert to default gateway

Listing 16 shows the observation for *tracert* to the default gateway. It is obvious that this should complete in one hop since a gateway is essentially one hop away from the IP address of the system. This is verified from the observation as well.

```
Tracing route to vianet.com.np [110.44.112.54]
over a maximum of 30 hops:

  1     4 ms     1 ms     1 ms  192.168.1.1
  2   503 ms     3 ms     1 ms  100.66.0.1
  3    10 ms     6 ms     8 ms  103.10.28.3
  4    19 ms     3 ms     3 ms  110.44.112.54

Trace complete.
```

Listing 17: Observation for tracert to vianet.com.np

Listing 17 shows the observation for *tracert* to the ISPs website, i.e. vianet.com.np. The number of hops taken by a packet leaving a system to reach it's subscribed ISPs website is generally lower than any other websites. This is seen from the observation as well, since the packet only takes 4 hops to reach the destination.

```
Tracing route to google.com [172.217.166.46]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1
  2     1 ms     1 ms     1 ms  100.66.0.1
  3     2 ms     3 ms     2 ms  103.10.29.1
  4     7 ms     5 ms     5 ms  ae0-bg1.vianet.com.np [110.44.112.65]
  5    58 ms    15 ms    11 ms  125.16.219.33
  6    96 ms    73 ms   145 ms  116.119.61.109
  7    59 ms    62 ms    72 ms  72.14.216.192
  8    58 ms    62 ms    59 ms  74.125.252.219
  9    63 ms    64 ms    64 ms  108.170.253.122
 10    66 ms    66 ms    67 ms  209.85.251.242
 11    69 ms    68 ms    70 ms  172.253.68.120
 12   395 ms    64 ms    67 ms  108.170.248.193
 13    67 ms    65 ms    64 ms  108.170.234.209
 14    66 ms    66 ms    66 ms  bom07s18-in-f14.1e100.net
    [172.217.166.46]

Trace complete.
```

Listing 18: Observation for tracert to google.com

Listing 18 shows the observation for *tracert* to google.com. The packet takes 17 hops to reach the destination and as observed, takes a route that passes through the subscribed ISP's subnet before hoping on to another IP to reach the destination.

```
Tracing route to 103.5.150.3 over a maximum of 30 hops

  1     3 ms     1 ms     1 ms  192.168.1.1
  2     8 ms     5 ms     3 ms  100.66.0.1
  3     2 ms     6 ms     2 ms  103.10.28.2
  4    36 ms    18 ms    58 ms  198-32-231-15.setg.net [198.32.231.15]
  5     3 ms     3 ms     5 ms  202.70.93.81
  6     6 ms     6 ms     5 ms  202.70.93.94
  7     3 ms     3 ms     2 ms  202.70.79.97
  8    13 ms     3 ms     2 ms  103.5.150.3

Trace complete.
```

Listing 19: Observation for tracert to 103.5.150.3

Listing 19 shows the observation for *tracert* to 103.5.150.3. It is seen that the packet hops on a Nepal Telecommunications Corporation IP which shows that the ISP for the destination IP is Nepal Telecommu-

nications. A notable informations that can be gathered from the *tracert* command executions shown in Listing 16 to Listing 19 is that the packet initially hops on the default gateway address 192.168.1.1 regardless of the destination. This is true since the gateway is essentially a bridge for the private network and the internet.

e. Using arp

```
Interface: 192.168.56.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.1.19 --- 0x9
  Internet Address      Physical Address      Type
  192.168.1.1           c8-50-e9-63-da-9a     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.99.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.99.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Listing 20: Observation for arp -a

Listing 20 shows the observation for *arp -a* command. The IP-to-Physical address table for all devices or modules that the various network adapter interfaces have interacted and thus stored in the ARP table are displayed. The wireless LAN adapter which is the second entry, is seen to interact with the default gateway. The physical address c8-50-e9-63-da-9a is indeed the MAC address of the router used for the wirless connection.

```
Pinging 192.168.1.13 with 32 bytes of data:
Reply from 192.168.1.13: bytes=32 time=25ms TTL=64
Reply from 192.168.1.13: bytes=32 time=46ms TTL=64
Reply from 192.168.1.13: bytes=32 time=78ms TTL=64
```

```
Reply from 192.168.1.13: bytes=32 time=90ms TTL=64

Ping statistics for 192.168.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 90ms, Average = 59ms

Interface: 192.168.56.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.1.19 --- 0x9
  Internet Address      Physical Address      Type
  192.168.1.1           c8-50-e9-63-da-9a     dynamic
  192.168.1.13          94-7b-e7-f6-cc-c9     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.99.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.99.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Listing 21: Observation for ping to another device on the network followed by arp -a

Listing 21 shows the observation for *arp -a* command after another device on the same network was pinged. The IP address obtained by a mobile device on the network was 192.168.1.13, which is pinged from the system. After that, execution of the *arp -a* command shows that the wireless LAN adapter has an additional entry in its ARP table which gives the IP and the physical address of the mobile device that was pinged.

f. Using hostname

```
LAPTOP-QLRVLCUC
```

Listing 22: Observation for hostname

Listing 22 shows the observation for *hostname* command. The hostname for the system on which the

experiment was performed is LAPTOP-QLRVLCUC.

g. Using netstat

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:5040           LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:5357           LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:6800           LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:49670          LAPTOP-QLRVLCUC:0      LISTENING
  TCP    0.0.0.0:49671          LAPTOP-QLRVLCUC:0      LISTENING
  TCP    127.0.0.1:6463         LAPTOP-QLRVLCUC:0      LISTENING
  TCP    127.0.0.1:8092         LAPTOP-QLRVLCUC:0      LISTENING
  TCP    127.0.0.1:53394        LAPTOP-QLRVLCUC:53395  ESTABLISHED
  TCP    127.0.0.1:53395        LAPTOP-QLRVLCUC:53394  ESTABLISHED
  TCP    127.0.0.1:53665        LAPTOP-QLRVLCUC:0      LISTENING
  TCP    127.0.0.1:53666        LAPTOP-QLRVLCUC:0      LISTENING
  TCP    127.0.0.1:53666        LAPTOP-QLRVLCUC:53690  ESTABLISHED
  TCP    127.0.0.1:53666        LAPTOP-QLRVLCUC:53888  TIME_WAIT
  TCP    127.0.0.1:53690        LAPTOP-QLRVLCUC:53666  ESTABLISHED
  TCP    127.0.0.1:53882        LAPTOP-QLRVLCUC:53883  ESTABLISHED
  TCP    127.0.0.1:53883        LAPTOP-QLRVLCUC:53882  ESTABLISHED
  TCP    127.0.0.1:53889        LAPTOP-QLRVLCUC:53666  TIME_WAIT
  TCP    192.168.1.19:139       LAPTOP-QLRVLCUC:0      LISTENING
  TCP    192.168.1.19:53348     40.90.189.152:https    ESTABLISHED
  TCP    192.168.1.19:53396     bom07s20-in-f10:https  ESTABLISHED
  TCP    192.168.1.19:53634     162.159.134.234:https  ESTABLISHED
  TCP    192.168.1.19:53758     edge-star-shv-02
                                -sin6:https            TIME_WAIT
  TCP    192.168.1.19:53832     11140-22491:458        ESTABLISHED
  TCP    192.168.1.19:53857     199.232.193.7:https    ESTABLISHED
  TCP    192.168.1.19:53866     edge-star-mini-shv-02
                                -sin6:https            ESTABLISHED
  TCP    192.168.1.19:53873     any-in-2015:https      ESTABLISHED
  TCP    192.168.1.19:53874     199.232.254.109:https  ESTABLISHED
  TCP    192.168.1.19:53875     server-99-86-154-
                                15:https               ESTABLISHED
  TCP    192.168.1.19:53877     any-in-2015:https      ESTABLISHED
  TCP    192.168.1.19:53879     server-13-227-250
```

```
                                -7:https                ESTABLISHED
  TCP    192.168.1.19:53880     110.44.120.81:https     ESTABLISHED
  TCP    192.168.1.19:53884     hkg12s10-in-f42:https   ESTABLISHED
  TCP    192.168.1.19:53891     xx-fbcdn-shv-01
                                -bom1:https             ESTABLISHED
  TCP    192.168.1.19:53893     110.44.120.82:https     ESTABLISHED
  TCP    192.168.1.19:53895     xx-fbcdn-shv-01
                                -bom1:https             ESTABLISHED
  TCP    192.168.56.1:139       LAPTOP-QLRVLCUC:0       LISTENING
  TCP    192.168.99.1:139       LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:135               LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:445               LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:5357              LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:49664             LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:49665             LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:49666             LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:49667             LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:49668             LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:49670             LAPTOP-QLRVLCUC:0       LISTENING
  TCP    [::]:49671             LAPTOP-QLRVLCUC:0       LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:52403          *:*
  UDP    0.0.0.0:54617          *:*
  UDP    0.0.0.0:54702          *:*
  UDP    0.0.0.0:57786          *:*
  UDP    0.0.0.0:59668          *:*
  UDP    0.0.0.0:61931          *:*
  UDP    0.0.0.0:62813          *:*
  UDP    0.0.0.0:62814          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:53319        *:*
  UDP    127.0.0.1:59667        *:*
  UDP    192.168.1.19:137       *:*
  UDP    192.168.1.19:138       *:*
```

```
  UDP    192.168.1.19:1900      *:*
  UDP    192.168.1.19:2177      *:*
  UDP    192.168.1.19:59666     *:*
  UDP    192.168.56.1:137       *:*
  UDP    192.168.56.1:138       *:*
  UDP    192.168.56.1:1900      *:*
  UDP    192.168.56.1:2177      *:*
  UDP    192.168.56.1:59664     *:*
  UDP    192.168.99.1:137       *:*
  UDP    192.168.99.1:138       *:*
  UDP    192.168.99.1:1900      *:*
  UDP    192.168.99.1:2177      *:*
  UDP    192.168.99.1:59665     *:*
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:57787             *:*
  UDP    [::]:59669             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:59663            *:*
  UDP    [fe80::509d:f9df:2bd5:9ab%9]:1900  *:*
  UDP    [fe80::509d:f9df:2bd5:9ab%9]:2177  *:*
  UDP    [fe80::509d:f9df:2bd5:9ab%9]:59662  *:*
  UDP    [fe80::c8fa:6525:b46c:39db%13]:1900  *:*
  UDP    [fe80::c8fa:6525:b46c:39db%13]:2177  *:*
  UDP    [fe80::c8fa:6525:b46c:39db%13]:59661  *:*
  UDP    [fe80::d94a:5427:b7ca:594a%6]:1900  *:*
  UDP    [fe80::d94a:5427:b7ca:594a%6]:2177  *:*
  UDP    [fe80::d94a:5427:b7ca:594a%6]:59660  *:*
```

Listing 23: Observation for netstat -a

Listing 23 shows the observation for *netstat -a* command. All the active ports with the local address, foreign address and the status along with the protocol used are displayed. The same IP has been used with varying port numbers to establish different connections on the system which is clear from the observation.

```
Interface Statistics

                          Received            Sent

Bytes                    669778004        92752926
```

```
Unicast packets             3520938         1010010
Non-unicast packets              12            8118
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

Listing 24: Observation for netstat -e

Listing 24 shows the observation for *netstat -e* command. The network connection statistics such as bytes of data sent and received, unicast packets, non-unicast packets and any discards or error are observed by executing the *netstat -e* command.

```
===========================================================================
Interface List
 23...5e 58 40 0a ab e1 ......VPN Client Adapter - VPN
 14...00 ff 80 4f 8a c2 ......TAP-NordVPN Windows Adapter V9
  6...0a 00 27 00 00 06 ......VirtualBox Host-Only Ethernet Adapter #2
 13...0a 00 27 00 00 0d ......VirtualBox Host-Only Ethernet Adapter #3
  9...6e 76 04 c6 70 57 ......Intel(R) Dual Band Wireless-AC 7265
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network         Netmask           Gateway       Interface     Metric
Destination
0.0.0.0         0.0.0.0           192.168.1.1   192.168.1.19     55
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
192.168.1.0     255.255.255.0     On-link       192.168.1.19    311
192.168.1.19    255.255.255.255   On-link       192.168.1.19    311
192.168.1.255   255.255.255.255   On-link       192.168.1.19    311
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
192.168.99.0    255.255.255.0     On-link       192.168.99.1    281
192.168.99.1    255.255.255.255   On-link       192.168.99.1    281
192.168.99.255  255.255.255.255   On-link       192.168.99.1    281
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       192.168.99.1    281
224.0.0.0       240.0.0.0         On-link       192.168.1.19    311
255.255.255.255 255.255.255.255   On-link       127.0.0.1       331
255.255.255.255 255.255.255.255   On-link       192.168.56.1    281
255.255.255.255 255.255.255.255   On-link       192.168.99.1    281
255.255.255.255 255.255.255.255   On-link       192.168.1.19    311
===========================================================================
```

```
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  9    311 ::/0                     fe80::1
  1    331 ::1/128                  On-link
  6    281 fe80::/64                On-link
 13    281 fe80::/64                On-link
  9    311 fe80::/64                On-link
  9    311 fe80::509d:f9df:2bd5:9ab/128
                                    On-link
 13    281 fe80::c8fa:6525:b46c:39db/128
                                    On-link
  6    281 fe80::d94a:5427:b7ca:594a/128
                                    On-link
  1    331 ff00::/8                 On-link
  6    281 ff00::/8                 On-link
 13    281 ff00::/8                 On-link
  9    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Listing 25: Observation for netstat -r

Listing 25 shows the observation for *netstat -r* command. The routing table information such as interfaces available, active routes, persistent routes, including both the IPv4 and IPv6 route tables are displayed.

h. Using route

```
===========================================================================
Interface List
 23...5e 58 40 0a ab e1 ......VPN Client Adapter - VPN
 14...00 ff 80 4f 8a c2 ......TAP-NordVPN Windows Adapter V9
  6...0a 00 27 00 00 06 ......VirtualBox Host-Only Ethernet Adapter #2
 13...0a 00 27 00 00 0d ......VirtualBox Host-Only Ethernet Adapter #3
  9...6e 76 04 c6 70 57 ......Intel(R) Dual Band Wireless-AC 7265
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network         Netmask          Gateway       Interface     Metric
Destination
0.0.0.0          0.0.0.0          192.168.1.1  192.168.1.19     55
```

```
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
192.168.1.0      255.255.255.0     On-link      192.168.1.19     311
192.168.1.19     255.255.255.255   On-link      192.168.1.19     311
192.168.1.255    255.255.255.255   On-link      192.168.1.19     311
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
192.168.99.0     255.255.255.0     On-link      192.168.99.1     281
192.168.99.1     255.255.255.255   On-link      192.168.99.1     281
192.168.99.255   255.255.255.255   On-link      192.168.99.1     281
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      192.168.99.1     281
224.0.0.0        240.0.0.0         On-link      192.168.1.19     311
255.255.255.255  255.255.255.255   On-link      127.0.0.1        331
255.255.255.255  255.255.255.255   On-link      192.168.56.1     281
255.255.255.255  255.255.255.255   On-link      192.168.99.1     281
255.255.255.255  255.255.255.255   On-link      192.168.1.19     311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  9    311 ::/0                     fe80::1
  1    331 ::1/128                  On-link
  6    281 fe80::/64                On-link
 13    281 fe80::/64                On-link
  9    311 fe80::/64                On-link
  9    311 fe80::509d:f9df:2bd5:9ab/128
                                    On-link
 13    281 fe80::c8fa:6525:b46c:39db/128
                                    On-link
  6    281 fe80::d94a:5427:b7ca:594a/128
                                    On-link
  1    331 ff00::/8                 On-link
  6    281 ff00::/8                 On-link
 13    281 ff00::/8                 On-link
  9    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Listing 26: Observation for route print

Listing 26 shows the observation for *route print* command. The execution results in an observation similar

to the *netstat -r* command, which also prints the route table informations. The command defaults to display both the IPv4 and IPv6 routing tables.

```
===========================================================================
Interface List
 23...5e 58 40 0a ab e1 ......VPN Client Adapter - VPN
 14...00 ff 80 4f 8a c2 ......TAP-NordVPN Windows Adapter V9
  6...0a 00 27 00 00 06 ......VirtualBox Host-Only Ethernet Adapter #2
 13...0a 00 27 00 00 0d ......VirtualBox Host-Only Ethernet Adapter #3
  9...6e 76 04 c6 70 57 ......Intel(R) Dual Band Wireless-AC 7265
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network           Netmask           Gateway       Interface     Metric
Destination
0.0.0.0           0.0.0.0           192.168.1.1   192.168.1.19     50
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
192.168.1.0       255.255.255.0     On-link       192.168.1.19    306
192.168.1.19      255.255.255.255   On-link       192.168.1.19    306
192.168.1.255     255.255.255.255   On-link       192.168.1.19    306
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
192.168.99.0      255.255.255.0     On-link       192.168.99.1    281
192.168.99.1      255.255.255.255   On-link       192.168.99.1    281
192.168.99.255    255.255.255.255   On-link       192.168.99.1    281
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       192.168.99.1    281
224.0.0.0         240.0.0.0         On-link       192.168.1.19    306
255.255.255.255   255.255.255.255   On-link       127.0.0.1       331
255.255.255.255   255.255.255.255   On-link       192.168.56.1    281
255.255.255.255   255.255.255.255   On-link       192.168.99.1    281
255.255.255.255   255.255.255.255   On-link       192.168.1.19    306
===========================================================================
Persistent Routes:
  None
```

Listing 27: Observation for route print -4

Listing 27 shows the observation for *route print -4* command. The additional parameter on this command displays only the IPv4 route table.

```
===========================================================================
Interface List
 23...5e 58 40 0a ab e1 ......VPN Client Adapter - VPN
 14...00 ff 80 4f 8a c2 ......TAP-NordVPN Windows Adapter V9
  6...0a 00 27 00 00 06 ......VirtualBox Host-Only Ethernet Adapter #2
 13...0a 00 27 00 00 0d ......VirtualBox Host-Only Ethernet Adapter #3
  9...6e 76 04 c6 70 57 ......Intel(R) Dual Band Wireless-AC 7265
  1...........................Software Loopback Interface 1
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  9    311 ::/0                     fe80::1
  1    331 ::1/128                  On-link
  6    281 fe80::/64                On-link
 13    281 fe80::/64                On-link
  9    311 fe80::/64                On-link
  9    311 fe80::509d:f9df:2bd5:9ab/128
                                    On-link
 13    281 fe80::c8fa:6525:b46c:39db/128
                                    On-link
  6    281 fe80::d94a:5427:b7ca:594a/128
                                    On-link
  1    331 ff00::/8                 On-link
  6    281 ff00::/8                 On-link
 13    281 ff00::/8                 On-link
  9    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Listing 28: Observation for route print -6

Listing 28 shows the observation for *route print -6* command. The additional parameter on this command displays only the IPv6 route table.

Problem 3
What is the actual IP address of your computer? Also find the Public IP address that is being used for your computer's Internet connectivity. Note down both the IP addresses.

The actual IP address of the system on which the experiments were performed is observed in Listing 9 and Listing 10. There are a few different methods to check the public IP address.

a. Using the Command Prompt (nslookup) and OpenDNS service

The command *nslookup myip.opendns.com resolver1.opendns.com* can be used to know the public IP of a system.

```
Server:  resolver1.opendns.com
Address:  208.67.222.222

Name:    myip.opendns.com
Address:  103.10.31.52
```

Listing 29: Observation for public IP address using nslookup and OpenDNS service

b. Using the Powershell

On a Windows platform, the Powershell command *(Invoke-WebRequest ifconfig.me/ip).Content.Trim()* gives the public IP address of the system.

```
103.10.31.52
```

Listing 30: Observation for public IP address using Powershell

c. Using third party websites

There are numerous websites that can be used to check the public IP address that the system is using to interact on the internet. Google has a service that allows users to check their public IP address by simply searching for *my ip* or *what is my ip* using the google search engine.

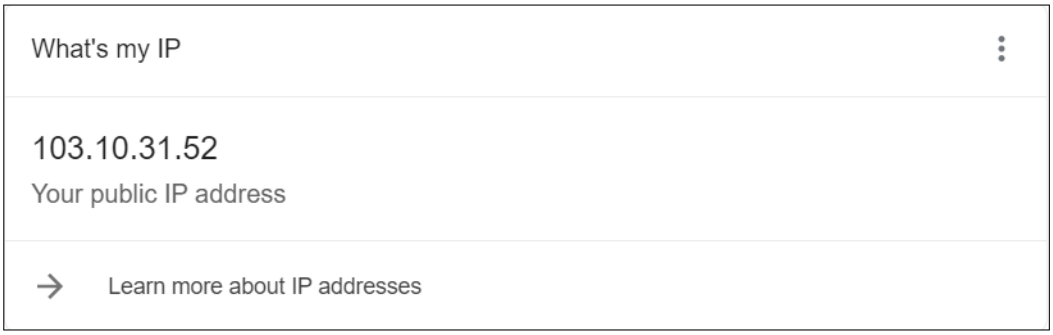

Figure 1: Observation for public IP address using google search engine

From this, the following remarks can be made,
Actual IP address: 192.168.1.19
Public IP address: 103.10.31.52

4 Conclusion

The various networking commands that can be used to know the IP addresses, MAC addresses, configuration status of adapters, check for internet connectivity, trace the route of packets that are sent over the network to a specified destination, display and manipulate the Address Resolution Protocol cache table, route tables were discussed and executed throughout the lab. This report encompasses all the observations made during the experiment with some key comments on the functioning and behavior of the aforementioned commands.