ACN LAB - 03
Introduction to Basic Network Commands

Chaitanya Talware (MIS No: 712422005)
Yogesh Toshniwal (MIS No: 712422021)

1 Introduction to Basic Network Commands

Networking commands are fundamental tools for diagnosing and maintaining computer networks. They allow users to monitor network configurations, check connectivity, and troubleshoot potential issues. Whether managing a small home network or administering a complex enterprise system, understanding these commands is essential.

This assignment aims to explore widely used network commands such as `ipconfig`, `ping`, `traceroute`, and others, emphasizing their significance in practical scenarios. Each command is detailed with its available options and expected output to provide a clear and comprehensive understanding.

2 Commands Overview

2.1 `ipconfig`

The `ipconfig` command is used to display and manage the IP address configuration of a system. It provides detailed information about network adapters, including their IP addresses, subnet masks, and gateways. This command is commonly used for troubleshooting network issues or updating DHCP settings.

2.1.1 Options

- `/?` - Shows a help message with a list of available options.
- `/all` - Displays detailed information about all network adapters.
- `/release` - Releases the IPv4 address for the specified adapter.
- `/release6` - Releases the IPv6 address for the specified adapter.
- `/renew` - Renews the IPv4 address for the specified adapter.
- `/renew6` - Renews the IPv6 address for the specified adapter.
- `/flushdns` - Clears the DNS resolver cache.
- `/registerdns` - Refreshes DHCP leases and re-registers DNS names.
- `/displaydns` - Displays the contents of the DNS resolver cache.
- `/showclassid` - Lists all DHCP class IDs available for the adapter.
- `/setclassid` - Updates the DHCP class ID for the adapter.
- `/showclassid6` - Lists all IPv6 DHCP class IDs available for the adapter.
- `/setclassid6` - Updates the IPv6 DHCP class ID for the adapter.

2.1.2 Example 1

To view the complete network configuration of all adapters:

```
ipconfig /all
```

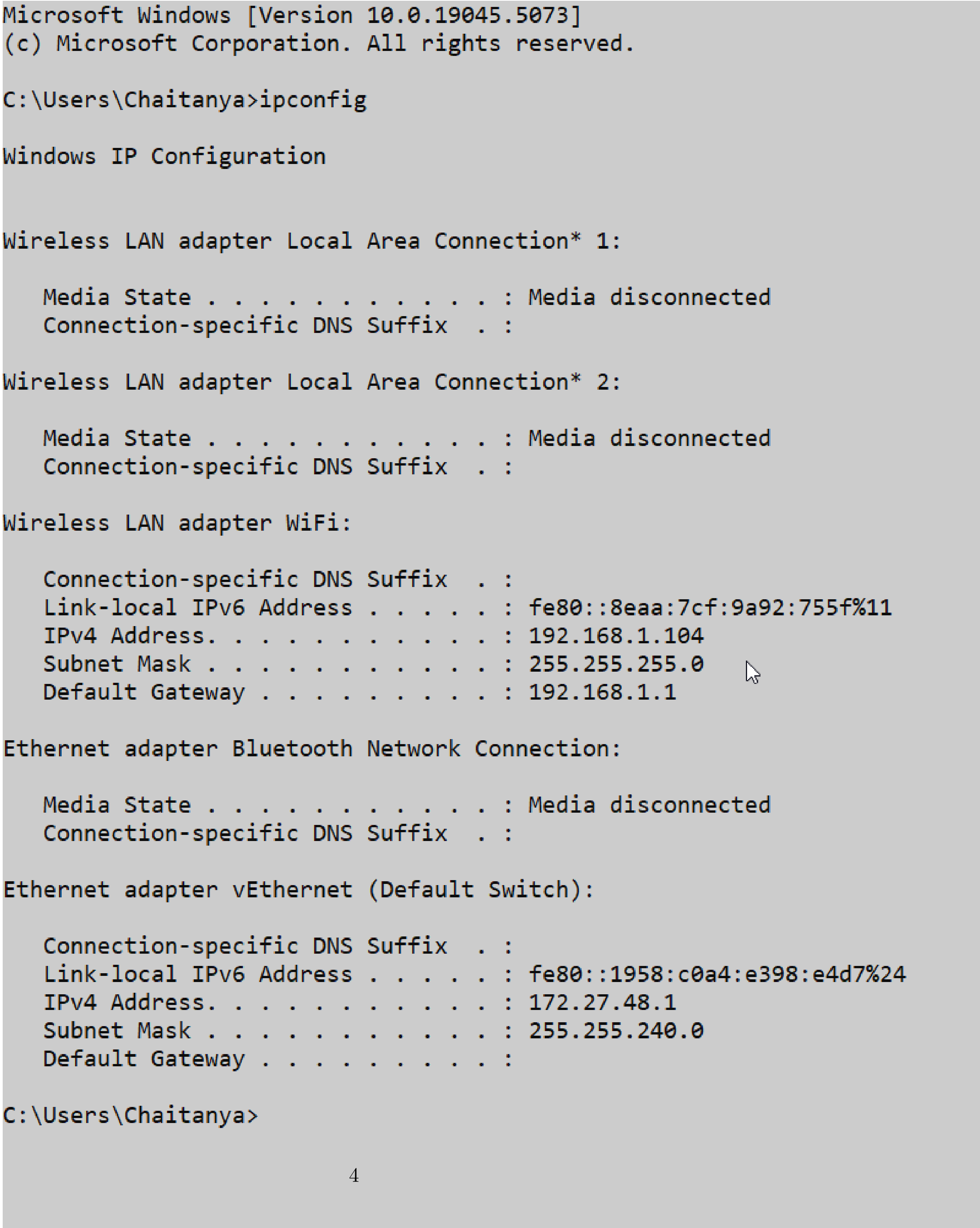
2.1.3 Example 2

```
ipconfig
```

Running the `ipconfig` command without any options provides a concise summary of the network adapter configurations. The output typically includes the following information:

IPv4 Address: The IP address currently assigned to the system. Subnet Mask: Specifies the size of the network segment. Default Gateway: The router's IP address used to access external networks. Connection Status: Indicates whether the adapter is active or disconnected.

2.1.4 Command Output



```
Microsoft Windows [Version 10.0.19045.5073]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Chaitanya>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8eaa:7cf:9a92:755f%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1958:c0a4:e398:e4d7%24
   IPv4 Address. . . . . . . . . . . : 172.27.48.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Users\Chaitanya>
```

Figure 1: ipconfig Command Output

2.2 ping

The `ping` command is used to test the reachability of a network host and measure the round-trip time for messages sent from the originating host to a destination. It helps in diagnosing network connectivity issues.

2.2.1 Options

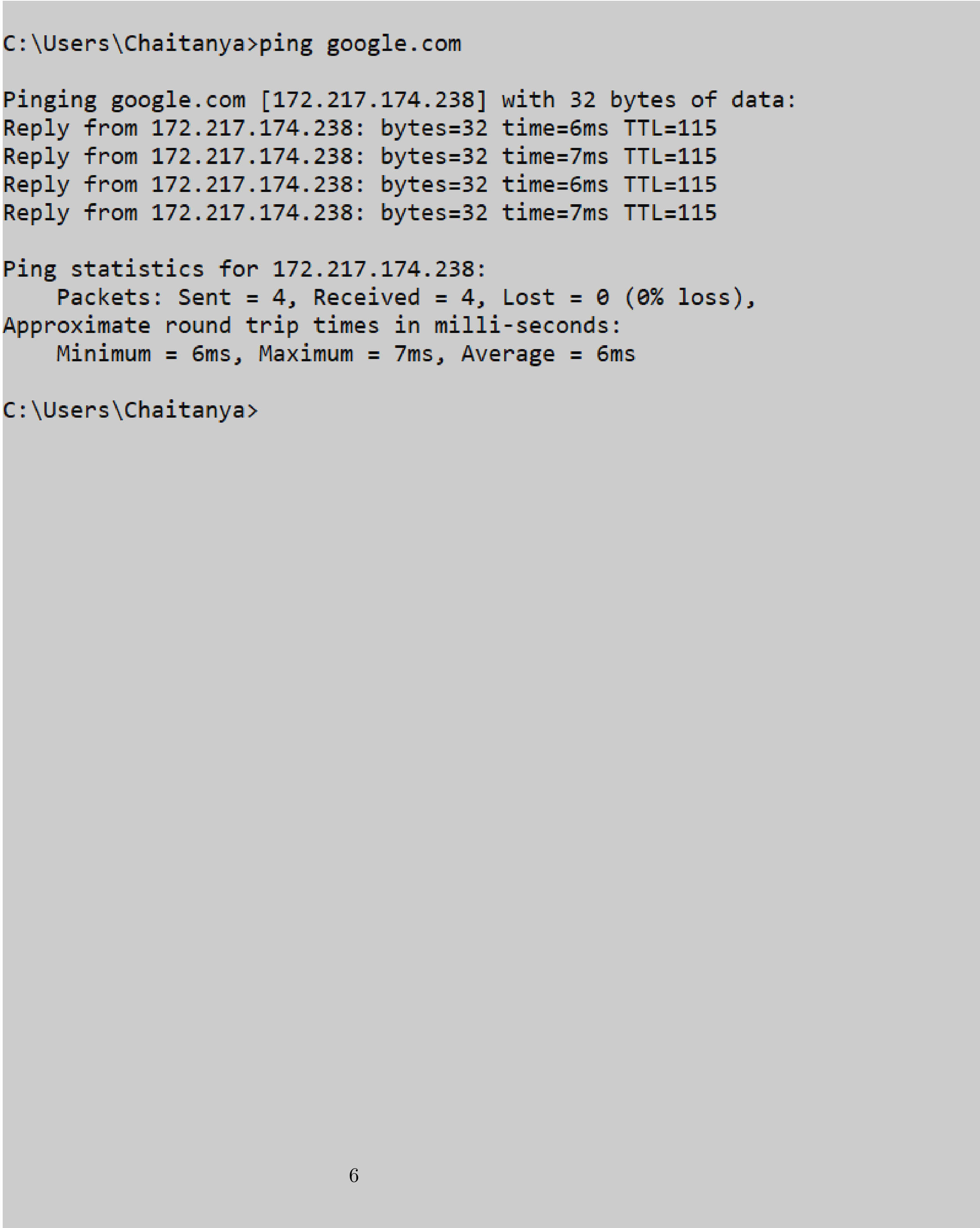
- `-t` - Pings the specified host continuously until stopped manually.
- `-a` - Resolves addresses to hostnames during the ping.
- `-n <count>` - Specifies the number of echo requests to send.
- `-l <size>` - Sends packets of a specified size.
- `-w <timeout>` - Sets the timeout (in milliseconds) for each reply.
- `-4` - Forces the use of IPv4 for the ping.
- `-6` - Forces the use of IPv6 for the ping.
- `-f` - Sets the "Don't Fragment" flag in the packet header.
- `-i <TTL>` - Specifies the Time to Live (TTL) value for packets.
- `-r <count>` - Records the route for a specified number of hops.

2.2.2 Example 1

To send 4 ping requests to the specified host:

```
ping google.com
```

2.2.3 Command Output



```
C:\Users\Chaitanya>ping google.com

Pinging google.com [172.217.174.238] with 32 bytes of data:
Reply from 172.217.174.238: bytes=32 time=6ms TTL=115
Reply from 172.217.174.238: bytes=32 time=7ms TTL=115
Reply from 172.217.174.238: bytes=32 time=6ms TTL=115
Reply from 172.217.174.238: bytes=32 time=7ms TTL=115

Ping statistics for 172.217.174.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 7ms, Average = 6ms

C:\Users\Chaitanya>
```

Figure 2: Ping Command Output

2.3 traceroute

The traceroute command traces the path taken by packets from the source machine to a destination host, showing the routers and devices along the way. It helps in diagnosing network routing issues or delays.

2.3.1 Options

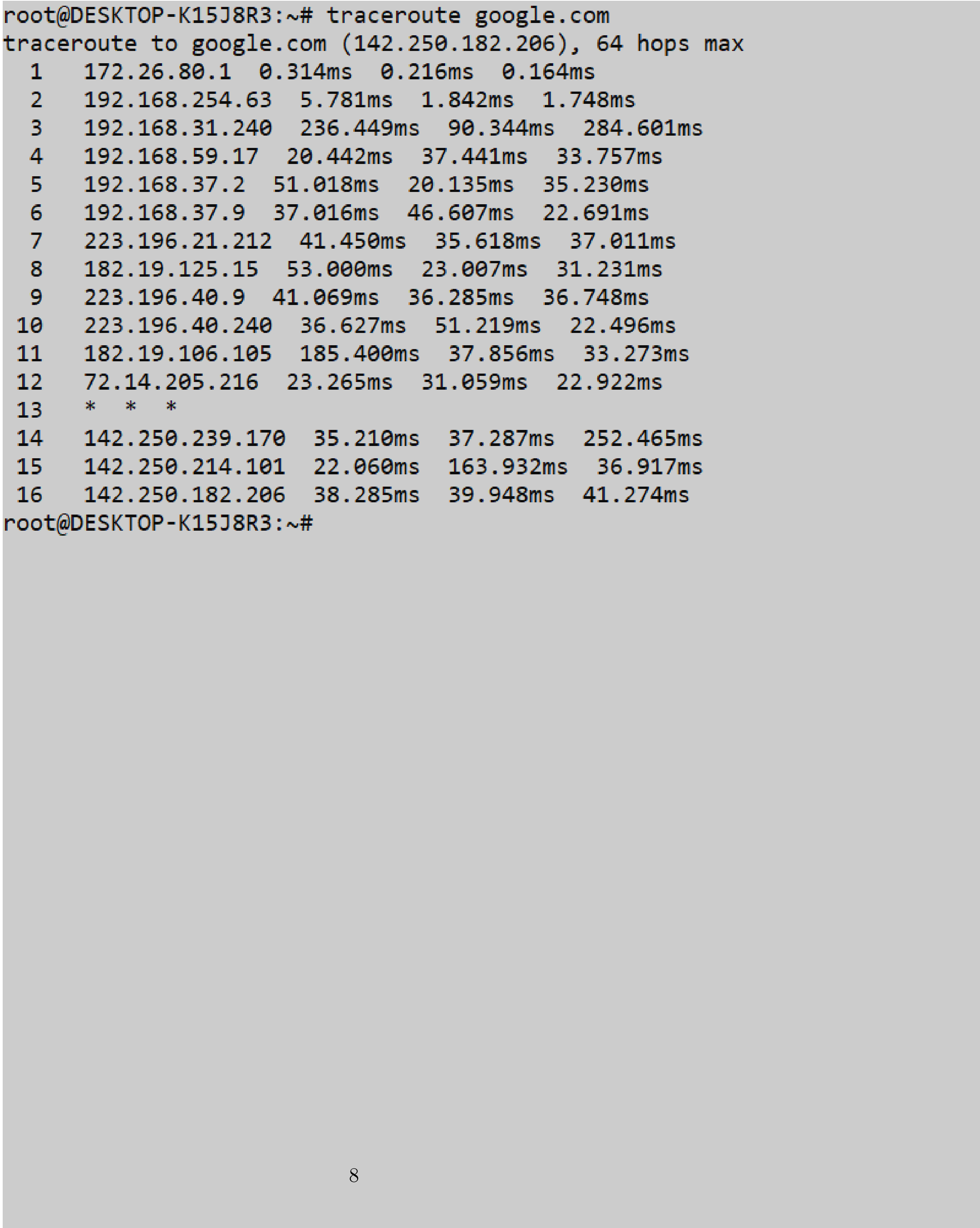
- `-h <max_hops>` - Specifies the maximum number of hops (routers) to trace.
- `-w <timeout_seconds>` - Sets the timeout for waiting for each reply.
- `-m <max_ttl>` - Specifies the maximum time-to-live (TTL) for the traceroute packets.
- `-n` - Displays IP addresses instead of domain names.
- `-I` - Uses ICMP echo requests instead of UDP packets.
- `-T` - Uses TCP packets instead of UDP packets.
- `-p <port_number>` - Specifies the destination port for TCP packets.
- `-q <queries_per_hop>` - Specifies the number of probe packets sent at each hop.
- `-l <packet_size>` - Sets the packet size.

2.3.2 Example 1

To trace the route to a host (e.g., google.com):

```
traceroute google.com
```

2.3.3 Command Output



```
root@DESKTOP-K15J8R3:~# traceroute google.com
traceroute to google.com (142.250.182.206), 64 hops max
  1   172.26.80.1  0.314ms  0.216ms  0.164ms
  2   192.168.254.63  5.781ms  1.842ms  1.748ms
  3   192.168.31.240  236.449ms  90.344ms  284.601ms
  4   192.168.59.17  20.442ms  37.441ms  33.757ms
  5   192.168.37.2  51.018ms  20.135ms  35.230ms
  6   192.168.37.9  37.016ms  46.607ms  22.691ms
  7   223.196.21.212  41.450ms  35.618ms  37.011ms
  8   182.19.125.15  53.000ms  23.007ms  31.231ms
  9   223.196.40.9  41.069ms  36.285ms  36.748ms
 10   223.196.40.240  36.627ms  51.219ms  22.496ms
 11   182.19.106.105  185.400ms  37.856ms  33.273ms
 12   72.14.205.216  23.265ms  31.059ms  22.922ms
 13   *  *  *
 14   142.250.239.170  35.210ms  37.287ms  252.465ms
 15   142.250.214.101  22.060ms  163.932ms  36.917ms
 16   142.250.182.206  38.285ms  39.948ms  41.274ms
root@DESKTOP-K15J8R3:~#
```

Figure 3: Traceroute Command Output

2.4 nslookup

The `nslookup` command is used to query DNS servers for domain name or IP address information. It is helpful for troubleshooting DNS-related issues.

2.4.1 Options

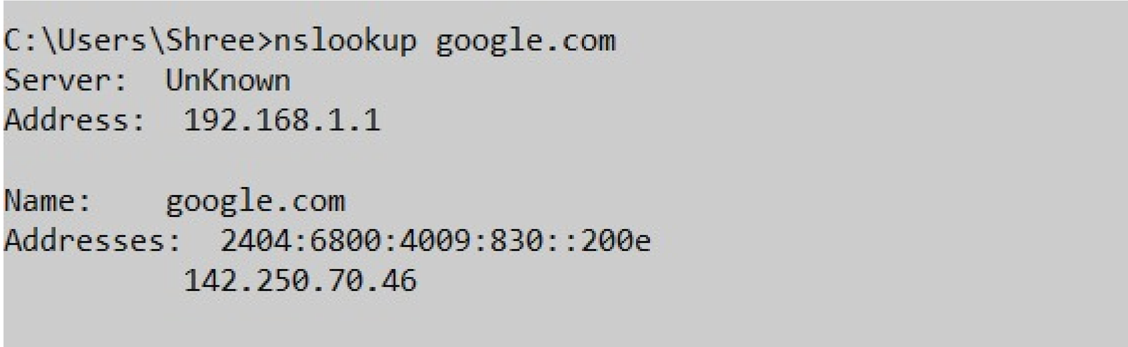
- `-type=<record_type>` - Specifies the type of DNS record to query (e.g., A, MX, NS).
- `-timeout=<seconds>` - Sets the timeout for a response.
- `-debug` - Enables debug mode for detailed output.
- `-query=<domain>` - Queries a specific domain or IP.

2.4.2 Example 1

To query the DNS records for a domain:

```
nslookup google.com
```

2.4.3 Command Output



```
C:\Users\Shree>nslookup google.com
Server:  UnKnown
Address:  192.168.1.1

Name:    google.com
Addresses:  2404:6800:4009:830::200e
          142.250.70.46
```

Figure 4: NSLookup Command Output

2.5 pathping

The pathping command provides detailed information about packet loss and latency along a network route. It combines the features of ping and traceroute.

2.5.1 Options

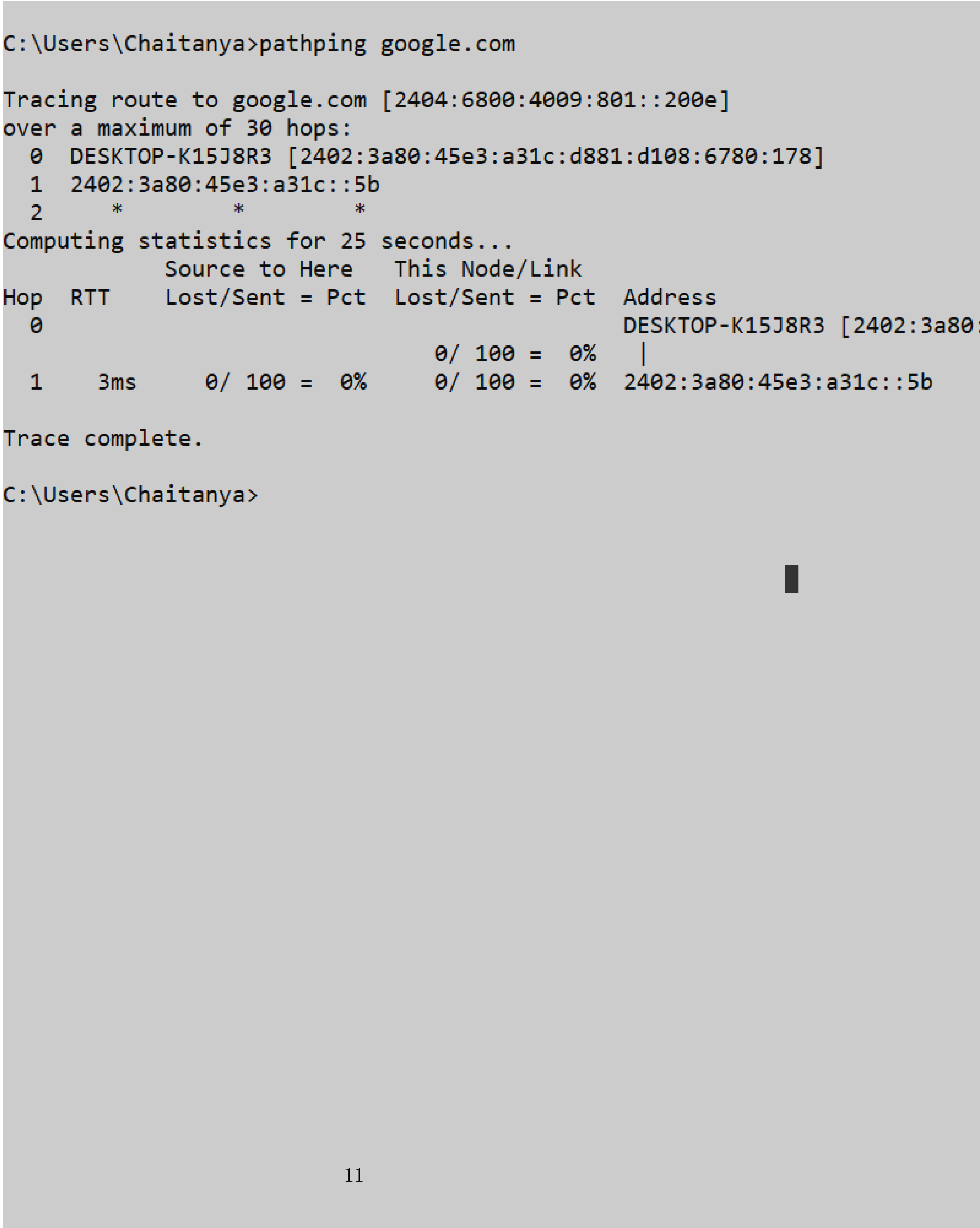
- /q - Sets the number of query packets per hop.
- /n - Prevents the resolution of hostnames to IP addresses.
- /h <max_hops> - Specifies the maximum number of hops.
- /w <timeout> - Sets the wait time for each reply.

2.5.2 Example 1

To analyze a route with pathping:

```
pathping google.com
```

2.6 Command Output



```
C:\Users\Chaitanya>pathping google.com

Tracing route to google.com [2404:6800:4009:801::200e]
over a maximum of 30 hops:
  0  DESKTOP-K15J8R3 [2402:3a80:45e3:a31c:d881:d108:6780:178]
  1  2402:3a80:45e3:a31c::5b
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           DESKTOP-K15J8R3 [2402:3a80:
                                0/ 100 =  0%   |
  1    3ms     0/ 100 =  0%     0/ 100 =  0%  2402:3a80:45e3:a31c::5b

Trace complete.

C:\Users\Chaitanya>
```

Figure 5: Pathping Command Output

2.7 tracert

The `tracert` command traces the route packets take to reach a destination. It is primarily used for diagnosing routing issues.

2.7.1 Options

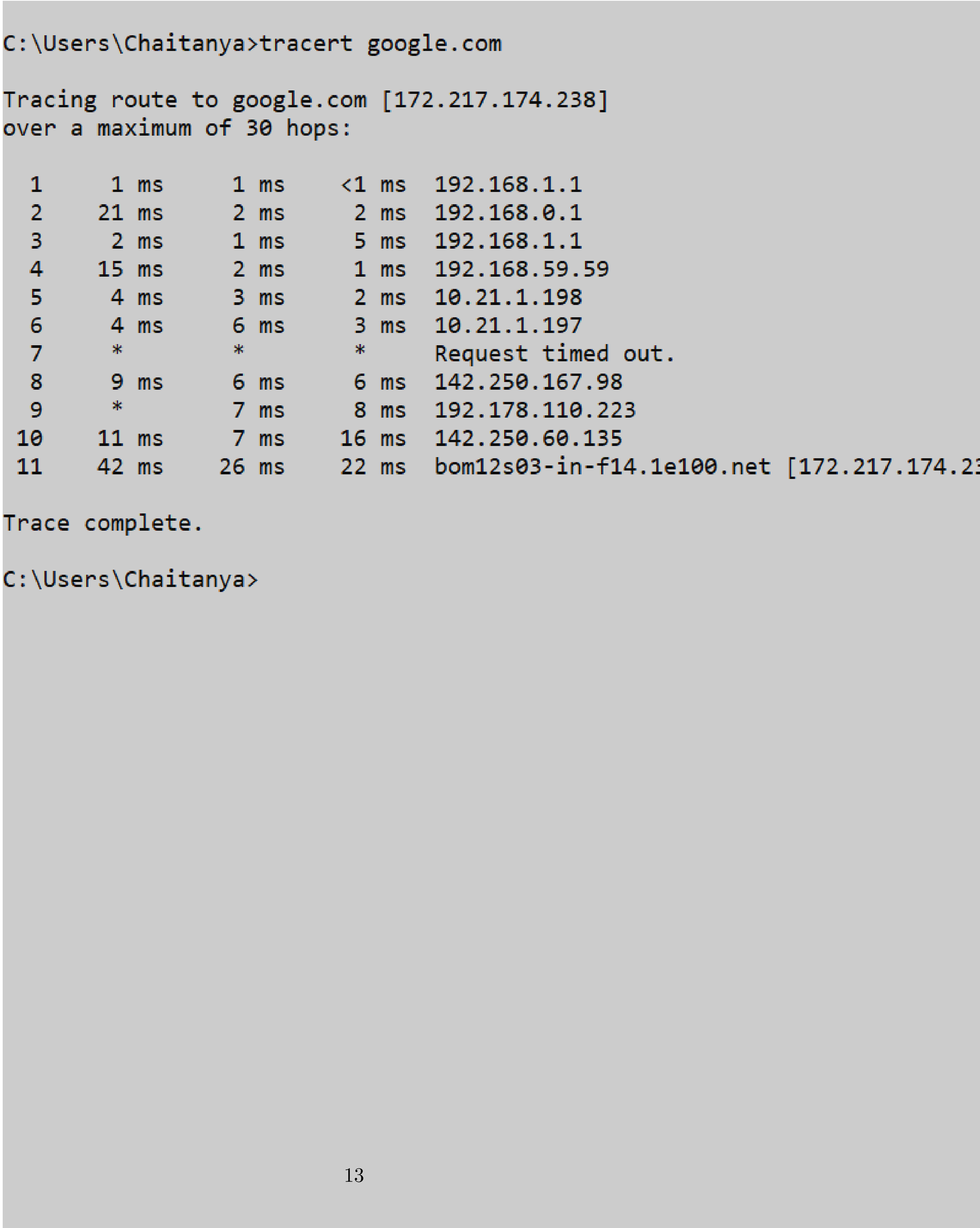
- `/h` <`max_hops`> - Specifies the maximum number of hops.
- `/d` - Prevents the resolution of IP addresses to hostnames.
- `/w` <`timeout`> - Sets the timeout for each reply.

2.7.2 Example 1

To trace the route to a domain:

```
tracert google.com
```

2.8 Command Output



```
C:\Users\Chaitanya>tracert google.com

Tracing route to google.com [172.217.174.238]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  192.168.1.1
  2    21 ms     2 ms     2 ms  192.168.0.1
  3     2 ms     1 ms     5 ms  192.168.1.1
  4    15 ms     2 ms     1 ms  192.168.59.59
  5     4 ms     3 ms     2 ms  10.21.1.198
  6     4 ms     6 ms     3 ms  10.21.1.197
  7     *        *        *     Request timed out.
  8     9 ms     6 ms     6 ms  142.250.167.98
  9     *        7 ms     8 ms  192.178.110.223
 10    11 ms     7 ms    16 ms  142.250.60.135
 11    42 ms    26 ms    22 ms  bom12s03-in-f14.1e100.net [172.217.174.23

Trace complete.

C:\Users\Chaitanya>
```

Figure 6: Tracert Command Output

2.9 `netstat`

The `netstat` command provides information about active network connections, routing tables, and network statistics.

2.9.1 Options

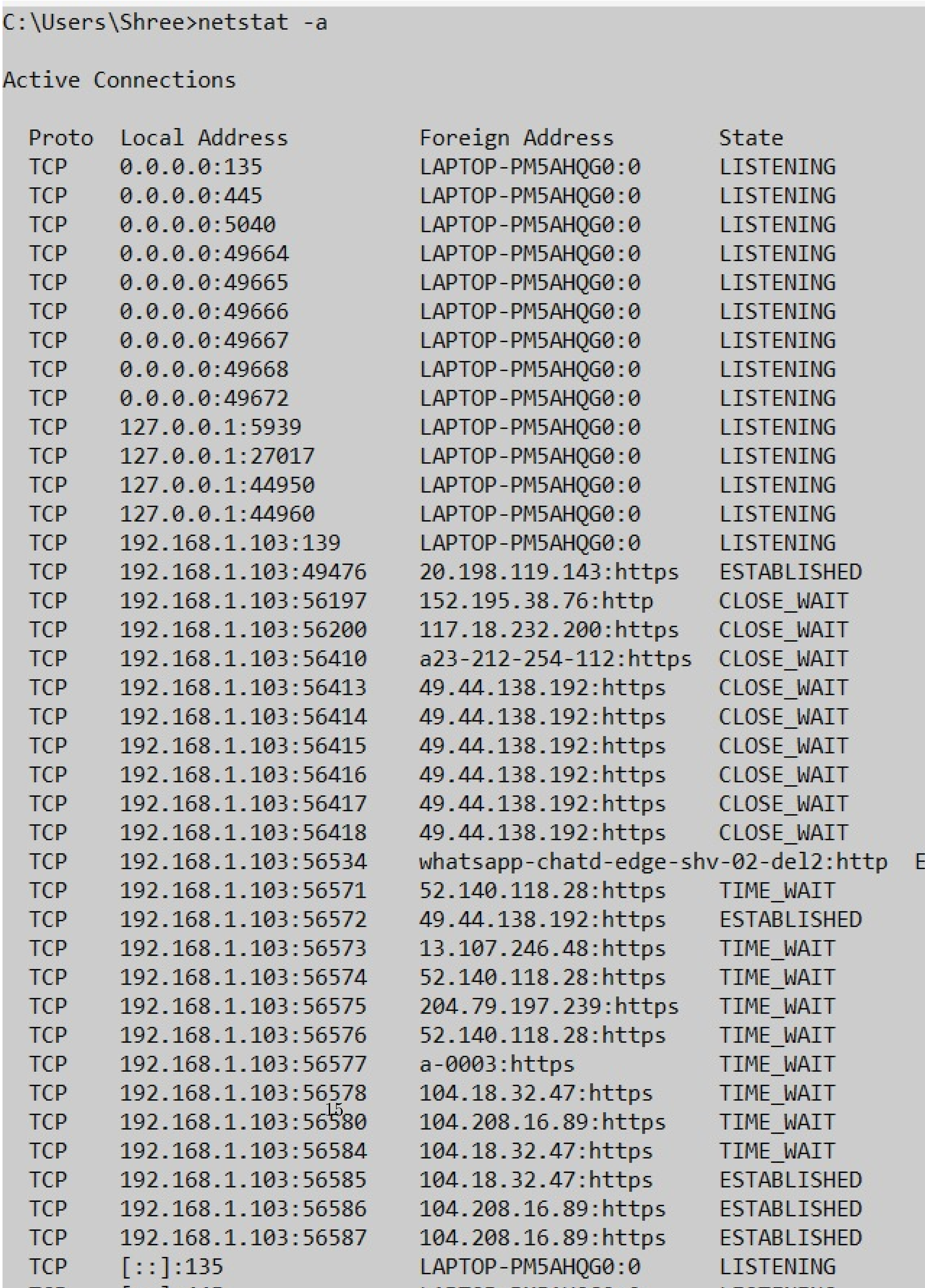
- `-a` - Displays all active connections and listening ports.
- `-n` - Shows addresses and port numbers in numerical format.
- `-r` - Displays the routing table.
- `-s` - Displays statistics for each protocol.

2.9.2 Example 1

To view all active connections:

```
netstat -a
```

2.10 Command Output



```
C:\Users\Shree>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:5040           LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-PM5AHQG0:0      LISTENING
  TCP    0.0.0.0:49672          LAPTOP-PM5AHQG0:0      LISTENING
  TCP    127.0.0.1:5939         LAPTOP-PM5AHQG0:0      LISTENING
  TCP    127.0.0.1:27017        LAPTOP-PM5AHQG0:0      LISTENING
  TCP    127.0.0.1:44950        LAPTOP-PM5AHQG0:0      LISTENING
  TCP    127.0.0.1:44960        LAPTOP-PM5AHQG0:0      LISTENING
  TCP    192.168.1.103:139      LAPTOP-PM5AHQG0:0      LISTENING
  TCP    192.168.1.103:49476    20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.103:56197    152.195.38.76:http     CLOSE_WAIT
  TCP    192.168.1.103:56200    117.18.232.200:https   CLOSE_WAIT
  TCP    192.168.1.103:56410    a23-212-254-112:https  CLOSE_WAIT
  TCP    192.168.1.103:56413    49.44.138.192:https    CLOSE_WAIT
  TCP    192.168.1.103:56414    49.44.138.192:https    CLOSE_WAIT
  TCP    192.168.1.103:56415    49.44.138.192:https    CLOSE_WAIT
  TCP    192.168.1.103:56416    49.44.138.192:https    CLOSE_WAIT
  TCP    192.168.1.103:56417    49.44.138.192:https    CLOSE_WAIT
  TCP    192.168.1.103:56418    49.44.138.192:https    CLOSE_WAIT
  TCP    192.168.1.103:56534    whatsapp-chatd-edge-shv-02-del2:http  E
  TCP    192.168.1.103:56571    52.140.118.28:https    TIME_WAIT
  TCP    192.168.1.103:56572    49.44.138.192:https    ESTABLISHED
  TCP    192.168.1.103:56573    13.107.246.48:https    TIME_WAIT
  TCP    192.168.1.103:56574    52.140.118.28:https    TIME_WAIT
  TCP    192.168.1.103:56575    204.79.197.239:https   TIME_WAIT
  TCP    192.168.1.103:56576    52.140.118.28:https    TIME_WAIT
  TCP    192.168.1.103:56577    a-0003:https           TIME_WAIT
  TCP    192.168.1.103:56578    104.18.32.47:https     TIME_WAIT
  TCP    192.168.1.103:56580    104.208.16.89:https    TIME_WAIT
  TCP    192.168.1.103:56584    104.18.32.47:https     TIME_WAIT
  TCP    192.168.1.103:56585    104.18.32.47:https     ESTABLISHED
  TCP    192.168.1.103:56586    104.208.16.89:https    ESTABLISHED
  TCP    192.168.1.103:56587    104.208.16.89:https    ESTABLISHED
  TCP    [::]:135               LAPTOP-PM5AHQG0:0      LISTENING
```

2.11 arp

The `arp` command manages the ARP cache, resolving IP addresses to MAC addresses.

2.11.1 Options

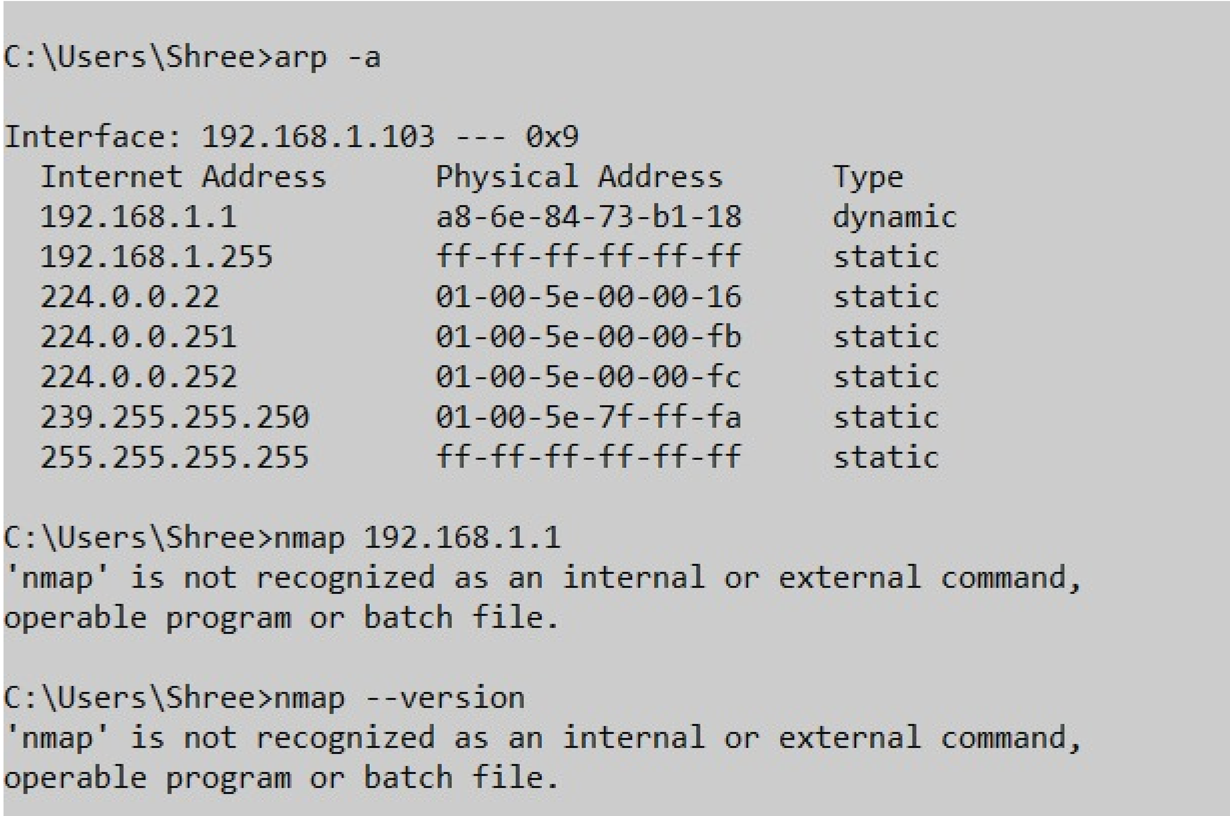
- `-a` - Displays all entries in the ARP cache.
- `-d` <`ip_address`> - Deletes a specific entry.
- `-s` <`ip_address`><`mac_address`> - Adds a static ARP entry.

2.11.2 Example 1

To view the ARP cache:

```
arp -a
```

2.12 Command Output



```
C:\Users\Shree>arp -a

Interface: 192.168.1.103 --- 0x9
  Internet Address      Physical Address      Type
  192.168.1.1           a8-6e-84-73-b1-18     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

C:\Users\Shree>nmap 192.168.1.1
'nmap' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Shree>nmap --version
'nmap' is not recognized as an internal or external command,
operable program or batch file.
```

Figure 8: ARP Command Output

2.13 nmap

The `nmap` command scans networks to discover hosts, services, and open ports.

2.13.1 Options

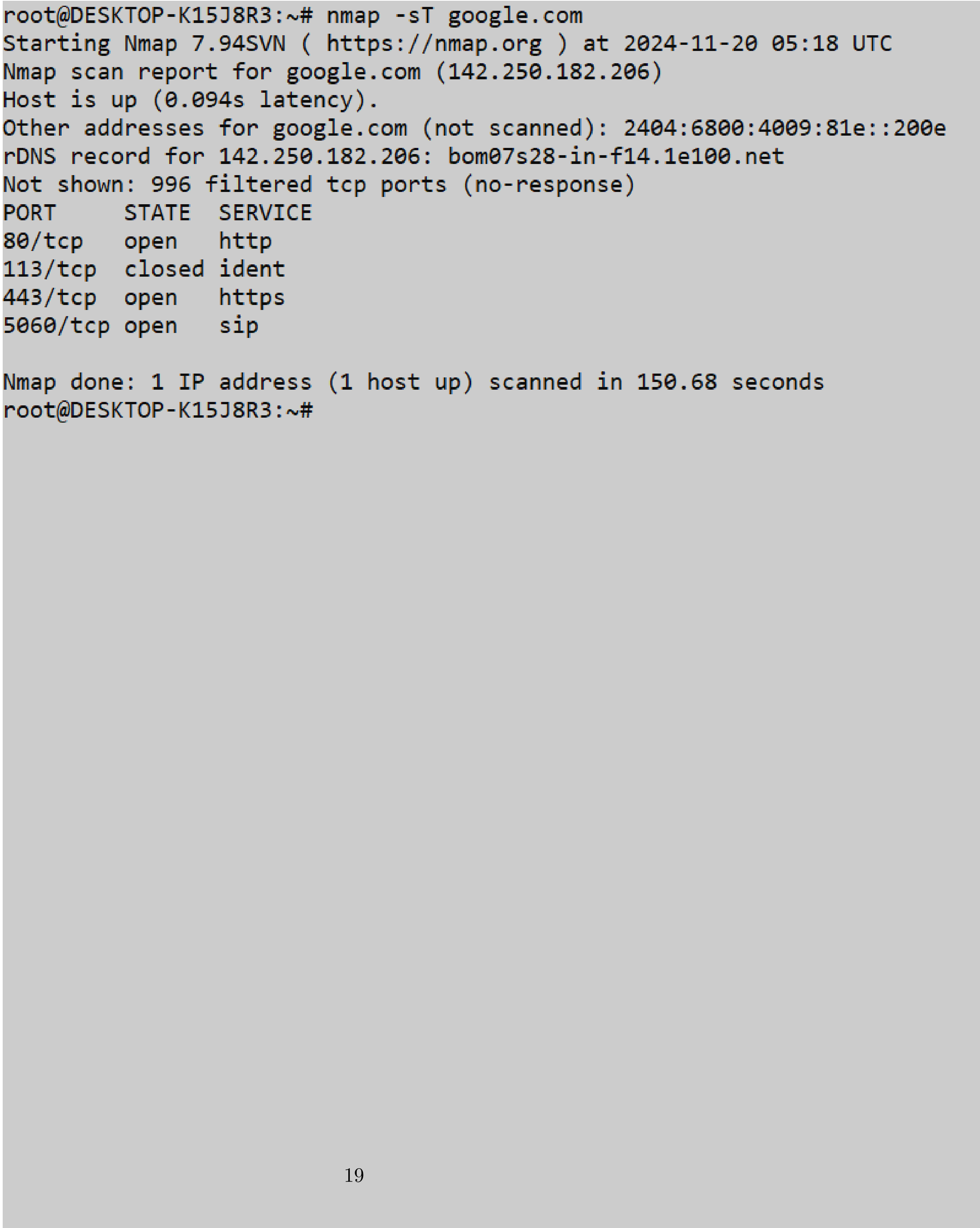
- `-sP` - Performs a ping scan to identify live hosts.
- `-sT` - Performs a TCP connect scan.
- `-p <port_range>` - Scans specified ports or ranges.
- `-A` - Enables advanced options like OS detection and version scanning.
- `-v` - Displays verbose output.

2.13.2 Example 1

To scan for open ports on a host:

```
nmap -sT google.com
```

2.14 Command Output



```
root@DESKTOP-K15J8R3:~# nmap -sT google.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 05:18 UTC
Nmap scan report for google.com (142.250.182.206)
Host is up (0.094s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:81e::200e
rDNS record for 142.250.182.206: bom07s28-in-f14.1e100.net
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
5060/tcp open   sip

Nmap done: 1 IP address (1 host up) scanned in 150.68 seconds
root@DESKTOP-K15J8R3:~#
```

Figure 9: Nmap Command Output