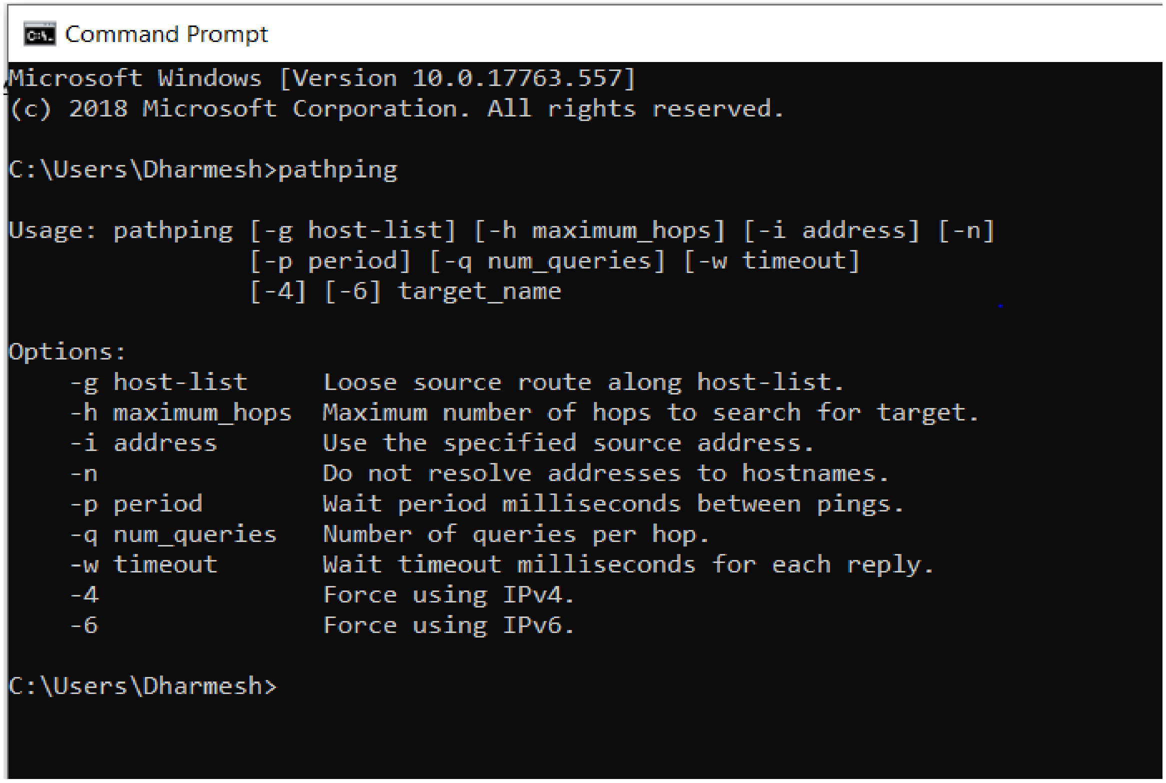
Practical -1

Aim: study of basic network command and network configuration command

1) Pathping:-

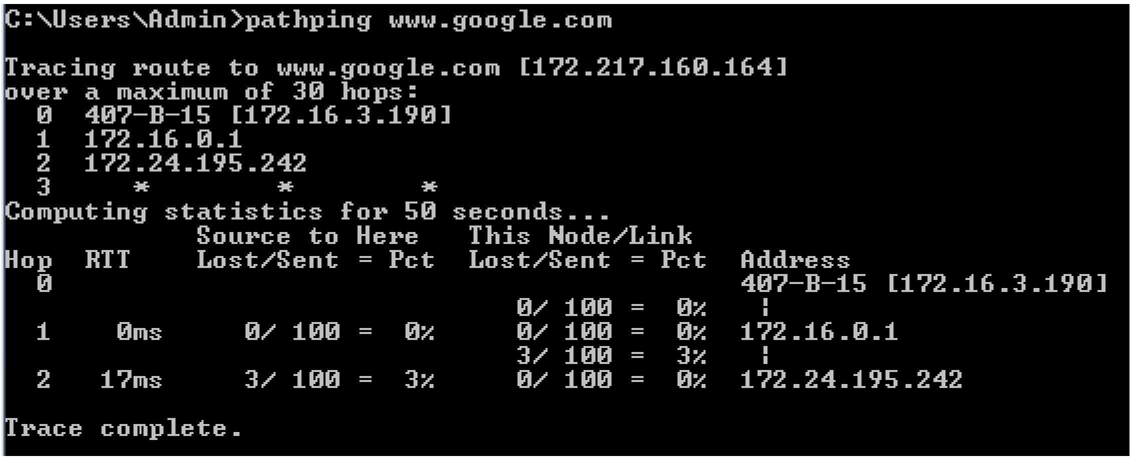
Pathping provides information about network latency and network loss at intermediate hops between a source address and destination address.
Pathping command has included many options as under



Command Prompt

```
Microsoft Windows [Version 10.0.17763.557]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Dharmesh>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\Users\Dharmesh>
```

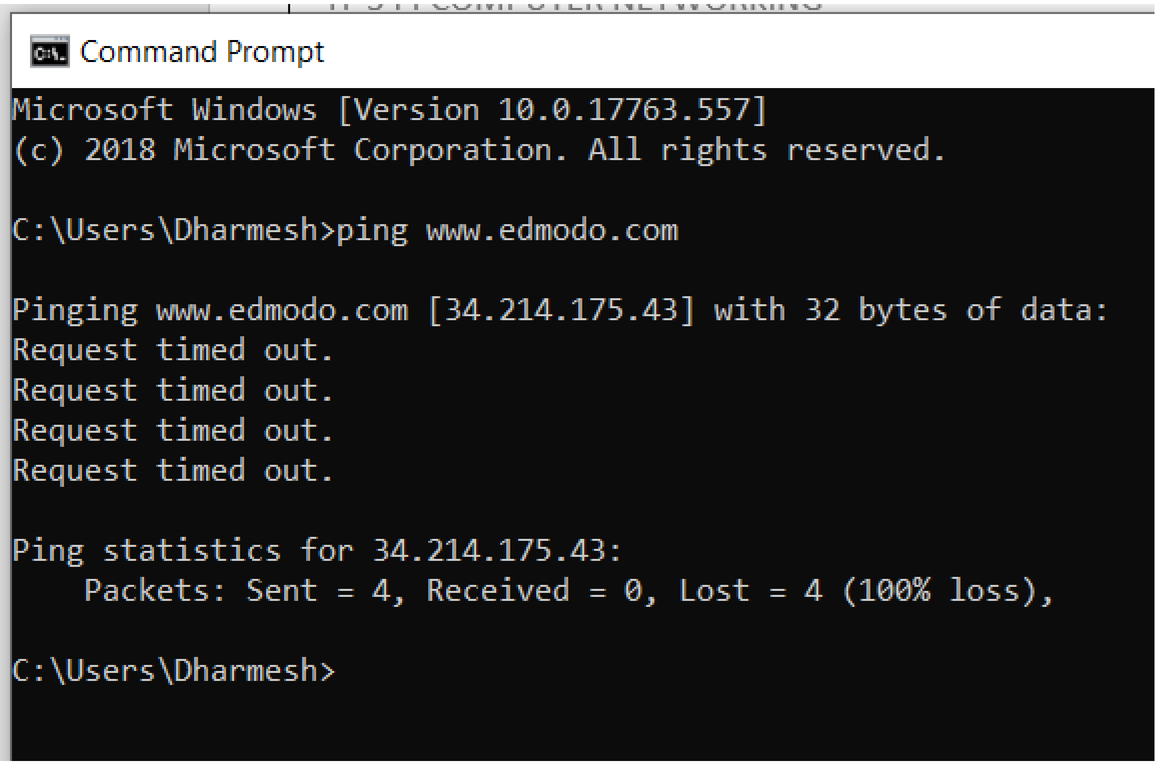
Use of pathping:



```
C:\Users\Admin>pathping www.google.com

Tracing route to www.google.com [172.217.160.164]
over a maximum of 30 hops:
  0  407-B-15 [172.16.3.190]
  1  172.16.0.1
  2  172.24.195.242
  3     *        *        *
Computing statistics for 50 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           407-B-15 [172.16.3.190]
                                0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  172.16.0.1
                                3/ 100 =  3%   |
  2   17ms     3/ 100 =  3%     0/ 100 =  0%  172.24.195.242

Trace complete.
```

2) Ping:

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.

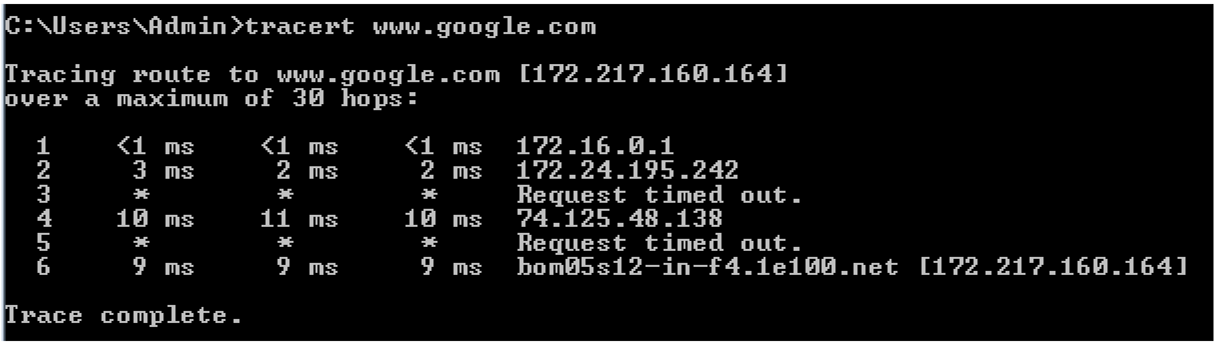


Command Prompt

```
Microsoft Windows [Version 10.0.17763.557]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Dharmesh>ping www.edmodo.com

Pinging www.edmodo.com [34.214.175.43] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.214.175.43:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Dharmesh>
```

3) Tracert (Trace Root):

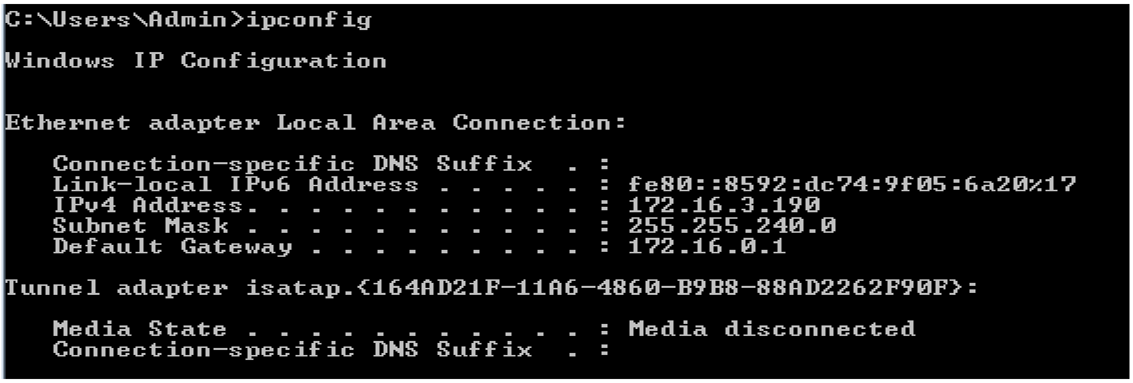
Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each hop fro router to router takes.



```
C:\Users\Admin>tracert www.google.com

Tracing route to www.google.com [172.217.160.164]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2     3 ms     2 ms     2 ms  172.24.195.242
  3     *        *        *     Request timed out.
  4    10 ms    11 ms    10 ms  74.125.48.138
  5     *        *        *     Request timed out.
  6     9 ms     9 ms     9 ms  bom05s12-in-f4.1e100.net [172.217.160.164]

Trace complete.
```

4) IPconfig:

Type ipconfig to run the utility with default options. The output of the default command contains the IP address, network mask, and gateway for all physical and virtual network adapters.

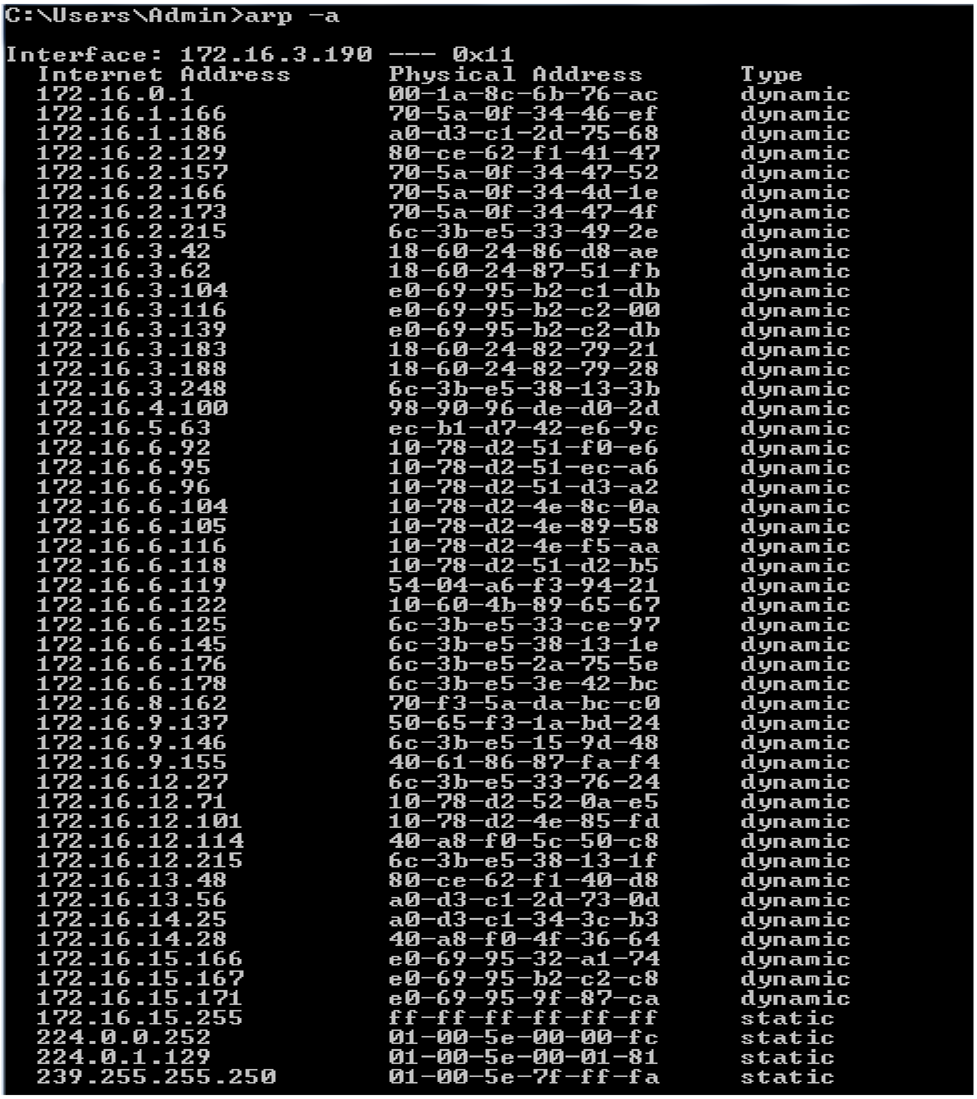


```
C:\Users\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8592:dc74:9f05:6a20%17
   IPv4 Address. . . . . . . . . . . : 172.16.3.190
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.16.0.1

Tunnel adapter isatap.{164AD21F-11A6-4860-B9B8-88AD2262F90F}:

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

5) Arp (Address resolution protocol)

Arp stands for address resolution protocol. Arp is used for mapping of IP address to a physical address (MAC address) in a network. Each host and routers have their own ARP cache in which they store their ARP table.

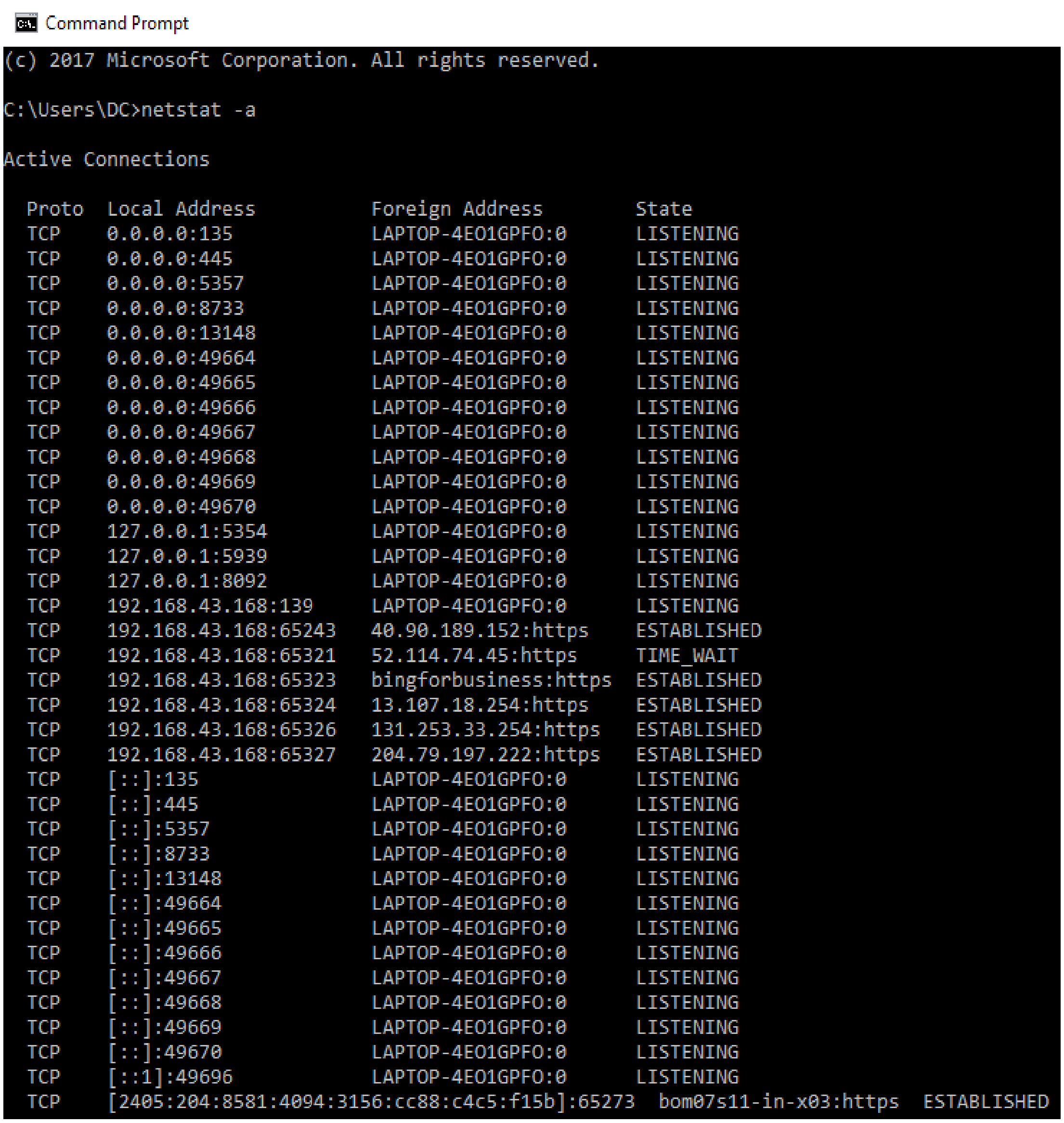
Arp –a command is used to show the arp table for the device.



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

Interface: 172.16.3.190 --- 0x11
  Internet Address      Physical Address      Type
  172.16.0.1            00-1a-8c-6b-76-ac     dynamic
  172.16.1.166          70-5a-0f-34-46-ef     dynamic
  172.16.1.186          a0-d3-c1-2d-75-68     dynamic
  172.16.2.129          80-ce-62-f1-41-47     dynamic
  172.16.2.157          70-5a-0f-34-47-52     dynamic
  172.16.2.166          70-5a-0f-34-4d-1e     dynamic
  172.16.2.173          70-5a-0f-34-47-4f     dynamic
  172.16.2.215          6c-3b-e5-33-49-2e     dynamic
  172.16.3.42           18-60-24-86-d8-ae     dynamic
  172.16.3.62           18-60-24-87-51-fb     dynamic
  172.16.3.104          e0-69-95-b2-c1-db     dynamic
  172.16.3.116          e0-69-95-b2-c2-00     dynamic
  172.16.3.139          e0-69-95-b2-c2-db     dynamic
  172.16.3.183          18-60-24-82-79-21     dynamic
  172.16.3.188          18-60-24-82-79-28     dynamic
  172.16.3.248          6c-3b-e5-38-13-3b     dynamic
  172.16.4.100          98-90-96-de-d0-2d     dynamic
  172.16.5.63           ec-b1-d7-42-e6-9c     dynamic
  172.16.6.92           10-78-d2-51-f0-e6     dynamic
  172.16.6.95           10-78-d2-51-ec-a6     dynamic
  172.16.6.96           10-78-d2-51-d3-a2     dynamic
  172.16.6.104          10-78-d2-4e-8c-0a     dynamic
  172.16.6.105          10-78-d2-4e-89-58     dynamic
  172.16.6.116          10-78-d2-4e-f5-aa     dynamic
  172.16.6.118          10-78-d2-51-d2-b5     dynamic
  172.16.6.119          54-04-a6-f3-94-21     dynamic
  172.16.6.122          10-60-4b-89-65-67     dynamic
  172.16.6.125          6c-3b-e5-33-ce-97     dynamic
  172.16.6.145          6c-3b-e5-38-13-1e     dynamic
  172.16.6.176          6c-3b-e5-2a-75-5e     dynamic
  172.16.6.178          6c-3b-e5-3e-42-bc     dynamic
  172.16.8.162          70-f3-5a-da-bc-c0     dynamic
  172.16.9.137          50-65-f3-1a-bd-24     dynamic
  172.16.9.146          6c-3b-e5-15-9d-48     dynamic
  172.16.9.155          40-61-86-87-fa-f4     dynamic
  172.16.12.27          6c-3b-e5-33-76-24     dynamic
  172.16.12.71          10-78-d2-52-0a-e5     dynamic
  172.16.12.101         10-78-d2-4e-85-fd     dynamic
  172.16.12.114         40-a8-f0-5c-50-c8     dynamic
  172.16.12.215         6c-3b-e5-38-13-1f     dynamic
  172.16.13.48          80-ce-62-f1-40-d8     dynamic
  172.16.13.56          a0-d3-c1-2d-73-0d     dynamic
  172.16.14.25          a0-d3-c1-34-3c-b3     dynamic
  172.16.14.28          40-a8-f0-4f-36-64     dynamic
  172.16.15.166         e0-69-95-32-a1-74     dynamic
  172.16.15.167         e0-69-95-b2-c2-c8     dynamic
  172.16.15.171         e0-69-95-9f-87-ca     dynamic
  172.16.15.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.129           01-00-5e-00-01-81     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

6) Netstat:

Netstat is a command line TCP/IP networking utility. Netstat provides information and statics about protocols in use and current TCP/IP network connections.

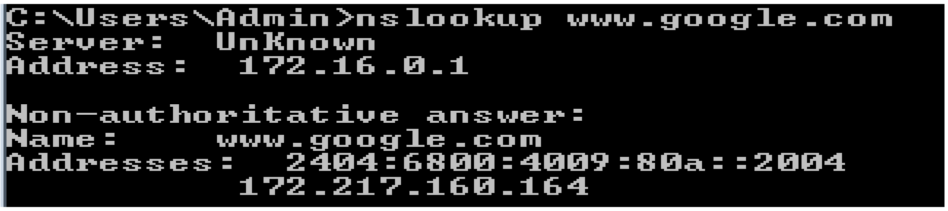


Command Prompt

```
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\DC>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:5357           LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:8733           LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:13148          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:49669          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    0.0.0.0:49670          LAPTOP-4EO1GPFO:0      LISTENING
  TCP    127.0.0.1:5354         LAPTOP-4EO1GPFO:0      LISTENING
  TCP    127.0.0.1:5939         LAPTOP-4EO1GPFO:0      LISTENING
  TCP    127.0.0.1:8092         LAPTOP-4EO1GPFO:0      LISTENING
  TCP    192.168.43.168:139     LAPTOP-4EO1GPFO:0      LISTENING
  TCP    192.168.43.168:65243   40.90.189.152:https    ESTABLISHED
  TCP    192.168.43.168:65321   52.114.74.45:https     TIME_WAIT
  TCP    192.168.43.168:65323   bingforbusiness:https  ESTABLISHED
  TCP    192.168.43.168:65324   13.107.18.254:https    ESTABLISHED
  TCP    192.168.43.168:65326   131.253.33.254:https   ESTABLISHED
  TCP    192.168.43.168:65327   204.79.197.222:https   ESTABLISHED
  TCP    [::]:135               LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:445               LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:5357              LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:8733              LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:13148             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:49664             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:49665             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:49666             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:49667             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:49668             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:49669             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::]:49670             LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [::1]:49696            LAPTOP-4EO1GPFO:0      LISTENING
  TCP    [2405:204:8581:4094:3156:cc88:c4c5:f15b]:65273  bom07s11-in-x03:https  ESTABLISHED
```

7) Nslookup:

The nslookup command is a network utility program used to obtain information about internet servers. It finds name server information for domains by querying the Domain name system.



```
C:\Users\Admin>nslookup www.google.com
Server:  UnKnown
Address:  172.16.0.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:80a::2004
          172.217.160.164
```