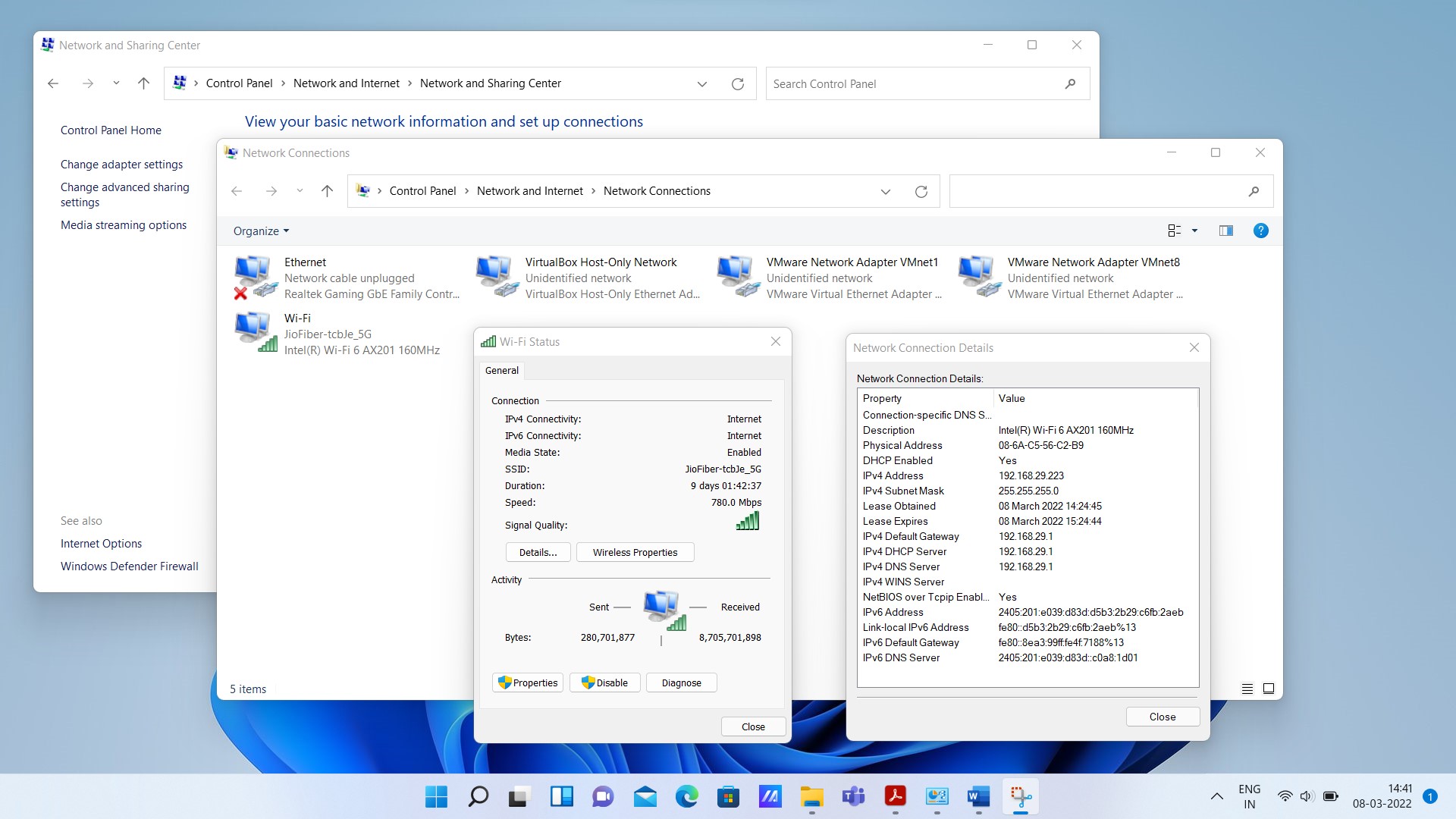
20CYS114 - Cyber Security Essentials Labs

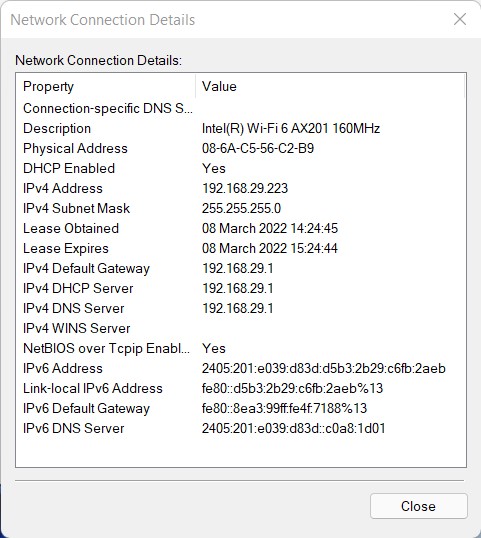
Lab 1 - Computer Network Fundamentals

Task 1: Find the status of your Active network.

Steps followed: Go to Control Panel-> Network and Internet Settings -> View Network Status and Tasks -> Change Adapter Settings -> Right Click on your adapter (Either ethernet or Wi-Fi) -> Click status -> Click Details.

Output:

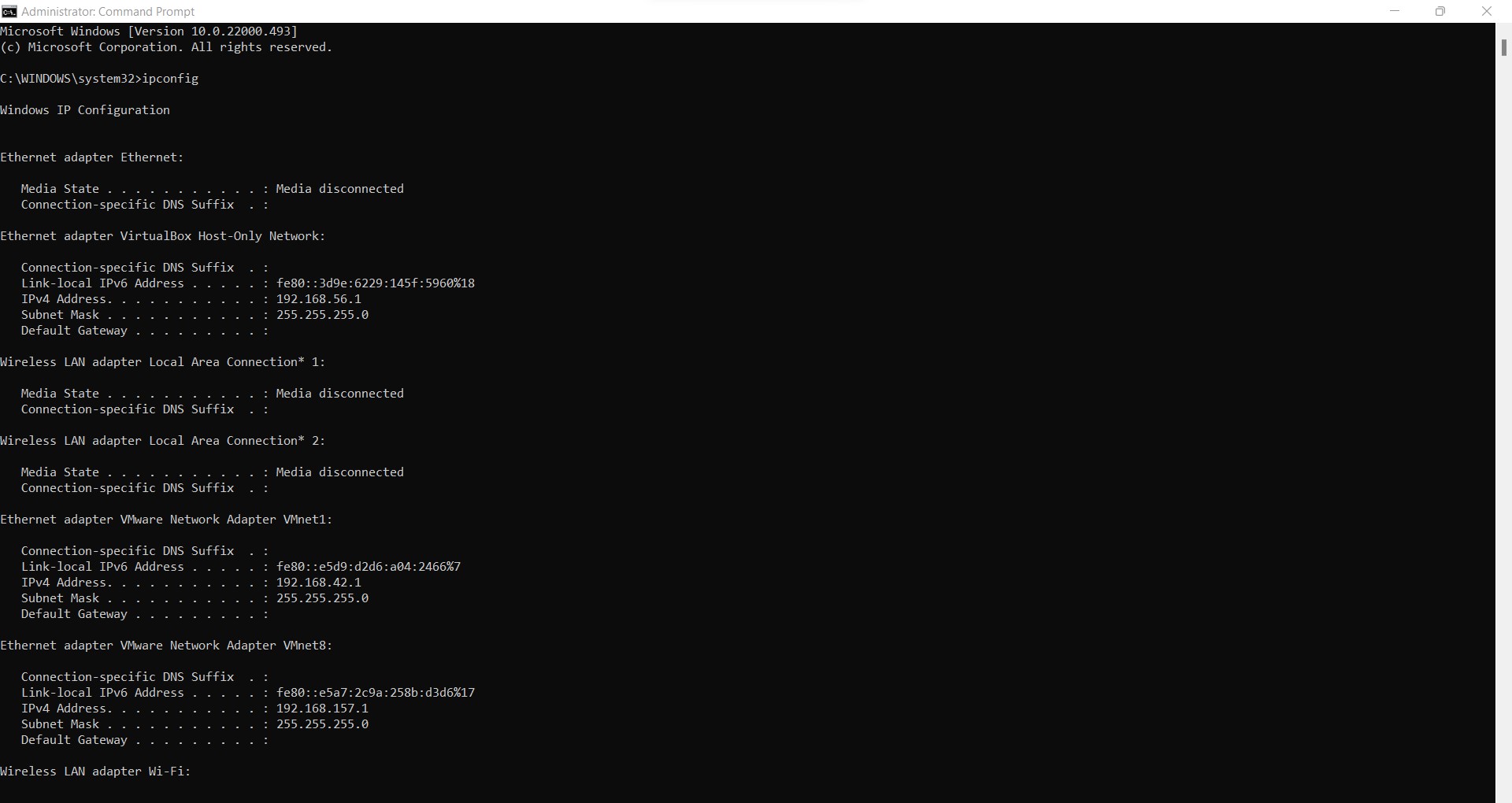




Observations:

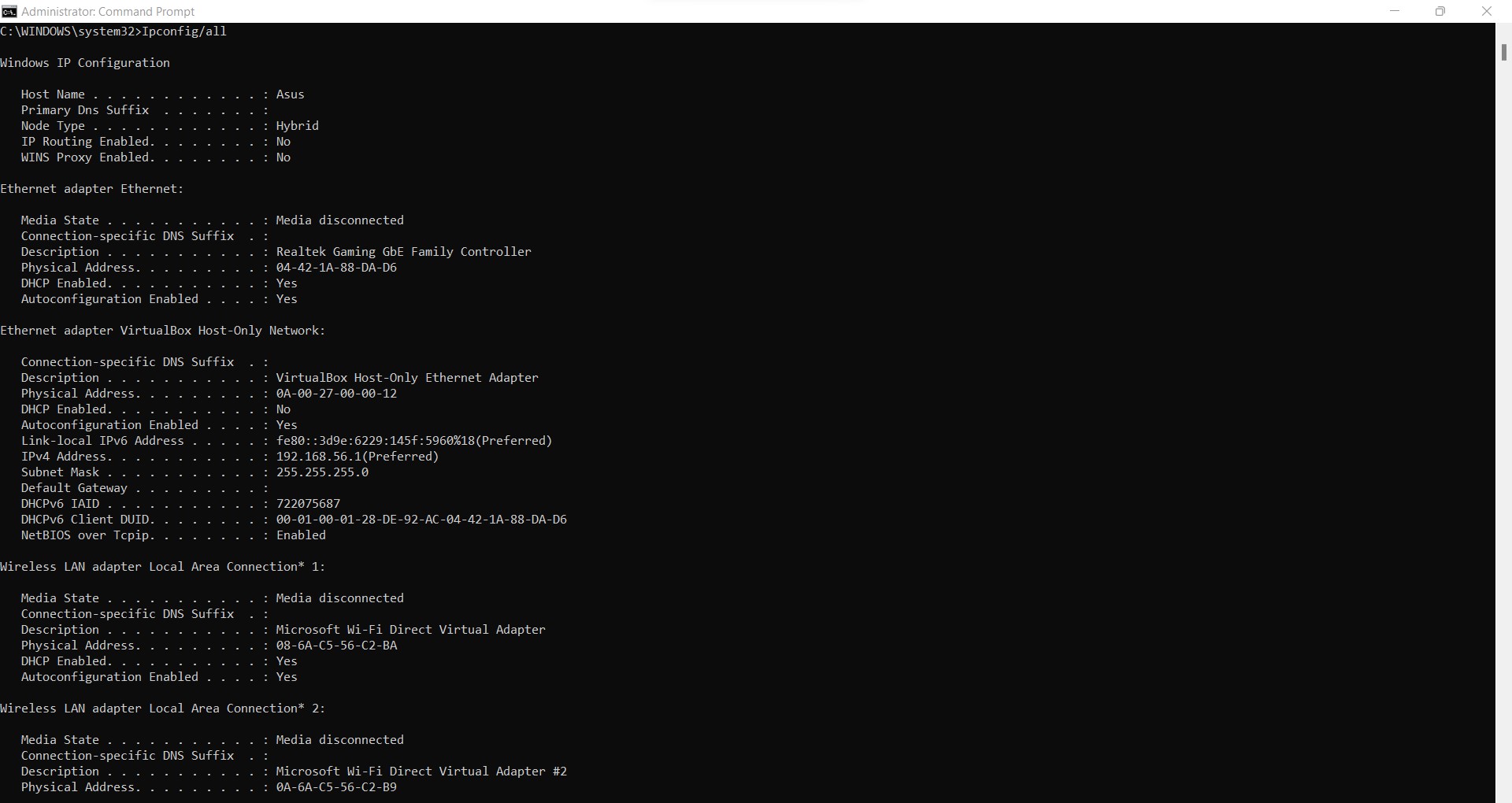
* The network connection window gives the details about physical address, IPv4 and IPv6 address, lease obtained and lease expired, its network type and its availability in the current windows system.
* The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
* When you enable DHCP, it means you allow DHCP server to automatically assign IP address for your device, so you don't need to manually type the IP address and DNS for your computer from time to time.
* The IPv4 address is a 32-bit number that uniquely identifies a network interface on a machine.
* IPv6 (Internet Protocol version 6) is the sixth revision to the Internet Protocol and the successor to IPv4. It functions similarly to IPv4 in that it provides the unique IP addresses necessary for Internet-enabled devices to communicate.
* Subnet masks (IPv4) and prefixes (IPv6) identify the range of IP addresses that make up a subnet, or group of IP addresses on the same network.
* The lease obtained is simply stating when your computer received it's IP address. The lease expiration is when your computer will renew it's IP address with the DHCP server.
* A default gateway is the node in a computer network using the Internet protocol suite that serves as the forwarding host to other networks when no other route specification matches the destination IP address of a packet.
* Domain Name System is the Internet's system for converting alphabetic names into numeric IP addresses.

Task 2: Identifying current TCP/IP network configuration values using IPCONFIG



This command (ipconfig) allows you to get the IP address information of a Windows computer. It also allows some control over active TCP/IP connections.

1. Ipconfig/all



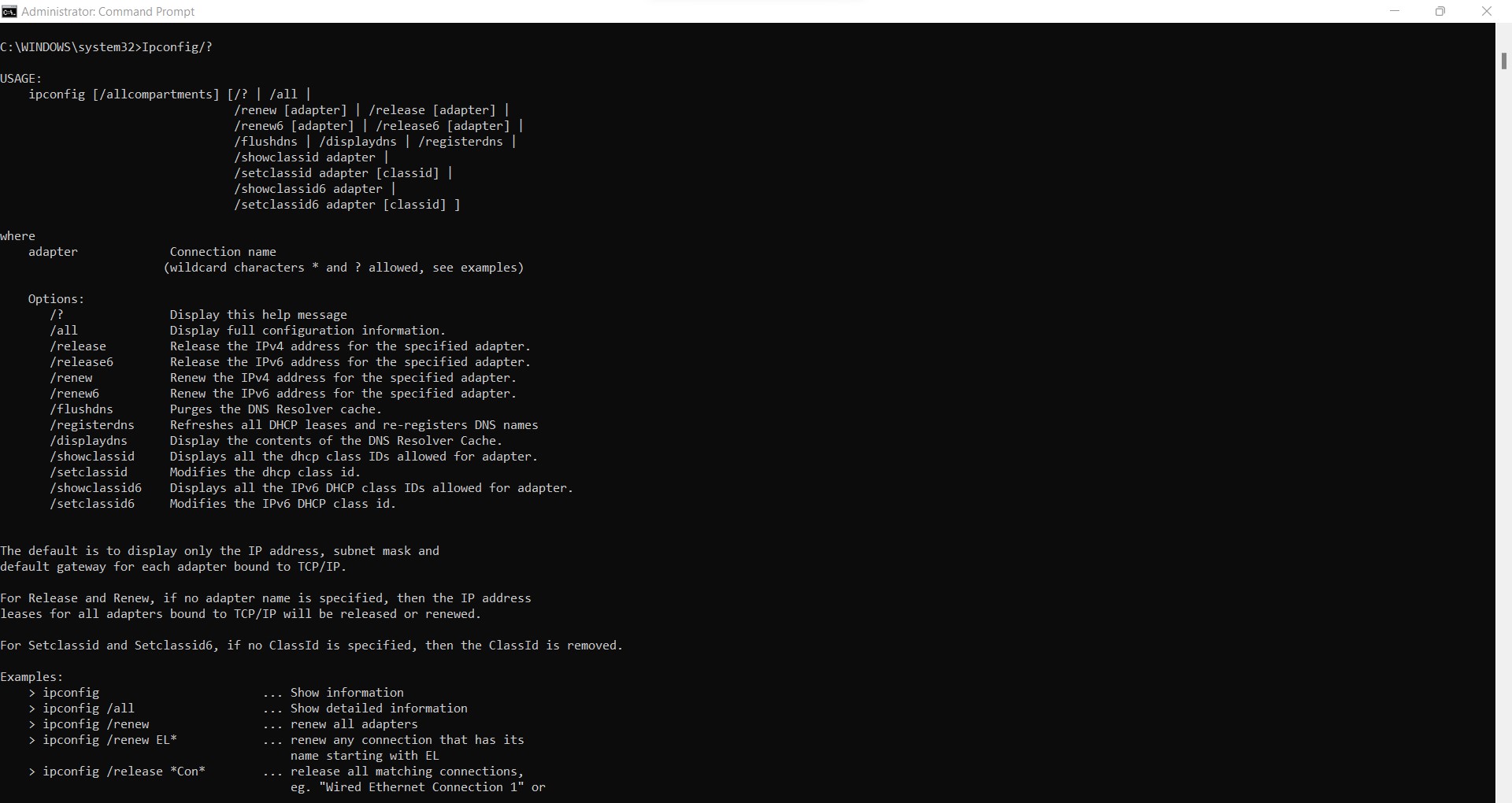
The ipconfig /all command displays all configuration information for each adapter bound to TCP/IP.

b. Ipconfig/flushdns



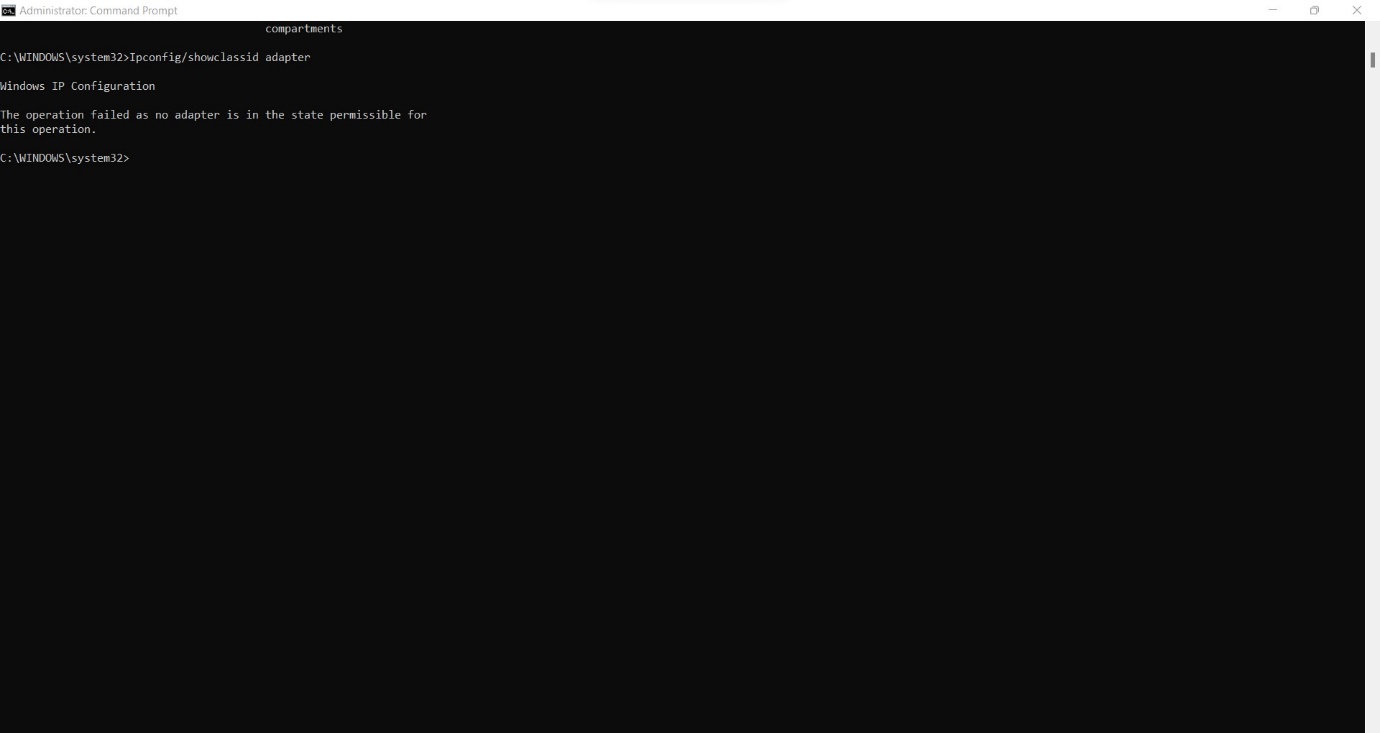
The ipconfig /flushdns command clears the cache of name to IP entries and reloads them from the connected DNS server.

c. Ipconfig/?



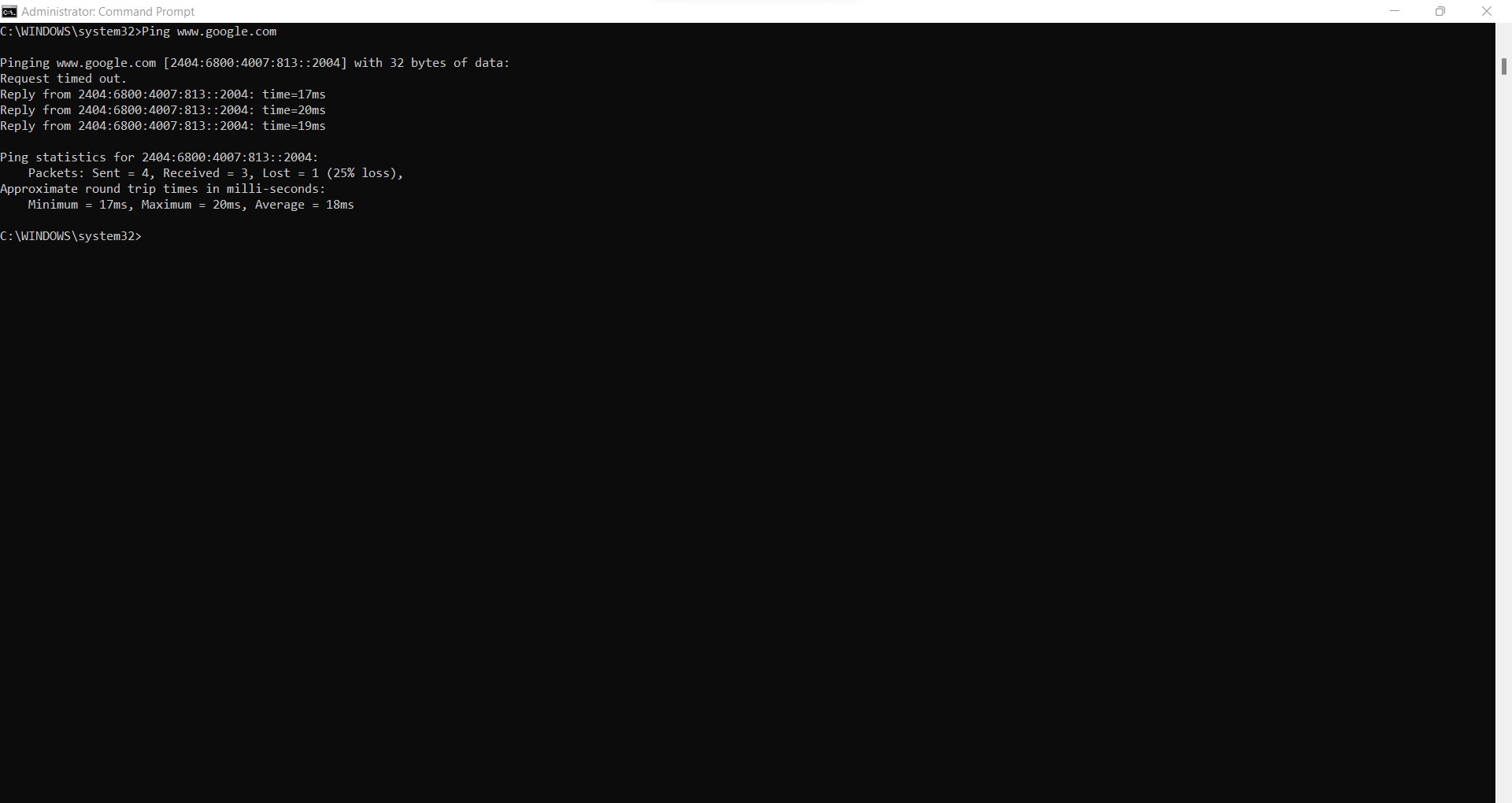
The ipconfig/? command shows the small description of the ipconfig command with all of it’s arguments.

d. Ipconfig/showclassid adapter



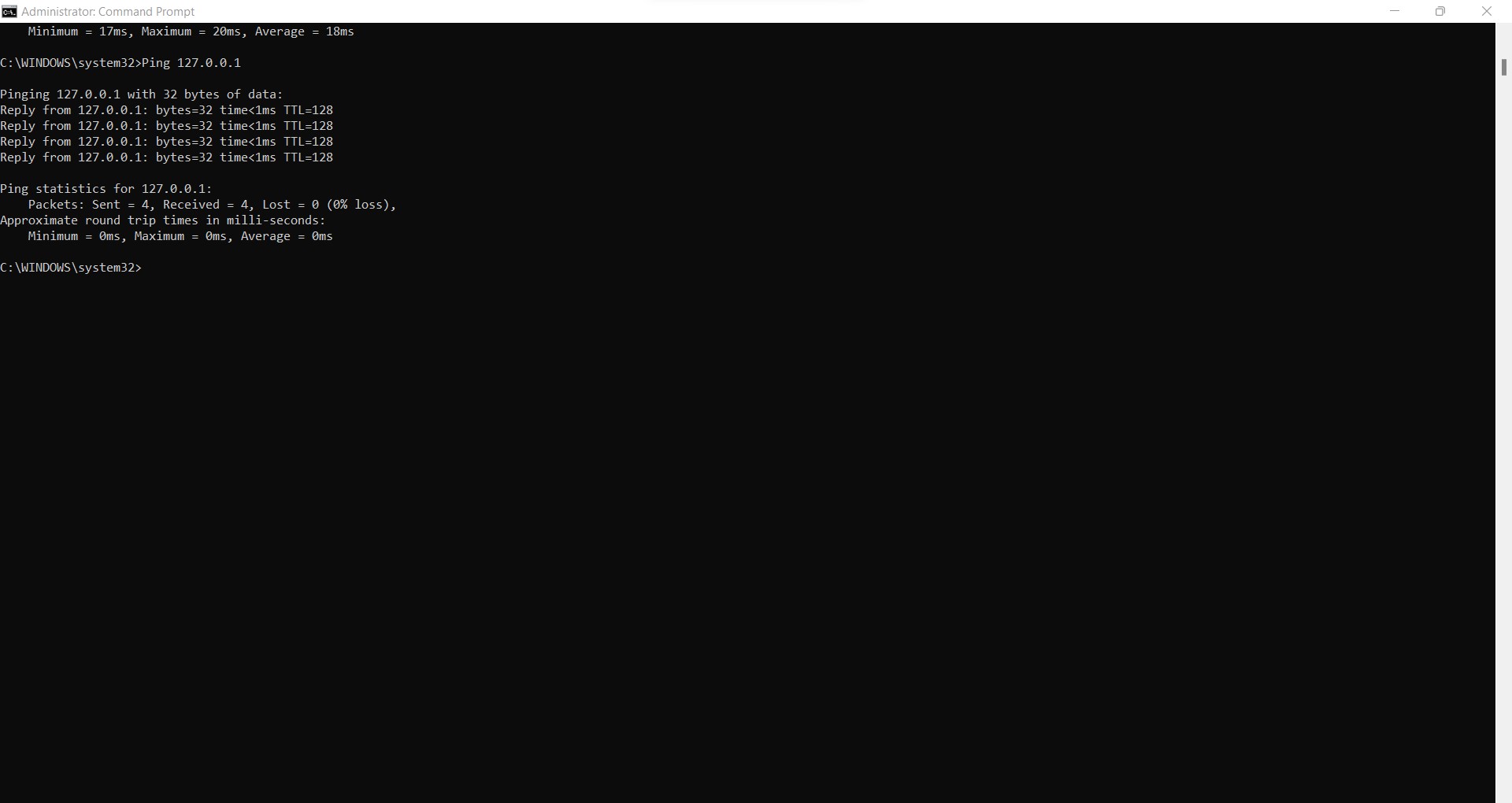
The ipconfig/showclassid adapter command displays the DHCP class IDs allowed for the current adapter, as my current adapter is not state permissible this action has failed.

Task 3: Test the reachability of a host on an Internet using PING

a. Ping [www.google.com](http://www.google.com)

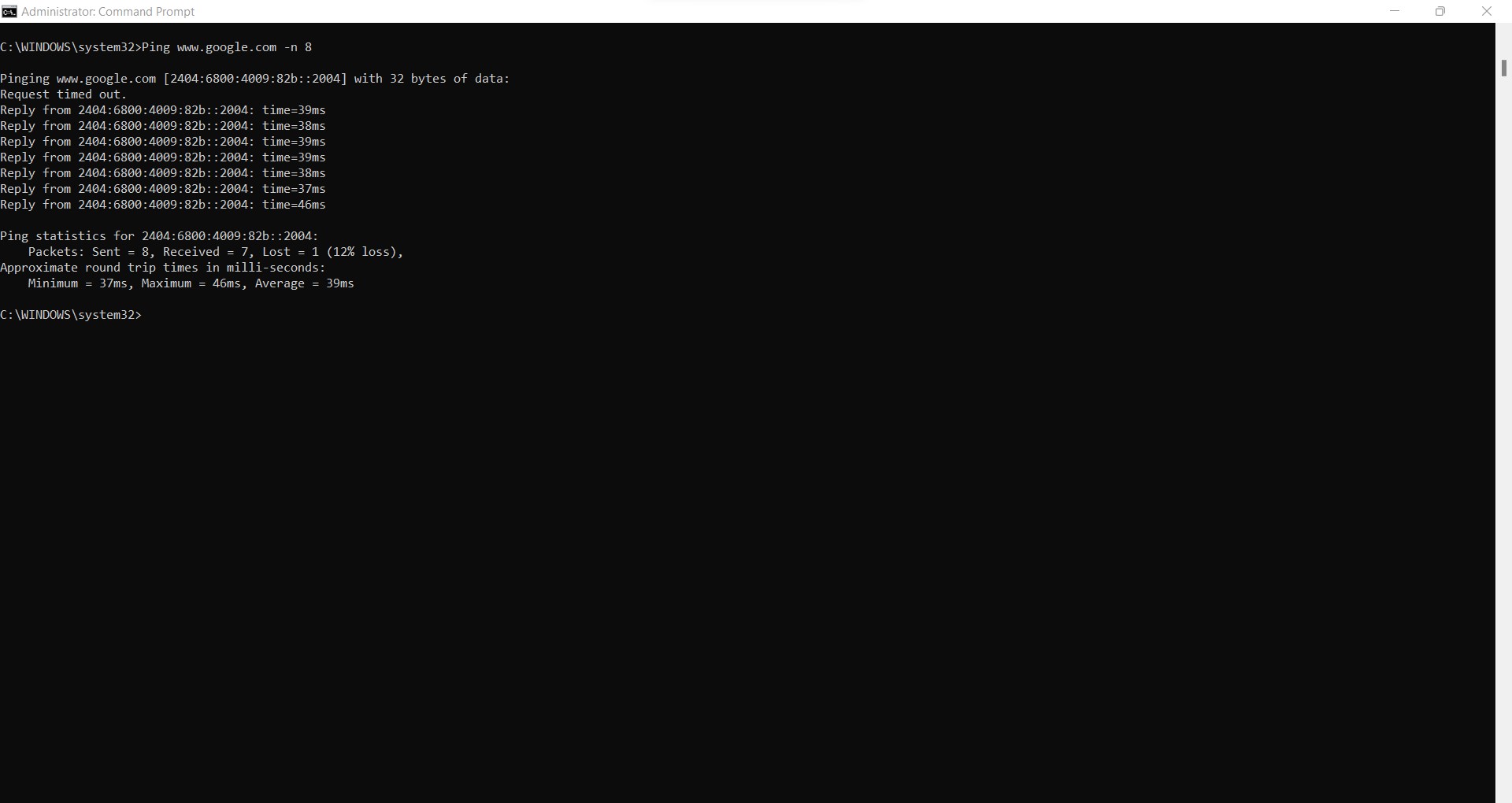
The ping command is used to test if you can reach your target and how much time it will take to do it. When you use this command, you will send few echo requests, usually 4. Then you will receive a result for each of them, that indicates if they were successful, how much data was received, the time it took for the response and TTL (Time to live).

b. Ping 127.0.0.1



The ping command pings the given 127.0.0.1 and sends packets of data to which we get replies from the machine with that IP address, with the important information about the packet loss and the minimum and maximum time taken by that packet.

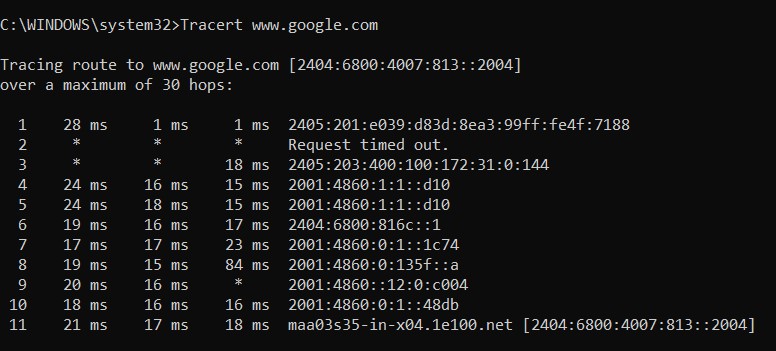
c. Ping www.google.com -n 8



This ping command differs from the first subdivision (a. Ping www.google.com) as now the number of packets sent are controlled by the -n parameter, which here is 8 packets

Task 4: Diagnostic analysis of network using TRACERT

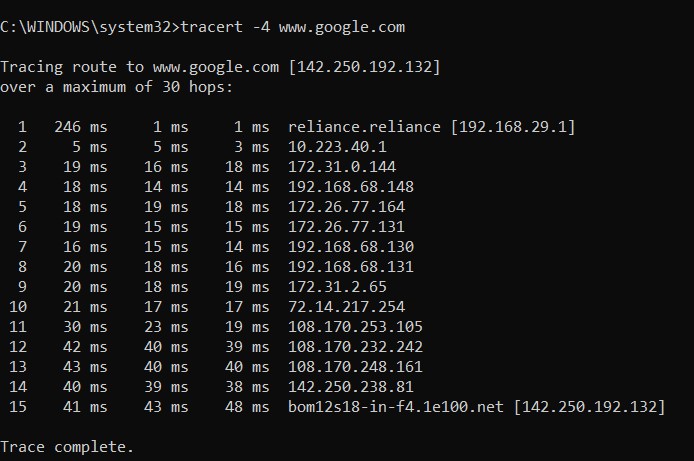
1. a. Tracert www.google.com



Tracert is a command for displaying possible routes (paths) and measuring transit delays of packets across an Internet Protocol (IP) network.

Here, the command gives the detailed information given above while tracerouting the given www.google.com and has shown the output and tabulates it.

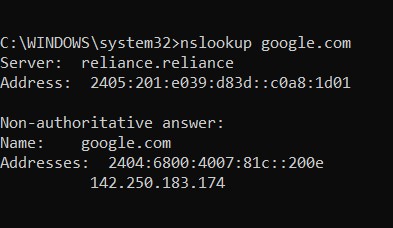
1. b. Tracert -4 www.google.com



The tracert orders the packets to use IPV4 address to travel from the local computer to the domain and displaying possible routes (paths) and measuring transit delays of packets across an IP.

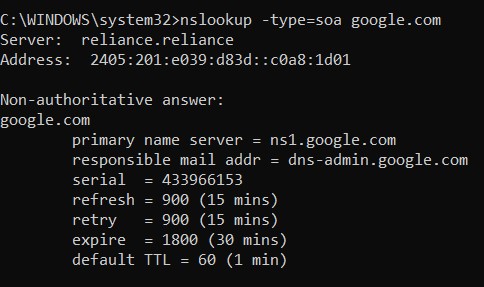
Task 5: Diagnostic analysis of Domain Name service using NSLOOKUP

a. nslookup google.com



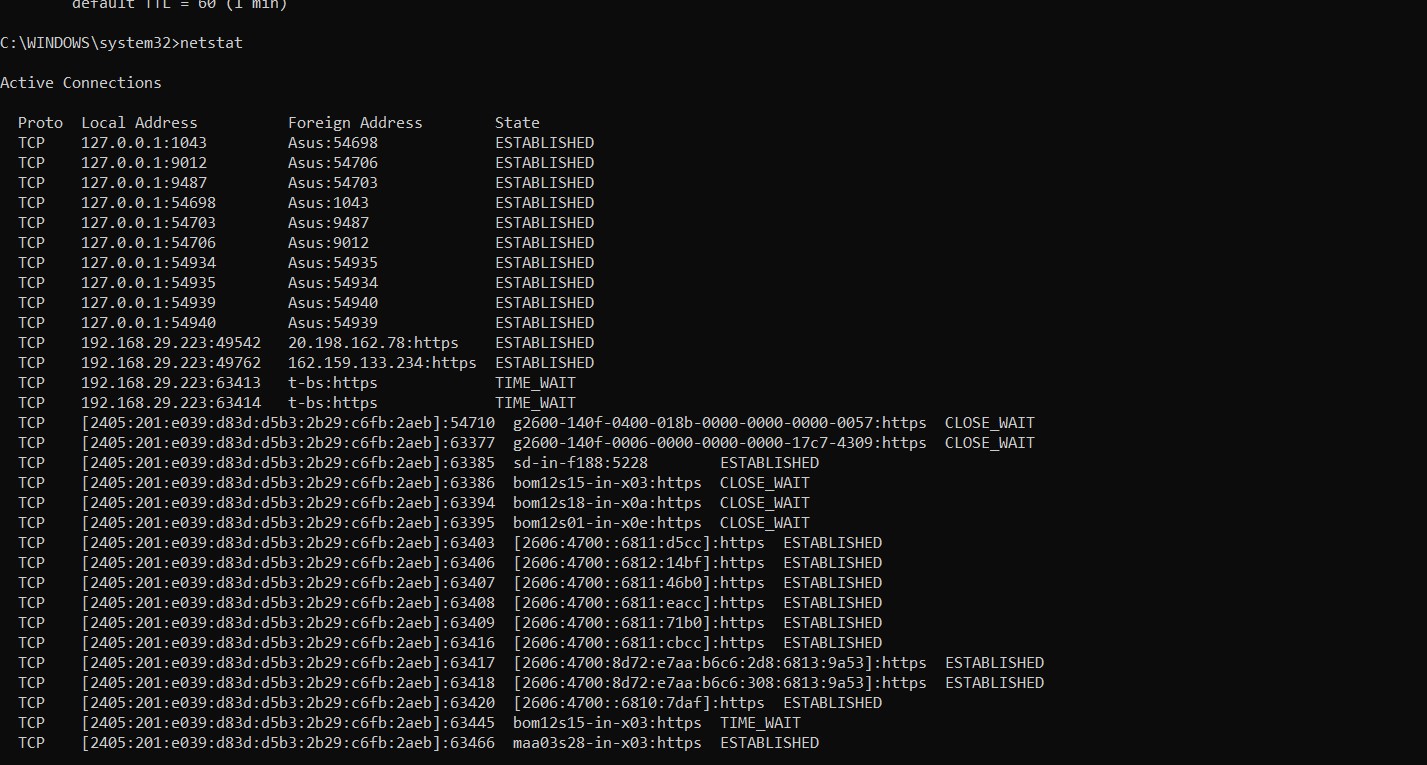
The nslookup command retrieves the relevant address information directly from the DNS cache of name servers, a process which can be achieved through two different modes that the user can choose from. Here it is google and displays the relevant address information.

b. nslookup -type=soa google.com



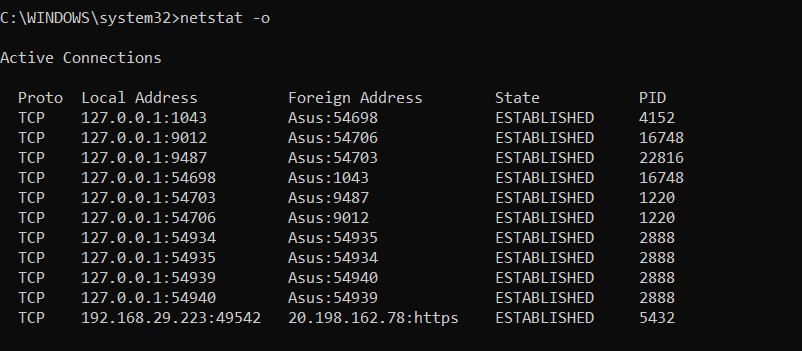
This command queries the DNS server for a resource record of a domain and displays it.

Task 6: Analyzing Network Statistics using NETSTAT, ARP

a. Netstat

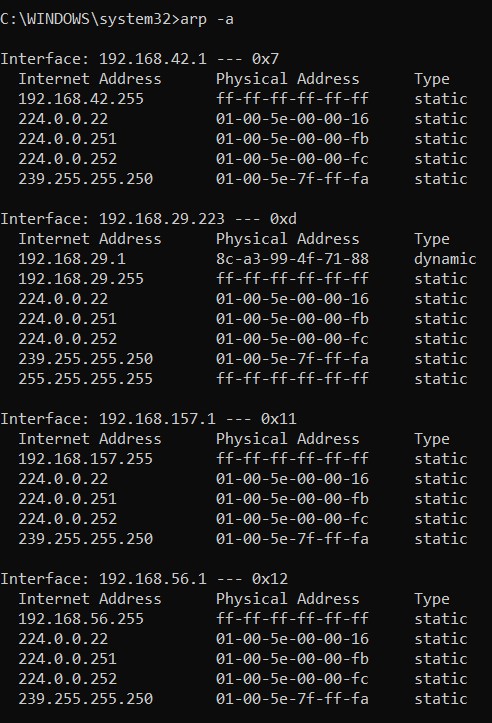
The netstat command delivers basic statistics on all network activities and informs users on which ports and addresses the corresponding connections (TCP, UDP) are running and which ports are open for tasks.

b. Netstat –o



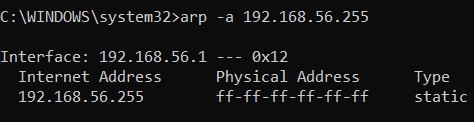
This command displays information same as netstat along with the process identifier (PID) associated with each displayed connection.

c. Arp –a



The arp command displays the internet to adapter address translation tables used by the address in networking, the -a parameter makes it display all the entries of the ARP table.

d. arp –a IP Address



The arp command displays the internet to adapter address translation tables used by the address in networking , the -a parameter makes it display all the entries of the ARP table along with its physical address and it’s type.