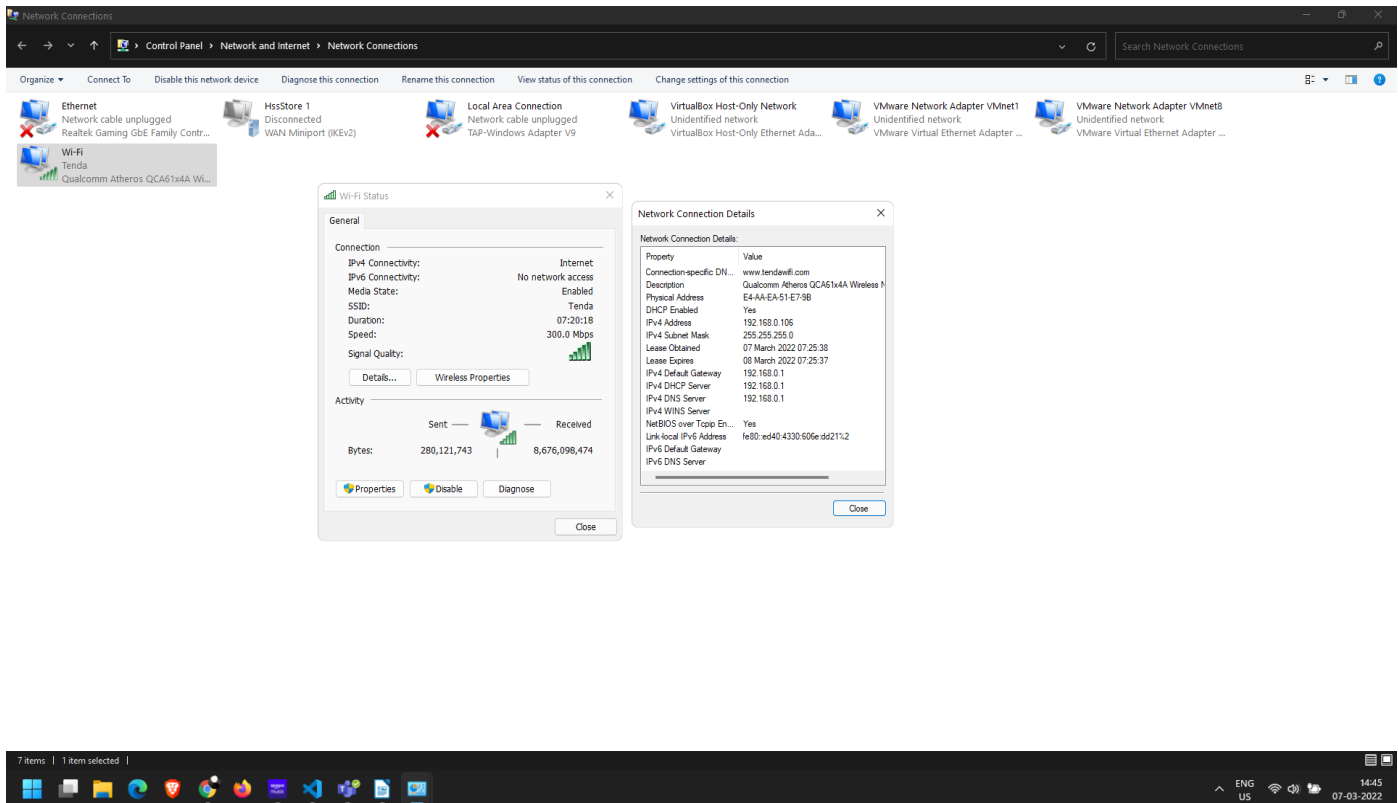


# 20CYS114 -Cyber Security Essentials Labs

## Task 1: Find the status of your Active network.



Time since the internet connected(Duration): 07hours, 20minutes, 18seconds.

We can see speed and signal quality in the wifi-status.

Also, we can see the bytes sent and received.

On the right, we can see the IPV4 address and IPV4 subnet mask, also IPV4 Default gateway, IPV4 DHCP and IPV4 DNS server. Also, we can see the mac address(physical address).

On right dialogue-box, we can see lease obtained and lease expired. That is DHCP-assigned(automatic) IP address is not permanent and expires in about 24 hours.

We can also view the name of our network adapters.

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

```
Select Administrator: Command Prompt

Wireless LAN adapter Local Area Connection* 2:

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

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::946a14fca:33d1:815e%10
    IPv4 Address. . . . . : 192.168.98.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::d9c8:8434:c4b2:ef90%8
    IPv4 Address. . . . . : 192.168.175.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : www.tendawifi.com
    Link-local IPv6 Address . . . . . : fe80::ed40:4330:606e:dd21%2
    IPv4 Address. . . . . : 192.168.0.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\Windows\system32>
```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : www.tendawifi.com  
Link-local IPv6 Address . . . . : fe80::ed50:4330:606e:dd21%2  
IPv4 Address. . . . . : 192.168.0.106  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.0.1

we can see the IPV4 address and subnet mask, also Default gateway. Also, we can see the mac address(physical address).

---

**ipconfig/all**- Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

```
Administrator: Command Prompt
C:\Windows\system32>ipconfig/all

Windows IP Configuration

Host Name . . . . . : zeus
Primary Dns Suffix . . . . . : 
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : www.tendawifi.com

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Realtek Gaming GbE family controller
Physical Address. . . . . : 88-97-98-8E-8C-43
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . : 
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-00
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::397a:6119:29a0:d253:(Preferred)
IPv6 Address. . . . . : 192.168.98.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
Dhcpv6 Iaid . . . . . : 648521255
Dhcpv6 Client DUID. . . . . : 00-01-00-01-29-2A-AB-0F-08-97-98-8E-8C-43
NetBIOS over Tcpip. . . . . : Enabled

Unknown adapter Local Area Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : TAP-Windows Adapter V9
Physical Address. . . . . : 80-FF-BE-49-AB-A3
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : E6-AA-EA-51-67-98
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : F6-AA-EA-51-67-98
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . : 
Description . . . . . : VMware virtual ethernet adapter for VMnet1
Physical Address. . . . . : 00-50-56-C0-00-01
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::946a:4fc3:33d1:8156:(Preferred)
IPv6 Address. . . . . : 192.168.98.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 07 March 2022 07:25:53
Lease Expires . . . . . : 07 March 2022 15:40:34
Default Gateway . . . . . : 
Dhcp Server . . . . . : 192.168.98.254
```

**ipconfig/flushdns** -Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

```
Administrator: Command Prompt
C:\Windows\system32>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>
```

## ipconfig/? -Displays Help at the command prompt.

```
Administrator: Command Prompt
C:\Windows\system32>ipconfig/?

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, see examples)

Options:
    /?                Display this help message.
    /all              Display full configuration information.
    /release          Release the IPv4 address for the specified adapter.
    /release6         Release the IPv6 address for the specified adapter.
    /renew            Renew the IPv4 address for the specified adapter.
    /renew6           Renew the IPv6 address for the specified adapter.
    /flushdns         Purges 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 allowed for adapter.
    /setclassid       Modifies the dhcp class id.
    /showclassid6     Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6      Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
> ipconfig           ... Show information
> ipconfig /all      ... Show detailed information
> ipconfig /renew     ... Renew all adapters
> ipconfig /renew EL* ... Renew any connection that has its
                        name starting with EL
> ipconfig /release *Con* ... Release all matching connections,
                        eg. "Wired Ethernet Connection 1" or
                        "Wired Ethernet Connection 2"
> ipconfig /allcompartments ... Show information about all
                        compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                        compartments

C:\Windows\system32>
```

## ipconfig/showclassid -Displays the DHCP class ID for a specified adapter. To see the DHCP class ID for all adapters, use the asterisk (\*) wildcard character in place of *adapter*. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically.

```
Administrator: Command Prompt
There are no DHCPv4 classes defined for Wi-Fi.
C:\Windows\system32>ipconfig/setclassid "Wi-Fi" test
Windows IP Configuration
Successfully set the DHCPv4 class id for adapter Wi-Fi.
C:\Windows\system32>ipconfig/showclassid "Wi-Fi"
Windows IP Configuration
There are no DHCPv4 classes defined for Wi-Fi.
C:\Windows\system32>ipconfig/setclassid "Wi-Fi"
Windows IP Configuration
Successfully set the DHCPv4 class id for adapter Wi-Fi.
C:\Windows\system32>ipconfig/showclassid "Wi-Fi"
Windows IP Configuration
There are no DHCPv4 classes defined for Wi-Fi.
C:\Windows\system32>ipconfig/showclassid *
Windows IP Configuration
Unable to modify the DHCPv4 class id for adapter Ethernet: The system cannot find the file specified.
There are no DHCPv4 classes defined for VirtualBox Host-Only Network.
Unable to modify the DHCPv4 class id for adapter Local Area Connection: The system cannot find the file specified.
Unable to modify the DHCPv4 class id for adapter Local Area Connection* 1: The system cannot find the file specified.
Unable to modify the DHCPv4 class id for adapter Local Area Connection* 2: The system cannot find the file specified.
There are no DHCPv4 classes defined for VMware Network Adapter VMnet1.
There are no DHCPv4 classes defined for VMware Network Adapter VMnet8.
There are no DHCPv4 classes defined for Wi-Fi.
Unable to modify the DHCPv4 class id for adapter Loopback Pseudo-Interface 1: The system cannot find the file specified.
C:\Windows\system32>
```

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

ping command used to test the reachability of a host on an Internet Protocol network.

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

```
Administrator: Command Prompt
C:\Windows\system32>ping www.google.com

Pinging www.google.com [142.250.183.228] with 32 bytes of data:
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56
Reply from 142.250.183.228: bytes=32 time=13ms TTL=56
Reply from 142.250.183.228: bytes=32 time=10ms TTL=56
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56

Ping statistics for 142.250.183.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 13ms, Average = 10ms

C:\Windows\system32>
```

### Ping 127.0.0.1

```
Administrator: Command Prompt
C:\Windows\system32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

## Ping www.google.com-n 8

```
Administrator: Command Prompt
C:\Windows\system32>ping www.google.com -n 8
Ping request could not find host www.google.com-n. Please check the name and try again.

C:\Windows\system32>ping www.google.com -n 8

Pinging www.google.com [142.250.183.228] with 32 bytes of data:
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56
Reply from 142.250.183.228: bytes=32 time=10ms TTL=56
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56
Reply from 142.250.183.228: bytes=32 time=16ms TTL=56
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56
Reply from 142.250.183.228: bytes=32 time=9ms TTL=56

Ping statistics for 142.250.183.228:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 16ms, Average = 10ms

C:\Windows\system32>
```

## Task 4: Diagnostic analysis of network using TRACERT

is computer network diagnostic commands for displaying possible routes and measuring transit delays of packets across an Internet Protocol network.

**tracert www.google.com**

```
Administrator: Command Prompt

C:\Windows\system32>Tracert www.google.com

Tracing route to www.google.com [142.250.183.228]
over a maximum of 30 hops:

  0  2 ms    2 ms    4 ms  192.168.0.1
  1  5 ms    4 ms    4 ms  100.114.0.1
  2  9 ms    9 ms    9 ms  172.31.200.207
  3  14 ms   10 ms   10 ms  172.31.200.112
  4  8 ms    9 ms    9 ms  100.100.107.96
  5  8 ms    8 ms   10 ms  100.100.107.97
  6  9 ms    9 ms    9 ms  172.31.170.26
  7  12 ms   10 ms   10 ms  ws135-195-133-112.rc11.gov.in [112.133.192.135]
  8  10 ms   10 ms   10 ms  142.251.227.213
  9  10 ms   10 ms   10 ms  209.85.247.251
 10  15 ms   13 ms   15 ms  maa05s23-in-f4.1e100.net [142.250.183.228]

Trace complete.

C:\Windows\system32>
```

**tracert -4 [www.google.com](http://www.google.com)**  
(-4 forces tracert to use IPv4 only.)

```
Administrator: Command Prompt

C:\Windows\system32>Tracert www.google.com

Tracing route to www.google.com [142.250.183.228]
over a maximum of 30 hops:

  0  2 ms    2 ms    4 ms  192.168.0.1
  1  5 ms    4 ms    4 ms  100.114.0.1
  2  9 ms    9 ms    9 ms  172.31.200.207
  3  14 ms   10 ms   10 ms  172.31.200.112
  4  8 ms    9 ms    9 ms  100.100.107.96
  5  8 ms    8 ms   10 ms  100.100.107.97
  6  9 ms    9 ms    9 ms  172.31.170.26
  7  12 ms   10 ms   10 ms  ws135-195-133-112.rc11.gov.in [112.133.192.135]
  8  10 ms   10 ms   10 ms  142.251.227.213
  9  10 ms   10 ms   10 ms  209.85.247.251
 10  15 ms   13 ms   15 ms  maa05s23-in-f4.1e100.net [142.250.183.228]

Trace complete.

C:\Windows\system32>tracert -4 www.google.com

Tracing route to www.google.com [142.250.183.228]
over a maximum of 30 hops:

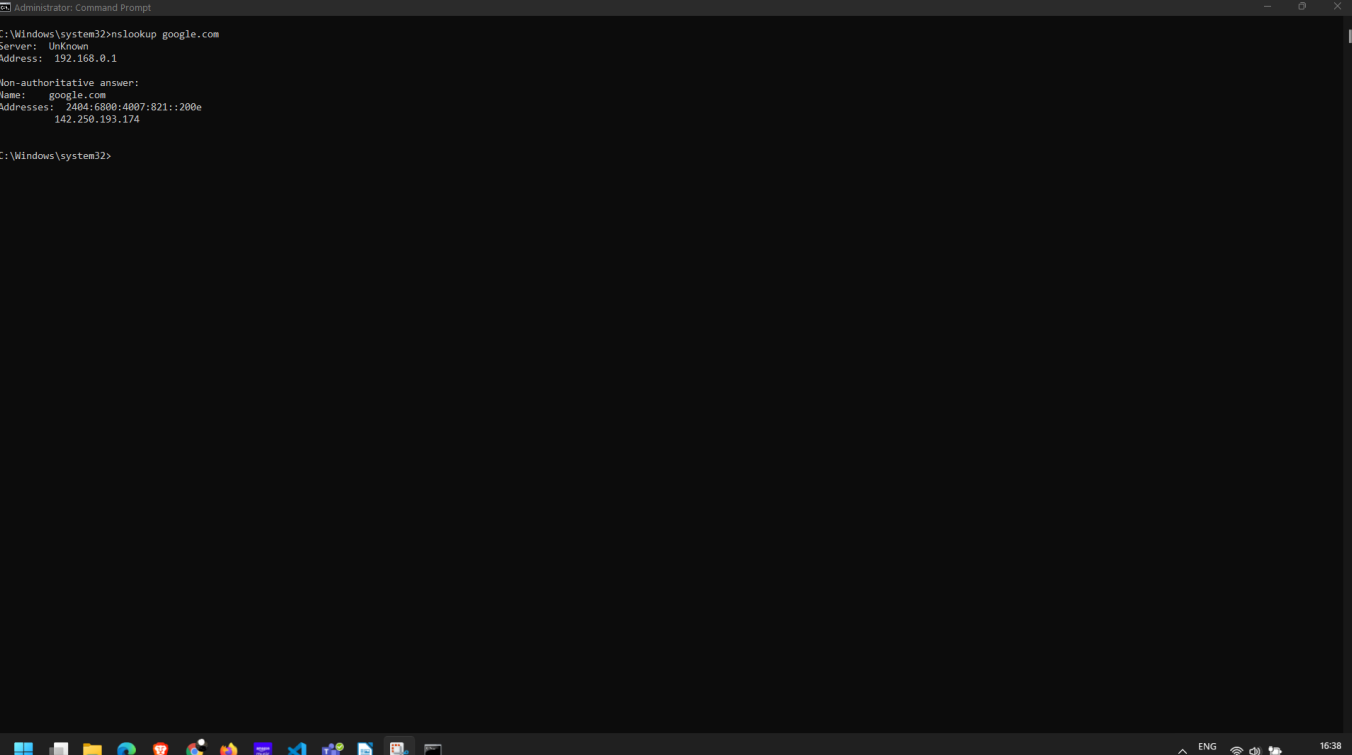
  0  2 ms    5 ms    3 ms  192.168.0.1
  1  5 ms    6 ms    4 ms  100.114.0.1
  2  12 ms   9 ms   13 ms  172.31.200.207
  3  9 ms    9 ms   11 ms  172.31.200.112
  4  12 ms   13 ms    9 ms  100.100.107.96
  5  8 ms    9 ms   21 ms  100.100.107.97
  6  9 ms    9 ms   10 ms  172.31.170.26
  7  15 ms   10 ms   10 ms  ws135-195-133-112.rc11.gov.in [112.133.192.135]
  8  10 ms   10 ms    9 ms  142.251.227.213
  9  10 ms   14 ms    9 ms  209.85.247.251
 10  9 ms    9 ms    9 ms  maa05s23-in-f4.1e100.net [142.250.183.228]

Trace complete.

C:\Windows\system32>
```

## Task 5: Diagnostic analysis of Domain Name service using NSLOOKUP

nslookup is a network administration command-line tool for querying the Domain Name System to obtain the mapping between domain name and IP address, or other



```
Administrator: Command Prompt
C:\Windows\system32>nslookup google.com
Server: Unknown
Address: 192.168.0.1

Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4007:821::200e
          142.250.193.174


C:\Windows\system32>
```

DNS records.

**nslookup -type=soa google.com**



# Syntax

 Copy

```
set type=<resourcerecordtype>
```

## Parameters

### Parameter

### Description

**<resourcerecordtype>**

Specifies a DNS resource record type. The default resource record type is **A**, but you can use any of the following values:

- **A**: Specifies a computer's IP address.
- **ANY**: Specifies a computer's IP address.
- **CNAME**: Specifies a canonical name for an alias.
- **GID**: Specifies a group identifier of a group name.
- **HINFO**: Specifies a computer's CPU and type of operating system.
- **MB**: Specifies a mailbox domain name.
- **MG**: Specifies a mail group member.
- **MINFO**: Specifies mailbox or mail list information.
- **MR**: Specifies the mail rename domain name.
- **MX**: Specifies the mail exchanger.
- **NS**: Specifies a DNS name server for the named zone.
- **PTR**: Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information.
- **SOA**: Specifies the start-of-authority for a DNS zone.
- **TXT**: Specifies the text information.
- **UID**: Specifies the user identifier.
- **UINFO**: Specifies the user information.
- **WKS**: Describes a well-known service.

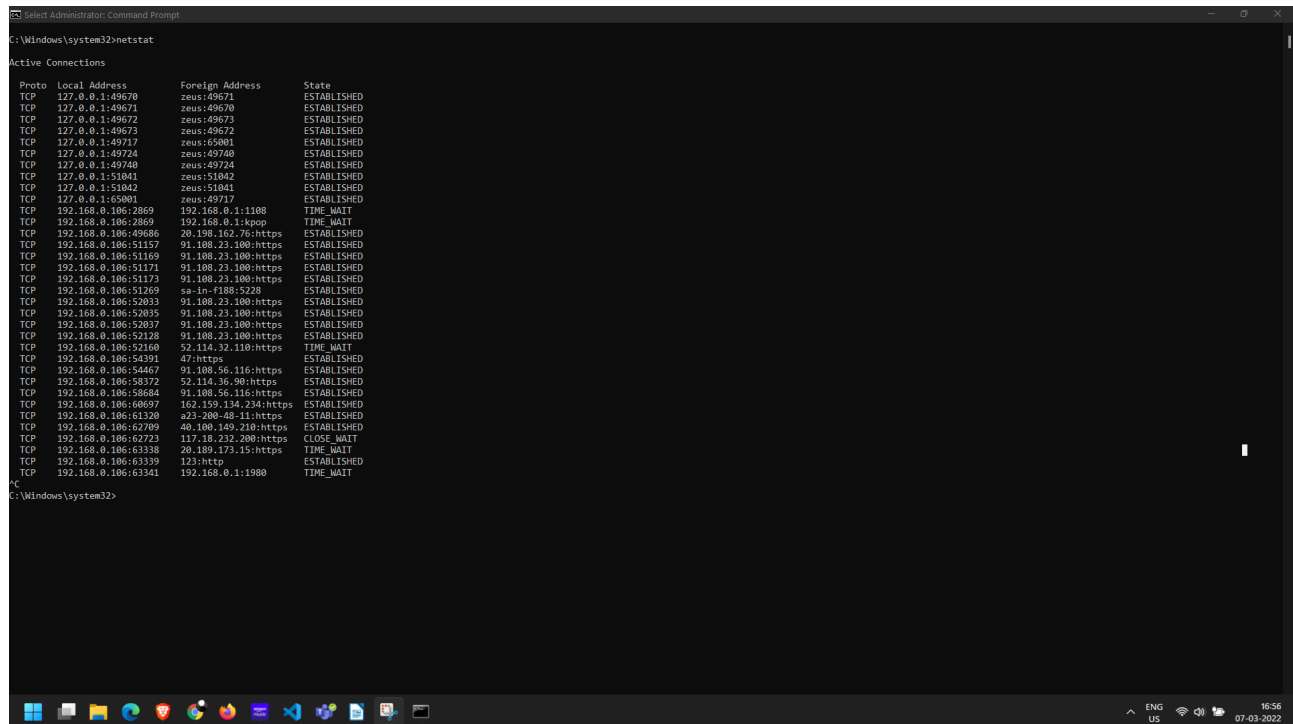
```
Administrator: Command Prompt
C:\Windows\system32>nslookup -type=soa google.com
Server: Unknown
Address: 192.168.0.1

Non-authoritative answer:
google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial = 422753714
    refresh = 900 (15 mins)
    retry = 900 (15 mins)
    expire = 1800 (30 mins)
    default TTL = 60 (1 min)

C:\Windows\system32>
```

## Task 6: Analyzing Network Statistics using NETSTAT, ARP

**netstat:** netstat is a command-line network utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics.



```
Select Administrator: Command Prompt
C:\Windows\system32>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:49670          zeus:49671             ESTABLISHED
TCP    127.0.0.1:49671          zeus:49670             ESTABLISHED
TCP    127.0.0.1:49672          zeus:49673             ESTABLISHED
TCP    127.0.0.1:49673          zeus:49672             ESTABLISHED
TCP    127.0.0.1:49717          zeus:65001             ESTABLISHED
TCP    127.0.0.1:49724          zeus:49740             ESTABLISHED
TCP    127.0.0.1:49740          zeus:49724             ESTABLISHED
TCP    127.0.0.1:51041          zeus:51042             ESTABLISHED
TCP    127.0.0.1:51042          zeus:51041             ESTABLISHED
TCP    127.0.0.1:50801          zeus:49717             ESTABLISHED
TCP    192.168.0.106:2869      192.168.0.1:1188       TIME_WAIT
TCP    192.168.0.106:2869      192.168.0.1:kpop       TIME_WAIT
TCP    192.168.0.106:49686     20.198.162.76:https     ESTABLISHED
TCP    192.168.0.106:51157     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:51169     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:51171     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:51173     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:51269     sa-in-f108:5228        ESTABLISHED
TCP    192.168.0.106:52033     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:52035     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:52037     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:52128     91.108.23.100:https     ESTABLISHED
TCP    192.168.0.106:52168     52.114.32.110:https     TIME_WAIT
TCP    192.168.0.106:54391     47:https               ESTABLISHED
TCP    192.168.0.106:54467     91.108.56.116:https     ESTABLISHED
TCP    192.168.0.106:58372     52.114.36.90:https      ESTABLISHED
TCP    192.168.0.106:58684     91.108.56.116:https     ESTABLISHED
TCP    192.168.0.106:60697     162.159.134.234:https   ESTABLISHED
TCP    192.168.0.106:61320     a23-200-48-11:https     ESTABLISHED
TCP    192.168.0.106:62709     40.100.149.210:https    ESTABLISHED
TCP    192.168.0.106:62723     117.18.232.200:https    CLOSE_WAIT
TCP    192.168.0.106:63338     20.189.173.15:https     TIME_WAIT
TCP    192.168.0.106:63339     123:http               ESTABLISHED
TCP    192.168.0.106:63341     192.168.0.1:1980       TIME_WAIT

C:\Windows\system32>
```

**netstat -o** -Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.

```
Administrator: Command Prompt
C:\Windows\system32>netstat -o

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP   127.0.0.1:49670          zeus:49671             ESTABLISHED 5920
TCP   127.0.0.1:49671          zeus:49670             ESTABLISHED 5920
TCP   127.0.0.1:49672          zeus:49673             ESTABLISHED 5920
TCP   127.0.0.1:49673          zeus:49672             ESTABLISHED 5920
TCP   127.0.0.1:49717          zeus:65001             ESTABLISHED 5116
TCP   127.0.0.1:49724          zeus:49740             ESTABLISHED 11208
TCP   127.0.0.1:49740          zeus:49724             ESTABLISHED 11076
TCP   127.0.0.1:51041          zeus:51042             ESTABLISHED 3628
TCP   127.0.0.1:51042          zeus:51041             ESTABLISHED 3628
TCP   127.0.0.1:65001          zeus:49717             ESTABLISHED 5116
TCP   192.168.0.106:49686      20.198.162.76:https    ESTABLISHED 5672
TCP   192.168.0.106:51157      91.108.23.100:https    ESTABLISHED 12844
TCP   192.168.0.106:51169      91.108.23.100:https    ESTABLISHED 12844

C:\Windows\system32>
```

**ARP:** The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. An *ARP cache* is a simple mapping of IP addresses to MAC addresses.

Parameter	Description
<code>[/a [&lt;inetaddr&gt;]</code> <code>[/n &lt;ifaceaddr&gt;]</code>	Displays current arp cache tables for all interfaces. The <code>/n</code> parameter is case-sensitive. To display the arp cache entry for a specific IP address, use <code>arp /a</code> with the <code>inetaddr</code> parameter, where <code>inetaddr</code> is an IP address. If <code>inetaddr</code> is not specified, the first applicable interface is used. To display the arp cache table for a specific interface, use the <code>/n ifaceaddr</code> parameter in conjunction with the <code>/a</code> parameter where <code>inetaddr</code> is the IP address assigned to the interface.
<code>[/g [&lt;inetaddr&gt;]</code> <code>[/n &lt;ifaceaddr&gt;]</code>	Identical to <code>/a</code> .
<code>[/d &lt;inetaddr&gt;]</code> <code>[&lt;ifaceaddr&gt;]</code>	Deletes an entry with a specific IP address, where <code>inetaddr</code> is the IP address. To delete an entry in a table for a specific interface, use the <code>ifaceaddr</code> parameter where <code>ifaceaddr</code> is the IP address assigned to the interface. To delete all entries, use the asterisk (*) wildcard character in place of <code>inetaddr</code> .
<code>[/s &lt;inetaddr&gt;]</code> <code>&lt;etheraddr&gt;</code> <code>[&lt;ifaceaddr&gt;]</code>	Adds a static entry to the arp cache that resolves the IP address <code>inetaddr</code> to the physical address <code>etheraddr</code> . To add a static arp cache entry to the table for a specific interface, use the <code>ifaceaddr</code> parameter where <code>ifaceaddr</code> is an IP address assigned to the interface.
<code>/?</code>	Displays help at the command prompt.

```
Administrator: Command Prompt

C:\Windows\system32>arp -a

Interface: 192.168.0.106 --- 0x2
Internet Address      Physical Address      Type
192.168.0.1           04-95-e6-b0-9d-e0    dynamic
192.168.0.255         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: 192.168.175.1 --- 0x8
Internet Address      Physical Address      Type
192.168.175.254       00-50-56-e6-19-76    dynamic
192.168.175.255       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: 192.168.98.1 --- 0xa
Internet Address      Physical Address      Type
192.168.98.254        00-50-56-e6-c7-a7    dynamic
192.168.98.255        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: 192.168.56.1 --- 0xd
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

C:\Windows\system32>
```

arp -a <ipaddress> this command will display arp entries for that specific or distinct ipaddress.

```
Administrator: Command Prompt

C:\Windows\system32>arp -a

Interface: 192.168.0.106 --- 0x2
Internet Address      Physical Address      Type
192.168.0.1           04-95-e6-b0-9d-e0    dynamic
192.168.0.255         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: 192.168.175.1 --- 0x8
Internet Address      Physical Address      Type
192.168.175.254       00-50-56-e6-19-76    dynamic
192.168.175.255       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: 192.168.98.1 --- 0xa
Internet Address      Physical Address      Type
192.168.98.254        00-50-56-e6-c7-a7    dynamic
192.168.98.255        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: 192.168.56.1 --- 0xd
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

C:\Windows\system32>arp -a 192.168.56.1
No ARP Entries Found.

C:\Windows\system32>arp -a 192.168.98.1
No ARP Entries Found.

C:\Windows\system32>arp -a 192.168.0.106
No ARP Entries Found.

C:\Windows\system32>arp -a 192.168.175.1
No ARP Entries Found.

C:\Windows\system32>
```

Done by,  
Pranav A N [ch.en.u4cys21056]  
Cys 1<sup>st</sup> year, Chennai Campus.