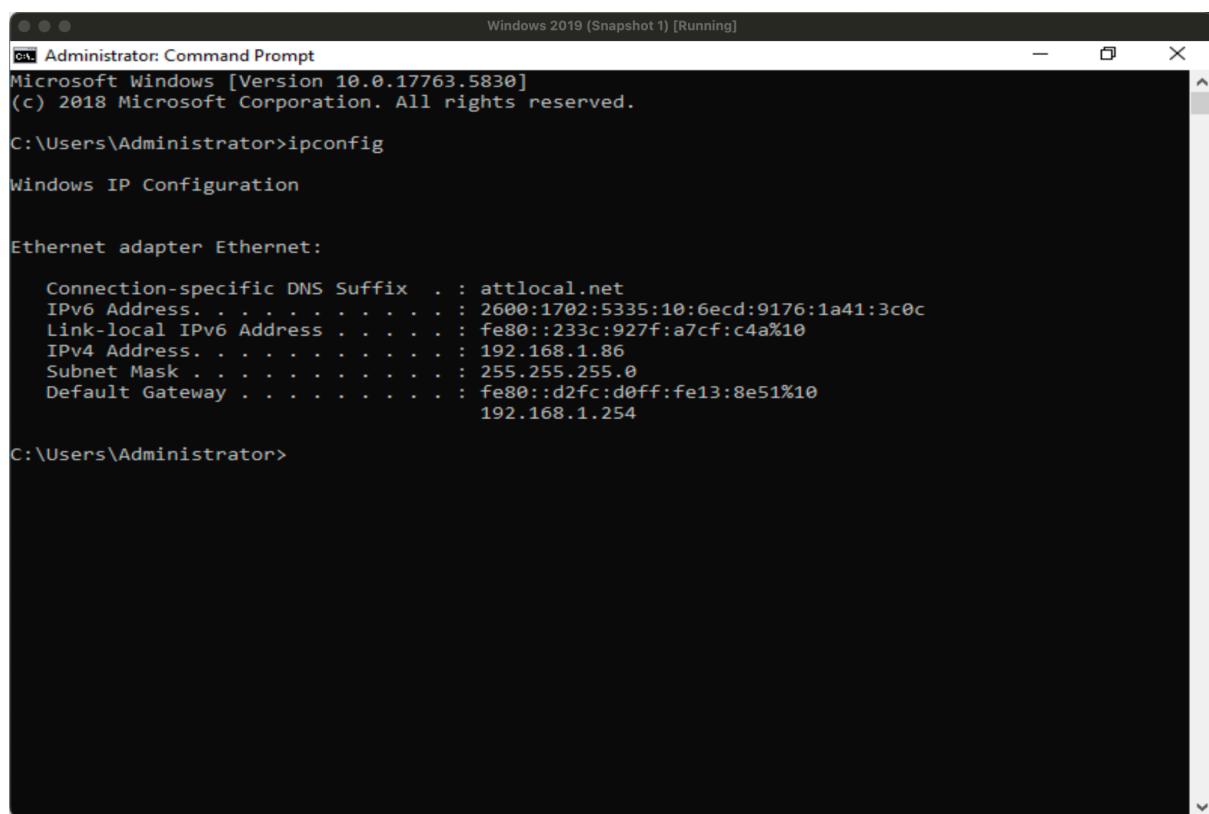


Assignment #1 - Applied Networking Concepts

Networking Stacks in Windows

In Windows, the networking stack provides the infrastructure needed for network communication in Windows-based systems. Interacting with the networking stack entails actions such as configurations and troubleshooting procedures to manage network connections, access resources, and ensure network connectivity. A thorough knowledge of the networking stack is vital for network administrators, developers, and users to effectively manage, configure, and troubleshoot network connections in Windows environments.

The ‘ipconfig’ Command: this command, when run in the Command Prompt, displays the basic IP configuration settings of all network adapters on a Windows computer. It provides information such as the IP address, subnet mask, default gateway, and DNS server addresses. An illustration is shown below:



```
Windows 2019 (Snapshot 1) [Running]
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.5830]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

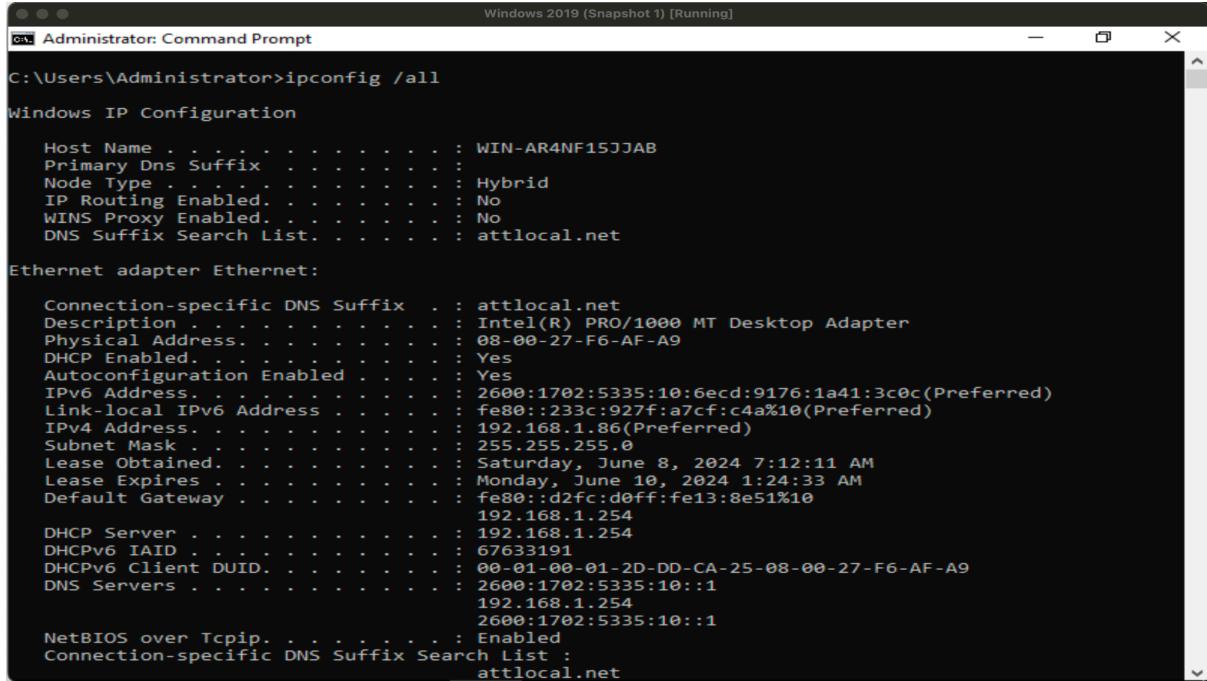
Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : attlocal.net
  IPv6 Address . . . . . : 2600:1702:5335:10:6ecd:9176:1a41:3c0c
  Link-local IPv6 Address . . . . . : fe80::233c:927f:a7cf:c4a%10
  IPv4 Address . . . . . : 192.168.1.86
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::d2fc:d0ff:fe13:8e51%10
                           192.168.1.254

C:\Users\Administrator>
```

The ‘ipconfig /all’ Command: this command provides detailed IP configuration information for all network adapters, including additional details such as the MAC (Media Access Control) address, Dynamic Host Configuration Protocol (DHCP) lease information, and DNS suffix. An illustration is shown below:



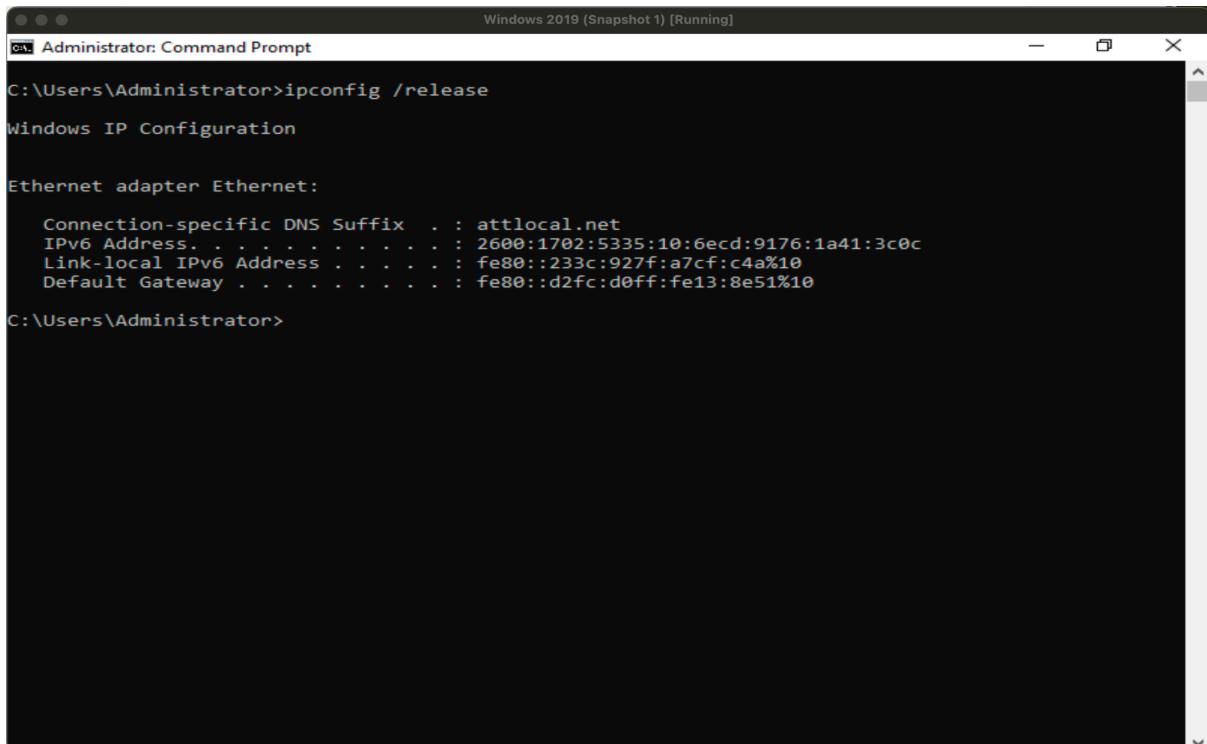
```
Windows 2019 (Snapshot 1) [Running]
Administrator: Command Prompt
C:\Users\Administrator>ipconfig /all
Windows IP Configuration

Host Name . . . . . : WIN-AR4NF15JJAB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : attlocal.net

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : attlocal.net
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-F6-AF-A9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2600:1702:5335:10:6ecd:9176:1a41:3c0c(PREFERRED)
Link-local IPv6 Address . . . . . : fe80::233c:927f:a7cf:c4a%10(PREFERRED)
IPv4 Address . . . . . : 192.168.1.86(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, June 8, 2024 7:12:11 AM
Lease Expires . . . . . : Monday, June 10, 2024 1:24:33 AM
Default Gateway . . . . . : fe80::d2fc:d0ff:fe13:8e51%10
                           192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 67633191
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-DD-CA-25-08-00-27-F6-AF-A9
DNS Servers . . . . . : 2600:1702:5335:10::1
                           192.168.1.254
                           2600:1702:5335:10::1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List. . . . . : attlocal.net
```

The ‘ipconfig /release’ Command: this command cancels the lease on any IP address obtained from a DHCP server for all network adapters on the computer. This makes that particular IP address available for lease to another device. It is illustrated below:



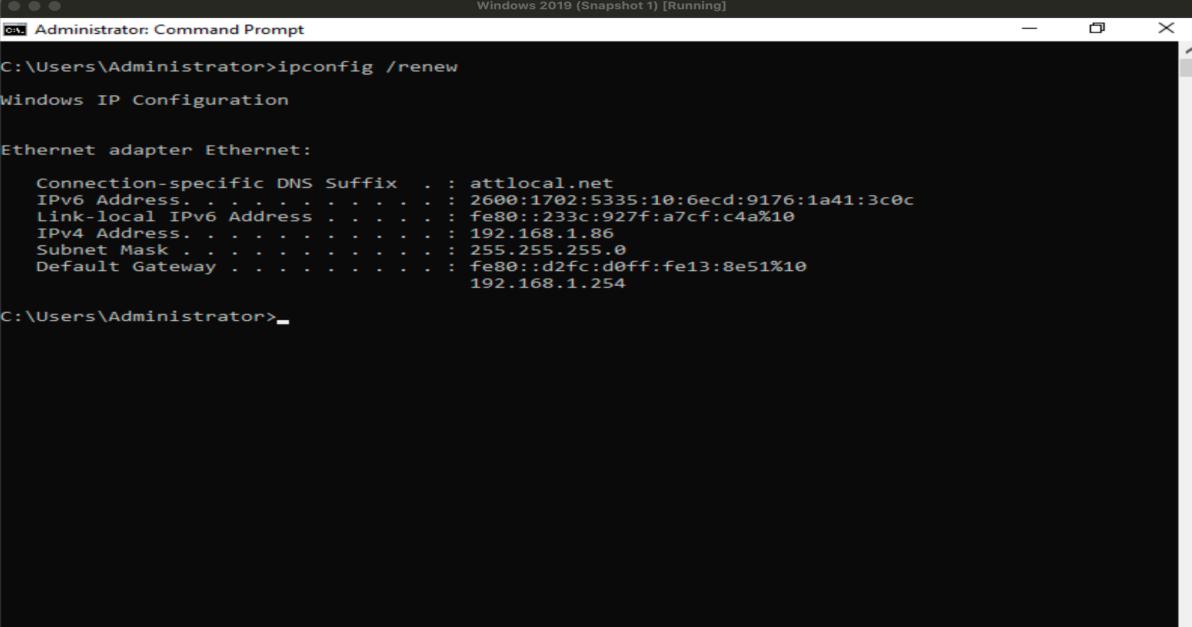
```
Windows 2019 (Snapshot 1) [Running]
Administrator: Command Prompt
C:\Users\Administrator>ipconfig /release
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : attlocal.net
IPv6 Address. . . . . : 2600:1702:5335:10:6ecd:9176:1a41:3c0c
Link-local IPv6 Address . . . . . : fe80::233c:927f:a7cf:c4a%10
Default Gateway . . . . . : fe80::d2fc:d0ff:fe13:8e51%10

C:\Users\Administrator>
```

The ‘ipconfig /renew’ Command: this command reverses the previous command; ipconfig /release. Running the ‘ipconfig /renew’ command sends a request for a new IP address from the DHCP server. This helps to obtain a new IP address or updating DHCP lease information. An illustration is shown below:



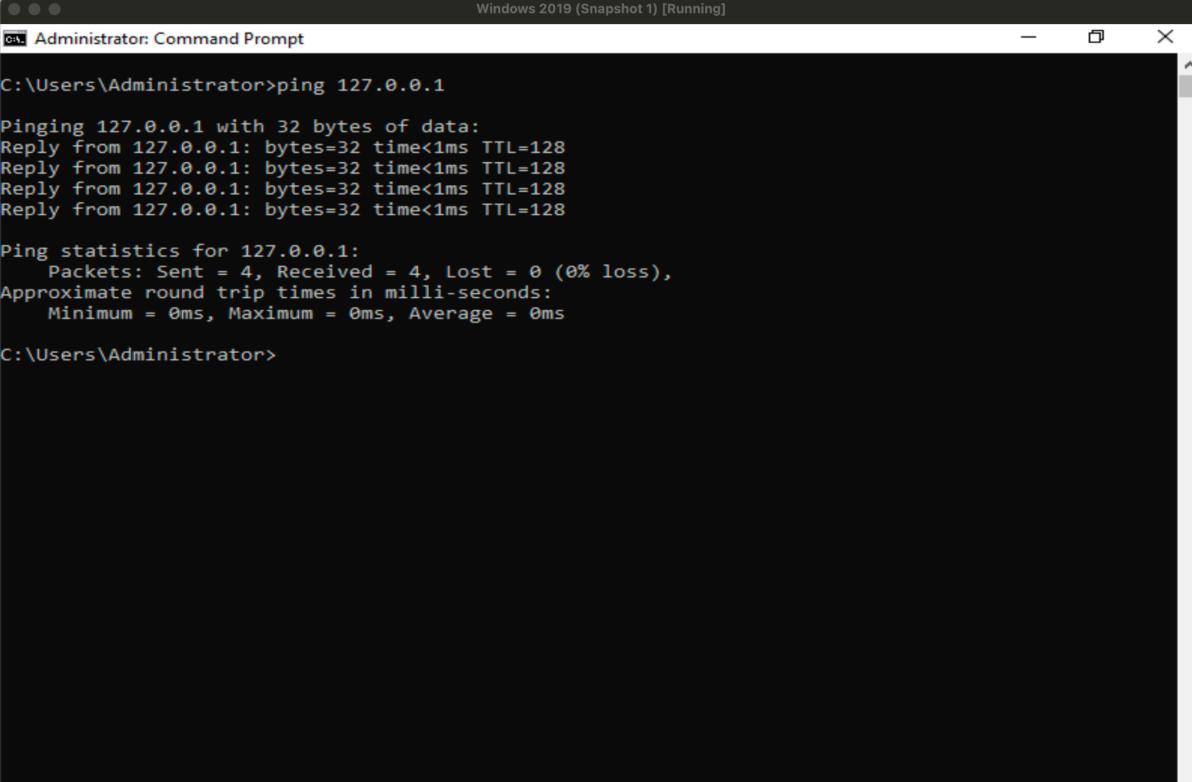
```
Windows 2019 (Snapshot 1) [Running]
Administrator: Command Prompt
C:\Users\Administrator>ipconfig /renew
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : attlocal.net
IPv6 Address . . . . . : 2600:1702:5335:10:6ecd:9176:1a41:3c0c
Link-local IPv6 Address . . . . . : fe80::233c:927f:a7cf:c4a%10
IPv4 Address . . . . . : 192.168.1.86
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::d2fc:d0ff:fe13:8e51%10
                           192.168.1.254

C:\Users\Administrator>
```

The ‘ping’ Command: this command is used to check if a remote host is reachable and to measure the time it takes to get a response. In summary, the ‘ping’ command is used to test connectivity. This is illustrated below:



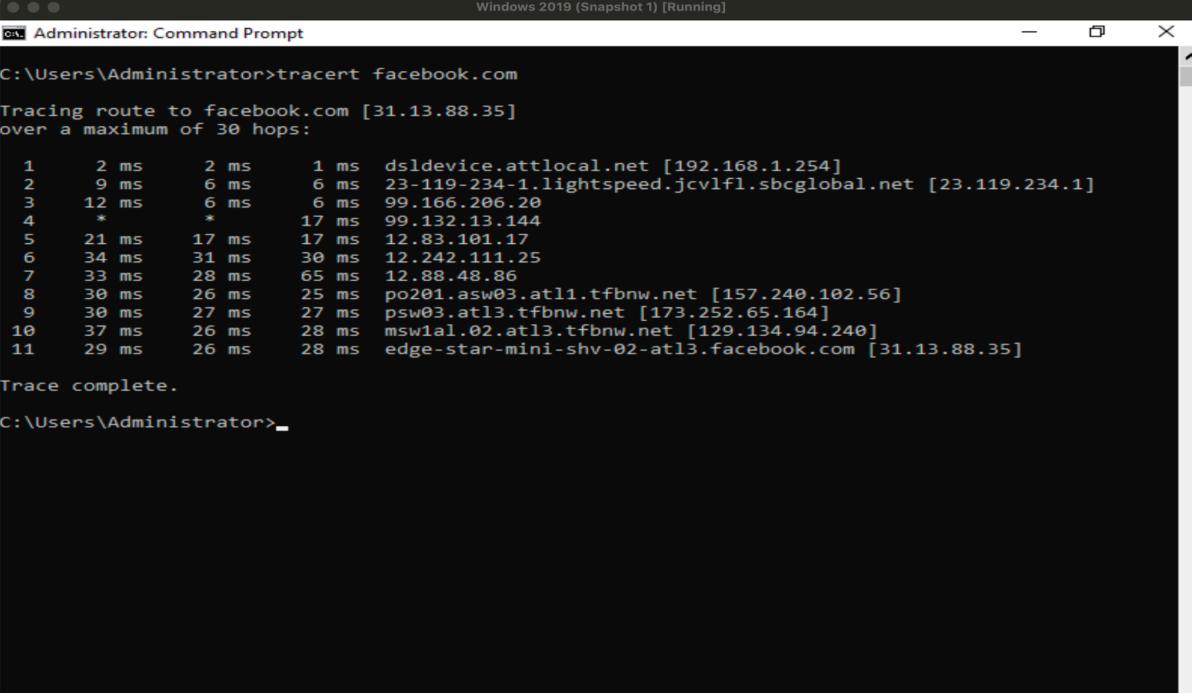
```
Windows 2019 (Snapshot 1) [Running]
Administrator: Command Prompt
C:\Users\Administrator>ping 127.0.0.1

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

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:\Users\Administrator>
```

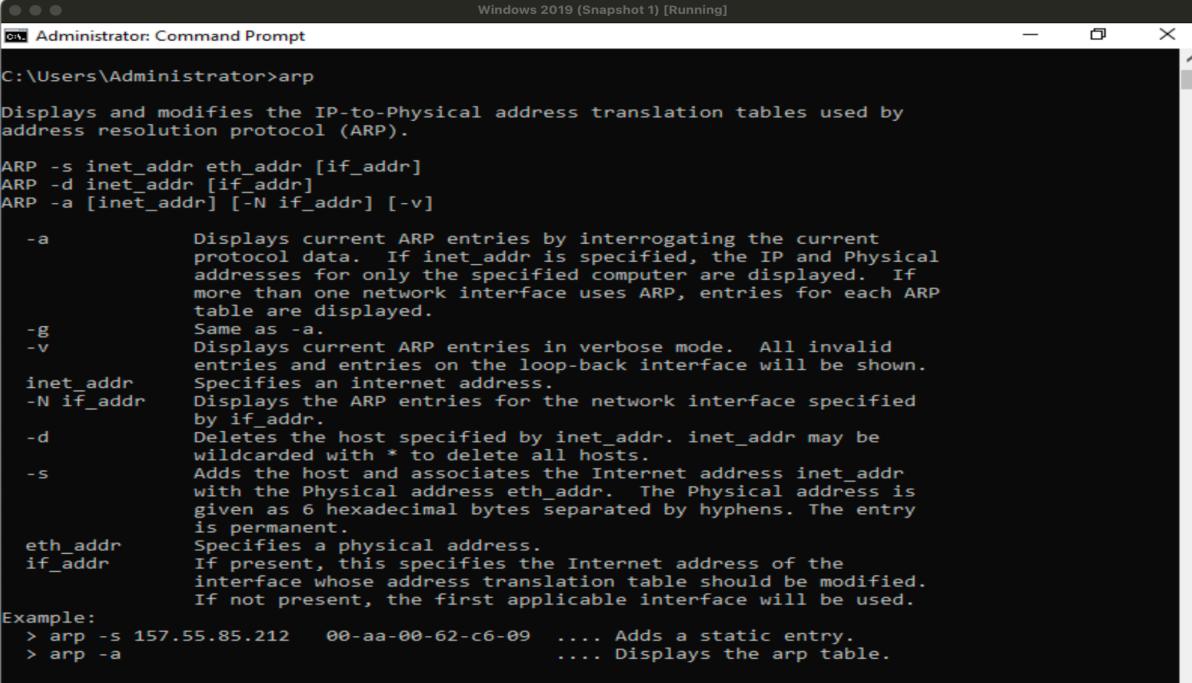
The ‘tracert’ Command: this command is short for trace route. Like the name applies, it is used to trace the route that packets take from a local computer to a specified destination. It shows the IP address of each router along the way and how long it took the packets to get to the router. An illustration is shown below:



```
Windows 2019 (Snapshot 1) [Running]
Administrator: Command Prompt
C:\Users\Administrator>tracert facebook.com
Tracing route to facebook.com [31.13.88.35]
over a maximum of 30 hops:
  1    2 ms      2 ms      1 ms  dsldevice.attlocal.net [192.168.1.254]
  2    9 ms      6 ms      6 ms  23-119-234-1.lightspeed.jcvlf.sbcglobal.net [23.119.234.1]
  3   12 ms      6 ms      6 ms  99.166.206.20
  4    *         *         17 ms  99.132.13.144
  5   21 ms      17 ms     17 ms  12.83.101.17
  6   34 ms      31 ms     30 ms  12.242.111.25
  7   33 ms      28 ms     65 ms  12.88.48.86
  8   30 ms      26 ms     25 ms  po201.asw03.atl1.tfbnw.net [157.240.102.56]
  9   30 ms      27 ms     27 ms  psw03.atl3.tfbnw.net [173.252.65.164]
 10   37 ms      26 ms     28 ms  msw1al.02.atl3.tfbnw.net [129.134.94.240]
 11   29 ms      26 ms     28 ms  edge-star-mini-shv-02-atl3.facebook.com [31.13.88.35]

Trace complete.
C:\Users\Administrator>
```

The ‘arp -a’ Command: ARP stands for Address Resolution Protocol. ARP is used, especially in IPv4 networks, to map an IP address to a physical machine address (MAC address) that is recognized in the local network. The ‘arp -a’ command displays the current ARP collection of IP addresses mapped to MAC addresses on the local network. This is shown below:



```
Windows 2019 (Snapshot 1) [Running]
Administrator: Command Prompt
C:\Users\Administrator>arp
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-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.
-g          Same as -a.
-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.
-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.
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.

Example:
> arp -s 157.55.85.212  00-aa-00-62-c6-09  .... Adds a static entry.
> arp -a                  .... Displays the arp table.
C:\Users\Administrator>
```

Assignment #2 - Applied Networking Concepts

To obtain a MAC, IP and DNS Server address using the Command Prompt, the ‘ipconfig /all’ command is used. This displays a comprehensive view of the computer configurations to include the MAC (physical) and IP address. This is shown below:

```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-AR4NF15JJAB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : attlocal.net

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : attlocal.net
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-F6-AF-A9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2600:1702:5335:10:6ecd:9176:1a41:3c0c(Preferred)
Link-local IPv6 Address . . . . . : fe80::233c:927f:a7cf:c4a%10(Preferred)
IPv4 Address. . . . . : 192.168.1.86(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, June 8, 2024 7:12:11 AM
Lease Expires . . . . . : Monday, June 10, 2024 1:24:33 AM
Default Gateway . . . . . : fe80::d2fc:d0ff:fe13:8e51%10
192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 67633191
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-DD-CA-25-08-00-27-F6-AF-A9
DNS Servers . . . . . : 2600:1702:5335:10::1
192.168.1.254
2600:1702:5335:10::1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
attlocal.net
```

To obtain an arp table mapping, the ‘arp -a’ command is used in the Command Prompt. This displays all IP addresses, their corresponding MAC (physical addresses), and how these addresses were obtained; Type (Dynamic - through ARP requests, and Static - manually configured). This is illustrated below:

```
Administrator: Command Prompt
C:\Users\Administrator>arp -a

Interface: 192.168.1.86 --- 0xa
 Internet Address      Physical Address          Type
 192.168.1.254          d0-fc-d0-13-8e-51    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\Administrator>
```

The ‘ipconfig /all’ command can be used to display the MAC Address, the IP Address, and the DNS Server Address as displayed below:

```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-AR4NF15JJAB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : attlocal.net

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : attlocal.net
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address . . . . . : 08-00-27-F6-AF-A9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2600:1702:5335:10:6ecd:9176:1a41:3c0c(Preferred)
Link-local IPv6 Address . . . . . : fe80::233c:927f:a7cf:c4a%10(Preferred)
IPv4 Address. . . . . : 192.168.1.86(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, June 8, 2024 7:12:11 AM
Lease Expires . . . . . : Monday, June 10, 2024 1:24:33 AM
Default Gateway . . . . . : fe80::d2fc:d0ff:fe13:8e51%10
                           192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 67633191
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-DD-CA-25-08-00-27-F6-AF-A9
DNS Servers . . . . . : 2600:1702:5335:10::1
                           192.168.1.254
                           2600:1702:5335:10::1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                               attlocal.net
```

Assignment #3 - Applied Networking Concepts

To install net-tools in the Linux CLI, use the command ‘`sudo apt install net-tools`’. This is illustrated below:

```
tee@demo2:~$ sudo apt install net-tools
[sudo] password for tee:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 204 kB of archives.
After this operation, 819 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+git20181103.0eebece-1ubuntu5 [204 kB]
Fetched 204 kB in 1s (287 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 111255 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ...
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
tee@demo2:~$
```

ifconfig

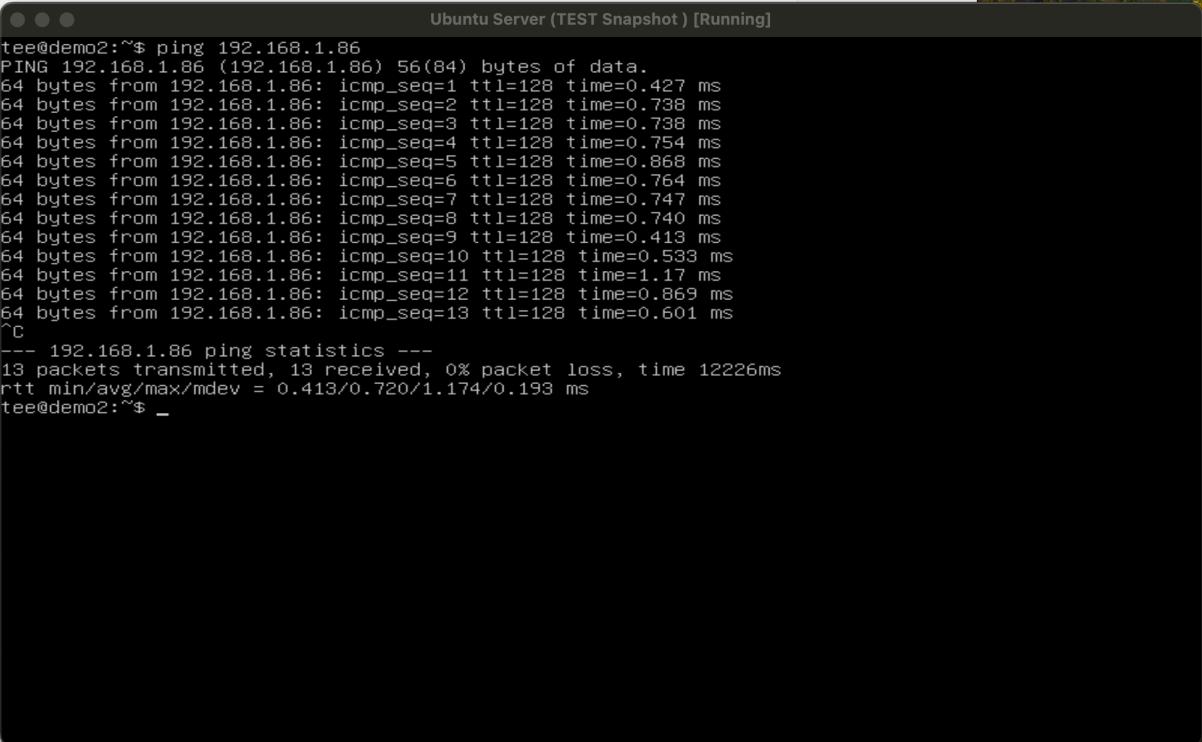
This is the command line used to configure and display network interface parameters. It displays information about all active network interfaces on the system, including IP addresses, netmasks, broadcast addresses, and more. This is illustrated below:



```
tee@demo2:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.85 brd 192.168.1.255 netmask 255.255.255.0 broadcast 192.168.1.255
                inet6 2600:1702:5335:10:a00:27ff:fe2f:2adf prefixlen 64 scopeid 0x0<global>
                inet6 2600:1702:5335:10::2d prefixlen 128 scopeid 0x0<global>
                ether 08:00:27:2f:2a:df txqueuelen 1000 (Ethernet)
                    RX packets 7328 bytes 1086460 (1.0 MB)
                    RX errors 0 dropped 1546 overruns 0 frame 0
                    TX packets 913 bytes 92378 (92.3 KB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 111 bytes 9243 (9.2 KB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 111 bytes 9243 (9.2 KB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
tee@demo2:~$
```

Ping

This command is used to check if a remote host is reachable and to measure the time it takes to get a response. In summary, the ‘ping’ command is used to test connectivity. This is illustrated below:



```
tee@demo2:~$ ping 192.168.1.86
PING 192.168.1.86 (192.168.1.86) 56(84) bytes of data.
64 bytes from 192.168.1.86: icmp_seq=1 ttl=128 time=0.427 ms
64 bytes from 192.168.1.86: icmp_seq=2 ttl=128 time=0.738 ms
64 bytes from 192.168.1.86: icmp_seq=3 ttl=128 time=0.738 ms
64 bytes from 192.168.1.86: icmp_seq=4 ttl=128 time=0.754 ms
64 bytes from 192.168.1.86: icmp_seq=5 ttl=128 time=0.868 ms
64 bytes from 192.168.1.86: icmp_seq=6 ttl=128 time=0.764 ms
64 bytes from 192.168.1.86: icmp_seq=7 ttl=128 time=0.747 ms
64 bytes from 192.168.1.86: icmp_seq=8 ttl=128 time=0.740 ms
64 bytes from 192.168.1.86: icmp_seq=9 ttl=128 time=0.413 ms
64 bytes from 192.168.1.86: icmp_seq=10 ttl=128 time=0.533 ms
64 bytes from 192.168.1.86: icmp_seq=11 ttl=128 time=1.17 ms
64 bytes from 192.168.1.86: icmp_seq=12 ttl=128 time=0.869 ms
64 bytes from 192.168.1.86: icmp_seq=13 ttl=128 time=0.601 ms
^C
--- 192.168.1.86 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12226ms
rtt min/avg/max/mdev = 0.413/0.720/1.174/0.193 ms
tee@demo2:~$ _
```

Traceroute

Like the name applies, it is used to trace the route that packets take from a local computer to a specified destination. It shows the IP address of each router along the way and how long it took the packets to get to the router. An illustration is shown below:

```
traceroute to cnn.com (151.101.195.5), 30 hops max, 60 byte packets
  1  dsldevice.attlocal.net (192.168.1.254)  2.329 ms  2.076 ms  1.835 ms
  2  23-119-234-1.lightspeed.jcvif1.sbcglobal.net (23.119.234.1)  4.649 ms  4.476 ms  4.307 ms
  3  99.166.206.20 (99.166.206.20)  9.261 ms  9.088 ms  8.919 ms
  4  * * *
  5  12.83.101.17 (12.83.101.17)  18.768 ms  12.83.101.9 (12.83.101.9)  18.603 ms  18.471 ms
  6  12.123.43.201 (12.123.43.201)  28.312 ms  27.665 ms  30.203 ms
  7  * * *
  8  * * *
  9  * * *
 10  * * *
 11  * * *
 12  * * *
 13  * * *
 14  * * *
 15  * * *
 16  * * *
 17  * * *
 18  * * *
 19  * * *
 20  * * *
 21  * * *
 22  * * *
 23  * * *
 24  * * *
 25  * * *
 26  * * *
 27  * * *
 28  * * *
 29  * * *
 30  * * *
tee@demo2:~$ _
```

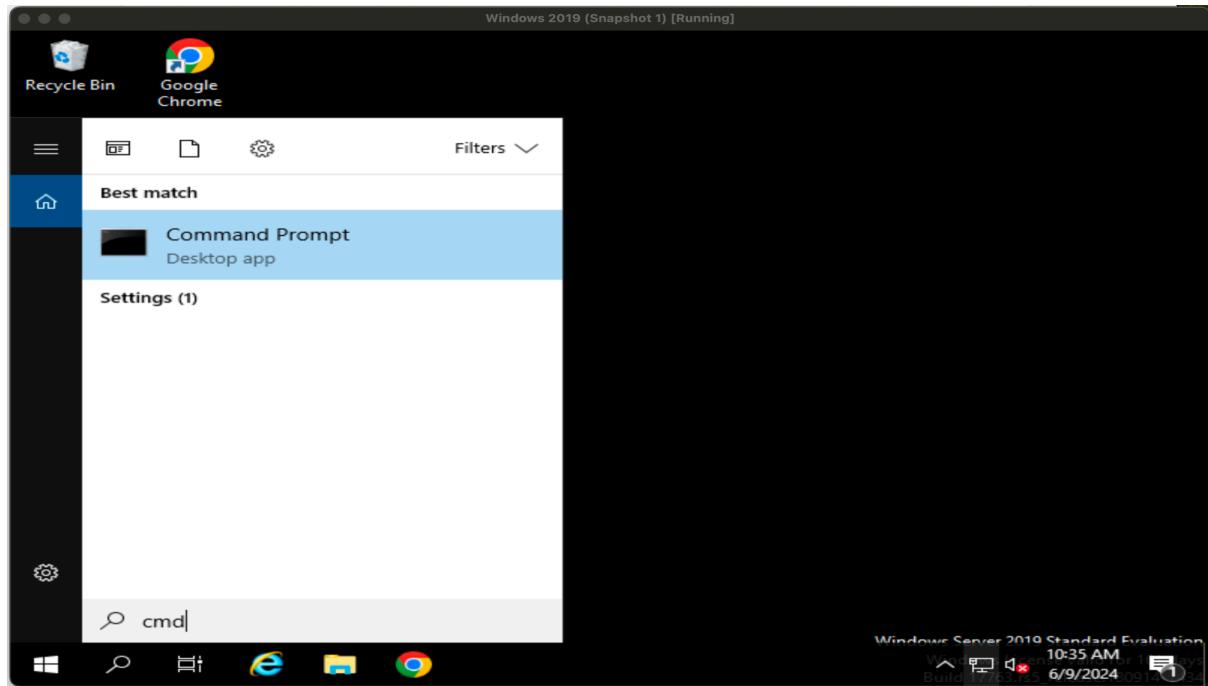
arp -a

ARP is used, especially in IPv4 networks, to map an IP address to a physical machine address (MAC address) that is recognized in the local network. The ‘arp -a’ command displays the current ARP collection of IP addresses mapped to MAC addresses on the local network. This is shown below:

```
arp -a
Tab-iMac.attlocal.net (192.168.1.66) at 5c:52:30:a4:1e:49 [ether] on enp0s3
dsldevice.attlocal.net (192.168.1.254) at d0:fc:d0:13:8e:51 [ether] on enp0s3
? (192.168.1.86) at 08:00:27:f6:af:a9 [ether] on enp0s3
tee@demo2:~$
```

Assignment #4 - Applied Networking Concepts

In the Windows CLI Command Prompt, the ‘ipconfig /all’ command can be used to display the MAC and IP addresses. Click on the search bar on the Windows Desktop page, and type in ‘cmd’. Click on the Command Prompt desktop app as shown below:



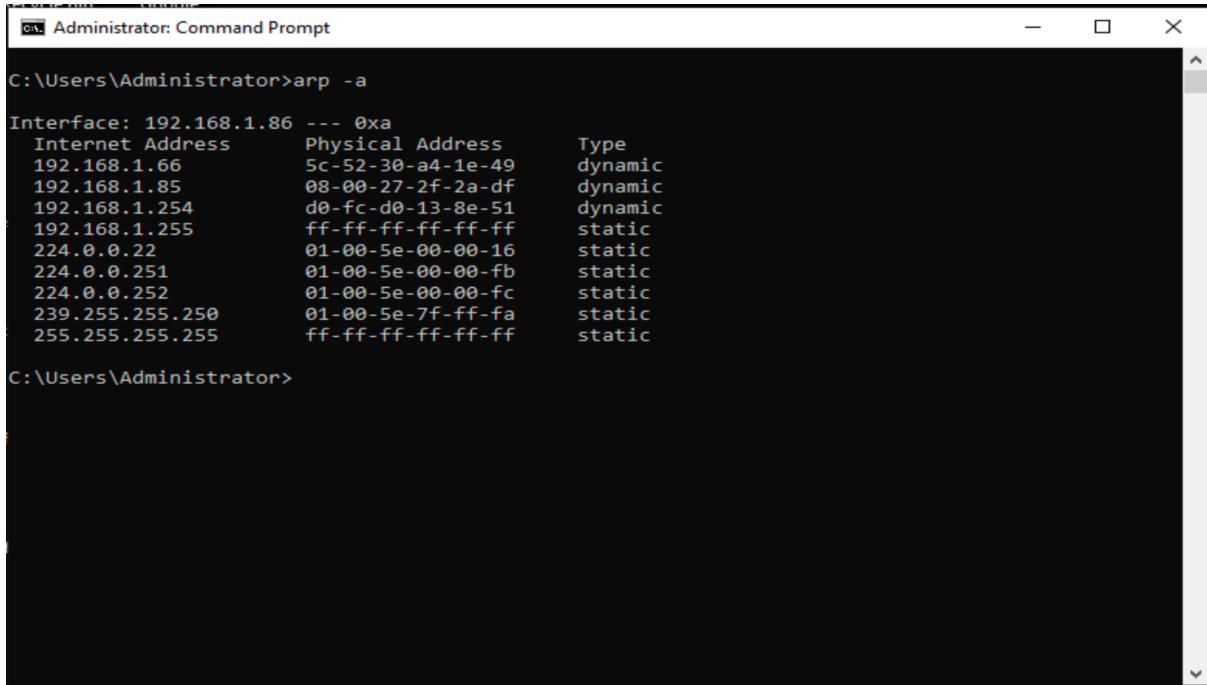
When in the Command Prompt, type in the ‘ipconfig /all’ command to display detailed IP configuration information for all network adapters. This includes the MAC and IP addresses as shown below:

A screenshot of a Windows Command Prompt window titled 'Administrator: Command Prompt'. The window shows the output of the 'ipconfig /all' command. The output displays various network configuration details for the 'Ethernet adapter Ethernet' interface, including the MAC address (08-00-27-F6-AF-A9), IP address (192.168.1.254), and subnet mask (255.255.255.0). The command prompt also shows the current working directory as 'C:\Users\Administrator>' and the full path 'C:\Users\Administrator>ipconfig /all'. At the bottom of the window, a license message reads 'Windows License valid for 161 days Build 17763.rs5_release.180914-1434'.

From the illustration above, the following can be deduced:

MAC (Physical) Address is 08-00-27-F6-AF-A9 | IPv4 Address is 192.168.1.86

To obtain the ARP Table Mapping, navigate to the Command Prompt interface and type in the 'arp -a' command. This displays the Address Resolution Protocol Table Mapping as shown below:



```
C:\Administrator: Command Prompt
C:\Users\Administrator>arp -a

Interface: 192.168.1.86 --- 0xa
 Internet Address      Physical Address      Type
 192.168.1.66          5c-52-30-a4-1e-49    dynamic
 192.168.1.85          08-00-27-2f-2a-df    dynamic
 192.168.1.254         d0-fc-d0-13-8e-51    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\Administrator>
```

As shown in the Command Prompt interface above, a list of the IP addresses mapped to various devices through their MAC address, and how these addresses were obtained; Type (Dynamic - through ARP requests, and Static - manually configured).

Assignment #5 - Applied Networking Concepts

Hubs, Switches, and Routers

Hubs: this is a networking device that connects devices within a network making them act as a single network segment. The hub receives packets from one port and sends it to all other ports, irrespective of the destination. It is in Layer 1 of the Open Systems Interconnection (OSI) Model.



Switch: this is used to connect devices within a network and enable communication between them. It uses MAC addresses to forward data to the right destination. It is in Layer 2 of the Open Systems Interconnection (OSI) Model.



Routers: this is used to connect multiple networks. They direct data packets to the right network using the IP address assigned to the device. It is in Layer 3 of the Open Systems Interconnection (OSI) Model.



All three devices (hub, switch, router) are used to connect network devices. A hub does not manage traffic intelligently; it merely repeats signals. It does not differentiate between different network devices. Like a hub, a switch connects multiple devices; however, it does so more efficiently. Unlike a hub, a switch intelligently forwards data based on MAC addresses, reducing unnecessary traffic. Routers, like switches and hubs, connect devices but do so at a higher level (network layer).

Routers determine the best path for packet delivery between different networks, using IP addresses, and they manage more complex tasks such as DHCP, and firewall protection, which neither hubs or switches handle.

Assignment #5 - Applied Networking Concepts

MAC Address

A MAC Address is a unique ID assigned to a network interface controller for use in network communication. It is 48 bits long, consisting of 6 bytes. It is typically represented as six pairs of hexadecimal digits separated by colons (:) or hyphens (-). An example is 08-00-27-F6-AF-A9.

The first 24 bits or 3 bytes, known as the Organizationally Unique Identifier(OUI) are assigned by the Institute of Electrical and Electronics Engineers (IEEE). The remaining 3 bytes are assigned by the Network Interface Controller (NIC) manufacturer for unique identification.

Internet Protocol (IP) Address

An IP address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. There are two types: IPv4 and IPv6. IPv4 addresses come in 32 bits while IPv6 addresses come in 128 bits.

IPv4 is represented as four decimal numbers separated by dots, e.g., 192.168.1.1.

IPv6 is represented as eight groups of four hexadecimal digits separated by colons e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Domain Name System (DNS)

DNS is an internet naming system that assigns names to known domains. It translates a domain into an IP address and vice versa DNS provides human-readable domain names e.g. www.cnn.com into IP addresses e.g. 192.168.1.77. When you type a website name into your browser, DNS helps find the IP address of the website so your browser can load it

Dynamic Host Configuration Protocol (DHCP)

DHCP automatically assigns IP addresses and other network configuration parameters to devices on a network. When a device connects to a network and sends a request for an IP address, DHCP assigns it one so it can communicate with other devices on the network. The DHCP server assigns an available IP address to the device and provides other network settings (such as the gateway and DNS servers).

DORA Protocol

The DORA protocol stands for Discovery, Offer, Request, and Acknowledge. This describes the steps through which an IP address is obtained from a DHCP Server.

Discover: The client broadcasts a "DHCP Discover" message to find available DHCP servers.

Offer: DHCP servers respond with a "DHCP Offer" message, offering an IP address.

Request: The client responds with a "DHCP Request" message, asking to use one of the offered IP addresses.

Acknowledge: The DHCP server sends a "DHCP Acknowledge" message, confirming that the IP address has been assigned to the client.

Understanding these concepts is fundamental for networking, as they form the basis of how devices communicate and access resources on a network.

The Illustration below shows a Command Prompt interface displaying a MAC and IPv4 Address. It also shows that DHCP is enabled on this Windows server. The command line ‘ipconfig /all’ can be used to get this data.

Windows 2019 (Snapshot 1) [Running]

Recycle Bin Google

Administrator: Command Prompt

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : WIN-AR4NF15JJAB
    Primary Dns Suffix  . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : attlocal.net

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : attlocal.net
    Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Physical Address. . . . . : 08-00-27-F6-AF-A9
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IPv6 Address. . . . . : 2600:1702:5335:10:6ecd:9176:1a41:3c0c(Preferred)
    Link-local IPv6 Address . . . . . : fe80::233c:927f:a7cf:c4a%10(Preferred)
    IPv4 Address. . . . . : 192.168.1.86(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Sunday, June 9, 2024 7:10:11 AM
    Lease Expires . . . . . : Monday, June 10, 2024 7:10:32 AM
    Default Gateway . . . . . : fe80::d2fc:d0ff:fe13:8e51%10
                                192.168.1.254
    DHCP Server . . . . . : 192.168.1.254
    DHCPv6 IAID . . . . . : 67633191
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-DD-CA-25-08-00-27-F6-AF-A9
    DNS Servers . . . . . : 2600:1702:5335:10::1
```

The Illustration below shows a nslookup query:

```
tee@demo2:~$ nslookup cnn.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: cnn.com
Address: 151.101.131.5
Name: cnn.com
Address: 151.101.195.5
Name: cnn.com
Address: 151.101.67.5
Name: cnn.com
Address: 151.101.3.5
Name: cnn.com
Address: 2a04:4e42:c00::773
Name: cnn.com
Address: 2a04:4e42:200::773
Name: cnn.com
Address: 2a04:4e42:e00::773
Name: cnn.com
Address: 2a04:4e42:400::773
Name: cnn.com
Address: 2a04:4e42:a00::773
Name: cnn.com
Address: 2a04:4e42::773
Name: cnn.com
Address: 2a04:4e42:800::773
Name: cnn.com
Address: 2a04:4e42:600::773
```