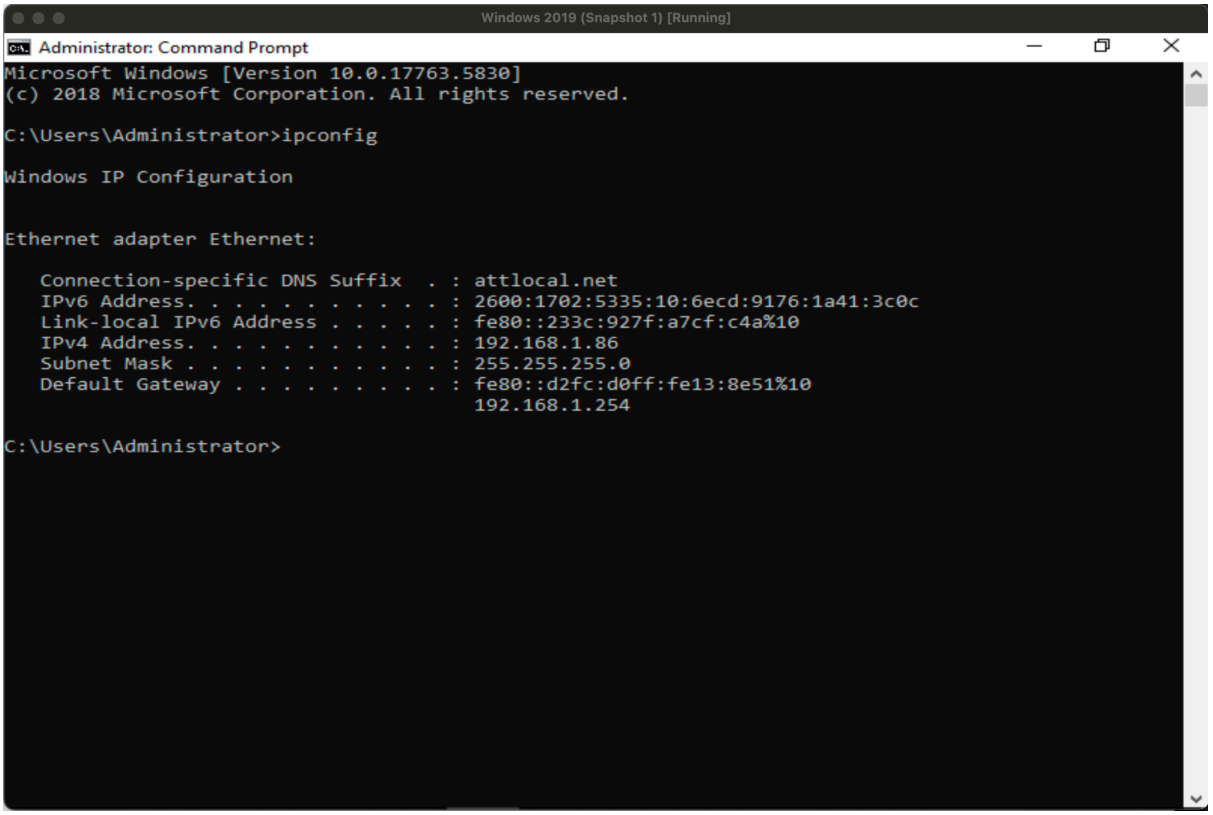
Assignment #1 - Applied Networking Concepts

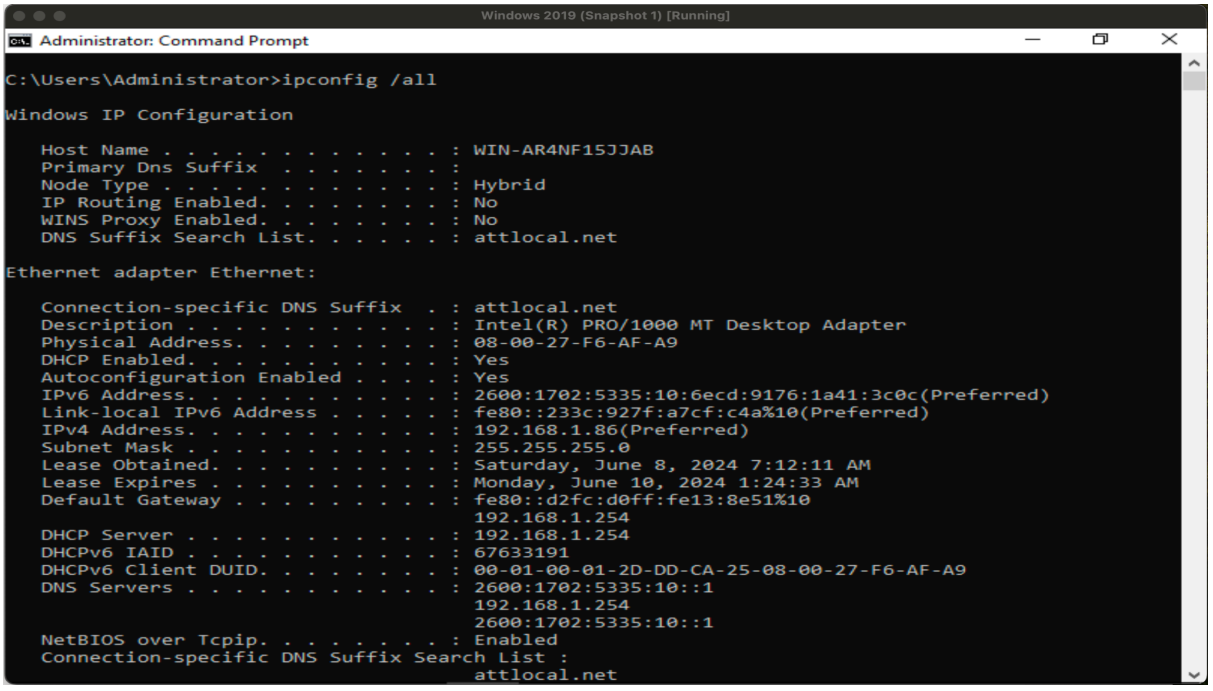
Networking Stacks in Windows

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.

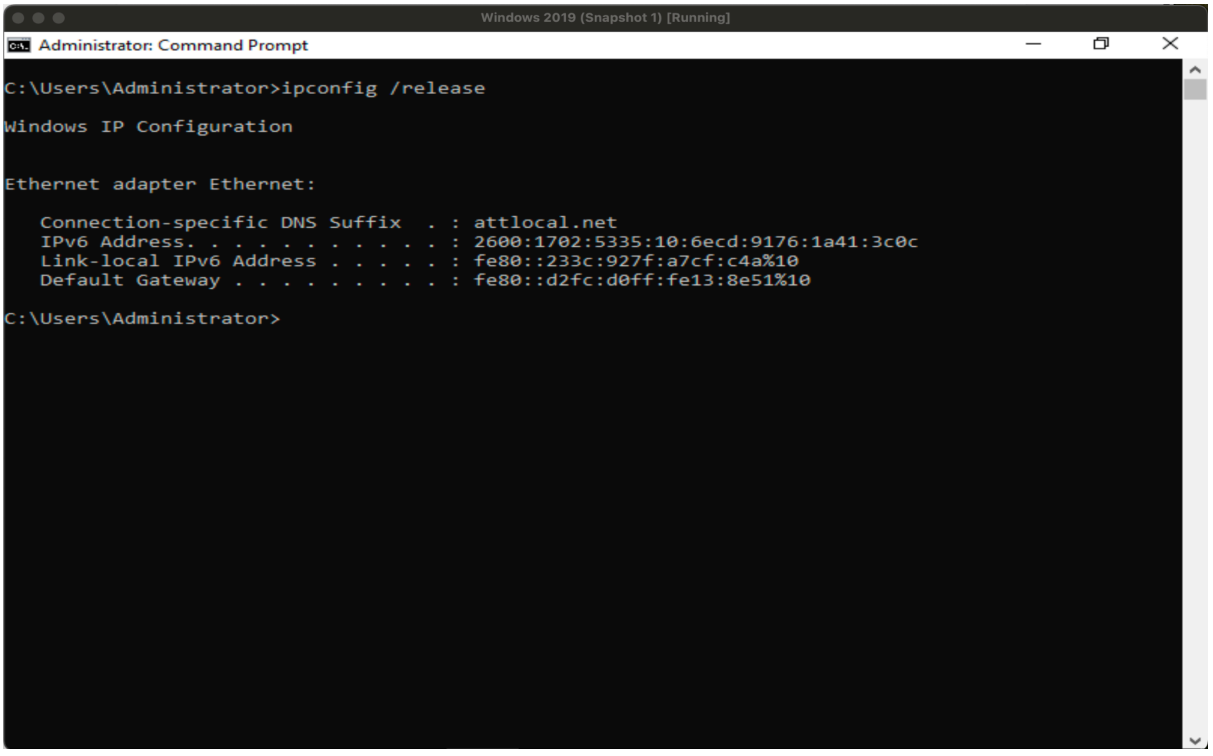
The 'ipconfig' Command: this command, when run in the Command Prompt, displays the basic IP configuration settings of all network adapters on a Windows computer. It provides information such as the IP address, subnet mask, default gateway, and DNS server addresses. An illustration is shown below:



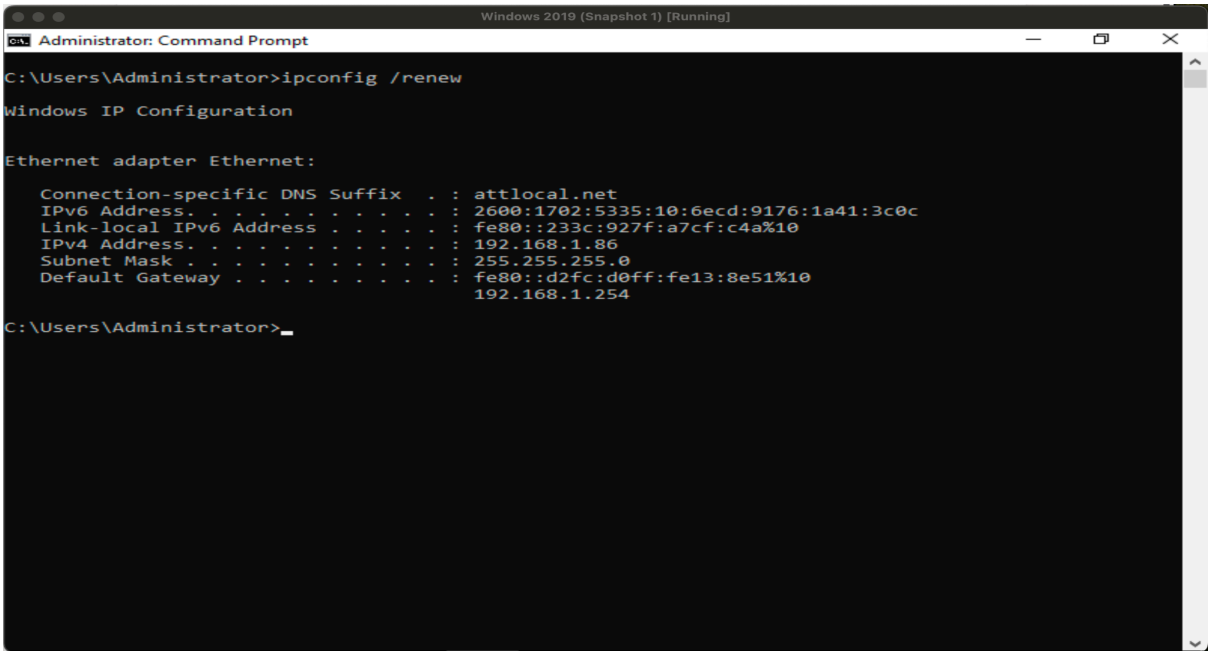
The 'ipconfig /all' Command: this command provides detailed IP configuration information for all network adapters, including additional details such as the MAC (Media Access Control) address, Dynamic Host Configuration Protocol (DHCP) lease information, and DNS suffix. An illustration is shown below:



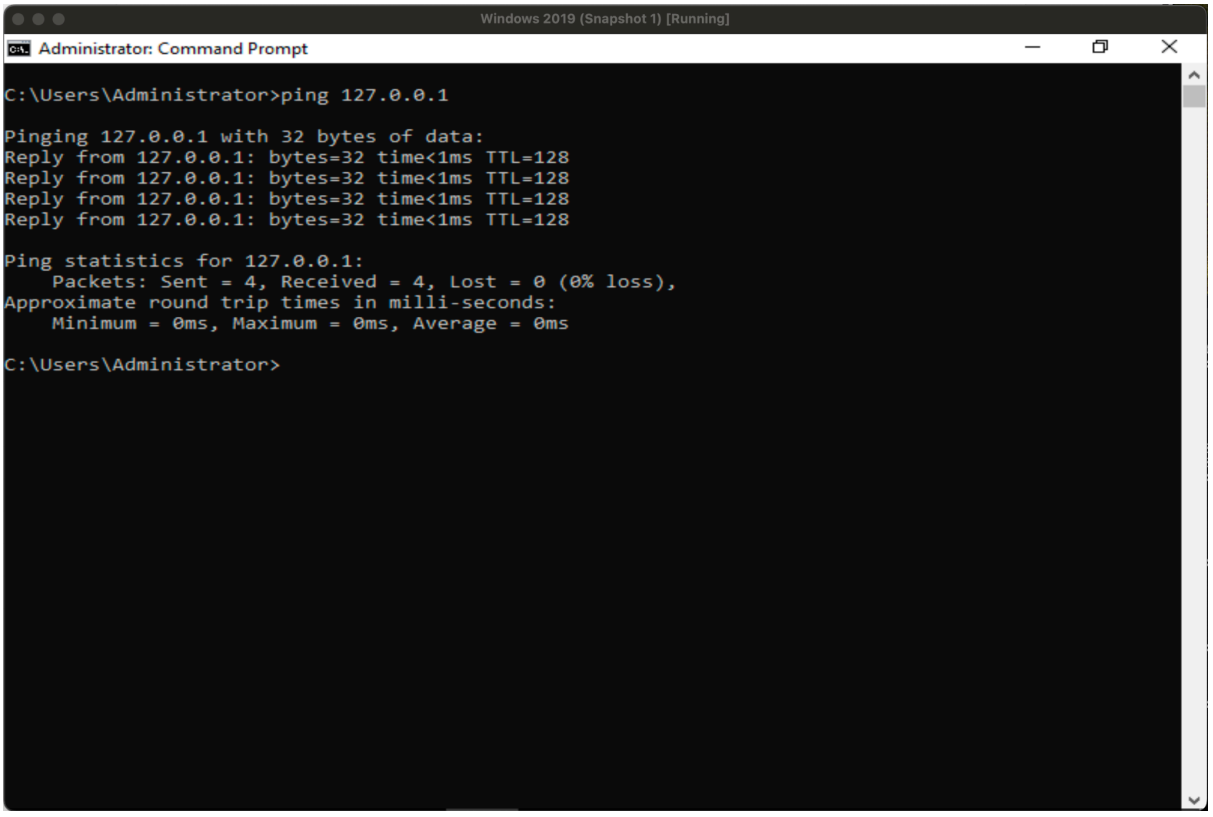
The 'ipconfig /release' Command: this command cancels the lease on any IP address obtained from a DHCP server for all network adapters on the computer. This makes that particular IP address available for lease to another device. It is illustrated below:



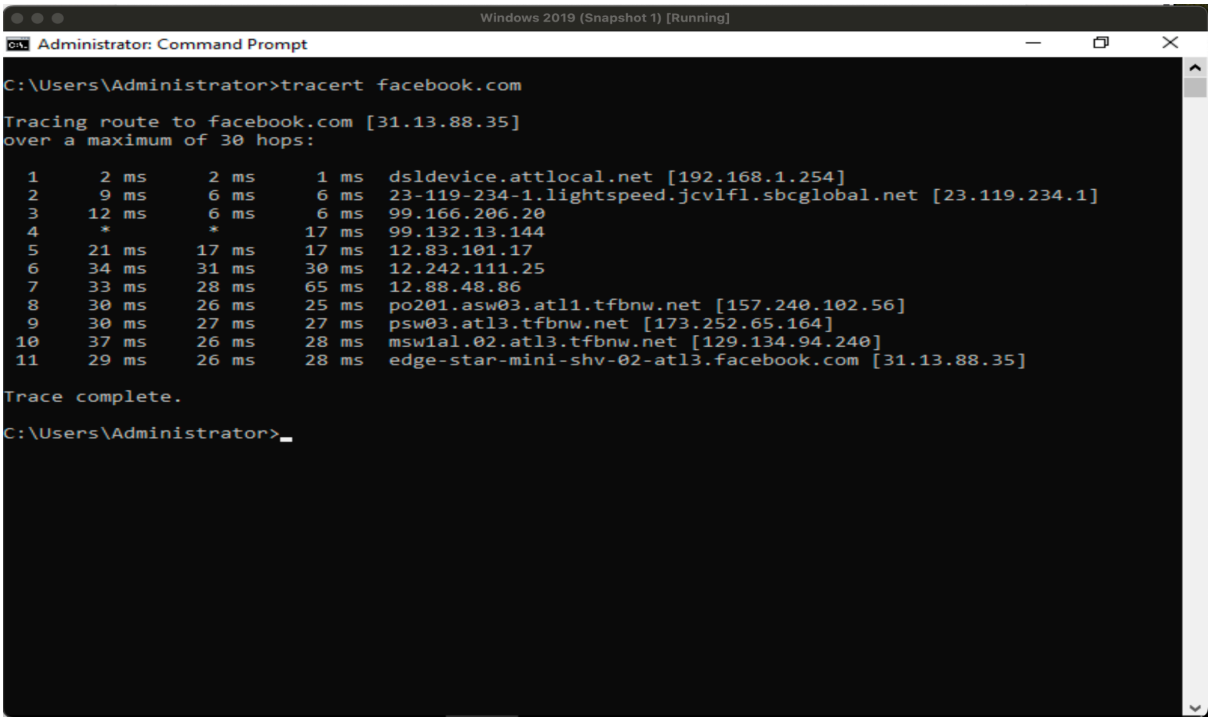
The 'ipconfig /renew' Command: this command reverses the previous command; ipconfig /release. Running the 'ipconfig /renew' command sends a request for a new IP address from the DHCP server. This helps to obtain a new IP address or updating DHCP lease information. An illustration is shown below:



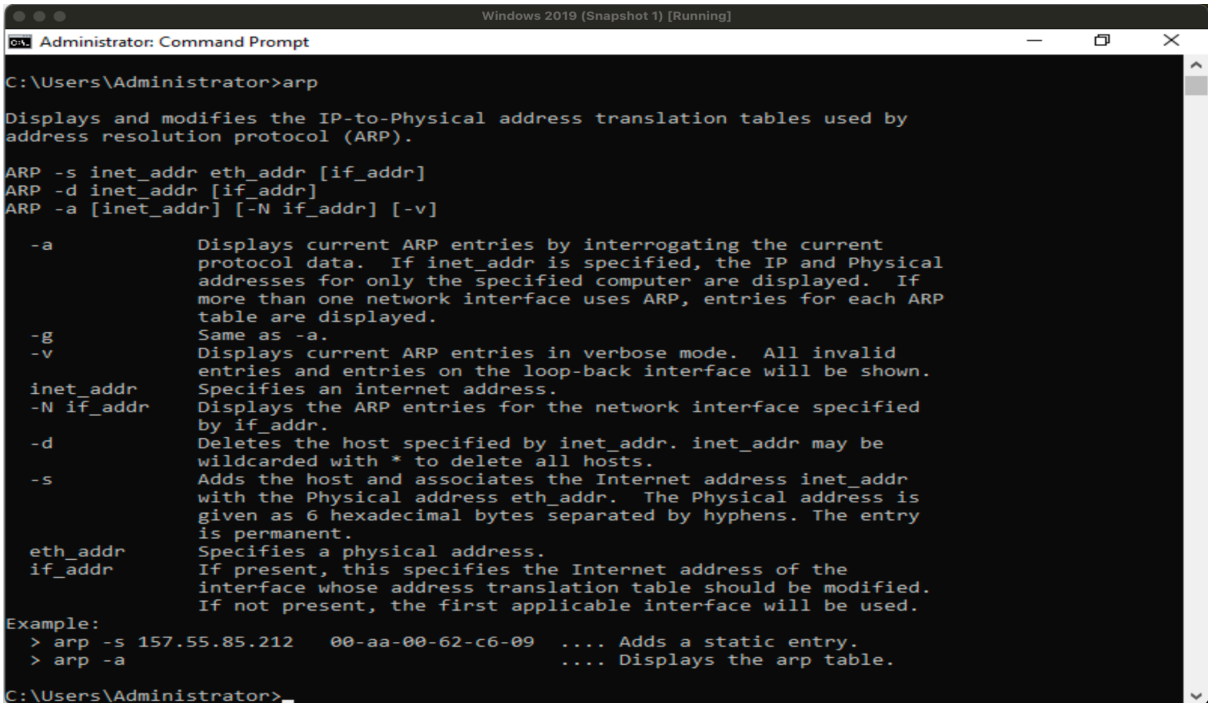
The 'ping' Command: this command is used to check if a remote host is reachable and to measure the time it takes to get a response. In summary, the 'ping' command is used to test connectivity. This is illustrated below:



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:

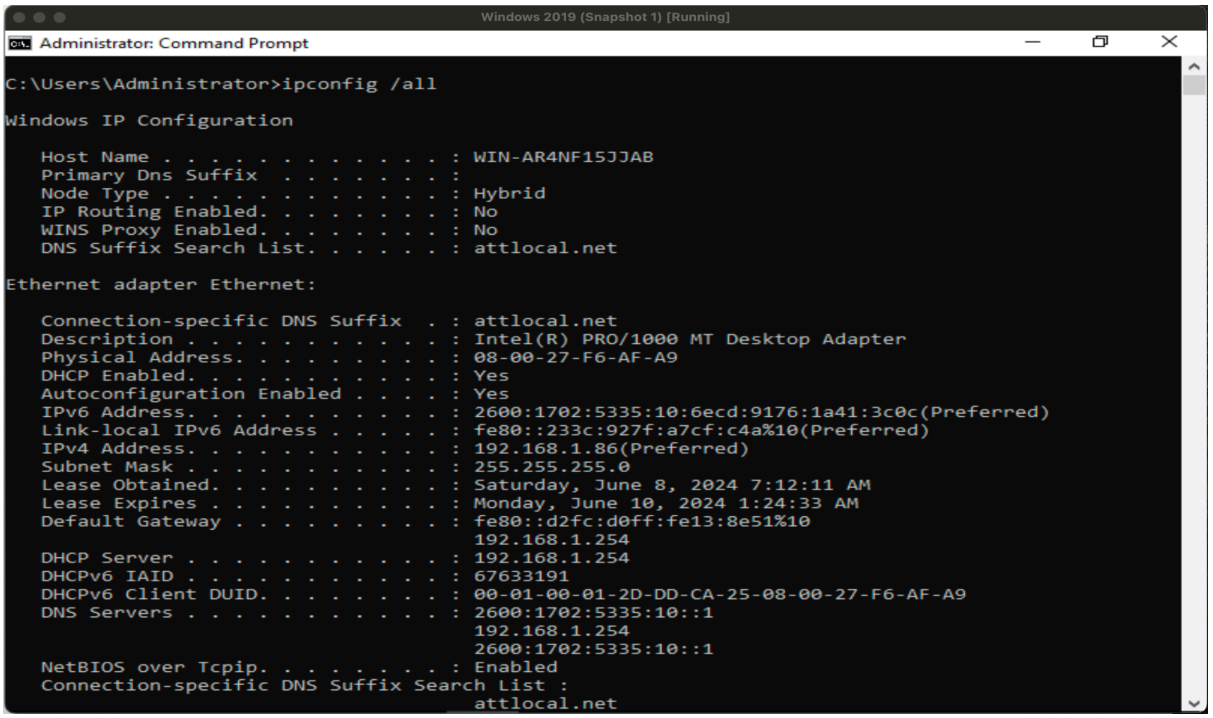


The 'arp -a' Command: ARP stands for Address Resolution Protocol. ARP is used, especially in IPv4 networks, to map an IP address to a physical machine address (MAC address) that is recognized in the local network. The 'arp -a' command displays the current ARP collection of IP addresses mapped to MAC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

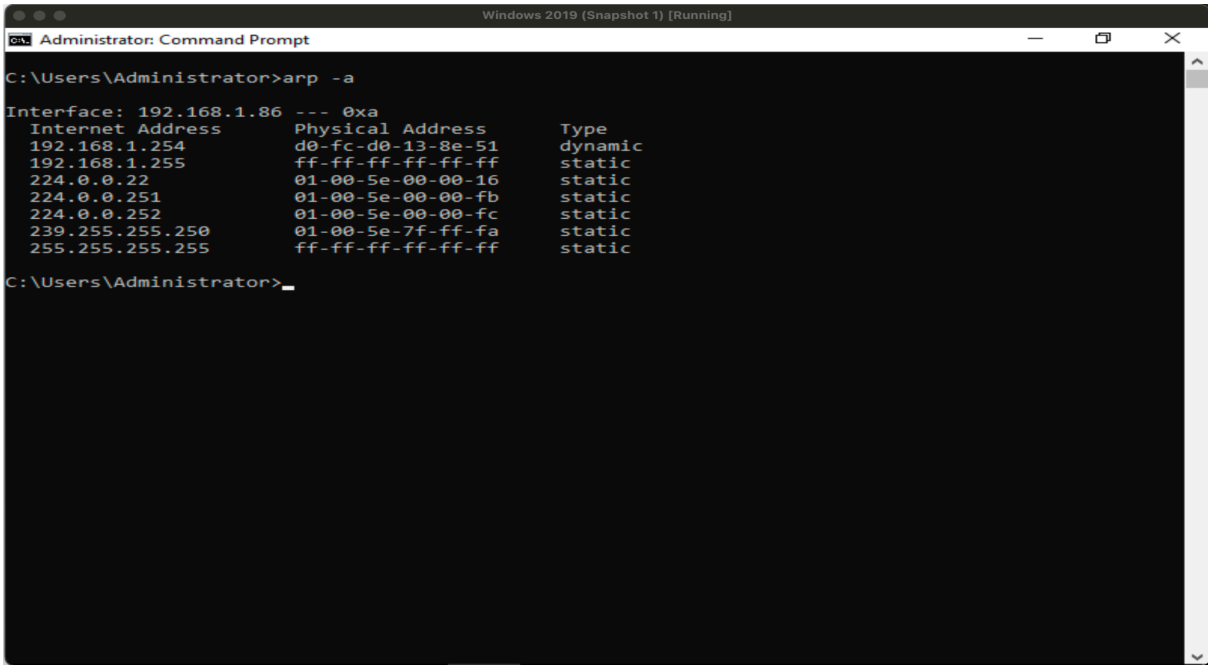


Assignment #2 - Applied Networking Concepts

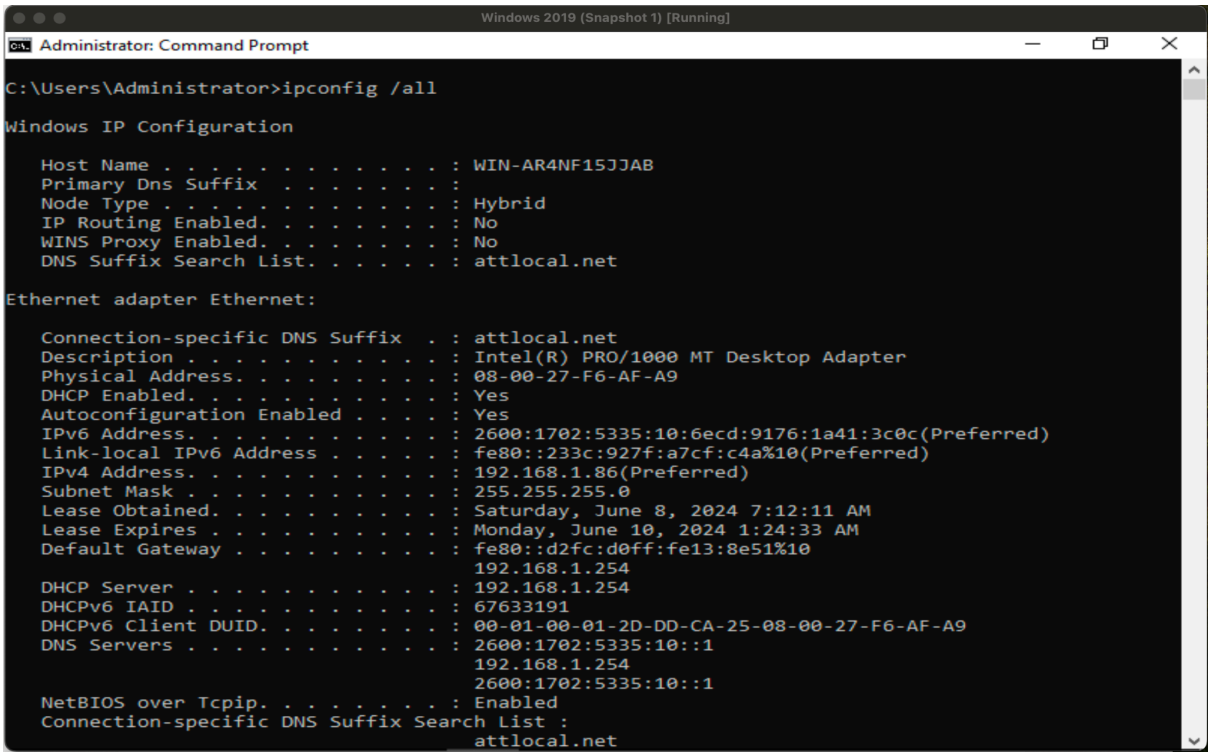
To obtain a MAC, IP and DNS Server address using the Command Prompt, the 'ipconfig /all' command is used. This displays a comprehensive view of the computer configurations to include the MAC (physical) and IP address. This is shown below:



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:

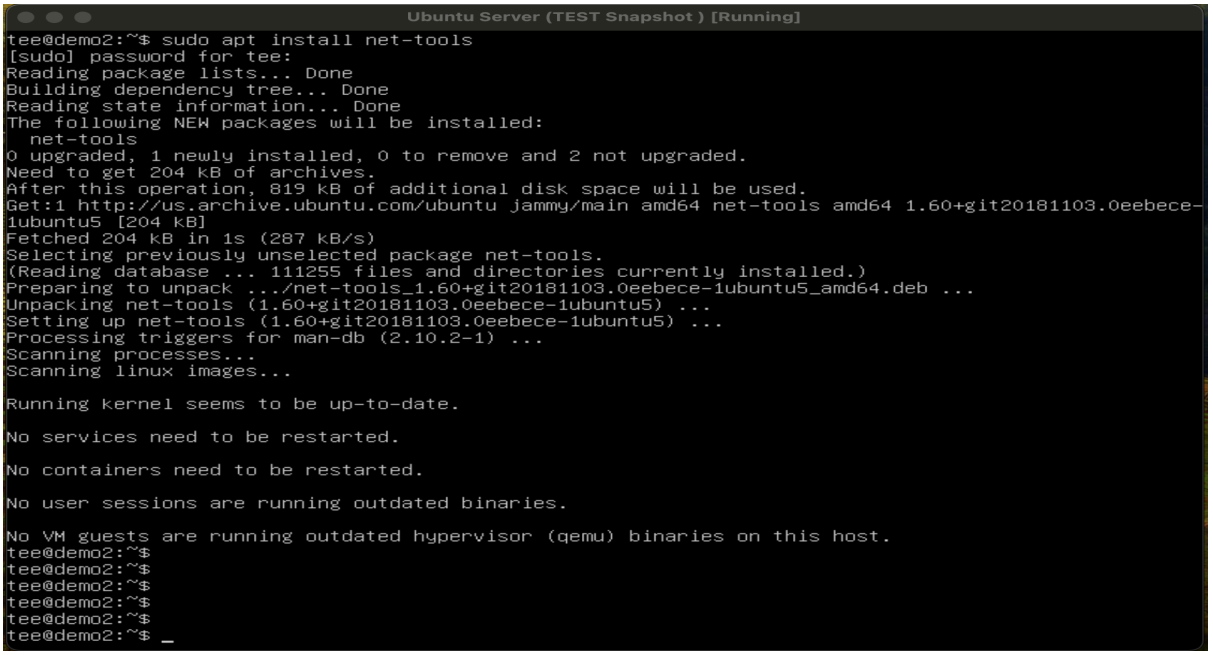


The ‘ipconfig /all’ command can be used to display the MAC Address, the IP Address, and the DNS Server Address as displayed below:



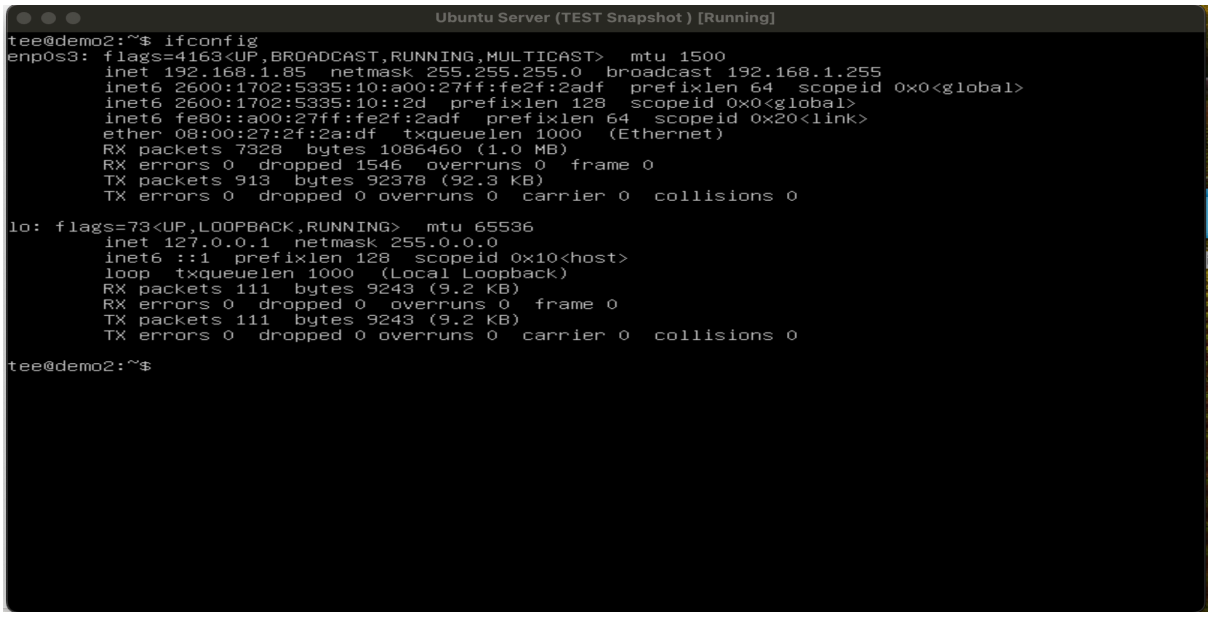
Assignment #3 - Applied Networking Concepts

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



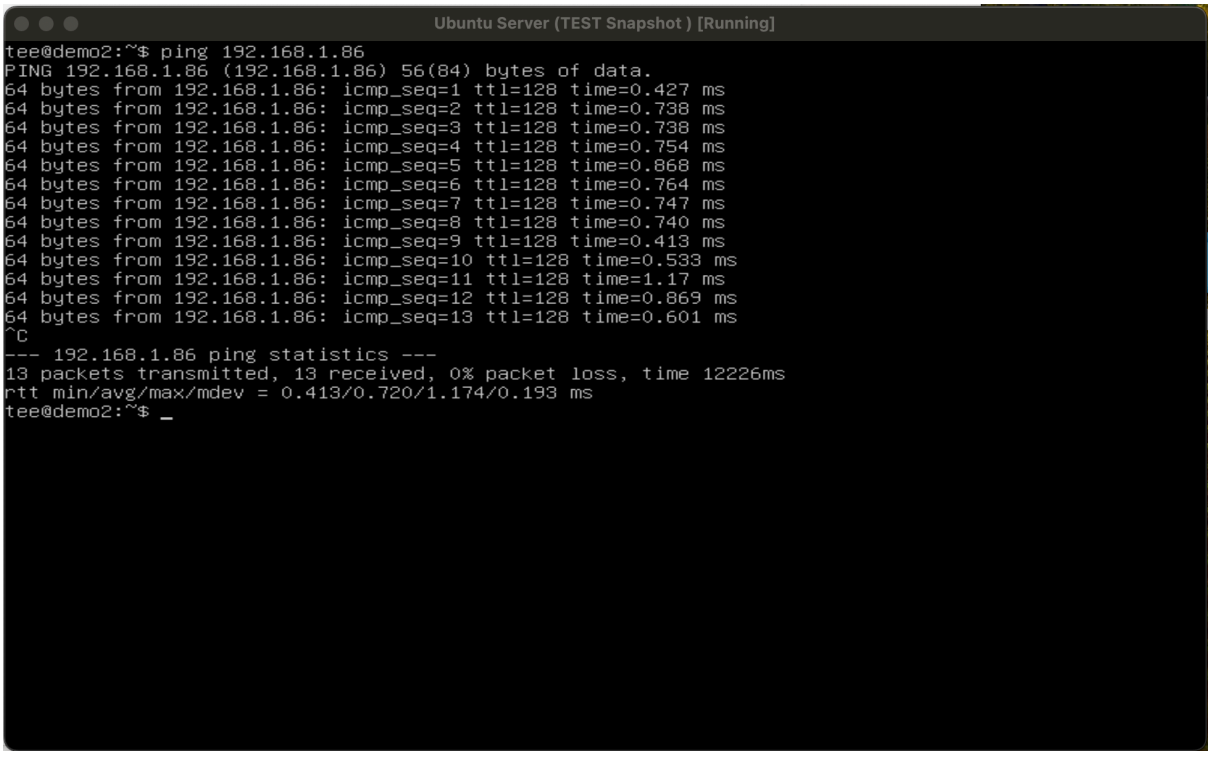
ifconfig

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:



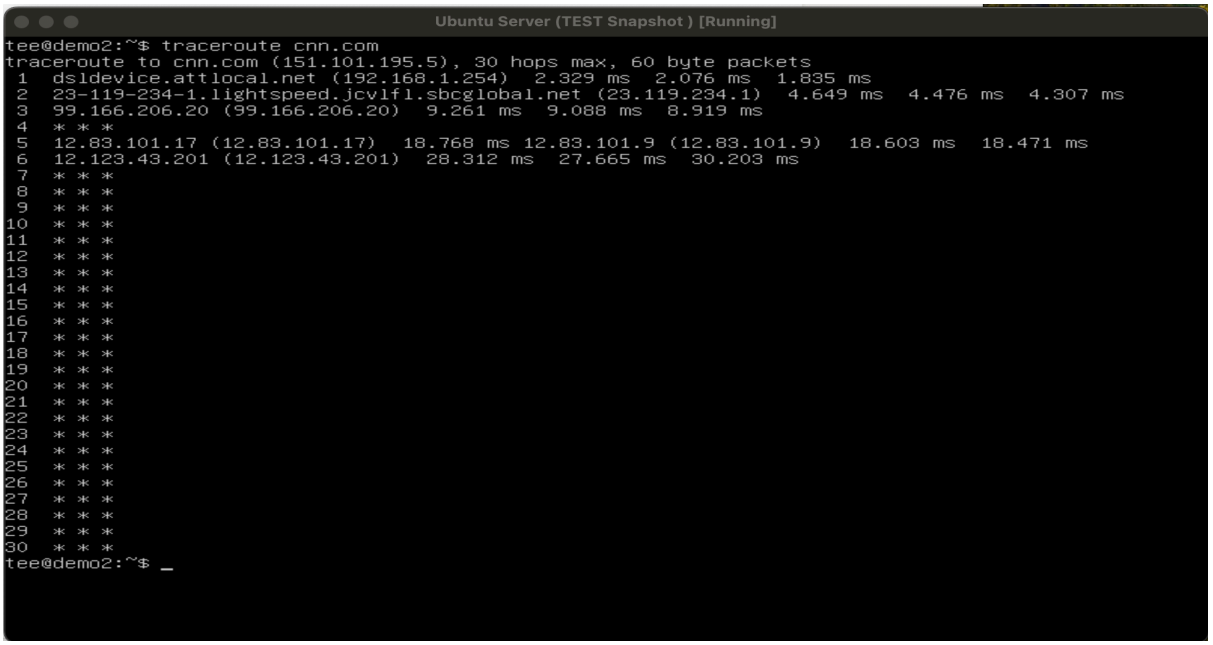
Ping

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:



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:

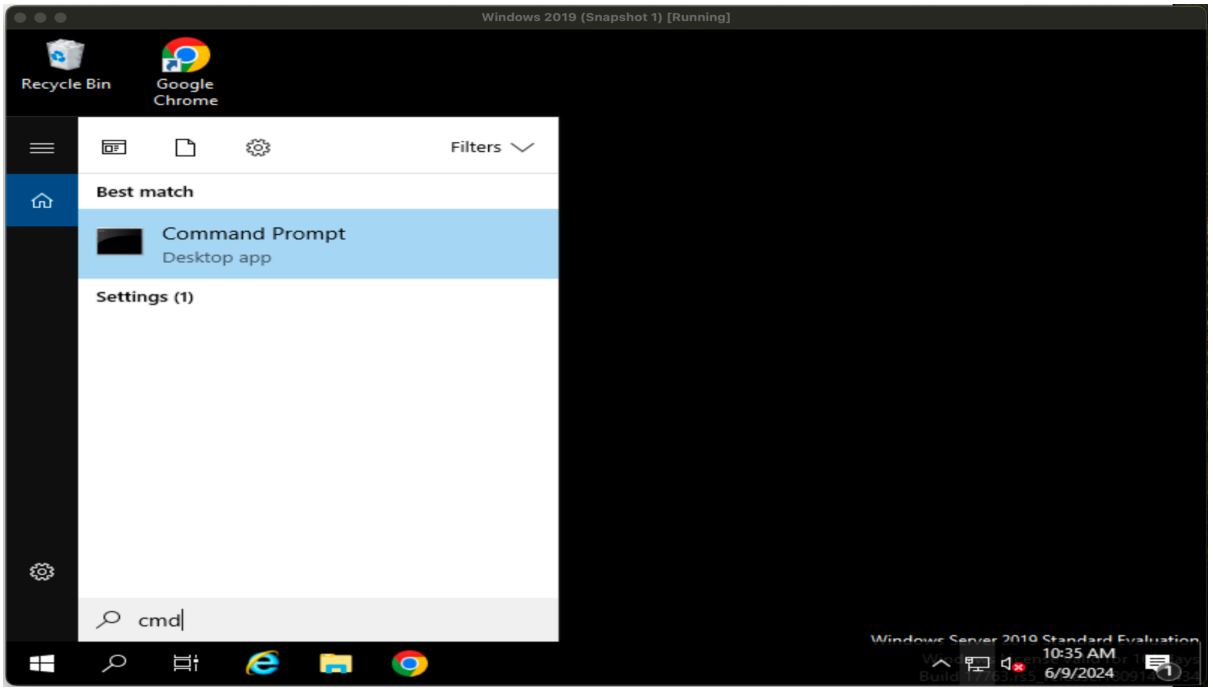


arp -a

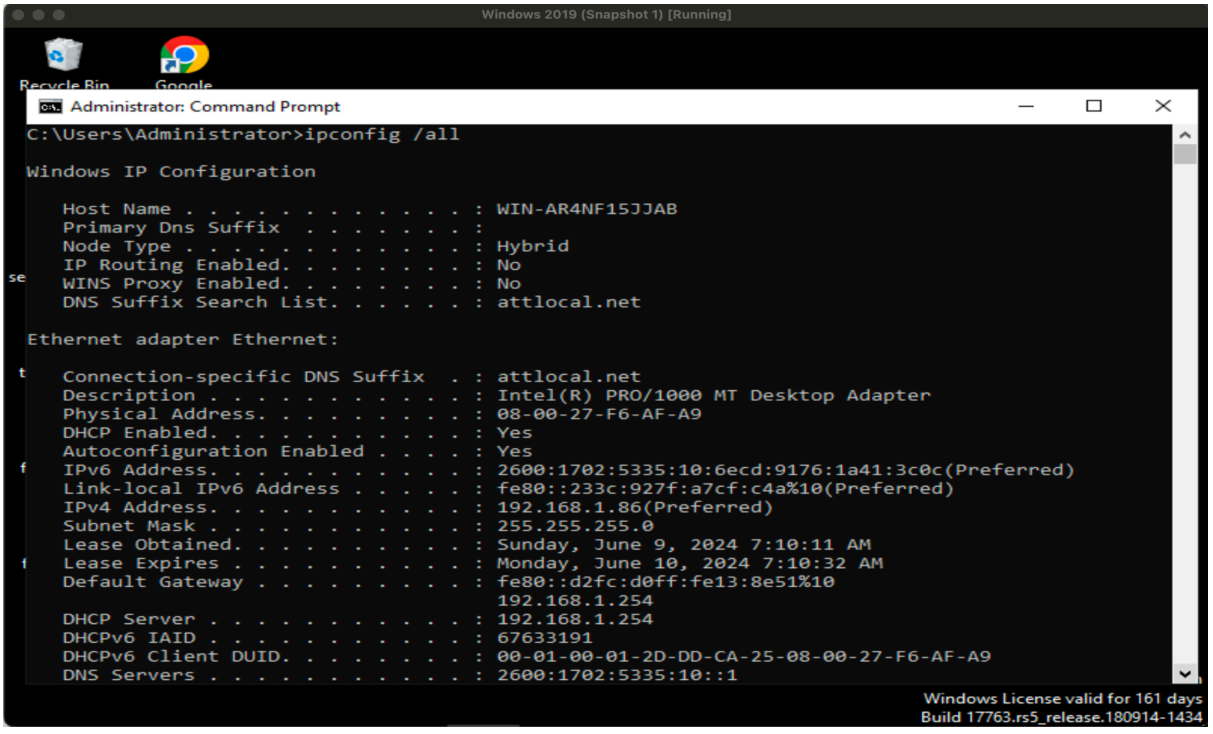
ARP is used, especially in IPv4 networks, to map an IP address to a physical machine address (MAC address) that is recognized in the local network. The ‘arp -a’ command displays the current ARP collection of IP addresses mapped to MAC addresses on the local network. This is shown below:

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:



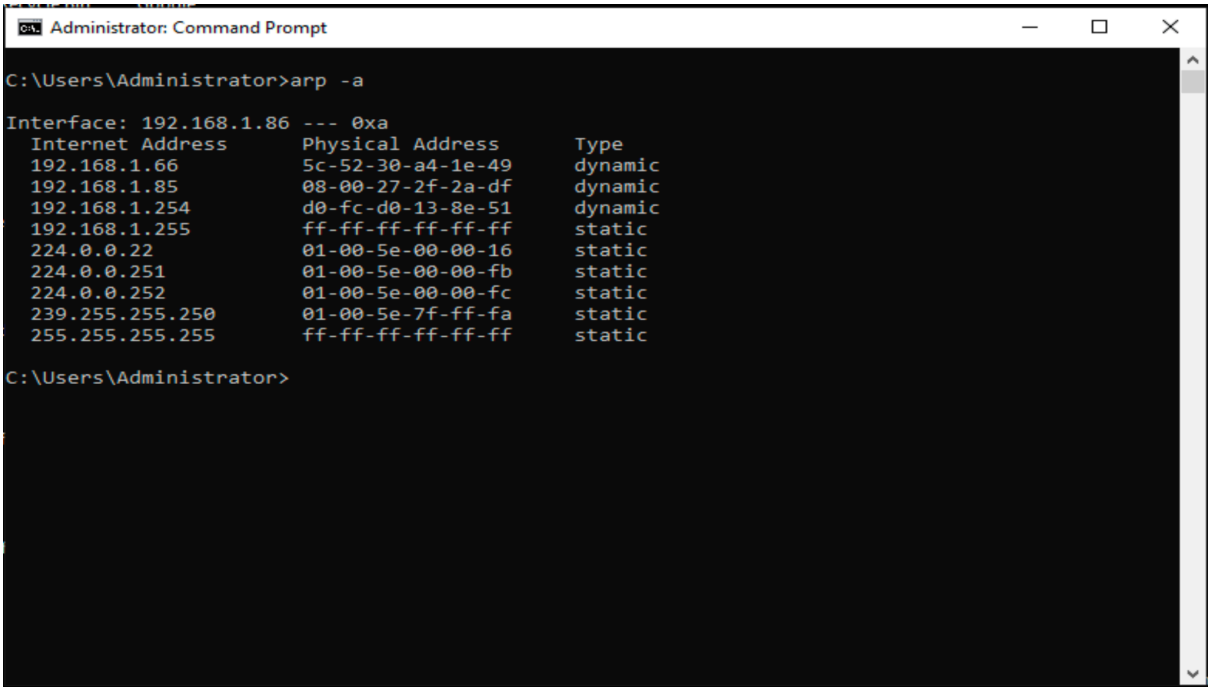
When in the Command Prompt, type in the 'ipconfig /all' command to display detailed IP configuration information for all network adapters. This includes the MAC and IP addresses as shown below:



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:



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.

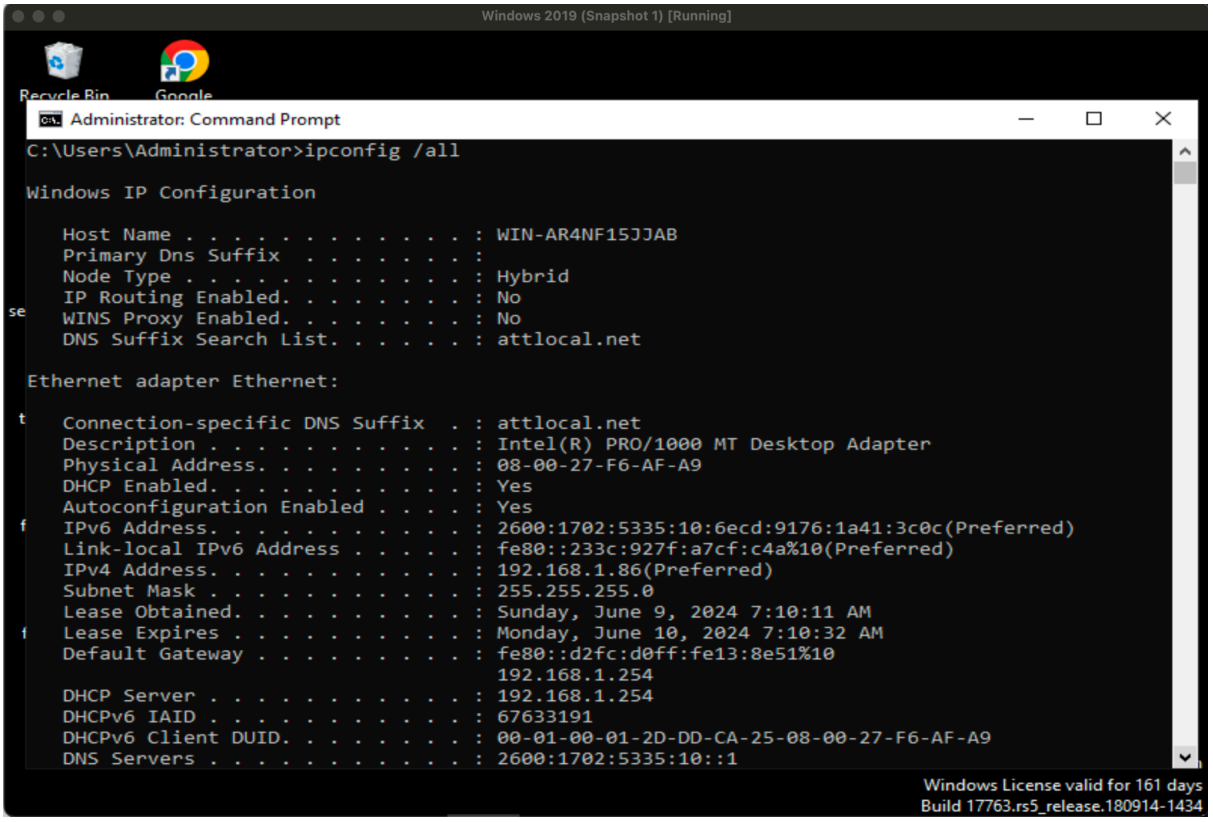
Offer: DHCP servers respond with a "DHCP Offer" message, offering an IP address.

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.



The Illustration below shows a nslookup query: