COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING.

INDIVIDUAL ASSIGNMENT

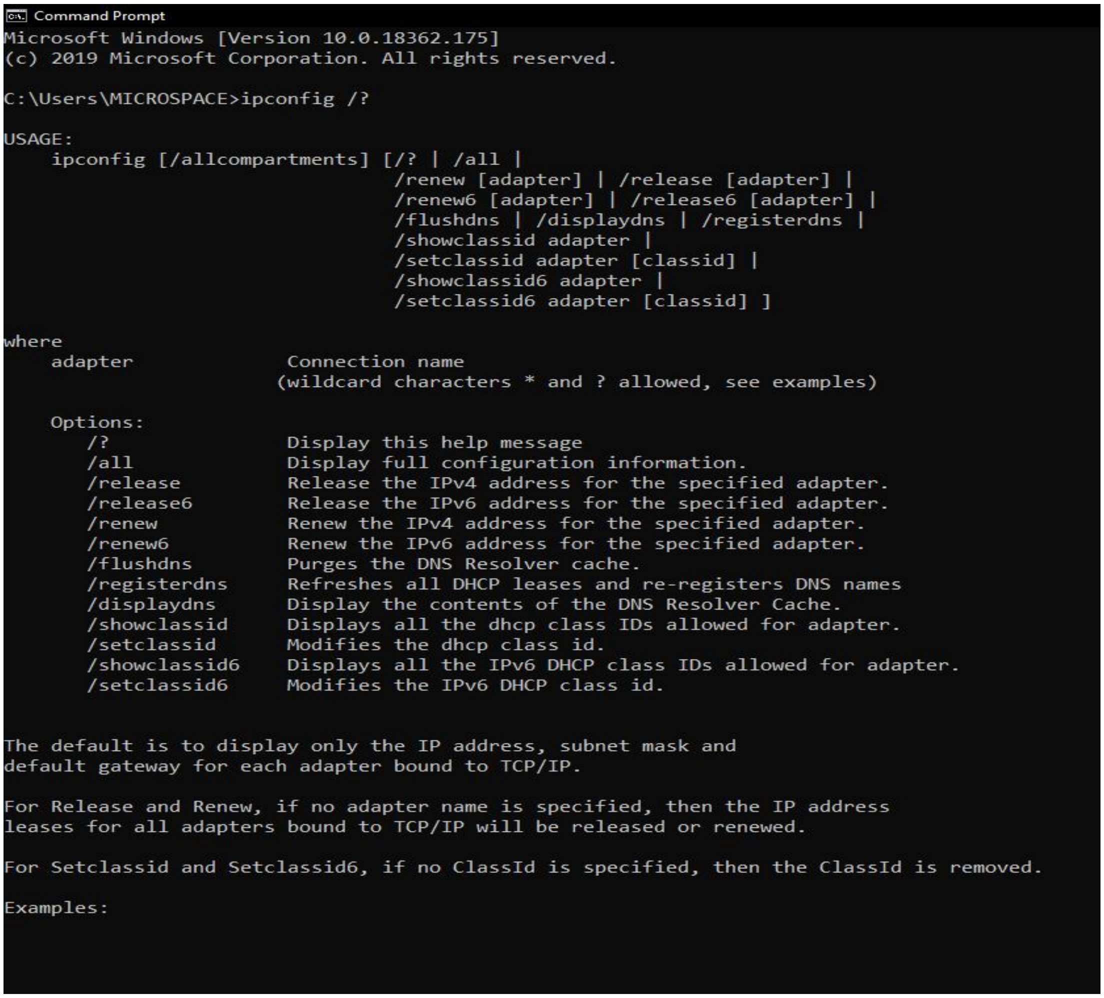
NAME: **ELIA WILLIAM MARIKI**

REGISTRATION NO: **T22-03-13063**

PROGRAM NAME: **SOFTWARE ENGINEERING (SE).**

COURSE NAME: NETWORKING
COURSE CODE:

1. Issue the command ipconfig /? capture the screen and briefly explain what it does



```
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\MICROSPACE>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:
```

The command "ipconfig /?" is used to display the help documentation and available options for the "ipconfig" command. Here's a breakdown of the command and its function:

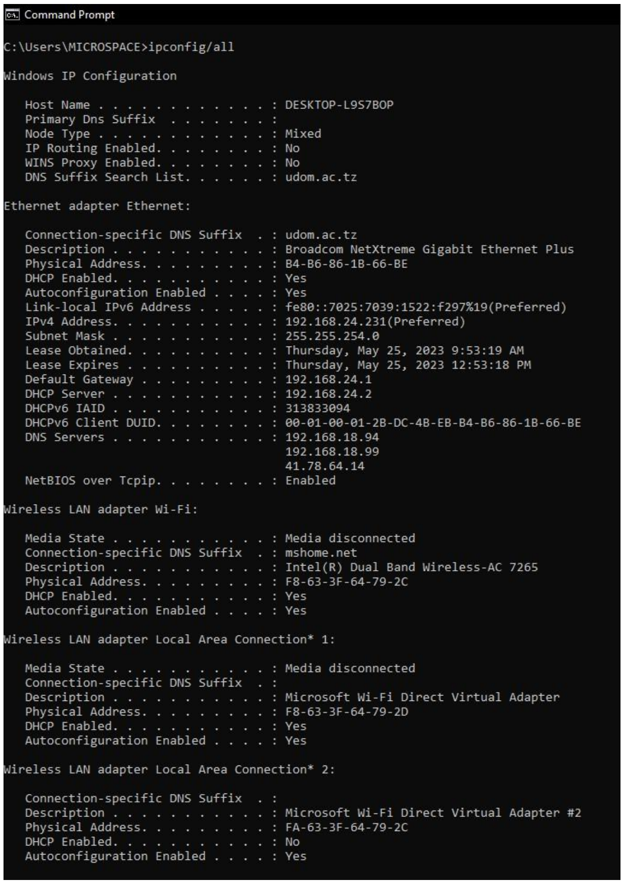
"ipconfig": This is the command itself, which is commonly available on Windows operating systems.

"/?": This is an argument passed to the command that requests the display of the command's help documentation.By executing "ipconfig /?", you can view the usage information, command syntax, and available options specific to the "ipconfig" command. The help documentation will typically provide details on how to use the command to retrieve and manage network configuration information on your Windows computer.The "ipconfig" command is used to display various network-related information, including IP addresses, subnet masks, default gateways, and more. It can be used to troubleshoot network connectivity issues, view network configuration details, and release or renew IP addresses obtained through DHCP (Dynamic Host Configuration Protocol).

The specific functionality and options available with the "ipconfig" command may vary depending on the version of Windows you are using. Therefore, it's recommended to execute "ipconfig /?" on your specific system to obtain the precise help documentation for the command.

2. Issue each subcommand in ipconfig, capture its screen and briefly explain what it does.

- **ipconfig/all**



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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-L9S7BOP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : udom.ac.tz

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : udom.ac.tz
   Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet Plus
   Physical Address. . . . . . . . . : B4-B6-86-1B-66-BE
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7025:7039:1522:f297%19(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.24.231(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : Thursday, May 25, 2023 9:53:19 AM
   Lease Expires . . . . . . . . . . : Thursday, May 25, 2023 12:53:18 PM
   Default Gateway . . . . . . . . . : 192.168.24.1
   DHCP Server . . . . . . . . . . . : 192.168.24.2
   DHCPv6 IAID . . . . . . . . . . . : 313833094
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-DC-4B-EB-B4-B6-86-1B-66-BE
   DNS Servers . . . . . . . . . . . : 192.168.18.94
                                       192.168.18.99
                                       41.78.64.14
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : mshome.net
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Physical Address. . . . . . . . . : F8-63-3F-64-79-2C
   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. . . . . . . . . : F8-63-3F-64-79-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : FA-63-3F-64-79-2C
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

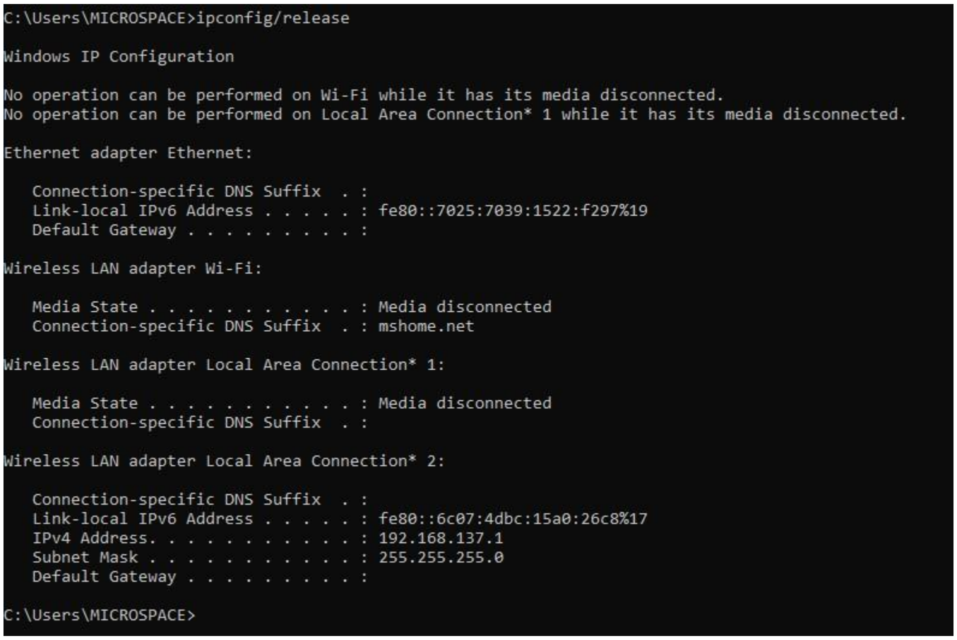
- **ipconfig/all** : This command is used in networking to gather detailed information about the network configuration of a Windows computer and connection adapters of the computer (Wired Ethernet, WiFi, Vmware adapters etc).

- This means that it display IP Configuration(including the IP address, subnet mask, default gateway, and DNS (Domain Name System)).

- It shows the Media Access Control (MAC) address of the computer's network interface card (NIC).

- It shows whether the computer is configured to obtain its IP address dynamically from a DHCP (Dynamic Host Configuration Protocol) server or if it has a static IP address assigned. It also displays the lease duration for the DHCP-assigned IP address

- **ipconfig/release**



```
C:\Users\MICROSPACE>ipconfig/release

Windows IP Configuration

No operation can be performed on Wi-Fi while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7025:7039:1522:f297%19
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c07:4dbc:15a0:26c8%17
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\MICROSPACE>
```

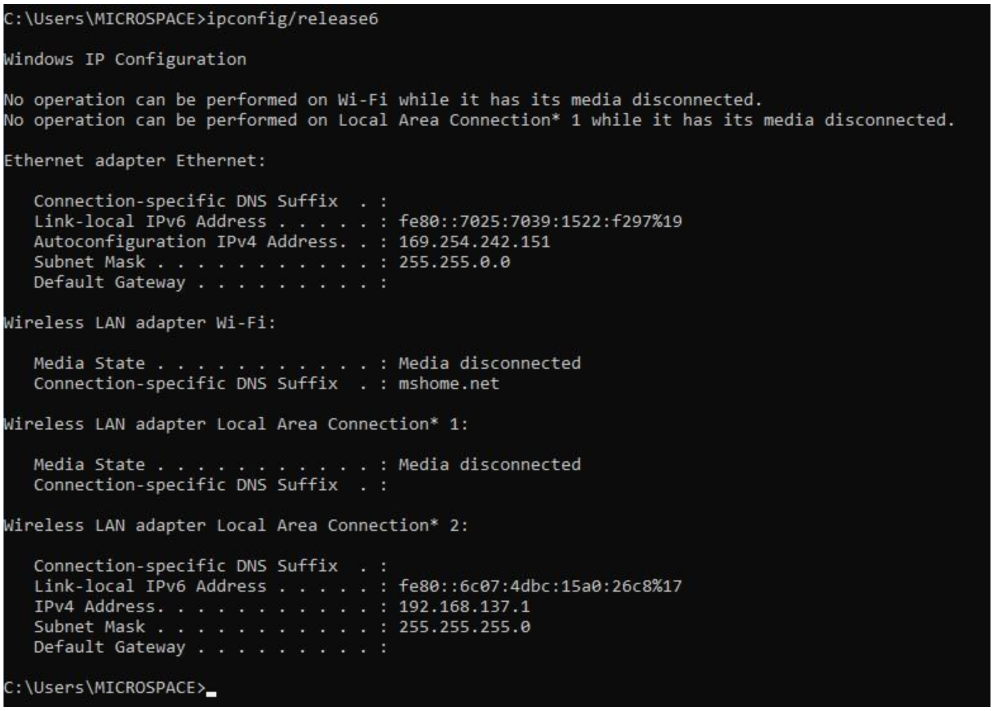
- **ipconfig/release :** This command is used in Windows networking to release the IP address assigned to a network interface card (NIC) using DHCP (Dynamic Host Configuration Protocol). but this is only for IPv4 by default

- When you execute ipconfig/release it sends a request to the DHCP server to release the current IP address assigned to the network interface , the DHCP server keeps track of IP address leases and manages the allocation of IP addresses to devices on the network

- There for it can be said that this command does process of clearing the IP configuration and finishes with prepering for renewal of new ip address.

- Also this command is useful for troubleshooting network connectivity issues or when you need to refresh your IP configuration on window computer.

- **ipconfig/release6**



```
C:\Users\MICROSPACE>ipconfig/release6

Windows IP Configuration

No operation can be performed on Wi-Fi while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7025:7039:1522:f297%19
   Autoconfiguration IPv4 Address. . : 169.254.242.151
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c07:4dbc:15a0:26c8%17
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\MICROSPACE>
```

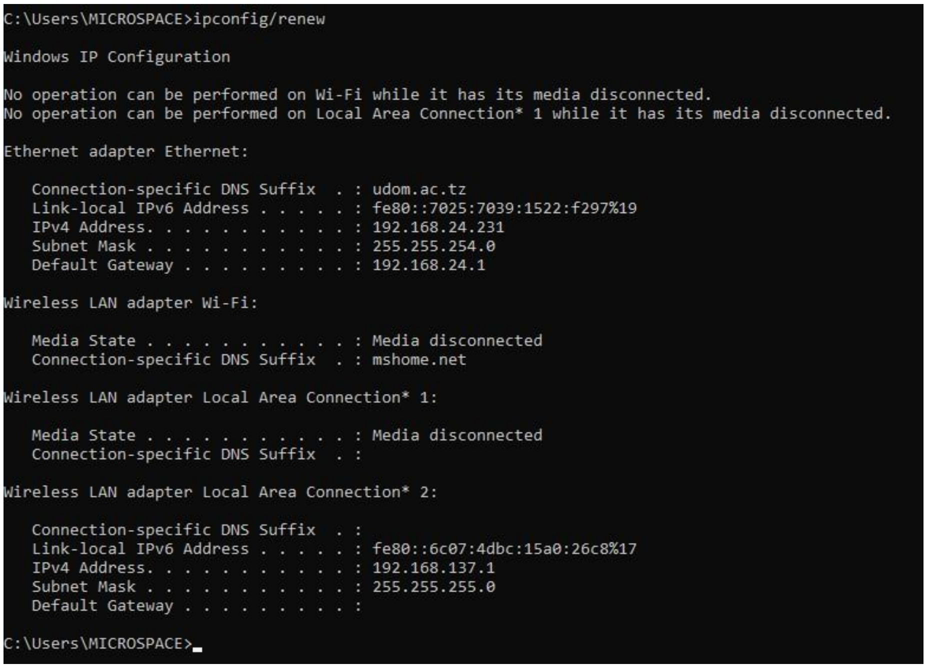
ipconfig/release6 : This command is similar to "ipconfig/release," but it specifically releases IPv6 (Internet Protocol version 6) addresses assigned to network interfaces using DHCPv6 (Dynamic Host Configuration Protocol for IPv6) hence even the it similar on how its works

❖ When you execute ipconfig/release it sends a request to the DHCP server to release the current IP address assigned to the network interface , the DHCP server keeps track of IP address leases and manages the allocation of IP addresses to devices on the network

❖ There for it can be said that this command does process of clearing the IP configuration and finishes with prepering for renewal of new ip address.r.

❖ This command is useful for troubleshooting network connectivity issues or when you need to refresh your IP configuration on a Windows computer.

- **ipconfig/renew :**



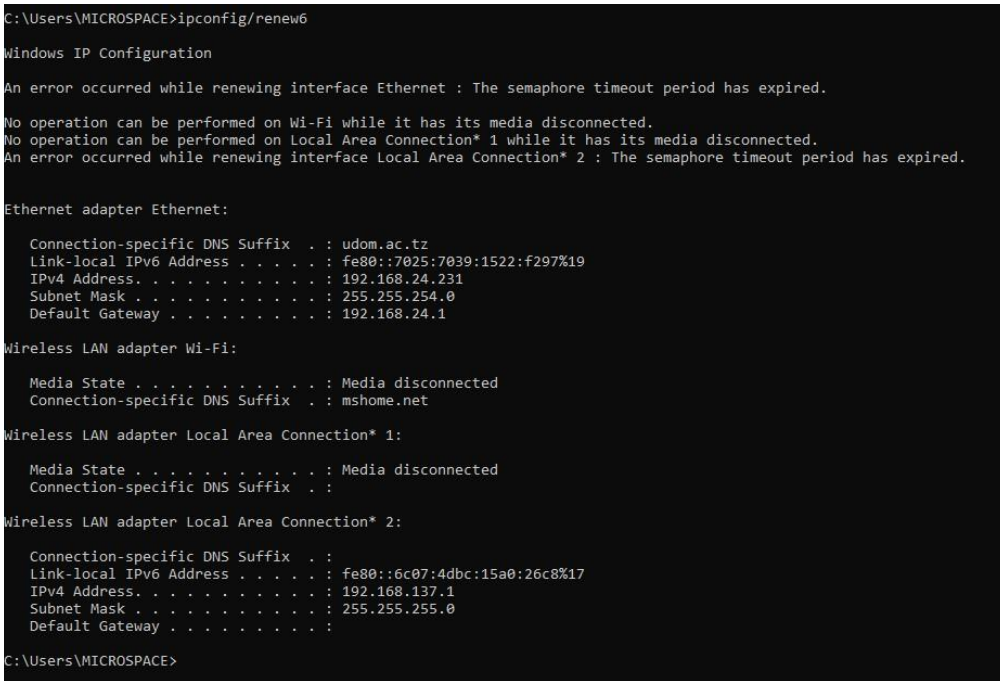
```
C:\Users\MICROSPACE>ipconfig/renew

Windows IP Configuration

No operation can be performed on Wi-Fi while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : udom.ac.tz
   Link-local IPv6 Address . . . . . : fe80::7025:7039:1522:f297%19
   IPv4 Address. . . . . . . . . . . : 192.168.24.231
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 192.168.24.1

Wireless LAN adapter Wi-Fi:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c07:4dbc:15a0:26c8%17
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\MICROSPACE>_
```

ipconfig/renew : This command is used in Windows networking to renew the IP address lease for a network interface card (NIC) using DHCP (Dynamic Host Configuration Protocol)

The major function of this command is

- ❖ Requesting a New IP Address: This means when "ipconfig/renew" is executed it sends a request to the DHCP server to obtain a new IP address lease for the network interface. The DHCP server manages the allocation of IP addresses and configuration information to devices on the network.
- ❖ Updating the IP Configuration: If the DHCP server approves the renewal request, the network interface's IP address, subnet mask, default gateway, and other network configuration settings are updated with the new values provided by the DHCP server. This allows the computer to establish connectivity on the network.
- ❖ Restoring Network Connectivity: By obtaining a renewed IP address, the computer regains network connectivity. It can communicate with other devices on the network and access the internet if applicable.

- **ipconfig/renew6 :**



```
C:\Users\MICROSPACE>ipconfig/renew6

Windows IP Configuration

An error occurred while renewing interface Ethernet : The semaphore timeout period has expired.

No operation can be performed on Wi-Fi while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
An error occurred while renewing interface Local Area Connection* 2 : The semaphore timeout period has expired.


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : udom.ac.tz
   Link-local IPv6 Address . . . . . : fe80::7025:7039:1522:f297%19
   IPv4 Address. . . . . . . . . . . : 192.168.24.231
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 192.168.24.1

Wireless LAN adapter Wi-Fi:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c07:4dbc:15a0:26c8%17
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\MICROSPACE>
```

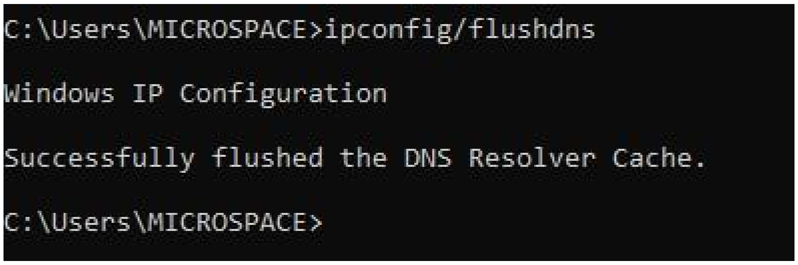
❖ **ipconfig/renew6:** This command is used in Windows to renew the IP address configuration of a network interface. When followed by the number "6," it specifies the network interface index that means IPv6. and it perform the followings functions

◆ IP Address Renewal: The primary function of "ipconfig/renew" is to renew the IP address configuration of a specific network interface. By appending "6" to the command, it targets the network interface with index 6 and requests a new IP address lease from the Dynamic Host Configuration Protocol (DHCP) server. This is useful when you want to refresh the network settings of a particular interface.

◆ Updating DHCP Lease: When a computer is connected to a network using DHCP, it leases an IP address for a specific duration. The "ipconfig/renew" command triggers the renewal process, which involves contacting the DHCP server and requesting a lease extension or a new IP address. By specifying "6," it ensures that only the network interface with index 6 attempts to renew its DHCP lease.

◆ Fixing Networking Issues: Sometimes, network connectivity issues can arise due to an expired IP address lease or incorrect configuration. By using "ipconfig/renew 6," you can attempt to resolve such issues by forcing the renewal of the IP address specifically for the network interface with index 6. This can help troubleshoot problems related to network connectivity, ensuring that the interface receives a valid IP address to establish communication within the network

- **ipconfig/flushdns:**



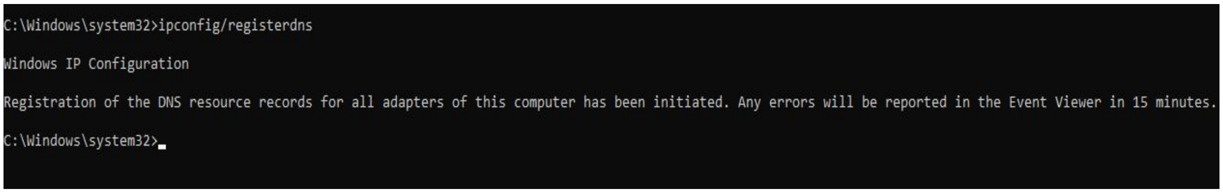
```
C:\Users\MICROSPACE>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\MICROSPACE>
```

❖ **ipconfig/flushdns :** This command is used in Windows OS to clear the DNS resolver cache

❖ The primary function of this command is to clear the DNS resolver cache on your computer.

❖ The DNS resolver cache stores the IP addresses of previously resolved domain names. When you visit a website or connect to a network resource, your computer first checks the DNS cache to see if it already has the IP address associated with the domain name. By executing this condition you can clear this cache and force your computer to retrieve the latest IP address information from DNS servers the next time you access a domain.

- **ipconfig/registerdns :**

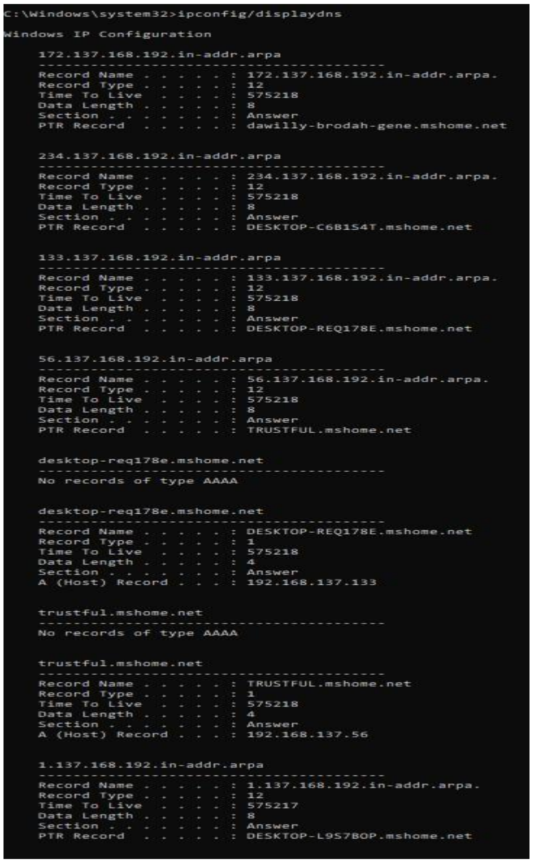


```
C:\Windows\system32>ipconfig/registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.

C:\Windows\system32>
```

❖ **ipconfig/registerdns :** This command is serves the purpose of manually registering DNS records for a computer with the DNS server

❖ This means that the primary function of this command is to manually initiate the registration of DNS records for your computer with the DNS server. When executed, the command instructs the computer to send a registration request to the DNS server, updating or creating the appropriate DNS records for the computer's hostname and IP address.

- **ipconfig/displaydns :**

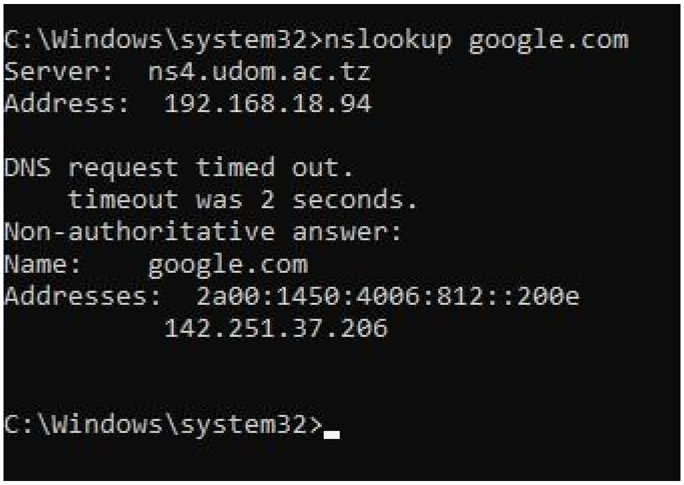


```
C:\Windows\system32>ipconfig/displaydns

Windows IP Configuration

    172.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 172.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 575218
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : dawilly-brodah-gene.mshome.net


    234.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 234.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 575218
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : DESKTOP-C6B154T.mshome.net


    133.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 133.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 575218
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : DESKTOP-REQ178E.mshome.net


    56.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 56.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 575218
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : TRUSTFUL.mshome.net


    desktop-req178e.mshome.net
    ----------------------------------------
    No records of type AAAA


    desktop-req178e.mshome.net
    ----------------------------------------
    Record Name . . . . . : DESKTOP-REQ178E.mshome.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 575218
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.137.133


    trustful.mshome.net
    ----------------------------------------
    No records of type AAAA


    trustful.mshome.net
    ----------------------------------------
    Record Name . . . . . : TRUSTFUL.mshome.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 575218
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.137.56


    1.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 1.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 575217
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : DESKTOP-L9S7BOP.mshome.net
```

ipconfig/displaydns : This command function is to display the contents of the DNS resolver cache on your computer. The DNS resolver cache stores the IP addresses of previously resolved domain names, allowing for faster subsequent access to those domains. By executing "ipconfig/displaydns," you can view the list of domain names and their corresponding IP addresses that are currently stored in the cache**.**

3.Issue the command nslookup [Use one domain address of your choice] capture the screen and briefly explain what it does.

- **nslookup google.com**



```
C:\Windows\system32>nslookup google.com
Server:  ns4.udom.ac.tz
Address:  192.168.18.94

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:4006:812::200e
          142.251.37.206


C:\Windows\system32>
```

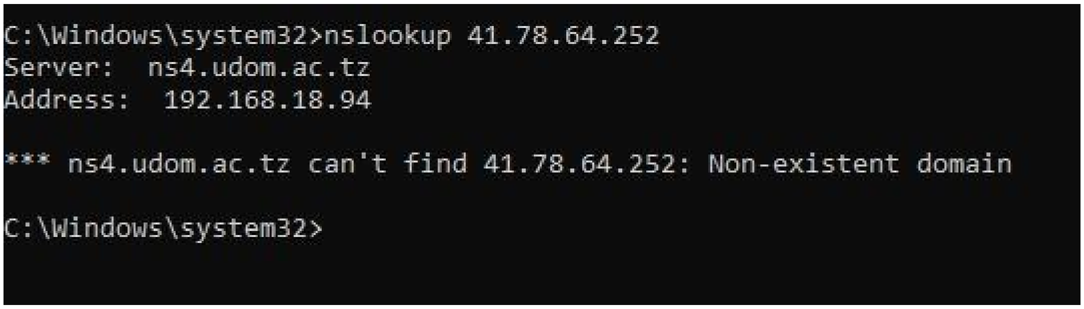
❖ This command "nslookup google.com" is used to perform a DNS lookup for the domain name "google.com".

❖ it provides a DNS Resolution this means that the primary function of "nslookup google.com" is to query the DNS (Domain Name System) server for the IP address associated with the domain name "google.com". When you execute this command, it sends a DNS lookup request to your computer's configured DNS server, which then responds with the IP address information for "google.com".

4.Issue the command nslookup [Use your public IP address, obtain it from google] capture the screen and briefly explain what it does

>from google my ip address is 41.78.64.252

- **nslookup 41.78.64.252**



```
C:\Windows\system32>nslookup 41.78.64.252
Server:  ns4.udom.ac.tz
Address:  192.168.18.94

*** ns4.udom.ac.tz can't find 41.78.64.252: Non-existent domain

C:\Windows\system32>
```

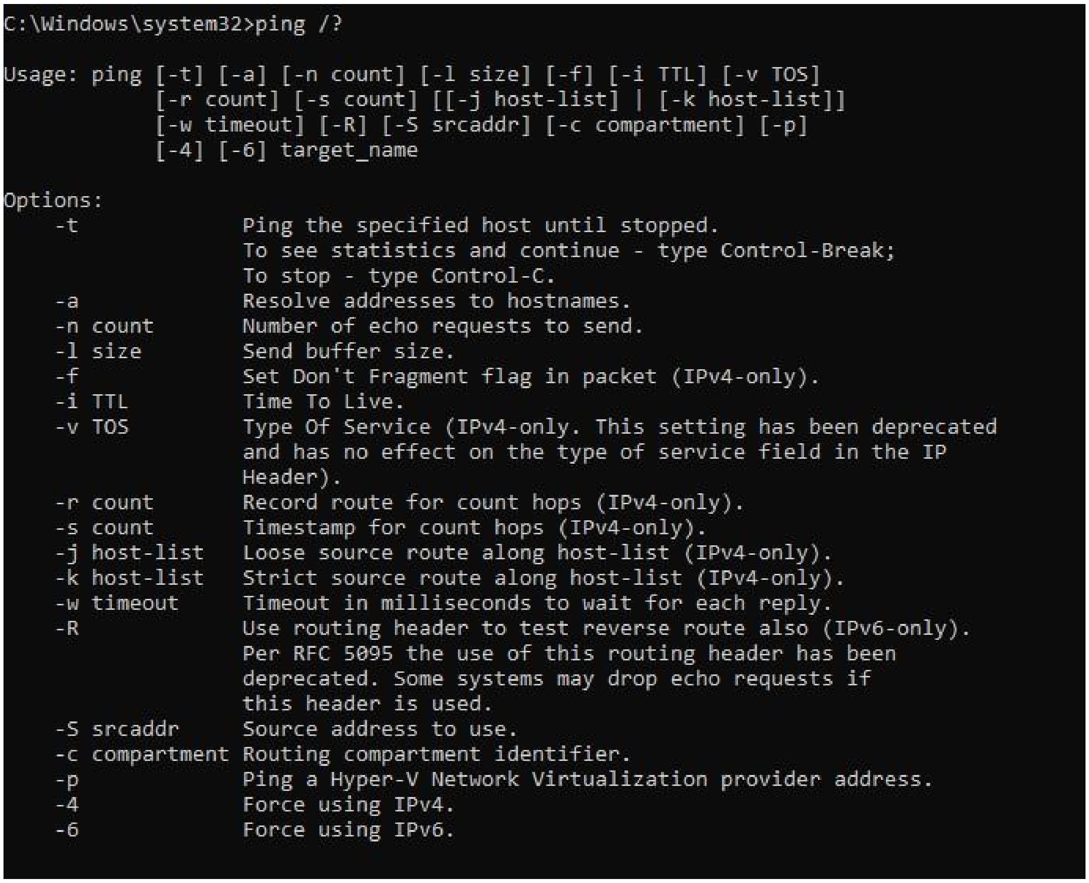
When the command "nslookup 41.78.64.252," executed you are performing a reverse DNS lookup for the IP address 41.78.64.252.

Reverse DNS Lookup: The primary function of "nslookup 41.78.64.252" is to query the DNS (Domain Name System) server for the hostname associated with the given IP address, in this case, 41.78.64.252. Instead of looking up a domain name to obtain its IP address, a reverse DNS lookup looks up an IP address to find its associated hostname.

but according to the screenshot output "******ns4.udom.ac.tz can't find 42.78.64.252: Non-existent domain": This is the result of the reverse DNS lookup. The message states that the DNS server "ns4.udom.ac.tz" was unable to find a domain associated with the IP address 42.78.64.252, indicating that no reverse DNS record exists for that IP address.

5. Issue the command ping /? capture the screen and briefly explain what it does.

- **ping /?**



```
C:\Windows\system32>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

The command "ping /?" is used to display the help information and usage options for the "ping" command in Windows operating systems. When you execute "ping /?", it provides a brief description of the command and lists the available command-line options and parameters

also it gives the otherinformation like

Usage: This section provides a basic usage example of the "ping" command, demonstrating how to use it with different options and parameters.

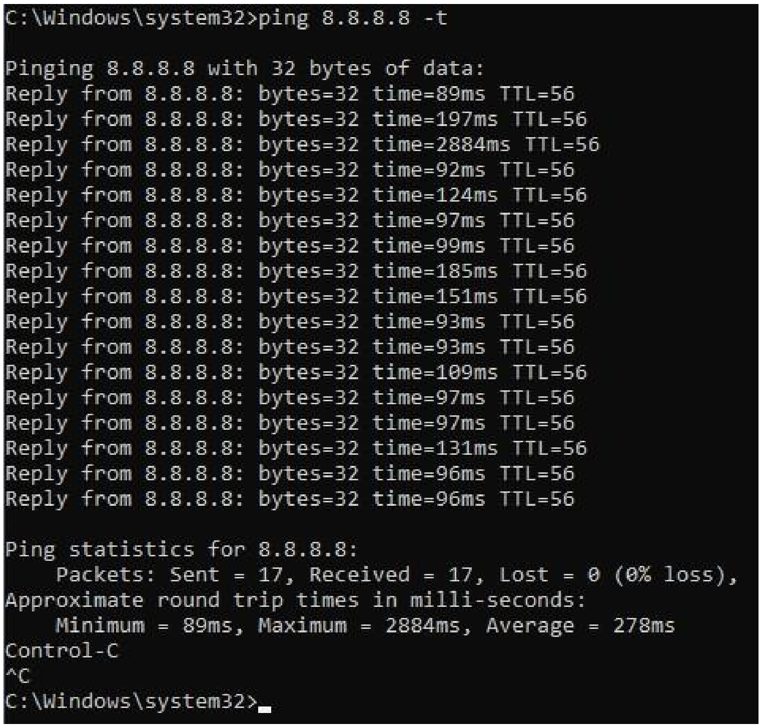
Description: This section gives a brief explanation of the "ping" command and its purpose, which is to send ICMP echo request packets to a specified network host or IP address and receive ICMP echo reply packets in response.

Options: This section lists the various command-line options available with the "ping" command. It includes options such as "-t" for continuous pinging, "-n" for specifying the number of echo requests to send, "-l" for setting the size of the ICMP packets, and more. Each option is typically accompanied by a brief description of its functionality.

Examples: This section provides some usage examples that demonstrate how to utilize the "ping" command with different options and parameters for specific scenarios.

6. Issue each subcommand in ping, capture its screen and briefly explain what it does.

- **ping 8.8.8.8 -t**



```
C:\Windows\system32>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=89ms TTL=56
Reply from 8.8.8.8: bytes=32 time=197ms TTL=56
Reply from 8.8.8.8: bytes=32 time=2884ms TTL=56
Reply from 8.8.8.8: bytes=32 time=92ms TTL=56
Reply from 8.8.8.8: bytes=32 time=124ms TTL=56
Reply from 8.8.8.8: bytes=32 time=97ms TTL=56
Reply from 8.8.8.8: bytes=32 time=99ms TTL=56
Reply from 8.8.8.8: bytes=32 time=185ms TTL=56
Reply from 8.8.8.8: bytes=32 time=151ms TTL=56
Reply from 8.8.8.8: bytes=32 time=93ms TTL=56
Reply from 8.8.8.8: bytes=32 time=93ms TTL=56
Reply from 8.8.8.8: bytes=32 time=109ms TTL=56
Reply from 8.8.8.8: bytes=32 time=97ms TTL=56
Reply from 8.8.8.8: bytes=32 time=97ms TTL=56
Reply from 8.8.8.8: bytes=32 time=131ms TTL=56
Reply from 8.8.8.8: bytes=32 time=96ms TTL=56
Reply from 8.8.8.8: bytes=32 time=96ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 17, Received = 17, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 89ms, Maximum = 2884ms, Average = 278ms
Control-C
^C
C:\Windows\system32>
```

This command "ping 8.8.8.8 -t" is used in Windows os to continuously send ICMP echo request packets to the IP address 8.8.8.8 (which is Google's public DNS server) and receive ICMP echo reply packets in response

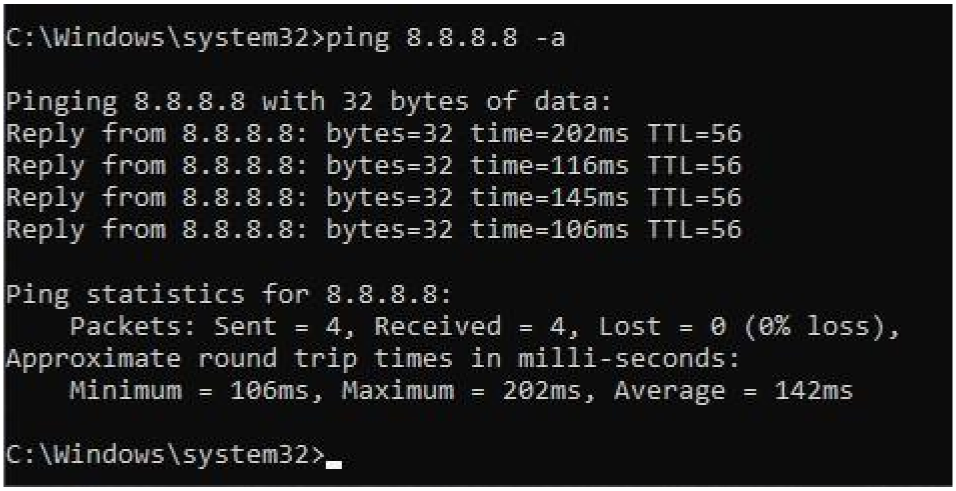
Here's a brief explanation of what this command does:

Pinging a Specific IP Address: The "ping" command is used to test network connectivity between your computer and a target IP address or hostname. In this case, the target IP address is 8.8.8.8, which is the IP address of Google's public DNS server. The command sends ICMP echo request packets to this IP address.

Continuous Pinging: The "-t" option is used to instruct the "ping" command to keep sending echo request packets continuously, without stopping. By using this option, the command will keep pinging the specified IP address until it is manually stopped by the user.

ICMP Echo Request and Reply: ICMP (Internet Control Message Protocol) echo request packets are used to request a response from the target IP address. When the target receives the echo request packet, it sends an ICMP echo reply packet back to the source IP address. This exchange of packets allows the "ping" command to measure the round-trip time (RTT) and determine the network connectivity and latency between the source and target.

- **ping 8.8.8.8 -a :**



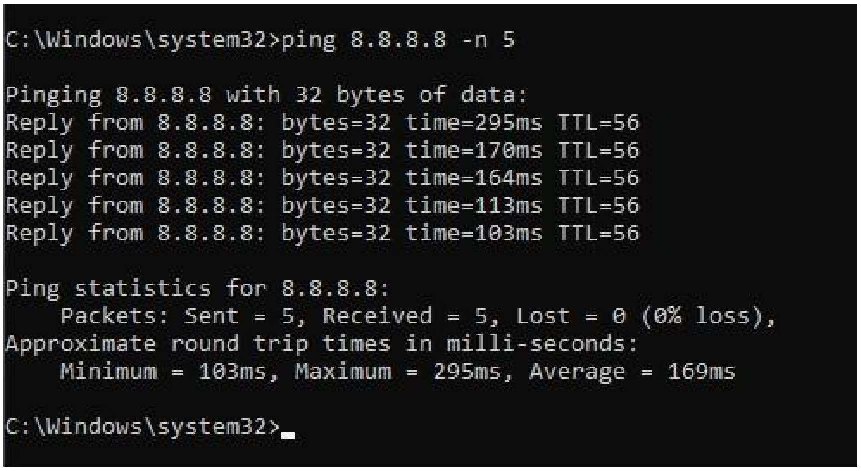
```
C:\Windows\system32>ping 8.8.8.8 -a

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=202ms TTL=56
Reply from 8.8.8.8: bytes=32 time=116ms TTL=56
Reply from 8.8.8.8: bytes=32 time=145ms TTL=56
Reply from 8.8.8.8: bytes=32 time=106ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 106ms, Maximum = 202ms, Average = 142ms

C:\Windows\system32>
```

The command "ping 8.8.8.8 -a" is used in Windows operating systems to ping the IP address 8.8.8.8 (Google's public DNS server) and attempt to resolve its corresponding hostname. Here's a brief explanation of what this command does:

Pinging a Specific IP Address: The "ping" command is used to test network connectivity between your computer and a target IP address. In this case, the target IP address is 8.8.8.8, which is the IP address of Google's public DNS server. The command sends ICMP echo request packets to this IP address.

Resolving Hostname with the "-a" Option: The "-a" option is used to enable hostname resolution in the "ping" command. By including this option, the command attempts to resolve the IP address 8.8.8.8 to its corresponding hostname.

- **ping 8.8.8.8 -n 5 :**



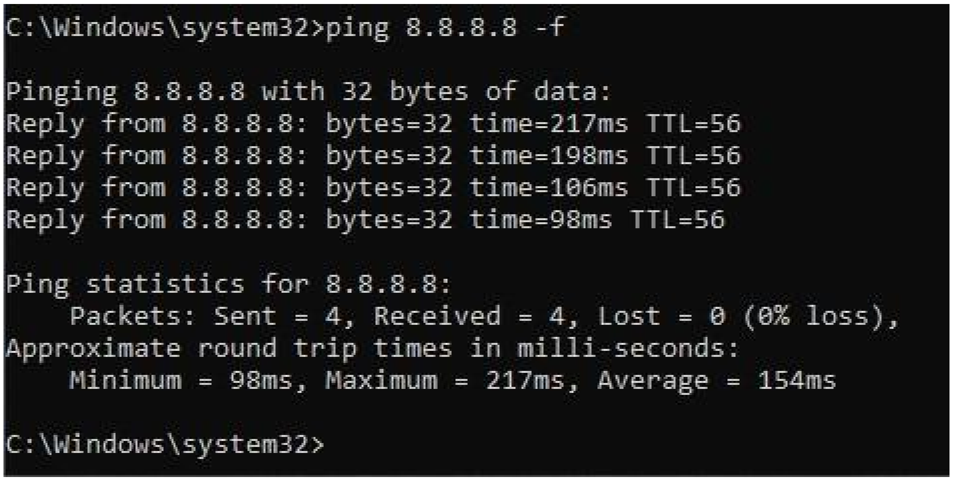
```
C:\Windows\system32>ping 8.8.8.8 -n 5

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=295ms TTL=56
Reply from 8.8.8.8: bytes=32 time=170ms TTL=56
Reply from 8.8.8.8: bytes=32 time=164ms TTL=56
Reply from 8.8.8.8: bytes=32 time=113ms TTL=56
Reply from 8.8.8.8: bytes=32 time=103ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 103ms, Maximum = 295ms, Average = 169ms

C:\Windows\system32>
```

The command "ping 8.8.8.8 -n 5" is used in Windows operating systems to send a specified number of ICMP echo request packets to the IP address 8.8.8.8 (which is Google's public DNS server). Here's a brief explanation of what this command does:

Pinging a Specific IP Address: The "ping" command is used to test network connectivity between your computer and a target IP address or hostname. In this case, the target IP address is 8.8.8.8, which is the IP address of Google's public DNS server. The command sends ICMP echo request packets to this IP address.

Specifying the Number of Echo Requests: The "-n" option is used to specify the number of echo request packets to send. In the command "ping 8.8.8.8 -n 5", the value "5" indicates that the command will send 5 ICMP echo request packets to the IP address 8.8.8.8.

- **ping 8.8.8.8 -f :**



```
C:\Windows\system32>ping 8.8.8.8 -f

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=217ms TTL=56
Reply from 8.8.8.8: bytes=32 time=198ms TTL=56
Reply from 8.8.8.8: bytes=32 time=106ms TTL=56
Reply from 8.8.8.8: bytes=32 time=98ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 98ms, Maximum = 217ms, Average = 154ms

C:\Windows\system32>
```

The command "ping 8.8.8.8 -f" is used in Windows operating systems to send ICMP echo request packets to the IP address 8.8.8.8 (Google's public DNS server) with the "Don't Fragment" (DF) flag set. Here's a brief explanation of what this command does:

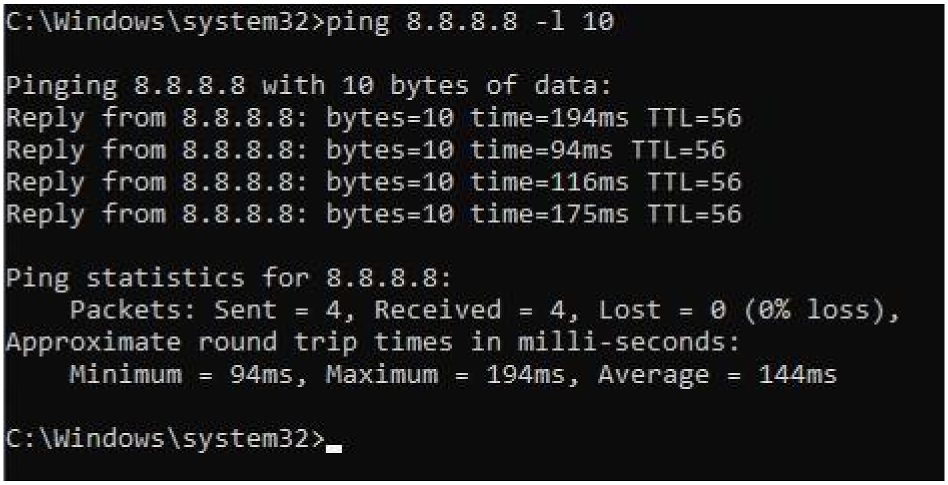
Pinging a Specific IP Address: The "ping" command is used to test network connectivity between your computer and a target IP address. In this case, the target IP address is 8.8.8.8, which is the IP address of Google's public DNS server. The command sends ICMP echo request packets to this IP address.

Setting the "Don't Fragment" Flag: The "-f" option is used to set the "Don't Fragment" (DF) flag in the ICMP echo request packets. The DF flag indicates that the packet should not be fragmented if its size exceeds the maximum transmission unit (MTU) of the network path.

The output of the command will include the ping statistics for the specified IP address, such as round-trip time (RTT), packet loss, and other relevant details. The statistics will be based on the ICMP echo request packets sent with the "Don't Fragment" flag set.

By executing "ping 8.8.8.8 -f", you initiate pinging to Google's public DNS server with ICMP echo request packets that have the "Don't Fragment" flag set. This command can be useful for testing network connectivity and determining if the network path allows for packet fragmentation.

- **ping 8.8.8.8 -l 10 :**



```
C:\Windows\system32>ping 8.8.8.8 -l 10

Pinging 8.8.8.8 with 10 bytes of data:
Reply from 8.8.8.8: bytes=10 time=194ms TTL=56
Reply from 8.8.8.8: bytes=10 time=94ms TTL=56
Reply from 8.8.8.8: bytes=10 time=116ms TTL=56
Reply from 8.8.8.8: bytes=10 time=175ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 94ms, Maximum = 194ms, Average = 144ms

C:\Windows\system32>
```

The command "ping 8.8.8.8 -l 10" is used in Windows operating systems to send ICMP echo request packets to the IP address 8.8.8.8 (Google's public DNS server) with a specific packet size. Here's a brief explanation of what this command does:

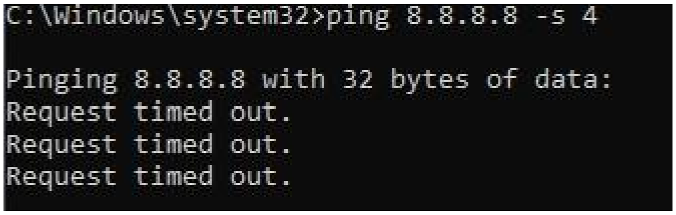
Pinging a Specific IP Address: The "ping" command is used to test network connectivity between your computer and a target IP address. In this case, the target IP address is 8.8.8.8, which is the IP address of Google's public DNS server. The command sends ICMP echo request packets to this IP address.

Specifying the Packet Size: The "-l" option is used to specify the size of the ICMP echo request packets to send. In the command "ping 8.8.8.8 -l 10", the value "10" indicates that the command will send ICMP echo request packets with a size of 10 bytes.

The output of the command will include the ping statistics for the specified IP address, such as round-trip time (RTT), packet loss, and other relevant details. The statistics will be based on the ICMP echo request packets sent with the specified packet size.

By executing "ping 8.8.8.8 -l 10", you initiate pinging to Google's public DNS server with ICMP echo request packets of 10 bytes in size. This command can be useful for testing network connectivity and measuring the response time for small packet sizes.

- **ping 8.8.8.8 -s 4 :**



```
C:\Windows\system32>ping 8.8.8.8 -s 4

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

The command "ping 8.8.8.8 -i 12" is used to test the network connectivity between your computer and a specific IP address, in this case, 8.8.8.8. Here's a breakdown of the command and its functions:

"ping": This is the command itself, which is typically available on most operating systems.

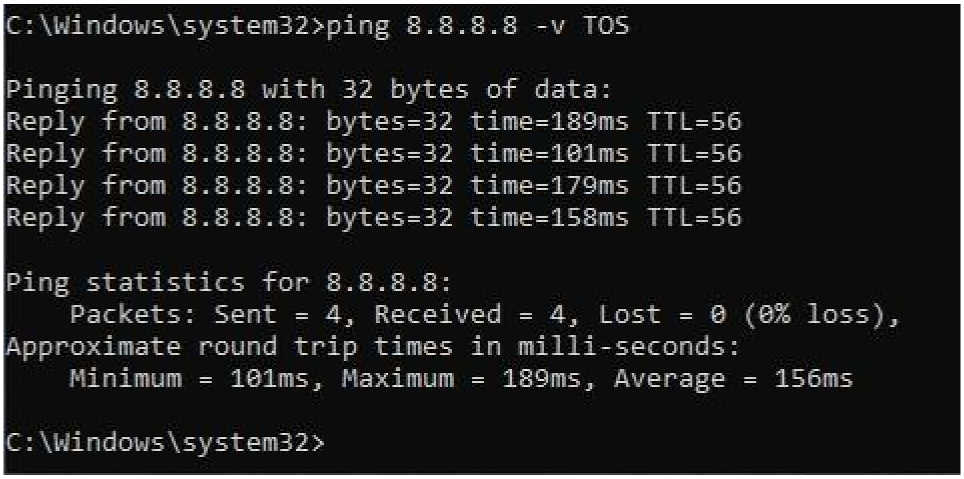
"8.8.8.8": This is the IP address that you want to ping. In this case, it's the IP address of Google's public DNS server.

"-i 12": This is an optional flag that specifies the interval between ping requests. In this case, it's set to 12 seconds.

When you run this command, your computer will send a series of ICMP (Internet Control Message Protocol) echo request packets to the specified IP address, and it will wait for a response. The destination device, in this case, the Google DNS server, will receive these packets and respond with ICMP echo reply packets if it's reachable and responsive.

The interval of 12 seconds specified by the "-i" flag means that the ping command will send a new ICMP echo request packet every 12 seconds until you manually stop it. The response time and other statistics will be displayed for each ping reply received, allowing you to assess the quality of the network connection to the target IP address.

- **ping 8.8.8.8 -v TOS :**



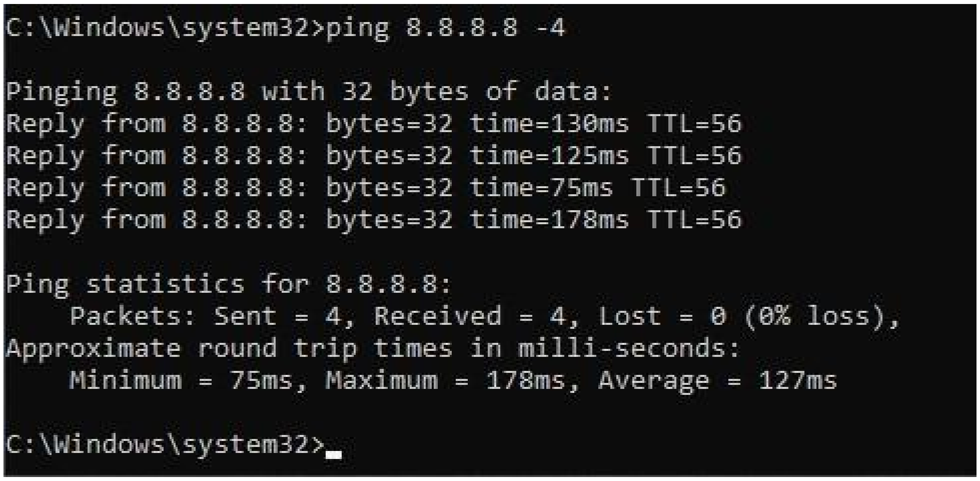
```
C:\Windows\system32>ping 8.8.8.8 -v TOS

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=189ms TTL=56
Reply from 8.8.8.8: bytes=32 time=101ms TTL=56
Reply from 8.8.8.8: bytes=32 time=179ms TTL=56
Reply from 8.8.8.8: bytes=32 time=158ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 101ms, Maximum = 189ms, Average = 156ms

C:\Windows\system32>
```

The "ping" command is primarily used for testing network connectivity and measuring round-trip time (RTT) between a source device and a destination IP address. It sends ICMP echo request packets and receives ICMP echo reply packets from the destination.

If you have a specific requirement related to the TOS (Type of Service) field, it's unlikely that you can directly specify it using the "ping" command alone. The TOS field is used to prioritize or differentiate network traffic based on specific requirements such as QoS (Quality of Service) or differentiated services.

If you need to set the TOS field for network traffic, you might need to use specialized tools or utilities that allow you to manipulate packet headers and set the TOS field explicitly. These tools could include low-level networking libraries or specific network testing utilities that provide more advanced options than the basic "ping" command.

- ***ping 8.8.8.8 -4***



```
C:\Windows\system32>ping 8.8.8.8 -4

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=130ms TTL=56
Reply from 8.8.8.8: bytes=32 time=125ms TTL=56
Reply from 8.8.8.8: bytes=32 time=75ms TTL=56
Reply from 8.8.8.8: bytes=32 time=178ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 75ms, Maximum = 178ms, Average = 127ms

C:\Windows\system32>
```

The command "ping 8.8.8.8 -4" is used to explicitly specify the IP version to use for the ping command. Here's a breakdown of the command:

"ping": This is the command itself, which is typically available on most operating systems.

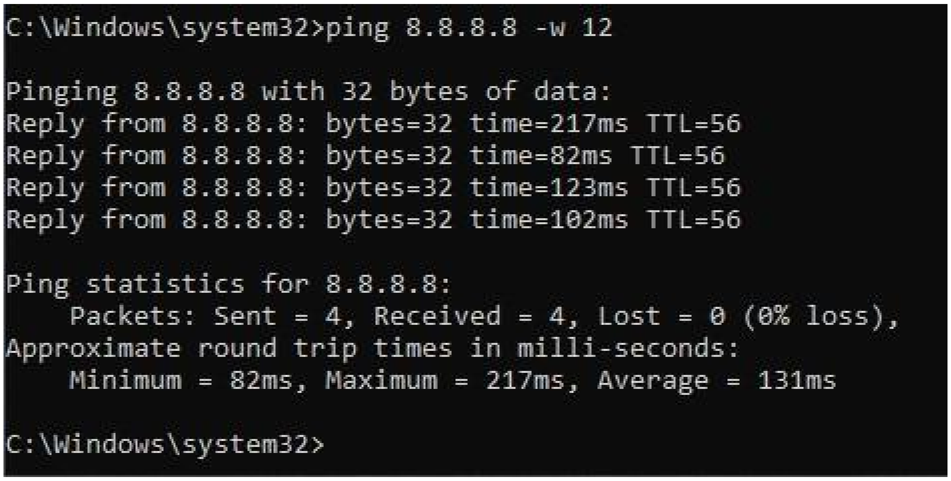
"8.8.8.8": This is the IP address that you want to ping. In this case, it's the IP address of Google's public DNS server.

"-4": This option instructs the ping command to use IPv4 for the ping operation.

By default, the ping command may automatically determine whether to use IPv4 or IPv6 based on the network configuration and the availability of the IP address type. However, using the "-4" option forces the ping command to use IPv4 explicitly.

This can be useful in scenarios where you want to test the connectivity specifically over IPv4 or if your system has both IPv4 and IPv6 enabled, and you want to ensure that the ping uses IPv4 for troubleshooting or compatibility purposes.

- **ping 8.8.8.8 -w 12 :**



```
C:\Windows\system32>ping 8.8.8.8 -w 12

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=217ms TTL=56
Reply from 8.8.8.8: bytes=32 time=82ms TTL=56
Reply from 8.8.8.8: bytes=32 time=123ms TTL=56
Reply from 8.8.8.8: bytes=32 time=102ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 82ms, Maximum = 217ms, Average = 131ms

C:\Windows\system32>
```

The command "ping 8.8.8.8 -w 12" is used to test network connectivity to the IP address 8.8.8.8 with a specific timeout value. Here's a breakdown of the command and its function:

"ping": This is the command itself, which is used to send ICMP echo request packets and receive ICMP echo reply packets.

"8.8.8.8": This is the IP address you want to ping. In this case, it's the IP address of Google's public DNS server.

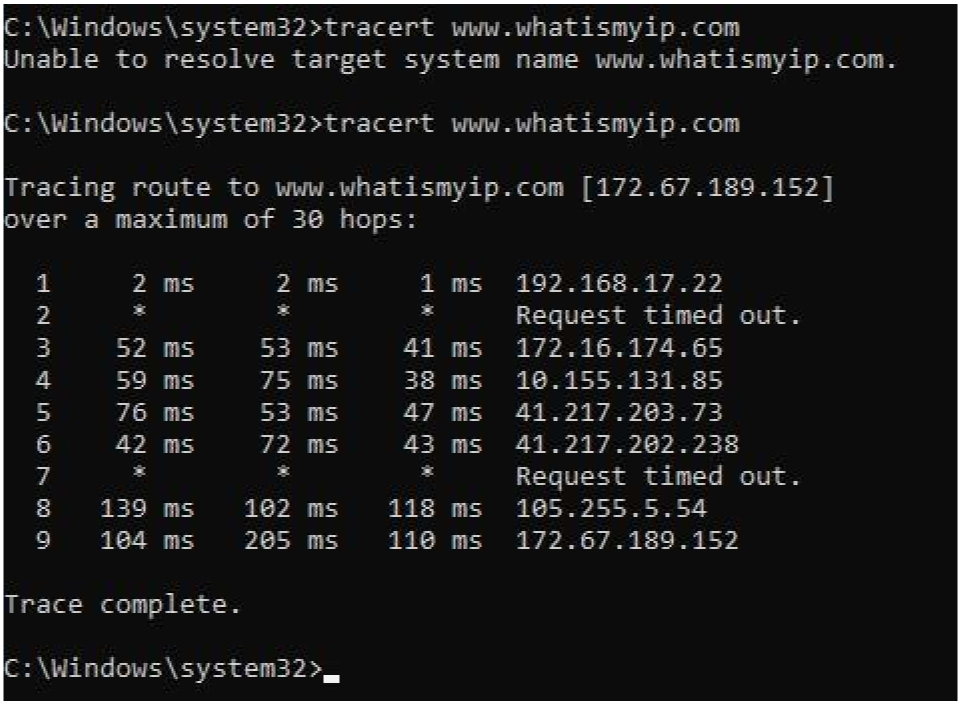
"-w 12": This is an optional flag that specifies the timeout value in milliseconds. In this case, it's set to 12 milliseconds.

When you run this command, your computer will send ICMP echo request packets to the specified IP address (8.8.8.8) and wait for ICMP echo reply packets. The timeout value of 12 milliseconds specified by the "-w" flag means that if your computer does not receive a reply within that time frame, it will consider the ping as unsuccessful and report a timeout.

By specifying a timeout value, you can control the duration for which your computer waits for a response from the destination IP address. This can be useful to determine if there are any network connectivity issues or if the target device is not responding within the specified time.

7. Issue the command tracert [Use three different domain addresses of your choice] capture the screen and briefly explain what it does.

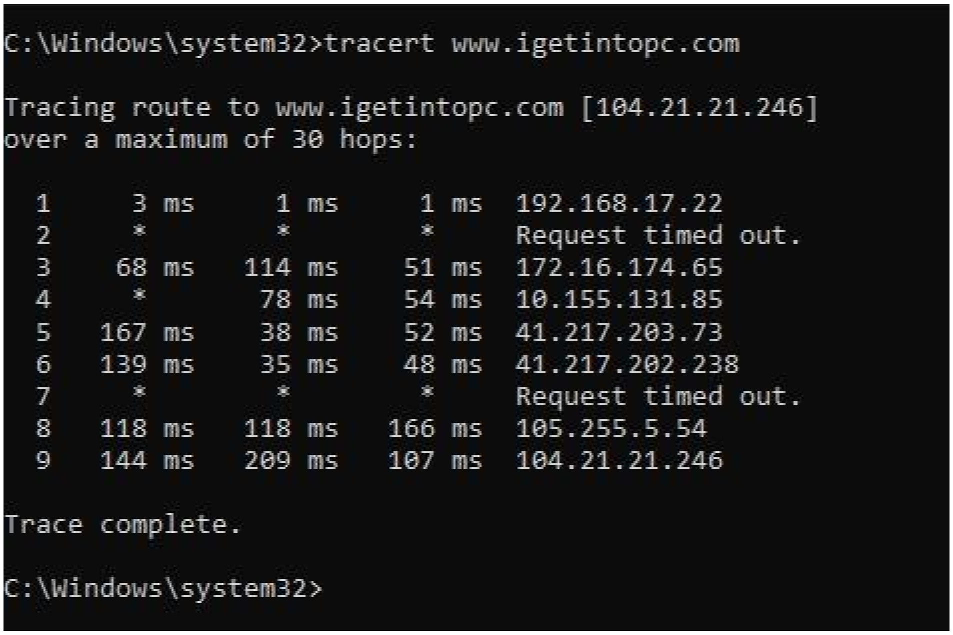
- **tracert www.whatismyip.com**



```
C:\Windows\system32>tracert www.whatismyip.com
Unable to resolve target system name www.whatismyip.com.

C:\Windows\system32>tracert www.whatismyip.com

Tracing route to www.whatismyip.com [172.67.189.152]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.17.22
  2     *        *        *     Request timed out.
  3    52 ms    53 ms    41 ms  172.16.174.65
  4    59 ms    75 ms    38 ms  10.155.131.85
  5    76 ms    53 ms    47 ms  41.217.203.73
  6    42 ms    72 ms    43 ms  41.217.202.238
  7     *        *        *     Request timed out.
  8   139 ms   102 ms   118 ms  105.255.5.54
  9   104 ms   205 ms   110 ms  172.67.189.152

Trace complete.

C:\Windows\system32>
```

The command "tracert www.whatismyip.com" is used to track the network path from your computer to the destination website. It works by sending a series of ICMP (Internet Control Message Protocol) echo request packets with varying time-to-live (TTL) values. Each router along the path decrements the TTL value, and when it reaches zero, the router sends an ICMP time exceeded message back to your computer. This allows you to see the IP addresses of the intermediate routers and measure the latency or response time at each hop.

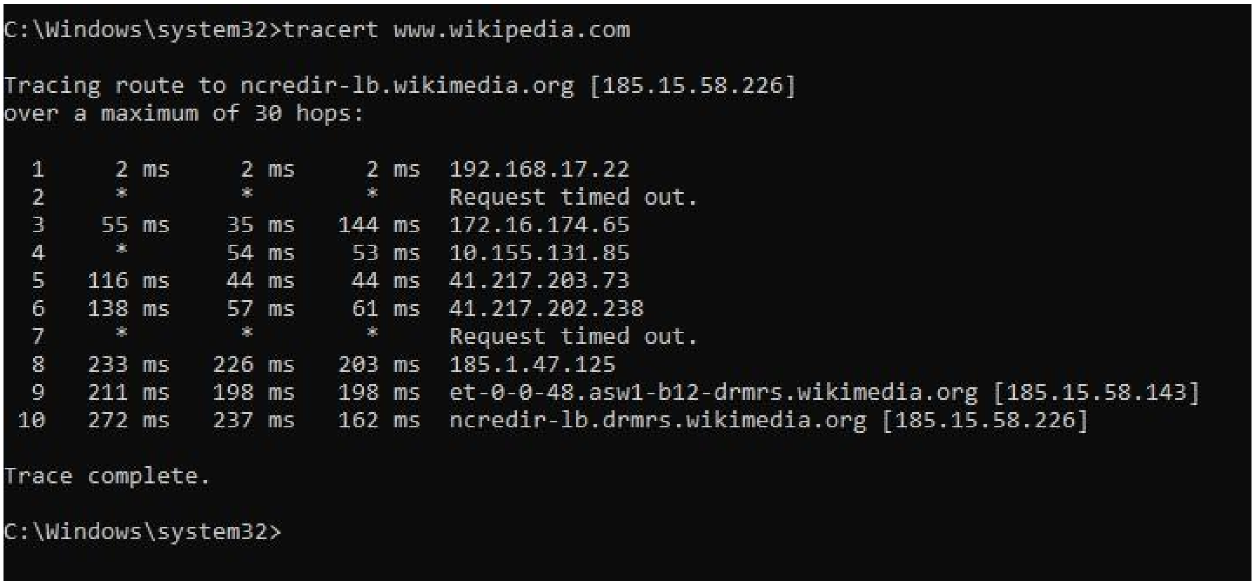
- **tracert www.igetintopc.com**



```
C:\Windows\system32>tracert www.igetintopc.com

Tracing route to www.igetintopc.com [104.21.21.246]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  192.168.17.22
  2     *        *        *     Request timed out.
  3    68 ms   114 ms    51 ms  172.16.174.65
  4     *       78 ms    54 ms  10.155.131.85
  5   167 ms    38 ms    52 ms  41.217.203.73
  6   139 ms    35 ms    48 ms  41.217.202.238
  7     *        *        *     Request timed out.
  8   118 ms   118 ms   166 ms  105.255.5.54
  9   144 ms   209 ms   107 ms  104.21.21.246

Trace complete.

C:\Windows\system32>
```

The command "tracert www.igetintopc.com" is used to track the network path from your computer to the destination website. It works by sending a series of ICMP (Internet Control Message Protocol) echo request packets with varying time-to-live (TTL) values. Each router along the path decrements the TTL value, and when it reaches zero, the router sends an ICMP time exceeded message back to your computer. This allows you to see the IP addresses of the intermediate routers and measure the latency or response time at each hop.

- **tracert www.wikipedia.com**

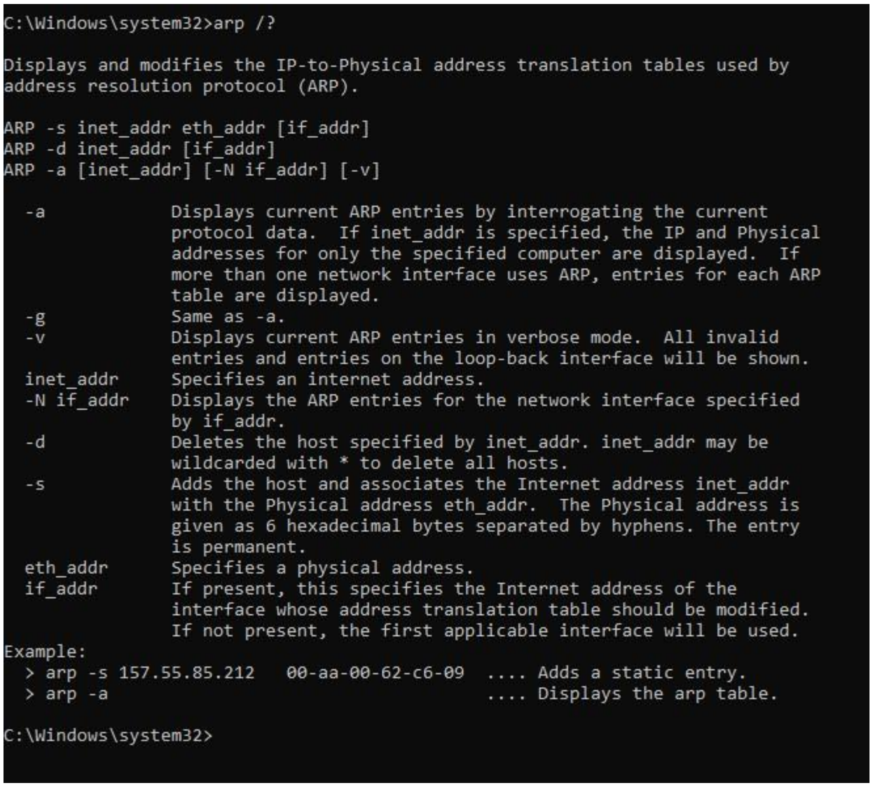


```
C:\Windows\system32>tracert www.wikipedia.com

Tracing route to ncredir-lb.wikimedia.org [185.15.58.226]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.17.22
  2     *        *        *     Request timed out.
  3    55 ms    35 ms   144 ms  172.16.174.65
  4     *       54 ms    53 ms  10.155.131.85
  5   116 ms    44 ms    44 ms  41.217.203.73
  6   138 ms    57 ms    61 ms  41.217.202.238
  7     *        *        *     Request timed out.
  8   233 ms   226 ms   203 ms  185.1.47.125
  9   211 ms   198 ms   198 ms  et-0-0-48.asw1-b12-drmrs.wikimedia.org [185.15.58.143]
 10   272 ms   237 ms   162 ms  ncredir-lb.drmrs.wikimedia.org [185.15.58.226]

Trace complete.

C:\Windows\system32>
```

The command "trace www.wikipedia.com" is used to track the network path from your computer to the destination website. It works by sending a series of ICMP (Internet Control Message Protocol) echo request packets with varying time-to-live (TTL) values. Each router along the path decrements the TTL value, and when it reaches zero, the router sends an ICMP time exceeded message back to your computer. This allows you to see the IP addresses of the intermediate routers and measure the latency or response time at each hop.

8.Issue the command arp /? capture the screen and briefly explain what it does.

- **arp /?**



```
C:\Windows\system32>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:\Windows\system32>
```

The command "arp /?" is used to display the help documentation and available options for the "arp" (Address Resolution Protocol) command. Here's a breakdown of the command and its function:

"arp": This is the command itself, which is typically available on most operating systems.

"/?": This is an argument passed to the command that requests the display of the command's help documentation.

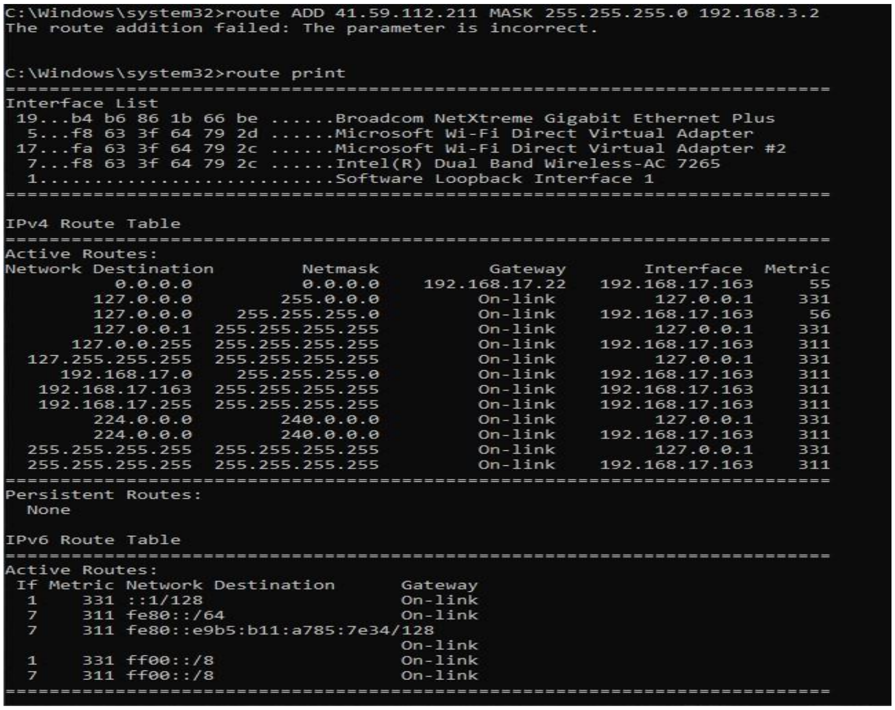
By executing "arp /?", you can view the usage information, command syntax, and available options specific to the "arp" command. The help documentation will typically provide details on how to use the command to manage and view the ARP cache, which is a table that maps IP addresses to their corresponding MAC (Media Access Control) addresses on a local network.

The "arp" command is commonly used for troubleshooting network connectivity issues, checking ARP cache entries, and manually manipulating ARP tables. It allows you to view, add, modify, or delete ARP cache entries, which can help in resolving network communication problems or verifying the accuracy of IP-to-MAC address mappings.

The specific functionality and options available with the "arp" command may vary depending on the operating system or platform you are using. Therefore, it's recommended to execute "arp /?" on your specific system to obtain the precise help documentation for the command.

9. Issue the command route add a static route 41.59.112.211 MASK 255.255.255.0

192.168.3.2 to your PC routing table.



```
C:\Windows\system32>route ADD 41.59.112.211 MASK 255.255.255.0 192.168.3.2
The route addition failed: The parameter is incorrect.


C:\Windows\system32>route print
===========================================================================
Interface List
 19...b4 b6 86 1b 66 be ......Broadcom NetXtreme Gigabit Ethernet Plus
  5...f8 63 3f 64 79 2d ......Microsoft Wi-Fi Direct Virtual Adapter
 17...fa 63 3f 64 79 2c ......Microsoft Wi-Fi Direct Virtual Adapter #2
  7...f8 63 3f 64 79 2c ......Intel(R) Dual Band Wireless-AC 7265
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.17.22   192.168.17.163     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.0    255.255.255.0         On-link    192.168.17.163     56
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
      127.0.0.255  255.255.255.255         On-link    192.168.17.163    311
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.17.0    255.255.255.0         On-link    192.168.17.163    311
   192.168.17.163  255.255.255.255         On-link    192.168.17.163    311
   192.168.17.255  255.255.255.255         On-link    192.168.17.163    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.17.163    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.17.163    311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  7    311 fe80::/64                On-link
  7    311 fe80::e9b5:b11:a785:7e34/128
                                    On-link
  1    331 ff00::/8                 On-link
  7    311 ff00::/8                 On-link
===========================================================================
```

The command "route add 41.59.112.211 MASK 255.255.255.0 192.168.3.2" is used to add a static route to the routing table of a computer or networking device. Let's break down the command and understand its components:

"route": This is the command used to manage or modify routes in the routing table.

"add": This option specifies that you want to add a new route to the routing table.

"41.59.112.211": This is the destination IP address or network for which you want to create the static route.

"MASK 255.255.255.0": This indicates the subnet mask associated with the destination network. In this case, it's a subnet mask of 255.255.255.0, which corresponds to a network with a 24-bit prefix.

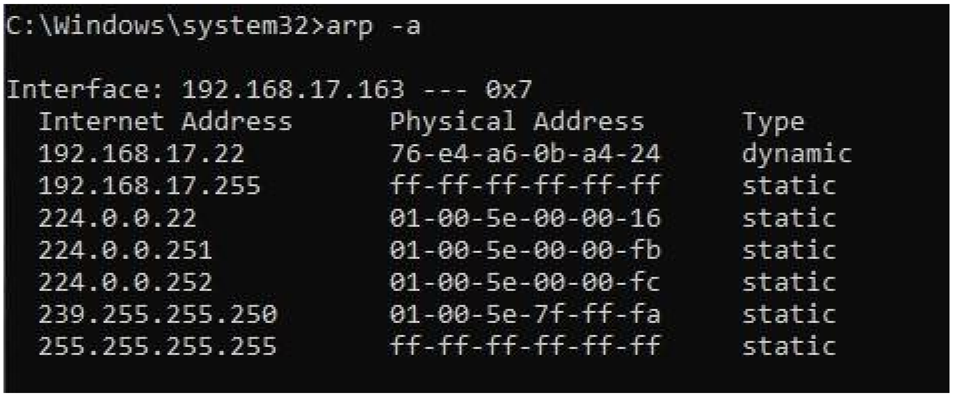
"192.168.3.2": This is the gateway or next hop IP address. It specifies the IP address of the device to which the traffic should be sent for forwarding toward the destination network.

When you execute this command, you are instructing your computer or networking device to add a static route to its routing table. The static route will match any traffic destined for the IP address 41.59.112.211 with a subnet mask of 255.255.255.0. Instead of using the default routing behavior, the device will forward the traffic to the specified gateway IP address, 192.168.3.2, which will be responsible for further routing the traffic towards the destination network.

Adding static routes can be useful in situations where you need to explicitly define the routing path for specific networks or subnets, bypassing the default routing behavior. It allows you to have more control over the network traffic flow and direct it through specific gateways

9.Issue at least three subcommands in arp, capture each screen and briefly explain what each does.

- **arp -a**



```
C:\Windows\system32>arp -a

Interface: 192.168.17.163 --- 0x7
  Internet Address      Physical Address      Type
  192.168.17.22         76-e4-a6-0b-a4-24     dynamic
  192.168.17.255        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
```

The command "arp -a" is used to display the current ARP (Address Resolution Protocol) cache on a computer or networking device. Here's what the command does:

"arp": This is the command itself, which is commonly available on most operating systems.

"-a": This option is used to display the ARP cache.

When you execute the "arp -a" command, your computer will retrieve and display the ARP cache entries that it has cached. The ARP cache is a table that maps IP addresses to their corresponding MAC (Media Access Control) addresses on a local network.

The output of the "arp -a" command typically includes the following information for each entry in the ARP cache:

IP address: The IP address for which the MAC address is resolved.

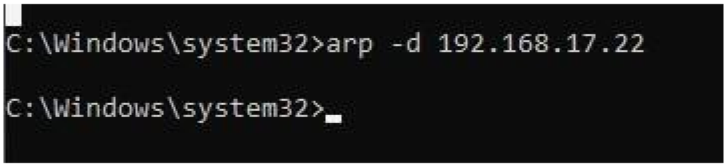
Physical address: The corresponding MAC address for the IP address.

Type: The type of network interface associated with the IP address (e.g., dynamic or static).

Interface: The network interface through which the IP address is reachable.

By inspecting the ARP cache, you can see the mapping between IP addresses and MAC addresses that your computer has learned through ARP requests and responses. This information is essential for devices to communicate on a local network, as it allows them to correctly address data packets and determine the MAC address of the destination device

- **arp -d 192.168.17.22 :**



```
C:\Windows\system32>arp -d 192.168.17.22

C:\Windows\system32>_
```

The command "arp -d 192.168.17.22" is used to delete a specific entry from the ARP cache on a computer or networking device. Here's a breakdown of the command:

"arp": This is the command itself, which is commonly available on most operating systems.

"-d": This option is used to delete an entry from the ARP cache.

"192.168.17.22": This is the IP address for which you want to delete the corresponding entry from the ARP cache.

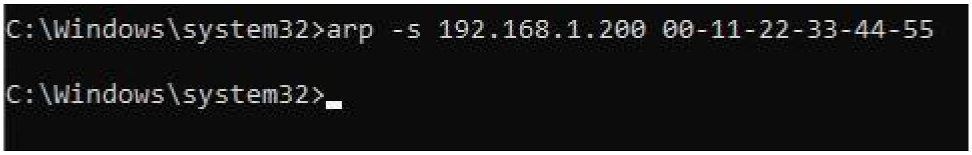
When you execute the "arp -d 192.168.17.22" command, your computer will remove the entry that maps the specified IP address (192.168.17.22) to its corresponding MAC address from the ARP cache.

This can be useful in situations where you need to refresh or update the ARP cache or if you encounter issues with incorrect or outdated ARP entries. By deleting a specific entry, you force your computer to perform a new ARP resolution for that IP address when necessary.

Please note that administrative privileges may be required to delete entries from the ARP cache, depending on the operating system you are using.

.

- **arp -s 192.168.1.200 00-11-22-33-44-55**



```
C:\Windows\system32>arp -s 192.168.1.200 00-11-22-33-44-55

C:\Windows\system32>_
```

The command "arp -s 192.168.1.200 00-11-22-33-44-55" is used to manually add an entry to the ARP cache on a computer or networking device. Here's a breakdown of the command:

"arp": This is the command itself, which is commonly available on most operating systems.

"-s": This option is used to add a static entry to the ARP cache.

"192.168.1.200": This is the IP address for which you want to manually set the corresponding MAC address in the ARP cache.

"00-11-22-33-44-55": This is the MAC address you want to associate with the specified IP address.

When you execute the "arp -s 192.168.1.200 00-11-22-33-44-55" command, your computer will add a static entry to the ARP cache, specifying that the IP address 192.168.1.200 should be resolved to the MAC address 00-11-22-33-44-55. This manual entry allows your computer to directly map the IP address to the MAC address without needing to perform an ARP resolution.

Adding static entries to the ARP cache can be useful in situations where you want to ensure specific IP-to-MAC address mappings or if you want to optimize network performance by bypassing the ARP resolution process.

Please note that administrative privileges may be required to add static entries to the ARP cache, depending on the operating system you are using.