Task-6

6a). Configure and implementation of a Switch within a Network using Packet Tracer.

The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.

Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices. Different types of communication are supported here like unicast, multicast, and broadcast communication.

Modes of operation:

Mode	Purpose	Prompt	Command to enter	Command to exit
User EXEC	Allow you to connect with remote devices, perform basic tests, temporary change terminal setting and list system information	Router >	Default mode after booting. Login with password, if configured.	Use **exit** command
Privileged EXEC	Allow you to set operating parameters. It also includes high level testing and list commands like show, copy and debug.	Router #	Use **enable** command from user exec mode	Use **exit** command
Global Configuration	Contain commands those affect the entire system	Router(config)#	Use **configure terminal** command from privileged exec mode	Use **exit** command
Interface Configuration	Contain commands those modify the operation of an interface	Router(config-if)#	Use **interface *type number*** command from global configuration mode	Use **exit** command to return in global configuration mode
Sub-Interface Configuration	Configure or modify the virtual interface created from physical interface	Router(config-subif)	Use **interface *type sub interface*** number command from global configuration mode or interface configure mode	Use **exit** to return in previous mode. Use **end** command to return in privileged exec mode.

Step 1: Open Cisco Packet Tracer

- Launch Cisco Packet Tracer on your computer.

Step 2: Create a New Project

- Click on "File" > "New" to start a new project.

Step 3: Add Devices

1. **Add a Switch:**
    - From the bottom left device list, choose the "Switch-PT" category.
    - Drag a switch (e.g., 2960) onto the workspace.

Step 4: Configure the Host name of the swicth0.

- Click on switch0 and go to Command Line Interface.
- Then change the hostname to “sh”

Command:

```
switch>
switch>en
switch#conf t

switch(config)#hostname sh
```

Step 5: Set a message of the day (MOTD) banner for the users.

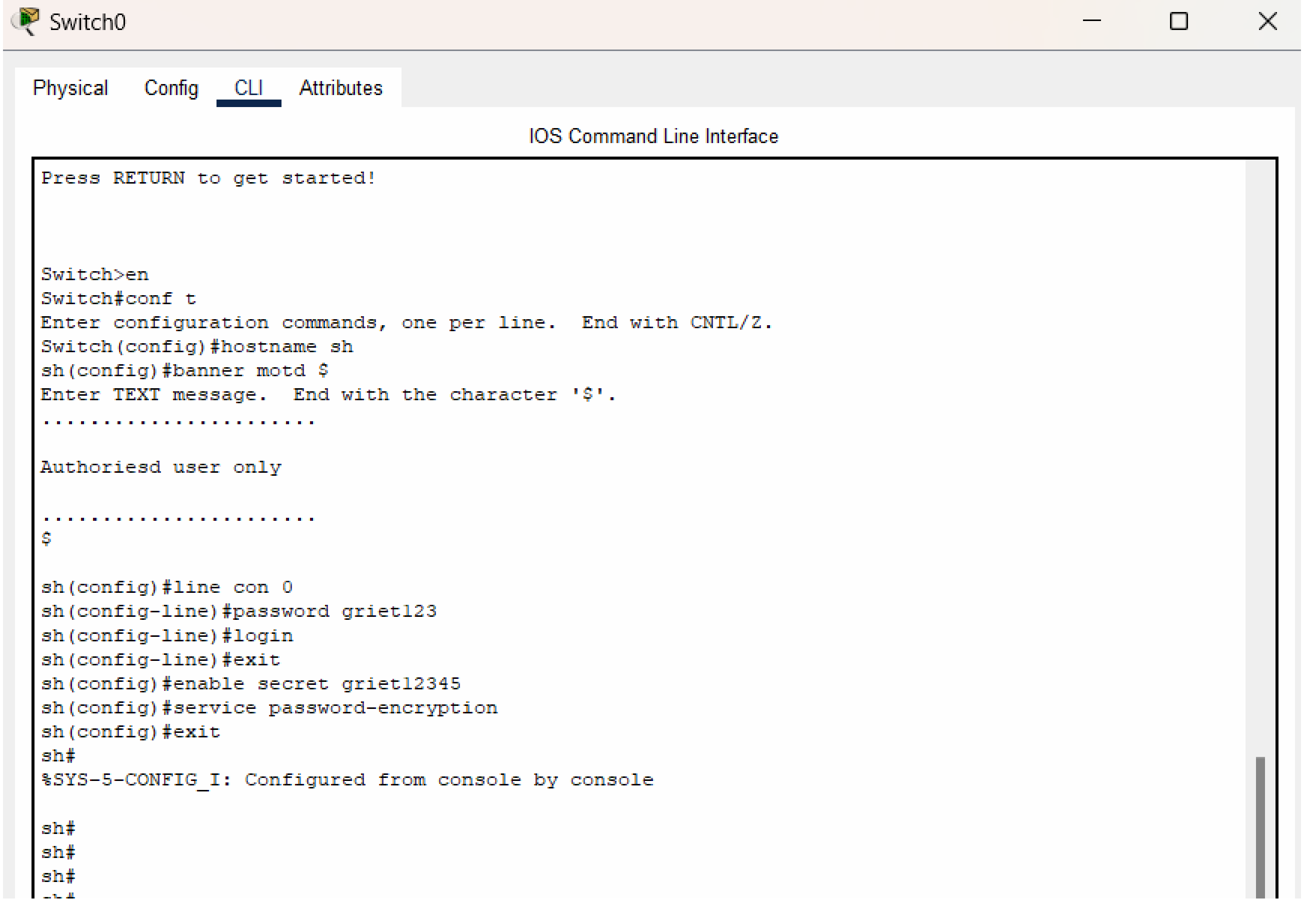
Command:

```
sh(config)#banner motd $

…………………………………………….


Authorised user only

……………………………………………

$
```

Step 6: Set up line control password and enable secret password.

To configure the Line Control password and Enable secret follow the below commands:

```
sh#conf t
sh(config)#

sh(config)#line con 0

sh(config-line)#password griet123
sh(config-line)#login
sh(config-line)#exit
sh(config)#enable secret griet12345

sh(config)#service password-encryption  // encrypts the password
sh(config)#exit
```

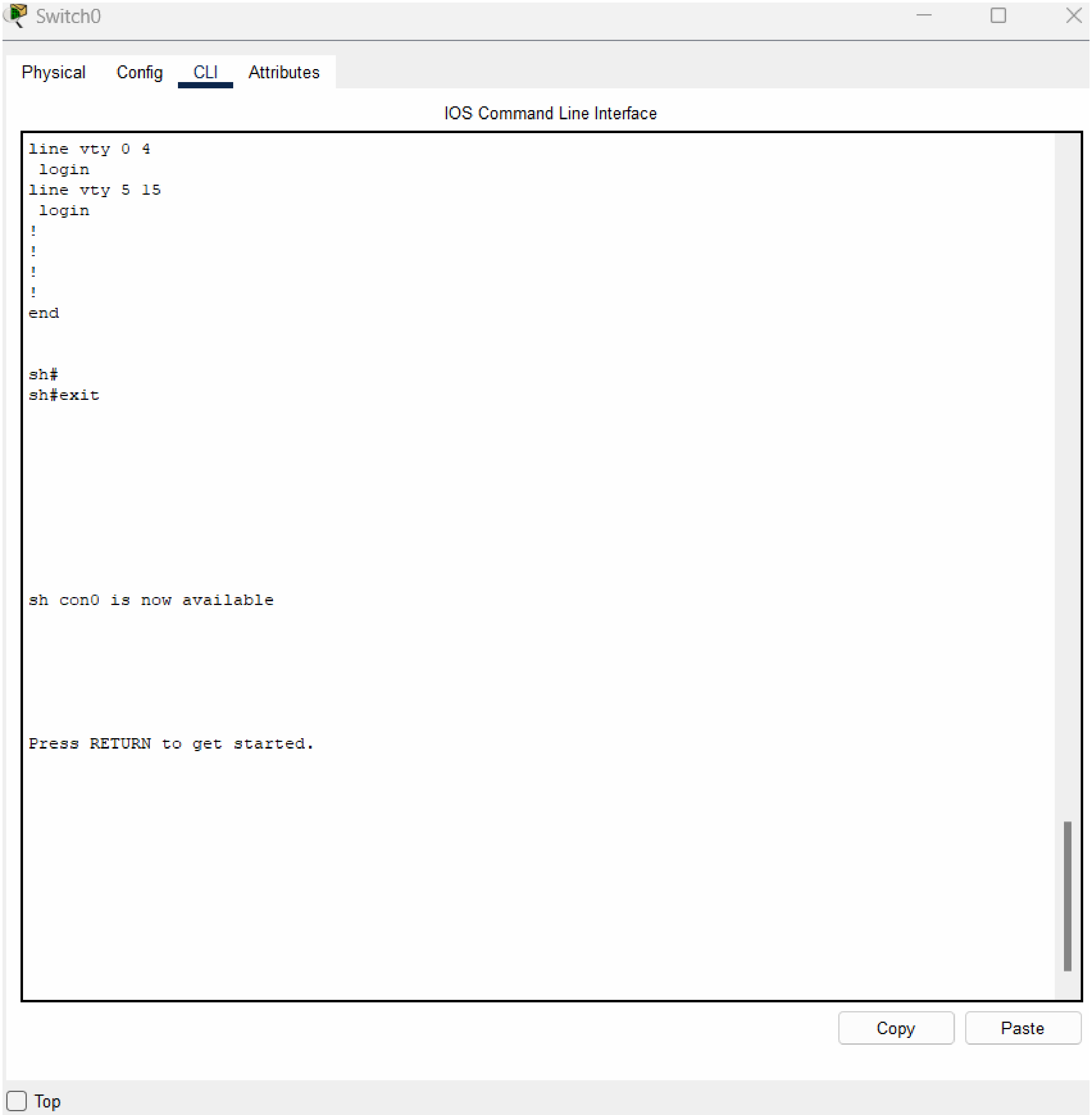


```
Press RETURN to get started!



Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sh
sh(config)#banner motd $
Enter TEXT message.  End with the character '$'.
.......................

Authoriesd user only

.......................
$

sh(config)#line con 0
sh(config-line)#password griet123
sh(config-line)#login
sh(config-line)#exit
sh(config)#enable secret griet12345
sh(config)#service password-encryption
sh(config)#exit
sh#
%SYS-5-CONFIG_I: Configured from console by console

sh#
sh#
sh#
```

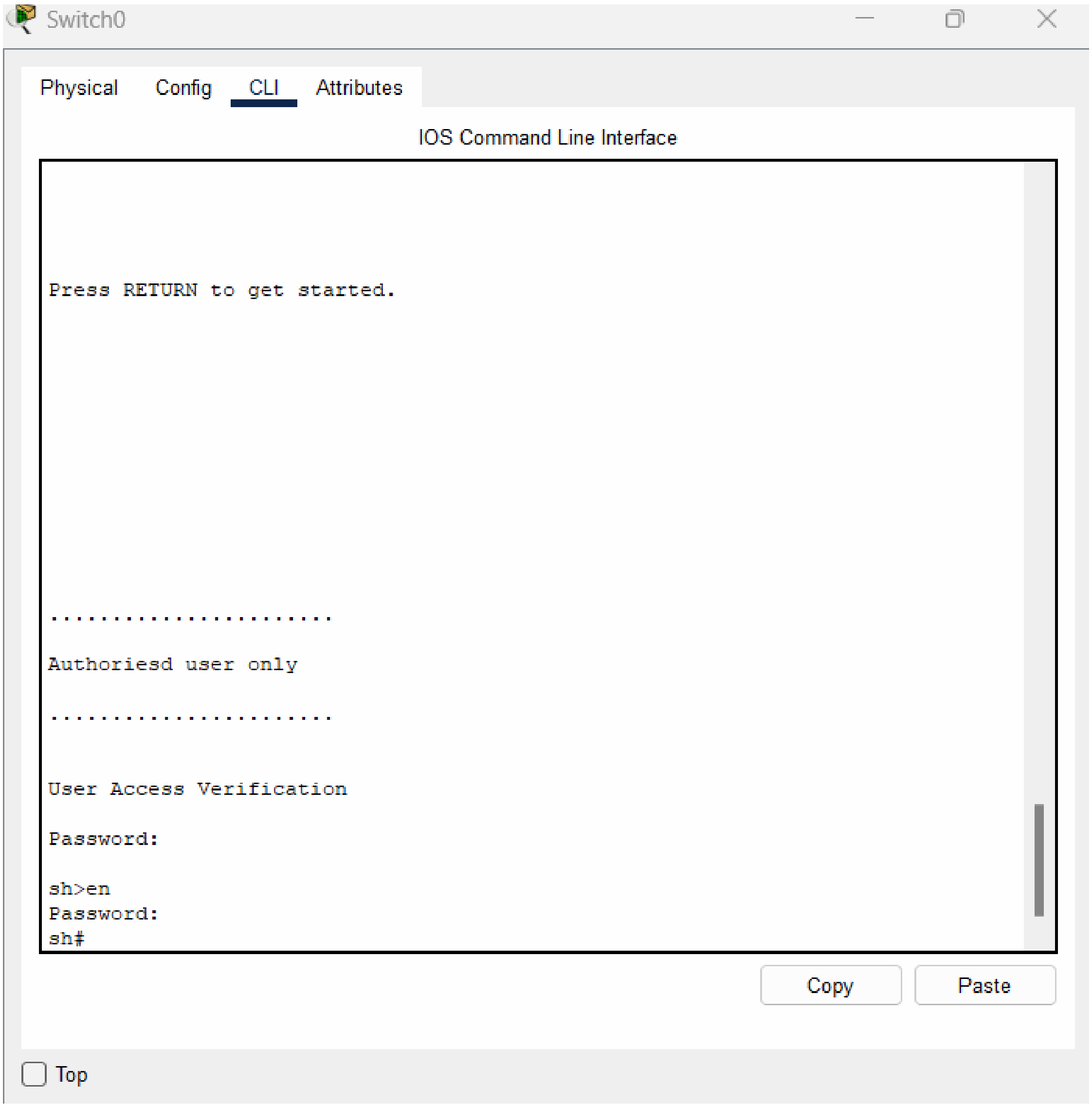
Step 7: Verify the password

- When you try to log in first, it will ask for the **line control password.**
- Then, to configure the terminal it will ask to **enable a secret password.**

Note: To verify password, need to exit from all commands and enter into user mode



```
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


sh#
sh#exit










sh con0 is now available






Press RETURN to get started.
```



```
Press RETURN to get started.






.......................

Authoriesd user only

.......................


User Access Verification

Password:

sh>en
Password:
sh#
```

To save the run configuration to startup file use the below command:

Command:

```
sh#copy run startup-config    (OR)     write
```

sh# no ip domain-lookup   // used to prevent the router from trying to resolve incorrectly pasted commands in the cli by sending out a DNS query.

Select the switch – goto cli mode and type the below configuration commands.

```
Switch>
Switch>enable
Switch#config terminal
Switch(config)#hostname sh
sh(config)#banner motd #Warning Unauthorised access is prohibited#

sh(config)#line con 0
sh(config-line)#password griet1234
sh(config-line)#login
sh(config-line)#exit

sh(config)#enable secret griet5678
sh(config)#service password-encryption

sh(config)#no ip domain-lookup

sh#copy running-config startup-config
Destination  filename  [startup-config]?
Building configuration...
[OK]


sh#show start
sh#show startup-config
Using 1238 bytes
!

version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!

hostname sh
!

enable secret 5 $1$mERr$vyUGBRk3bfoMV8qV.wJrB0
!

!

!

no ip domain-lookup
!

!

!

spanning-tree mode pvst
spanning-tree extend system-id
!
```

```
interface FastEthernet0/1
!
```

```
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5

!< deleted some part>
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^CWarning Unauthorised access is prohibited^C
!

!

!
line con 0
password 7 08265E470C0D5445415F
login
!
line vty 0 4
login
line vty 5 15
login
!
```

!

!

!

End

6B : Learn and Implement basic commands.

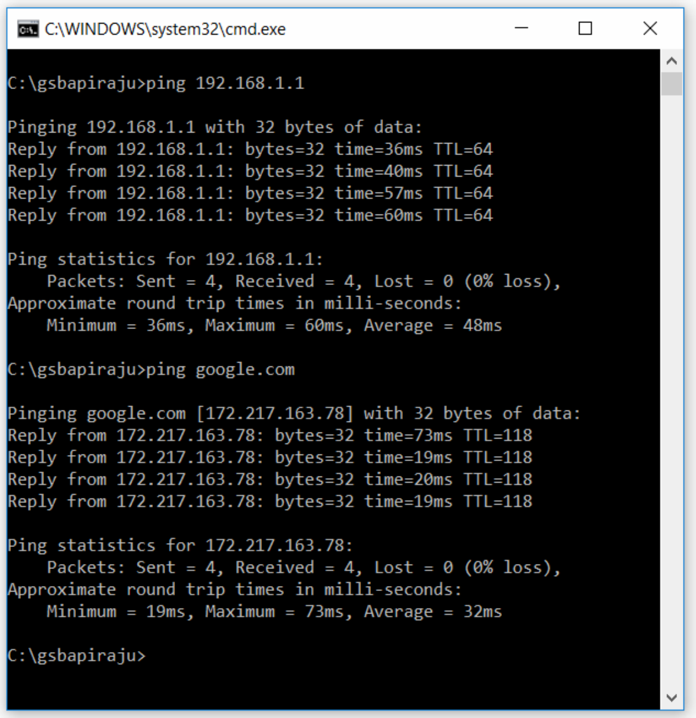
1. Ping

Ping is most commonly used network tool used to test the connection between the source and destination host.

Ping command uses Internet Control Message Protocol (ICMP) to send an echo packet from the source host to a destination host and listen to the response. If the source host receives a response from the destination host, this host is reachable. If not there is a connection error.

Using Ping command the user can identify in which area the connection problem is there, is it local or outside their LAN.

Ex: You can ping either by using the IP address or by the website name or URL. In the below example I pinged to my wireless router with its IP Address and google.com by its domain name.

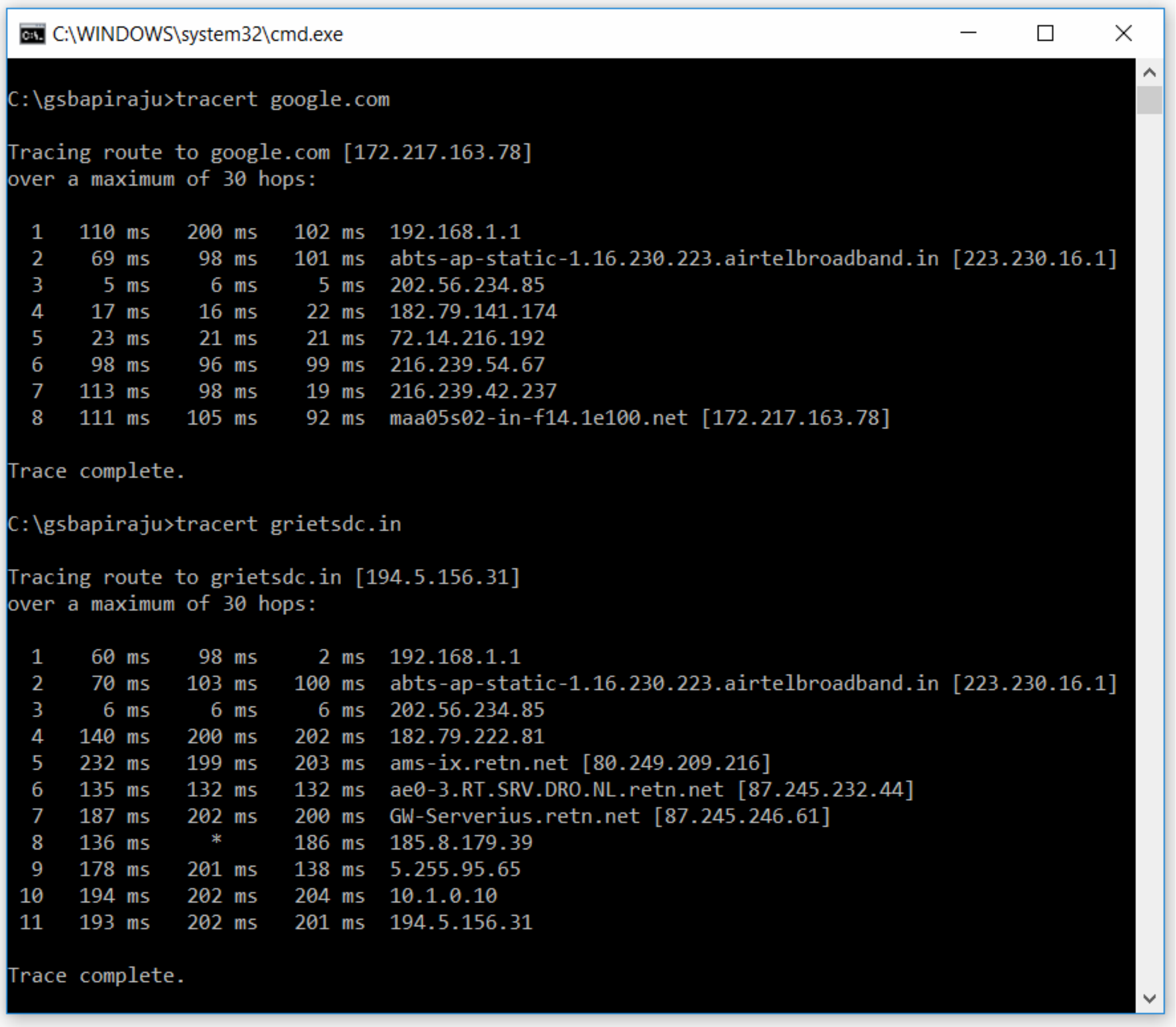


```
C:\gsbapiraju>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=36ms TTL=64
Reply from 192.168.1.1: bytes=32 time=40ms TTL=64
Reply from 192.168.1.1: bytes=32 time=57ms TTL=64
Reply from 192.168.1.1: bytes=32 time=60ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 60ms, Average = 48ms

C:\gsbapiraju>ping google.com

Pinging google.com [172.217.163.78] with 32 bytes of data:
Reply from 172.217.163.78: bytes=32 time=73ms TTL=118
Reply from 172.217.163.78: bytes=32 time=19ms TTL=118
Reply from 172.217.163.78: bytes=32 time=20ms TTL=118
Reply from 172.217.163.78: bytes=32 time=19ms TTL=118

Ping statistics for 172.217.163.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 73ms, Average = 32ms

C:\gsbapiraju>
```

2. Tracert/traceroute.

Ping is a basic tool to check the basic connectivity. But if you want to identify the complete path from the source node to the destination node than tracert/traceroute utility is very useful.

The tracert utility for windows and traceroute utility for Linux gives you the entire path, including the number of hops packet travelled.

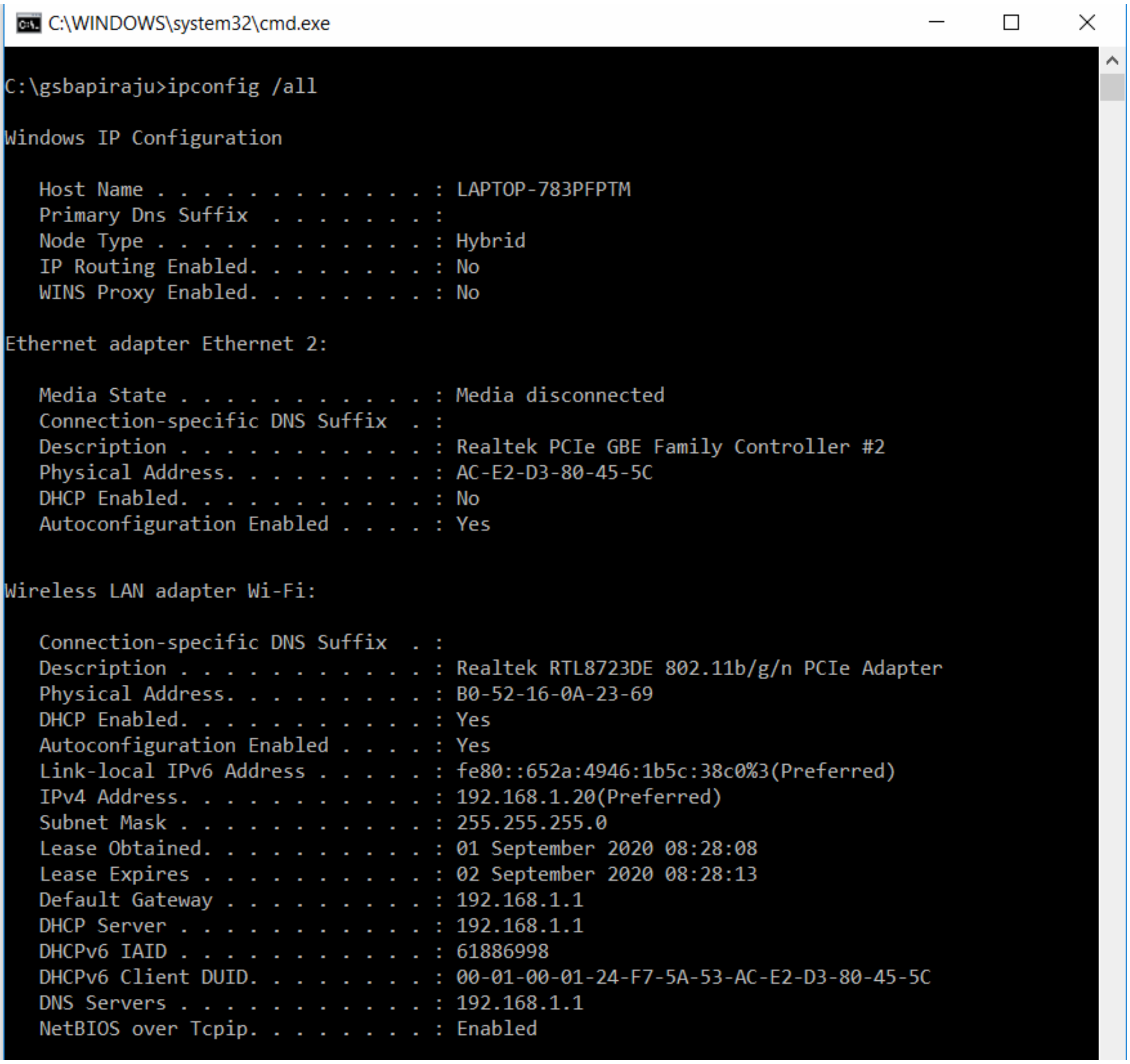


```
C:\gsbapiraju>tracert google.com

Tracing route to google.com [172.217.163.78]
over a maximum of 30 hops:

  1   110 ms   200 ms   102 ms  192.168.1.1
  2    69 ms    98 ms   101 ms  abts-ap-static-1.16.230.223.airtelbroadband.in [223.230.16.1]
  3     5 ms     6 ms     5 ms  202.56.234.85
  4    17 ms    16 ms    22 ms  182.79.141.174
  5    23 ms    21 ms    21 ms  72.14.216.192
  6    98 ms    96 ms    99 ms  216.239.54.67
  7   113 ms    98 ms    19 ms  216.239.42.237
  8   111 ms   105 ms    92 ms  maa05s02-in-f14.1e100.net [172.217.163.78]

Trace complete.

C:\gsbapiraju>tracert grietsdc.in

Tracing route to grietsdc.in [194.5.156.31]
over a maximum of 30 hops:

  1    60 ms    98 ms     2 ms  192.168.1.1
  2    70 ms   103 ms   100 ms  abts-ap-static-1.16.230.223.airtelbroadband.in [223.230.16.1]
  3     6 ms     6 ms     6 ms  202.56.234.85
  4   140 ms   200 ms   202 ms  182.79.222.81
  5   232 ms   199 ms   203 ms  ams-ix.retn.net [80.249.209.216]
  6   135 ms   132 ms   132 ms  ae0-3.RT.SRV.DRO.NL.retn.net [87.245.232.44]
  7   187 ms   202 ms   200 ms  GW-Serverius.retn.net [87.245.246.61]
  8   136 ms     *      186 ms  185.8.179.39
  9   178 ms   201 ms   138 ms  5.255.95.65
 10   194 ms   202 ms   204 ms  10.1.0.10
 11   193 ms   202 ms   201 ms  194.5.156.31

Trace complete.
```

3. Ipconfig

Ipconfig is one of the most important tool for system admins for troubleshooting networking issue. It is a command-line tool that shows the current TCP/IP configuration of the installed networking stack of a computer connected to a network.

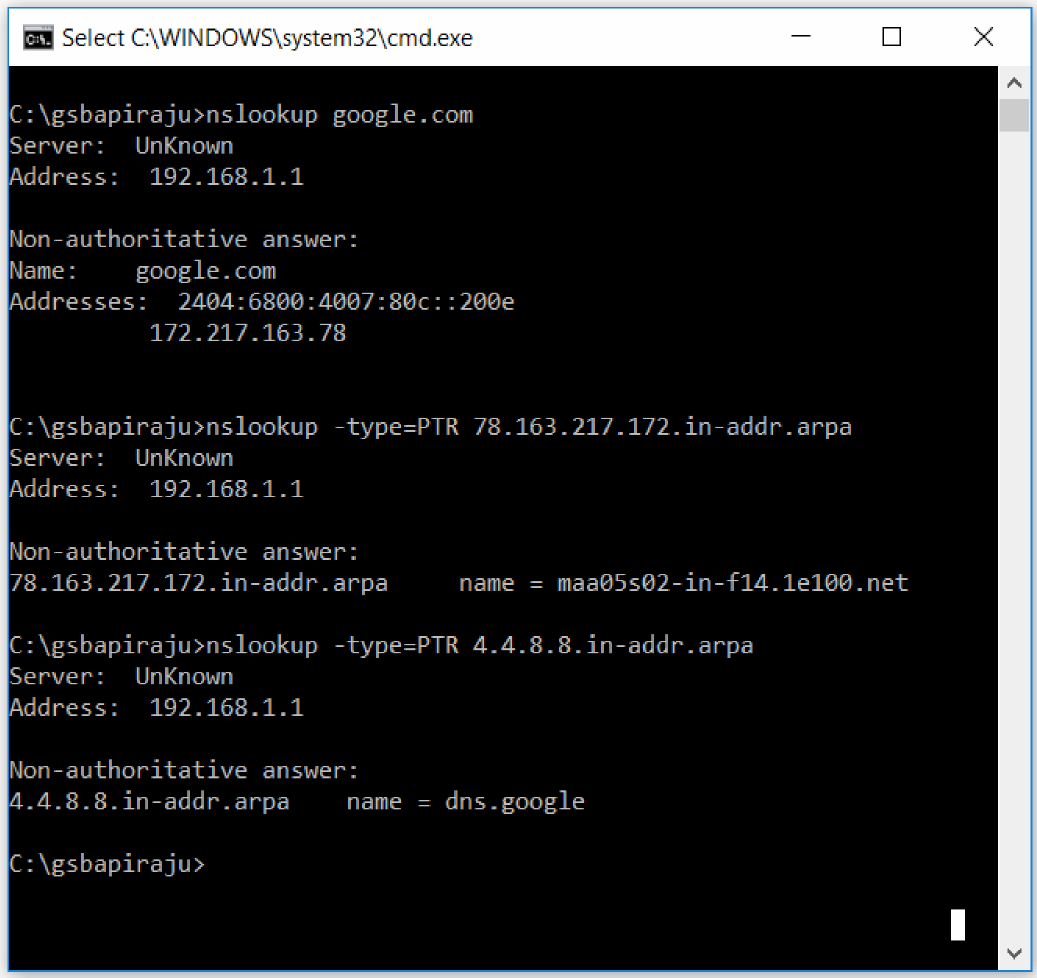
This tool includes a number of switches to perform different actions. In the below example I am using /all which Produces a detailed configuration report for all interfaces. You can observe the 48 bit MAC address, IPaddress, DHCP details etc.



```
C:\gsbapiraju>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-783PFPTM
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller #2
   Physical Address. . . . . . . . . : AC-E2-D3-80-45-5C
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes


Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8723DE 802.11b/g/n PCIe Adapter
   Physical Address. . . . . . . . . : B0-52-16-0A-23-69
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::652a:4946:1b5c:38c0%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 01 September 2020 08:28:08
   Lease Expires . . . . . . . . . . : 02 September 2020 08:28:13
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 61886998
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F7-5A-53-AC-E2-D3-80-45-5C
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

4. Nslookup

Some of the most common networking issues revolve around issues with Dynamic Name System (DNS) address resolution issues. nslookup or "name server lookup" is a network administration command-line tool used for querying the Domain Name System to obtain domain name or IP address mapping, or other DNS records. This utility can be used to lookup the specific IP address(es) associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue.

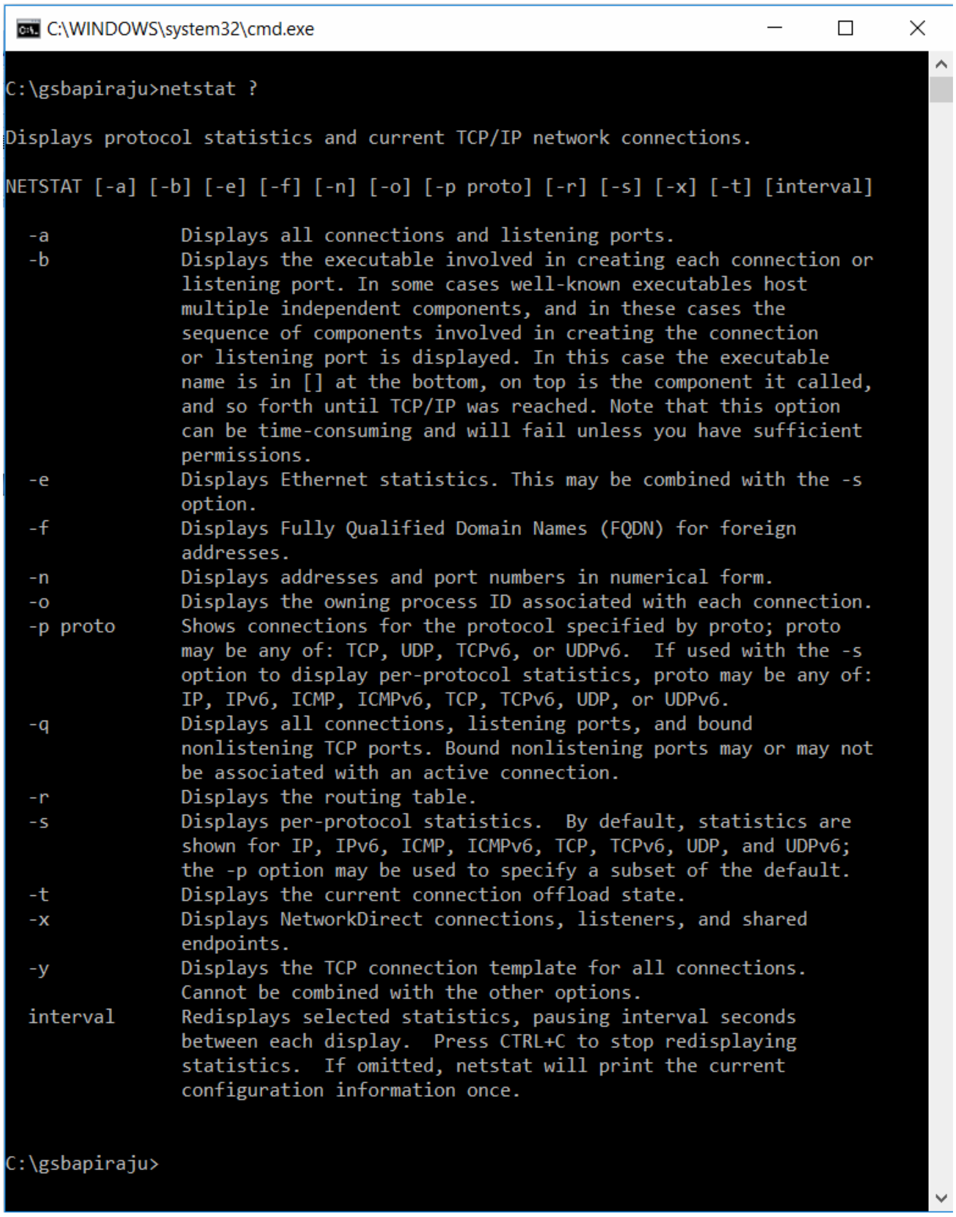


```
C:\gsbapiraju>nslookup google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:80c::200e
          172.217.163.78


C:\gsbapiraju>nslookup -type=PTR 78.163.217.172.in-addr.arpa
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
78.163.217.172.in-addr.arpa     name = maa05s02-in-f14.1e100.net

C:\gsbapiraju>nslookup -type=PTR 4.4.8.8.in-addr.arpa
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
4.4.8.8.in-addr.arpa    name = dns.google

C:\gsbapiraju>
```

A typical DNS lookup is used to determine which IP address is associated with a hostname. A reverse DNS lookup is used for the opposite, to determine which hostname is associated with an IP address. Sometimes reverse DNS lookups are required for diagnostic purposes.

5. Netstat.

Netstat (*network statistics)* is a program that's controlled via commands issued in the command line. It delivers basic statistics on all network activities and informs users on which **ports and addresses** the corresponding connections (TCP, UDP) are running and which ports are open for tasks. The below example illustrates various switches of netstat.



```
C:\gsbapiraju>netstat ?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.


C:\gsbapiraju>
```