Lab File

Exploring the Networks

(IT 307)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Submitted to:

Dr A. Shankar

Ast. Professor

CSE Department, ASET

Submitted by:

Shaina Mehta

A2305219268

B.tech. C.S.E.

5CSE-4Y

AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY

AMITY UNIVERSITY UTTAR PRADESH

NOIDA -201301

Exp No	Assignment Category	Code	Name of Experiment	Date of Allotment	Date of Evaluation	Max Marks	Marks Obtained	Faculty Sign
1	Mandatory Experiment		To explore the basic networking commands.	20-07-2021	03-08-2021			
2			To design and simulate client to server and peer to peer network.	03-08-2021	10-08-2021			
3			To allocate the static IP Addresses to the devices and check the connectivity of the end devices using the ping command.	10-08-2021	17-08-2021			
4			To configure the switch in a network and add banner message to it.	17-08-2021	24-08-2021			
5			To set the password for the switch network and check its authentication using telnet command.	24-08-2021	31-08-2021			
6			To secure the USER and EXEC mode and VTY lines of a switch and check its authentication using telnet command.	31-08-2021	07-09-2021			
7			To perform automatic configuration of the IP address of the end devices using DHCP protocol and assigning IP address of Default Gateway and DNS Server.	07-09-2021	23-09-2021			
8			To simulate the ARP protocol in the CISCO Packet Tracer..	23-09-2021	07-10-2021			
9			To explore about the commands related to router and perform router	7-10-2021	21-10-2021			

			configuration in CISCO Packet Tracer.					
10			To explore about wireshark.	21-10-2021	28-10-2021			
11			To capture and analyse TCP and UDP packets in Wireshark.	28-10-2021	11-11-2021			
12			To capture and analyse DNS query and ICMP packets in Wireshark.	28-10-2021	11-11-2021			
	Viva	Viva						

Experiment 1

Date: 20-07-2021

Aim: To explore the basic networking commands.

Software Used: Command Prompt.

Theory:

1. **tracert:** tracert command determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.
   This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it.
   Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer. Tracert determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the -h parameter.
   The path is determined by examining the ICMP Time Exceeded messages returned by intermediate routers and the Echo Reply message returned by the destination. However, some routers do not return Time Exceeded messages for packets with expired TTL values and are invisible to the tracert command. In this case, a row of asterisks (*) is displayed for that hop.
   Syntax: tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]
   Parameters:
   - **-d:** Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results.
   - **-h:** MaximumHops Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.
   - **-j:** HostList Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in HostList. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The HostList is a series of IP addresses (in dotted decimal notation) separated by spaces.
   - **-w:** Timeout Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

```
C:\Users\hp>tracert www.google.co.in

Tracing route to www.google.co.in [2404:6800:4002:808::2003]
over a maximum of 30 hops:

  1   407 ms     5 ms     2 ms  2405:201:4013:81dc:3249:50ff:fe2f:8046
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4    11 ms     7 ms     7 ms  2001:4860:1:1::1ef4
  5     9 ms    12 ms    22 ms  2404:6800:812f::1
  6     *        *        7 ms  2001:4860:0:1::539c
  7     *        6 ms     *     2001:4860:0:1::1e5
  8     6 ms     7 ms     6 ms  del03s13-in-x03.1e100.net [2404:6800:4002:808::2003]

Trace complete.
```

```
C:\Users\hp>tracert -d www.google.com

Tracing route to www.google.com [2404:6800:4002:809::2004]
over a maximum of 30 hops:

  1   159 ms    13 ms     3 ms  2405:201:4013:81dc:3249:50ff:fe2f:8046
  2     *        *        *     Request timed out.
  3    24 ms     *       10 ms  ::ffff:172.16.18.33
  4     9 ms     8 ms     8 ms  2001:4860:1:1::1ef4
  5     6 ms     8 ms     8 ms  2404:6800:8120::1
  6     8 ms    14 ms    21 ms  2001:4860:0:1::54f6
  7     7 ms     *        *     2001:4860:0:1a::5
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    11 ms    12 ms    13 ms  2404:6800:4002:809::2004

Trace complete.
```

```
C:\Users\hp>tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 www.google.com

Tracing route to www.google.com [142.250.192.164]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

2. **ping:** ping command verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.
   Or
   The ping command lets you verify that you have network connectivity with another network device. It is commonly used to help troubleshoot networking issues. To use ping, provide the IP address or machine name of the other device.
   You can use ping to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might

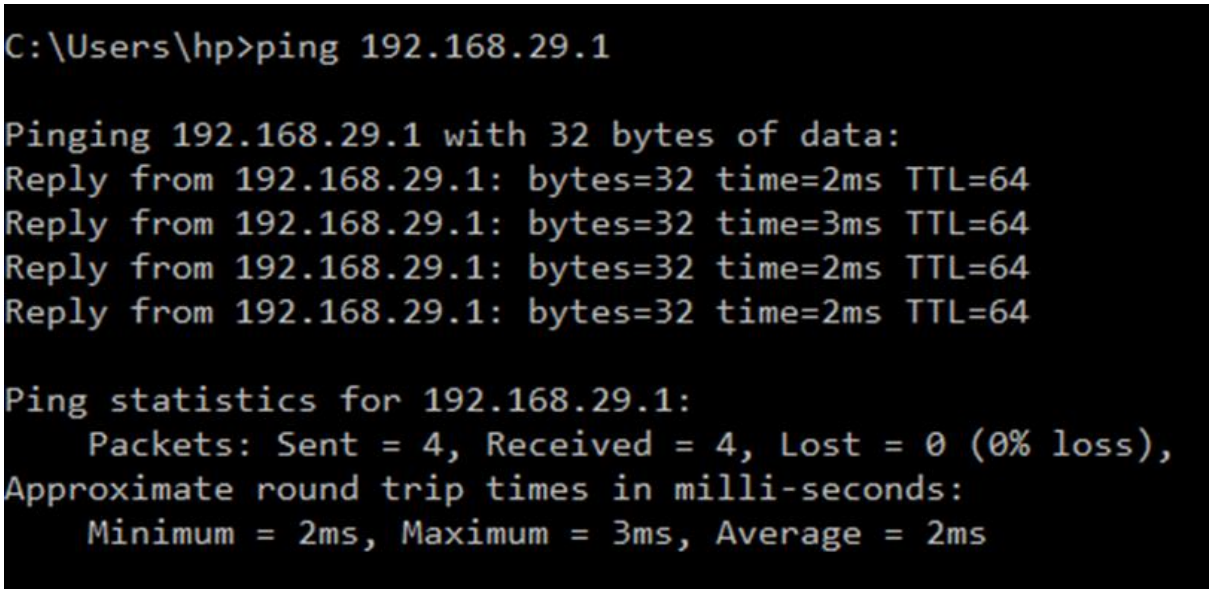
have a name resolution problem. In this case, ensure that the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.

To test a TCP/IP configuration by using the ping command:

- To quickly obtain the TCP/IP configuration of a computer, open Command Prompt, and then type **ipconfig**. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
- At the command prompt, ping the loopback address by typing ping **127.0.0.1**.
- Ping the IP address of the computer.
- Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
- Ping the IP address of a remote host (a host that is on a different subnet). If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
- Ping the IP address of the DNS server. If the ping command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

Syntax: ping

```
C:\Users\hp>ping codingninjas.com

Pinging codingninjas.com [54.192.155.19] with 32 bytes of data:
Reply from 54.192.155.19: bytes=32 time=383ms TTL=239
Reply from 54.192.155.19: bytes=32 time=10ms TTL=239
Reply from 54.192.155.19: bytes=32 time=8ms TTL=239
Reply from 54.192.155.19: bytes=32 time=16ms TTL=239

Ping statistics for 54.192.155.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 383ms, Average = 104ms
```



3. **arp:** arp command displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer.
   Syntax: arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]
   Parameters:
   - **Used without parameters:** displays help
   - **-a [InetAddr] [-N IfaceAddr]:** Displays current ARP cache tables for all interfaces. To display the ARP cache entry for a specific IP address, use arp -a with the InetAddr parameter, where InetAddr is an IP address. To display the ARP cache table for a specific interface, use the -N IfaceAddr parameter where IfaceAddr is the IP address assigned to the interface. The -N parameter is case-sensitive.
   - **-g [InetAddr] [-N IfaceAddr]:** Identical to -a.
   - **-d InetAddr [IfaceAddr]:** Deletes an entry with a specific IP address, where InetAddr is the IP address. To delete an entry in a table for a specific interface, use the IfaceAddr parameter where IfaceAddr is the IP address assigned to the interface. To delete all entries, use the asterisk (*) wildcard character in place of InetAddr.
   - **-s InetAddr EtherAddr [IfaceAddr]:** Adds a static entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. To add a static ARP cache entry to the table for a specific interface, use the IfaceAddr parameter where IfaceAddr is an IP address assigned to the interface.

```
C:\Users\hp>arp -a

Interface: 192.168.29.226 --- 0xa
  Internet Address      Physical Address      Type
  192.168.29.1          30-49-50-2f-80-46     dynamic
  192.168.29.6          68-db-f5-c1-b6-e1     dynamic
  192.168.29.190        28-24-ff-60-10-13     dynamic
  192.168.29.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

```
C:\Users\hp> arp -a -N 192.168.29.226

Interface: 192.168.29.226 --- 0xa
  Internet Address      Physical Address      Type
  192.168.29.1          30-49-50-2f-80-46     dynamic
  192.168.29.6          68-db-f5-c1-b6-e1     dynamic
  192.168.29.190        28-24-ff-60-10-13     dynamic
  192.168.29.255        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
```

4. **netstat:** netstat command displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

   Netstat provides statistics for the following:

   - **Proto:** The name of the protocol (TCP or UDP).
   - **Local Address:** The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
   - **Foreign Address:** The IP address and port number of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

   (state) Indicates the state of a TCP connection. The possible states are as follows:

   - CLOSE_WAIT
   - CLOSED
   - ESTABLISHED

- FIN_WAIT_1
- FIN_WAIT_2
- LAST_ACK
- LISTEN
- SYN_RECEIVED
- SYN_SEND
- TIMED_WAIT

Syntax: netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

Parameters:

- **Used without parameters:** displays active TCP connections.
- **-a:** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n:** Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p:** Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- **-s:** Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.
- **Interval:** Redisplays the selected information every Interval seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, netstat prints the selected information only once.
- **/?:** Displays help at the command prompt.

```
C:\Users\hp>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:52124        DESKTOP-BQK27U3:52125  ESTABLISHED
  TCP    127.0.0.1:52125        DESKTOP-BQK27U3:52124  ESTABLISHED
  TCP    127.0.0.1:59994        DESKTOP-BQK27U3:65376  ESTABLISHED
  TCP    127.0.0.1:60045        DESKTOP-BQK27U3:60046  ESTABLISHED
  TCP    127.0.0.1:60046        DESKTOP-BQK27U3:60045  ESTABLISHED
  TCP    127.0.0.1:65376        DESKTOP-BQK27U3:59994  ESTABLISHED
  TCP    192.168.29.226:49505   104.208.16.0:https     ESTABLISHED
  TCP    192.168.29.226:49506   ec2-50-112-53-100:https  TIME_WAIT
  TCP    192.168.29.226:49507   ec2-50-112-44-181:https  TIME_WAIT
  TCP    192.168.29.226:50852   52.114.14.217:https    ESTABLISHED
  TCP    192.168.29.226:52128   ec2-54-186-175-197:https  CLOSE_WAIT
  TCP    192.168.29.226:52136   server-54-192-166-140:https  ESTABLISHED
  TCP    192.168.29.226:52137   161.69.226.29:https    TIME_WAIT
  TCP    192.168.29.226:52146   104.208.16.0:https     TIME_WAIT
  TCP    192.168.29.226:52231   156:https              ESTABLISHED
  TCP    192.168.29.226:54704   20.198.162.78:https    ESTABLISHED
  TCP    192.168.29.226:56461   52.114.44.75:https     ESTABLISHED
  TCP    192.168.29.226:58070   server-54-192-166-206:https  ESTABLISHED
  TCP    192.168.29.226:59449   52.114.16.141:https    ESTABLISHED
  TCP    192.168.29.226:61100   215:https              TIME_WAIT
  TCP    192.168.29.226:62895   ec2-3-112-115-143:https  ESTABLISHED
  TCP    192.168.29.226:63998   20.198.162.76:https    ESTABLISHED
  TCP    192.168.29.226:64573   ec2-54-225-152-45:https  ESTABLISHED
  TCP    192.168.29.226:65342   52.114.20.18:https     TIME_WAIT
  TCP    192.168.29.226:65344   52.109.124.51:https    TIME_WAIT
  TCP    192.168.29.226:65345   52.109.124.51:https    TIME_WAIT
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:49503  del03s10-in-x0e:https  TIME_WAIT
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:50483  del03s06-in-x03:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:52133  [2603:1046:500:e::2]:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:52138  [2606:2800:147:120f:30c:1ba0:fc6:265a]:https  CLOSE_WAIT
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:55628  [2404:6800:4003:c11::bc]:5228  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:56459  del11s07-in-x0e:http   ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:57042  [2603:1046:c04:818::2]:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:57043  [2603:1046:c04:818::2]:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:58370  del03s09-in-x03:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:58527  del12s07-in-x0e:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:59386  [2620:1ec:42::132]:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:59440  del12s02-in-x03:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:59749  del11s12-in-x0a:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:61216  del03s10-in-x0e:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:61439  del12s02-in-x0a:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:61604  del11s13-in-x0e:https  CLOSE_WAIT
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:64571  del03s17-in-x0a:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:65065  del11s18-in-x03:https  ESTABLISHED
  TCP    [2405:201:4013:81dc:2424:70de:e7bd:b6ed]:65341  del11s13-in-x02:https  TIME_WAIT
```

5. **nbtstat:** nbtstat command displays NetBIOS over TCP/IP (NetBT) protocol statistics. NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Nbtstat command-line parameters are case-sensitive.

   Syntax: nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]

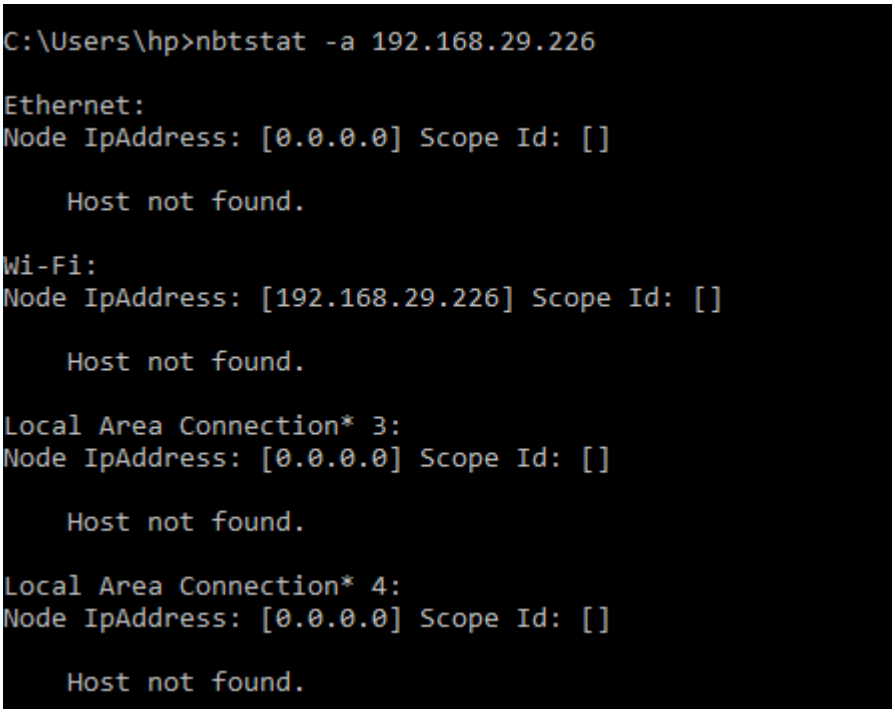
   Parameters:

   Used without parameters: displays help.

   - **-a:** RemoteName Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer. The NetBIOS name table is the list of NetBIOS names that corresponds to NetBIOS applications running on that computer.
   - **-A:** IPAddress Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer.
   - **-c:** Displays the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses.

- **-n:** Displays the NetBIOS name table of the local computer. The status of Registered indicates that the name is registered either by broadcast or with a WINS server.
- **-r:** Displays NetBIOS name resolution statistics. On a Windows XP computer that is configured to use WINS, this parameter returns the number of names that have been resolved and registered using broadcast and WINS.
- **-R:** Purges the contents of the NetBIOS name cache and then reloads the #PRE-tagged entries from the Lmhosts file.
- **-RR:** Releases and then refreshes NetBIOS names for the local computer that is registered with WINS servers.
- **-s:** Displays NetBIOS client and server sessions, attempting to convert the destination IP address to a name.
- **-S:** Displays NetBIOS client and server sessions, listing the remote computers by destination IP address only.
- **Interval:** Redisplays selected statistics, pausing the number of seconds specified in Interval between each display. Press CTRL+C to stop redisplaying statistics. If this parameter is omitted, nbtstat prints the current configuration information only once.
- **/?:** Displays help at the command prompt.

```
C:\Users\hp>nbstat
'nbstat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\hp>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```



6. **ipconfig:** Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is most useful on computers that are configured to obtain an IP address automatically. This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.
    - If the Adapter name contains any spaces, use quotation marks around the adapter name (that is, "Adapter Name").
    - For adapter names, ipconfig supports the use of the asterisk (*) wildcard character to specify either adapters with names that begin with a specified string or adapters with names that contain a specified string.
    - For example, Local* matches all adapters that start with the string Local and *Con* matches all adapters that contain the string Con.

    Syntax: ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassid Adapter] [/setclassid Adapter [ClassID]]

    Parameters:

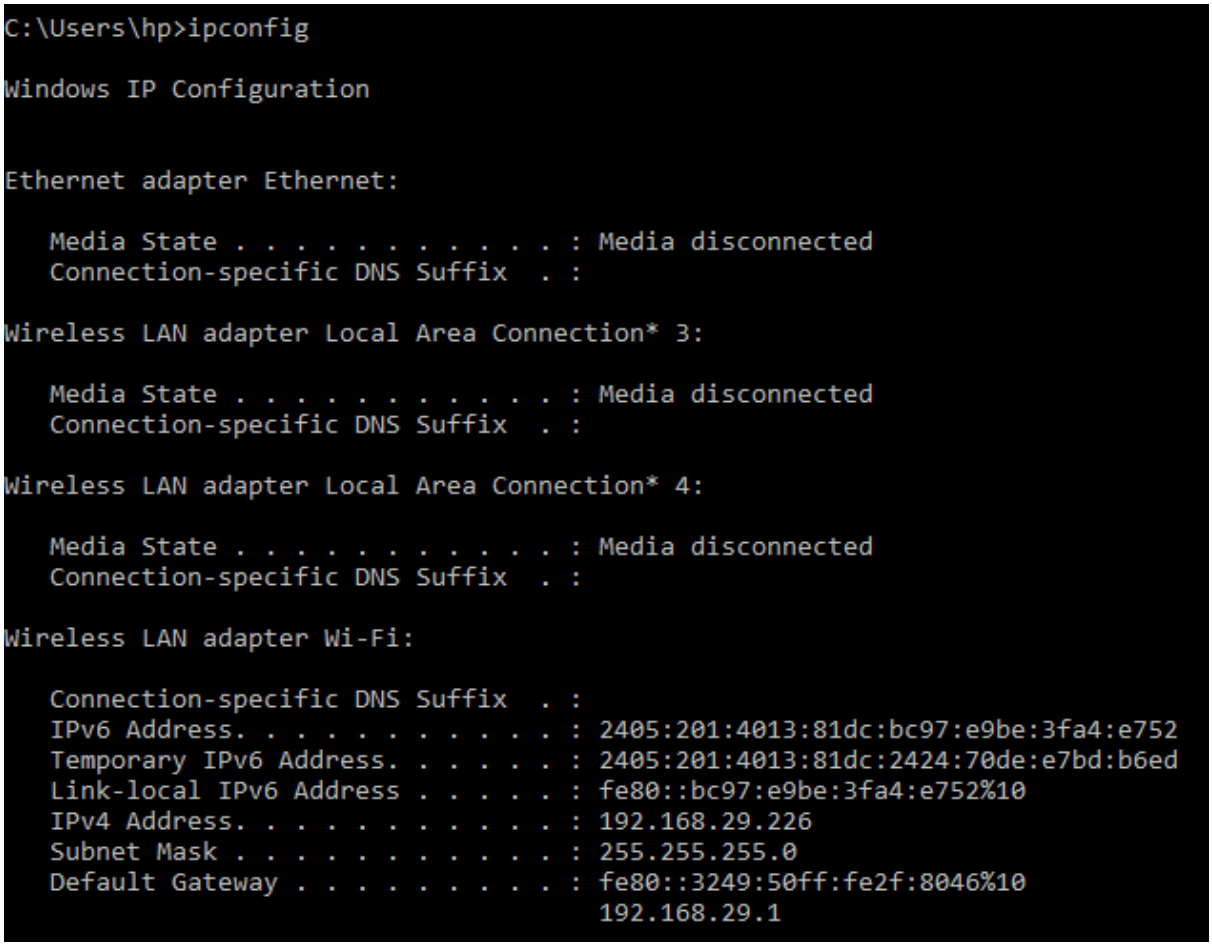
    - **Used without parameters:** displays the IP address, subnet mask, and default gateway for all adapters.
    - **/all:** Displays the full TCP/IP configuration for all adapters. Without this parameter, ipconfig displays only the IP address, subnet mask, and default gateway values for each adapter. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.
    - **/renew [Adapter]:** Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter is available only on computers with adapters that are configured

to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.

- **/release [Adapter]:** Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter disables TCP/IP for adapters configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.
- **/flushdns:** Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.
- **/displaydns:** Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.
- **/registerdns:** Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.
- **/showclassid:** Adapter Displays the DHCP class ID for a specified adapter. To see the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of Adapter. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically.
- **/setclassid:** Adapter [ClassID] Configures the DHCP class ID for a specified adapter. To set the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of Adapter. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. If a DHCP class ID is not specified, the current class ID is removed.

Examples:

- **ipconfig:** To display the basic TCP/IP configuration for all adapters
- **ipconfig /all:** To display the full TCP/IP configuration for all adapters
- **ipconfig /renew "Local Area Connection":** To renew a DHCP-assigned IP address configuration for only the Local Area Connection adapter
- **ipconfig /flushdns:** To flush the DNS resolver cache when troubleshooting DNS name resolution problems
- **ipconfig /showclassid Local:** To display the DHCP class ID for all adapters with names that start with Local
- **ipconfig /setclassid "Local Area Connection" TEST:** To set the DHCP class ID for the Local Area Connection adapter to TEST


C:\Users\hp>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 4:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2405:201:4013:81dc:bc97:e9be:3fa4:e752
Temporary IPv6 Address. . . . . : 2405:201:4013:81dc:2424:70de:e7bd:b6ed
Link-local IPv6 Address . . . . . : fe80::bc97:e9be:3fa4:e752%10
IPv4 Address. . . . . : 192.168.29.226
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::3249:50ff:fe2f:8046%10
192.168.29.1

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-BQK27U3
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : A0-8C-FD-23-28-DB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : AC-2B-6E-32-9D-6D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : AE-2B-6E-32-9D-6C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3165
   Physical Address. . . . . . . . . : AC-2B-6E-32-9D-6C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2405:201:4013:81dc:bc97:e9be:3fa4:e752(Preferred)
   Temporary IPv6 Address. . . . . . : 2405:201:4013:81dc:2424:70de:e7bd:b6ed(Preferred)
   Link-local IPv6 Address . . . . . : fe80::bc97:e9be:3fa4:e752%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.29.226(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 24 July 2021 21:41:50
   Lease Expires . . . . . . . . . . : 24 July 2021 23:37:29
   Default Gateway . . . . . . . . . : fe80::3249:50ff:fe2f:8046%10
                                       192.168.29.1
   DHCP Server . . . . . . . . . . . : 192.168.29.1
   DHCPv6 IAID . . . . . . . . . . . : 78392174
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-12-7D-66-A0-8C-FD-23-28-DB
   DNS Servers . . . . . . . . . . . : 2405:201:4013:81dc::c0a8:1d01
                                       192.168.29.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

7. **nslookup:** nslookup (Name Server lookup) is a UNIX shell command to query Internet domain name servers.

   Definitions:

   - **Nameserver:** These are the servers that the internet uses to find out more about the domain. Usually they are an ISP's computer.

- **Mailserver:** Where email is sent to.
- **Webserver:** The domains website.
- **FTPserver:** FTP is file transfer protocol, this server is where files may be stored.
- **Hostname:** The name of the host as given by the domain.
- **Real Hostname:** This is hostname that you get by reverse resolving the IP address, may be different to the given hostname.
- **IP Address:** Unique four numbered identifier that is obtained by resolving the hostname.

```
C:\Users\hp>nslookup
Default Server:  reliance.reliance
Address:  2405:201:4013:81dc::c0a8:1d01

> set type*nx
> gmail.com
Server:  reliance.reliance
Address:  2405:201:4013:81dc::c0a8:1d01

Non-authoritative answer:
Name:    gmail.com
Addresses:  2404:6800:4002:81a::2005
          142.250.182.165

> exit
```

8. **getmac:** getmac command is used for quickly finding out your MAC address.
   In order to be compliant with the IEEE 802 standards, each device must have a unique MAC (Media Access Control) address. The manufacturer of your device will assign it a MAC address and store it within the hardware. The getmac command provides an easy way to find the MAC address of your device. If you see more than one MAC address for your device, it will have multiple network adapters. As an example, a laptop with both Ethernet and Wi-Fi will have two separate MAC addresses. Some administrators will use the unique MAC addresses of devices to limit what can and cannot connect to a network.
   Syntax: getmac

```
C:\Users\hp>getmac

Physical Address    Transport Name
=================== ============================================================
AC-2B-6E-32-9D-6C   \Device\Tcpip_{65F25BFB-0949-499A-9DEA-7A781898499D}
A0-8C-FD-23-28-DB   Media disconnected
```

9. **hostname:** hostname command provides you with an easy way of identifying the hostname that has been assigned to your Windows device. There are ways of being able to find this through Windows but using the command line is much quicker. Simply type hostname into the command prompt and it will present you with the local computer name of your device.
   Syntax: hostname

```
C:\Users\hp>hostname
DESKTOP-BQK27U3
```

10. **net:** net command is definitely a versatile one, allowing you to manage many different aspects of a network and its settings such as network shares, users and print jobs, as just a few examples. Running just net won't do much, but it will present you with a list of all the switches that are available. These include accounts to set password and logon requirements, file to show a list of open files and sessions to list, or even disconnect, sessions on the network. If you are ever in doubt as to what task each switch performs, run net help and you'll find the answer.
    Syntax: net

```
C:\Users\hp>net
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\hp>net view
System error 6118 has occurred.

The list of servers for this workgroup is not currently available
```

11. **pathping:** pathping command is used troubleshooting the network connection issues. It combines that best of both ping and tracert into a single utility. Enter pathping followed by a hostname into the command prompt and it will initiate what looks like a regular old tracert command. Let the process finish, however, and you will be provided with more detail than either ping or tracert can provide, such as latency reports and statistics on packet loss. Be patient when using the pathping command as it will take five minutes in order to gather all of the statistics for you.
    Syntax: pathping [-g host-list] [-h maximum_hops] [-i address] [-n] [-p period] [-q num_queries] [-w timeout] [-4] [-6] target_name
    Parameters:
    - **-g host-list:** Loose source route along host-list.
    - **-h maximum_hops:** Maximum number of hops to search for target.
    - **-i address:** Use the specified source address.
    - **-n:** Do not resolve addresses to hostnames.
    - **-p period:** Wait period milliseconds between pings.
    - **-q num_queries:** Number of queries per hop.
    - **-w timeout:** Wait timeout milliseconds for each reply.
    - **-4:** Force using IPv4.
    - **-6:** Force using IPv6.

```
C:\Users\hp>pathping DESKTOP-BQK27U3

Tracing route to DESKTOP-BQK27U3 [fe80::bc97:e9be:3fa4:e752%10]
over a maximum of 30 hops:
  0  DESKTOP-BQK27U3 [fe80::bc97:e9be:3fa4:e752%10]
  1  DESKTOP-BQK27U3 [fe80::bc97:e9be:3fa4:e752]

Computing statistics for 25 seconds...
           Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          DESKTOP-BQK27U3 [fe80::bc97:e9be:3fa4:e752%10]
                                   0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  DESKTOP-BQK27U3 [fe80::bc97:e9be:3fa4:e752]

Trace complete.
```

12. **netsh:** netsh command is used for displaying and configuring network adapters. Netsh is another very powerful command, allowing you to view and configure almost all of the network adapters in your device in much greater detail compared with some other commands. When you run the netsh command on its own, the command prompt will be shifted into network shell mode. Within this mode, there are several different "contexts", such as one for DHCP-related commands, one for diagnostics and one for routing. It is possible to still run individual commands from netsh, though.
    - In order to see all of the available netsh contexts, run **netsh /?**
    - To see all of the commands available within a context, run **netsh contextname /?** Subcommands are available within certain commands.
    - To view these, run netsh contextname **show /?**
    - As an example, you can run the **netsh wlan** show drivers command to view all of the wireless network drivers on your device and their properties.

    Syntax: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]UserName] [-p Password | *] [Command | -f ScriptFile]

    Parameters:

    - **?:** Displays a list of commands.
    - **add:** Adds a configuration entry to a list of entries.
    - **advfirewall:** Changes to the `netsh advfirewall' context.
    - **bridge:** Changes to the `netsh bridge' context.
    - **delete:** Deletes a configuration entry from a list of entries.
    - **dhcpclient:** Changes to the `netsh dhcpclient' context.
    - **dnsclient:** Changes to the `netsh dnsclient' context.
    - **dump:** Displays a configuration script.
    - **exec:** Runs a script file.
    - **firewall:** Changes to the `netsh firewall' context.
    - **help:** Displays a list of commands.
    - **http:** Changes to the `netsh http' context.
    - **interface:** Changes to the `netsh interface' context.
    - **ipsec:** Changes to the `netsh ipsec' context.
    - **lan:** Changes to the `netsh lan' context.

- **mbn:** Changes to the `netsh mbn' context.
- **namespace:** Changes to the `netsh namespace' context.
- **netio:** Changes to the `netsh netio' context.
- **p2p:** Changes to the `netsh p2p' context.
- **ras:** Changes to the `netsh ras' context.
- **rpc:** Changes to the `netsh rpc' context.
- **set:** Updates configuration settings.
- **show:** Displays information.
- **trace:** Changes to the `netsh trace' context.
- **wcn:** Changes to the `netsh wcn' context.
- **wfp:** Changes to the `netsh wfp' context.
- **winhttp:** Changes to the `netsh winhttp' context.
- **winsock:** Changes to the `netsh winsock' context.
- **wlan:** Changes to the `netsh wlan' context.

```
C:\Users\hp>netsh
netsh>lan
netsh lan>exit
```

```
C:\Users\hp>netsh/?

Usage: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]UserName] [-p Password | *]
             [Command | -f ScriptFile]

The following commands are available:

Commands in this context:
?               - Displays a list of commands.
add             - Adds a configuration entry to a list of entries.
advfirewall     - Changes to the `netsh advfirewall' context.
bridge          - Changes to the `netsh bridge' context.
delete          - Deletes a configuration entry from a list of entries.
dhcpclient      - Changes to the `netsh dhcpclient' context.
dnsclient       - Changes to the `netsh dnsclient' context.
dump            - Displays a configuration script.
exec            - Runs a script file.
firewall        - Changes to the `netsh firewall' context.
help            - Displays a list of commands.
http            - Changes to the `netsh http' context.
interface       - Changes to the `netsh interface' context.
ipsec           - Changes to the `netsh ipsec' context.
lan             - Changes to the `netsh lan' context.
mbn             - Changes to the `netsh mbn' context.
namespace       - Changes to the `netsh namespace' context.
netio           - Changes to the `netsh netio' context.
p2p             - Changes to the `netsh p2p' context.
ras             - Changes to the `netsh ras' context.
rpc             - Changes to the `netsh rpc' context.
set             - Updates configuration settings.
show            - Displays information.
trace           - Changes to the `netsh trace' context.
wcn             - Changes to the `netsh wcn' context.
wfp             - Changes to the `netsh wfp' context.
winhttp         - Changes to the `netsh winhttp' context.
winsock         - Changes to the `netsh winsock' context.
wlan            - Changes to the `netsh wlan' context.

The following sub-contexts are available:
 advfirewall bridge dhcpclient dnsclient firewall http interface ipsec lan mbn namespace netio p2p ras rpc trace wcn wfp winhttp winsock wlan

To view help for a command, type the command, followed by a space, and then
 type ?.
```

13. **net view:** net view command is used for viewing devices connected to a network. There may be a time where you want to see what devices are connected to your network. This is where the net view command comes in. Simply run the net view command and after a short while you will be presented with a list of devices that are connected to the same network as you. The caveat with this command is that it may not show all of the devices connected to your network. It works well enough for private networks but will fail to identify devices such as smartphones and printers, and it can have trouble identifying devices running a different operating system to Windows. This simple command may

work perfectly for you and your home network, but if not, you can always use the arp command we discussed earlier instead.
Syntax: net view

```
C:\Users\hp>net view
System error 6118 has occurred.

The list of servers for this workgroup is not currently available
```

14. **route:** route tool displays the routing table that allows Windows 10 to understand the network and communicate with other devices and services. The tool also offers some options to modify and clear the table as needed. Like the arp tool, you typically do not have to worry about the routing table, but the command-line tool will come in handy when troubleshooting related problems.
Syntax: ROUTE [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]
Parameters:
    - **-f:** Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.
    - **-p:** When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, which always affect the appropriate persistent routes.
    - **-4:** Force using IPv4.
    - **-6:** Force using IPv6.

    Commands:
    - **PRINT:** Prints a route
    - **ADD:** Adds a route
    - **DELETE:** Deletes a route
    - **CHANGE:** Modifies an existing route
    - **destination:** Specifies the host.
    - **MASK:** Specifies that the next parameter is the 'netmask' value.
    - **netmask:** Specifies a subnet mask value for this route entry. If not specified, it defaults to 255.255.255.255.
    - **gateway:** Specifies gateway.
    - **interface:** the interface number for the specified route.
    - **METRIC:** specifies the metric, ie. cost for the destination.

```
C:\Users\hp>route print
===========================================================================
Interface List
  9...a0 8c fd 23 28 db ......Realtek PCIe FE Family Controller
 11...ac 2b 6e 32 9d 6d ......Microsoft Wi-Fi Direct Virtual Adapter #2
 16...ae 2b 6e 32 9d 6c ......Microsoft Wi-Fi Direct Virtual Adapter #3
 10...ac 2b 6e 32 9d 6c ......Intel(R) Dual Band Wireless-AC 3165
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.29.1   192.168.29.226     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.29.0    255.255.255.0         On-link    192.168.29.226    311
   192.168.29.226  255.255.255.255         On-link    192.168.29.226    311
   192.168.29.255  255.255.255.255         On-link    192.168.29.226    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    192.168.29.226    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    192.168.29.226    311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 10     71 ::/0                     fe80::3249:50ff:fe2f:8046
  1    331 ::1/128                  On-link
 10     71 2405:201:4013:81dc::/64  On-link
 10    311 2405:201:4013:81dc:1951:5a2f:8df7:7347/128
                                    On-link
 10    311 2405:201:4013:81dc:bc97:e9be:3fa4:e752/128
                                    On-link
 10    311 fe80::/64                On-link
 10    311 fe80::bc97:e9be:3fa4:e752/128
                                    On-link
  1    331 ff00::/8                 On-link
 10    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

15. **systeminfo:** systeminfo command is used to display system information. If you need to know anything about the device you are using, be it details of the processor used, the version of Windows you are operating on, or what the boot device is configured as, you can find it all through the Windows GUI. But this command will poll your device and display the most important information in a clean, easy to read format.

Syntax: systeminfo

```
C:\Users\hp>systeminfo

Host Name:                 DESKTOP-BQK27U3
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          hp
Registered Organization:
Product ID:                00342-41314-45822-AAOEM
Original Install Date:     22-05-2021, 15:25:21
System Boot Time:          23-07-2021, 19:43:16
System Manufacturer:       HP
System Model:              HP Pavilion Notebook
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 78 Stepping 3 GenuineIntel ~2492 Mhz
BIOS Version:              Insyde F.02, 14-03-2016
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             4009
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     16,274 MB
Available Physical Memory: 8,941 MB
Virtual Memory: Max Size:  20,114 MB
Virtual Memory: Available: 11,349 MB
Virtual Memory: In Use:    8,765 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-BQK27U3
Hotfix(s):                 6 Hotfix(s) Installed.
                           [01]: KB5003537
                           [02]: KB4562830
                           [03]: KB4577586
                           [04]: KB4580325
                           [05]: KB5004237
                           [06]: KB5003742
Network Card(s):           2 NIC(s) Installed.
                           [01]: Intel(R) Dual Band Wireless-AC 3165
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.29.1
                                 IP address(es)
                                 [01]: 192.168.29.226
                                 [02]: fe80::bc97:e9be:3fa4:e752
                                 [03]: 2405:201:4013:81dc:a012:1b6b:fa78:9459
                                 [04]: 2405:201:4013:81dc:bc97:e9be:3fa4:e752
                           [02]: Realtek PCIe FE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: No
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes
```

Result: Basic Networking commands has been executed successfully.

Experiment 2

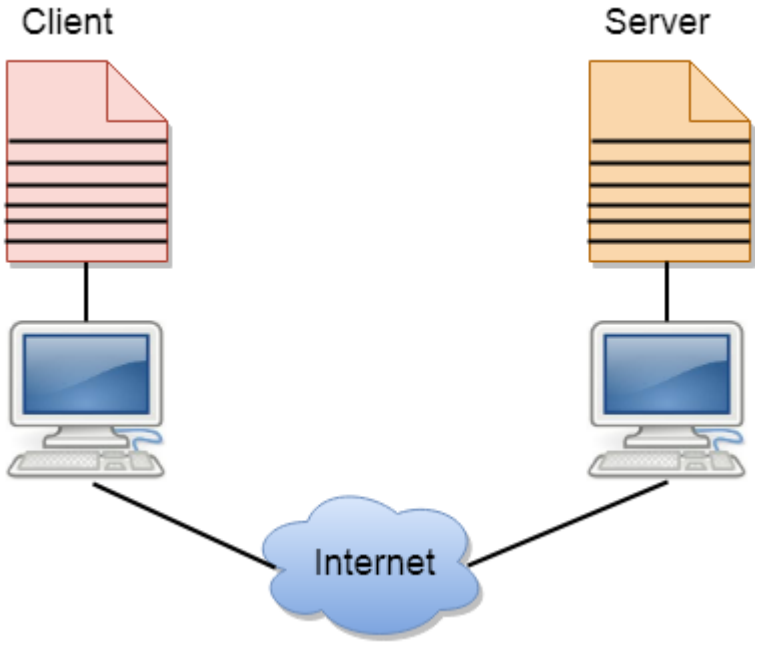
Date: 03-08-2021

Aim: To design and simulate client to server and peer to peer network.

Software Used: Cisco Packet Tracer.

Theory:

1. **Client to Server Network:**
    - A client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.
    - The application programs using the client-server model should follow the given below strategies:



    - An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.
    - A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.
    - A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.
    - Services are required frequently, and many users have a specific client-server application program. For example, the client-server application program allows the user to access the files, send e-mail, and so on. If the services are more customized, then we should have one generic application program that allows the user to access the services available on the remote computer.

Client: A client is a program that runs on the local machine requesting service from the server. A client program is a finite program means that the service started by the user and terminates when the service is completed.

Server: A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, then the server opens the door for the incoming requests, but it never initiates the service. A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

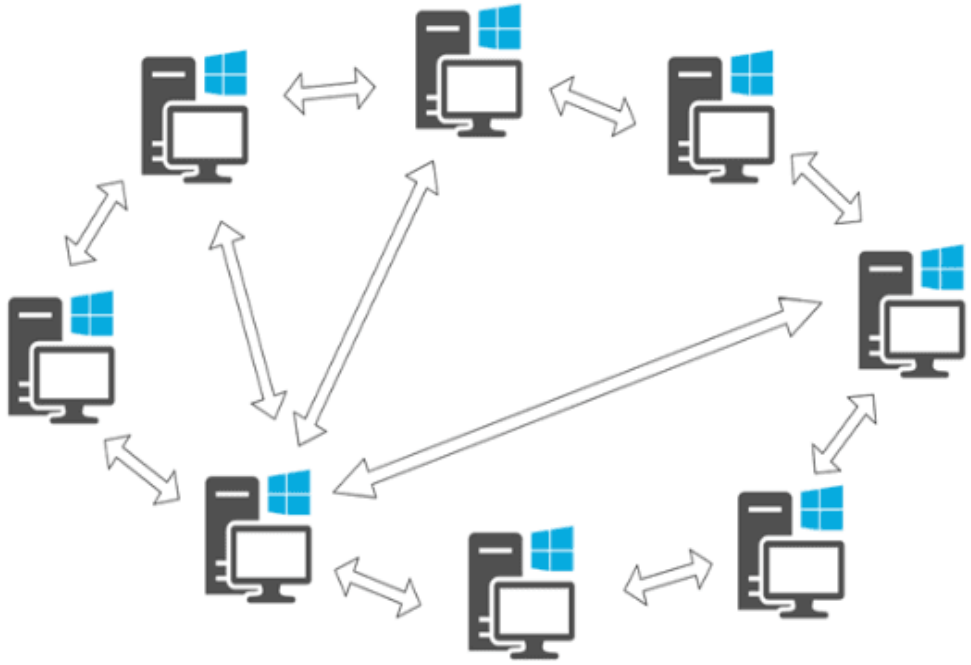
Advantages of Client to Server Network:

- **Centralized:** Centralized back-up is possible in client-server networks, i.e., all the data is stored in a server.
- **Security:** These networks are more secure as all the shared resources are centrally administered.
- **Performance:** The use of the dedicated server increases the speed of sharing resources. This increases the performance of the overall system.
- **Scalability:** We can increase the number of clients and servers separately, i.e., the new element can be added, or we can add a new node in a network at any time

Disadvantages of Client to Server Network:

- **Traffic Congestion** is a big problem in Client/Server networks. When a large number of clients send requests to the same server may cause the problem of Traffic congestion.
- It does not have a robustness of a network, i.e., when the server is down, then the client requests cannot be met.
- A client/server network is very decisive. Sometimes, regular computer hardware does not serve a certain number of clients. In such situations, specific hardware is required at the server side to complete the work.
- Sometimes the resources exist in the server but may not exist in the client. For example, If the application is web, then we cannot take the printout directly on printers without taking out the print view window on the web.

2. Peer to Peer Network:
    - A peer to peer network is a simple network of computers. It first came into existence in the late 1970s. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server to the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.



Types of Peer to Peer Network:

- **Unstructured P2P Networks:** In this type of P2P network, each device is able to make an equal contribution. This network is easy to build as devices can be connected randomly in the network. But being unstructured, it becomes difficult to find content.
- **Structured P2P Networks:** It is designed using the software which creates a virtual layer in order to put the nodes in a specific structure. These are not easy to set-up but can give easy access to users to the content.
- **Hybrid P2P Networks:** It combines the features of both P2P network and client-server architecture. An example of such a network is to find a node using the central server.

Features of Peer to Peer Network:

These networks do not involve a large number of nodes, usually less than 12. All the computers in the network store their own data but this data is accessible by the group. Unlike client-server networks, P2P uses resources and also provides them. This results in additional resources if the number of nodes increases. It requires specialized software. It allows resource sharing among the network. Since the nodes act as servers also, there is a constant threat of attack. Almost all the OS today support P2P networks.

How to Use Peer to Peer Network Efficiently:

Firstly secure your network via privacy solutions. Design a strategy that suits the underlying architecture in order to manage applications and underlying data. Keep a check on the cyber security threats which might prevail in the network. Invest in good quality software that can sustain attacks and prevent the network from being exploited. Update your software regularly.

Advantages of Peer to Peer Network:

- Network is easy to maintain because each node is independent of each other.
- Since each node acts as a server, therefore the cost of the central server is saved.
- Adding, deleting and repairing nodes in this network is easy.

Disadvantages of Peer to Peer Network:

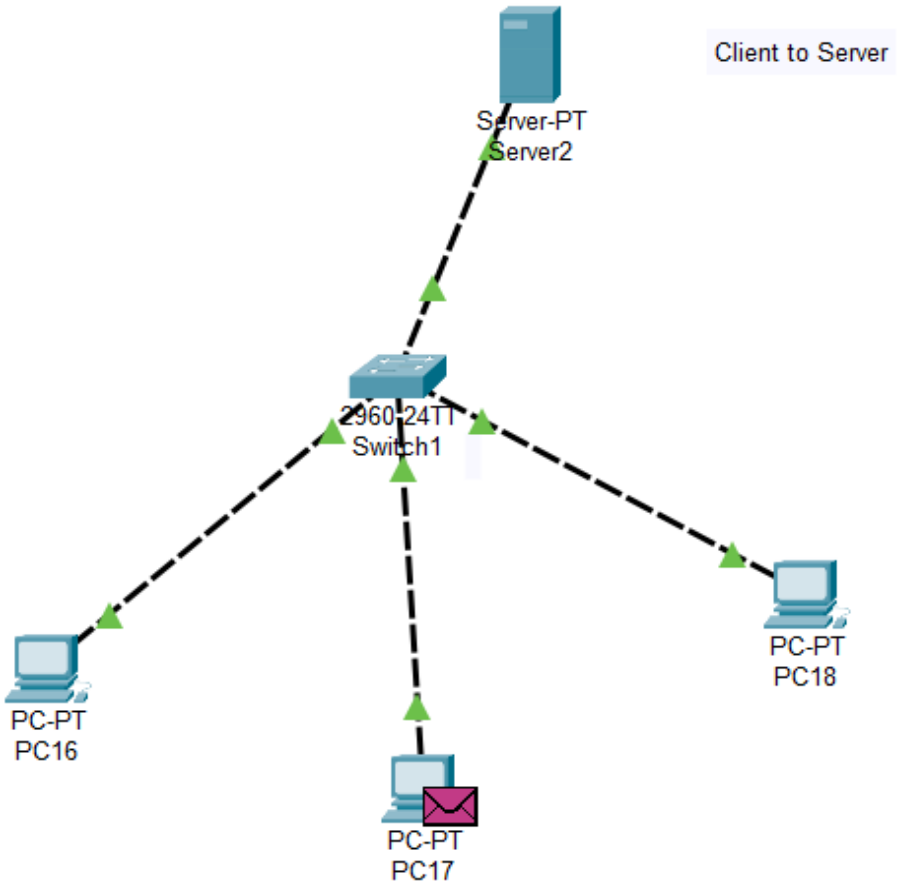
- Because of no central server, data is always vulnerable to get lost because of no backup.
- It becomes difficult to secure the complete network because each node is independent.

Example of Peer to Peer Network:

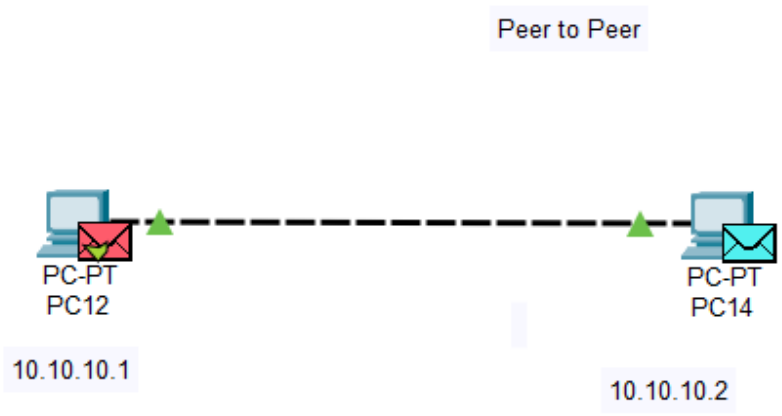
P2P networks can be basically categorized into three levels. The first level is the basic level which uses a USB to create a P2P network between two systems. The second is the intermediate level which involves the usage of copper wires in order to connect more than two systems. The third is the advanced level which uses software to establish protocols in order to manage numerous devices across the internet.

Observations:

1. **Client to Server Network:**



2. **Peer to Peer Network:**



Result: The design and simulation of Client to Server and Peer to Peer Networking Model has been done successfully.

Experiment 3

Date: 10-08-2021

Aim: To allocate the static IP Addresses to the devices and check the connectivity of the end devices using the ping command.

Software Used: Cisco Packet Tracer.

Theory: An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network. In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255. IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

How do IP Addresses Work?

If you want to understand why a particular device is not connecting in the way you would expect or you want to troubleshoot why your network may not be working, it helps understand how IP addresses work. Internet Protocol works the same way as any other language, by communicating using set guidelines to pass information. All devices find, send, and exchange information with other connected devices using this protocol. By speaking the same language, any computer in any location can talk to one another. The use of IP addresses typically happens behind the scenes. The process works like this:

- Your device indirectly connects to the internet by connecting at first to a network connected to the internet, which then grants your device access to the internet.
- When you are at home, that network will probably be your Internet Service Provider (ISP). At work, it will be your company network.
- Your IP address is assigned to your device by your ISP.
- Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.
- However, your IP address can change. For example, turning your modem or router on or off can change it. Or you can contact your ISP, and they can change it for you.
- When you are out and about – for example, traveling – and you take your device with you, your home IP address does not come with you. This is because you will be using

another network (Wi-Fi at a hotel, airport, or coffee shop, etc.) to access the internet and will be using a different (and temporary) IP address, assigned to you by the ISP of the hotel, airport or coffee shop.

Types of IP Addresses

1. There are different categories of IP addresses, and within each category, different types.
2. **Consumer IP Addresses:** Every individual or business with an internet service plan will have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.
3. **Private IP Addresses:** Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network.
4. **Public IP Addresses:** A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.
5. **Public IP Addresses:** Public IP addresses come in two forms – dynamic and static.
    - **Dynamic IP Addresses:** Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP addresses means they don't have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.
    - **Static IP Addresses:** In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

This leads to the next point – which is the two types of website IP addresses.

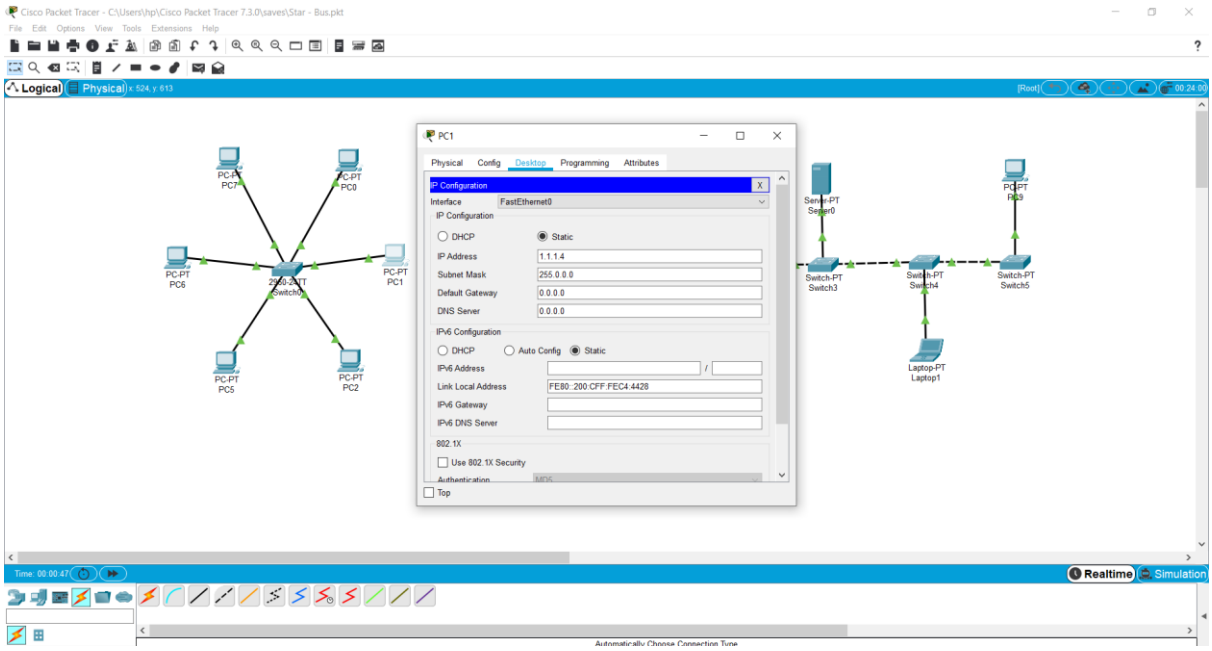
There are two types of website IP addresses

For website owners who don’t host their own server, and instead rely on a web hosting package – which is the case for most websites – there are two types of website IP addresses. These are shared and dedicated.

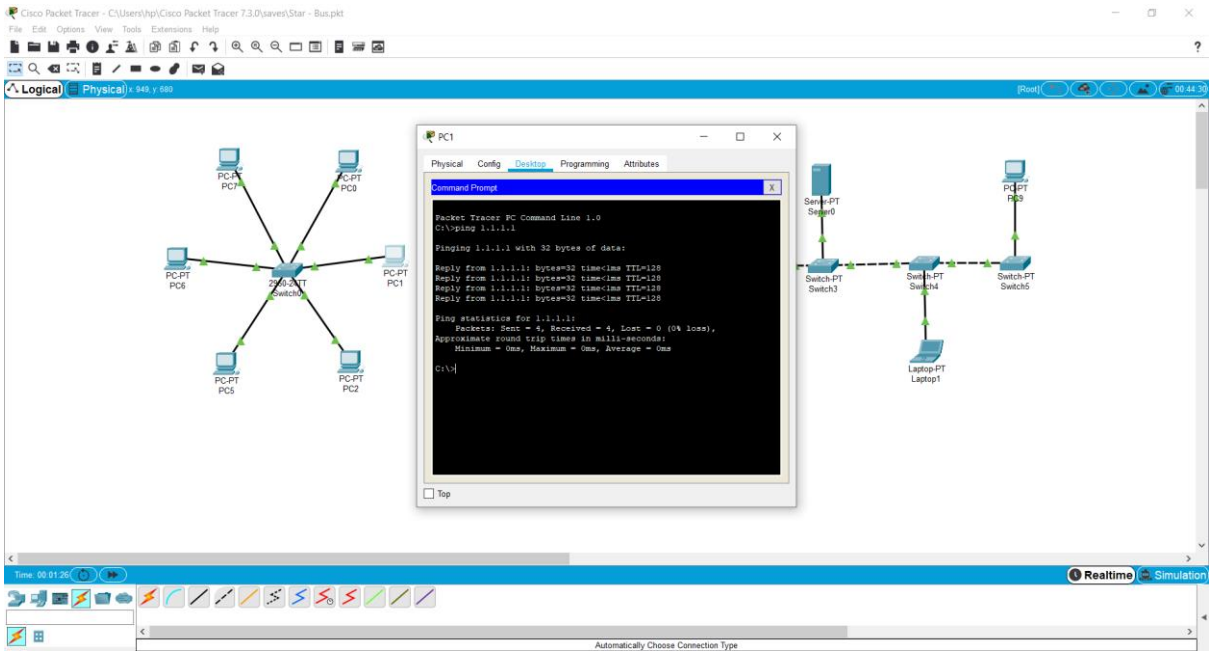
1. **Shared IP Addresses:** Websites that rely on shared hosting plans from web hosting providers will typically be one of many websites hosted on the same server. This tends to be the case for individual websites or SME websites, where traffic volumes are manageable, and the sites themselves are limited in terms of the number of pages, etc. Websites hosted in this way will have shared IP addresses.
2. **Dedicated IP Addresses:** Some web hosting plans have the option to purchase a dedicated IP address (or addresses). This can make obtaining an SSL certificate easier and allows you to run your own File Transfer Protocol (FTP) server. This makes it easier to share and transfer files with multiple people within an organization and allow anonymous FTP sharing options. A dedicated IP address also allows you to access your website using the IP address alone rather than the domain name — useful if you want to build and test it before registering your domain.

Observations:

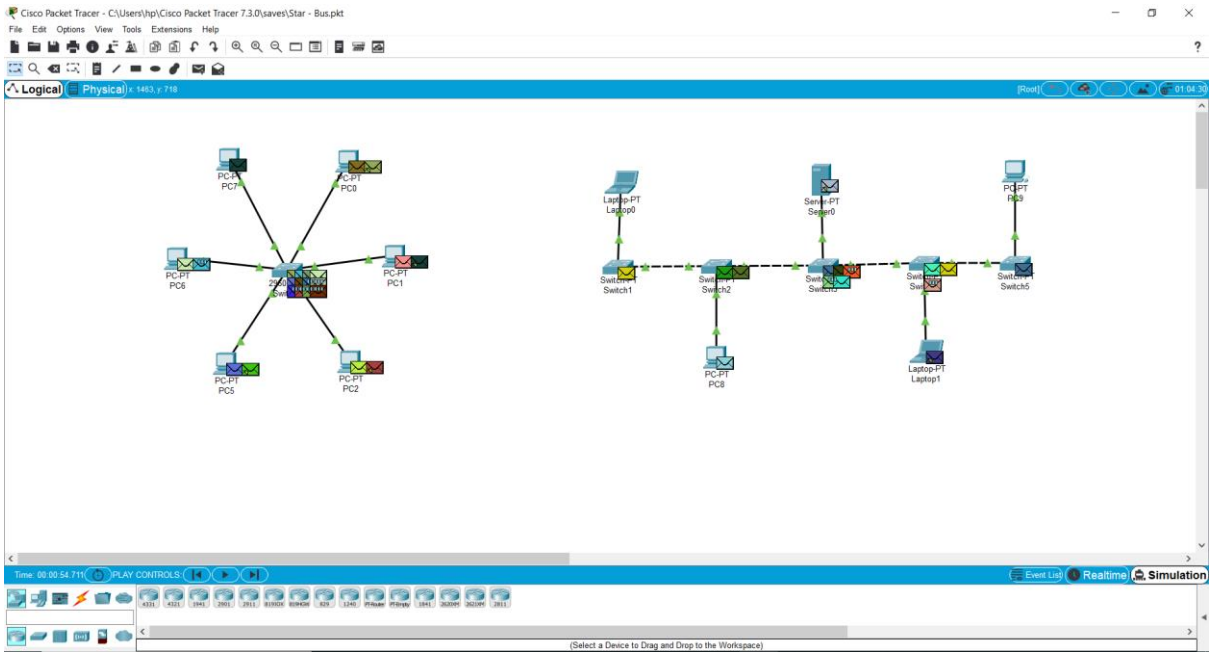
1. Allocating the IP Address to the Devices



2. To Check whether the Devices are Connected to the Network using ping Command



3. Simulation of the Network



Results: The allocate the static IP Addresses to the devices and check the connectivity of the end devices using the ping command.

Experiment 4

Date: 17-08-2021

Aim: To configure the switch in a network and add banner message to it.

Software Used: Cisco Packet Tracer.

Theory: The Cisco Catalyst 2960 switch comes preconfigured and just should be alloted fundamental security data before being associated with a system. To utilize an IP-based administration item or Telnet with a Cisco switch, you should design an administration IP address.

Steps to Configure Cisco Switch Using CLI:

Step 1: Use an external emulator such as Telnet or a PuTTY to login to the switch.

- Initial command prompt **"Switch>"** appears on the screen.
- Type **"enable"** next to it and press "Enter".
- This will take you into the **"EXEC"** mode, also known as the Global Configuration mode.
- Go into configure mode using configure terminal.
- Enter the configuration commands one per line.

Switch# configure terminal

Switch(config)#

Step 2: Provide a hostname for the switch to function in a particular network environment

Switch(config)#hostname switch

Switch(config)#

Step 3: Configure an administration password (enable secret password)

Switch(config)#enable secret somestrongpass

Note: This password will have to be given before entering into config mode, once it is configured.

Step 4: Configure default gateway

Switch(config)# ip default-gateway IP-address

Switch# show ip route

Step 5: Configure static route

Switch(config)# ip route dest_IP_address mask

Switch# show running-config

Step 6: Configure interface description

Switch(config)#interface fastethernet 0/1

Switch(config-if)#description Development VLAN

Step 7: Clear MAC address table

switch#clear mac address-table

Step 8: Set Duplex mode

Switch(config-if)#duplex full

Step 9: Exit interface configuration mode

Switch(config-if)#exit

Switch(config)#

Step 10: Exit config mode

Switch(config)#exit

Switch#

Step 11: Copy the running configuration into startup configuration using below command

Switch#write memory

Building configuration... [OK]

Switch#

Banner Message

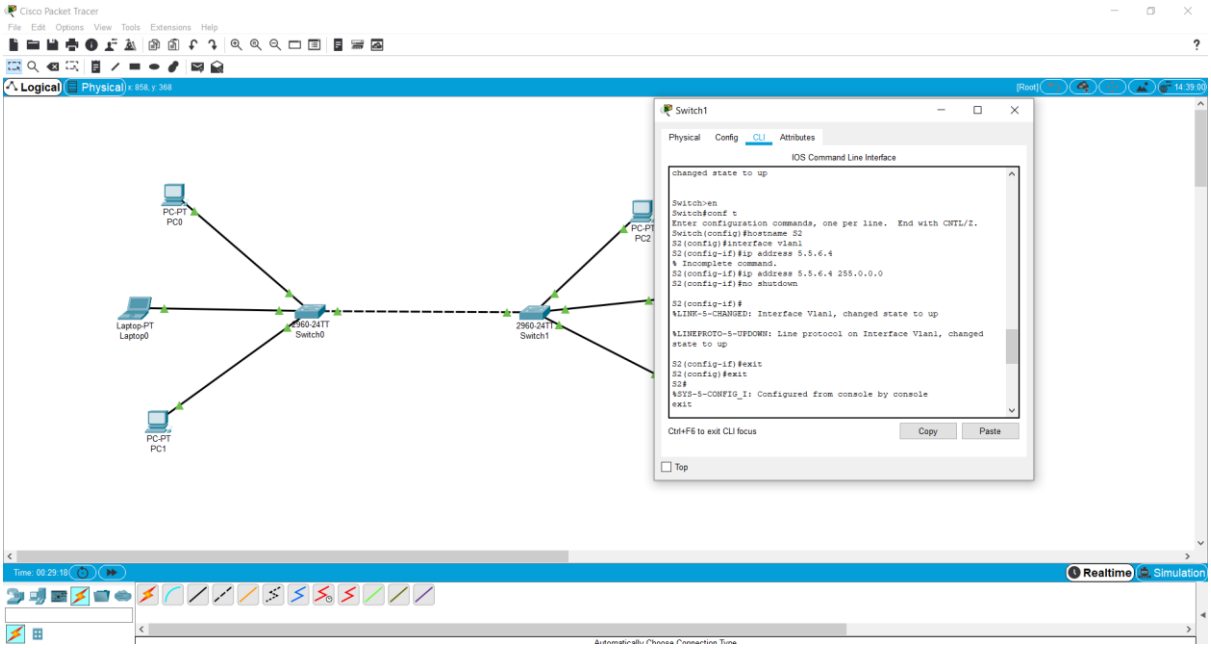
Banner Message:

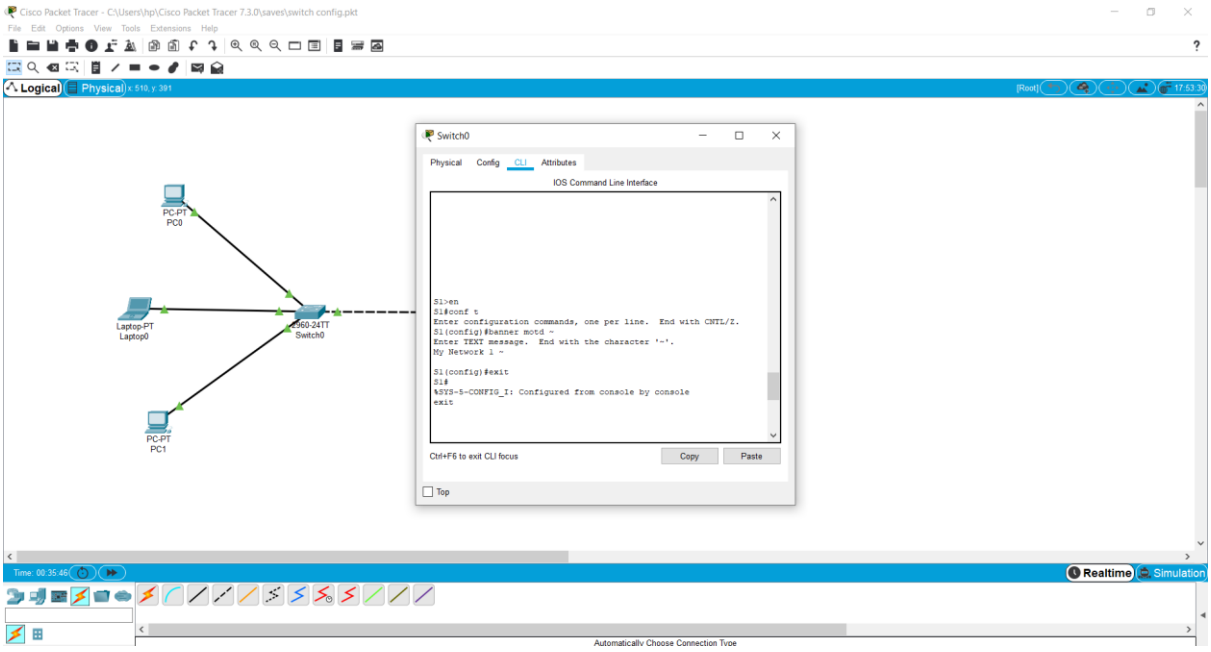
Banners are messages that are displayed when someone attempts to gain access to a device. Banners are an important part of the legal process in the event that someone is prosecuted for breaking into a device.

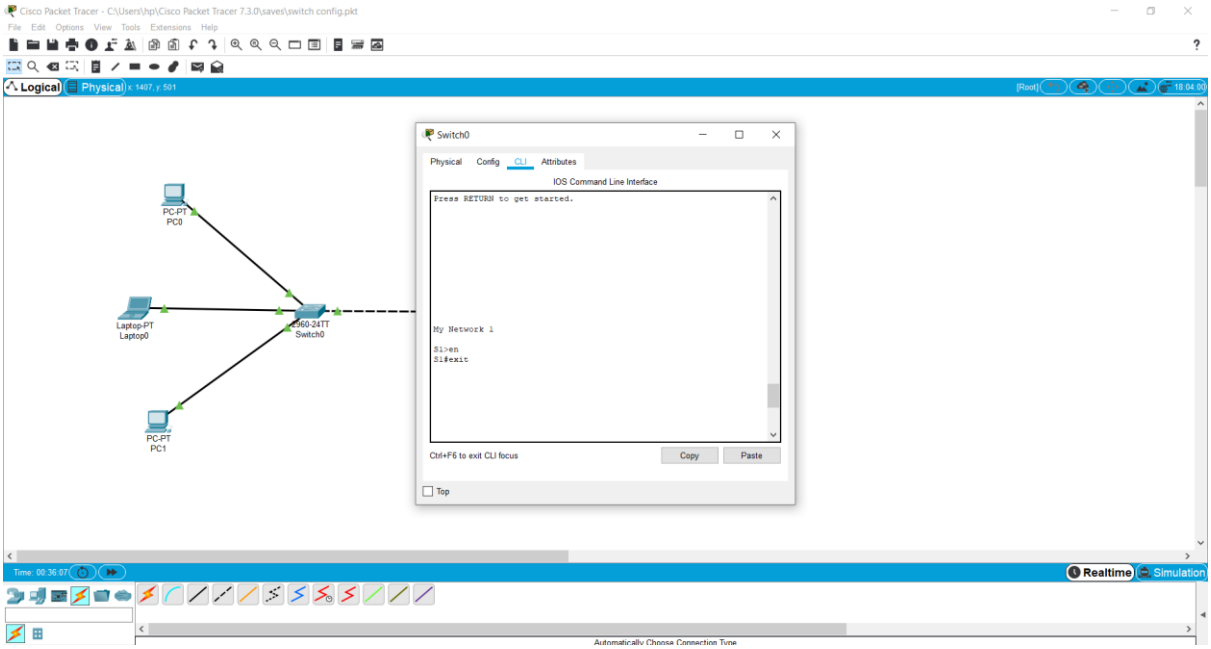
Configured using the **banner motd** *delimiter message delimiter* command from global configuration mode. The delimiting character can be any character as long as it isunique and does not occur in the message (e.g., #$%^&*)

Observations:

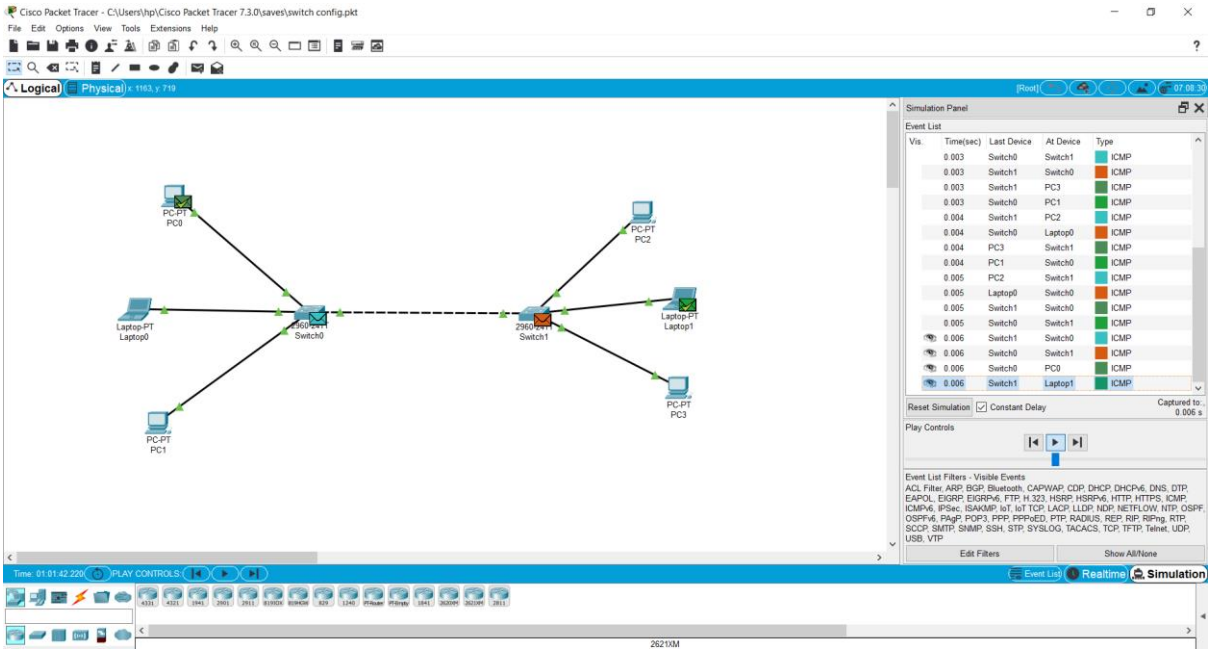
4. Configuration of Switch and Adding Banner Message to it:







5. Simulation of the Network:



Results: The configure the switch in a network and addition of banner message has been done successfully.

Experiment 5

Date: 24-08-2021

Aim: To set the password for the switch network and check its authentication using telnet command.

Software Used: Cisco Packet Tracer.

Theory: The Cisco Catalyst 2960 switch comes preconfigured and just should be alloted fundamental security data before being associated with a system. To utilize an IP-based administration item or Telnet with a Cisco switch, you should design an administration IP address.

Steps to Configure Cisco Switch Using CLI:

Step 1: Use an external emulator such as Telnet or a PuTTY to login to the switch.

- Initial command prompt **"Switch>"** appears on the screen.
- Type **"enable"** next to it and press "Enter".
- This will take you into the **"EXEC"** mode, also known as the Global Configuration mode.
- Go into configure mode using configure terminal.
- Enter the configuration commands one per line.

Switch# configure terminal

Switch(config)#

Step 2: Provide a hostname for the switch to function in a particular network environment

Switch(config)#hostname switch

Switch(config)#

Step 3: Configure an administration password (enable secret password)

Switch(config)#enable secret somestrongpass

Note: This password will have to be given before entering into config mode, once it is configured.

Step 4: Configure default gateway

Switch(config)# ip default-gateway IP-address

Switch# show ip route

Step 5: Configure static route

Switch(config)# ip route dest_IP_address mask

Switch# show running-config

Step 6: Configure interface description

Switch(config)#interface fastethernet 0/1

Switch(config-if)#description Development VLAN

Switch(config-if)#exit

Switch(config)#

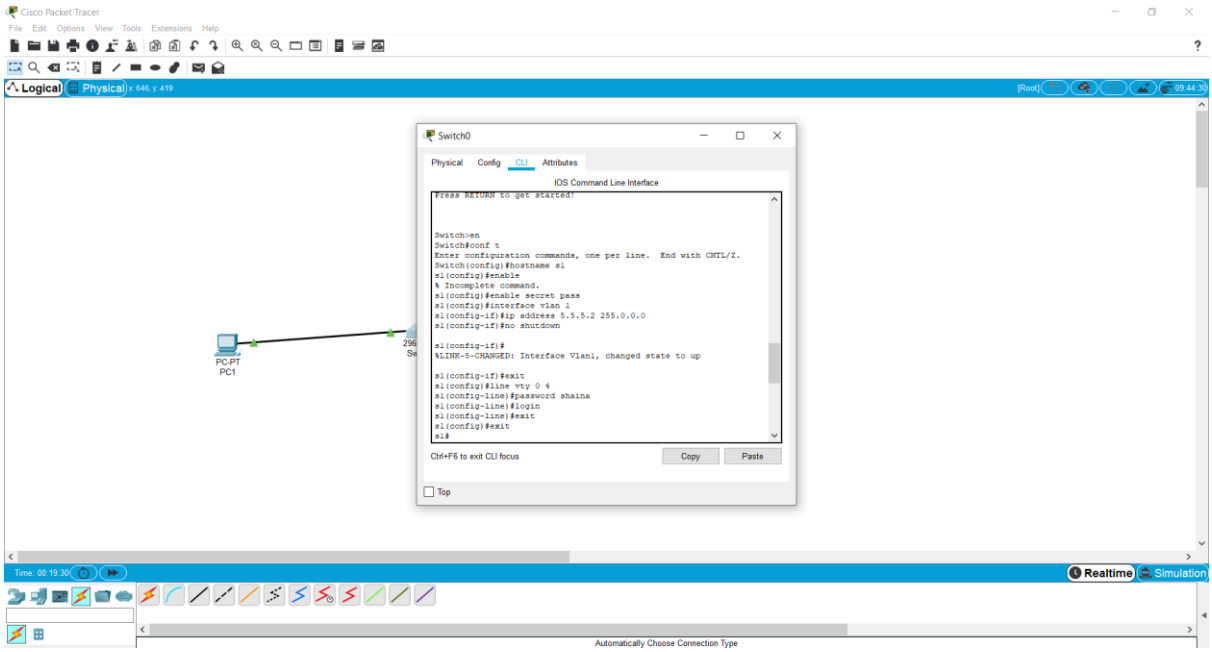
Step 10: Exit config mode

Switch(config)#exit

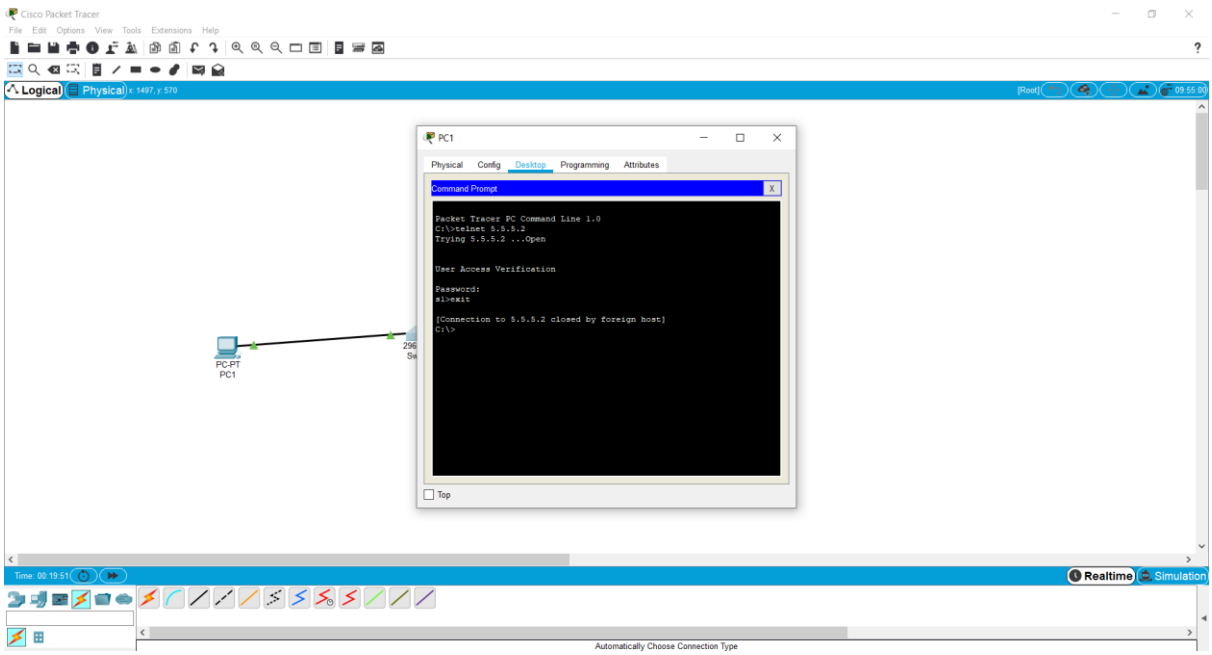
Switch#

Observations:

6. **Configuration of Switch and Adding Banner Message to it:**



7. Checking the Authentication of the Switch using TELNET command:



Results: Setting of password for the switch network and check its authentication using telnet command.

Experiment 6

Date: 24-08-2021

Aim: To secure the USER and EXEC mode and VTY lines of a switch and check its authentication using telnet command.

Software Used: Cisco Packet Tracer.

Theory:

Password Guidelines: The use of weak or easily guessed passwords continues to be the biggest security concern of organizations. Network devices, including home wireless routers, should always have passwords configured to limit administrative access.

Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device.

All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

When choosing passwords, use strong passwords that are not easily guessed. There are some key points to consider when choosing passwords:

- Use passwords that are more than eight characters in length.
- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
- Avoid using the same password for all devices.
- Do not use common words because they are easily guessed.

Use an internet search to find a password generator. Many will allow you to set the length, character set, and other parameters.

Note: Most of the labs in this course use simple passwords such as cisco or class. These passwords are considered weak and easily guessable and should be avoided in production environments. We only use these passwords for convenience in a classroom setting, or to illustrate configuration examples.

Configure Passwords:

When you initially connect to a device, you are in user EXEC mode. This mode is secured using the console.

To secure user EXEC mode access, enter line console configuration mode using the line console 0 global configuration command, as shown in the example. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the password password command. Finally, enable user EXEC access using the login command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Console access will now require a password before allowing access to the user EXEC mode.

To have administrator access to all IOS commands including configuring a device, you must gain privileged EXEC mode access. It is the most important access method because it provides complete access to the device.

To secure privileged EXEC access, use the enable secret password global config command, as shown in the example.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Virtual terminal (VTY) lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

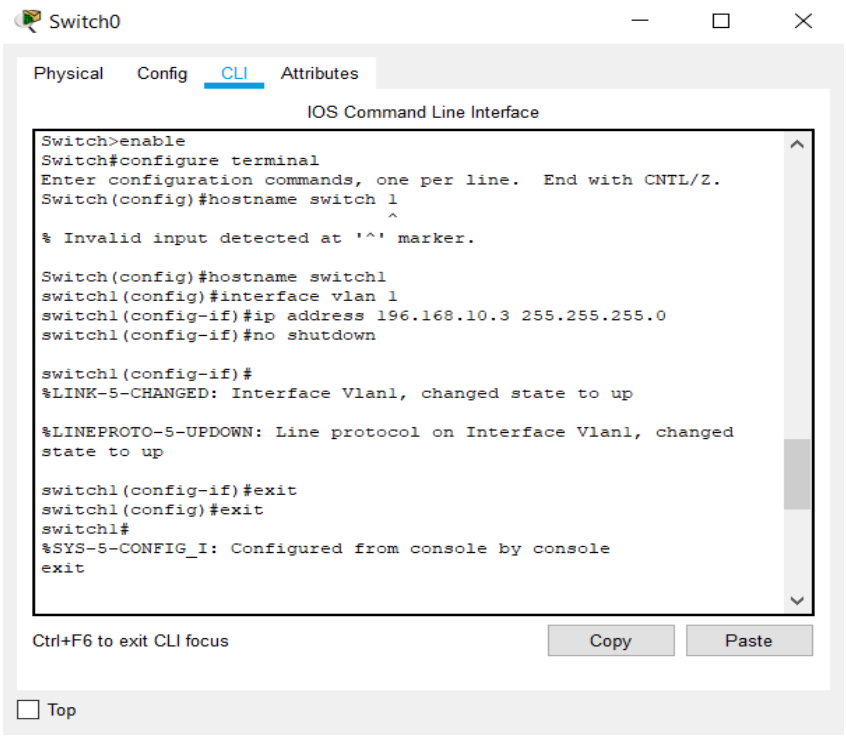
To secure VTY lines, enter line VTY mode using the line vty 0 15 global config command. Next, specify the VTY password using the password password command. Lastly, enable VTY access using the login command.

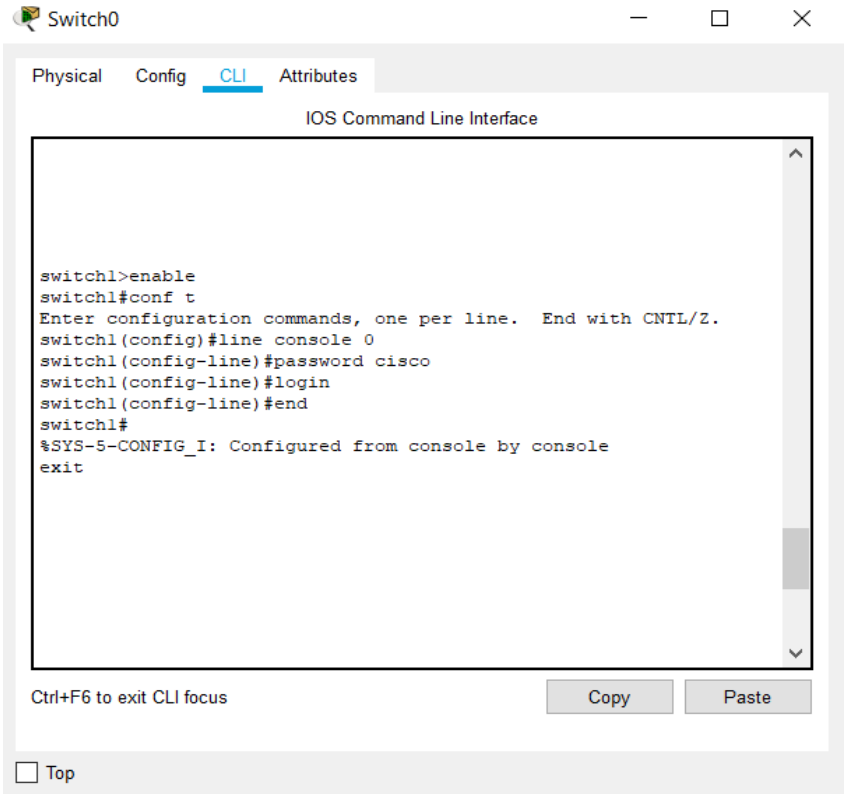
An example of securing the VTY lines on a switch is shown.

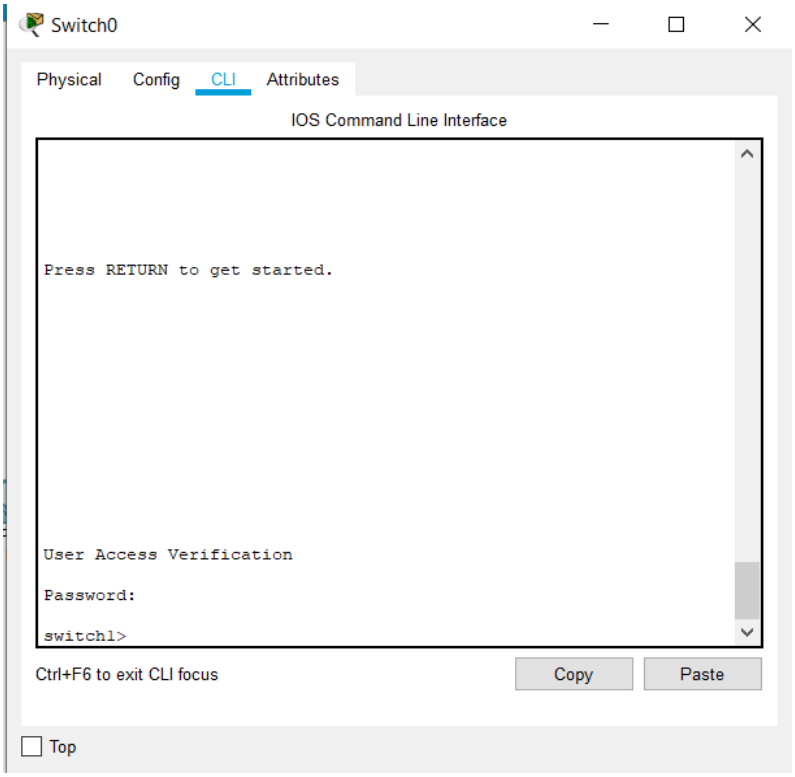
```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

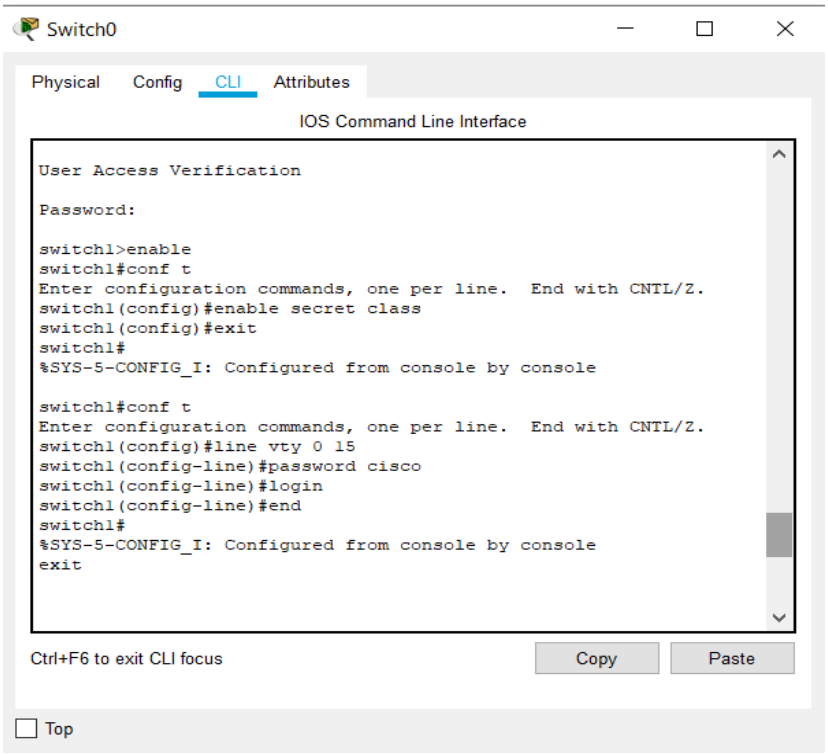
Observations:

8. Securing the USER and EXEC mode and VTY Lines:

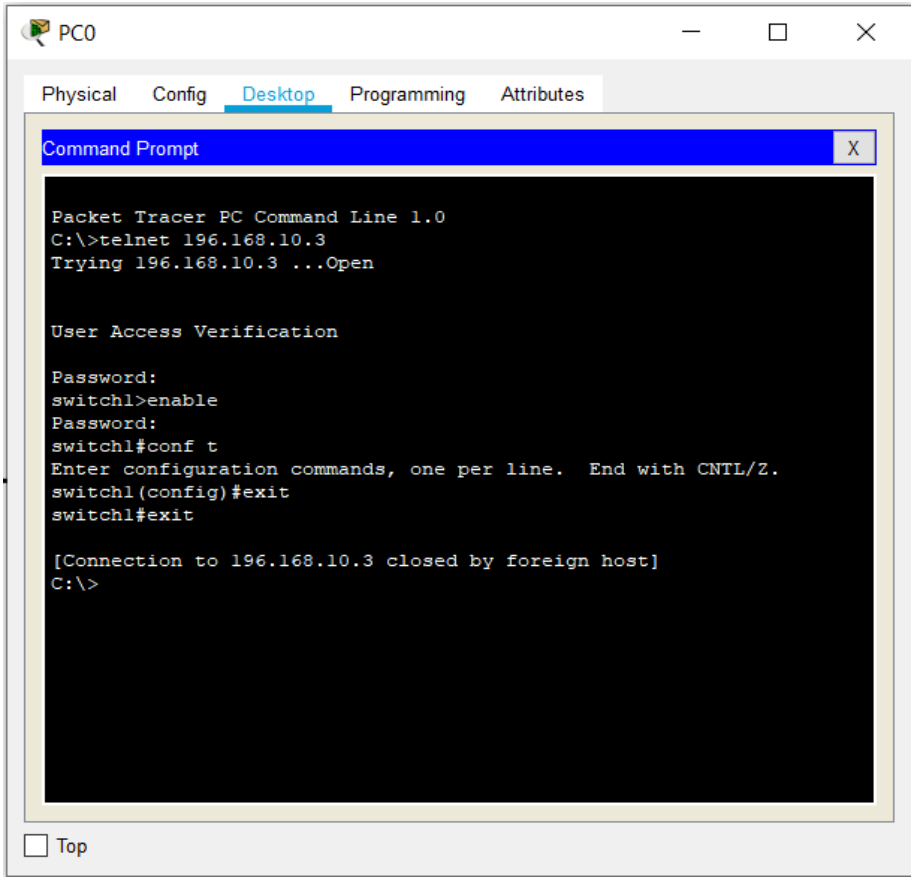





Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
User Access Verification
Password:
switch1>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Password:
switch1>enable
switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)#enable secret class
switch1(config)#exit
switch1#
%SYS-5-CONFIG_I: Configured from console by console
switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)#line vty 0 15
switch1(config-line)#password cisco
switch1(config-line)#login
switch1(config-line)#end
switch1#
%SYS-5-CONFIG_I: Configured from console by console
exit
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

9. Checking the Authentication of the Switch using TELNET command:



Results: Securing the USER and EXEC mode and VTY lines of a switch and check its authentication using telnet command.

Experiment 7

Date: 7-09-2021

Aim: To perform automatic configuration of the IP address of the end devices using DHCP protocol and assigning IP address of Default Gateway and DNS Server.

Software Used: Cisco Packet Tracer.

Theory:

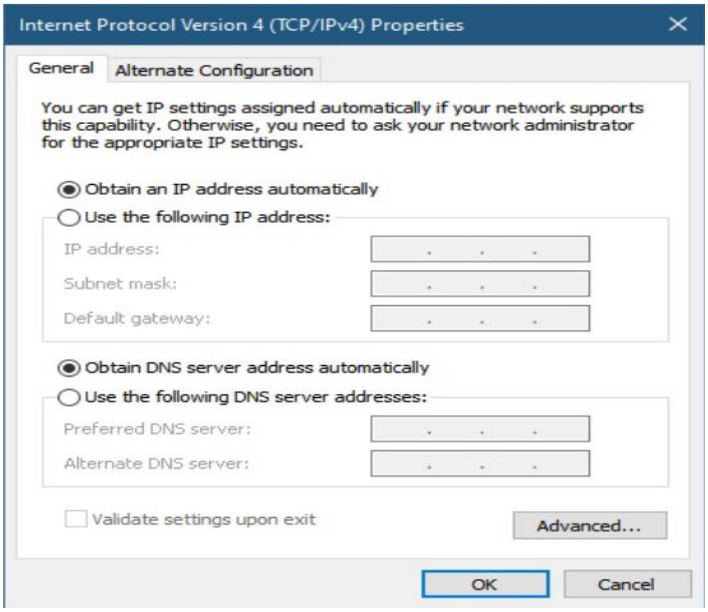
Automatic IP Address Configuration for End Devices:

End devices typically default to using DHCP for automatic IPv4 address configuration. DHCP is a technology that is used in almost every network. The best way to understand why DHCP is so popular is by considering all the extra work that would have to take place without it.

In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. Imagine the amount of time it would take if every time you connected to the network, you had to manually enter the IPv4 address, the subnet mask, the default gateway, and the DNS server. Multiply that by every user and every device in an organization and you see the problem. Manual configuration also increases the chance of misconfiguration by duplicating another device's IPv4 address.

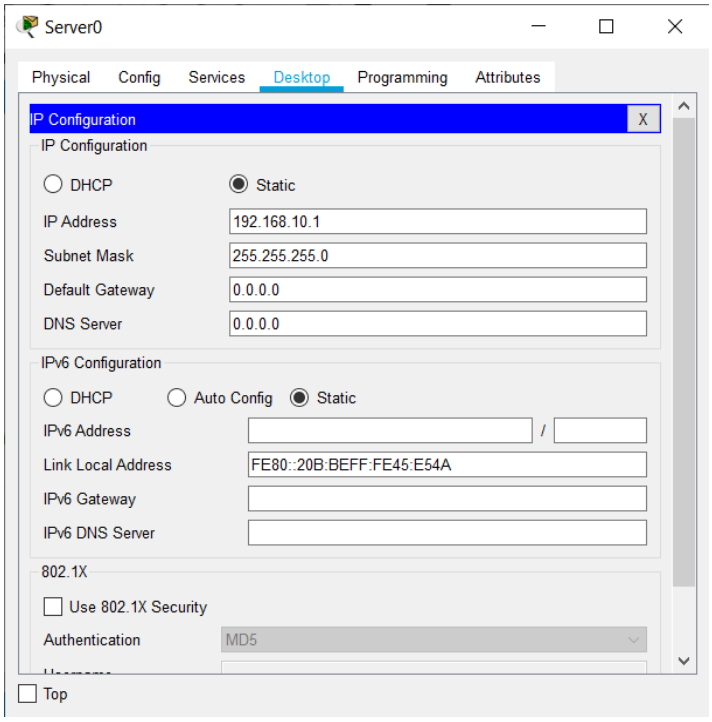
As shown in the figure, to configure DHCP on a Windows PC, you only need to select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Your PC will search out a DHCP server and be assigned the address settings necessary to communicate on the network.

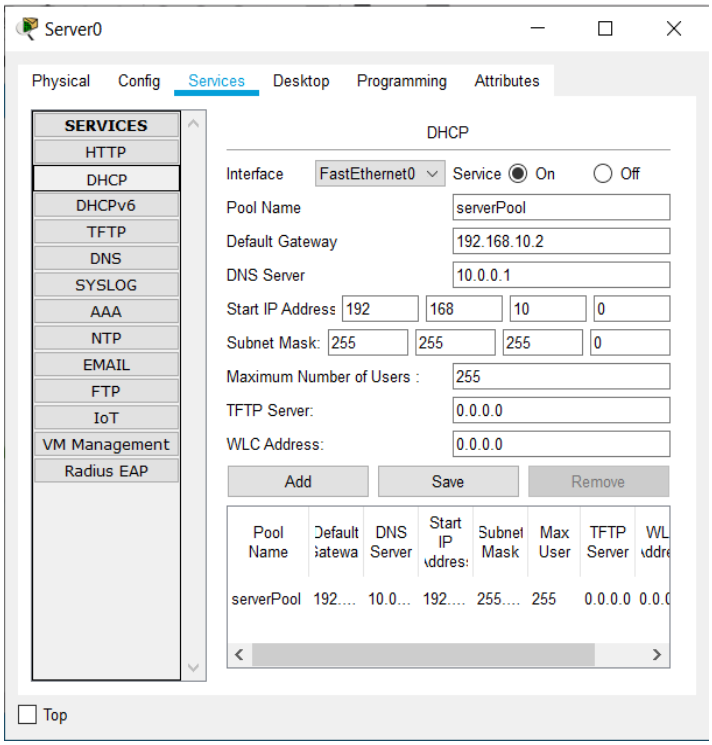
Note: IPv6 uses DHCPv6 and SLAAC (Stateless Address Autoconfiguration) for dynamic address allocation.

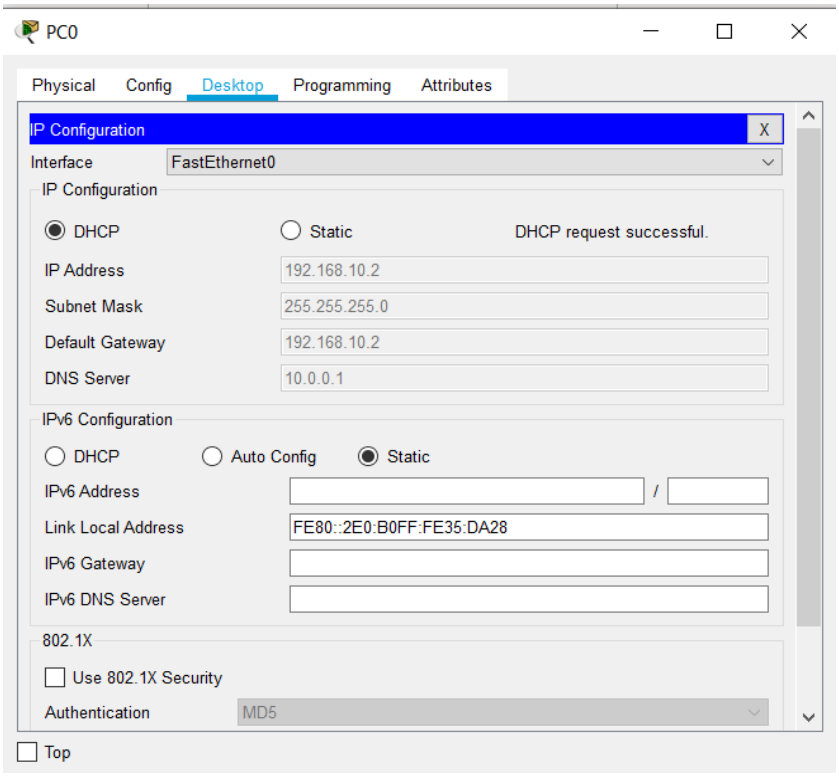


Observations:

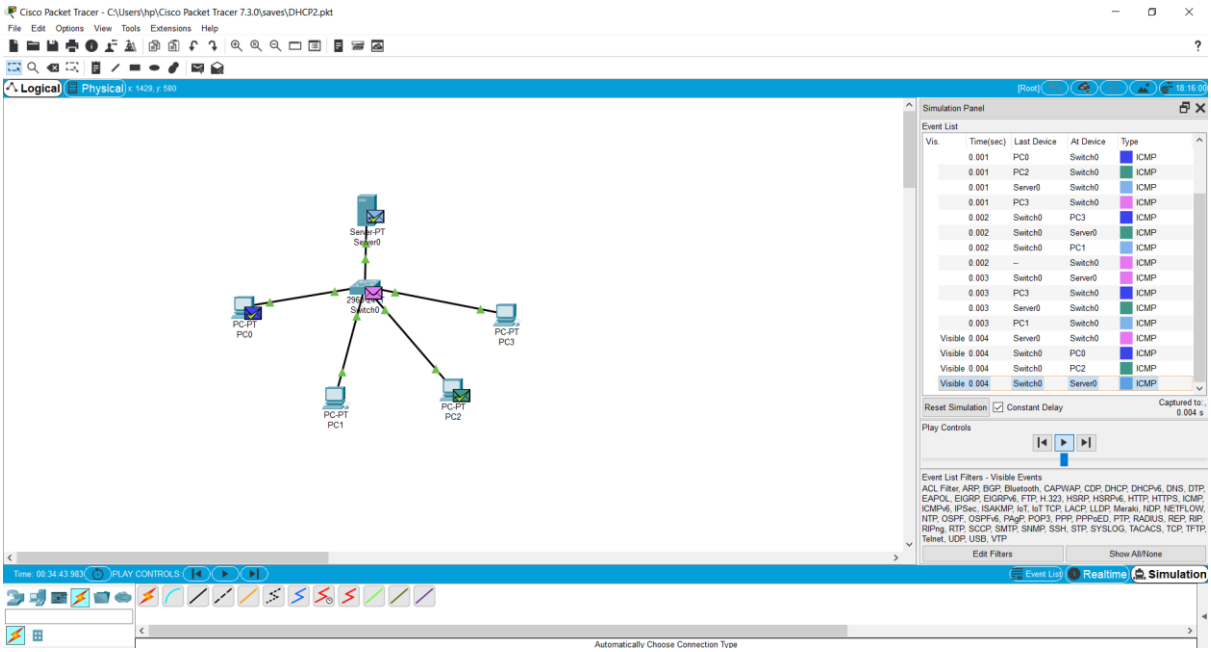
1. **Automatically Configuring the IP Addresses of End Devices using DHCP Protocols and Assigning the IP Address Default Gateway and DNS Server:**







2. Simulation of the Network:



Results and Conclusion: Automatic configuration of the IP Address of the end devices using DHCP protocol and assigning IP Address of Default Gateway and DNS Server has been done successfully.

Experiment 8

Date: 23-09-2021

Aim: To simulate the ARP protocol in the CISCO Packet Tracer.

Software Used: Cisco Packet Tracer.

Theory:

About ARP -

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

This mapping procedure is important because the lengths of the IP and MAC addresses differ, and a translation is needed so that the systems can recognize one another. The most used IP today is IP version 4 (IPv4). An IP address is 32 bits long. However, MAC addresses are 48 bits long. ARP translates the 32-bit address to 48 and vice versa.

There is a networking model known as the Open Systems Interconnection (OSI) model. First developed in the late 1970s, the OSI model uses layers to give IT teams a visualization of what is going on with a particular networking system. This can be helpful in determining which layer affects which application, device, or software installed on the network, and further, which IT or engineering professional is responsible for managing that layer.

The MAC address is also known as the data link layer, which establishes and terminates a connection between two physically connected devices so that data transfer can take place. The IP address is also referred to as the network layer or the layer responsible for forwarding packets of data through different routers. ARP works between these layers.

What Does ARP Do and How Does It Work?

When a new computer joins a local area network (LAN), it will receive a unique IP address to use for identification and communication.

Packets of data arrive at a gateway, destined for a particular host machine. The gateway, or the piece of hardware on a network that allows data to flow from one network to another, asks the ARP program to find a MAC address that matches the IP address. The ARP cache keeps a list of each IP address and its matching MAC address. The ARP cache is dynamic, but users on a network can also configure a static ARP table containing IP addresses and MAC addresses.

ARP caches are kept on all operating systems in an IPv4 Ethernet network. Every time a device requests a MAC address to send data to another device connected to the LAN, the device verifies its ARP cache to see if the IP-to-MAC-address connection has already been completed. If it exists, then a new request is unnecessary. However, if the translation has not yet been carried out, then the request for network addresses is sent, and ARP is performed.

An ARP cache size is limited by design, and addresses tend to stay in the cache for only a few minutes. It is purged regularly to free up space. This design is also intended for privacy and

security to prevent IP addresses from being stolen or spoofed by cyberattacks. While MAC addresses are fixed, IP addresses are constantly updated.

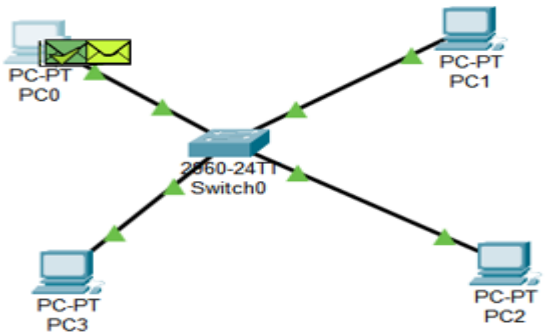
In the purging process, unutilized addresses are deleted; so is any data related to unsuccessful attempts to communicate with computers not connected to the network or that are not even powered on.

ARP in CISCO Packet Tracer –

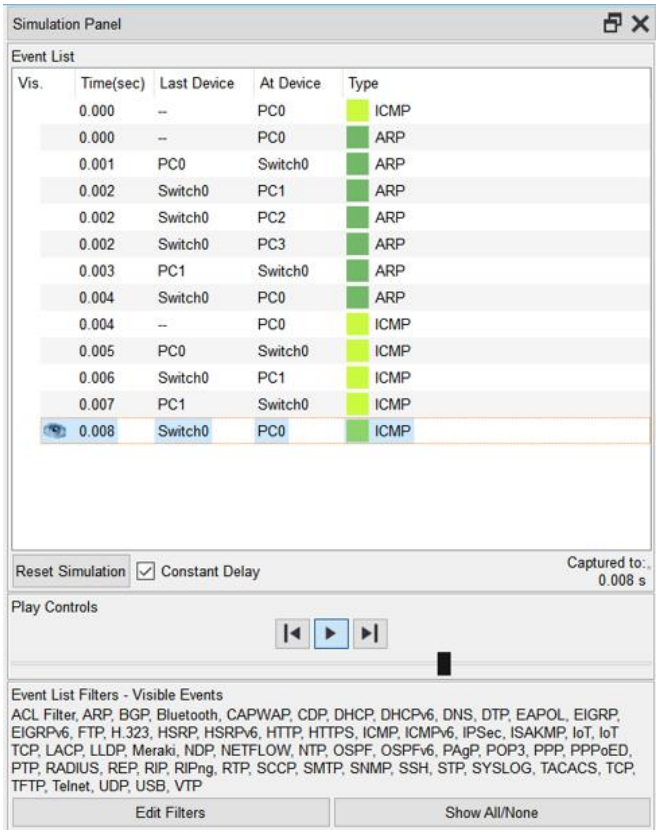
1. Make a sample network and assign IP addresses to the end devices.
2. Open the command prompt of any one of the PC that is **PC0** and open the **simulation mode** of cisco packet tracer.
3. To check for **ARP table**, enter **arp -a** command in command prompt initially you will see that there's no ARP entries showed.
4. Now, enter the **ping** command in the command prompt along with the destination IP address let's say we are taking the **IP address of PC4**, and press enter. You will see that in the Simulation Panel, there is a one packet which is **ICMP** and there is another package which is of an **ARP**.
5. Paly the simulation and observe the movement of an **ARP packet**. As soon as ARP packet gets acknowledged to the ***source PC*** that is a **PC0**, then pause the simulation and click on the **magnifying glass icon** on the on the left corner of the CISCO Packet Tracer and then right click on the source PC. A drop-down menu having the ARP table option will be shown. Click on the ARP table option, the **ARP table** consisting of the destination IP address and MAC address will be shown.
6. Replay the simulation so that all the packets will be transferred successfully. After that, in the command prompt of the source PC enter **arp -a** command and press enter you will see an **ARP table** having a **destination IP address** as well as a **MAC address** that is of **PC4.**

Observations:

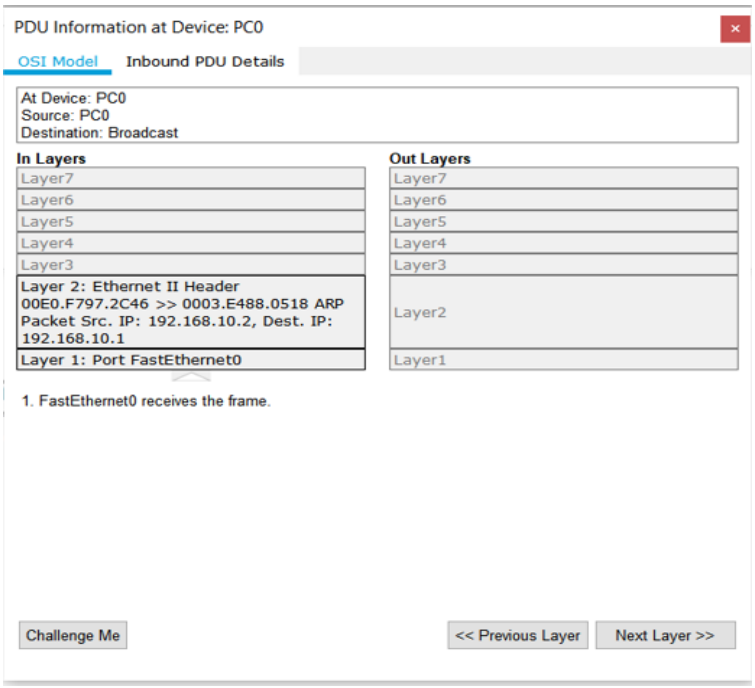
1. **Network Simulation:**



2. ARP Packet in Simulation Panel:

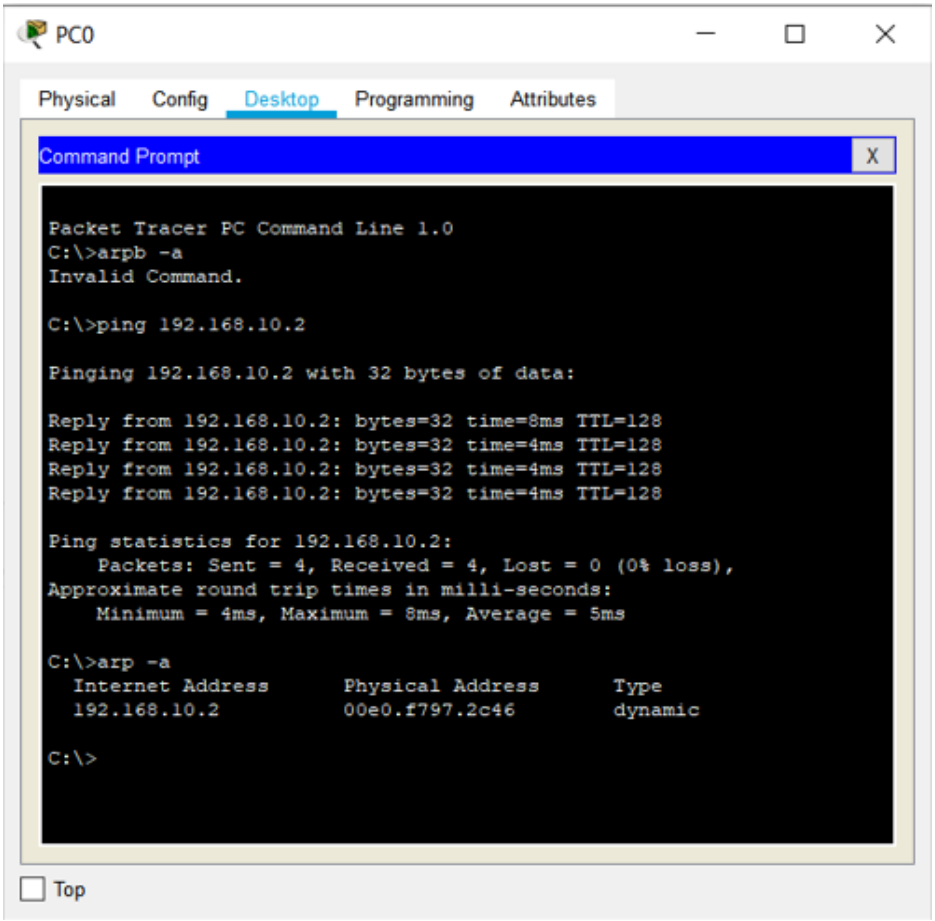


3. PDU Information at Source PC:



4. **ARP Table:**

5. **APR Table in Command Prompt:**



Results and Conclusion: The simulation of the ARP protocol in the CISCO Packet Tracer has been done successfully.

Experiment 9

Date: 07-10-2021

Aim: To explore about the commands related to router and perform router configuration in CISCO Packet Tracer.

Software Used: Cisco Packet Tracer.

Theory:

About Routers:

A router is a layer 3 device used to forward packet from one network to another. It forwards the packet through one of its port on the basis of destination IP address and the entry in the routing table. By using routing table, it finds an optimised path between the source and destination network.

Here, we will talk about Cisco router basic commands like assigning IP address to an interface, bringing up an interface, applying enable and secret password.

Administrative Configuration:

1. **Giving Hostname to Routers:** It is used to set a name to a device stating an identity to a device. This is important as these hostnames are used in WAN for authentication purpose. We can set the hostname as:

   router(config)#hostname GeeksforGeeksrouter

   GeeksforGeeksrouter(config)#

2. **Applying Banner:** These are specifically used to give a small security notice to the user who wants to access the router. We can customize it According to our need as like asking for credentials needed for the login.

   Types of banner are:

   1. ***banner motd:*** Here motd means message of the day and # means delimiter i.e message should end with the symbol provided. This message will be shown while entering into the router's user execution mode

      GeeksforGeeksrouter(config)#banner motd #

      Enter Text message. End with character '#'

      $ No unauthorised access allowed. Enter your credentials!! #

   2. ***Exec banner:*** It will be displayed on the screen when the user will login through the VTY lines.
   3. ***Login banner:*** This banner will be displayed after the banner motd but before the login.

   These banners are used to make login interactive.

3. **Setting password:** There are five passwords used to secure a cisco device:

1. ***enable password:*** The enable password is used for securing privilege mode. This password will be shown in clear text by command "show running-configuration". These are replaced by secret password nowadays.

   router(config)#enable password GeeksforGeeks

2. ***enable secret password:*** This is also used for securing privilege mode but the d the difference is that it will be displayed as cipher in "show running-configuration". This password will override the enable password if both passwords are set.

   router(config)#enable secret GeeksforGeeks

3. ***line console password:*** When a user will take access through console port then this password will be asked.

   router(config)#line console 0

   router(config-line)#password GeeksforGeeks

   router(config-line)#login

4. ***line VTY password:*** When a user want to access a router through VTY lines (telnet or ssh) then this password will be asked. Following configuration is shown for telnet password.

   router(config)#line VTY 0 4

   router(config-line)#password GeeksforGeeks

   router(config-line)#exit

5. ***auxiliary password:*** This password will secure the aux port.

   router(config)#line aux 0

   router(config-line)#password GeeksforGeeks

   router(config-line)#login

4. **Assigning IP address to a router's interface:** As we know router is a layer 3 device therefore every port of a router should have an IP address to work. By default, a router's port has no IP address and its line protocol is also down.

   router(config)#interface fa0/0

   router(config-if)#ip address 192.168.1.1 255.255.255.0

router(config-if)#no shut

Here first we have to specify the router's interface on which we want to give an IP address. Then we will enter interface mode where we will give an IP address as shown followed by its subnet mask (255.255.255.0). Then, we have made the router port administratively up by no shut command.

5. **Copying and erasing configuration:** We can manually copy the running-configuration (configuration in RAM) to startup-configuration (configuration in NVRAM). Therefore, when the next time router will boot up, it will load the configuration that we have copied (as by default the configuration of NVRAM is loaded).

   router#copy running-config startup-config

   To erase the configuration of NVRAM, use the command

   router#erase startup-config

Building a Basic Network from Router Configuration Commands:

1. Connect all the end devices with the switches and switches with the routers.
2. Provide IP Addresses and Default Gateway to the end devices.
3. Go to the router let's say go to Router 0 and connect WIC- 1T wire to it and configure router according to it by assigning the clock time and IP address to it and Default Gateway to it for Serial port and Fast Ethernet port. Do the same with other routers also.
4. Connect the routers with Serial DCE wire.
5. Do the rest of the router configuration and simulate the n/w.

Observations:

1. Router Configuration Commands:

Changing the hostname

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname shaina
shaina(config)#exit
shaina#
%SYS-5-CONFIG_I: Configured from console by console
```

Applying banner

```
shaina#config t
Enter configuration commands, one per line.  End with CNTL/Z.
shaina(config)#banner motd #
Enter TEXT message.  End with the character '#'.
No unauthorized access allowed. Enter your credentials!!#

shaina(config)#banner exec #
                      ^
% Invalid input detected at '^' marker.

shaina(config)#
```

For privilege mode

```
r1>en
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#enable secret password
r1(config)#
```

```
Welcome to the network.

r1>en
Password:
r1#
```

Line VTY password

```
r1>en
Password:
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#line vty 0 4
r1(config-line)#password pass@12
r1(config-line)#login
r1(config-line)#
```

Assigning IP Address for the ports

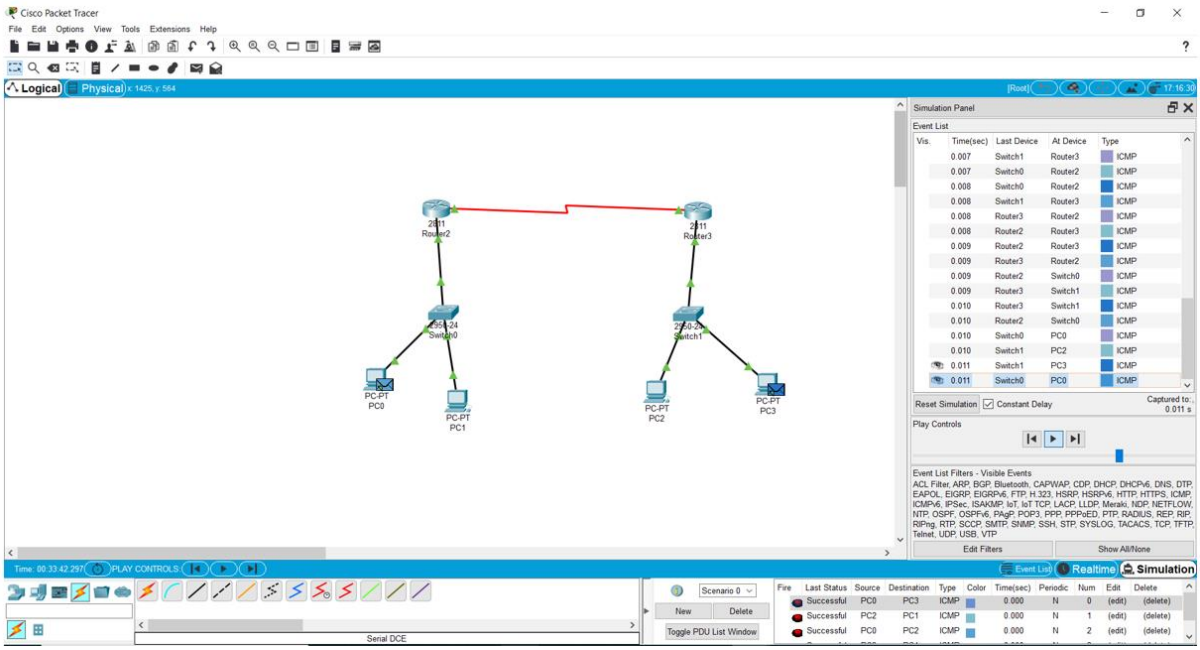
```
r1>en
Password:
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#
r1(config)#interface GigabitEthernet0/0/0
r1(config-if)#ip address 192.168.1.1 255.255.255.0
r1(config-if)#no shut

r1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
```

```
r1>en
Password:
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#
r1(config)#interface GigabitEthernet0/0/0
r1(config-if)#
r1(config-if)#exit
r1(config)#interface GigabitEthernet0/0/1
r1(config-if)#ip address 192.168.2.1 255.255.255.0
r1(config-if)#no shut

r1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
```

Testing telnet connection

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.5
Trying 192.168.1.5 ...Open
Welcome to the network.

Log onto the network.

User Access Verification

Password:
r1>en
Password:
r1#
```

2. Building and Simulation of N/W:



Results and Conclusion: Exploring about the commands related to router and perform router configuration in CISCO Packet Tracer has been done successfully.

Experiment 10

Date: 21-10-2021

Aim: To explore about Wireshark.

Software Used: Wireshark.

Theory:

About Wireshark:

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

One could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Purpose:

Here are some reasons people use Wireshark:

- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- QA engineers use it to verify network applications.
- Developers use it to debug protocol implementations.
- People use it to learn network protocol internals.

Wireshark can also be helpful in many other situations.

Features of Wireshark:

The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.
- …and a lot more!

However, to really appreciate its power you have to start using it.

What does Wireshark do?

Wireshark does three things:

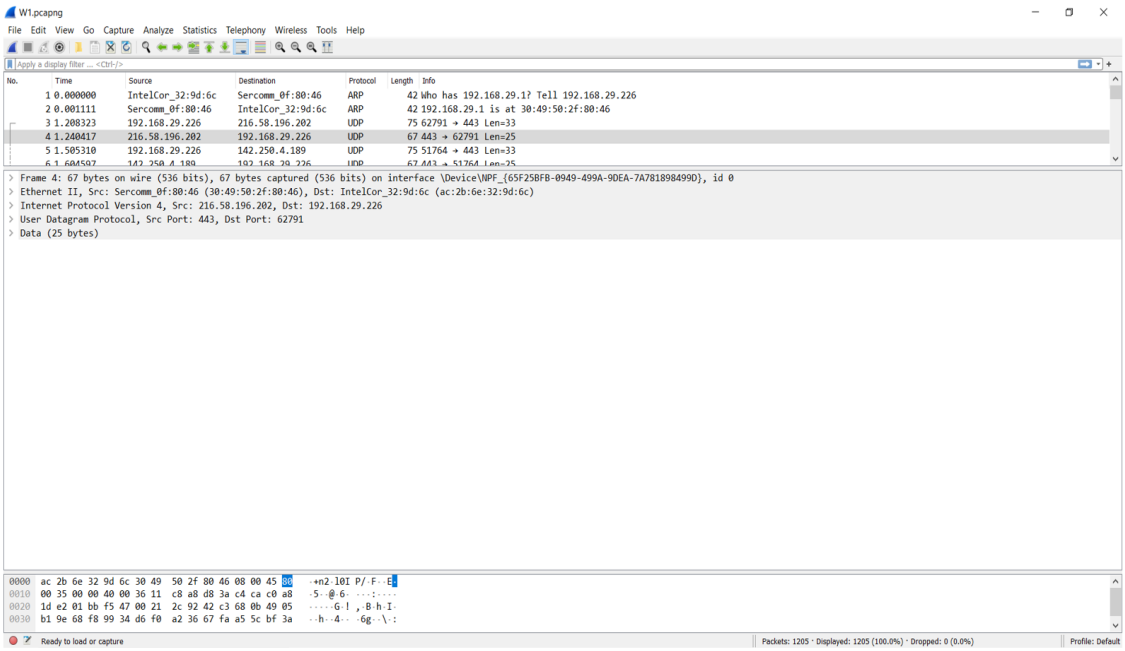
1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

Further Documentation: *For further documentation please refer to the link give below:*

https://www.wireshark.org/docs/wsug_html/#ChIntroWhatIs

Observations:

1. **Capturing of the Random Packet in Wireshark:**
   (a) Selection of Packet:



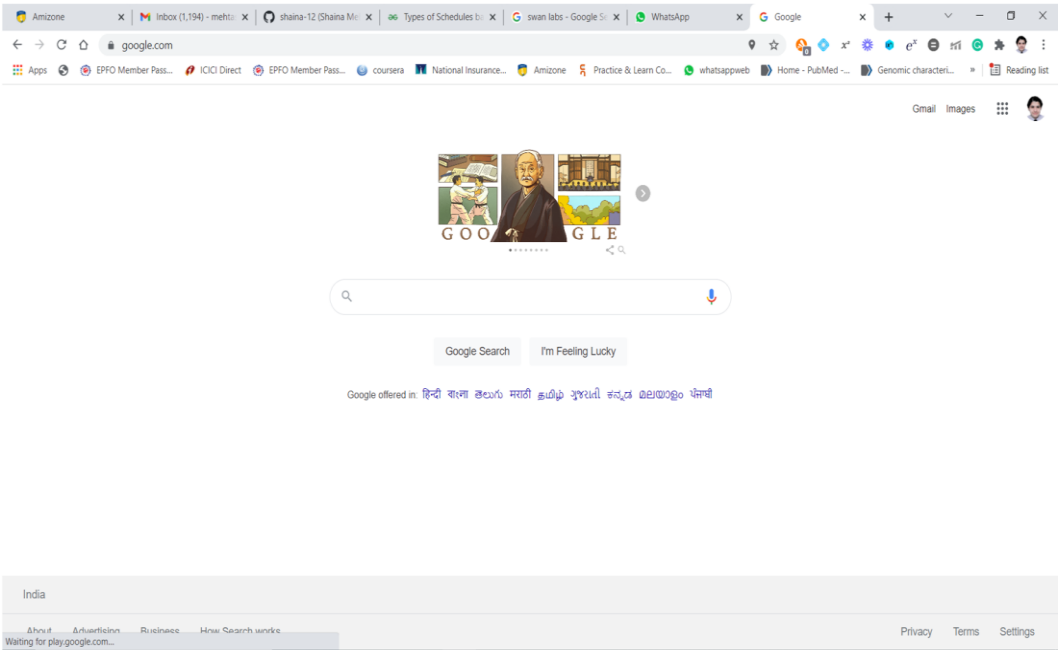
   (b) Examining of Different Layers of the Packet:

```
Frame 4: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D}, id 0
  > Interface id: 0 (\Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 28, 2021 10:34:30.975108000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1635397470.975108000 seconds
    [Time delta from previous captured frame: 0.032094000 seconds]
    [Time delta from previous displayed frame: 0.032094000 seconds]
    [Time since reference or first frame: 1.240417000 seconds]
    Frame Number: 4
    Frame Length: 67 bytes (536 bits)
    Capture Length: 67 bytes (536 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

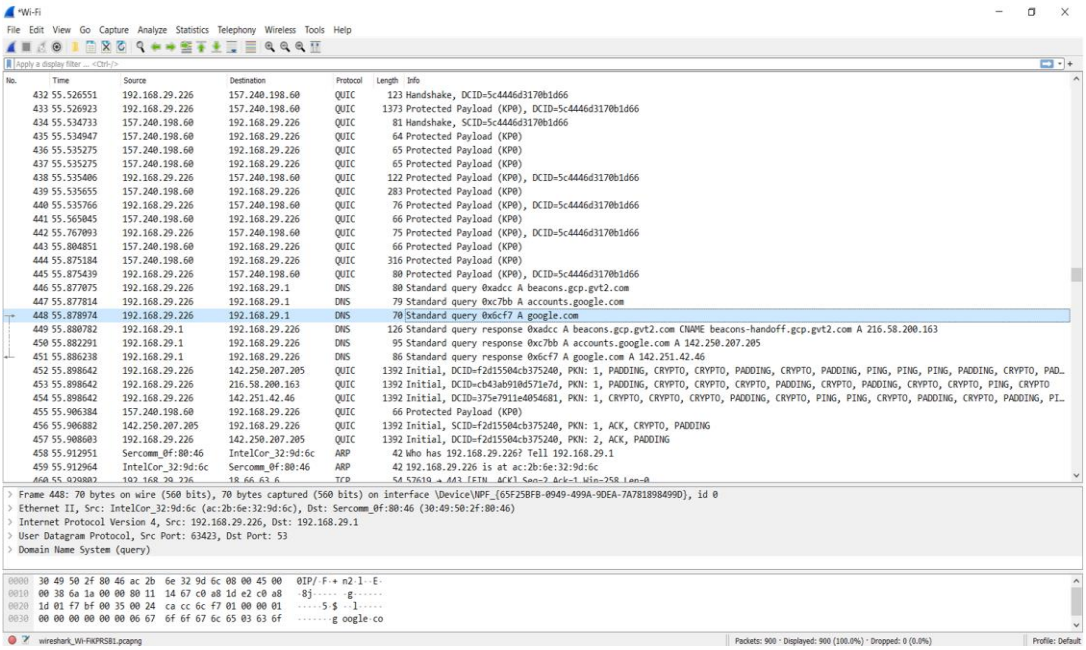
```
Ethernet II, Src: Sercomm_0f:80:46 (30:49:50:2f:80:46), Dst: IntelCor_32:9d:6c (ac:2b:6e:32:9d:6c)
  Destination: IntelCor_32:9d:6c (ac:2b:6e:32:9d:6c)
       Address: IntelCor_32:9d:6c (ac:2b:6e:32:9d:6c)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Sercomm_0f:80:46 (30:49:50:2f:80:46)
       Address: Sercomm_0f:80:46 (30:49:50:2f:80:46)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 216.58.196.202, Dst: 192.168.29.226
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)
       1000 00.. = Differentiated Services Codepoint: Class Selector 4 (32)
       .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 53
    Identification: 0x0000 (0)
  Flags: 0x40, Don't fragment
       0... .... = Reserved bit: Not set
       .1.. .... = Don't fragment: Set
       ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 54
    Protocol: UDP (17)
    Header Checksum: 0xc8a8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 216.58.196.202
    Destination Address: 192.168.29.226
User Datagram Protocol, Src Port: 443, Dst Port: 62791
    Source Port: 443
    Destination Port: 62791
    Length: 33
    Checksum: 0x2c92 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  [Timestamps]
       [Time since first frame: 0.032094000 seconds]
       [Time since previous frame: 0.032094000 seconds]
    UDP payload (25 bytes)
Data (25 bytes)
    Data: 42c3680b4905b19e68f89934d6f0a23667faa55cbf3a8c2de7
    [Length: 25]
```

2. Capturing of the Website Packet in Wireshark:

(a) Screenshot of Website:



(b) Selection of the Packet:



(c) Examining of Different Layers of the Packet:

```
Frame 448: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D}, id 0
  Interface id: 0 (\Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D})
      Interface name: \Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D}
      Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 28, 2021 10:55:03.718010000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1635398703.718010000 seconds
  [Time delta from previous captured frame: 0.001160000 seconds]
  [Time delta from previous displayed frame: 0.001160000 seconds]
  [Time since reference or first frame: 55.878974000 seconds]
  Frame Number: 448
  Frame Length: 70 bytes (560 bits)
  Capture Length: 70 bytes (560 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
```

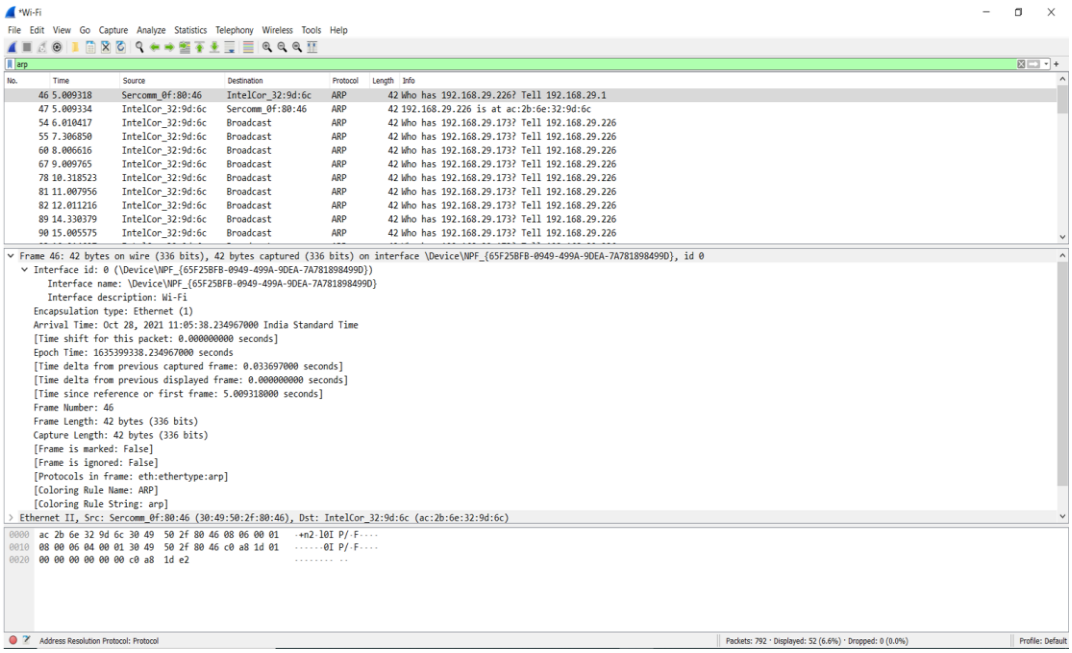
```
▾ Ethernet II, Src: IntelCor_32:9d:6c (ac:2b:6e:32:9d:6c), Dst: Sercomm_0f:80:46 (30:49:50:2f:80:46)
  ▾ Destination: Sercomm_0f:80:46 (30:49:50:2f:80:46)
      Address: Sercomm_0f:80:46 (30:49:50:2f:80:46)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_32:9d:6c (ac:2b:6e:32:9d:6c)
      Address: IntelCor_32:9d:6c (ac:2b:6e:32:9d:6c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.29.226, Dst: 192.168.29.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x6a1a (27162)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x1467 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.29.226
    Destination Address: 192.168.29.1
▾ User Datagram Protocol, Src Port: 63423, Dst Port: 53
    Source Port: 63423
    Destination Port: 53
    Length: 36
    Checksum: 0xcacc [unverified]
    [Checksum Status: Unverified]
    [Stream index: 15]
  ▾ [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
    UDP payload (28 bytes)
```

```
Domain Name System (query)
    Transaction ID: 0x6cf7
  Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > google.com: type A, class IN
    [Response In: 451]
```

3. Filtering and Capturing of Packet in Wireshark:

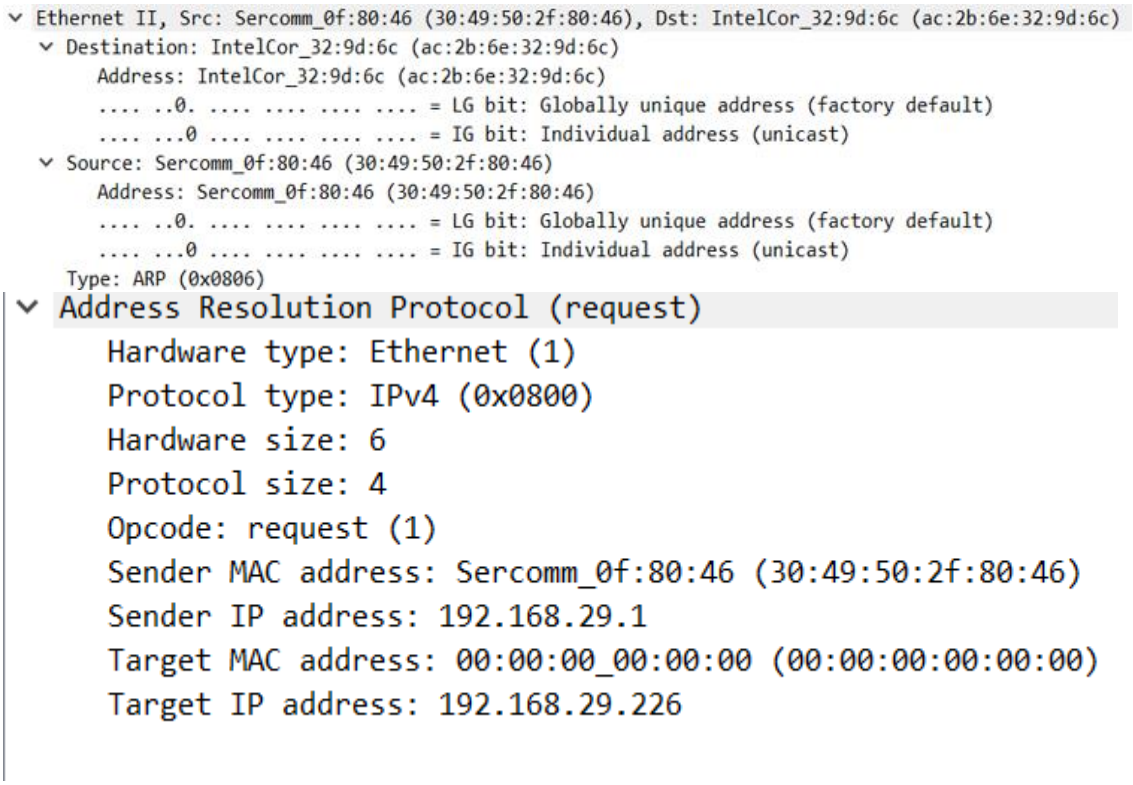
(a) Selection of the Packet:

(Here I have Selected ARP Packet)



(b) Examining of Different Layers of the Packet:

```
Frame 46: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D}, id 0
  Interface id: 0 (\Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D})
      Interface name: \Device\NPF_{65F25BFB-0949-499A-9DEA-7A781898499D}
      Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 28, 2021 11:05:38.234967000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1635399338.234967000 seconds
    [Time delta from previous captured frame: 0.033697000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 5.009318000 seconds]
    Frame Number: 46
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
```



Results and Conclusion: The exploration of Wireshark has been done successfully.

Experiment 11

Date: 28-10-2021

Aim: To capture and analyse TCP and UDP packets in Wireshark.

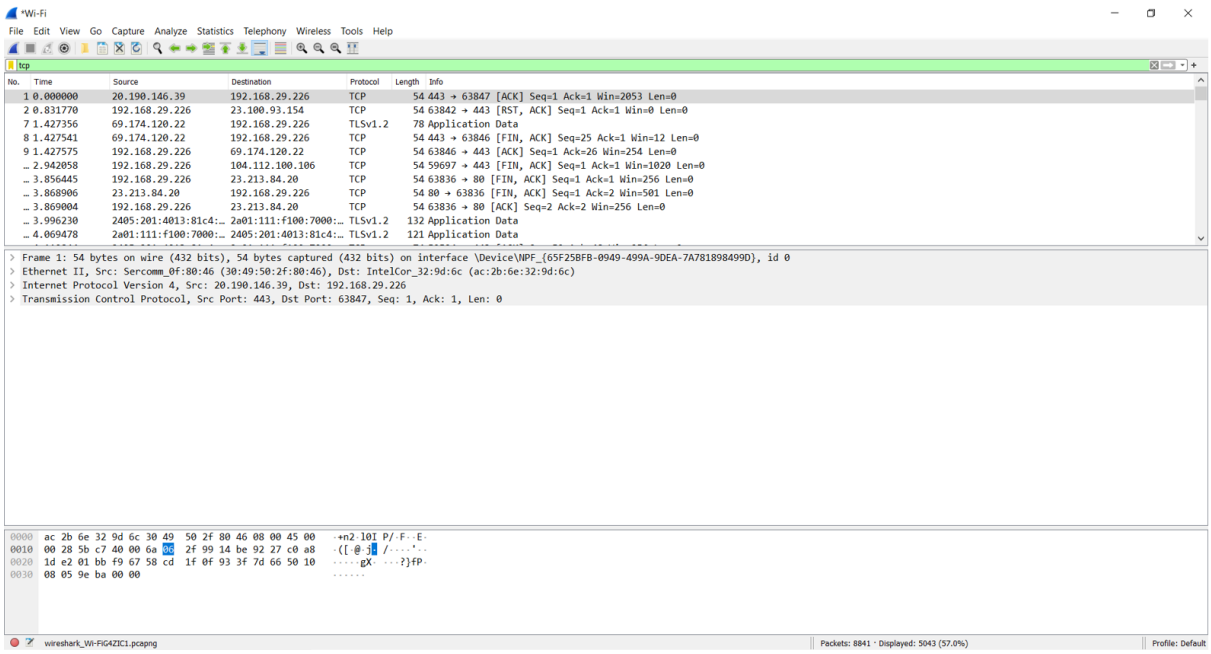
Software Used: Wireshark.

Theory:

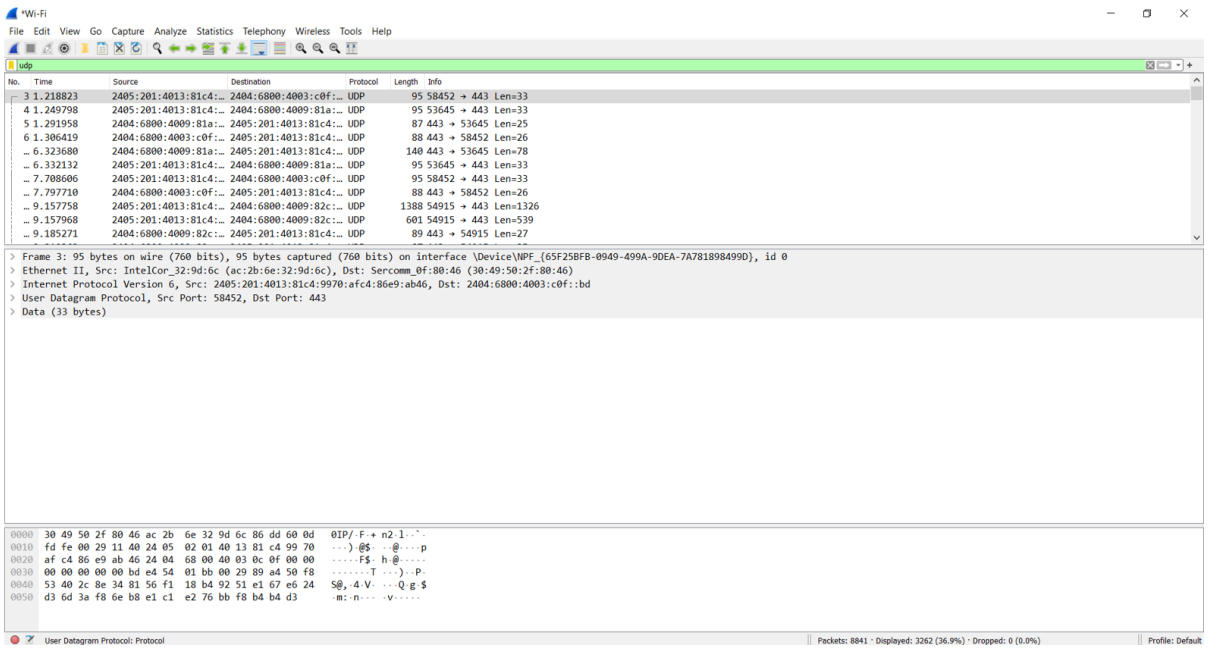
- **TCP:** Transmission Control Protocol (TCP) is a standard that defines how to establish and maintain a network conversation by which applications can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.
- **UDP:** User Datagram Protocol (UDP) is a communications protocol that is primarily used to establish low-latency and loss-tolerating connections between applications on the internet. UDP speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.

Observations:

TCP:



UDP:



Results and Conclusion: The capturing and analysis of TCP and UDP packets in Wireshark has been done successfully.

Experiment 12

Date: 28-10-2021

Aim: To capture and analyse DNS query and ICMP packets in Wireshark.

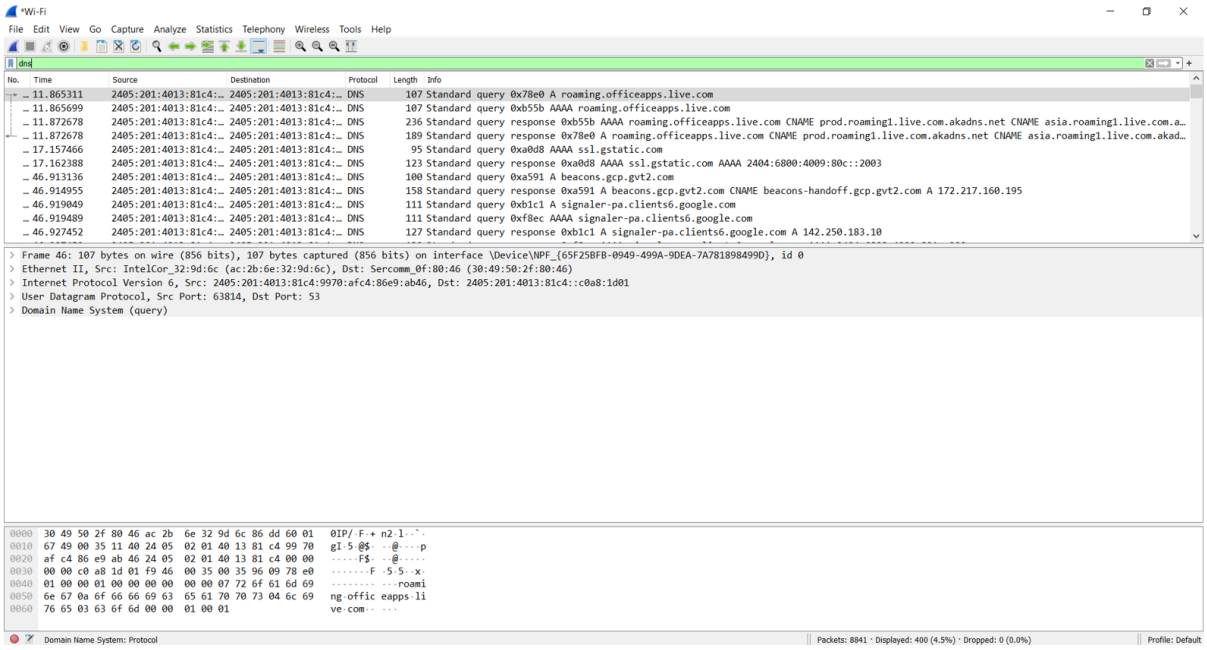
Software Used: Wireshark.

Theory:

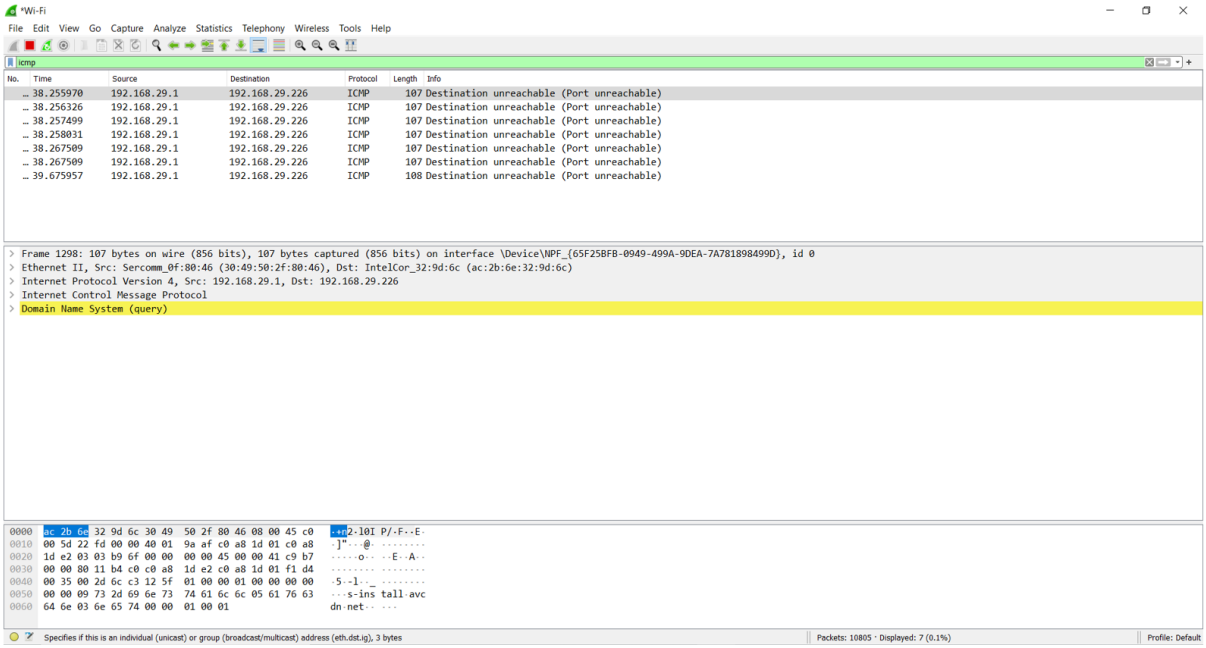
- **DNS:** The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.
- **ICMP:** The Internet Control Message Protocol (ICMP) is a protocol that devices within a network use to communicate problems with data transmission. In this ICMP definition, one of the primary ways in which ICMP is used is to determine if data is getting to its destination and at the right time.

Observations:

DNS:



ICMP:



Results and Conclusion: The capturing and analysis of DNS query and ICMP packets in Wireshark has been done successfully.