Darshan Institute of Engineering & Technology

Certificate

This is to certify that

Mr./Miss_____

Enrolment No. _____, B.Tech. CSE Semester 5th has satisfactorily completed the course in the Subject *Computer Networks (2301CS501)* in this Institute.

Submission Date: ___/___/_____

Staff in Charge **Program Coordinator**

_____ **_____**

Index

Sr.	Title	Date	Sign
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

Date: 13/06/2024

Lab Practical #01:

Study of basic networking commands and IP configuration.

Practical Assignment #01:

1. Perform and explain various networking commands listed below:
   i. ipconfig
   ii. ping
   iii. getmac
   iv. systeminfo
   v. traceroute / tracert
   vi. netstat
   vii. nslookup
   viii. hostname
   ix. pathping
   x. arp

1. ipconfig

Description:

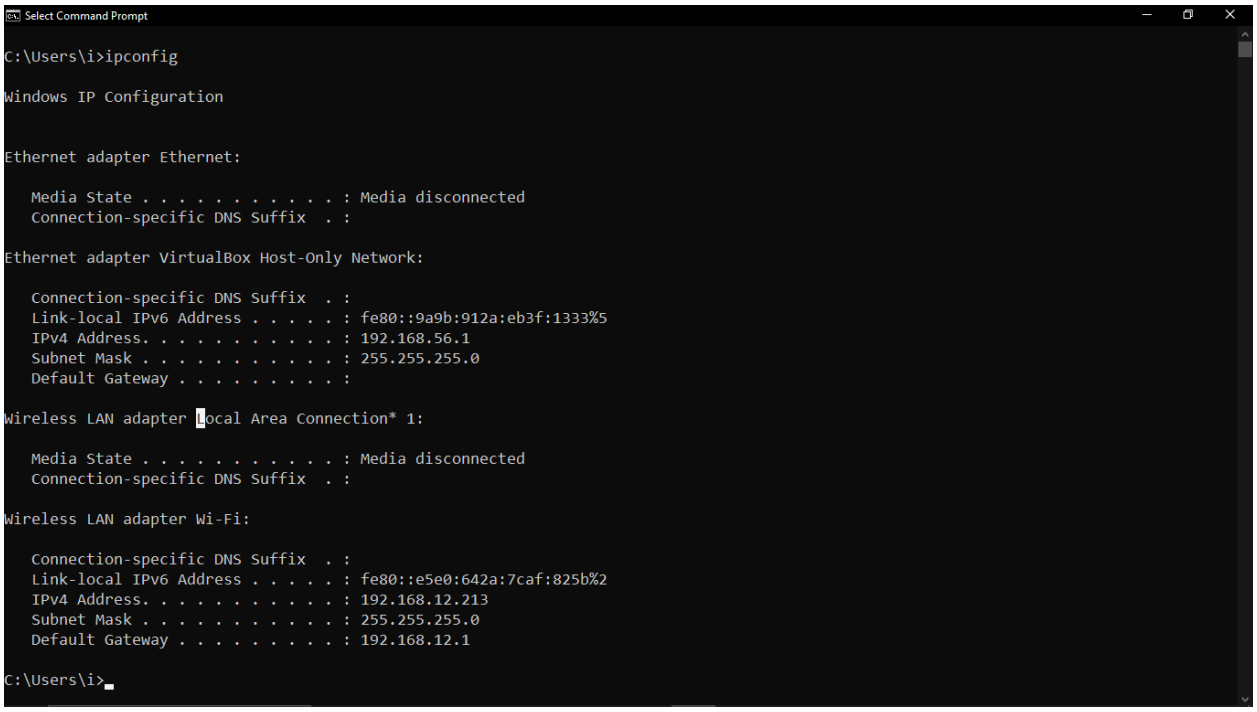
ipconfig is a command-line utility in Windows operating systems used to display and manage the network configuration of a computer. It provides details about the IP address, subnet mask, default gateway, and other network information for each network adapter. Additionally, it allows users to release and renew DHCP-assigned IP addresses and manage DNS settings.

No.	Option	Description
1	/all	Display full configuration information.
2	/renew	Renew the IPv4 address for the specified adapter.
3	/release	Release the IPv4 address for the specified adapter.
4	/displaydns	Display the contents of the DNS Resolver Cache.
5	/flushdns	Purges the DNS Resolver cache.

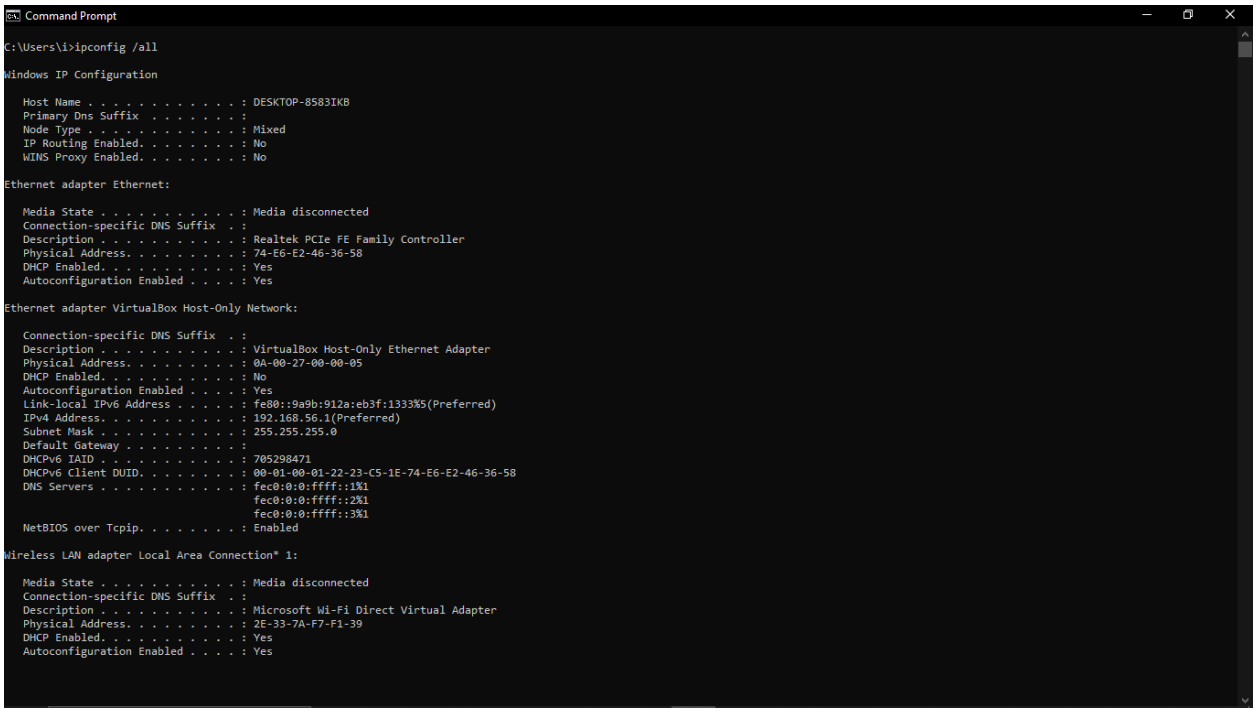
Implementation:

Date: 13/06/2024

- ipconfig

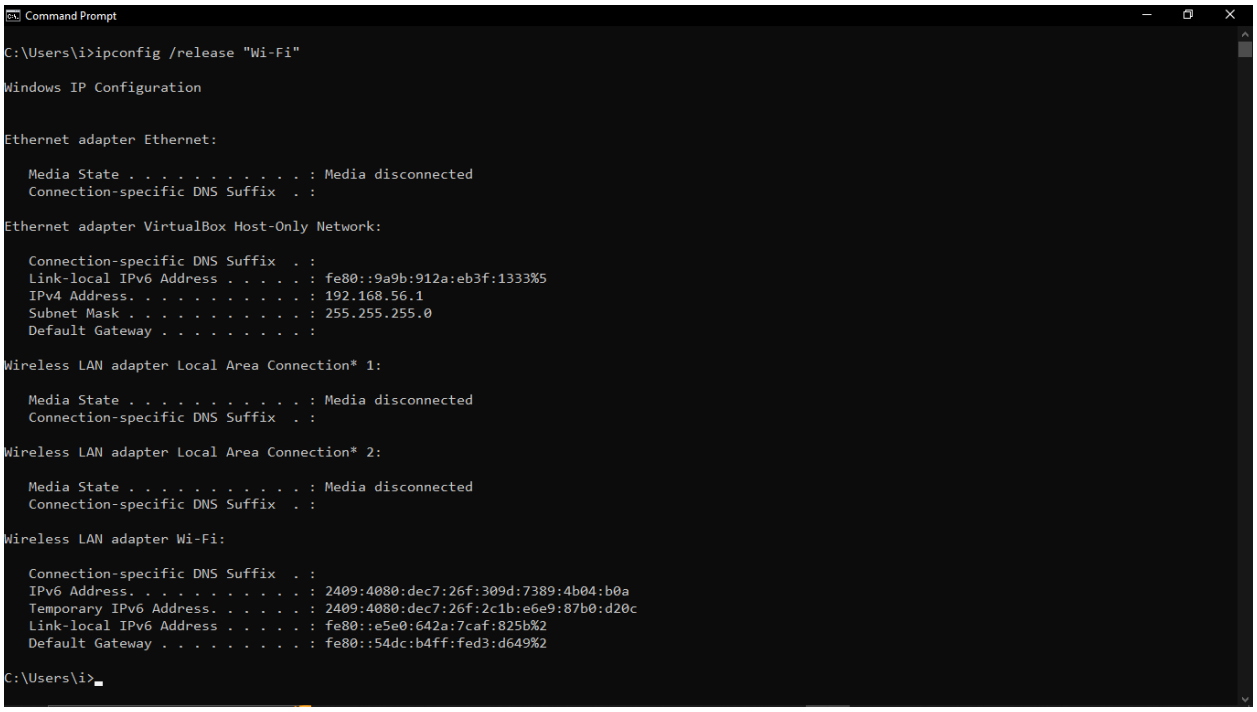


- ipconfig /all

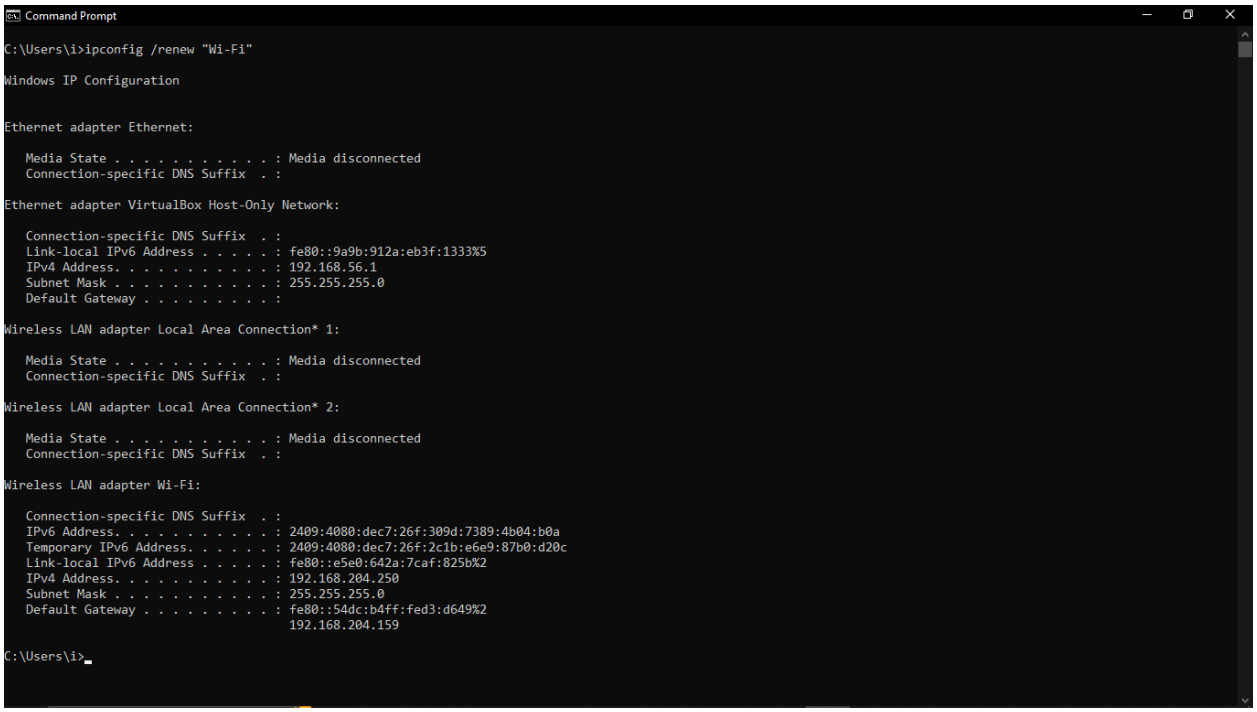


Date: 13/06/2024

- ipconfig /release

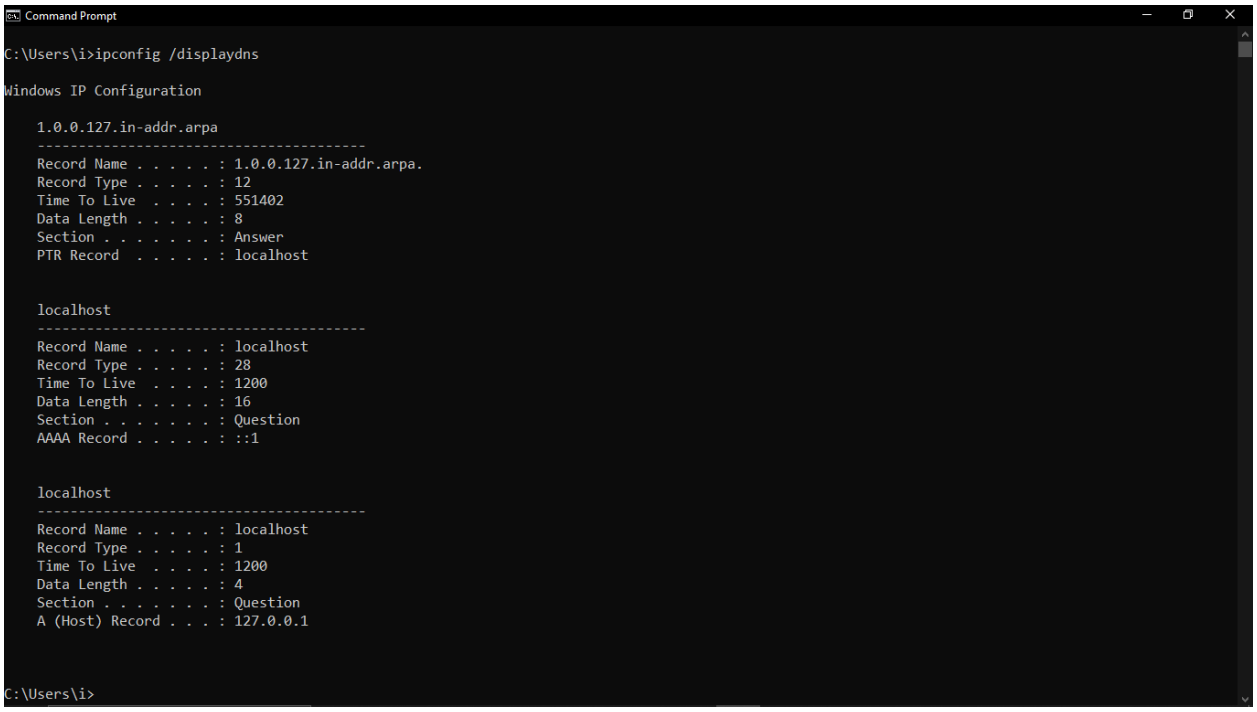


- ipconfig /renew

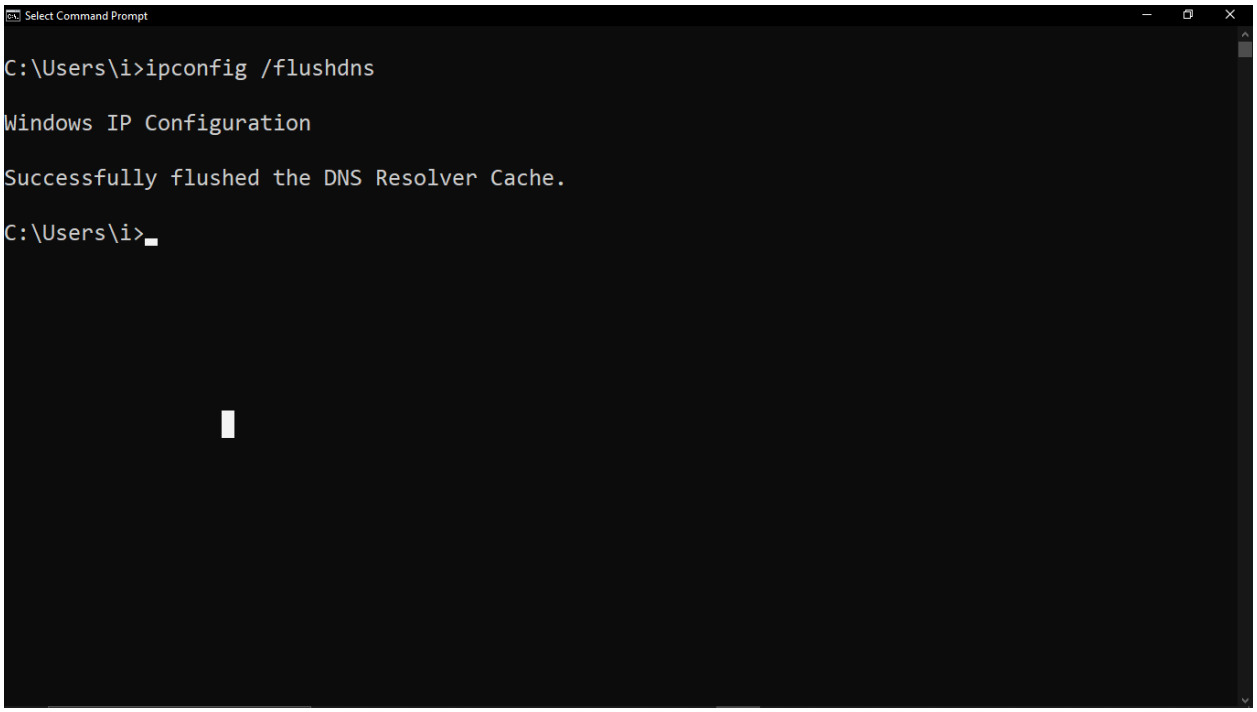


Date: 13/06/2024

- ipconfig /displaydns



- ipconfig /flushdns



Date: 13/06/2024

2. ping

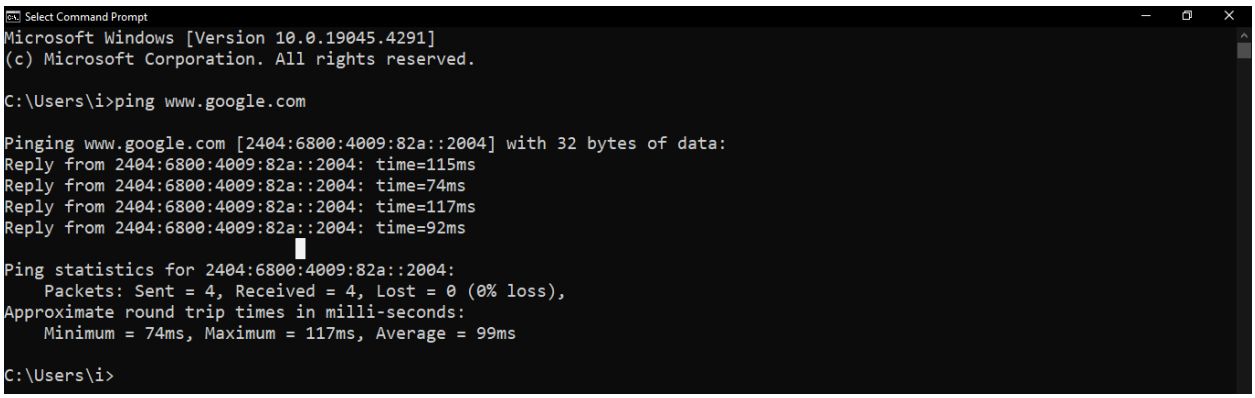
Description:

The ping command is a network utility used to test the reachability of a host on an IP network. It also measures the round-trip time for messages sent from the originating host to a destination computer. This command is useful for diagnosing network connectivity issues.

No.	Option	Description
1	-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break. To stop - type Control-C.
2	-n count	Number of echo requests to send.
3	-l size	Send buffer size.
4	-4	Force using IPv4.
5	-i TTL	Time To Live.

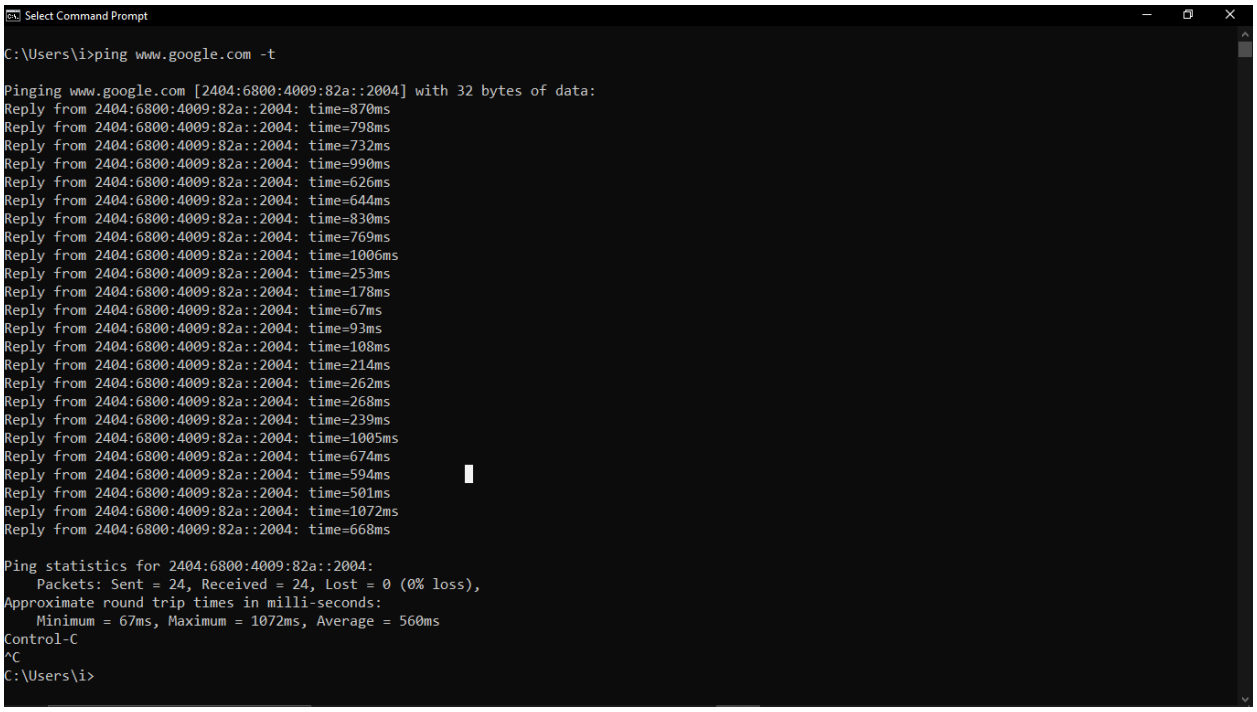
Implementation:

- ping www.google.com

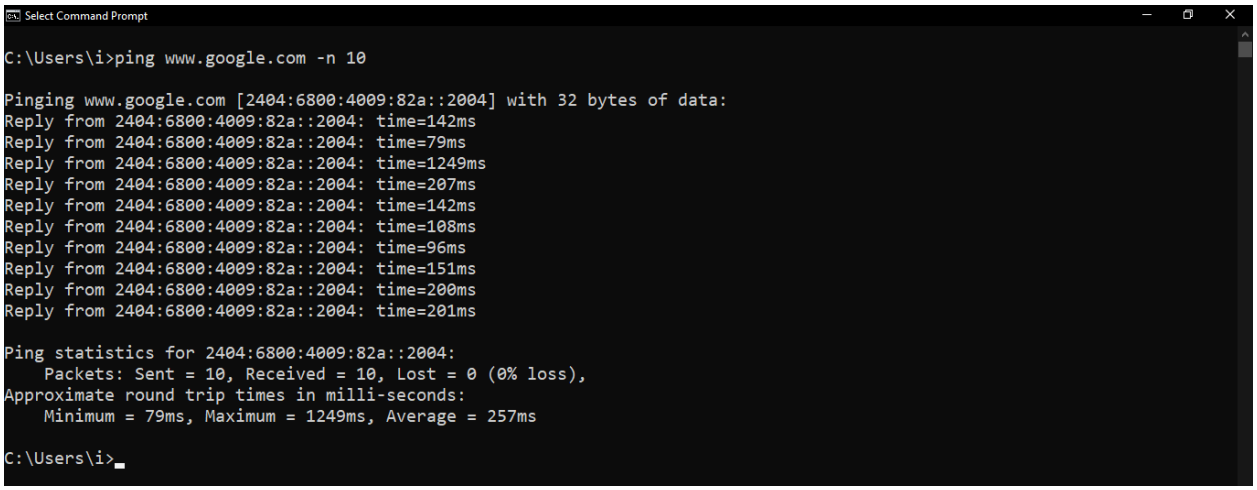


Date: 13/06/2024

- ping www.google.com -t



- ping www.google.com –n 10



Date: 13/06/2024

- ping www.google.com –l 1000

```
Command Prompt

C:\Users\i>ping www.google.com -l 1000

Pinging www.google.com [2404:6800:4009:827::2004] with 1000 bytes of data:
Reply from 2404:6800:4009:827::2004: time=844ms
Reply from 2404:6800:4009:827::2004: time=130ms
Reply from 2404:6800:4009:827::2004: time=124ms
Reply from 2404:6800:4009:827::2004: time=136ms

Ping statistics for 2404:6800:4009:827::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 124ms, Maximum = 844ms, Average = 308ms

C:\Users\i>
```

- ping www.google.com -4

```
Command Prompt

C:\Users\i>ping www.google.com -4

Pinging www.google.com [142.250.192.4] with 32 bytes of data:
Reply from 142.250.192.4: bytes=32 time=68ms TTL=54
Reply from 142.250.192.4: bytes=32 time=57ms TTL=54
Reply from 142.250.192.4: bytes=32 time=87ms TTL=54
Reply from 142.250.192.4: bytes=32 time=87ms TTL=54

Ping statistics for 142.250.192.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 87ms, Average = 74ms

C:\Users\i>
```

- ping -i 4 www.google.com

```
Command Prompt

C:\Users\i>ping -i 4 www.google.com

Pinging www.google.com [2404:6800:4009:827::2004] with 32 bytes of data:
Reply from 2404:6800:4009:827::2004: TTL expired in transit.
Reply from 2404:6800:4009:827::2004: TTL expired in transit.
Reply from 2404:6800:4009:827::2004: TTL expired in transit.
Reply from 2404:6800:4009:827::2004: TTL expired in transit.

Ping statistics for 2404:6800:4009:827::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\i>
```

Date: 13/06/2024

3. getmac

Description:

The getmac command is a command-line utility in Windows operating systems that displays the MAC addresses for network adapters on the system. The MAC address, or Media Access Control address, is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.

No.	Option	Description
1	/S system	Specifies the remote system to connect to.
2	/U [domain\]user	Specifies the user context under which the command should execute.
3	/V	Specifies that verbose output is displayed.
4	/FO format	Specifies the format in which the output is to be displayed.Valid values: "TABLE", "LIST", "CSV".
5	/NH	Specifies that the "Column Header" should not be displayed in the output.Valid only for TABLE and CSV formats.

Implementation:

- getmac

```
Command Prompt

C:\Users\i>getmac

Physical Address    Transport Name
=================== ============================================================
74-E6-E2-46-36-58   Media disconnected
2C-33-7A-F7-F1-39   \Device\Tcpip_{0134B6F2-3C30-41CE-A536-B0AAA0B9DD21}
0A-00-27-00-00-05   \Device\Tcpip_{2869F44D-AA1B-4915-8B00-7D9D61D6B283}

C:\Users\i>
```

- getmac /FO TABLE

```
Command Prompt

C:\Users\i>getmac /FO TABLE

Physical Address    Transport Name
=================== ============================================================
74-E6-E2-46-36-58   \Device\Tcpip_{DAC633D5-8A98-42B8-B678-927F03F8F244}
2C-33-7A-F7-F1-39   Media disconnected
2E-33-7A-F7-F9-39   \Device\Tcpip_{1EB77F20-4859-4C2B-9E65-462798A34EF7}
0A-00-27-00-00-05   \Device\Tcpip_{2869F44D-AA1B-4915-8B00-7D9D61D6B283}

C:\Users\i>
```

Date: 13/06/2024

- getmac /FO LIST

```
Command Prompt

C:\Users\i>getmac /FO LIST

Physical Address: 74-E6-E2-46-36-58
Transport Name:   \Device\Tcpip_{DAC633D5-8A98-42B8-B678-927F03F8F244}

Physical Address: 2C-33-7A-F7-F1-39
Transport Name:   Media disconnected

Physical Address: 2E-33-7A-F7-F9-39
Transport Name:   \Device\Tcpip_{1EB77F20-4859-4C2B-9E65-462798A34EF7}

Physical Address: 0A-00-27-00-00-05
Transport Name:   \Device\Tcpip_{2869F44D-AA1B-4915-8B00-7D9D61D6B283}

C:\Users\i>
```

- getmac /FO CSV

```
Command Prompt

C:\Users\i>getmac /FO CSV
"Physical Address","Transport Name"
"74-E6-E2-46-36-58","\Device\Tcpip_{DAC633D5-8A98-42B8-B678-927F03F8F244}"
"2C-33-7A-F7-F1-39","Media disconnected"
"2E-33-7A-F7-F9-39","\Device\Tcpip_{1EB77F20-4859-4C2B-9E65-462798A34EF7}"
"0A-00-27-00-00-05","\Device\Tcpip_{2869F44D-AA1B-4915-8B00-7D9D61D6B283}"

C:\Users\i>
```

- getmac /FO CSV /NH

```
Command Prompt

C:\Users\i>getmac /FO CSV /NH
"74-E6-E2-46-36-58","\Device\Tcpip_{DAC633D5-8A98-42B8-B678-927F03F8F244}"
"2C-33-7A-F7-F1-39","Media disconnected"
"2E-33-7A-F7-F9-39","\Device\Tcpip_{1EB77F20-4859-4C2B-9E65-462798A34EF7}"
"0A-00-27-00-00-05","\Device\Tcpip_{2869F44D-AA1B-4915-8B00-7D9D61D6B283}"

C:\Users\i>
```

- getmac /v

```
Command Prompt

C:\Users\i>getmac /v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== ================== ============================================================
Ethernet        Realtek PCIe FE 74-E6-E2-46-36-58   Media disconnected
Wi-Fi           Dell Wireless 1 2C-33-7A-F7-F1-39   \Device\Tcpip_{0134B6F2-3C30-41CE-A536-B0AAA0B9DD21}
Local Area Conn Microsoft Wi-Fi 2E-33-7A-F7-F9-39   Media disconnected
VirtualBox Host VirtualBox Host 0A-00-27-00-00-05   \Device\Tcpip_{2869F44D-AA1B-4915-8B00-7D9D61D6B283}

C:\Users\i>
```

Date: 13/06/2024

4. systeminfo

Description:

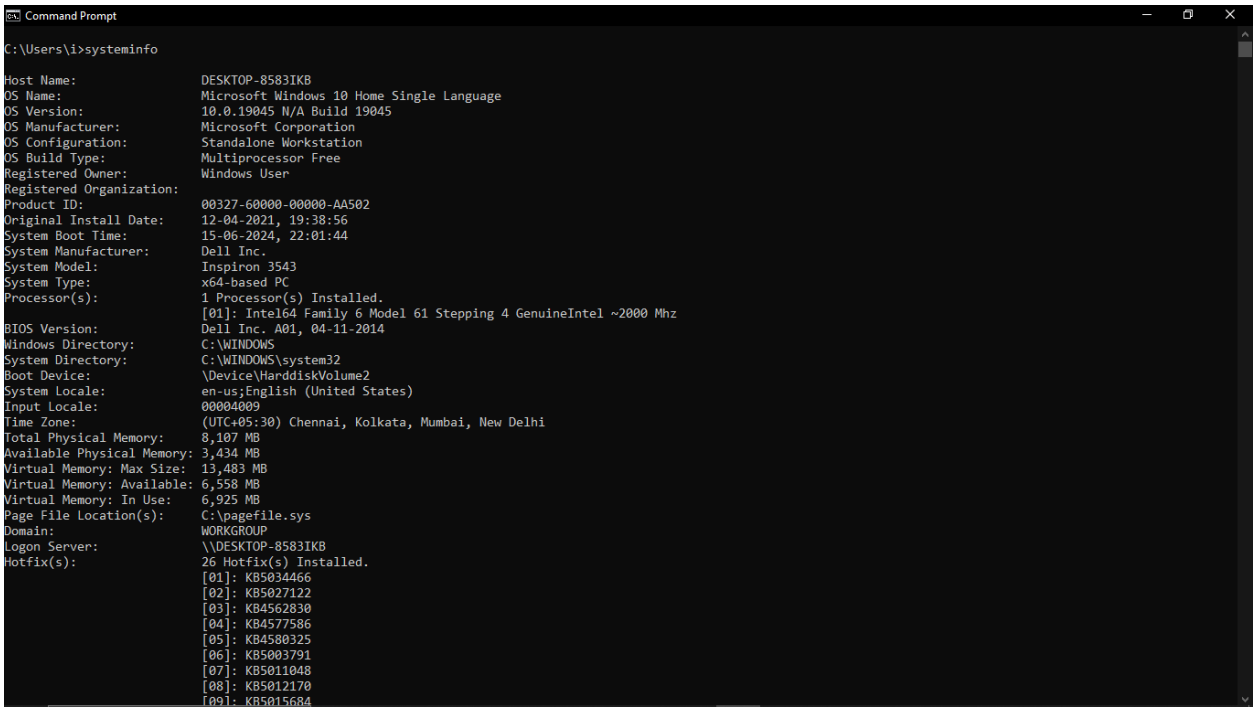
`systeminfo` is a command-line utility in Microsoft Windows that provides detailed information about the system's configuration. It gathers and displays various parameters related to the operating system, hardware, and software environment

No.	Option	Description
1	/S system	Specifies the remote system to connect to.
2	/U [domain\]user	Specifies the user context under which the command should execute.
3	/P [password]	Specifies the password for the given user context. Prompts for input if omitted.
4	/FO format	Specifies the format in which the output is to be displayed.Valid values: "TABLE", "LIST", "CSV".
5	/NH	Specifies that the "Column Header" should not be displayed in the output. Valid only for "TABLE" and "CSV" formats.

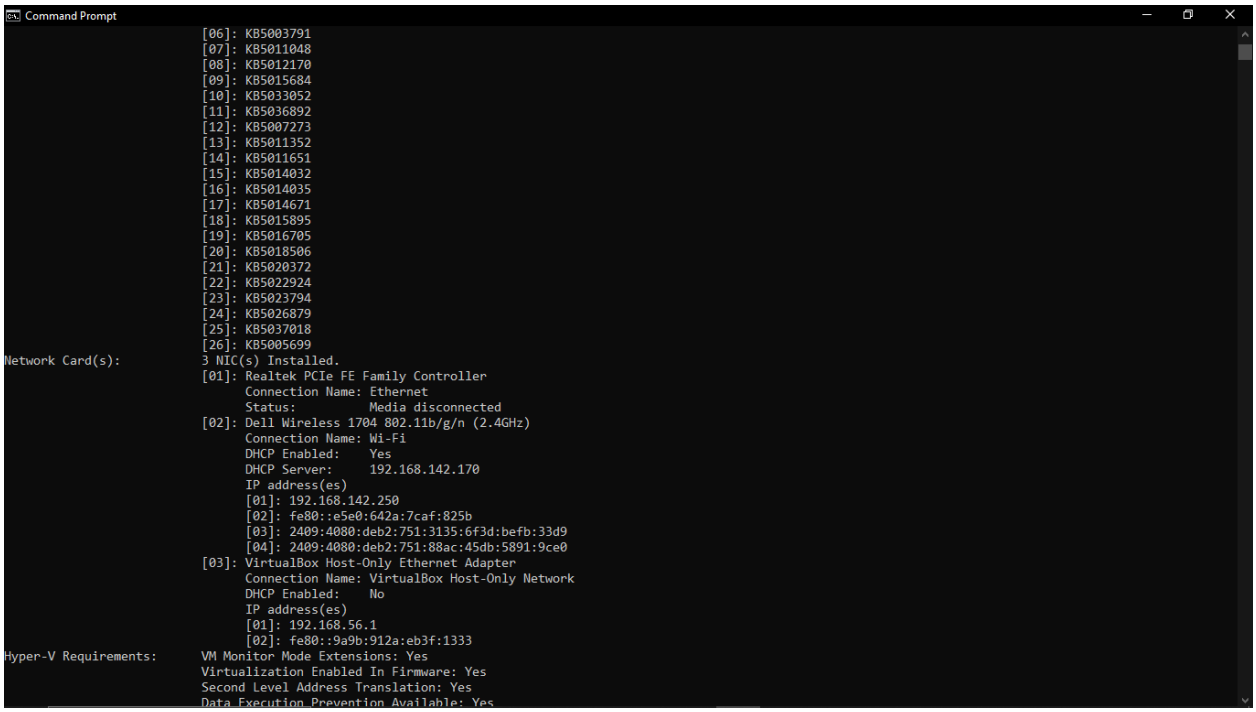
Implementation:

Date: 13/06/2024

- systeminfo



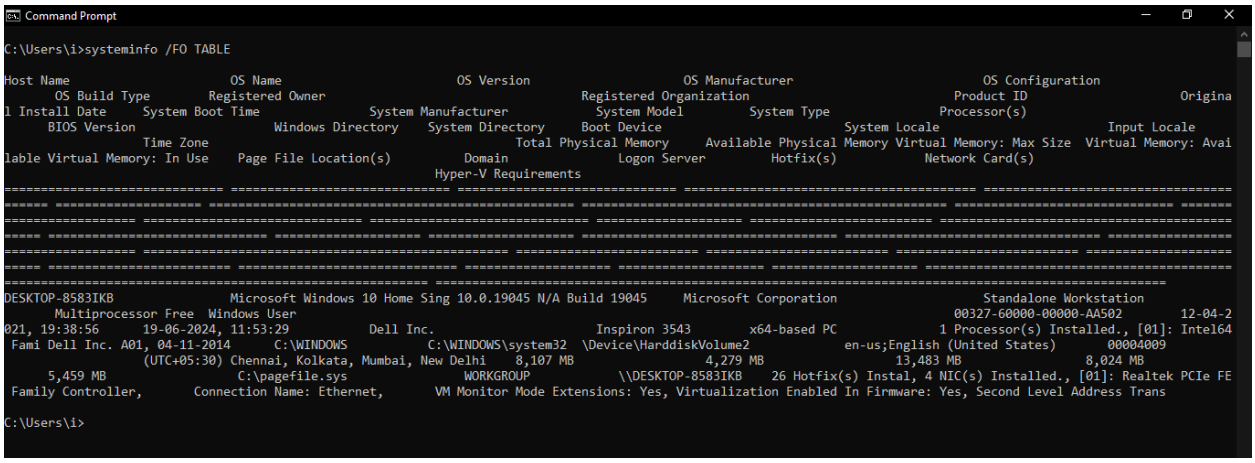
```
Command Prompt

C:\Users\i>systeminfo

Host Name:                 DESKTOP-8583IKB
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00327-60000-00000-AA502
Original Install Date:     12-04-2021, 19:38:56
System Boot Time:          15-06-2024, 22:01:44
System Manufacturer:       Dell Inc.
System Model:              Inspiron 3543
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 61 Stepping 4 GenuineIntel ~2000 Mhz
BIOS Version:              Dell Inc. A01, 04-11-2014
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,107 MB
Available Physical Memory: 3,434 MB
Virtual Memory: Max Size:  13,483 MB
Virtual Memory: Available: 6,558 MB
Virtual Memory: In Use:    6,925 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-8583IKB
Hotfix(s):                 26 Hotfix(s) Installed.
                           [01]: KB5034466
                           [02]: KB5027122
                           [03]: KB4562830
                           [04]: KB4577586
                           [05]: KB4580325
                           [06]: KB5003791
                           [07]: KB5011048
                           [08]: KB5012170
                           [09]: KB5015684
```



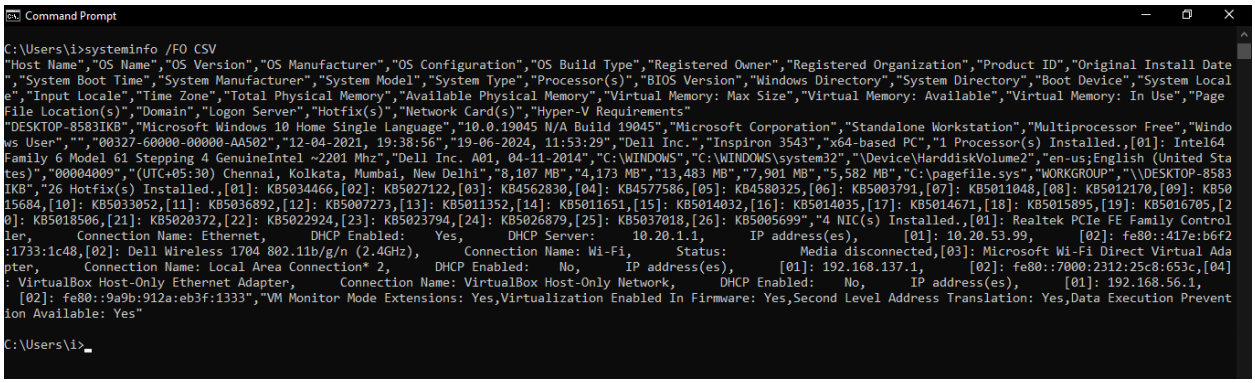
```
Command Prompt

                           [06]: KB5003791
                           [07]: KB5011048
                           [08]: KB5012170
                           [09]: KB5015684
                           [10]: KB5033052
                           [11]: KB5036892
                           [12]: KB5007273
                           [13]: KB5011352
                           [14]: KB5011651
                           [15]: KB5014032
                           [16]: KB5014035
                           [17]: KB5014671
                           [18]: KB5015895
                           [19]: KB5016705
                           [20]: KB5018506
                           [21]: KB5020372
                           [22]: KB5022924
                           [23]: KB5023794
                           [24]: KB5026879
                           [25]: KB5037018
                           [26]: KB5005699
Network Card(s):           3 NIC(s) Installed.
                           [01]: Realtek PCIe FE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
                           [02]: Dell Wireless 1704 802.11b/g/n (2.4GHz)
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.142.170
                                 IP address(es)
                                 [01]: 192.168.142.250
                                 [02]: fe80::e5e0:642a:7caf:825b
                                 [03]: 2409:4080:deb2:751:3135:6f3d:befb:33d9
                                 [04]: 2409:4080:deb2:751:88ac:45db:5891:9ce0
                           [03]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: VirtualBox Host-Only Network
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.56.1
                                 [02]: fe80::9a9b:912a:eb3f:1333
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes
```

Date: 13/06/2024

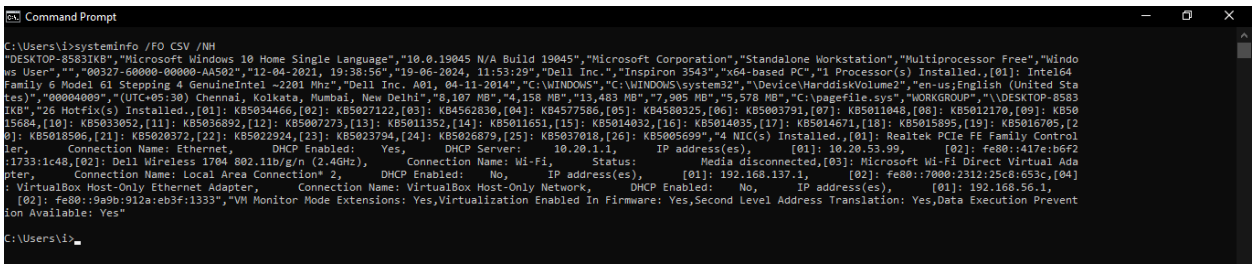
- systeminfo /FH TABLE



- systeminfo /FO CSV



- systeminfo /NH



Date: 13/06/2024

5. traceroute/tracert

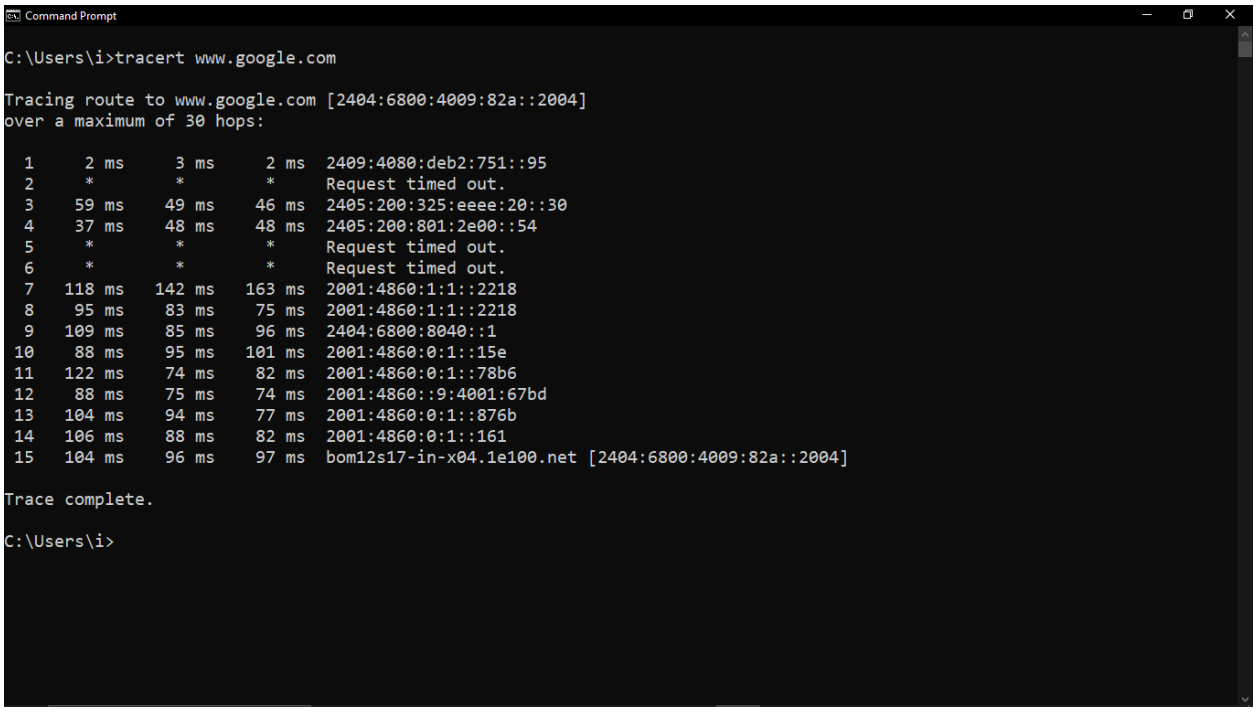
Description:

The tracert command (short for "trace route") is a network diagnostic tool available in Windows operating systems. It is used to determine the path packets take from your computer to a destination host. This command helps in identifying where in the network the issues are occurring, such as delays or failures in data transmission.

No.	Option	Description
1	-d	Do not resolve addresses to hostnames.
2	-h maximum_hops	Maximum number of hops to search for target.
3	-w timeout	Wait timeout milliseconds for each reply.
4.	-S srcaddr	Source address to use (IPv6-only).
5	-4	Force using IPv4.

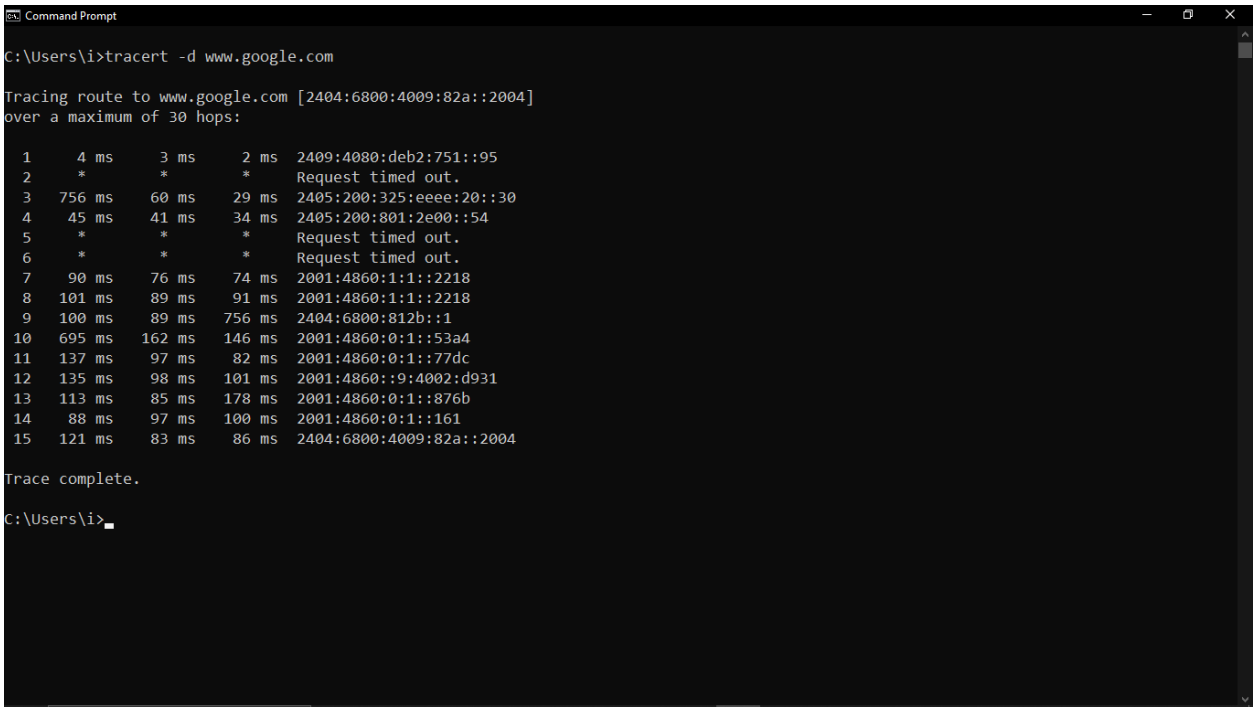
Implementation:

- tracert www.google.com

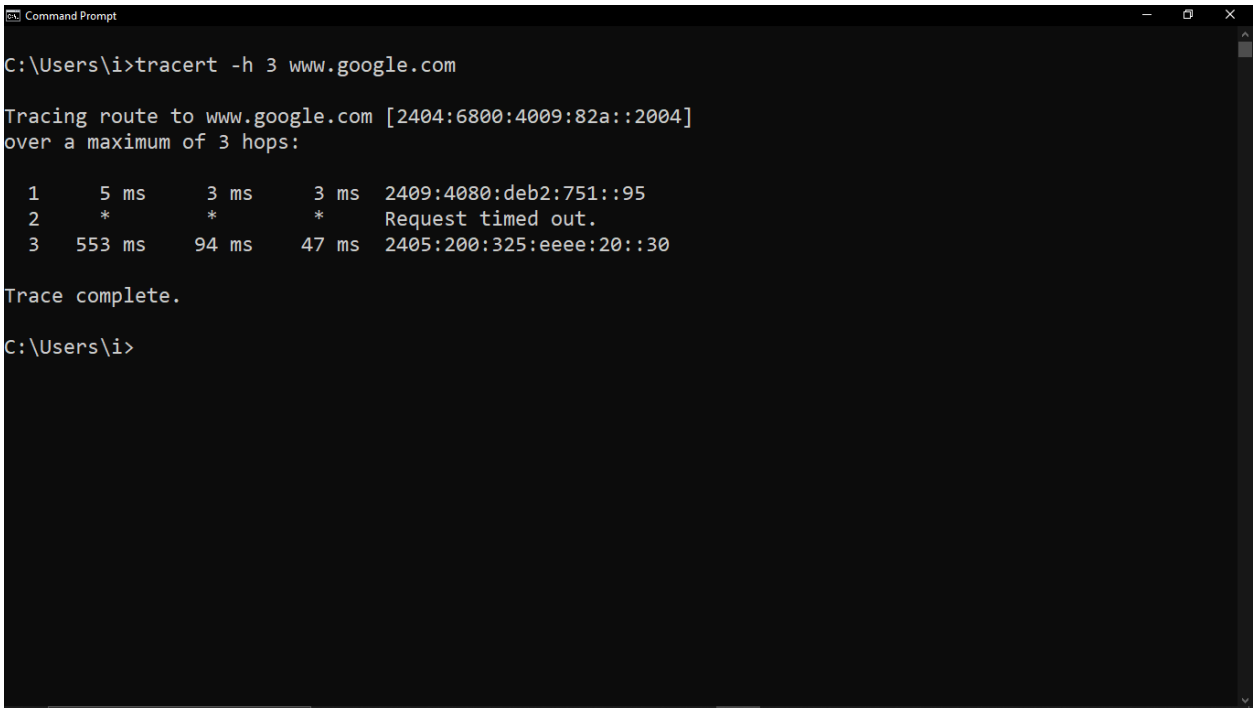


Date: 13/06/2024

- tracert –d www.google.com



- tracert –h 3 www.google.com



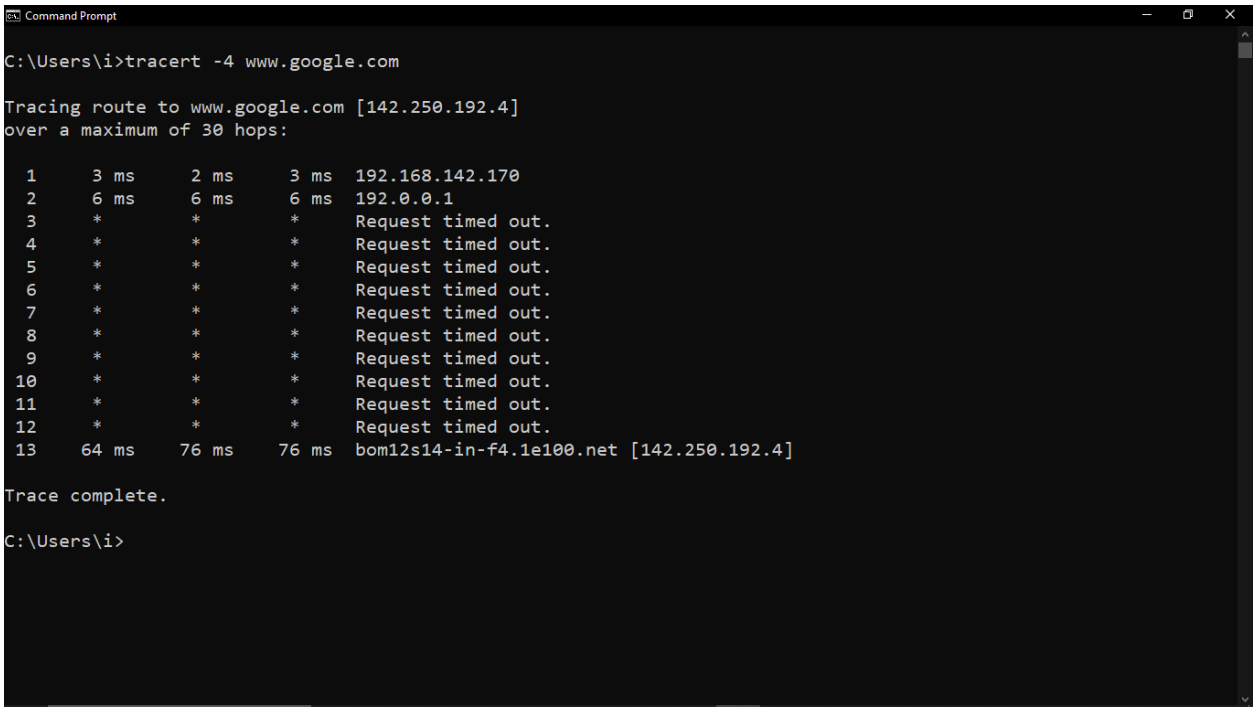
Date: 13/06/2024

- tracert –w 3000 www.google.com

- tracert –S 2001:0db8:85a3:0000:0000:8a2e:0370:7334 ipv6.google.com

Date: 13/06/2024

- tracert –4 www.google.com



Date: 13/06/2024

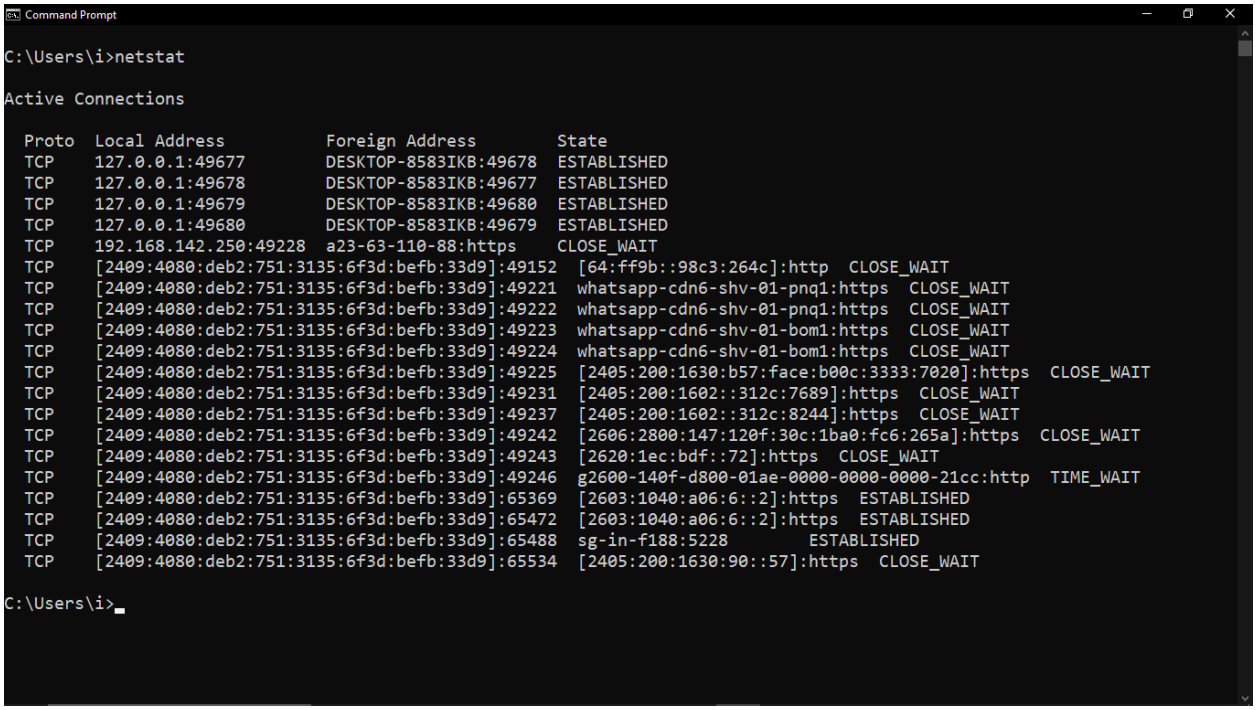
6. netstat

Description:

The netstat command is a network utility that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. It is available in various operating systems including Windows, Linux, and macOS. The command is useful for network troubleshooting and performance monitoring.

No.	Option	Description
1	-a	Displays all connections and listening ports.
2	-e	Displays Ethernet statistics. This may be combined with the –s option.
3	-f	Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
4	-o	Displays the owning process ID associated with each connection
5	-r	Displays the routing table.

Implementation:



Date: 13/06/2024

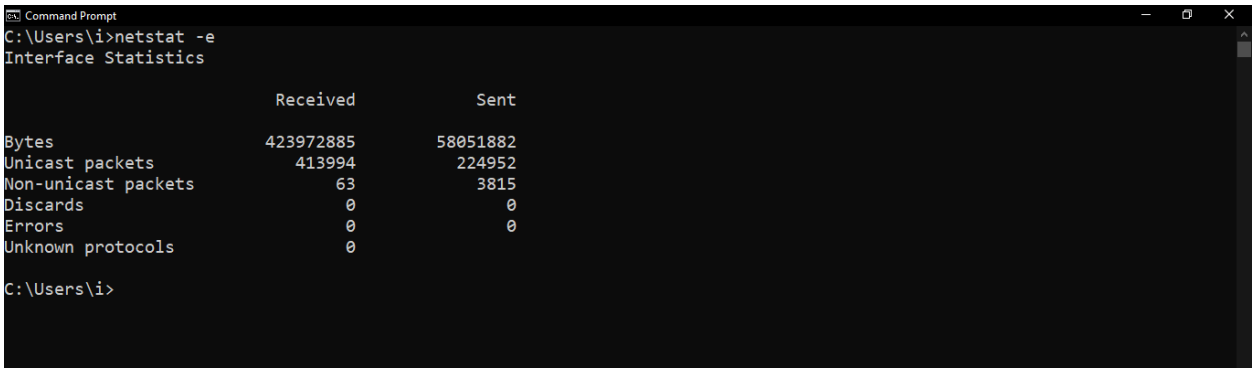
- netstat -a

```
Command Prompt
C:\Users\i>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:8080           DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:33060          DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-8583IKB:0      LISTENING
  TCP    0.0.0.0:49676          DESKTOP-8583IKB:0      LISTENING
  TCP    127.0.0.1:1434         DESKTOP-8583IKB:0      LISTENING
  TCP    127.0.0.1:23402        DESKTOP-8583IKB:0      LISTENING
  TCP    127.0.0.1:27017        DESKTOP-8583IKB:0      LISTENING
  TCP    127.0.0.1:49677        DESKTOP-8583IKB:49678  ESTABLISHED
  TCP    127.0.0.1:49678        DESKTOP-8583IKB:49677  ESTABLISHED
  TCP    127.0.0.1:49679        DESKTOP-8583IKB:49680  ESTABLISHED
  TCP    127.0.0.1:49680        DESKTOP-8583IKB:49679  ESTABLISHED
  TCP    127.0.0.1:58880        DESKTOP-8583IKB:0      LISTENING
  TCP    192.168.56.1:139       DESKTOP-8583IKB:0      LISTENING
  TCP    192.168.142.250:139    DESKTOP-8583IKB:0      LISTENING
  TCP    192.168.142.250:49228  a23-63-110-88:https    CLOSE_WAIT
  TCP    [::]:135               DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:445               DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:8080              DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:33060             DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:49664             DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:49665             DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:49666             DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:49667             DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:49668             DESKTOP-8583IKB:0      LISTENING
  TCP    [::]:49676             DESKTOP-8583IKB:0      LISTENING
  TCP    [::1]:1434             DESKTOP-8583IKB:0      LISTENING
  TCP    [::1]:49669            DESKTOP-8583IKB:0      LISTENING
  TCP    [::1]:58880            DESKTOP-8583IKB:0      LISTENING
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49152  [64:ff9b::98c3:264c]:http  CLOSE_WAIT
```

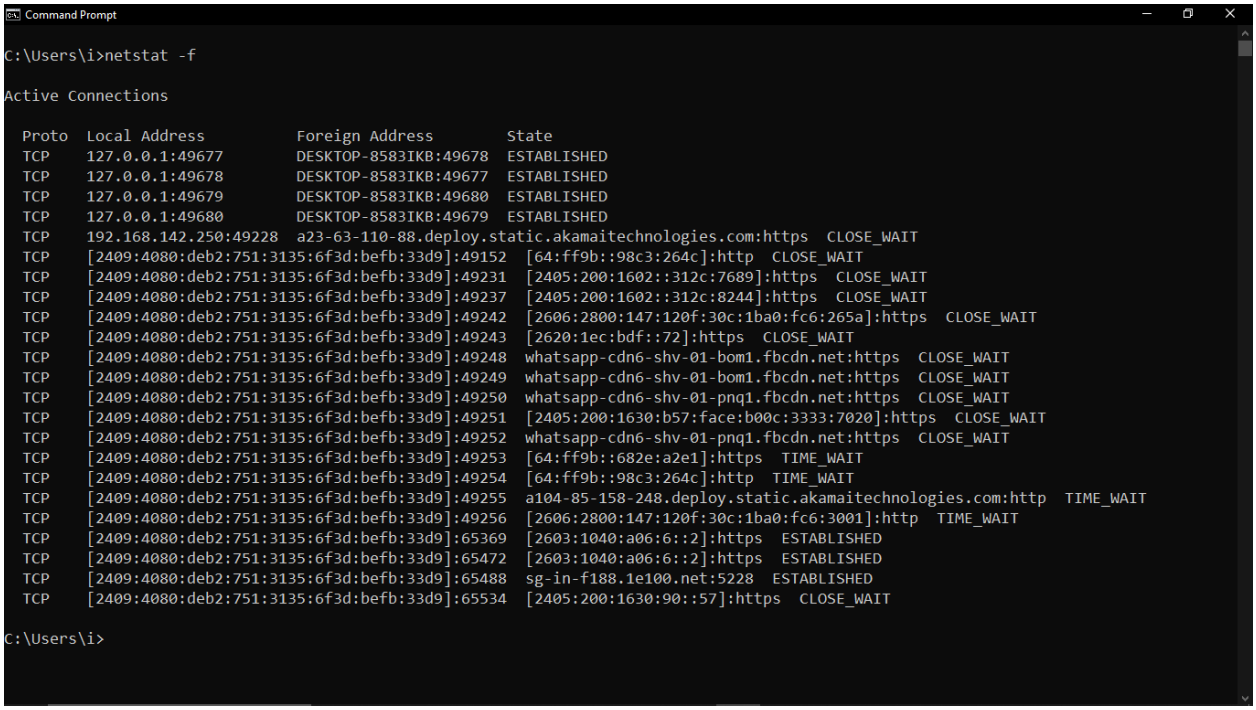
```
Select Command Prompt
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49231  [2405:200:1602::312c:7689]:https  CLOSE_WAIT
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49237  [2405:200:1602::312c:8244]:https  CLOSE_WAIT
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49242  [2606:2800:147:120f:30c:1ba0:fc6:265a]:https  CLOSE_WAIT
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49243  [2620:1ec:bdf::72]:https  CLOSE_WAIT
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49247  whatsapp-chatd-edge6-shv-01-pnq1:http  TIME_WAIT
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49248  whatsapp-cdn6-shv-01-bom1:https  ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49249  whatsapp-cdn6-shv-01-bom1:https  ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49250  whatsapp-cdn6-shv-01-pnq1:https  ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49251  [2405:200:1630:b57:face:b00c:3333:7020]:https  ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49252  whatsapp-cdn6-shv-01-pnq1:https  ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65369  [2603:1040:a06:6::2]:https  ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65472  [2603:1040:a06:6::2]:https  ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65488  sg-in-f188:5228        ESTABLISHED
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65534  [2405:200:1630:90::57]:https  CLOSE_WAIT
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:48300        *:*
  UDP    127.0.0.1:48301        *:*
  UDP    127.0.0.1:52915        *:*
  UDP    127.0.0.1:54765        *:*
  UDP    192.168.56.1:137       *:*
  UDP    192.168.56.1:138       *:*
  UDP    192.168.56.1:1900      *:*
  UDP    192.168.56.1:52913     *:*
  UDP    192.168.142.250:137    *:*
  UDP    192.168.142.250:138    *:*
  UDP    192.168.142.250:1900   *:*
  UDP    192.168.142.250:52914  *:*
  UDP    [::]:123               *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:52912            *:*
  UDP    [fe80::9a9b:912a:eb3f:1333%5]:1900  *:*
  UDP    [fe80::9a9b:912a:eb3f:1333%5]:52910  *:*
  UDP    [fe80::e5e0:642a:7caf:825b%2]:1900  *:*
  UDP    [fe80::e5e0:642a:7caf:825b%2]:52911  *:*
```

Date: 13/06/2024

- netstat -e



- netstat -f



Date: 13/06/2024

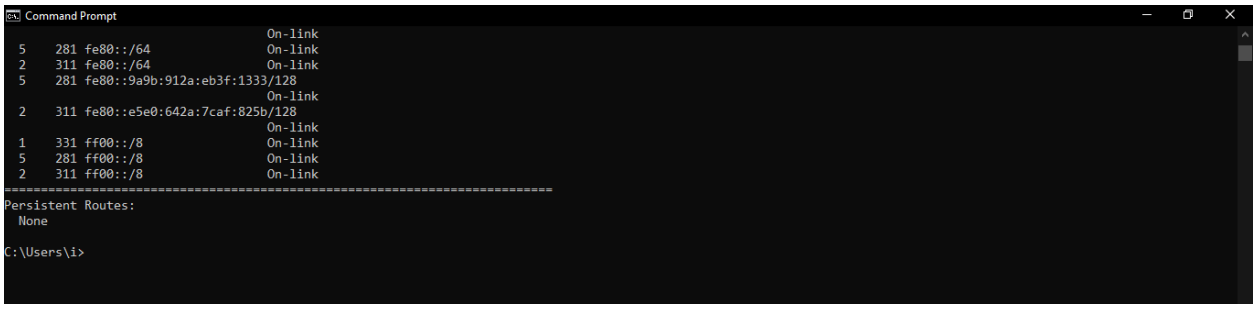
- netstat -o

```
Select Command Prompt

C:\Users\i>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49677        DESKTOP-8583IKB:49678  ESTABLISHED     4644
  TCP    127.0.0.1:49678        DESKTOP-8583IKB:49677  ESTABLISHED     4644
  TCP    127.0.0.1:49679        DESKTOP-8583IKB:49680  ESTABLISHED     4644
  TCP    127.0.0.1:49680        DESKTOP-8583IKB:49679  ESTABLISHED     4644
  TCP    192.168.142.250:49228  a23-63-110-88:https    CLOSE_WAIT      7372
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49152  [64:ff9b::98c3:264c]:http  CLOSE_WAIT      2912
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49231  [2405:200:1602::312c:7689]:https  CLOSE_WAIT      6756
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49237  [2405:200:1602::312c:8244]:https  CLOSE_WAIT      6756
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49242  [2606:2800:147:120f:30c:1ba0:fc6:265a]:https  CLOSE_WAIT      6756
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49243  [2620:1ec:bdf::72]:https  CLOSE_WAIT      6756
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49248  whatsapp-cdn6-shv-01-bom1:https  CLOSE_WAIT      14284
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49249  whatsapp-cdn6-shv-01-bom1:https  CLOSE_WAIT      14284
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49250  whatsapp-cdn6-shv-01-pnq1:https  CLOSE_WAIT      14284
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49251  [2405:200:1630:b57:face:b00c:3333:7020]:https  CLOSE_WAIT      14284
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49252  whatsapp-cdn6-shv-01-pnq1:https  CLOSE_WAIT      14284
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49253  [64:ff9b::682e:a2e1]:https  TIME_WAIT       0
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49254  [64:ff9b::98c3:264c]:http  TIME_WAIT       0
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49255  a104-85-158-248:http   TIME_WAIT       0
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:49256  [2606:2800:147:120f:30c:1ba0:fc6:3001]:http  TIME_WAIT       0
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65369  [2603:1040:a06:6::2]:https  ESTABLISHED     3880
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65472  [2603:1040:a06:6::2]:https  ESTABLISHED     3880
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65488  sg-in-f188:5228        ESTABLISHED     264
  TCP    [2409:4080:deb2:751:3135:6f3d:befb:33d9]:65534  [2405:200:1630:90::57]:https  CLOSE_WAIT      2912

C:\Users\i>
```

- netstat -r

```
Command Prompt

C:\Users\i>netstat -r
===========================================================================
Interface List
 19...74 e6 e2 46 36 58 ......Realtek PCIe FE Family Controller
  5...0a 00 27 00 00 05 ......VirtualBox Host-Only Ethernet Adapter
 10...2e 33 7a f7 f1 39 ......Microsoft Wi-Fi Direct Virtual Adapter
  4...2e 33 7a f7 f9 39 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  2...2c 33 7a f7 f1 39 ......Dell Wireless 1704 802.11b/g/n (2.4GHz)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0  192.168.142.170  192.168.142.250     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
      192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
      192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
    192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
    192.168.142.0    255.255.255.0         On-link   192.168.142.250    311
  192.168.142.250  255.255.255.255         On-link   192.168.142.250    311
  192.168.142.255  255.255.255.255         On-link   192.168.142.250    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      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link   192.168.142.250    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      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link   192.168.142.250    311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  2     71 ::/0                     fe80::60ff:a4ff:fec0:b889
  1    331 ::1/128                  On-link
  2     71 2409:4080:deb2:751::/64  On-link
  2    311 2409:4080:deb2:751:3135:6f3d:befb:33d9/128
                                    On-link
  2    311 2409:4080:deb2:751:88ac:45db:5891:9ce0/128
                                    On-link
  5    281 fe80::/64               On-link
  2    311 fe80::/64               On-link
```

Date: 13/06/2024



7. nslookup

Description:

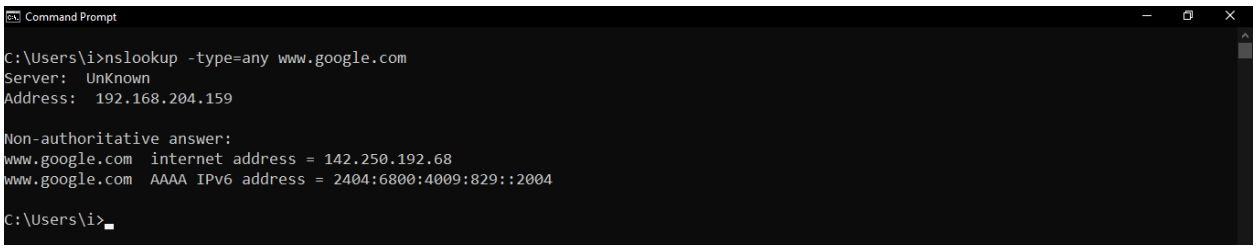
The nslookup command is a network administration command-line tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping information. It can be used to find the IP address associated with a domain name or the domain name associated with an IP address. This tool is useful for diagnosing DNS issues and verifying DNS configurations.

No.	Option	Description
1	-debug	Enables the display of debugging information
2	-type=any	Lookup for any record We can also view all the available DNS records using the -type=any option.
3	-type=SOA	Lookup for a soa record SOA record (start of authority), provides the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc…

Implementation:

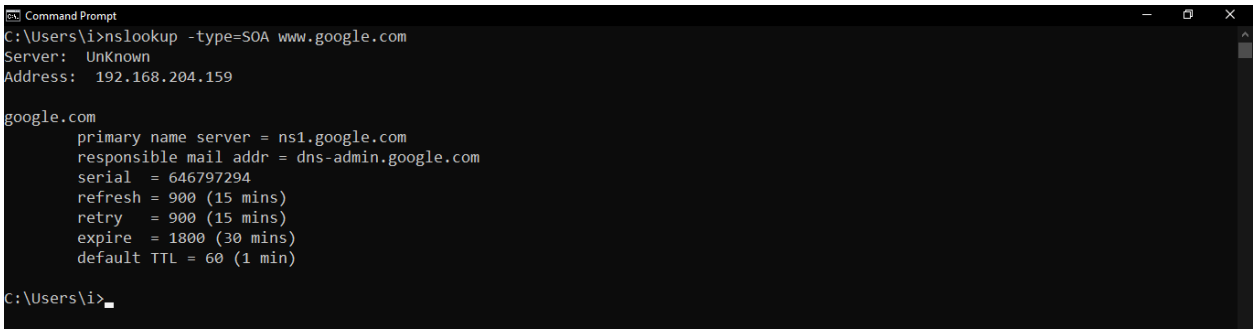
- nslookup www.google.com

- nslookup –type=any www.google.com

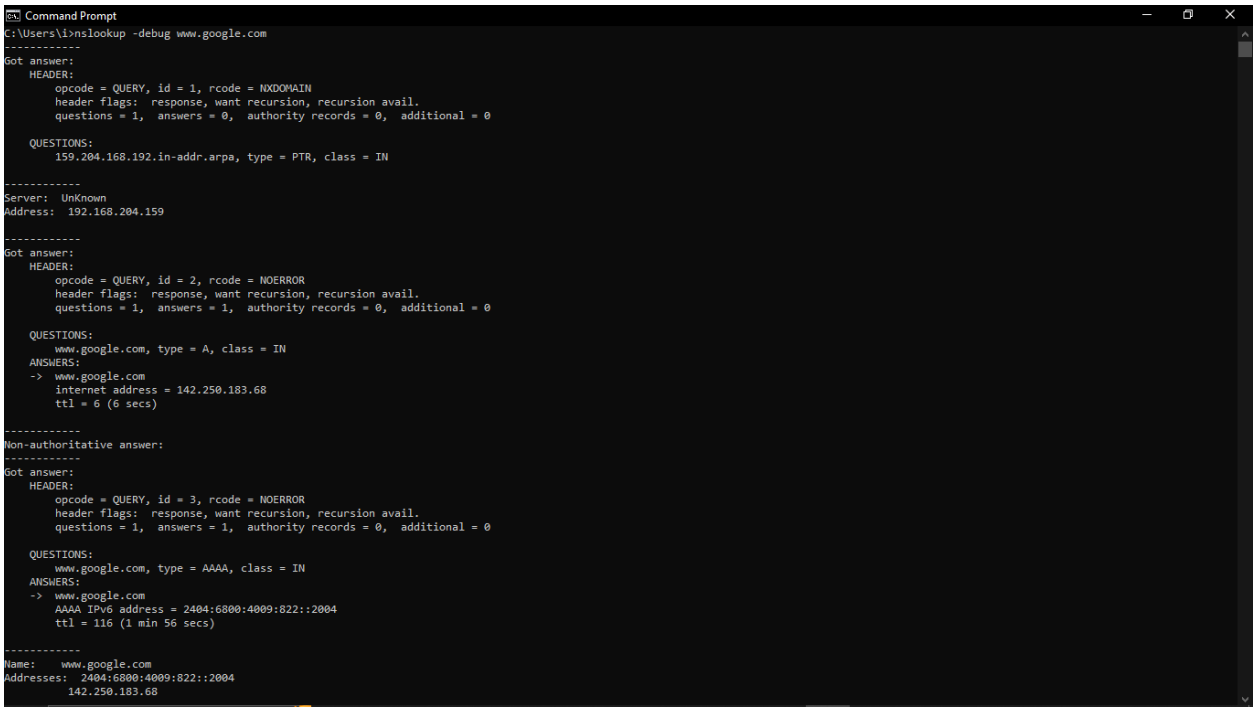


Date: 13/06/2024

- nslookup –type=SOA www.google.com



- nslookup –debug www.google.com



Date: 13/06/2024

8. hostname

Description:

The hostname command is a simple command-line utility used in various operating systems (Windows, Linux, macOS) to display or set the name of the current host system. The hostname is a unique identifier assigned to a machine on a network.

Implementation:

Date: 13/06/2024

9. pathping

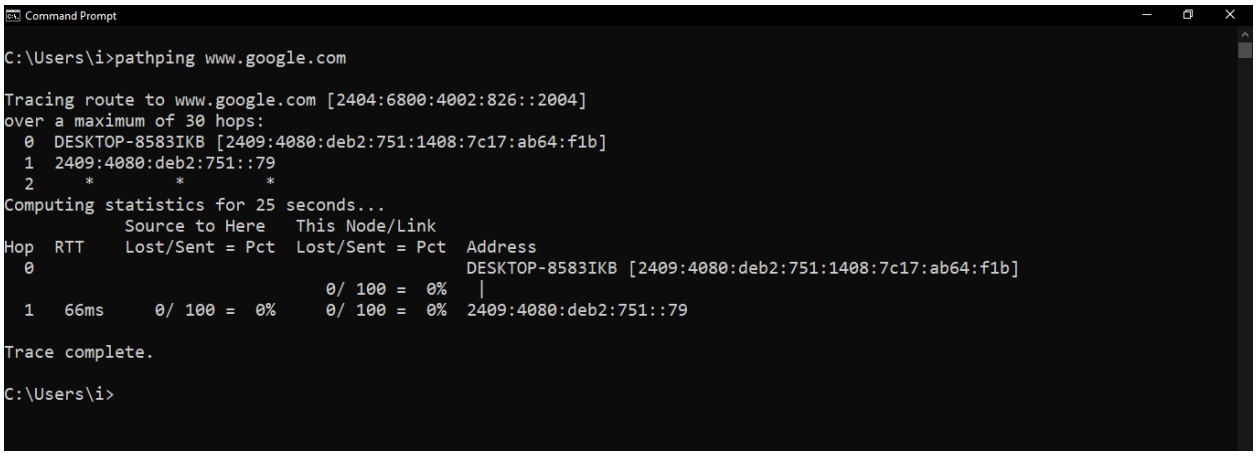
Description:

The pathping command in Windows is a network diagnostic tool that combines the features of ping and tracert. It provides detailed information about network latency and packet loss along the route from the source to the destination. This tool is particularly useful for identifying problematic routers or links in a network path.

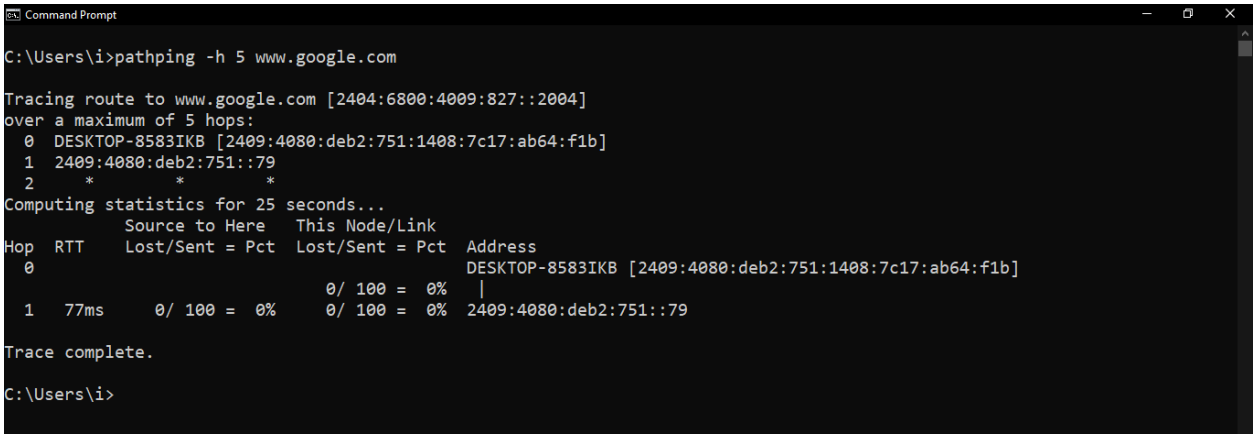
No.	Option	Description
1	-h maximum_hops	Maximum number of hops to search for target.
2	-n	Do not resolve addresses to hostnames.
3	q num_queries	Number of queries per hop.
4	-w timeout	Wait timeout milliseconds for each reply.
5	-4	Force using IPv4.

Implementation:

- pathping www.google.com



- pathping –h 5 www.google.com



Date: 13/06/2024

- pathping –n www.google.com

```
Command Prompt

C:\Users\i>pathping -n www.google.com

Tracing route to www.google.com [2404:6800:4009:827::2004]
over a maximum of 30 hops:
  0  2409:4080:deb2:751:1408:7c17:ab64:f1b
  1  2409:4080:deb2:751::79
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          2409:4080:deb2:751:1408:7c17:ab64:f1b
                                 0/ 100 =  0%   |
  1   66ms     0/ 100 =  0%     0/ 100 =  0%  2409:4080:deb2:751::79

Trace complete.

C:\Users\i>
```

- pathping –q 5 www.google.com

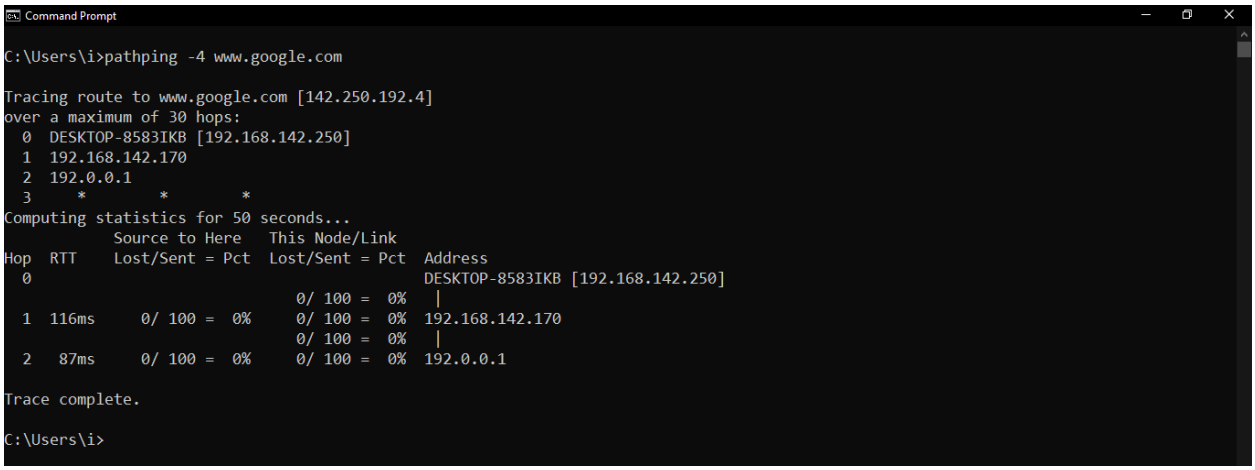
```
Command Prompt

C:\Users\i>pathping -q 5 www.google.com

Tracing route to www.google.com [2404:6800:4009:827::2004]
over a maximum of 30 hops:
  0  DESKTOP-8583IKB [2409:4080:deb2:751:1408:7c17:ab64:f1b]
  1  2409:4080:deb2:751::79
  2     *        *        *
Computing statistics for 1 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          DESKTOP-8583IKB [2409:4080:deb2:751:1408:7c17:ab64:f1b]
                                 0/   5 =  0%   |
  1   58ms     0/   5 =  0%     0/   5 =  0%  2409:4080:deb2:751::79

Trace complete.

C:\Users\i>
```

- pathping –w 3000 www.google.com

```
Command Prompt

C:\Users\i>pathping -w 3000 www.google.com

Tracing route to www.google.com [2404:6800:4009:827::2004]
over a maximum of 30 hops:
  0  DESKTOP-8583IKB [2409:4080:deb2:751:1408:7c17:ab64:f1b]
  1  2409:4080:deb2:751::79
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          DESKTOP-8583IKB [2409:4080:deb2:751:1408:7c17:ab64:f1b]
                                 0/ 100 =  0%   |
  1   56ms     0/ 100 =  0%     0/ 100 =  0%  2409:4080:deb2:751::79

Trace complete.

C:\Users\i>
```

Date: 13/06/2024

- pathping -4 www.google.com



Date: 13/06/2024

10.arp

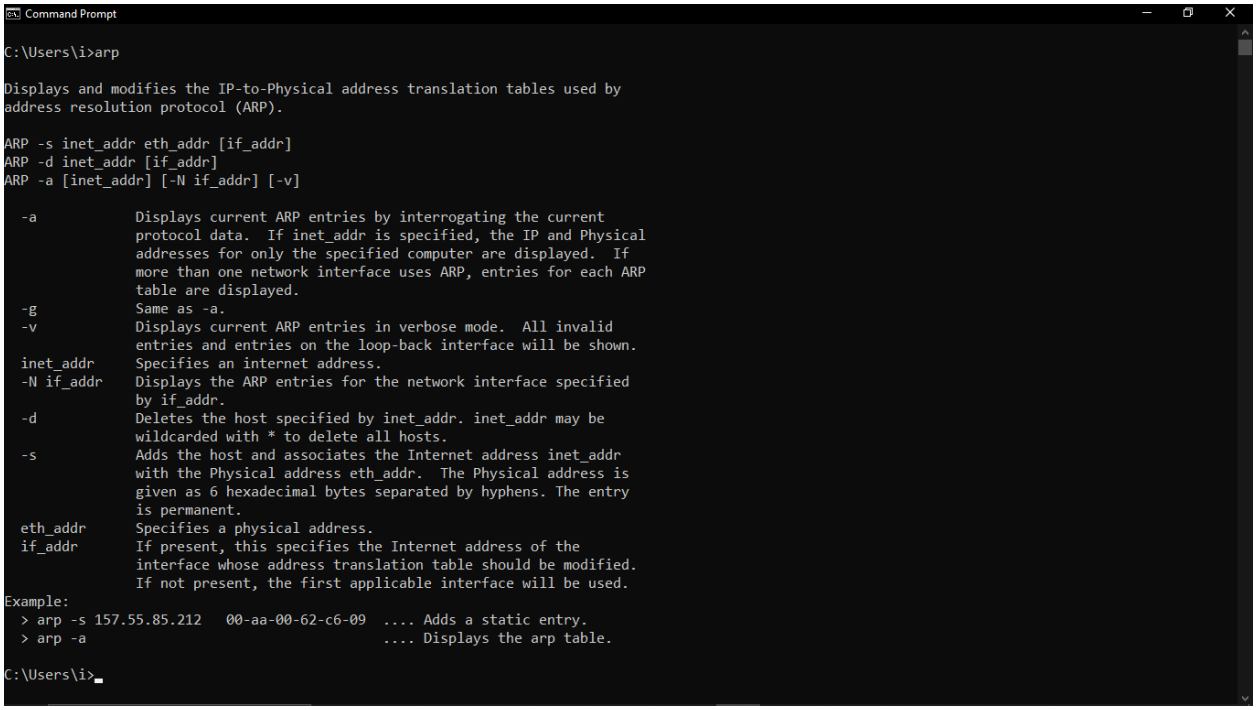
Description:

The arp (Address Resolution Protocol) command in Windows is used to view and manipulate the ARP cache, which stores mappings of IP addresses to physical MAC addresses. This command is useful for diagnosing network issues and ensuring proper network configuration.

No.	Option	Description
1	-a	Displays current ARP entries by interrogating the currentprotocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
2	-v	Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.
3	inet_addr.	Specifies an internet address

Implementation:

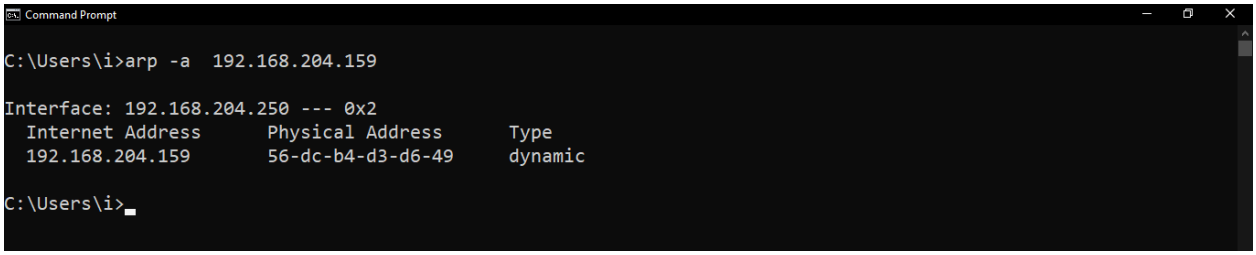
- arp



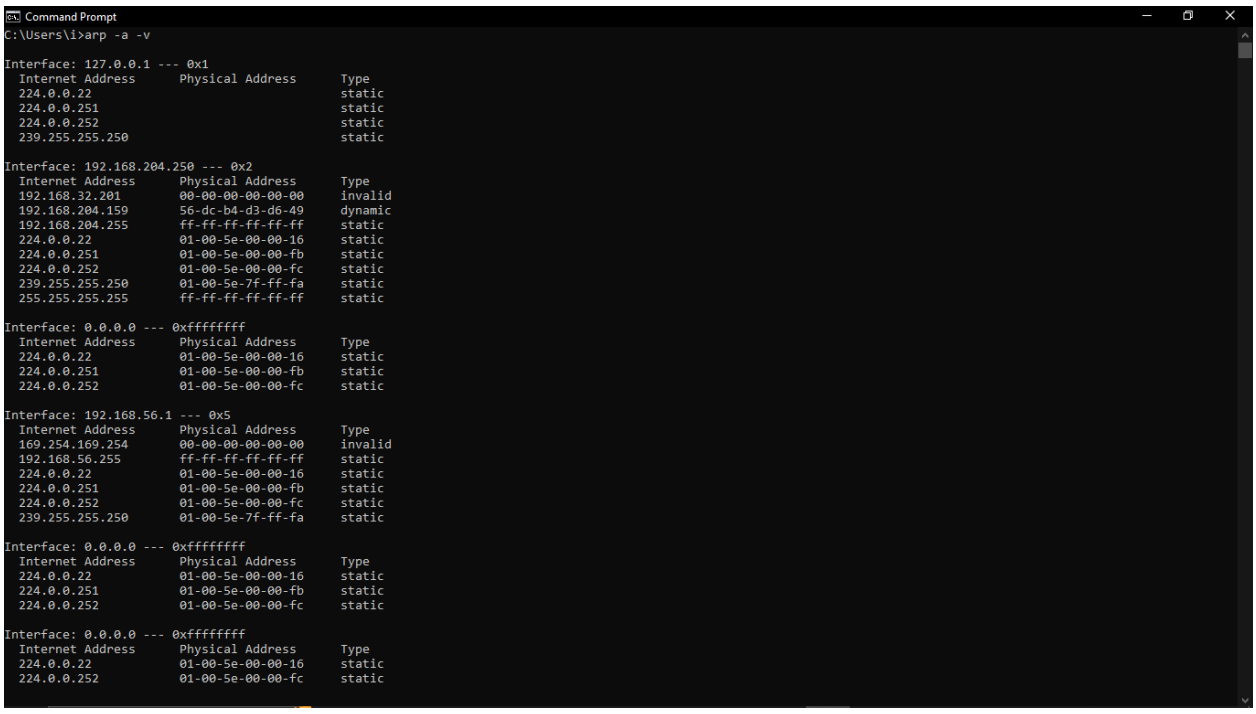
Date: 13/06/2024

- arp -a

- arp –a



- arp –a –v



Date: 27/06 /2024

Lab Practical #02:

Study of different types of network cables & connectors and crimping a LAN.

Practical Assignment #02:

1. List various networks cable. Also, write short description.
2. Difference between guided and unguided media.
3. Give cross-wired cable and straight through cable diagram (Color Code wise).

1. List various networks cable and connectors. Also, write short description.

a) Twisted Pair Cable:

- **Description**:

  Twisted-pair Category 5e cables, also called CAT5e, are the industry standard for unshielded twisted-pair cables (UTP) for in-home and small business networking. Cables that are manufactured to prevent electromagnetic interference are shielded twisted-pair, or STP cables. CAT5e cables have an Ethernet capability of up to 1,000 megabits per second (Mbps) and can often carry infrared (IR or remote) control signals, eliminating the need for a separate IR network. They connect phones, computer networks, home automation networks and audio/video distribution systems.

  CAT5e cables typically consist of four pairs of wire (eight total conductors) wrapped in a single jacket. In addition, Category 6, or CAT6 cable, is a standardized twisted pair network cable designed to meet more stringent standards for crosstalk and system noise than CAT5e. Older categories, such as CAT5, have reduced transmission rates.

- **Diagram**:

b) Coaxial Cable:

- **Description**:

  Coaxial cables are metallic cables most often used to carry television signals and connect video equipment. They provide protection from electromagnetic interference, allowing signals with low power to be transmitted over longer distances. They feature a central bayonet wire

conductor covered with a dielectric or non-conducting insulator surrounded by mesh or a metal sheath. These components are then covered by a thin plastic layer for protection.

Sometimes called “coax,” they often carry infrared (IR or remote) control signals, eliminating the need for a separate IR network. While no longer installed for the purpose, coax was among the first Ethernet network cable types.

Coaxial cable conductors carry electromagnetic signals and can come either in single-core or multi-core models. While a single-core coaxial cable has only one central metal, multi-core cables have many metal wires.

Coaxial cables were used in the earlier days of computer networks.

- **Diagram**:

c) Fiber Optic Cable:

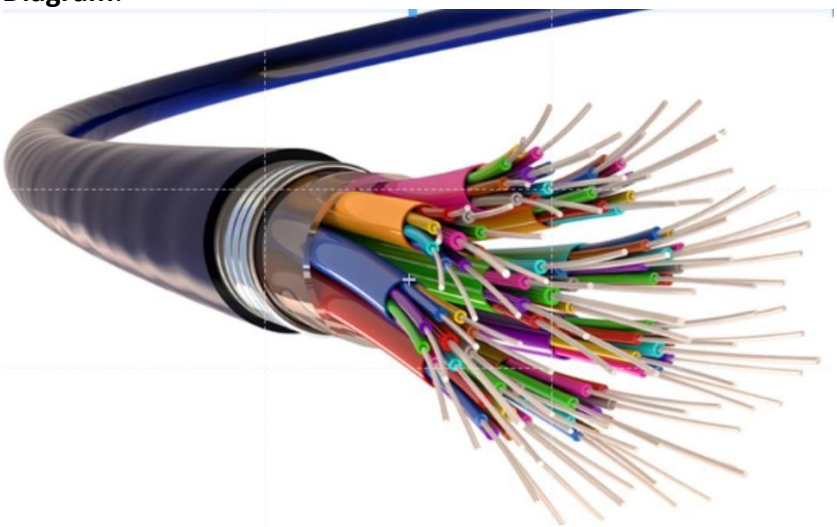
- **Description**:

Fiber optic cables use glass or plastic threads to transmit data quickly and efficiently using pulses of light rather than electrical signals. Apart from connecting components in home theaters, they are not as readily available for residential use as are coax and CAT5e. They transmit data at higher rates than coaxial or twisted-pair cables.

Optical audio cables may be used for phones, computer networks and cable television. They have less signal loss than copper and deliver clearer phone conversations or television reception. Multi-mode fiber is designed to carry data over shorter distances by using several rays of light at the same time.

Date: 27/06 /2024

- **Diagram**:



d) BNC connectors:

- **Description**:

BNC(Bayonet Neill–Concelman) connectors are a type of F-series connectors commonly found in households. This type of connector for RG59 or RG6 coaxial cable is used for cable television equipment, broadcast TV antennas and CCTV security camera installations. They are easy to connect and disconnect from equipment and provide inexpensive, stable connections to these communications devices and other cables.

To install a BNC connector, use a stripping tool to remove protective shields from the cable. The connector is pushed onto the end and then squeezed around the conductive material using a special compression crimper.

Twist-on F-connectors are also available for making quick and easy repairs to TV equipment without the need for special tools.

- **Diagram**:

Date: 27/06 /2024

e) RJ45 connector:

- **Description**:

RJ45 connectors are used for CAT6 cables and CAT5e cables. These connectors for twisted-pair Ethernet cables are similar in appearance to a standard telephone cord connector. They are wider, however, because they have eight conductors compared to only four conductors on a telephone jack.

To install these types of wiring connectors, a stripping tool is used to expose the twisted pairs of wires from the cable, which are then positioned into the appropriate slots on the terminal plug. The connector is then crimped to the cable using a crimping tool.

- **Diagram**:

f) Fiber optic connector:

- **Description**:

Fiber optic connectors require different types of connectors from those used with coax or twisted-pair cables, such as CAT5e. These types of connectors in networking must align glass fibers with precision to allow for communication. If you choose to use optical cable over twisted pair Ethernet, you may need to install a special adapter in your computer to utilize various fiber optic cable connector types.

The type of wiring connector used depends on the style of jack in the peripheral device.

- SC connectors: A push-pull latching mechanism in SC connectors provides quick insertion and removal while also ensuring a positive connection.
- ST connectors: ST connectors were among the first connectors in networking fiber optic cable. These use a plug and socket, which is locked in place with a twist-style bayonet lock.
- LC connectors: LC-type connectors have a squarish duplex configuration. Installation of this small form factor (SFF) connector is quick for rapid repair of replacement needs.

Date: 27/06 /2024

- **Diagram**:

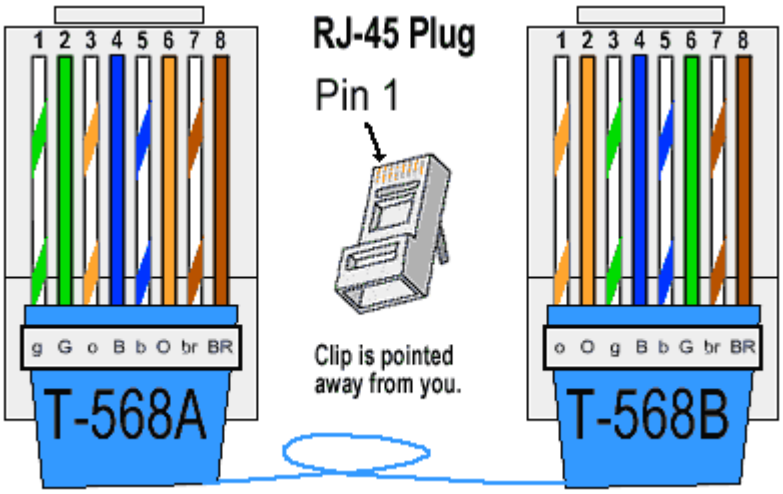
2. Difference between guided and unguided media.

Guided Media	Unguided Media
Also called Wired communication.	Also called wireless communication.
Signal energy propagates through wires in guided media.	Signal energy propagates thought the air in unguided media.
It is cost effective.	It is quiet expensive.
It is best for shorter distances.	It would be better for longer distances.
Point-to-Point connection	Suited for radio broadcasting in all directions.
Examples of guided media are Twisted Pair cables, Coaxial cables, and Fiber Optic cables.	Examples of unguided media are microwave, radio wave, infrared waves.

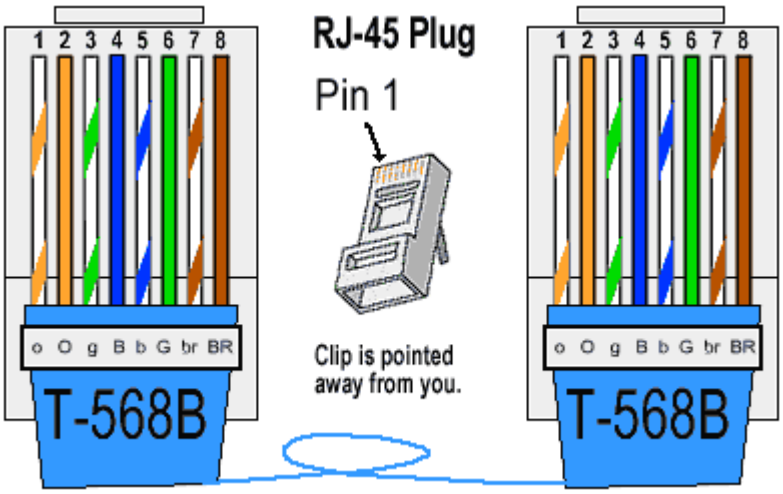
Date: 27/06 /2024

3. Give cross-wired cable and straight through cable diagram (Color Code wise).

a) Cross-wired Cable Diagram (Color Code)



b) Straight Through Cable Diagram (Color Code)



Date: 07/ 07/2024

Lab Practical #03:

Study of different network devices in detail.

Practical Assignment #03:

1. Give difference between below network devices.
   - Hub and Switch
   - Switch and Router
   - Router and Gateway
2. Working of below network devices:
   - Switch
   - Router
   - Gateway

Hub and Switch

No.	Hub	Switch
1	Hubs function on Physical layer of the OSI framework.	Switches function on Data Link layer of the OSI framework.
2	Hubs are less intelligent devices and always send all information to all connected devices.	Switches record MAC addresses in a table to learn which devices to transmit information to
3	Hubs group Ethernet devices on a LAN, broadcasting all data to all devices.	Switches connect devices to a singular LAN to transmit data from one device to another.
4	Hubs operate at half duplex, making them slower and forcing devices to share bandwidth equally.	Switches can operate at full duplex or half duplex, using all available bandwidth, creating faster and more efficient networks.
5	Hubs send information using bits.	Switches send information using data packets.
6	Hub have 4/12 ports.	Switch can have 24 to 48 ports.
7	Hub cannot be used as a repeater.	Switch can be used as a repeater.
8	In hub, Packet filtering is not provided.	In switch, Packet filtering is provided.
9	Speed of original hub 10Mbps and modern internet hub is 100Mbps.	Maximum speed is 10Mbps to 100Mbps.

Switch and Router

No.	Switch	Router
1	It connects multiple networked devices in the network.	It connects multiple switches & their corresponding networks.
2	It works on the data link layer of the OSI model.	It works on the network layer of the OSI model.
3	It is used within a LAN.	It can be used in LAN or MAN.
4	A switch cannot perform NAT or Network Address Translation.	A router can perform Network Address Translation.
5	The switch takes more time while making complicated routing decisions.	A router can take a routing decision much faster than a switch.

6	It provides only port security.	It provides security measures to protect the network from security threats.
7	It works in either half or full-duplex transmission mode.	It works in the full-duplex transmission mode. However, we can change it manually to work on half-duplex mode.
8	Switches can only work with the wired network.	Routers can work with both wired & wireless networks.
9	Switches are available with different ports, such as 8, 16, 24, 48, and 64.	A router contains two ports by default, such as Fast Ethernet Port. But we can also add the serial ports explicitly.
10	It uses the CAM (Content Addressable Memory) table for the source and destination MAC address.	It uses the routing table to get the best route for the destination IP.

Router and Gateway

No.	Router	Gateway
1	Usually, routers run on the 3rd layer of the protocol and transmit the packets from one system to another. A router chooses the network's path to transport the data packets.	Gateway interprets the network system as endpoints from one packet to another.
2	It is available only to dedicated applications	It is hosted on the dedicated application, physical servers, and virtual applications
3	It routes the data packets via similar networks.	It connects two dissimilar networks.
4	It is deployed on the router hardware in a specific appliance.	The gateway is deployed as the virtual or physical server or the specific appliance.
5	It can operate only on **3** and **4** layers.	It can operate only on the **5** layers.
6	Router supports dynamic routing.	Gateway doesn't support dynamic routing.
7	The additional features provided by a router are Wireless networking, Static routing, NAT, DHCP server etc.	The additional features provided by a gateway are network access control, protocol conversion etc.

Working of below network devices:

1. Switch

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

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

Date: 07/ 07/2024

- It operates in Data Link Layer in OSI Model.
- It performs error checking before forwarding data.
- It transfers the data only to the device that has been addressed.
- It operates in full duplex mode.
- It allocates each LAN segment a limited bandwidth.
- It uses Unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) transmission modes.
- Packet Switching techniques are used to transfer data packets from source to destination.
- Switches have a more significant number of ports.

- **Working :**

When the source wants to send the data packet to the destination, the packet first enters the switch and the switch reads its header and finds the MAC address of the destination to identify the device then it sends the packet out through the appropriate ports that lead to the destination devices.

Switch establishes a temporary connection between the source and destination for communication and terminates the connection once the conversation is done. Also, it offers full bandwidth to network traffic going to and from a device simultaneously to reduce collision.

2. Router

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

- **Working :**

A router works by using a protocol called the Internet Protocol (IP), which is a set of rules that govern how data is transmitted across the internet. When a device on your network sends data, the data is broken up into small packets, which are then sent to the router.

The router then examines the destination IP address of the packet to determine where it should be sent. If the destination IP address is on your network, the router sends the packet directly to the device with that IP address. If the destination IP address is not on your network, the router sends the packet to the modem, which then sends the packet to the internet.

Date: 07/ 07/2024

In addition to directing traffic between devices, a router also performs other important functions, such as providing security for your network. Routers often include features such as firewalls and network address translation (NAT), which help protect your network from unauthorised access.

Routers connect computers and other devices to the Internet. A router acts as a dispatcher, choosing the best route for your information to travel. It connects your business to the world, protects information from security threats, and can even decide which computers get priority over others

3. Gateway

A gateway is a network node used in telecommunications that connects two networks with different transmission protocols together. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed. In most IP-based networks, the only traffic that does not go through at least one gateway is traffic flowing among nodes on the same local area network (LAN) segment. The term default gateway or network gateway may also be used to describe the same concept.

- **Working :**

All networks have a boundary that limits communication to devices that are directly connected to it. Due to this, if a network wants to communicate with devices, nodes or networks outside of that boundary, they require the functionality of a gateway. A gateway is often characterized as being the combination of a router and a modem.

The gateway is implemented at the edge of a network and manages all data that is directed internally or externally from that network. When one network wants to communicate with another, the data packet is passed to the gateway and then routed to the destination through the most efficient path. In addition to routing data, a gateway will also store information about the host network's internal paths and the paths of any additional networks that are encountered.

Gateways are basically protocol converters, facilitating compatibility between two protocols and operating on any layer of the open systems interconnection (OSI) model.

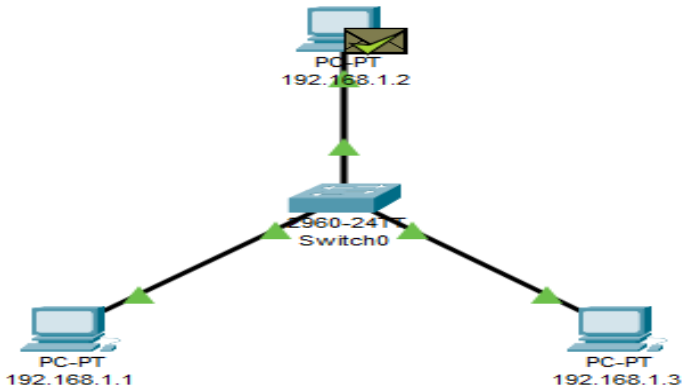
Date: 13/07/2024

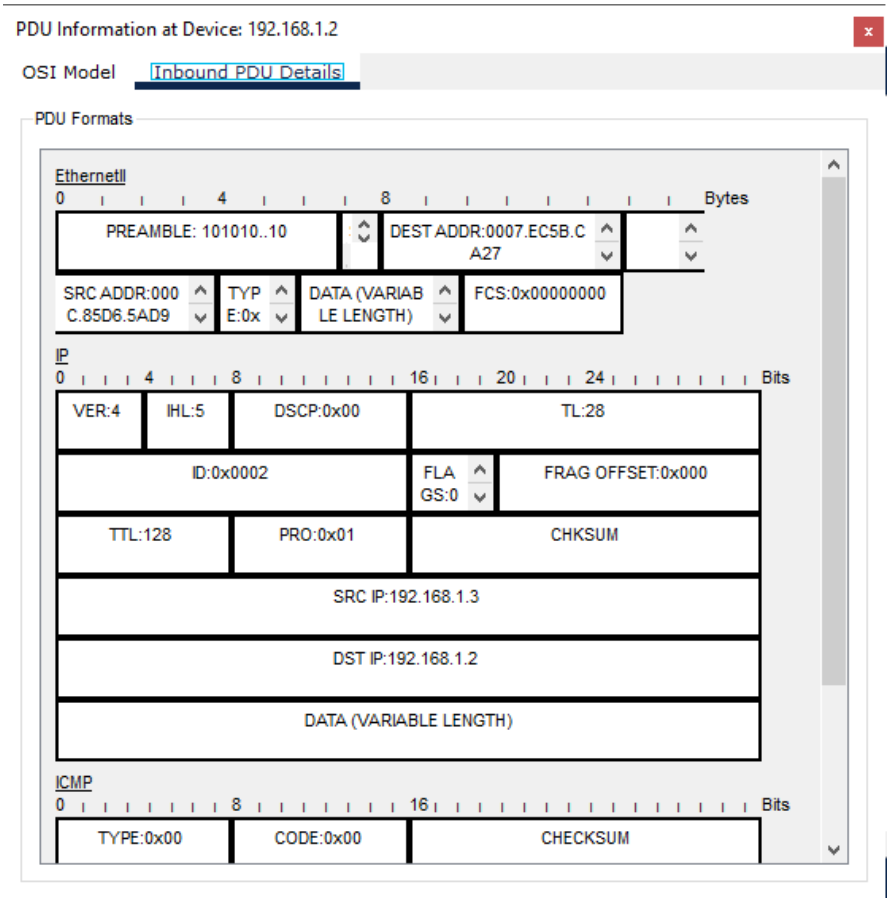
Lab Practical #04:

Installation of Network Simulator (Packet Tracer) and Implement different LAN topologies.

Practical Assignment #04:

1. **Create a simple network with switch and two or more pc. Also check connectivity between them using ping command or PDU utility.**

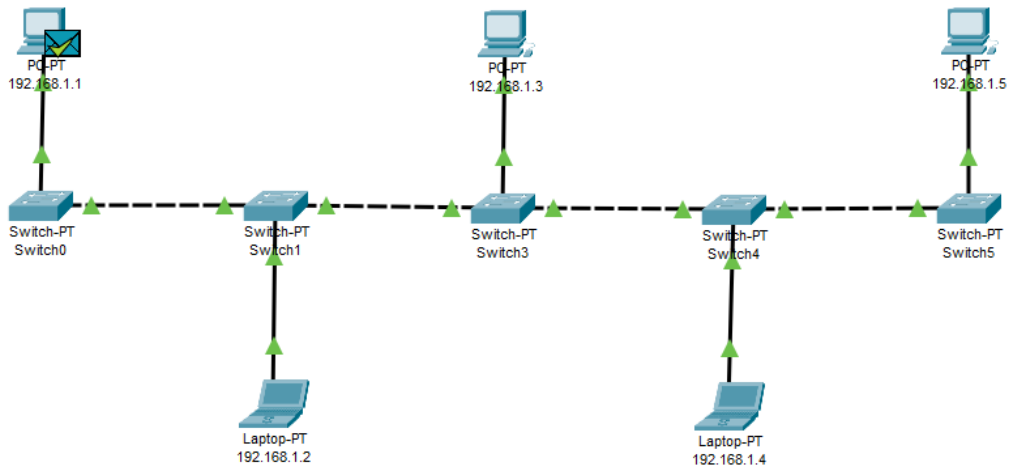


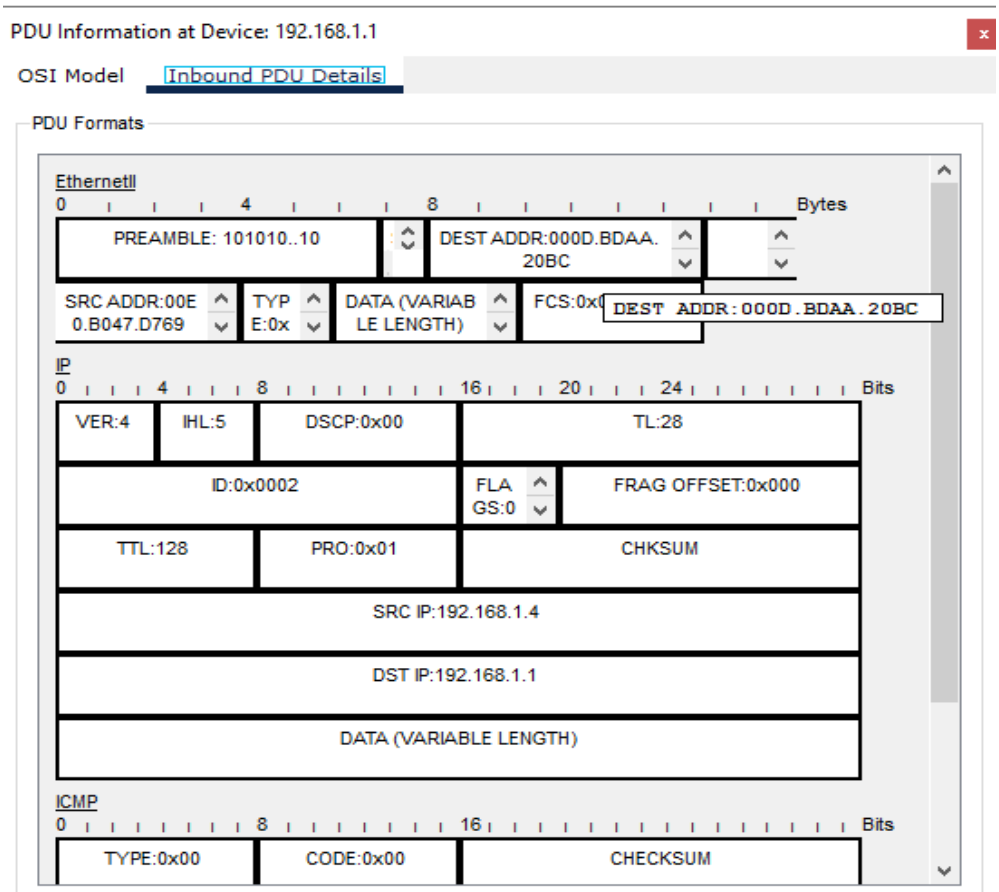


Date: 13/07/2024

2. Implement different topologies in packet tracer.

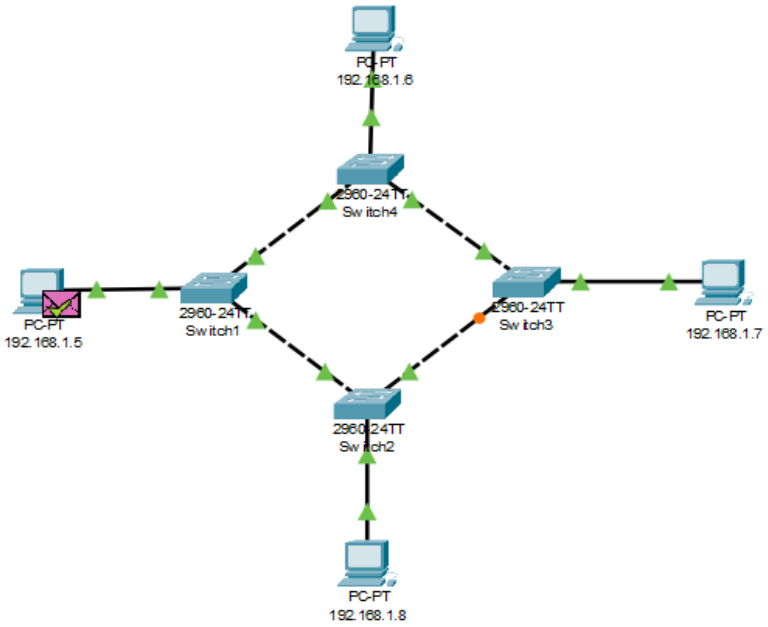
a. Bus

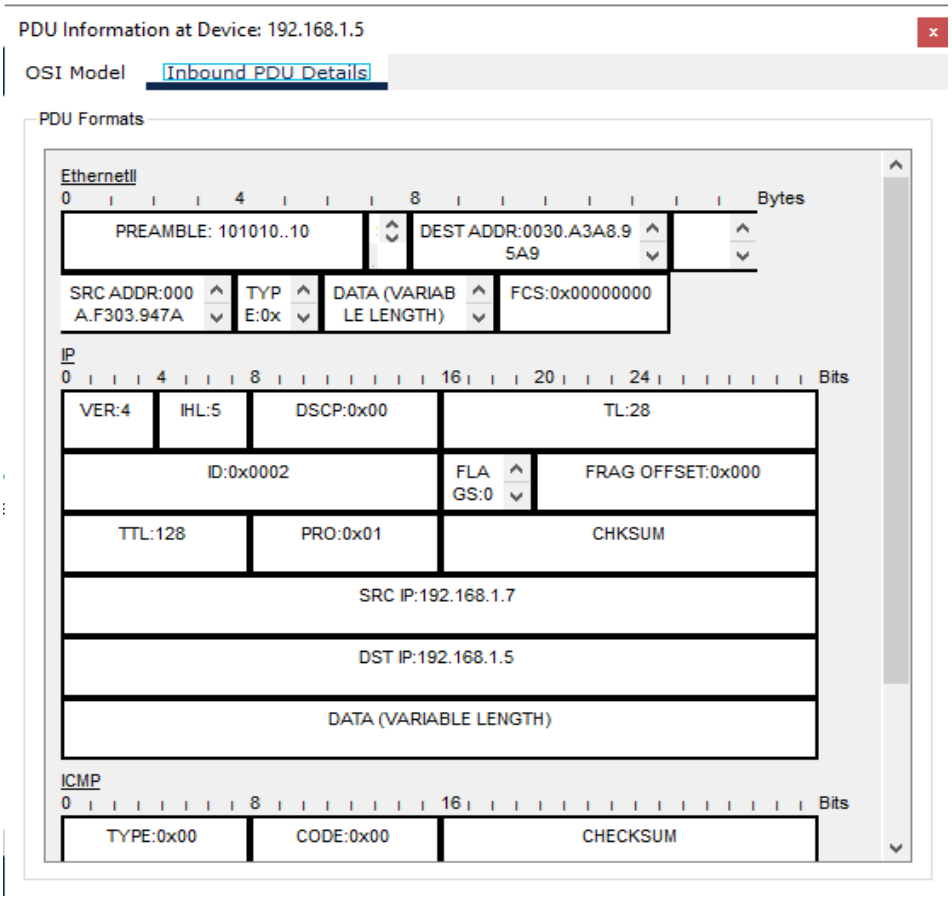




Date: 13/07/2024

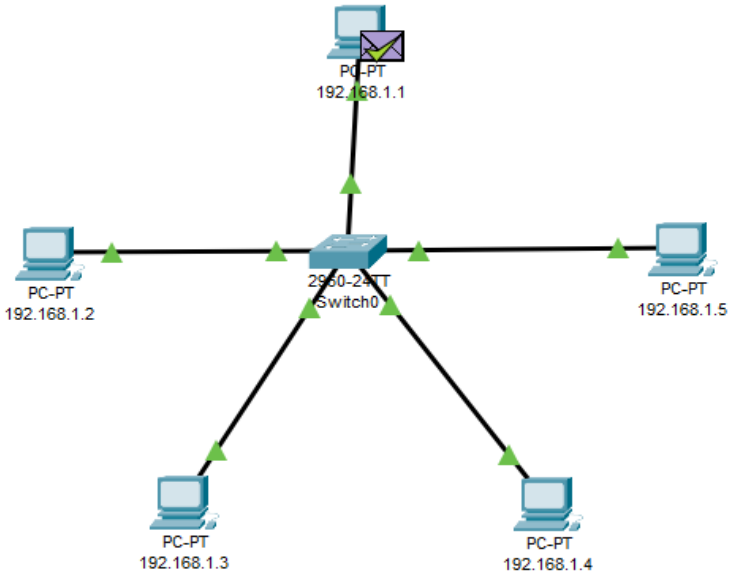
b. Ring

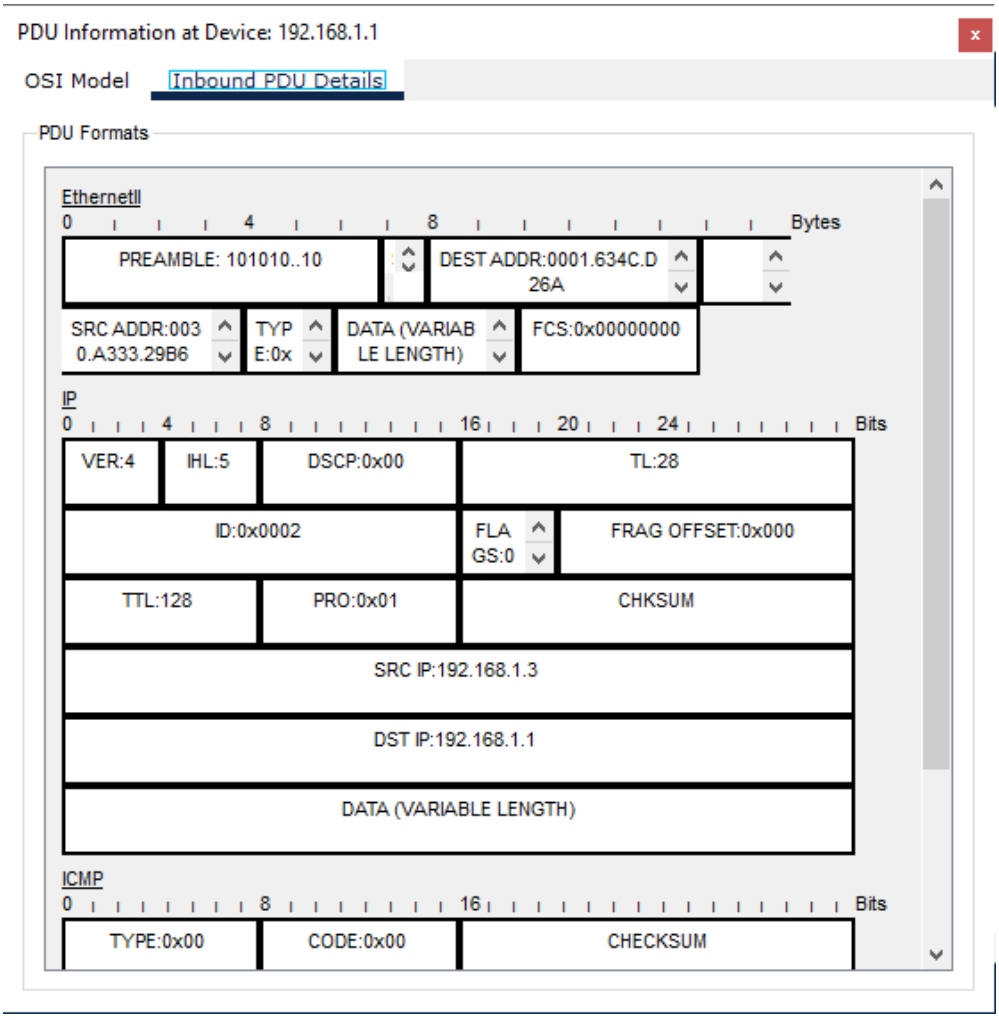




Date: 13/07/2024

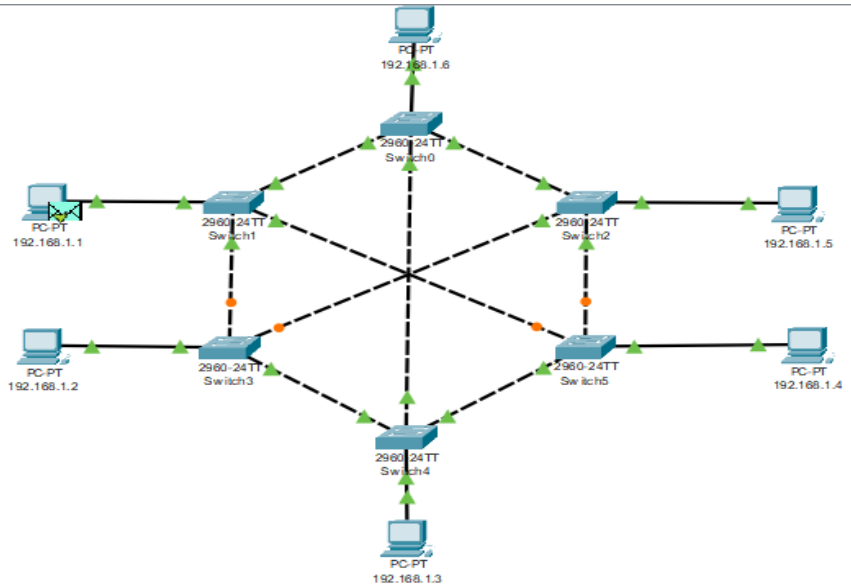
c. Star

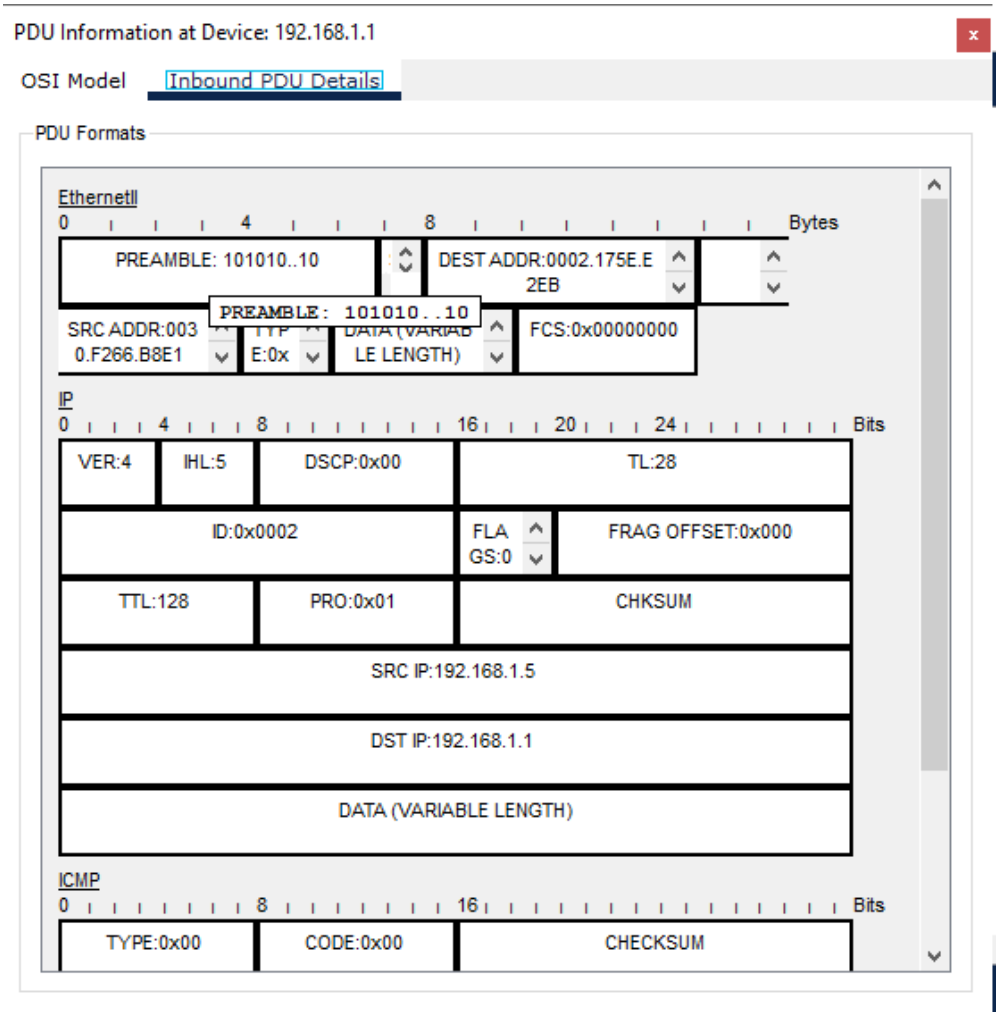




Date: 13/07/2024

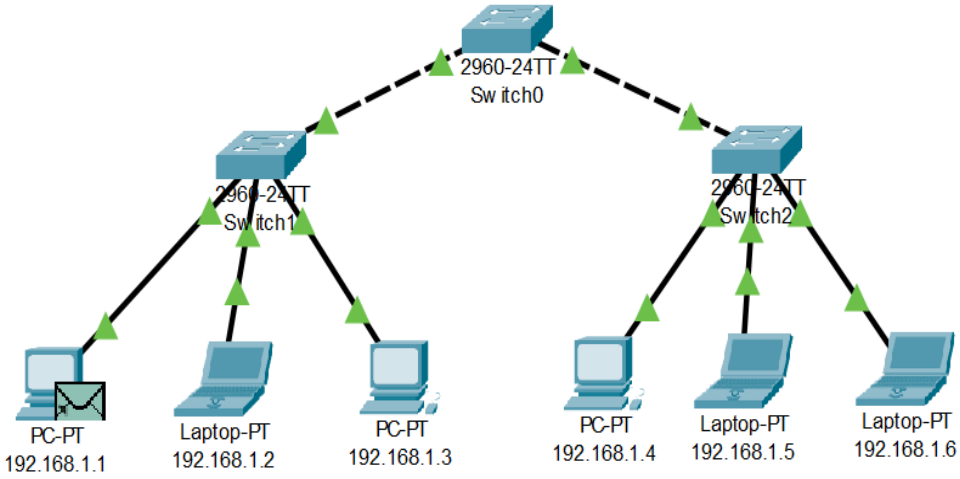
d. Mesh

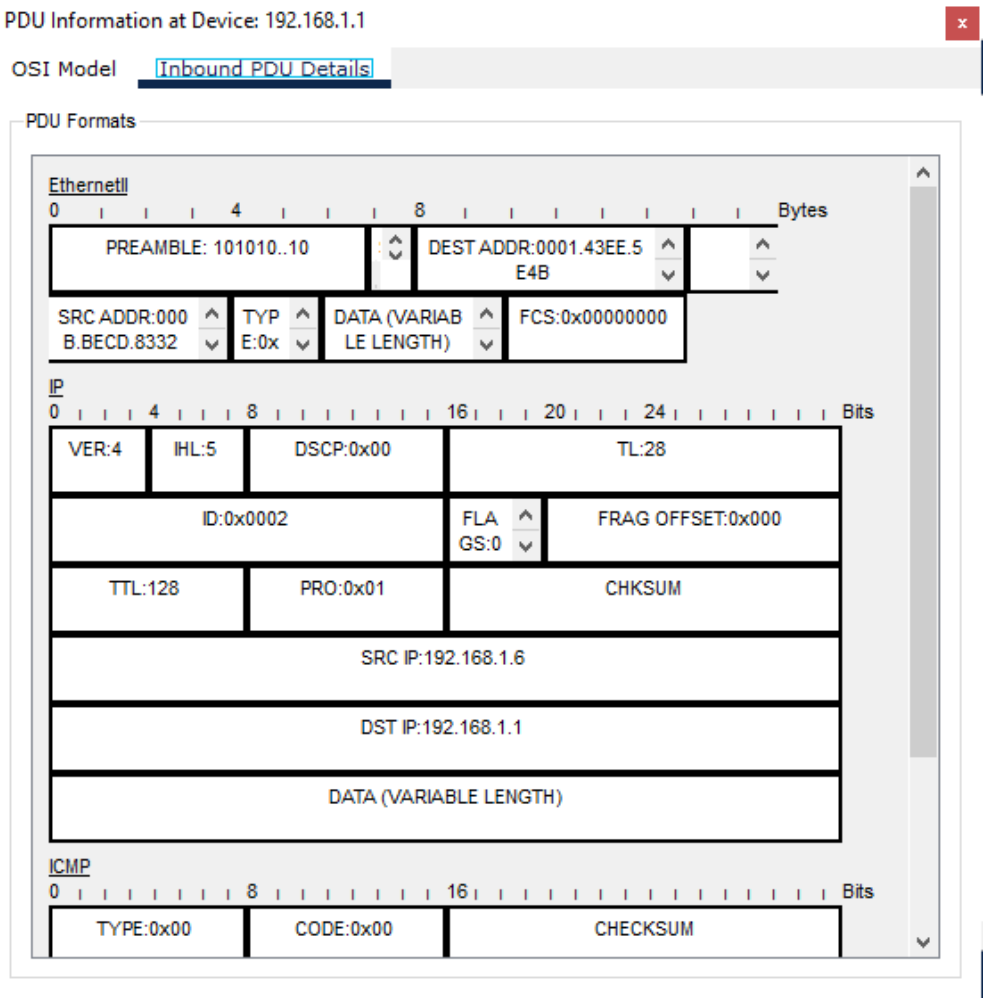




Date: 13/07/2024

e. Tree





Date: 24/07/2024

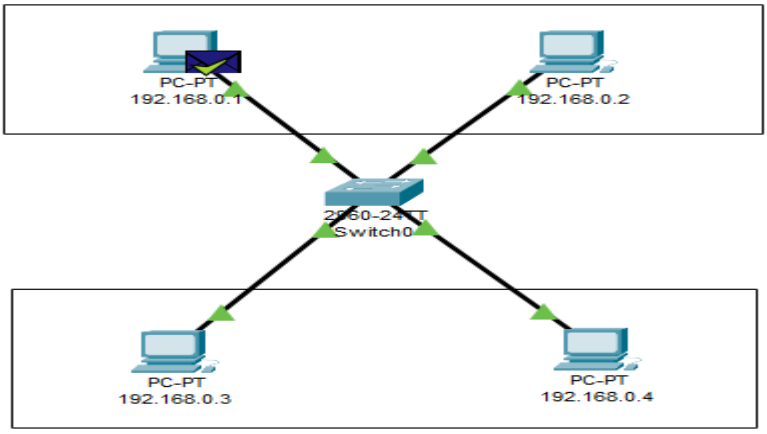
Lab Practical #05:

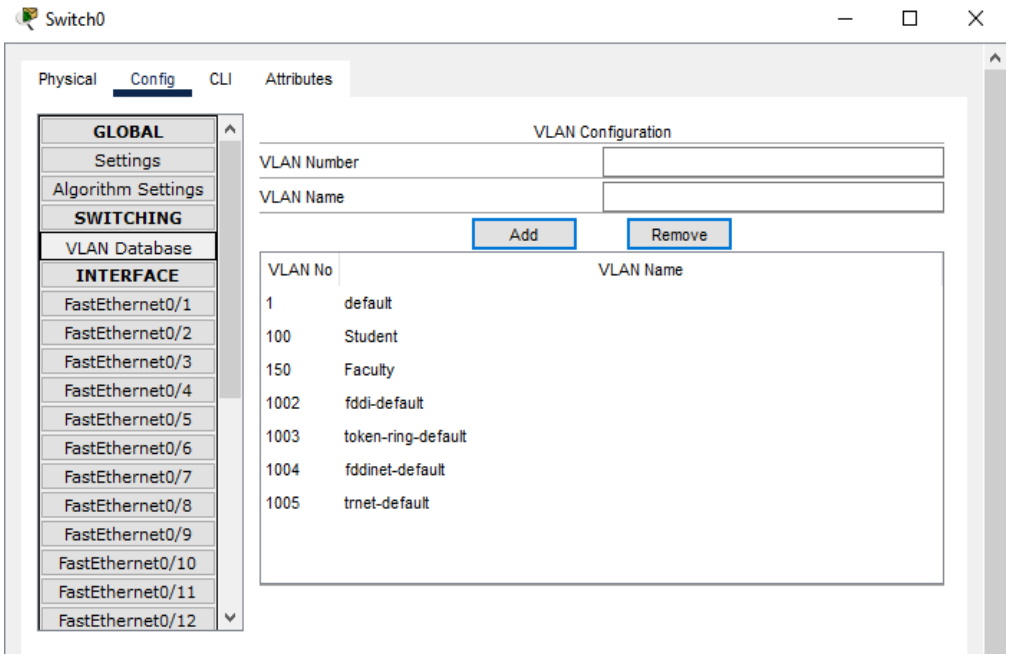
Study the concept of VLAN using packet tracer.

Practical Assignment #05:

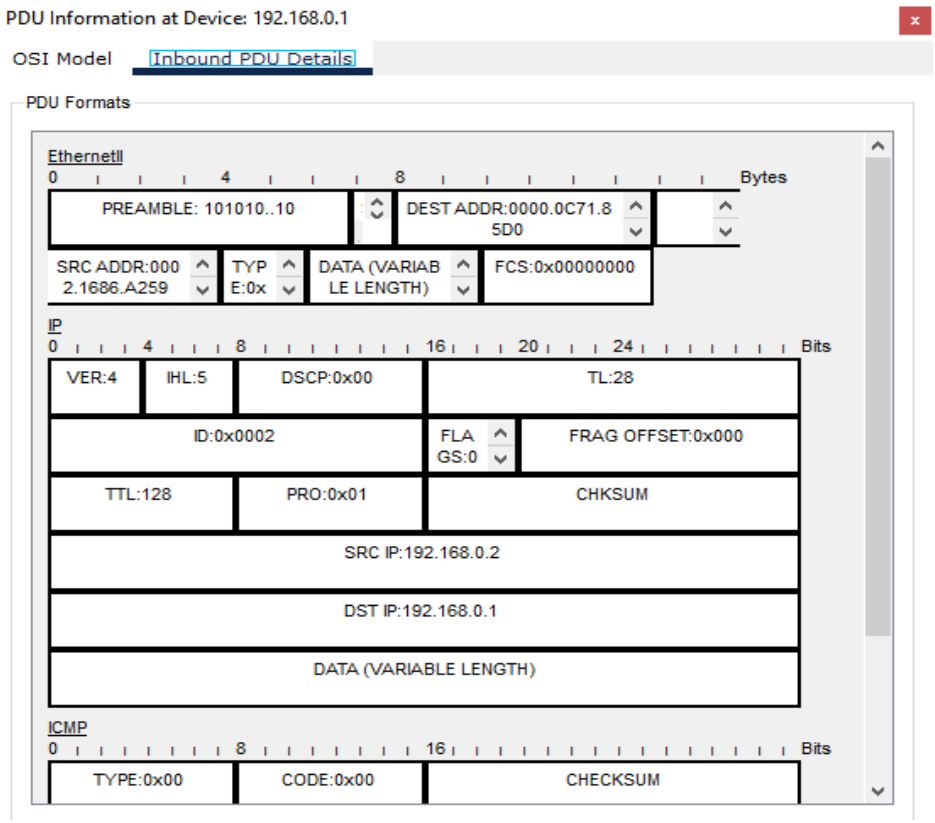
1. **Implement the different network structures in VLAN and VLAN trunking. Also check connectivity between them using ping command or PDU utility.**

Example-1





Date: 24/07/2024



➢ Steps

Step 1: Set Up the Network Devices

1. Add a Switch: - Drag and drop a switch onto the workspace from the "Switches" section.
2. Add PCs: - Drag and drop four PCs onto the workspace from the "End Devices" section.

Step 2: Assign IP Addresses to PCs

- Click on PC to open its configuration window.
- Go to Config tab and after go to FastEthernet0.
- Now set the IP address and set Subnet Mask.
- Click on Setting and set Display Name same as your IP Address.
- Do these for all other PCs.

Step 3: Connect the PCs to the Switch

- o Use the "Copper Straight-Through" cable to connect each PC to the switch.
- o Connect 192.168.0.1 to port FastEthernet0/1.
- o Connect 192.168.0.2 to port FastEthernet0/2.
- o Connect 192.168.0.3 to port FastEthernet0/3.
- o Connect 192.168.0.4 to port FastEthernet0/4.

Step 4: Configure the VLANs

1. Open the Switch Configuration:
   - o Click on the switch to open its configuration window.
   - o Go to the "Config" tab.
2. Create VLANs:
   - o In the "VLAN Database" section, add VLAN 100 and name it "Students".
   - o Add VLAN 150 and name it "Faculty".

Date: 24/07/2024

3. Assign Ports to VLANs:
    - o In the "Interface" section, select FastEthernet0/1.
        - ▪ Set the "VLAN ID" to 100.
    - o Select FastEthernet0/2.
        - ▪ Set the "VLAN ID" to 100.
    - o Select FastEthernet0/3.
        - ▪ Set the "VLAN ID" to 150
    - o Select FastEthernet0/4.
        - ▪ Set the "VLAN ID" to 150.

Step 5: Verify the VLAN Configuration

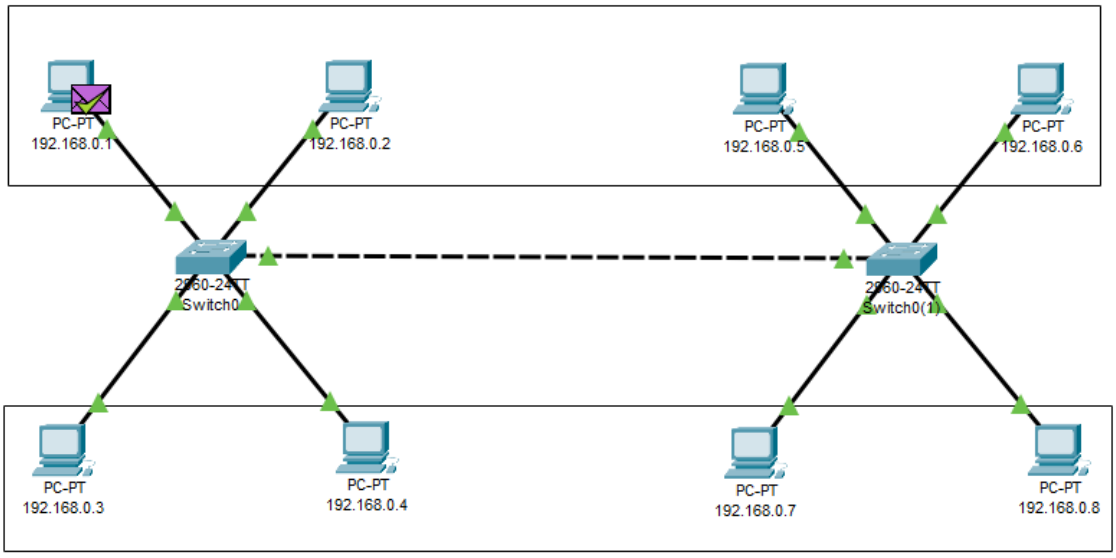
1. Verify VLANs on the Switch:
    - Go to the "VLAN Database" section in the switch configuration and ensure VLAN 100 and VLAN 150 are listed with the correct ports.
2. Test Connectivity:
    - Send a Message (PDU) from PC 192.168.0.1to the 192.168.0.2 if Message was send
    - successfully then VLAN is works.
    - Send a Message (PDU) from 192.168.0.1 to the 192.168.0.2 if Message was failed then VLAN is not works.

Date: 24/07/2024

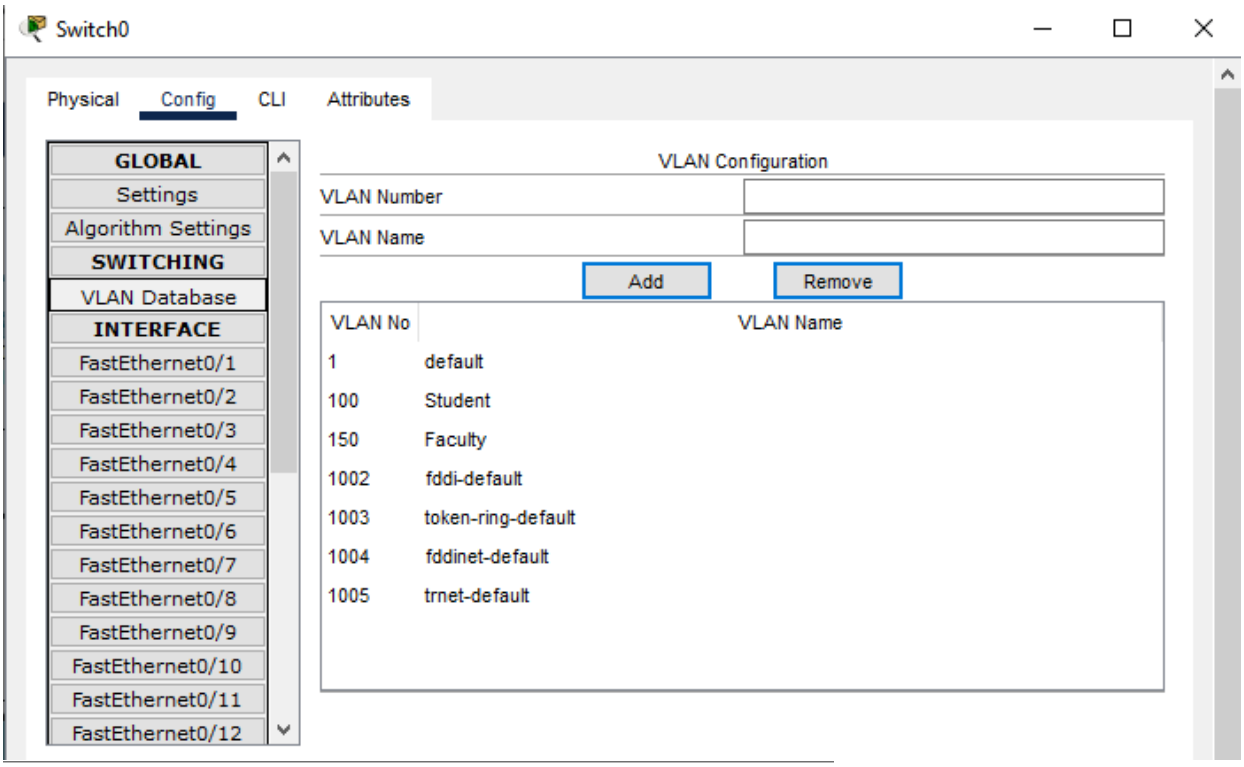
Example-2

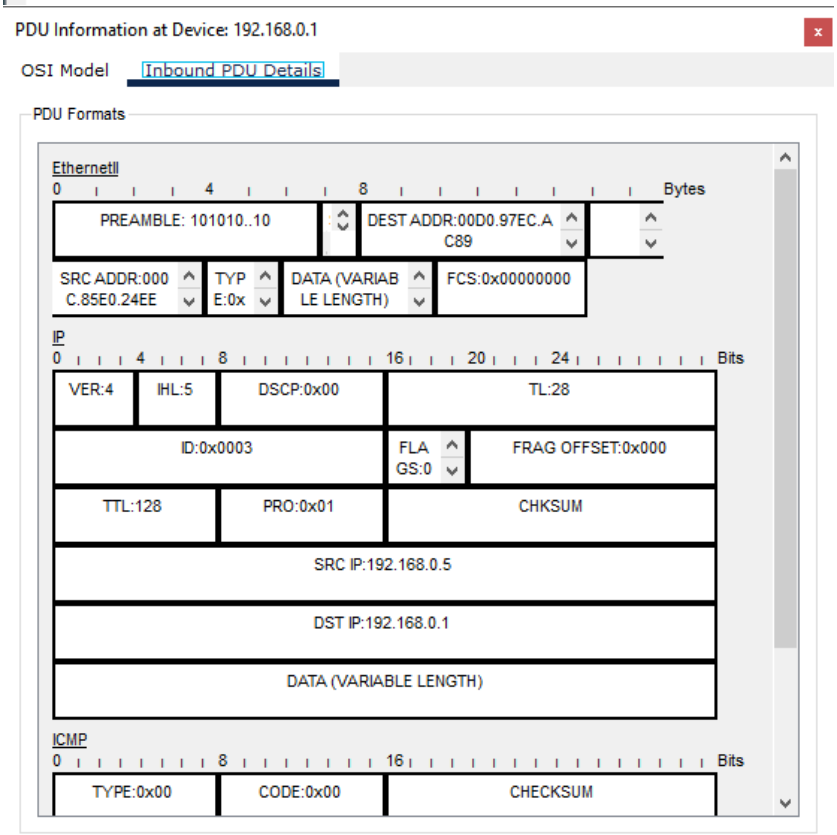
➢ Steps

- Take 8 pc and assign Ip address and label to each pc.
- Take 2 Switch and Make 2 Lan with 4 pc each.
- Now there is local area network but We need to implement Virtual Lan database
- for implement Virtual Lan we need to configure Virtual Lan database in configure
- Section in switch.
- Make 2 New Virtual Lan configuration with unique Virtual Lan number and name.
- Now check the Port where the pc is connected and open that port configuration
- in switch and set Virtual Lan to access mode and select your Virtual Lan database
- name in dropdown.
- Now we need to connect both Switch but here we need to give Virtual Lan mode
- to trunk because there are number different Virtual Lan signal travel threw it.
- Now you configure two Virtual Lan in different local area network



Date: 24/07/2024



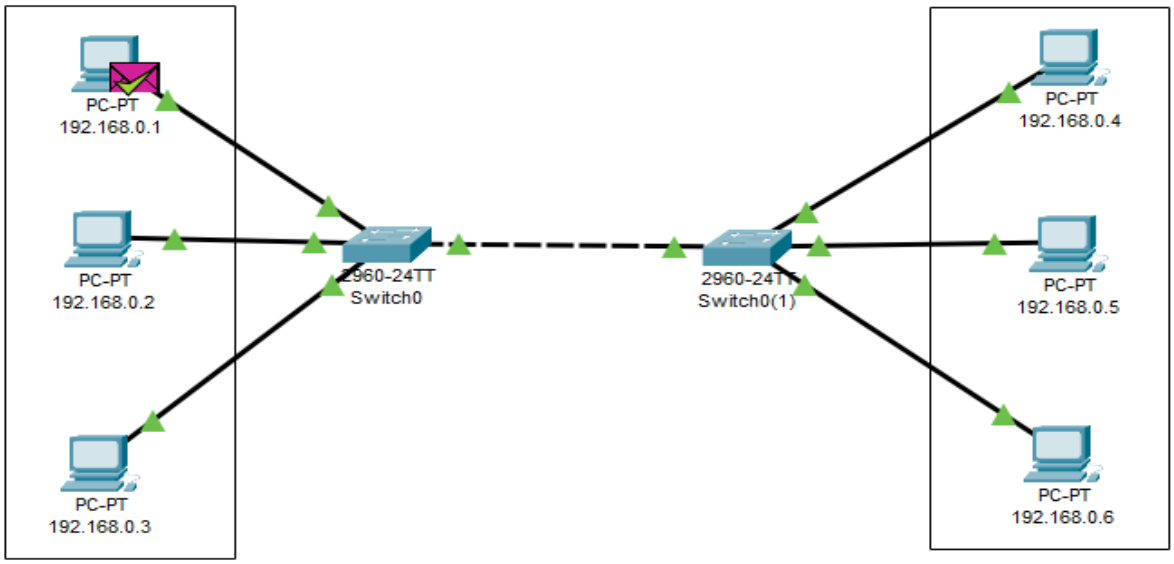


Date: 24/07/2024

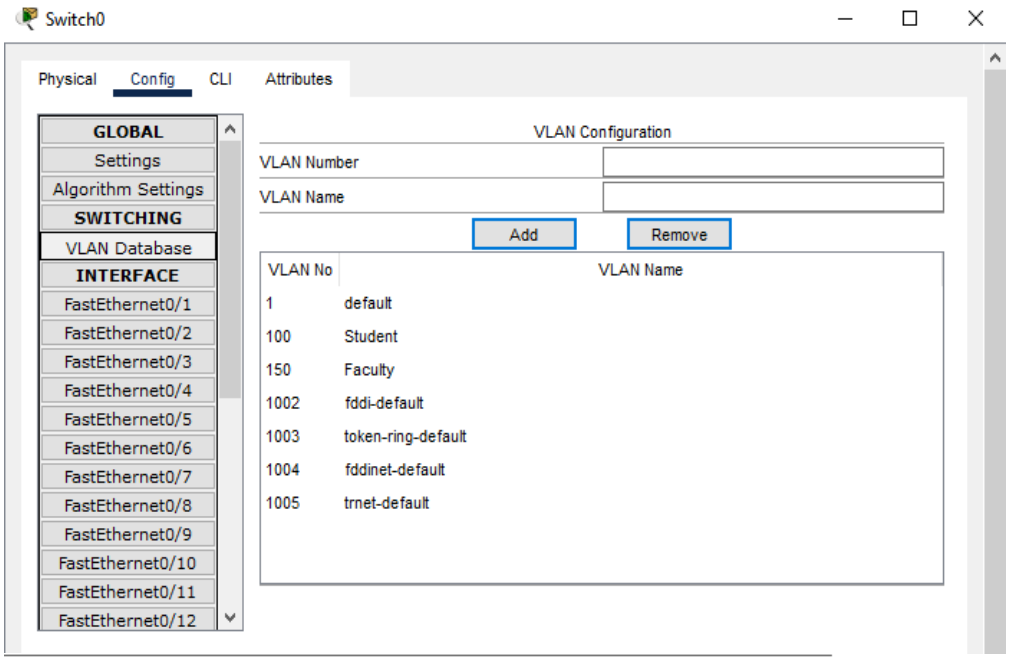
Example-3

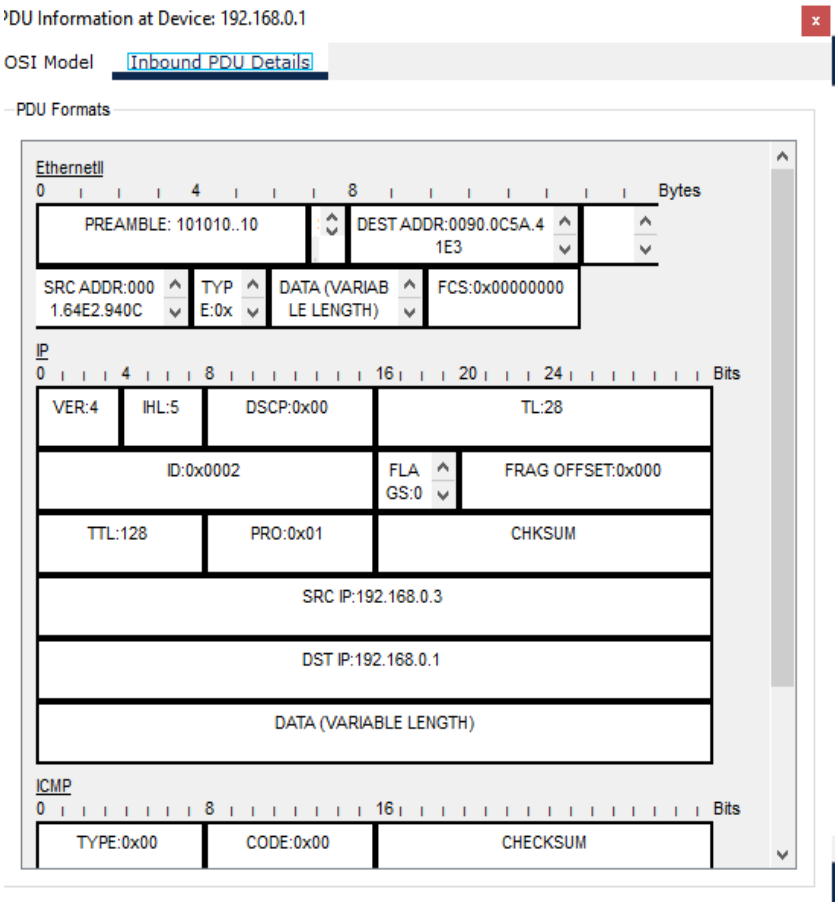
➢ Steps

- Take 6 pc and assign Ip address and label to each pc.
- Take 2 Switch and Make 2 Lan with 3 pc each.
- Now there is local area network first for Group-1(Students) and second for Group2(Faculty) but We need to implement Virtual Lan database for implement Virtual
- Lan we need to configure Virtual Lan database in configure Section in switch.
- Make 2 New Virtual Lan configuration with unique Virtual Lan number and name.
- Now check the Port where the pc is connected and open that port configuration
- in switch and set Virtual Lan to access mode and select your Virtual Lan database
- name in dropdown.
- Now we need to connect both Switch but here we need to give Virtual Lan mode
- to trunk because there are number different Virtual Lan signal travel threw it.
- Now you configure two Virtual Lan in different local area network.



Date: 24/07/2024



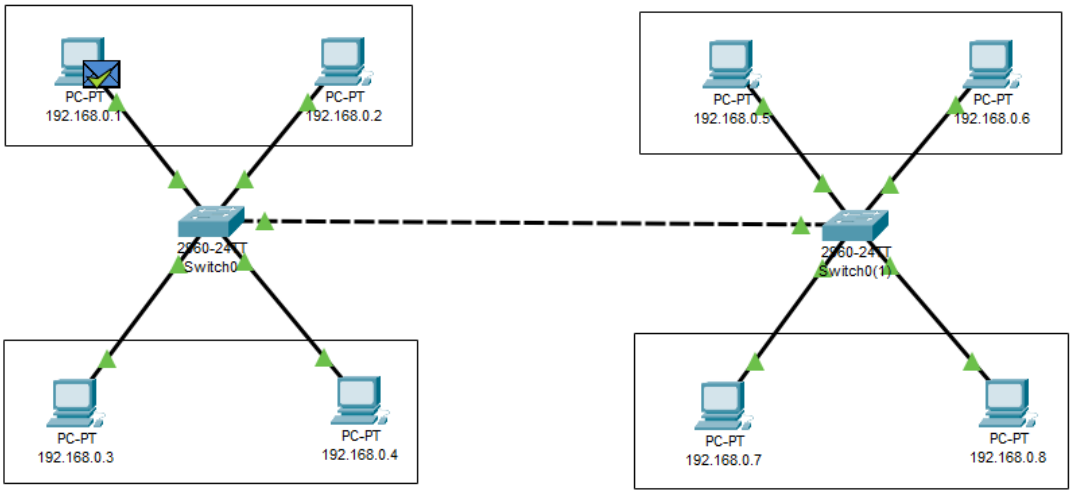


Date: 24/07/2024

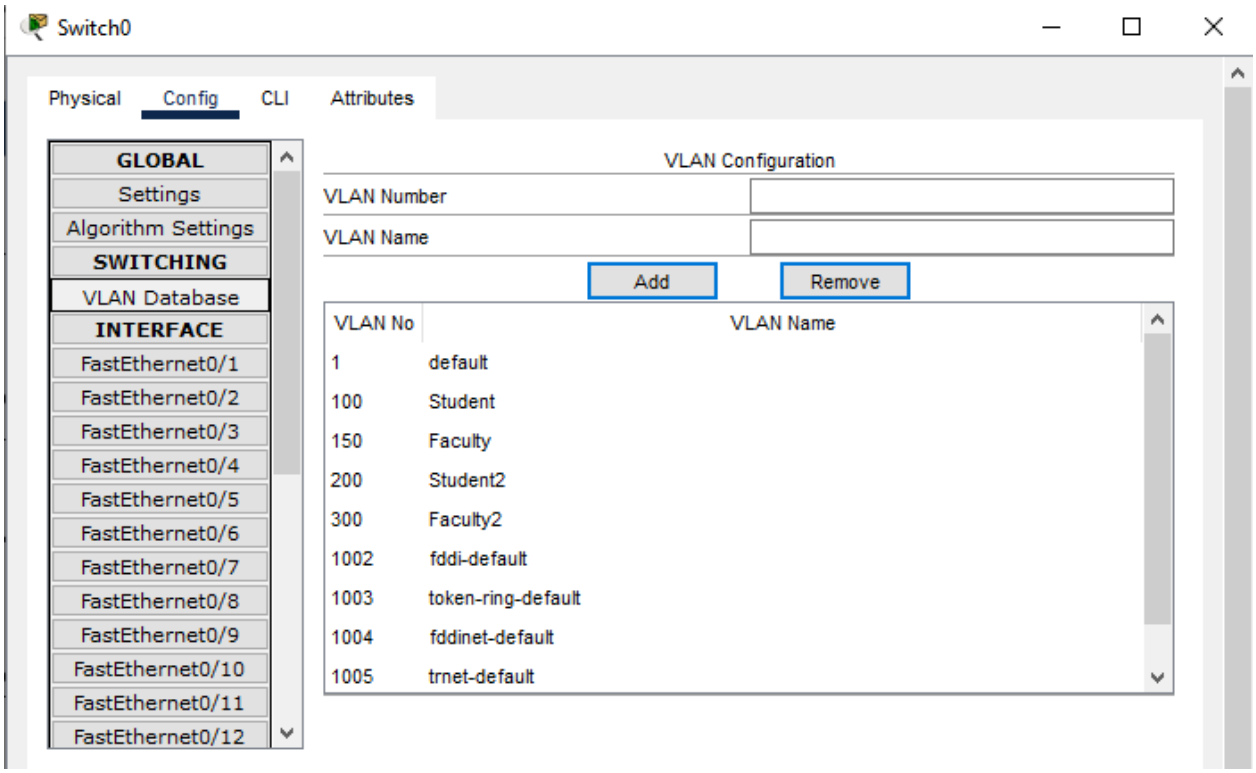
Example-4

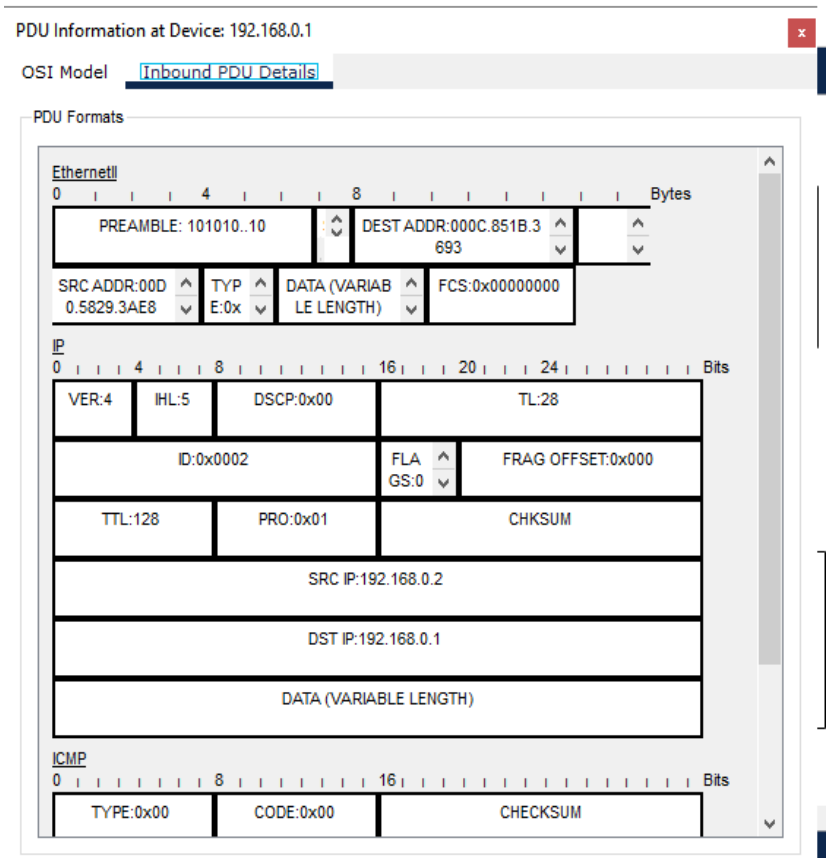
➢ Steps

- Take 8 pc and assign Ip address and label to each pc.
- Take 2 Switch and Make 2 Lan with 4 pc each.
- Now there is local area network and group in to Group-1(Student), Group2(Faculty), Group-3(Student2) and Group-4(Faculty2) but We need to implement Virtual
- Lan database for implement Virtual Lan we need to configure Virtual Lan database
- in configure Section in switch.
- Make 4 New Virtual Lan configuration with unique Virtual Lan number and name.
- Now check the Port where the pc is connected and open that port configuration
- in switch and set Virtual Lan to access mode and select your Virtual Lan database
- name in dropdown.
- Now we need to connect both Switch but here we need to give Virtual Lan mode
- to trunk because there are number different Virtual Lan signal travel threw it.
- Now you configure two Virtual Lan in different local area network.



Date: 24/07/2024





Date: 13/08/2024

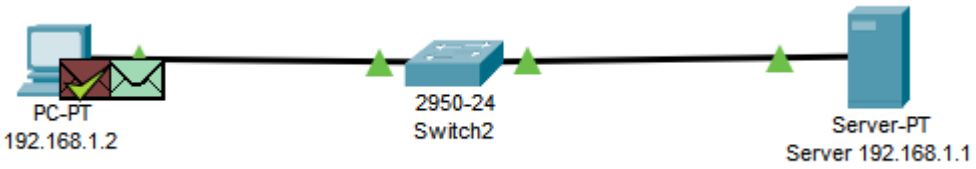
Lab Practical #06:

Study the application layer protocol DNS, DHCP, FTP.

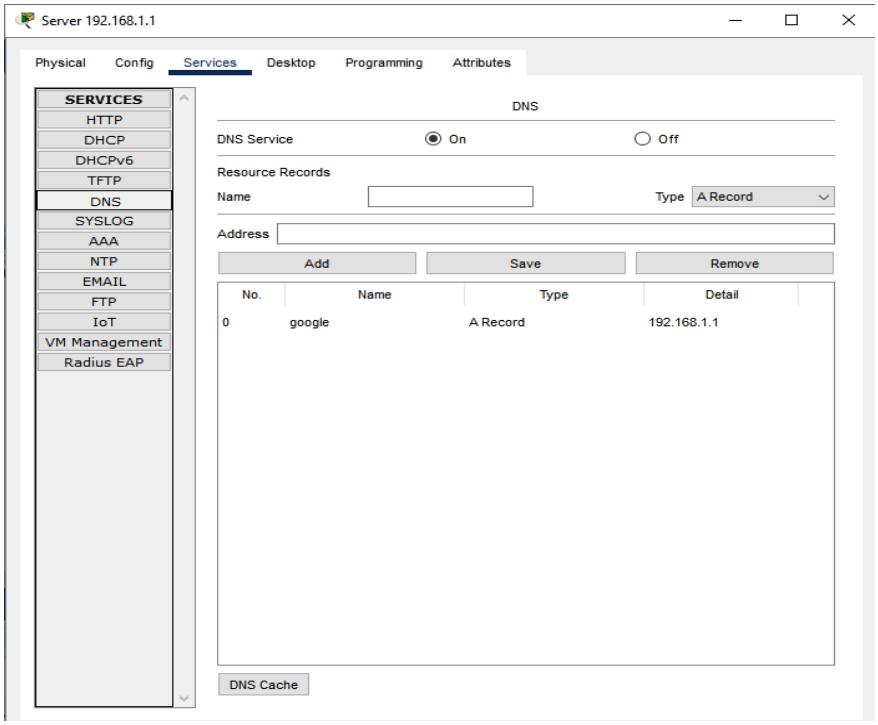
Practical Assignment #06:

1. Implement the application layer protocol DNS, DHCP, and FTP. Also check connectivity between them using ping command or PDU utility.

DNS(Domain Name System) :

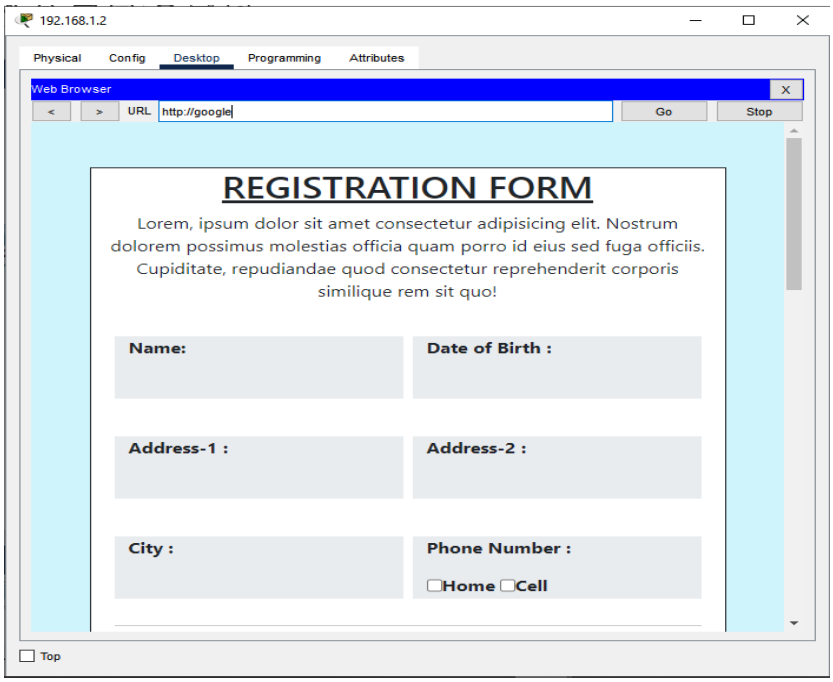


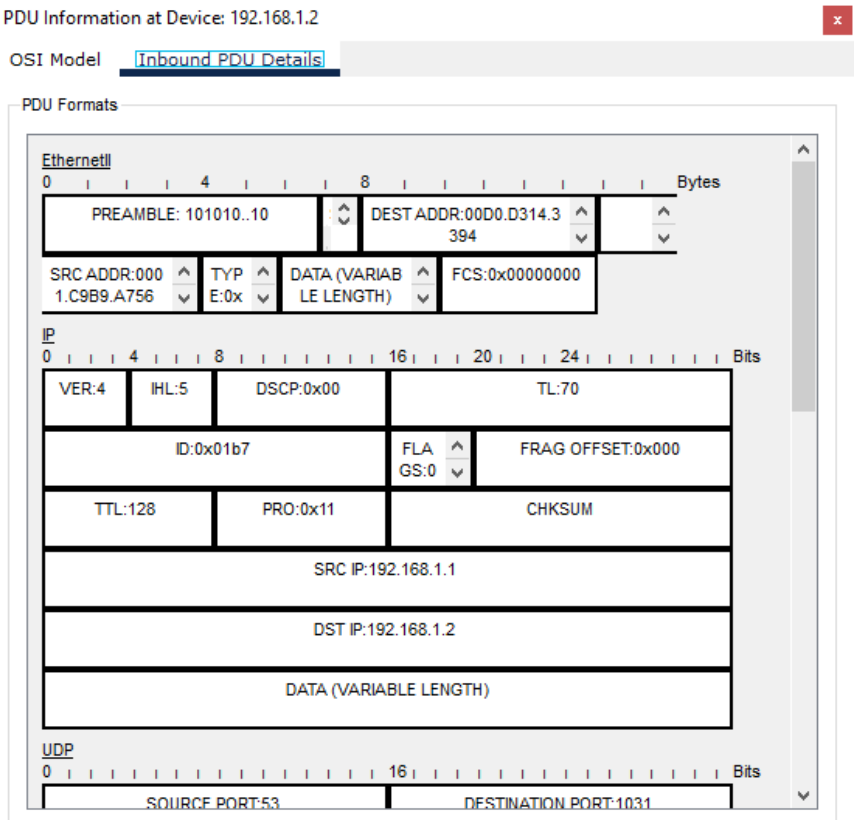
- Make a network displayed as per the above image.
- Assign **192.168.1.1** IP address to Server and assign **192.168.1.2** IP address to PC.
- Click on **Server(192.168.1.1)** and choose **Services**
- Now Choose **DNS** from the left side.
- Now click **On the** radio button as per the below image.
- Fill out **google** in Name textbox and **192.168.1.1** in Address textbox. Click on the Add button.



Date: 13/08/2024

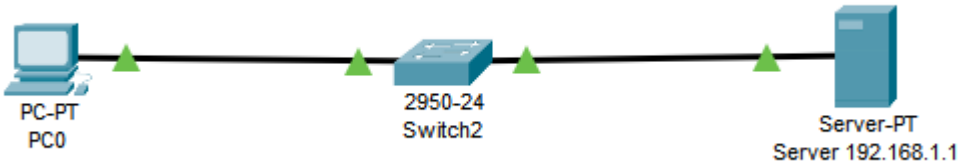
- Click on **192.168.1.2(PC)** and choose **Desktop** then choose **web browser** from it.
- Enter **http://google** in the URL textbox and click on Go.
- After some time output will be displayed.



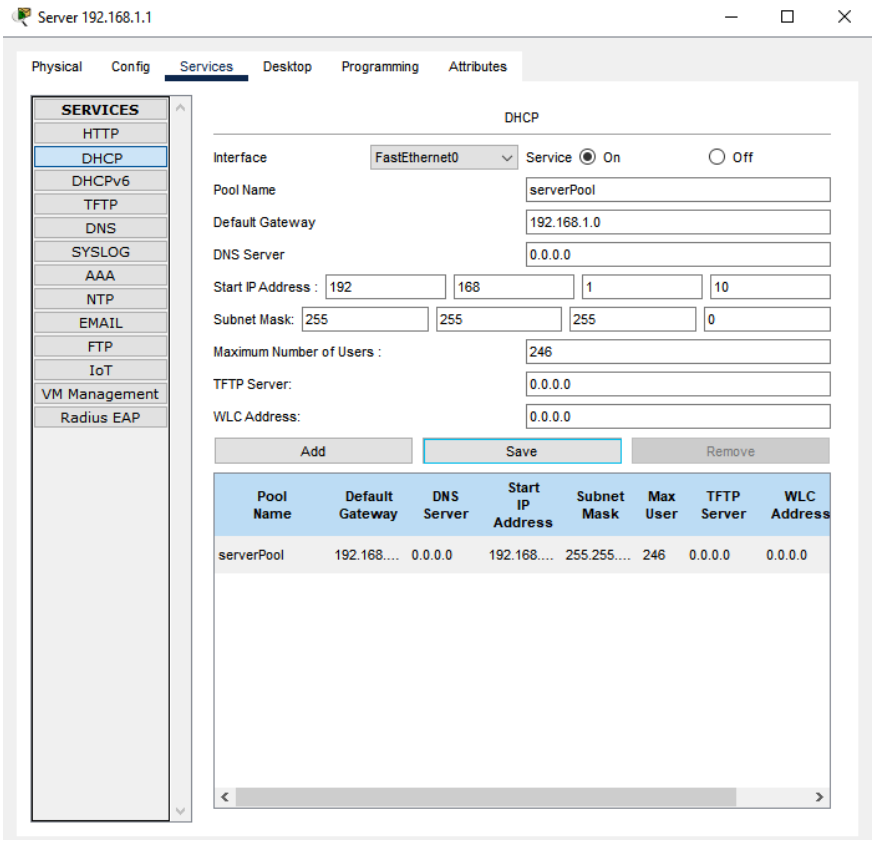


Date: 13/08/2024

DHCP(Dynamic Host Configuration Protocol) :



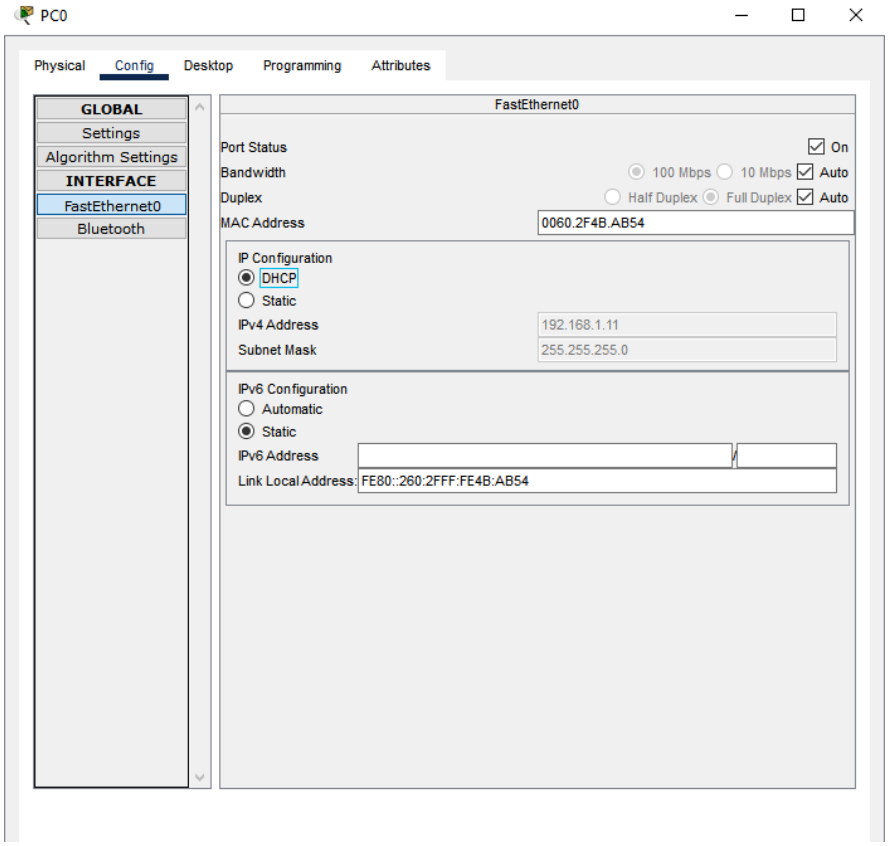
- Make a network displayed as per the above image.
- Assign **192.168.1.1** IP Address to Server.
- Click on Server(**192.168.1.1)** and choose **Services**
- Now Choose **DHCP** from the left side.
- Now select the **On** radio button of Service as per the below image.
- Enter **Default Gateway, Start IP Address, Subnet Mask, and Maximum Number of Users** as per the below image.
- Click on the Add button.
- Your added serverPool will displayed below.

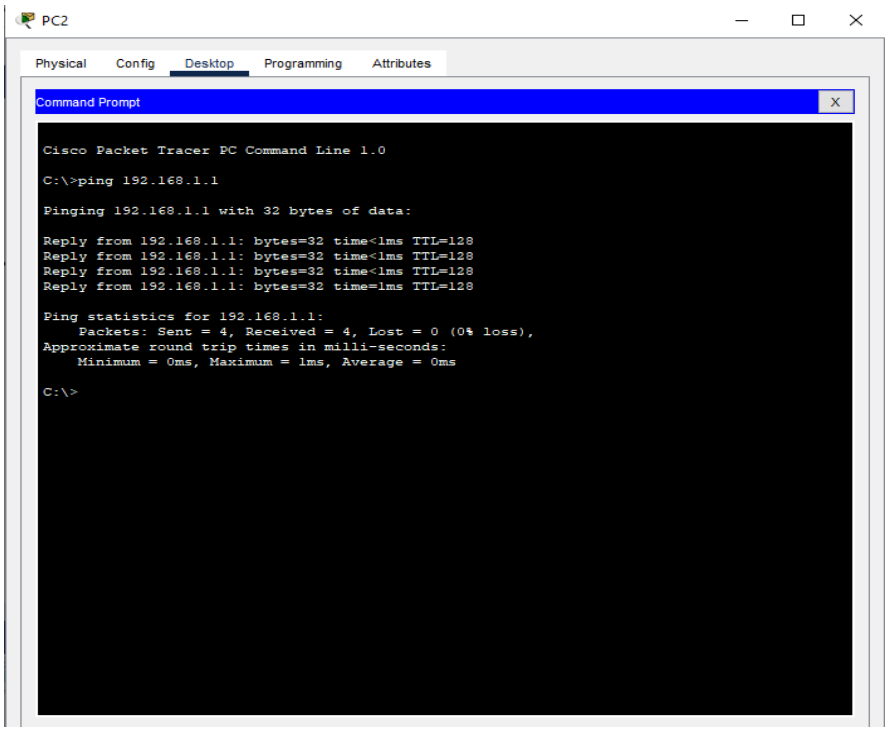


- Click on **PC0** and choose **Config**.
- Choose **FastEthernet0** from the left side.

Date: 13/08/2024

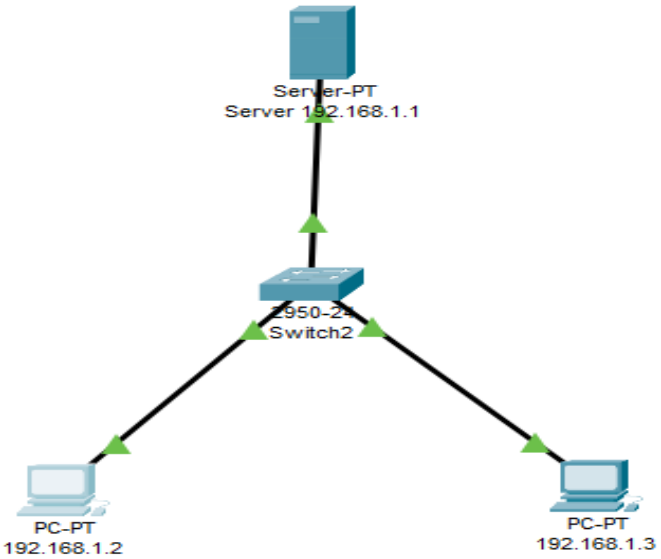
- In the **IP Configuration tab** select **DHCP** after some time server will automatically assign the IP Address from a given range.

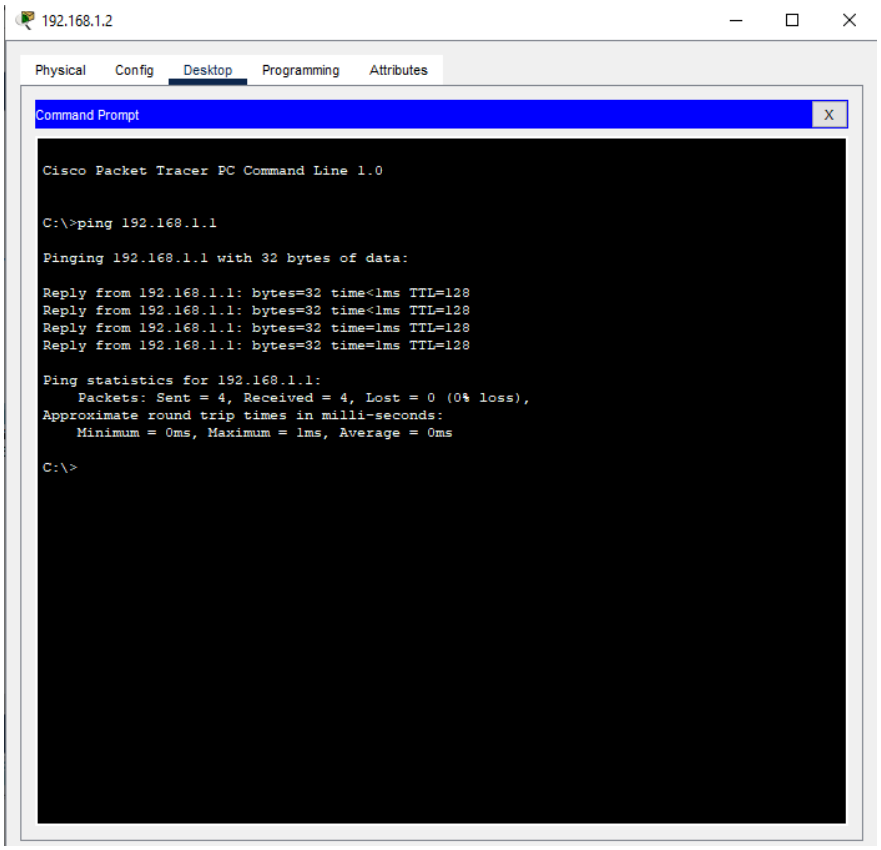




Date: 13/08/2024

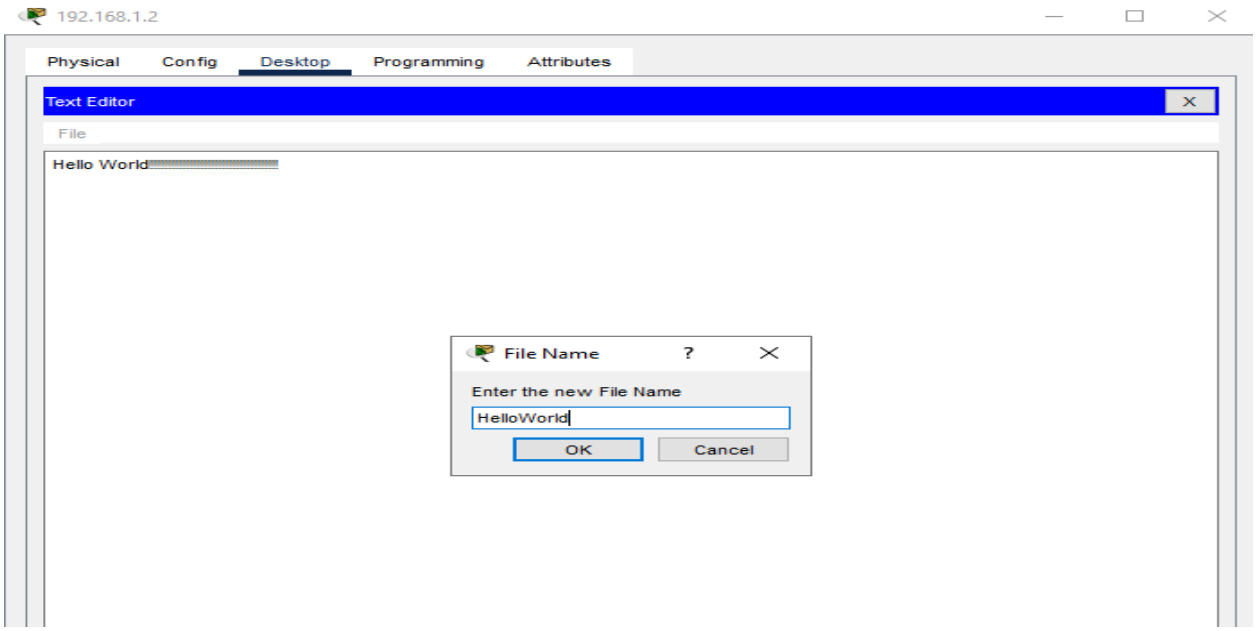
FTP(File Transfer Protocol) :





- Click on **192.168.1.2** choose desktop and select Text Editor
- Make new text file named “HelloWorld.txt”

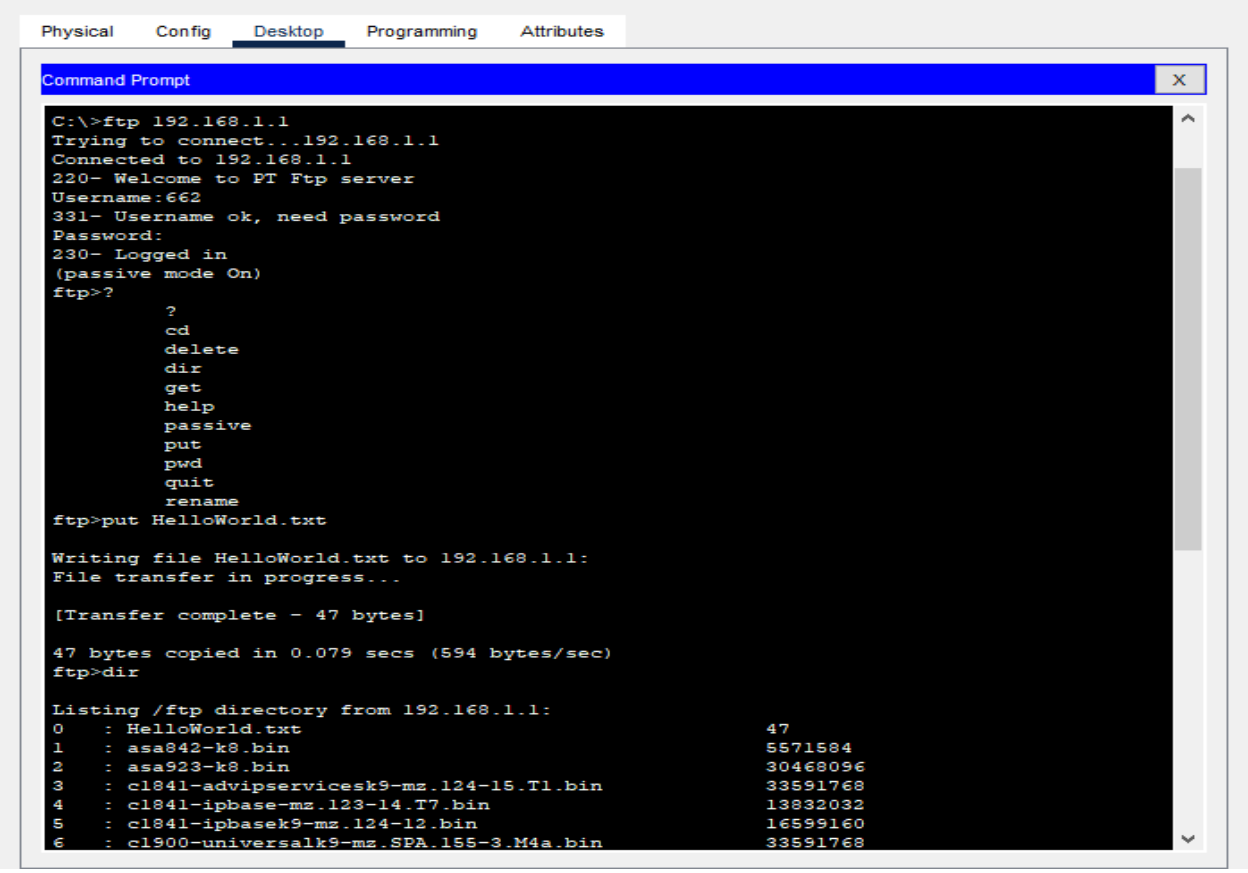
Date: 13/08/2024



- Now again click on **192.168.1.2** and choose **desktop** and select **Command Prompt**.
- Write ftp 192.168.1.1 in Command Prompt.
- Enter **Username** and **Password**.
- Write **"?"** to display all ftp related options.

- Now write **"put HelloWorld.txt"** to upload file on server.
- Now write "**dir"** to check file uploaded to server or not.

Date: 13/08/2024

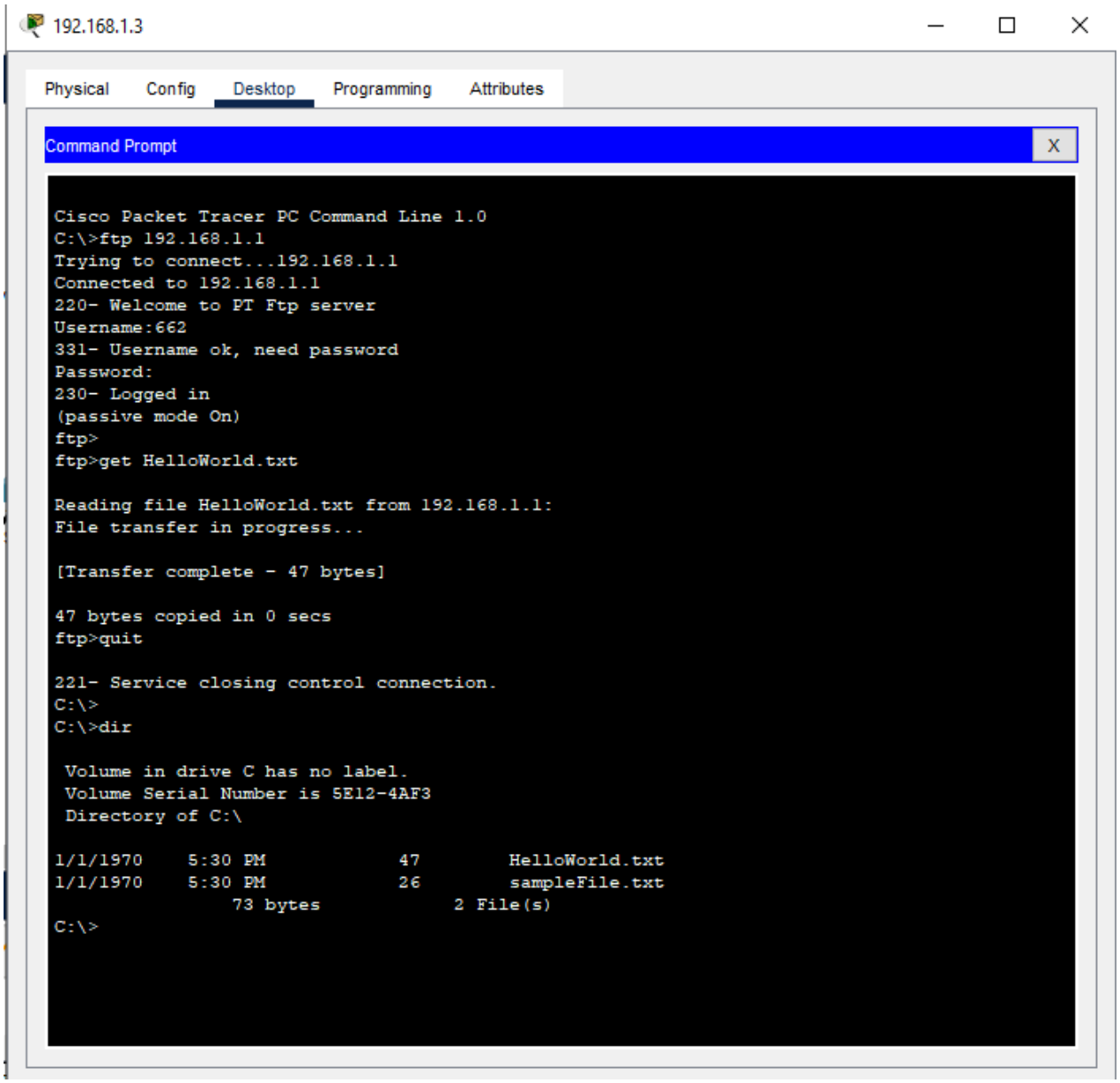


- Write “quit” to close ftp service.

- Now click on **192.168.1.3** and choose **desktop** and select **Command Prompt**.
- Write **ftp 192.168.1.1** in Command Prompt.
- Enter **Username** and **Password.**

- Write **“get HelloWorld.txt”** to download file from server.
- Write “**quit”** to close ftp service.
- Write **“dir”** to check required file downloaded or not.

Date: 13/08/2024



Date: 22/08/2024

Lab Practical #07:

Study Client-Server Socket programming - TCP & UDP

Practical Assignment #07:

1. **Write a C/Java code for TCP Server-Client Socket Programming.**
2. **Write a C/Java code for UDP Server-Client Socket Programming.**

1. For TCP Server-Client:

TCP Server Program:

```
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.io.PrintWriter;
import java.net.ServerSocket;
import java.net.Socket;

public class TCPServer {
   public static void main(String[] args) {
      ServerSocket serverSocket = null;
      Socket clientSocket = null;
      BufferedReader in = null;
      PrintWriter out = null;

      try {
         // Creating server socket
         serverSocket = new ServerSocket(Integer.parseInt(args[0]));
         System.out.println("Server is running on port " + args[0]);
         // Accepting client connection
         clientSocket = serverSocket.accept();
         System.out.println("Client connected");
         // Getting input and output streams
         in = new BufferedReader(new InputStreamReader(clientSocket.getInputStream()));
         out = new PrintWriter(clientSocket.getOutputStream(), true);

         String messageFromClient = in.readLine();
         System.out.println("Received message: " + messageFromClient);
```

```
            // Sending message to client
            out.println("Server received your message: " + messageFromClient);
        } catch (Exception e) {
            e.printStackTrace();
        } finally {
            try {
                if (in != null)
                    in.close();
                if (out != null)
                    out.close();
                if (clientSocket != null)
                    clientSocket.close();
                if (serverSocket != null)
                    serverSocket.close();
            } catch (IOException e) {
                e.printStackTrace();
            }
        }
    }
}
```

TCP Client Program:

```
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.io.PrintWriter;
import java.net.Socket;

public class TCPClient {
    public static void main(String[] args) {
        Socket socket = null;
        BufferedReader in = null;
        PrintWriter out = null;

        try{
            // Creating client socket
```

```
            socket = new Socket(args[0],Integer.parseInt(args[1]));

            // Setting up input and output streams
            in = new BufferedReader(new InputStreamReader(socket.getInputStream()));
            out = new PrintWriter(socket.getOutputStream(), true);

            //sending response from server
            String messageFromServer = in.readLine();
            System.out.println("Message fro server: " + messageFromServer);
        } catch(IOException e){
            e.printStackTrace();
        } finally{
            try {
                if (in != null)
                    in.close();
                if (out != null)
                    out.close();
                if (socket != null)
                    socket.close();
            } catch (IOException e) {
              e.printStackTrace();
            }
        }
    }
}
```

2. For UDP Server-Client:

UDP Server Program:

```
import java.net.DatagramPacket;
import java.net.DatagramSocket;
import java.net.InetAddress;

public class UDPServer {
    public static void main(String[] args) {
        DatagramSocket socket = null;
        try {
```

Date: 22/08/2024

```
            socket = new DatagramSocket(8080);
            byte[] receiveBuffer = new byte[1024];
            byte[] sendBuffer;

            while (true) {
                DatagramPacket receivePacket = new DatagramPacket(receiveBuffer, receiveBuffer.length);
                socket.receive(receivePacket);
                String clientMessage = new String(receivePacket.getData(), 0, receivePacket.getLength());
                System.out.println("Client: " + clientMessage);

                InetAddress clientAddress = receivePacket.getAddress();
                int clientPort = receivePacket.getPort();

                String serverMessage = "Hello from server";
                sendBuffer = serverMessage.getBytes();
                DatagramPacket sendPacket = new DatagramPacket(sendBuffer, sendBuffer.length, clientAddress,
                        clientPort);
                socket.send(sendPacket);
            }
        } catch (Exception e) {
            e.printStackTrace();
        } finally {
            if (socket != null && !socket.isClosed()) {
                socket.close();
            }
        }
    }
}
```

UDP Client Program:

```
import java.net.DatagramPacket;
import java.net.DatagramSocket;
import java.net.InetAddress;

public class UDPClient {
    public static void main(String[] args) {
        DatagramSocket socket = null;
```

Date: 22/08/2024

```
        try {
            socket = new DatagramSocket();
            InetAddress serverAddress = InetAddress.getByName("localhost");
            byte[] sendBuffer;
            byte[] receiveBuffer = new byte[1024];

            String clientMessage = "Hello from client";
            sendBuffer = clientMessage.getBytes();
            DatagramPacket sendPacket = new DatagramPacket(sendBuffer, sendBuffer.length, serverAddress, 8080);
            socket.send(sendPacket);

            DatagramPacket receivePacket = new DatagramPacket(receiveBuffer, receiveBuffer.length);
            socket.receive(receivePacket);
            String serverMessage = new String(receivePacket.getData(), 0, receivePacket.getLength());
            System.out.println("Server: " + serverMessage);
        } catch (Exception e) {
            e.printStackTrace();
        } finally {
            if (socket != null && !socket.isClosed()) {
                socket.close();
            }
        }
    }
}
```

Date: 22/08/2024

Lab Practical #08:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #08:

1. Explain usage of Wireshark tool.

Wireshark is a network protocol analyzer that captures and inspects data traveling across a network in real-time. It's an essential tool for network administrators, cybersecurity professionals, and developers for troubleshooting, analysis, and monitoring of network traffic

How to Use :

1. **Install Wireshark:** First, download and install Wireshark from the official website.
2. **Select a Network Interface:** When you open Wireshark, you'll see a list of network interfaces (like Wi-Fi, Ethernet). These represent the different connections your computer is using. Choose the one you want to monitor (e.g., your Wi-Fi connection).
3. **Start Capturing Packets:** Click the "Start Capturing Packets" button (the blue shark fin icon). Wireshark will begin recording all the network traffic passing through the selected interface.
4. **Analyze the Data:** As Wireshark captures packets, you'll see them listed in real-time with details like the source and destination IP addresses, protocols used, and data. You can stop the capture at any time to analyze the data more closely.
5. **Use Filters:** Wireshark lets you apply filters to narrow down the data. For example, you can filter by IP address, protocol, or even specific data within the packets.
6. **Save and Export:** Once you've captured the data you need, you can save it for future analysis or export it in various formats

Usage:

- **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.
- **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.
- **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.
- **Network Troubleshooting:** Identify and diagnose issues like slow network performance, packet loss, or connectivity problems by analyzing packet data.
- **Protocol Analysis:** Examine how specific protocols (e.g., HTTP, DNS, TCP) operate on the network, helping in debugging and understanding network communication.

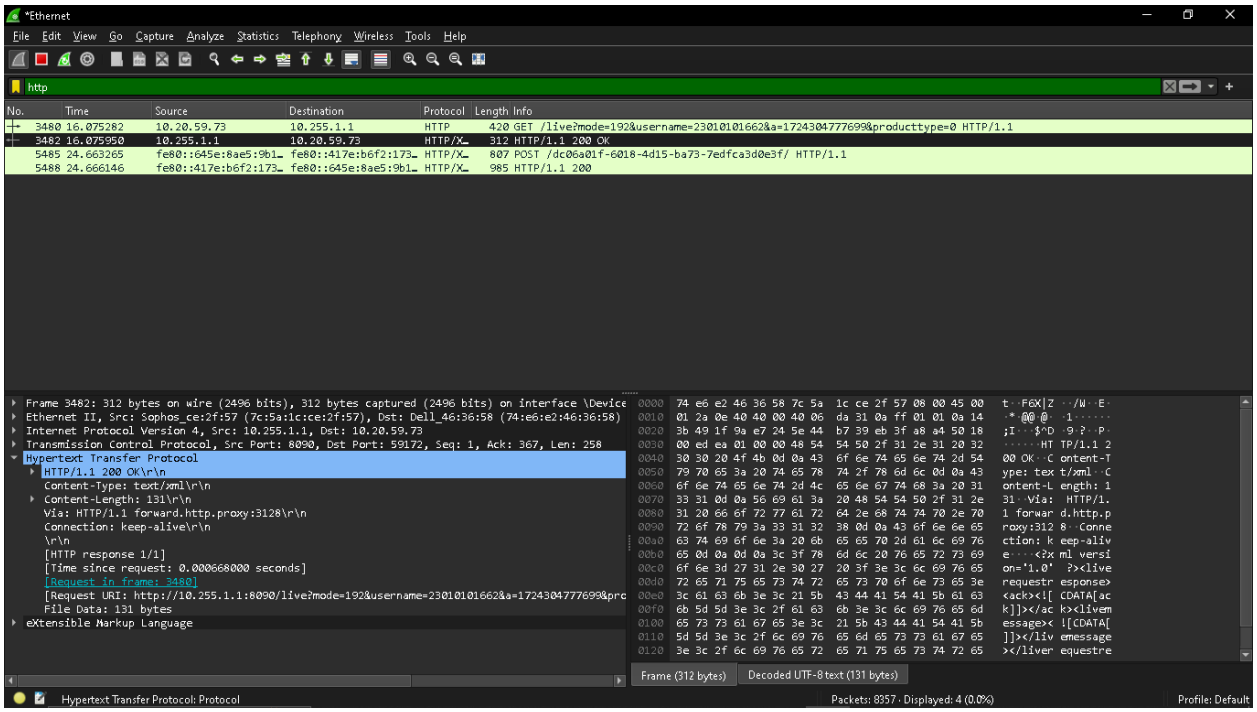
Date: 22/08/2024

- **Security Monitoring:** Detect unauthorized access, malware activity, or unusual traffic patterns that could indicate a security breach.
- **Application Performance Tuning:** Monitor and optimize the performance of networked applications by analyzing the communication between client and server.
- **VoIP Analysis:** Capture and analyze Voice over IP (VoIP) traffic to troubleshoot call quality issues and inspect SIP and RTP protocols.
- **Network Forensics:** Investigate network incidents, such as data breaches or cyberattacks, by reviewing captured packet data for evidence.
- **Learning and Education:** Study network protocols, packet structures, and traffic patterns to enhance your understanding of networking concepts.
- **Bandwidth Usage Analysis:** Monitor and analyze network bandwidth consumption to identify heavy bandwidth users or applications.
- **Network Mapping:** Visualize the flow of data across the network, helping in understanding network topology and device communication.
- **Compliance Auditing:** Ensure that network communications adhere to organizational policies and regulatory requirements by capturing and inspecting relevant traffic.

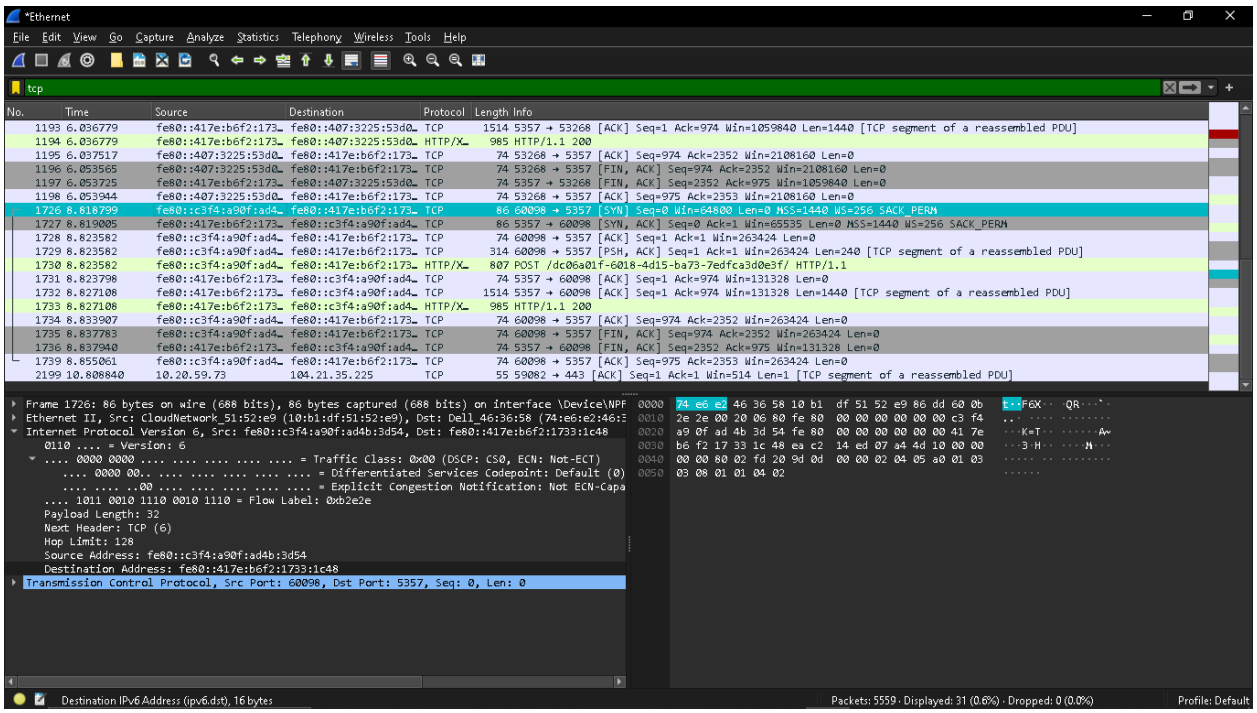
Date: 22/08/2024

2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

- **HTTP :**

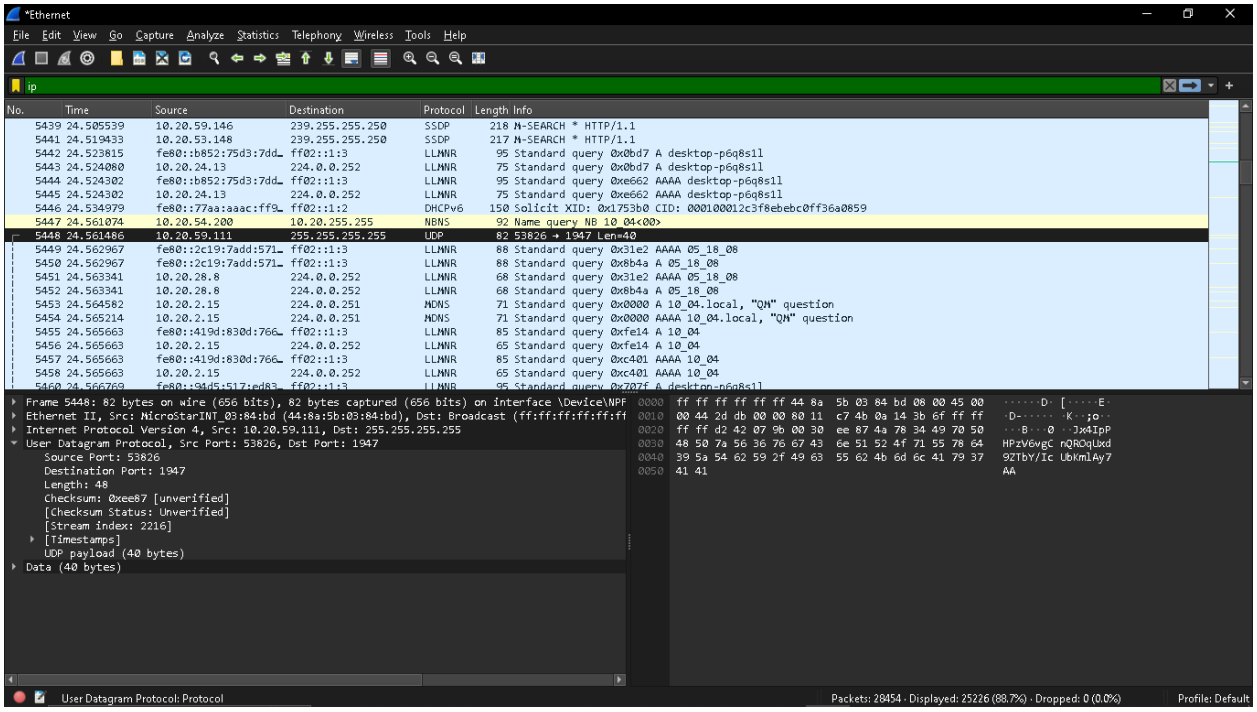


- **TCP :**

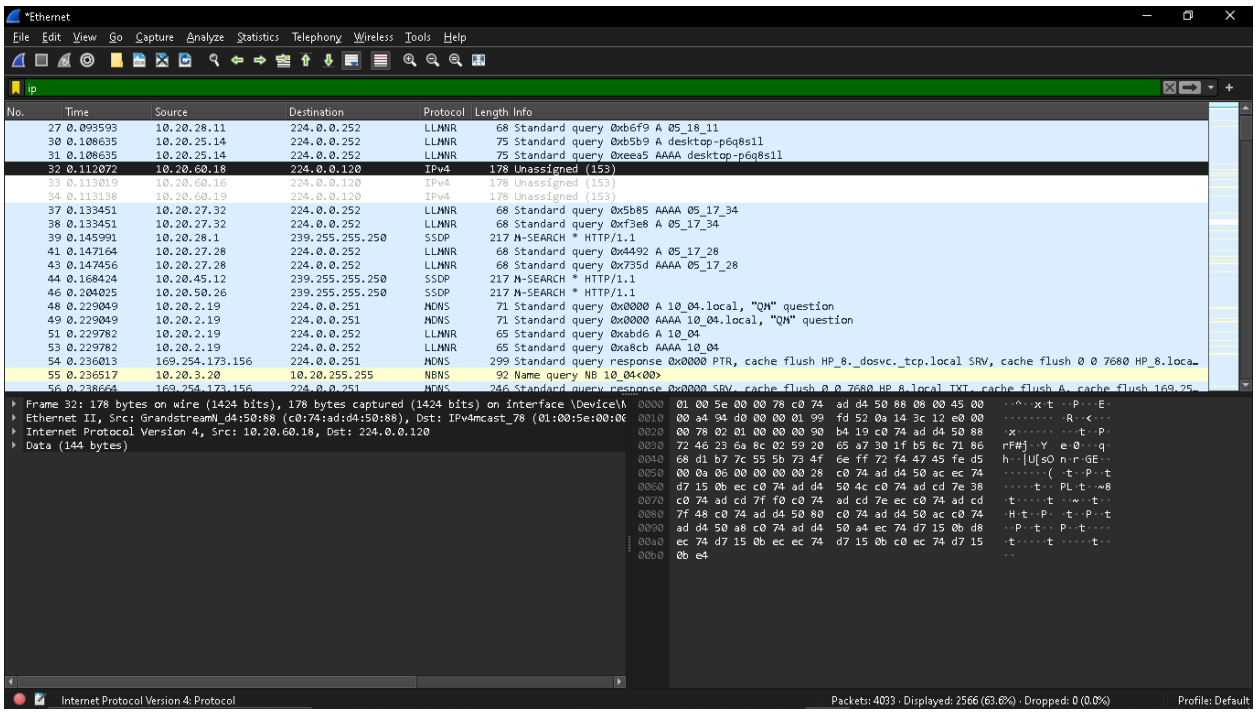


Date: 22/08/2024

- **UDP :**



- **IP :**



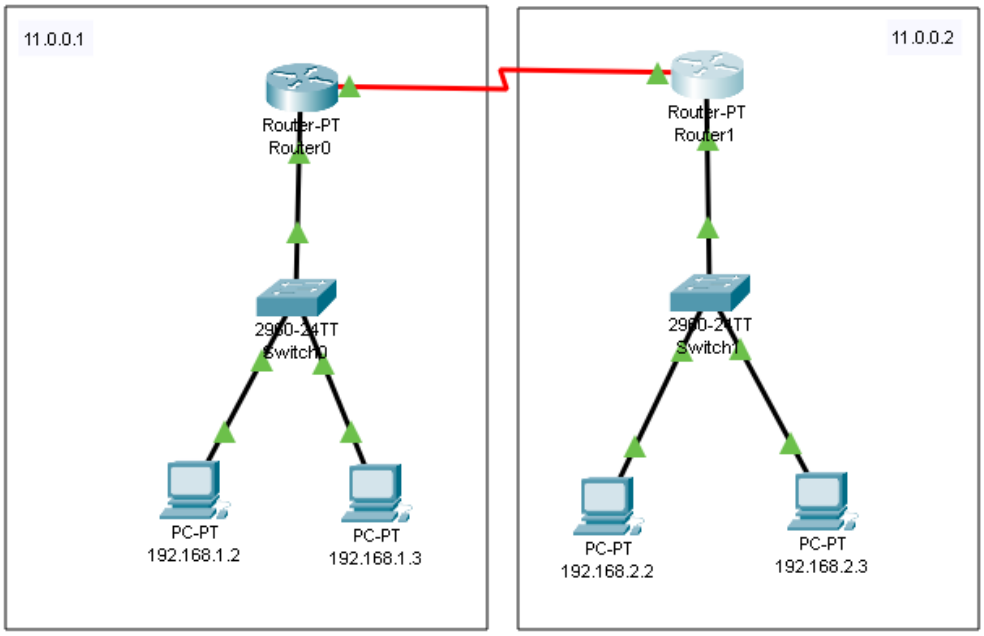
Date: 17/ 09/2024

Lab Practical #10:

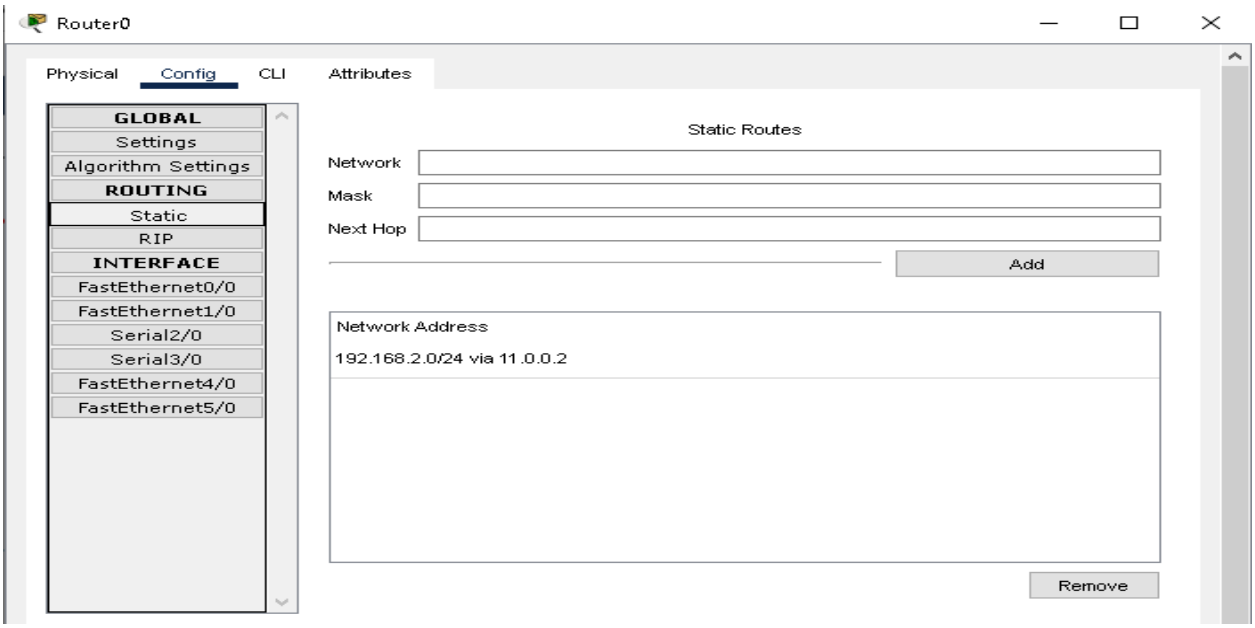
Study the concept of routing using packet tracer. (Static Routing)

Practical Assignment #10:

1. Connect the two different networks based on the calculated IP addresses and subnet using a packet tracer.
   Router

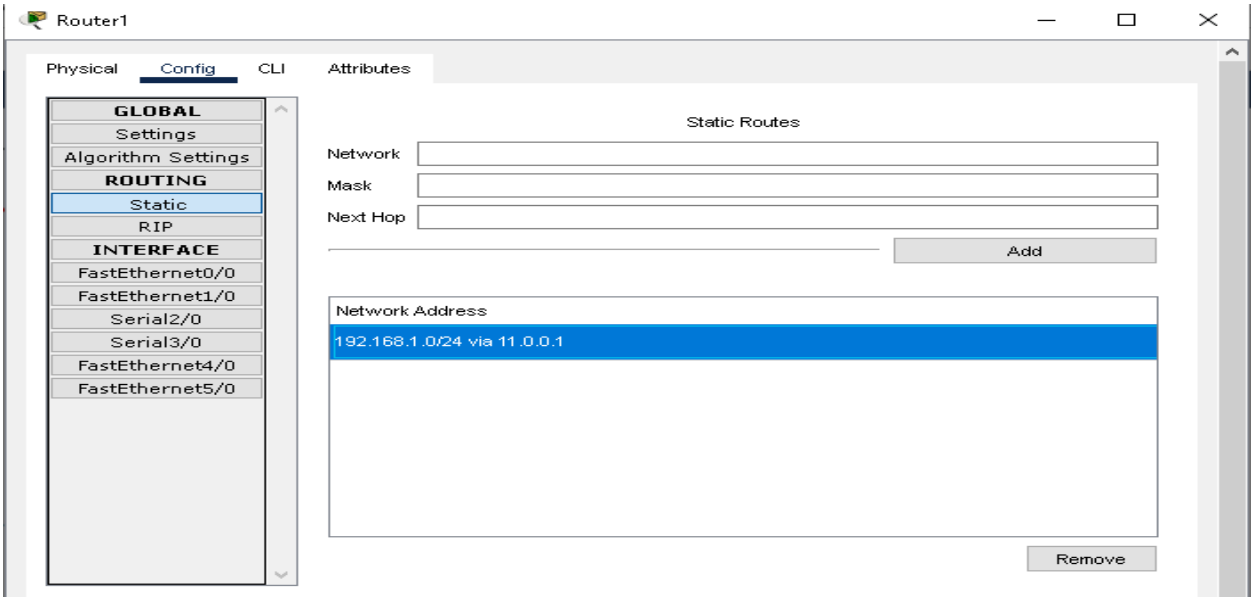


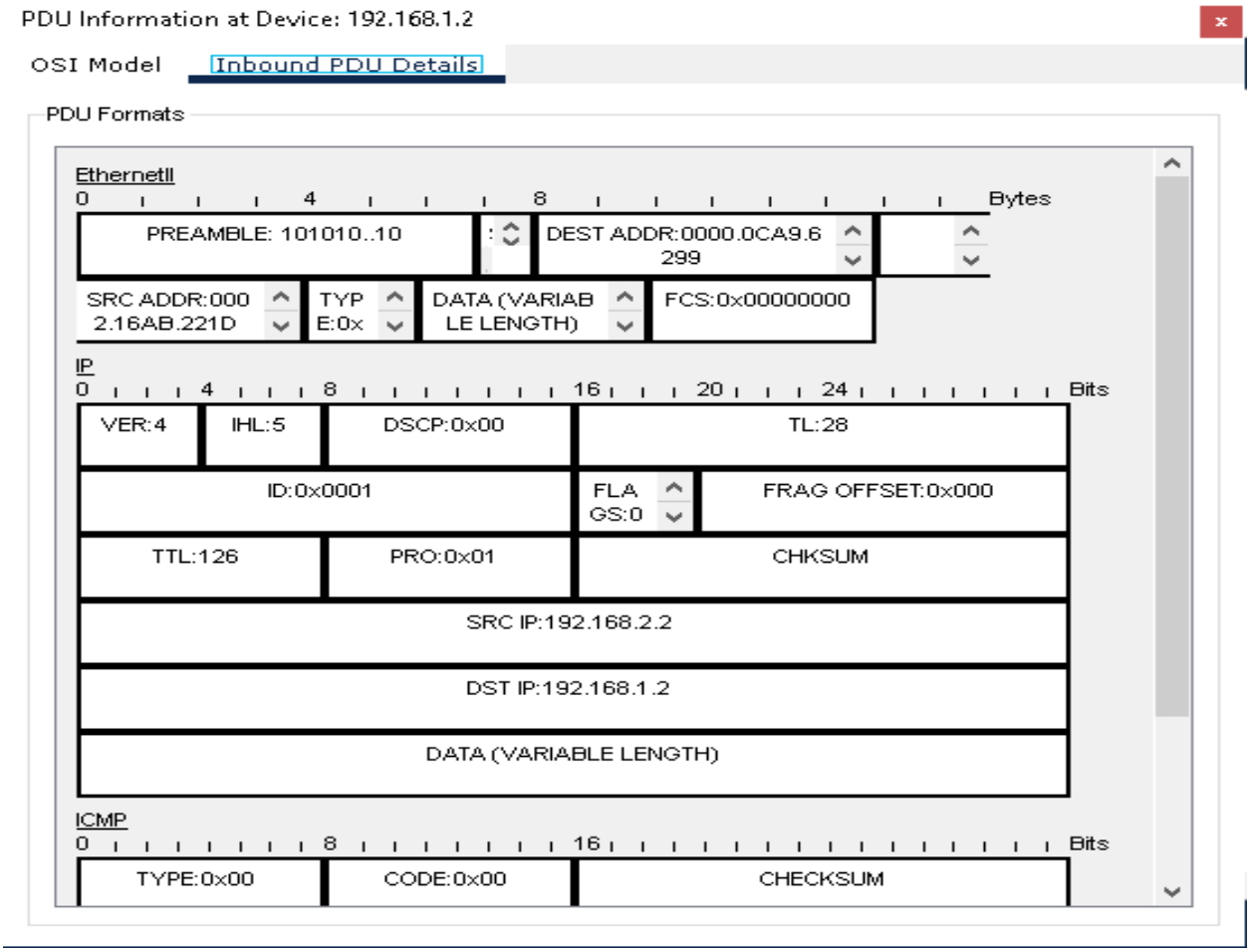
- **Router0 :**



Date: 17/ 09/2024

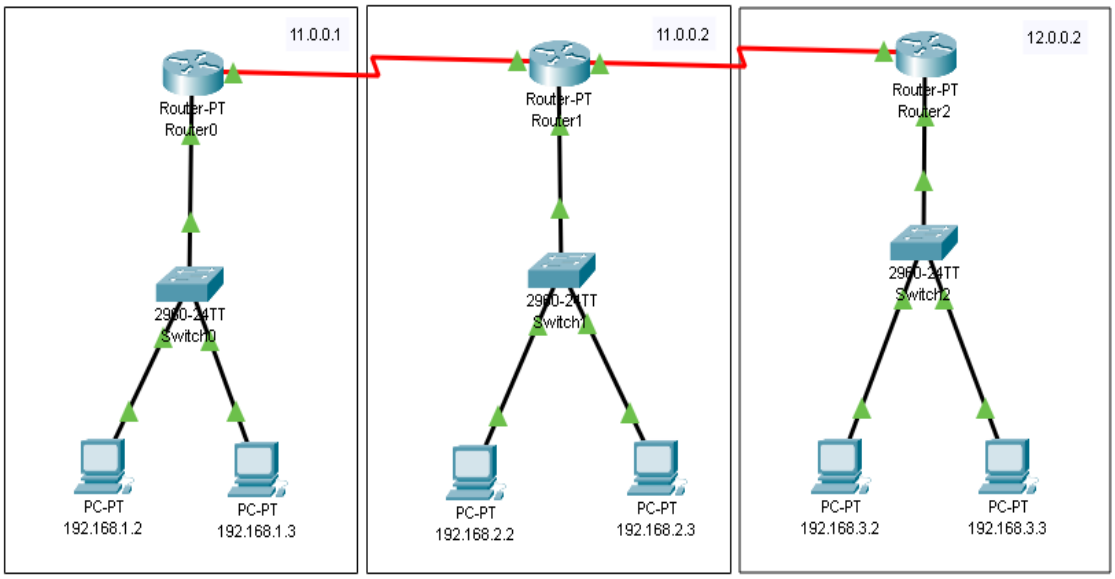
- **Router1 :**



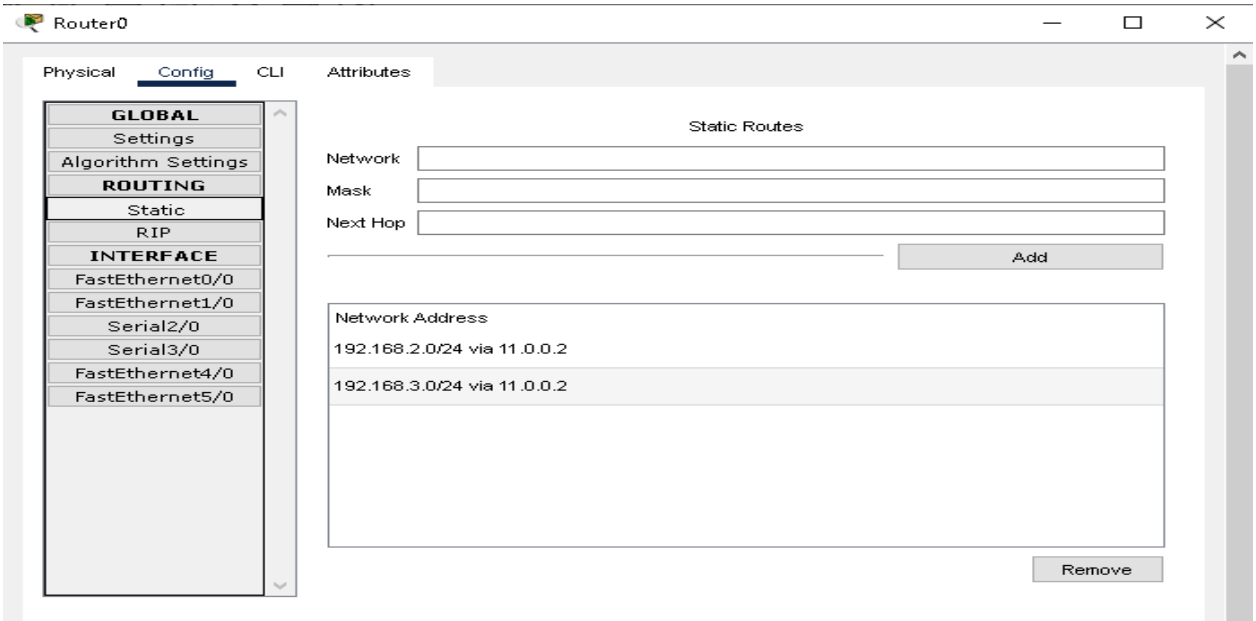


Date: 17/ 09/2024

2. Connect the three different networks based on the calculated IP addresses and subnet using a packet tracer.

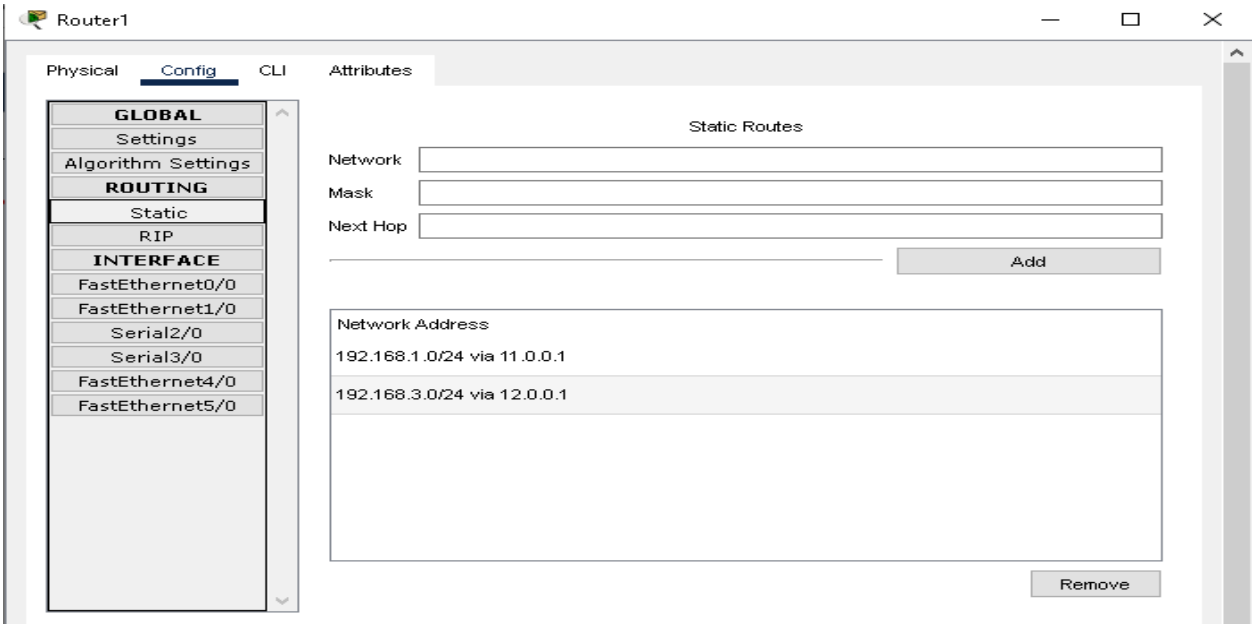


- **Router0 :**

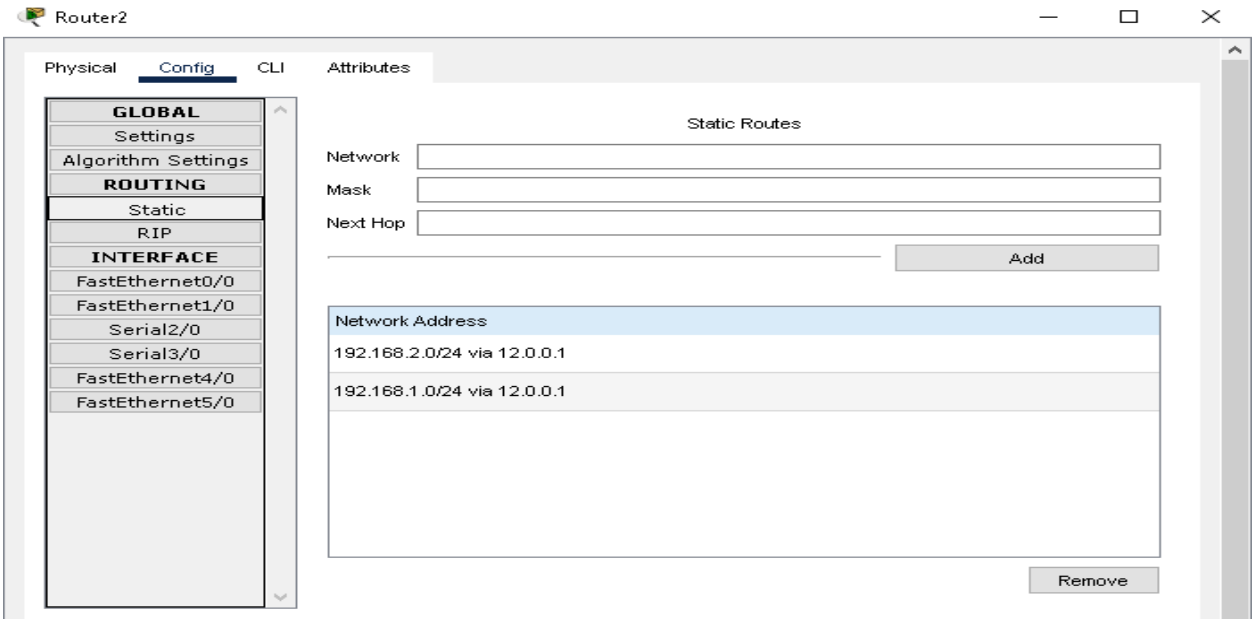


Date: 17/ 09/2024

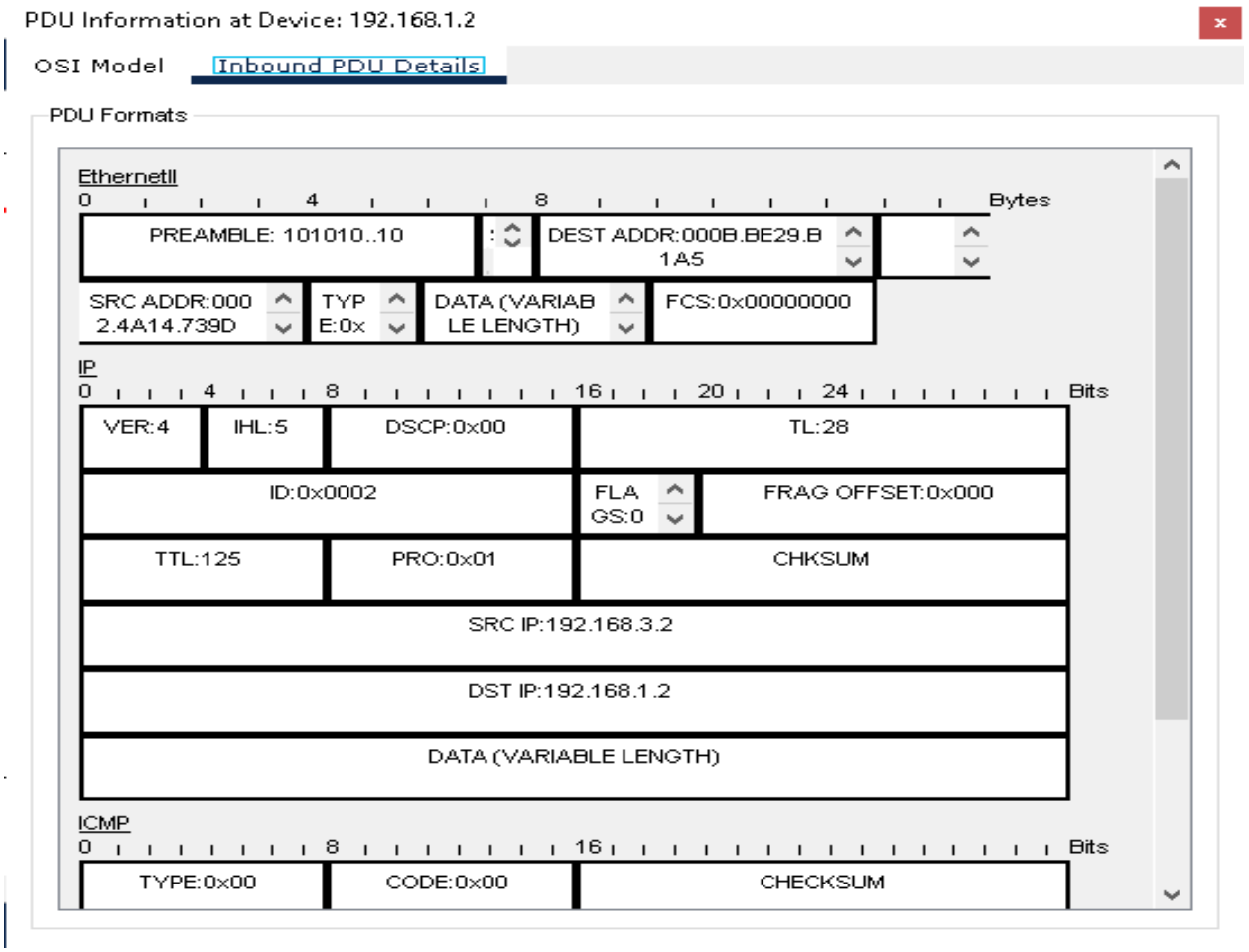
- **Router1 :**



- **Router2:**



Date: 17/ 09/2024



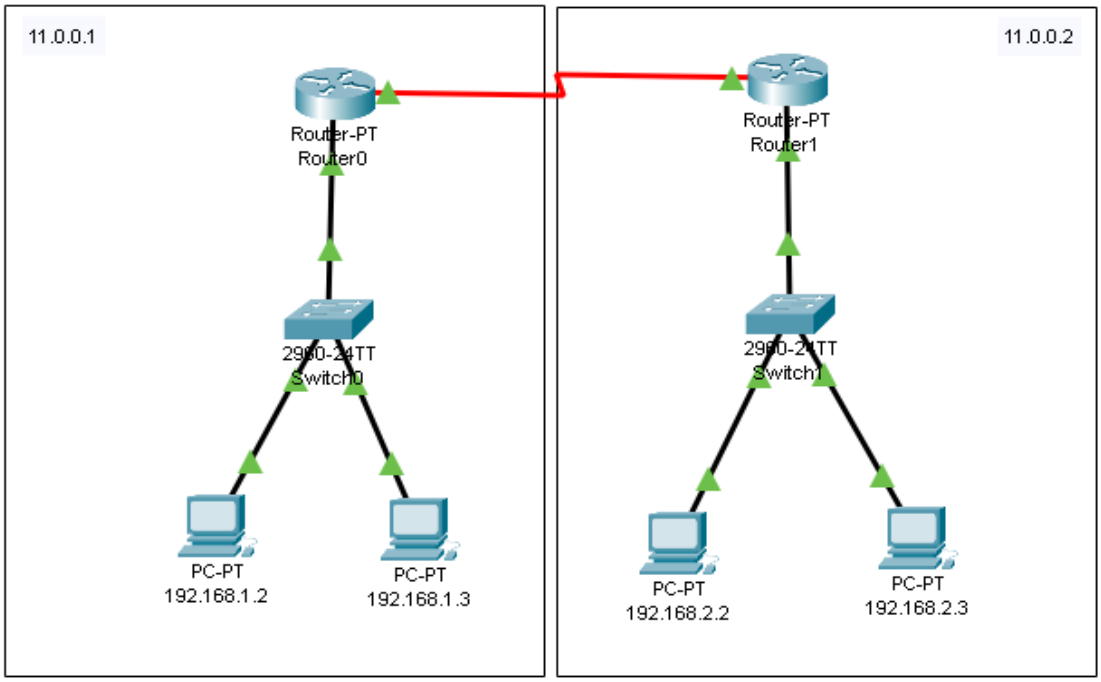
Date: 19/09/2024

Lab Practical #11:

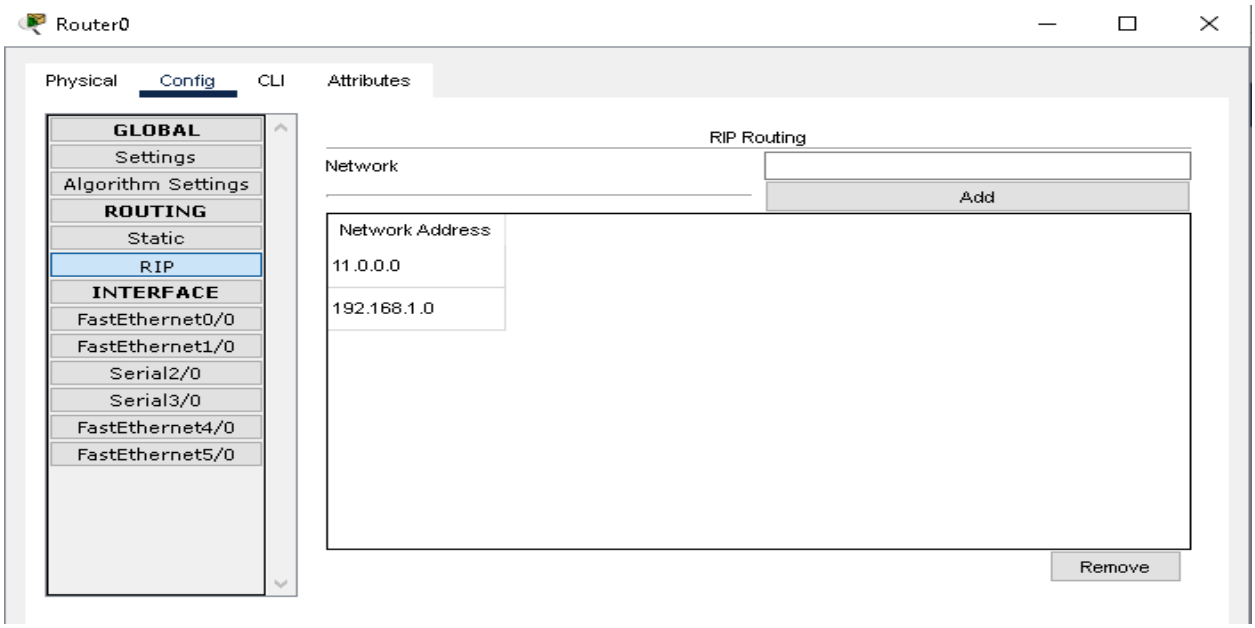
Study the concept of routing using packet tracer. (Dynamic Routing)

Practical Assignment #11:

1. Connect the two different networks based on the calculated IP addresses and subnet using a packet tracer.

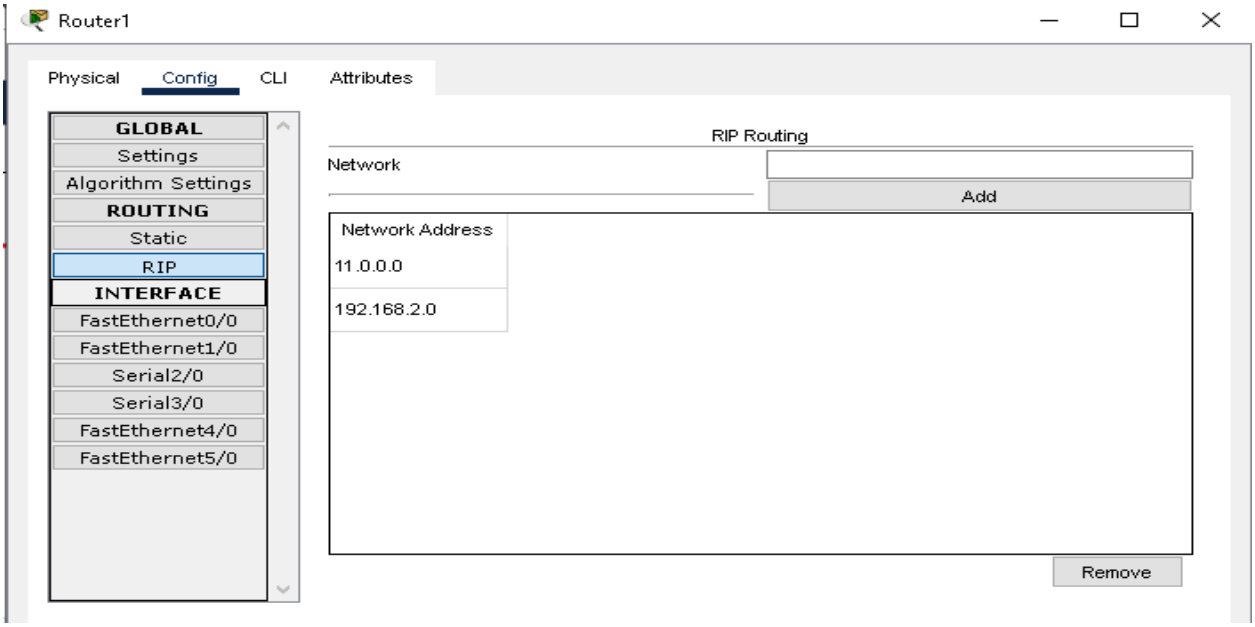


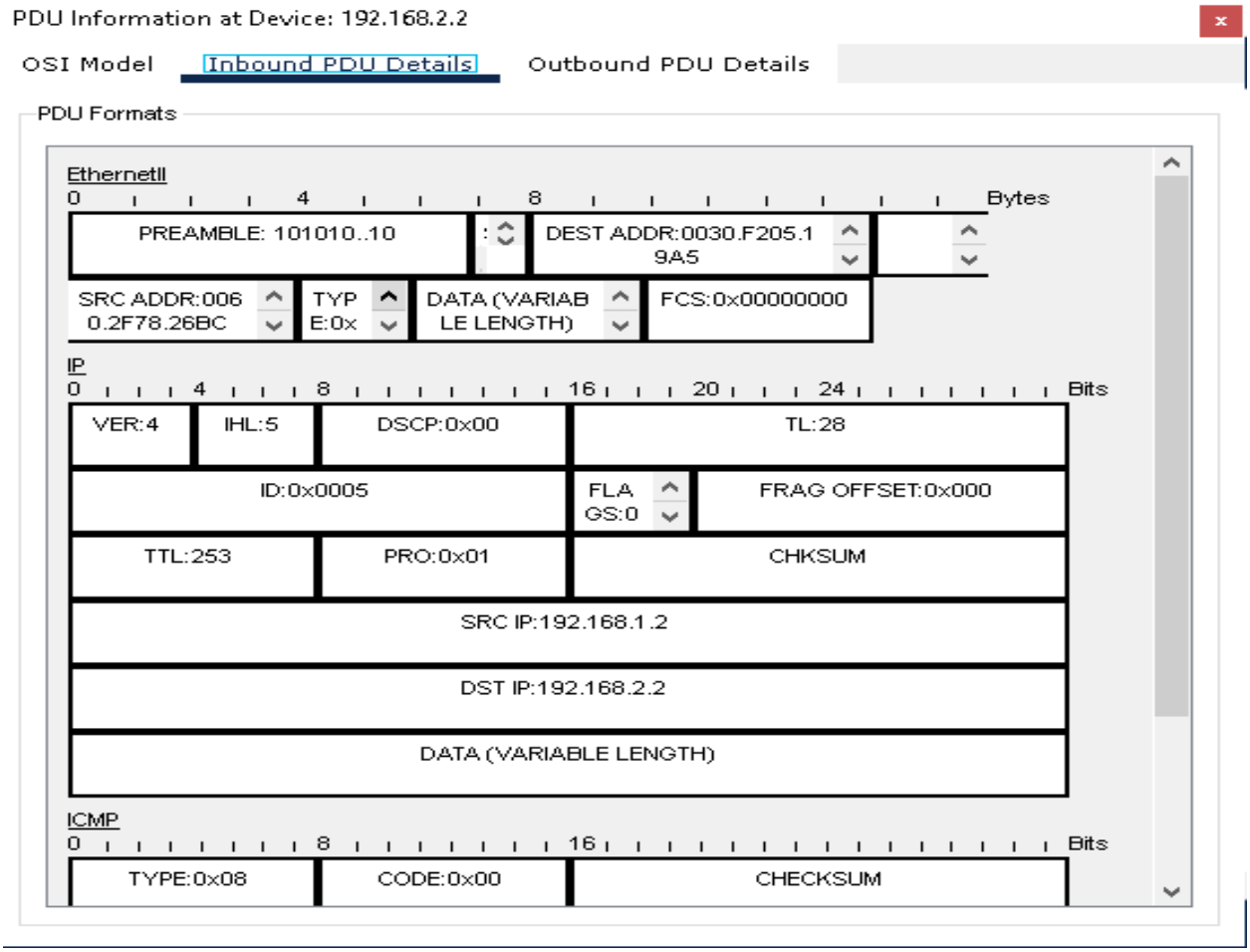
- **Router0 :**



Date: 19/09/2024

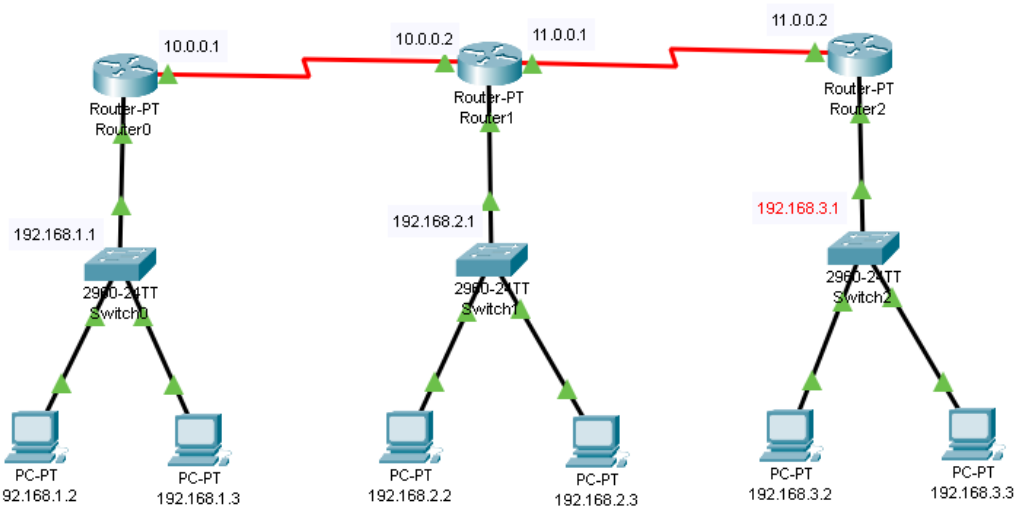
- **Router1 :**



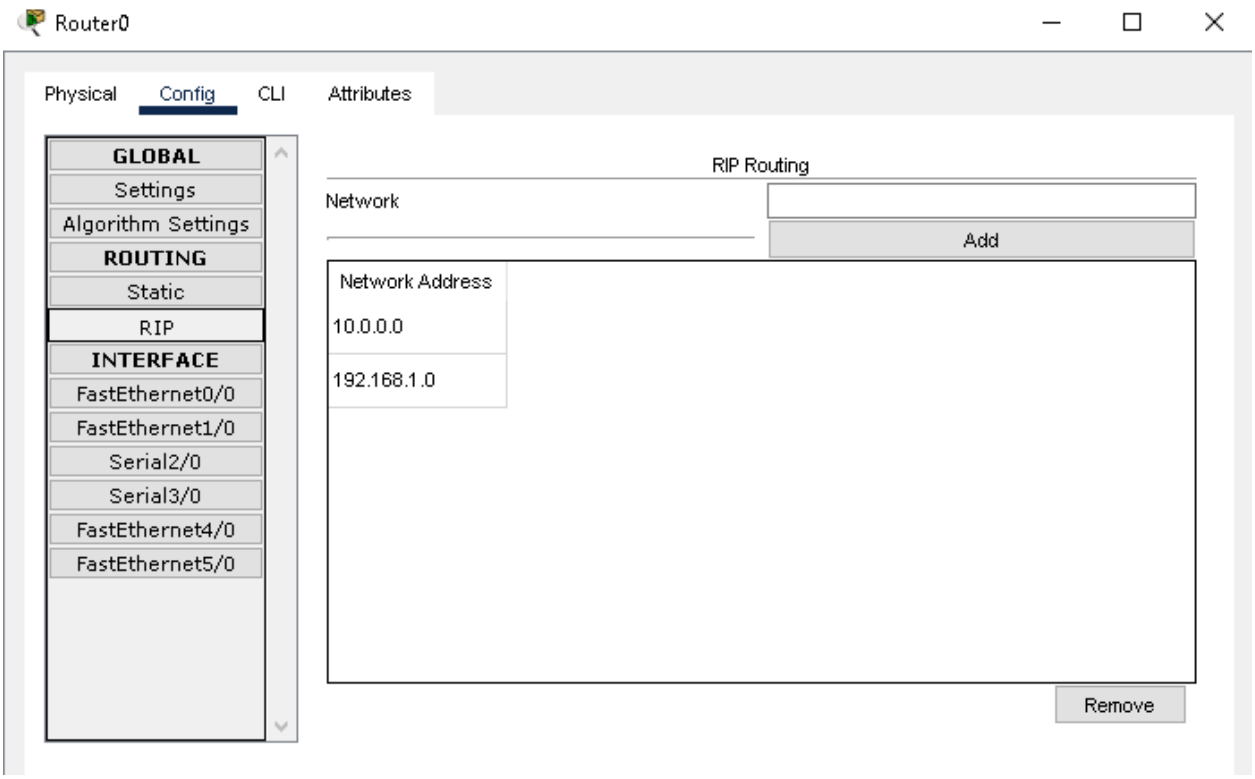


Date: 19/09/2024

2. Connect the three different networks based on the calculated IP addresses and subnet using a packet tracer.

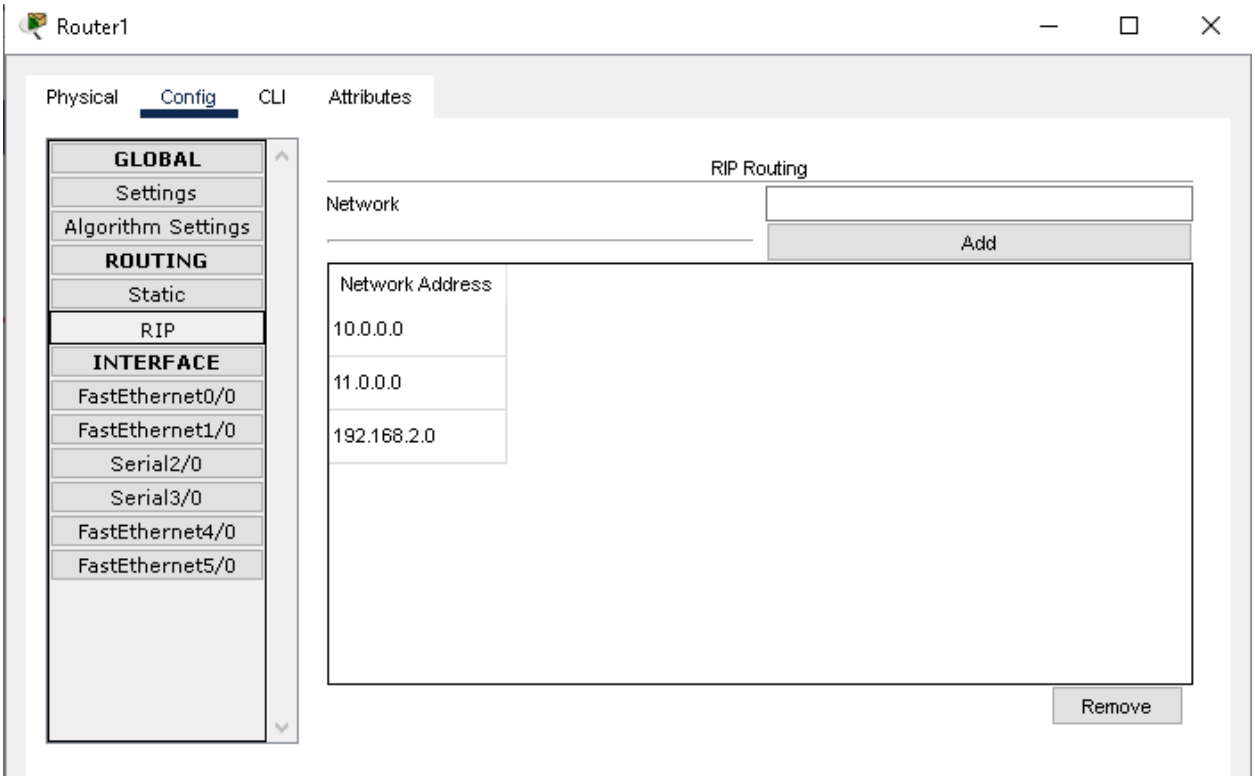


- **Router0 :**

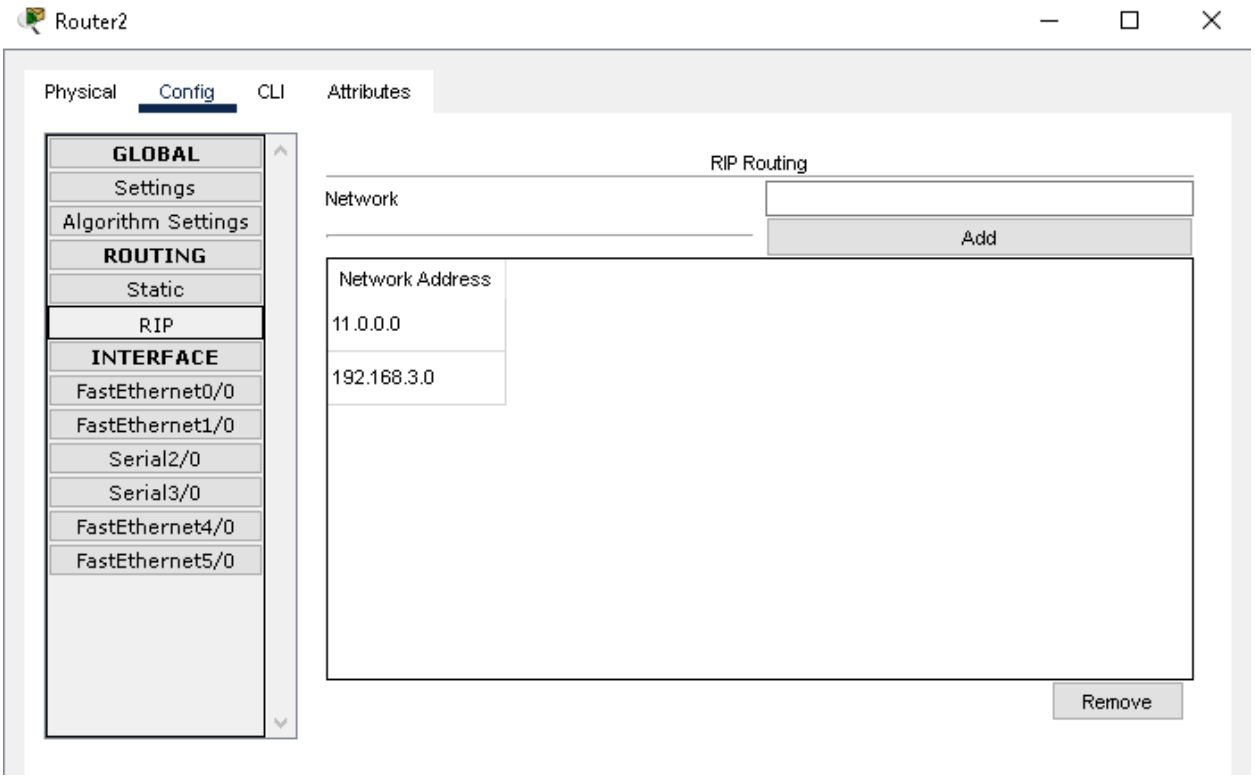


Date: 19/09/2024

- **Router1 :**

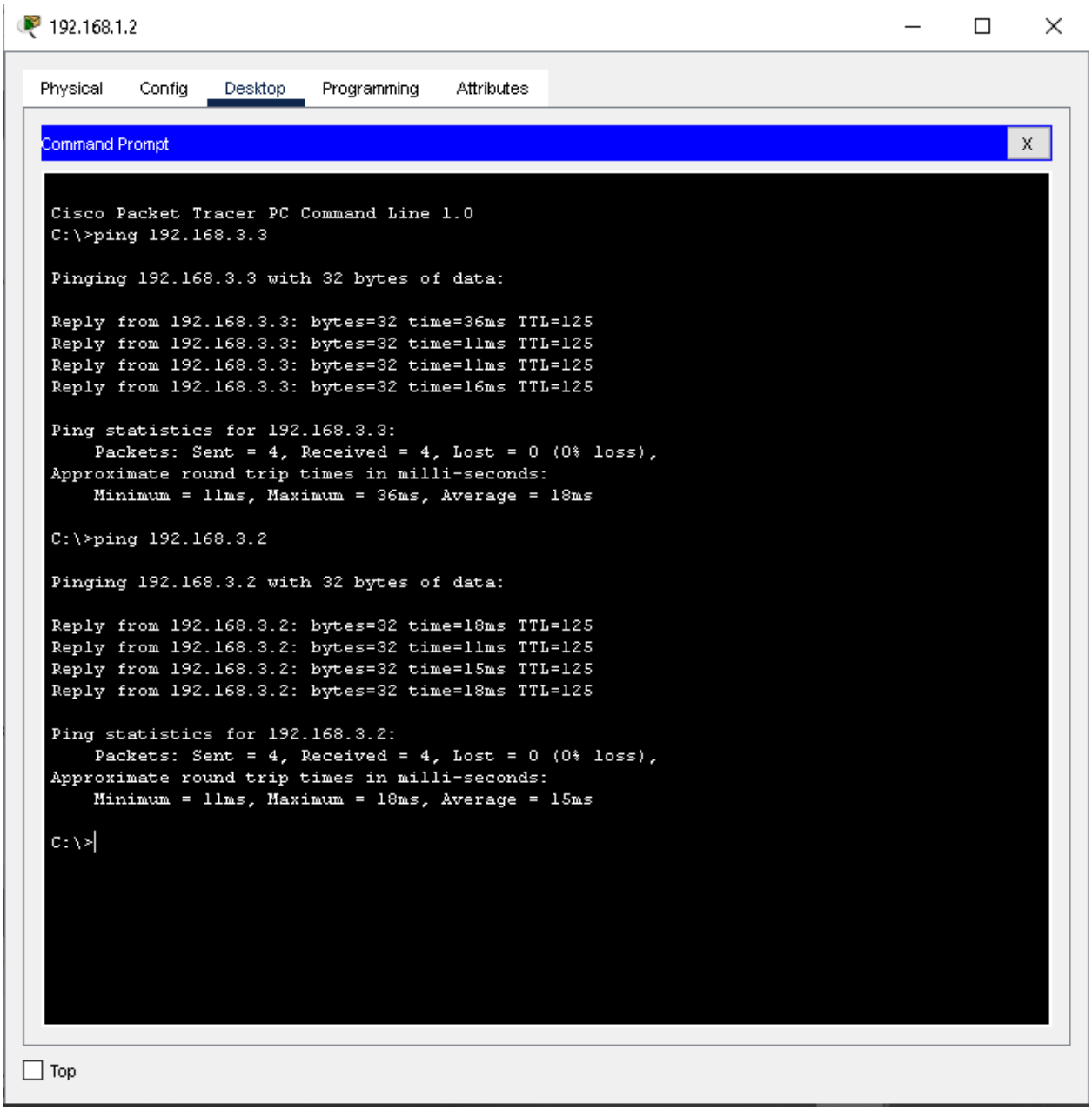


- **Router2 :**



Date: 19/09/2024

- **ping 192.168.3.3 :**



Date: 20/09/2024

Lab Practical #12:

To develop network using distance vector routing protocol and link state routing protocol.

Practical Assignment #12:

1. C/Java Program: Distance Vector Routing Algorithm using Bellman Ford's Algorithm.

```
import java.util.Arrays;
public class DistanceVectorRouting {

   private static final int V = 5;  // Number of vertices (or routers)
   private static final int INF = 999;  // Infinity representation

   static class Node {
      int[] distance = new int[V];
      int[] nextHop = new int[V];
   }

   public static void bellmanFord(int[][] graph) {
      Node[] routingTable = new Node[V];

      for (int i = 0; i < V; i++) {
         routingTable[i] = new Node();
         for (int j = 0; j < V; j++) {
            routingTable[i].distance[j] = graph[i][j];
            routingTable[i].nextHop[j] = j;
         }
      }

      // Relax all edges V-1 times (Bellman-Ford)
      for (int k = 0; k < V - 1; k++) {
         for (int i = 0; i < V; i++) {
            for (int j = 0; j < V; j++) {
               for (int v = 0; v < V; v++) {
                  if (routingTable[i].distance[v] > graph[i][j] + routingTable[j].distance[v]) {
                     routingTable[i].distance[v] = graph[i][j] + routingTable[j].distance[v];
                     routingTable[i].nextHop[v] = j;
                  }
               }
            }
         }
      }

      // Print the final routing table
      for (int i = 0; i < V; i++) {
```

Date: 20/09/2024

```
        System.out.println("Routing table for router " + (i+1) + ":");
        System.out.println("Destination\tNext Hop\tDistance");
        for (int j = 0; j < V; j++) {
            System.out.println(j + "\t\t\t" + routingTable[i].nextHop[j] + "\t\t\t" + routingTable[i].distance[j]);
        }
        System.out.println();
    }
  }

  public static void main(String[] args) {
    int[][] graph = {
          {0, 2, INF, 1, INF},
          {2, 0, 3, INF, INF},
          {INF, 3, 0, 2, 1},
          {1, INF, 2, 0, 3},
          {INF, INF, 1, 3, 0}
    };
    bellmanFord(graph);
  }
}
```

Date: 20/09/2024

2. C/Java Program: Link state routing algorithm.

```
import java.util.Arrays;

public class LinkStateRouting {

   private static final int V = 5;  // Number of vertices (or routers)
   private static final int INF = 9999;  // Infinity

   int minDistance(int[] dist, boolean[] sptSet) {
      int min = INF, min_index = -1;

      for (int v = 0; v < V; v++) {
         if (!sptSet[v] && dist[v] <= min) {
            min = dist[v];
            min_index = v;
         }
      }
      return min_index;
   }

   void dijkstra(int[][] graph, int src) {
      int[] dist = new int[V];
      boolean[] sptSet = new boolean[V];

      Arrays.fill(dist, INF);
      Arrays.fill(sptSet, false);

      dist[src] = 0;

      for (int count = 0; count < V - 1; count++) {
         int u = minDistance(dist, sptSet);

         sptSet[u] = true;

         for (int v = 0; v < V; v++) {
            if (!sptSet[v] && graph[u][v] != 0 && dist[u] != INF && dist[u] + graph[u][v] < dist[v]) {
               dist[v] = dist[u] + graph[u][v];
            }
         }
      }

      System.out.println("Vertex \t Distance from Source " + src);
      for (int i = 0; i < V; i++) {
         System.out.println(i + " \t\t " + dist[i]);
      }
```

Date: 20/09/2024

```
    }

    public static void main(String[] args) {
        int[][] graph = {
                {0, 2, INF, 1, INF},
                {2, 0, 3, INF, INF},
                {INF, 3, 0, 2, 1},
                {1, INF, 2, 0, 3},
                {INF, INF, 1, 3, 0}
        };

        LinkStateRouting lsr = new LinkStateRouting();
        lsr.dijkstra(graph, 0);
    }
}
```

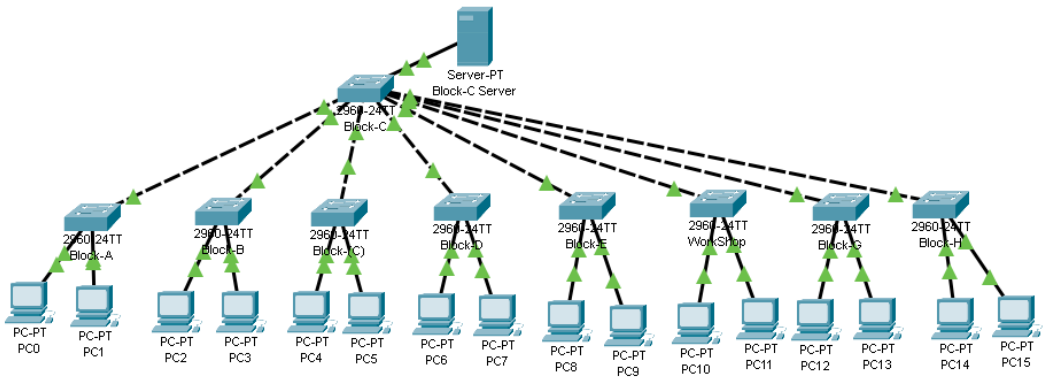
Date: 12/09/2024

Lab Practical #13:

Study & Survey of Institute organization network infrastructure.

Practical Assignment #13:

1. **Identify type of network in your institute. Draw a design of network in your institute (Any Lab/Floor/Building).**



- **Explanation :**
  - Above Diagram is the network of Darshan University
  - C - Block is the designated primarily to Computer Department and the Server Room is located here
  - Through Air-fiber on the terrace of C - Block we are receiving internet connection
  - from the ISP from Madhapar Chawk, Rajkot
  - Each Block of Darshan University is connected to server room which is located at Block-C
  - Through a L-3/L-2 Switch placed in each lab connected directly to server room provides ethernet Connection to each Computer in lab.
  - In some labs we have WiFi-6E routers available for extra connectivity
  - For more security Sophos is implemented.
  - Sophos provides firewall protection, Intrusion detection and prevention to protect from cyber threats.
  - When we want to use Internet then we need to connect to Sophos using userid and password.
  - Here we have our Fiber Optic Switch which is used to connect to the ISP and to provide Fast Internet to all other blocks

Date: 12/09/2024

2. List how many network devices and types of cable used and give its details.

- Network type : LAN
- Network Devices :
  - **Sophos:** for firewall and gateway
  - **L-3 Switch:** used to connect each block and ISP from C-Block to provide internet to each block.
  - **Router:** used for wireless connectivity to each block.
  - **L-2 Switch:** used to connect each Computer in labs of each block to use internet service.
  - **Wireless APs:** wireless Access Points are used to provide connectivity in H Block
  - **Uninterruptible Power Supplies(UPS):** provide backup power to critical devices in case of outages.
  - **Antennas:** used to connect to the ISP which is located 18 km far from Darshan University
  - **Servers:** to store data centrally
  - **Cables:** twisted pair cable and fiber optic cable
  - **Connectors:** RJ45

- Darshan University pay 12 lakh INR , which covers the usage and maintenance of ISP connection.