Date: 8/8/2025

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:

The ipconfig command is used in **Windows** to **view and manage the IP address** and **network configuration** of your system. It helps you check your system's **IP address**, **subnet mask**, **default gateway**, and other important network details.

It is very useful for **troubleshooting internet issues** and checking if your computer is properly connected to a network.

No.	Option	Description
1.	ipconfig	Shows **basic network info**, like IP address, subnet mask, and gateway.
2.	ipconfig /all	Shows **detailed network info**, including MAC address, DHCP status, etc.
3.	ipconfig /release	**Releases the current IP address** (disconnects from the network).
4.	ipconfig /renew	**Renews the IP address** from the DHCP server (reconnects to the network).
5.	ipconfig /flushdns	Clears the **DNS cache**, helpful for fixing DNS-related issues.

Date: 8/8/2025

Implementation:

```
D:\¥@$#>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Unknown adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40c1:315f:4457:4f36:a4bf:e7d3:8577
   Temporary IPv6 Address. . . . . . : 2409:40c1:315f:4457:18eb:701f:7b88:ee6
   Link-local IPv6 Address . . . . . : fe80::829f:656:7621:3e1d%15
   IPv4 Address. . . . . . . . . . . : 192.168.159.195
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::44da:f9ff:fea2:ee02%15
                                       192.168.159.156
```

Date: 8/8/2025

```
D:\¥@$#>ipconfig /all

Windows IP Configuration

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

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 04-BF-1B-92-BB-25
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-8F-B2-62-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 30-F6-EF-C7-06-E2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 32-F6-EF-C7-06-E1
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 30-F6-EF-C7-06-E1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2409:40c1:3018:64bc:dd22:fcc6:6229:feff(Preferred)
   Temporary IPv6 Address. . . . . . : 2409:40c1:3018:64bc:f996:1959:8158:250c(Preferred)
   Link-local IPv6 Address . . . . . : fe80::829f:656:7621:3e1d%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.51.195(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 08 August 2025 05:10:39 PM
   Lease Expires . . . . . . . . . . : 08 August 2025 06:10:39 PM
   Default Gateway . . . . . . . . . : fe80::94e0:f1ff:fe7e:2cc3%14
                                       192.168.51.126
   DHCP Server . . . . . . . . . . . : 192.168.51.126
   DHCPv6 IAID . . . . . . . . . . . : 154203887
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-B8-BC-72-04-BF-1B-92-BB-25
   DNS Servers . . . . . . . . . . . : 192.168.51.126
                                       2409:40c1:3018:64bc::31
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Date: 8/8/2025

```
D:\¥@$#>ipconfig /release

Windows IP Configuration

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

Ethernet adapter Ethernet:

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

Unknown adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40c1:3018:64bc:dd22:fcc6:6229:feff
   Temporary IPv6 Address. . . . . . : 2409:40c1:3018:64bc:f996:1959:8158:250c
   Link-local IPv6 Address . . . . . : fe80::829f:656:7621:3e1d%14
   Default Gateway . . . . . . . . . : fe80::94e0:f1ff:fe7e:2cc3%14
```

Date: 8/8/2025

```
D:\¥@$#>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Ethernet adapter Ethernet:

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

Unknown adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40c1:3018:64bc:dd22:fcc6:6229:feff
   Temporary IPv6 Address. . . . . . : 2409:40c1:3018:64bc:f996:1959:8158:250c
   Link-local IPv6 Address . . . . . : fe80::829f:656:7621:3e1d%14
   IPv4 Address. . . . . . . . . . . : 192.168.51.195
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::94e0:f1ff:fe7e:2cc3%14
                                       192.168.51.126
```

```
D:\¥@$#>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Date: 8/8/2025

2. ping

Description:

The ping command is used to **check the connection between your computer and another device** (like a website or another computer). It helps you **test if a device is reachable** and how long it takes for data to travel (latency).

It works by sending small packets of data and waits for a reply - if it gets a reply, it means the network is working fine.

No.	Option	Description
1	ping -t	**Ping continuously** until manually stopped (use Ctrl + C to stop).
2	ping -a	**Resolves hostname** from an IP address (reverse DNS lookup).
3	ping –n <count>	Sends a specific **number of ping requests**.
4	ping –l <size>	Sets the **packet size** (in bytes) for the ping request.

Implementation:

```
D:\¥@$#>ping -t google.com

Pinging google.com [2404:6800:4009:823::200e] with 32 bytes of data:
Reply from 2404:6800:4009:823::200e: time=126ms
Reply from 2404:6800:4009:823::200e: time=156ms
Reply from 2404:6800:4009:823::200e: time=103ms
Reply from 2404:6800:4009:823::200e: time=133ms
Reply from 2404:6800:4009:823::200e: time=87ms
Reply from 2404:6800:4009:823::200e: time=103ms
Reply from 2404:6800:4009:823::200e: time=100ms

Ping statistics for 2404:6800:4009:823::200e:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 87ms, Maximum = 156ms, Average = 115ms
Control-C
^C
D:\¥@$#>
```

Date: 8/8/2025

```
D:\¥@$#>ping -a google.com

Pinging google.com [2404:6800:4009:823::200e] with 32 bytes
of data:
Reply from 2404:6800:4009:823::200e: time=184ms
Reply from 2404:6800:4009:823::200e: time=117ms
Reply from 2404:6800:4009:823::200e: time=142ms
Reply from 2404:6800:4009:823::200e: time=91ms

Ping statistics for 2404:6800:4009:823::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 91ms, Maximum = 184ms, Average = 133ms
```

```
D:\¥@$#>ping -n 7 google.com

Pinging google.com [2404:6800:4009:823::200e] with 32 bytes of
 data:
Reply from 2404:6800:4009:823::200e: time=359ms
Reply from 2404:6800:4009:823::200e: time=143ms
Reply from 2404:6800:4009:823::200e: time=88ms
Reply from 2404:6800:4009:823::200e: time=125ms
Reply from 2404:6800:4009:823::200e: time=146ms
Reply from 2404:6800:4009:823::200e: time=92ms
Reply from 2404:6800:4009:823::200e: time=116ms

Ping statistics for 2404:6800:4009:823::200e:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 88ms, Maximum = 359ms, Average = 152ms
```

Date: 8/8/2025

```
D:\¥@$#>ping -l 7 google.com

Pinging google.com [2404:6800:4009:823::200e] with 7 bytes of
data:
Reply from 2404:6800:4009:823::200e: time=148ms
Reply from 2404:6800:4009:823::200e: time=113ms
Reply from 2404:6800:4009:823::200e: time=129ms
Reply from 2404:6800:4009:823::200e: time=174ms

Ping statistics for 2404:6800:4009:823::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 113ms, Maximum = 174ms, Average = 141ms
```

3. getmac

Description:

The getmac command is used to **find the MAC address** (Media Access Control address) of your computer. A **MAC address** is a unique hardware ID assigned to your network adapter.

This command helps in **identifying devices** on a network and is often used in **network security and troubleshooting**.

No.	Option	Description
1	getmac	Displays the **MAC address** of all network interfaces.
2	getmac /FO csv	Outputs the result in **CSV (comma-separated)** format.
3	getmac /FO table	Outputs the result in a **formatted table**. This is the default display.
4	getmac /nh	**No Header** – Removes the column headers from the output (used with /FO).

Implementation:

```
D:\¥@$#>getmac

Physical Address    Transport Name
=================== ============================================================
======
00-FF-8F-B2-62-6E   Media disconnected
30-F6-EF-C7-06-E1   \Device\Tcpip_{ACE21DA7-85B0-45B7-8DD4-A2D6FBBB6667}
04-BF-1B-92-BB-25   Media disconnected
```

Date: 8/8/2025

```
D:\¥@$#>getmac /fo csv
"Physical Address","Transport Name"
"00-FF-8F-B2-62-6E","Media disconnected"
"30-F6-EF-C7-06-E1","\Device\Tcpip_{ACE21DA7-85B0-45B7-8DD4-A2D6FBBB6667}"
"04-BF-1B-92-BB-25","Media disconnected"
```

```
D:\¥@$#>getmac /fo table

Physical Address    Transport Name

=================== ==========================================================
======
00-FF-8F-B2-62-6E   Media disconnected

30-F6-EF-C7-06-E1   \Device\Tcpip_{ACE21DA7-85B0-45B7-8DD4-A2D6FBBB6667}

04-BF-1B-92-BB-25   Media disconnected
```

```
D:\¥@$#>getmac /nh

00-FF-8F-B2-62-6E   Media disconnected
30-F6-EF-C7-06-E1   \Device\Tcpip_{ACE21DA7-85B0-45B7-8DD4-A2D6FBBB6667}
04-BF-1B-92-BB-25   Media disconnected
```

4. systeminfo

Description:

The systeminfo command displays **detailed information about your computer system**. It includes details like **OS version, processor, RAM, system type, BIOS version**, and more.

It is helpful for **checking system specifications**, **troubleshooting issues**, or **creating system reports**.

No.	Option	Description
1	systeminfo	Displays detailed **system configuration** info like OS, RAM, processor, etc.
2	systeminfo /fo csv	Outputs results in **CSV (Comma-Separated Values)** format.
3	systeminfo /fo table	Displays output in a **formatted table**. This is the **default format**.
4	systeminfo /s user	Tries to fetch info from a **remote machine named "user"**.

Date: 8/8/2025

Implementation:

```
D:\¥@$#>systeminfo

Host Name:                     YASH
OS Name:                       Microsoft Windows 11 Home Single Language
OS Version:                    10.0.26100 N/A Build 26100
OS Manufacturer:               Microsoft Corporation
OS Configuration:              Standalone Workstation
OS Build Type:                 Multiprocessor Free
Registered Owner:              YASH
Registered Organization:       N/A
Product ID:                    00356-24715-75136-AAOEM
Original Install Date:         14-10-24, 04:55:17 PM
System Boot Time:              08-08-25, 05:10:19 PM
System Manufacturer:           Dell Inc.
System Model:                  Dell G15 5530
System Type:                   x64-based PC
Processor(s):                  1 Processor(s) Installed.
                               [01]: Intel64 Family 6 Model 183 Stepping 1 GenuineIntel ~2400 Mhz
BIOS Version:                  Dell Inc. 1.23.0, 04-03-25
Windows Directory:             C:\WINDOWS
System Directory:              C:\WINDOWS\system32
Boot Device:                   \Device\HarddiskVolume1
System Locale:                 en-us;English (United States)
Input Locale:                  00004009
Time Zone:                     (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:         7,877 MB
Available Physical Memory:     1,055 MB
Virtual Memory: Max Size:      20,677 MB
Virtual Memory: Available:     8,467 MB
Virtual Memory: In Use:        12,210 MB
Page File Location(s):         E:\pagefile.sys
Domain:                        WORKGROUP
Logon Server:                  \\YASH
Hotfix(s):                     3 Hotfix(s) Installed.
                               [01]: KB5056579
                               [02]: KB5062660
                               [03]: KB5064485
Network Card(s):               3 NIC(s) Installed.
                               [01]: TAP-Windows Adapter V9
                                     Connection Name: Local Area Connection
                                     Status:          Media disconnected
                               [02]: Intel(R) Wi-Fi 6 AX201 160MHz
                                     Connection Name: Wi-Fi
                                     DHCP Enabled:    Yes
                                     DHCP Server:     192.168.51.126
                                     IP address(es)
                                     [01]: 192.168.51.195
                                     [02]: fe80::829f:656:7621:3e1d
                                     [03]: 2409:40c1:3018:64bc:f996:1959:8158:250c
                                     [04]: 2409:40c1:3018:64bc:dd22:fcc6:6229:feff
                               [03]: Realtek PCIe GbE Family Controller
                                     Connection Name: Ethernet
                                     Status:          Media disconnected
Virtualization-based security: Status: Running
                               Required Security Properties:
                               Available Security Properties:
                                     Base Virtualization Support
                                     Secure Boot
                                     DMA Protection
                                     UEFI Code Readonly
                                     SMM Security Mitigations 1.0
                                     Mode Based Execution Control
                                     APIC Virtualization
                               Services Configured:
                               Services Running:
                               App Control for Business policy: Enforced
                               App Control for Business user mode policy: Off
                               Security Features Enabled:
Hyper-V Requirements:          A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

Date: 8/8/2025

```
D:\¥@$#>systeminfo /fo table

Host Name                      OS Name                       OS Version                    OS Manufacturer
OS Configuration                         OS Build Type        Registered Owner                                  Registered Organizati
on                             Product ID                    Original Install Date     System Boot Time              System Manufactu
rer            System Model          System Type              Processor(s)                                  BIOS Version
     Windows Directory    System Directory     Boot Device                      System Locale                       Input Locale
                    Time Zone                                      Total Physical Memory     Available Physical Memory Virtual Me
mory: Max Size  Virtual Memory: Available Virtual Memory: In Use    Page File Location(s)          Domain               Logon Server
       Hotfix(s)            Network Card(s)                                                                                  Virtu
alization-based security                                                                  Hyper-V Requirements
============================ ============================ ============================ ====================================
=================================== ================== ============================================ ==================
============================ ========================== ======================= ========================== ================
============= ================== ====================== ========================================== ======================
==== ================== ================== ================================ ============================== ==============
================= ================================================ ======================= ======================= ==========
============== ====================== ====================== ========================== ================== ==============
====== ================== ============================================================================================================ =====
================================================================================================== ====================================
============================================================
YASH                           Microsoft Windows 11 Home Sing 10.0.26100 N/A Build 26100     Microsoft Corporation
Standalone Workstation                   Multiprocessor Free  YASH                                              N/A
                               00356-24715-75136-AAOEM        14-10-24, 04:55:17 PM     08-08-25, 05:10:19 PM          Dell Inc.
               Dell G15 5530        x64-based PC             1 Processor(s) Installed., [01]: Intel64 Fami Dell Inc. 1.23.0, 04-03-25
     C:\WINDOWS           C:\WINDOWS\system32  \Device\HarddiskVolume1             en-us;English (United States)       00004009
                    (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi    7,877 MB                 1,165 MB                20,677 MB
              8,281 MB                 12,396 MB               E:\pagefile.sys               WORKGROUP            \\YASH
       3 Hotfix(s) Install, 3 NIC(s) Installed., [01]: TAP-Windows Adapter V9,       Connection Name: Local Area Connection,     Statu
s: Running, Required Security Properties:, Available Security Properties:,       Base Virtualiz A hypervisor has been detected. Featur
es required for Hyper-V will not be displayed.
```

Date: 8/8/2025

```
Host Name:                     YASH
OS Name:                       Microsoft Windows 11 Home Single Language
OS Version:                    10.0.26100 N/A Build 26100
OS Manufacturer:               Microsoft Corporation
OS Configuration:              Standalone Workstation
OS Build Type:                 Multiprocessor Free
Registered Owner:              YASH
Registered Organization:       N/A
Product ID:                    00356-24715-75136-AAOEM
Original Install Date:         14-10-24, 04:55:17 PM
System Boot Time:              08-08-25, 05:10:19 PM
System Manufacturer:           Dell Inc.
System Model:                  Dell G15 5530
System Type:                   x64-based PC
Processor(s):                  1 Processor(s) Installed.
                               [01]: Intel64 Family 6 Model 183 Stepping 1 GenuineIntel ~2400 Mhz
BIOS Version:                  Dell Inc. 1.23.0, 04-03-25
Windows Directory:             C:\WINDOWS
System Directory:              C:\WINDOWS\system32
Boot Device:                   \Device\HarddiskVolume1
System Locale:                 en-us;English (United States)
Input Locale:                  00004009
Time Zone:                     (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:         7,877 MB
Available Physical Memory:     1,060 MB
Virtual Memory: Max Size:      20,677 MB
Virtual Memory: Available:     8,292 MB
Virtual Memory: In Use:        12,385 MB
Page File Location(s):         E:\pagefile.sys
Domain:                        WORKGROUP
Logon Server:                  \\YASH
Hotfix(s):                     3 Hotfix(s) Installed.
                               [01]: KB5056579
                               [02]: KB5062660
                               [03]: KB5064485
Network Card(s):               3 NIC(s) Installed.
                               [01]: TAP-Windows Adapter V9
                                     Connection Name: Local Area Connection
                                     Status:          Media disconnected
                               [02]: Intel(R) Wi-Fi 6 AX201 160MHz
                                     Connection Name: Wi-Fi
                                     DHCP Enabled:    Yes
                                     DHCP Server:     192.168.51.126
                                     IP address(es)
                                     [01]: 192.168.51.195
                                     [02]: fe80::829f:656:7621:3e1d
                                     [03]: 2409:40c1:3018:64bc:f996:1959:8158:250c
                                     [04]: 2409:40c1:3018:64bc:dd22:fcc6:6229:feff
                               [03]: Realtek PCIe GbE Family Controller
                                     Connection Name: Ethernet
                                     Status:          Media disconnected
Virtualization-based security: Status: Running
                               Required Security Properties:
                               Available Security Properties:
                                     Base Virtualization Support
                                     Secure Boot
                                     DMA Protection
                                     UEFI Code Readonly
                                     SMM Security Mitigations 1.0
                                     Mode Based Execution Control
                                     APIC Virtualization
                               Services Configured:
                               Services Running:
                               App Control for Business policy: Enforced
                               App Control for Business user mode policy: Off
                               Security Features Enabled:
Hyper-V Requirements:          A hypervisor has been detected. Features required for Hyper-V will not be displayed
```

Date: 8/8/2025

5. traceroute / tracert

Description:

In **Windows**, the command is tracert,
In **Linux/macOS**, it's called traceroute
Both work similarly.

Description:

The tracert command shows the **path that data takes from your computer to a destination (like a website)**. It helps you **see all the routers** (called "hops") the data passes through on the internet.

Very useful for **troubleshooting network issues** and checking **where delays or failures occur** in the network.

No.	Option	Description
1	tracert -d	Prevents tracert from resolving IP addresses to **hostnames**. Speeds up output.
2	tracert /h	Specifies the **maximum number of hops** to search for the target (default is 30).
3	tracert /w	Specifies the **wait time (in milliseconds)** for each reply (default is 4000 ms).
4	tracert /6	Forces tracert to use **IPv6** instead of IPv4.

Implementation:

```
D:\¥@$#>tracert /d 7

Tracing route to 0.0.0.7 over a maximum of 30 hops

  1  Transmit error: code 1231.

Trace complete.
```

Date: 8/8/2025

```
D:\¥@$#>tracert /h 7 google.com

Tracing route to google.com [2404:6800:4002:805::200e]
over a maximum of 7 hops:

  1     4 ms     3 ms     5 ms  2409:40c1:3018:64bc::31
  2    68 ms    78 ms    78 ms  2405:200:5210:5:3924:110:3:108
  3    96 ms    76 ms    59 ms  2405:200:5210:5:3925::1
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6    56 ms    97 ms    26 ms  2405:200:801:2e00::84
  7     *        *        *     Request timed out.

Trace complete.
```

```
D:\¥@$#>tracert /w 7777 google.com

Tracing route to google.com [2404:6800:4009:808::200e]
over a maximum of 30 hops:

  1     5 ms     3 ms     3 ms  2409:40c1:3018:64bc::31
  2    71 ms    25 ms    51 ms  2405:200:5210:5:3924:110:3:108
  3    44 ms   107 ms    31 ms  2405:200:5210:5:3925::1
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6    84 ms    25 ms    52 ms  2405:200:801:2e00::80
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *       99 ms    92 ms  2404:6800:80b2::1
 11    78 ms   101 ms    77 ms  2001:4860:0:1::27e4
 12    93 ms    77 ms    88 ms  2001:4860:0:1::8760
 13    65 ms     *      137 ms  2001:4860:0:1::7975
 14    68 ms    77 ms    71 ms  2001:4860:0:1::4fe9
 15    64 ms    73 ms    78 ms  pnbomb-aw-in-x0e.1e100.net [2404:6800:4009:808::200e]

Trace complete.
```

Date: 8/8/2025

```
D:\¥@$#>tracert /6 google.com

Tracing route to google.com [2404:6800:4009:823::200e]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  2409:40c1:3018:64bc::31
  2    66 ms    26 ms    48 ms  2405:200:5210:5:3924:110:3:108
  3    71 ms    25 ms    49 ms  2405:200:5210:5:3925::1
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6    91 ms    26 ms    50 ms  2405:200:801:2e00::80
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9   424 ms    95 ms   137 ms  2001:4860:1:1::f48
 10   123 ms    78 ms    77 ms  2001:4860:1:1::f48
 11   109 ms    82 ms   153 ms  2404:6800:81e2:200::1
 12   104 ms   156 ms   158 ms  2001:4860:0:1::5398
 13   141 ms    71 ms    77 ms  2001:4860:0:1::77d0
 14   107 ms    81 ms   138 ms  2001:4860::c:4004:2137
 15   138 ms   157 ms   158 ms  2001:4860::9:4001:7733
 16   128 ms   108 ms   105 ms  2001:4860:0:1::fb5
 17   122 ms   157 ms   114 ms  bom12s13-in-x0e.1e100.net [2404:6800:4009:823::200e]
```

6. netstat

Description:

The netstat command shows **network statistics** and details about **current network connections**, **ports in use**, **protocols**, and more. It's very helpful for **monitoring network activity** and **troubleshooting network or port issues**.

You can use it to find out which **programs are using the internet** or **which ports are open** on your system.

No.	Option	Description
1	netstat -n	Displays addresses and ports in **numeric format**, skipping DNS resolution.
2	netstat –o	Shows the **Process ID (PID)** for each connection. Useful for identifying apps.
3	netstat -e	Shows **Ethernet statistics** (bytes sent/received, errors, etc.).
4	netstat -r	Displays the **routing table** (same as route print).

Date: 8/8/2025

Implementation:

```
D:\¥@$#>netstat /n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49738        127.0.0.1:49739        ESTABLISHED
  TCP    127.0.0.1:49739        127.0.0.1:49738        ESTABLISHED
  TCP    127.0.0.1:49740        127.0.0.1:49741        ESTABLISHED
  TCP    127.0.0.1:49741        127.0.0.1:49740        ESTABLISHED
  TCP    127.0.0.1:49743        127.0.0.1:49744        ESTABLISHED
  TCP    127.0.0.1:49744        127.0.0.1:49743        ESTABLISHED
  TCP    127.0.0.1:49745        127.0.0.1:49746        ESTABLISHED
  TCP    127.0.0.1:49746        127.0.0.1:49745        ESTABLISHED
  TCP    127.0.0.1:49824        127.0.0.1:49825        ESTABLISHED
  TCP    127.0.0.1:49825        127.0.0.1:49824        ESTABLISHED
  TCP    127.0.0.1:49830        127.0.0.1:49831        ESTABLISHED
  TCP    127.0.0.1:49831        127.0.0.1:49830        ESTABLISHED
  TCP    192.168.51.195:50955   148.113.20.106:443     ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:49408  [2603:1040:a06:6::]:443  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:49409  [2603:1040:a06:6::]:443  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:49947  [64:ff9b::d4e:6da2]:8883  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:50918  [2404:6800:4003:c01::bc]:5228  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:50919  [2404:6800:4003:c01::bc]:5228  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:51722  [64:ff9b::9d5a:5b47]:443  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52522  [2606:4700:8d7b:5e56:bd9:ae5:df20:bd83]:443  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52531  [2606:4700:90cb:5e56:bd7:ae6:df20:bd83]:443  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52542  [2600:1901:0:47fc::]:443  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52546  [2600:1901:0:47fc::]:443  ESTABLISHED
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52570  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52571  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52572  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52576  [64:ff9b::2ffc:6108]:80  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52578  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52579  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52580  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52581  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52582  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52583  [2409:40c1:3018:64bc::31]:53  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52584  [2603:1046:1400::7]:443  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52585  [2603:1046:1400::7]:443  TIME_WAIT
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52589  [64:ff9b::2ffc:610a]:80  TIME_WAIT
```

Date: 8/8/2025

```
D:\¥@$#>netstat /o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49738        YASH:49739             ESTABLISHED     1660
  TCP    127.0.0.1:49739        YASH:49738             ESTABLISHED     1660
  TCP    127.0.0.1:49740        YASH:49741             ESTABLISHED     1816
  TCP    127.0.0.1:49741        YASH:49740             ESTABLISHED     1816
  TCP    127.0.0.1:49743        YASH:49744             ESTABLISHED     4912
  TCP    127.0.0.1:49744        YASH:49743             ESTABLISHED     4912
  TCP    127.0.0.1:49745        YASH:49746             ESTABLISHED     3132
  TCP    127.0.0.1:49746        YASH:49745             ESTABLISHED     3132
  TCP    127.0.0.1:49824        YASH:49825             ESTABLISHED     16488
  TCP    127.0.0.1:49825        YASH:49824             ESTABLISHED     16488
  TCP    127.0.0.1:49830        YASH:49831             ESTABLISHED     16520
  TCP    127.0.0.1:49831        YASH:49830             ESTABLISHED     16520
  TCP    192.168.51.195:50955   relay-291946ef:https   ESTABLISHED     4816
  TCP    192.168.51.195:52752   104.26.7.95:https      ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:49408  [2603:1040:a06:6::]:https  ESTABLISHED     5476
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:49409  [2603:1040:a06:6::]:https  ESTABLISHED     5476
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:49947  [64:ff9b::d4e:6da2]:8883  ESTABLISHED     24008
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:50918  sb-in-f188:5228        ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:50919  sb-in-f188:5228        ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:51722  static:https           ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52680  [64:ff9b::142a:415d]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52697  [2606:4700:90c2:7cbc:c2a8:ae7:5ff2:75c4]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52698  [2606:4700:90cb:5e56:bd7:ae6:df20:bd83]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52699  [2606:4700:90cb:5e56:bd7:ae6:df20:bd83]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52701  [2606:4700:90cb:5e56:bd7:ae7:df20:bd83]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52702  [2606:4700:90cb:5e56:bd7:ae7:df20:bd83]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52705  [2606:4700:90c2:7cbc:c2a8:ae7:5ff2:75c4]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52720  [2600:1901:0:47fc::]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52721  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52722  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52723  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52724  [2600:1901:0:47fc::]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52725  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52726  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52727  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52728  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52729  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52730  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52736  [64:ff9b::2ffc:610d]:http  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52738  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52739  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52740  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52741  [2606:4700:8d7b:5e56:bd7:ae4:df20:bd83]:https  ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52742  [2606:4700:8d7b:5e56:bd7:ae4:df20:bd83]:https  ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52746  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52747  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52749  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52750  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52751  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52753  [2606:4700:90c2:7cbc:c2a8:ae6:5ff2:75c4]:https  ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52754  [2606:4700:8d7b:5e56:bd9:ae4:df20:bd83]:https  ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52756  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52757  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52758  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52759  [2606:4700:90c2:7cbc:c2a8:ae7:5ff2:75c4]:https  ESTABLISHED     7364
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52760  [2603:1046:1406::5]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52761  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52762  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52763  [2409:40c1:3018:64bc::31]:domain  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52764  [2603:1046:1406::5]:https  TIME_WAIT       0
  TCP    [2409:40c1:3018:64bc:f996:1959:8158:250c]:52768  [64:ff9b::2ffc:6109]:http  TIME_WAIT       0
```

Date: 8/8/2025

```
D:\¥@$#>netstat /e
Interface Statistics

                           Received            Sent

Bytes                    1173772008        133397670
Unicast packets             822060           552000
Non-unicast packets            324             5868
Discards                         0                0
Errors                           0                0
Unknown protocols                0
```

Date: 8/8/2025

```
D:\¥@$#>netstat /r
===========================================================================
Interface List
  9...04 bf 1b 92 bb 25 ......Realtek PCIe GbE Family Controller
 11...00 ff 8f b2 62 6e ......TAP-Windows Adapter V9
  6...30 f6 ef c7 06 e2 ......Microsoft Wi-Fi Direct Virtual Adapter
  7...32 f6 ef c7 06 e1 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 14...30 f6 ef c7 06 e1 ......Intel(R) Wi-Fi 6 AX201 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.51.126   192.168.51.195     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
     192.168.51.0    255.255.255.0         On-link    192.168.51.195    311
   192.168.51.195  255.255.255.255         On-link    192.168.51.195    311
   192.168.51.255  255.255.255.255         On-link    192.168.51.195    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    192.168.51.195    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    192.168.51.195    311
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.0.2  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 14     71 ::/0                     fe80::94e0:f1ff:fe7e:2cc3
  1    331 ::1/128                  On-link
 14     71 2409:40c1:3018:64bc::/64 On-link
 14    311 2409:40c1:3018:64bc:dd22:fcc6:6229:feff/128
                                    On-link
 14    311 2409:40c1:3018:64bc:f996:1959:8158:250c/128
                                    On-link
 14    311 fe80::/64                On-link
 14    311 fe80::829f:656:7621:3e1d/128
                                    On-link
  1    331 ff00::/8                 On-link
 14    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Date: 8/8/2025

7. nslookup

Description:

The nslookup (Name Server Lookup) command is used to **get the IP address of a domain name** or **find the domain name of an IP address**. It helps in **troubleshooting DNS (Domain Name System) issues**.

It's commonly used to check if a domain is properly resolving to the correct IP address.

No.	Option	Description
1	nslookup	Enters **interactive mode** where you can run multiple DNS queries
2	nslookup [domain]	Returns the **IP address** of the given domain (e.g., nslookup google.com)
3	nslookup [IP]	Returns the **domain name** of the given IP (reverse lookup).
4	nslookup -debug	Displays **detailed debug** info for the DNS query.

Date: 8/8/2025

Implementation:

```
D:\¥@$#>nslookup
Default Server:  UnKnown
Address:  192.168.51.126

> google.com
Server:  UnKnown
Address:  192.168.51.126

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:823::200e
          142.251.223.142

> youtube.com
Server:  UnKnown
Address:  192.168.51.126

Non-authoritative answer:
Name:    youtube.com
Addresses:  2404:6800:4009:81d::200e
          142.250.193.14

>
```

Date: 8/8/2025

```
D:\¥@$#>nslookup google.com
Server:  UnKnown
Address:  192.168.51.126

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:808::200e
          142.251.223.142
```

```
D:\¥@$#>nslookup 8.8.8.8
Server:  UnKnown
Address:  192.168.51.126

Name:    dns.google
Address:  8.8.8.8
```

Date: 8/8/2025

```
D:\¥@$#>nslookup -debug
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NXDOMAIN
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 0,  additional = 0

    QUESTIONS:
        126.51.168.192.in-addr.arpa, type = PTR, class = IN

------------
Default Server:  UnKnown
Address:  192.168.51.126

> google.com
Server:  UnKnown
Address:  192.168.51.126

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.com, type = A, class = IN
    ANSWERS:
    ->  google.com
        internet address = 216.58.200.206
        ttl = 186 (3 mins 6 secs)

------------
Non-authoritative answer:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.com, type = AAAA, class = IN
    ANSWERS:
    ->  google.com
        AAAA IPv6 address = 2404:6800:4009:827::200e
        ttl = 111 (1 min 51 secs)

------------
Name:    google.com
Addresses:  2404:6800:4009:827::200e
          216.58.200.206

>
```

Date: 8/8/2025

8. hostname

Description:

The hostname command is used to **display the name of your computer (device name)** on the network. This name is used to **identify your system** on local or organizational networks.

It is very simple and useful for checking or confirming your system's **network identity**.

On **Windows**, hostname is mostly just for viewing.
On **Linux**, it can also be used to **change** the hostname (with root access).

No.	Option	Description
1	hostname	Displays the **name of the current computer (host)** on the network.
2	hostname /?	Shows **help and usage options** for the command.

Implementation:

```
D:\¥@$#>hostname
YASH
```

```
D:\¥@$#>hostname /?

Prints the name of the current host.

hostname
```

Date: 8/8/2025

9. pathping

Description:

The pathping command is a combination of **ping and tracert**. It not only shows the **route data takes** to reach a destination but also gives **detailed statistics about packet loss** at each hop (network device) along the way.

It is especially useful for **troubleshooting unreliable networks** or **identifying where packet loss is happening**.

Takes longer to complete than tracert, but provides **more detailed results**.

No.	Option	Description
1	pathping	Traces and analyzes route to google.com
2	pathping -h <max_hops>	Limits the number of **maximum hops** (default is 30)
3	pathping -w <timeout>	Sets **wait time** (ms) per reply (default is 3000ms)
4	pathping -q <queries>	Sets number of **queries (pings)** per hop (default is 100)

Implementation:

```
D:\¥@$#>pathping google.com

Tracing route to google.com [2404:6800:4002:812::200e]
over a maximum of 30 hops:
  0  YASH [2409:40c1:3018:64bc:f996:1959:8158:250c]
  1  2409:40c1:3018:64bc::31
  2  2405:200:5210:5:3924:110:3:108
  3  2405:200:5210:5:3925::1
  4     *        *        *
Computing statistics for 75 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           YASH [2409:40c1:3018:64bc:f996:1959:8158:25
0c]
                                     0/ 100 =  0%   |
  1    6ms     0/ 100 =  0%     0/ 100 =  0%  2409:40c1:3018:64bc::31
                                     0/ 100 =  0%   |
  2   42ms     0/ 100 =  0%     0/ 100 =  0%  2405:200:5210:5:3924:110:3:108
                                   100/ 100 =100%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  2405:200:5210:5:3925::1

Trace complete.
```

Date: 8/8/2025

```
D:\¥@$#>pathping -h 7 google.com

Tracing route to google.com [2404:6800:4002:812::200e]
over a maximum of 7 hops:
  0  YASH [2409:40c1:3018:64bc:f996:1959:8158:250c]
  1  2409:40c1:3018:64bc::31
  2  2405:200:5210:5:3924:110:3:108
  3  2405:200:5210:5:3925::1
  4     *        *        *
Computing statistics for 75 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           YASH [2409:40c1:3018:64bc:f996:1959:8158:25
0c]
                                  0/ 100 =  0%   |
  1    6ms     0/ 100 =  0%     0/ 100 =  0%  2409:40c1:3018:64bc::31
                                  0/ 100 =  0%   |
  2   41ms     0/ 100 =  0%     0/ 100 =  0%  2405:200:5210:5:3924:110:3:108
                                100/ 100 =100%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  2405:200:5210:5:3925::1

Trace complete.
```

```
D:\¥@$#>pathping -w 7777 google.com

Tracing route to google.com [2404:6800:4002:812::200e]
over a maximum of 30 hops:
  0  YASH [2409:40c1:3018:64bc:f996:1959:8158:250c]
  1  2409:40c1:3018:64bc::31
  2  2405:200:5210:5:3924:110:3:108
  3  2405:200:5210:5:3925::1
  4     *        *        *
Computing statistics for 75 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           YASH [2409:40c1:3018:64bc:f996:1959:8158:25
0c]
                                  0/ 100 =  0%   |
  1    6ms     0/ 100 =  0%     0/ 100 =  0%  2409:40c1:3018:64bc::31
                                  0/ 100 =  0%   |
  2   45ms     0/ 100 =  0%     0/ 100 =  0%  2405:200:5210:5:3924:110:3:108
                                100/ 100 =100%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  2405:200:5210:5:3925::1

Trace complete.
```

Date: 8/8/2025

```
D:\¥@$#>pathping -q 77 google.com

Tracing route to google.com [2404:6800:4002:812::200e]
over a maximum of 30 hops:
  0  YASH [2409:40c1:3018:64bc:f996:1959:8158:250c]
  1  2409:40c1:3018:64bc::31
  2  2405:200:5210:5:3924:110:3:108
  3  2405:200:5210:5:3925::1
  4     *        *        *
Computing statistics for 57 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          YASH [2409:40c1:3018:64bc:f996:1959:8158:25
0c]
                                     0/  77 =  0%   |
  1    5ms     0/  77 =  0%     0/  77 =  0%  2409:40c1:3018:64bc::31
                                     0/  77 =  0%   |
  2   40ms     0/  77 =  0%     0/  77 =  0%  2405:200:5210:5:3924:110:3:108
                                    77/  77 =100%   |
  3  ---      77/  77 =100%     0/  77 =  0%  2405:200:5210:5:3925::1

Trace complete.
```

10. arp

Description:

The arp (Address Resolution Protocol) command is used to **view and manage the ARP cache** on your system. ARP is the protocol that maps **IP addresses to MAC addresses**. When your computer communicates over a network, it needs to know the **MAC address** of other devices — and ARP helps with that.

This command is useful for **network diagnostics**, especially in **local networks (LANs)**.

Mostly used by network administrators to **inspect or control device communication** on a LAN.

No.	Option	Description
1	arp -a	Displays the **current** ARP table (IP–MAC mappings).
2	arp -g	Same as arp -a (just **another way** to show the table).
3	arp -d <IP>	**Deletes** a specific ARP entry. Requires admin rights.
4	arp -s <IP> <MAC>	**Adds a static entry** (manual IP-to-MAC mapping).

Date: 8/8/2025

Implementation:

```
D:\¥@$#>arp -a

Interface: 192.168.51.195 --- 0xe
  Internet Address      Physical Address      Type
  192.168.51.126        96-e0-f1-7e-2c-c3     dynamic
  192.168.51.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

```
D:\¥@$#>arp -g

Interface: 192.168.51.195 --- 0xe
  Internet Address      Physical Address      Type
  192.168.51.126        96-e0-f1-7e-2c-c3     dynamic
  192.168.51.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Date: 8/8/2025

Lab Practical #02:

Study of different network devices in detail.

Practical Assignment #02:

1. Give difference between below network devices.
   - Hub and Switch
   - Switch and Router
   - Router and Gateway
2. Working of below network devices:
   - Repeater
   - Modem((DSL and ADSL)
   - Hub
   - Bridge
   - Switch
   - Router
   - Gateway

Date: 8/8/2025

1. Give difference between below network devices.

Hub and Switch

No.	Hub	Switch
1	Operates at OSI Layer 1 (Physical Layer)	Operates at OSI Layer 2 (Data Link Layer)
2	Broadcasts data to all connected devices	Sends data only to the intended recipient device
3	Less intelligent – no MAC address learning	More intelligent – uses MAC address table to forward data
4	More network collisions, less efficient	Fewer collisions due to full-duplex communication
5	Generally cheaper, but outdated	More expensive but efficient and widely used today

Switch and Router

No.	Switch	Router
1	Operates at OSI Layer 2 (Data Link Layer)	Operates at OSI Layer 3 (Network Layer)
2	Connects devices within the same network (LAN)	Connects different networks (LAN to WAN or LAN to LAN)
3	Uses MAC addresses to forward data	Uses IP addresses to route data
4	No need for IP address configuration	Requires IP address configuration
5	Mainly used to expand network within a building	Mainly used to provide internet access or connect networks

Router and Gateway

No.	Router	Gateway
1	Operates at OSI Layer 3 (Network Layer)	Can operate at any OSI layer (typically Layer 3 or above)
2	Connects two or more similar networks (e.g., LAN to LAN)	Connects two dissimilar networks (e.g., a private network to the internet)
3	Uses IP routing to forward packets	Performs protocol conversion as needed between networks
4	Commonly used in home and enterprise networks	Acts as an entry/exit point to external networks
5	Handles packet forwarding and routing	Translates data formats, addresses, or protocols

Date: 8/8/2025

2. Working of below network devices:

1. Repeater

- A repeater is a network device used to regenerate and amplify signals.
- It operates at the **Physical Layer (Layer 1)** of the OSI model.
- When a signal travels over long distances, it weakens or degrades.
- The repeater receives this weak signal, strengthens it, and retransmits it.
- It helps extend the physical range of a network (e.g., Ethernet).
- Repeaters do **not** filter or route traffic, only regenerate it.
- Commonly used in both wired and wireless communication.
- It does not read the data; only deals with electrical signals.
- Ideal for LAN setups with distance limitations.

2. Modem (DSL and ADSL)

- A **Modem** (modulator-demodulator) converts digital data to analog and vice versa.
- **DSL** stands for Digital Subscriber Line, using phone lines for internet.
- **ADSL** is Asymmetric DSL: higher download speed than upload.
- It allows simultaneous voice and data communication.
- Modems are used to connect homes/offices to ISPs.
- Operates between digital networks (PCs) and analog systems (telephone lines).
- The modem modulates outgoing digital signals and demodulates incoming analog.
- Essential for internet access over copper telephone wires.
- Modern DSL modems often come integrated with routers.

3. Hub

- A **hub** is a basic networking device that connects multiple computers.
- Operates at the **Physical Layer (Layer 1)** of the OSI model.
- It simply repeats incoming data to all ports, regardless of the recipient.
- Causes unnecessary traffic and increases chances of data collisions.
- Hubs do not use MAC addresses or perform filtering.
- All connected devices share the same bandwidth.
- Performance degrades with network size and traffic.
- Useful in small, temporary, or legacy networks.
- Largely replaced by switches in modern networks.

4. Bridge

- A **bridge** connects two or more separate network segments.
- Operates at the **Data Link Layer (Layer 2)**.
- Uses MAC addresses to filter and forward data frames.
- Helps reduce network traffic by dividing a large network into segments.
- Prevents unnecessary traffic from crossing into other segments.
- Useful in managing congestion and improving performance.
- Can be hardware-based or software-based.

- Typically used in LAN environments.
- Unlike routers, bridges do not use IP addresses.

5. Switch

- A **switch** is a smart device that connects multiple devices within a LAN.
- Works at the **Data Link Layer (Layer 2)**, sometimes Layer 3 for advanced models.
- Uses MAC address tables to forward data to the intended device only.
- Reduces unnecessary traffic and collisions compared to hubs.
- Supports full-duplex communication, increasing efficiency.
- Improves bandwidth usage and network performance.
- Each port on a switch has its own collision domain.
- Widely used in modern Ethernet networks.
- Some switches support VLANs and Layer 3 routing.

6. Router

- A **router** connects multiple networks, such as LAN to WAN.
- Operates at the **Network Layer (Layer 3)** of the OSI model.
- Uses **IP addresses** to determine the best path for data packets.
- Performs network address translation (NAT) for internet sharing.
- Routes data between different subnets and networks.
- Can provide firewall and DHCP services.
- Essential for internet connectivity in homes and businesses.
- Maintains routing tables for efficient data forwarding.
- Can be wired, wireless, or combined with switches/modems.

7. Gateway

- A **gateway** connects two dissimilar networks using different protocols.
- Operates at **any OSI layer**, commonly Layer 3 and above.
- Translates data formats, addresses, or protocols as needed.
- Serves as an entry or exit point for a network.
- Often used when connecting enterprise networks to the internet.
- Converts protocols like TCP/IP to others (e.g., VoIP, email).
- Can be a standalone device or built into routers/firewalls.
- Handles data encapsulation and protocol conversion.
- Acts as a protocol interpreter between incompatible systems.

Date: 8/8/2025

Lab Practical #03:

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

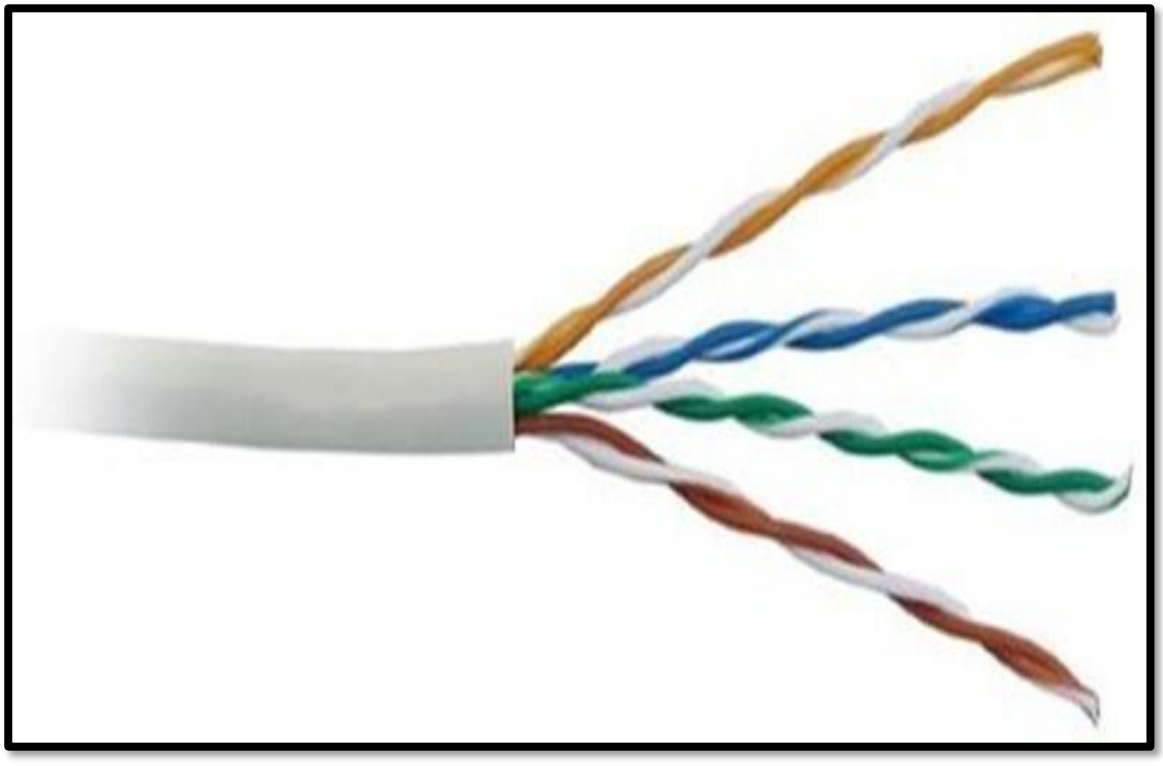
Practical Assignment #03:

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) Unshielded Twisted Pair (UTP) Cable:

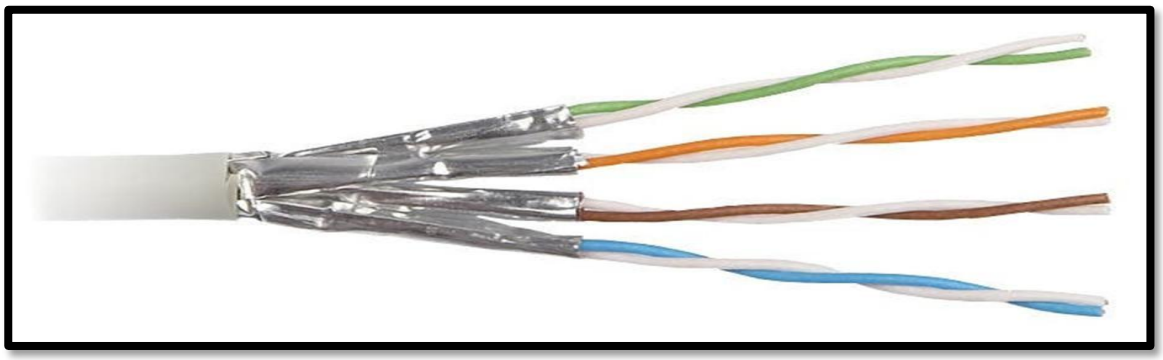
- **Description**: Unshielded twisted pair cable is one of the most commonly used cables in computer networks at present time. UTP consists of two insulated copper wires twisted around one another, the twisting of wires helps in controlling interference. It is inexpensive and easy to install. It is also Flexible and lightweight.
- **Diagram**:



Date: 8/8/2025

b) Shielded Twisted Pair (STP) Cable:

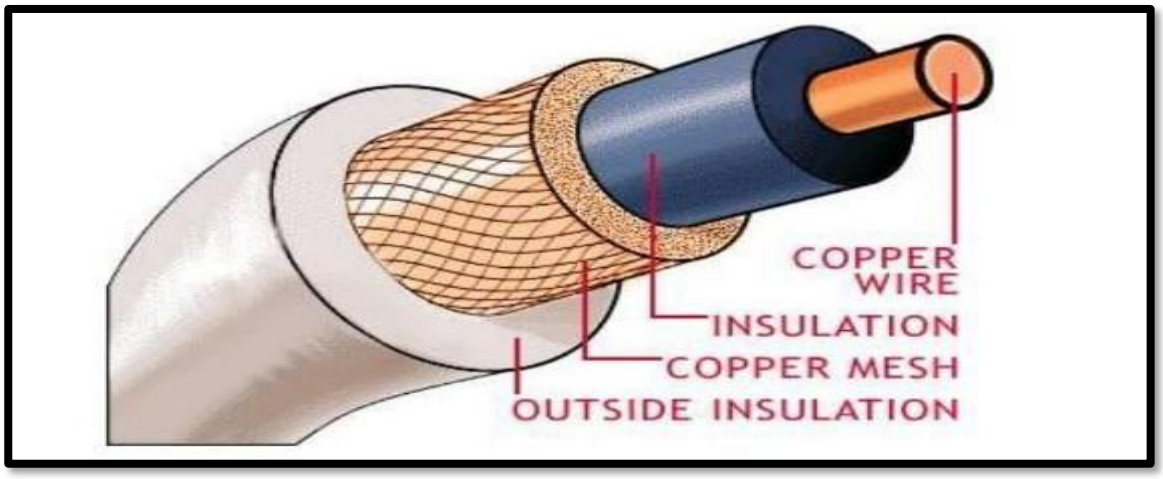
- **Description**: In STP the wires are covered by a copper braid covering or a foil shield, this foil shield adds a layer that protects it against interference leaking into and out of the cable. Hence, they are used for longer distances and higher transmission rates. Much better at blocking interference (EMI and radio-frequency interference). More reliable in "noisy" environments. Thicker, heavier, and more expensive than UTP.
- **Diagram**:



c) Coaxial Cables:

- **Description**: Coaxial cables contain a center conductor and a metal shield insulated by a plastic layer placed in between. The metal shield in coaxial cables blocks any elements or interferences from the outside.
  In a coaxial cable, the outer layer, known as sheath, protects the cable from physical damage. Meanwhile, the metal shield protects the cable from any external interference, and the insulation between the metal shield and the conductor protects the conductor – the core of the coaxial cable. Good protection from interference thanks to its thick shielding. Can carry high-frequency signals.

- **Diagram**:

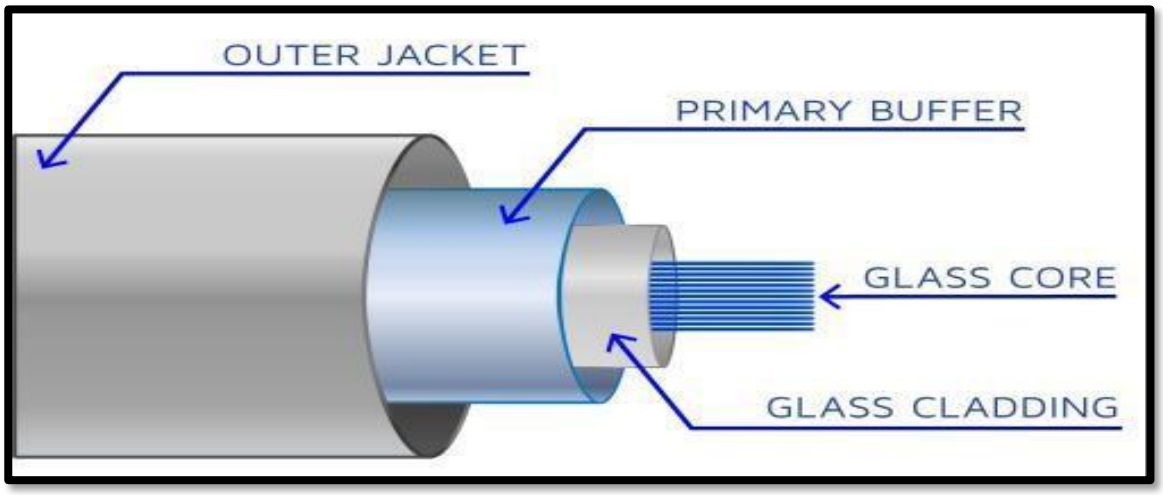


Date: 8/8/2025

d) Fiber Optic Cables:

- **Description**: Fiber optic cables use optical fibers which are made of glass cores surrounded by several layers of covering material generally made of PVC or Teflon. It transmits data in the form of light signals due to which there are no interference issues in fiber optics. Fiber optics can transmit signals over a very long distance as compared to twisted pairs or coaxial cables. Immune to electromagnetic interference. Far greater bandwidth (can carry more data at once). Extremely long-distance runs without boosters

- **Diagram**:



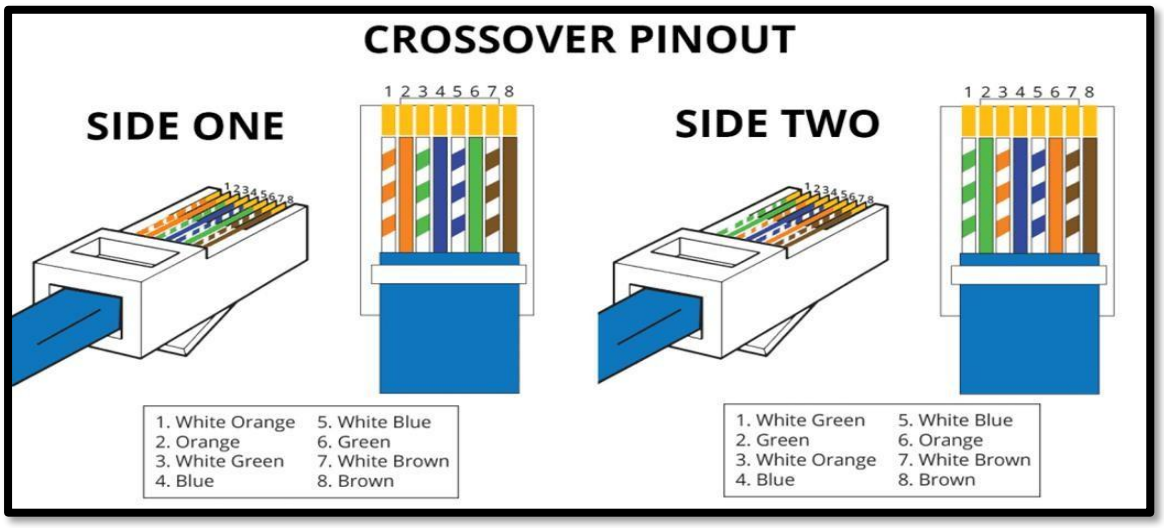
2. Difference between guided and unguided media.

Feature	Guided Media	Unguided Media
Definition	Data travels through a **physical medium**	Data travels through **air or space**
Examples	Twisted Pair, Coaxial, Fiber Optic	Radio waves, Microwaves, Infrared
Reliability	More reliable, less interference	Less reliable, affected by weather/interference
Speed	Usually faster due to dedicated paths	Slower over long distances
Cost	Installation is costlier	Cheaper to deploy, especially over large areas
Usage	LAN, WAN, telephony	Wi-Fi, satellite, cellular communication

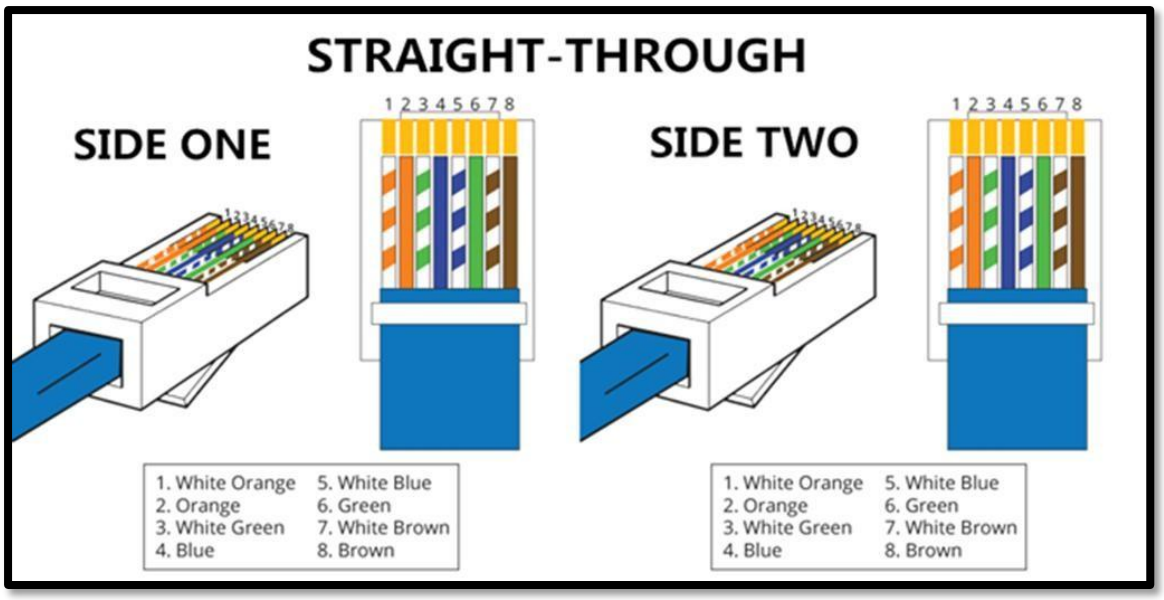
Date: 8/8/2025

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)



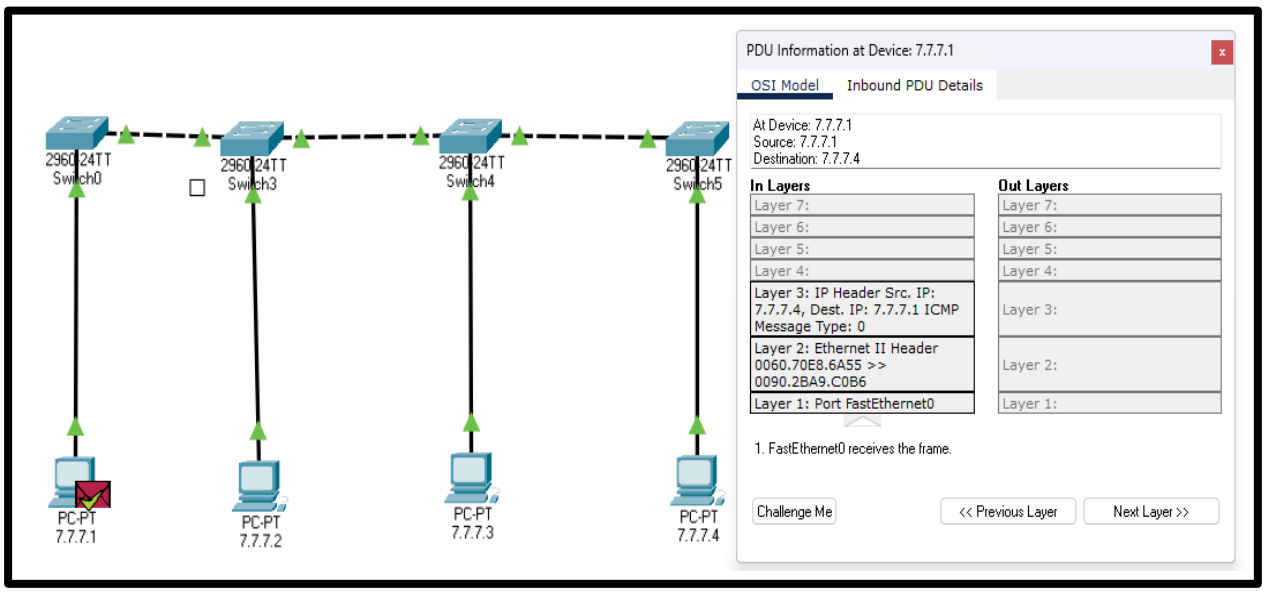
Date: 8/22/2025

Lab Practical #04:

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

Practical Assignment #04:

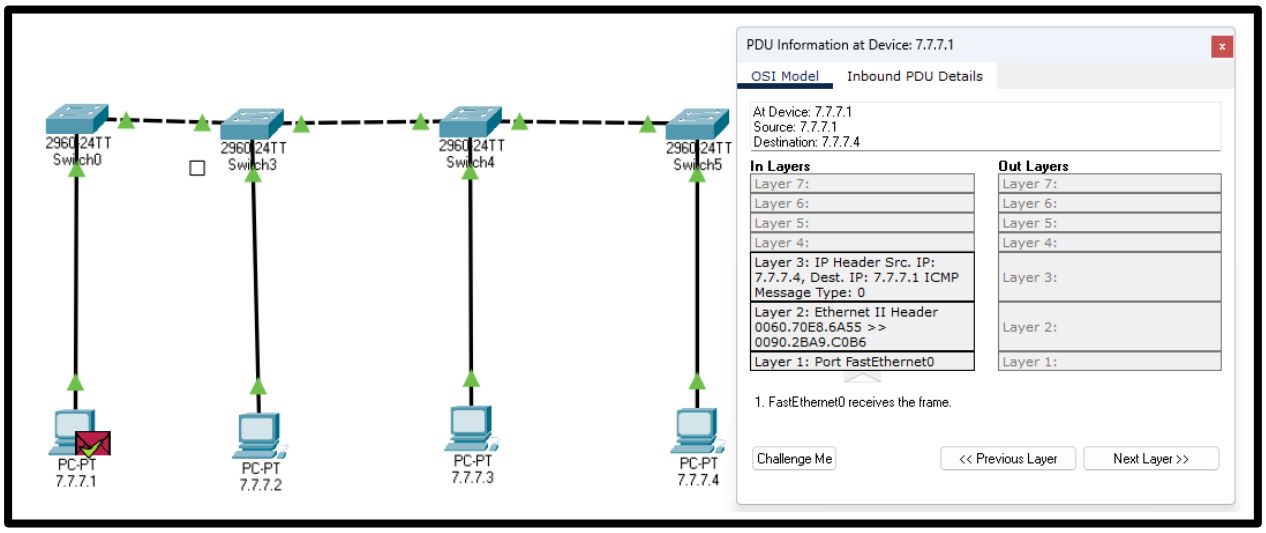
1. **Create a simple network with switch and two or more pc. Also check connectivity between them using ping command or PDU utility.**

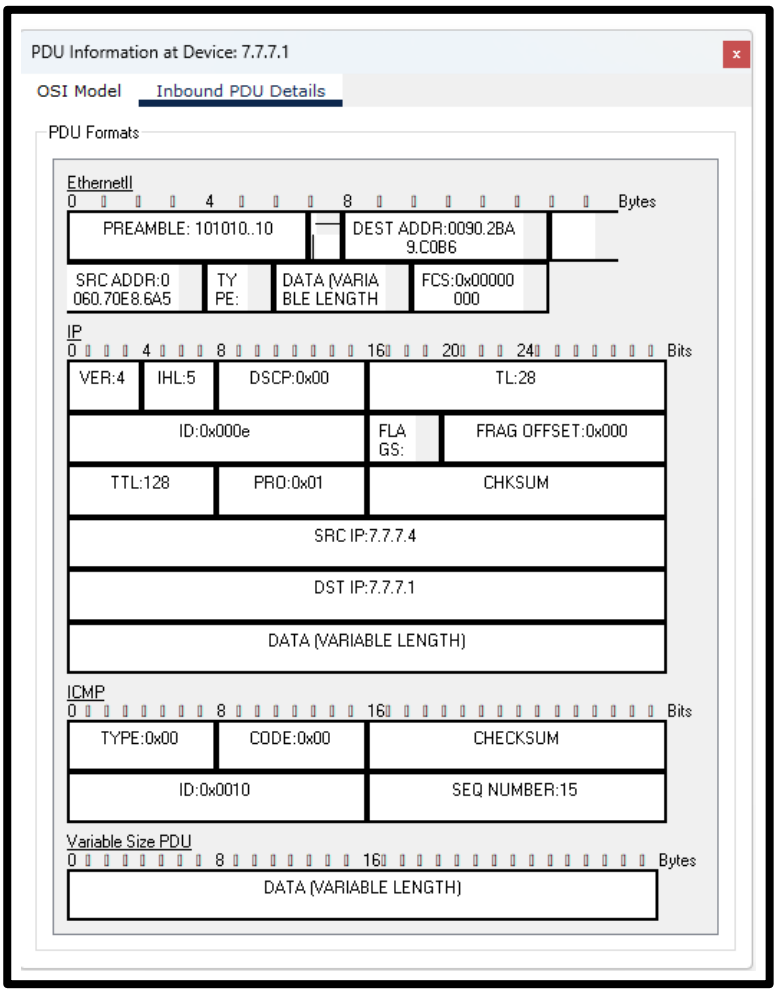


Date: 8/22/2025

2. Implement different topologies in packet tracer.

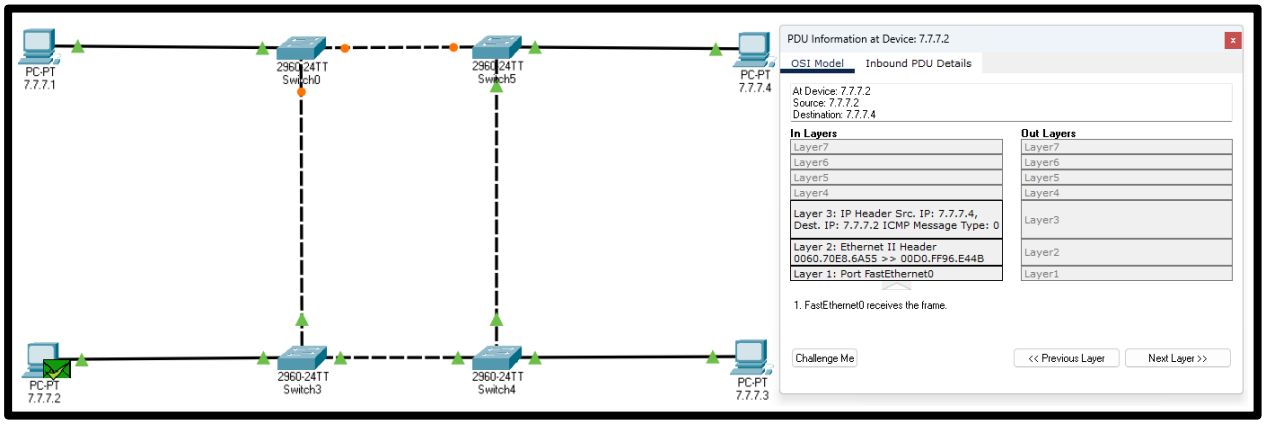
a. Bus

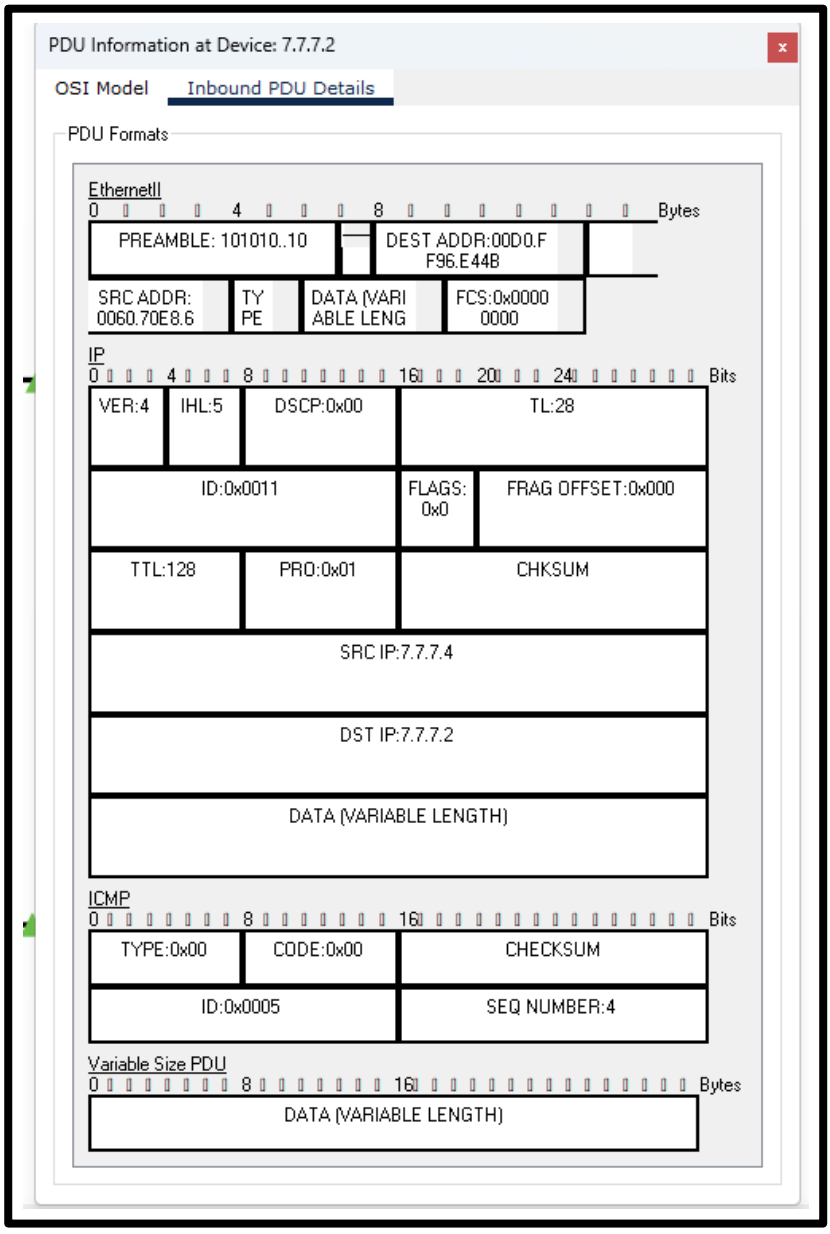




Date: 8/22/2025

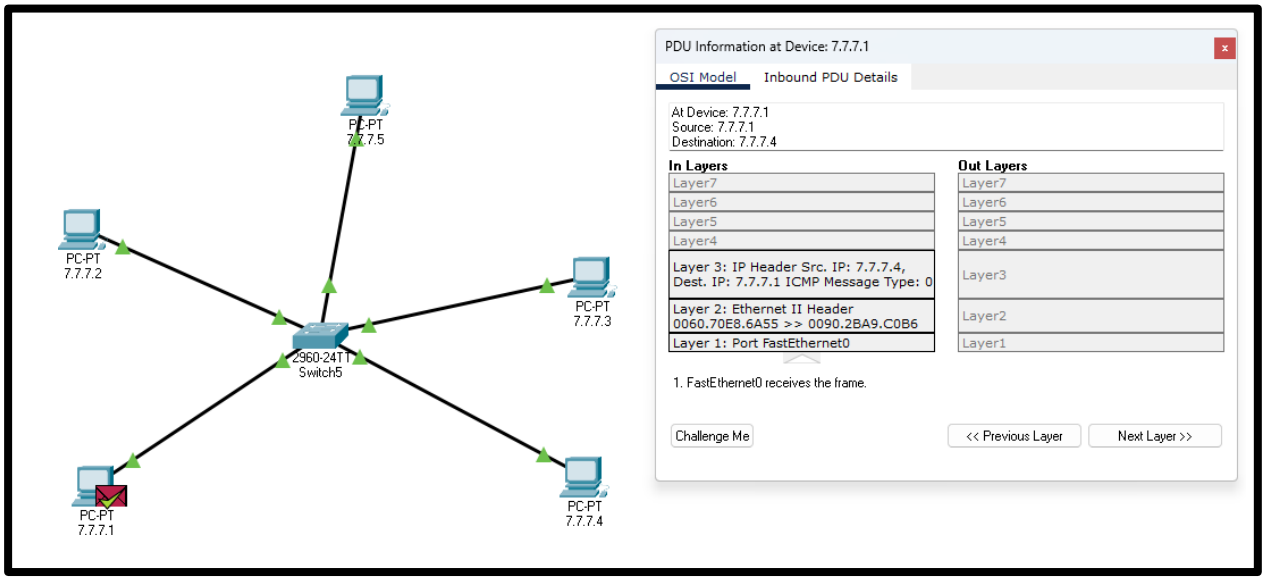
b. Ring

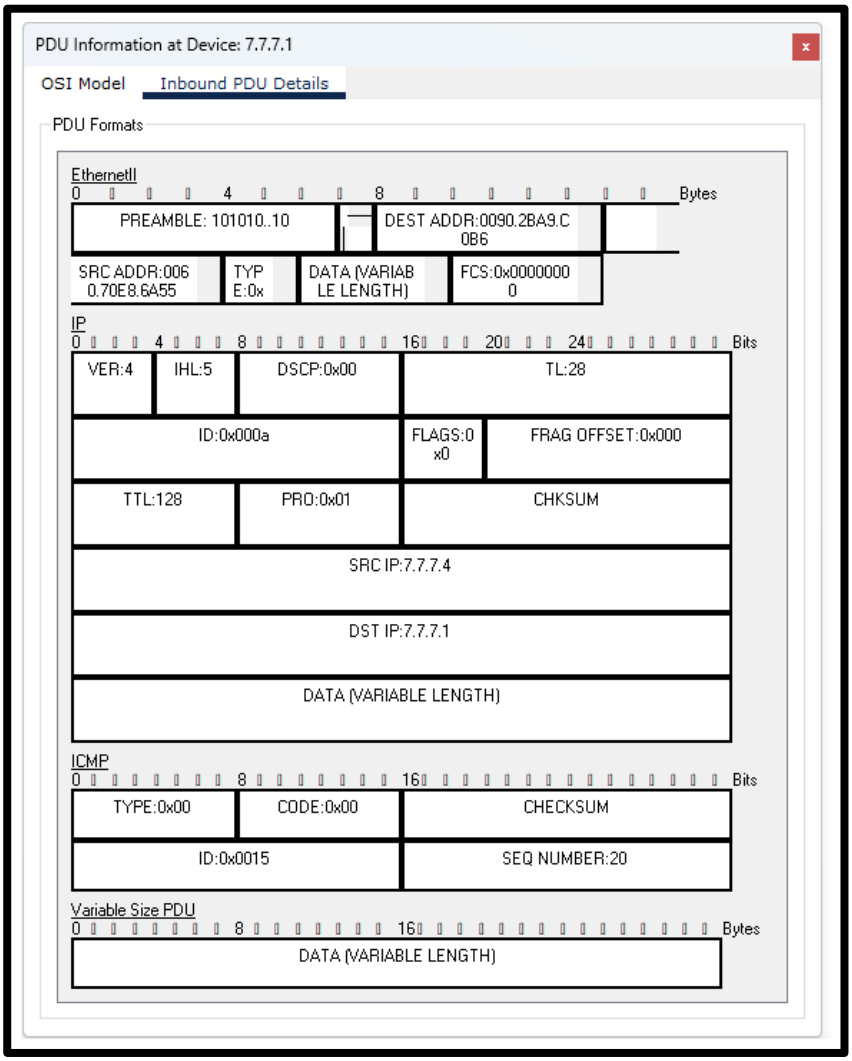




Date: 8/22/2025

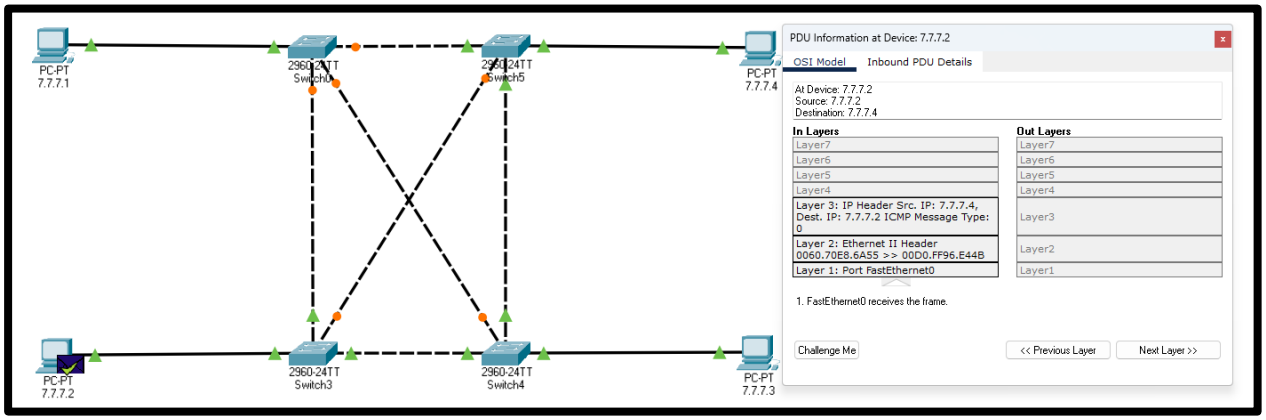
c. Star

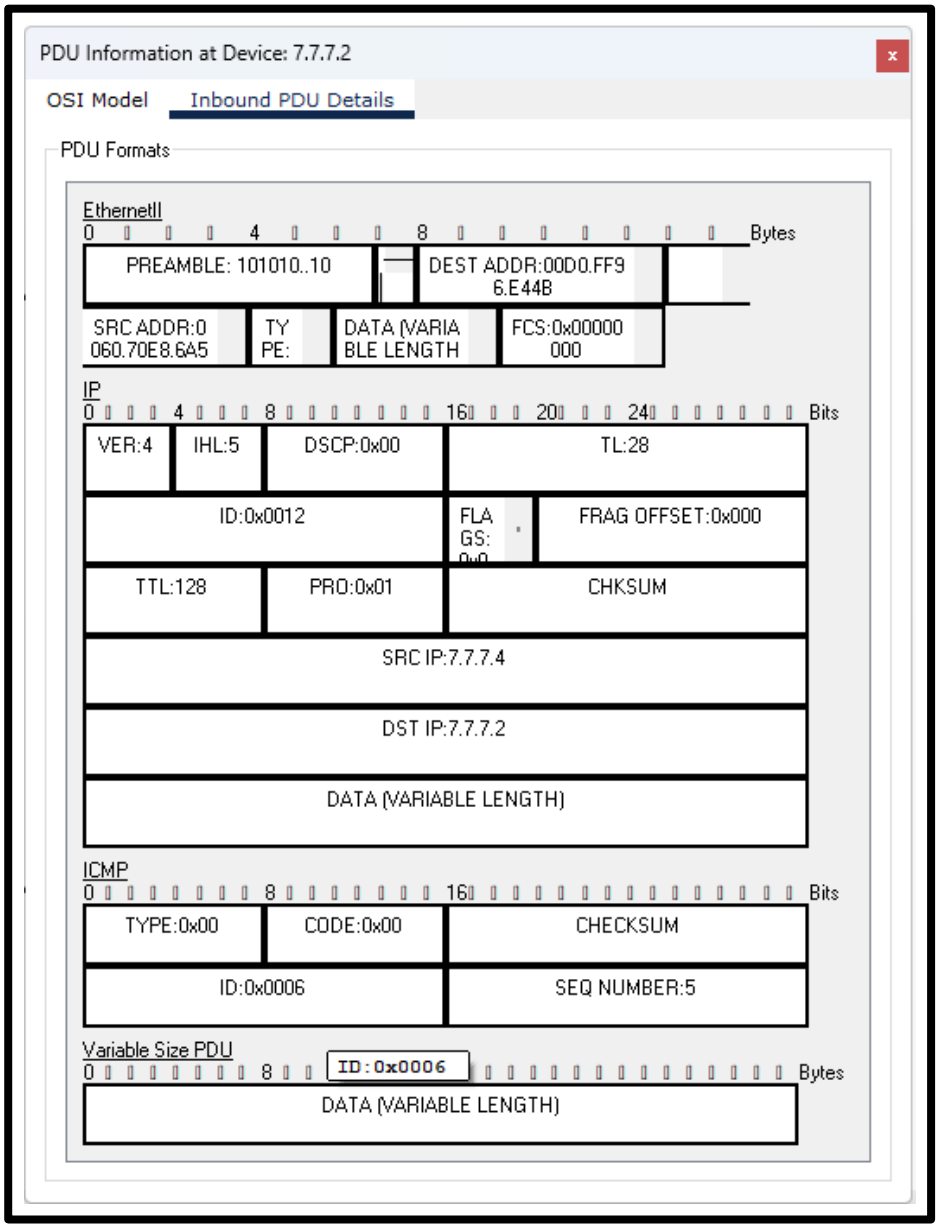




Date: 8/22/2025

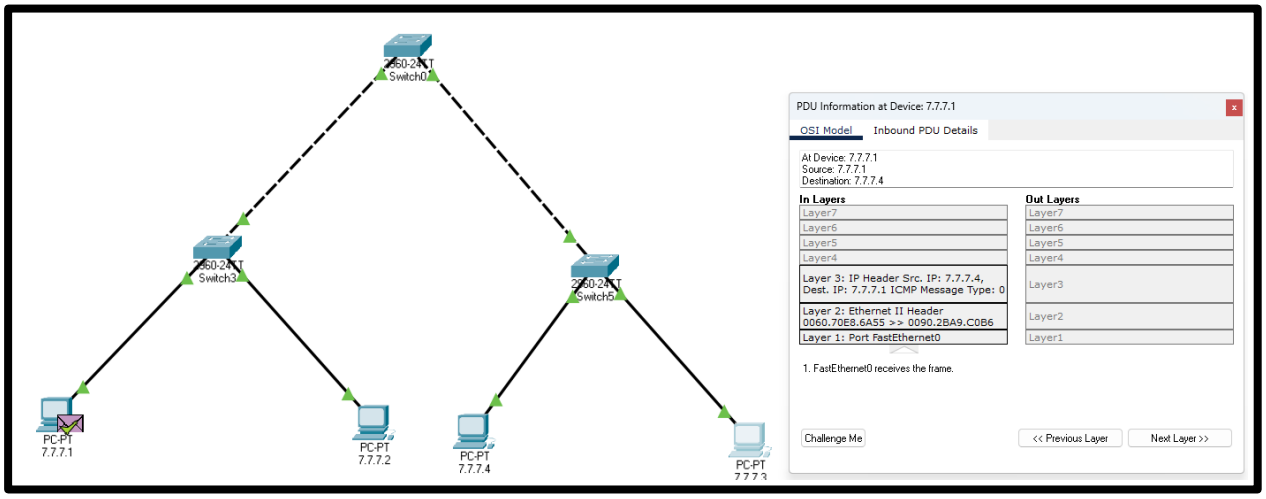
d. Mesh

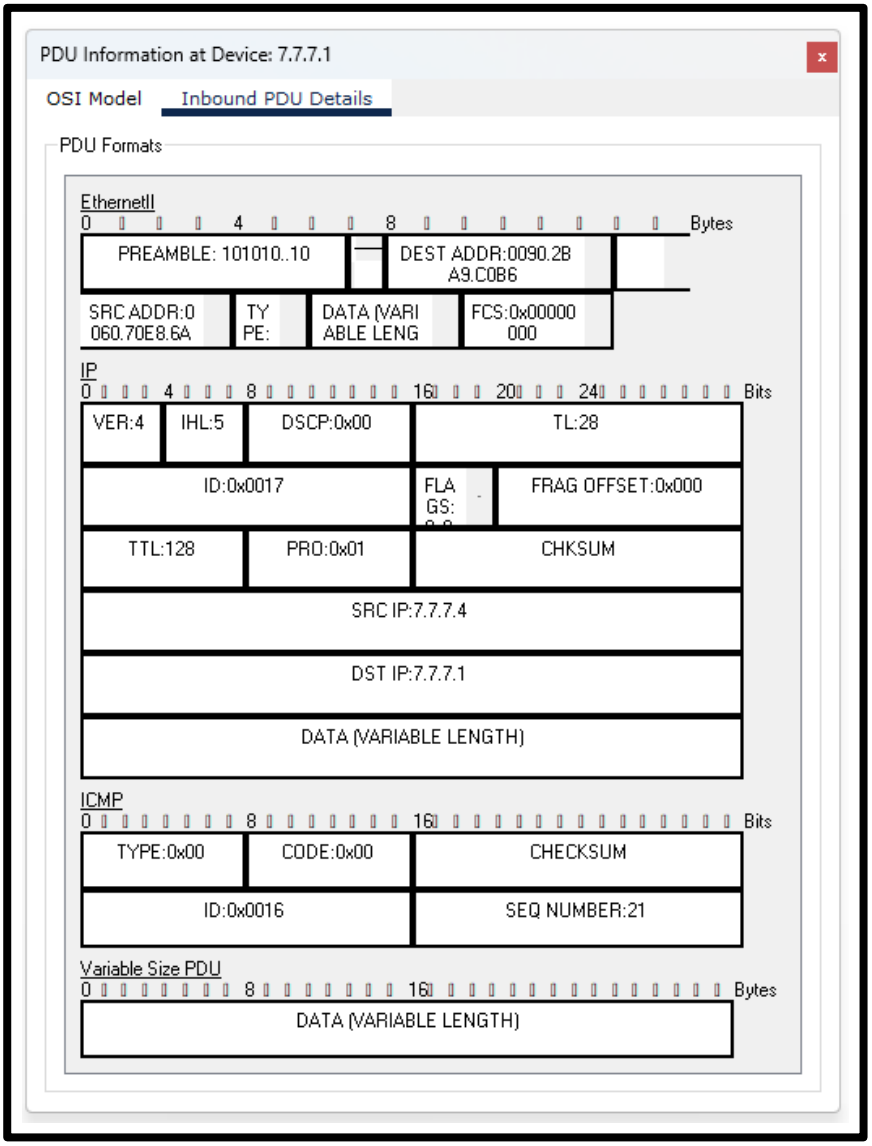




Date: 8/22/2025

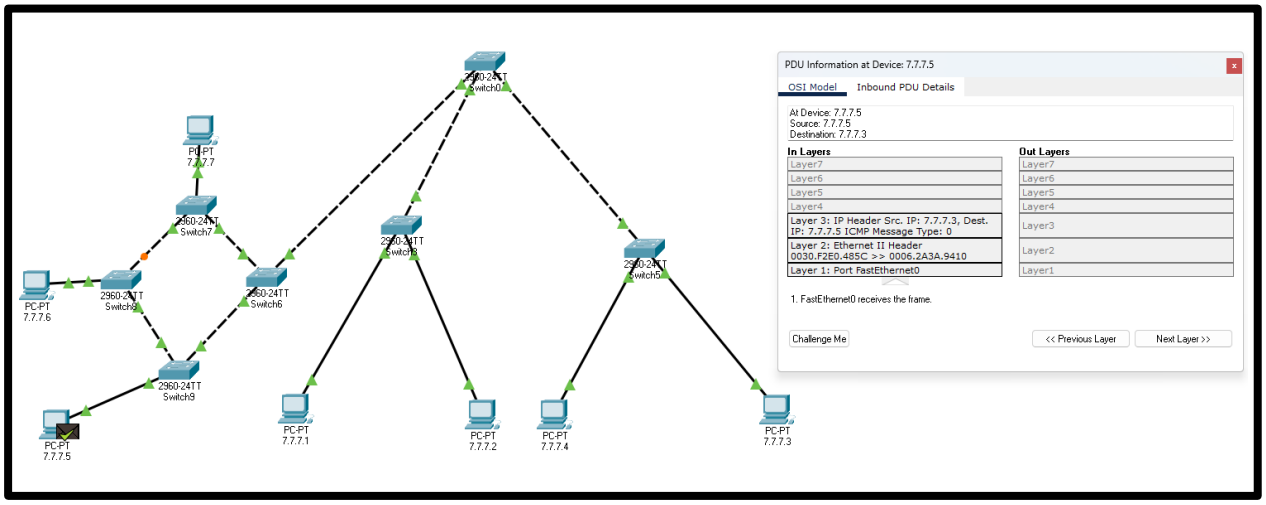
e. Tree

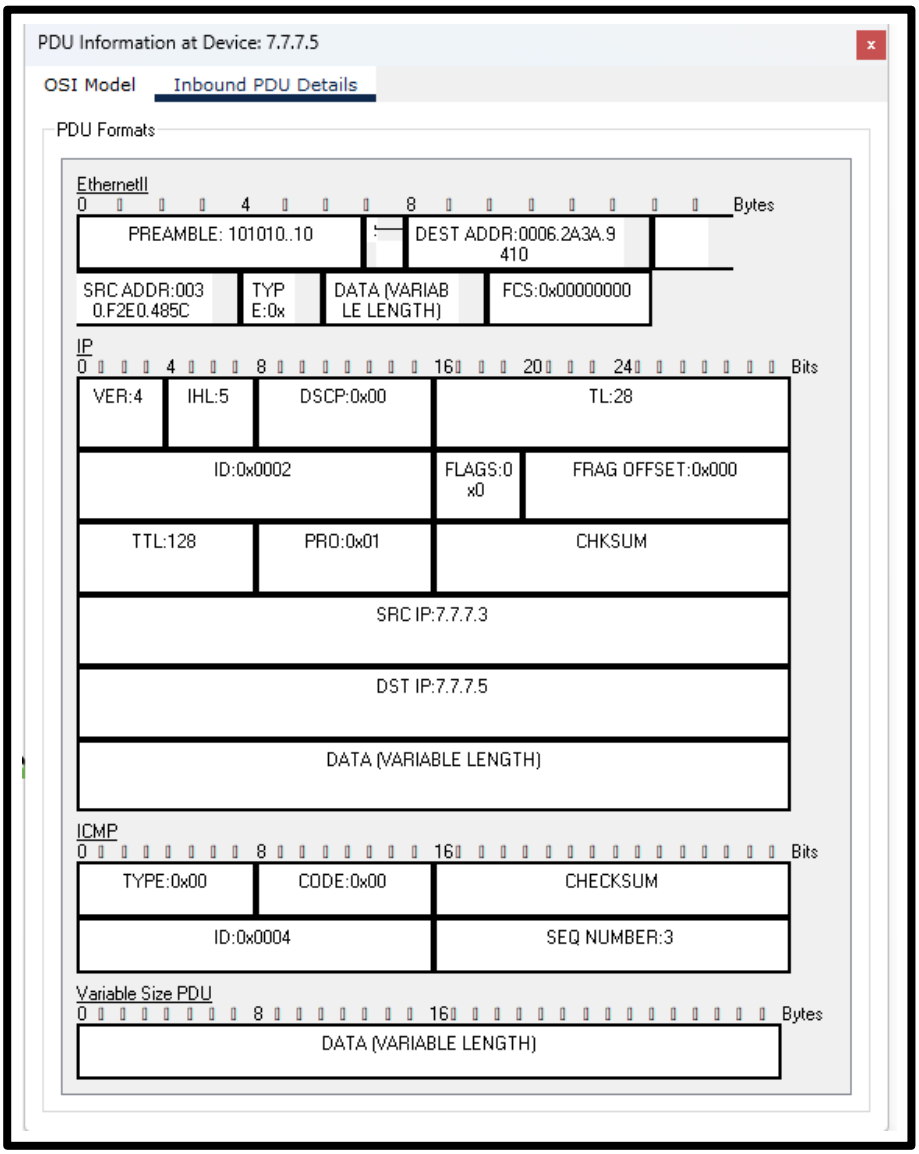




Date: 8/22/2025

f. Hybrid





Date: 8/22/2025

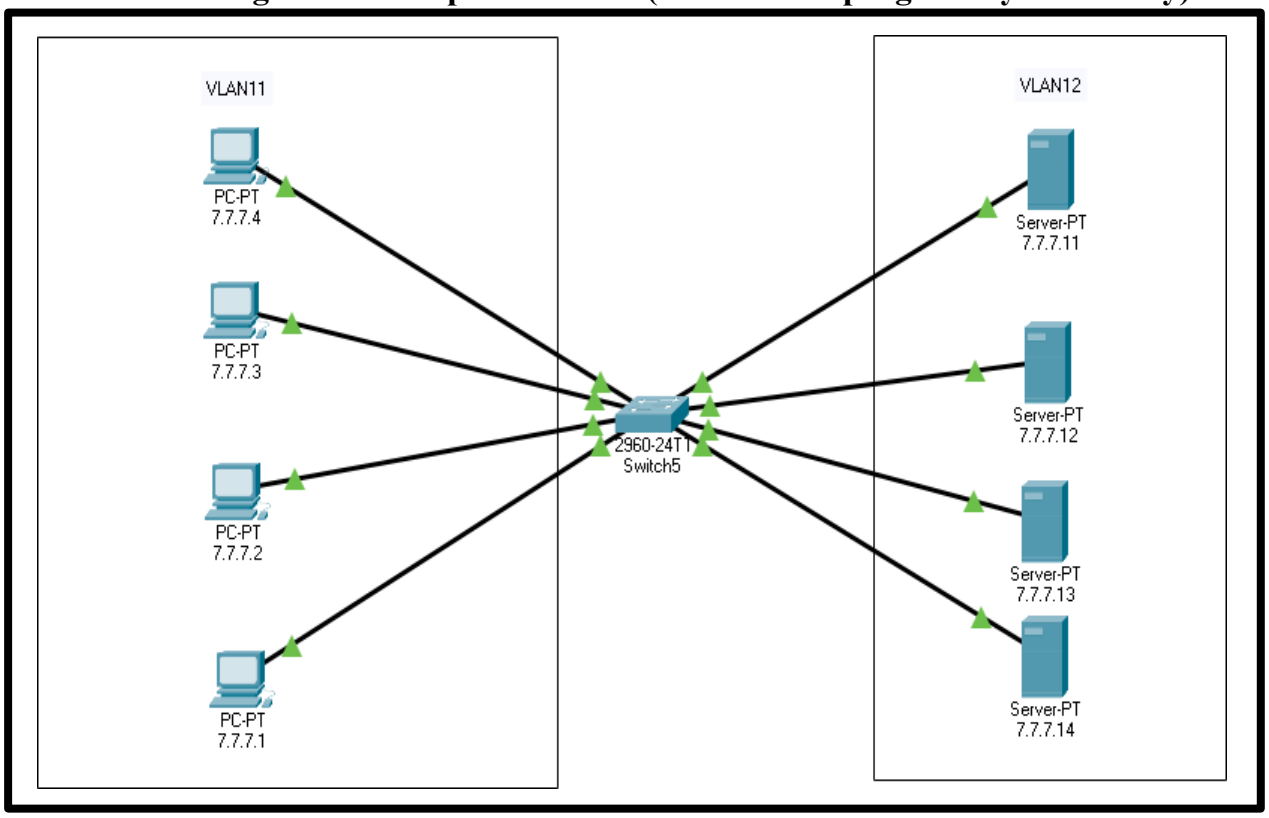
Lab Practical #05:

Study the concept of VLAN using packet tracer.

Practical Assignment #05:

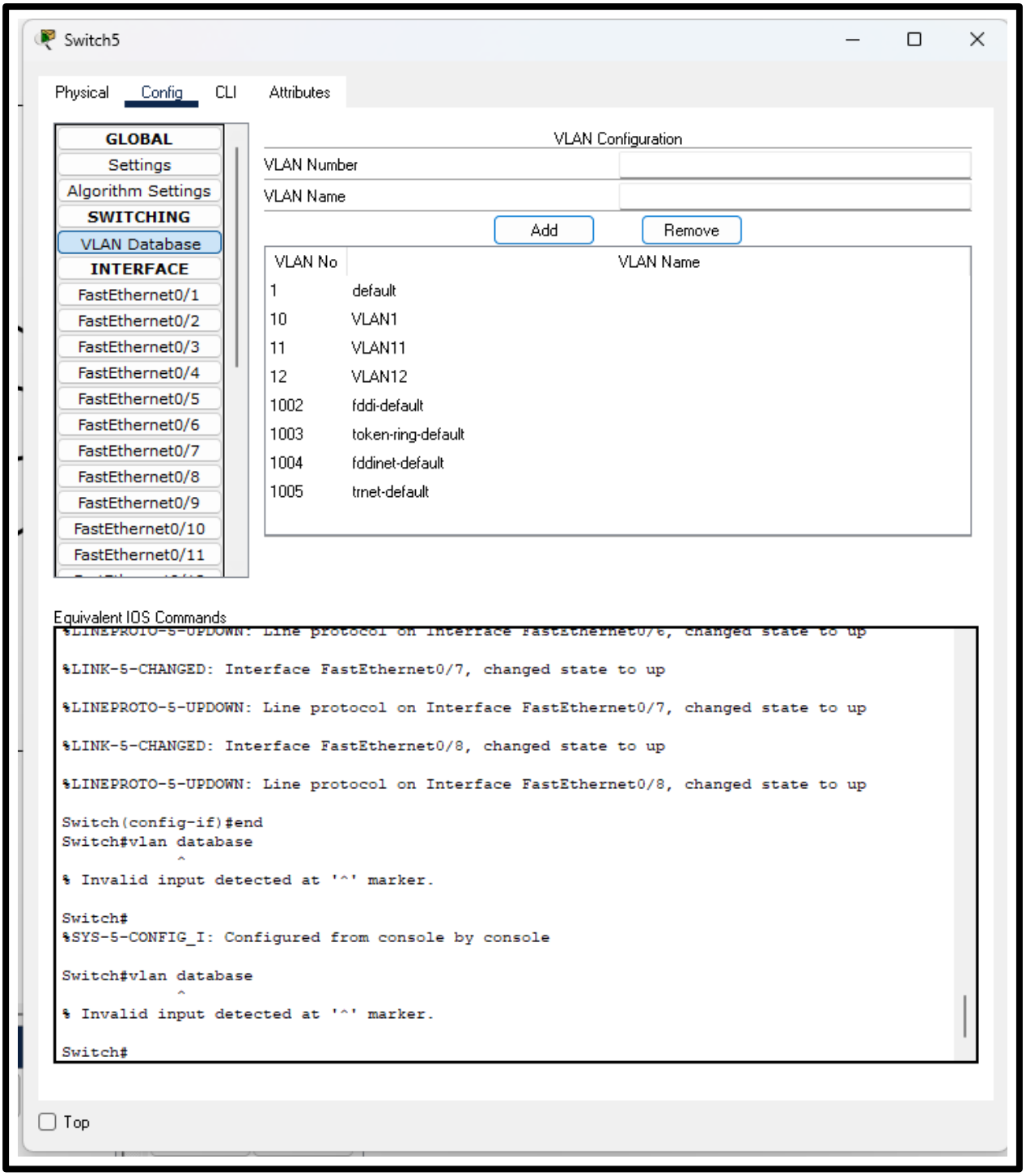
1. **Implement the different network structures in VLAN and VLAN trunking. Also check connectivity between them using ping command or PDU utility.**

1. **VLANs configuration setup screenshot. (VLAN example given by lab faculty)**



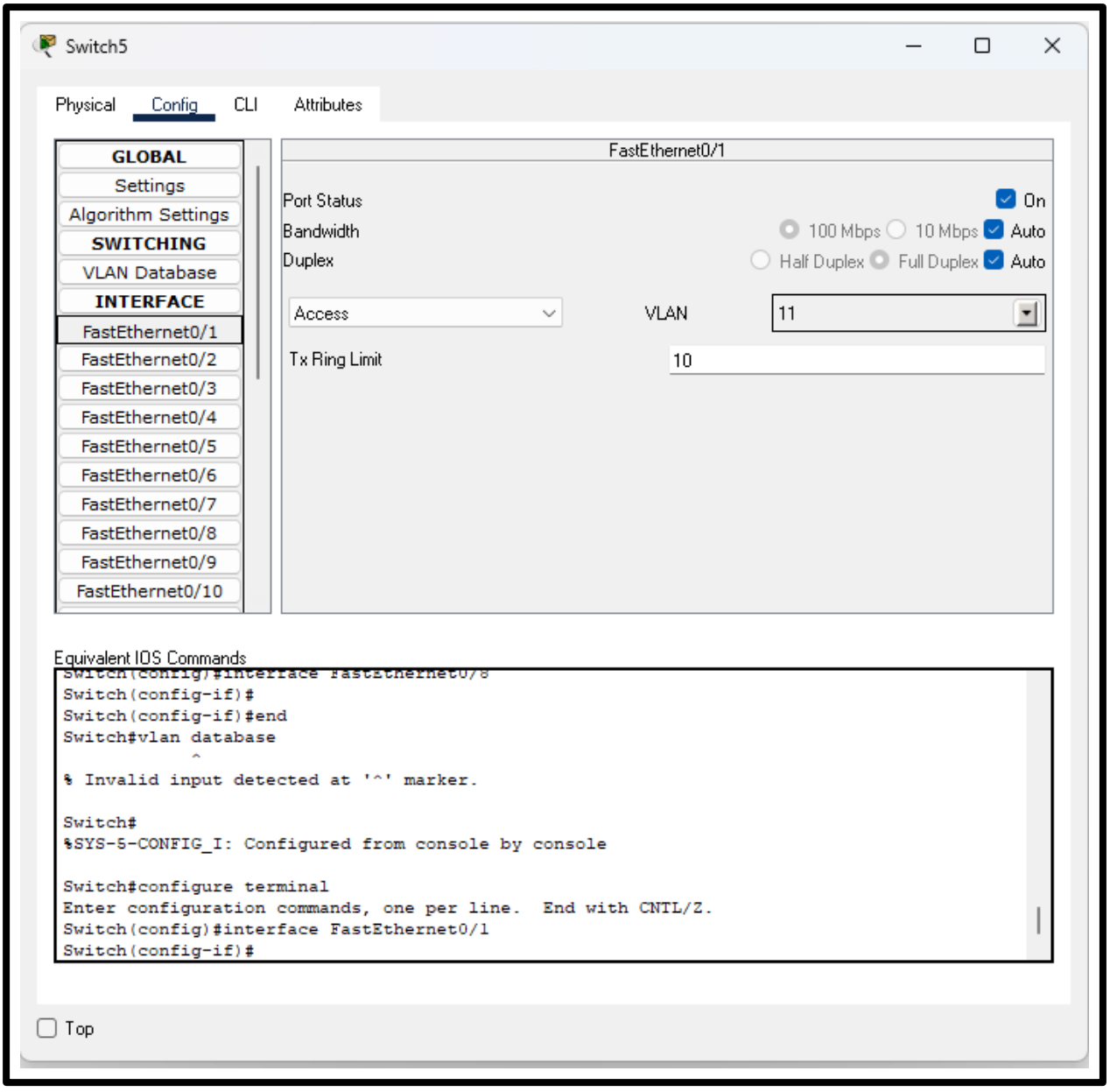
Date: 8/22/2025

VLAN Database



Date: 8/22/2025

Port



Date: 8/22/2025

2. Steps to create VLANs in packet tracer.

1. Open Packet Tracer and Add Devices

- Drag and drop a **2960 Switch** from the network devices section.
- Add some **PCs** and **Servers** to the workspace.
- Connect them to the switch using **Copper Straight-Through cables**.

2. Create VLANs on the Switch

1. Click on the switch.
2. Go to the **Config** tab.
3. From the left panel, click on **VLAN Database**.
4. In the VLAN Number field, type the VLAN ID (e.g., **11**) and give it a name (e.g., **VLAN11**).
5. Click **Add**.
6. Repeat the same process for VLAN 12 (name it **VLAN12**).
7. Now you will see both VLANs listed in the VLAN table.

3. Assign Ports to VLANs

1. In the same **Config** tab, click on **FastEthernet0/1** (or whichever port a PC is connected to).
2. Change **Port Mode** to **Access**.
3. From the VLAN drop-down menu, select **VLAN11** for PCs.
4. Do the same for all other PC ports (assign them to VLAN11).
5. Next, select the ports where servers are connected (e.g., FastEthernet0/5, 0/6, etc.).
6. Set **Port Mode** to **Access** and assign them to **VLAN12**.

4. Configure IP Addresses

- Assign IP addresses to each PC and Server by clicking on the device → **Desktop tab** → **IP Configuration**.
- Example:
    - PCs in VLAN11: **7.7.7.1 – 7.7.7.4**
    - Servers in VLAN12: **7.7.7.11 – 7.7.7.14**

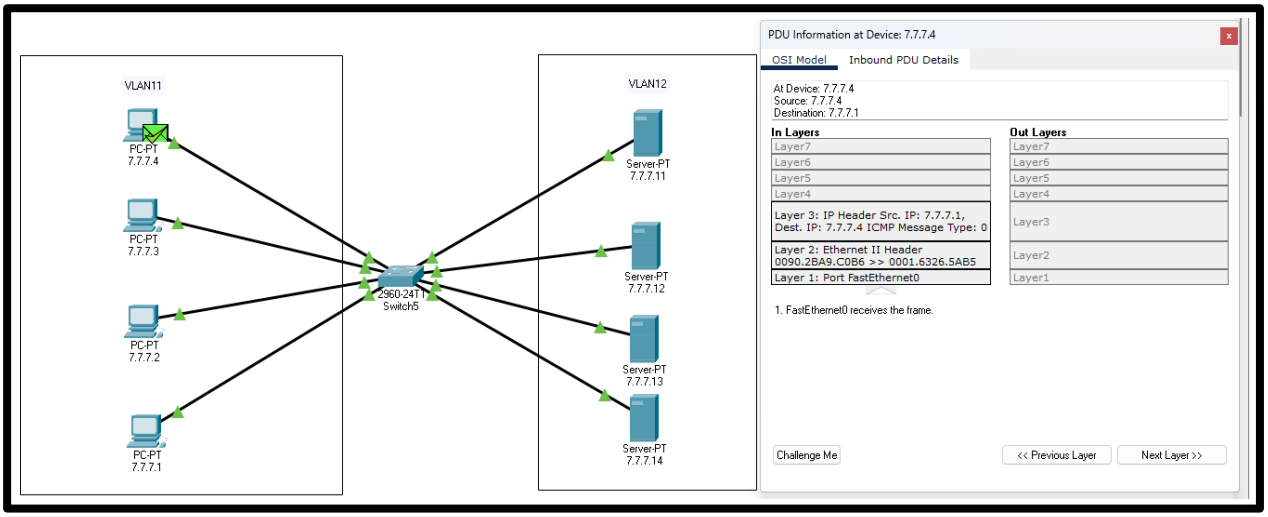
5. Test Connectivity

- Use the **ping tool** or **add a PDU** to check communication.
- Devices in the **same VLAN** will be able to communicate with each other.
- Devices in **different VLANs** will not communicate unless you configure a router or Layer 3 switch for inter-VLAN routing.

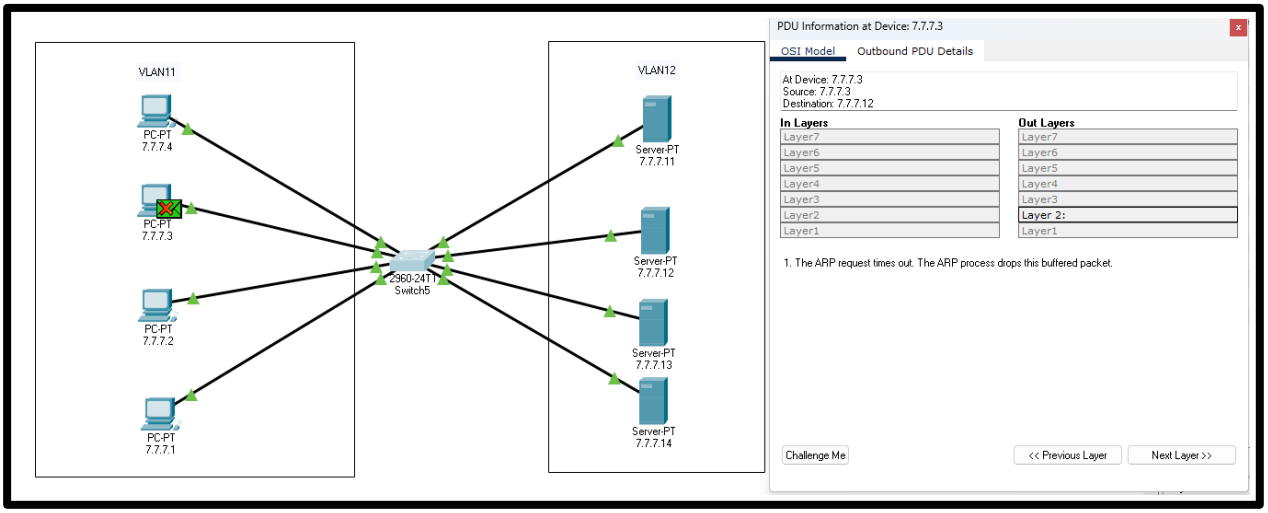
Date: 8/22/2025

3. PDU screenshot between two VLANs.

Successful



Failed



Date: 8/22/2025

4. Mention IP address of each pc as label.

For VLAN11 (PCs):

1. PC1 → 7.7.7.1
2. PC2 → 7.7.7.2
3. PC3 → 7.7.7.3
4. PC4 → 7.7.7.4

For VLAN12 (Servers):

1. Server1 → 7.7.7.11
2. Server2 → 7.7.7.12
3. Server3 → 7.7.7.13
4. Server4 → 7.7.7.14

Date: 8/29/2025

Practical Assignment #06:

Server-Client Socket Programming

Write a C/Java code for TCP Server-Client Socket Programming.

Write a C/Java code for UDP Server-Client Socket Programming.

1.For TCP Server-Client:

TCP Server Program:

```
// Demonstrating Server-side Programming
import java.net.*;
import java.io.*;

public class Server {

   // Initialize socket and input stream
   private Socket s = null;
   private ServerSocket ss = null;
   private DataInputStream in = null;

   // Constructor with port
   public Server(int port) {

      // Starts server and waits for a connection
      try {
         ss = new ServerSocket(port);
         System.out.println("Server started");

         System.out.println("Waiting for a client ...");

         s = ss.accept();
         System.out.println("Client  accepted");

         // Takes input from the client socket
         in = new DataInputStream(
               new BufferedInputStream(s.getInputStream()));

         String m = "";

         // Reads message from client until "Over" is sent
         while (!m.equals("Over")) {
            try {
               m = in.readUTF();
               System.out.println(m);
```

```
            } catch (IOException i) {
                System.out.println(i);
            }
        }
        System.out.println("Closing  connection");

        // Close connection
        s.close();
        in.close();
    } catch (IOException i) {
        System.out.println(i);
    }
  }

  public static void main(String args[]) {
    Server s = new Server(7777);
  }
}
```

TCP Client Program:

```
// Demonstrating Client-side Programming
import java.io.*;
import java.net.*;

public class Client {

  // Initialize socket and input/output streams
  private Socket s = null;
  private DataInputStream in = null;
  private DataOutputStream out = null;

  // Constructor to put IP address and port
  public Client(String addr, int port) {
    // Establish a connection
    try {
      s = new Socket(addr, port);
      System.out.println("Connected");

      // Takes input from terminal
      in = new DataInputStream(System.in);

      // Sends output to the socket
      out = new DataOutputStream(s.getOutputStream());
    } catch (UnknownHostException u) {
      System.out.println(u);
      return;
    } catch (IOException i) {
```

Date: 8/29/2025

```
            System.out.println(i);
            return;
        }

        // String to read message from input
        String m = "";

        // Keep reading until "Over" is input
        while (!m.equals("Over")) {
            try {
                m = in.readLine();
                out.writeUTF(m);
            } catch (IOException i) {
                System.out.println(i);
            }
        }

        // Close the connection
        try {
            in.close();
            out.close();
            s.close();
        } catch (IOException i) {
            System.out.println(i);
        }
    }

    public static void main(String[] args) {
        Client c = new Client("127.0.0.1", 7777);
    }
}
```

2.For UDP Server-Client:

UDP Server Program:

```
// Java program to illustrate Server side
// Implementation using DatagramSocket
import java.io.IOException;
import java.net.DatagramPacket;
import java.net.DatagramSocket;

public class Server
```

Date: 8/29/2025

```
{
   public static void main(String[] args) throws IOException
   {
      // Step 1 : Create a socket to listen at port 7777
      DatagramSocket ds = new DatagramSocket(7777);
      byte[] receive = new byte[65535];

      DatagramPacket DpReceive = null;
      while (true)
      {

         // Step 2 : create a DatgramPacket to receive the data.
         DpReceive = new DatagramPacket(receive, receive.length);

         // Step 3 : revieve the data in byte buffer.
         ds.receive(DpReceive);

         System.out.println("Client:-" + data(receive));

         // Exit the server if the client sends "bye"
         if (data(receive).toString().equals("Over"))
         {
            System.out.println("Client sent bye..... EXITING");
            break;
         }

         // Clear the buffer after every message.
         receive = new byte[65535];
      }
   }

   // A utility method to convert the byte array
   // data into a string representation.
   public static StringBuilder data(byte[] a)
   {
      if (a == null)
         return null;
      StringBuilder ret = new StringBuilder();
      int i = 0;
      while (a[i] != 0)
      {
         ret.append((char) a[i]);
         i++;
      }
      return ret;
   }
}
```

Date: 8/29/2025

UDP Client Program:

```
// Java program to illustrate Client side
// Implementation using DatagramSocket
import java.io.IOException;
import java.net.DatagramPacket;
import java.net.DatagramSocket;
import java.net.InetAddress;
import java.util.Scanner;

public class Client
{
   public static void main(String args[]) throws IOException
   {
      Scanner sc = new Scanner(System.in);

      // Step 1:Create the socket object for
      // carrying the data.
      DatagramSocket ds = new DatagramSocket();

      InetAddress ip = InetAddress.getLocalHost();
      byte buf[] = null;

      // loop while user not enters "bye"
      while (true)
      {
         String inp = sc.nextLine();

         // convert the String input into the byte array.
         buf = inp.getBytes();

         // Step 2 : Create the datagramPacket for sending
         // the data.
         DatagramPacket DpSend =
               new DatagramPacket(buf, buf.length,ip, 7777);

         // Step 3 : invoke the send call to actually send
         // the data.
         ds.send(DpSend);

         // break the loop if user enters "bye"
         if (inp.equals("Over"))
            break;
      }
   }
}
```

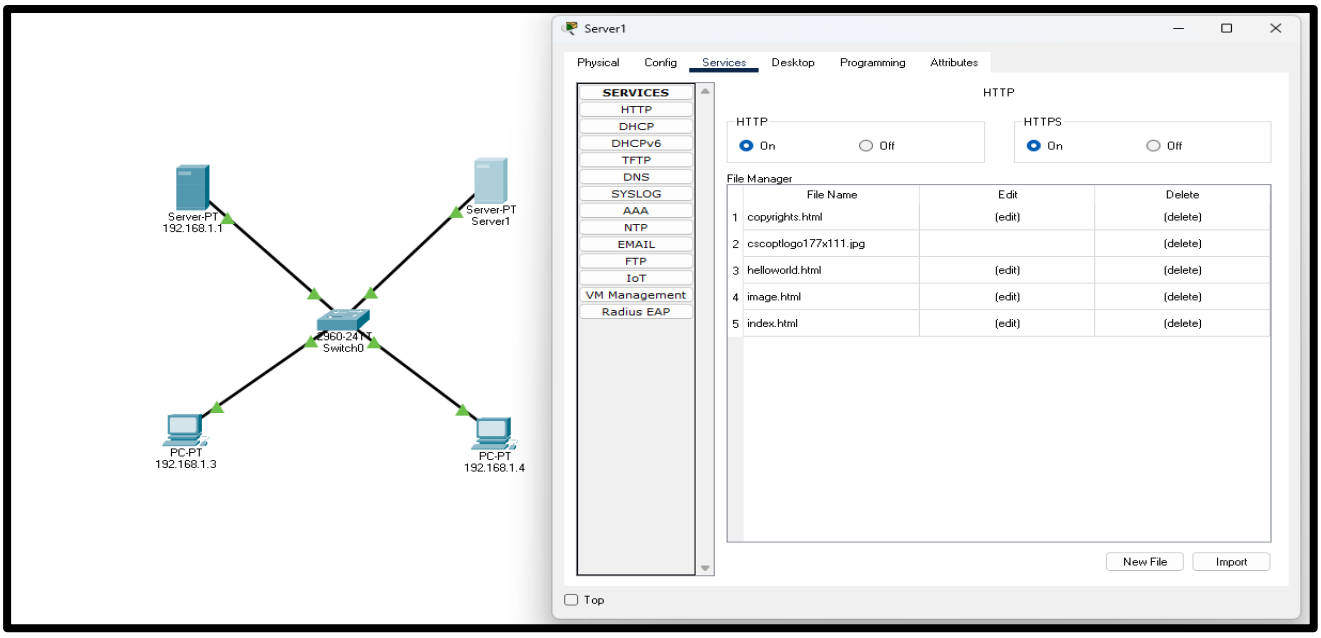
Date: 8/29/2025

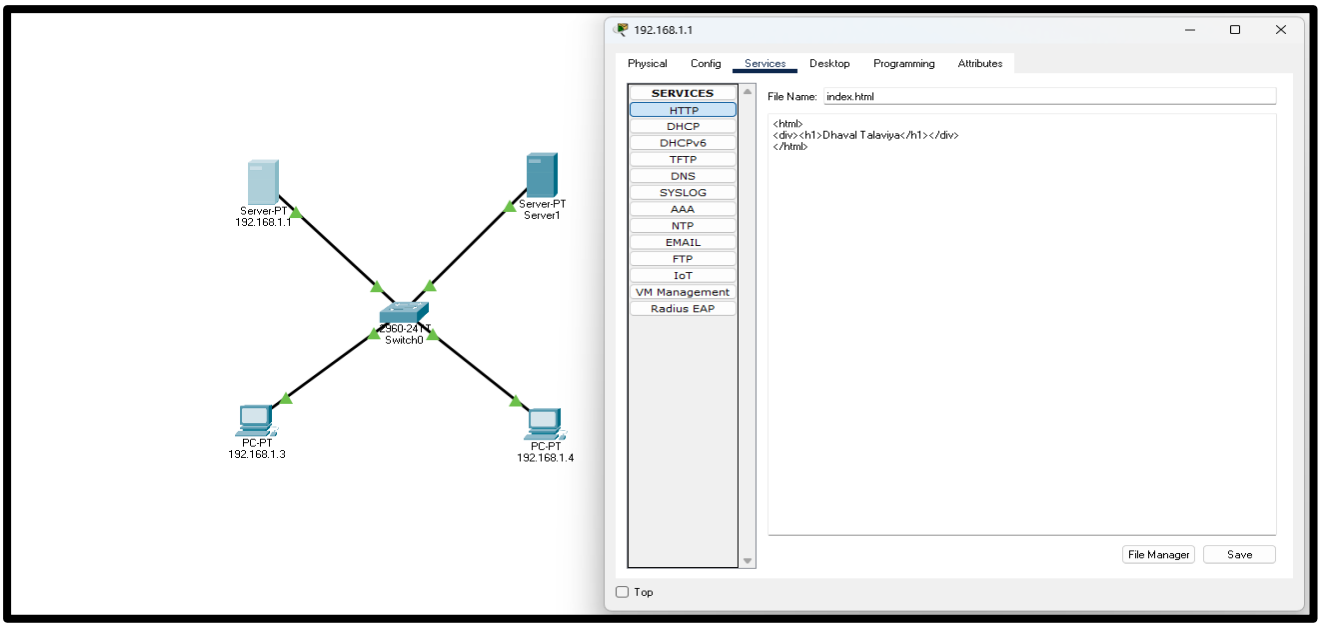
Practical Assignment #07:

Study the application layer protocol DNS, DHCP, FTP.

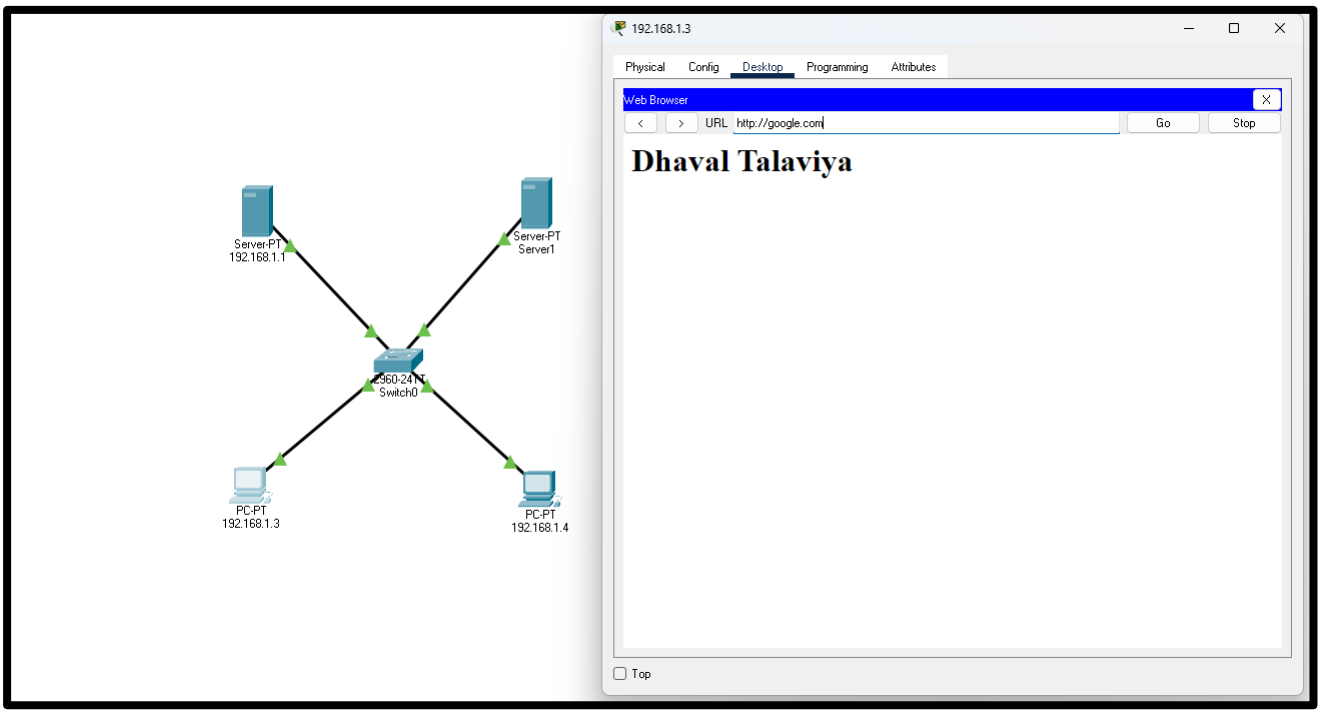
1.Implement the application layer protocol DNS, DHCP, and FTP. Also check connectivity between them using ping command or PDU utility.

a. DNS :

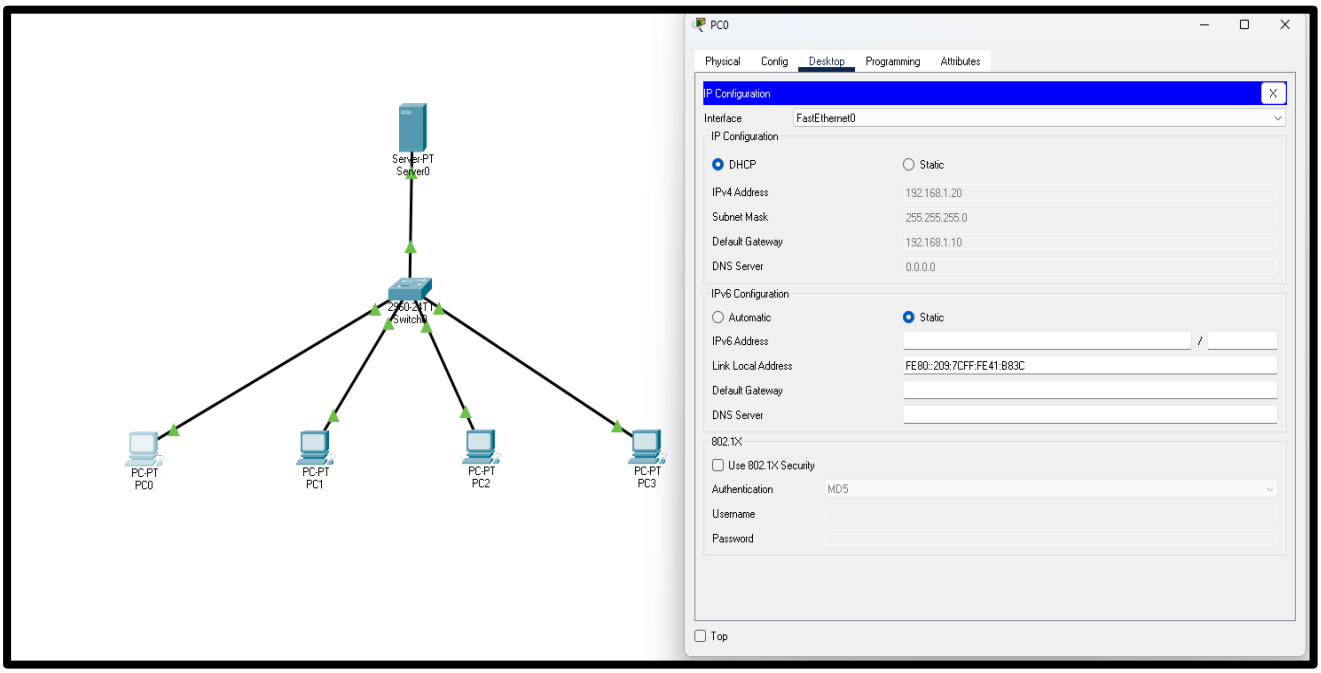




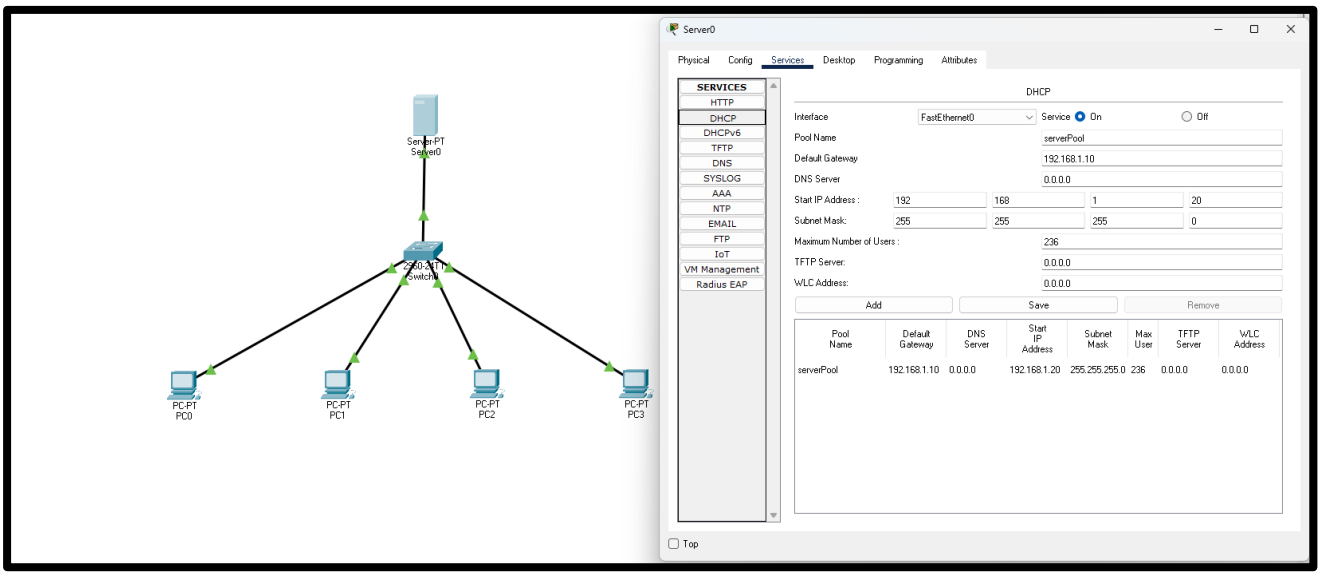
Date: 8/29/2025

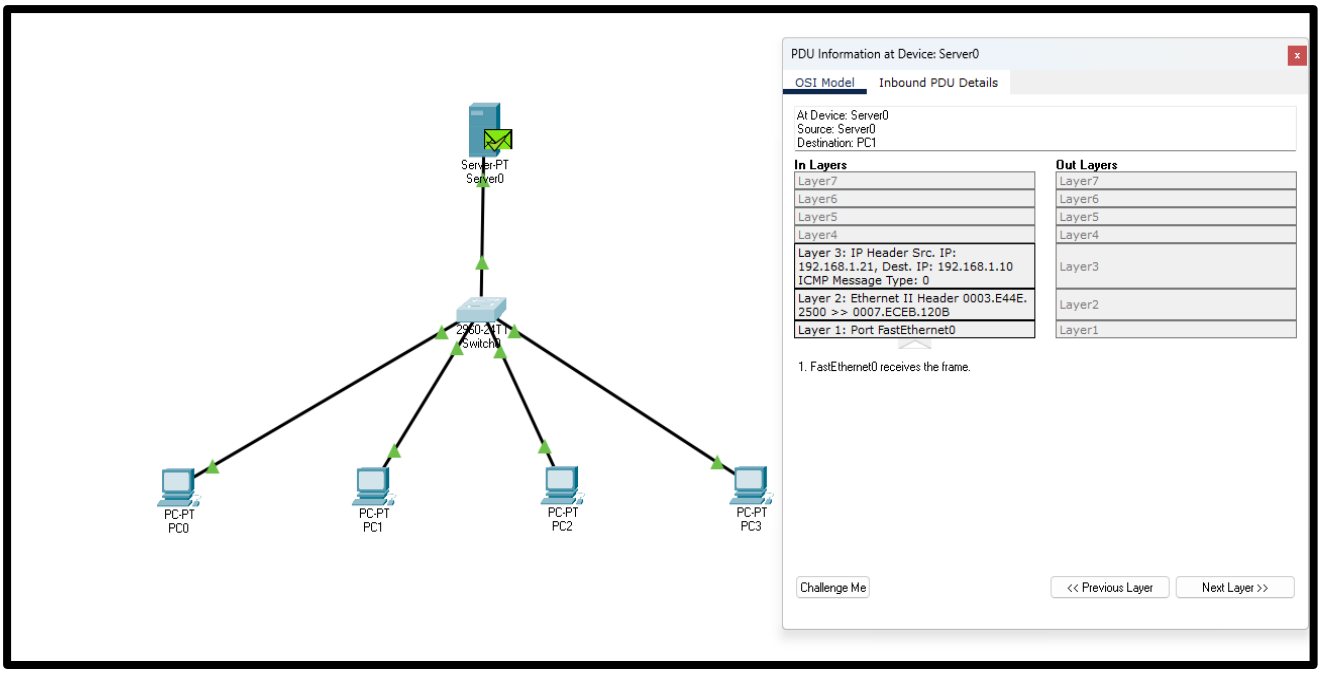


b. DHCP :



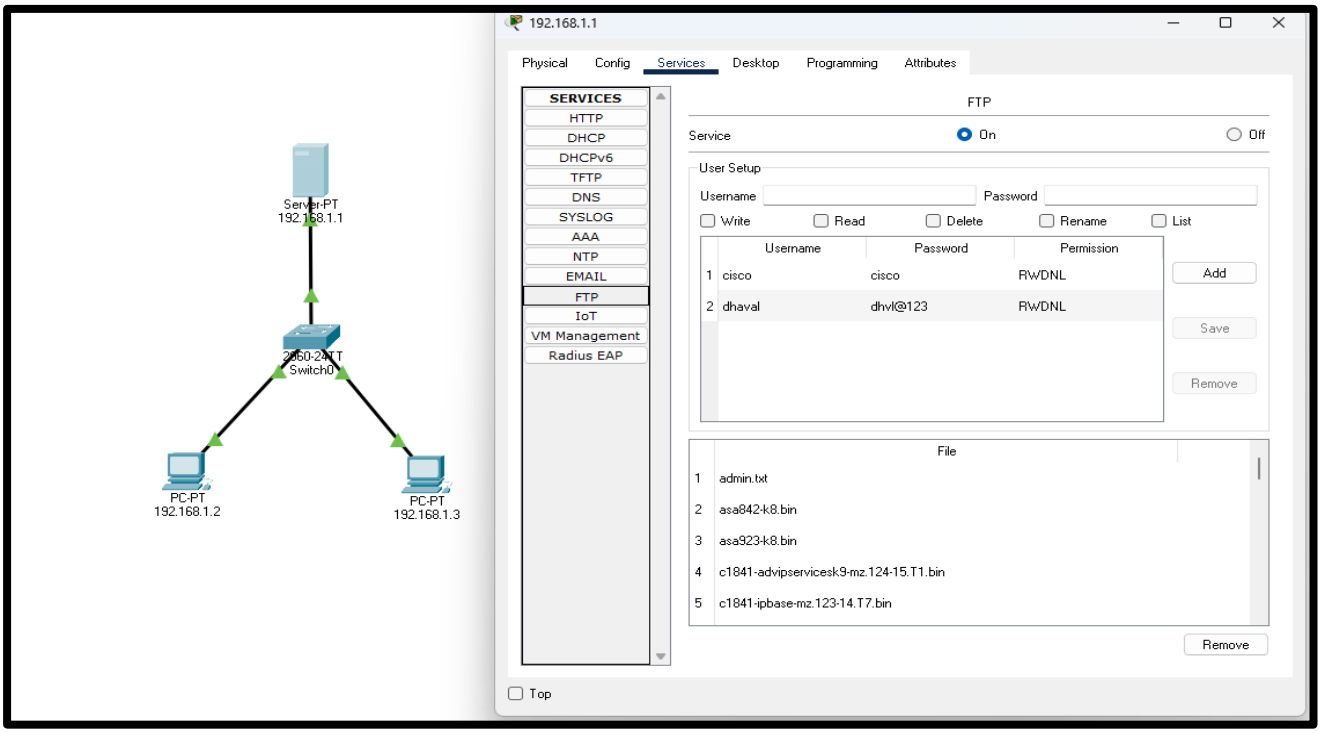
Date: 8/29/2025

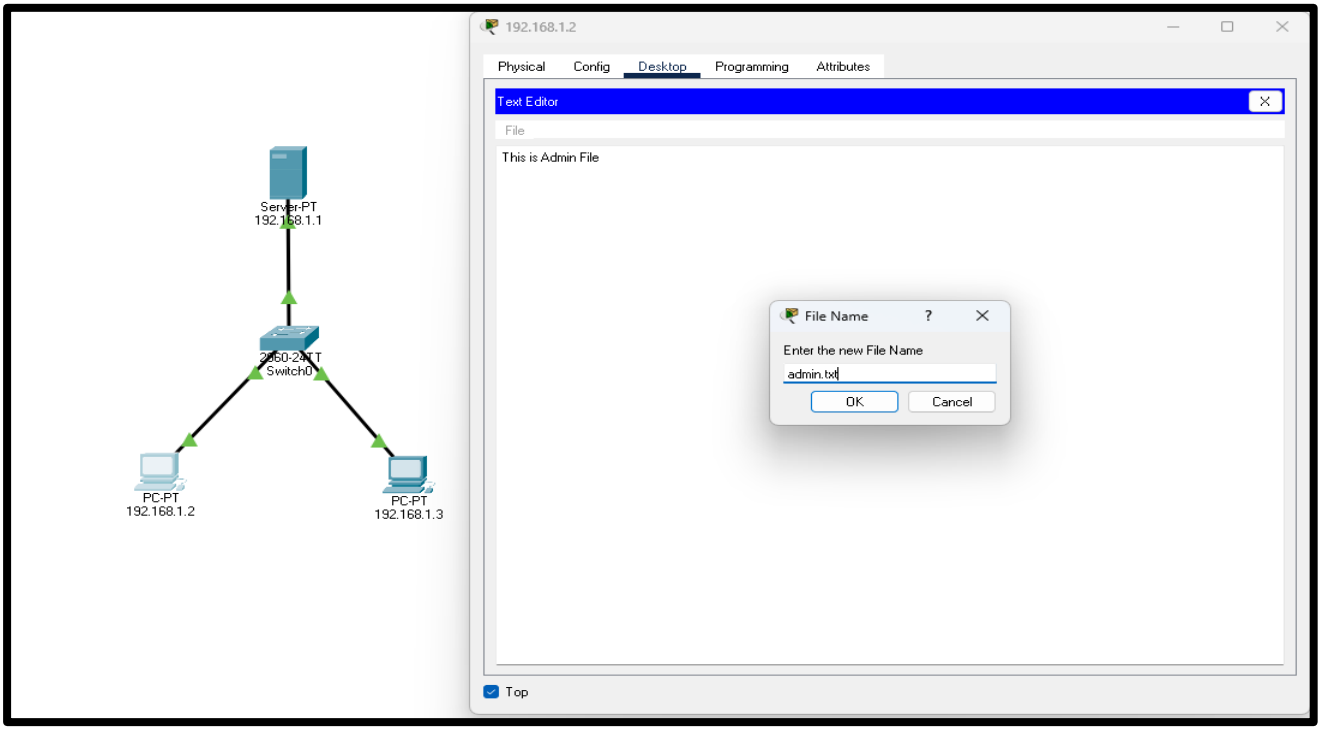




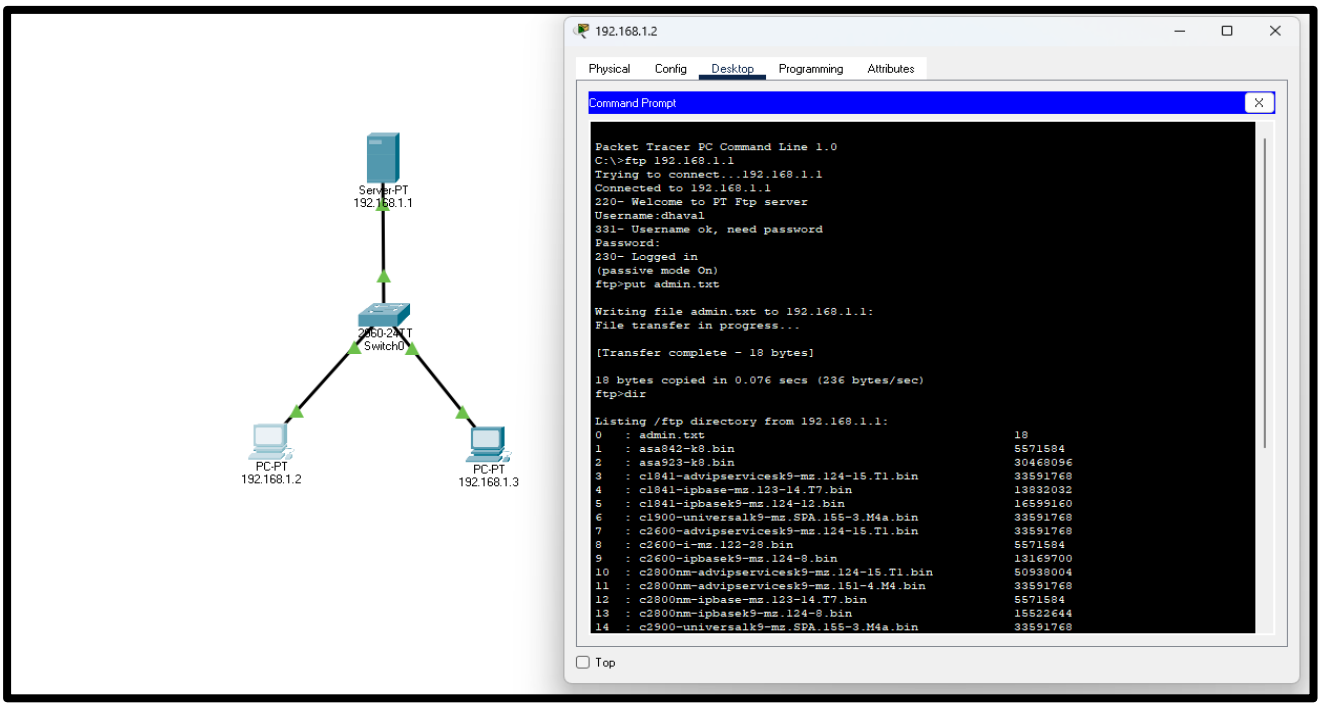
Date: 8/29/2025

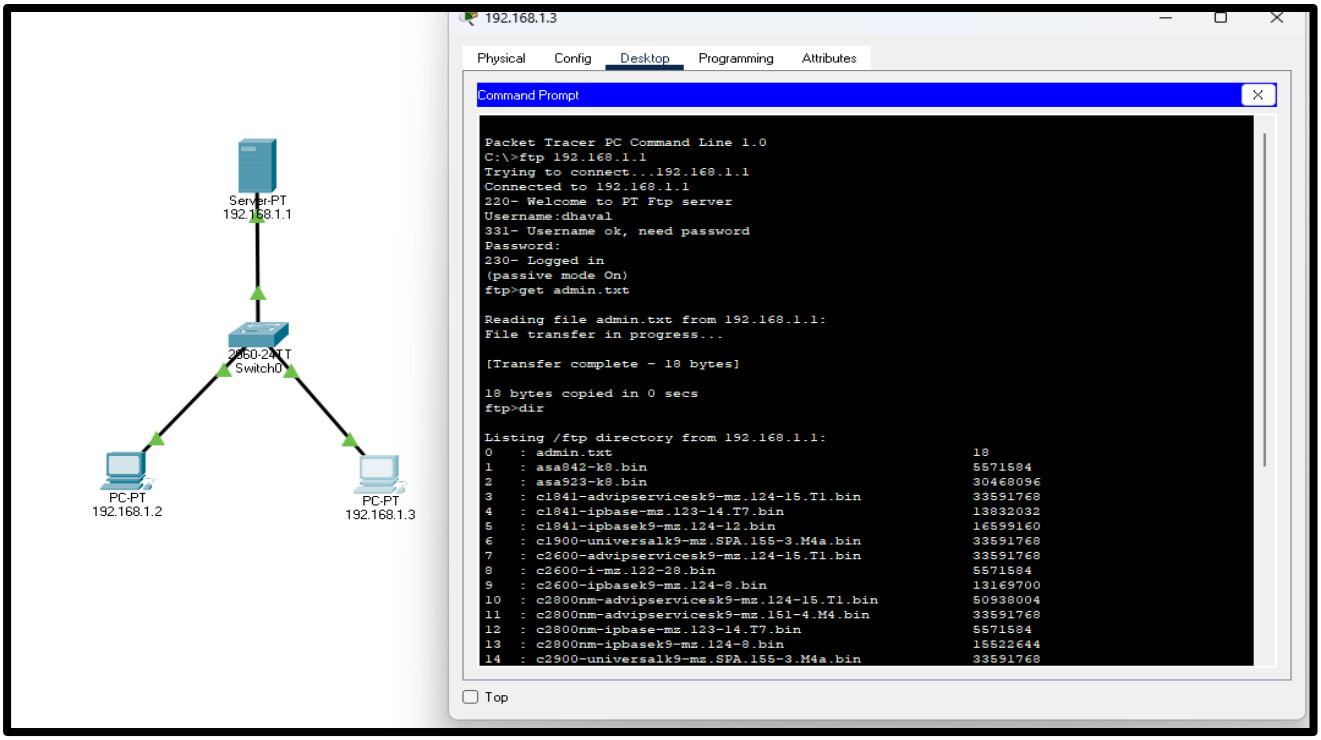
c. FTP :





Date: 8/29/2025





Date: 9/3/2025

Lab Practical #8:

Study & Survey of Institute organization network infrastructure.

Practical Assignment #8:

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

Type of Network in Institute:

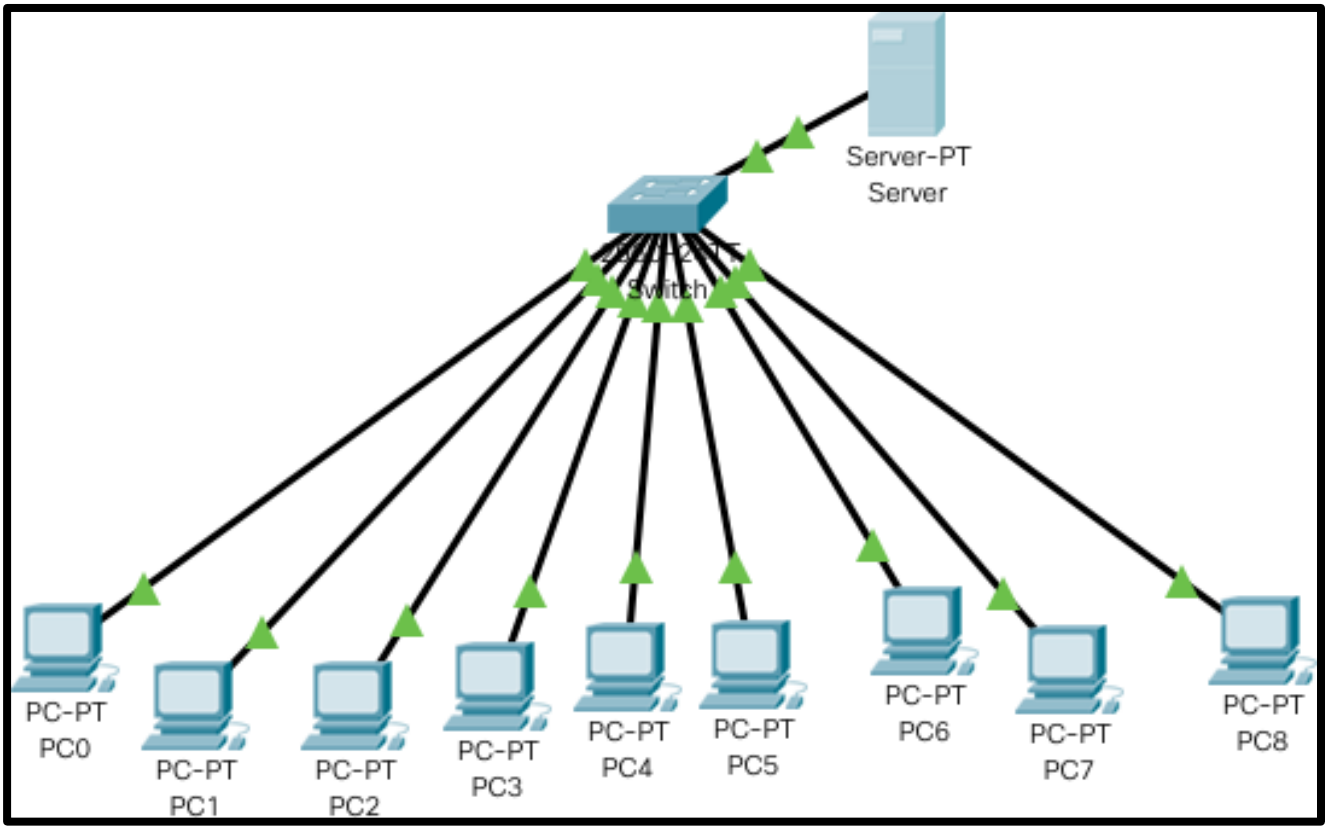
The institute's internal network is a **Local Area Network (LAN)**, which connects different labs, classrooms, and administrative offices within the campus.

Topology Used: Star Topology

- In this topology, all devices (computers, printers, etc.) are connected to a central networking device such as a **switch**.
- The switch acts as the hub that manages and forwards data to the correct device.

Lab No: C- 302

Topology: Star Topology



Date: 9/3/2025

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

Network Devices:

a. **Router**
- Connects the institute's LAN to the Internet Service Provider (ISP).
- Responsible for forwarding packets between different networks.

b. **Switch**
- A central device to which multiple computers in the lab are connected.
- Provides efficient communication within the local network.

c. **Firewall**
- Ensures secure communication by filtering unwanted traffic and preventing unauthorized access.

d. **Wireless Access Point (AP)**
- Extends network connectivity wirelessly so laptops and mobile devices can join the LAN.

e. **Network Interface Card (NIC)**
- Every computer system has a NIC installed (either integrated or separate) that allows it to connect to the network.

f. **Modem**
- Converts digital signals from the router into signals that can travel over the ISP's medium (fiber/DSL).

g. **Load Balancer**
- Distributes internet and network traffic efficiently across multiple servers, improving performance and reducing downtime.

Types of Cables:

a. **Ethernet Cable (Twisted Pair - Cat5e, Cat6, Cat6a)**
- Used for wired connections between PCs, switches, and routers.
- Supports high data transfer speeds (up to 1–10 Gbps depending on category).

b. **Fiber Optic Cable**
- Used for backbone connections across different buildings/floors.
- Provides very high-speed data transfer with minimal loss.

c. **Coaxial Cable**
- Less commonly used now, but may exist in older parts of the network.
- Provides a shielded medium for carrying electrical signals.

d. **Console Cable (RJ45 to Serial/USB)**
- Used by administrators for configuring routers and switches directly through a computer terminal.

Date: 9/3/2025

Lab Practical #09:

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

Practical Assignment #09:

Explain usage of Wireshark tool.

Wireshark is one of the most popular open-source network protocol analyzers. It captures real-time network traffic and displays it in detail, allowing administrators, developers, and students to study how data flows across the network.

Primary Uses of Wireshark:

1. **Network Troubleshooting**
   - Helps diagnose common network issues such as high latency, dropped packets, or connectivity failures.
   - Can detect misconfigurations in routing or protocol setups.
2. **Protocol Analysis**
   - Provides detailed inspection of how various protocols (e.g., TCP, UDP, ICMP, HTTP, DNS) function.
   - Helps verify whether devices are communicating correctly according to standards.
3. **Security Monitoring**
   - Useful in spotting suspicious or malicious activities (e.g., packet sniffing, man-in-the-middle attacks).
   - Aids in detecting unauthorized access attempts and data leaks.
4. **Performance Measurement**
   - Monitors bandwidth usage and data flow patterns.
   - Identifies bottlenecks affecting network performance.
5. **Application Debugging**
   - Developers can analyze how their applications exchange data with servers.
   - Helps track down bugs in client-server communication.
6. **Educational Purposes**
   - A valuable tool for students and professionals to understand networking protocols and packet structures.

Date: 9/3/2025

Basic Steps to Use Wireshark:

1. **Install Wireshark**
   - Available on Windows, macOS, and Linux platforms.
   - Requires administrative rights for capturing live network data.

2. **Start Capturing Packets**
   - Select the correct interface (Ethernet, Wi-Fi, etc.).
   - Click the Start button to begin recording network traffic.

3. **Apply Filters**
   - Select the correct interface (Ethernet, Wi-Fi, etc.).
   - Click the Start button to begin recording network traffic.

4. **Analyze Packets**
   - Every packet can be viewed in three panes:
     1. Packet List (summary)
     2. Packet Details (protocol hierarchy)
     3. Packet Bytes (raw data view)
   - Information includes IP addresses, ports, flags, and payload.

5. **Save and Export Data**
   - Packet captures can be stored as .pcap files for further analysis or sharing.

6. **Use Built-in Tools**
   - View statistics like **Protocol Hierarchy**, **Conversations**, and **I/O Graphs**.
   - Use **Follow TCP Stream** to see the entire conversation between two endpoints.

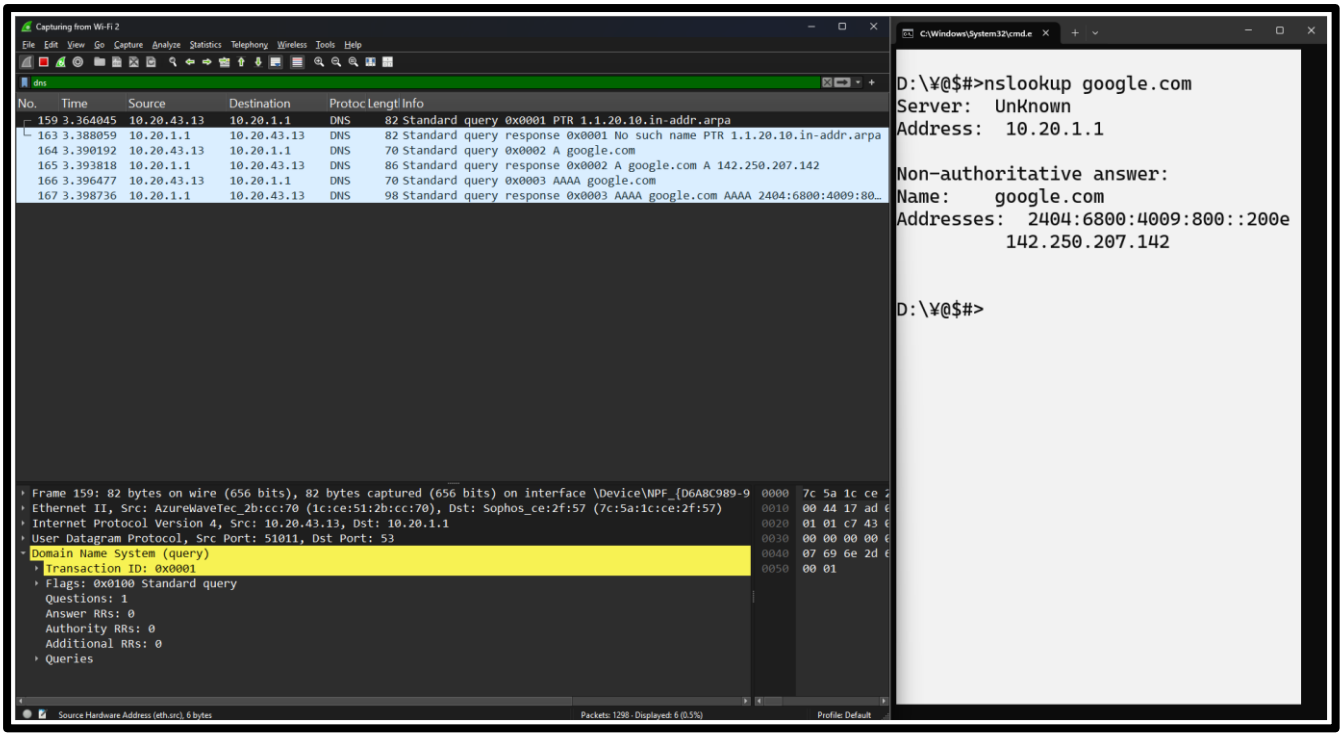
Example Use Case:
Suppose a website is loading unusually slowly:

1. Start capturing traffic while accessing the website.
2. Apply a filter such as http to focus on web requests.
3. Look for delays in TCP handshakes or slow response times from the server.
4. Examine headers and response codes to find possible misconfigurations.

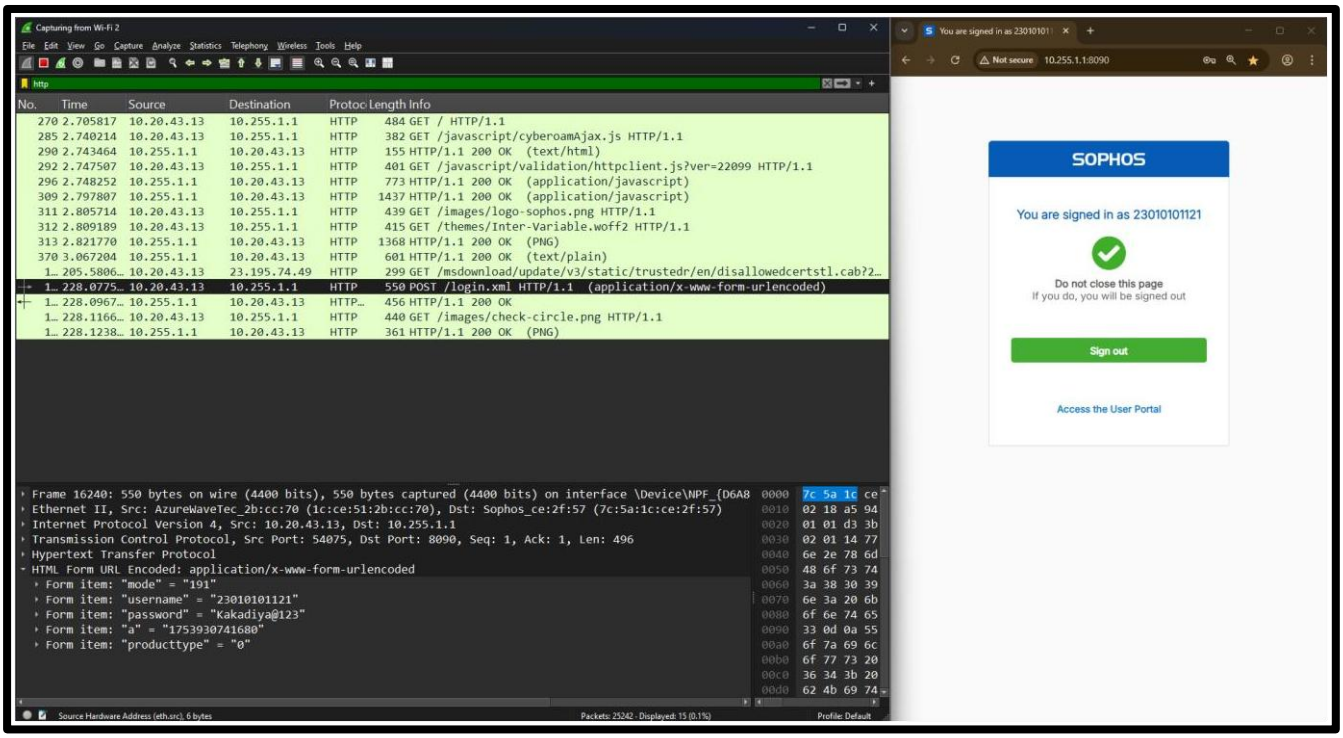
Date: 9/3/2025

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

1. DNS :

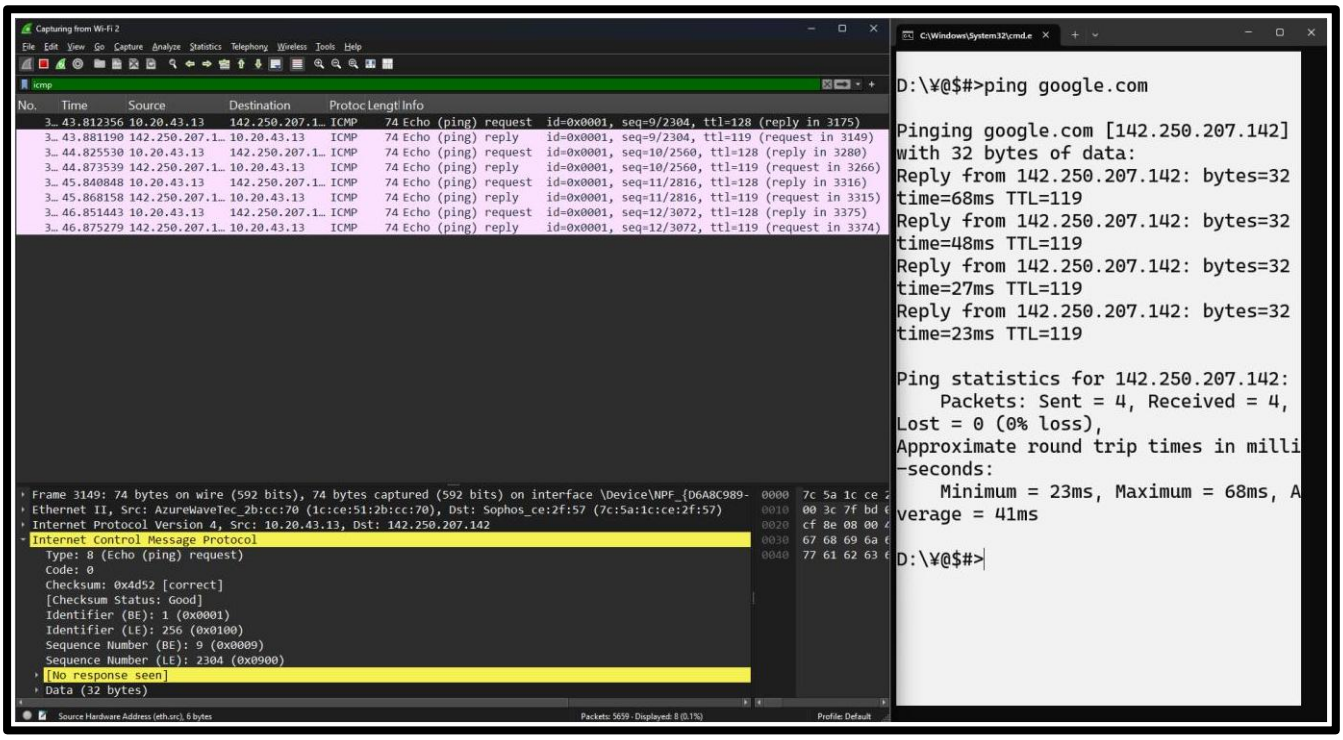


2. HTTP :

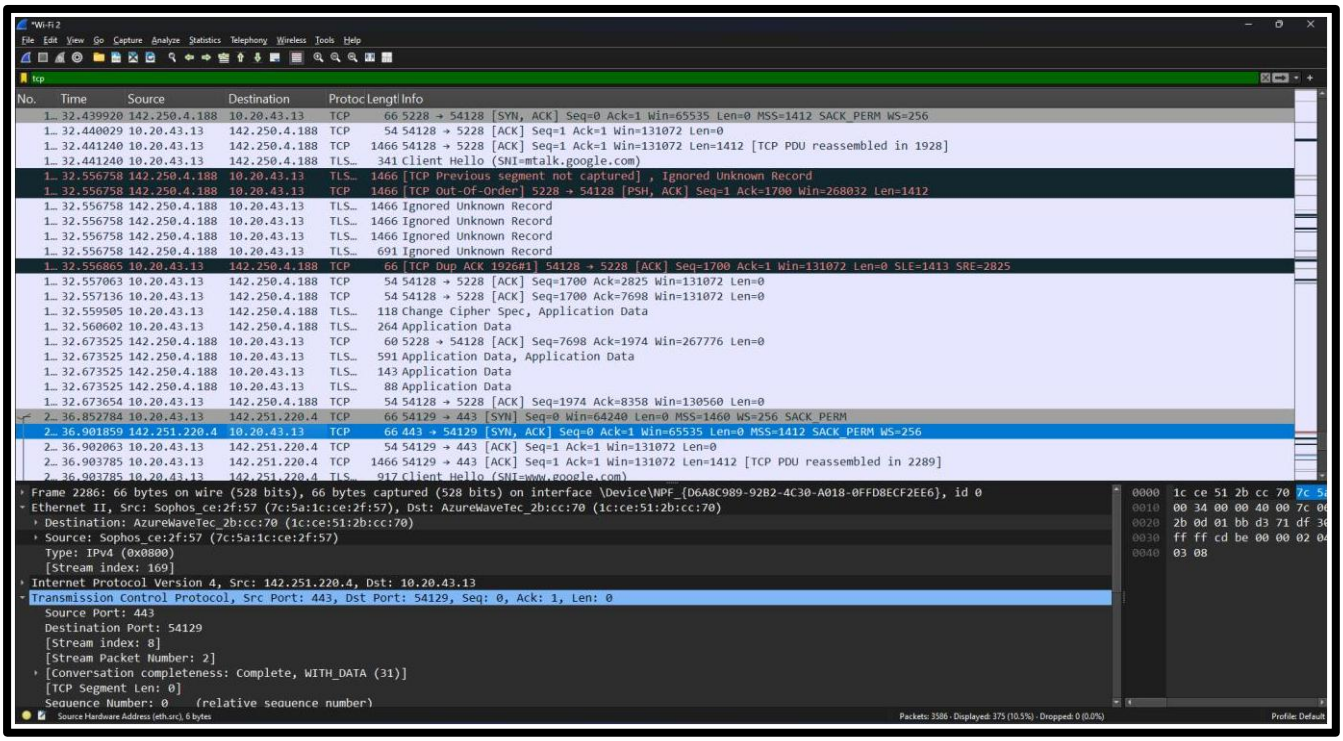


Date: 9/3/2025

3. ICMP :



4. TCP :



Date: 9/3/2025

5. UDP :