Date: 12/06/2024

Himanshu Parmar
22010101132

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:

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

No.	Option	Description
1	ipconfig /all	Display full configuration information.
2	Ipconfig /release	Release the IPv4 address for the specified adapter.
3	Ipconfig /displaydns	Display the contents of the DNS Resolver Cache.
4	ipconfig /allcompartments	Show information about all compartments
5	Ipconfig /renew6	It Is Use For Renew The Ipv6 Address For The Specified Adapter.

Date: 12/06/2024

Implementation:

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-2KTO83LV
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : FA-54-F6-1B-29-25
   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. . . . . . . . . : FA-54-F6-1B-29-35
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Physical Address. . . . . . . . . : F8-54-F6-1B-29-05
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2405:204:8580:c500:3929:4d05:4d52:c24f(Preferred)
   Temporary IPv6 Address. . . . . . : 2405:204:8580:c500:b133:9743:f7c2:1bdc(Preferred)
   Link-local IPv6 Address . . . . . : fe80::9b2c:568b:4a09:c795%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.139(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 16 June 2024 11:03:22
   Lease Expires . . . . . . . . . . : 16 June 2024 12:03:21
   Default Gateway . . . . . . . . . : fe80::4486:7bff:fe1f:ced5%15
                                       192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . . : 184046838
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-C4-32-CE-F8-54-F6-1B-29-05
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>Ipconfig /release

Windows IP Configuration

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.

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. . . . . . . . . . . : 2405:204:8580:c500:3929:4d05:4d52:c24f
   Temporary IPv6 Address. . . . . . : 2405:204:8580:c500:b133:9743:f7c2:1bdc
   Link-local IPv6 Address . . . . . : fe80::9b2c:568b:4a09:c795%15
   Default Gateway . . . . . . . . . : fe80::4486:7bff:fe1f:ced5%15
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>Ipconfig /displaydns

Windows IP Configuration

    ecs.office.com
    ----------------------------------------
    Record Name . . . . . : ecs.office.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 44
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : ecs.office.trafficmanager.net


    Record Name . . . . . : ecs.office.trafficmanager.net
    Record Type . . . . . : 5
    Time To Live  . . . . : 44
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : s-0005-office.config.skype.com


    Record Name . . . . . : s-0005-office.config.skype.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 44
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : ecs-office.s-0005.s-msedge.net


    Record Name . . . . . : ecs-office.s-0005.s-msedge.net
    Record Type . . . . . : 5
    Time To Live  . . . . : 44
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : s-0005.s-msedge.net


    Record Name . . . . . : s-0005.s-msedge.net
    Record Type . . . . . : 28
    Time To Live  . . . . : 44
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2620:1ec:42::132
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>ipconfig /allcompartments

Windows IP Configuration


================================================================================
Network Information for Compartment 1 (ACTIVE)
================================================================================

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. . . . . . . . . . . : 2405:204:8580:c500:3929:4d05:4d52:c24f
   Temporary IPv6 Address. . . . . . : 2405:204:8580:c500:b133:9743:f7c2:1bdc
   Link-local IPv6 Address . . . . . : fe80::9b2c:568b:4a09:c795%15
   IPv4 Address. . . . . . . . . . . : 192.168.43.139
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::4486:7bff:fe1f:ced5%15
                                       192.168.43.1
```

```
C:\Users\HIMANSHU>Ipconfig /renew6

Windows IP Configuration

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.
```

Date: 12/06/2024

2. ping

Description:

The `ping` command is a utility used to test the reachability of a host on an IP network and to measure the round-trip time for messages sent from the originating host to a destination computer. It's commonly used for network diagnostics and troubleshooting.

No.	Option	Description
1	Ping -t google.com	Ping the specified host until stopped.
2	Ping -a google.com	Resolve addresses to hostnames.
3	ping -n count google.com	Number of echo requests to send.
4	Ping -l 16 google.com	Send buffer size.
5	Ping -r 6 google.com	Record route for count hops

Implementation:

```
C:\Users\HIMANSHU>ping google.com

Pinging google.com [2404:6800:4009:803::200e] with 32 bytes of data:
Reply from 2404:6800:4009:803::200e: time=99ms
Reply from 2404:6800:4009:803::200e: time=73ms
Reply from 2404:6800:4009:803::200e: time=66ms
Reply from 2404:6800:4009:803::200e: time=70ms

Ping statistics for 2404:6800:4009:803::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 66ms, Maximum = 99ms, Average = 77ms
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>Ping -t google.com

Pinging google.com [2404:6800:4009:803::200e] with 32 bytes of data:
Reply from 2404:6800:4009:803::200e: time=45ms
Reply from 2404:6800:4009:803::200e: time=75ms
Reply from 2404:6800:4009:803::200e: time=62ms
Reply from 2404:6800:4009:803::200e: time=70ms
Reply from 2404:6800:4009:803::200e: time=64ms
Reply from 2404:6800:4009:803::200e: time=61ms
Reply from 2404:6800:4009:803::200e: time=70ms
Reply from 2404:6800:4009:803::200e: time=82ms

Ping statistics for 2404:6800:4009:803::200e:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 82ms, Average = 66ms
Control-C
```

```
C:\Users\HIMANSHU>Ping -a google.com

Pinging google.com [2404:6800:4009:803::200e] with 32 bytes of data:
Reply from 2404:6800:4009:803::200e: time=69ms
Reply from 2404:6800:4009:803::200e: time=81ms
Reply from 2404:6800:4009:803::200e: time=73ms
Reply from 2404:6800:4009:803::200e: time=66ms

Ping statistics for 2404:6800:4009:803::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 66ms, Maximum = 81ms, Average = 72ms
```

```
C:\Users\HIMANSHU>ping -n 8 google.com

Pinging google.com [2404:6800:4009:803::200e] with 32 bytes of data:
Reply from 2404:6800:4009:803::200e: time=103ms
Reply from 2404:6800:4009:803::200e: time=70ms
Reply from 2404:6800:4009:803::200e: time=73ms
Reply from 2404:6800:4009:803::200e: time=63ms
Reply from 2404:6800:4009:803::200e: time=75ms
Reply from 2404:6800:4009:803::200e: time=77ms
Reply from 2404:6800:4009:803::200e: time=73ms
Reply from 2404:6800:4009:803::200e: time=80ms

Ping statistics for 2404:6800:4009:803::200e:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 103ms, Average = 76ms
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>Ping -l 16 google.com

Pinging google.com [2404:6800:4009:803::200e] with 16 bytes of data:
Reply from 2404:6800:4009:803::200e: time=63ms
Reply from 2404:6800:4009:803::200e: time=75ms
Reply from 2404:6800:4009:803::200e: time=65ms
Reply from 2404:6800:4009:803::200e: time=76ms

Ping statistics for 2404:6800:4009:803::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 76ms, Average = 69ms
```

```
C:\Users\HIMANSHU>Ping -r 6 google.com

Pinging google.com [142.250.70.78] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 142.250.70.78:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Date: 12/06/2024

3. getmac

Description:

The getmac command is used in Windows operating systems to display the Media Access Control (MAC) addresses of network interfaces. It provides information about the MAC addresses for all network adapters, including both physical and virtual network interfaces, and is useful for network troubleshooting and configuration tasks. The command can be run in the Command Prompt and also supports various options for customizing the output.

No.	Option	Description
1	getmac	This tool enables an administrator to display the MAC address network adapters on a system.
2	getmac /v	Specifies that verbose output is displayed.
3	getmac /nh	Specifies that the "Column Header" should not be displayed in the output. Valid only for TABLE and CSV formats.
4	getmac /fo Format	Specifies the format in which the output is to be displayed. values: "TABLE", "LIST", "CSV".
5	getmac /?	Displays This Help Message and Option.

Implementation:

```
C:\Users\HIMANSHU>getmac

Physical Address    Transport Name
=================== ============================================================
F8-54-F6-1B-29-05   \Device\Tcpip_{95F0D6CA-2668-4E34-96B8-BAC5822C9C5E}
```

```
C:\Users\HIMANSHU>getmac

Physical Address    Transport Name
=================== ============================================================
F8-54-F6-1B-29-05   \Device\Tcpip_{95F0D6CA-2668-4E34-96B8-BAC5822C9C5E}

C:\Users\HIMANSHU>getmac /v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== =================== ============================================================
Wi-Fi           MediaTek Wi-Fi  F8-54-F6-1B-29-05   \Device\Tcpip_{95F0D6CA-2668-4E34-96B8-BAC5822C9C5E}
```

```
C:\Users\HIMANSHU>getmac /nh

F8-54-F6-1B-29-05   \Device\Tcpip_{95F0D6CA-2668-4E34-96B8-BAC5822C9C5E}
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>getmac /fo csv
"Physical Address","Transport Name"
"F8-54-F6-1B-29-05","\Device\Tcpip_{95F0D6CA-2668-4E34-96B8-BAC5822C9C5E}"
```

```
C:\Users\HIMANSHU>getmac /?

GETMAC [/S system [/U username [/P [password]]]] [/FO format] [/NH] [/V]

Description:
    This tool enables an administrator to display the MAC address
    for network adapters on a system.

Parameter List:
    /S      system          Specifies the remote system to connect to.

    /U      [domain\]user   Specifies the user context under
                            which the command should execute.

    /P      [password]      Specifies the password for the given
                            user context. Prompts for input if omitted.

    /FO     format          Specifies the format in which the output
                            is to be displayed.
                            Valid values: "TABLE", "LIST", "CSV".

    /NH                     Specifies that the "Column Header" should
                            not be displayed in the output.
                            Valid only for TABLE and CSV formats.

    /V                      Specifies that verbose output is displayed.

    /?                      Displays this help message.

Examples:
    GETMAC /?
    GETMAC /FO csv
    GETMAC /S system /NH /V
    GETMAC /S system /U user
    GETMAC /S system /U domain\user /P password /FO list /V
    GETMAC /S system /U domain\user /P password /FO table /NH
```

Date: 12/06/2024

4. systeminfo

Description:

The systeminfo command in Windows is used to display detailed configuration information about a computer and its operating system. It provides data such as the OS version, system manufacturer, processor type, BIOS version, memory, network adapter details, and more. This command is useful for diagnosing system issues, performing audits, and gathering information for support purposes.

No.	Option	Description
1	systeminfo	This tool displays operating system configuration information for a local or remote machine, including service pack levels.
2	systeminfo /nh	Specifies that the "Column Header" should not be displayed in the output. Valid only for TABLE and CSV formats.
3	systeminfo /fo "TABLE", "LIST", "CSV"	Specifies the format in which the output is to be displayed. values: "TABLE", "LIST", "CSV".
4	Systeminfo /?	Displays This Help Message and Option.

Date: 12/06/2024

Implementation:

```
C:\Users\HIMANSHU>systeminfo

Host Name:                 LAPTOP-2KTO83LV
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22631 N/A Build 22631
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          HIMANSHU
Registered Organization:   N/A
Product ID:                00342-42650-86791-AAOEM
Original Install Date:     07-11-2023, 08:41:25
System Boot Time:          13-06-2024, 12:14:34
System Manufacturer:       ASUSTeK COMPUTER INC.
System Model:              VivoBook_ASUSLaptop M1603QA_M1603QA
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~1908 Mhz
BIOS Version:              American Megatrends International, LLC. M1603QA.308, 22-05-2023
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:     15,773 MB
Available Physical Memory: 8,583 MB
Virtual Memory: Max Size:  16,797 MB
Virtual Memory: Available: 8,008 MB
Virtual Memory: In Use:    8,789 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-2KTO83LV
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5037591
                           [02]: KB5012170
                           [03]: KB5027397
                           [04]: KB5039212
                           [05]: KB5037959
Network Card(s):           1 NIC(s) Installed.
                           [01]: MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.43.1
                                 IP address(es)
                                 [01]: 192.168.43.139
                                 [02]: fe80::9b2c:568b:4a09:c795
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>systeminfo /fo csv
"Host Name","OS Name","OS Version","OS Manufacturer","OS Configuration","OS Build Type","Registered Owner","Registered Organization","Product ID","Original
Install Date","System Boot Time","System Manufacturer","System Model","System Type","Processor(s)","BIOS Version","Windows Directory","System Directory","Bo
ot Device","System Locale","Input Locale","Time Zone","Total Physical Memory","Available Physical Memory","Virtual Memory: Max Size","Virtual Memory: Availa
ble","Virtual Memory: In Use","Page File Location(s)","Domain","Logon Server","Hotfix(s)","Network Card(s)","Hyper-V Requirements"
"LAPTOP-2KTO83LV","Microsoft Windows 11 Home Single Language","10.0.22631 N/A Build 22631","Microsoft Corporation","Standalone Workstation","Multiprocessor
Free","HIMANSHU","N/A","00342-42650-86791-AAOEM","07-11-2023, 08:41:25","13-06-2024, 12:14:34","ASUSTeK COMPUTER INC.","VivoBook_ASUSLaptop M1603QA_M1603QA"
,"x64-based PC","1 Processor(s) Installed.,[01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~1908 Mhz","American Megatrends International, LLC. M1603Q
A.308, 22-05-2023","C:\Windows","C:\Windows\system32","\Device\HarddiskVolume1","en-us;English (United States)","00004009","(UTC+05:30) Chennai, Kolkata, Mu
mbai, New Delhi","15,773 MB","8,724 MB","16,797 MB","8,122 MB","8,675 MB","C:\pagefile.sys","WORKGROUP","\\LAPTOP-2KTO83LV","5 Hotfix(s) Installed.,[01]: KB
5037591,[02]: KB5012170,[03]: KB5027397,[04]: KB5039212,[05]: KB5037959","1 NIC(s) Installed.,[01]: MediaTek Wi-Fi 6 MT7921 Wireless LAN Card,      Connecti
on Name: Wi-Fi,      DHCP Enabled:    Yes,      DHCP Server:     192.168.43.1,      IP address(es),      [01]: 192.168.43.139,      [02]: fe80::9b2c:568b:4a
09:c795,      [03]: 2405:204:8580:c500:b133:9743:f7c2:1bdc,      [04]: 2405:204:8580:c500:3929:4d05:4d52:c24f","A hypervisor has been detected. Features req
uired for Hyper-V will not be displayed."
```

```
C:\Users\HIMANSHU>Systeminfo /?

SYSTEMINFO [/S system [/U username [/P [password]]]] [/FO format] [/NH]

Description:
    This tool displays operating system configuration information for
    a local or remote machine, including service pack levels.

Parameter List:
    /S      system          Specifies the remote system to connect to.

    /U      [domain\]user   Specifies the user context under which
                            the command should execute.

    /P      [password]      Specifies the password for the given
                            user context. Prompts for input if omitted.

    /FO     format          Specifies the format in which the output
                            is to be displayed.
                            Valid values: "TABLE", "LIST", "CSV".

    /NH                     Specifies that the "Column Header" should
                            not be displayed in the output.
                            Valid only for "TABLE" and "CSV" formats.

    /?                      Displays this help message.

Examples:
    SYSTEMINFO
    SYSTEMINFO /?
    SYSTEMINFO /S system
    SYSTEMINFO /S system /U user
    SYSTEMINFO /S system /U domain\user /P password /FO TABLE
    SYSTEMINFO /S system /FO LIST
    SYSTEMINFO /S system /FO CSV /NH
```

Date: 12/06/2024

5. traceroute / tracert

Description:

The traveroute (or tracert on Windows) command is a network diagnostic tool used to track the path packets take from a source to a destination. It identifies each hop along the route and measures the transit delays of packets across the network. This helps in pinpointing network congestion or failures.

No.	Option	Description
1	Tracert -d	Do not resolve addresses to hostnames.
2	tracert -4	Force using IPv4.
3	tracert -6	Force using Ipv6.
4	tracert -w timeout	The tracert -w timeout command specifies the time, in milliseconds, to wait for each reply before timing out, allowing users to adjust the sensitivity of the response time for each hop in the trace route.
5	Tracert -h maximum_hops	tracert -h maximum_hops command sets the maximum number of hops (or steps) the traceroute will take in its attempt to reach the destination, allowing users to limit the scope of the trace.

Implementation:

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

Tracing route to google.com [2404:6800:4009:803::200e]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  2405:204:8580:c500::2c
  2     *        *        *     Request timed out.
  3   134 ms    43 ms    73 ms  2405:200:320:1504::2
  4    69 ms    47 ms    45 ms  2405:200:801:b00::a9a
  5    58 ms    39 ms    55 ms  2405:200:801:b00::ab1
  6    60 ms    54 ms    44 ms  2405:200:801:b00::ab0
  7    63 ms    60 ms    54 ms  2405:200:801:200::9b3
  8    67 ms    57 ms    59 ms  2001:4860:1:1::270
  9    76 ms    58 ms    59 ms  2001:4860:0:1::8097
 10    71 ms    61 ms    56 ms  2001:4860:0:1::7b7f
 11    67 ms    63 ms    57 ms  2404:6800:4009:803::200e

Trace complete.
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>tracert -4 google.com

Tracing route to google.com [142.251.42.46]
over a maximum of 30 hops:

  1     3 ms     2 ms     1 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    49 ms    36 ms    38 ms  10.71.48.114
  4   338 ms    42 ms    40 ms  192.168.21.188
  5   115 ms    28 ms    39 ms  172.26.101.5
  6    98 ms    40 ms    57 ms  172.26.100.242
  7    55 ms    37 ms    58 ms  192.168.38.27
  8     *        *        *     Request timed out.
  9   378 ms    58 ms    61 ms  172.26.40.5
 10    61 ms    59 ms    57 ms  172.26.40.5
 11    88 ms    53 ms    58 ms  172.26.40.64
 12   118 ms    57 ms    71 ms  172.26.40.64
 13     *      146 ms    89 ms  49.44.18.38
 14     *        *        *     Request timed out.
 15    51 ms    58 ms    77 ms  72.14.211.138
 16   106 ms    56 ms    60 ms  142.251.225.77
 17    99 ms    59 ms    58 ms  142.251.69.45
 18    57 ms    61 ms    59 ms  bom12s20-in-f14.1e100.net [142.251.42.46]

Trace complete.
```

```
C:\Users\HIMANSHU>tracert -6 google.com

Tracing route to google.com [2404:6800:4009:82c::200e]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  2405:204:8580:c500::2c
  2     *        *        *     Request timed out.
  3    73 ms    45 ms    38 ms  2405:200:320:1504::2
  4    66 ms    48 ms    52 ms  2405:200:801:b00::a9a
  5    69 ms    66 ms    51 ms  2405:200:801:b00::ab7
  6    54 ms    37 ms    59 ms  2405:200:801:b00::ab6
  7    69 ms    52 ms    58 ms  2405:200:801:200::9b5
  8    76 ms    57 ms    60 ms  2405:200:802:760::8
  9    63 ms    60 ms    56 ms  2405:200:802:760::8
 10     *        *        *     Request timed out.
 11     *       67 ms    44 ms  2001:4860:1:1::a14
 12    63 ms    59 ms    57 ms  2404:6800:8015::1
 13    68 ms    58 ms    58 ms  2001:4860:0:1::5ece
 14    61 ms    59 ms    55 ms  2001:4860:0:1::269d
 15    75 ms    72 ms    69 ms  bom07s35-in-x0e.1e100.net [2404:6800:4009:82c::200e]

Trace complete.
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>tracert -w 100 google.com

Tracing route to google.com [2404:6800:4009:82c::200e]
over a maximum of 30 hops:

  1     3 ms     1 ms     3 ms  2405:204:8580:c500::2c
  2     *        *        *     Request timed out.
  3    58 ms    38 ms    39 ms  2405:200:320:1504::2
  4    52 ms    41 ms    59 ms  2405:200:801:b00::a9a
  5    49 ms    61 ms    66 ms  2405:200:801:b00::ab7
  6    48 ms    40 ms     *     2405:200:801:b00::ab6
  7    66 ms    48 ms    56 ms  2405:200:801:200::9b5
  8    69 ms    61 ms    57 ms  2405:200:802:760::8
  9    52 ms    59 ms    57 ms  2405:200:802:760::8
 10     *        *        *     Request timed out.
 11    59 ms    57 ms    58 ms  2001:4860:1:1::a14
 12    62 ms    62 ms    66 ms  2404:6800:8015::1
 13    49 ms    56 ms    61 ms  2001:4860:0:1::5ece
 14    64 ms     *       50 ms  2001:4860:0:1::269d
 15    70 ms    60 ms    58 ms  bom07s35-in-x0e.1e100.net [2404:6800:4009:82c::200e]

Trace complete.
```

```
C:\Users\HIMANSHU>tracert -h 10 google.com

Tracing route to google.com [2404:6800:4009:82c::200e]
over a maximum of 10 hops:

  1     3 ms     2 ms     1 ms  2405:204:8580:c500::2c
  2     *        *        *     Request timed out.
  3   101 ms    36 ms    38 ms  2405:200:320:1504::2
  4    49 ms    38 ms    48 ms  2405:200:801:b00::a9a
  5    67 ms    36 ms    54 ms  2405:200:801:b00::ab7
  6    62 ms    37 ms    56 ms  2405:200:801:b00::ab6
  7    77 ms    53 ms    83 ms  2405:200:801:200::9b5
  8    63 ms    75 ms    75 ms  2405:200:802:760::8
  9    70 ms    58 ms    58 ms  2405:200:802:760::8
 10     *        *        *     Request timed out.

Trace complete.
```

Date: 12/06/2024

6. netstart

Description:

The netstart command is a network utility that displays active network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. It provides detailed information about the network status and is commonly used for troubleshooting and network monitoring. The command works across various operating systems, including Unix, Linux, and Windows.

No.	Option	Description
1	netstart -a	Displays all connections and listening ports.
2	netstart -e	Displays Ethernet statistics.
3	netstart -f	Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
4	netstart -i	Displays the time spent by a TCP connection in its current state.
5	netstart -n	Displays addresses and port numbers in numerical form.

Implementation:

```
C:\Users\HIMANSHU>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:64650        LAPTOP-2KTO83LV:64651  ESTABLISHED
  TCP    127.0.0.1:64651        LAPTOP-2KTO83LV:64650  ESTABLISHED
  TCP    127.0.0.1:64652        LAPTOP-2KTO83LV:64653  ESTABLISHED
  TCP    127.0.0.1:64653        LAPTOP-2KTO83LV:64652  ESTABLISHED
  TCP    192.168.43.139:64602   relay-7d896c2c:https   ESTABLISHED
  TCP    192.168.43.139:64726   172.64.155.141:https   ESTABLISHED
  TCP    192.168.43.139:65023   49.44.192.11:https     CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64590  [2603:1040:a06:6::1]:https  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64598  sg-in-f188:5228        ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64701  sd-in-f188:5228        ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64724  [2606:4700:8d73:ac57:edd7:97:a5d5:4e6e]:https  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65027  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65028  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65029  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65030  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65031  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65032  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65083  [2406:da1a:e20:7902:998:8754:ed98:e407]:https  TIME_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65084  [2406:da1a:e20:7902:998:8754:ed98:e407]:https  TIME_WAIT
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:5040           LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:7070           LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:9095           LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49672          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49734          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49735          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49738          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49739          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49742          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49743          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49746          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49751          LAPTOP-2KTO83LV:0      LISTENING
  TCP    0.0.0.0:49752          LAPTOP-2KTO83LV:0      LISTENING
  TCP    127.0.0.1:5037         LAPTOP-2KTO83LV:0      LISTENING
  TCP    127.0.0.1:5939         LAPTOP-2KTO83LV:0      LISTENING
  TCP    127.0.0.1:9093         LAPTOP-2KTO83LV:0      LISTENING
  TCP    127.0.0.1:17400        LAPTOP-2KTO83LV:0      LISTENING
  TCP    127.0.0.1:42950        LAPTOP-2KTO83LV:0      LISTENING
  TCP    127.0.0.1:60680        LAPTOP-2KTO83LV:0      LISTENING
  TCP    127.0.0.1:64650        LAPTOP-2KTO83LV:64651  ESTABLISHED
  TCP    127.0.0.1:64651        LAPTOP-2KTO83LV:64650  ESTABLISHED
  TCP    127.0.0.1:64652        LAPTOP-2KTO83LV:64653  ESTABLISHED
  TCP    127.0.0.1:64653        LAPTOP-2KTO83LV:64652  ESTABLISHED
  TCP    192.168.43.139:139     LAPTOP-2KTO83LV:0      LISTENING
  TCP    192.168.43.139:64602   relay-7d896c2c:https   ESTABLISHED
  TCP    192.168.43.139:64726   172.64.155.141:https   ESTABLISHED
  TCP    192.168.43.139:65023   49.44.192.11:https     CLOSE_WAIT
  TCP    [::]:135               LAPTOP-2KTO83LV:0      LISTENING
  TCP    [::]:445               LAPTOP-2KTO83LV:0      LISTENING
  TCP    [::]:9095              LAPTOP-2KTO83LV:0      LISTENING
  TCP    [::]:49664             LAPTOP-2KTO83LV:0      LISTENING
  TCP    [::]:49665             LAPTOP-2KTO83LV:0      LISTENING
  TCP    [::]:49666             LAPTOP-2KTO83LV:0      LISTENING
```

Date: 12/06/2024

```
TCP    [::]:49667             LAPTOP-2KTO83LV:0      LISTENING
TCP    [::]:49668             LAPTOP-2KTO83LV:0      LISTENING
TCP    [::]:49672             LAPTOP-2KTO83LV:0      LISTENING
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64590  [2603:1040:a06:6::1]:https  ESTABLISHED
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64598  sg-in-f188:5228        ESTABLISHED
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64701  sd-in-f188:5228        ESTABLISHED
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64724  [2606:4700:8d73:ac57:edd7:97:a5d5:4e6e]:https  ESTABLISHED
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65027  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65028  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65029  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65030  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65031  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65032  g2600-140f-1c00-0000-0000-0000-312c-8ca9:https  CLOSE_WAIT
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:4500           *:*
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    0.0.0.0:5355           *:*
UDP    0.0.0.0:49671          *:*
UDP    0.0.0.0:50001          *:*
UDP    0.0.0.0:52323          *:*
UDP    0.0.0.0:56502          *:*
UDP    127.0.0.1:1900         *:*
UDP    127.0.0.1:5353         *:*
UDP    127.0.0.1:49664        127.0.0.1:49664
UDP    127.0.0.1:56946        *:*
UDP    192.168.43.139:137     *:*
UDP    192.168.43.139:138     *:*
UDP    192.168.43.139:1900    *:*
UDP    192.168.43.139:56945   *:*
UDP    [::]:500               *:*
UDP    [::]:4500              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5355              *:*
UDP    [::]:49672             *:*
UDP    [::]:52323             *:*
UDP    [::]:56502             *:*
UDP    [::1]:1900             *:*
UDP    [::1]:56944            *:*
UDP    [fe80::9b2c:568b:4a09:c795%15]:1900  *:*
UDP    [fe80::9b2c:568b:4a09:c795%15]:56943  *:*
```

```
C:\Users\HIMANSHU>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     815148432       137569944
Unicast packets              666252          293892
Non-unicast packets              84            7392
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:64650        LAPTOP-2KTO83LV:64651  ESTABLISHED
  TCP    127.0.0.1:64651        LAPTOP-2KTO83LV:64650  ESTABLISHED
  TCP    127.0.0.1:64652        LAPTOP-2KTO83LV:64653  ESTABLISHED
  TCP    127.0.0.1:64653        LAPTOP-2KTO83LV:64652  ESTABLISHED
  TCP    192.168.43.139:64602   relay-7d896c2c.net.anydesk.com:https  ESTABLISHED
  TCP    192.168.43.139:64726   172.64.155.141:https   ESTABLISHED
  TCP    192.168.43.139:65091   49.44.192.11:https     CLOSE_WAIT
  TCP    192.168.43.139:65127   49.44.117.58:https     ESTABLISHED
  TCP    192.168.43.139:65128   a-0003.a-msedge.net:https  ESTABLISHED
  TCP    192.168.43.139:65129   a-0003.a-msedge.net:https  TIME_WAIT
  TCP    192.168.43.139:65131   52.178.17.235:https    ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64590  [2603:1040:a06:6::1]:https  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64598  sg-in-f188.1e100.net:5228  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64701  sd-in-f188.1e100.net:5228  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64724  [2606:4700:8d73:ac57:edd7:97:a5d5:4e6e]:https  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65094  g2600-140f-1c00-0000-0000-0000-312c-8ca9.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65110  [2620:1ec:bdf::254]:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65111  [2606:2800:247:b713:6f8:1d37:ecd5:e137]:https  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65117  [2620:1ec:bdf::72]:https  TIME_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65121  whatsapp-chatd-edge6-shv-02-bom1.facebook.com:https  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65132  [2620:1ec:bdf::72]:https  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65136  [2406:da1a:e20:7902:998:8754:ed98:e407]:https  TIME_WAIT
```

```
C:\Users\HIMANSHU>netstat -i

Active Connections

  Proto  Local Address          Foreign Address        State           Time in State (ms)
TCP    192.168.43.139:64602   relay-7d896c2c:https   ESTABLISHED     3655473
TCP    127.0.0.1:64650        LAPTOP-2KTO83LV:64651  ESTABLISHED     3540860
TCP    127.0.0.1:64651        LAPTOP-2KTO83LV:64650  ESTABLISHED     3540860
TCP    127.0.0.1:64652        LAPTOP-2KTO83LV:64653  ESTABLISHED     3540858
TCP    127.0.0.1:64653        LAPTOP-2KTO83LV:64652  ESTABLISHED     3540858
TCP    192.168.43.139:64726   172.64.155.141:https   ESTABLISHED     3242697
TCP    192.168.43.139:65091   49.44.192.11:https     CLOSE_WAIT      148383
TCP    192.168.43.139:65127   49.44.117.58:https     ESTABLISHED     104588
TCP    192.168.43.139:65128   a-0003:https           ESTABLISHED     102660
TCP    192.168.43.139:65129   a-0003:https           TIME_WAIT       90681
TCP    192.168.43.139:65131   52.178.17.235:https    ESTABLISHED     100203
```

```
C:\Users\HIMANSHU>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:64650        127.0.0.1:64651        ESTABLISHED
  TCP    127.0.0.1:64651        127.0.0.1:64650        ESTABLISHED
  TCP    127.0.0.1:64652        127.0.0.1:64653        ESTABLISHED
  TCP    127.0.0.1:64653        127.0.0.1:64652        ESTABLISHED
  TCP    192.168.43.139:64602   208.115.231.86:443     ESTABLISHED
  TCP    192.168.43.139:64726   172.64.155.141:443     ESTABLISHED
  TCP    192.168.43.139:65091   49.44.192.11:443       CLOSE_WAIT
  TCP    192.168.43.139:65128   204.79.197.203:443     TIME_WAIT
  TCP    192.168.43.139:65131   52.178.17.235:443      TIME_WAIT
  TCP    192.168.43.139:65151   20.189.173.18:443      TIME_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64590  [2603:1040:a06:6::1]:443  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64598  [2404:6800:4003:c1a::bc]:5228  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64701  [2404:6800:4003:c0f::bc]:5228  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:64724  [2606:4700:8d73:ac57:edd7:97:a5d5:4e6e]:443  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65094  [2600:140f:1c00::312c:8ca9]:443  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65110  [2620:1ec:bdf::254]:443  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65111  [2606:2800:247:b713:6f8:1d37:ecd5:e137]:443  CLOSE_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65121  [2a03:2880:f22f:1c7:face:b00c:0:7260]:443  ESTABLISHED
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65132  [2620:1ec:bdf::72]:443  TIME_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65136  [2406:da1a:e20:7902:998:8754:ed98:e407]:443  TIME_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65139  [2406:da1a:52f:6200:1b0d:edb:15da:4247]:8080  TIME_WAIT
  TCP    [2405:204:8580:c500:b133:9743:f7c2:1bdc]:65145  [2406:da1a:e20:7902:998:8754:ed98:e407]:443  TIME_WAIT
```

Date: 12/06/2024

7. nslookup

Description:

Nslookup is a command-line network administration tool used to query Domain Name System (DNS) servers. It translates domain names into IP addresses and can also retrieve other DNS records, aiding in diagnosing and troubleshooting DNS issues. Available on various operating systems, it is commonly used to verify DNS configurations and resolve network connectivity problems.

No.	Option	Description
1	nslookup -debug	Print details of debug information.
2	nslookup - timeout=number	Set the time to wait for a reply from the DNS server.
3	nslookup - port=number	Specify the port number to use for the DNS query (default is 53).
4	nslookup – vc	Use a virtual circuit when sending requests to the server.
5	nslookup - tcp	Use TCP instead of UDP.

Implementation:

```
C:\Users\HIMANSHU>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> google.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:805::200e
          142.250.70.110

> 1
Server:  UnKnown
Address:  192.168.43.1

Name:    1
Address:  0.0.0.1
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>nslookup  -debug
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NXDOMAIN
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional = 0

    QUESTIONS:
        1.43.168.192.in-addr.arpa, type = PTR, class = IN
    AUTHORITY RECORDS:
    ->  168.192.in-addr.arpa
        ttl = 10800 (3 hours)
        primary name server = localhost
        responsible mail addr = nobody.invalid
        serial  = 1
        refresh = 3600 (1 hour)
        retry   = 1200 (20 mins)
        expire  = 604800 (7 days)
        default TTL = 10800 (3 hours)

------------
Default Server:  UnKnown
Address:  192.168.43.1
```

```
C:\Users\HIMANSHU>nslookup -timeout=50 google.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:830::200e
          142.250.70.110
```

Date: 12/06/2024

```
$ nslookup -vc
Default Server:  UnKnown
Address:  192.168.43.1

> 2
Server:  UnKnown
Address:  192.168.43.1

Name:    2
Address:  0.0.0.2

> 3
Server:  UnKnown
Address:  192.168.43.1

Name:    3
Address:  0.0.0.3

> |
```

```
$ nslookup -tcp
*** Invalid option: tcp
Default Server:  UnKnown
Address:  192.168.43.1

> 12
Server:  UnKnown
Address:  192.168.43.1

Name:    12
Address:  0.0.0.12

> |
```

Date: 12/06/2024

8. hostname

Description:

The hostname command in a Unix-like operating system is used to display or set the system's hostname. When executed without any arguments, it returns the current hostname of the machine. When used with options or an argument, it can change the hostname or provide more detailed information about the network configuration of the system.

No.	Option	Description
1	hostname	Prints the name of the current host.
2	Hostname -a	This option is used to get the alias name of the host system (if any). It will return an empty line if no alias name is set.
3	hostname -d	Used to always set a hostname.
4	hostname -i	This option is used to get the IP (network) addresses.
5	hostname -I	This option is used to get all IP(network) addresses.

Implementation:

```
C:\Users\HIMANSHU>hostname
LAPTOP-2KTO83LV
```

```
HIMANSHU@LAPTOP-2KTO83LV ~
$ hostname -a
```

```
$ hostname -i
fe80::9b2c:568b:4a09:c795%15 2409:4041:d98:ab63:f5ac:6929:fca6:5b99 2409:4041:d9
8:ab63:3da3:78e:b3e1:980a 192.168.43.139
```

```
$ hostname -I
169.254.168.110 169.254.127.131 2409:4041:d98:ab63:3da3:78e:b3e1:980a 2409:4041:
d98:ab63:f5ac:6929:fca6:5b99 192.168.43.139
```

Date: 12/06/2024

9. pathing

Description:

Pathping is a network utility in Windows that combines the features of ping and tracert. It provides information about latency and packet loss at different points along a network path, helping diagnose network performance issues.

No.	Option	Description
1	pathping -h	Maximum number of hops to search for target.
2	pathping -n	Do not resolve addresses to hostnames.
3	pathping -w timeout	Wait timeout milliseconds for each reply.
4	pathping -4	Force Using Ipv4
5	pathping -6	Force Using IPv6

```
C:\Users\HIMANSHU>pathping google.com

Tracing route to google.com [2404:6800:4009:805::200e]
over a maximum of 30 hops:
  0  LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
  1  2405:204:8580:c500::2c
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
                                    1/ 100 =  1%   |
  1    4ms     1/ 100 =  1%     0/ 100 =  0%  2405:204:8580:c500::2c

Trace complete.
```

```
C:\Users\HIMANSHU>pathping -n 10 google.com

Tracing route to google.com [2404:6800:4009:805::200e]
over a maximum of 10 hops:
  0  LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
  1  2405:204:8580:c500::2c
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
                                    0/ 100 =  0%   |
  1    4ms     0/ 100 =  0%     0/ 100 =  0%  2405:204:8580:c500::2c

Trace complete.
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>pathping -w 10 google.com

Tracing route to google.com [2404:6800:4009:803::200e]
over a maximum of 30 hops:
  0  LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
  1  2405:204:8580:c500::2c
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
                                    0/ 100 =  0%   |
  1    4ms     0/ 100 =  0%     0/ 100 =  0%  2405:204:8580:c500::2c

Trace complete.
```

```
C:\Users\HIMANSHU>pathping -4 google.com

Tracing route to google.com [142.250.70.78]
over a maximum of 30 hops:
  0  LAPTOP-2KTO83LV [192.168.43.139]
  1  192.168.43.1
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAPTOP-2KTO83LV [192.168.43.139]
                                    0/ 100 =  0%   |
  1    8ms     0/ 100 =  0%     0/ 100 =  0%  192.168.43.1

Trace complete.
```

```
$ pathping -6 google.com

Tracing route to google.com [2404:6800:4009:803::200e]
over a maximum of 30 hops:
  0  LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
  1  2405:204:8580:c500::2c
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAPTOP-2KTO83LV [2405:204:8580:c500:b133:9743:f7c2:1bdc]
                                    0/ 100 =  0%   |
  1    4ms     0/ 100 =  0%     0/ 100 =  0%  2405:204:8580:c500::2c

Trace complete.
```

```
Tracing route to google.com [2404:6800:4009:803::200e]
over a maximum of 30 hops:
  0  2405:204:8580:c500:b133:9743:f7c2:1bdc
  1  2405:204:8580:c500::2c
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           2405:204:8580:c500:b133:9743:f7c2:1bdc
                                    0/ 100 =  0%   |
  1    3ms     0/ 100 =  0%     0/ 100 =  0%  2405:204:8580:c500::2c

Trace complete.
```

Date: 12/06/2024

10. Arp

Description:

ARP (Address Resolution Protocol) is a networking protocol used to map an IP address to a physical machine address (MAC address) that is recognized in the local network. It operates at the data link layer of the OSI model and helps devices communicate within a network by maintaining a table of IP addresses and their corresponding MAC addresses.

No.	Option	Description
1	arp -a	Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
2	arp -v	Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.
3	arp -d	Display or manipulate ARP entries for a specific network interface.
4	arp -n	Show IP addresses in numerical format instead of trying to resolve hostnames.
5	arp Eth_addr	Specifies a physical address.

Date: 12/06/2024

Implements:

```
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

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

Interface: 192.168.43.139 --- 0xf
  Internet Address      Physical Address      Type
  192.168.43.1          46-86-7b-1f-ce-d5     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Date: 12/06/2024

```
C:\Users\HIMANSHU>arp -n

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

```
C:\Users\HIMANSHU>arp -d
The ARP entry deletion failed: The requested operation requires elevation.


C:\Users\HIMANSHU>arp Eth_addr
```

Date: 19/06/2024

Himanshu Parmar
22010101132

Lab Practical #02:

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

Practical Assignment #02:

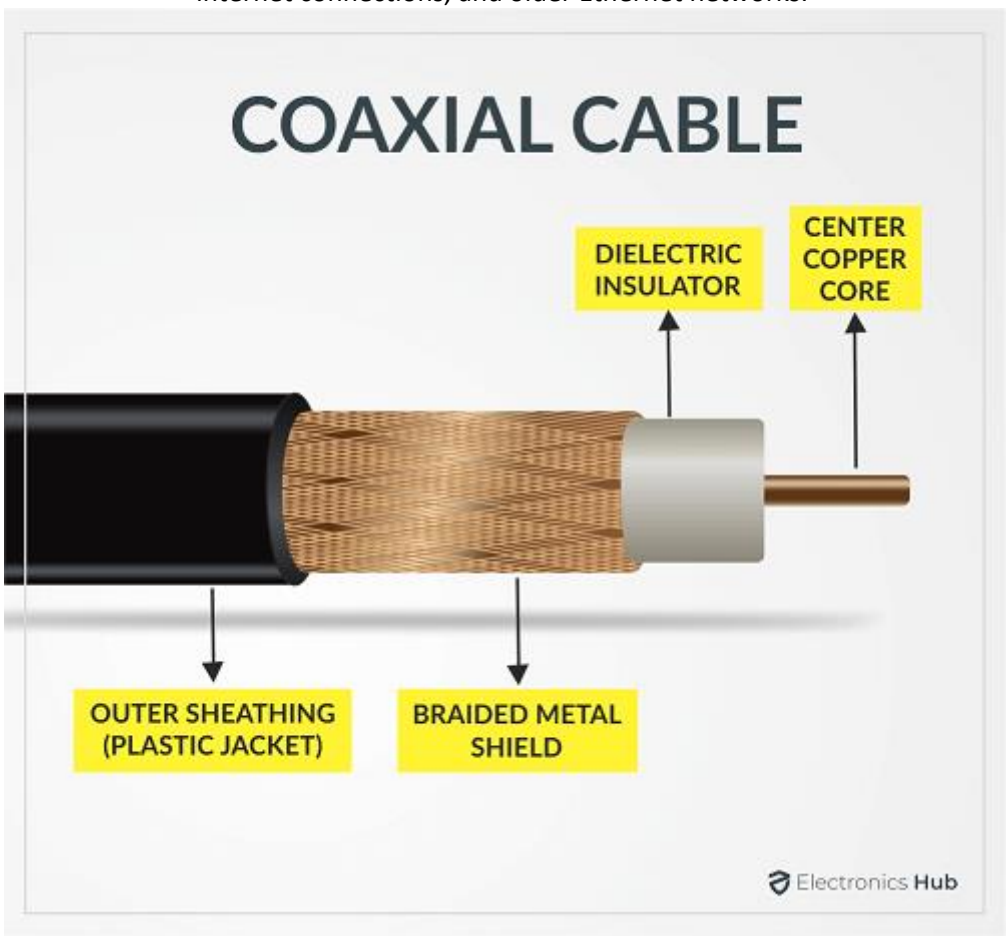
1. List various networks cable. Also, write short description.
2. Difference between guided and unguided media.
3. Give cross-wired cable and straight through cable diagram (Color Code wise).

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

1) **Cables**:

a) Coaxial Cable:

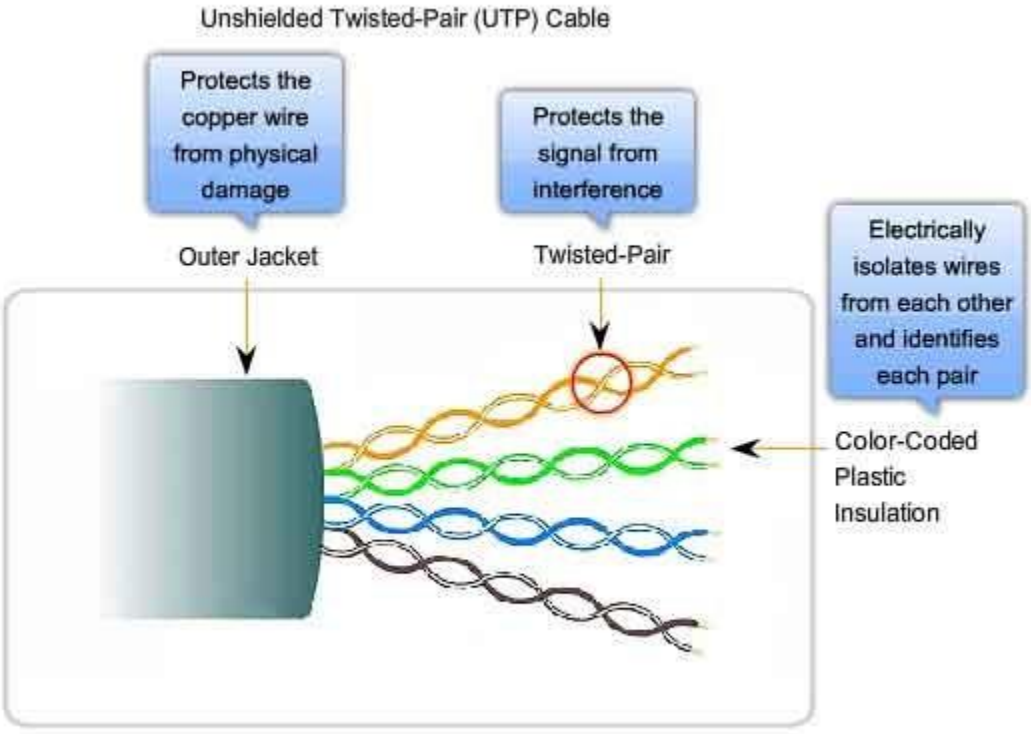
- Coaxial cables consist of a central copper conductor, surrounded by a plastic insulating layer, a metallic shield, and an outer insulating layer. They are commonly used for cable television, internet connections, and older Ethernet networks.



Date: 19/06/2024

b) Unshielded Twisted Pair(UTP)

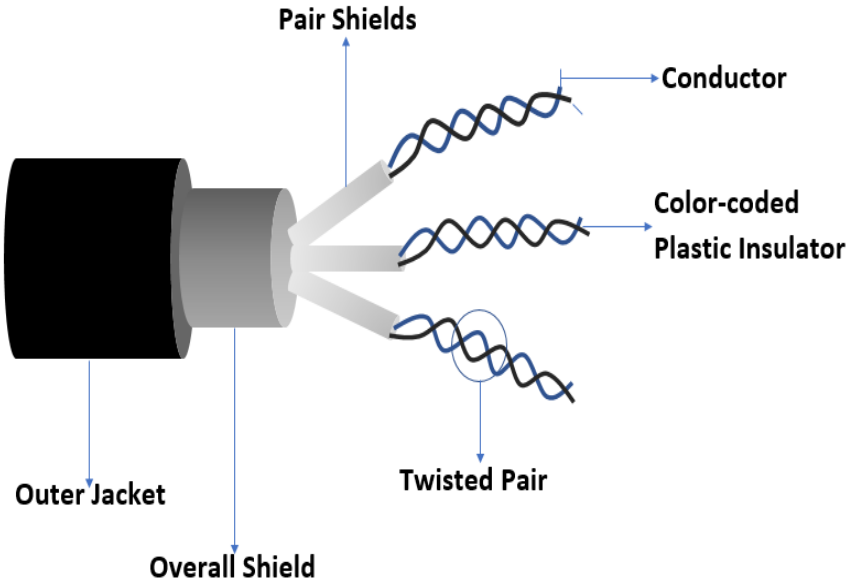
- UTP cables have pairs of twisted copper wires without additional shielding. They are widely used in Ethernet networks for both residential and commercial applications due to their flexibility and ease of installation.



c) Shielded Twisted Pair(STP):

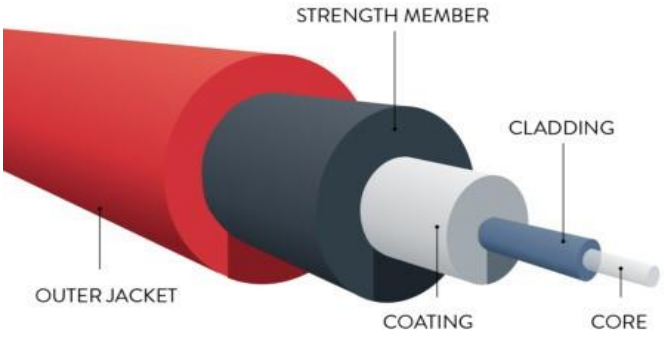
- STP cables are similar to UTP but have an additional shielding to protect against electromagnetic interference (EMI) and radio frequency interference (RFI). They are used in environments with high interference.

Date: 19/06/2024



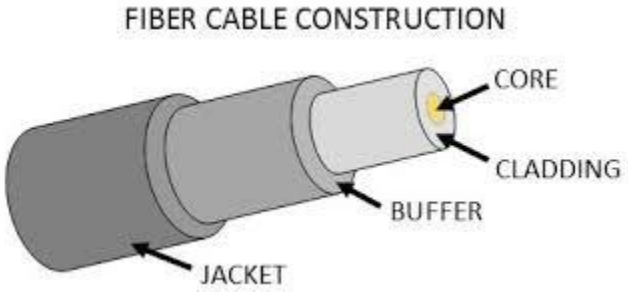
d) Fiber Optic Cable:

- Fiber optic cables use light to transmit data, offering high bandwidth and long-distance capabilities. They consist of strands of glass fibers surrounded by protective layers.



e) Single-mode Fiber (SMF):

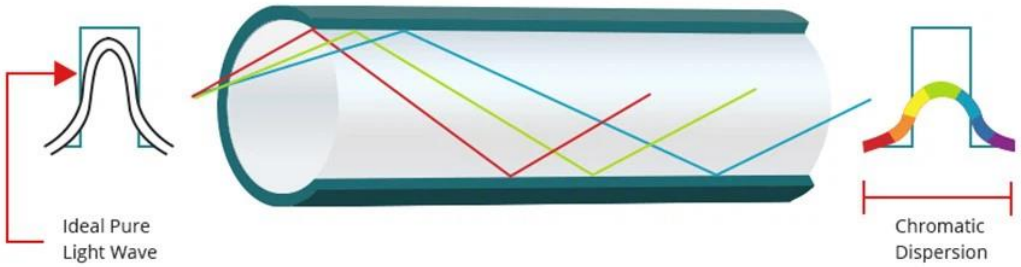
- SMF cables use a single strand of glass fiber and are used for long-distance data transmission with higher bandwidth capabilities.



Date: 19/06/2024

f) Multi-mode Fiber (MMF)

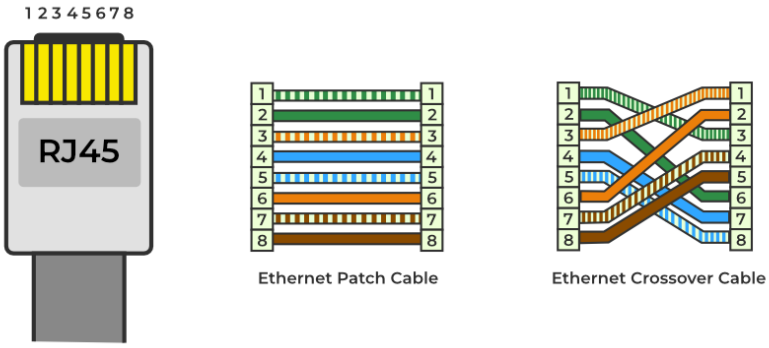
- MMF cables use multiple strands of glass fiber and are used for shorter distance data transmission with moderate bandwidth capabilities.



2) **Connectors**:

a) RJ45

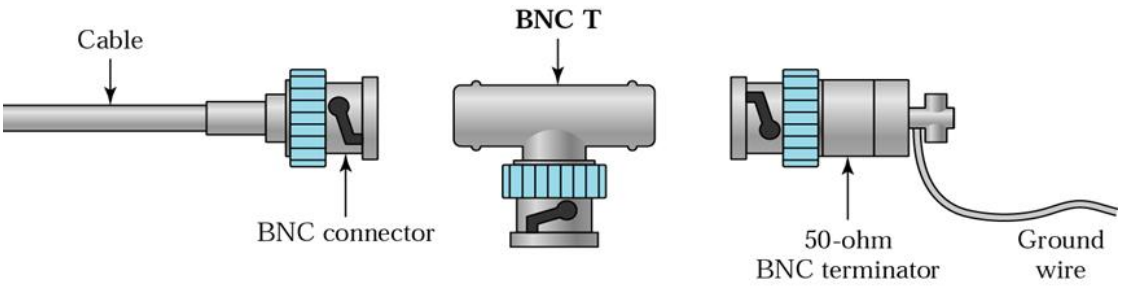
- The RJ45 connector is an 8-pin modular plug commonly used for Ethernet networking. It connects twisted pair cables to networking devices like routers, switches, and computers.



Date: 19/06/2024

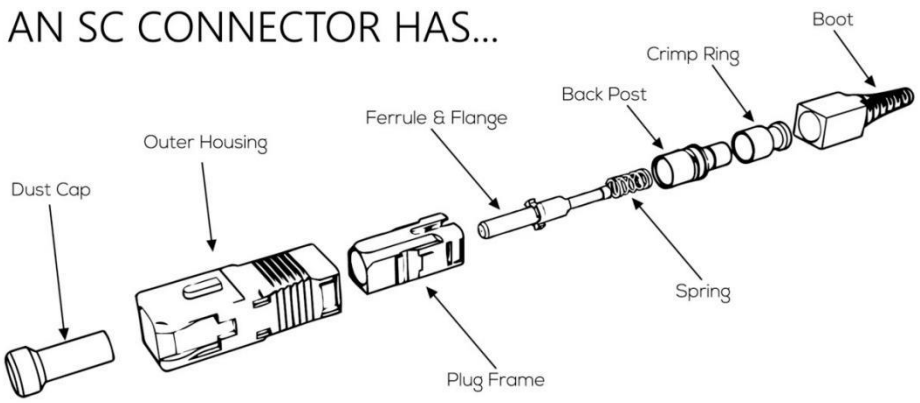
b) BNC (Bayonet Neill-Concelman)

- BNC connectors are quick connect/disconnect RF connectors used with coaxial cables. They are widely used in television, radio, and other radio-frequency applications.



c) SC (Subscriber Connector)

- SC connectors are used for fiber optic cables. They are push-pull connectors that provide excellent performance for single-mode and multi-mode fiber applications.



Date: 19/06/2024

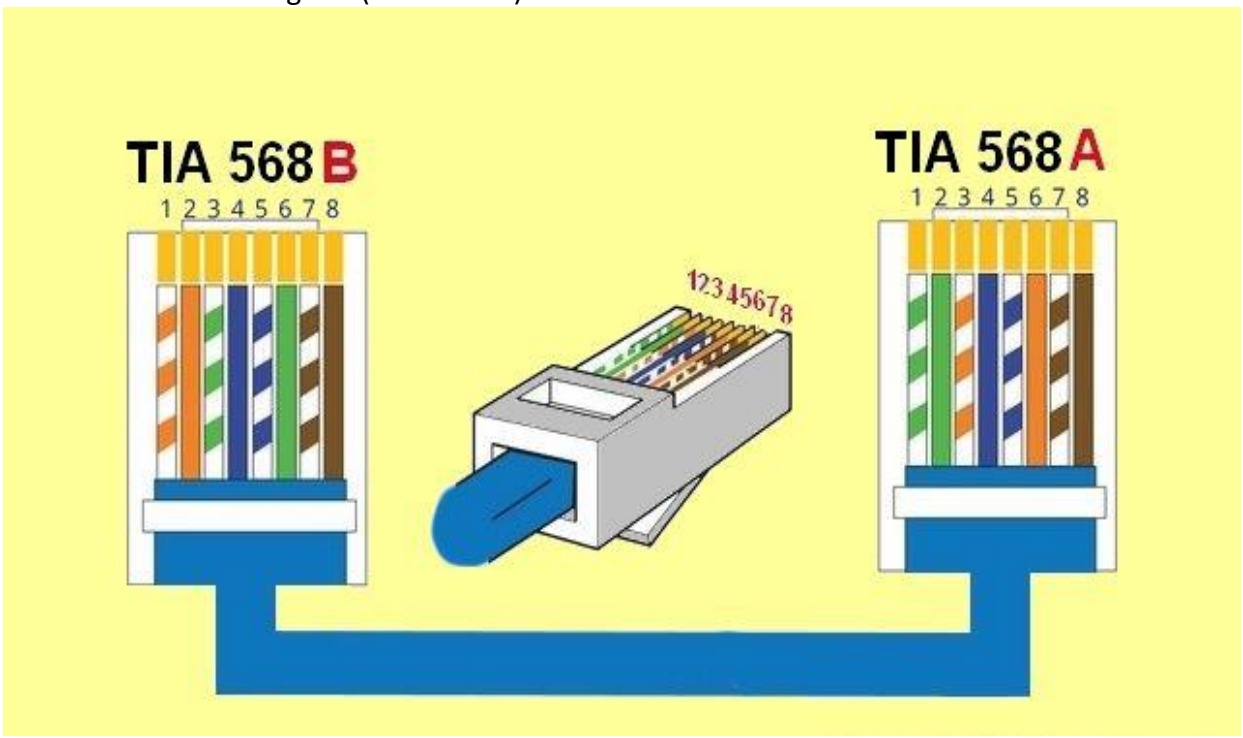
2. Difference between guided and unguided media.

S. No.	Guided Media	Unguided Media
1.	The guided media is also called wired communication or bounded transmission media.	The unguided media is also called wireless communication or unbounded transmission media.
2.	The signal energy propagates through wires in guided media.	The signal energy propagates through the air in unguided media.
3.	Guided media is used for point-to-point communication.	Unguided media is generally suited for radio broadcasting in all directions.
4.	It is cost-effective.	It is expensive.
5.	Discrete network topologies are formed by the guided media.	Continuous network topologies are formed by the unguided media.
6.	Signals are in the form of voltage, current, or photons in the guided media.	Signals are in the form of electromagnetic waves in unguided media.
7.	Examples of guided media are twisted pair wires, coaxial cables, and optical fiber cables.	Examples of unguided media are microwave or radio links and infrared light.
8.	By adding more wires, the transmission capacity can be increased in guided media.	It is not possible to obtain additional capacity in unguided media.

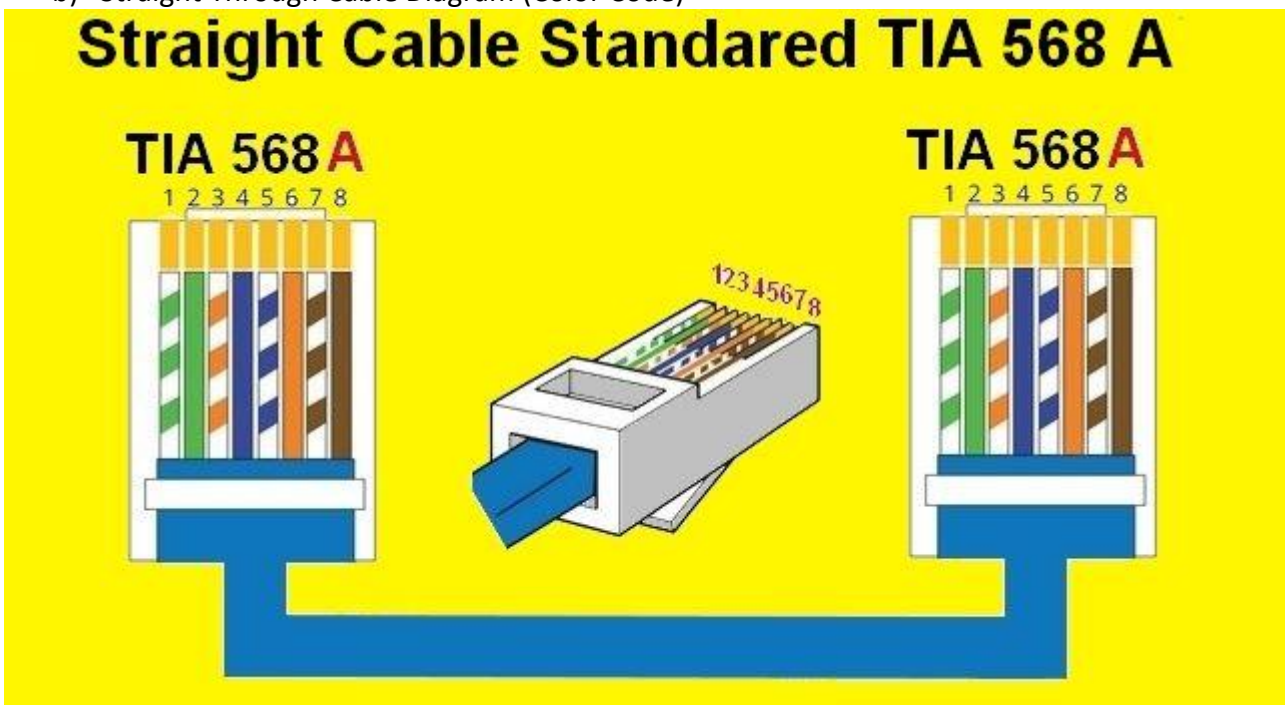
Date: 19/06/2024

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:03/07/2024

Himanshu Parmar
22010101132

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

Difference between network devices:

Hub and Switch

No.	Hub	Switch
1	Hub is operated on Physical layer of OSI model.	While Switch is operated on Data link layer of OSI model.
2	Hub is a broadcast type transmission.	While Switch is a Unicast, multicast and broadcast type transmission.
3	Int Hub, there is only one collision domain.	While in switch, different ports have own collision domain
4	Hub sends data in the form of binary bits	Switch sends data in the form of frames
5	Cheaper as compare to switch	Expensive as compare to Hub
6	Hub does not store any MAC address or IP address	Switch store MAC address

Switch and Router

No.	Switch	Router
1	While the main objective of switch is to connect various devices simultaneously.	The main objective of router is to connect various networks simultaneously.
2	While it works in data link layer.	It works in network layer.
3	While switch is used by only LAN.	Router is used by LAN as well as MAN.
4	While through switch data is sent in the form of frame.	Through the router, data is sent in the form of packets.

Date:03/07/2024

5	Maximum speed is 10Mbps to 100Mbps.	maximum speed for wireless is 1-10 Mbps and maximum speed for wired connections is 100 Mbps.

Router and Gateway

No.	Router	Gateway
1	It is a hardware device which is responsible for receiving, analyzing and forwarding the data packets to other networks.	It is a device that is used for the communication among the networks which have a different set of protocols.
2	It supports the dynamic routing.	It does not support dynamic routing.
3	The main function of a router is routing the traffic from one network to the other.	The main function of a gateway is to translate one protocol to the other.
4	It is hosted on only the dedicated applications.	It is hosted on dedicated applications, physical servers or virtual applications.
5	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

How it works:

- **Layer 2 Device**: Operates at the Data Link Layer (Layer 2) of the OSI model.
- **MAC Addresses**: Uses MAC (Media Access Control) addresses to identify and forward data to the correct destination.
- **Packet Switching**: When a device sends data, the switch receives it and looks at the MAC address to determine the appropriate port to forward the data to.
- **Learning**: Switches maintain a MAC address table (or CAM table) where they learn and store the MAC addresses of devices connected to each port.
- **Full-Duplex**: Most modern switches support full-duplex communication, meaning devices can send and receive data simultaneously.

2. Router

How it works:

- **Layer 3 Device**: Operates at the Network Layer (Layer 3) of the OSI model.
- **IP Addresses**: Uses IP addresses to determine the best path to forward packets to their destination.
- **Routing Tables**: Maintains a routing table with information about different networks and the best routes to reach them.
- **Routing Protocols**: Uses routing protocols (like OSPF, BGP, EIGRP) to dynamically learn about network topology changes and update the routing table.
- **NAT**: Often performs Network Address Translation (NAT), allowing multiple devices on a LAN to share a single public IP address for Internet access.

Date:03/07/2024

3. Gateway

How it works:

- **Protocol Translation**: Performs protocol conversion to ensure communication between different network architectures or systems (e.g., from TCP/IP to another protocol).
- **Application Layer**: Can operate at various layers of the OSI model, often at the Application Layer (Layer 7), but also at lower layers depending on the function.
- **Security and Filtering**: Often incorporates security functions like firewall capabilities, filtering, and traffic management.
- **Connectivity**: Provides connectivity between different networks, such as connecting a local network to the Internet or bridging different network environments.

Date: 10/07/2024

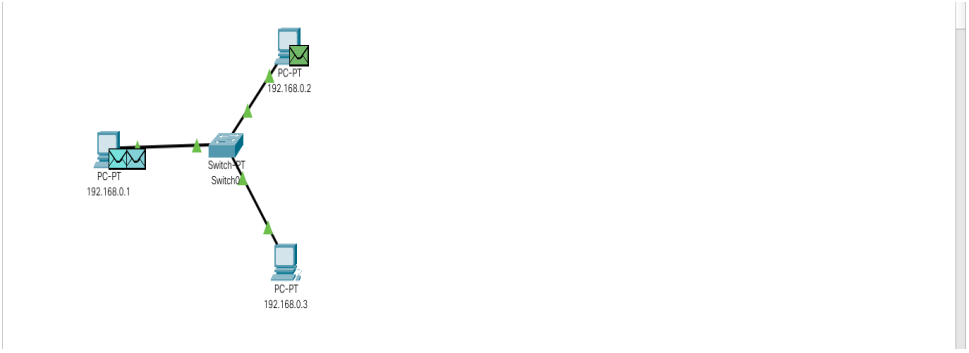
Himanshu Parmar
22010101132

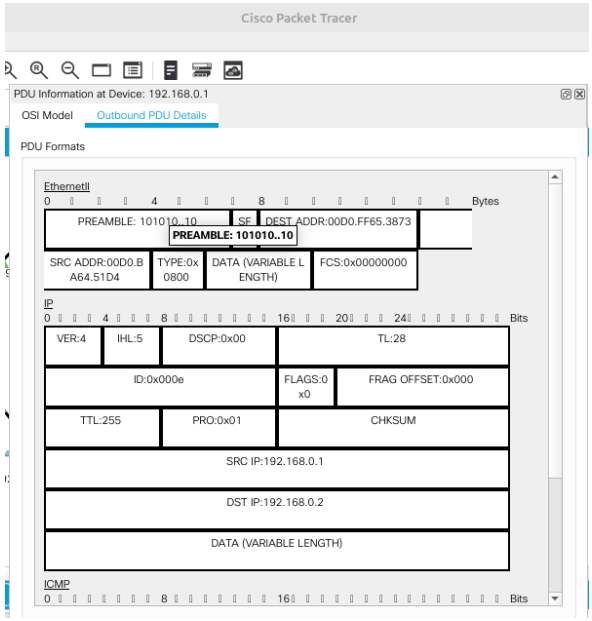
Lab Practical #04:

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.**

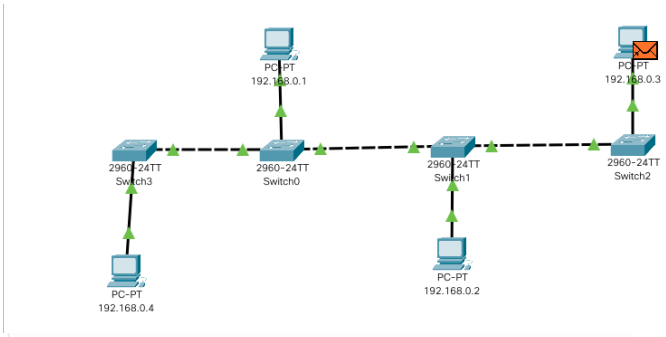


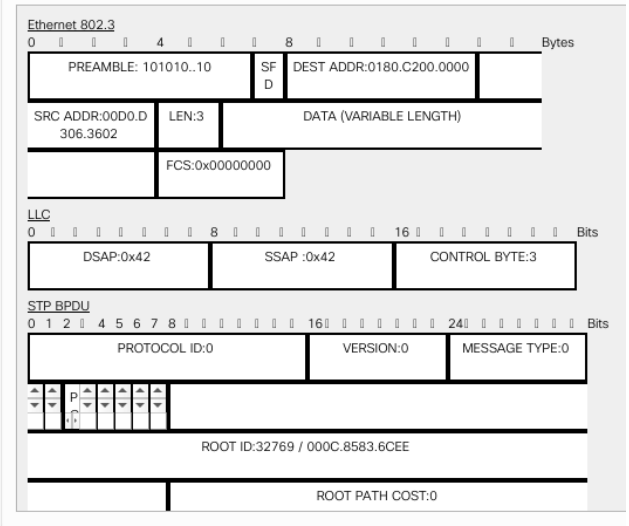


Date: 10/07/2024

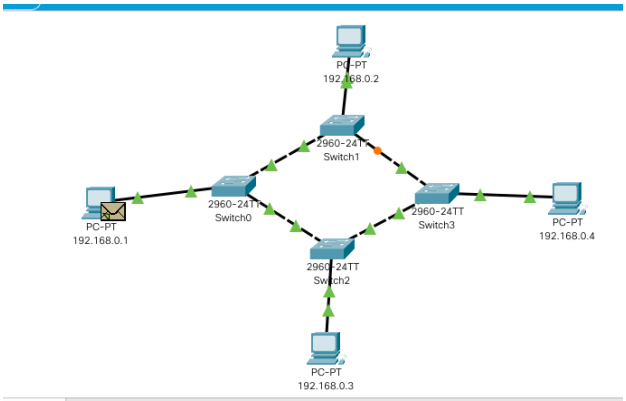
2. Implement different topologies in packet tracer.

a. Bus

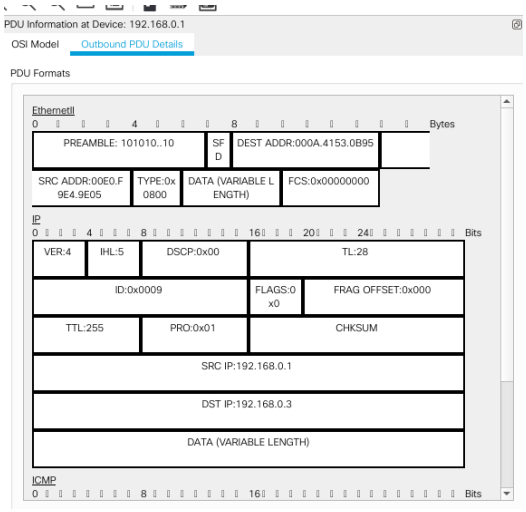




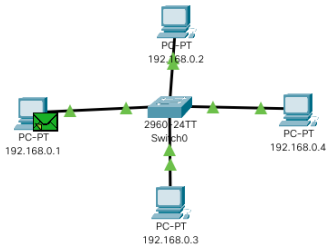
b. Ring

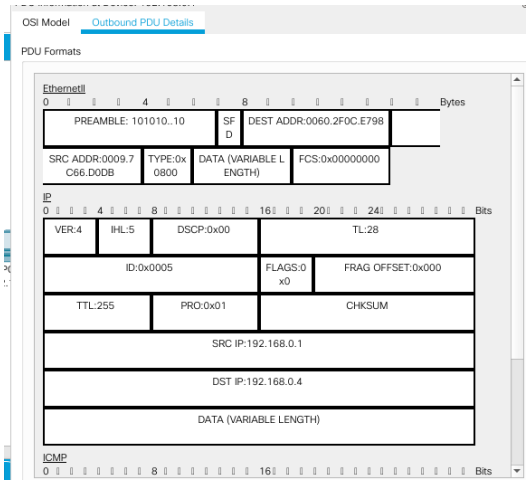


Date: 10/07/2024



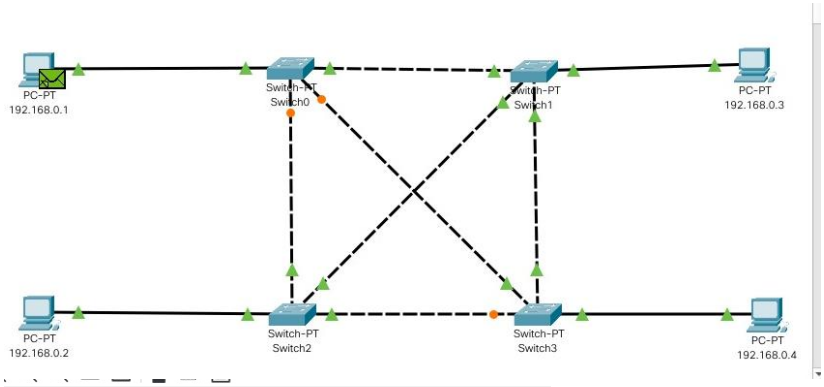
c. Star

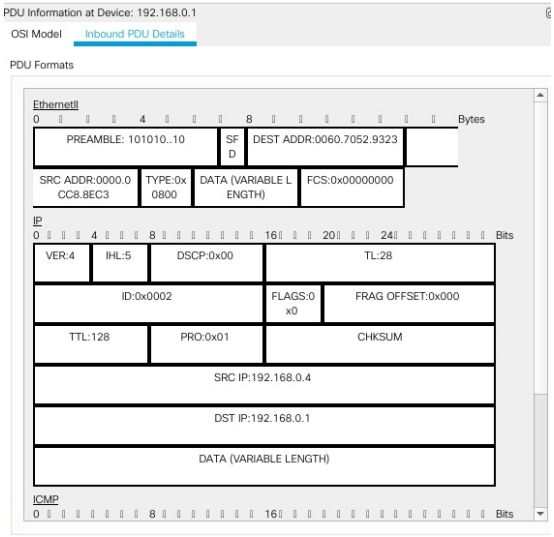




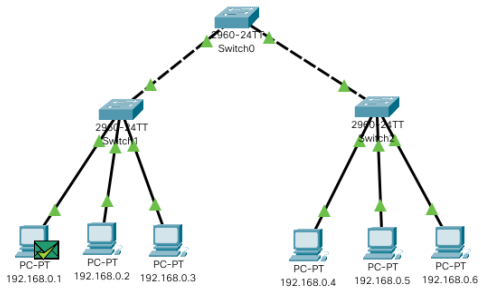
Date: 10/07/2024

d. Mesh

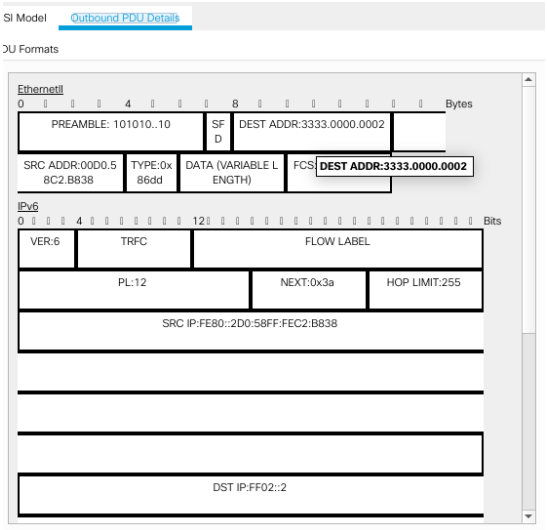




e. Tree



Date: 10/07/2024



Date: 17/07/2024

Himanshu Parmar
22010101132

Lab Practical #05:

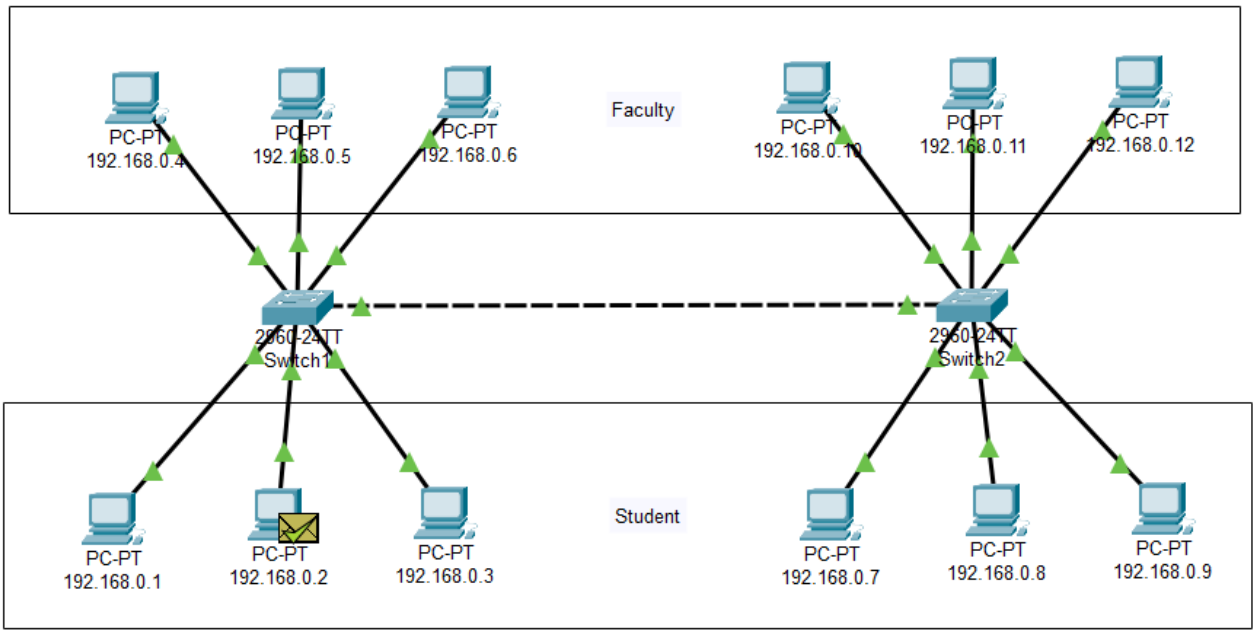
Study the concept of VLAN using packet tracer.

Practical Assignment #05:

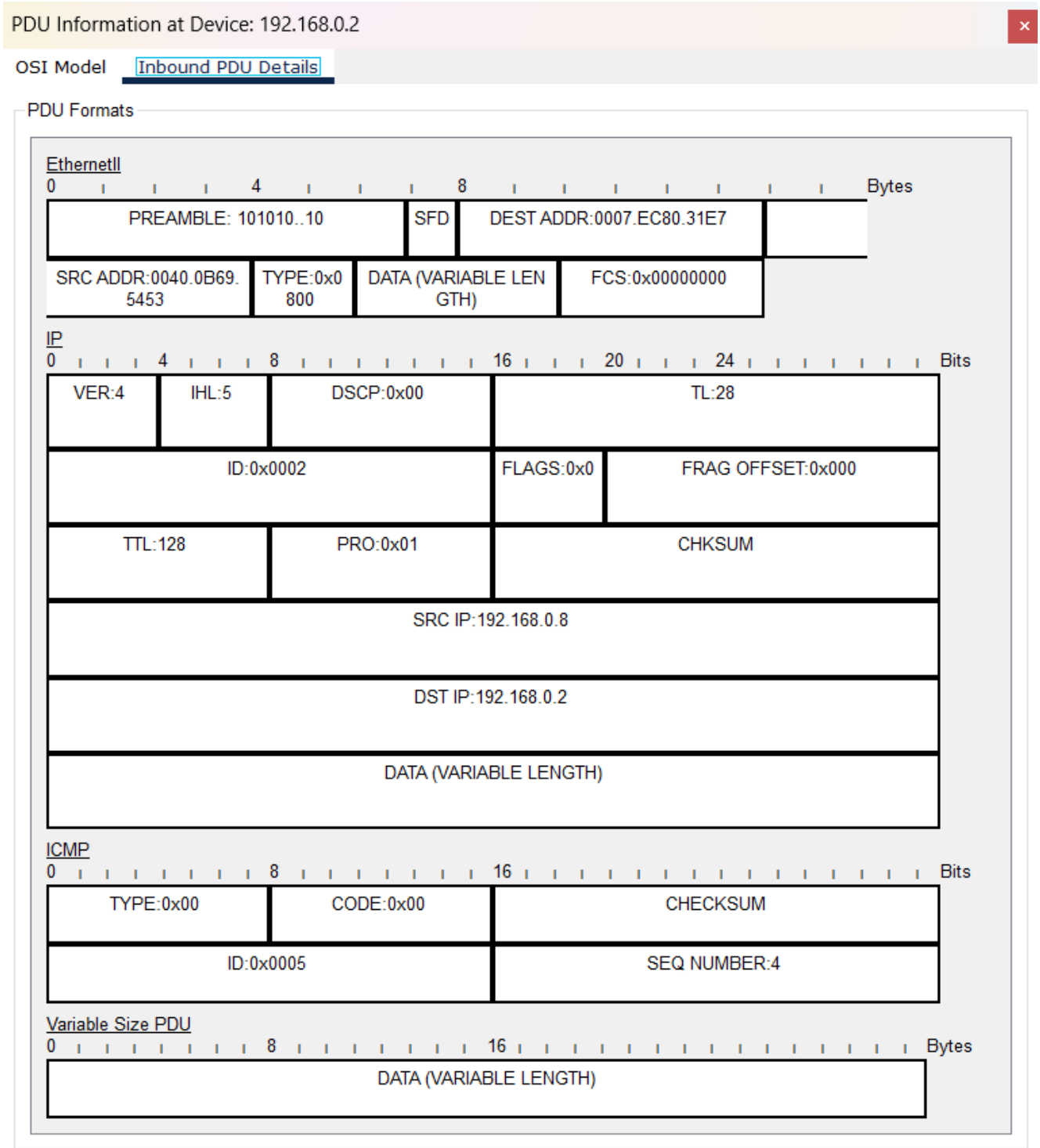
1. **Implement the different network structures in VLAN and VLAN trunking. Also check connectivity between them using ping command or PDU utility.**

➢ How to Create VLAN in packet tracer

- Open Cisco Packet Tracer on your computer.
- First Create Network Topologies.
- After Creating Topologies, Click on a switch to open its configuration window. Go to the Config tab. In the Config tab, find the VLAN Database section. Here, you can add new VLANs by entering the VLAN number and name.
- To add Add Devices to Separate VLAN, Click on a switch to open its configuration window. Go to the Config tab and select the specific port that is connected to a device. In the port configuration section, set the port mode to Access and select the VLAN number .



Date: 17/07/2024



Date: 17/07/2024

VLAN Configuration

VLAN Number

VLAN Name

Add Remove

VLAN No	VLAN Name
1	default
150	Student
250	Faculty
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

Date:31/07/2024

Himanshu Parmar
22010101132

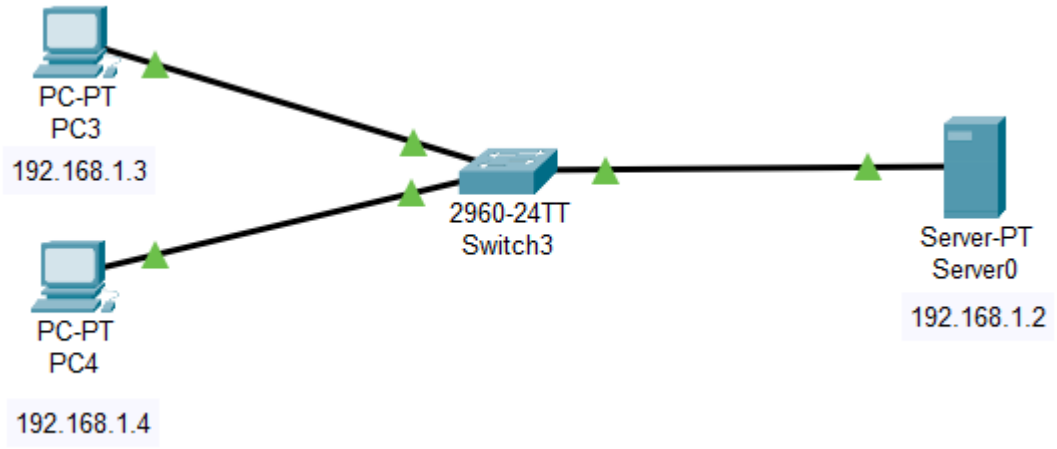
Lab Practical #06:

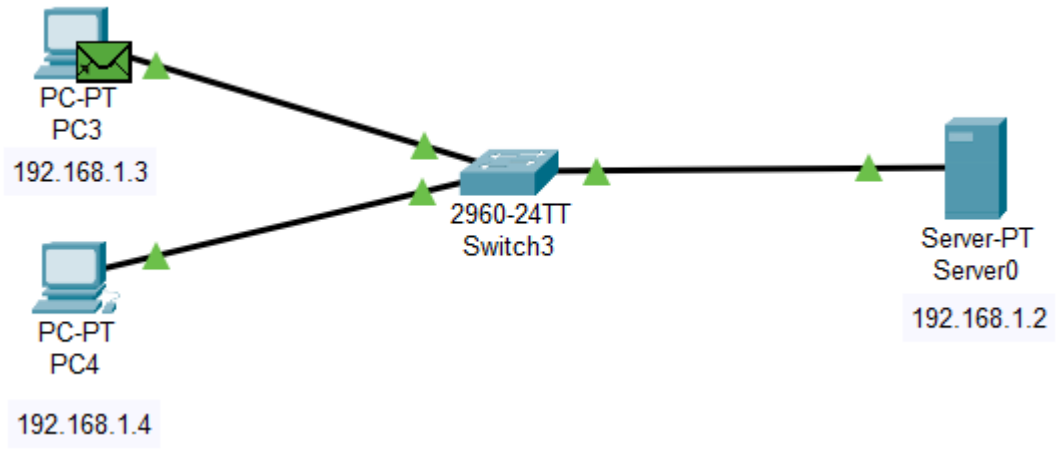
Study the application layer protocol DNS, DHCP, FTP.

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:





Date:31/07/2024

PDU Information at Device: PC3

OSI Model | Inbound PDU Details

PDU Formats

Ethernetll

0	4	8	Bytes
PREAMBLE: 101010..10	SFD	DEST ADDR:0090.219B.D779	
SRC ADDR:0001.964C.1456	TYPE:0x0800	DATA (VARIABLE LENGTH)	FCS:0x00000000

IP

0	4	8	16	20	24	Bits
VER:4	IHL:5	DSCP:0x00	TL:28			
ID:0x0003			FLAGS:0x0	FRAG OFFSET:0x000		
TTL:128	PRO:0x01	CHKSUM				
SRC IP:192.168.1.4						
DST IP:192.168.1.3						
DATA (VARIABLE LENGTH)						

ICMP

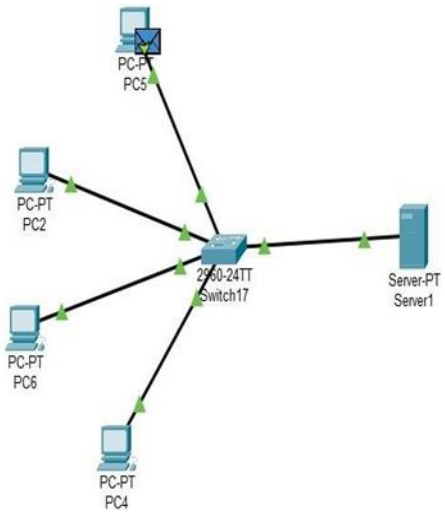
0	8	16	Bits
TYPE:0x00	CODE:0x00	CHECKSUM	
ID:0x0004		SEQ NUMBER:3	

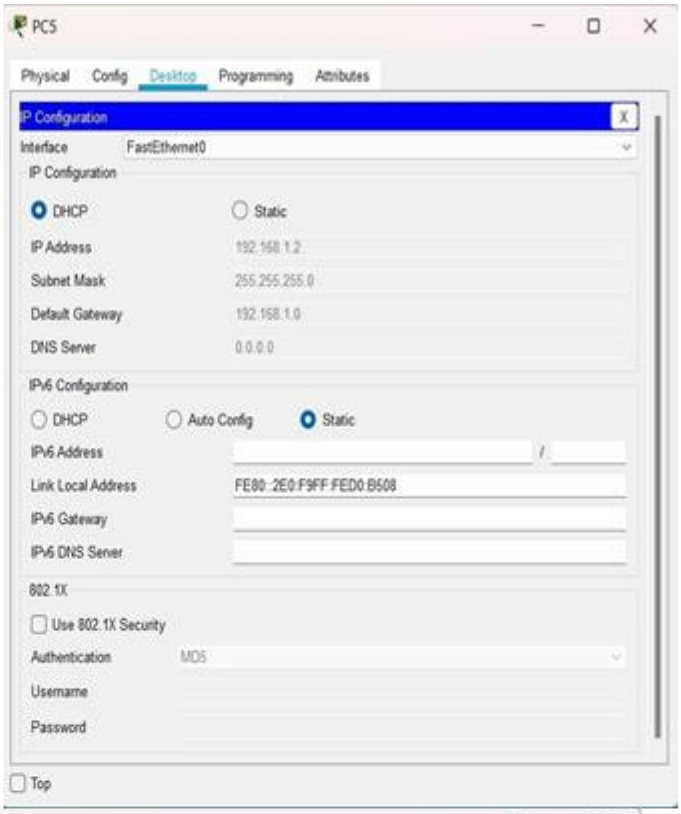
Variable Size PDU

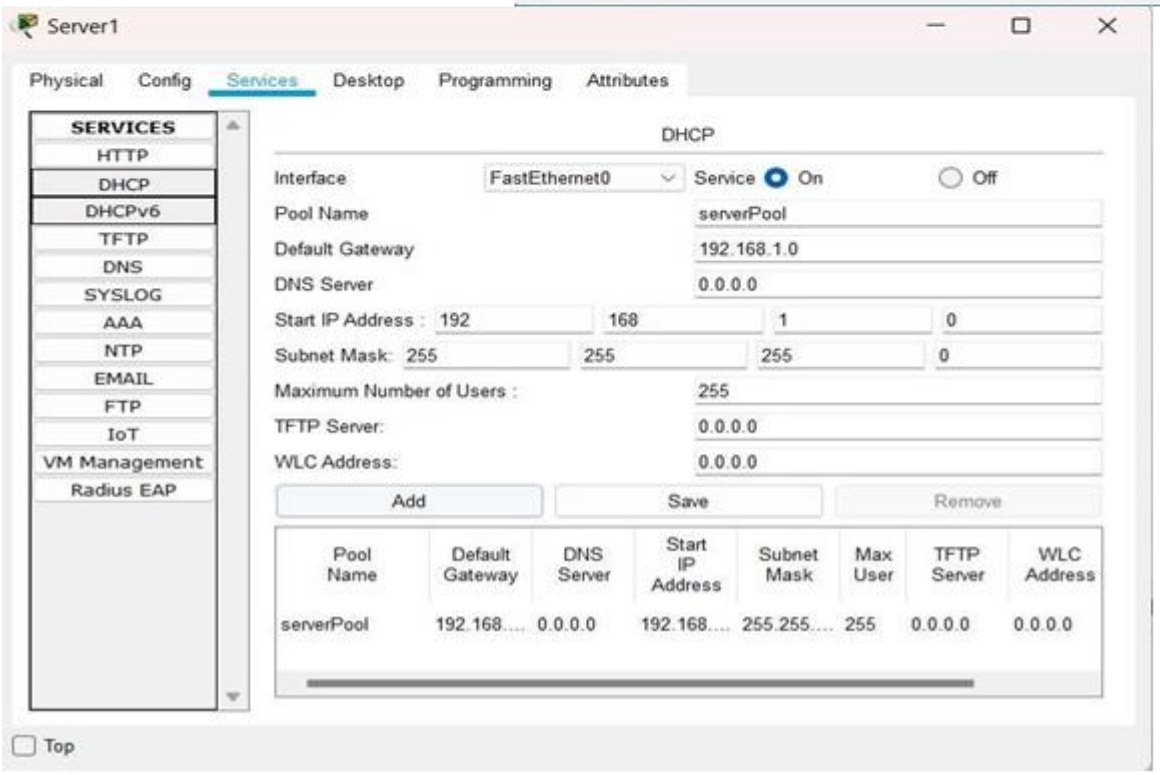
0	8	16	Bytes
DATA (VARIABLE LENGTH)			

Date:31/07/2024

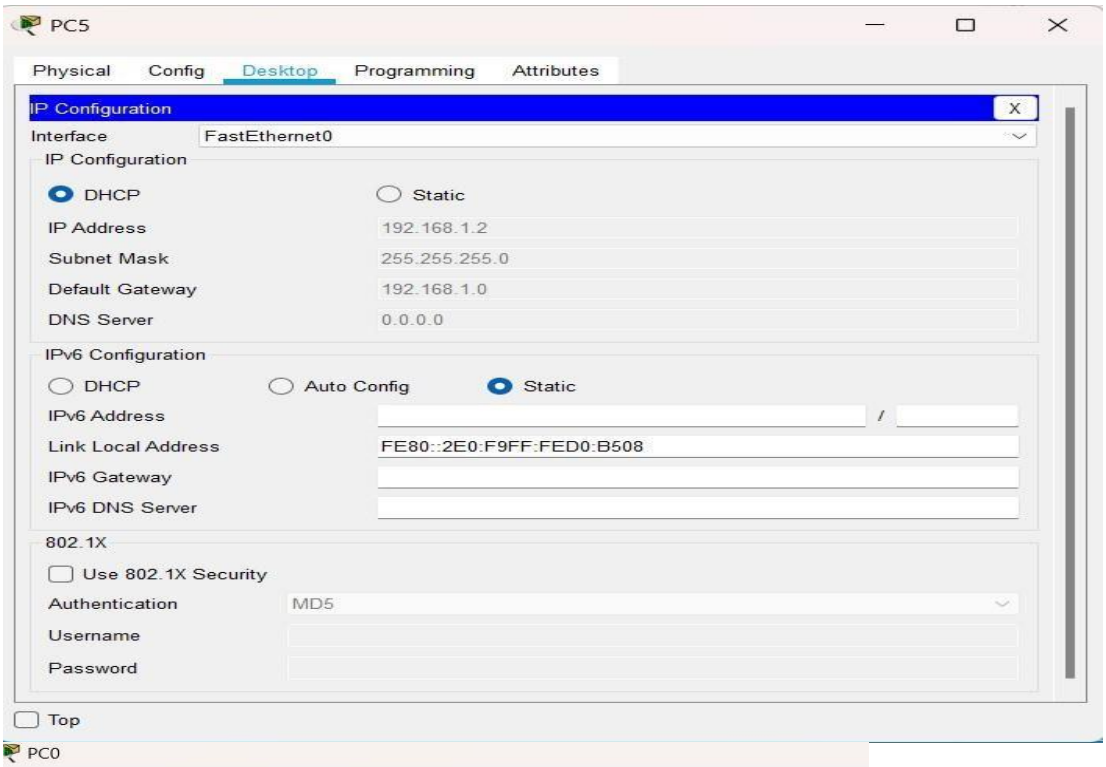
DHCP:

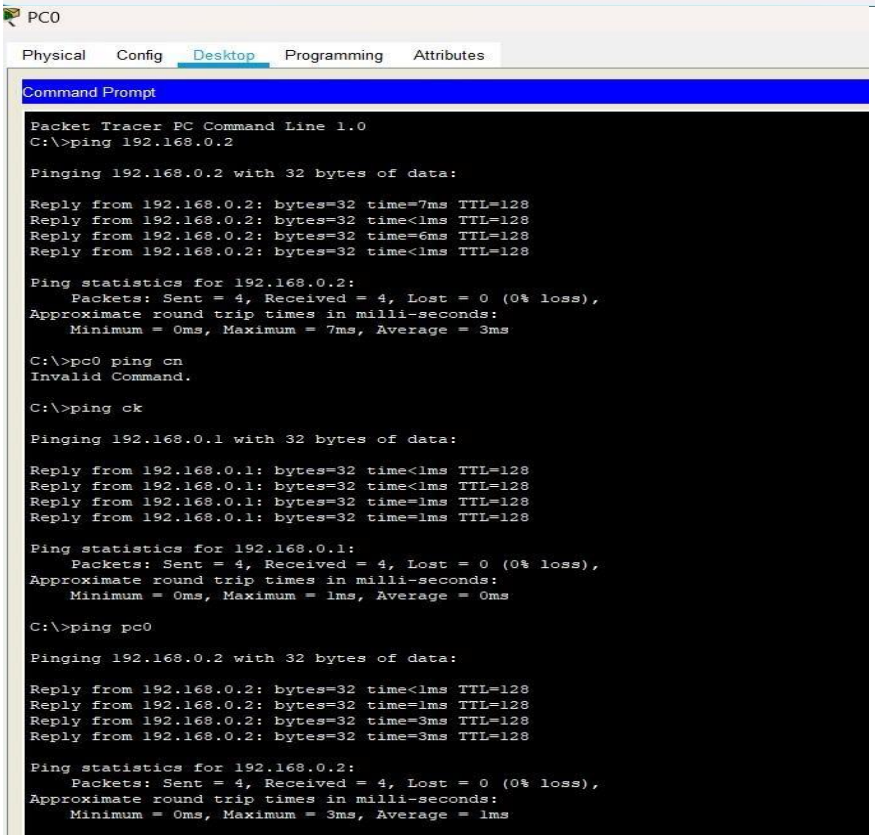






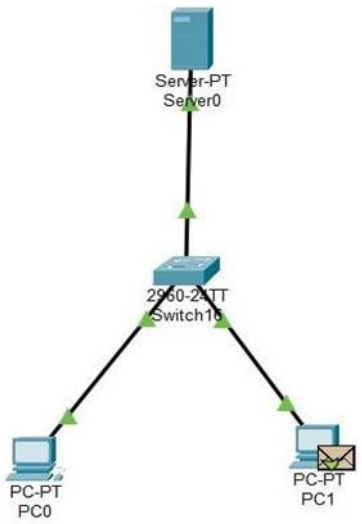
Date:31/07/2024

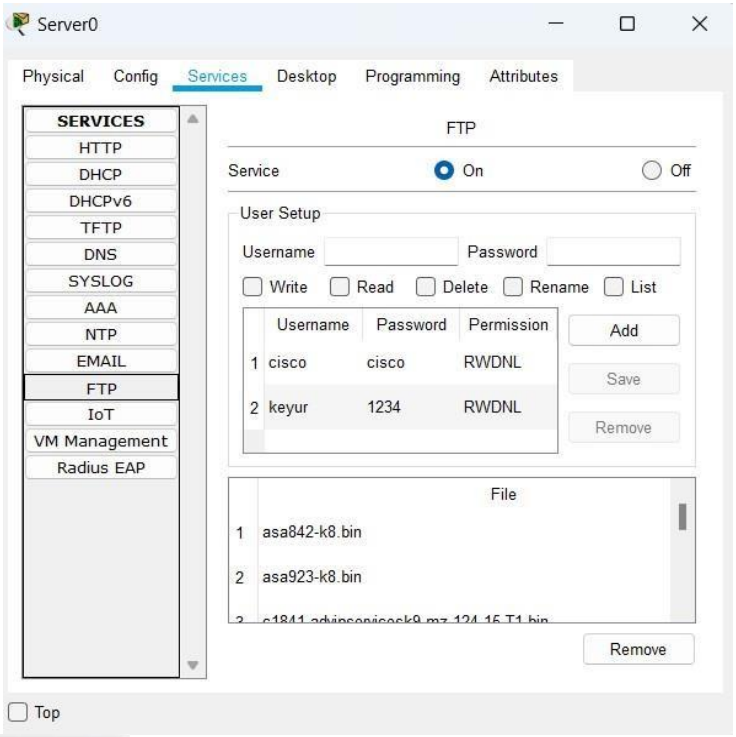


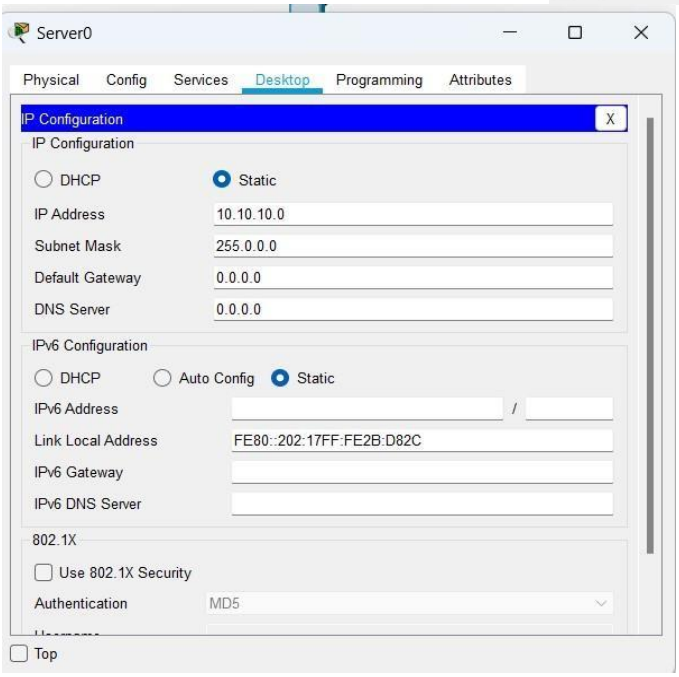


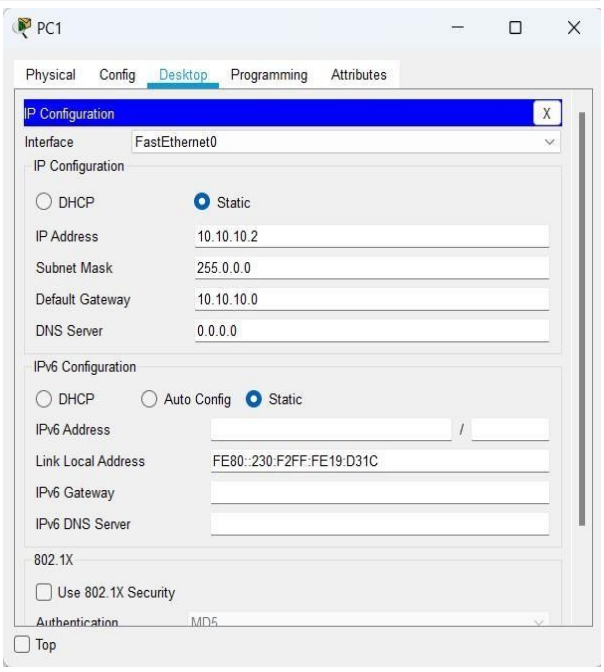
Date:31/07/2024

FTP:



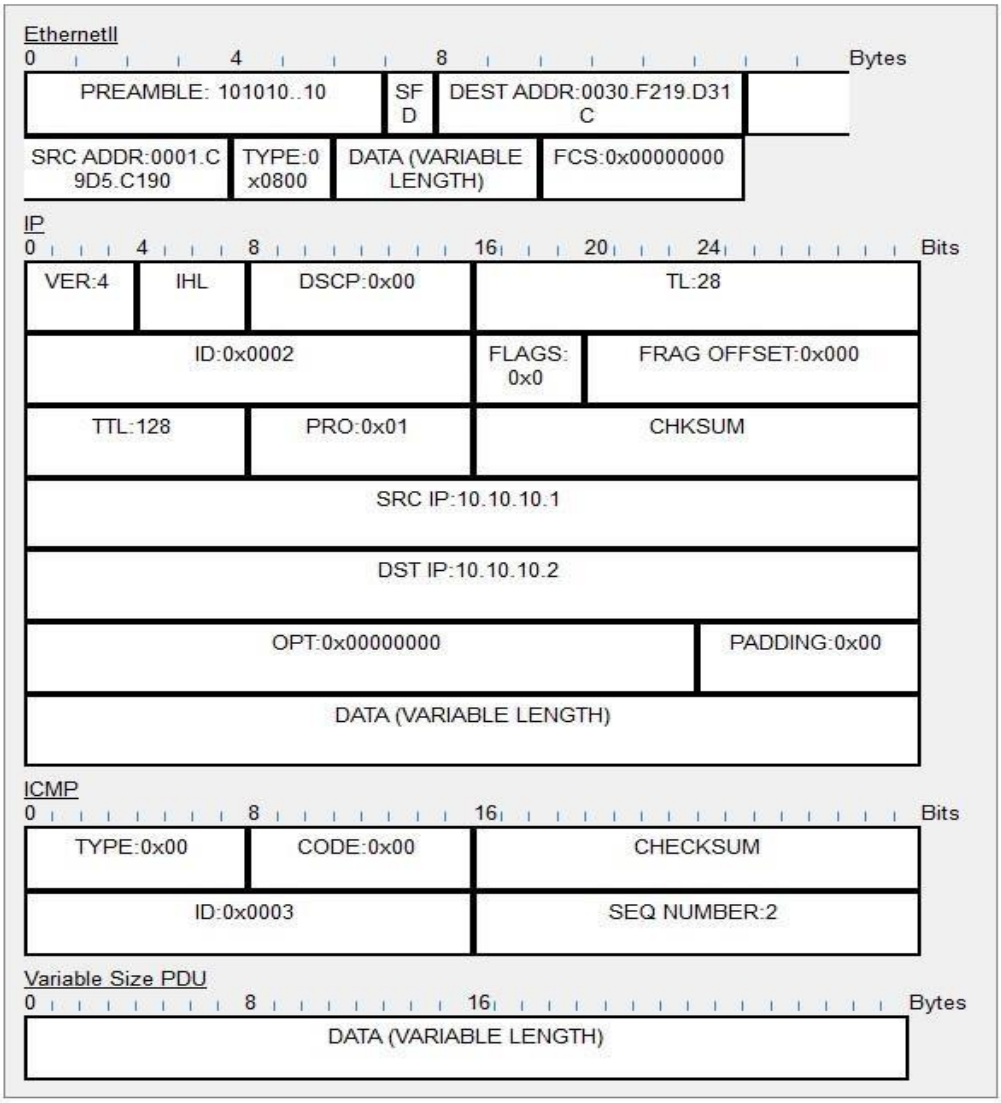






Date:31/07/2024

PDU Formats



Date:31/07/2024

```
C:\>ftp 10.10.10.0
Trying to connect...10.10.10.0
Connected to 10.10.10.0
220- Welcome to PT Ftp server
Username:keyur
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 10.10.10.0:
0    : asa842-k8.bin                                    5571584
1    : asa923-k8.bin                                    30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin           33591768
3    : c1841-ipbase-mz.123-14.T7.bin                    13832032
4    : c1841-ipbasek9-mz.124-12.bin                     16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin           33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin           33591768
7    : c2600-i-mz.122-28.bin                            5571584
8    : c2600-ipbasek9-mz.124-8.bin                      13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin         50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin          33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin                  5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                    15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin           33591768
14   : c2950-i6q412-mz.121-22.EA4.bin                   3058048
15   : c2950-i6q412-mz.121-22.EA8.bin                   3117390
16   : c2960-lanbase-mz.122-25.FX.bin                   4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin                 4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin                 4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin          8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin           10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin             33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin            83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin           505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG              159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG              184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin         160968869
27   : ir800-universalk9-mz.SPA.155-3.M                 61750062
28   : ir800-universalk9-mz.SPA.156-3.M                 63753767
29   : ir800_yocto-1.7.2.tar                            2877440
30   : ir800_yocto-1.7.2_python-2.7.3.tar               6912000
31   : pt1000-i-mz.122-28.bin                           5571584
32   : pt3000-i6q412-mz.121-22.EA4.bin                  3117390
ftp>put ck.html

Writing file ck.html to 10.10.10.0:
File transfer in progress...

[Transfer complete - 14 bytes]
```

Date: 14/08/2024

Himanshu Parmar
22010101132

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.*;
import java.net.*;

public class TCPServer {
    public static void main(String[] args) {
        try {
            ServerSocket serverSocket = new ServerSocket(3000);
            System.out.println("Server is listening on port 3000");

            Socket connectionSocket = serverSocket.accept();
            System.out.println("Client connected SucessFully");
            BufferedReader inFromClient = new BufferedReader(new
InputStreamReader(connectionSocket.getInputStream()));
t
            DataOutputStream outToClient = new
DataOutputStream(connectionSocket.getOutputStream());

            String clientSentence = inFromClient.readLine();
            System.out.println("Received from client: " + clientSentence);

            String capitalizedSentence = clientSentence.toUpperCase() + "\n";


            outToClient.writeBytes(capitalizedSentence);

            connectionSocket.close();
            serverSocket.close();
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```

Date: 14/08/2024

TCP Client Program:

```
import java.io.*;
import java.net.*;
public class TCPClient {
    public static void main(String[] args) {
        try {
            Socket clientSocket = new Socket("localhost", 3000);
            DataOutputStream outToServer = new
DataOutputStream(clientSocket.getOutputStream());
            BufferedReader inFromServer = new BufferedReader(new
InputStreamReader(clientSocket.getInputStream()));
            BufferedReader inFromUser = new BufferedReader(new
InputStreamReader(System.in));

            System.out.print("Enter text: ");
            String s = inFromUser.readLine();
            outToServer.writeBytes(s + "\n");
            String modifiedSentence = inFromServer.readLine();
            System.out.println("Received from server: " + modifiedSentence);

            clientSocket.close();
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```

Date: 14/08/2024

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) {
        try {
            DatagramSocket serverSocket = new DatagramSocket(9876);
            byte[] receiveData = new byte[1024];
            byte[] sendData = new byte[1024];

            while (true) {
                DatagramPacket receivePacket = new DatagramPacket(receiveData,
receiveData.length);
                serverSocket.receive(receivePacket);
                String sentence = new String(receivePacket.getData(), 0,
receivePacket.getLength());
                System.out.println("received: " + sentence);

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

                String capitalizedSentence = sentence.toUpperCase();
                sendData = capitalizedSentence.getBytes();

                DatagramPacket sendPacket = new DatagramPacket(sendData,
sendData.length, clientAddress, clientPort);
                serverSocket.send(sendPacket);
            }
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Date: 14/08/2024

UDP Client Program:

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

public class UDPClient {
    public static void main(String[] args) {
        try {
            DatagramSocket clientSocket = new DatagramSocket();
            InetAddress serverAddress = InetAddress.getByName("localhost");

            byte[] sendData;
            byte[] receiveData = new byte[1024];

            Scanner scanner = new Scanner(System.in);

            System.out.print("Enter a sentence: ");
            String sentence = scanner.nextLine();
            sendData = sentence.getBytes();

            DatagramPacket sendPacket = new DatagramPacket(sendData, sendData.length,
serverAddress, 9876);
            clientSocket.send(sendPacket);

            DatagramPacket receivePacket = new DatagramPacket(receiveData,
receiveData.length);
            clientSocket.receive(receivePacket);

            String modifiedSentence = new String(receivePacket.getData(), 0,
receivePacket.getLength());
            System.out.println("FROM SERVER: " + modifiedSentence);

            clientSocket.close();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Date: 21/08/2024

Himanshu Parmar
22010101132

Lab Practical #08:

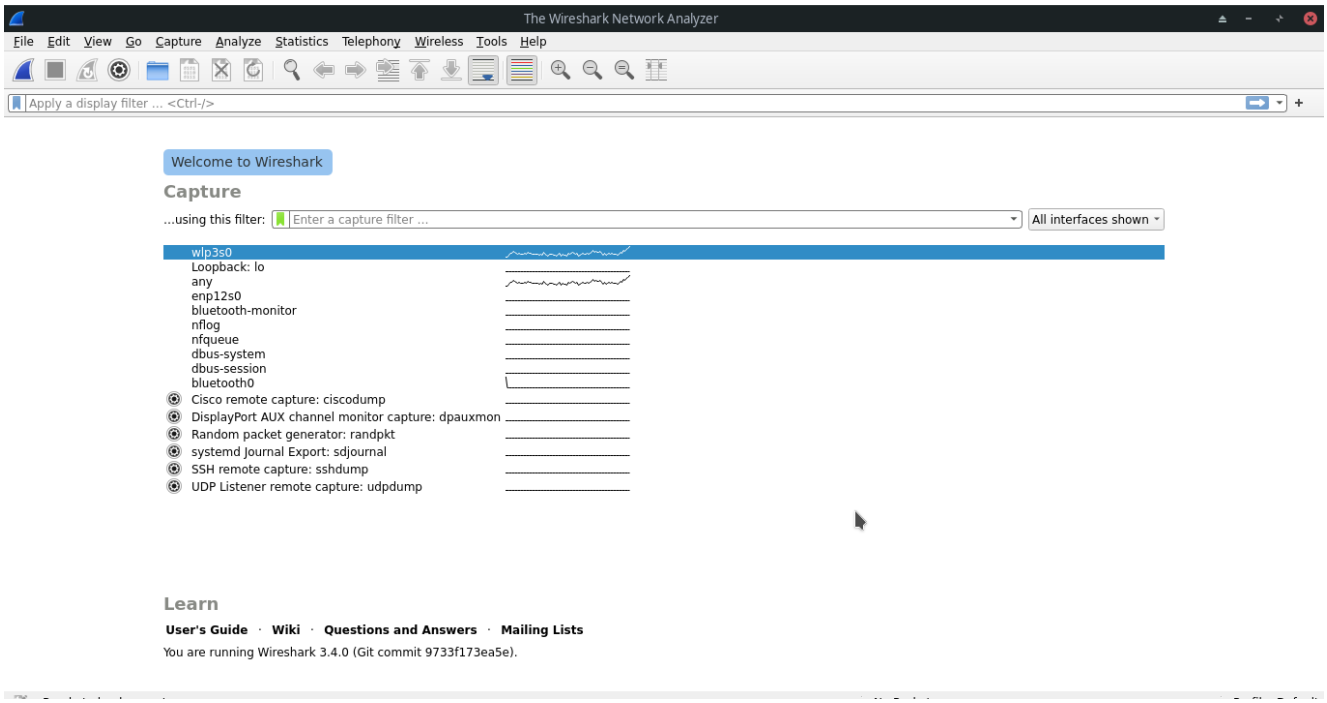
Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #08:

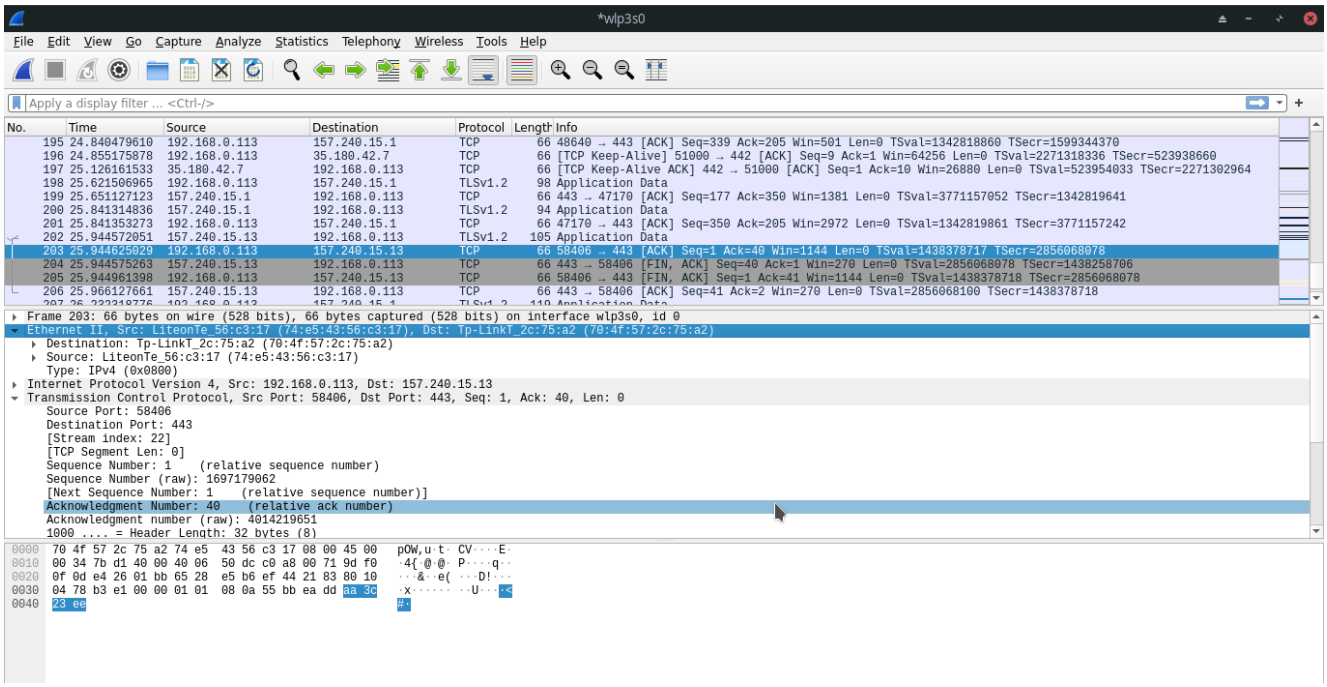
1. Explain usage of Wireshark tool.

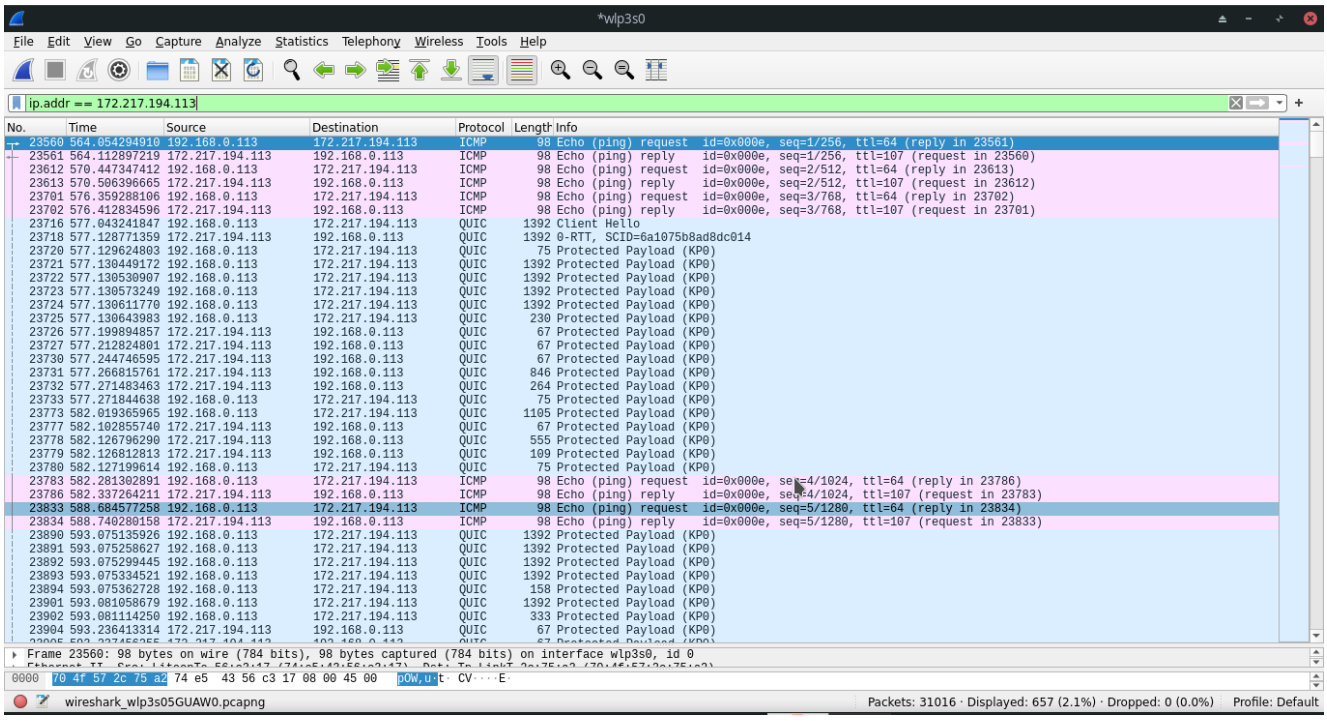
- Wireshark is a network protocol analyzer, which means it's an application that captures packets from a network connection, like the one between your computer and the internet or your home office. In a typical Ethernet network, a packet refers to a discrete unit of data.
- Wireshark serves multiple purposes, such as troubleshooting network performance issues. Cybersecurity professionals frequently use it to trace connections, examine the contents of suspicious network transactions, and identify bursts of network traffic. It's an essential tool in any IT professional's toolkit, provided they have the expertise to use it effectively.

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



Date: 21/08/2024





Date: 28/08/2024

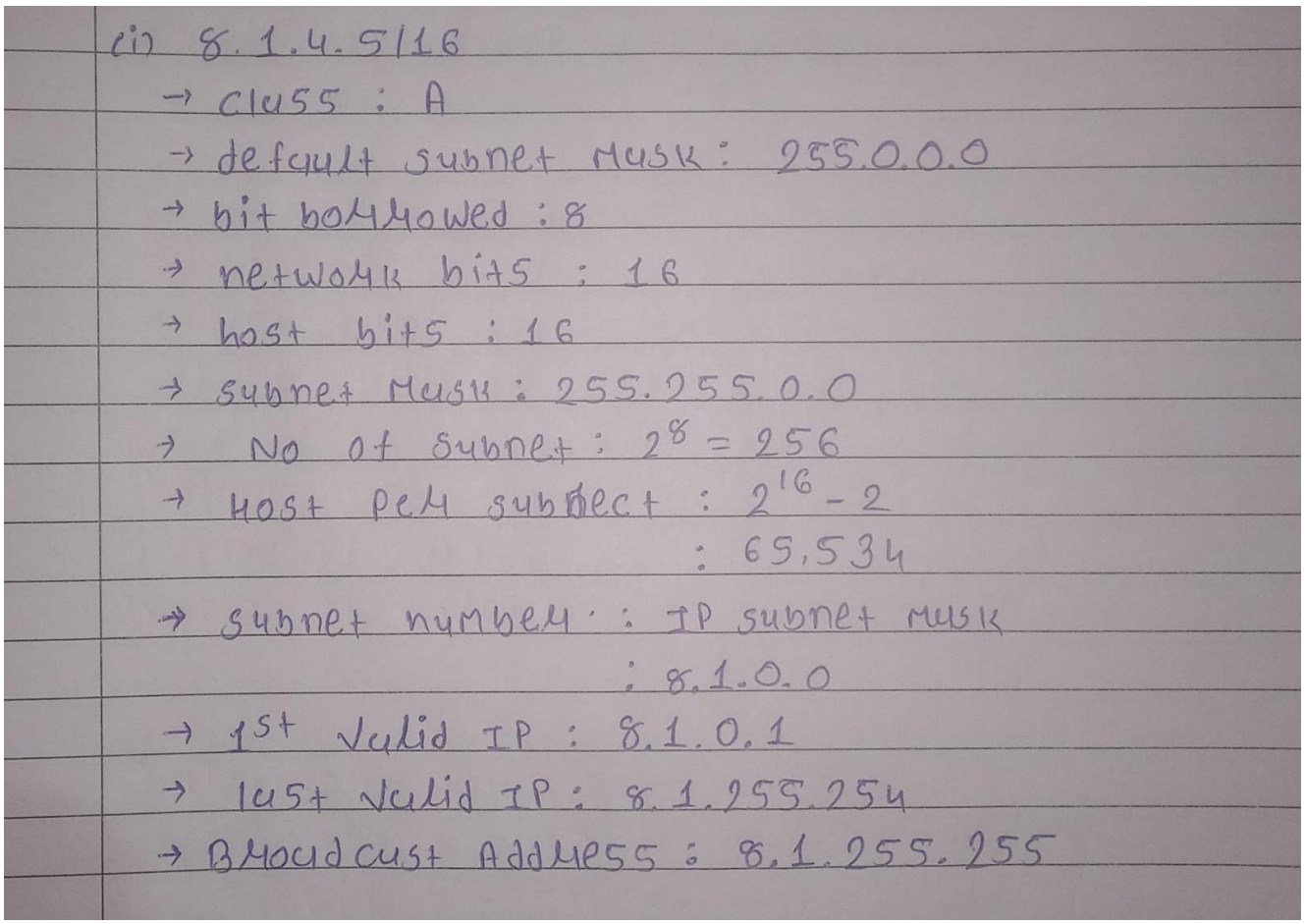
Himanshu Parmar
22010101132

Lab Practical #09:

Study of IP Addressing and sub-netting.

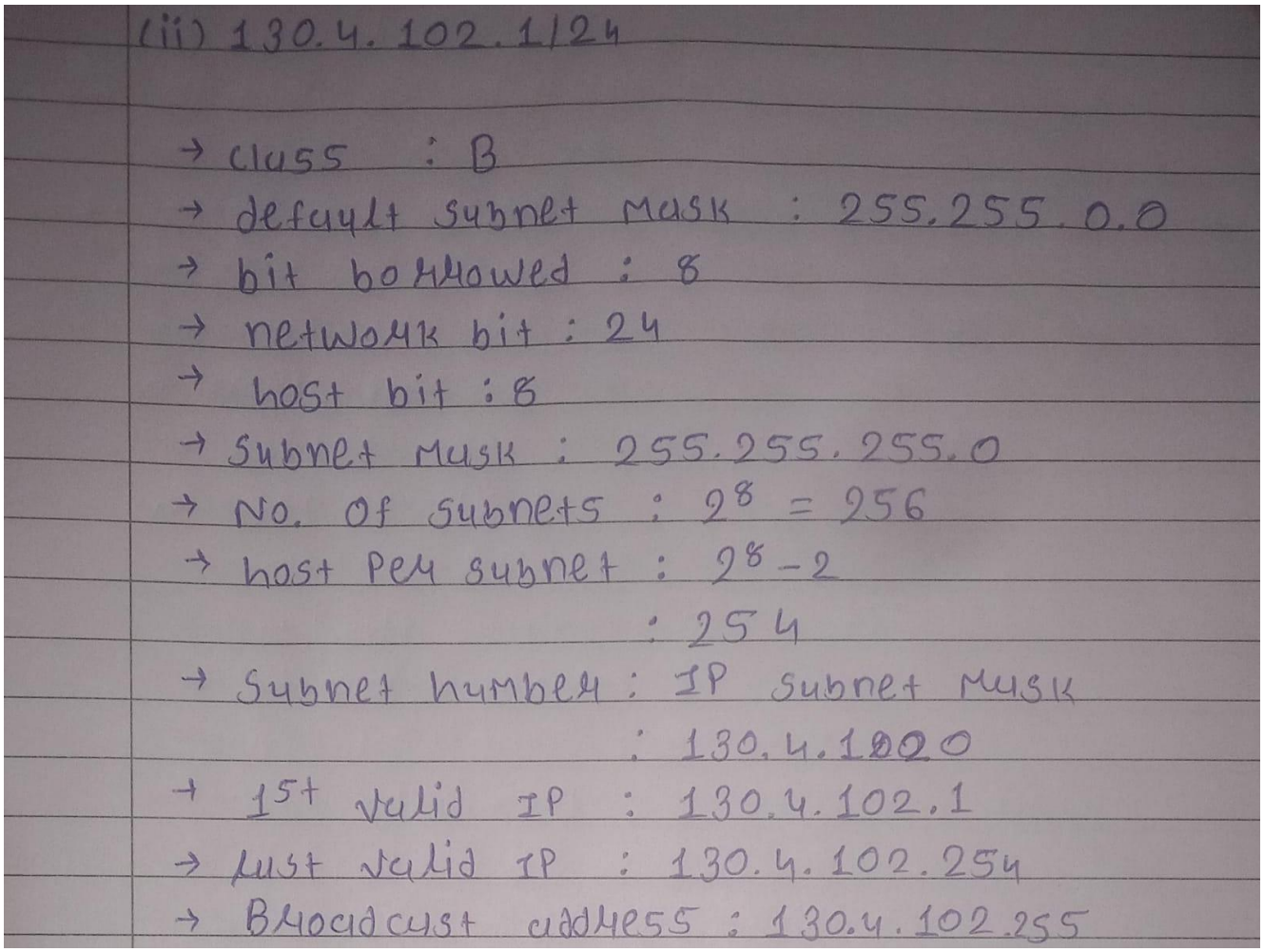
Practical Assignment #09:

1. Find default subnet marks, network bits, host bits, hosts per subnet, no of subnets, subnet number, 1st valid IP address, last valid IP address, and broadcast address.
   i. 8.1.4.5/16



Date: 28/08/2024

ii. 130.4.102.1/24



Date: 28/08/2024

iii. 199.1.1.1/24

(iii) 199.1.1.1/24

→ Class : C
→ default subnet mask : 255.255.255.0
→ bit borrowed : 0
→ network bits : 8
→ host per subnet : $2^8 - 2$
: 254
→ subnet mask : 255.255.255.0
→ No. of subnet : $2^0 = 1$
→ subnet number : IP & subnet mask
: 199.1.1.0
→ 1st valid IP : 199.1.1.1
→ Last valid IP : 189.1.1.254

Date: 28/08/2024

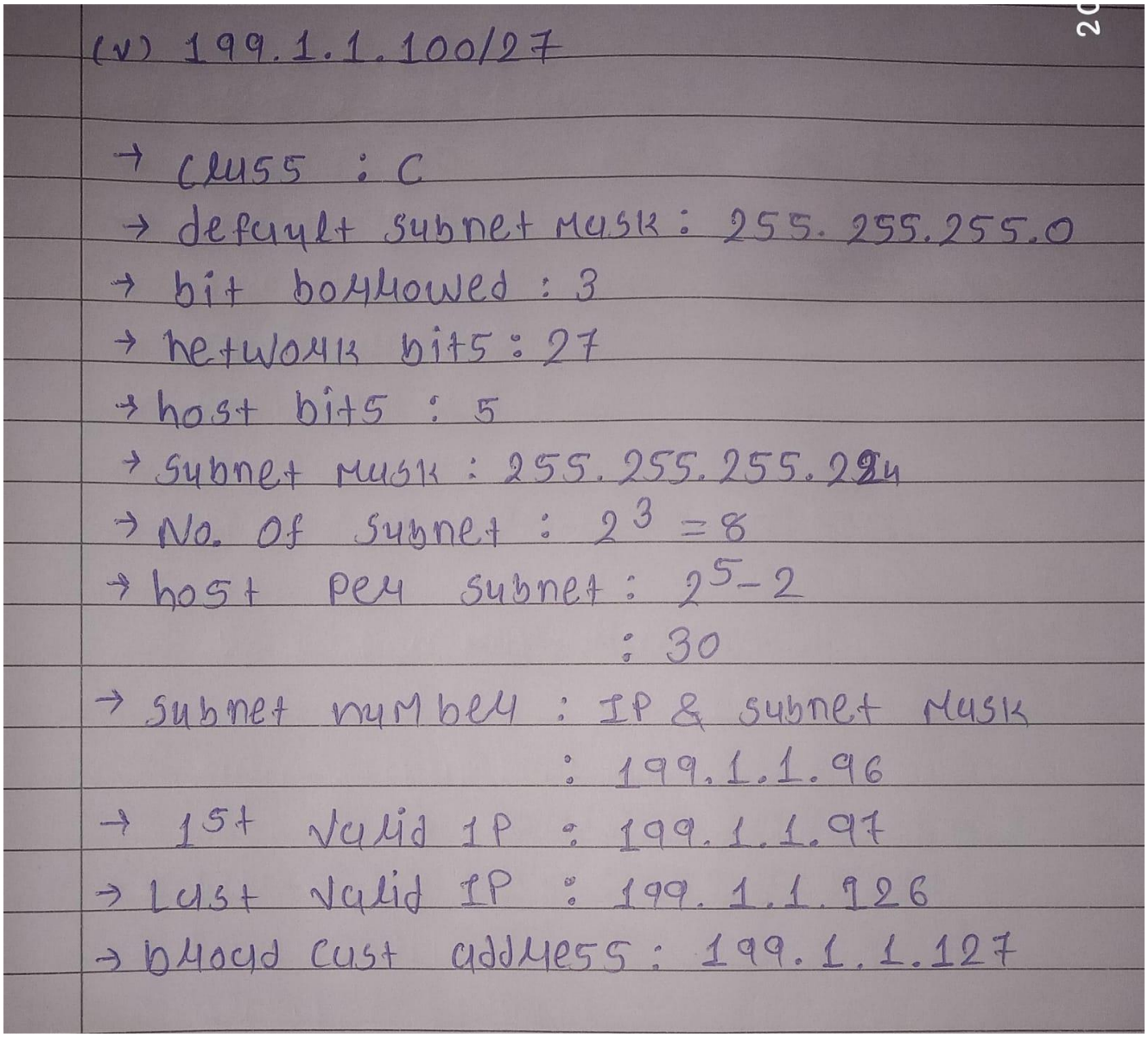
iv. 130.4.102.1/22

(iv) 130.4.102.1/22

→ class : B
→ default subnet mask : 255.255.0.0
→ bit borrowed : 6
→ network bit : 22
→ host bits : 10
→ subnet mask : 255.255.252.0
→ No. of subnet : $2^6 = 64$
→ host per subnet = $2^{10} - 2$
: 1022
→ subnet number : IP & subnet mask
: 130.4.100.0
→ 1st valid IP : 130.4.100.1
→ Last valid IP : 130.4.103.254
→ broadcast Address : 130.4.103.255

Date: 28/08/2024

v. 199.1.1.100/27

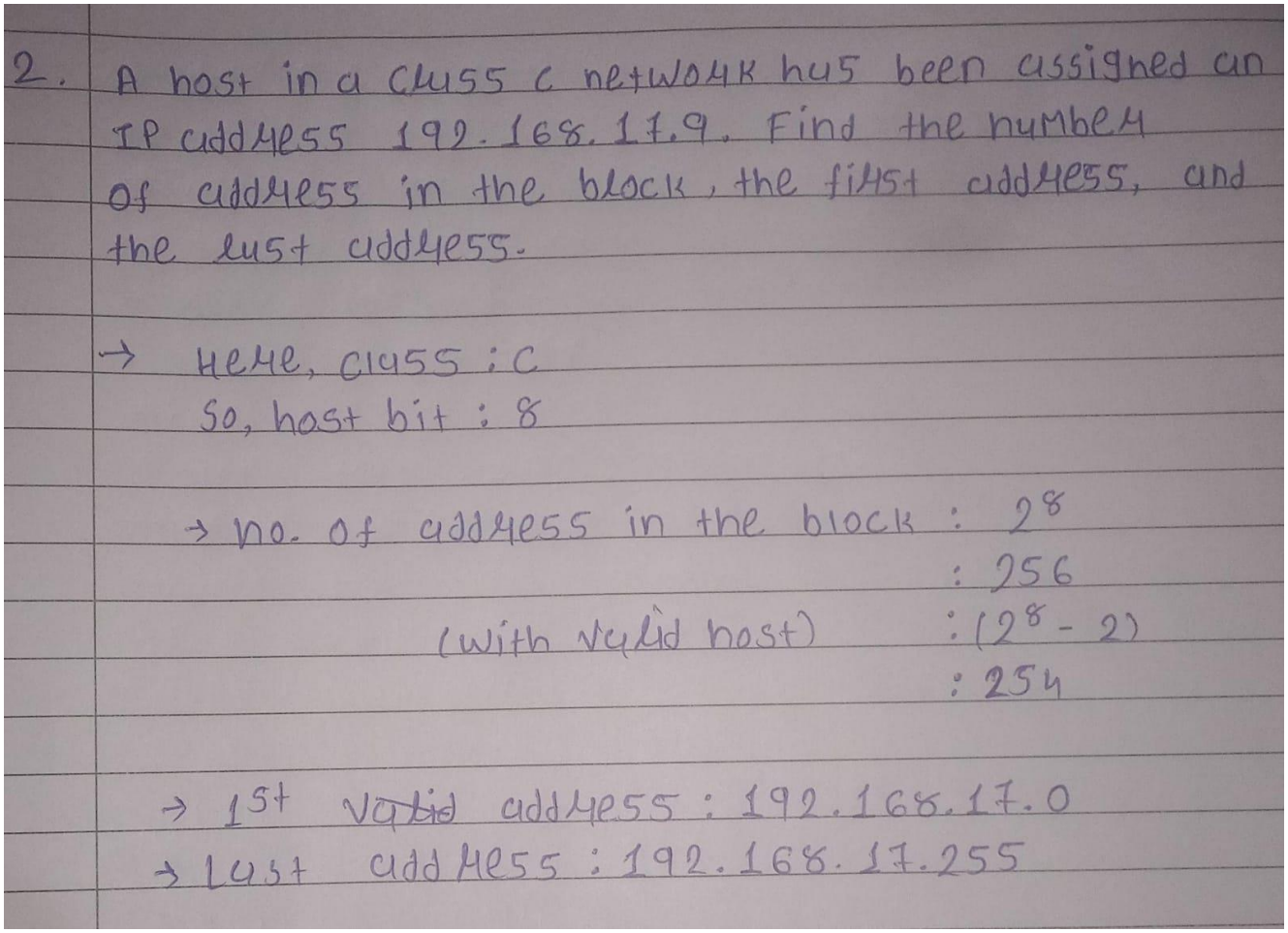


(v) 199.1.1.100/27

→ Class : C
→ default subnet Mask : 255.255.255.0
→ bit borrowed : 3
→ network bits : 27
→ host bits : 5
→ subnet Mask : 255.255.255.224
→ No. of subnet : $2^3 = 8$
→ host per subnet : $2^5 - 2$
: 30
→ subnet number : IP & subnet Mask
: 199.1.1.96
→ 1st valid IP : 199.1.1.97
→ last valid IP : 199.1.1.126
→ bhoad cast address : 199.1.1.127

Date: 28/08/2024

2. A host in a class C network has been assigned an IP address 192.168.17.9. Find the number of addresses in the block, the first address, and the last address.



2. A host in a class C network has been assigned an IP address 192.168.17.9. Find the number of address in the block, the first address, and the last address.

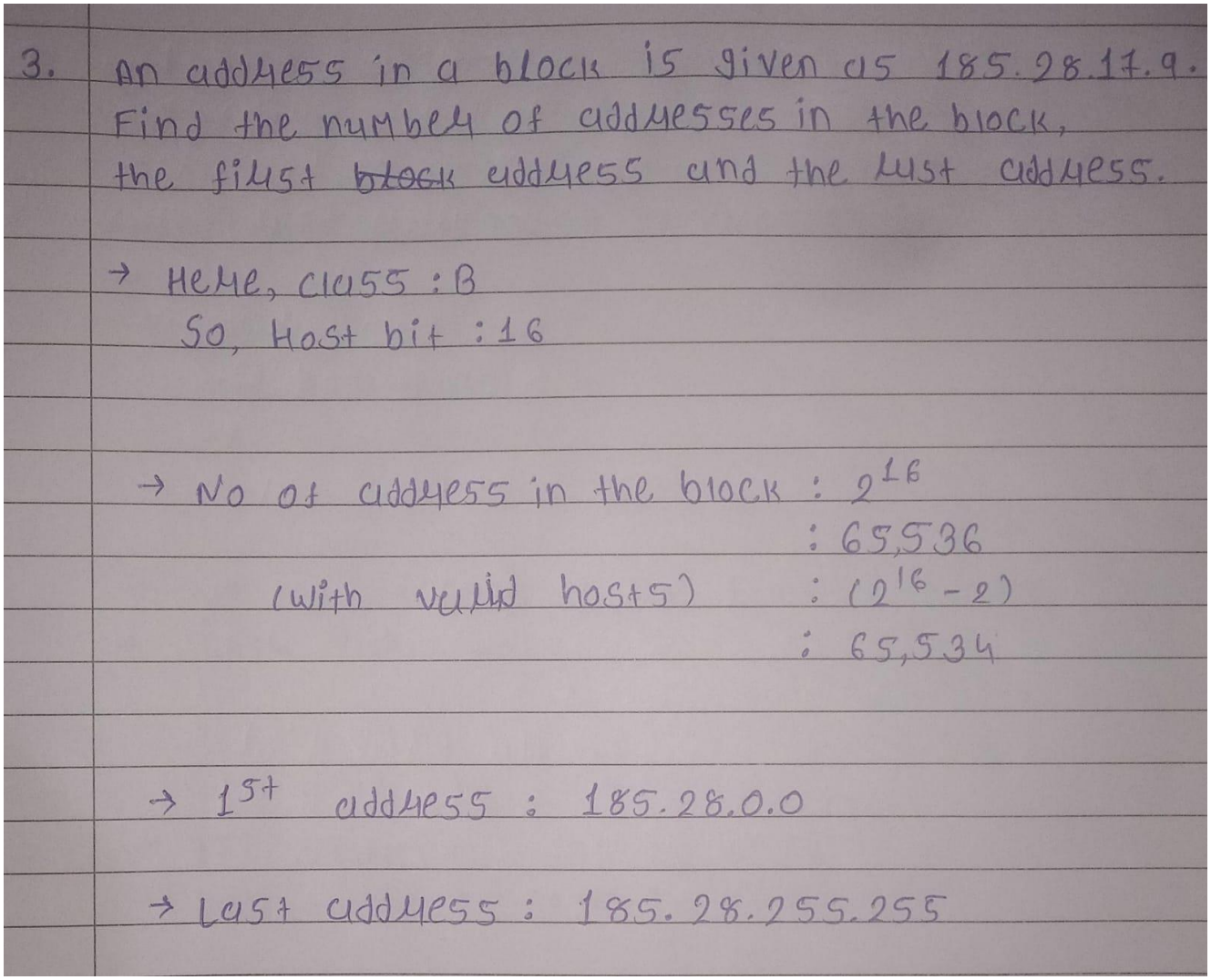
→ Here, class : C
So, host bit : 8

→ no. of address in the block : 2^8
: 256
(with valid host) : $(2^8 - 2)$
: 254

→ 1st valid address : 192.168.17.0
→ Last address : 192.168.17.255

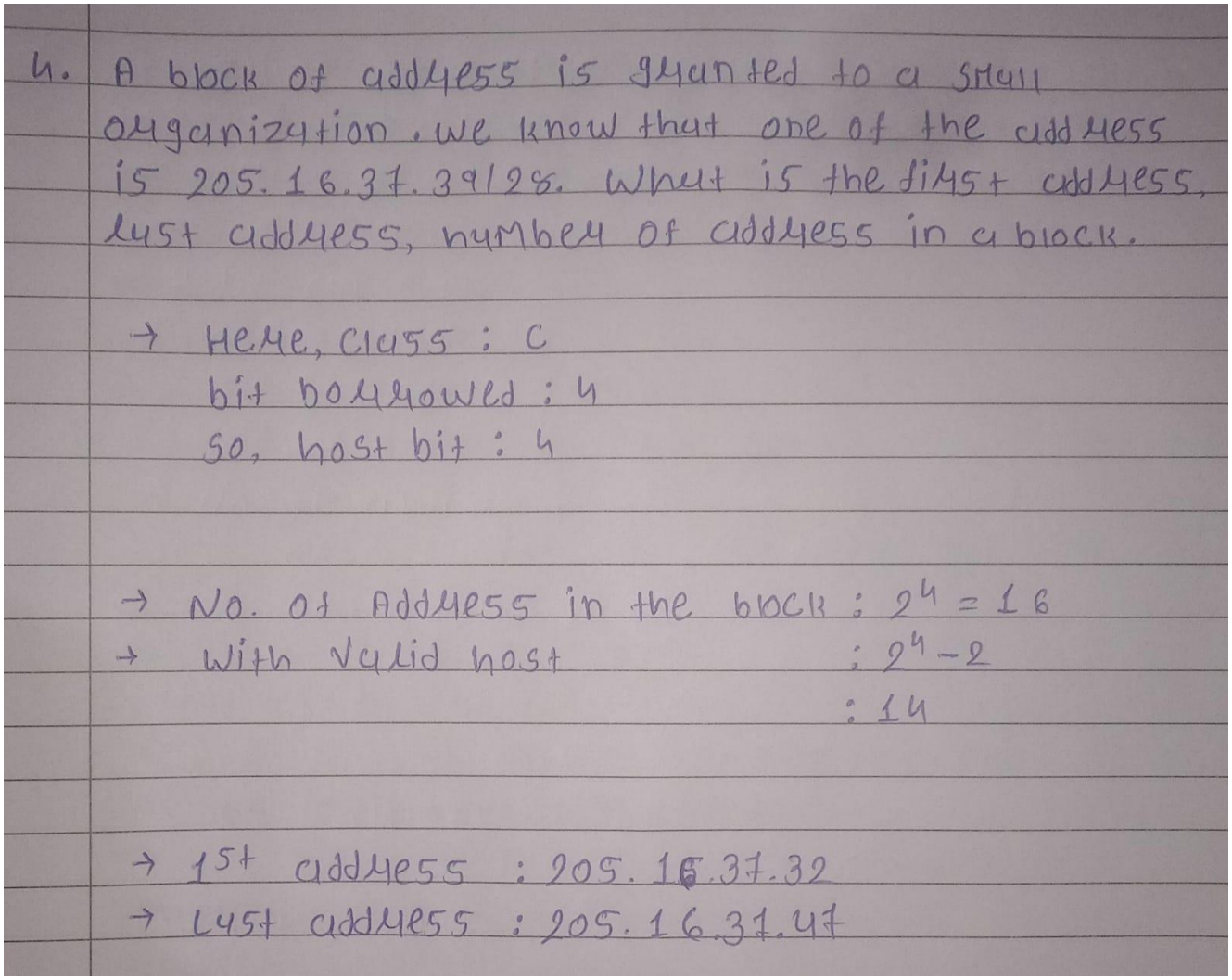
Date: 28/08/2024

3. An address in a block is given as 185.28.17.9. Find the number of addresses in the block, the first address, and the last address.



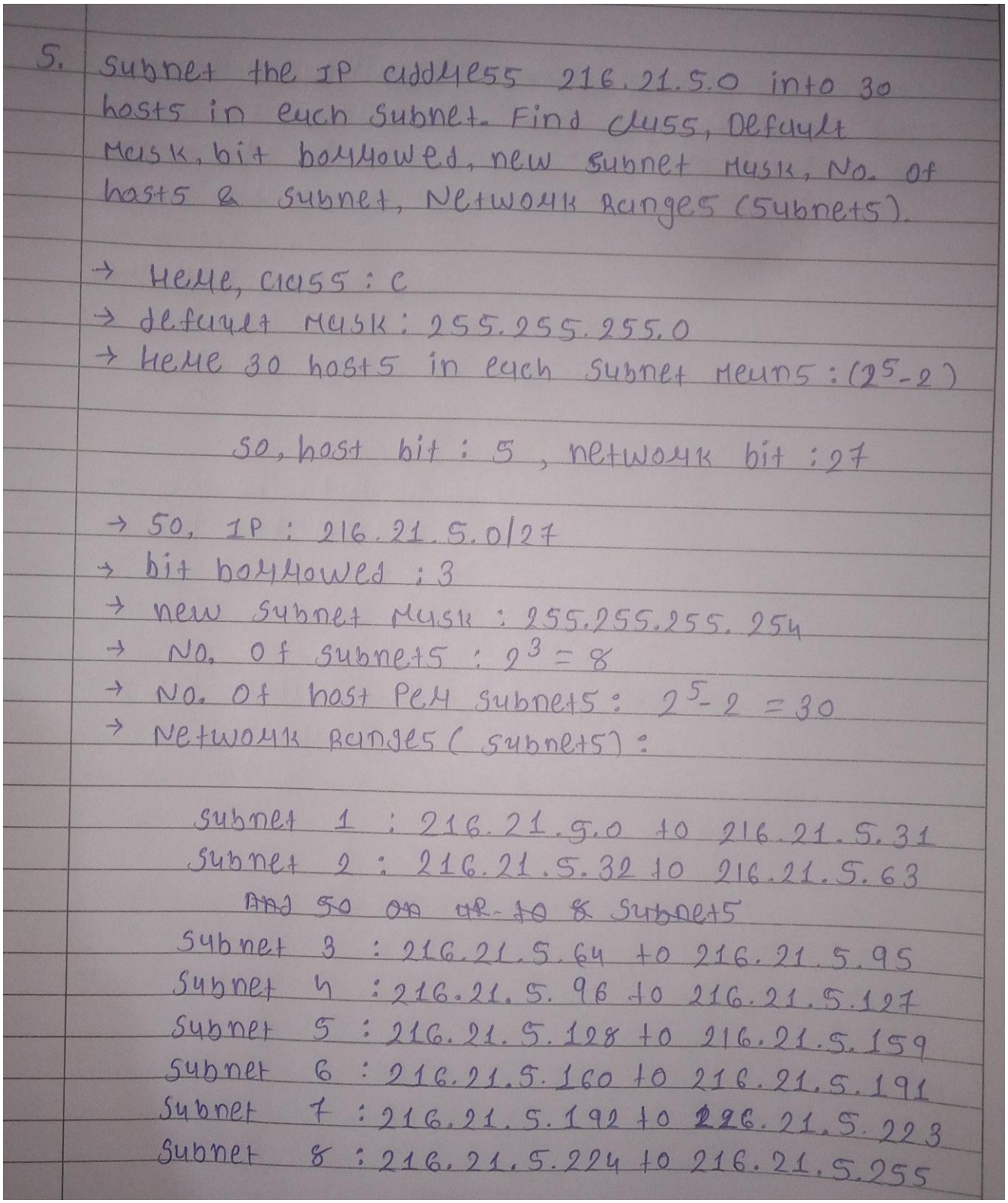
Date: 28/08/2024

4. A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address, last address, number of addresses in a block.



Date: 28/08/2024

5. Subnet the IP address 216.21.5.0 into 30 hosts in each subnet. Find Class, Default Mask, Bit Borrowed, New subnet mask, No. of Hosts & Subnet, Network Ranges (Subnets).



5. Subnet the IP address 216.21.5.0 into 30 hosts in each subnet. Find class, Default Mask, bit borrowed, new subnet mask, No. of hosts & subnet, Network Ranges (Subnets).

→ Here, class : C
→ default Mask : 255.255.255.0
→ Here 30 hosts in each subnet means : $(2^5 - 2)$

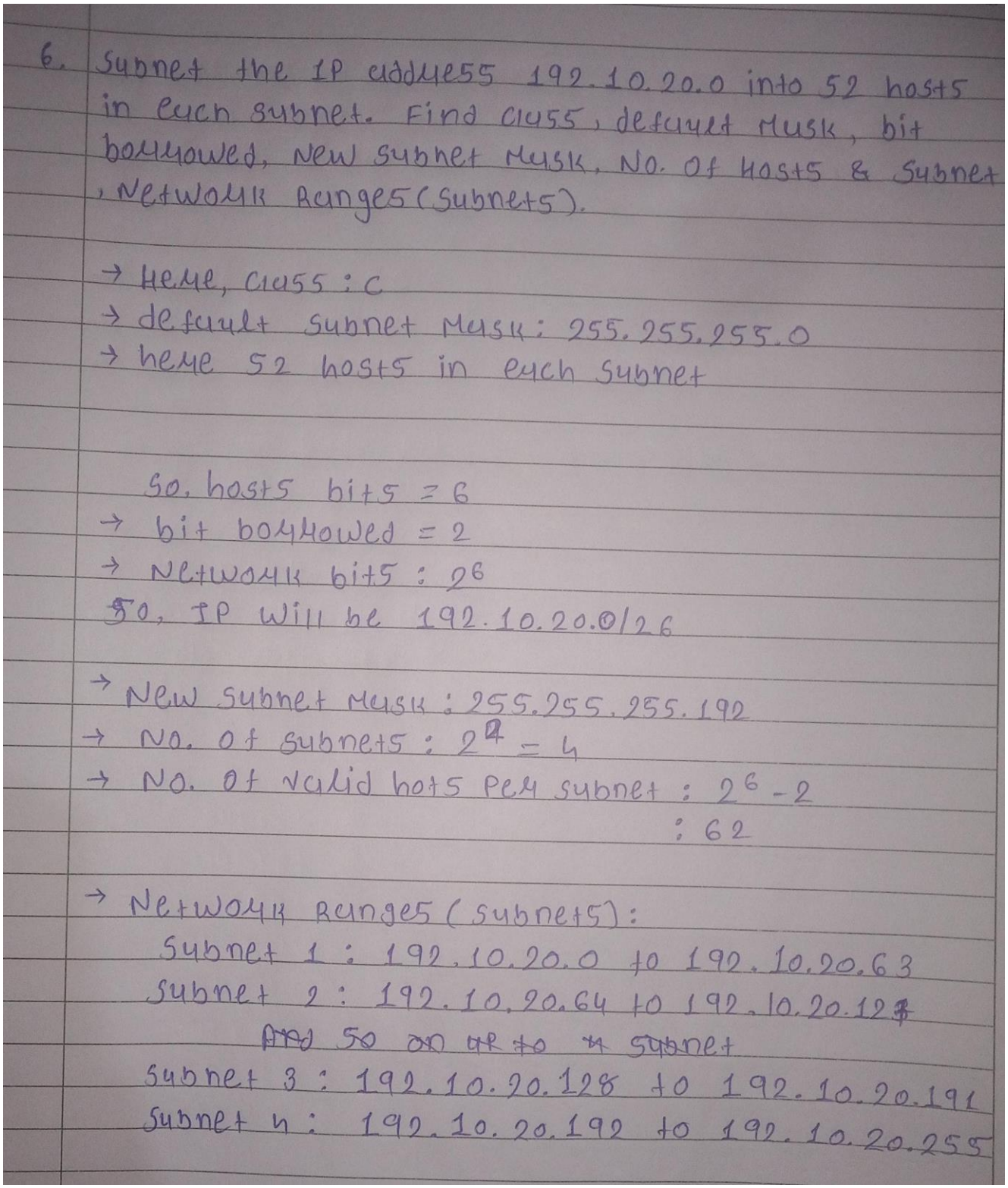
So, host bit : 5 , network bit : 27

→ So, IP : 216.21.5.0/27
→ bit borrowed : 3
→ new subnet Mask : 255.255.255.254
→ No. of subnets : $2^3 = 8$
→ No. of host Per subnets : $2^5 - 2 = 30$
→ Network Ranges (subnets) :

subnet 1 : 216.21.5.0 to 216.21.5.31
subnet 2 : 216.21.5.32 to 216.21.5.63
And so on upto 8 subnets
subnet 3 : 216.21.5.64 to 216.21.5.95
subnet 4 : 216.21.5.96 to 216.21.5.127
subnet 5 : 216.21.5.128 to 216.21.5.159
subnet 6 : 216.21.5.160 to 216.21.5.191
subnet 7 : 216.21.5.192 to 216.21.5.223
subnet 8 : 216.21.5.224 to 216.21.5.255

Date: 28/08/2024

6. Subnet the IP address 192.10.20.0 into 52 hosts in each subnet. Find Class, Default Mask, Bit Borrowed, New subnet mask, No. of Hosts & Subnet, Network Ranges (Subnets).



6. Subnet the IP address 192.10.20.0 into 52 hosts in each subnet. Find class, default mask, bit borrowed, New subnet mask, No. of Hosts & Subnet, Network Ranges (Subnets).

→ Here, Class : C
→ default subnet Mask : 255.255.255.0
→ here 52 hosts in each subnet

So, hosts bits = 6
→ bit borrowed = 2
→ Network bits : 2^6
So, IP will be 192.10.20.0/26

→ New subnet Mask : 255.255.255.192
→ No. of subnets : $2^2 = 4$
→ No. of valid hots per subnet : $2^6 - 2$
: 62

→ Network Ranges (subnets):
Subnet 1 : 192.10.20.0 to 192.10.20.63
Subnet 2 : 192.10.20.64 to 192.10.20.127
~~And~~ so on upto to 4th subnet
Subnet 3 : 192.10.20.128 to 192.10.20.191
Subnet 4 : 192.10.20.192 to 192.10.20.255

Date:11/09/2024

Himanshu Parmar
22010101132

Lab Practical #10:

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

Practical Assignment #10:

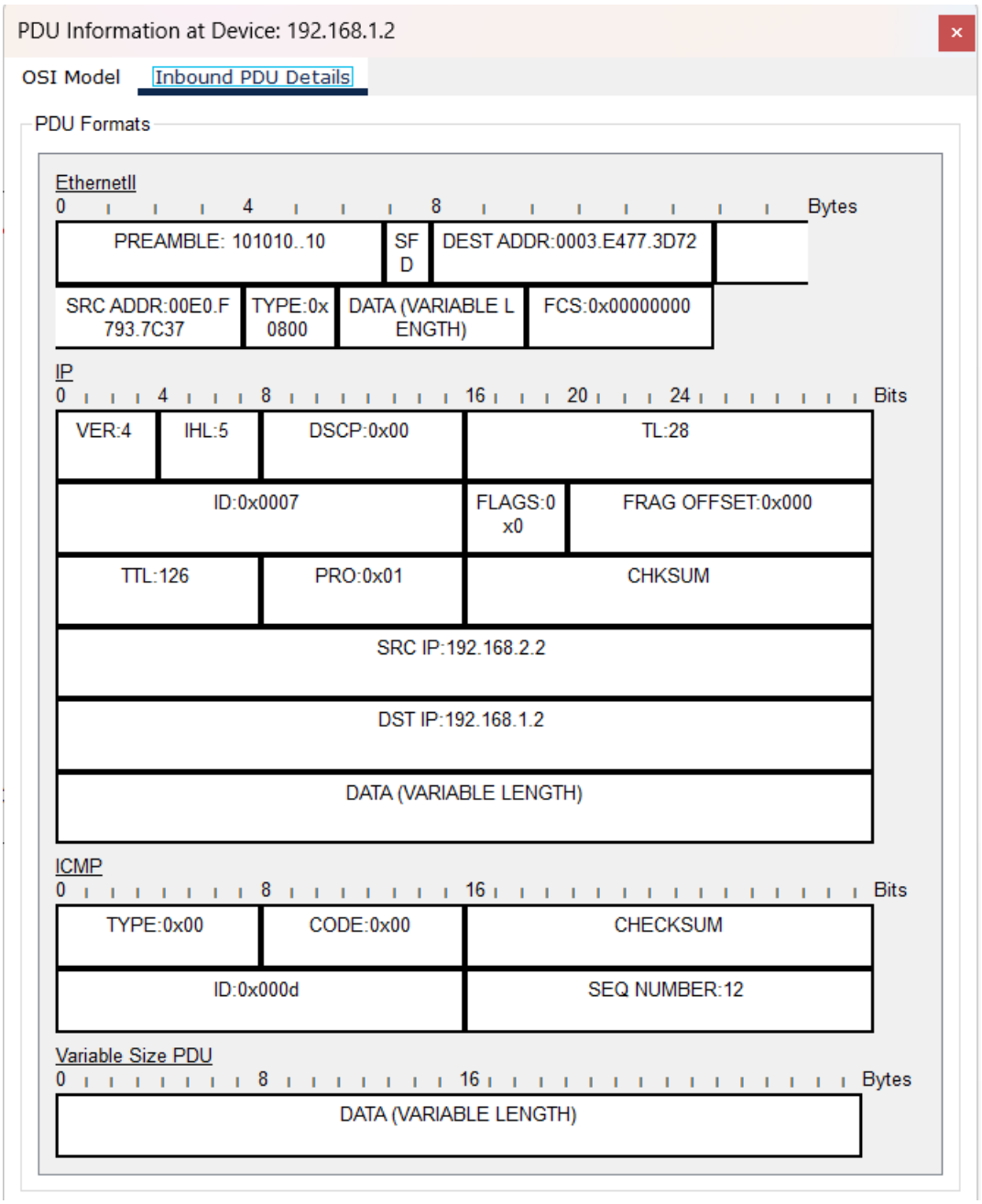
1. Connect the two different networks based on the calculated IP addresses and subnet using a packet tracer.

Device	IPv4 Address	Subnet Mask	Default Gateway
192.168.1.2	192.168.1.2	255.255.255.0	192.168.1.1
192.168.1.3	192.168.1.3	255.255.255.0	192.168.1.1
192.168.2.2	192.168.2.2	255.255.255.0	192.168.2.1
192.168.2.3	192.168.2.3	255.255.255.0	192.168.2.1

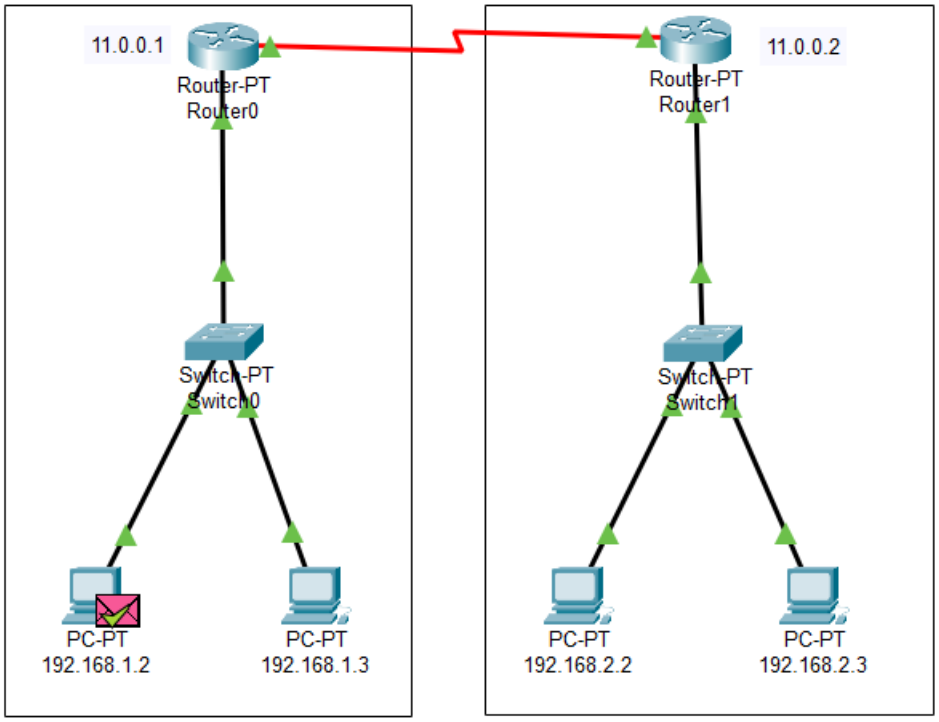
Date:11/09/2024

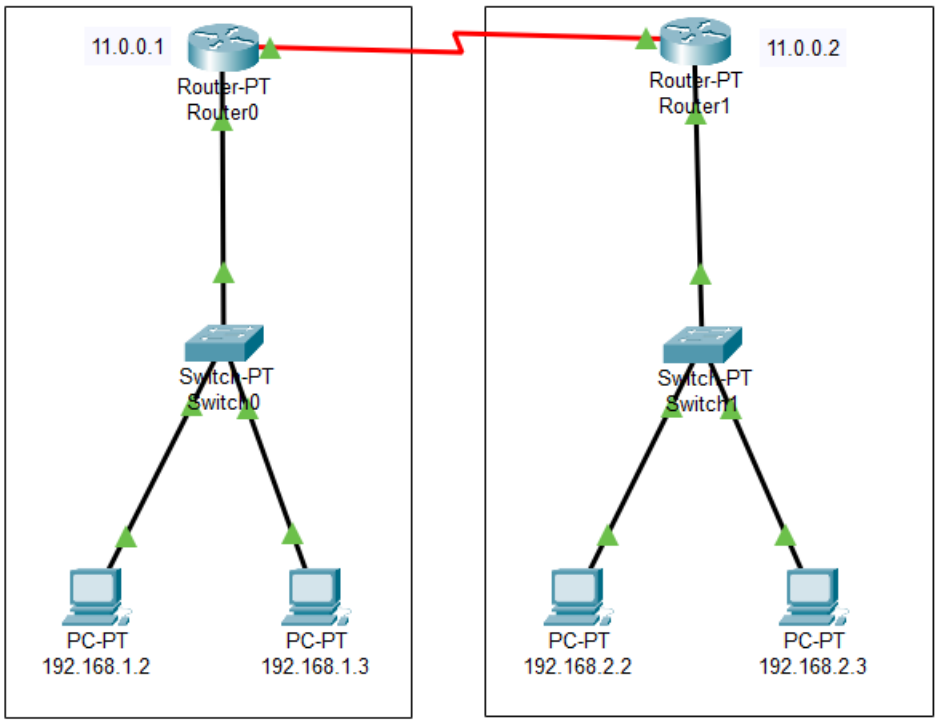
Device	Interface	IPv4 Addressing	Subnet Mask
11.0.0.1	FastEthernet0/0	192.168.1.1	255.255.255.0
	Serial2/0	11.0.0.1	255.255.255.0
11.0.0.2	FastEthernet0/0	192.168.2.1	255.255.255.0
	Serial2/0	11.0.0.2	255.255.255.0

Date:11/09/2024



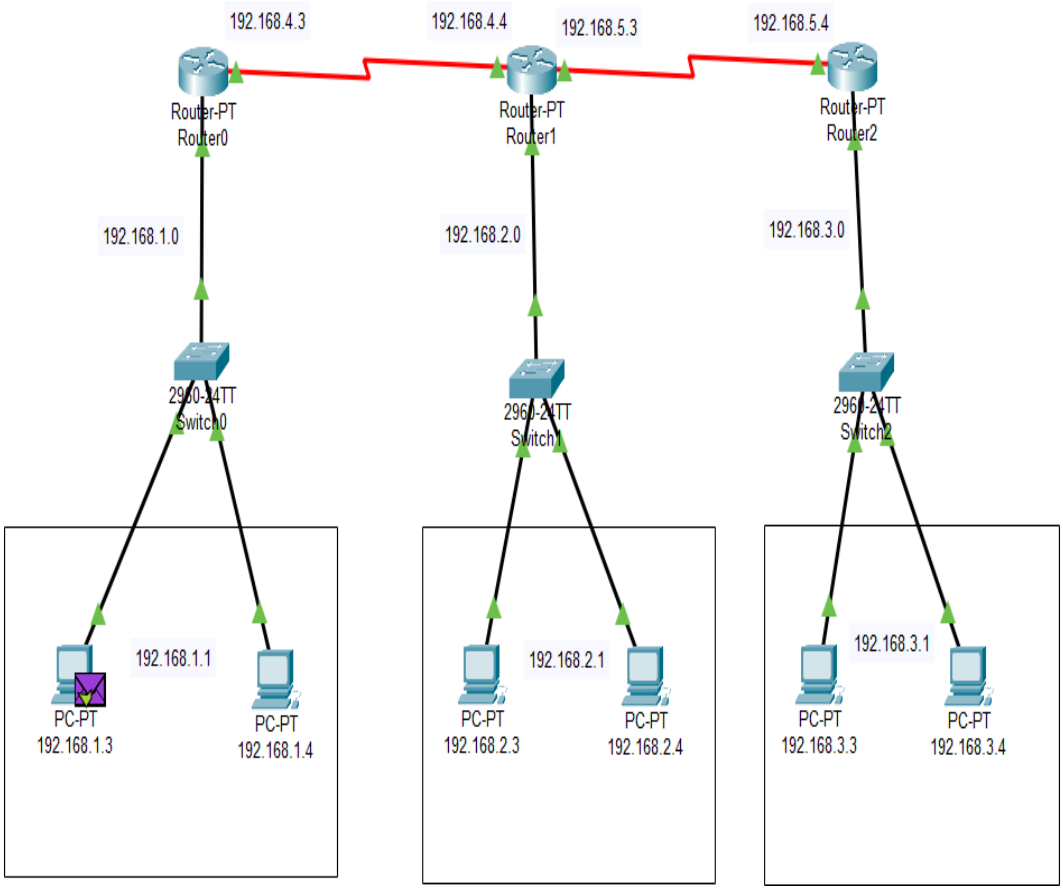
Date:11/09/2024

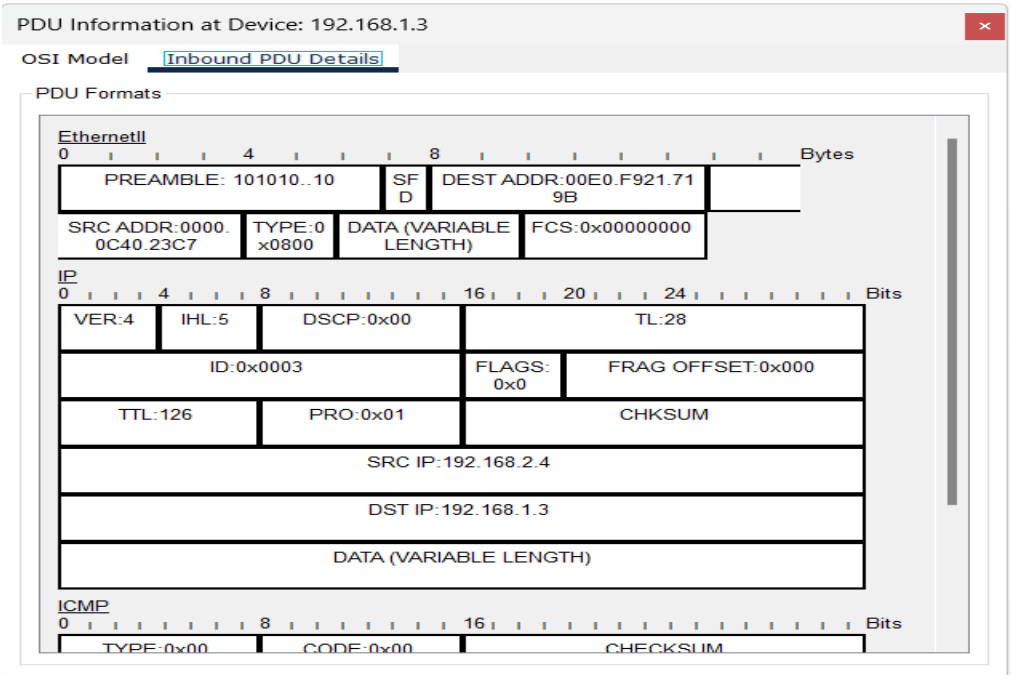




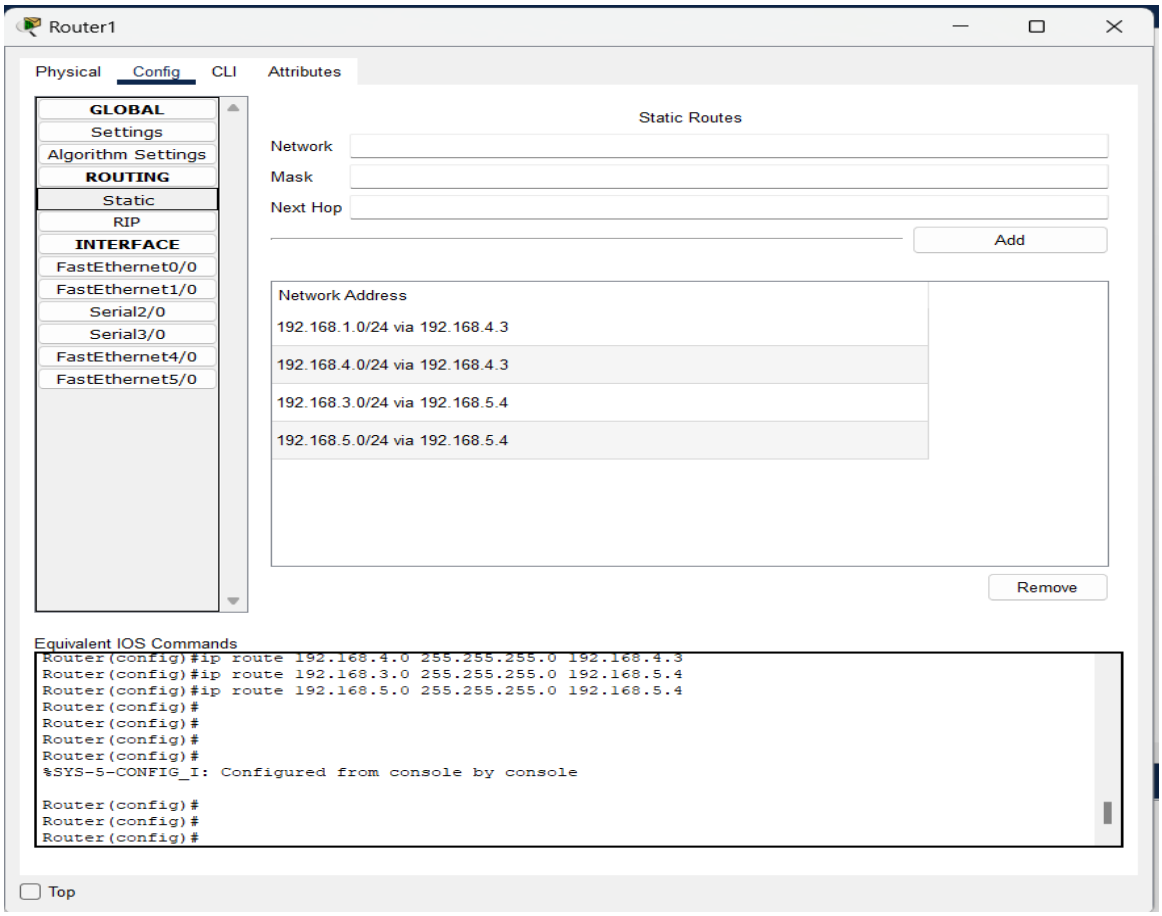
Date:11/09/2024

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





Date:11/09/2024



Date:11/09/2024

Himanshu Parmar
22010101132

Lab Practical #11:

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

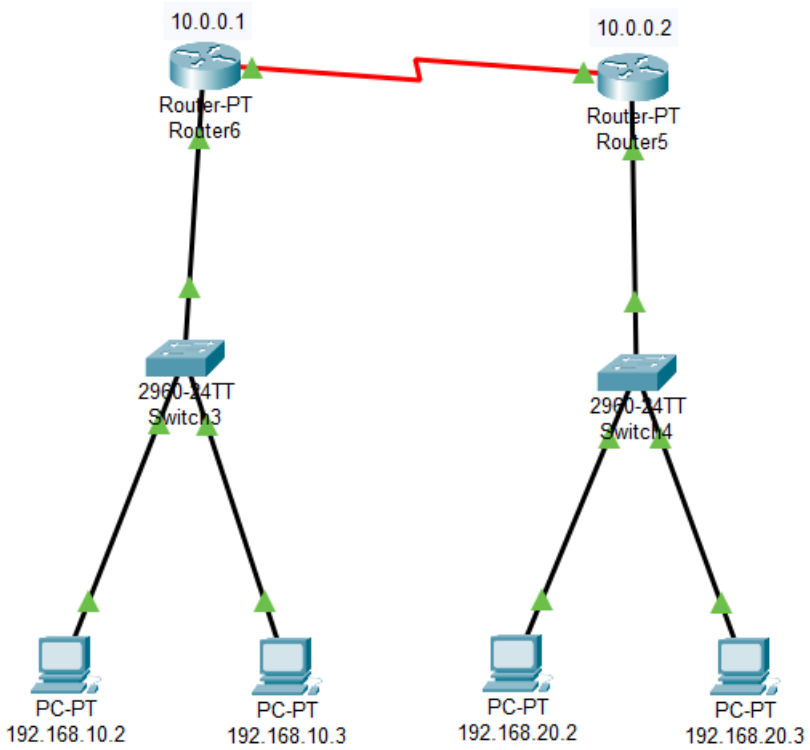
Practical Assignment #11:

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

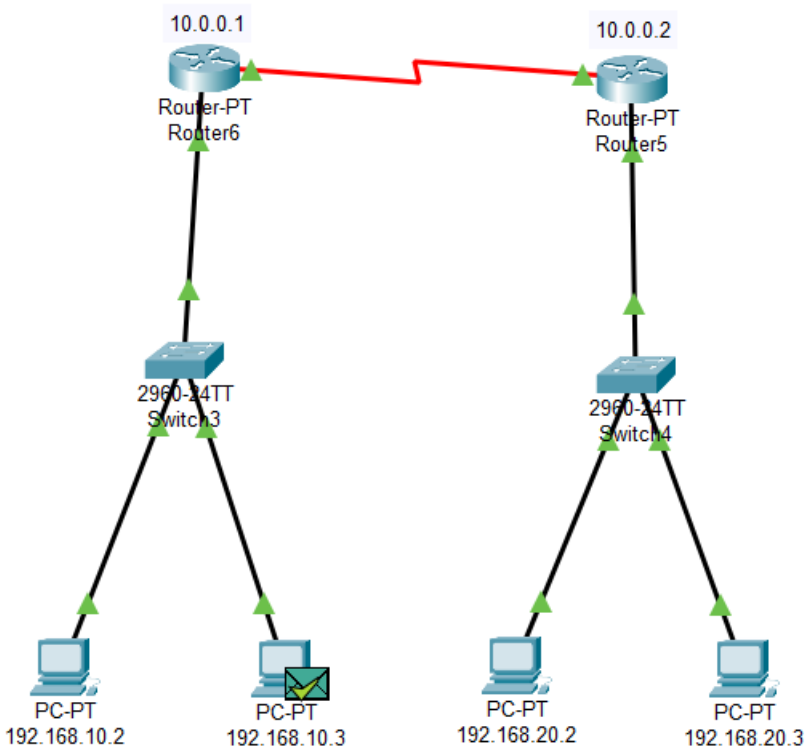
Device	IPv4 Address	Subnet-Mask	Default-Gateway
192.168.10.2	192.168.10.2	255.255.255.0	192.168.10.1
192.168.10.3	192.168.10.3	255.255.255.0	192.168.10.1
192.168.20.2	192.168.20.2	255.255.255.0	192.168.20.1
192.168.20.3	192.168.20.3	255.255.255.0	192.168.20.1

Date:11/09/2024

Device	Interface	IPv4 Address	Subnet Mask
10.0.0.1	FastEthernet0/0	192.168.10.1	255.255.255.0
	Serial 2/0	10.0.0.1	255.0.0.0
10.0.0.2	FastEthernet0/0	192.168.20.1	255.255.255.0
	Serial 2/0	10.0.0.2	255.0.0.0



Date:11/09/2024



Date:11/09/2024

PDU Information at Device: 192.168.10.3

OSI Model | Inbound PDU Details

PDU Formats

Ethernetll

0	4	8	Bytes
PREAMBLE: 101010..10	SFD	DEST ADDR:0030.A37E.638B	
SRC ADDR:00E0.A3B3.70EA	TYPE:0x0800	DATA (VARIABLE LENGTH)	FCS:0x00000000

IP

0	4	8	16	20	24	Bits
VER:4	IHL:5	DSCP:0x00	TL:28			
ID:0x0006			FLAGS:0x0	FRAG OFFSET:0x000		
TTL:126	PRO:0x01	CHKSUM				
SRC IP:192.168.20.2						
DST IP:192.168.10.3						
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	Bits
TYPE:0x00	CODE:0x00	CHECKSUM	
ID:0x0004		SEQ NUMBER:3	

Variable Size PDU

0	8	16	Bytes
DATA (VARIABLE LENGTH)			

Date:11/09/2024

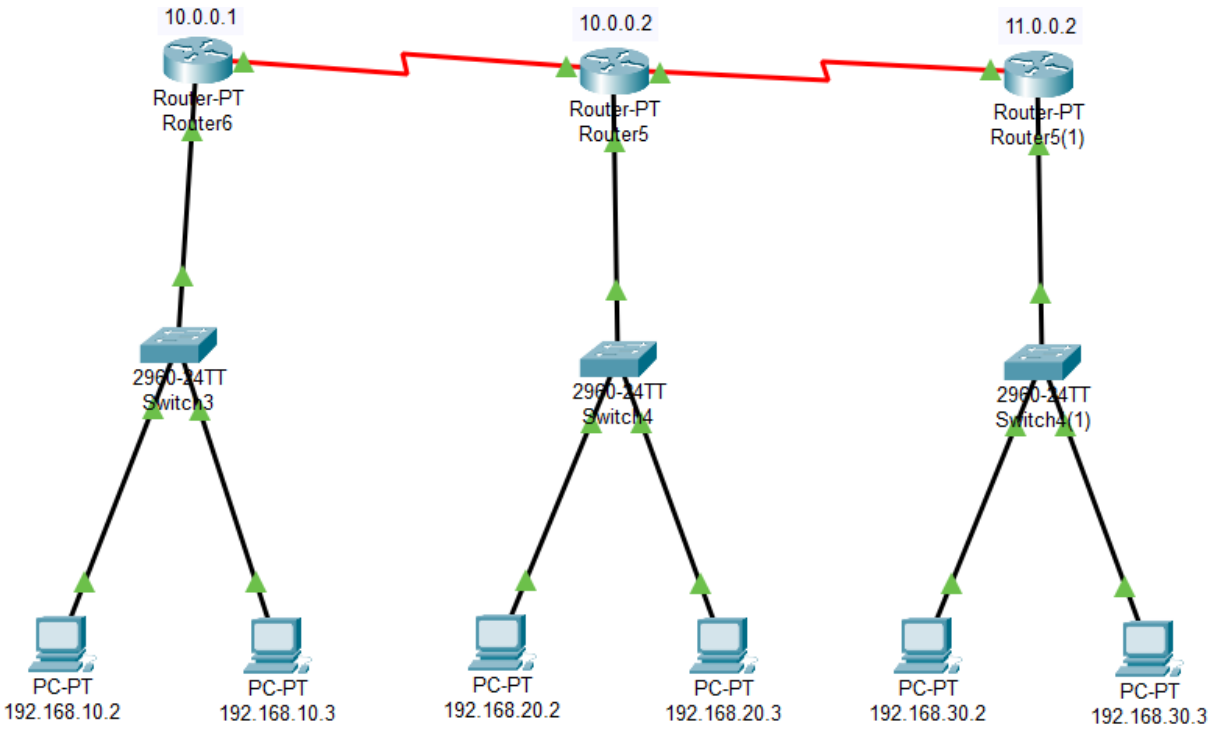
2. Connect the three different networks based on the calculated IP addresses and subnet using a packet tracer.

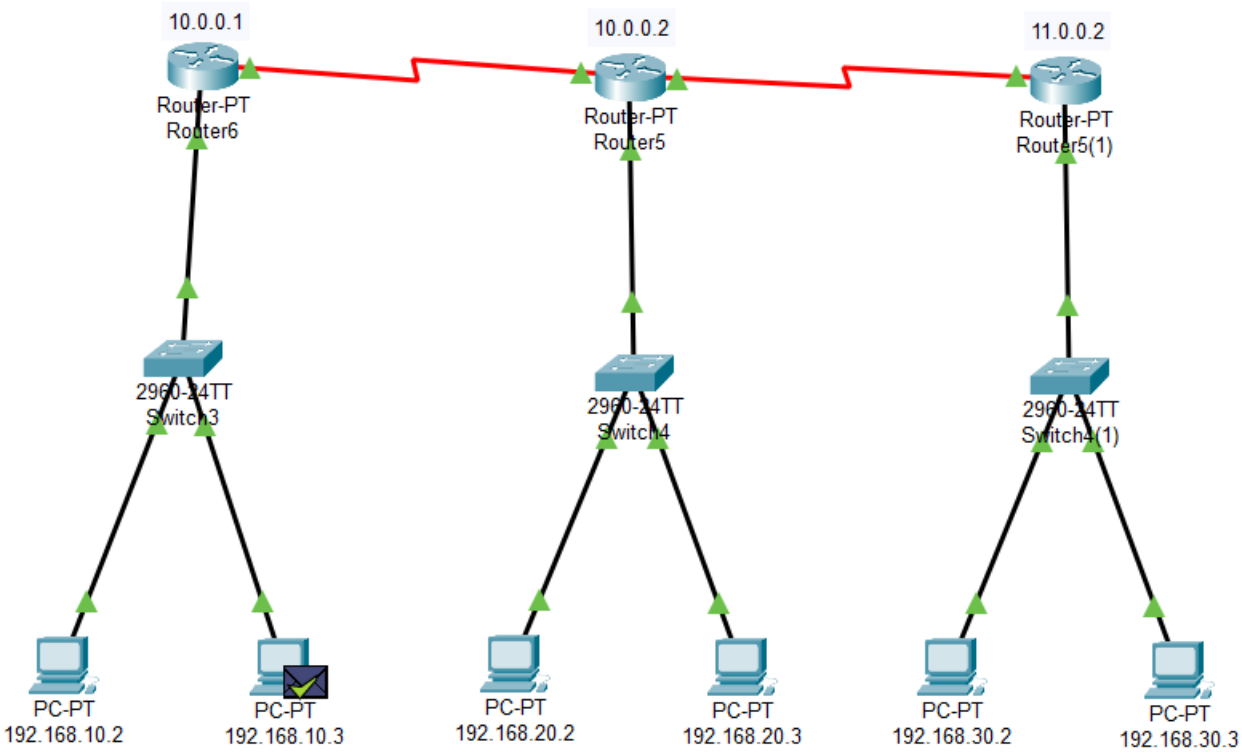
Device	IPv4 Address	Subnet mask	Default Gateway
192.168.10.2	192.168.10.2	255.255.255.0	192.168.10.1
192.168.10.3	192.168.10.3	255.255.255.0	192.168.10.1
192.168.20.2	192.168.20.2	255.255.255.0	192.168.20.1
192.168.20.3	192.168.20.3	255.255.255.0	192.168.20.1
192.168.30.2	192.168.30.2	255.255.255.0	192.168.30.1
192.168.30.3	192.168.30.3	255.255.255.0	192.168.30.1

Date:11/09/2024

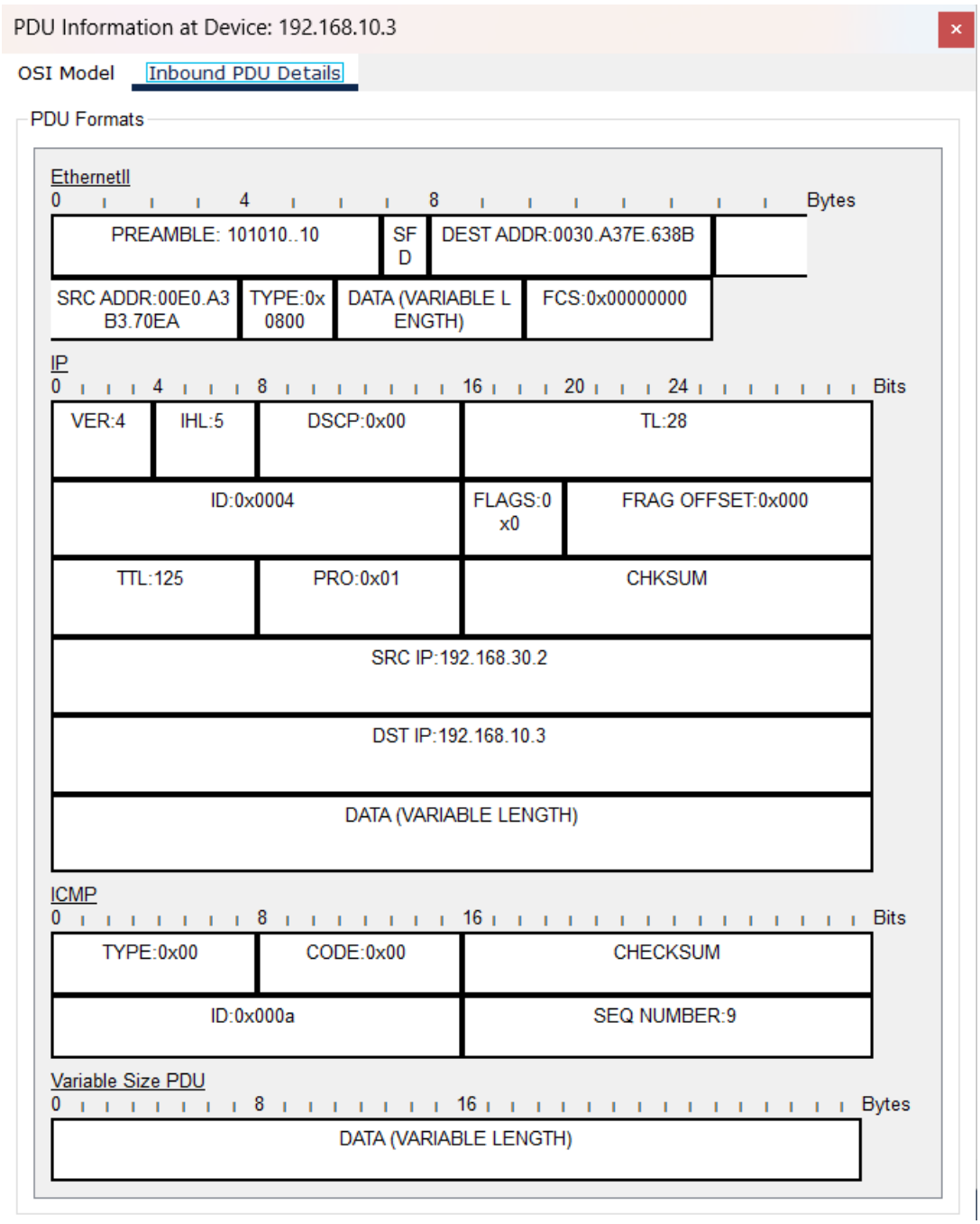
Device	Interface	IPv4 Address	Subnet mask
10.0.0.1	FastEthernet0/0	192.168.10.1	255.255.255.0
	Serial2/0	10.0.0.1	255.0.0.0
10.0.0.2	FastEthernet0/0	192.168.20.1	255.255.255.0
	Serial2/0	10.0.0.2	255.0.0.0
	Serial3/0	11.0.0.1	255.0.0.0
11.0.0.2	FastEthernet0/0	192.168.30.1	255.255.255.0
	Serial2/0	11.0.0.2	255.0.0.0

Date:11/09/2024





Date:11/09/2024



Date:18/09/2024

Himanshu Parmar
22010101132

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.

```java
import java.util.*;

class Router {
    int id;
    int[] distance;
    int[] nextHop;
    List<Integer> neighbors;

    public Router(int id, int numRouters) {
        this.id = id;
        this.distance = new int[numRouters];
        this.nextHop = new int[numRouters];
        this.neighbors = new ArrayList<>();
        for (int i = 0; i < numRouters; i++) {
            if (i == id) {
                distance[i] = 0;
            } else {
                distance[i] = Integer.MAX_VALUE;
            }
            nextHop[i] = -1;
        }
    }

    public void addNeighbor(int neighbor) {
        neighbors.add(neighbor);
    }
}

public class DistanceVectorRouting {
    private static final int INFINITY = Integer.MAX_VALUE;
    private int numRouters;
    private Router[] routers;
    private int[][] costMatrix;

    public DistanceVectorRouting(int numRouters) {
```

Date:18/09/2024

```
        this.numRouters = numRouters;
        routers = new Router[numRouters];
        costMatrix = new int[numRouters][numRouters];
        for (int i = 0; i < numRouters; i++) {
            routers[i] = new Router(i, numRouters);
            for (int j = 0; j < numRouters; j++) {
                costMatrix[i][j] = (i == j) ? 0 : INFINITY;
            }
        }
    }

    public void addLink(int from, int to, int cost) {
        costMatrix[from][to] = cost;
        costMatrix[to][from] = cost;
        routers[from].addNeighbor(to);
        routers[to].addNeighbor(from);
    }

    public void bellmanFord() {
        boolean updated;
        for (int step = 0; step < numRouters - 1; step++) {
            updated = false;
            for (int i = 0; i < numRouters; i++) {
                Router router = routers[i];

                for (int neighbor : router.neighbors) {
                    for (int dest = 0; dest < numRouters; dest++) {
                        if (router.distance[dest] > routers[neighbor].distance[dest]
+ costMatrix[i][neighbor]) {
                            router.distance[dest] = routers[neighbor].distance[dest]
+ costMatrix[i][neighbor];
                            router.nextHop[dest] = neighbor;
                            updated = true;
                        }
                    }
                }
            if (!updated) {
                break;
            }
        }
    }

    public void printRoutingTable() {
        System.out.println("Routing Tables:");
        for (Router router : routers) {
            System.out.println("\nRouter " + router.id + ":");
```

Date:18/09/2024

```
            System.out.println("Destination\tDistance\tNext Hop");
            for (int i = 0; i < numRouters; i++) {
                System.out.println(i + "\t\t" + (router.distance[i] == INFINITY ?
"Inf" : router.distance[i]) + "\t\t" + (router.nextHop[i] == -1 ? "-" :
router.nextHop[i]));
            }
        }
    }

    public static void main(String[] args) {
        int numRouters = 4;
        DistanceVectorRouting dvr = new DistanceVectorRouting(numRouters);
        dvr.addLink(0, 1, 1);
        dvr.addLink(0, 2, 4);
        dvr.addLink(1, 2, 2);
        dvr.addLink(1, 3, 6);
        dvr.addLink(2, 3, 3);
        dvr.bellmanFord();
        dvr.printRoutingTable();
    }
}
```

Date:18/09/2024

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

```
import java.util.Arrays;

public class LinkStateRouting {

    static final int V = 6;
    static final int INF = Integer.MAX_VALUE;

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

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

        return min_index;
    }

    void printSolution(int dist[]) {
        System.out.println("Vertex \t Distance from Source");
        for (int i = 0; i < V; i++) {
            System.out.println(i + " \t\t " + dist[i]);
        }
    }
    void dijkstra(int graph[][], int src) {
        int dist[] = new int[V];
        boolean visited[] = new boolean[V];

        Arrays.fill(dist, INF);
        Arrays.fill(visited, false);
        dist[src] = 0;
        for (int count = 0; count < V - 1; count++) {
            int u = minDistance(dist, visited);
            visited[u] = true;

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

Date:18/09/2024

```
        }
        printSolution(dist);
    }

    public static void main(String[] args) {
        int graph[][] = {
            {0, 2, INF, 1, INF, INF},
            {2, 0, 3, 2, INF, INF},
            {INF, 3, 0, INF, 7, 4},
            {1, 2, INF, 0, 5, INF},
            {INF, INF, 7, 5, 0, 6},
            {INF, INF, 4, INF, 6, 0}
        };

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

Date:28/08/2024

Himanshu Parmar
22010101132

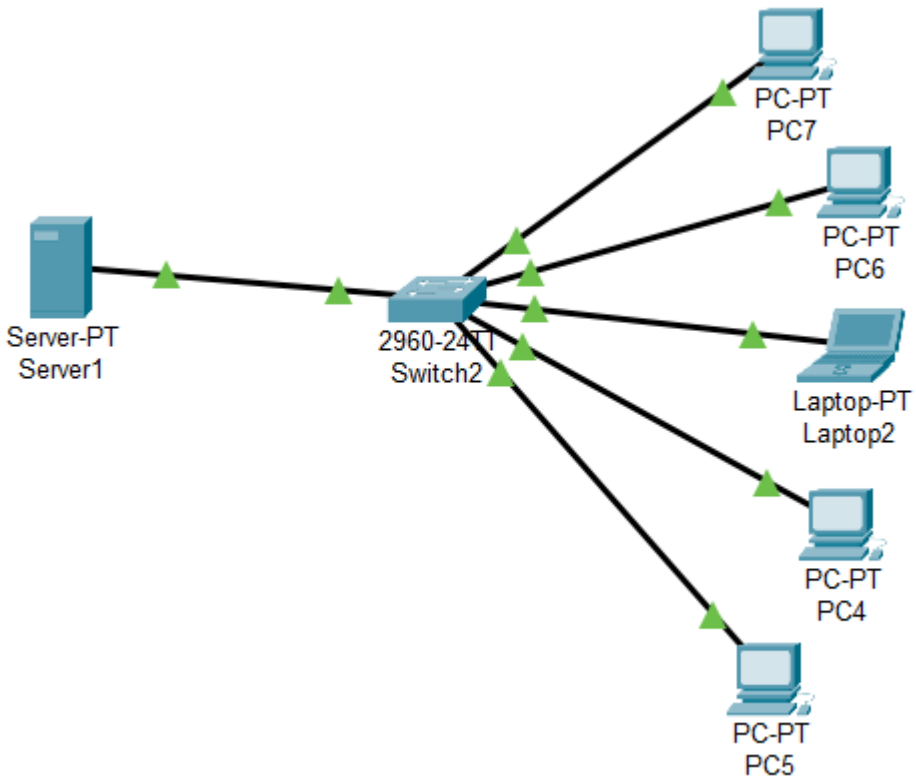
Lab Practical #13:

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).**

Lab No.:C-209
Topology: Star Topology



Date:28/08/2024

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

Total No Of PC: - 9

Total Number of Switch: - 1

Total Server: DHCP Server

Types Of Cable: - Twisted Pair Cable

Connectors: RJ-45

Network Type: Lan