K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

Batch:	C2	Roll No.:	110

Experiment / assignment / tutorial No._____

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of the Staff In-charge with date

Experiment No.:6

TITLE: IP classes and Implementation of Subnet mask concept.

AIM: To study IP classes and Implementation of Subnet mask concept.

An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

This experiment enables student for identifying the class of the IP address and design particular subnets as per user requirements.

Expected Outcome of Experiment:
CO:Understand Ip subnetting

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

Pre Lab/ Prior Concepts: IP Address, Classes, Subnet concept

New Concepts to be learned: Subnet mask calculation, Subnet address calculation

Stepwise-Procedure:

Applying a subnet mask to an IP address allows to identify the network and node parts of the address. The network bits are represented by the 1s in the mask, and the node bits are

represented by the 0s. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address* or Number.

Default subnet masks:

Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000
Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000
Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

Additional bits can be added to the default subnet mask for a given Class to further subnet, or break down, a network. When a bitwise logical AND operation is performed between the subnet mask and IP address, the result defines the *Subnet Address* (also called the *Network Address* or *Network Number*). There are some restrictions on the subnet address. Node addresses of all "0"s and all "1"s are reserved for specifying the local network (when a host does not know its network address) and all hosts on the network (broadcast address), respectively. This also applies to subnets. A subnet address cannot be all "0"s or all "1"s. This also implies that a 1 bit subnet mask is not allowed. This restriction is required because older standards enforced this restriction. Recent standards that allow use of these subnets have superseded these standards, but many "legacy" devices do not support the newer standards. If you are operating in a controlled environment, such as a lab, you can safely use these restricted subnets.

CIDR -- **C**lassless **I**nter **D**omain **R**outing:

The "classful" system of allocating IP addresses can be very wasteful; Under supernetting, the classful subnet masks are extended so that a network address and subnet mask could, for example, specify multiple Class C subnets with one address.

For example, If about 1000 addresses are required, it could be possible to supernet 4 Class C networks together:

192.60.128.0 (11000000.00111100.10000000.00000000)Class C subnet address
192.60.129.0(11000000.00111100.10000001.00000000) Class C subnet address
192.60.130.0(11000000.00111100.10000010.00000000) Class C subnet address
192.60.131.0(11000000.00111100.10000011.00000000) Class C subnet address
---
192.60.128.0 (11000000.00111100.10000000.00000000) Supernetted subnet address
255.255.252.0 (11111111.11111111.11111100.00000000)Subnet Mask 192.60.131.255
(11000000.00111100.10000011.11111111) Broadcast address

In this example, the subnet 192.60.128.0 includes all the addresses from 192.60.128.0 to 192.60.131.255. In the binary representation of the subnet mask, the Network portion of the address is 22 bits long, and the host portion is 10 bits long. Under CIDR, the subnet mask notation is reduced to simplified shorthand. Instead of spelling out the bits of the subnet mask, it is simply listed as the number of 1s bits that start the mask. In the above example, instead of writing the address and subnet mask as 192.60.128.0, Subnet Mask

255.255.252.0 .the network address would be written simply as: 192.60.128.0/22 Which indicates starting address of the network, and number of 1s bits (22) in the network portion of the address. Subnet mask in binary

11111111.11111111.11111100.00000000.

The use of a CIDR notated address is the same as for a Classful address. Classful addresses can easily be written in CIDR notation as Class A = /8, Class B = /16, and Class C = /24
To calculate the number of subnets or nodes,

No. of Nodes/ Subnets $=2^n-2$

Where n = number of bits in either field.

Multiplying the number of subnets by the number of nodes available per subnet gives you the total number of nodes available for your class and subnet mask. Also, note that although subnet masks with non-contiguous mask bits are allowed, they are not recommended.

Example:

10001100.10110011.11011100.11001000	140.179.220.200IP Address
11111111.11111111.**111**00000.00000000	255.255.**224**.000Subnet Mask
10001100.10110011.11000000.00000000	140.179.192.000Subnet Address
10001100.10110011.11011111.11111111	40.179.223.255 Broadcast Address

1. Program starts with taking IP address from user and the number of subnets from the user.
2. Then the calculation for subnet mask is done as specified in methodology.
3. Then with AND ing with subnet mask the subnet addresses are calculated.

IMPLEMENTATION: (printout of code)

CLASSLESS

```
def toBinary(a):
    a=int(a)
    answer=[]
    if(a==0):
        return 0
```

```
    while(a!=0):
        answer.append(str(a%2))
        a=a//2

    while(len(answer)<8):
        answer.append('0')
    return("".join(answer[::-1]))
def toDecimal(a):
    a=str(a)
    answer=0
    power=0
    for digit in a[::-1]:
        if(digit=='1'):
            answer+=2**power
        power+=1
    return answer



ip=input("Please enter ip: ")
subnetMask=input("Please enter subnetmask: ")
ip="".join([toBinary(i) for i in ip.split(".")])
print(ip)
subnetMask = "".join(['1' if i<int(subnetMask) else '0' for i in range(32)])

first = ['1' if(int(ip[i])*int(subnetMask[i])==1) else '0' for i in
range(0,len(ip))]
first=["".join(first[i:i + 8]) for i in range(0, len(first), 8)] # split in 4
parts of 8
first=".".join([str(toDecimal(i)) for i in first])

print(first) #network ip

subnetMask = ['0' if i=='1' else '1' for i in subnetMask]

last = ['0' if(int(ip[i])+int(subnetMask[i])==0) else '1' for i in
range(0,len(ip))]
last=["".join(last[i:i + 8]) for i in range(0, len(last), 8)] # split in 4 parts
of 8
```

```
last=".".join([str(toDecimal(i)) for i in last])

print(last) #network ip
```

Classfull

```
#classfull
ip=input("Please enter ip: ")
first=int(ip.split(".")[0])
if(first in(0,127)):
    print("Class A")
    print("subnet mask: 255.0.0.0")
elif(first in(128,191)):
    print("Class B")
    print("subnet mask: 255.255.0.0")
elif(first in(192,223)):
    print("Class C")
    print("subnet mask: 255.255.255.0")
elif(first in(224,239)):
    print("Class D")
    print("subnet mask: - ")
elif(first in(240,256)):
    print("Class E")
    print("subnet mask: - ")

print(first,".0.0.1")
print(first,".255.255.255")
```

```
Please enter subnetmask: 23
11000000000000010000000100000001
192.1.0.0
192.1.1.255
```

```
Please enter ip: 126.36.3.2
Class A
subnet mask: 255.0.0.0
126 .0.0.1
126 .255.255.255
```

CONCLUSION:
Thus we have studied classless and classful ip addressing in computer networks. We studied how subnetting works and how classes are divided. We also understood how to apply subnet masks on classless ip addressing.

Post Lab Questions

1. Which of the following is private IP address?
   A. 12.0.0.1 B. 168.172.19.39
   C. 172.15.14.36 D. 192.168.24.43
   D
2. Which class of IP address provides a maximum of only 254 host addresses per network ID?
   A. Class A
   B. Class B
   C. Class C
   D. Class D
   D
3. What is the address range of a Class B network address in binary?
   A. 01xxxxxx
   B. 0xxxxxxx
   C. 10xxxxxx
   D. 110xxxxx
   D
4. Which two statements describe the IP address 10.16.3.65/23?
   1.The subnet address is 10.16.3.0 255.255.254.0.
   2.The lowest host address in the subnet is 10.16.2.1 255.255.254.0.
   3.The last valid host address in the subnet is 10.16.2.254 255.255.254.0.
   4.The broadcast address of the subnet is 10.16.3.255 255.255.254.0.

A. 1 and 3
B. 2 and 4
C. 1, 2 and 4
D. 2, 3 and 4

B

5. What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask?

A. 14 B. 15
C. 16 D. 30

D

6. You need to subnet a network that has 5 subnets, each with at least 16 hosts. Which classful subnet mask would you use?

A. 255.255.255.192 B. 255.255.255.224
C. 255.255.255.240 D. 255.255.255.248

A

7. You have a network that needs 29 subnets while maximizing the number of host addresses available on each subnet. How many bits must you borrow from the host field to provide the correct subnet mask?

A. 2 B. 3
C. 4 D. 5

Date: 10 oct 23 **Signature of faculty in-charge**

Batch: C2 Roll No.: 110

Experiment / assignment / tutorial No._____

Grade: AA / AB / BB / BC / CC / CD /DD

Experiment No.:7

TITLE: Study Cisco Switch Router Configu

Signature of the Staff In-charge with date

AIM: To study basic Cisco Switch & Router Configuration Commands and configure

i. Virtual LAN (VLAN).
ii. Static Routing

Expected Outcome of Experiment:
CO:understanding vlan and static routing

Books/ Journals/ Websites referred:
1. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

Pre Lab/ Prior Concepts: Basics of Routing and Cisco Packet Tracer

New Concepts to be learned: Different Modes of Operation of Cisco router

Cisco IOS Modes of Operation:

- The Cisco IOS software provides access to several different command modes. Each command mode provides a different group of related commands.
- For security purposes, the Cisco IOS software provides two levels of access to commands:
  - User mode
  - Privileged mode
- The unprivileged user mode is called user EXEC mode. The privileged mode is called privileged EXEC mode and requires a password. The commands available in user EXEC mode are a subset of the commands available in privileged EXEC mode.
- The following table describes some of the most commonly used modes, how to

enter the modes, and the resulting prompts. The prompt helps you identify which mode you are in and, therefore, which commands are available to you

Modes of Operation	Usage	How to enter the mode	Prompt
User EXEC	Change terminal settings on a temporary basis, perform basic tests, and list system information.	First level accessed.	Router>
Privileged EXEC	System administration, set operating parameters.	From user EXEC mode, enter enable password command	Router#
Global Config	Modify configuration that affect the system as a whole.	From privileged EXEC, enter configure terminal.	Router(config)#
Interface Config	Modify the operation of an interface.	From global mode, enter interface type number.	Router(config-if)#
Setup	Create the initial configuration.	From privileged EXEC mode, enter command setup.	Prompted dialog

User EXEC Mode:
When you are connected to the router, you are started in user EXEC mode. The user EXEC commands are a subset of the privileged EXEC commands.

Privileged EXEC Mode:
Privileged commands include the following:
• Configure – Changes the software configuration.
• Debug – Display process and hardware event messages.
• Setup – Enter configuration information at the prompts.
Enter the command disable to exit from the privileged EXEC mode and return to user EXEC mode.

Configuration Mode:
Configuration mode has a set of sub-modes that you use for modifying interface settings, routing protocol settings, line settings, and so forth. Use caution with configuration mode because all changes you enter take effect immediately.
To enter configuration mode, enter the command configure terminal and exit by pressing Ctrl-Z.

Note: Almost every configuration command also has a no form. In general, use the no form to disable a feature or function. Use the command without the keyword no to re-enable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, enter the no IP routing command and enter IP routing to re-enable it.

i. Virtual LAN (VLAN):

A virtual local area network (VLAN) is a LAN which is not configured by physical wiring but it is configured by software. A VLAN is logical group of network devices that appear to be on same LAN despite their geographical distribution. A VLAN is implemented so that network administrators can connect a group of host in the same domain inspite of their physical location to achieve scalability and improve security features.

To subdivide a network into virtual LANs, one configures a network switch or router. Simpler network devices can partition only per physical port (if at all) , in which case each VLAN is connected with a dedicated network cable (and VLAN connectivity is limited by the number of hardware ports available) More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. VLAN can greatly simplify network design and deployment, because VLAN membership can be configured through software.

Stepwise-Procedure:

A. Creating a simple LAN network using packet tracer:

Step 1: Select 12 PCs from the end devices and one fast ethernet switch (2950/24 ports)

Step 2: Connect PCs and switch via copper cable from the panel. Connection can be verified by appearance of all green dots on the links.

Step 3: For PCs to communicate click on PC0.

- Dialog box for PC0 appears.
- Click on desktop applications by packet tracer.
- Go to IP configuration.
- Enter IP address to identify host i.e., PC0 (for example: 192.168.1.1)
- Subnet mask-by default already set one can change it as per his/her specification.

Step 4: Repeat step 3 for PC1

Step 5: Ping the PCs and check their working status.

Step 6: Simple PDU (Protocol Data Unit) to simulate network traffic by sending ICMP PDU to assess the network traffic. View simulation in simulation mode

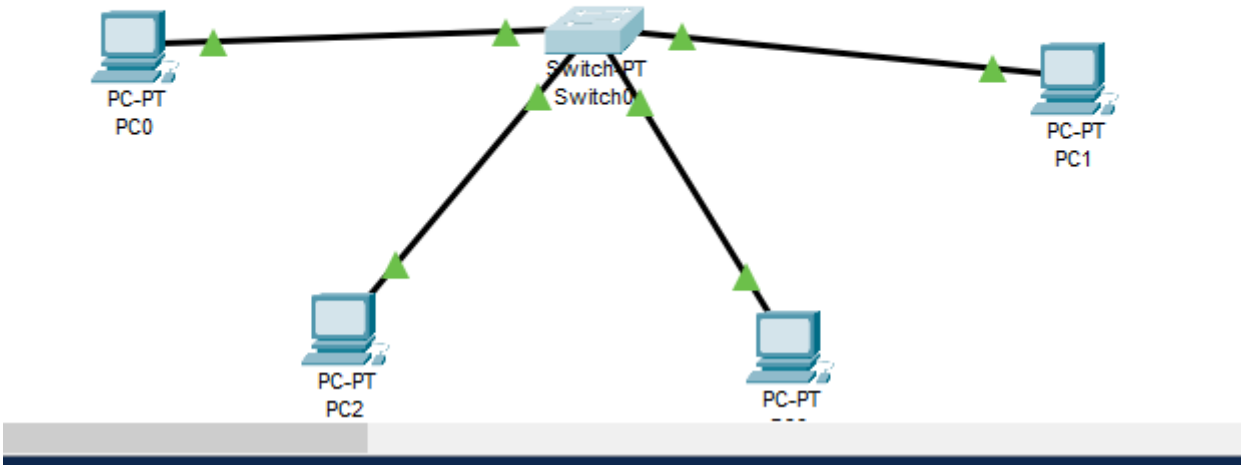
Step 7: Configure two VLAN in a switch in 6 verticals.

Step 8: As per design, assign membership of VLAN to port using following command.

```
# switch port access vlan2 or vlan3
```

Step 9: Check the status of VLAN.

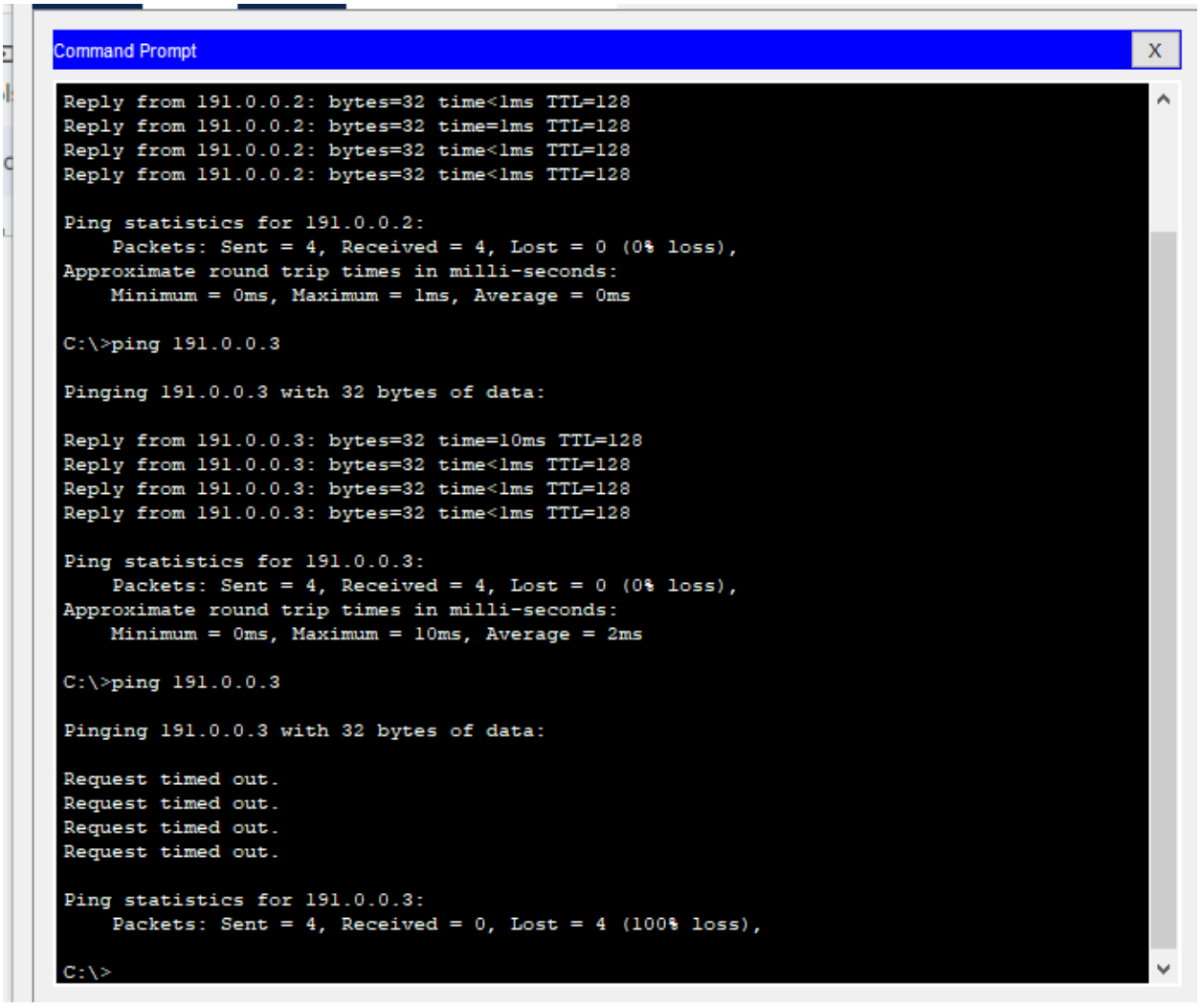
ii. Static Routing Configuration

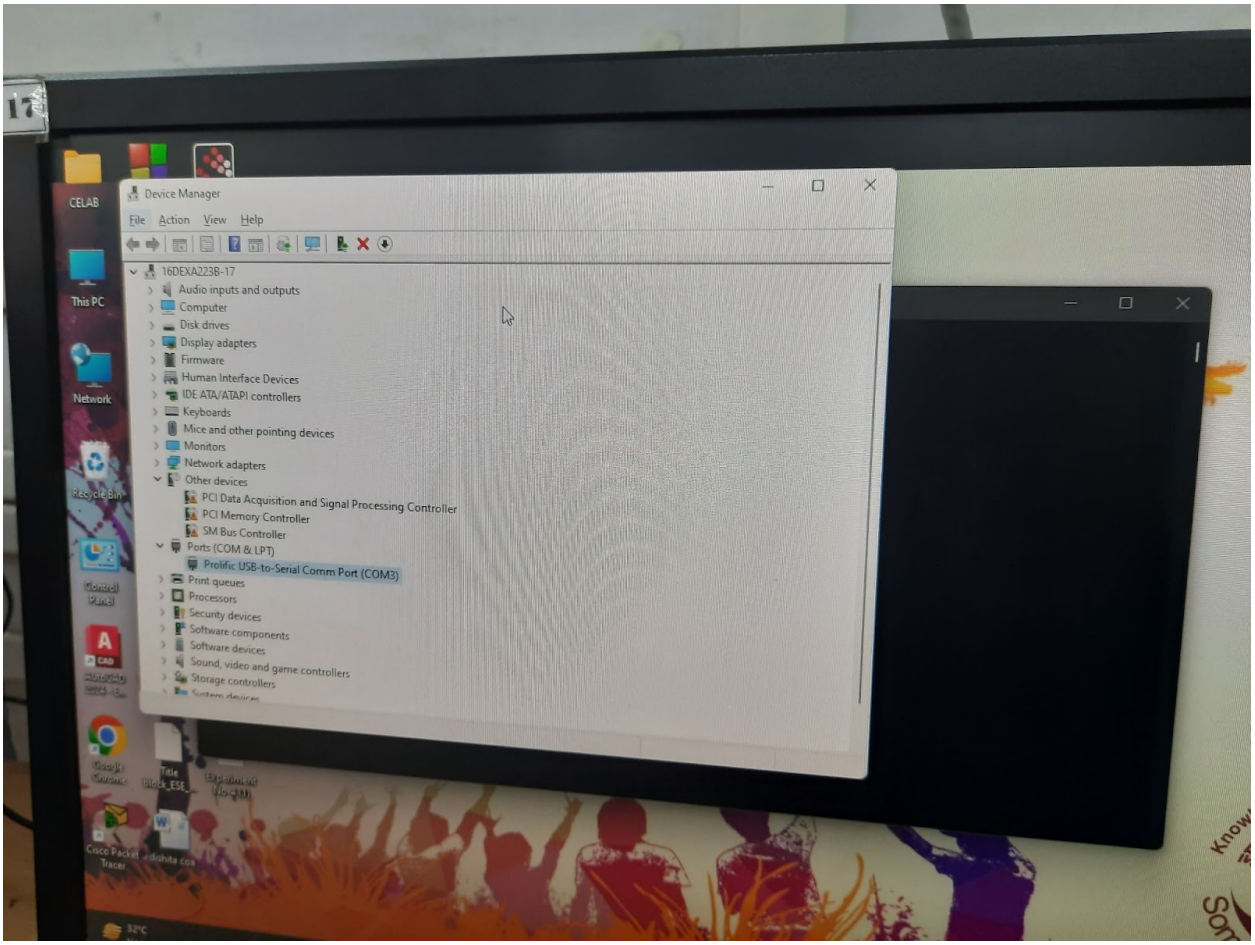


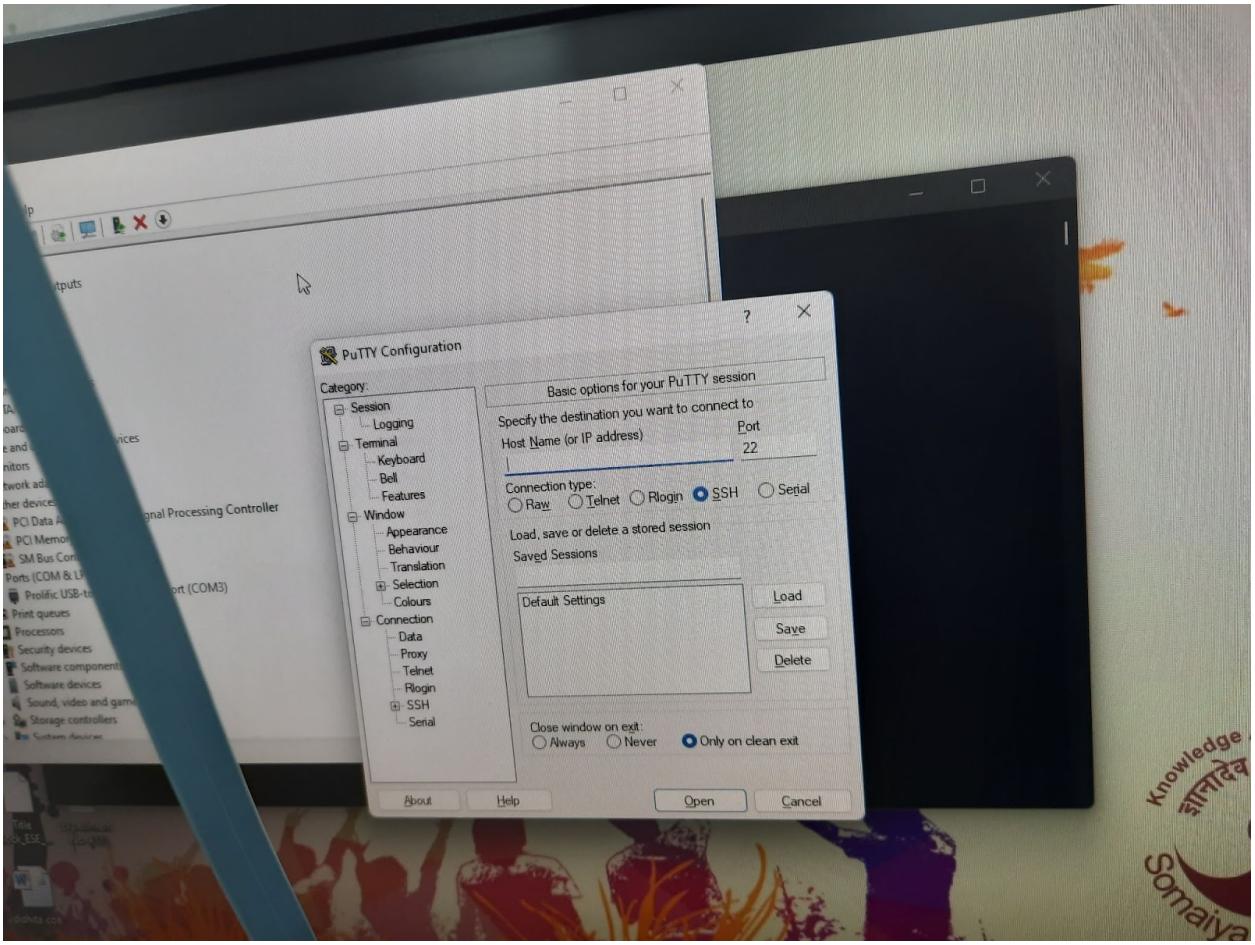

```
Switch>en
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 13
Switch(config-vlan)#name aatmaj
Switch(config-vlan)#exit
Switch(config)#vlan 14
Switch(config-vlan)#name zephyr
Switch(config-vlan)#exit
Switch(config)#do show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
                                                 Fa4/1, Fa5/1
13   aatmaj                            active
14   zephyr                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
13   enet  100013     1500  -      -      -        -    -        0      0
14   enet  100014     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

 --More--
```

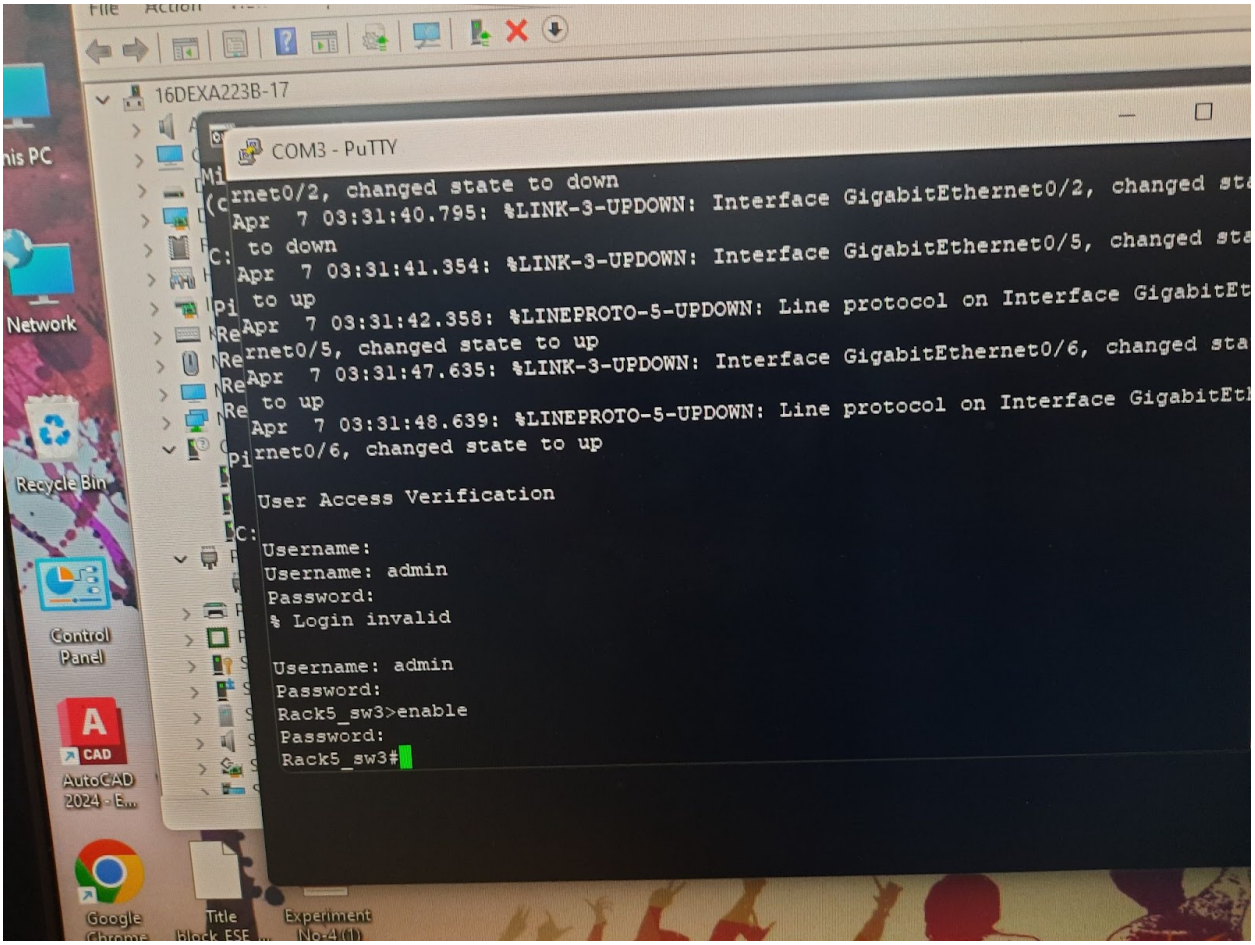
Copy Paste

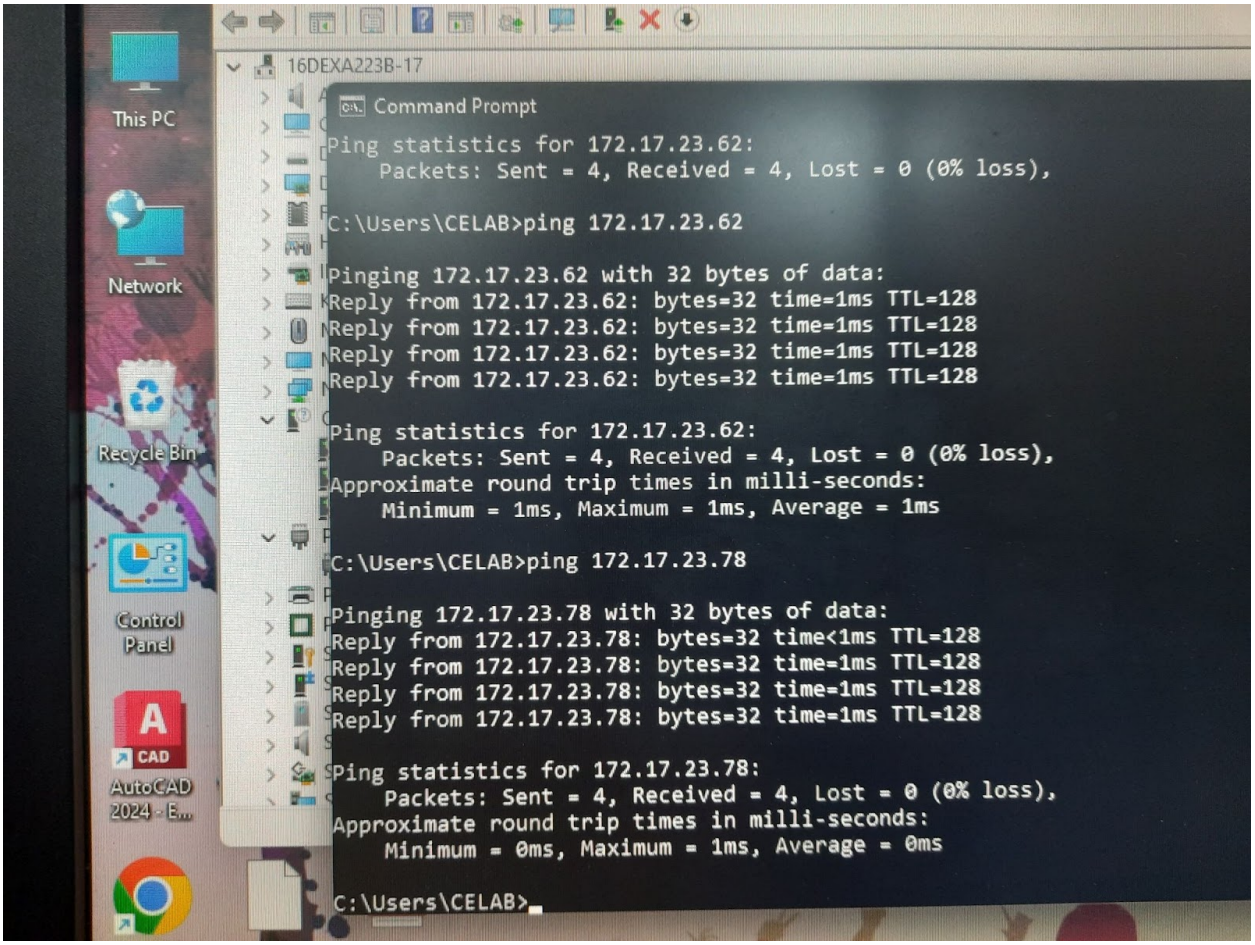
```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
13   enet  100013     1500  -      -      -        -    -        0      0
14   enet  100014     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0


Switch(config)#interface range fa 0/1-2
interface range not validated - command rejected
Switch(config)#interface range fa 0//1
                                    ^
% Invalid input detected at '^' marker.

Switch(config)#interface range fa 0/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 13
Switch(config-if-range)#exit
Switch(config)#interface range fa 1/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 13
Switch(config-if-range)#exit
Switch(config)#interface range fa 2/1
Switch(config-if-range)#switchport access vlan 14
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 14
Switch(config-if-range)#exit
Switch(config)#interface range fa 3/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 14
Switch(config-if-range)#exit
Switch(config)#
```

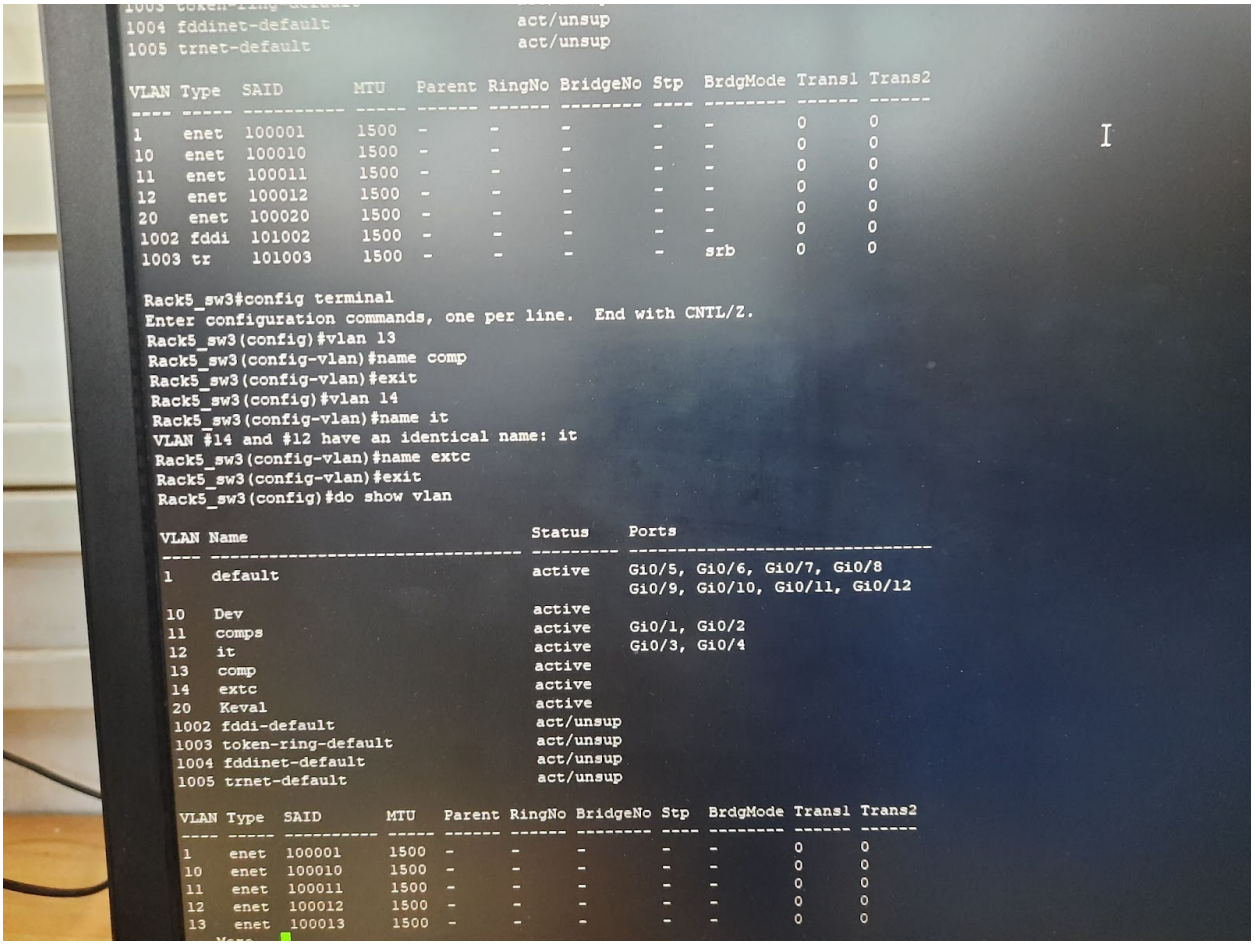

Command Prompt
X
Reply from 191.0.0.2: bytes=32 time<1ms TTL=128
Reply from 191.0.0.2: bytes=32 time=1ms TTL=128
Reply from 191.0.0.2: bytes=32 time<1ms TTL=128
Reply from 191.0.0.2: bytes=32 time<1ms TTL=128
Ping statistics for 191.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 191.0.0.3
Pinging 191.0.0.3 with 32 bytes of data:
Reply from 191.0.0.3: bytes=32 time=10ms TTL=128
Reply from 191.0.0.3: bytes=32 time<1ms TTL=128
Reply from 191.0.0.3: bytes=32 time<1ms TTL=128
Reply from 191.0.0.3: bytes=32 time<1ms TTL=128
Ping statistics for 191.0.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>ping 191.0.0.3
Pinging 191.0.0.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 191.0.0.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>


Device Manager
File Action View Help
16DEXA223B-17
Audio inputs and outputs
Computer
Disk drives
Display adapters
Firmware
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Other devices
PCI Data Acquisition and Signal Processing Controller
PCI Memory Controller
SM Bus Controller
Ports (COM & LPT)
Prolific USB-to-Serial Comm Port (COM3)
Print queues
Processors
Security devices
Software components
Software devices
Sound, video and game controllers
Storage controllers
CELAB
This PC
Network
Recycle Bin

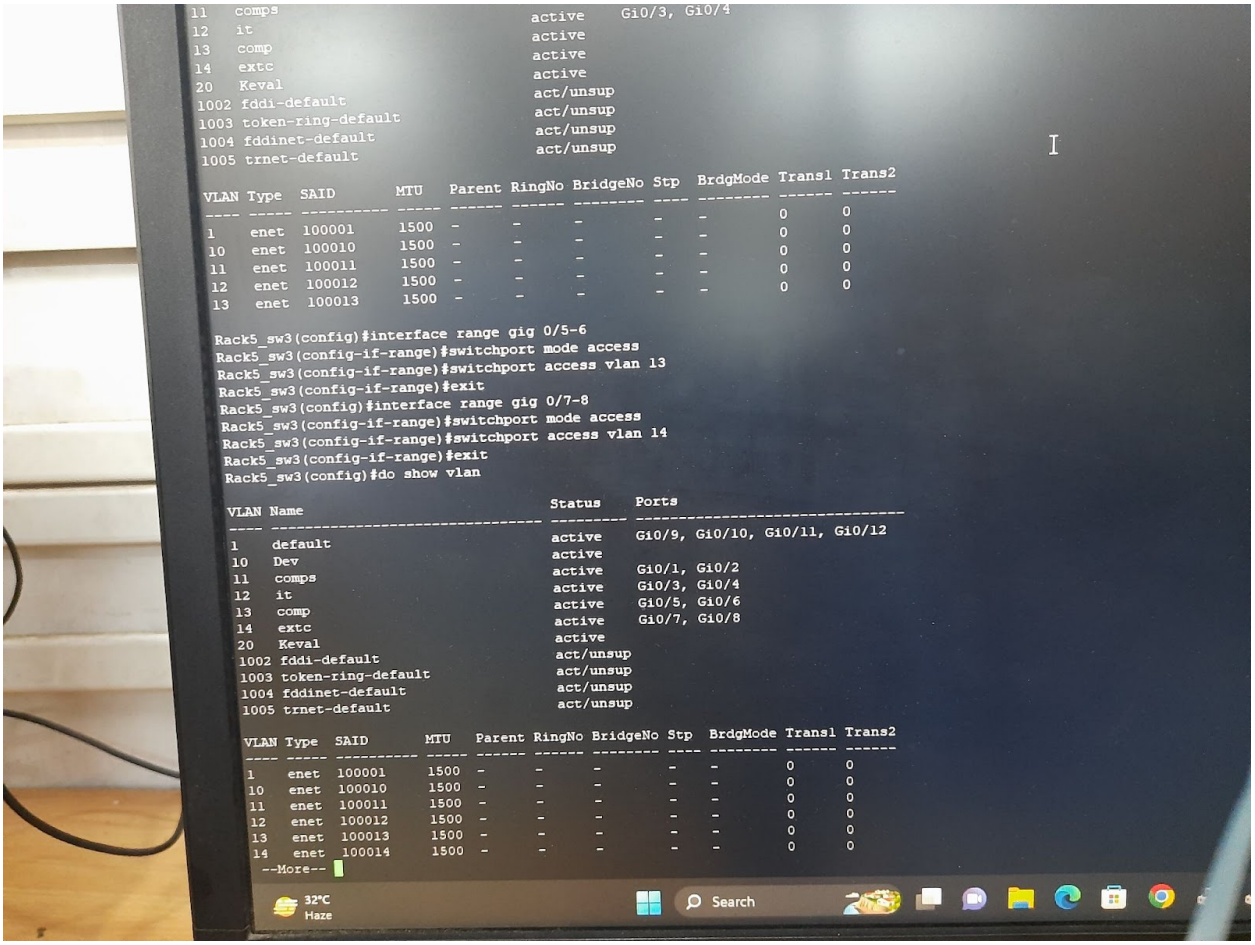

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

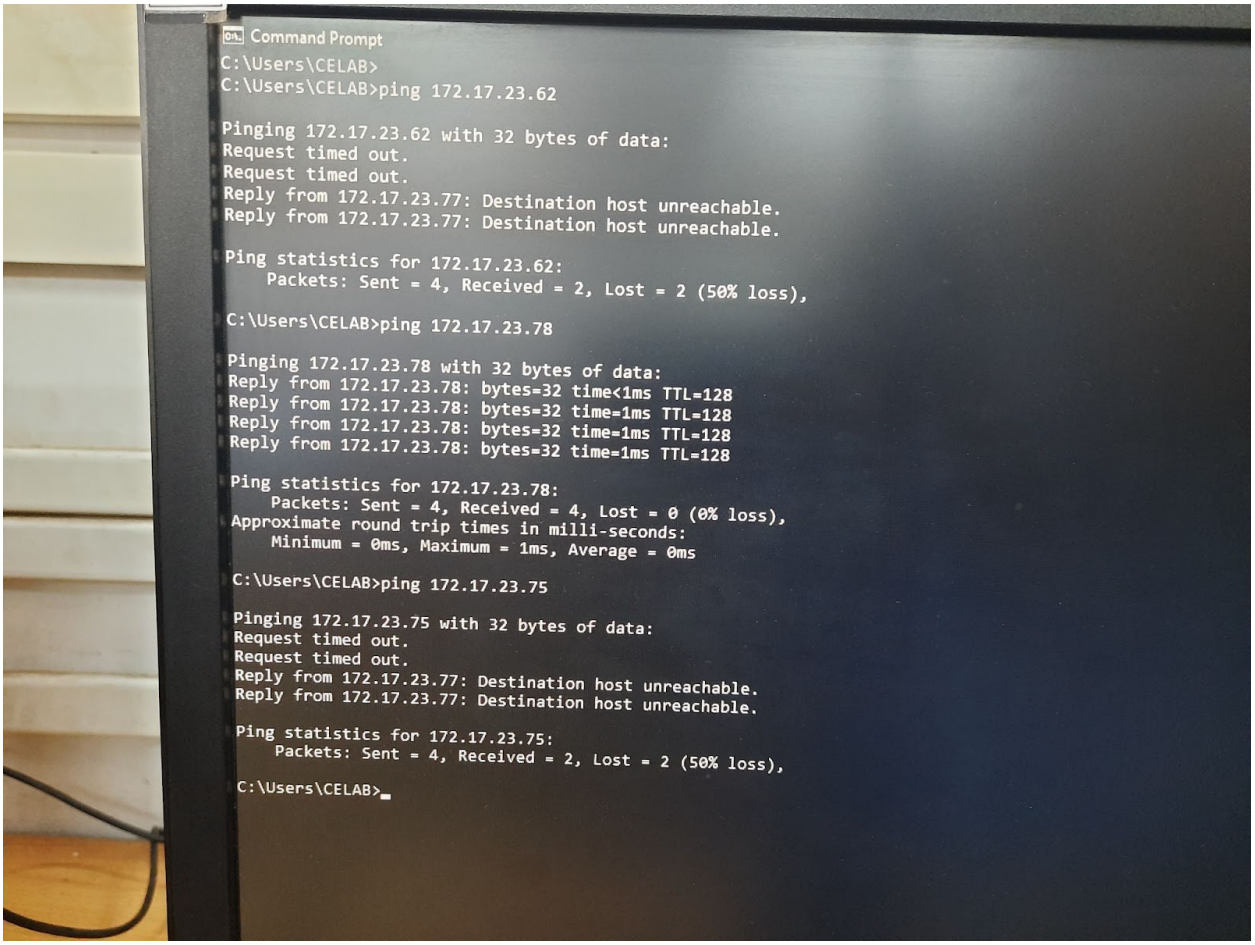

16DEXA223B-17
COM3 - PuTTY
rnet0/2, changed state to down
Apr 7 03:31:40.795: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed st
to down
Apr 7 03:31:41.354: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed st
to up
Apr 7 03:31:42.358: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEt
rnet0/5, changed state to up
Apr 7 03:31:47.635: %LINK-3-UPDOWN: Interface GigabitEthernet0/6, changed sta
to up
Apr 7 03:31:48.639: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEt
rnet0/6, changed state to up
User Access Verification
Username:
Username: admin
Password:
% Login invalid
Username: admin
Password:
Rack5_sw3>enable
Password:
Rack5_sw3#
Network
Recycle Bin
Control Panel
AutoCAD 2024 - E...
Google Chrome
Title block ESE ...
Experiment No-4 (1)


16DEXA223B-17
This PC
Network
Recycle Bin
Control Panel
AutoCAD 2024 - E...
Command Prompt
Ping statistics for 172.17.23.62:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\CELAB>ping 172.17.23.62
Pinging 172.17.23.62 with 32 bytes of data:
Reply from 172.17.23.62: bytes=32 time=1ms TTL=128
Reply from 172.17.23.62: bytes=32 time=1ms TTL=128
Reply from 172.17.23.62: bytes=32 time=1ms TTL=128
Reply from 172.17.23.62: bytes=32 time=1ms TTL=128
Ping statistics for 172.17.23.62:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\CELAB>ping 172.17.23.78
Pinging 172.17.23.78 with 32 bytes of data:
Reply from 172.17.23.78: bytes=32 time<1ms TTL=128
Reply from 172.17.23.78: bytes=32 time=1ms TTL=128
Reply from 172.17.23.78: bytes=32 time=1ms TTL=128
Reply from 172.17.23.78: bytes=32 time=1ms TTL=128
Ping statistics for 172.17.23.78:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\CELAB>



```
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID        MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
12   enet  100012     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    srb      0      0

Rack5_sw3#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Rack5_sw3(config)#vlan 13
Rack5_sw3(config-vlan)#name comp
Rack5_sw3(config-vlan)#exit
Rack5_sw3(config)#vlan 14
Rack5_sw3(config-vlan)#name it
VLAN #14 and #12 have an identical name: it
Rack5_sw3(config-vlan)#name extc
Rack5_sw3(config-vlan)#exit
Rack5_sw3(config)#do show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                Gi0/9, Gi0/10, Gi0/11, Gi0/12
10   Dev                              active
11   comps                            active    Gi0/1, Gi0/2
12   it                               active    Gi0/3, Gi0/4
13   comp                             active
14   extc                             active
20   Keval                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID        MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
12   enet  100012     1500  -      -      -        -    -        0      0
13   enet  100013     1500  -      -      -        -    -        0      0
```


11 comps active Gi0/3, Gi0/4
12 it active
13 comp active
14 extc active
20 Keval act/unsup
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 0 0
10 enet 100010 1500 0 0
11 enet 100011 1500 0 0
12 enet 100012 1500 0 0
13 enet 100013 1500 0 0
Rack5_sw3(config)#interface range gig 0/5-6
Rack5_sw3(config-if-range)#switchport mode access
Rack5_sw3(config-if-range)#switchport access vlan 13
Rack5_sw3(config-if-range)#exit
Rack5_sw3(config)#interface range gig 0/7-8
Rack5_sw3(config-if-range)#switchport mode access
Rack5_sw3(config-if-range)#switchport access vlan 14
Rack5_sw3(config-if-range)#exit
Rack5_sw3(config)#do show vlan
VLAN Name Status Ports
1 default active Gi0/9, Gi0/10, Gi0/11, Gi0/12
10 Dev active
11 comps active Gi0/1, Gi0/2
12 it active Gi0/3, Gi0/4
13 comp active Gi0/5, Gi0/6
14 extc active Gi0/7, Gi0/8
20 Keval active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 0 0
10 enet 100010 1500 0 0
11 enet 100011 1500 0 0
12 enet 100012 1500 0 0
13 enet 100013 1500 0 0
14 enet 100014 1500 0 0
--More--
32°C Haze
Search


Command Prompt
C:\Users\CELAB>
C:\Users\CELAB>ping 172.17.23.62
Pinging 172.17.23.62 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 172.17.23.77: Destination host unreachable.
Reply from 172.17.23.77: Destination host unreachable.
Ping statistics for 172.17.23.62:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
C:\Users\CELAB>ping 172.17.23.78
Pinging 172.17.23.78 with 32 bytes of data:
Reply from 172.17.23.78: bytes=32 time<1ms TTL=128
Reply from 172.17.23.78: bytes=32 time=1ms TTL=128
Reply from 172.17.23.78: bytes=32 time=1ms TTL=128
Reply from 172.17.23.78: bytes=32 time=1ms TTL=128
Ping statistics for 172.17.23.78:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\CELAB>ping 172.17.23.75
Pinging 172.17.23.75 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 172.17.23.77: Destination host unreachable.
Reply from 172.17.23.77: Destination host unreachable.
Ping statistics for 172.17.23.75:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
C:\Users\CELAB>

CONCLUSION: Thus we have understood how vlan works. we implemented vlan on actual physical devices as well as on virtual simulations using cisco packet tracer. Vlans are useful for segregation networks. We also did static routing on cisco packet tracer.

Date: 10 oct 2023 **Signature of faculty in-charge**

Batch: C2	Roll No.: 110
Experiment / assignment / tutorial No._____	
Grade: AA / AB / BB / BC / CC / CD /DD	

Signature of the Staff In-charge with date

Experiment No.:8

TITLE: Study and configure RIP protocol using Cisco Packet tracer

AIM: To study and configure RIP protocol using Cisco Packet tracer

Expected Outcome of Experiment:
CO: To study and configure RIP protocol using Cisco Packet tracer

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

Pre Lab/ Prior Concepts:
IPv4 Addressing, Subnetting, Distance Vector Protocol, Router configuration Commands.

New Concepts to be learned: RIP Protocol and its configuration.

RIP (Routing Information Protocol)
RIP is a standardized Distance Vector protocol, designed for use on smaller networks. RIP was one of the first true Distance Vector routing protocols and is supported on a wide variety of systems.
RIP adheres to the following Distance Vector characteristics:

- RIP sends out periodic routing updates (every 30 seconds)
- RIP sends out the full routing table every periodic update.
- RIP uses a form of distance as its metric (in this case, hop count).
- RIP uses the Bellman-Ford Distance Vector algorithm to determine the best “path” to a particular destination

Other characteristics of RIP include:

- RIP supports IP and IPX routing.
- RIP utilizes UDP port 520
- RIP routes have an administrative distance of 120.

• RIP has a maximum hop count of 15 hops.

RIP Versions

RIP has two versions, Version 1 (RIPv1) and Version 2 (RIPv2).

RIPv1 (RFC 1058) is ***classful***, and thus does not include the subnet mask with its routing table updates. Because of this, RIPv1 does not support **Variable Length Subnet Masks (VLSMs)**. When using RIPv1, networks must be contiguous, and subnets of a major network must be configured with identical subnet masks. Otherwise, route table inconsistencies (or worse) will occur.

RIPv1 sends updates as broadcasts to address 255.255.255.255.

RIPv2 (RFC 2543) is ***classless***, and thus does include the subnet mask with its routing table updates. RIPv2 fully supports VLSMs, allowing discontiguous networks and varying subnet masks to exist.

Other enhancements offered by RIPv2 include:

- Routing updates are sent via multicast, using address 224.0.0.9
- Encrypted authentication can be configured between RIPv2 routers
- Route tagging is supported.

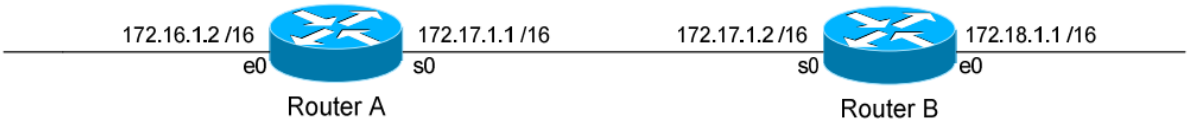
RIPv2 can interoperate with RIPv1. By default:

- RIPv1 routers will send only Version 1packets
- RIPv1 routers will receive both Version 1 and 2 updates
- RIPv2 routers will both send and receive only Version 2 updates

We can control the version of RIP a particular interface will “send” or “receive.”

Unless RIPv2 is manually specified, a Cisco will default to RIPv1 when configuring RIP.

RIPv1 Basic Configuration



Routing protocol configuration occurs in Global Configuration mode. On Router A, to configure RIP, we would type:

```
Router(config)# router rip
Router(config-router)# network 172.16.0.0
Router(config-router)# network 172.17.0.0
```

The first command, router rip, enables the RIP process.

The network statements tell RIP which networks you wish to advertise to other RIP routers. We simply list the networks that are directly connected to our router. Notice that we specify the networks at their classful boundaries, and we do not specify a subnet mask.

To configure Router B:

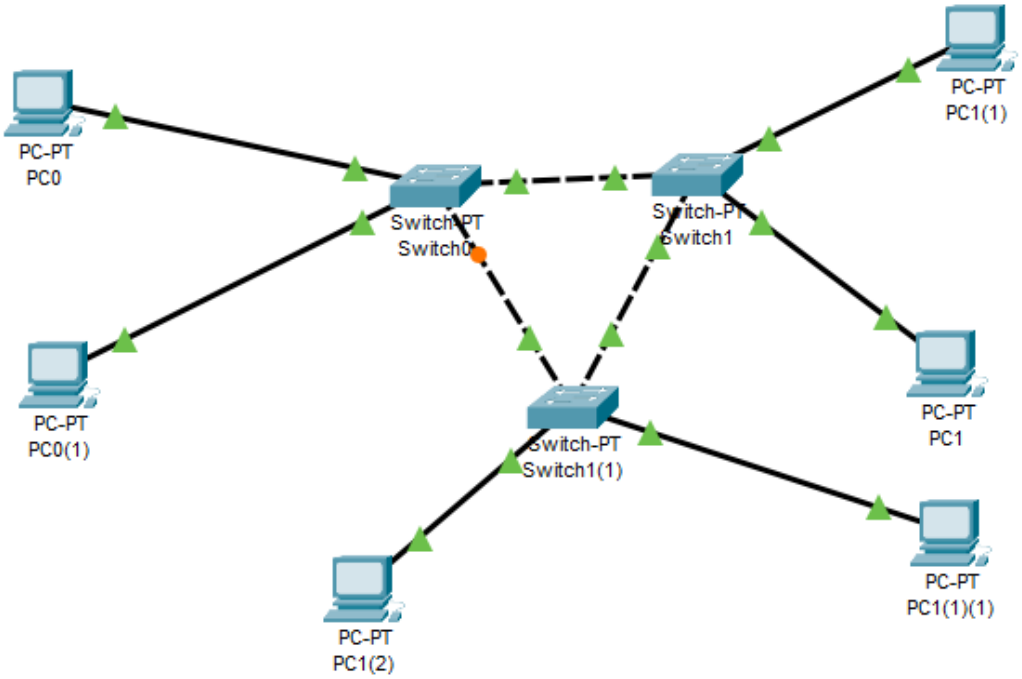
```
Router(config)# router rip
Router(config-router)# network 172.17.0.0
Router(config-router)# network 172.18.0.0
```

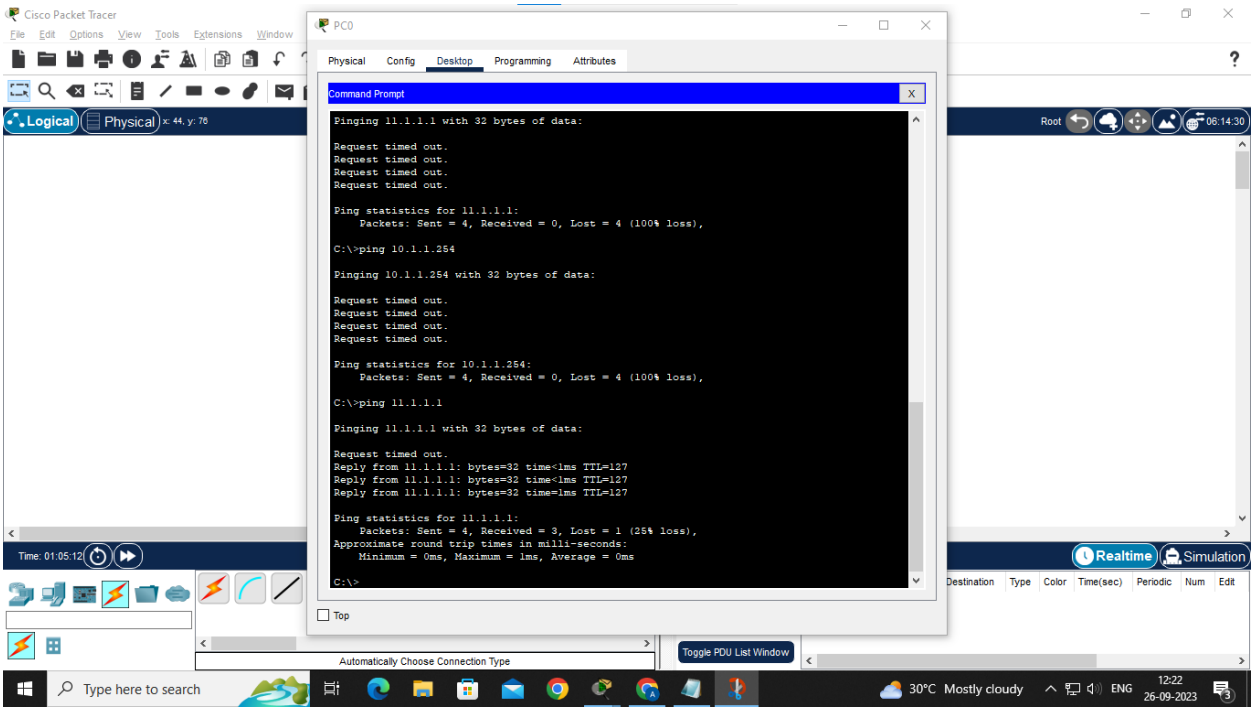
The routing table on Router A will look like:

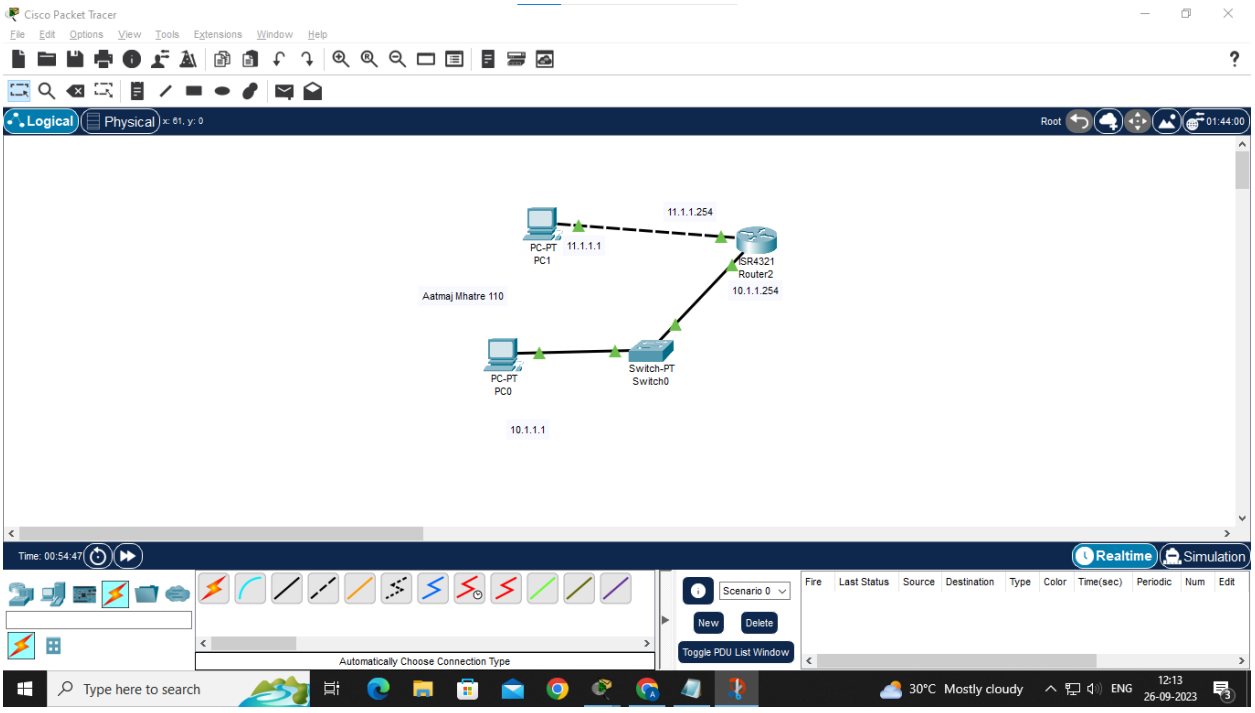
```
RouterA# show ip route

Gateway of last resort is not set
 C     172.16.0.0 is directly connected, Ethernet0
 C     172.17.0.0 is directly connected, Serial0
 R     172.18.0.0 [120/1] via 172.17.1.2, 00:00:00, Serial0
```

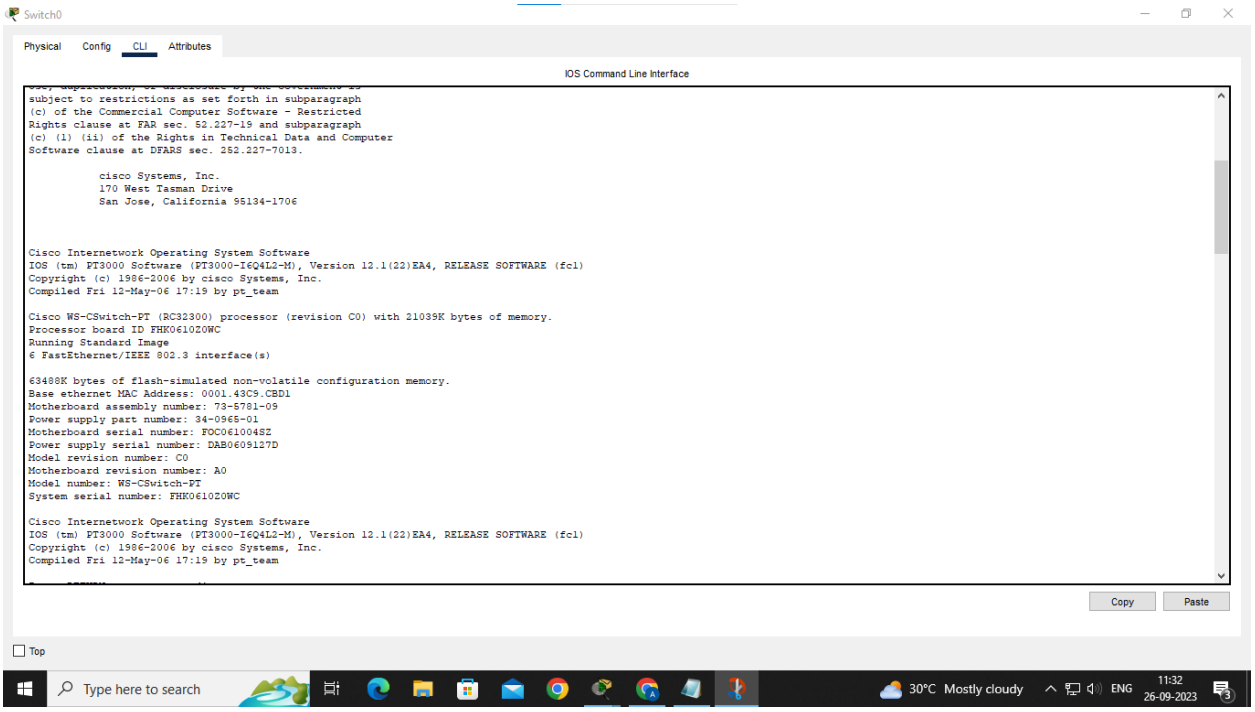
The routing table on Router B will look like:

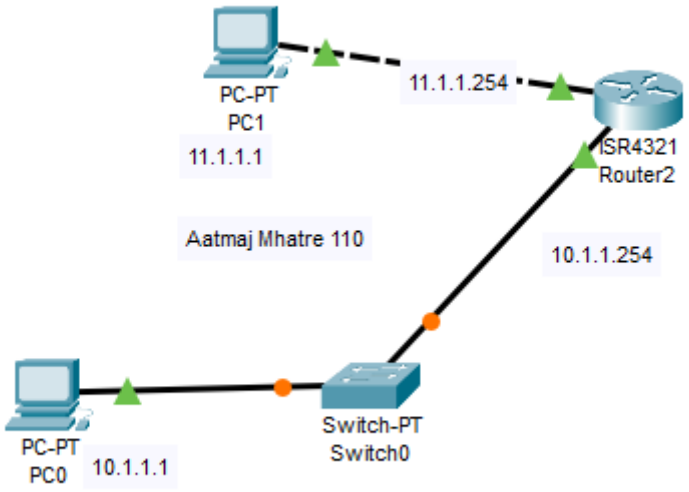
```
RouterB# show ip route

Gateway of last resort is not set
C      172.17.0.0 is directly connected, Serial0
C      172.18.0.0 is directly connected, Ethernet0
R      172.16.0.0 [120/1] via 172.17.1.1, 00:00:00, Serial0
```

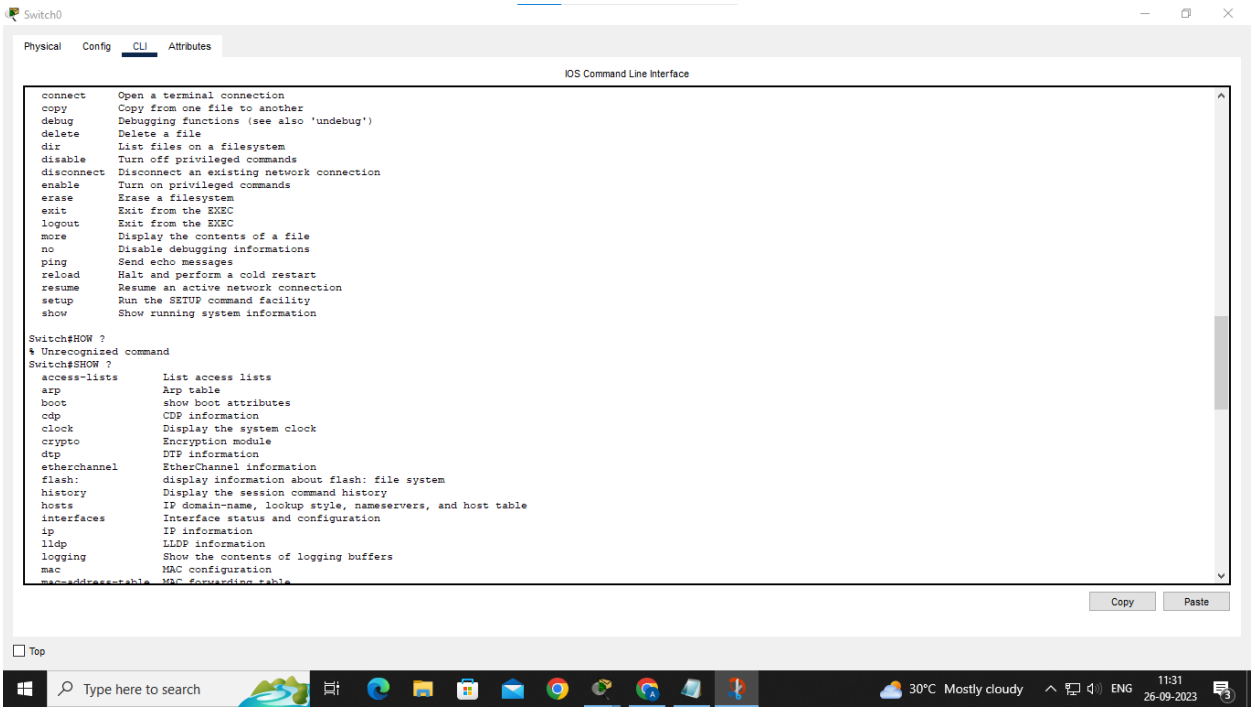


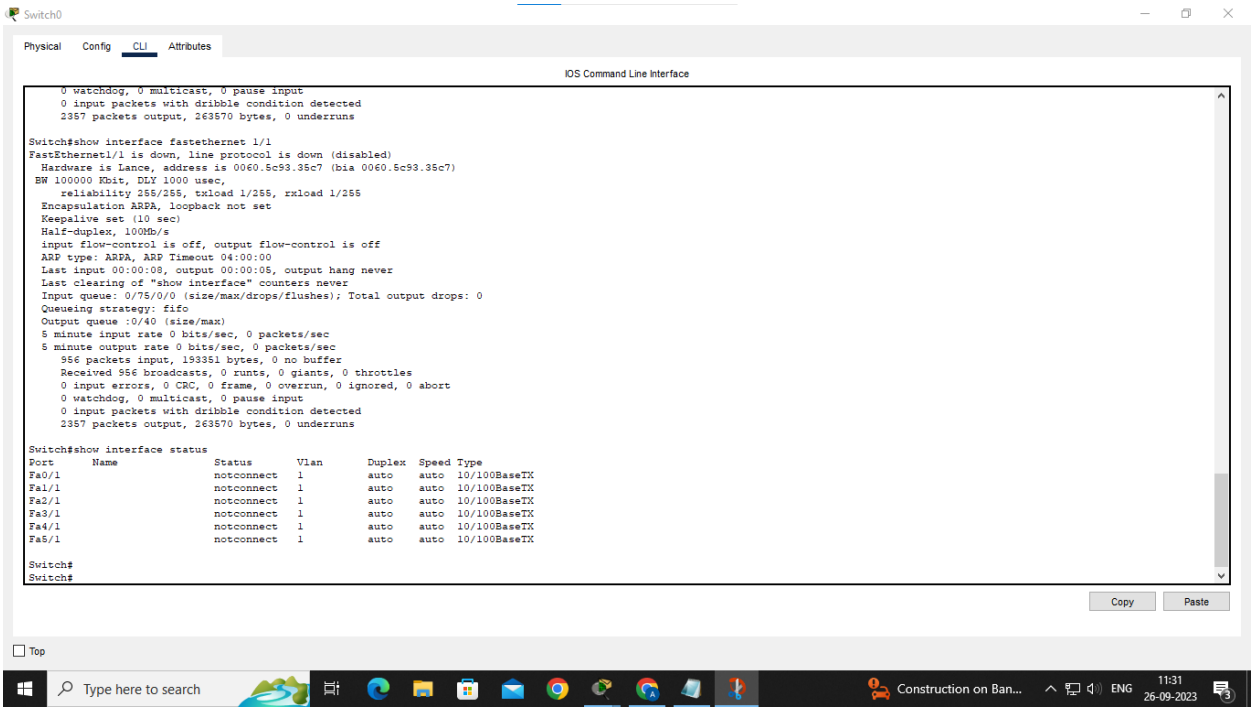

Cisco Packet Tracer
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Pinging 11.1.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 11.1.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.1.1.254
Pinging 10.1.1.254 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.1.254:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 11.1.1.1
Pinging 11.1.1.1 with 32 bytes of data:
Request timed out.
Reply from 11.1.1.1: bytes=32 time<1ms TTL=127
Reply from 11.1.1.1: bytes=32 time<1ms TTL=127
Reply from 11.1.1.1: bytes=32 time=1ms TTL=127
Ping statistics for 11.1.1.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top
Logical
Physical
Realtime
Simulation
Automatically Choose Connection Type
Toggle PDU List Window
Type here to search
30°C Mostly cloudy
ENG
12:22
26-09-2023

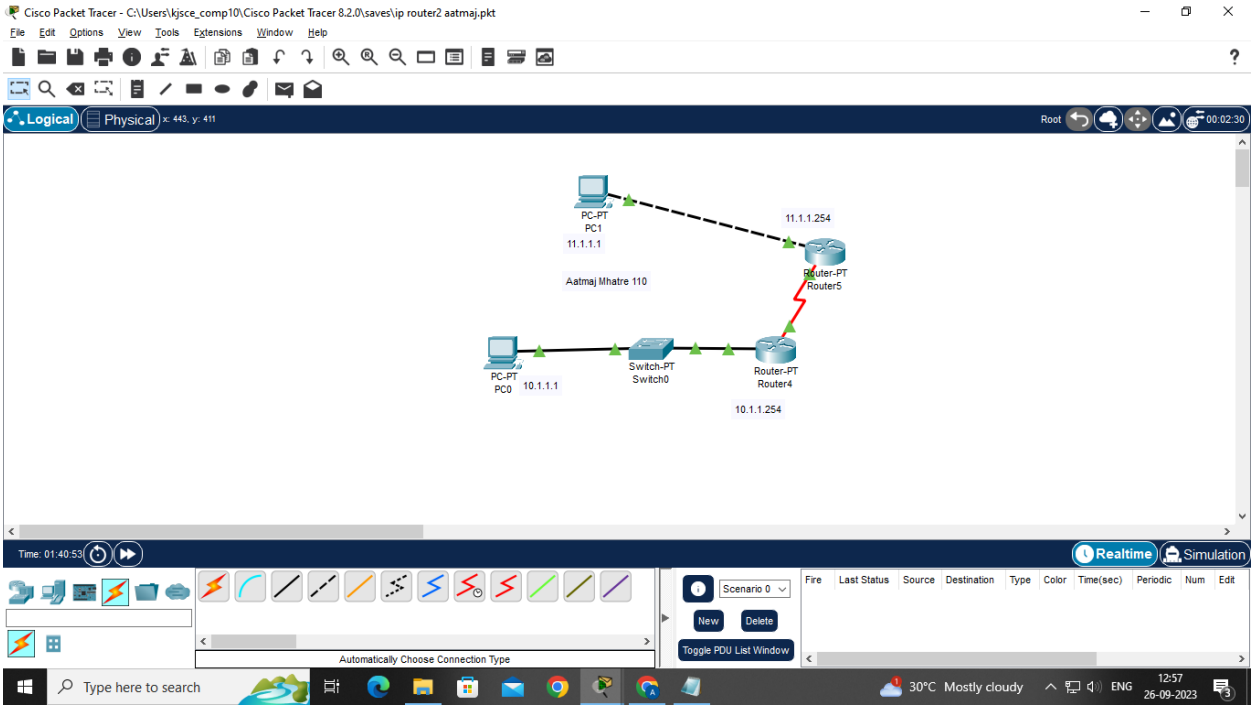

Cisco Packet Tracer
Logical
Physical
11.1.1.254
PC-PT
PC1
11.1.1.1
ISR4321
Router2
10.1.1.254
Aatmaj Mhatre 110
PC-PT
PC0
Switch-PT
Switch0
10.1.1.1
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Type here to search
30°C Mostly cloudy
ENG
12:13
26-09-2023

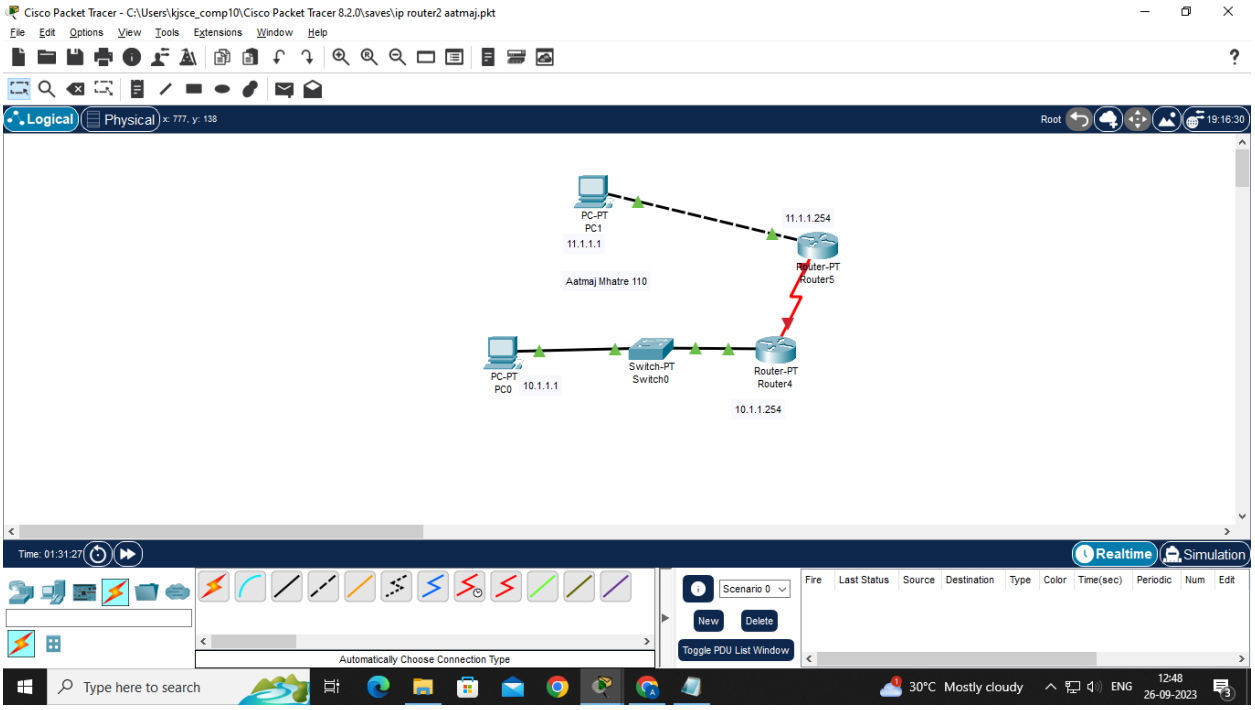

Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) PT3000 Software (PT3000-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Fri 12-May-06 17:19 by pt_team
Cisco WS-CSwitch-PT (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Running Standard Image
6 FastEthernet/IEEE 802.3 interface(s)
63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0001.43C9.CBD1
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-CSwitch-PT
System serial number: FHK0610Z0WC
Cisco Internetwork Operating System Software
IOS (tm) PT3000 Software (PT3000-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Fri 12-May-06 17:19 by pt_team
Copy
Paste
Top
Type here to search
30°C Mostly cloudy
ENG
11:32
26-09-2023


PC-PT
PC1
11.1.1.1
11.1.1.254
ISR4321
Router2
Aatmaj Mhatre 110
10.1.1.254
PC-PT
PC0
10.1.1.1
Switch-PT
Switch0


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
connect Open a terminal connection
copy Copy from one file to another
debug Debugging functions (see also 'undebug')
delete Delete a file
dir List files on a filesystem
disable Turn off privileged commands
disconnect Disconnect an existing network connection
enable Turn on privileged commands
erase Erase a filesystem
exit Exit from the EXEC
logout Exit from the EXEC
more Display the contents of a file
no Disable debugging informations
ping Send echo messages
reload Halt and perform a cold restart
resume Resume an active network connection
setup Run the SETUP command facility
show Show running system information
Switch#HOW ?
% Unrecognized command
Switch#SHOW ?
access-lists List access lists
arp Arp table
boot show boot attributes
cdp CDP information
clock Display the system clock
crypto Encryption module
dtp DTP information
etherchannel EtherChannel information
flash: display information about flash: file system
history Display the session command history
hosts IP domain-name, lookup style, nameservers, and host table
interfaces Interface status and configuration
ip IP information
lldp LLDP information
logging Show the contents of logging buffers
mac MAC configuration
Copy
Paste
Top
Type here to search
30°C Mostly cloudy
ENG
11:31
26-09-2023


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
Switch#show interface fastethernet 1/1
FastEthernet1/1 is down, line protocol is down (disabled)
Hardware is Lance, address is 0060.5c93.35c7 (bia 0060.5c93.35c7)
BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
Switch#show interface status
Port Name Status Vlan Duplex Speed Type
Fa0/1 notconnect 1 auto auto 10/100BaseTX
Fa1/1 notconnect 1 auto auto 10/100BaseTX
Fa2/1 notconnect 1 auto auto 10/100BaseTX
Fa3/1 notconnect 1 auto auto 10/100BaseTX
Fa4/1 notconnect 1 auto auto 10/100BaseTX
Fa5/1 notconnect 1 auto auto 10/100BaseTX
Switch#
Switch#
Copy
Paste
Top
Type here to search
Construction on Ban...
ENG
11:31
26-09-2023


Cisco Packet Tracer - C:\Users\kjsce_comp10\Cisco Packet Tracer 8.2.0\saves\ip router2 aatmaj.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
PC-PT PC1
11.1.1.1
Aatmaj Mhatre 110
11.1.1.254
Router-PT Router5
PC-PT PC0
10.1.1.1
Switch-PT Switch0
Router-PT Router4
10.1.1.254
Realtime Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Type here to search
30°C Mostly cloudy
ENG
12:57
26-09-2023


Cisco Packet Tracer - C:\Users\kjsce_comp10\Cisco Packet Tracer 8.2.0\saves\ip router2 aatmaj.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
PC-PT PC1
11.1.1.1
Aatmaj Mhatre 110
11.1.1.254
Router-PT Router5
PC-PT PC0
10.1.1.1
Switch-PT Switch0
Router-PT Router4
10.1.1.254
Realtime Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Type here to search
30°C Mostly cloudy
ENG
12:48
26-09-2023

CONCLUSION: Thus we have don RIP on few networks using cisco packet tracer. RIP is a protocol used to determining the path in a network.

Post Lab Questions

1. ..... are two popular examples of distance vector routing protocols.
A. OSPF and RIP
B. **RIP and BGP**
C. BGP and OSPF
D. BGP and SPF

2. A ..... routing table contains information entered manually.
A. **static**
B. dynamic
C. hierarchical
D. non static

3. A ..... routing table is updated periodically using one of the dynamic routing protocols.
A. static
B. **dynamic**
C. hierarchical
D. non static

4. Which of the following is not the category of dynamic routing algorithm.
A. Distance vector protocols
B. Link state protocols
C. **Hybrid protocols**
D. Automatic state protocols

5. In ..... forwarding, the mask and destination addresses are both 0.0.0.0 in the routing table.
A. next-hop
B. network-specific
C. host-specific
D. **default**

6. Differentiate between Distance Vector Routing and Link State Routing.

S.No.	Distance Vector Routing	Link State Routing
1.	Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
2.	Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it have knowledge about entire network.
3.	Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
4.	Traffic is less.	Traffic is more.
5.	Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.

6.	Count of infinity problem.	No count of infinity problem.
7.	Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
8.	Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

Date: 10 oct 2023 **Signature of faculty in-charge**

Batch: C2	Roll No.: 110
Experiment / assignment / tutorial No._____	
Grade: AA / AB / BB / BC / CC / CD /DD	

Experiment No.:9

Signature of the Staff In-charge with date

TITLE: Study and configure DHCP & DNS protocol using Cisco Packet tracer

AIM: To study and configure **DHCP/DNS** protocol using Cisco Packet tracer

Expected Outcome of Experiment:
CO:

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

Pre Lab/ Prior Concepts:
IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

New Concepts to be learned: DHCP/DNS Protocol and its configuration.

THEORY:

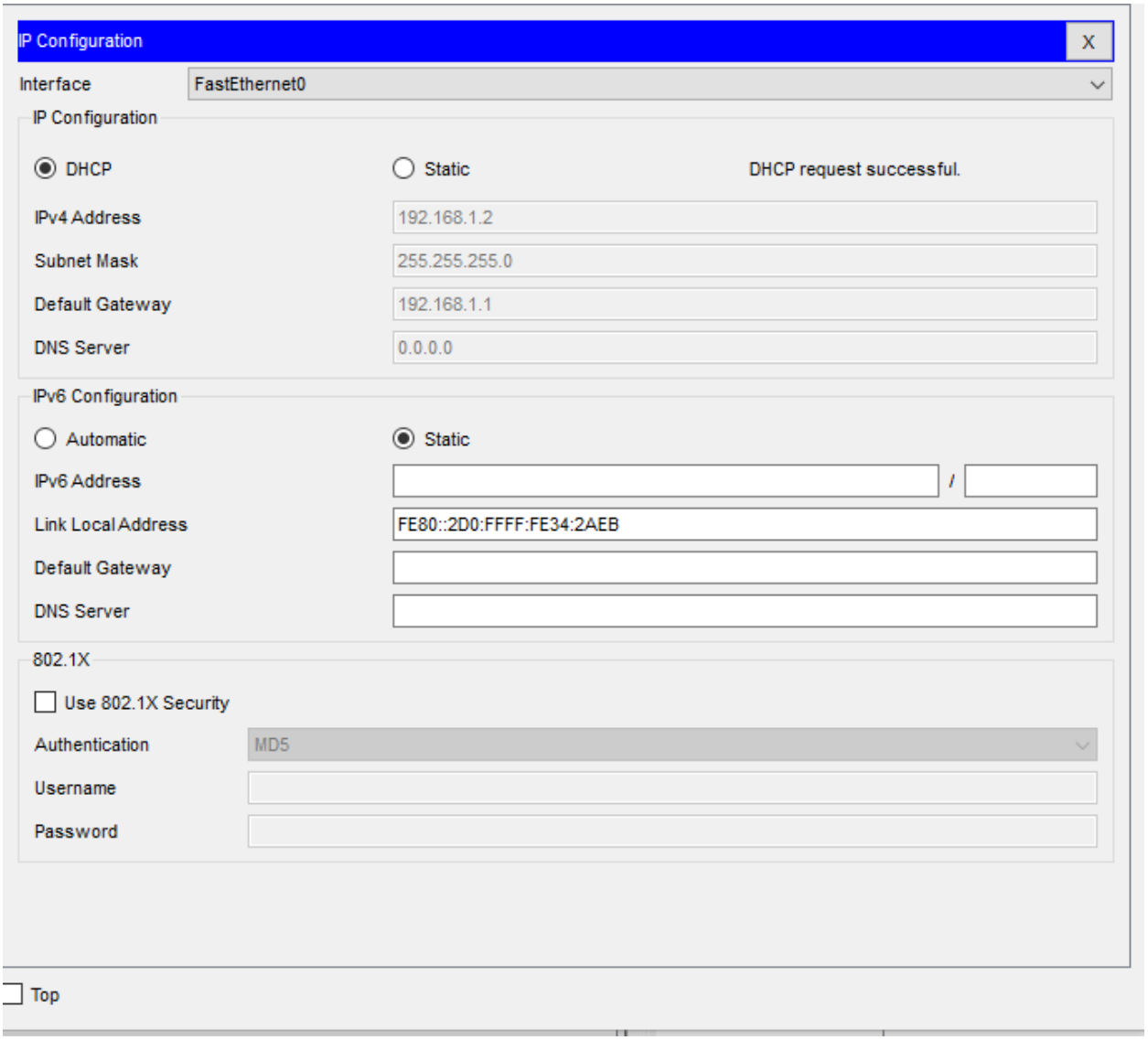
Domain Name System (DNS) is an Internet service that translates domain names (e.g., its.umich.edu) into IP addresses. Dynamic Host Configuration Protocol (DHCP) is a protocol for automatically assigning IP addresses and other configurations to devices when they connect to a network.

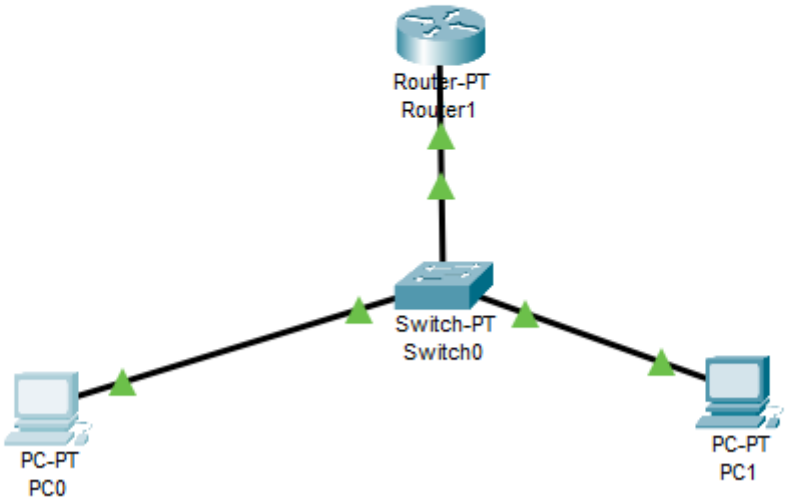
DHCP is a network protocol that is used to assign various network parameters to a device. This greatly simplifies the administration of a network, since there is no need to assign static network parameters for each device.

DHCP is a client-server protocol. A client is a device that is configured to use DHCP to request network parameters from a DHCP server. DHCP server maintains a pool of available IP addresses and assigns one of them to the host. A DHCP server can also provide some other parameters, such as:

- **subnet mask**
- **default gateway**
- **domain name**
- **DNS server**

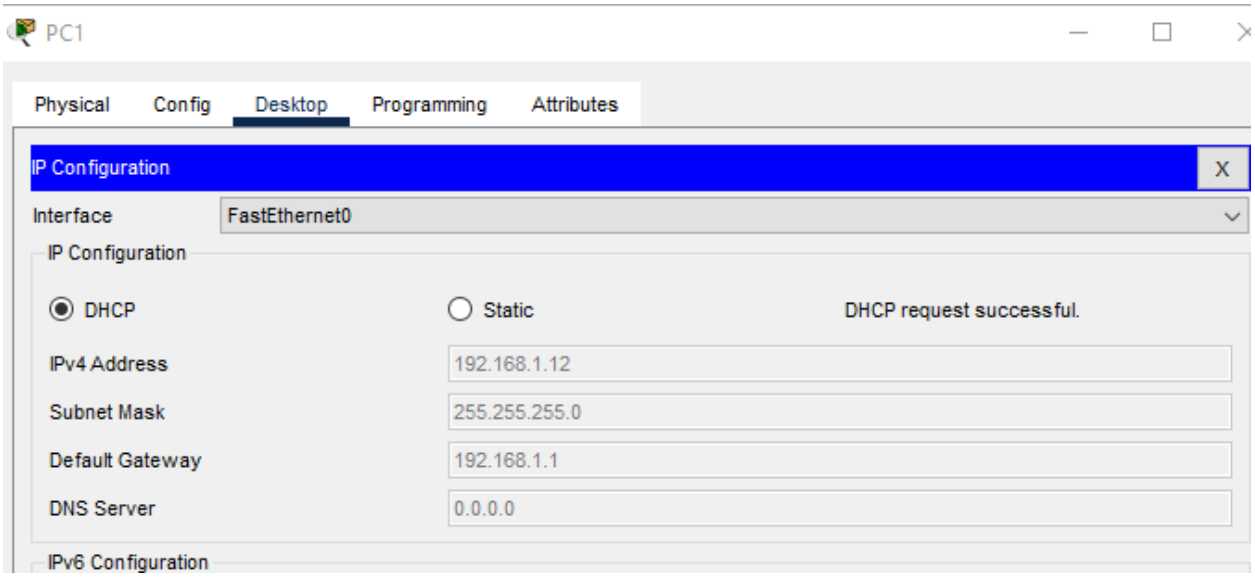
IMPLEMENTATION:


IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:FFFF:FE34:2AEB
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

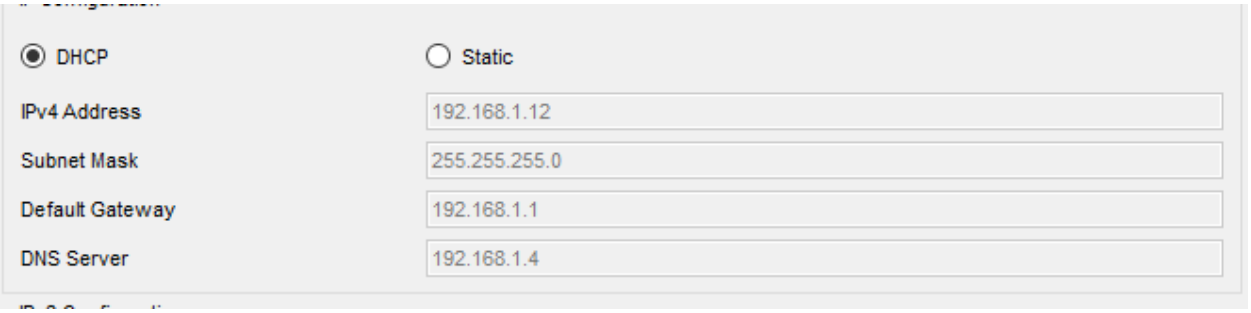


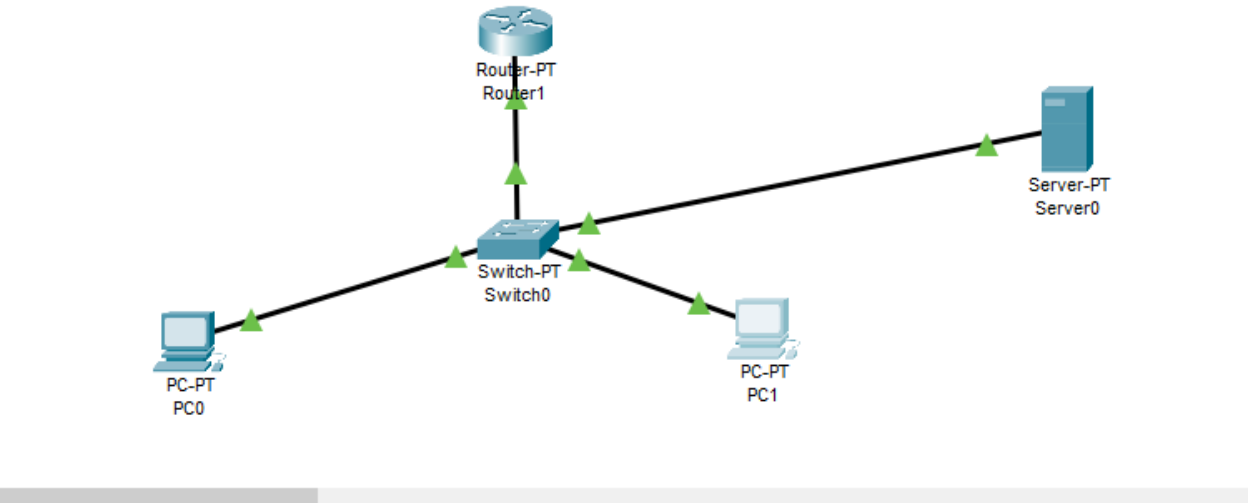

```
Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool computers
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#exit
Router(config)#int fa0/0
Router(config-if)#ip addr 192.168.1.1
% Incomplete command.
Router(config-if)#ip addr 192.168.1.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#
Router(config-if)#
```

After excluding the addresses



AFTER DNS SERVER


DHCP
Static
IPv4 Address
192.168.1.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
192.168.1.4


Router-PT
Router1
Server-PT
Server0
Switch-PT
Switch0
PC-PT
PC0
PC-PT
PC1

CONCLUSION: Thus we have implemented DNS server and DHCP on cisco packet tracer. We made our own custom DNS names and accessed them using DNS.

Date: _____ **Signature of faculty in-charge**

K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

Batch: Roll No.:
Experiment / assignment / tutorial No._____
Grade: AA / AB / BB / BC / CC / CD /DD

Experiment No.:10

Signature of the Staff In-charge with date

TITLE: Study of Packet Analyzer tool: Wireshark

AIM: To study and analyse various Protocols using Packet Analyzer tool: Wireshark

---

Expected Outcome of Experiment:
CO:4

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

---

Pre Lab/ Prior Concepts:
IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

---

New Concepts to be learned: Packet Analyzer tool: Wireshark.

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

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

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

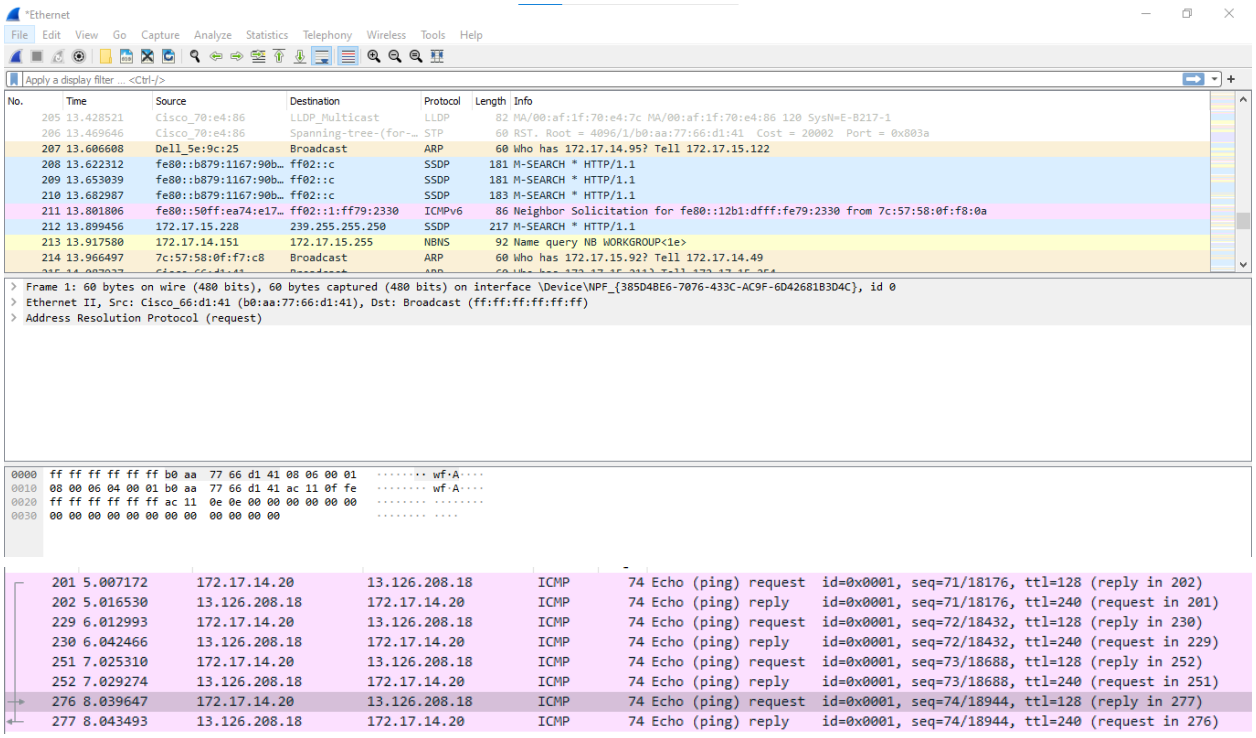
Some intended purposes
Here are some reasons people use Wireshark:

Network administrators use it to troubleshoot network problems
Network security engineers use it to examine security problems
QA engineers use it to verify network applications
Developers use it to debug protocol implementations
People use it to learn network protocol internals
Wireshark can also be helpful in many other situations.

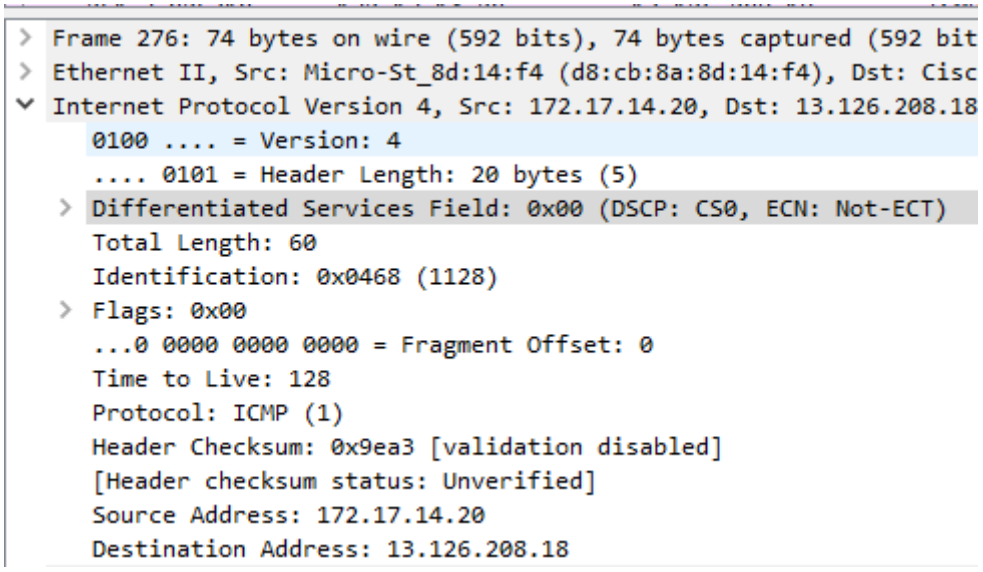
Features
The following are some of the many features Wireshark provides:

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

IMPLEMENTATION:



IP header



Analysis - IPv4
Time to Live is 128 hops
From flags we can say that It is the last fragment and fragmentation is disabled.
Source address and destination address is mentioned in the header.

ARP Header

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 7c:57:58:13:62:8d (7c:57:58:13:62:8d)
    Sender IP address: 172.17.14.112
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 169.254.169.254
```

Analysis

This is a broadcast address hence target mac address is 0 and opcode is request.

arp

No.	Time	Source	Destination	Protocol	Length	Info
280	8.442447	Dell_5b:3a:eb	Broadcast	ARP	60	Who has 172.17.14.143? Tell 172.17.15.136
281	8.442447	Dell_5b:3a:eb	Broadcast	ARP	60	Who has 172.17.15.10? Tell 172.17.15.136
289	8.704113	LCFCHeFe_54:1c:83	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.17.14.231
303	9.126353	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.134? Tell 172.17.14.220
304	9.126735	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.125? Tell 172.17.14.220
305	9.127119	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.131? Tell 172.17.14.220
306	9.127803	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.121? Tell 172.17.14.220
307	9.127803	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.149? Tell 172.17.14.220
308	9.128109	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.23? Tell 172.17.14.220
309	9.128363	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.136? Tell 172.17.14.220
310	9.128602	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.14.66? Tell 172.17.14.220
311	9.128874	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.14.31? Tell 172.17.14.220
312	9.129216	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.166? Tell 172.17.14.220
313	9.129519	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.15.126? Tell 172.17.14.220
314	9.129784	HP_05:b6:56	Broadcast	ARP	60	Who has 172.17.14.164? Tell 172.17.14.220
315	9.144561	Cisco_66:d1:41	Broadcast	ARP	60	Who has 172.17.14.109? Tell 172.17.15.254

TCP:

219	5.674076	74.214.196.131	172.17.14.20	TCP	60	443 → 50665 [FIN, ACK] Seq=40 Ack=1 Win=131 Len=0
220	5.674514	172.17.14.20	74.214.196.131	TCP	54	50665 → 443 [ACK] Seq=1 Ack=41 Win=8212 Len=0
221	5.674709	172.17.14.20	74.214.196.131	TCP	54	50665 → 443 [FIN, ACK] Seq=1 Ack=41 Win=8212 Len=0
222	5.674987	74.214.196.131	172.17.14.20	TCP	60	443 → 50665 [ACK] Seq=41 Ack=2 Win=131 Len=0
223	5.679010	54.164.154.71	172.17.14.20	TCP	60	443 → 50505 [FIN, ACK] Seq=32 Ack=1 Win=176 Len=0
224	5.679354	172.17.14.20	54.164.154.71	TCP	54	50505 → 443 [ACK] Seq=1 Ack=33 Win=8209 Len=0
231	6.046132	52.194.88.39	172.17.14.20	TCP	60	443 → 50491 [FIN, ACK] Seq=32 Ack=1 Win=178 Len=0
232	6.046370	172.17.14.20	52.194.88.39	TCP	54	50491 → 443 [ACK] Seq=1 Ack=33 Win=8210 Len=0
242	6.315406	23.106.127.38	172.17.14.20	TCP	60	443 → 50694 [FIN, ACK] Seq=25 Ack=1 Win=150 Len=0
243	6.316560	172.17.14.20	23.106.127.38	TCP	54	50694 → 443 [ACK] Seq=1 Ack=26 Win=1026 Len=0

```
Source Port: 443
Destination Port: 50665
[Stream index: 36]
[Conversation completeness: Incomplete (28)]
[TCP Segment Len: 0]
Sequence Number: 41    (relative sequence number)
Sequence Number (raw): 2733942633
[Next Sequence Number: 41    (relative sequence number)]
Acknowledgment Number: 2    (relative ack number)
Acknowledgment number (raw): 3103236875
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window: 131
[Calculated window size: 131]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x77cc [unverified]
[Checksum Status: Unverified]
```

Analysis:

Source port is 443 hence it is HTTPS service

UDP:

No.	Time	Source	Destination	Protocol	Length	Info
271	7.530166	172.17.14.62	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
273	7.697625	172.17.14.20	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
274	7.772914	172.17.14.62	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
278	8.394680	172.17.14.222	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
282	8.469500	172.17.14.162	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
283	8.530980	172.17.14.62	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
288	8.677824	172.17.14.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
290	8.711986	172.17.14.20	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
329	9.397407	172.17.14.222	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
331	9.476313	172.17.14.162	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
332	9.531081	172.17.14.62	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
338	9.689382	172.17.14.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
360	10.499060	172.17.14.162	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
361	10.531133	172.17.14.62	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

```
Total Length: 203
Identification: 0x3862 (14434)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0xd5d6 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.17.14.222
Destination Address: 239.255.255.250
```

Analysis:

Total length is packer is 203
checksum: is present
source and destination address is also present.

CONCLUSION:

Thus we have analyzed packets using wireshark. We have understood how different headers work. By using wireshark, we have analyzed the packets and understood how networking works.

Date: 17 oct 2023 **Signature of faculty in-charge**