Experiment No:6

TITLE: Implementation of VLAN

OBJECTIVES:

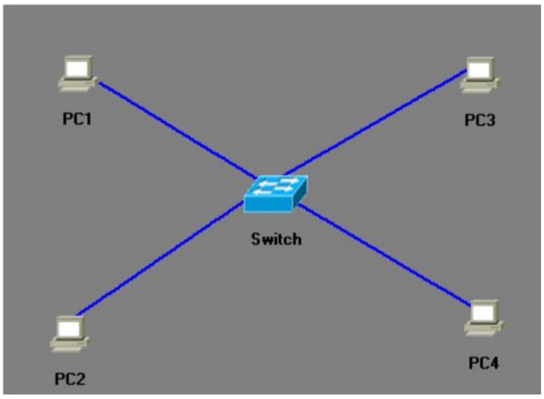
After completing study of this practical the students will be familiarized with… ➢ Concept of VLAN **THEORY:**

VLAN:

- VLAN refers to Virtual Local Area Network
- VLAN that extends its functionalities beyond a single LAN through VLAN a network is divided into different logical segments which known as broadcast domains.
- In technical terms, a VLAN is a broadcast domain created by switches.
- All devices, by default, are in VLAN 1.
- For devices in different VLAN’s to communicate, you must use a router or Layer 3 switch.
- The standard range consists of VLANs 1 to1024.
- The extended range consists of VLANs 1025 to4096.

Create Simple VLAN

We are creating simple VLAN. We will take Four PC & one switch. We will create two VLAN named “VLAN8” and “VLAN9”.Then we put ports 1 & 2 into VLAN8 and ports 3 & 4 into VLAN9.Then we will check how the communication is done between different nodes.



Step 1: configuration of VLAN in Switch

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Vlan_Switch
Vlan_Switch(config)#vlan 8
VLAN8 added: Name:VLAN0008
Vlan_Switch(config)#vlan 8 name ajay
Vlan_Switch(config)#vlan 9 namejashvant
VLAN9 added: Name:jashvant
Vlan_Switch(config)#interface fastethernet0/1
Vlan_Switch(config-if)#switchport mode access
Vlan_Switch(config-if)#switchport access vlan 8
Vlan_Switch(config-if)#exit
Vlan_Switch(config)#interface fastethernet0/2
Vlan_Switch(config-if)#switchport mode access
Vlan_Switch(config-if)#switchport access vlan 8
Vlan_Switch(config-if)#exit
Vlan_Switch(config)#interface fastethernet0/3
Vlan_Switch(config-if)#switchport mode access
Vlan_Switch(config-if)#switchport access vlan 9
Vlan_Switch(config-if)#exit
Vlan_Switch(config)#interface fastethernet0/4
Vlan_Switch(config-if)#switchport mode access
Vlan_Switch(config-if)#switchport access vlan 9
Vlan_Switch(config-if)#exit
```

Step 2: configuration of PC.

PC1

```
IPAddress : 10.1.1.1
SubnetMask : 255.0.0.0
DefaultGateway : 10.1.1.4
```

PC2

```
IPAddress : 10.1.1.2
SubnetMask : 255.0.0.0
DefaultGateway : 10.1.1.4
```

PC3

```
IPAddress : 10.1.1.3
SubnetMask : 255.0.0.0
DefaultGateway : 10.1.1.4
```

PC4

```
IPAddress : 10.1.1.4
SubnetMask : 255.0.0.0
DefaultGateway : 10.1.1.4
```

PC1:>ping 10.1.1.2

```
Pinging 10.1.1.2 with 32 bytes of data:

    Replyfrom10.1.1.2:bytes=32  time=60msTTL=241
    Replyfrom10.1.1.2:bytes=32  time=60msTTL=241
```

```
        Replyfrom10.1.1.2:bytes=32  time=60msTTL=241 Replyfrom10.1.1.2:bytes=32
        time=60msTTL=241

        Replyfrom10.1.1.2:bytes=32  time=60msTTL=241
        Replyfrom10.1.1.2:bytes=32  time=60msTTL=241
Ping statistics for 10.1.1.2:       Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average =55ms
```

PC1:>ping 10.1.1.3

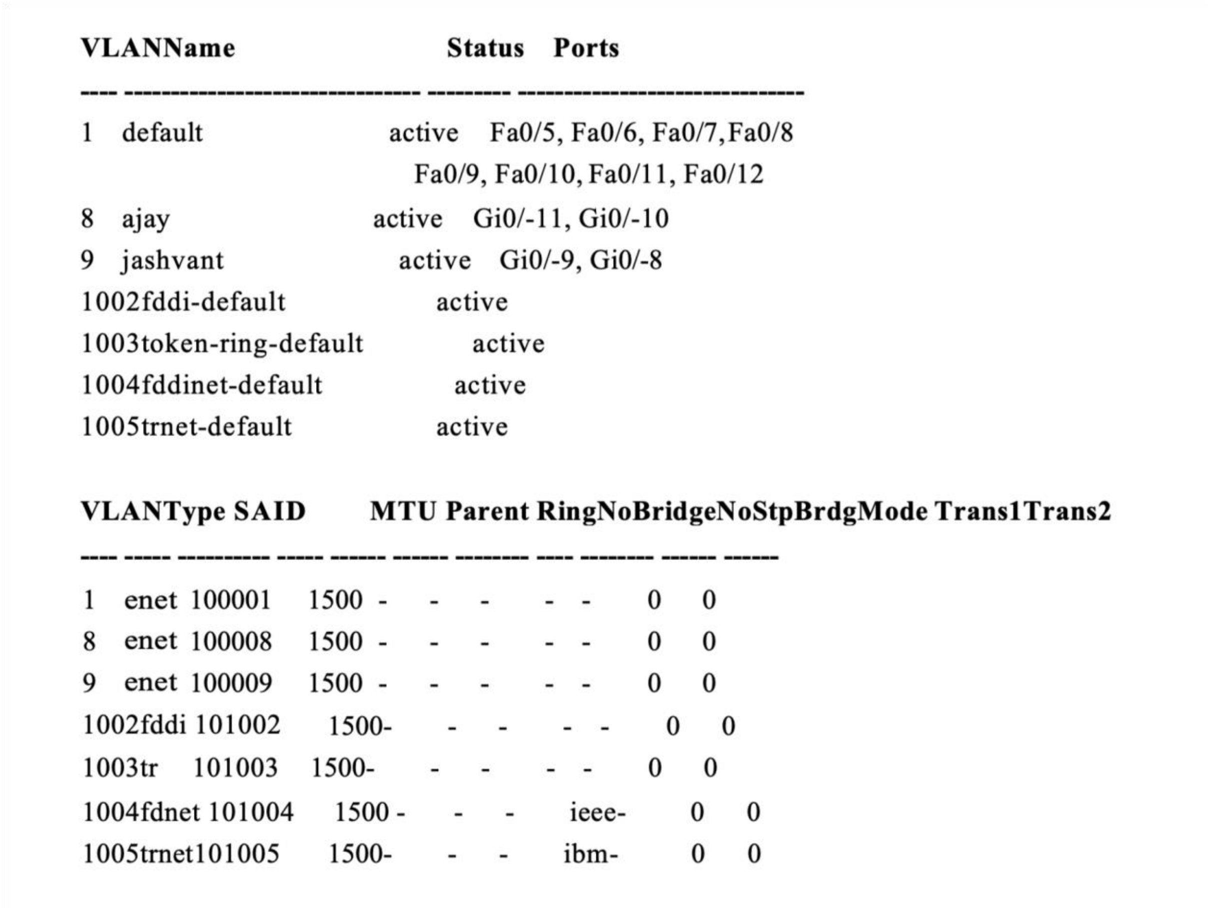
```
Pinging 10.1.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.3: Packets: Sent = 5, Received = 5, Lost = 0 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average =0ms
```

PC1:>ping 10.1.1.4

```
Pinging 10.1.1.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.4: Packets: Sent = 5, Received = 5, Lost = 0 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average =0ms
```

Step 4: Verify Configuration.

```
Vlan_Switch#
Vlan_Switch#showvlan
```

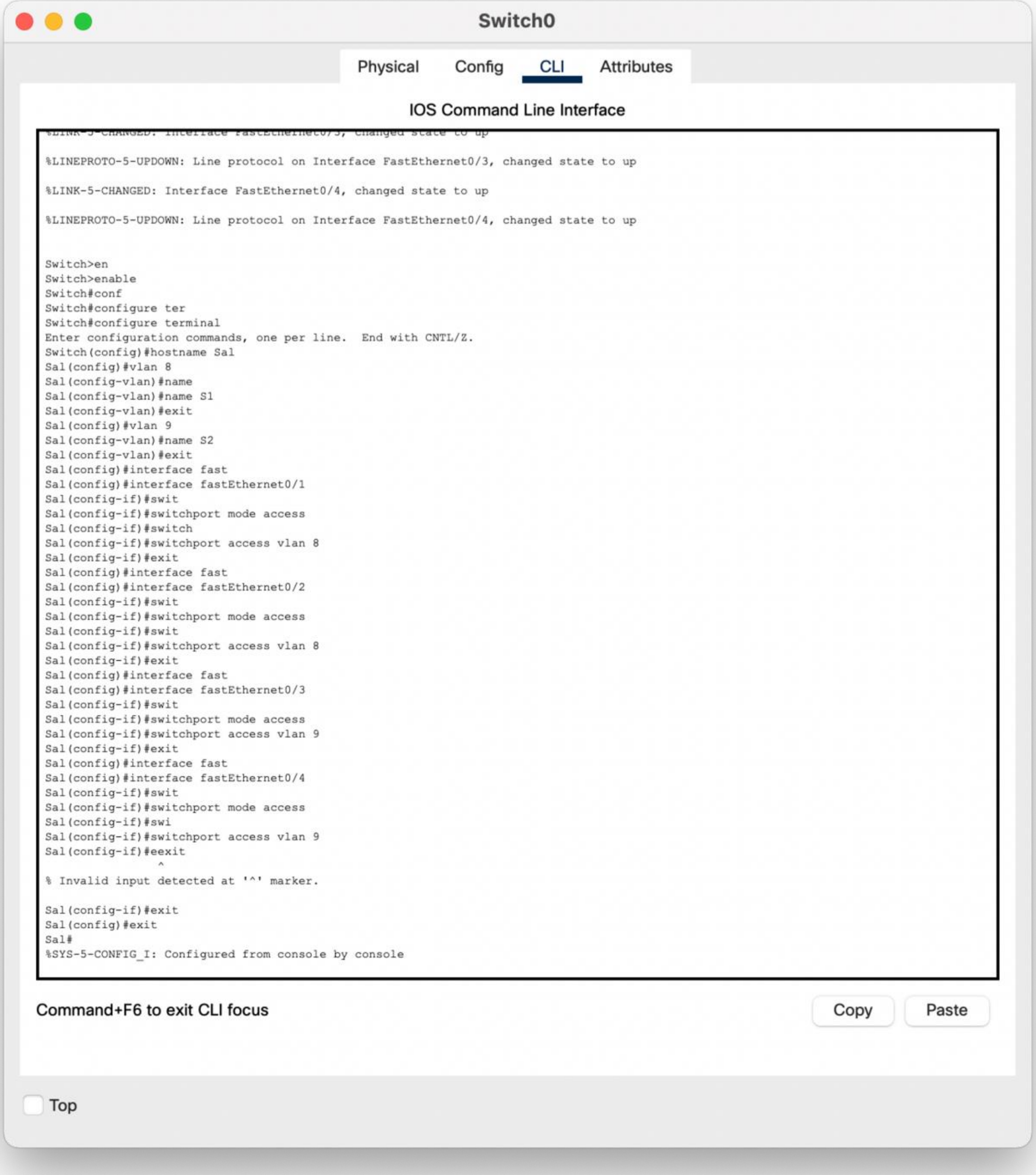


```
VLANName                          Status    Ports
---- ------------------------------ --------- ------------------------------
1    default                      active    Fa0/5, Fa0/6, Fa0/7,Fa0/8
                                     Fa0/9, Fa0/10, Fa0/11, Fa0/12
8    ajay                       active    Gi0/-11, Gi0/-10
9    jashvant                     active    Gi0/-9, Gi0/-8
1002fddi-default                active
1003token-ring-default              active
1004fddinet-default                active
1005trnet-default               active

VLANType SAID       MTU Parent RingNoBridgeNoStpBrdgMode Trans1Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001    1500 -    -    -      - -      0    0
8    enet  100008    1500 -    -    -      - -      0    0
9    enet  100009    1500 -    -    -      - -      0    0
1002fddi 101002      1500-      -    -      - -      0    0
1003tr    101003    1500-      -    -      - -      0    0
1004fdnet 101004     1500 -      -    -     ieee-      0    0
1005trnet101005      1500-      -    -    ibm-       0    0
```

EXCERCISE:

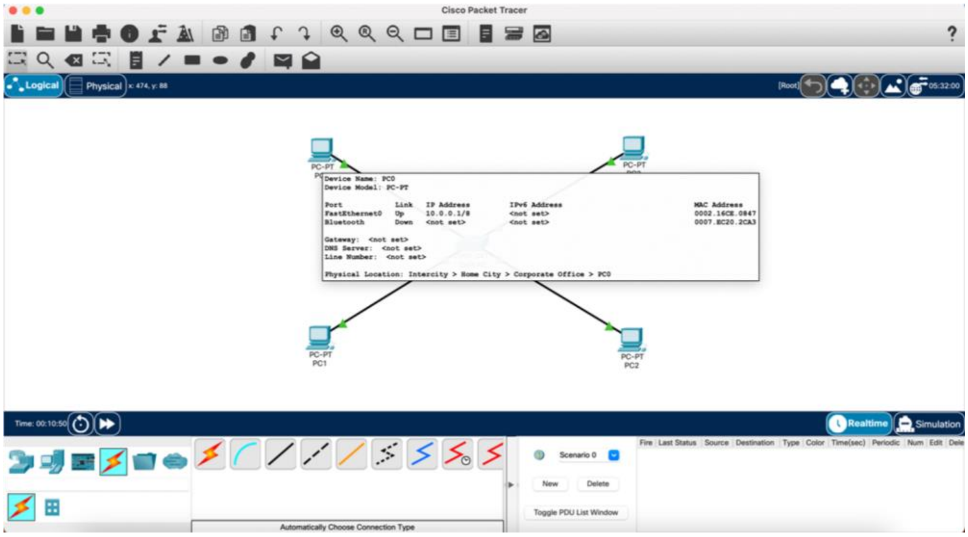
1) Create the Two VLAN from one LAN and write the configuration steps.

Step 1: configuration of VLAN in Switch

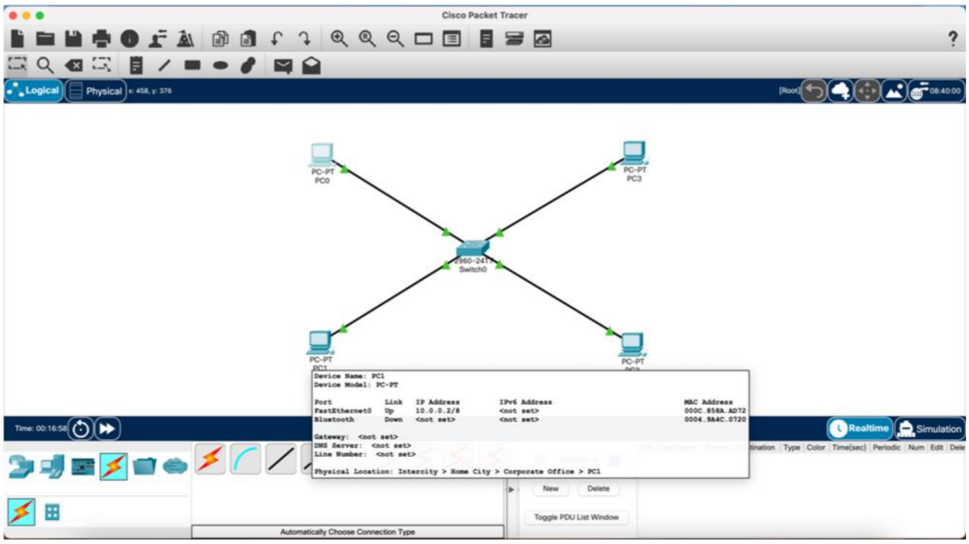


```
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up


Switch>en
Switch>enable
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sal
Sal(config)#vlan 8
Sal(config-vlan)#name
Sal(config-vlan)#name S1
Sal(config-vlan)#exit
Sal(config)#vlan 9
Sal(config-vlan)#name S2
Sal(config-vlan)#exit
Sal(config)#interface fast
Sal(config)#interface fastEthernet0/1
Sal(config-if)#swit
Sal(config-if)#switchport mode access
Sal(config-if)#switch
Sal(config-if)#switchport access vlan 8
Sal(config-if)#exit
Sal(config)#interface fast
Sal(config)#interface fastEthernet0/2
Sal(config-if)#swit
Sal(config-if)#switchport mode access
Sal(config-if)#swit
Sal(config-if)#switchport access vlan 8
Sal(config-if)#exit
Sal(config)#interface fast
Sal(config)#interface fastEthernet0/3
Sal(config-if)#swit
Sal(config-if)#switchport mode access
Sal(config-if)#switchport access vlan 9
Sal(config-if)#exit
Sal(config)#interface fast
Sal(config)#interface fastEthernet0/4
Sal(config-if)#swit
Sal(config-if)#switchport mode access
Sal(config-if)#swi
Sal(config-if)#switchport access vlan 9
Sal(config-if)#eexit
                ^
% Invalid input detected at '^' marker.

Sal(config-if)#exit
Sal(config)#exit
Sal#
%SYS-5-CONFIG_I: Configured from console by console
```

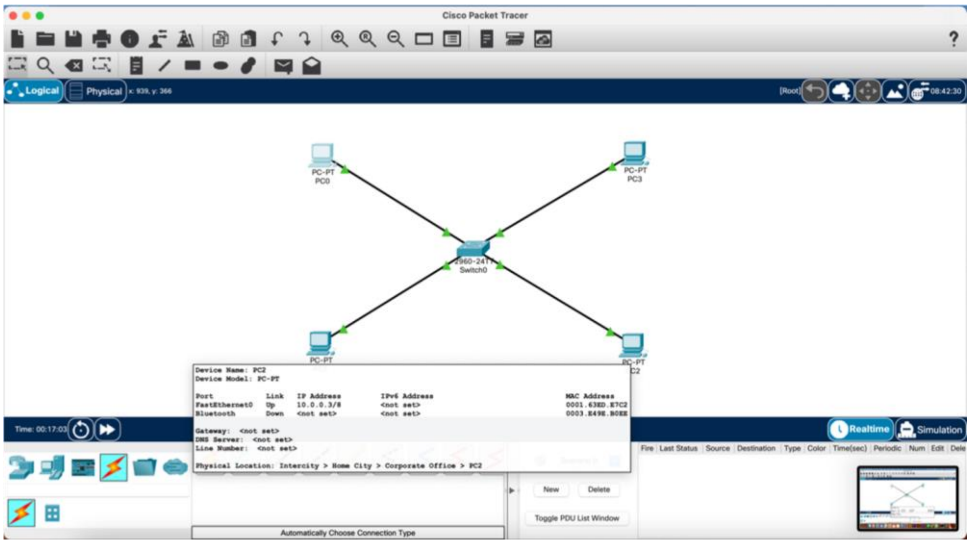
Step 2: configuration of PC.



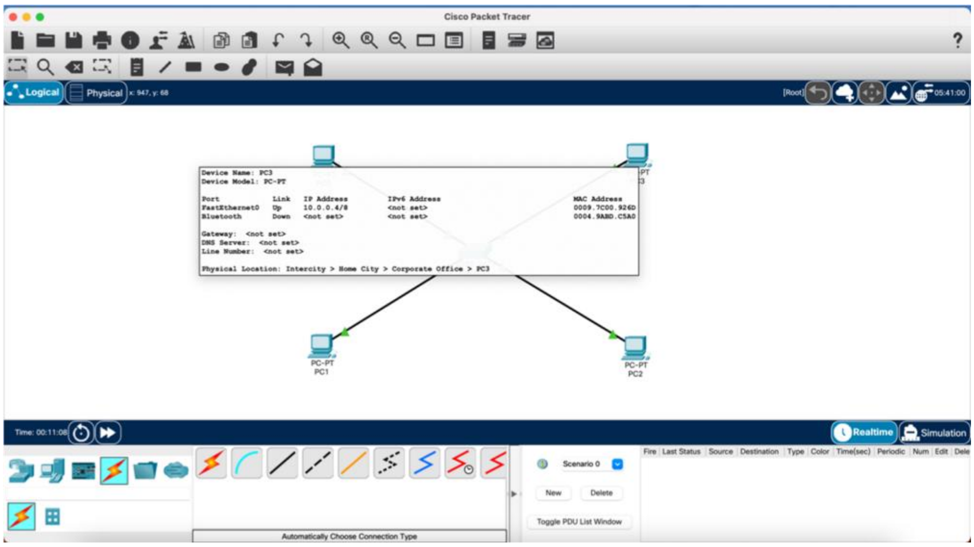
```
Device Name: PC0
Device Model: PC-PT

Port            Link   IP Address         IPv6 Address                      MAC Address
FastEthernet0   Up     10.0.0.1/8         <not set>                         0002.16CE.0847
Bluetooth       Down   <not set>          <not set>                         0007.EC20.2CA3

Gateway:  <not set>
DNS Server:  <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC0
```



```
Device Name: PC1
Device Model: PC-PT

Port            Link   IP Address         IPv6 Address                      MAC Address
FastEthernet0   Up     10.0.0.2/8         <not set>                         000C.858A.AD72
Bluetooth       Down   <not set>          <not set>                         0004.9A4C.0720

Gateway:  <not set>
DNS Server:  <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC1
```

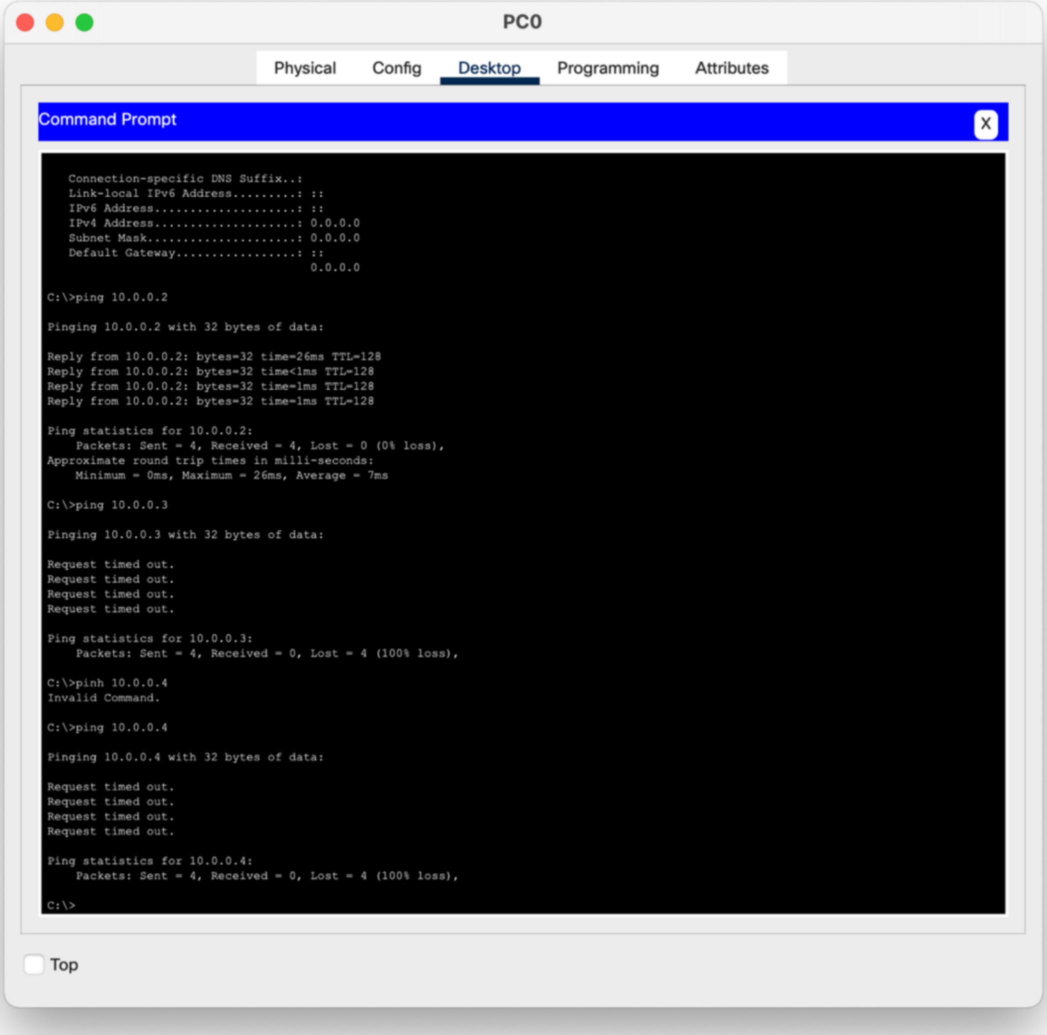


```
Device Name: PC2
Device Model: PC-PT

Port            Link   IP Address         IPv6 Address                      MAC Address
FastEthernet0   Up     10.0.0.3/8         <not set>                         0001.63ED.E7C2
Bluetooth       Down   <not set>          <not set>                         0003.E49E.B0EE

Gateway:  <not set>
DNS Server:  <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC2
```



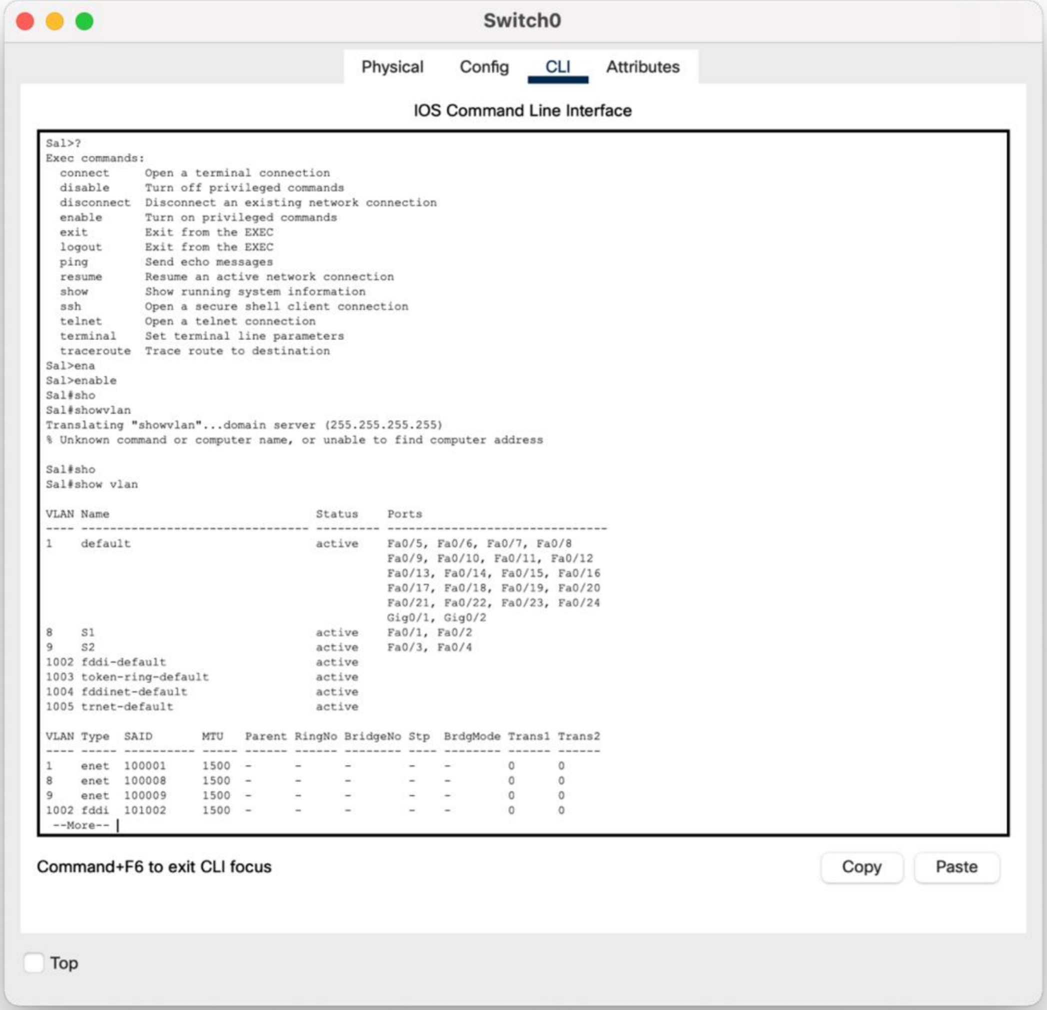
```
Device Name: PC3
Device Model: PC-PT

Port            Link   IP Address       IPv6 Address                 MAC Address
FastEthernet0   Up     10.0.0.4/8       <not set>                    0009.7C00.926D
Bluetooth       Down   <not set>        <not set>                    0004.9ABD.C5A0

Gateway:  <not set>
DNS Server:  <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC3
```

Step 3: Ping command.

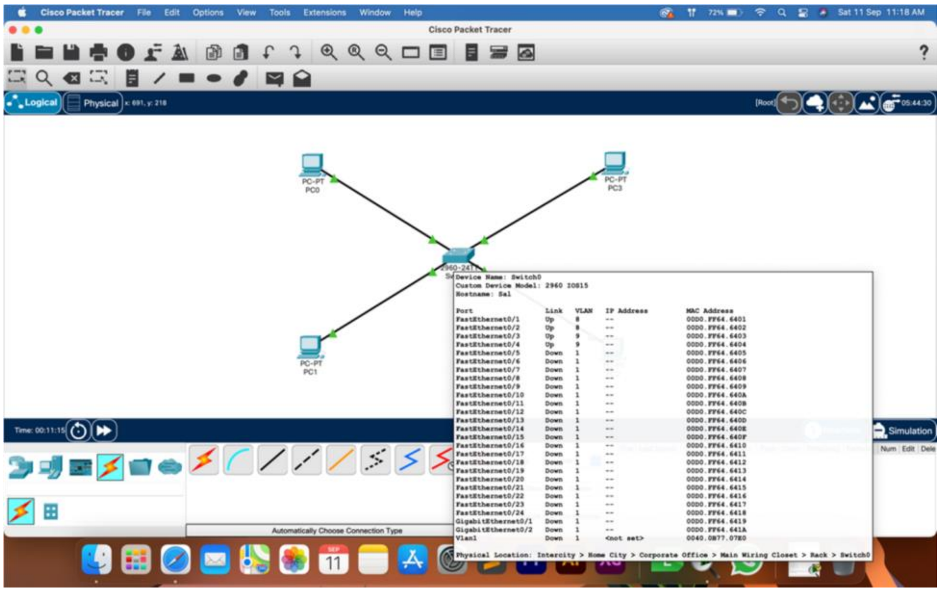


```
   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=26ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time=1ms TTL=128
Reply from 10.0.0.2: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 26ms, Average = 7ms

C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>pinh 10.0.0.4
Invalid Command.

C:\>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Step 4: Verify Configuration.



```
Sa1>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Sa1>ena
Sa1>enable
Sa1#sho
Sa1#showvlan
Translating "showvlan"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Sa1#sho
Sa1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
8    S1                               active    Fa0/1, Fa0/2
9    S2                               active    Fa0/3, Fa0/4
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
8    enet  100008     1500  -      -      -        -    -        0      0
9    enet  100009     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More--
```



```
Device Name: Switch0
Custom Device Model: 2960 IOS15
Hostname: Sa1

Port                 Link   VLAN   IP Address         MAC Address
FastEthernet0/1      Up     8      --                 00D0.FF64.6401
FastEthernet0/2      Up     8      --                 00D0.FF64.6402
FastEthernet0/3      Up     9      --                 00D0.FF64.6403
FastEthernet0/4      Up     9      --                 00D0.FF64.6404
FastEthernet0/5      Down   1      --                 00D0.FF64.6405
FastEthernet0/6      Down   1      --                 00D0.FF64.6406
FastEthernet0/7      Down   1      --                 00D0.FF64.6407
FastEthernet0/8      Down   1      --                 00D0.FF64.6408
FastEthernet0/9      Down   1      --                 00D0.FF64.6409
FastEthernet0/10     Down   1      --                 00D0.FF64.640A
FastEthernet0/11     Down   1      --                 00D0.FF64.640B
FastEthernet0/12     Down   1      --                 00D0.FF64.640C
FastEthernet0/13     Down   1      --                 00D0.FF64.640D
FastEthernet0/14     Down   1      --                 00D0.FF64.640E
FastEthernet0/15     Down   1      --                 00D0.FF64.640F
FastEthernet0/16     Down   1      --                 00D0.FF64.6410
FastEthernet0/17     Down   1      --                 00D0.FF64.6411
FastEthernet0/18     Down   1      --                 00D0.FF64.6412
FastEthernet0/19     Down   1      --                 00D0.FF64.6413
FastEthernet0/20     Down   1      --                 00D0.FF64.6414
FastEthernet0/21     Down   1      --                 00D0.FF64.6415
FastEthernet0/22     Down   1      --                 00D0.FF64.6416
FastEthernet0/23     Down   1      --                 00D0.FF64.6417
FastEthernet0/24     Down   1      --                 00D0.FF64.6418
GigabitEthernet0/1   Down   1      --                 00D0.FF64.6419
GigabitEthernet0/2   Down   1      --                 00D0.FF64.641A
Vlan1                Down   1      <not set>          0040.0B77.07E0

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch0
```

QUIZ:

Answer the Followings:

1) Give different types of VLAN.

Virtual LAN (VLAN) is created on Layer 2 switch to reduce the size of broadcast domain. It is one of the technologies used to improve network performance by the separation of large broadcast domains into smaller ones.

There are 5 main types of VLANs depending on the type of the network they carry:

Default VLAN –

When the switch initially starts up, all switch ports become a member of the default VLAN (generally all switches have default VLAN named as VLAN 1), which makes them all part of the same broadcast domain. Using default VLAN allows any network device connected to any of the switch port to connect with other devices on other switch ports. One unique feature of Default VLAN is that it can't be rename or delete.

Data VLAN –

Data VLAN is used to divide the whole network into 2 groups. One group of users and other group of devices. This VLAN also known as a user VLAN, the data VLAN is used only for user-generated data. This VLAN carrying data only. It is not used for carrying management traffic or voice.

Voice VLAN –

Voice VLAN is configured to carry voice traffic. Voice VLANs are mostly given high transmission priority over other types of network traffic. To ensure voice over IP (VoIP) quality (delay of less than 150 milliseconds (ms) across the network), we must have separate voice VLAN as this will preserve bandwidth for other applications.

Management VLAN –

A management VLAN is configured to access the management capabilities of a switch (traffic like system logging, monitoring). VLAN 1 is the management VLAN by default (VLAN 1 would be a bad choice for the management VLAN). Any of a switch VLAN could be define as the management VLAN if admin as not configured a unique VLAN to serve as the management VLAN. This VLAN ensures that bandwidth for management will be available even when user traffic is high.

Native VLAN –

This VLAN identifies traffic coming from each end of a trunk link. A native VLAN is allocated only to an 802.1Q trunk port. The 802.1Q trunk port places untagged traffic (traffic that does not come from any VLAN) on the native VLAN. It is a best to configure the native VLAN as an unused VLAN.

2) List out advantages of VLAN.

- It solves a broadcast problem.
- VLAN reduces the size of broadcast domains.
- VLAN allows you to add an additional layer of security.
- It can make device management simple and easier.
- You can make a logical grouping of devices by function rather than location.
- It allows you to create groups of logically connected devices that act like they are on their own network.
- You can logically segment networks based on departments, project teams, or functions.
- VLAN helps you to geographically structure your network to support the growing companies.
- Higher performance and reduced latency.
- VLANs provide increased performance.
- Users may work on sensitive information that must not be viewed by other users.
- VLAN removes the physical boundary.
- It lets you easily segment your network.
- It helps you to enhance network security.
- You can keep hosts separated by VLAN.
- You do not require additional hardware and cabling, which helps you to saves costs.
- It has operational advantages because of changing the IP subnet of the user is in software.
- It reduces the number of devices for particular network topology.
- VLAN makes managing physical devices less complex.

EVALUATION:

Involvement (4)	Understanding / Problem solving (3)	Timely Completion (3)	**Total** **(10)**

Experiment No:7

TITLE: IP Addressing Basics

OBJECTIVES:

- After completing this experiment students will be able to…
- Describe the characteristics and use of the different IP address classes
- Identify the class of an IP address based on the network number
- Determine which part, or octet, of an IP address is the network ID and which part is the host ID
- Identify valid and invalid IP host addresses based on the rules of IP addressing
- Define the range of addresses and default subnet mask for each class

THEORY:

- IP addresses are used to uniquely identify individual TCP/IP networks and hosts, such as computers and printers, on those networks in order for devices to communicate. Workstations and servers on a TCP/IP network are called hosts and each has a unique IP address.
- This address is referred to as its host address.
- TCP/IP is the most widely used protocol in the world.
- The Internet or World Wide Web only uses IP addressing.
- In order for a host to access the Internet, it must have an IP address.
- In its basic form, the IP address has two parts:
    - A network addresses o A host addresses
- IP addresses are 32 bits long according to the current version IPv4 and are divided into 4 octets of 8 bits each.
- They operate at the network layer (Layer 3) of the Open System Interconnection (OSI) model, which is the Internet layer of the TCP/IP model.
- IP addresses are assigned in the following ways:
    - Statically – manually, by a network administrator
    - Dynamically – automatically, by a Dynamic Host Configuration Protocol (DHCP)server
- The IP address of a workstation or host is a logical address, meaning it can be changed.
- The Media Access Control (MAC) address of the workstation is a 48-bit physical address.
- This address is burned into the network interface card (NIC) and cannot change unless the NIC is replaced.
- The combination of the logical IP address and the physical MAC address helps route packets to their proper destination
- There are five different classes of IP addresses, and depending on the class, the network and host part of the address will use a different number of bits.

Step 1: Review IP address classes and their characteristics

Address classes

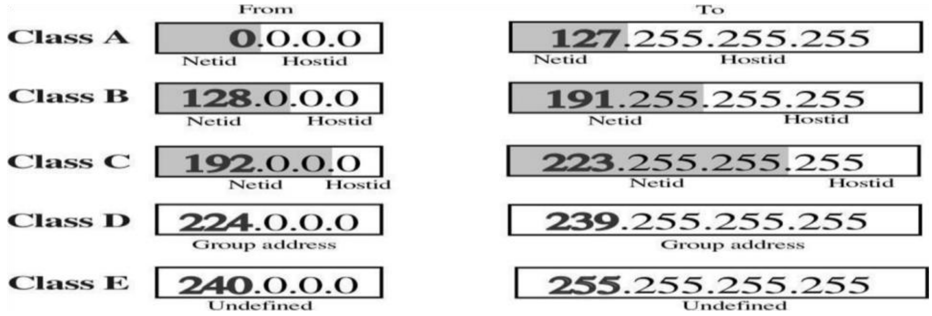
- There are five classes of IP addresses, A through.
- Only the first three classes are used commercially.
- The first column is the class of IP address. The second column is the first octet, which must fall within the range shown for a given class of addresses.
- The Class A address must start with a number between 1 and126.
- The first bit of a Class A address is always a zero, meaning the High Order Bit (HOB) or the 128 bit cannot be used. 127 is reserved for loopback testing.

Default subnet mask

- The default subnet mask uses all binary ones, decimal 255, to mask the first 8 bits of the Class A address.
- The default subnet mask helps routers and hosts determine if the destination host is on this network or another one.
- Because there are only 126 Class A networks, the remaining 24 bits, or 3 octets, can be used for hosts.
- Each Class A network can have 224, or over 16 million hosts. It is common to subdivide the network into smaller groupings called subnets

Network and host address

- The network or host portion of the address cannot be all ones or allegros.
- As an example, the Class A address of 118.0.0.5 is a valid IP address.
- The network portion, or first 8 bits, which are equal to 118, is not all zeros and the host portion, or last 24 bits, is not all zeros or all ones. If the host portion were all zeros, it would be the network address itself.
- If the host portion were all ones, it would be a broadcast for the network address. The value of any octet can never be greater than decimal 255 or binary11111111.



	From	To
Class A	0.0.0.0 Netid Hostid	127.255.255.255 Netid Hostid
Class B	128.0.0.0 Netid Hostid	191.255.255.255 Netid Hostid
Class C	192.0.0.0 Netid Hostid	223.255.255.255 Netid Hostid
Class D	224.0.0.0 Group address	239.255.255.255 Group address
Class E	240.0.0.0 Undefined	255.255.255.255 Undefined

Step 2: Determine basic IP addressing

Use the IP address chart and your knowledge of IP address classes to answer the following questions:

1. What is the decimal and binary range of the first octet of all possible Class B IP addresses?

A) Decimal: From: **128.0.0.0** To: **191.255.255.255**
Binary: From: **10000000.0.0.0** To: **10111111.1.1.1**

2. Which octet(s) represent the network portion of a Class C IP address?

A) Class C. In a Class C IP address, the network portion is represented by **the first, second, and third octets**; it has 110 (192) in its three leftmost bits.

3. Which octet(s) represent the host portion of a Class A IP address?

A) Class A addresses were intended to accommodate very large networks, so only the first octet is used to represent the network number. This leaves three octets, or 24 bits, to represent the host portion of the address. It has 0.0.0.0 to 127.255.255.255.

4. What is the maximum number of useable hosts with a Class C network address?

A) Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts--the maximum being 254. A class C network number occupies the first three bytes of an IP address.

5. How many Class B networks are there?

A) 0.0 to 191.255. 0.0 as Class B networks. There are 16,384 possible Class B networks.

6. How many hosts can each Class B network have?

A) 0.0 to 191.255. 0.0 as Class B networks. There are 65,534 possible host Class B can have.

7. How many octets are there in an IP address?

A) There are **four** octets in IP addresses. IP addresses are split up into **four** eight-bit numbers called octets for readability.

8. How many bits per octet?

A) The octet is a unit of digital information in computing and telecommunications that consists of **eight bits.**

Step 3: Given an IP address of 142.226.0.15 and a subnet mask of 255.255.255.0, answer the following questions:

1. What is the binary equivalent of the second octet? A) 11100010

2. What is the class of the address? A) class B

3. What is the network address of this IP address? A) 142.226.0.0

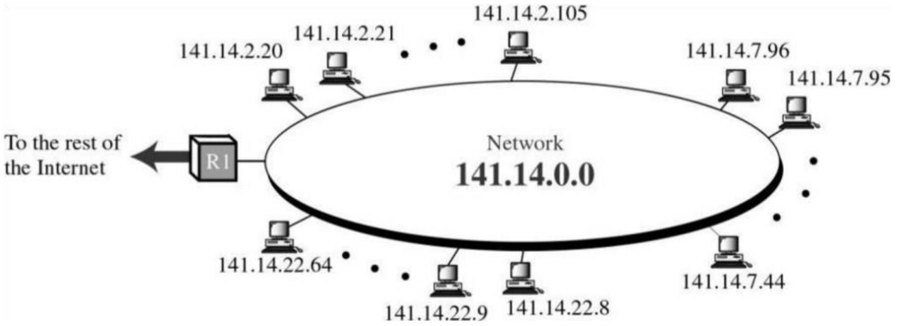
Step 4: Determine which IP host addresses are valid for commercial networks

For the following IP host addresses, determine which are valid for commercial networks
Fill in the following table

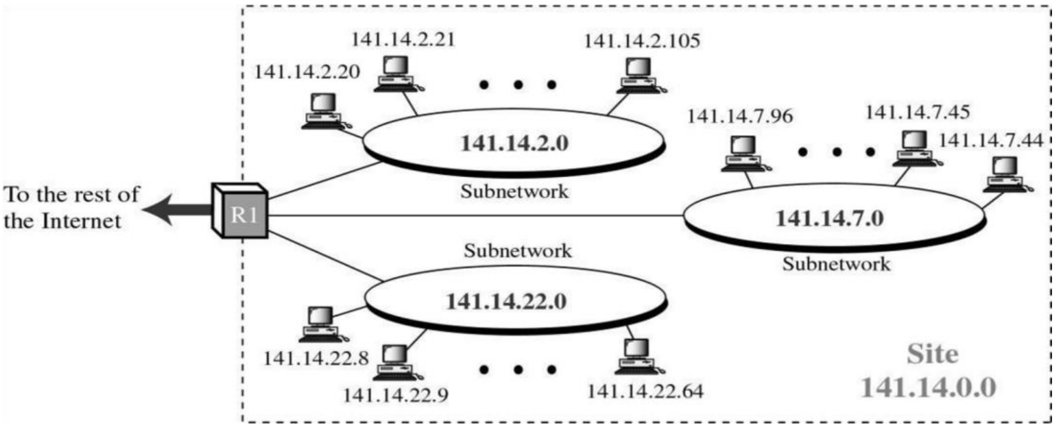
IP Host Address	**Valid Address? (Yes/No)**	**Why or Why Not**
150.100.255.255	No	Class B broadcast address – not valid IP for host
175.100.255.18	Yes	Valid Class B host address
195.234.253.0	No	Class C network address – not valid IP for host
100.0.0.23	Yes	Valid Class A host address
188.258.221.176	No	Invalid 2nd octet; is > 255
127.34.25.189	No	Reserved for loopback and diagnostic functions
224.156.217.73	No	Class D - Reserved for multicasting

Sub netting

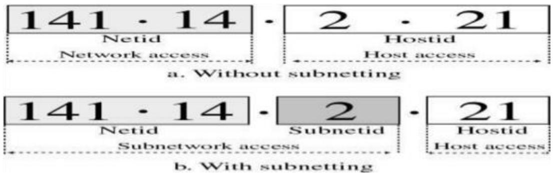
- Subnetting is a process to divide network into subnetworks.
- Host ID bit is used in NetID
- A Network with Two Levels of Hierarchy



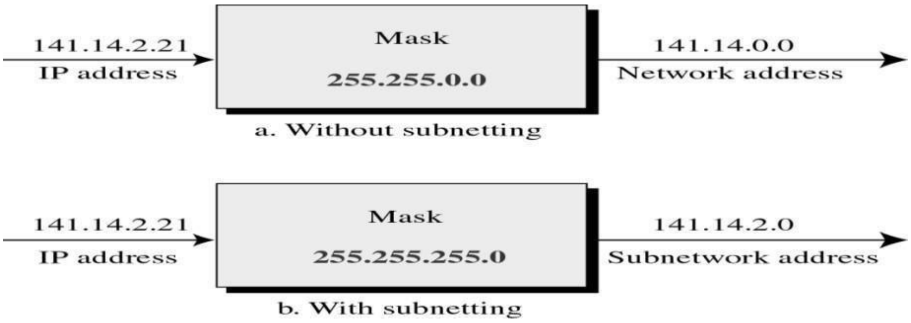
- A Network with Three Levels of Hierarchy



- Addresses with and without Subnetting



- Masking: Masking is a process that extracts the address of the physical network from an IP address.

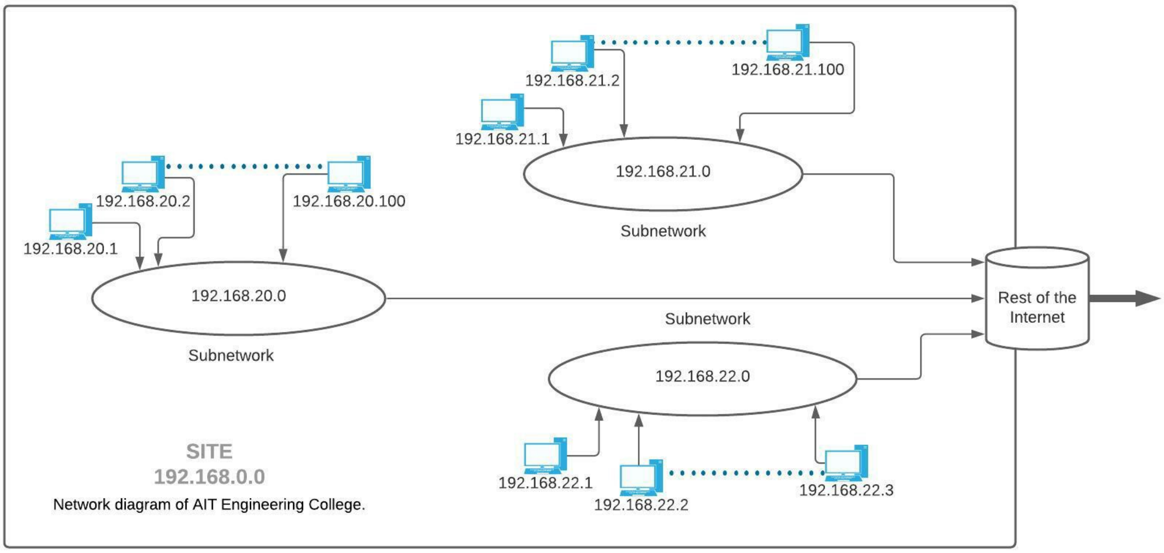


Fill the appropriate values in this table

Network Address	Prefix	Mask	Subnet Bits	Subnet Possible 2^n	Hosts Per Subnets
172.16.0.0	/16	255.255.0.0	0	1	65534
172.16.0.0	/17	255.255.128.0	1	2(0)	32766
172.16.0.0	/18	255.255.192.0	2	4(2)	16382
172.16.0.0	/19	255.255.224.0	3	8(6)	8190
172.16.0.0	/20	255.255.240.0	4	16(14)	4094
172.16.0.0	/21	255.255.248.0	5	32(30)	2046
172.16.0.0	/22	255.255.252.0	6	64(62)	1022
172.16.0.0	/23	255.255.254.0	7	128(126)	510
172.16.0.0	/24	255.255.255.0	8	256(254)	254
172.16.0.0	/25	255.255.255.128	9	512(510)	126
172.16.0.0	/26	255.255.255.192	10	1024(1022)	62
172.16.0.0	/27	255.255.255.224	11	2048(2046)	30
172.16.0.0	/28	255.255.255.240	12	4096(4094)	14
172.16.0.0	/29	255.255.255.248	13	8192(8190)	6
172.16.0.0	/30	255.255.255.252	14	16384(16382)	2

EXCERCISE:

1. Prepare the Network diagram of AIT Engineering College. A)



QUIZ:

Answer the Followings:

1. IP Address is used at which Layer?

A) IP Address is used at Internet Layer. The Internet Layer of the TCP/IP model aligns with the Layer 3 (Network) layer of the OSI model. This is where IP addresses and routing live. When data is transmitted from a node on one LAN to a node on a different LAN, the Internet Layer is used.

2. Give difference between IP Address and MAC Address.

A)

MAC Address	**IP Address**
MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
MAC Address is a six-byte hexadecimal address.	IP Address is either four-byte (IPv4) or eightbyte (IPv6) address.
A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
NIC Card’s Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
MAC Address is used to ensure the physical	IP Address is the logical address of the

address of computer.	computer.
MAC Address operates in the data link layer.	IP Address operates in the network layer.
MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
MAC Address can’t be found easily by third party.	IP Address can be found by third party.

EVALUATION:

Involvement (4)	Understanding / Problem solving (3)	Timely Completion (3)	**Total** **(10)**