Computer Networks

NAME : Vashuki Achari
ROLL : 102103503
CLASS : 2CO18

LAB ASSINMENT 1 :

1. Discuss the concept of networking, advantages ,disadvantages and application.

Networking is the practice of connecting computers or other devices together in order to facilitate communication and the sharing of information and resources. Networking allows devices to share resources such as printers, file servers, and internet connections, and enables the exchange of data between devices.

There are several advantages to networking:

1. Increased efficiency: Networking allows devices to share resources, so users don't have to waste time and effort transferring files or using multiple devices to complete a task.
2. Enhanced collaboration: Networking makes it easier for people to work together and share information, which can improve communication and collaboration within a team or organization.
3. Cost savings: Networking can reduce the need for expensive hardware such as printers or file servers, as these resources can be shared among multiple devices.
4. Improved access to information: Networking allows users to access information and resources from anywhere on the network, which can be especially useful for remote workers or people who need to access data from multiple locations.

There are also some disadvantages to networking:

1. Security risks: Networking can increase the risk of data breaches and cyber attacks, as it exposes devices to potential threats from external sources.
2. Complexity: Setting up and maintaining a network can be complex and require specialized knowledge and resources.
3. Dependency: Networked devices may become reliant on the network for access to resources, which can create problems if the network goes down or experiences problems.

Networking has a wide range of applications in both personal and professional settings. Some examples include:

1. Home networks: Many people use networking to connect their personal devices, such as laptops, smartphones, and tablets, to a single internet connection.
2. Business networks: Businesses use networking to connect devices and resources within an office or between multiple locations, enabling employees to share files and access information from any location.
3. Public networks: Public networks, such as those found in libraries or coffee shops, allow users to connect to the internet from any location.
4. Cloud computing: Networking is an essential component of cloud computing, which allows users to access data and applications over the internet rather than storing them on their own devices.
5. The Internet: The internet itself is a vast network that connects millions of devices around the world, enabling the exchange of information and resources on a global scale.

2. Discuss the peer-to-peer connections and multipoint connection.

In a peer-to-peer (P2P) connection, two or more devices are connected directly to each other without the need for a central server or other intermediary. Each device acts as both a client and a server, allowing them to communicate and exchange data directly. This can be useful for decentralized applications, as it allows devices to communicate and share data without the need for a central point of control.

A multipoint connection, on the other hand, involves multiple devices connecting to a central server or other intermediary. In this configuration, the central server acts as a hub, routing traffic and data between the connected devices. This can be useful for applications that require a centralized point of control or where a central server is necessary for some other reason.

Both P2P and multipoint connections have their own advantages and disadvantages, and which one is best suited for a particular application will depend on the specific requirements and needs of that application.

3. Discuss the components required to make a computer network.

There are several components that are typically required to create a computer network:

1. Network Interface Card (NIC): This is a hardware component that allows a computer to connect to a network. Each computer on the network will typically have a NIC.
2. Network Cable: This is a physical cable that is used to connect

devices on a network. There are several types of cables that can be used for this purpose, including twisted pair cables, coaxial cables, and fiber optic cables.
3. Hub or Switch: These are devices that are used to connect multiple devices on a network. A hub simply forwards data packets to all connected devices, while a switch is more intelligent and only forwards data to the specific device it is intended for.
4. Router: This is a device that connects multiple networks together and routes data between them. A router may be used to connect a local area network (LAN) to a wide area network (WAN), such as the Internet.
5. Access Point: This is a device that allows wireless devices to connect to a network. An access point typically connects to a wired network and then broadcasts a wireless signal, allowing wireless devices to connect to the network.
6. Firewall: This is a security system that is used to protect a network from external threats. A firewall can be hardware-based, software-based, or a combination of both. It is used to block unauthorized access to the network and to monitor and control incoming and outgoing network traffic.

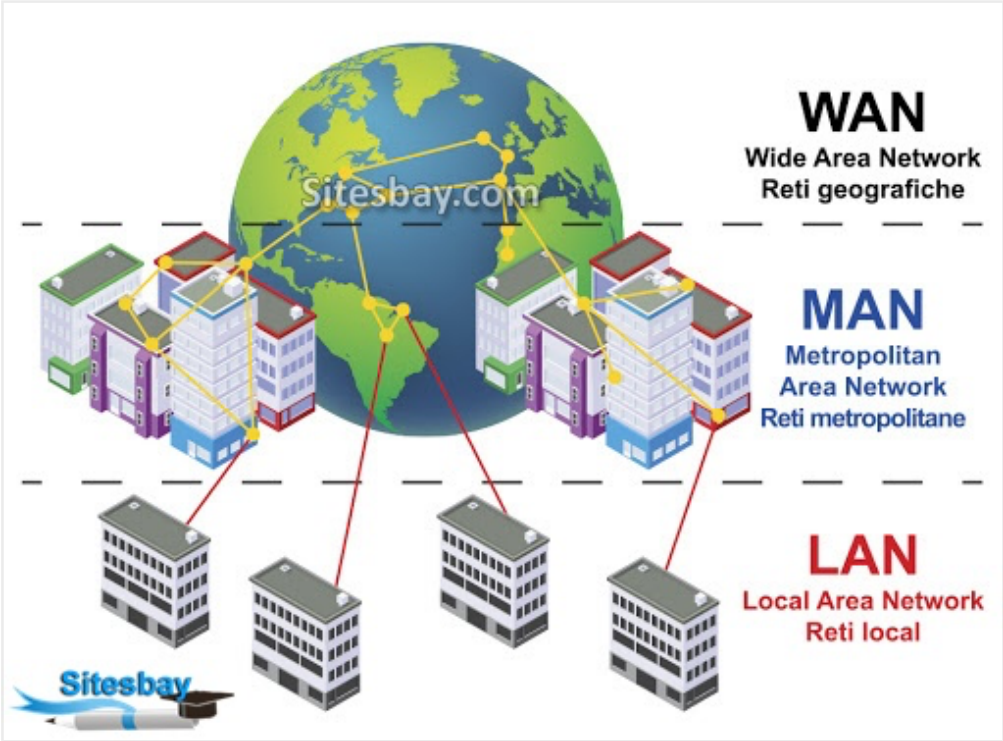
These are the main components that are typically required to create a computer network. However, there may be additional components that are needed depending on the specific requirements and needs of the network.

4. Discuss the types of networks as LAN, WAN and MAN.

There are three main types of computer networks:

1. Local Area Network (LAN): This is a small network that is typically used to connect devices in a single location, such as a home or office. A LAN allows devices to share resources, such as printers and files, and enables communication between devices.
2. Wide Area Network (WAN): This is a larger network that spans a wider geographical area, such as a city or a country. A WAN may be used to connect multiple LANs together, allowing devices on different LANs to communicate with each other. A WAN may be established using leased communication lines or through the Internet.
3. Metropolitan Area Network (MAN): This is a network that spans a metropolitan area, such as a city. A MAN may be used to connect LANs and WANs within a city, allowing devices on different networks to communicate with each other.

Each of these types of networks has its own characteristics and is suited for different types of applications. A LAN is suitable for small, localized networks, while a WAN is better suited for larger, geographically dispersed networks. A MAN is somewhere in between, being larger than a LAN but smaller than a WAN.



5. Differentiate between physical and logical topologies.

Physical topology refers to the physical layout of a network, including the location and type of devices and the cables that connect them. Some examples of physical topologies include bus, star, ring, and mesh.

Logical topology, on the other hand, refers to the way in which data is transmitted between devices on a network. It is the pattern of data flow, rather than the physical layout of the devices. Some examples of logical topologies include bus, star, and ring.

In general, physical topology is concerned with the actual layout of the network, while logical topology is concerned with the way in which data is transmitted between devices. It is possible for a network to have a physical topology that is different from its logical topology. For example, a network may have a physical star topology (with devices connected to a central hub) but a logical bus topology (with data transmitted in a linear fashion from one device to the next).

Physical Topology	Logical Topology
Refers to the physical layout of a network, including the location and type of devices and the cables that connect them	Refers to the way in which data is transmitted between devices on a network
Examples include bus, star, ring, and mesh	Examples include bus, star, and ring
Determined by the physical layout of the devices and cables	Determined by the way in which data is transmitted between devices

6. List the different types of networks from surroundings as client-server network, distributed networks, peer-to-peer networks and cloud based networks.

There are several types of networks that can be found in the surrounding environment:

1. Client-server network: This is a type of network in which one or more central servers are used to provide services to clients. The clients send requests to the server, which processes the request and returns the requested data or service. This type of network is common in businesses and organizations.
2. Distributed networks: These are networks in which resources and tasks are distributed among multiple devices. Distributed networks may be used to improve performance and reliability by allowing devices to share the workload.
3. Peer-to-peer (P2P) networks: In a P2P network, devices are connected directly to each other without the need for a central server. Each device acts as both a client and a server, allowing them to communicate and exchange data directly. P2P networks are often used for file sharing and other decentralized applications.
4. Cloud-based networks: These are networks that are based on cloud computing, in which resources and services are provided over the Internet. Cloud-based networks allow users to access resources and services remotely, without the need for local hardware or software.

These are some of the different types of networks that can be found in the surrounding environment. Each type of network has its own characteristics and is suited for different types of applications.

7. Discuss the concept of Network Topologies.

Network topology refers to the layout of a network, including the location and type of devices and the connections between them. The term "topology" refers to the way in which the network is arranged, or laid out. There are several types of network topologies that can be used to arrange devices on a network:

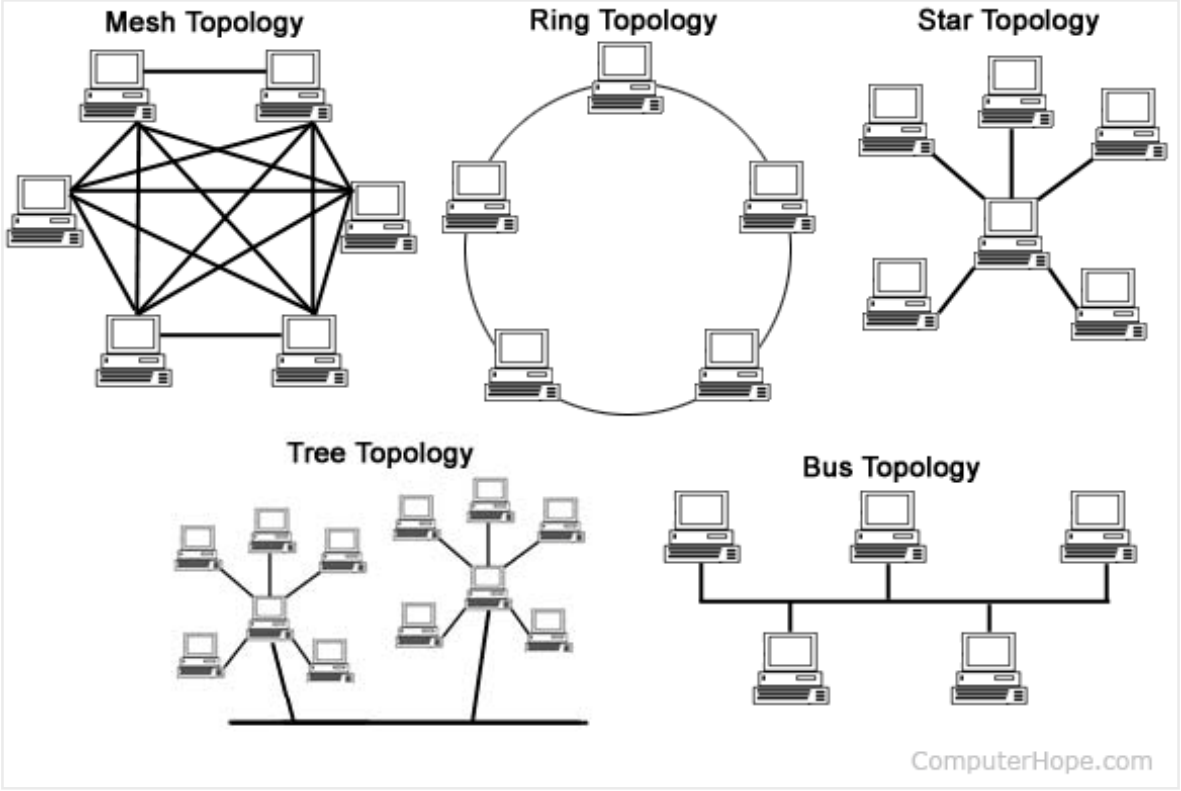
1. Bus topology: In a bus topology, devices are connected to a central cable or "bus" that carries data from one device to the next. This type of topology is simple and easy to set up, but it can be prone to problems if the central cable fails.
2. Star topology: In a star topology, devices are connected to a central hub or switch. This allows for more flexibility and easier troubleshooting, as each device has its own connection to the central hub.
3. Ring topology: In a ring topology, devices are connected to one another in a circular configuration. Data is transmitted around the ring in a single direction, with each device passing the data on to the next device in the ring.
4. Mesh topology: In a mesh topology, each device is connected to every other device on the network. This allows for multiple paths for data to be transmitted, increasing reliability and fault tolerance. However, it can be more complex and expensive to set up.

There are also hybrid topologies, which combine elements of two or more of the above topologies. The choice of which topology to use will depend on the specific requirements and needs of the network.

There are several common network topologies, each with its own advantages and disadvantages. Here is a brief overview of some of the most commonly used network topologies and their pros and cons:

1. Bus Topology: In this topology, all devices are connected to a single cable called a bus. Advantages of bus topology include its simplicity and ease of setup, as well as its ability to support multiple devices with a minimal amount of cable. However, one of the major disadvantages of bus topology is that if the bus cable fails, the entire network will go down. Additionally, bus topology can be affected by the problem of broadcast storms, which can slow down or bring down the entire network.
2. Star Topology: In a star topology, all devices are connected to a central hub. Advantages of this topology include its ability to be easily expanded and its fault-tolerance (if one device fails, the rest of the network is still operational). Additionally, star topology allows for easy isolation of devices that may be causing problems. The disadvantages

of star topology are that it can be expensive to implement and the central hub is a single point of failure.
3. Ring Topology: In a ring topology, all devices are connected in a closed loop, with data being transmitted from device to device in a single direction. Advantages of ring topology include its ability to support high-speed data transfer, as well as its ability to detect and correct errors. However, the disadvantages of ring topology include the fact that it can be expensive to implement, and the fact that if one device fails, the entire network will go down.
4. Advantages of a Mesh topology include its ability to be extremely fault-tolerant and its ability to support large numbers of devices. Additionally, since data can be transmitted via multiple routes, mesh topology can support high-speed data transfer. However, the major disadvantage of mesh topology is that it can be expensive to implement and can require a large amount of cabling.



8. Protocols and their usage e.g. TCP/IP, http, https, ftp.

Protocols are standardised rules and procedures that are used to facilitate communication between devices on a network. Here are some examples of common protocols and their uses:

1. TCP/IP (Transmission Control Protocol/Internet Protocol): This is a suite of protocols that is used to transmit data over the Internet and

other networks. TCP is responsible for breaking data into smaller packets and reassembling them at the destination, while IP is responsible for routing the packets to their destination.
2. HTTP (Hypertext Transfer Protocol): This is a protocol that is used to transmit data over the World Wide Web. HTTP is used to transfer the text, images, and other data that make up web pages.
3. HTTPS (HTTP Secure): This is a secure version of HTTP that is used to transmit data over the World Wide Web. HTTPS uses encryption to protect data as it is transmitted between devices.
4. FTP (File Transfer Protocol): This is a protocol that is used to transfer files between computers. FTP allows users to upload and download files to and from a server.

These are just a few examples of the many protocols that are used in networking. Protocols are an essential part of networking, as they provide the rules and standards that allow devices to communicate with one another.

LAB ASSIGNMENT 2

1. Network Interface Cards - their use, types and working.

A Network Interface Card which is also known as NIC is a hardware component that connects a computer to a network. It typically has one or more connectors to connect to a network cable, and it uses various technologies to transmit data over the network. The NIC is responsible for providing an interface between the computer's internal bus and the network, and it typically includes a variety of components such as a physical layer transceiver, a media access controller, and an integrated circuit.

Uses of NICs :

1. NIC allows both wired and wireless communications.
2. NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
3. NIC is both a physical layer and a data link layer device, i.e. it provides

the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NICs :

1. **Wireless.** These are NICs that use an antenna to provide wireless reception through radio waves at some frequency. Wireless NICs are designed for Wi-Fi connections.
2. **Wired.** These are NICs that have input jacks made for cables. The most popular wired LAN technology is Ethernet.
3. **USB.** These are NICs that provide network connections through a device plugged into the USB port.
4. **Fiber optics.** These are expensive and more complex NICs that are used as a high-speed support system for network traffic handling on server computers. This support could also be accomplished by combining multiple NICs.

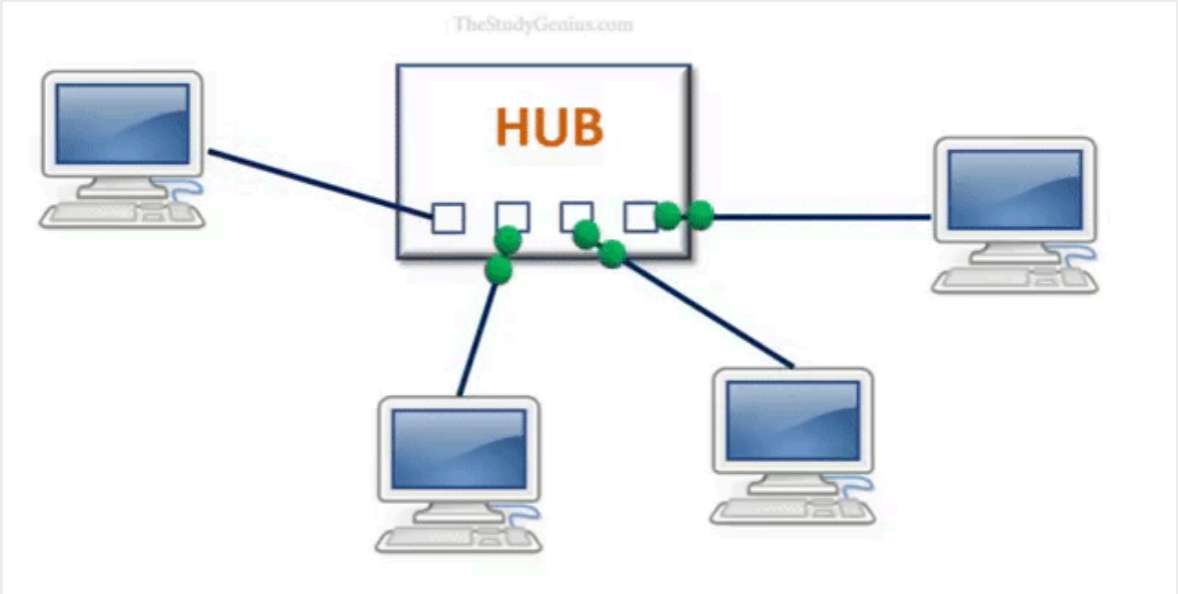
Working :
NICs work by sending and receiving packets of data across the network. A packet is a unit of data that is sent across the network and contains information such as the source and destination addresses, as well as the actual data being transmitted. When a computer wants to send data over the network, it sends the data to the NIC, which then packages it into a packet and sends it over the network. Similarly, when a packet is received by the NIC, it unpackages the data and sends it to the computer for processing.

2. Hub Device and its' working.

A hub is a common connection point, also known as a network hub, which is used for connection of devices in a network. It works as a central connection for all the devices that are connected through a hub. The hub has numerous ports. If a packet reaches at one port, it is able to see by all the segments of the network due to a packet is copied to the other ports. A network hub has no routing tables or intelligence (unlike a network switch or router), which is used to send information and broadcast all network data across each and every connection.

Working :
Hub works like an electric wire, it receives data signals from one device in his one port and forwards them to all the other ports, except the source port. It does not have any capability to identify any frames to know where it should forward because it does not maintain any kind of table like switch. So there is a lot of traffic on the network and network performance is also very poor, only one device transmits information at a particular time.
It works on star topology physically because all the devices are connected to

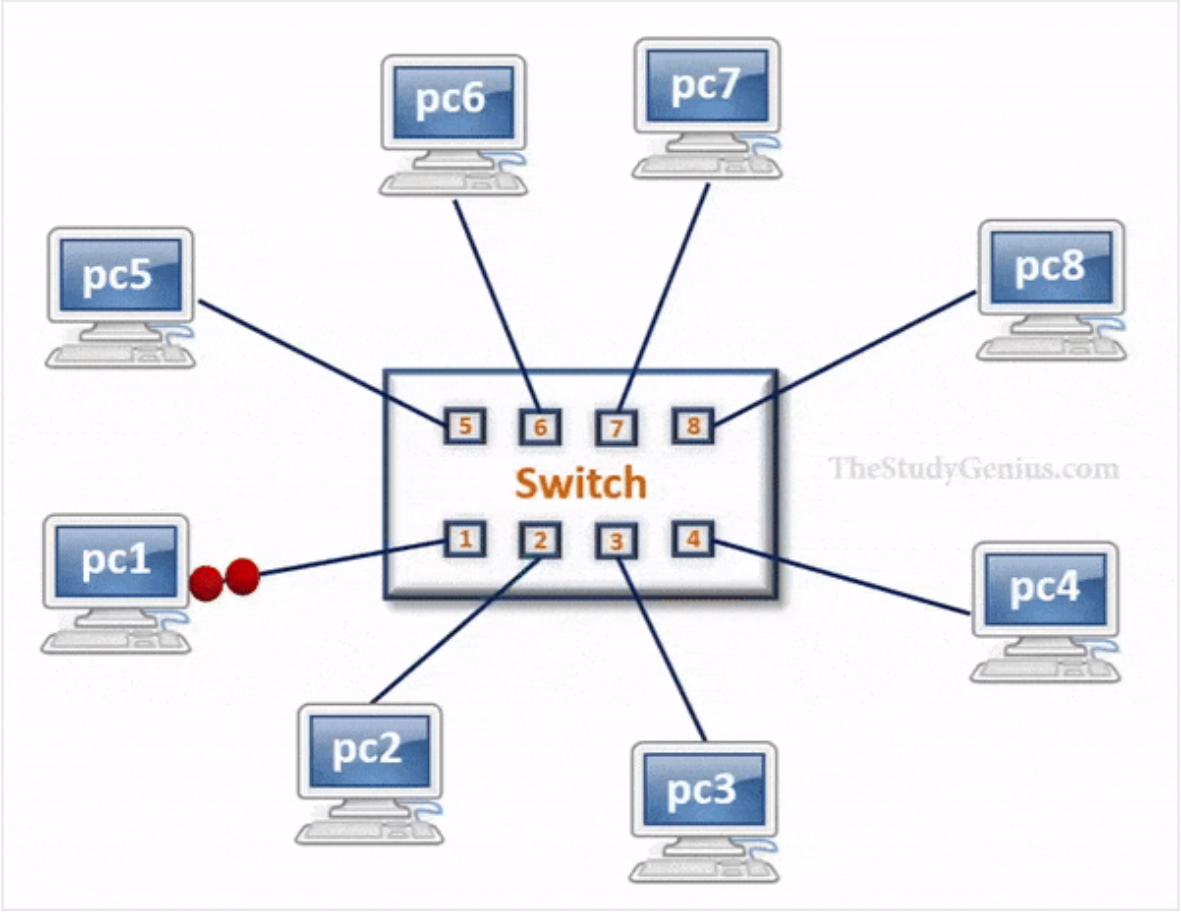
the central node, but logically it acts as a bus topology.



3. Switch Device and its' working.

   Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
   A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications

Working :
When the source wants to send the data packet to the destination, packet first enters the switch and the switch reads its header and find the MAC address of destination to identify the device then it sends the packet out through the appropriate ports that leads to the destination devices.
Switch establishes a temporary connection between source and destination for communication and terminates the connection once conversation is done. Also, it offers full bandwidth to network traffic going to and from a device at the same time to reduce collision.

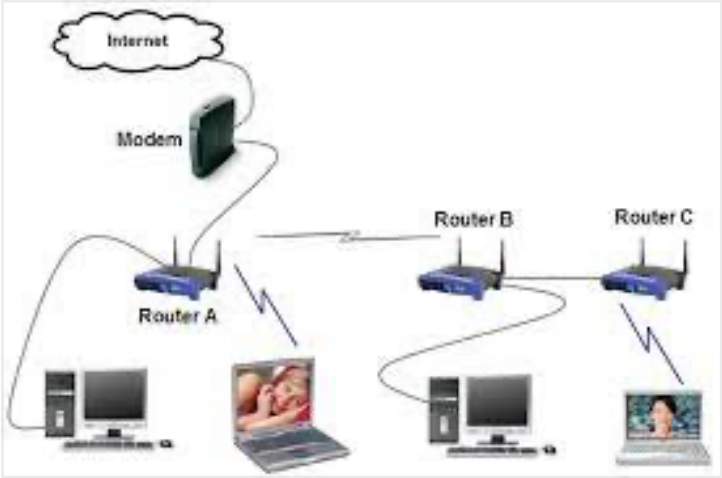


4. Router Device and its' working.

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**, etc.

Working :
A router analyzes a destination IP address of a given packet header and compares it with the routing table to decide the packet's next path. The list of routing tables provides directions to transfer the data to a particular network destination. They have a set of rules that compute the best path to forward the data to the given IP address.
Routers use a **modem** such as a cable, fiber, or DSL modem to allow communication between other devices and the internet. Most of the routers have several ports to connect different devices to the internet at the same time. It uses the **routing tables** to determine where to send data and from where the traffic is coming.
A routing table mainly defines the default path used by the router. So, it may fail

to find the best way to forward the data for a given packet. For example, the office router along a single default path instructs all networks to its internet services provider.
There are two types of tables in the router that are **static and dynamic**. The static routing tables are configured manually, and the dynamic routing tables are updated automatically by dynamic routers based on network activity.

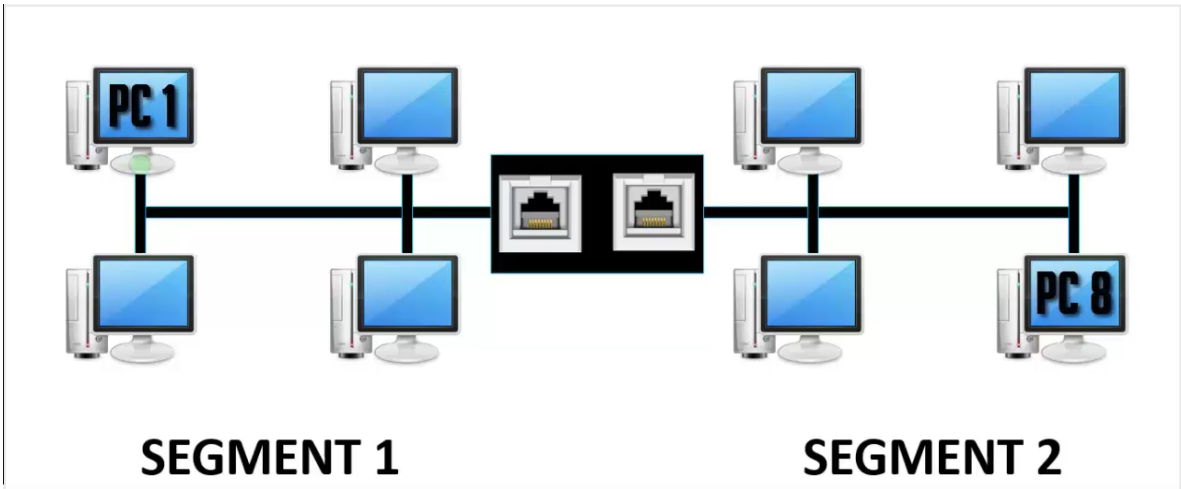


5. Bridge device and its' working.

The bridge is a networking device in a computer network that is used to connect multiple LANs to a larger LAN. In computer networks, we have multiple networking devices such as bridges, hubs, routers, switches, etc, each device has its own specification and is used for a particular purpose. The bridge is a networking device that connects the larger LAN networks with the group of smaller LAN networks.
In this article, we are going to discuss everything about the bridge including what exactly a bridge is, and the type of bridges we have in computer networks including transparent bridges, source routing bridges, and translational bridges, which will be followed by advantages and disadvantages of the bridge in networking. then how the bridge is different from the gateway and last we will look into the applications and functions of the bridge in the network.

Working :
Bridge in networking divides a LAN into two segments (Segment 1 and Segment 2) and stores all the connected PC's MAC address into its table. Let's take an example, Here PC 1 tries to send data to PC 2. Data will first travel to the bridge. The bridge will read its MAC address and decide whether to send the data to segment 1 or segment 2. Hence, the PC 2 is available in segment 1 means bridge will broadcast the data only in segment 1 and excludes all the PCs connected in segment 2. Like this bridge reduce the traffic on a computer network.
Let's take one more example. As mentioned in the below picture, PC 1 is trying to send data to PC 8. So, the data will first travel to the bridge. The bridge is

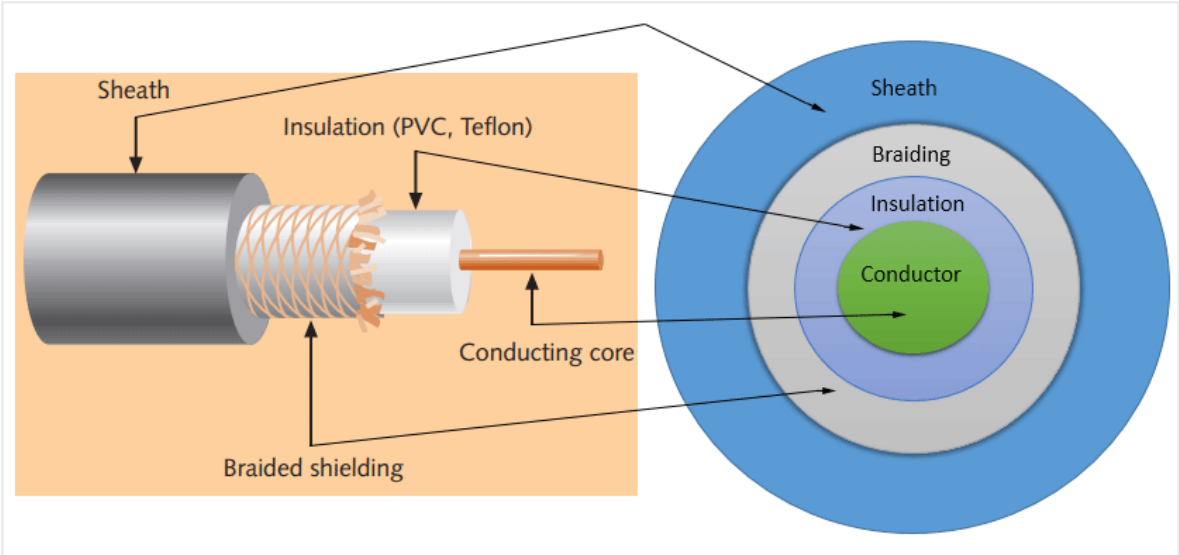
going to read it's MAC Address table and find whether PC 8 belongs to Segment 1 or Segment 2. Hence, the PC 8 is in segment 2 bridge will broadcast the data in segment 2 and excludes all the PCs connected to Segment 1. So, this is how the bridge works and reduce traffic in a computer network.



6. Types of networking wires and connectors, shapes and specifications.

1. COAXIAL CABLE

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, the braiding covers the insulation, and the insulation covers the conductor.
The following image shows these components.



Sheath : This is the outer layer of the coaxial cable. It protects the cable from

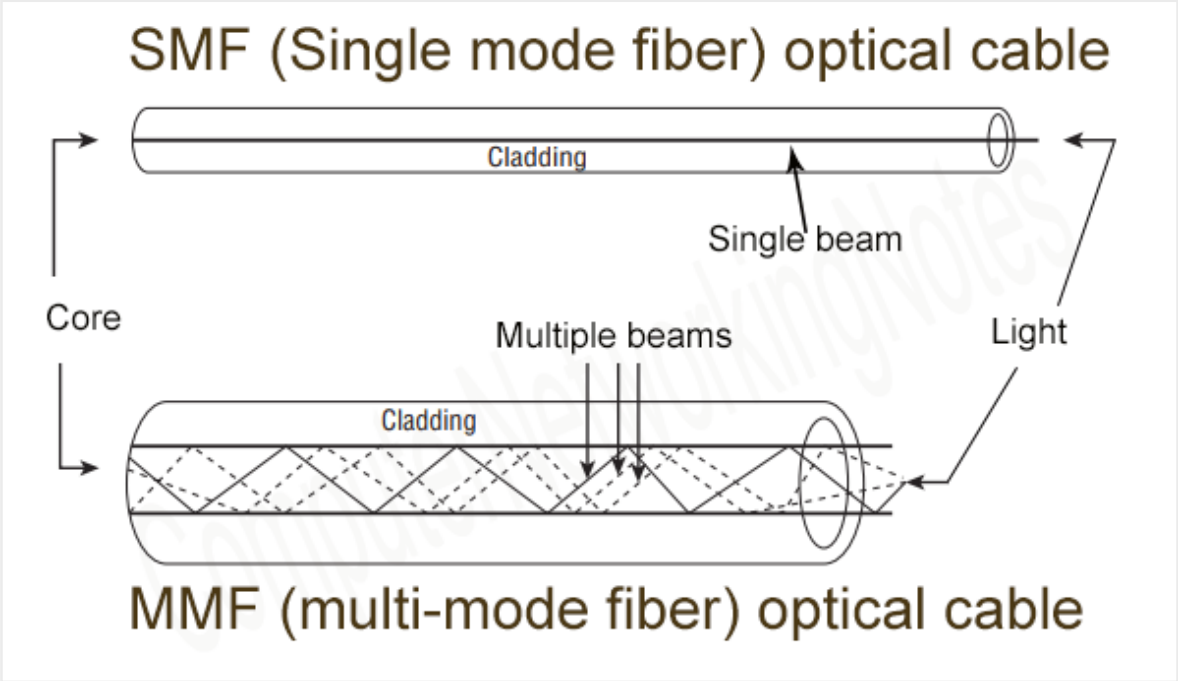
physical damage.
Braided shield : This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.
Insulation : Insulation protects the core. It also keeps the core separate from the braided shield. Since both the core and the braided shield use the same metal, without this layer, they will touch each other and create a short-circuit in the wire.
Conductor : The conductor carries electromagnetic signals. Based on conductor a coaxial cable can be categorized into two types; single-core coaxial cable and multi-core coaxial cable.
A single-core coaxial cable uses a single central metal (usually copper) conductor, while a **multi-core** coaxial cable uses multiple thin strands of metal wires. The following image shows both types of cable.

2. FIBER OPTICAL CABLE

This cable consists of a core, cladding, buffer, and jacket. The core is made from thin strands of glass or plastic that can carry data over a long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

- Core carries the data signals in the form of light.
- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.

Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.
Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.



SMF (Single-mode fiber) optical cable

This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

MMF (multi-mode fiber) optical cable

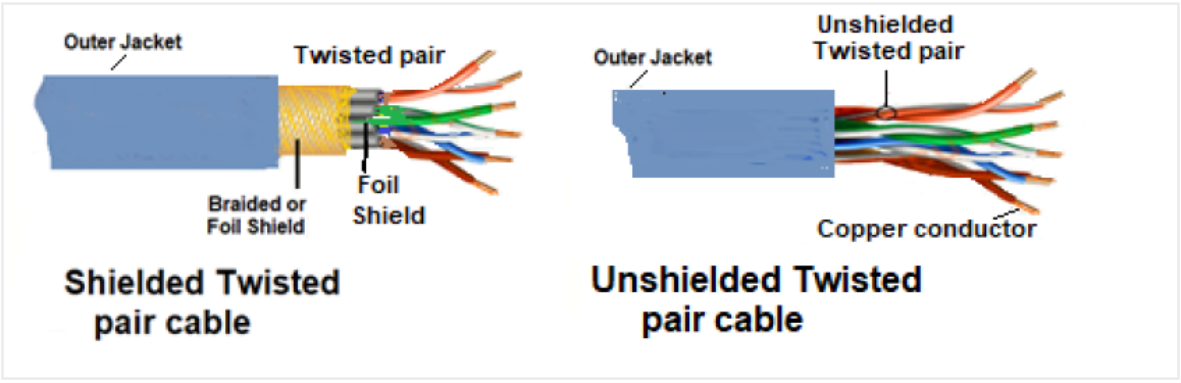
This cable carries multiple beams of light. Because of multiple beams, this cable carries much more data than the SMF cable. This cable is used for shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nano-meter wavelengths of light.

3. TWISTED PAIR CABLES

The twisted-pair cable was primarily developed for computer networks. This cable is also known as **Ethernet cable**. Almost all modern LAN computer networks use this cable.
This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green, and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable :

1. UTP cable (Unshielded twisted-pair) : all pairs are wrapped in a single plastic sheath.
2. STP cable (Shielded twisted-pair) : each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.



7. Wireless Access Points.

A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. A Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.
It is easier and simpler to understand and implant the device. It can be fixed, mobile or hybrid proliferated in the 21st century. The availability, confidentiality, and integrity of the communication and network are a responsibility and to be ensured about that.
A wireless AP connects the wired networks to the wireless client. It eases access to the network for mobile users which increases productivity and reduces the infrastructure cost.

Advantages of Wireless Access Point (WAP):
1. More User Access:
- Normally the wireless router allows 10 – 20 users or devices to access the network. While the WAP allows 50 – 100 or more users or devices to access the network.
- The WAP has a stronger ability to send and receives signals which enables high usage.

2. Broader Transmission Range:
- A wireless router signals cover up to a dozen or 10 -12 meters. However, a wireless access point covers more than 100 – 300 meters.
- The broad range is supremacy for the large cover offices or buildings for the bigger businesses. With this wireless access point, a user can easily roam that network.

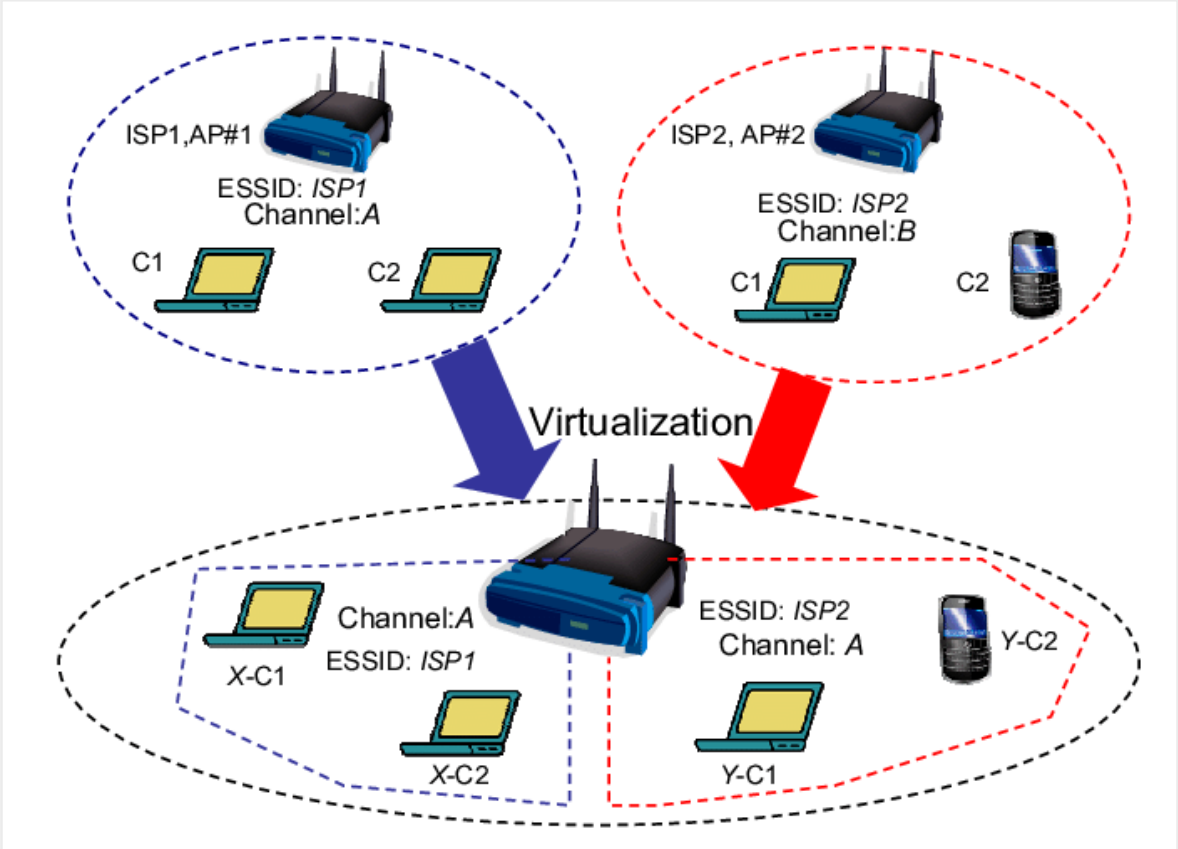
3. Flexible Networking:
- It is known that wireless networking except in homes, often involves many wireless devices and different networking patterns implanted based on the environment and requirements of the commercial locations.

Disadvantages of Wireless Access Point (WAP):
1. High cost:

- A wireless AP is a little bit expensive because the scale of enterprises the wireless scale network is larger, the more WAPs are needed the more cost will increase. So the enterprise has the priority to control the cost which leads many users to be reluctant to use WAP but instead of this, they end up using home routers with the lowest performances.

2. Poor stability:

- As wireless networks use air as a transmission medium, so the network stability is poor and slower in WAP as compared to the cable network because the transmission medium in wired network is cable. Especially in WLAN, there are more devices still it is slow and a cable network is faster and more stable than a wireless network.
- The wireless signals are blocked due to certain obstacles such as heavy rain, great walls, gates, storm, heavy wind, large gatherings of human beings, etc.
- The signal strength also depends upon the location where the wireless network is implanted.



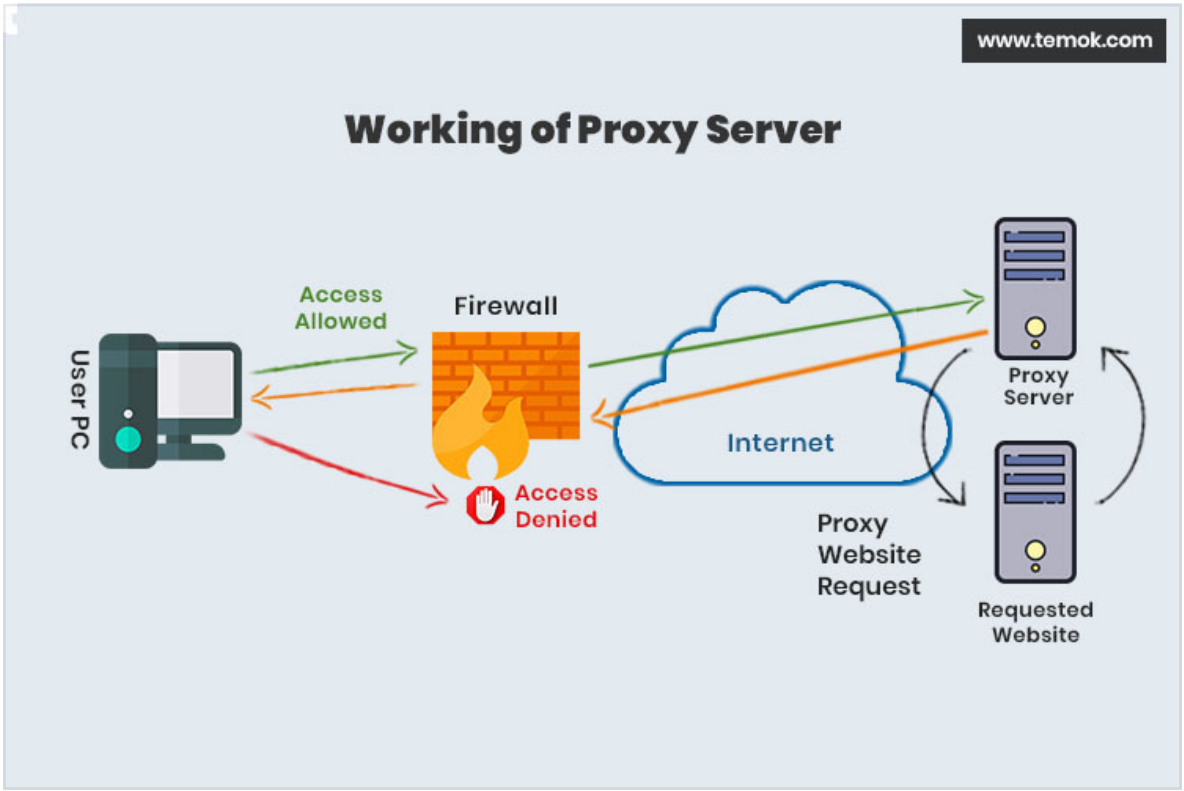
8. Proxy Servers and usages.

Proxy server refers to a server that acts as an intermediary between the

request made by clients, and a particular server for some services or requests for some resources. There are different types of proxy servers available that are put into use according to the purpose of a request made by the clients to the servers. The basic purpose of Proxy servers is to protect the direct connection of Internet clients and internet resources. The proxy server also prevents the identification of the client's IP address when the client makes any request is made to any other servers.

Its usage :

- **Internet Client and Internet resources:** For internet clients, Proxy servers also act as a shield for an internal network against the request coming from a client to access the data stored on the server. It makes the original IP address of the node remains hidden while accessing data from that server.
- **Protects true host identity:** In this method, outgoing traffic appears to come from the proxy server rather than internet navigation. It must be configured to the specific application such as HTTPs or FTP. For example, organizations can use a proxy to observe the traffic of its employees to get the work efficiently done. It can also be used to keep a check on any kind of highly confidential data leakage. Some can also use it to increase their websites rank.



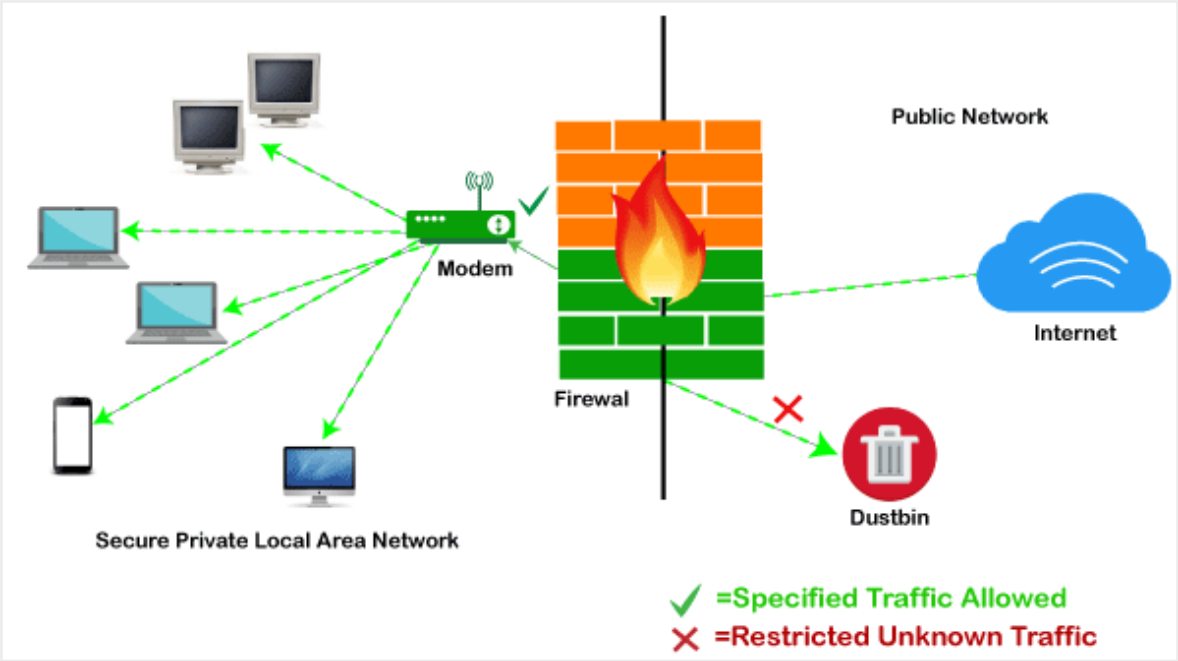
9. Firewall and working principle.

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules and policies. Its main function is to block unauthorized access while permitting authorized communications. Firewalls can be implemented as software or hardware, or a combination of both, and are used to protect a network or computer system from unauthorized access and potential attacks.

Working :
Firewalls analyze each block of data packets entering or leaving the Intranet or the host computer. Based on a defined set of security rules, a firewall can perform three actions:

1. **Accept:** allow the transmission of data packets.
2. **Drop:** block data packets with no reply.
3. **Reject:** Block data packets and send “unreachable error” to the source.

Let me explain this via an example of a mid-size company with one thousand employees. Suppose this is an IT company with hundreds of computers that are all connected through network cards.
The company will need at least one connection to link these computers with the outer network (Internet). Let’s say the X1 line connects the internal network (Intranet) to the Internet.
In this case, the company must implement a firewall on X1 line (and/or on each computer on the Intranet). Without a strong firewall in place, all those computers will become vulnerable to external threats.
If any employee makes a mistake and leaves a security hole, attackers (on the internet) can exploit this hole to probe internal computers and establish a connection.
However, with a firewall in place, they can keep dangerous traffic out. The company can establish security policies; for example, if they choose not to allow FTP connections, then the firewall will block all public FTP traffic from and to the external network.
Not only does a firewall restricts unwanted traffic, but it also blocks malicious programs from infecting host computers.



LAB ASSIGNMENT 3

Objective: To understand some Networking Commands
Instructions: The instructor is required to run and discuss the output of the following networking command on DOS prompt.

1. hostname :

The HOSTNAME command displays the hostname of the system. The hostname command is much easier to use than going into the system settings to search for it.

```
apple@Vashukis-MacBook-Air ~ % hostname
Vashukis-MacBook-Air.local
```

2. Ipconfig :

The Ipconfig network command provides a comprehensive view of information regarding the IP address configuration of the device we are currently working on.
The IPConfig command also provides us with some variation in the primary command that targets specific system settings or data, which are:

- IPConfig/all - Provides primary output with additional information about network adapters.
- IPConfig/renew - Used to renew the system's IP address.
- IPConfig/release - Removes the system's current IP address.

```
apple@Vashukis-MacBook-Air ~ % ipconfig
usage: ipconfig <command> <args>
where <command> is one of waitall, getifaddr, ifcount, getoption, getiflist, getsummar
y, getpacket, getv6packet, getra, getdhcpduid, getdhcpiaid, set, setverbose
```

3. getmac :

The getmac is a Windows command-line utility used typically when troubleshooting network issues to retrieve the MAC address, also known as the physical address, of network adapters in a computer. The getmac will only able to retrieve MAC addresses (the 6-byte 'burned-in' physical/hardware address) of connected adapters. If an adapter is disabled (in Windows Device Manager for example), or is not connected to the network, getmac will not be able to retrieve its MAC address.

```
C:>getmac

Physical Address    Transport Name
=================== ============================================================
30-5A-3A-7F-17-A1   \Device\Tcpip_{278F1BFF-B571-444D-B35F-3CF3FBF03B0C}
00-FF-49-B8-4F-89   Media disconnected
N/A                 Hardware not present
Disabled            Disconnected
N/A                 Hardware not present

C:>
```

4. ping :

The ping command is used to test connectivity between two hosts. It sends ICMP echo request messages to the destination. The destination host replies with ICMP reply messages. If the ping command gets a reply from the destination host, it displays the reply along with round-trip times.

```
apple@Vashukis-MacBook-Air ~ % ping
usage: ping [-AaDdfnoQqRrv] [-c count] [-G sweepmaxsize]
            [-g sweepminsize] [-h sweepincrsize] [-i wait]
            [-l preload] [-M mask | time] [-m ttl] [-p pattern]
            [-S src_addr] [-s packetsize] [-t timeout][-W waittime]
            [-z tos] host
       ping [-AaDdfLnoQqRrv] [-c count] [-I iface] [-i wait]
            [-l preload] [-M mask | time] [-m ttl] [-p pattern] [-S src_addr]
            [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
            [-z tos] mcast-group
Apple specific options (to be specified before mcast-group or host like all options)
            -b boundif           # bind the socket to the interface
            -k traffic_class     # set traffic class socket option
            -K net_service_type  # set traffic class socket options
            --apple-connect       # call connect(2) in the socket
            --apple-time          # display current time
```

5. arp :

The ARP (Address Resolution Protocol) command is used to access the mapping structure of IP addresses to the MAC address. This provides us with a better understanding of the transmission of packets in the network channel.

```
apple@Vashukis-MacBook-Air ~ % arp
usage: arp [-n] [-i interface] hostname
       arp [-n] [-i interface] [-l] -a
       arp -d hostname [pub] [ifscope interface]
       arp -d [-i interface] -a
       arp -s hostname ether_addr [temp] [reject] [blackhole] [pub [only]] [ifscope inter
face]
       arp -S hostname ether_addr [temp] [reject] [blackhole] [pub [only]] [ifscope inter
face]
       arp -f filename
```

6. nbtstat :

Nbtstat is a TCP/IP utility that displays current TCP/IP connections and statistics using NetBIOS over TCP/IP (NetBT). Nbtstat is installed on a computer running Microsoft Windows when the TCP/IP protocol stack is installed.

```
C:\>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

7. route :

The route command allows you to make manual entries into the network routing tables. The route command distinguishes between routes to hosts and routes to networks by interpreting the network address of the Destination variable, which can be specified either by symbolic name or numeric address.

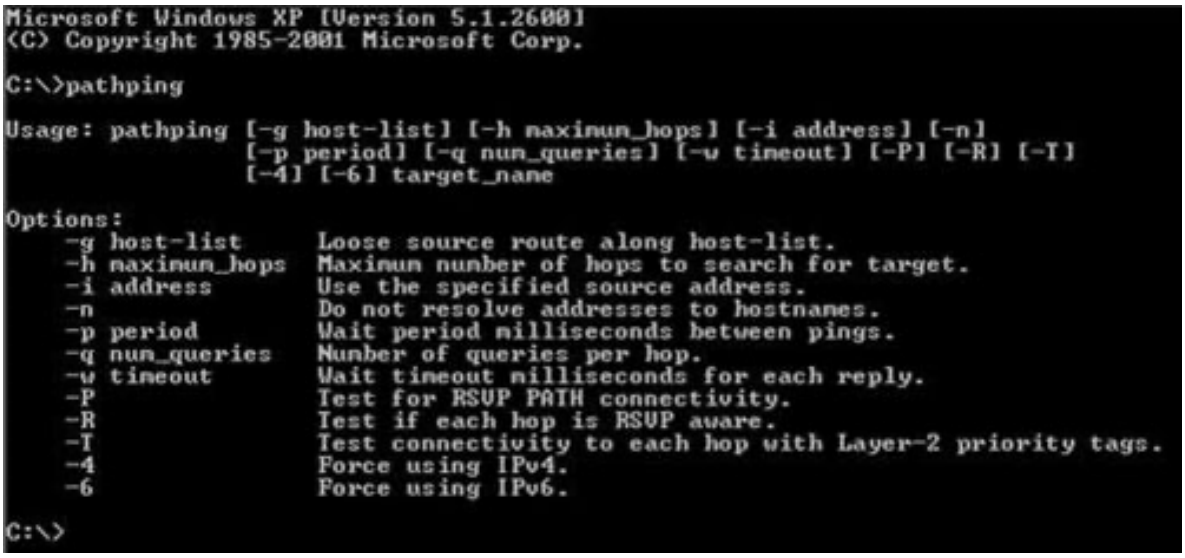
```
HQ_Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

8. path :

A path is a string of characters used to uniquely identify a location in a directory structure. It is composed by following the directory tree hierarchy in which components, separated by a delimiting character, represent each directory.

9. pathping :

This command sends multiple echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each router.



10. netstat :

The network statistics (netstat) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.

```
C:\Documents and Settings\Owner>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1027         0.0.0.0:0              LISTENING
  TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.100:2558     207.68.172.236:80      CLOSE_WAIT
  TCP    192.168.1.100:2916     204.14.90.25:21        CLOSE_WAIT
  TCP    192.168.1.100:2923     69.65.109.55:80        TIME_WAIT
  TCP    192.168.1.100:2924     204.245.162.25:80      ESTABLISHED
  TCP    192.168.1.100:2925     66.150.96.119:80       ESTABLISHED
  TCP    192.168.1.100:2930     204.245.162.27:80      ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1030           *:*
  UDP    0.0.0.0:1040           *:*
  UDP    0.0.0.0:1155           *:*
  UDP    0.0.0.0:1175           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1036         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:2922         *:*
  UDP    192.168.1.100:123      *:*
  UDP    192.168.1.100:137      *:*
  UDP    192.168.1.100:138      *:*
  UDP    192.168.1.100:1900     *:*
```

11. tracert :

The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values

```
C:\Users\Admin>tracert google.com

Tracing route to google.com [216.58.196.206]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.100
  2    12 ms     8 ms     5 ms  103.62.239.241
  3     *        4 ms     7 ms  172.22.22.37
  4     6 ms     7 ms     4 ms  172.22.22.1
  5    12 ms    12 ms    20 ms  45.120.248.10
  6     9 ms     5 ms     8 ms  108.170.251.113
  7    13 ms    12 ms    22 ms  216.239.56.253
  8     3 ms     3 ms     3 ms  del03s06-in-f14.1e100.net [216.58.196.206]

Trace complete.

C:\Users\Admin>
```

Command	Working
ping	command is one of the most often used networking utilities for detecting devices on a network and for troubleshooting network problems.
hostname	command that displays the host name of your machine
ipconfig	frequently used utility that is used for finding network information about your local machine like ip addresses, dns addresses etc.
nbtstat	diagnostic tool for troubleshooting netbios problems
netstat	used for displaying information about tcp and udp connections and ports.
getmac	command that shows the mac address of your network interfaces
arp	for showing the address resolution cache. this command must be used with a command line switch -a is the most common.
tracert	command prints the path. if all routers on the path are functional, this command prints the full path.
path	command specifies the location where ms-dos should look when it executes a command.
route	command allows you to make manual entries into the network routing tables.
pathping	after sending out packets from you to a given destination, it analyzes the route taken and computes packet loss on a per-hop basis.

LAB ASSIGNMENT 4

OBJECTIVE: To understand the concept of subnetting and configure a vpc in GNS3.

1. Significance of classful addressing:

Classful addressing was the original method of IP address allocation used on the
Internet until the introduction of Classless Inter-Domain Routing (CIDR) in the mid-1990s. Under classful addressing, IP addresses were divided into five classes: Class A, B, C, D, and E.
Each class of IP addresses had a fixed length network prefix and host identifier, which determined the maximum number of networks and hosts that could be supported.

Here's a brief overview of each class :
● Class A addresses use the first octet to represent the network ID, with the remaining three octets used to identify the host. This allows for a large number of networks (over 16 million) with a relatively small number of hosts per network (up to 16,777,214).

● Class B addresses use the first two octets to represent the network ID, with the remaining two octets used to identify the host. This allows for fewer networks (up to 65,536) with more hosts per network (up to 65,534).

● Class C addresses use the first three octets to represent the network ID, with the remaining octet used to identify the host. This allows for even fewer networks (up to 2,097,152) with even more hosts per network (up to 254).

● Class D addresses are used for multicasting, which allows one-to-many communication. The first four bits of the first octet are set to 1110, and the remaining bits represent the multicast group ID.

● Class E addresses are reserved for experimental or research purposes. The first four bits of the first octet are set to 1111.

The main significance of classful addressing is that it provided a simple and efficient way to allocate IP addresses when the Internet was first being developed. However, classful addressing had several drawbacks, including inefficient use of address space, difficulty in allocating addresses, and difficulty in managing routing tables.

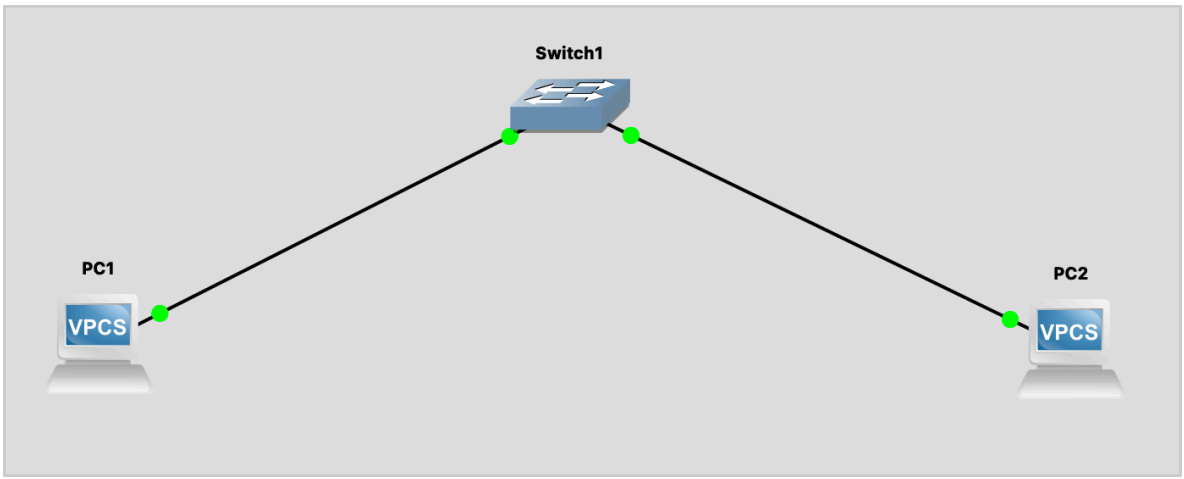
2. Discuss on subnetting and subnet mask

Subnetting is the process of dividing a larger network into smaller subnetworks, or subnets, to improve network performance, security, and manageability. Subnetting involves the use of a subnet mask, which is a 32-bit number that is used to divide an IP address into a network portion and a host portion.

The subnet mask is applied to an IP address to identify the network and host portions of the address. The network portion of the address identifies the subnet, while the host portion identifies the specific host within the subnet. The subnet mask is a binary number that consists of a sequence of ones followed by a sequence of zeros. The ones indicate the network portion of the address, while the zeros indicate the host portion of the address.

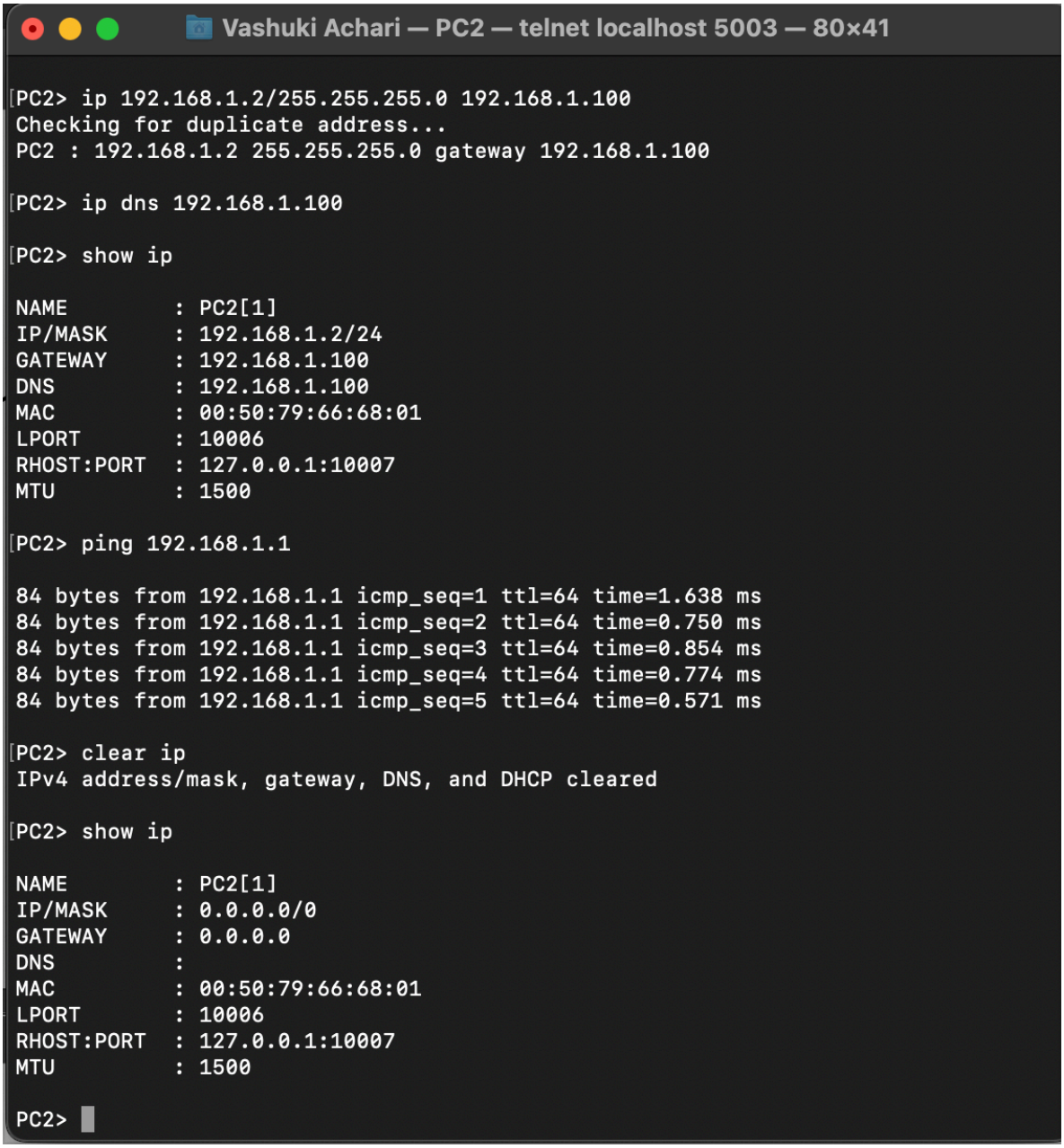
3.

To divide the network 200.1.2.0 into 4 subnets, we can borrow 2 bits from the host portion of the address to create 4 subnets. This gives us a subnet mask of 255.255.255.192, which has 26 network bits and 6 host bits.
a. The IP addresses of the subnets are as follows: Subnet 1: 200.1.2.0
Subnet 2: 200.1.2.64
Subnet 3: 200.1.2.128
Subnet 4: 200.1.2.192
b. The total number of IP addresses in each subnet is 64, as each subnet has a block size of 64 addresses.
c. The total number of hosts that can be configured in each subnet is 62, as 2 addresses are reserved for the network address and broadcast address in each subnet.
d. The range of IP addresses in each subnet is as follows: Subnet 1: 200.1.2.1 to 200.1.2.62
Subnet 2: 200.1.2.65 to 200.1.2.126
Subnet 3: 200.1.2.129 to 200.1.2.190 Subnet 4: 200.1.2.193 to 200.1.2.254
To calculate the range of IP addresses in each subnet, we can use the following formula:
Network address = subnet address
First host address = network address + 1 Last host address = broadcast address - 1 Broadcast address = next subnet address - 1



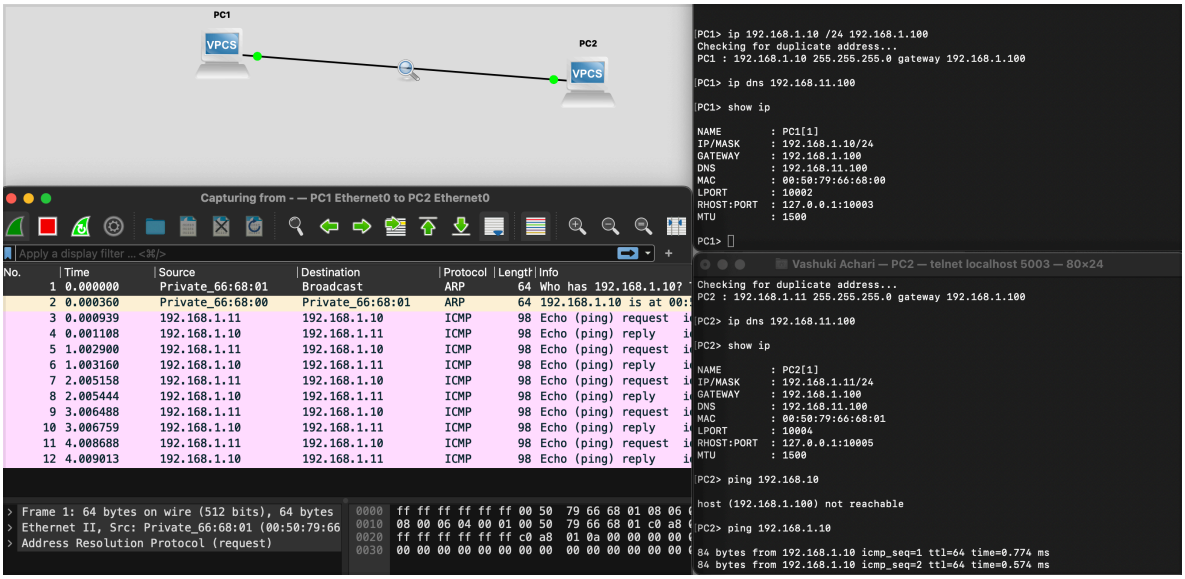
Vashuki Achari — PC1 — telnet localhost 5001 — 80×25

```
PC1> ip 192.168.1.1/255.255.255.0 192.168.1.100
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0 gateway 192.168.1.100

PC1> ip dns 192.168.1.100

PC1> ip dhcp
DDD

sho
Can't find dhcp server

PC1>
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 192.168.1.1/24
GATEWAY     : 192.168.1.100
DNS         : 192.168.1.100
MAC         : 00:50:79:66:68:00
LPORT       : 10004
RHOST:PORT  : 127.0.0.1:10005
MTU         : 1500

PC1>
```

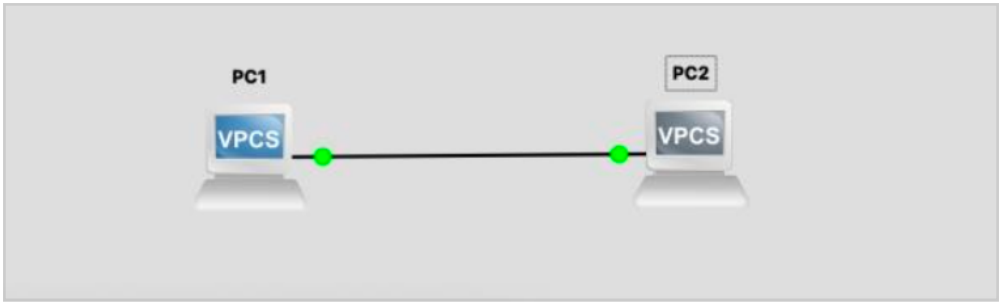


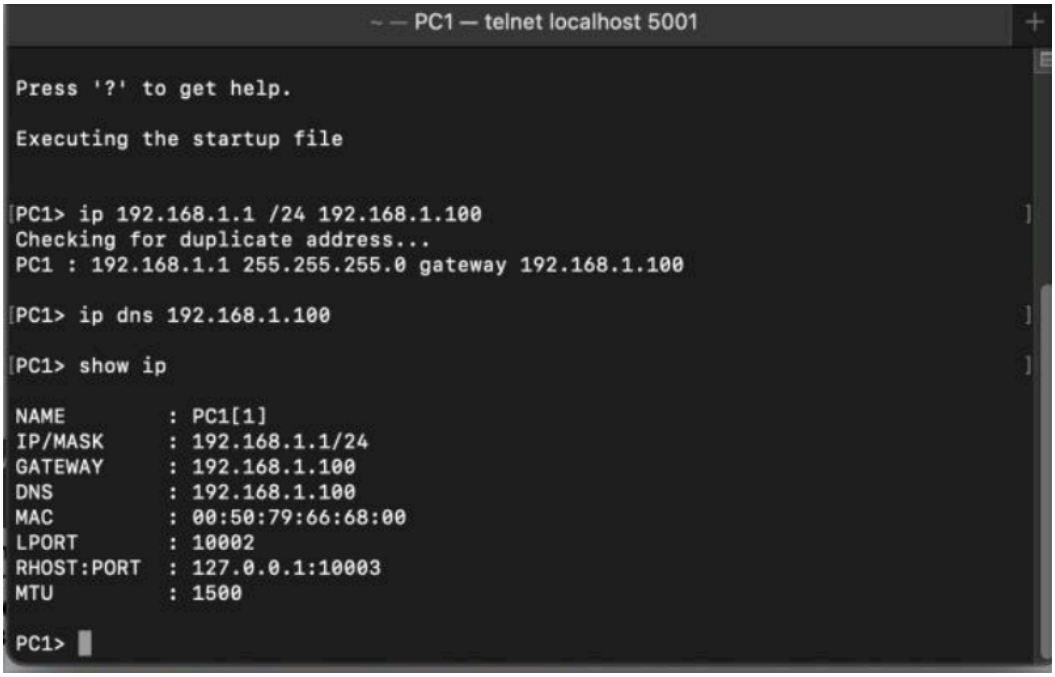
LAB ASSINMENT 5 :

1.


PC1
VPCS
PC2
VPCS
Capturing from - — PC1 Ethernet0 to PC2 Ethernet0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 Private_66:68:01 Broadcast ARP 64 Who has 192.168.1.10?
2 0.000360 Private_66:68:00 Private_66:68:01 ARP 64 192.168.1.10 is at 00:
3 0.000939 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) request
4 0.001108 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) reply
5 1.002900 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) request
6 1.003160 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) reply
7 2.005158 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) request
8 2.005444 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) reply
9 3.006488 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) request
10 3.006759 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) reply
11 4.008688 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) request
12 4.009013 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) reply
Frame 1: 64 bytes on wire (512 bits), 64 bytes
Ethernet II, Src: Private_66:68:01 (00:50:79:66
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 50 79 66 68 01 08 06
0010 08 00 06 04 00 01 00 50 79 66 68 01 c0 a8
0020 ff ff ff ff ff ff c0 a8 01 0a 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PC1> ip 192.168.1.10 /24 192.168.1.100
Checking for duplicate address...
PC1 : 192.168.1.10 255.255.255.0 gateway 192.168.1.100
PC1> ip dns 192.168.11.100
PC1> show ip
NAME : PC1[1]
IP/MASK : 192.168.1.10/24
GATEWAY : 192.168.1.100
DNS : 192.168.11.100
MAC : 00:50:79:66:68:00
LPORT : 10002
RHOST:PORT : 127.0.0.1:10003
MTU : 1500
PC1>
Vashuki Achari — PC2 — telnet localhost 5003 — 80×24
Checking for duplicate address...
PC2 : 192.168.1.11 255.255.255.0 gateway 192.168.1.100
PC2> ip dns 192.168.11.100
PC2> show ip
NAME : PC2[1]
IP/MASK : 192.168.1.11/24
GATEWAY : 192.168.1.100
DNS : 192.168.11.100
MAC : 00:50:79:66:68:01
LPORT : 10004
RHOST:PORT : 127.0.0.1:10005
MTU : 1500
PC2> ping 192.168.10
host (192.168.1.100) not reachable
PC2> ping 192.168.1.10
84 bytes from 192.168.1.10 icmp_seq=1 ttl=64 time=0.774 ms
84 bytes from 192.168.1.10 icmp_seq=2 ttl=64 time=0.574 ms

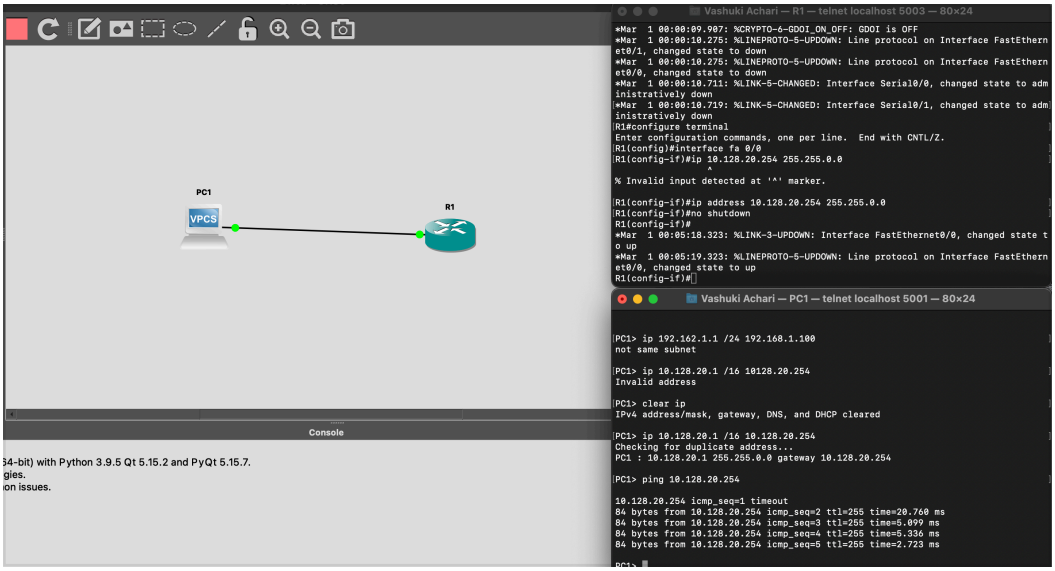
2.


PC1
VPCS
PC2
VPCS

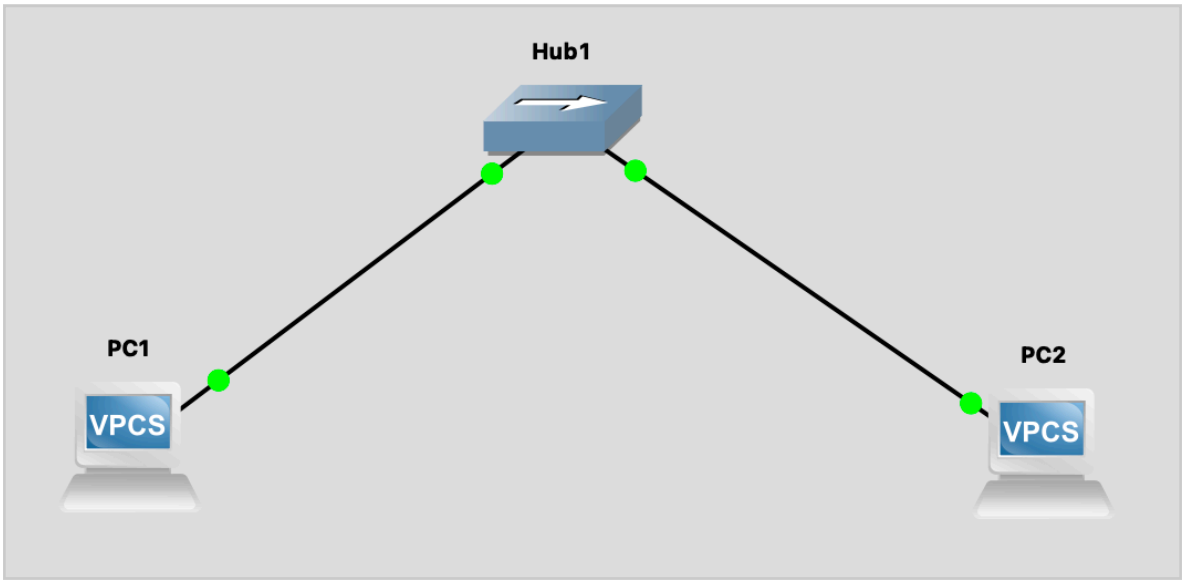

~ — PC1 — telnet localhost 5001
Press '?' to get help.
Executing the startup file
PC1> ip 192.168.1.1 /24 192.168.1.100
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0 gateway 192.168.1.100
PC1> ip dns 192.168.1.100
PC1> show ip
NAME : PC1[1]
IP/MASK : 192.168.1.1/24
GATEWAY : 192.168.1.100
DNS : 192.168.1.100
MAC : 00:50:79:66:68:00
LPORT : 10002
RHOST:PORT : 127.0.0.1:10003
MTU : 1500
PC1>

```
~ — PC2 — telnet localhost 5003
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC2> ip 192.168.1.2 /24 192.168.1.100
Checking for duplicate address...
PC2 : 192.168.1.2 255.255.255.0 gateway 192.168.1.100

PC2> ip dns 192.168.1.100

PC2> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=0.230 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=0.615 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=0.647 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=0.633 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=0.647 ms

PC2>
```

3.



4.

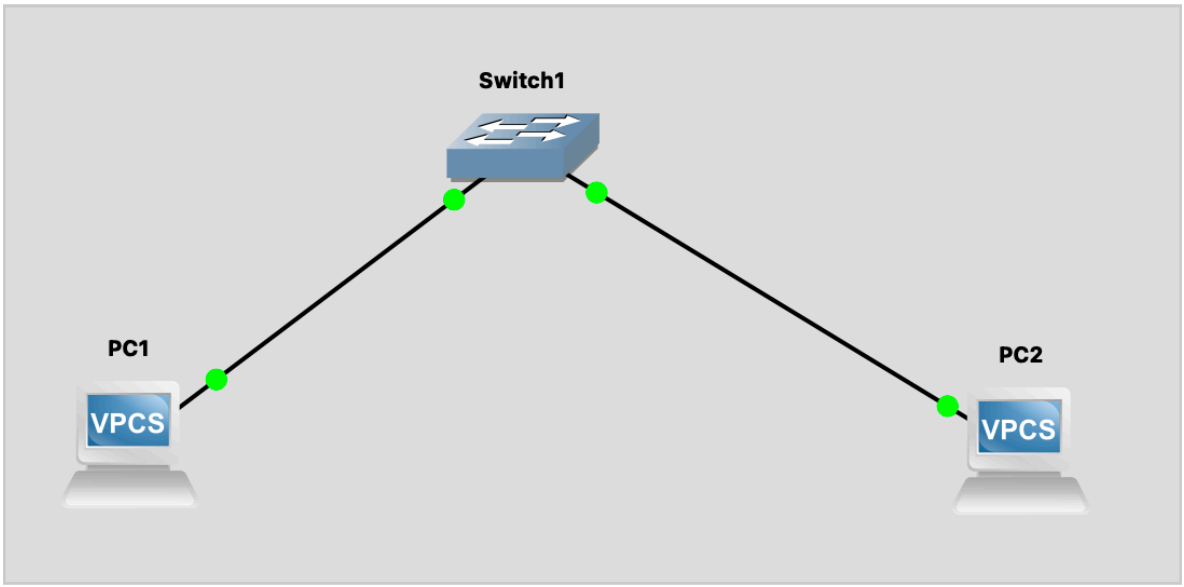


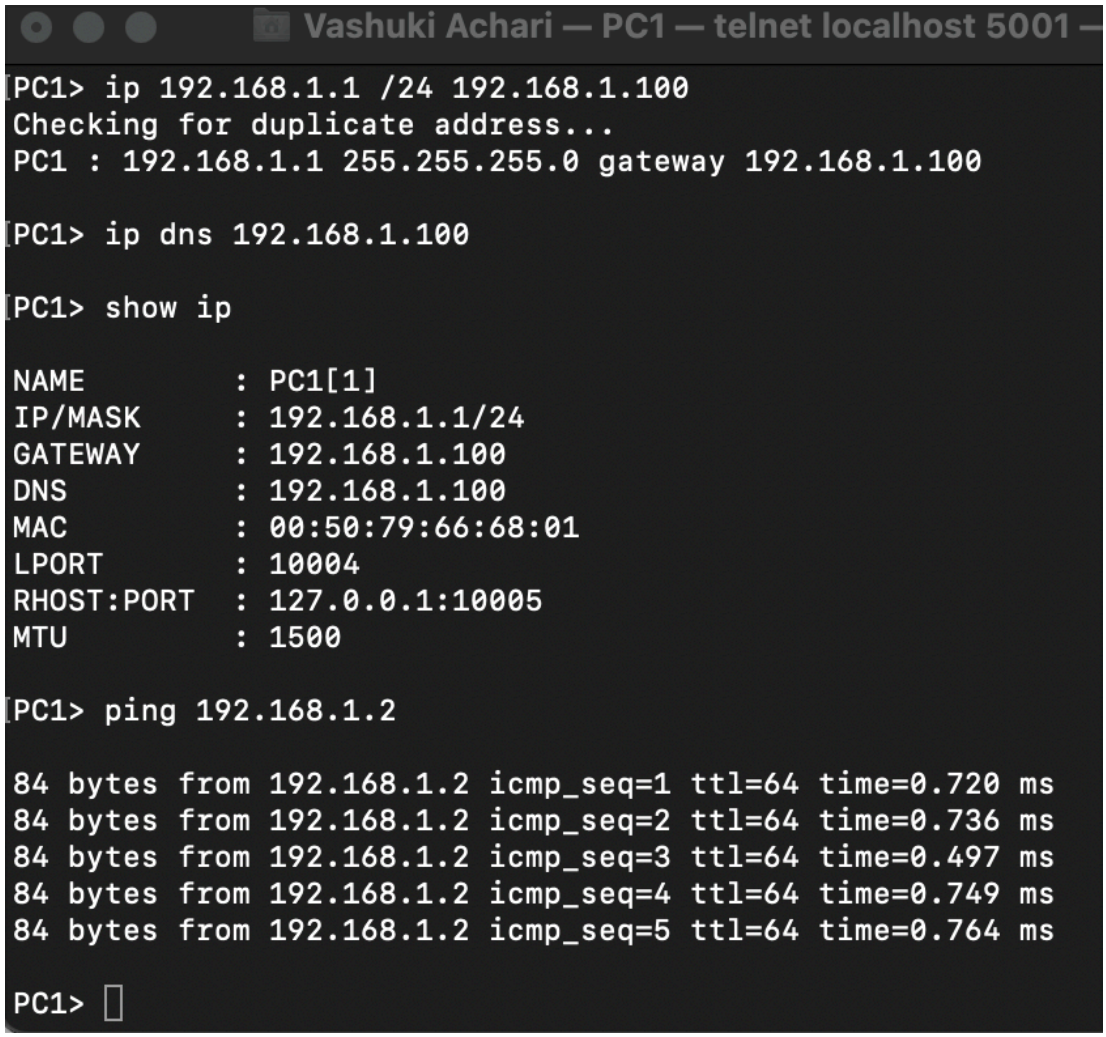
Vashuki Achari — PC1 — telnet localhost 5001 —

```
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 198.162.1.1/24
GATEWAY     : 198.162.1.100
DNS         : 198.162.1.100
MAC         : 00:50:79:66:68:01
LPORT       : 10004
RHOST:PORT  : 127.0.0.1:10005
MTU         : 1500

PC1> ping 198.162.1.2

host (198.162.1.2) not reachable

PC1> ping 198.162.1.2

84 bytes from 198.162.1.2 icmp_seq=1 ttl=64 time=0.506 ms
84 bytes from 198.162.1.2 icmp_seq=2 ttl=64 time=0.546 ms
84 bytes from 198.162.1.2 icmp_seq=3 ttl=64 time=0.748 ms
84 bytes from 198.162.1.2 icmp_seq=4 ttl=64 time=0.831 ms
84 bytes from 198.162.1.2 icmp_seq=5 ttl=64 time=0.601 ms

PC1>
```

```
Vashuki Achari — PC2 — telnet localhost 5003 -
PC2 : 198.162.1.2 255.255.255.0 gateway 198.162.1.100

PC2> ip dns 198.162.1.2

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 198.162.1.2/24
GATEWAY     : 198.162.1.100
DNS         : 198.162.1.2
MAC         : 00:50:79:66:68:00
LPORT       : 10006
RHOST:PORT  : 127.0.0.1:10007
MTU         : 1500

PC2> ping 198.162.1.1

84 bytes from 198.162.1.1 icmp_seq=1 ttl=64 time=1.546 ms
84 bytes from 198.162.1.1 icmp_seq=2 ttl=64 time=0.789 ms
84 bytes from 198.162.1.1 icmp_seq=3 ttl=64 time=0.636 ms
84 bytes from 198.162.1.1 icmp_seq=4 ttl=64 time=0.600 ms
84 bytes from 198.162.1.1 icmp_seq=5 ttl=64 time=0.750 ms

PC2>
```

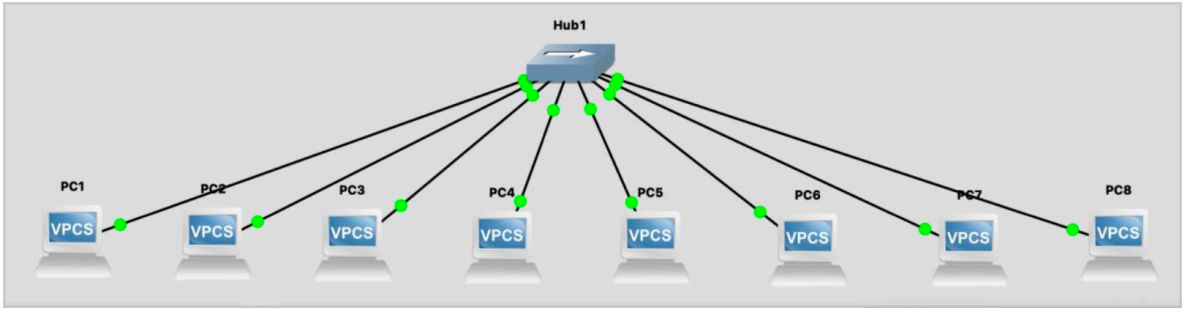
5.




Vashuki Achari — PC1 — telnet localhost 5001 —
PC1> ip 192.168.1.1 /24 192.168.1.100
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0 gateway 192.168.1.100
PC1> ip dns 192.168.1.100
PC1> show ip
NAME : PC1[1]
IP/MASK : 192.168.1.1/24
GATEWAY : 192.168.1.100
DNS : 192.168.1.100
MAC : 00:50:79:66:68:01
LPORT : 10004
RHOST:PORT : 127.0.0.1:10005
MTU : 1500
PC1> ping 192.168.1.2
84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=0.720 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=0.736 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=0.497 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=0.749 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=0.764 ms
PC1>

```
Vashuki Achari — PC2 — telnet localhost 5003 –

PC2> ip 192.168.1.2 /24 192.168.1.100
Checking for duplicate address...
PC2 : 192.168.1.2 255.255.255.0 gateway 192.168.1.100

PC2> ip dns 192.168.1.100

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 192.168.1.2/24
GATEWAY     : 192.168.1.100
DNS         : 192.168.1.100
MAC         : 00:50:79:66:68:00
LPORT       : 10006
RHOST:PORT  : 127.0.0.1:10007
MTU         : 1500

PC2> ping 192.168.1.2

192.168.1.2 icmp_seq=1 ttl=64 time=0.001 ms
192.168.1.2 icmp_seq=2 ttl=64 time=0.001 ms
192.168.1.2 icmp_seq=3 ttl=64 time=0.001 ms
192.168.1.2 icmp_seq=4 ttl=64 time=0.001 ms
192.168.1.2 icmp_seq=5 ttl=64 time=0.001 ms

PC2> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=0.510 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=0.718 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=0.728 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=0.747 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=0.711 ms

PC2>
```

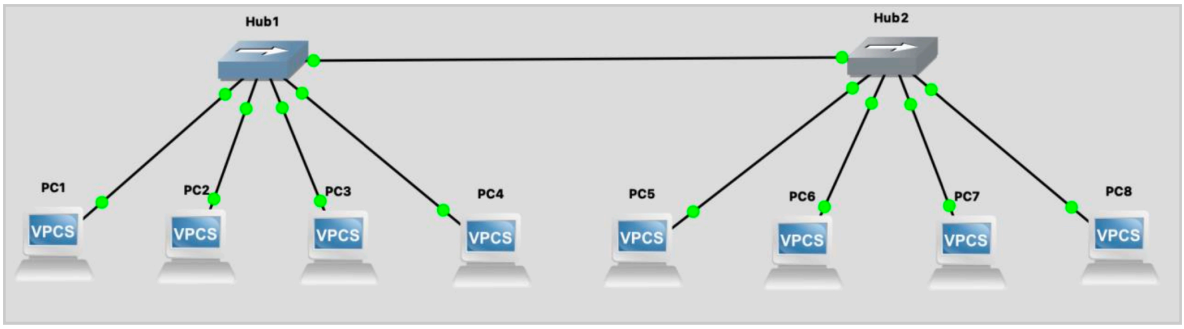
6. (a)

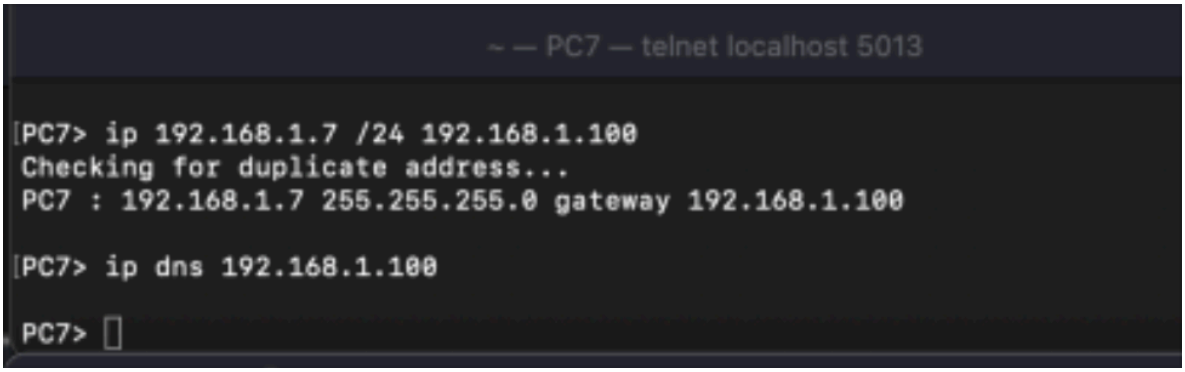


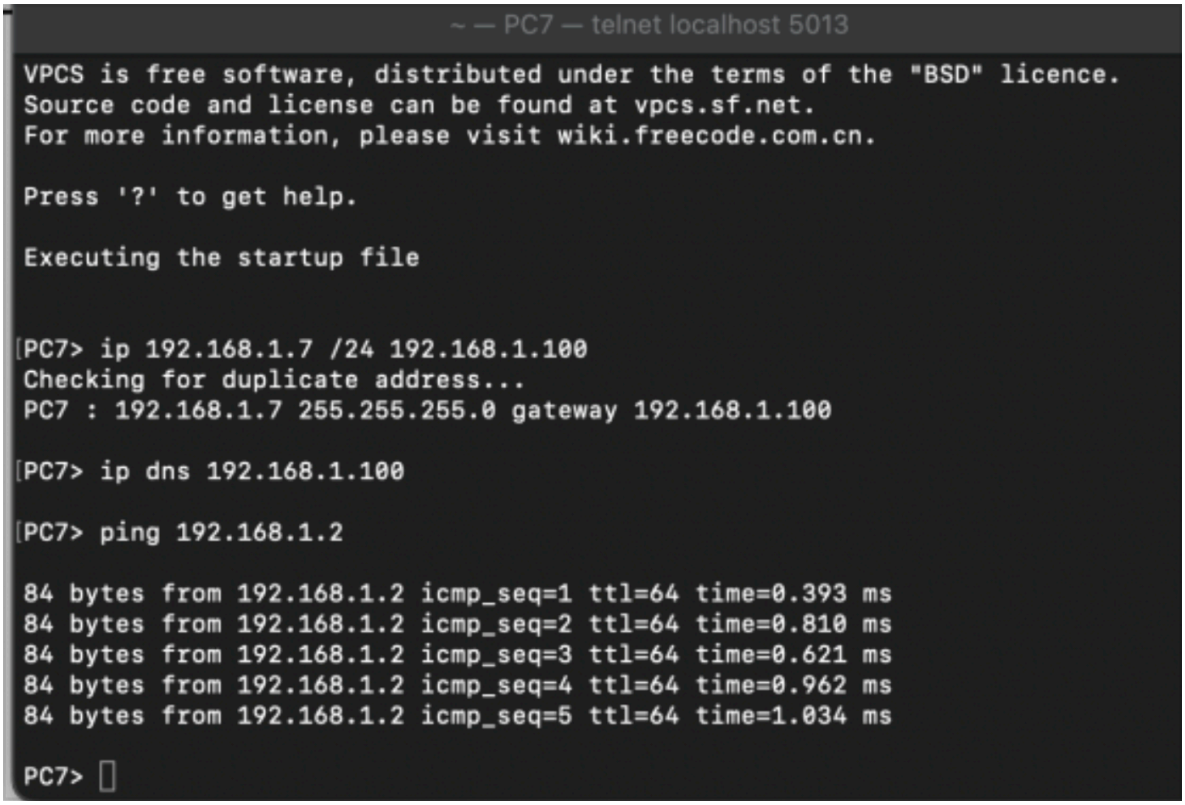
```
~ — PC1 — telnet localhost 5001

PC1> ip 192.168.1.1 /24 192.168.1.100
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0 gateway 192.168.1.100

PC1> ip dns 192.168.1.100

PC1>
```

```
~ — PC1 — telnet localhost 5001

Executing the startup file


PC1> ip 192.168.1.1 /24 192.168.1.100
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0 gateway 192.168.1.100

PC1> ip dns 192.168.1.100

PC1> ping 192.168.1.7

84 bytes from 192.168.1.7 icmp_seq=1 ttl=64 time=0.936 ms
84 bytes from 192.168.1.7 icmp_seq=2 ttl=64 time=0.809 ms
84 bytes from 192.168.1.7 icmp_seq=3 ttl=64 time=0.748 ms
84 bytes from 192.168.1.7 icmp_seq=4 ttl=64 time=0.766 ms
84 bytes from 192.168.1.7 icmp_seq=5 ttl=64 time=0.749 ms

PC1>
```

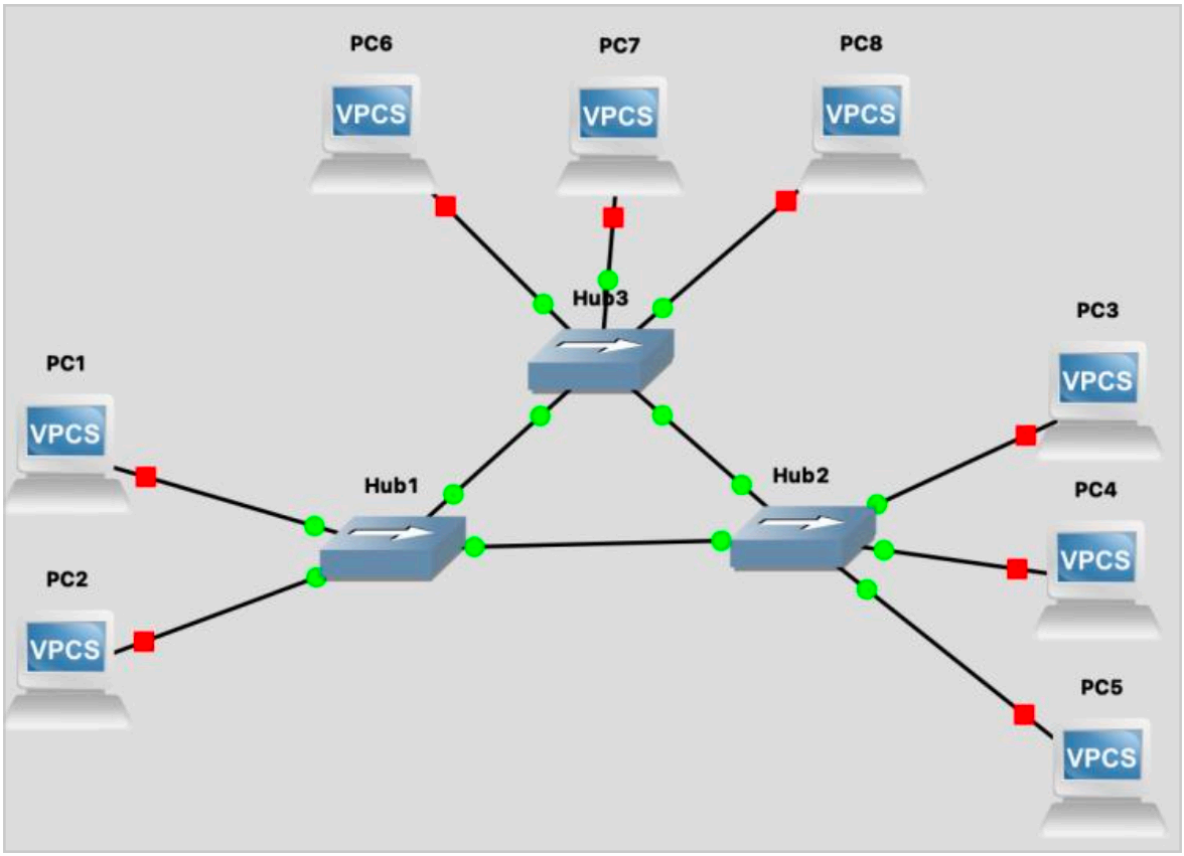
6. (b)



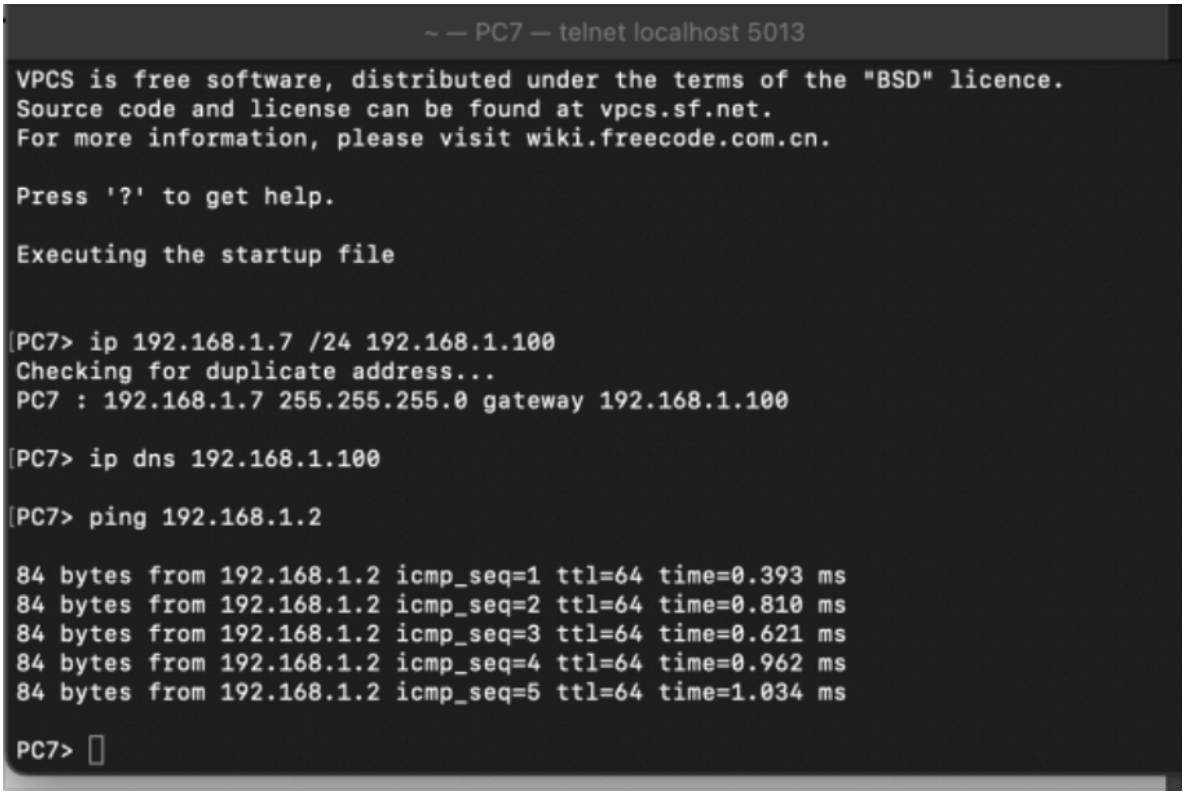

~ — PC7 — telnet localhost 5013
PC7> ip 192.168.1.7 /24 192.168.1.100
Checking for duplicate address...
PC7 : 192.168.1.7 255.255.255.0 gateway 192.168.1.100
PC7> ip dns 192.168.1.100
PC7>


~ — PC7 — telnet localhost 5013
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
PC7> ip 192.168.1.7 /24 192.168.1.100
Checking for duplicate address...
PC7 : 192.168.1.7 255.255.255.0 gateway 192.168.1.100
PC7> ip dns 192.168.1.100
PC7> ping 192.168.1.2
84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=0.393 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=0.810 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=0.621 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=0.962 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=1.034 ms
PC7>

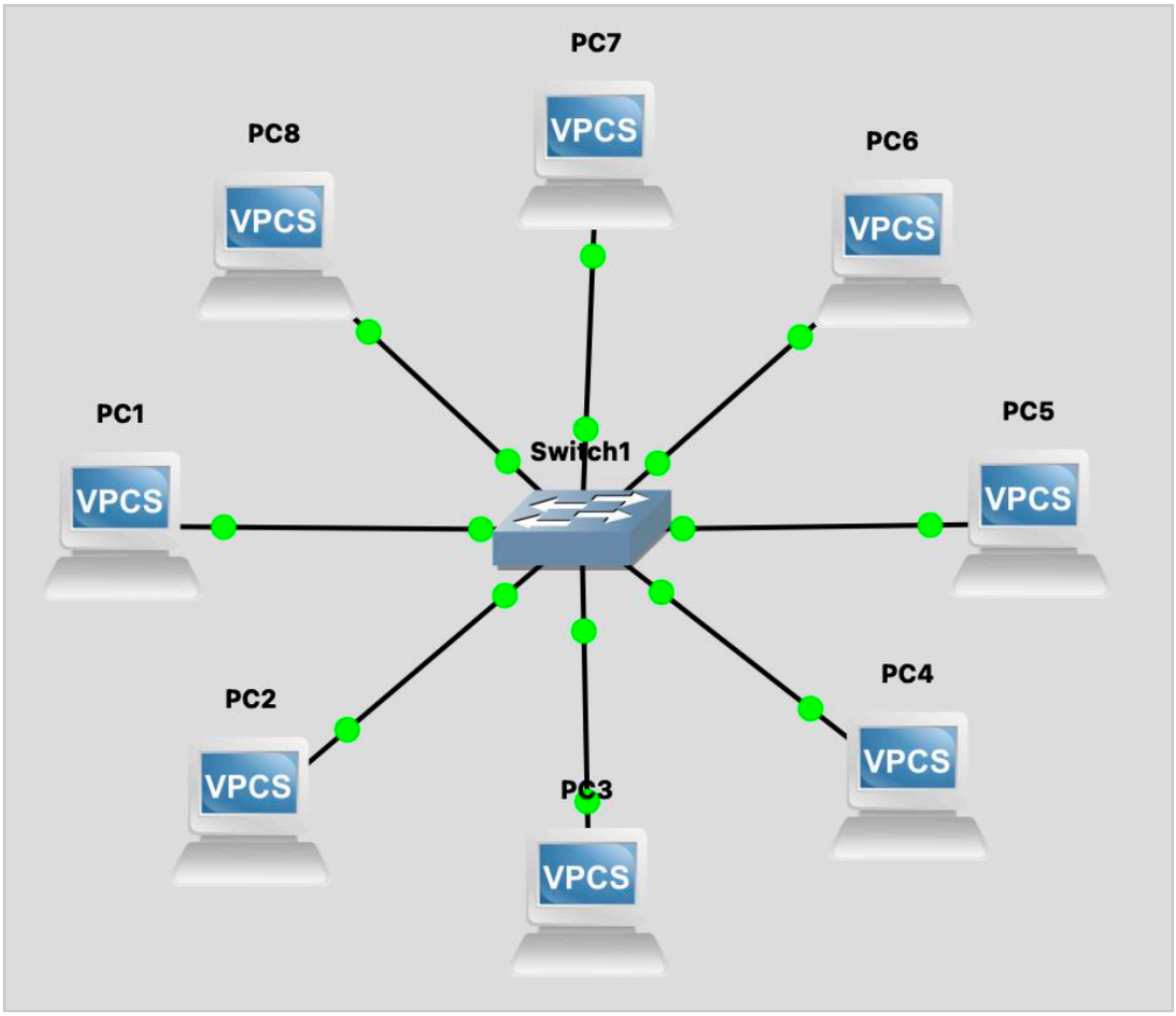
7.




```
~ — PC7 — telnet localhost 5013

PC7> ip 192.168.1.7 /24 192.168.1.100
Checking for duplicate address...
PC7 : 192.168.1.7 255.255.255.0 gateway 192.168.1.100

PC7> ip dns 192.168.1.100

PC7>
```


~ — PC7 — telnet localhost 5013
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
PC7> ip 192.168.1.7 /24 192.168.1.100
Checking for duplicate address...
PC7 : 192.168.1.7 255.255.255.0 gateway 192.168.1.100
PC7> ip dns 192.168.1.100
PC7> ping 192.168.1.2
84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=0.393 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=0.810 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=0.621 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=0.962 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=1.034 ms
PC7>

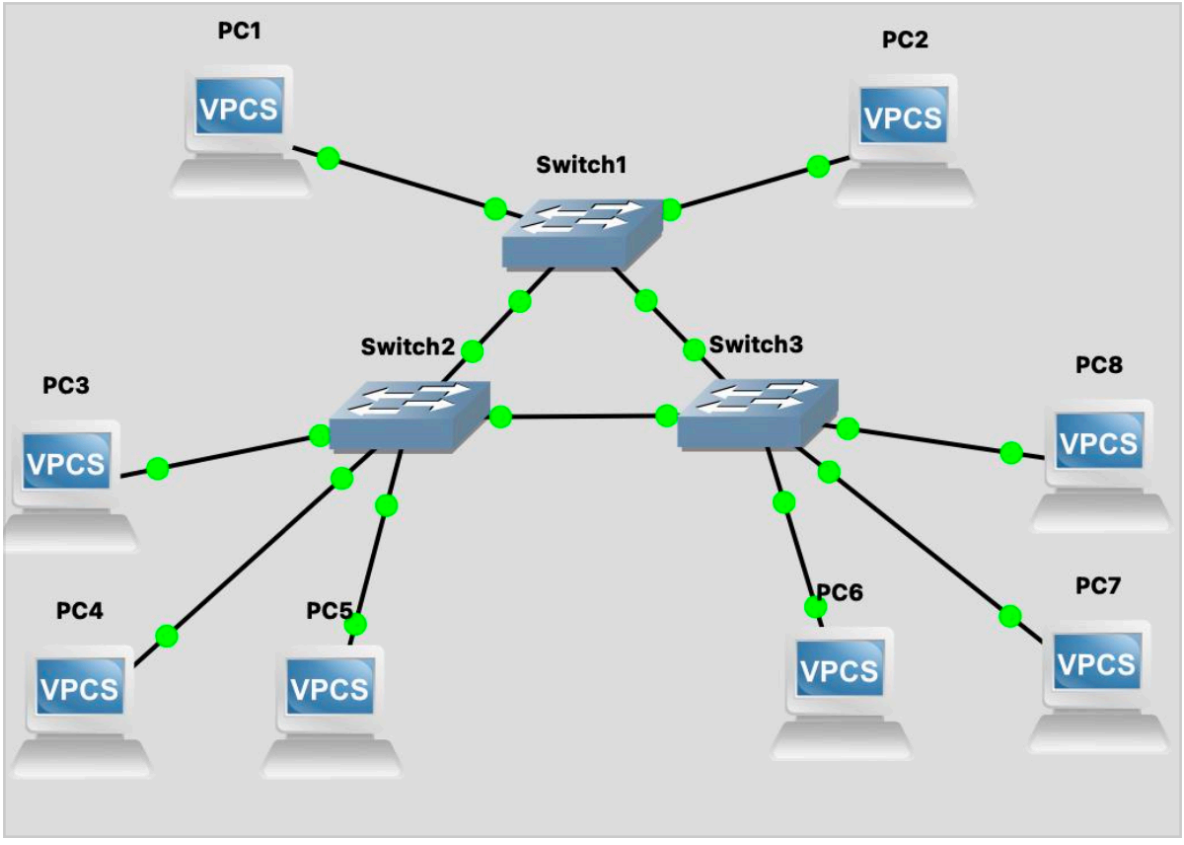
8.

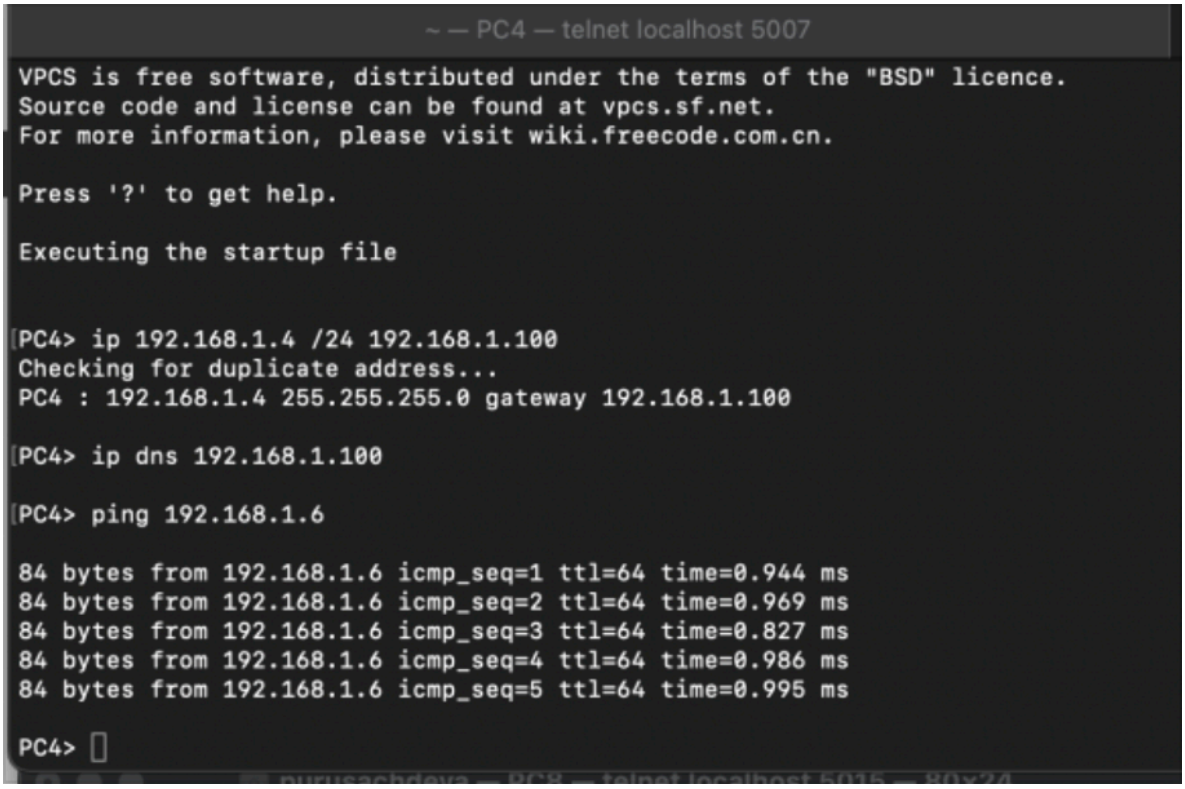



```
~ — PC7 — telnet localhost 5013

PC7> ip 192.168.1.7 /24 192.168.1.100
Checking for duplicate address...
PC7 : 192.168.1.7 255.255.255.0 gateway 192.168.1.100

PC7> ip dns 192.168.1.100

PC7>
```

```
~ — PC7 — telnet localhost 5013
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC7> ip 192.168.1.7 /24 192.168.1.100
Checking for duplicate address...
PC7 : 192.168.1.7 255.255.255.0 gateway 192.168.1.100

PC7> ip dns 192.168.1.100

PC7> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=0.393 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=0.810 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=0.621 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=0.962 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=1.034 ms

PC7>
```

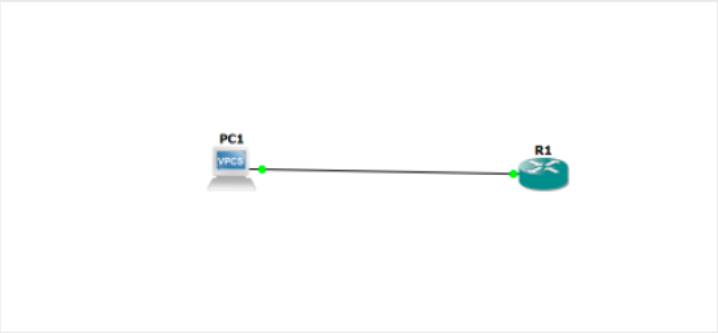
9.





LAB ASSINMENT 6 :

SETUP :



SETTING UP PC AND CONFIGURING IT :

```
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC1> ip 10.128.20.1 255.255.0.0
Checking for duplicate address...
PC1 : 10.128.20.1 255.255.0.0

PC1> ip 10.128.20.1 10.128.20.254
Checking for duplicate address...
PC1 : 10.128.20.1 255.255.255.0 gateway 10.128.20.254

PC1> show ip

NAME        : PC1[1]
IP/MASK     : 10.128.20.1/24
GATEWAY     : 10.128.20.254
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 10004
RHOST:PORT  : 127.0.0.1:10005
MTU:        : 1500

PC1>
```

Checking the interface for the router :

```
R1#show interfaces
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is DEC21140, address is ca01.3734.0000 (bia ca01.3734.0000)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:06:59, 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
     0 packets input, 0 bytes
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

To configure the router with IP address and subnet mask :

```
PC1> ping 10.128.20.254
84 bytes from 10.128.20.254 icmp_seq=1 ttl=255 time=15.939 ms
84 bytes from 10.128.20.254 icmp_seq=2 ttl=255 time=15.970 ms
84 bytes from 10.128.20.254 icmp_seq=3 ttl=255 time=15.614 ms
84 bytes from 10.128.20.254 icmp_seq=4 ttl=255 time=15.155 ms
84 bytes from 10.128.20.254 icmp_seq=5 ttl=255 time=15.347 ms

PC1>
```

To check the connection between pc and the router

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fa 0/0
R1(config-if)#ip address 10.128.20.254 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#
*Feb 20 20:30:24.215: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1(config-if)#
*Feb 20 20:30:25.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#
```

Setting up the console password for router :

```
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#enable password cisco
R1(config)#enable secret peter
R1(config)#
```