

COMPUTER NETWORKING FUNDAMENTALS

Volume I

by ROZANITA, NORHAYATI, MOHD NORALIMI



COMPUTER NETWORKING FUNDAMENTALS

Rozanita, 1969-

COMPUTER NETWORKING FUNDAMENTALS. Volume 1 / by ROZANITA,
NORHAYATI, MOHD NORALIMI.

Mode of access: Internet.

eISBN 978-967-2897-66-8

1. Computer networks.
2. Government publications--Malaysia.
3. Electronic books.

I. Norhayati, 1981-. II. Mohd. Noralimi, 1977-.

III. Title.

004.6

PUBLISHED BY:

POLITEKNIK PORT DICKSON
KM 14 JALAN PANTAI,
71050 SI RUSA, PORT DICKSON
NEGERI SEMBILAN
TEL: 06-662 2000/2111
FAKS: 06-662 2026/2027
Emel: webmaster@polipd.edu.my
Laman web: www.polipd.edu.my

SEPTEMBER 2022

Copyright Each part of this publication may not be reproduced or distributed in any forms by any means or retrieval system without prior written permission.

ACKNOWLEDGEMENT

PATRON

Dr. Ishak bin Mohamad
Director, Politeknik Port Dickson

ADVISORS

Abdul Rahim bin Ibrahim
Deputy Director (Academic), Politeknik Port Dickson
Abdul Razak bin Ismail
Head of Electrical Engineering Department, Politeknik Port Dickson

EDITOR

Ts. Ong Seng Keong
Senior Lecturer, Electrical Engineering Department , Politeknik Port Dickson

FACILITATORS

Nin Hayati Binti Mohd Yusof
Ragunathan A/L Jayaraman
Azilah binti Asri

WRITERS

Rozanita binti Baharudin
Norhayati binti Abdul Manaf
Mohd Noralimi bin Mohd Ali

We would like to convey our utmost gratitude to the Department of Polytechnic and Community College Education particularly the E-learning and Instructional Division (BIPD) for funding our e-book project.

We hereby declare that this module is our original work. To the best of our knowledge it contains no materials previously written or published by another person. However, if there is any, due acknowledgement and credit are mentioned accordingly in the e-book.

TABLE OF CONTENTS

ACKNOWLEDGEMENT	iii
------------------------	------------

1

INTRODUCTION TO NETWORKING

1.1 Computer networks	2
1.2 Networking standards	7
1.3 Types of networks	9
1.4 Classification of network	11
1.5 Computer network topology	13
1.6 Networking hardware	17
Exercise	22

2

OPEN SYSTEM INTERCONNECTION (OSI) MODEL AND NETWORK PROTOCOLS

2.1 OSI model	24
2.2 Internet Service Provider (ISP)	32
2.3 Domain Name System (DNS)	33
2.4 Email Protocol	37
2.5 TCP/IP Addressing	41
Exercise	47

ANSWER	49
---------------	-----------

REFERENCE	53
------------------	-----------



CHAPTER 1

Introduction to Networking

1.1

COMPUTER NETWORK

An arrangement that connects two or more computers together to communicate and exchange data is known as a computer network. Mobile phones and servers are both instances of computing hardware. These gadgets can communicate wirelessly or physically, such as through fiber optic cables.

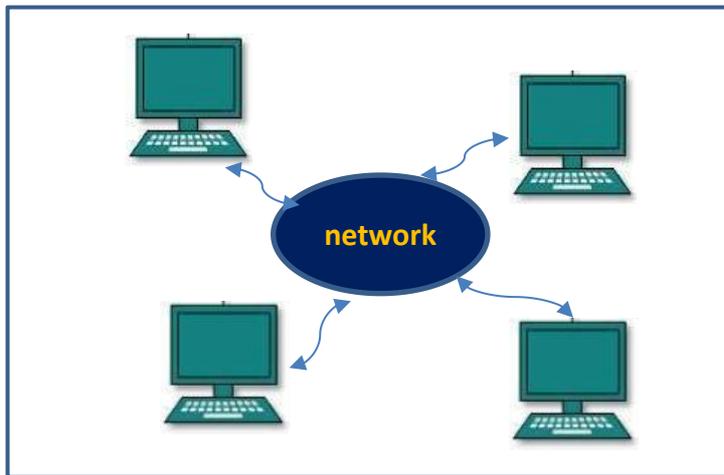


Figure 1.1(a) : Simple computer network connection

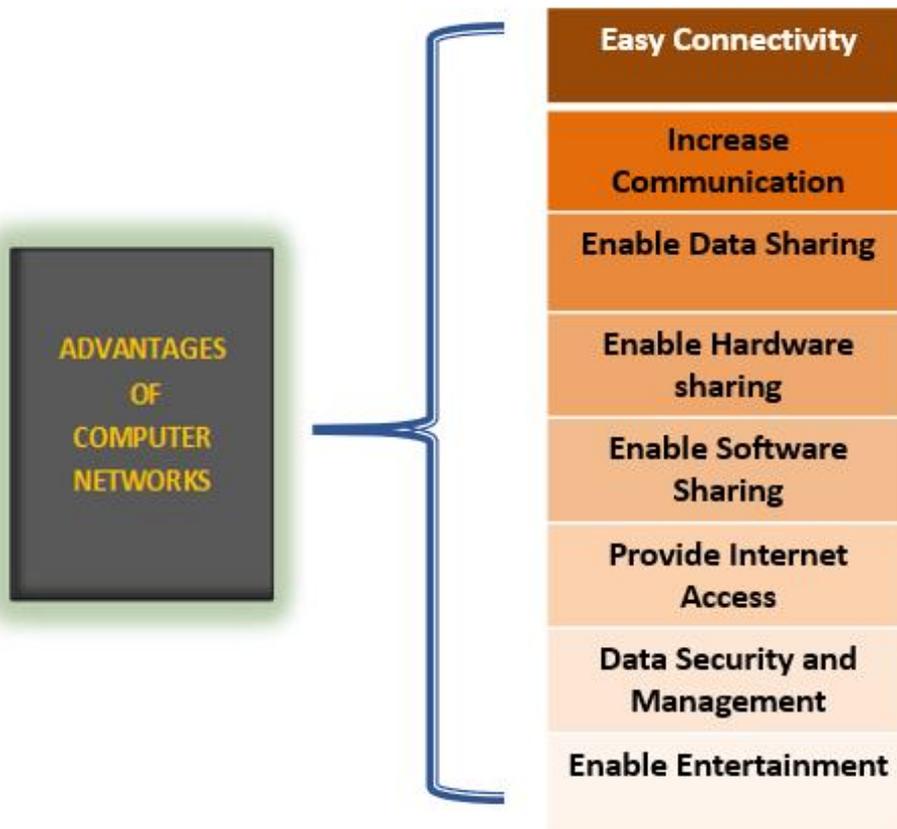
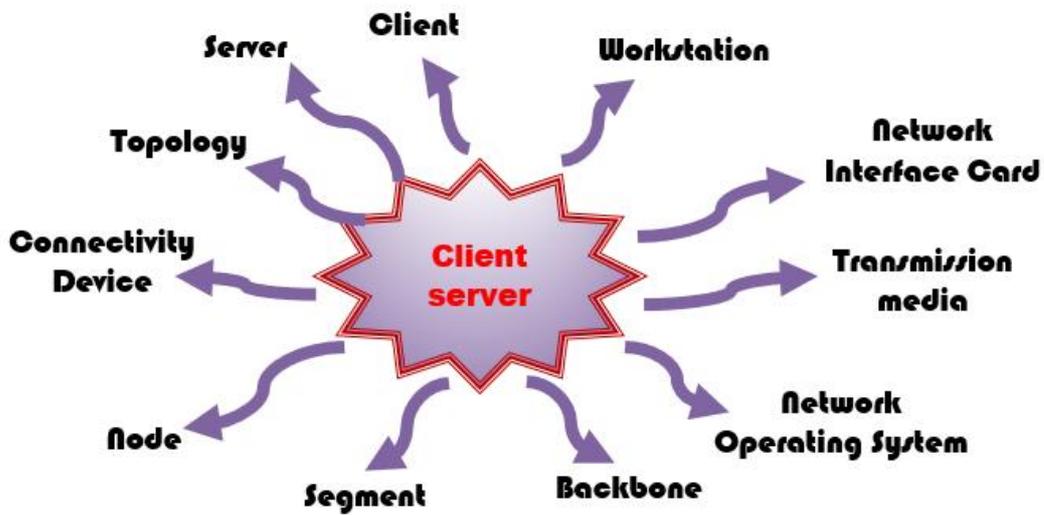


Figure 1.1(b) : Advantages of computer network

Element in client/server network



Client

A computer connect to a network that makes use of a server's services (such as shared peripherals or file access).

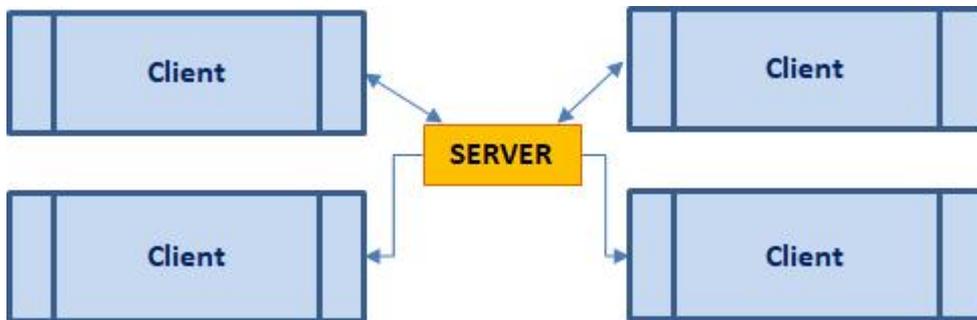


Figure 1.1(c) : Client

Server

A network machine that offers/manages the data and services used by other computers.



Figure 1.1(d) : Server box

Workstation

A personal computer (desktop or laptop) tend to be connected to a network.

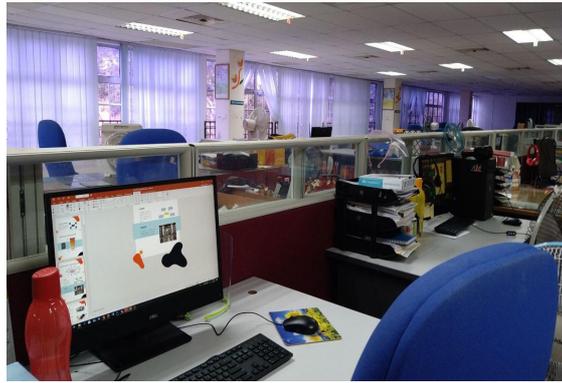


Figure 1.1(e) : Workstation in an office

Network Interface Card

A network interface card (NIC) is a piece of hardware that is installed into a computer to allow network connectivity.

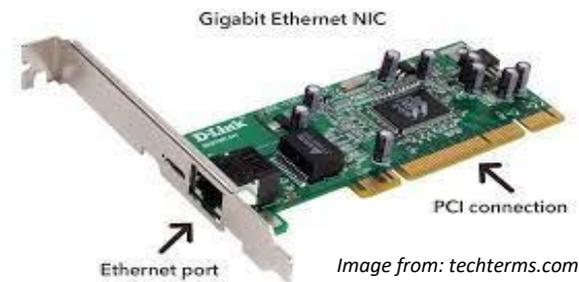


Figure 1.1(f) : Network Interface Card for desktop computer

Connectivity Device

Enables connection and data exchange between multiple networks or multiple parts of the networks.

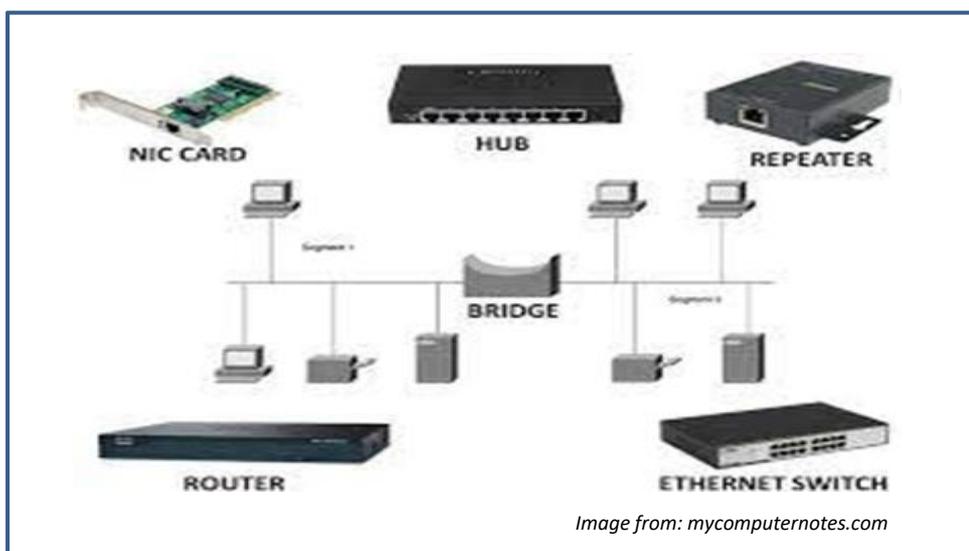


Figure 1.1(g) : Connectivity device arrangement in a connection

Network Topology

Network topology is a diagram that shows the arrangement of the logical and physical parts of nodes and connections in a network.

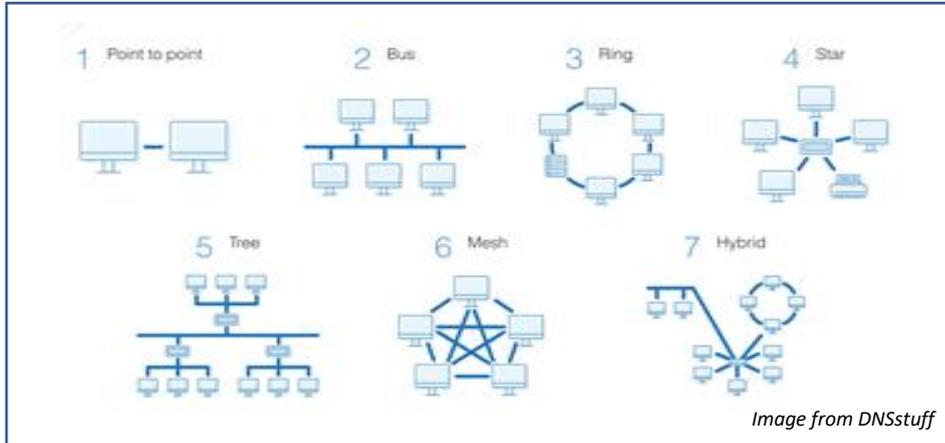


Figure 1.1(h) : Types of network topology

Segment

Network segmentation makes it possible for network administrators to control traffic between subnets in accordance with specific rules.

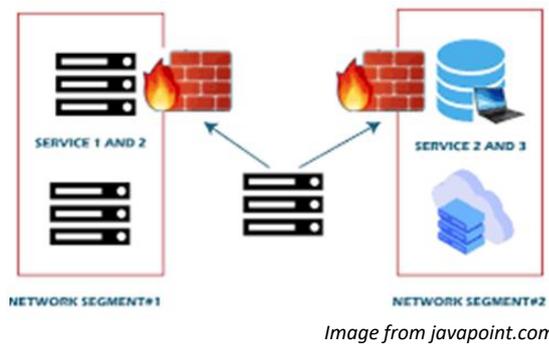


Figure 1.1(i) : Network segmentation

Network Operating System (NoS)

A system software (operating system), which support multiple devices and computers on the network.

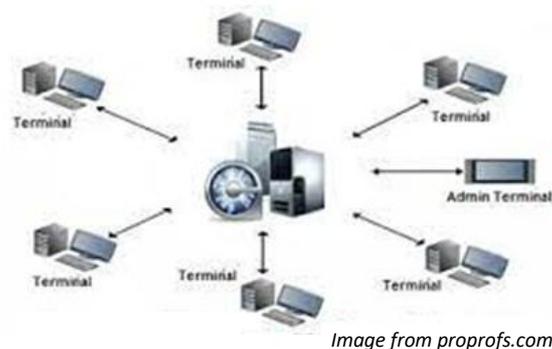


Figure 1.1(j) : Network operating system

Backbone

A part of computer network which providing a route for information to be exchanged across various LANs or subnetworks.

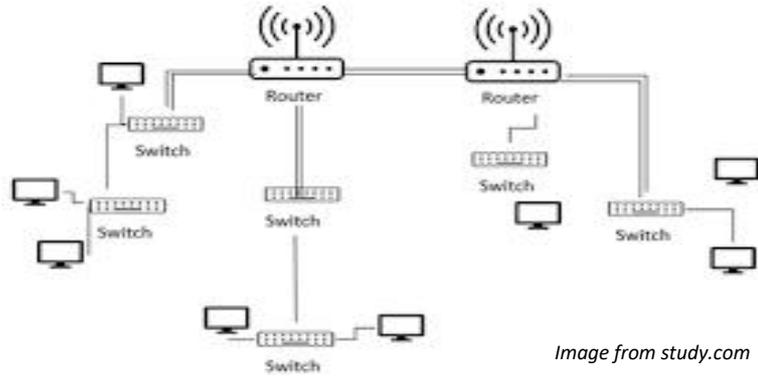


Image from study.com

Figure 1.1(k) : Backbone for a network connection

Transmission Media

The physical pathways which data is transmitted and received such as wire or cable (twisted-pair, coaxial and fiber optic) or atmospheric (wireless), such as radio waves, LAN or WAN.

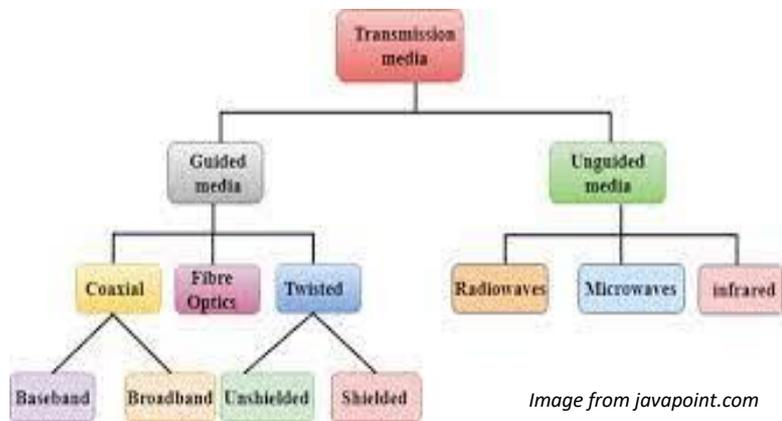


Image from javapoint.com

Figure 1.1(l) : Types of transmission media

Node

A client, server or other network-capable equipment that can be identified by specific number that sometimes referred to as its network address.

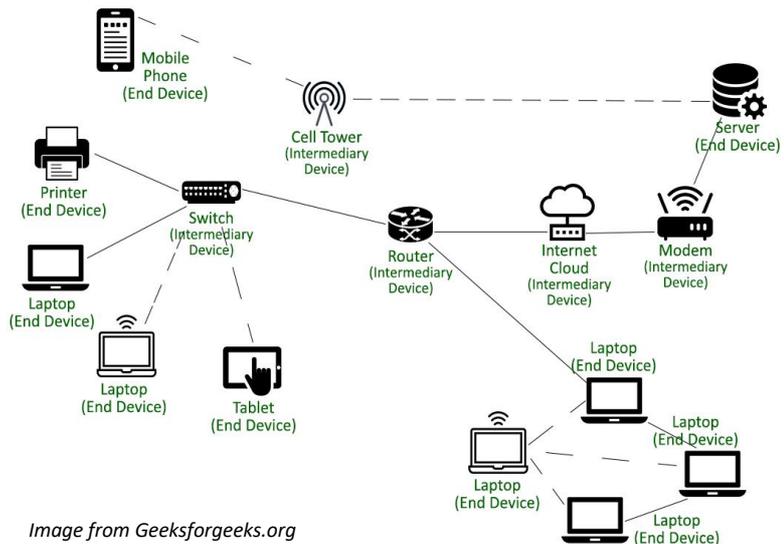


Image from Geeksforgeeks.org

Figure 1.1(m) : Types of transmission media

1.2

NETWORKING STANDARD

Networking standard is a documented description of the technical criteria, guidelines, and best practices that must be adhered to consistently in order to guarantee that the hardware, software, and other elements that regulate networking are appropriate for the task at hand. Effectiveness, quality, and safety are all guaranteed by standards.

Organization that establishes standards of networking



International
Organization for
Standardization

The objective of ISO is to create worldwide technology standards that will enable unrestricted trade and information sharing. Products and services must meet ISO standards for quality, dependability and safety.

The Institute for Electrical and Electronics Engineers (IEEE) is a professional organization that aims to advance technological innovation and excellence.



IEEE

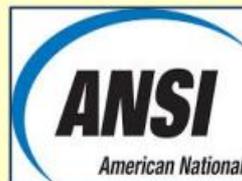
INSTITUTE FOR ELECTRICAL
AND ELECTRONICS ENGINEERS



International
Telecommunication
Union

The International Telecommunication Union (ITU) is the United Nations specialized agency for information and communication technologies

The American National Standards Institute determines whether voluntary consensus standards are being developed for American products, services, practices, infrastructure and personnel. It is a privately owned non-profit company.



ANSI
American National Standards Institute



The Internet Engineering Task Force (IETF) is an Internet standards body in charge of the engineering specifications that go into the TCP/IP family of Internet protocols.

An alliance of trade associations for American electronics manufacturers made up the American standards and trade organization known as the Electronic Industries Alliance.



The American National Standards Institute (ANSI) has accredited the Telecommunications Industry Association (TIA), a trade association, to create industry standards for information and communication technologies (ICT) products like cellular tower, data terminal, VoIP device, satellite, and telephone terminal equipment.

The Internet Society is a nonprofit advocacy group based in the United States that was established in 1992 and has local branches all around the world. Its aim is to promote the open development, evolution, and use of the Internet for the benefit of all people across the world.



Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization with members from all around the world that works to maintain the stability, interoperability and security of the Internet.

Computers and other networking devices can be positioned on a network in different ways relative to each other. The connection between networking devices can be established by two types of network, peer-to-peer network and client/server network.

Peer-to-Peer Network

Each computer in a peer-to-peer network is on an equal footing and has access to the same resources and information. Users can share content that is connected to or saved on their computers with other computers using this simple type of network.

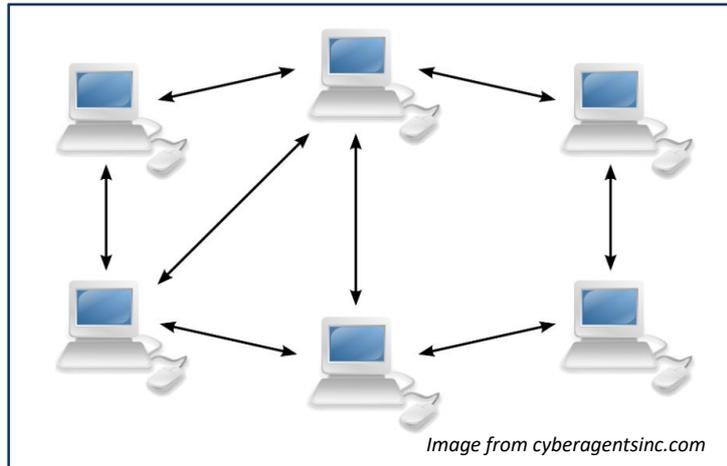


Figure 1.3(a) : Peer-to-peer network connection

Advantages and Disadvantages Peer-to-Peer Network

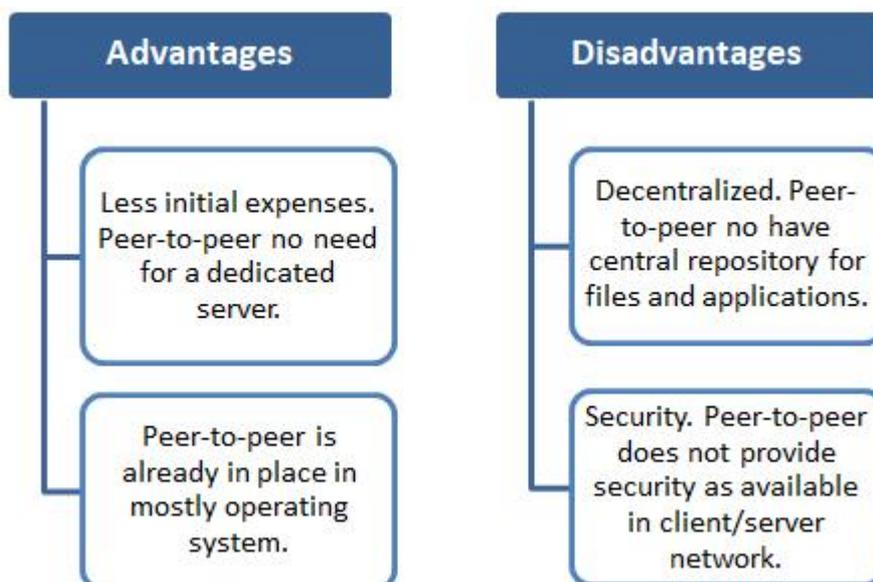


Figure 1.3(b) : Advantages and Disadvantages of peer-to-peer network

Client/Server Network

Every network resource, including shared devices, directories, files, and programs are managed and hosted centrally in a client-server network before being accessed by clients. Client-server networks are identified by the presence of servers that administer and provide security for them.

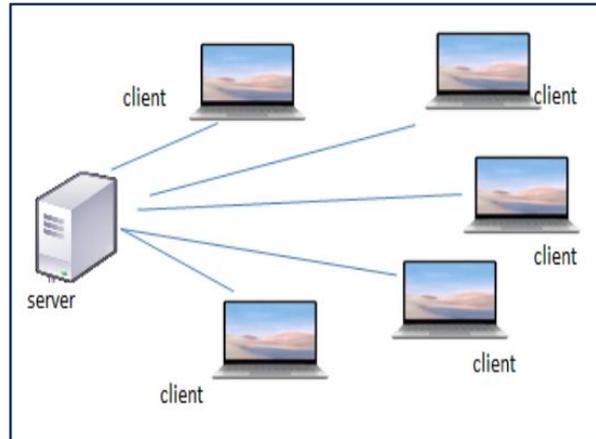


Figure 1.3(c) : Client/server network connection

Advantages and Disadvantages Client/Server Network

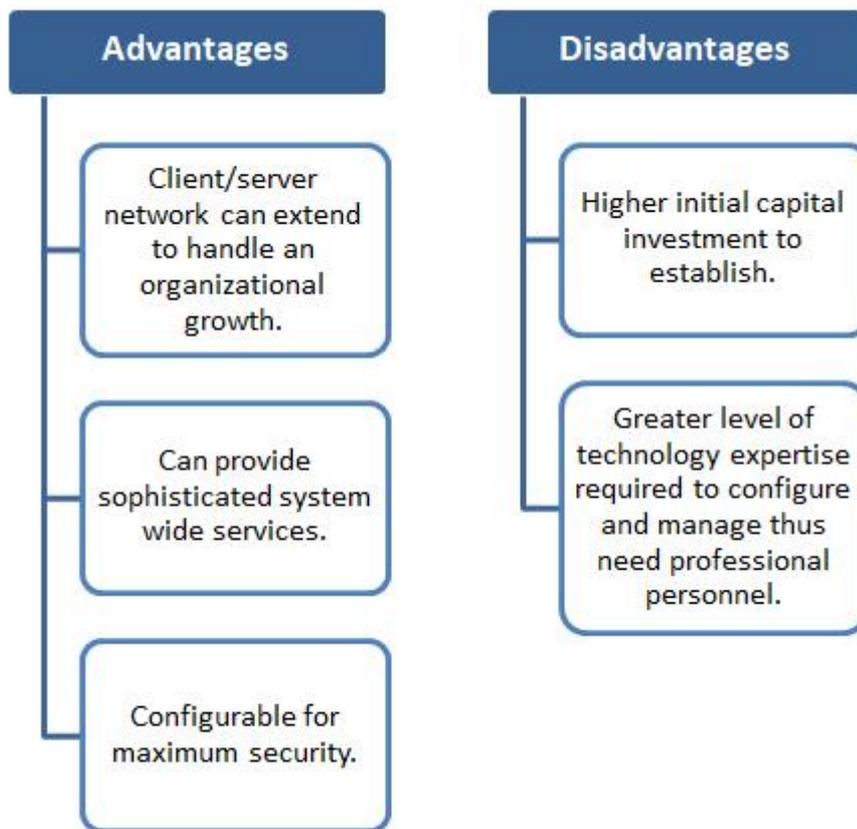


Figure 1.3(d) : Advantages and Disadvantages of client/server network

Local Area Network (LAN)

A local area network (LAN) is a type of computer network that connects computers in a single location such as a house, office, school, lab, or university campus.

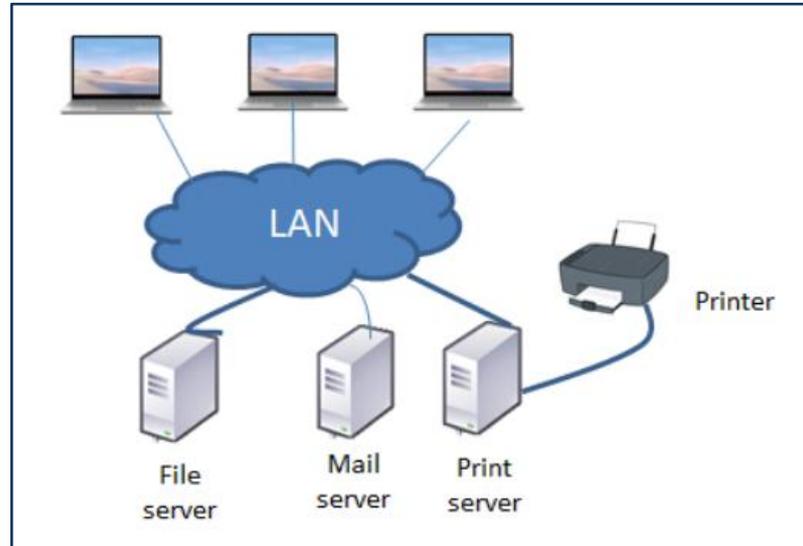


Figure 1.4(a) : Local Area Network connection

Metropolitan Area Network (MAN)

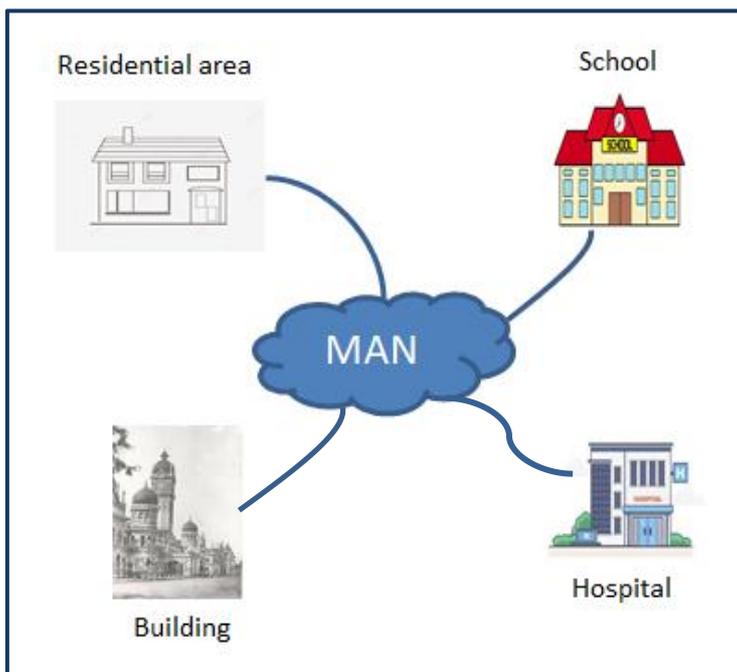


Figure 1.4(b) : Metropolitan Area Network connection

A metropolitan area network (MAN) covers an entire city, campus, or other area under the control of a municipality or other organization. Multiple LANs are connected to create MANs. It is ideal for many kinds of network users because it is a medium-size network.

Wide Area Network (MAN)

A wide area network (WAN) is a type of computer network that spans a substantial geographic area, such as an entire continent, country, or even the world. The technologies used by WAN allow data, picture, audio, and video to be transmitted over vast distances and between various LANs and MANs.



Figure 1.4(c): Wide Area Network connection

A topology is the configuration of how computer systems or network devices are connected to one another. A network's logical and physical components can be described by its topologies. The logical and physical topologies of a network may be the same or dissimilar.

Bus Topology

Consists of a single wire, known as the bus, which connects each network node without the need for additional connecting hardware in between. There is only one communication channel allowed in a bus topology, each node shares the bus's overall capacity. Until it reaches the intended recipient, a signal from the source goes in both directions to all machines linked to the bus wire.

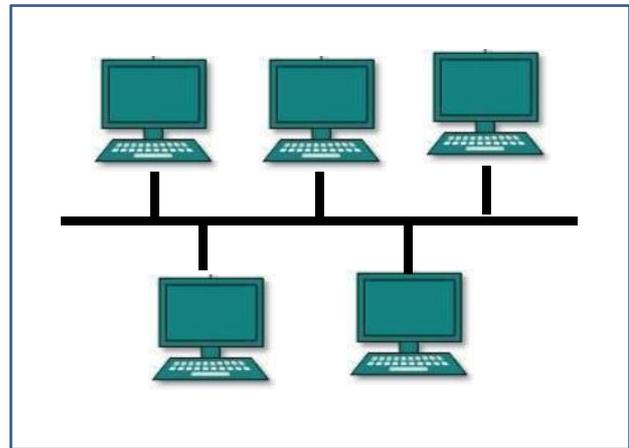
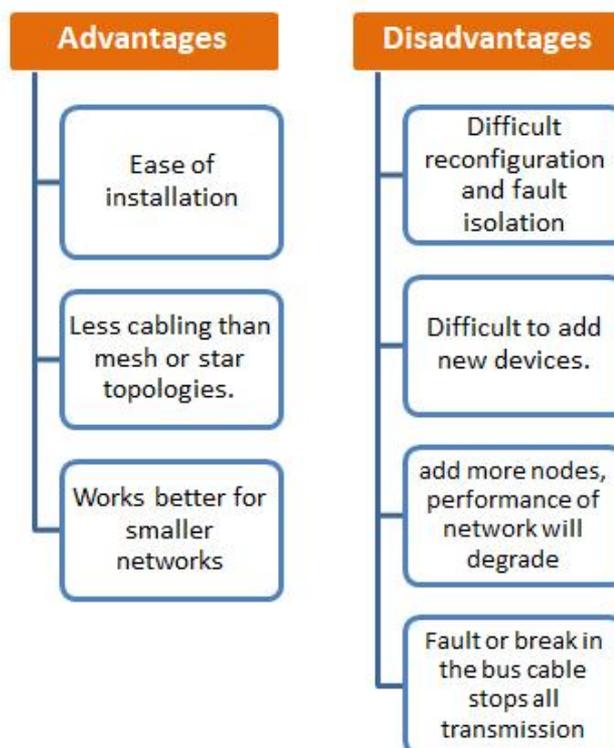


Figure 1.5(a) : Bus topology connection

Advantages and Disadvantages Bus Topology



Ring Topology

Devices are interconnected in a ring structure and communicate with one another based on the neighbouring nodes of their ring node.

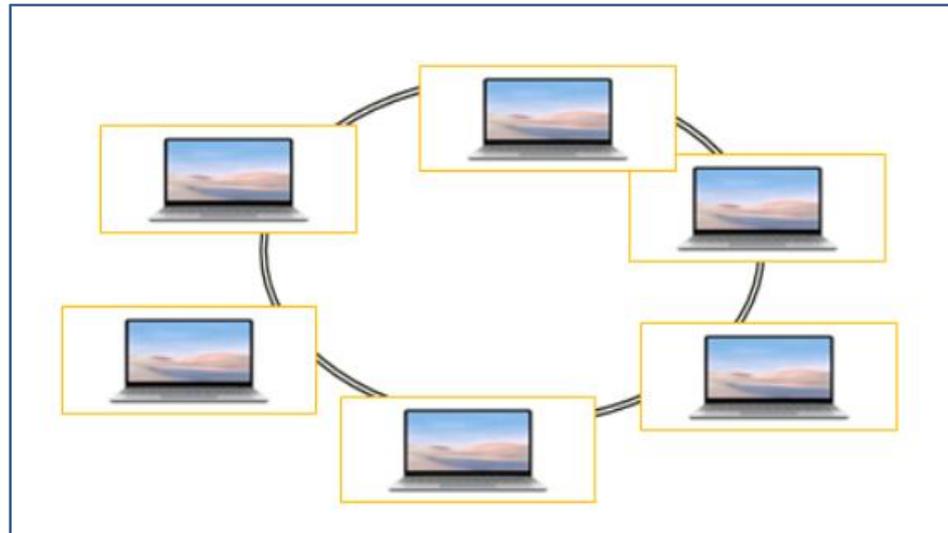
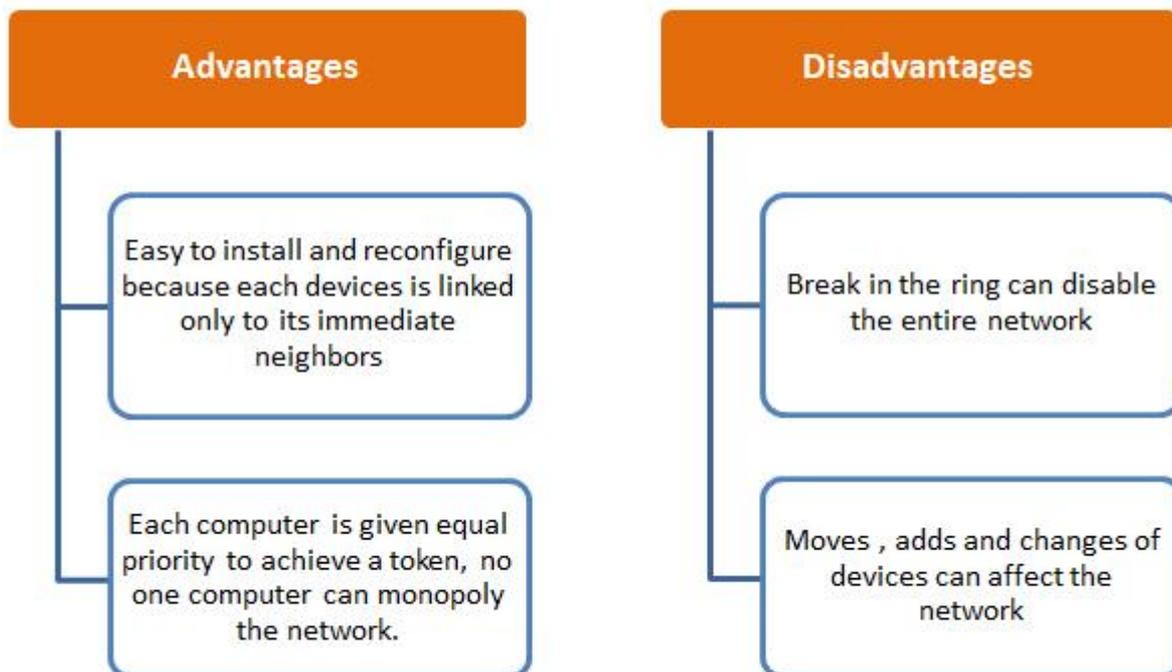


Figure 1.5(b) : Ring topology connection

Advantages and Disadvantages Ring Topology



Star Topology

A type of network topology in which each device is separately connected to a hub or switch as the network's central node.

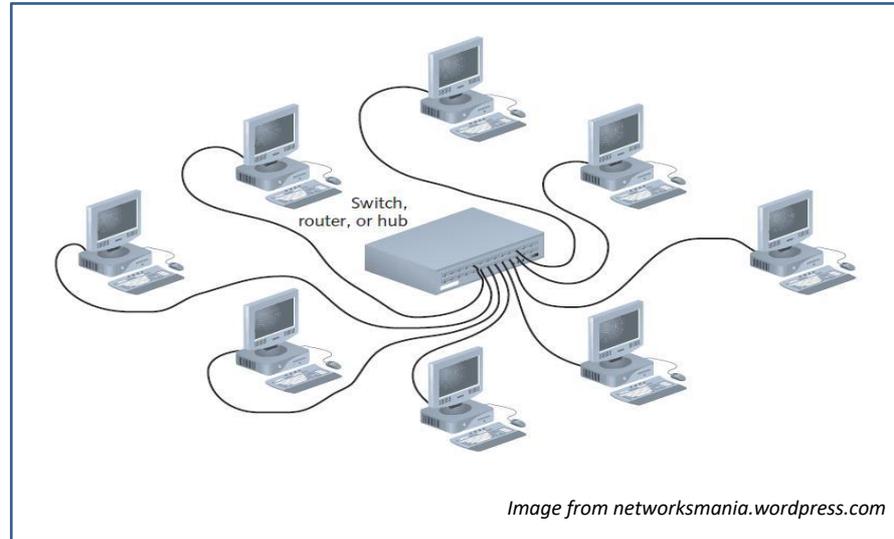
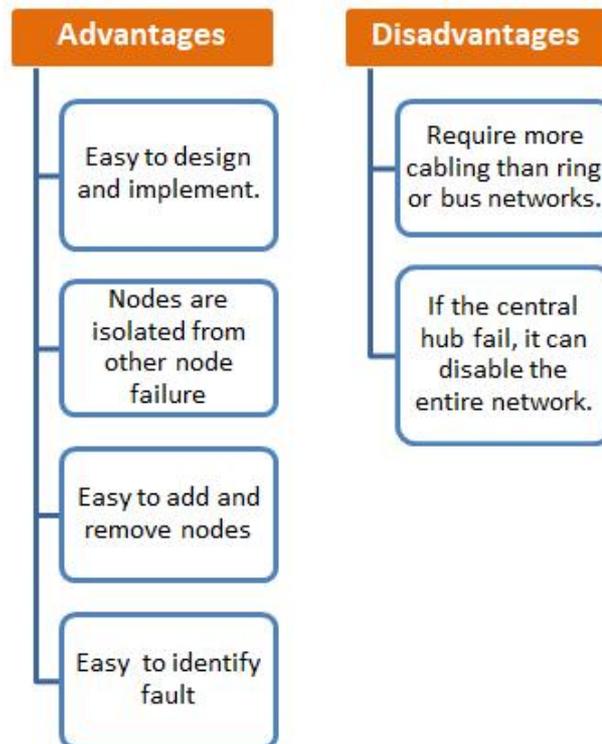


Figure 1.5(c) : Star topology connection

Advantages and Disadvantages Star Topology



Hybrid Topology

The combination of two or more topologies (Bus, Ring and Star). A hybrid topology is always produced when two different basic network topologies are connected.

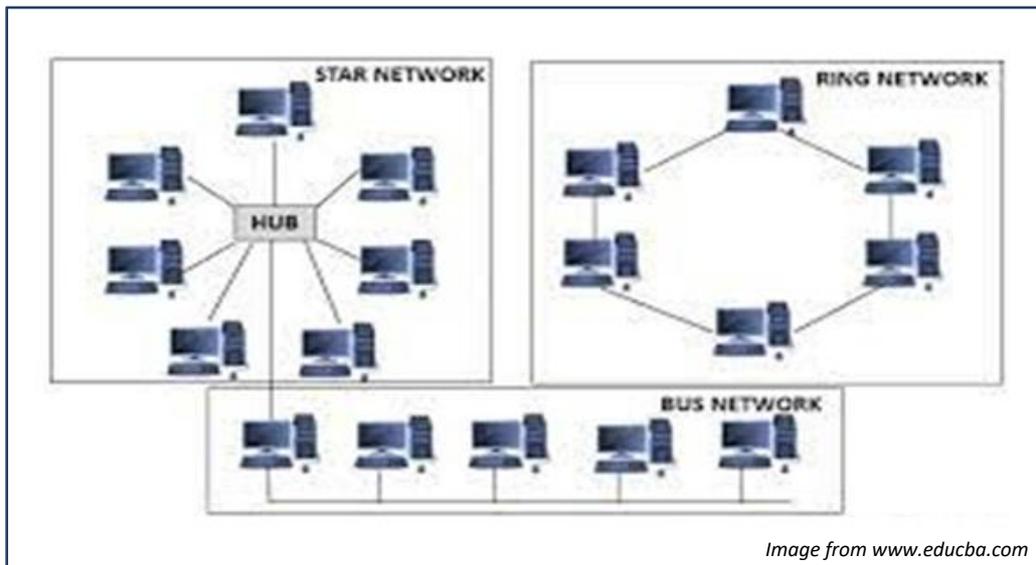


Figure 1.5(d) : Hybrid topology connection

Advantages and Disadvantages Hybrid Topology

Advantages

As hybrid networks are designed in a way that makes it simple to integrate new hardware components, it is easily scalable.

When two topologies are combined, topology's speed increases.

It is applied to build huge networks.

Disadvantages

The design is very complex.

Installation is a difficult process.

Fault finding is difficult if entire network shutdown

Networking Interface Card

A network interface card (NIC) is required for network connectivity on a computer. It is fitted inside a computer and gives it a dedicated network connection.

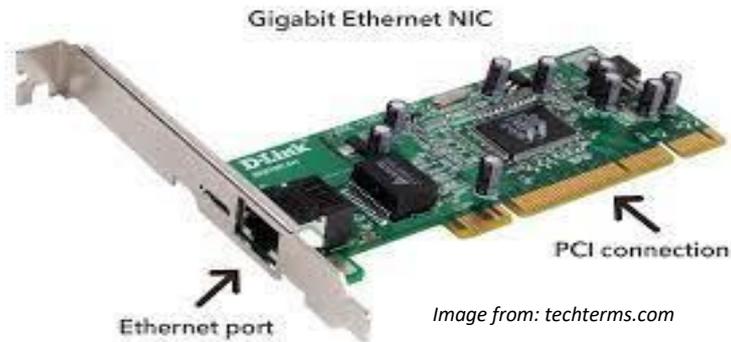


Figure 1.6(a) : Network Interface Card (NIC) for desktop computer

Repeater

Network repeater regenerate incoming electrical, wireless or optical signals. Data transmissions using media like Ethernet or Wi-Fi. Repeaters attempt to preserve signal integrity and extend the distance over which data can safely travel.

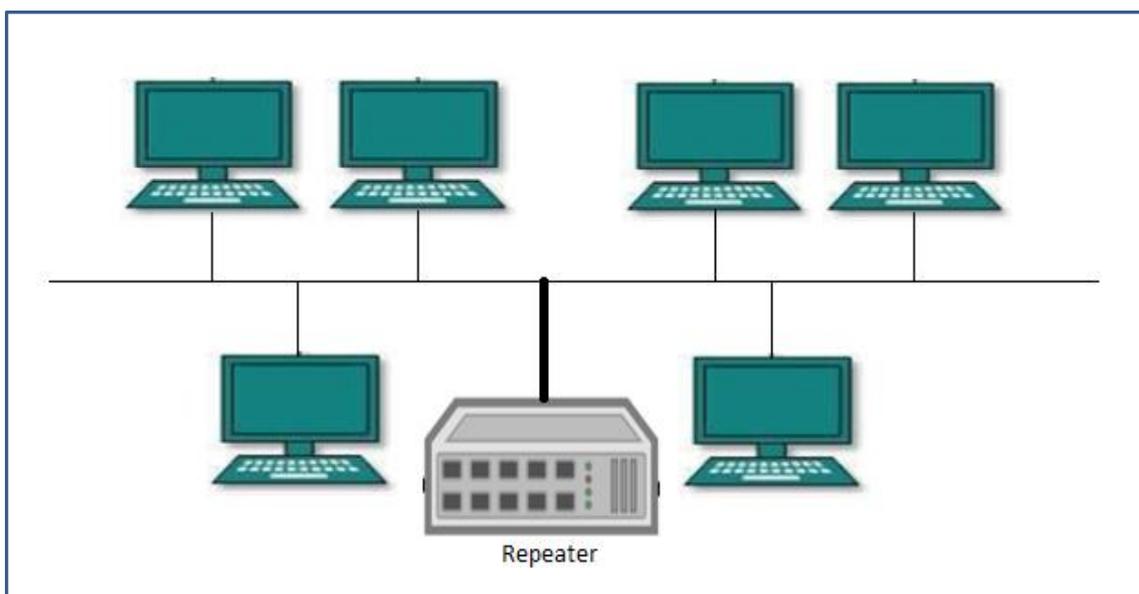


Figure 1.6(b) : Repeater in a workstation

Hub

Hub is the most basic networking tool for establishing a connection between multiple PCs or other network devices. A network hub, in contrast to a network switch or router, broadcasts all network data over each link and is devoid of routing tables and decision-making capabilities.



Figure 1.6(c) : Hub

Switch

Switch is a combination of hub and bridge technology. It offers a centralized location for workstation, server, and peripheral cable connections. The switch does not broadcast the data to all of its ports; rather, it exclusively transmits or forwards the data to the intended computer. The majority of switches operate as repeaters and are frequently employed in star or tree topologies.

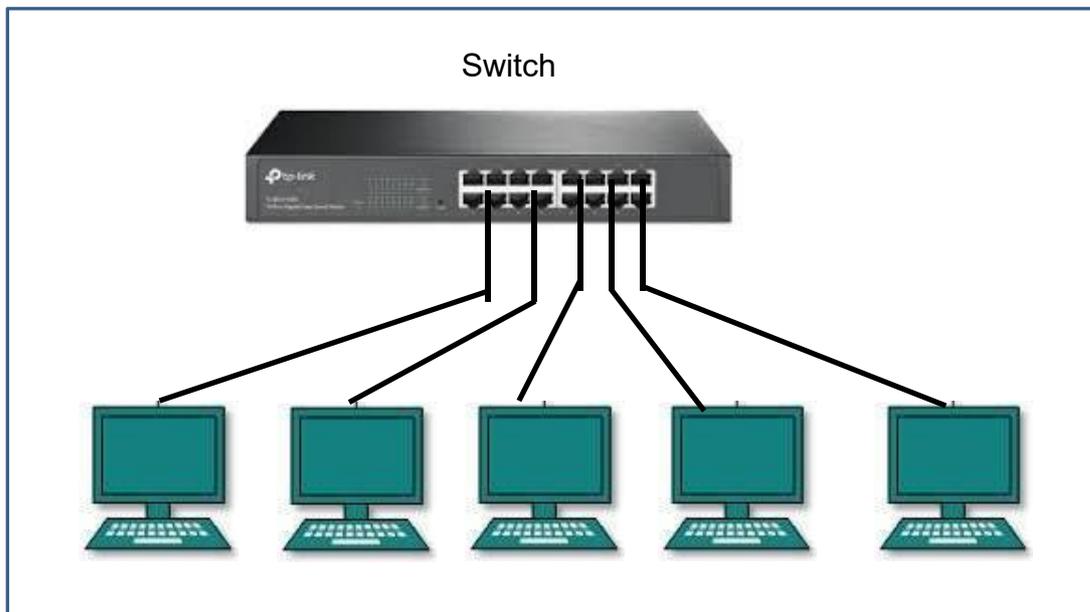


Figure 1.6(d) : Switch in a workstation

Bridge

A network bridge is a piece of hardware used in computer networking that joins together several communication networks or network segments into a single, comprehensive network.

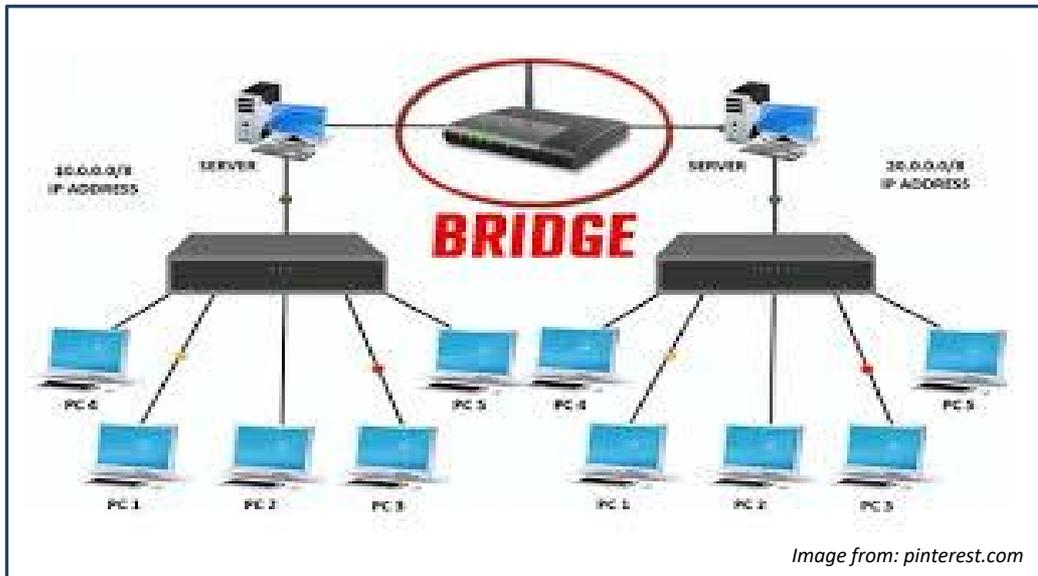


Figure 1.6(e) : Bridge in connection two groups of computer

Router

A router can connect one or more packet-switched networks or subnetworks. It controls traffic between several networks and enables multiple devices to share an Internet connection by transmitting data packets to their intended IP addresses.

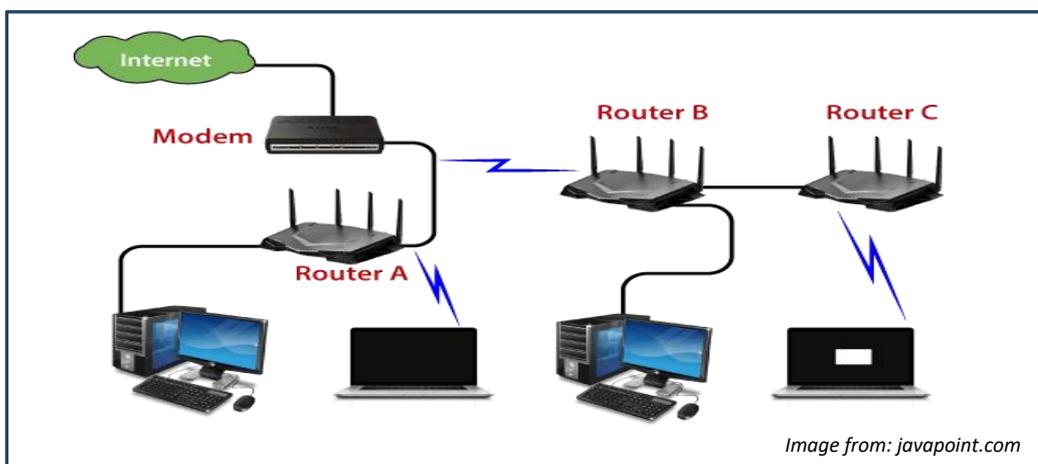


Figure 1.6(f) : Router in several group of users

Gateways

Using different transmission protocols, a gateway is a node in a telecommunications network that connects two networks. Because all data must pass through it or connect with it before being routed, a gateway serves as both the entry and departure points of a network. Without affecting the data itself, a gateway performs the task of converting data from one format to another.

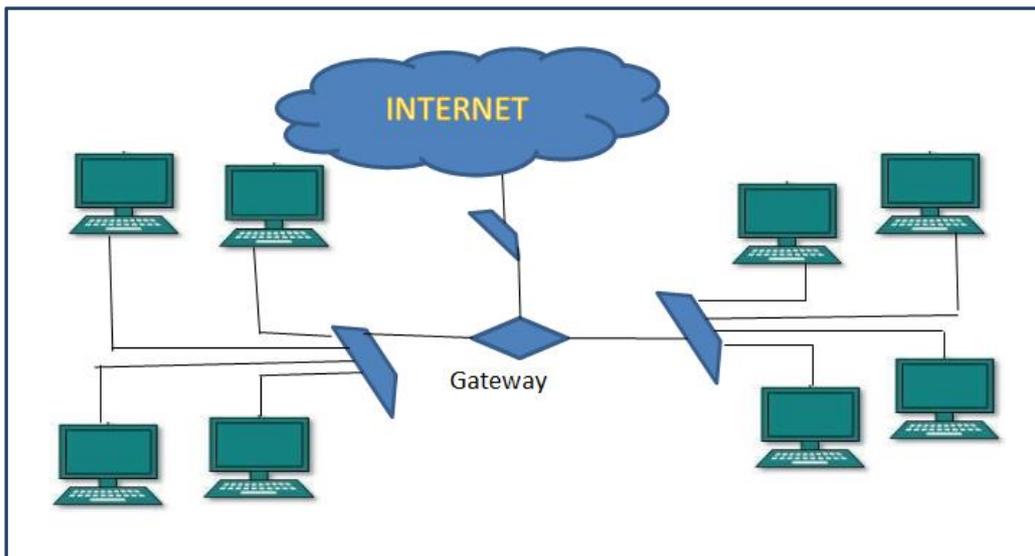


Figure 1.6(g) : Gateway in network connection

Install and Configure Network Interface Card (NIC)

1

Take the PC case off. When you do this, the power must be off.



Image from howtogeek.com

2

When working with a computer, make sure you are grounded to the device and wearing an antistatic wrist strap.



Image from wikihow.com

3

Before turning on the power, remove the strap.



Image from Insight.com

4

Next, insert the NIC card into a PCI slot by lining up the guidance notches with the PCI slot.



Image from hardwaretoexpert.blogspot.com

5

When the card is snugly seated in the PCI slot, gently press straight down.

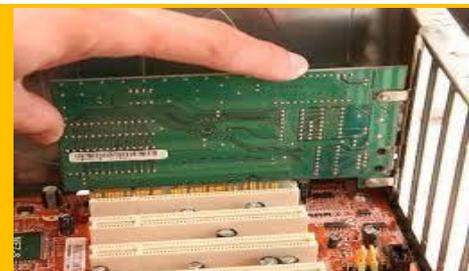


Image from theycybersecurityman.com

6

Use the same single screw that was used to fasten the card to the PC to secure it.

7

Verify the card to see if it has changed positions. If it happens, when the PC is turned on, it might harm itself..

8

Close the PC case and turn on the power.

9

Verify whether the internet is operational. If not, repeat the following procedures while checking the connections.

EXERCISE 1

Question 1

Network topology is the arrangement of the network, including the node and the way it connects. Interpret the advantages and disadvantages of bus topology, star topology and ring topology.

(7 marks)

Question 2

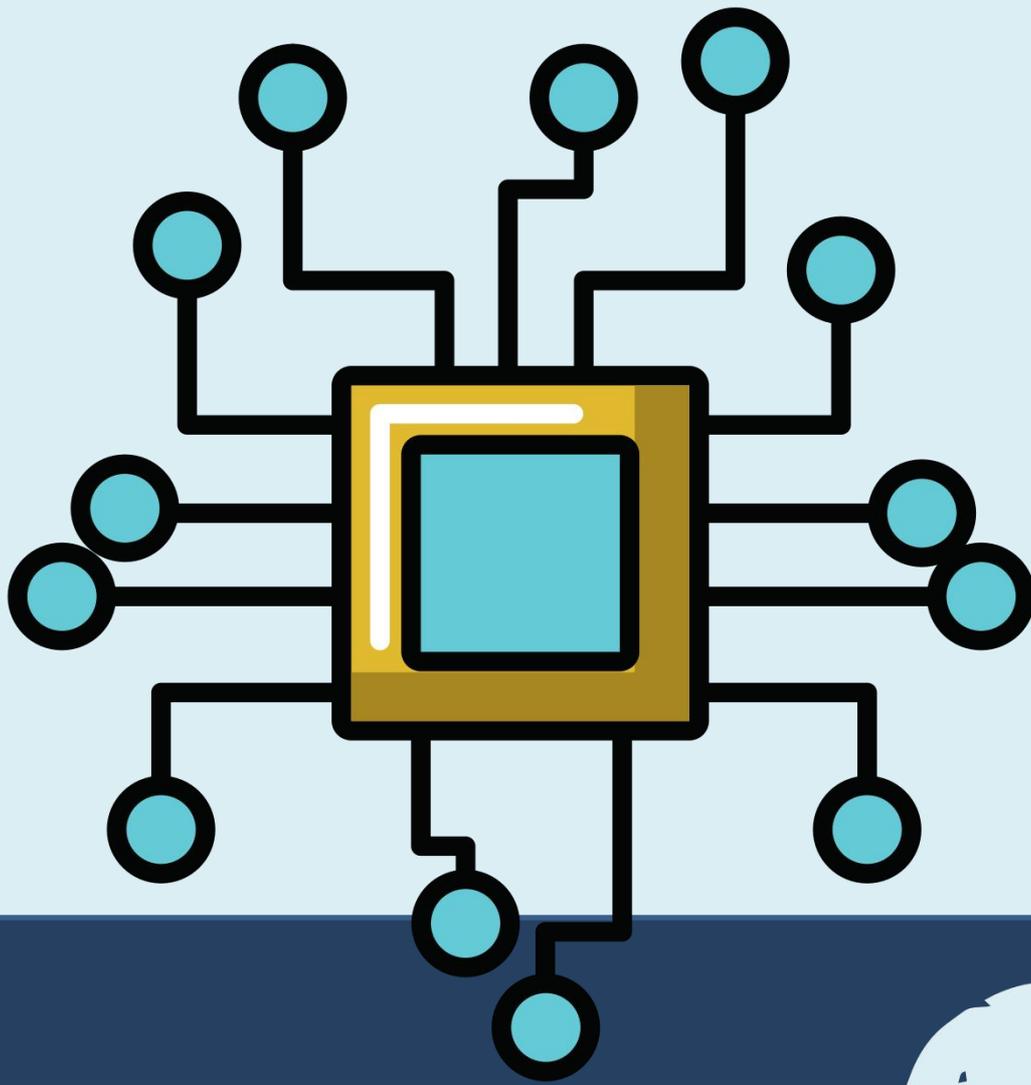
Client/Server and Peer-to-Peer networks are two fundamental types of networks. Differentiate between the types of networks by applying appropriate example or figure.

(7 marks)

Question 3

You undergo a practical training at ABC Company. ABC Company has a new project to build a network. This network project must consist of 9 computers with the minimum budget. As a practical student, you have been assigned with the project. Explain the type of network should you install?

(7 marks)



CHAPTER 2

Open Systems Interconnection (OSI) Model and Network Protocols

2.1

OSI MODEL

The OSI model is a logical and conceptual model, created in 1978 and revised in 1984 by the International Organization for Standardization (ISO). It describes network communication, a method of system communication and interconnection. It is a network architecture model which allows data to be transferred between computer systems.

The Important of OSI Model

- Helps in understanding the network communication.
- Divide the function into distinct network layers makes troubleshooting easy to implement.
- Helps in understanding new created technology.
- Enables primary functional relationships comparison across different network layers.

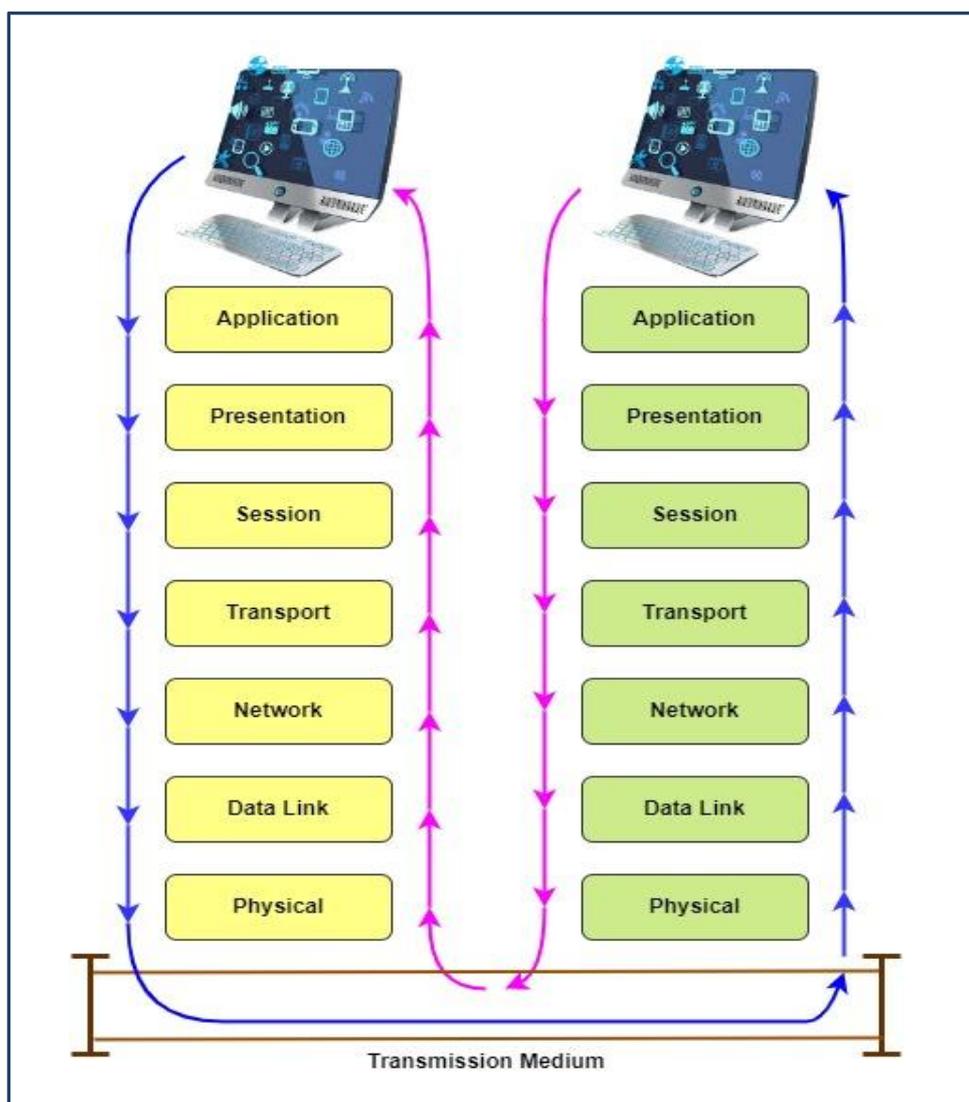


Figure 2.1 (a) : OSI Model layers

OSI Model Layer

Layer 1: Application (Network process to Application)

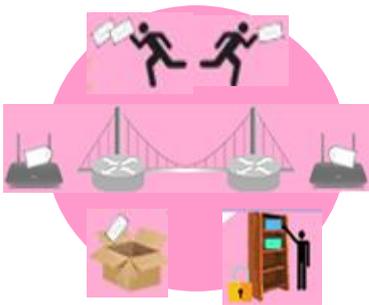


The application layer makes it easier for software applications and lower-layer network services to communicate. Software programmes like Netscape or Microsoft Word are not part of the layer.

Examples

Browser, Search Engines, Email Program etc. TCP/IP Protocol: Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Domain Name System (DNS) etc.

Layer 2: Presentation (Data representation and encryption)

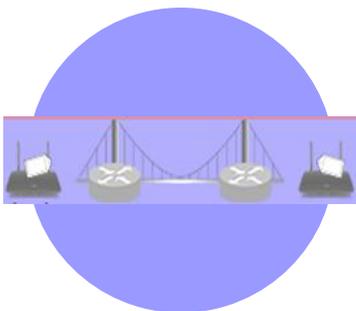


Data from the application layer is accepted by the presentation layer, which formats the data so that it is readable by a variety of hosts and applications. These layer protocols handle data encryption and decryption as well as coding and compression.

Examples

Text encoding methods ASCII and ANSI, compression methods like JPEG and MP3. TCP/IP Protocol: Secure Socket Layer (SSL), SSH, IMAP, FTP, MPEG, JPEG.

Layer 3: Session (Interhost communication)

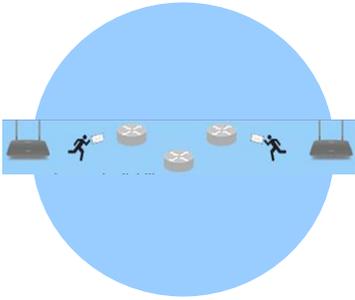


Two nodes' communications are arranged and maintained via the session layer. This layer manages all of the critical log-on or password validation, synchronise the dialogue between the two nodes, checks to see if communications have been interrupted, and if so, determines where to restart transmission and terminates communications.

Examples

Video and audio streams for a video session, Upload or download file session. TCP/IP Protocol: API's, Sockets, Winsock.

Layer 4: Transport (End-to-end connections and reliability)

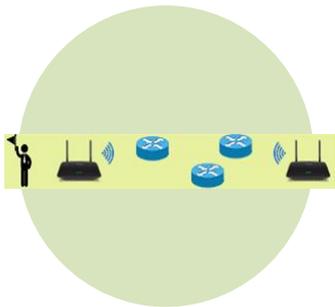


The Transport layer manages end-to-end delivery and accepts data from the Session layer. This layer makes ensuring that data is reliably, accurately, and error-free transported from point A to point B. Segments are used to divide up huge data units into several smaller ones.

TCP/IP Protocol

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Layer 3: Network (Path determination and logical addressing)

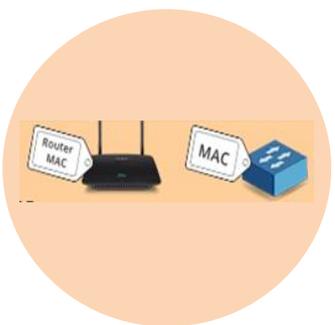


Network layer determines which physical path should be taken based on network conditions, priority of service, and other considerations, and gives the data with logical addressing. The data is organised into packets in this layer.

Examples

Router. TCP/IP Protocol: Internet Protocol (IP), Internet Protocol Security (IPsec), ICMP, IGMP etc.

Layer 2: Data Link (Physical addressing)

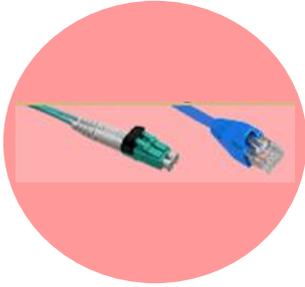


Data will be split up into frames by the data link layer so they may be transferred by the physical layer. Media Access Control (MAC) and Logical Link Control (LLC) are the two sublayers that make up the Data Link layer according to IEEE.

Examples

Switch and Bridge. TCP/IP Protocol: Ethernet, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), etc.

Layer 1: Physical (Media, Signal and binary transmission)



Frames from the Data Link layer are accepted by the Physical layer, which also produces signals as voltage changes at the transmission medium. Hubs and repeaters are devices that operate at the physical layer. Physical layer and Data Link layer operations are performed by network interface cards (NICs).

Example

Twisted pair, coaxial cable, optical fiber, wireless, or other transmission media, Hub and Repeater.

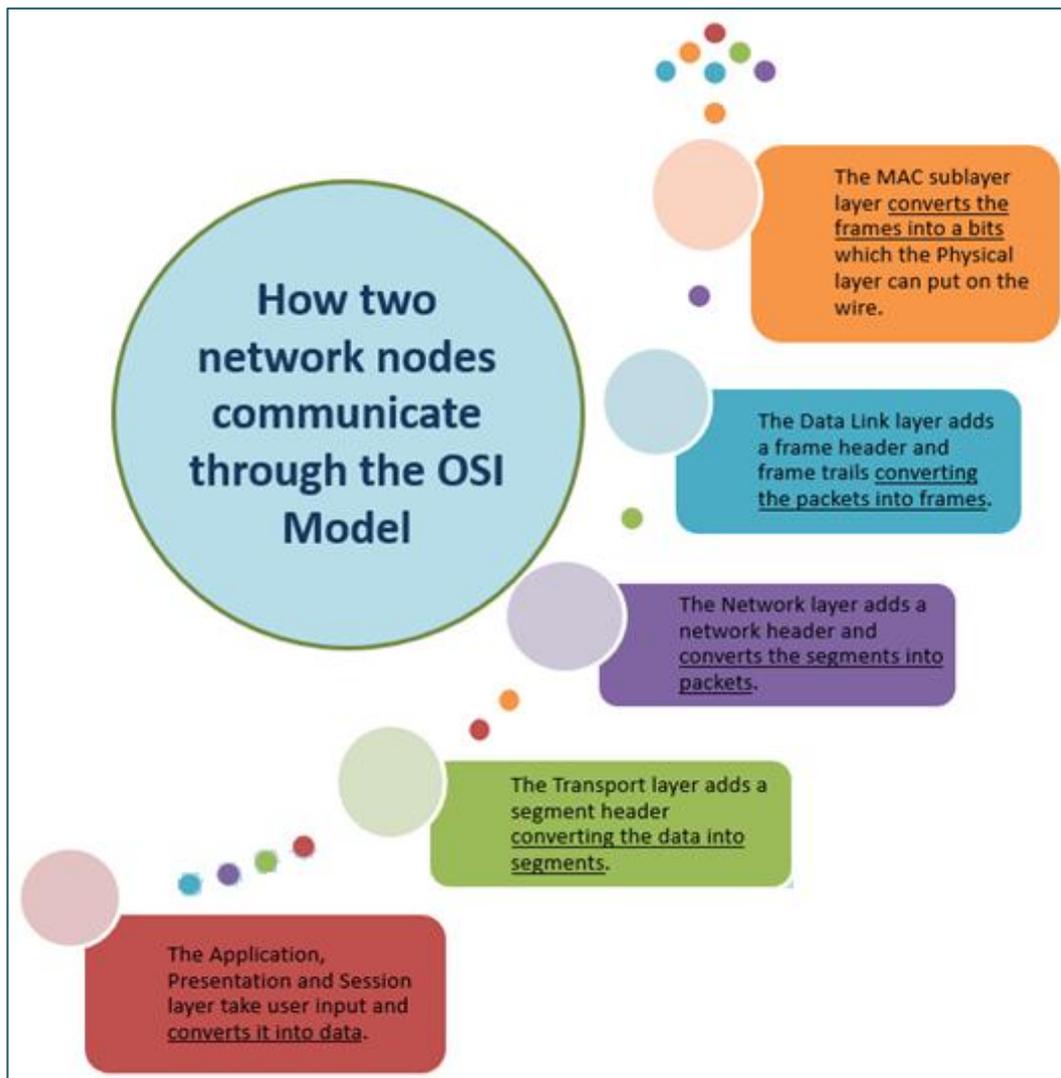


Figure 2.1 (b) : Two network nodes communicate through the OSI Model

Types of addressing covered by OSI Model

Media Access Control (MAC) address

Media Access Control (MAC) address is a hardware address that uniquely identifies each node of a network. Additionally known as a physical address. MAC addresses have a length of 6 bytes (48 bits), often represented by a string of 12 hexadecimal digits, such as 0C-0B-CD-34-54-A0. Valid hexadecimal characters are "0" to "9" and "A" to "F". Internet standards body assigns the manufacturer's ID number in the first three bytes. The manufacturer assigns the serial number in the second three bytes. MAC addresses are permanently engraved into hardware by hardware manufacturer.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\norhayatiam>ipconfig/all

Windows IP Configuration

Host Name . . . . . : Z1P8A0484
Primary Dns Suffix . . . . . : polipd.edu.my
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : polipd.edu.my

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : DC-21-48-55-2A-EE
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : DC-21-48-55-2A-EF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

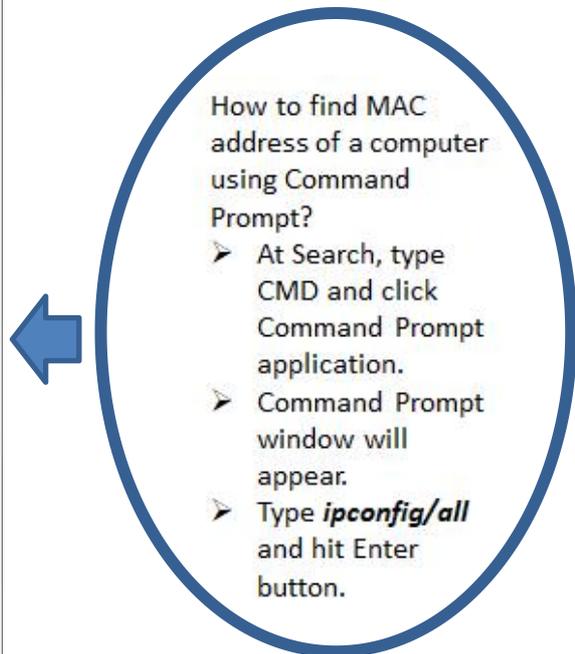
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : DE-21-48-55-2A-EE
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . : polipd.edu.my
Description . . . . . : Intel(R) Ethernet Connection (7) I219-LM
Physical Address. . . . . : 08-3A-88-6D-60-F9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::880a:5dd4:e23d:f307%7(Preferring)
IPv4 Address. . . . . : 10.20.39.176(Preferring)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, July 14, 2022 2:52:47 PM
Lease Expires . . . . . : Tuesday, August 9, 2022 3:26:07 PM
Default Gateway . . . . . : 10.20.39.1
DHCP Server . . . . . : 10.20.1.5
DHCPv6 IAID . . . . . : 134757000
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-95-03-7C-08-3A-88-6D-60-F9
DNS Servers . . . . . : 10.20.1.19
                        10.20.1.31
Primary WINS Server . . . . . : 8.8.8.8
Secondary WINS Server . . . . . : 10.20.1.31
                        10.20.1.19
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : DC-21-48-55-2A-F2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```



How to find MAC address of a computer using Command Prompt?

- At Search, type CMD and click Command Prompt application.
- Command Prompt window will appear.
- Type **ipconfig/all** and hit Enter button.

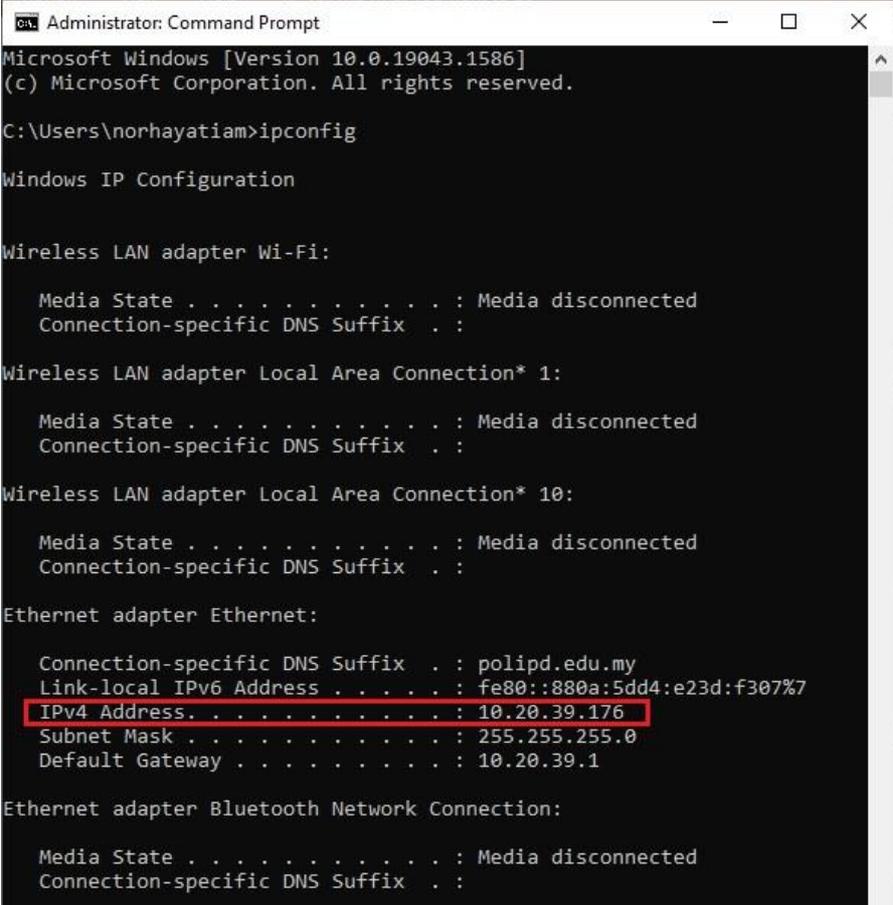
Figure 2.1 (c): To find MAC Address in a computer through Command Prompt

Internet Protocol (IP) address

Internet Protocol address (IP address) is the logical address of the network adapter device. The length of an IP address (IPv4) is 4 bytes (32 bits), and it specifies both the network address and the host address. Using "dotted decimal" notation, which separates each pair of four digits with a single dot (.). Each group represents an 8-bit number between (0-255). An example of IPv4 address is: 216.3.128.12 and 10.56.4.114. The network administrator assigns IP addresses to the network devices. In order to assign IP addresses to network devices, DHCP uses MAC addresses. The IP address is uniquely and identifies computers on a network.

How to find an IP address of a computer using Command Prompt?

- Open Command Prompt application
- Type *ipconfig* and press Enter



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\norhayatiam>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Ethernet adapter Ethernet:

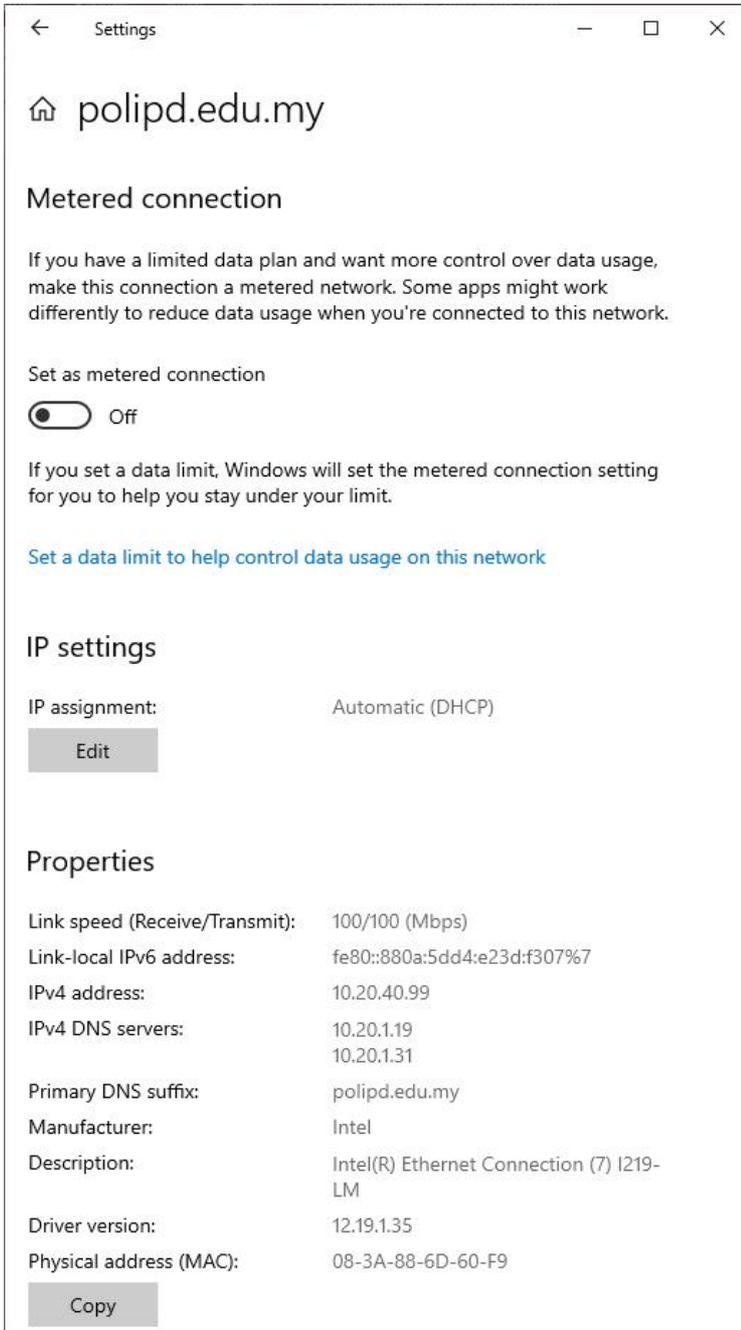
    Connection-specific DNS Suffix  . : polipd.edu.my
    Link-local IPv6 Address . . . . . : fe80::880a:5dd4:e23d:f307%7
    IPv4 Address. . . . . : 10.20.39.176
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.20.39.1

Ethernet adapter Bluetooth Network Connection:

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

Figure 2.1 (d): To find Logical Address in a computer through Command Prompt

Find MAC address and logical address of a computer using Windows function



How to find MAC Address and Logical Address of a computer using Windows function?

- Go to Start and click Setting
- Click Network & Internet
- Click Properties at network adapter available

Figure 2.1 (e) : To find MAC address and Logical address using Windows function

Ipv6 Addressing

In order to address the issue of IPv4 exhaustion, the Internet Engineering Task Force (IETF) developed Internet Protocol version 6 (IPv6). 3.4×10^{38} unique IP addresses are possible with IPv6, which has a 128-bit address and a substantially bigger address space than IPv4's 32 bits. Colon-Hexa representation is used for IPv6. There are 8 groups, each of which corresponds to 2 Bytes.

The vast address-space that carries addressing information to route packets for the next-generation Internet is one of IPv6's primary advantages over the previously utilised IPv4. Each and every device or node connected to the Internet can have a unique address thanks to IPv6's extensive address-space architecture.

2.2

INTERNET SERVICE PROVIDER (ISP)

An internet service provider (ISP) is a business or an organization that offers Internet access to its clients or members by facilitating data transmission between computers at clients' homes or places of business and computers connected to the Internet. These data transmissions typically use physical cable or wires in most populated areas. Wireless data transmission also the service which ISP offers to service clients who live or work in remote areas or who spend a lot of time on the road.

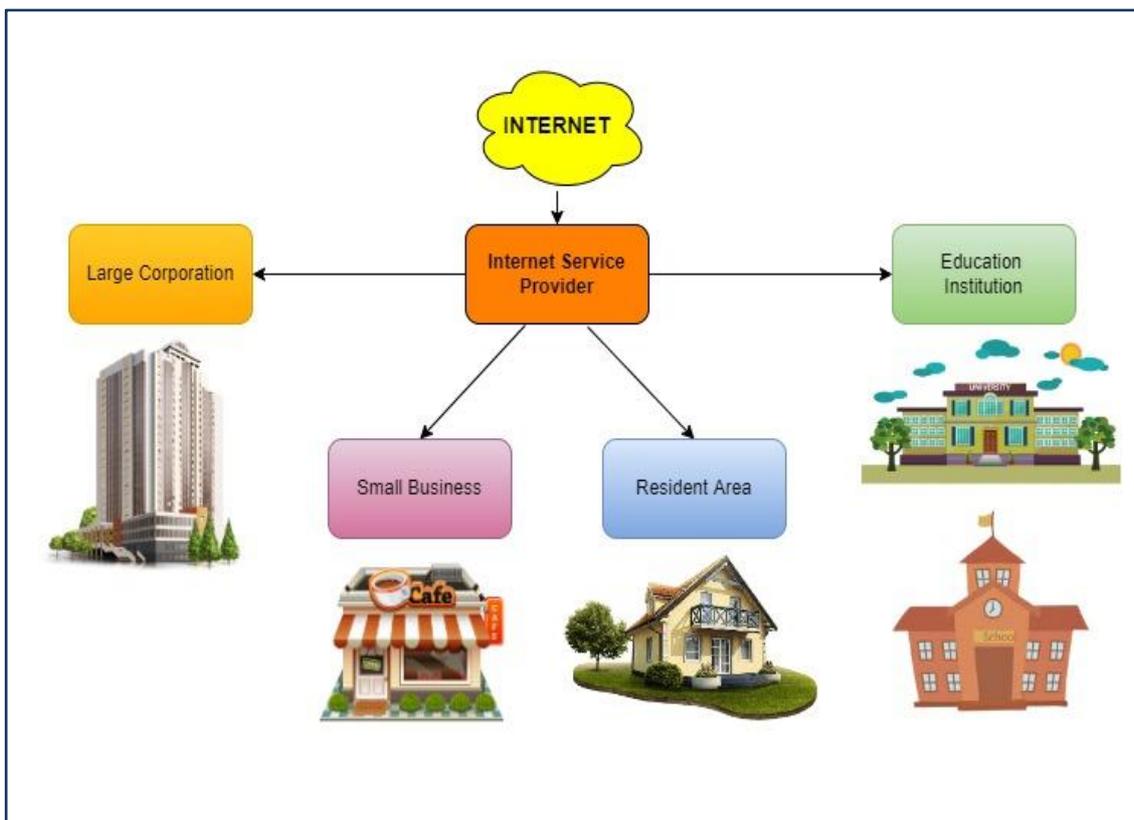


Figure 2.2 (a) : Connection between Internet, ISP and clients

Domain Name System is a naming system to assign name to host (host name) and domain. The host name and domain are given names via the Domain Name System (DNS). Typically, the name supplied describes the object or domain. A domain is a group of computers that typically belong to the same organization. Domain name is form by character string called labels separated by dots. The organisation in charge of domain name supervision is ICANN. Domain name use in internet must be registered with ICANN.

Computers connected to the internet can be identified and located using their domain names. Domain name represent in an unique form. The domain name of any two organisations cannot be the same. A domain name will always have two or more components, separated by dots ("."). "Subs domains" can be made within a domain name once it has been registered. Examples of the DNS are `www.polipd.edu.my`, `spmp.polipd.edu.my` and `mail.polipd.edu.my`.

Domain name is categorically divided into two levels,

E.g.: `www.google.com`

- `com`: top level domain (TLD)
- `google`: second level domain
- `www`: third level domain / subdomain

The second level domain can have multiple third level domain.

- E.g.: `maps.google.com`; `translate.google.com`; `play.google.com`



Figure 2.3 (a) : Domain Name System level

How DNS Work?

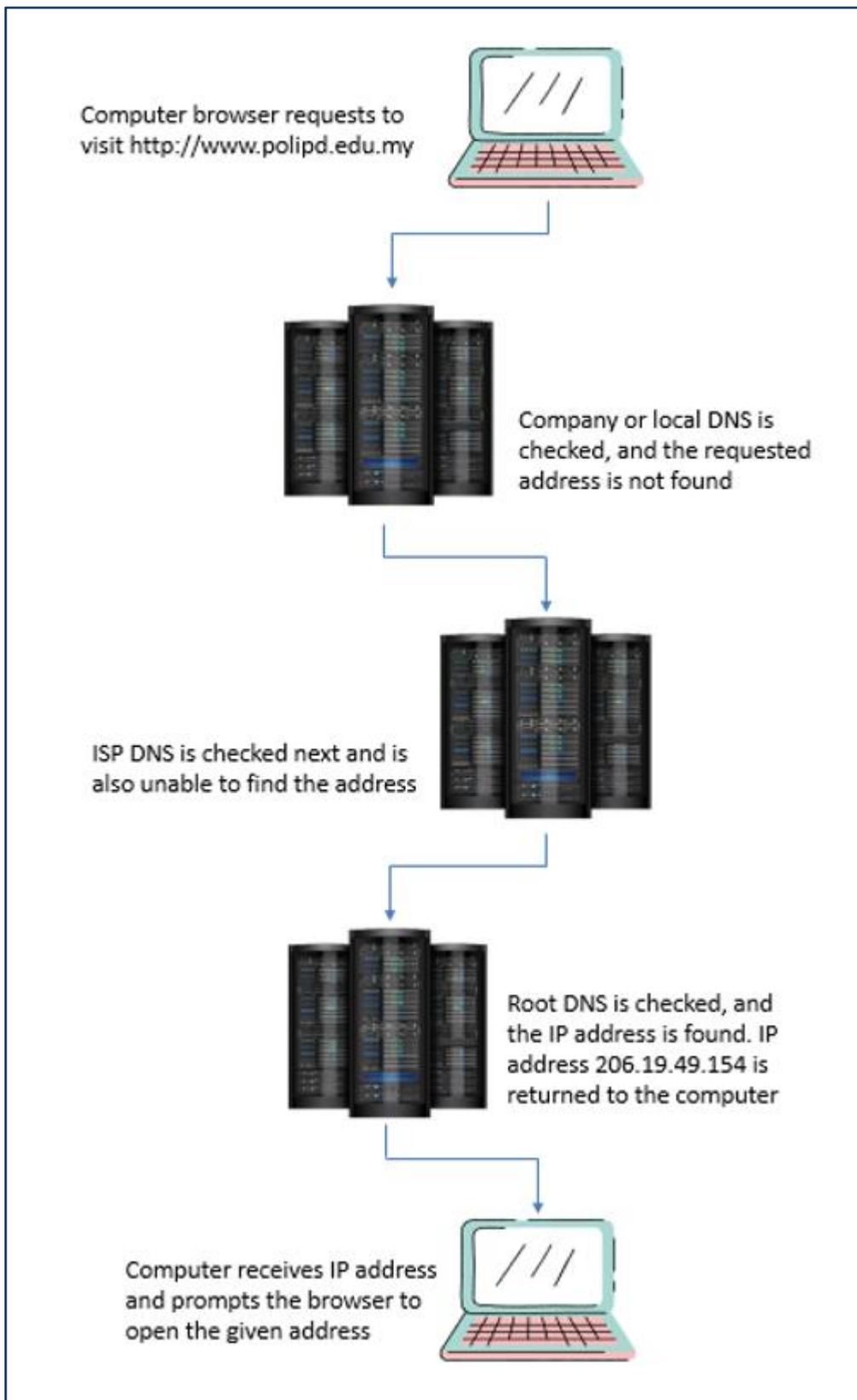
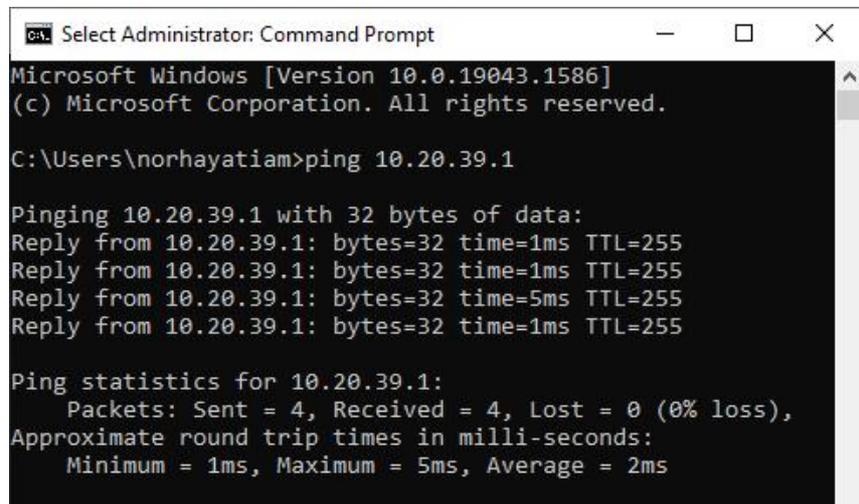


Figure 2.3 (b) : DNS work process

How to find the information on DNS through Command Prompt?

ping – can use to test for response from the host/site.

- Ping can use with IP address and also the host name.



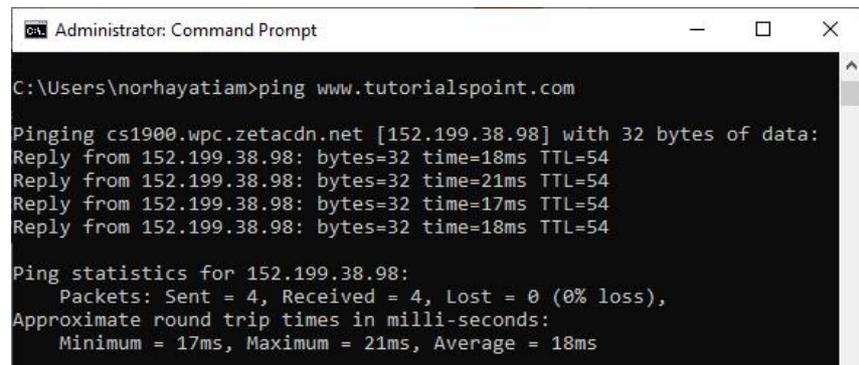
```
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\norhayatiam>ping 10.20.39.1

Pinging 10.20.39.1 with 32 bytes of data:
Reply from 10.20.39.1: bytes=32 time=1ms TTL=255
Reply from 10.20.39.1: bytes=32 time=1ms TTL=255
Reply from 10.20.39.1: bytes=32 time=5ms TTL=255
Reply from 10.20.39.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.20.39.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

Figure 2.3 (c) : Ping the host/site using IP address



```
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\norhayatiam>ping www.tutorialspoint.com

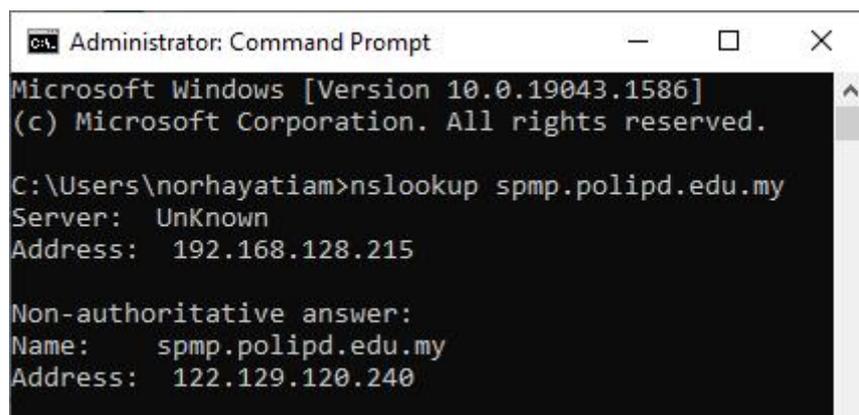
Pinging cs1900.wpc.zetacdn.net [152.199.38.98] with 32 bytes of data:
Reply from 152.199.38.98: bytes=32 time=18ms TTL=54
Reply from 152.199.38.98: bytes=32 time=21ms TTL=54
Reply from 152.199.38.98: bytes=32 time=17ms TTL=54
Reply from 152.199.38.98: bytes=32 time=18ms TTL=54

Ping statistics for 152.199.38.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 21ms, Average = 18ms
```

Figure 2.3 (d) : Ping the host/site using host name

nslookup – can use to determine,

- (i) the host name if the IP is known; or
- (ii) IP address if the host name is known.



```
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\norhayatiam>nslookup spmp.polipd.edu.my
Server: UnKnown
Address: 192.168.128.215

Non-authoritative answer:
Name: spmp.polipd.edu.my
Address: 122.129.120.240
```

Figure 2.3 (e) : *nslookup* command output

How Web Client and Web Server Communicate?

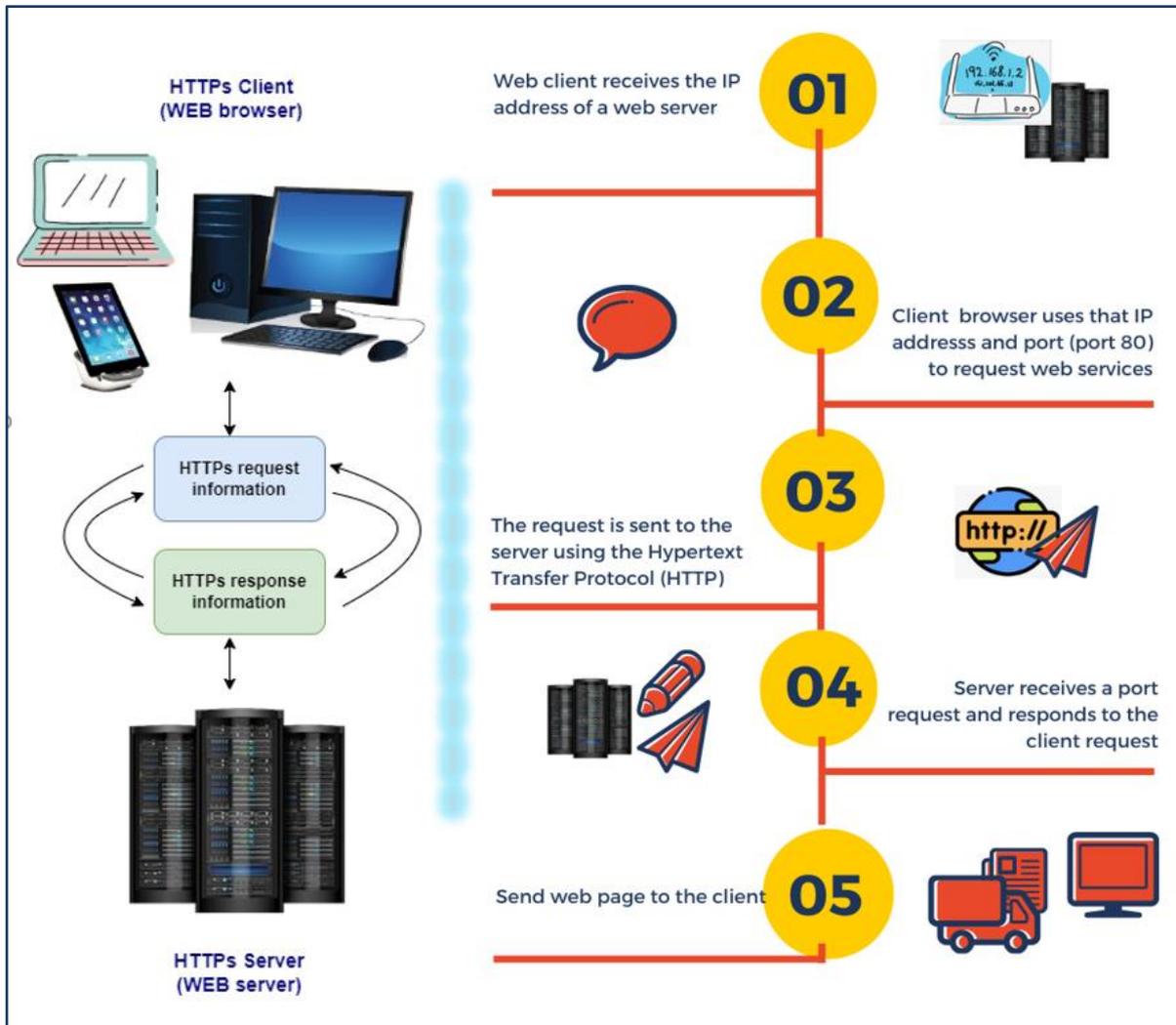


Figure 2.3(f) : Communication between Web Client and Web Server

Email is among the most widely used client/server applications online. Email servers communicate with clients and other email servers via the network using server software. Users whose mailboxes are set up on a mail server receive and store mail on that server. Each user who has a mailbox must then use an email client to visit the mail server and read these messages. Email is processed using the application protocols SMTP, POP3, and IMAP4.

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is the protocol used in sending the email from the client to the mail server. SMTP enables the exchange of email even sender and receiver in different email domains. The TCP port used is port 25.

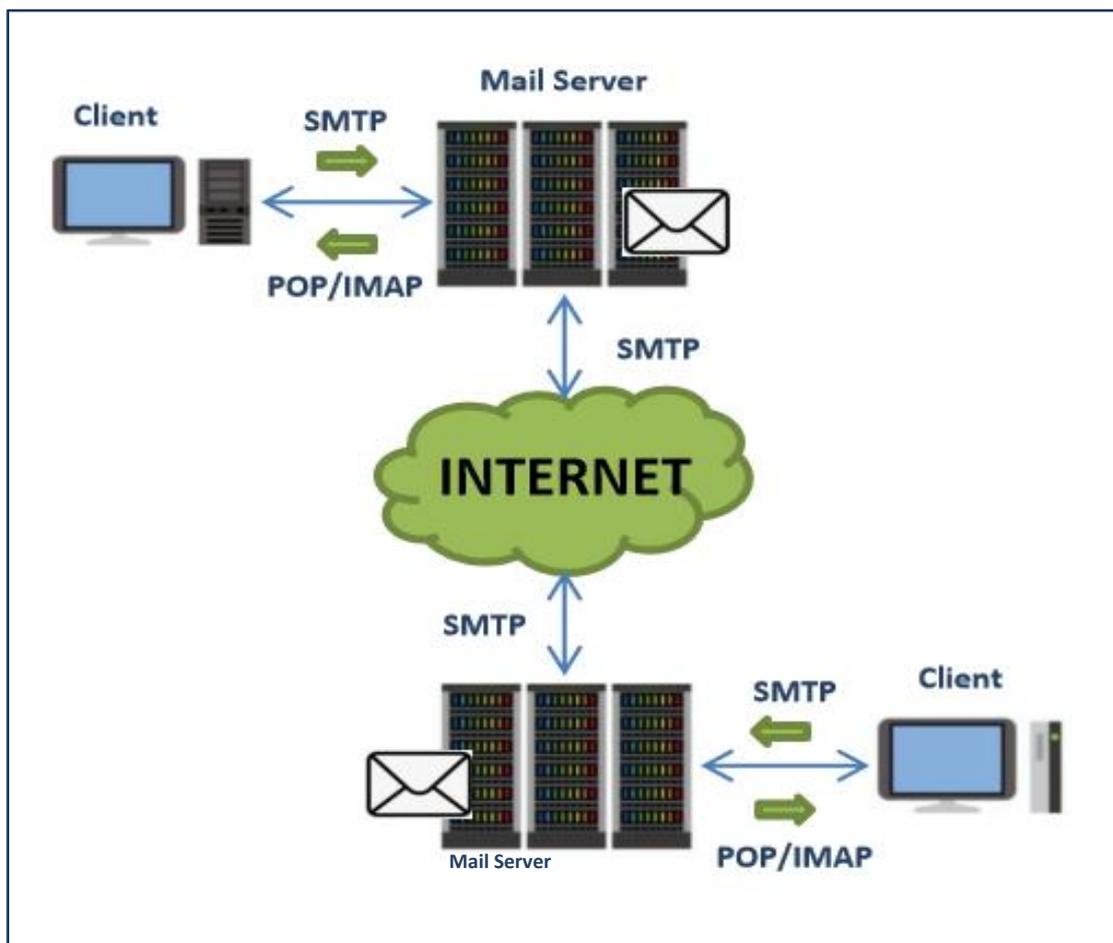


Figure 2.4 (a) : SMTP roles in email sending

Post Office Protocol (POP3)

Post Office Protocol (POP3) is the protocol used to retrieve mail from email servers. The email client accesses and manipulates (retrieves or deletes) the email from the server using POP3 commands including LIST, LOGIN, RETR, QUIT and DELE. POP3 uses port 110. After being downloaded to the local client using the POP3 protocol, the message is deleted from the server.

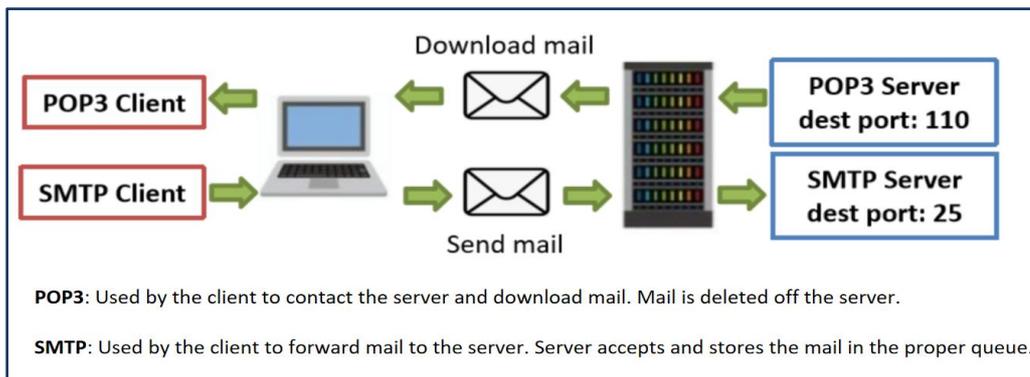


Figure 2.4 (b) : POP3/SMTP email client and server

Internet Message Access Protocol (IMAP4)

Internet Message Access Protocol (IMAP) is also retrieved from the email server. IMAP enables simultaneous read and retrieve the mail from many client devices. IMAP enables the user to access mail whenever they want, from any device. Using current trends, it is fairly typical to see users with more than one device to access emails (laptop, smartphone, etc.). The latest version of IMAP is 4 uses TCP port 143.

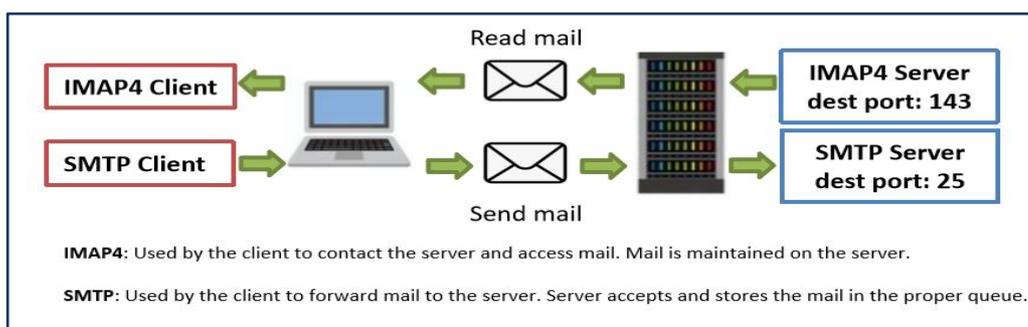


Figure 2.4 (c) : IMAP4/SMTP email client and server

Port Numbers

Port numbers are vary from 1 to 65,535 and its divided into three groups as below. Internet Corporation for Assigned Names and Numbers (ICANN) is responsible in assigned and managed the port numbers.

Well-known Ports

Well-known ports are destination ports that are associated with common network applications. (Range of 1 to 1023).

Registered ports

These ports can be used either source or destination ports. The Organizations can utilize these ports to register specific applications such as IM applications. (Range of 1024 to 49151).

Private ports

These ports are frequently used as source ports. Any application can use these ports. (Range of 49152 to 65535).

Table 2.4(a) : Port Number and description

Destination Port Number	Description
20	FTP Data (File Transfer Protocol – for data transfer)
21	FTP Control (File Transfer Protocol – to establish connection)
23	TELNET (TELEtype NETwork)
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name Service)
67	DHCP v4 Client (Dynamic Host Configuration Protocol - Client)
68	DHCP v4 Server (Dynamic Host Configuration Protocol - Server)
69	TFTP (Trivial File Transfer Protocol)
80	HTTP (Hypertext Transfer Protocol)
110	POP3 (Post Office Protocol (Version 3))
137	NBNS (Microsoft NetBIOS Name Service)
143	IMAP4 (Internet Message Access Protocol - Version 4)
161	SNMP (Simple Network Management Protocol)
443	HTTPS (Hypertext Transfer Protocol Secure)

2.5

TCP/IP ADDRESSING

A unique number used by machines (computers) to refer to each other when sending information via the Internet. Consists of 4-bytes addresses (w.x.y.z) to be assigned to each node in the network. Each IP address is divided into two parts, the **Network ID** and **Host ID**.

There are two ways to read the IP address, which is **binary** and **decimal**.

- Binary numbers are represented by numbers 0 and 1.
- Decimal numbers are represented by 0 to 9.

Table 2.5(a) : TCP/IP Addressing specifications

Class	A	B	C	D	E
1 st octet range (decimal)	1 – 127	128 - 191	192 - 223	224 - 239	240 - 255
1 st octet bits	0000 0000 – 0111 1111	1000 0000 – 1011 1111	1100 0000 – 1101 1111	1110 0000 – 1101 1111	1111 0000 – 1111 1111
Network (N) and Host (H) parts of address	N.H.H.H	N.N.H.H	N.N.N.H	Not for commercial use as a host	Not for commercial use as a host
Default subnet mask	255.0.0.0	255.255.0.0	255.255.255.0		
Numbers of possible networks and hosts per network	128 nets (2 ⁷) 16,777,215 hosts per net (2 ²⁴⁻²)	16,384 nets (2 ¹⁴) 65,534 hosts per net (2 ¹⁶⁻²)	2,097,152 nets (2 ²¹) 254 hosts per net (2 ⁸⁻²)		
Notes and host address range	Commercial 1.0.0.1 – 126.255.255.254	128.0.0.1 – 191.255.255.254	192.0.0.1 – 223.255.255.254	Multicast (reserved) 224.0.0.1 – 239.255.255.254	Experimental (reserved) 240.0.0.1 – 255.255.255.254

CLASS A

The first bit must be 0 refers to the eight bits in 1st Octet. So, the bits starting from 00000000 to 01111111. IP class A from 0 to 127 BUT the value 0 is the network number and can not be used and the value 127 is local loop back (used to perform tests on themselves, such as using the ping command on its own IP address), also can not be used. So IP class A from 1 to 126. E.g.: 1.10.134.8; 13.233.222.32.

CLASS B

2 initial bits is 10 (from right), referring to the eight bits in 1st Octet. So, the bits starting from 10000000 to 10111111. Class B IP address range starting from 128 to 191. E.g.: 155.76.76.8

CLASS C

3 initial bits is 110 (from right), referring to the eight bits in 1st Octet. So, the bits starting from 11000000 to 11011111. Class C IP address range starting from 192 to 223. E.g.: 200.56.17.8

CLASS D

4 initial bits is 1110 (from right), referring to the eight bits in 1st Octet. So, the bits starting from 11100000 to 11101111. Class D IP address range starting from 224 to 239. E.g.: 230.76.76.8

CLASS E

4 initial bits is 1111 (from right), referring to the eight bits in 1st Octet. So, the bits starting from 11110000 to 11111111. Class E IP address range starting from 240 to 255. E.g.: 243.76.76.8

Subnet Mask

Subnet is a calculation mechanism that used in the network system for breaking the network into classes of IP addresses. Subnet mask is designed for security purposes and distribution of working groups. It is used to distinguish the Network ID and Host ID. Default Subnet Mask for each class of IP address as below,

<p><u>Default Subnet Mask</u> IP Class A: 255.0.0.0 IP Class B: 255.255.0.0 IP Class C: 255.255.255.0</p>
--

Types of IP Addressing

Public IP Address

Public IP address are visible to the public. This address assigned to every computer that connects to the Internet. Public IP address assigned by Internet Service Provider (ISP) and the user have no control over it. Its also known as **Static IP Addresses**. Public IP addresses are reserved for the Internet.

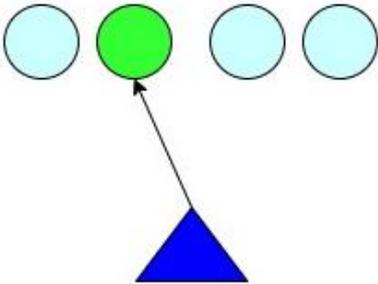
Private IP Address

Private IP address can be used on a private network. This type of IP address make our computer invisible to certain types of network attacks. The address not routable or valid on Internet. Its addresses are reserved for private networks. Range of private IP address for each class of IP address as below,

<p><u>Private IP addresses</u> Class A: 10.0.0.0 to 10.255.255.255 Class B: 172.16.0.0 to 172.31.255.255 Class C: 192.168.0.0 to 192.168.255.255</p>

Form of IP Addressing (support by IPv4)

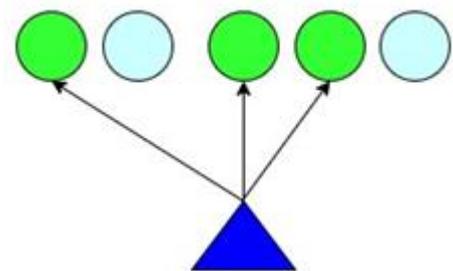
Unicast



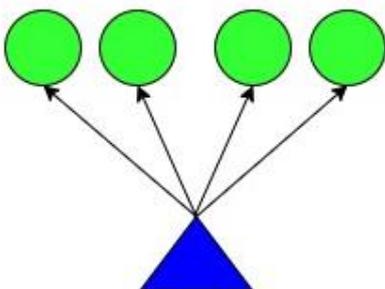
Assigned to a single network interface located on a specific subnet on the network and used for **one-to-one** communications. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient. Class A, B and C addresses.

Utilised for **one-to-many** communications and assigned to one or more network interfaces on different subnets of the network. The sender sends a single datagram (from the sender's unicast address) to the multicast address, and the intermediary routers take care of making copies and sending them to all receivers that have registered their interest in data from that sender. Class D addresses.

Multicast



Broadcast



Assigned to all network interfaces located on a subnet on the network and used for one-to-everyone-on-a-subnet communications. Permits the sender to send the data only once, and all receivers receive a copy of it.

Method of Addressing

Static (Manual)

IP address manually assigned to a device. Every time the computer connect to network, the IP addresses are the same. This method is manageable for small networks and need to check carefully to avoid IP conflict.

Dynamic (Automatic)

IP address automatically assigned by server when host boots. IP address derived automatically from a range of addresses. Each time you connect to the Internet, the addresses might be different.

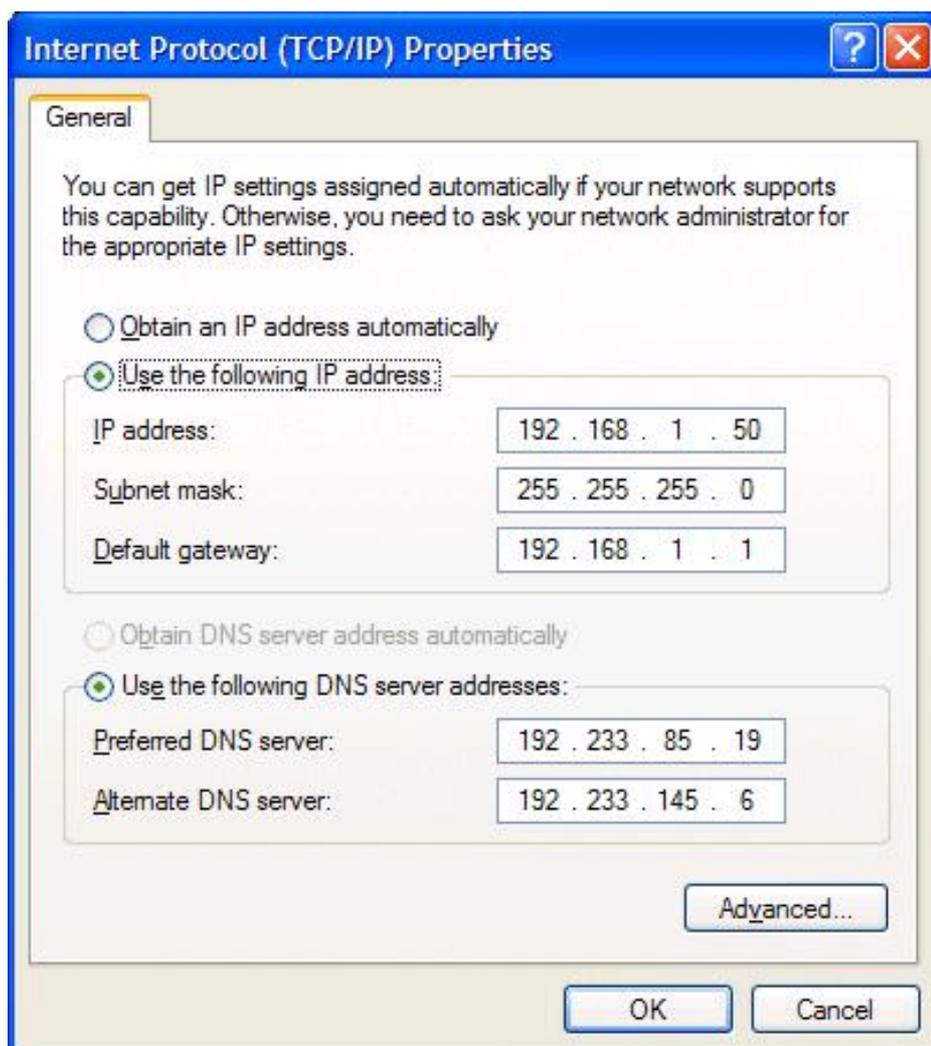


Figure 2.5 (a) : Manual IP address setting in Windows system

Configuration of DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol (DHCP) is automatically assigns device a unique IP address. Each device is given a unique IP address by DHCP automatically. DHCP is also responsible for assigning other network device characteristics, such as network mask, the IP address of one or more DNS servers, and the IP address of the default router. DHCP implementation is required in order to reduce the amount of effort and planning required for IP address management, eliminate IP address assignment mistakes, enable users to move workstations and printers, and make IP addressing accessible to mobile users.

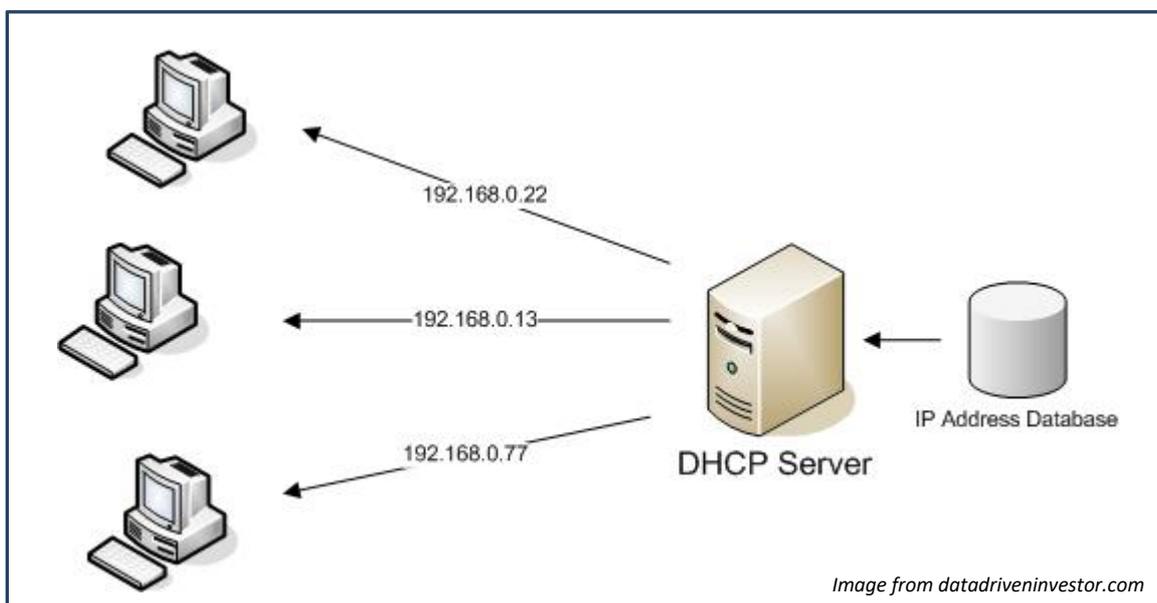


Figure 2.5 (b) : DHCP automatically assigned the IP address to the host

EXERCISE 2

Question 1

- a) Write the function for the following Open System Interconnection (OSI) layer:
- Data link layer
 - Presentation layer
- (3 marks)

- b) Explain what is the function of PING and what causes the PING command to not execute.
- (5 marks)

- c) Complete the table below by filling in the blanks with the appropriate type of IP class, default subnet mask, public or private address.
- (7 marks)

IP Address	Class Type	Default Subnet Mask	Public or Private Address
124.125.56.30	A	(i)	(ii)
172.16.0.1	(iii)	255.255.0.0	(iv)
221.225.78.65	(v)	(vi)	Public
192.168.1.1	(vii)	255.255.255.0	Private

Question 2

- a) Describe the Media Access Control (MAC) address?
- (3 marks)

- b) Complete the table below with the suitable answer.
- (5 marks)

Class	Range of 1 st Octet	Default Subnet Mask	Example of IP Address
(i)	(ii)	255.255.0.0	129.0.0.1
(iii)	(iv)	(v)	125.255.255.0

- c) Telekom Malaysia TM is one of the Internet Service Provider (ISP) in Malaysia. With the aid of diagram, explain how Telekom Malaysia TM supplied the internet to the customer.
- (7 marks)

EXERCISE 2

Question 3

a) A protocol is necessary in computer networks to allow access to all users. List **THREE** (3) Network Layer Protocol.

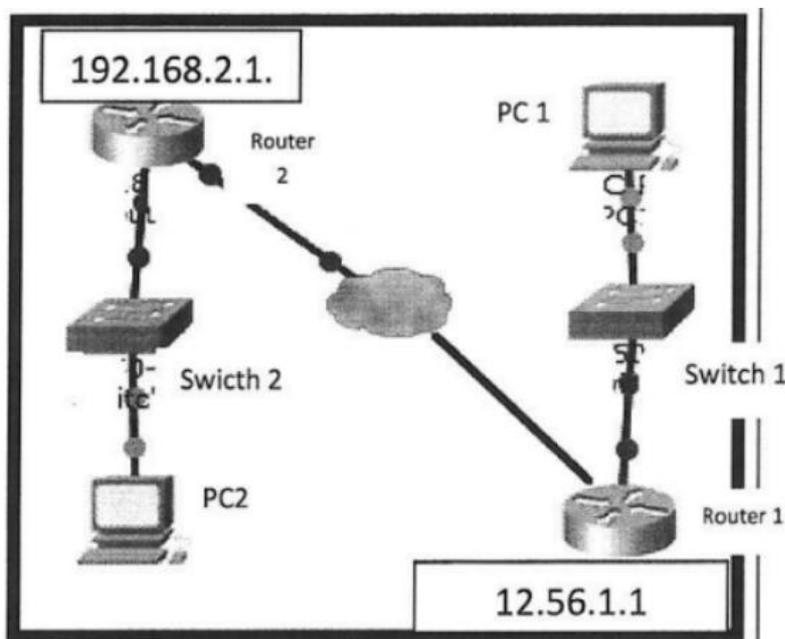
(3 marks)

b) Interpret the form of addressing for Unicast, Broadcast and Multicast.

(5 marks)

c) Refer to the figure below, complete the table below with the suitable answers.

(7 marks)



Hardware	Class of IP	IP Address	Subnet Mask
PC 1	(i)	(ii)	(iii)
PC 2	(iv)	(v)	(vi)
Router 1	-	12.56.1.1	(vii)



ANSWER

Exercise 1

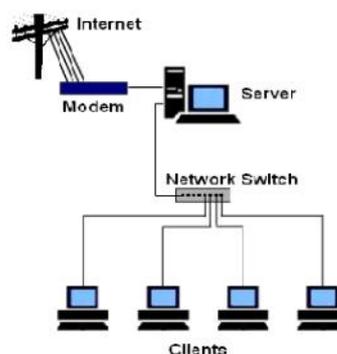
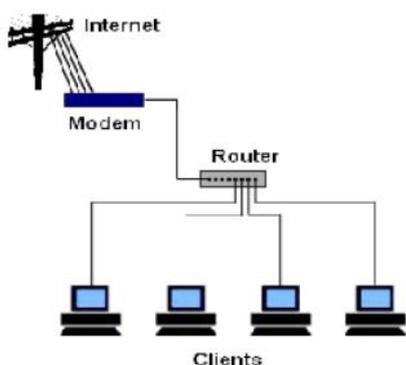
Question 1

	Advantages	Disadvantages
Bus	Easy to install because less cabling are used.	Fault or break in the bus cable stops all transmission.
Star	Easy to install and reconfigure because each devices is linked only to its immediate neighbours.	Break in the ring can disable the entire network.
Ring	Easy to design and implement. One malfunctioning node doesn't affect the rest of the network because the nodes are isolated from other node failure.	Each node must be linked to a central device, so require more cabling than ring or bus networks. Break in the central device can disable the entire network.

Question 2

Setup arrangement :

Peer-to-Peer Network	Client/Server Network
- In a peer-to-peer setup, not require a server and every computer acts as both the client and the server. - Common used in the home because the small group of clients.	- In a client-server setup, multiple clients (computers) connect to a single, central server. - Typical used in larger offices or businesses which consist big group of clients.



Question 3

Network install: Peer-to-Peer Networks.

Explanation:

- No need server: Peer-to-Peer is a network in which resources and files are shared without a centralized management source. There are no dedicated servers or hierarchy among the computers. All of the computers are equal and therefore known as peers.

- Less expensive: No server needed and the devices are only the router (one or more), ethernet cable and 9 computers which are the basic device of network.

- System requirements: The total of client are depend on type of Operating System. Microsoft imposes a limit of only 5, 10 or 20 concurrent client connections to computers running Windows.

Exercise 2

Question 1

1(a) :

- i. Data link layer
 - to divide data into distinct frames that can then be transmitted by the Physical layer.
- ii. Presentation layer
 - serve as a translator and are the standards which are involved in multimedia.

1(b) :

Function of PING :

- a diagnostic tool that allows a user to verify that a particular IP address exists and can accept requests.

Causes PING command to not execute:

- computer cannot recognize the IP address that you are trying to ping.
- the host that we are trying to ping is down or is not operating on the network.
- network adapter is disabled or the Ethernet cable was unplugged.

1(c)

IP Address	Class Type	Default Subnet Mask	Public or Private Address
124.125.56.30	A	255.0.0.0	Public
172.16.0.1	B	255.255.0.0	Private
221.225.78.65	C	255.255.255.0	Public
192.168.1.1	C	255.255.255.0	Private

Question 2

2(a) :

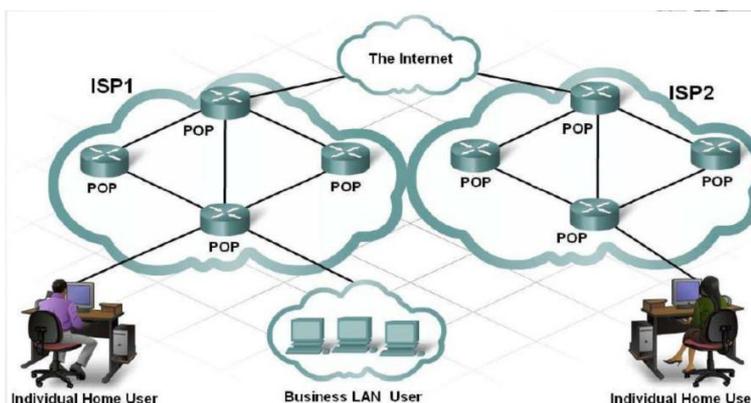
- is a hardware address that uniquely identifies each node of a network.
- the address length is 6 bytes (48-bits).
- MAC addresses are permanently burned into hardware by hardware manufacturer.

2(b) :

Class	Range of 1 st Octet	Default Subnet Mask	Example of IP Address
B	128 - 191	255.255.0.0	129.0.0.1
A	1 - 126	255.0.0.0	125.255.255.0

2(c) :

- An ISP supplies internet connectivity to customers through Point of Presence (POP).
- A POP is the connection point between the ISP's network and the particular geographical region that the POP is servicing.
- The Internet is made up of very high-speed data links that interconnect ISP POPs and ISPs to each other.
- These interconnections are part of the very large, high capacity network known as the Internet Backbone.



Exercise 2

Question 3

3(a) :

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

3(b)

Unicast :

- Assigned to a single network interface located on a specific subnet on the network and used for one-to-one communications.
- Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient.

Broadcast :

- Assigned to one or more network interfaces located on various subnets on the network and used for one-to-many communications.
- The sender sends a single datagram (from the sender's unicast address) to the multicast address, and the intermediary routers take care of making copies and sending them to all receivers that have registered their interest in data from that sender.

Multicasts:

- Assigned to all network interfaces located on a subnet on the network and used for one-to-everyone-on-a-subnet communications.
- Permits the sender to send the data only once, and all receivers receive a copy of it.

3(c) :

Hardware	Class of IP	IP Address	Subnet Mask
PC 1	A	12.56.1.2	255.0.0.0
PC 2	C	192.168.2.2	255.255.255.0
Router 1	-	12.56.1.1	255.0.0.0



REFERENCE

REFERENCE

Cisco System. (2005). *CCNA 1 and 2 Companion Guide, Revised (Cisco Networking Academy Program)*. 3rd Edition. Cisco Press

Dean, T. (2015). *Network+ Guide To Networks*. 7th Edition. Cengage Learning

H. Yamauchi, A. Nakao, M. Oguchi, S. Yamamoto and S. Yamaguchi, "Service Identification Based on SNI Analysis," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2020, pp. 1-6, doi: 10.1109/CCNC46108.2020.9045315.

Keogh, Jim. *Need-to-Know Technologies for a Successful Future*, Berlin, Boston: De|G Press, 2018.
<https://doi.org/10.1515/9781547400812>

Lammle, T. (2011). *CCNA Cisco Certified Network Associate Study Guide*. 7th Edition. Wiley Publishing.

Odom,W. & Knott, T. (2006). *Networking Basics CCNA Companion Guide(Cisco Networking Academy)*.Cisco Press.

P. Clark, M. (2003, May). *Data Networks, IP and the Internet: Protocols, Design and Operation*. Wiley.

Tanenbaum, A.S (2011). *Computer Networks*.5th Edition. Prentice Hall

<https://www.canva.com>

Computer Network | Definition & Types. (n.d.). Encyclopedia Britannica.
<https://www.britannica.com/technology/computer-network>

Education, I. C. (2021, March 30). *Networking*. <https://www.ibm.com/cloud/learn/networking-a-complete-guide>

Fundamentals of Computer Networking - javatpoint. (n.d.). www.javatpoint.com.
[https://www.javatpoint.com/fundamentals-of-computer-networking#:~:text=The%20Computer%20networks%20are%20formed,Bluetooth%2C%20Wi%2D-Fi\).](https://www.javatpoint.com/fundamentals-of-computer-networking#:~:text=The%20Computer%20networks%20are%20formed,Bluetooth%2C%20Wi%2D-Fi).)

REFERENCE

GeeksforGeeks. (2020, August 5). *Basics of Computer Networking*. <https://www.geeksforgeeks.org/basics-computer-networking/>

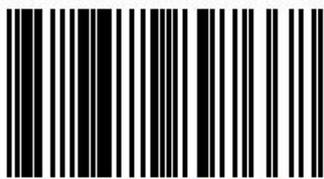
Mohanakrishnan, R. (2022, February 10). *What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices*. Spiceworks. <https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/>

What is Computer Networking? - Beginner's Guide to IT Networking - AWS. (n.d.). Amazon Web Services, Inc. <https://aws.amazon.com/what-is/computer-networking/>



THE END

e ISBN 978-967-2897-66-8



9 7 8 9 6 7 2 8 9 7 6 6 8

COMPUTER NETWORKING
FUNDAMENTALS