Ethical, Social and Economic Issues in Computing

Data Corruption

Data corruption occurs when computer data is made unstable by errors or alterations. This can happen during the reading, writing or transmission of data.

If the corrupted data cannot be recovered / replaced, this results in **data loss**.

Effects of Corruption and Data Loss

The effects vary depending on the amount of corrupted data and type of data that is represented.

If the corrupted data is not needed to read other data, only that data itself is lost. This is more likely if the amount of corrupted data is small.

However, if the corrupted data is related to other data in the computer, then both itself and its related data may be lost, as it may contain information required to read/interpret the related data. This is more likely if the amount of corrupted data is large.

Causes and Ways to Prevent Data Corruption and Loss

In all cases, making regular **backups** (copies of data made in case the original data is damaged or lost) of data will help to prevent the loss of data.

Causes of data corruption and loss include:

- **Human Error**
    - Storage devices may be damaged during transport.
    - Multiple users working on the same file may accidentally overwrite each other.
    - **Preventive Measures**
        - Make regular backups of data
        - Use adequate protection when transporting storage devices.
        - Set up rules when collaborating with multiple users to prevent them from writing to the same file at the same time.
- **Power Failure**
    - If the power supply to a computer fails, data in the process of being written to a storage device may become corrupted and data stored in volatile memory and not yet written to a storage device will become lost.
    - **Preventive Measures**
        - Regular backups
        - Set up a backup power supply, or **uninterruptible power supply (UPS)** so storage devices can complete any write operations in case of a power failure.
- **Hardware Failure/Damage**
    - All magnetic, optical and solid-state storage devices can fail, either due to

overuse, manufacturing defects, or age.
    - **Preventive Measures**
        - Regular backups
        - Check storage device regularly and replace them immediately when signs of failure are detected.
- **Malware/viruses**
    - Some malware may purposely damage and corrupt data as a way of attacking the computer
    - **Preventive Measures**
        - Regular backups
        - Avoid opening emails/attachments or files from unknown sources.
        - Install and configure a firewall to prevent malware from spreading through the network.
        - Install anti-virus and anti-spyware software and perform regular scans and updates

An **uninterruptible power supply** is a device that provides enough emergency power for a computer to properly shut down in the event of a power failure.

Authentication

Authentication is the process of verifying the identity of a user. It requires the user to prove their identity by providing evidence from one or more of the following categories:

- Something the user knows (password)
- Something the user owns (mobile phone)
- Something physically unique about the user (thumbprint)

Each category of evidence used for authentication is called an **authentication factor**

Passwords

Passwords are the most common form of authentication. Some passwords are entered together with a username that identifies who the user claims to be.

They can be a poor form of authentication if they are chosen poorly or not well-kept as a secret. Avoid using birthdates, surnames and other things that can be easily guessed.

Use hard to guess passwords that are a mixture of lowercase, uppercase letters, numbers and symbols.

Avoid re-using passwords or leaving them unchanged for a long time as it makes it easier for an intruder to guess the password. Use unique passwords for each computer and account, and update them at least once every 90 days.

Unauthorised Access

Some authentication systems require evidence from more than 1 authentication factor. Banks typically issue a device called a security token to users who wish to access their accounts online.

A **security token** is a device used specifically for authentication purposes, such as mobile

phones and one-time passwords (OTPs).

The type of authentication that uses evidence from both something a user knows and owns is called **2-factor authentication**.

2FA is stronger than a singular password as it is more difficult for an intruder to both guess a password and steal the user's security token. Hence, it is important to keep the security token in a secure location at all times and to report a missing security token as soon as possible.

If an OTP is sent wirelessly to a user's mobile phone, it may be intercepted and used by an intruder during the transmission process. If the secret algorithm used to generate OTPs is poorly chosen or accidentally revealed, an intruder may find out how to generate OTPs without needing the security token at all.

There is not much a user can do about this type of intrusion attempt.

Biometrics

Biometrics is a type of authentication that is based on the measurement of human physical characteristics.

For example, biometrics is used to identify a user by fingerprint or voice. Other characteristics used include the face, iris, retina, and DNA.

The use of biometric identification is more secure as the physical characteristics measured are typically unique to the individual and cannot be easily replicated. Thus, it helps prevent attempts to establish fraudulent identities and **identity theft**.

Identity theft is the impersonation of another person to steal personal details such as name and identity number for fraudulent purposes.

Authorisation

Once the user is authenticated, the ability of a computer to control the access of data and resources by that user is called **access control/authorisation**.

Computers provide access control through a variety of means.

File Permissions

Most operating systems have settings to control the ability of users to view or make changes to specific files or folders. These settings are called **permissions**.

An application of file permissions is when a teacher may set a presentation file to be read-only for students, so they do not accidentally (or intentionally) change its contents.

Typically, users can only change the permissions for any file or folder they own. However, most OS's allow for a special user called the **administrator**, who can override the permissions for almost any file or folder.

A normal user may also be given special **administrator rights** that allow them to override the permissions for certain files or folders, just like an administrator.

Managing permissions and administrative rights can be a complex task, and it is possible to accidentally grant access to a file or administrative rights to an unauthorised user. Such a user can then make use of such mistakes to gain unauthorised access to data and resources.

Authentication for the administrator must be especially strong, as an intruder that successfully claims to be an administrator can bypass file permissions entirely.

File permissions do not prevent an intruder with physical access to a storage device from accessing files or folders directly without going through the operating system. To prevent such access, it is necessary to use encryption.

File permissions can be used as access control for both computers connected to a network and computers that are not connected to a network, but are shared by multiple users.

Firewalls

Computers connected to a network are naturally more susceptible to intrusion as unauthorised access can occur without the physical presence of an intruder.

Hence, computers connected to a network usually require another layer of access control called a **firewall**

A firewall is a device/network that prevents unauthorised access to or from a private network. It works by monitoring each piece of data transmitted through a network. It then either blocks or allows data to pass based on a set of rules configured by an administrator.

When properly configured, a firewall can protect computers within a network from unauthorised access. They can be configured to block the transmission of data (aka **traffic**) between unauthorised senders and receivers, especially requests for data from anonymous users on the internet. This prevents intruders from gaining access to the computers within a network.

Since firewalls can also block traffic based on the type of application that is transmitting the data, it can also stop certain harmful programs from sending copies of themselves to other computers through the network.

Configuring a firewall correctly can be complex and a misconfigured firewall may have security vulnerabilities that allows intruders to gain unauthorised access.

A properly configured firewall allows for a private network (aka **intranet**) to be set up such that all external traffic is blocked and only authenticated and authorised users are able to access it. Since the users on a private network are generally trusted and expected to keep information on the network confidential, there are usually fewer concerns about unauthorised access when sharing data on a private network.

Conversely, a private network such as the Internet allows anyone to connect to it and share data. Since public networks have little-to-no restrictions, users need to be wary of possible security and privacy risks when accessing it.

Encryption

Encryption is the process of encoding data so that a secret key is required to read the

data. Like passwords, the secret key is usually provided as a sequence of bytes.

Before the encrypted data is decoded using the secret key, it appears as random and meaningless data.

Encryption is often used to protect data from unauthorised access by allowing only authorised users to have the secret key. It can be used in combination with file permissions so an unauthorised user who bypasses file permissions would still be unable to use the accessed data without knowing the secret key.

Understanding of Privacy Policies

Unauthorised access can occur indirectly due to the actions of 3rd-party users or services.

For example, a user alters file permissions to let a classmate access some private files. That classmate in turn shares those files with others without the original user's knowledge.

- **Privacy** - The ability to keep specific data or resources from being known by others.
  - In many countries, organisations are required by law to publicise or make available a privacy policy about the rules and practices they follow regarding the collection, protection and use of personal or private data provided by users.
  - **Example**: Organisations in Singapore are required by the Personal Data Protection Act (PDPA) to make their privacy policies available upon request.

An increasing number of users share personal information such as photos and location data using online services, many of them are unfamiliar with the relevant privacy policies or how such sharing habits may indirectly result in unauthorised access. A poor understanding of the privacy policies of these services can often result in unauthorised access.

Social Networking Sites

Social networking sites such as Twitter, Instagram and TikTok allow users to share photographs and information quickly with their families or friends. They can also be used to promote businesses or raise awareness of campaigns or causes.

However, these sites can pose many privacy concerns because most users do not read or consider the repercussions of the privacy policies used by these sites regarding personal information such as status updates, notes, photographs and location data.

The privacy policies for many social networking sites do not guarantee that personal data collected will never be exposed to unauthorised users and may even require that your personal data be shared with advertisers in order to use their sites. Hence, personal data can potentially be harvested for spam and other threats to privacy that users did not authorise directly.

Introduction to Networking

Public vs Private IP Addresses](#public-vs-private-ip-addresses) * Network Address Translation * Example of a MAC address * Why have we not run out of IPv4 Addresses? * Why are we still using IPv4 when there is a better IPv6? * IP Address in Singapore * IP Address in USA * Port Number * Did you know? * Service Set Identifier (SSID)

Computer Network

A computer network is a system of two or more computers (or devices) that are connected together by a transmission medium for the exchange of data.

Advantages

- **Shared Resources**
  - A network allows a group of computers to make use of shared resources such as printers or files
- **Shared Internet Access**
  - Depending on the network's configuration, every user who logs on to the network may have access to the internet
- **Shared software: Software**
  - Can be stored on the central server of a network and deployed to other computers over a network
- **Shared Storage**
  - Data files can be stored on a central server for ease of access and backup purposes
- **Communication**
  - Computers in the same network are often able to share instant messages and emails for communication

Disadvantages

- Initial Costs
  - Installing a network could be costly due to the high setup and equipment costs.
- Maintenance Costs
  - There are also subsequent costs associated with administering and maintaining the network
- Security Risks
  - As files are shared through a network, there is the risk of virus or worm attacks spreading throughout the network even with just one infected computer.
- Risk of data loss
  - Data may just become lost due to hardware failures or errors. Using a network means regular data backups are needed.
- Server outage
  - If the server fails, the network will not be able to function, thus affecting work processes.

Types of Computer Networks

Geographical Location

- Local Area Network (LAN) - Network of connecting devices connected within a small geographical area, typically within the same building, such as a home, school or office.
- Metropolitan Area Network (MAN) - Network of computing devices typically spanning across two or more buildings within the same
- Wide Area Network (WAN) - Network of computing devices covering a large-scale geographical area, typically across multiple geographical locations.

Network Protocols

Set of standards and rules that govern how two or more devices communicate over a network.

OSI stands for **Open Systems Interconnection**. The OSI model is a conceptual model created by the International Organisation for Standardisation which enables diverse communication to communicate using standard protocols.

The OSI model does not perform any functions in the networking process. It divides network communication into seven layers. The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.

Open Systems Interconnection (OSI). In this model, layers 1-4 are considered the lower layers and mostly concern themselves with moving data around.

Layers 5-7 called the upper layers, contain application-level data. It's basically 7 layers of Networking.

> **All People Seem To Need Data Processing**

OSI Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find "physical" resources such as network hubs, cabling, repeaters, network adapters or modems. E.g. RS-232, RJ45, 100ASE-TX.

OSI Data Link Layer

Physical Addressing

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols E.g. Ethernet, 802.11, WiFi 7, Fibre Channel, Frame Relay, Token Ring.

OSI Network Layer

Path Determination and Logical Addressing

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks e.g. IP, ARP, IPSEC, ICMP, IGMP, OSPF

ARP

What is ARP?

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address.

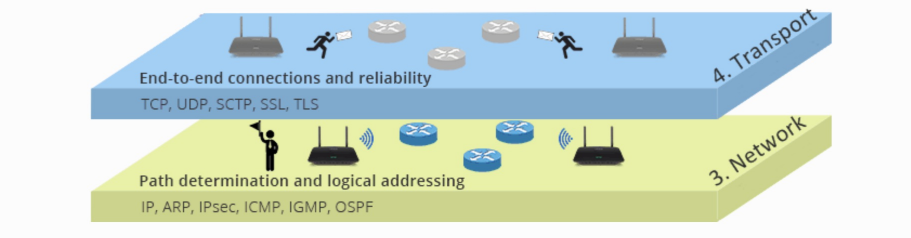
OSI Transport Layer

End to End Connection and Reliability

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol E.g. TCP, UDP, SCTP, SSL, TLS.

TCP/IP (Transmission Control Protocol/Internet Protocol; also known as the internet protocol suite) is the set of protocols used over the internet. It organises how data packets are communicated and make sure packets have the following information:

- **Source** - which computer the message came from.
- **Destination** - where the message should go
- **Packet Sequence** - The order the message data should be re-assembled
- **Data** - the data of the message
- **Error Check** - The check to see that the message has been sent correctly.



TCP/IP Protocol includes:

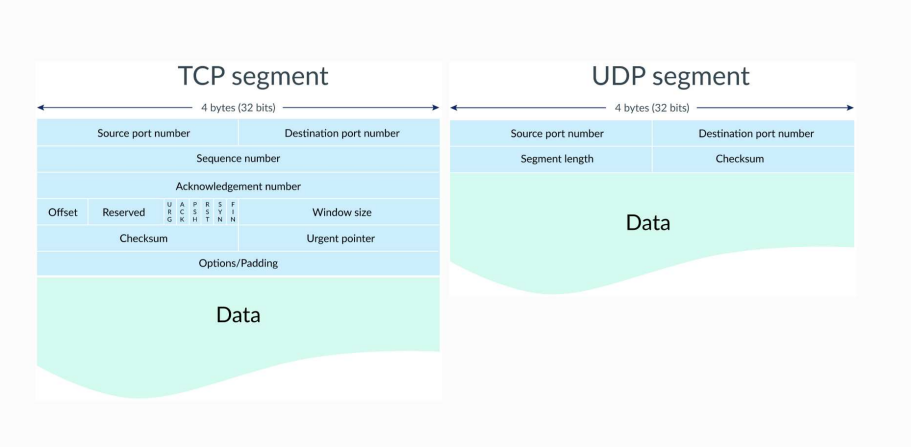
- HTTP - transfers web pages from web servers to the client. All web page addresses start with http. An https address is a secure web address which has been encrypted. An https address is used for sites holding bank details and secure information.
- FTP - used to transfer large files. It is often used for organising files on a web server for a website. You can have private access to download the documents that you have shared.
- UDP - User Datagram Protocol - Similar to TCP, but because messages are sent instead of packets - chunks - it is often faster, allowing for gaming or video calls over the internet.
- SMTP - Simple Mail Transfer Protocol - governs the sending of emails over a network to a mail server.
- IMAP/POP3 - Internet Message Access Protocol - governs retrieving emails from email servers.
- VOIP - is a set of protocols that enables people to have voice conversations over the internet.

TCP

- Slower but more reliable transfers
- Typical Applications:
  - File Transfer Protocol (FTP)
  - Web Browsing
  - Email

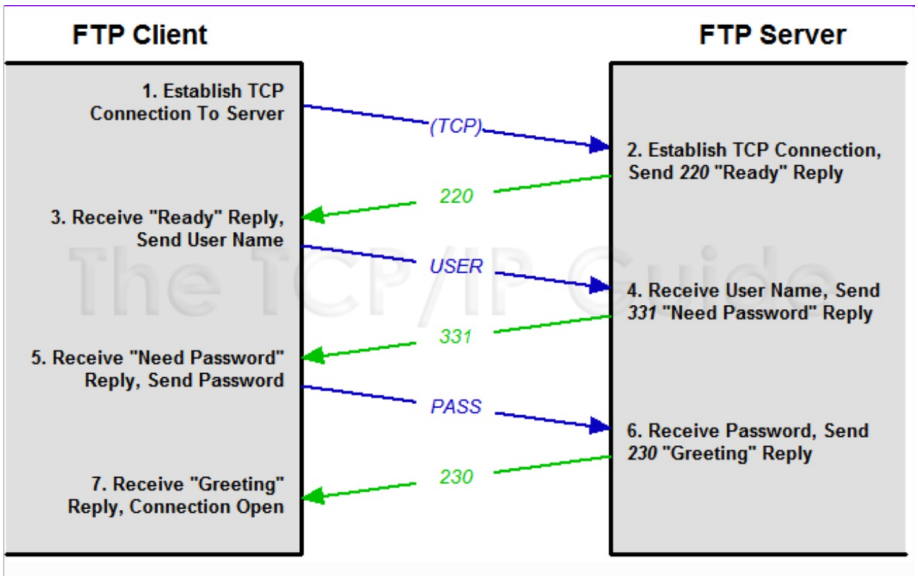
UDP

- Faster but not guaranteed transfers ("best effort")
- Typical Applications:
  - Live streaming
  - Online games
  - VoIP



The reason why FTP uses only TCP (Transmission Control Protocol) is that TCP provides a **reliable**, connection-oriented, byte-stream service, which is ideal for transferring files.

Additionally, FTP uses TCP's flow control and congestion control mechanisms to ensure that the network is not overloaded with too much traffic.



OSI Session Layer

Interhost Communication

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed and terminated at layer 5. Session layer services also include authentication and reconnections. E.g. Session establishment in TCP, SIP, RTP.

OSI Presentation Layer

Data Representation and Communication

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it is also at times is also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer. E.g. HTML, DOC, JPEG, MP3, M4V, Sockets

OSI Application Layer

Network process to Application

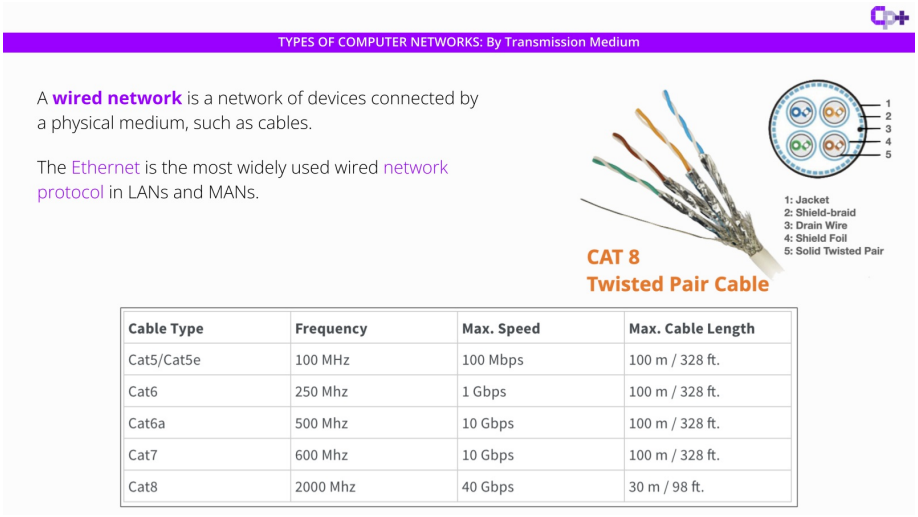
At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resources availability and synchronises communication. E.g. DNS, WWW/HTTP, P2P, EMAIL/POP, SMTO, Telnet FTP.

TCP is slower but more reliable it makes sure the data is safely passed. UDP on the other hand does not care and yeets the data hoping it works.

UDP uses time-sensitive transmissions. It speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party. Basically 2fast4u.

Transmission Mediums

A **wired network** is a network of devices connected by a physical medium, such as cables. The Ethernet is the most widely used wired network protocol in LANs and MANs.



Cable Type	Frequency	Max. Speed	Max. Cable Length
Cat5/Cat5e	100 MHz	100 Mbps	100 m / 328 ft.
Cat6	250 Mhz	1 Gbps	100 m / 328 ft.
Cat6a	500 Mhz	10 Gbps	100 m / 328 ft.
Cat7	600 Mhz	10 Gbps	100 m / 328 ft.
Cat8	2000 Mhz	40 Gbps	30 m / 98 ft.

A **wireless network** is a network of devices in which signals are transmitted without the use of a physical medium. The most common wireless network protocol is Wi-Fi, which uses radio waves to transmit data.

A **Wireless Access Point** (WAP) is a network device that provides a connection between wireless devices up to 100 metres away and can connect to wired networks.

Factor	Wired	Wireless

Factor	Wired	Wireless
Cost	Initially cheaper but becomes more expensive as network grows in size due to the cost of cables	Initially expensive due to the cost of wireless networking equipment but becomes more cost-effective as network grows in size
Speed of transmission / bandwidth	Faster and higher bandwidth as cables provide dedicated connection	Generally slower and lower bandwidth due to possible interference from radio-waves or microwaves; varies according to user location in relation to network
Reliability	More reliable as data transmission is unaffected by radio interference.	Less reliable due to potential interference from radio waves and microwaves or blockage from physical obstructions.
Security	More secure as the network is less susceptible to interception and hacking.	Less secure due to possible intrusion by hackers sniffing the wireless signals.
Mobility of users	Lower as network connections such as LAN points are fixed at specific spots and users cannot move to other locations.	Higher as users can move about freely within the range of the wireless network.
Scalability	More cumbersome to add new devices to the network as physical constraints and the running of cables and LAN points need to be considered.	Easier to add new devices to the network as the router can be easily configured for each new device.
Physical Organisation	Tend to look more disorganised due to cables running across floors	More organised without cables

To get 1m, talk about both Wired and Wireless.

VoIP

Advantages of VoIP include:

- Lower cost
- Completely portable
- Advanced features
- More scalable

Organisation (Client - Server Network)

Client-Server Network

- A **client** is a computer that initiates a connection to a server to request for resources and services to perform operations. E.g. Employees in offices or students in schools would normally use client computers to do their work.
- A **server** is a computer that shares resources and responds to requests from devices and other servers on the network. It usually has a higher capacity and is more powerful than a client as it needs to manage resources and services. E.g. Providing central storage of files, sharing hardware such as printers, controlling logins and network access.

Advantages

- Centralised control of data and resources
- Easy to schedule backups of all shared files at regular intervals
- Security may be enhanced with the use of specialised software or operating system features that are designed for servers.

Disadvantages

- Higher initial cost due to the need for a server
- Administrative costs needed for the maintenance of server and clients.

Peer-To-Peer (P2P) Network

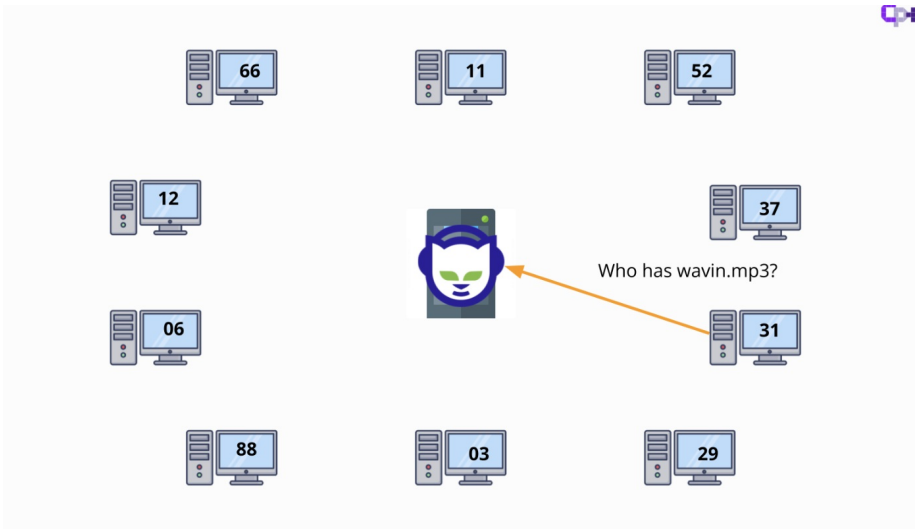
- All computers are considered as equals and the load is distributed among all computers. Each computer in the network is able to act as both a client and a server, communicating directly with other computers

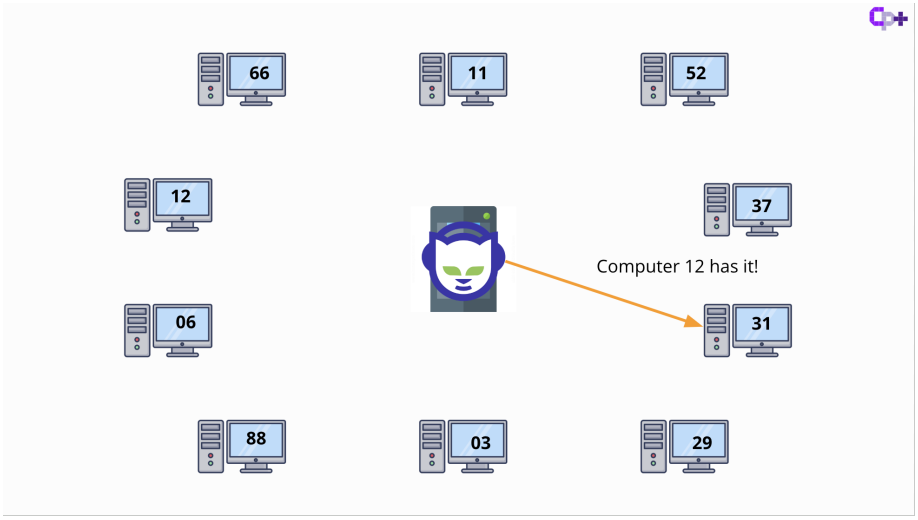
Advantages

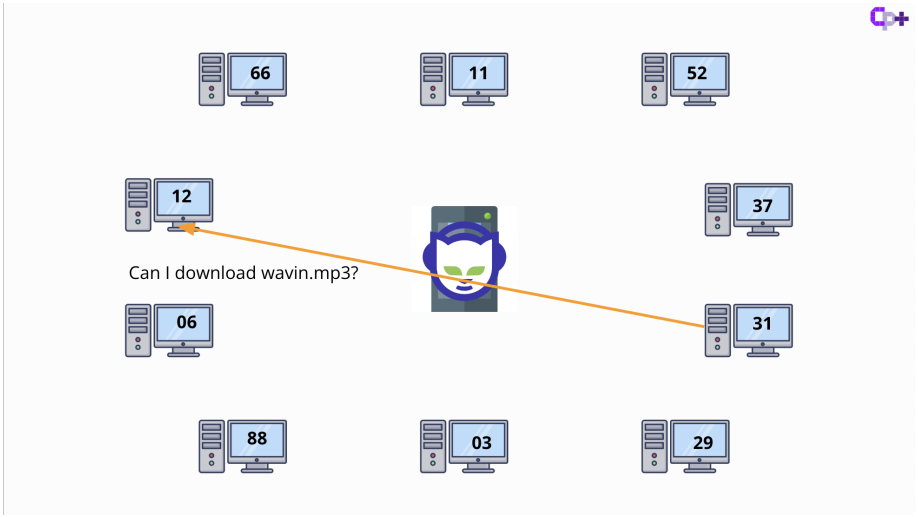
- Cheaper to set up as there is no cost related to dedicated servers
- Easy to set up as no specialised or operating system features are needed.

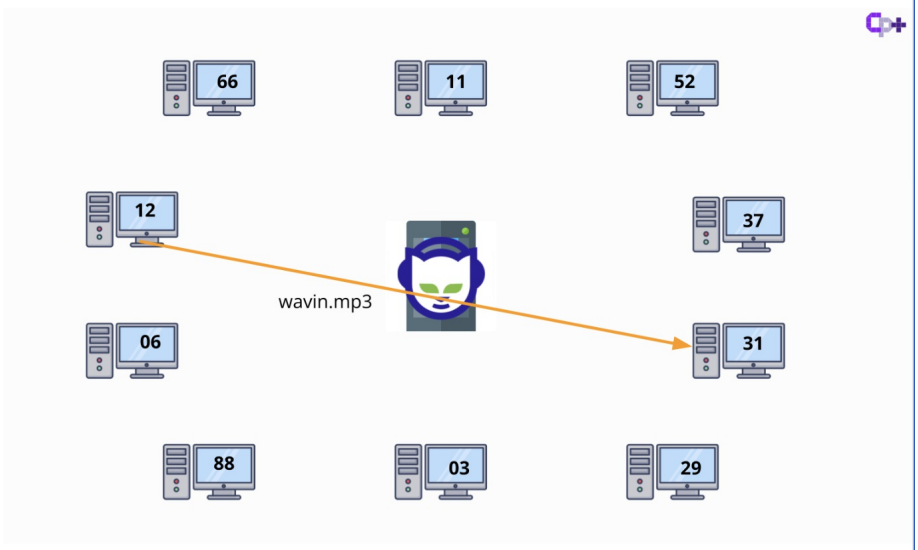
Disadvantages

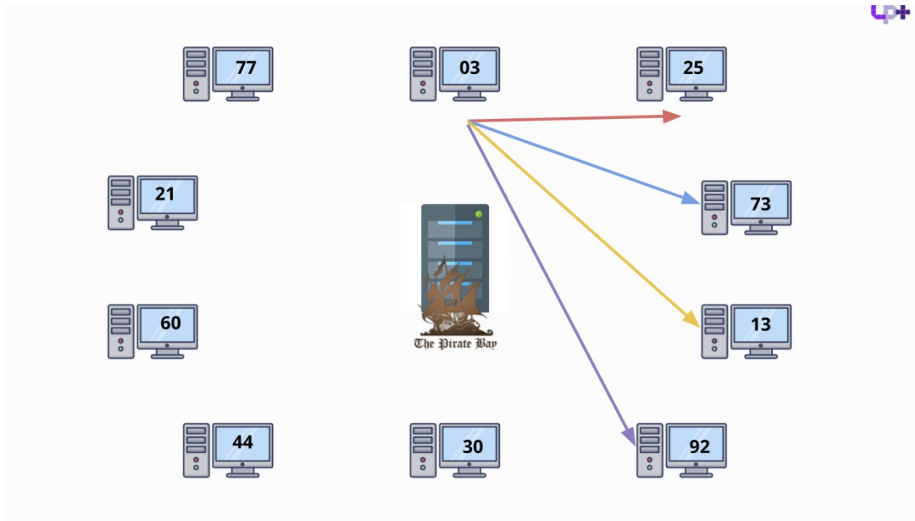
- More effort is required to access and backup resources as they are stored locally within each computer instead of centrally in a server.
- Security is an issue as access rights are not administered by a central server


66
11
52
12
37
Who has wavin.mp3?
06
31
88
03
29


66
11
52
12
37
Computer 12 has it!
06
31
88
03
29


66
11
52
12
37
Can I download wavin.mp3?
06
31
88
03
29





Factor	Client-Server	Peer-to-Peer
Function	Data and resources are shared using one or more dedicated servers; each computer has a distinct role — client or server.	Data and resources are shared directly between computers; each computer acts as both a client and a server.
Organisation of Hardware	Each client is connected to one or more dedicated servers.	Each computer in the network can serve as a client and a server at the same time.

Factor	Client-Server	Peer-to-Peer
Bandwidth	Typically high but limited by the capability of the server	Varies depending on how data needs to be transmitted; bandwidth may be reduced if a single computer must handle a large request, but may be increased if a large request can be divided into smaller requests that are handled by multiple computers simultaneously.
Security	High as access rights can be controlled centrally at a server	Low as security is handled by each computer and not by a central server.
Setup Cost	High as the use of specialised high-performance servers would be needed.	Low as basic computers can act as servers to share resources.
Storage	Centralised and carried out only at the server; usually managed by a network administrator	Decentralised and can be carried out by individual users at each computer.
Application	Found in businesses or organisations with a large number of users.	Found in homes or small businesses where there are few users.

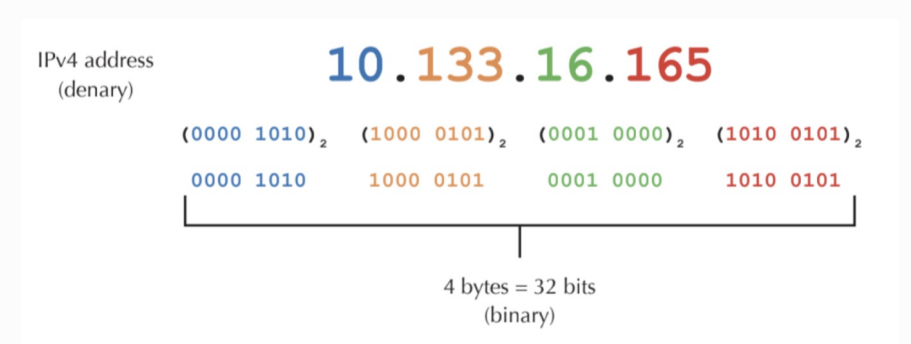
Identifiers

Identifiers

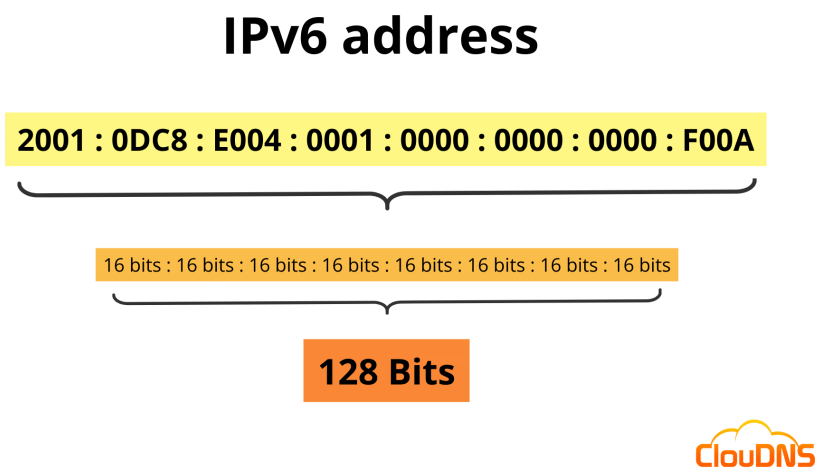
- IPv4 Address
- IPv6 Address
- MAC Address
- Port Number

IPv4 Addresses

Example of an IPv4 address



Example of IPv6 address

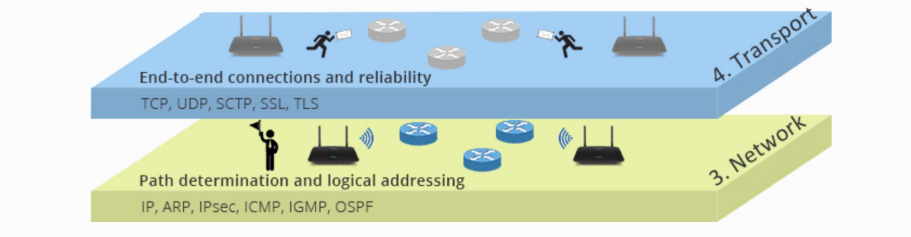


Public vs Private IP Addresses

- Each network will share the same public IP address. Other networks will be able to see your public IP address.
- When data meant for you is sent from another network to yours, it will be sent to your public IP address (which is your router's IP address)
- Your router keeps track of requests for data from each device by noting the private IP address down in a routing table. When it receives the data, it is able to route it to the correct device which requested for it.

Network Address Translation

Example of a MAC address



Why have we not run out of IPv4 Addresses?

- This is largely because of technologies like the **Network Address Translation (NAT)**, which maps many private IP addresses onto one public IP. There are also markets that sell and reallocate old IPv4 addresses for reuse.

Why are we still using IPv4 when there is a better IPv6?

- IPv4 is still the dominant internet protocol. A key benefit of IPv4 is its **ease of deployment and widespread use**. Because IPv4 is used so broadly, network administrators and other internet developers can assume it is everywhere because everyone is compelled to support it.

IP Address in Singapore

- Singapore has a total of ±20,297,984 IP address assigned.
- Population of SG in 2024 is 6.03 million.
- In SG, each home network has its own public IP.

IP Address in USA

- USA has a total of ± 1,528,537,344 IP addresses assigned.
- Population of USA in 2021 is 341.82 million
- In US, shared public IP by area/town/roads (determined by ISP)
- Each street has its own public IP address.

Port Number

- Used in combination with an IP address to identify a program that is running on a network
- All port numbers are assigned in a range from 0 to 65,535.

Service Set Identifier (SSID)

- A string of up to 32 bytes that identifies a Wireless Access Point (WAP) and all the devices connected to it.
- All wireless devices connected to the same WAP must use the same SSID.

Did you know?

You can list all the port numbers that are in use on your computer by entering `netstat -na` in the command prompt.

Service Set Identifier (SSID)

- A string of up to 32 bytes that identifies a wireless access point (WAP) and all the devices connected to it.
- All wireless devices connected to the same WAP must use the same SSID.

Number Systems

Denary Number System

Definition

A number system that is made up of **10 unique digits**.

- Uses place values of powers of 10.

Binary Number System

Definition

A number system that is made up of **2 unique digits**.

- Uses place values of powers of 2.

Notation

To distinguish binary numbers from denary numbers, they can be written in any of the following ways:

- 1101
- $(1101)_2$
- 0*b*1101

Leading zeros are sometimes also shown when using binary numbers in computer systems to show all 8 binary bits in a byte:

e.g. $0000 \space 1101$

Denary to Binary

Algorithm 1: Dividing by 2

1. Draw a table with three columns - one column for denary numbers, one column for the quotients and one column for the remainders.
2. Fill in the denary number in the first row.
3. Divide the denary number by 2 and fill in its quotient and remainder in the same row.
4. If the quotient is 0, proceed to step 5. Otherwise, copy the quotient to the denary number column of the next row and repeat step 3.
5. The equivalent binary number is the remainder column read from the bottom up.

Example: Converting 135 to binary

Denary	Quotient	Remainder

Denary	Quotient	Remainder
135	67	1
67	33	1
33	16	1
16	8	0
8	4	0
4	2	0
2	1	0
1	0	1

$\therefore (135)_{10} = (10000111)_2$

Algorithm 2: Sum of Place Values

E.g. Convert 135 to binary

Place value	256	128	64	32	16	8	4	2	1
	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binary digit		1	0	0	0	0	1	1	1

Hexadecimal Number System

Definition

Number system that is made up of 16 unique digits.

Denary equivalents of the hexadecimal

Hexadecimal digit	Denary equivalent
0	0
1	1
2	2
3	3
4	4
5	5
6	6

Hexadecimal digit	Denary equivalent
7	7
8	8
9	9
A	10
B	11
C	12
D	13
E	14
F	15

Example of Hexadecimal Number

$$1C6A$$

$$1C6A_{16} = 1 \times 16^3 + 12 \times 16^2 + 6 \times 16^1 + 10 \times 16^0$$

To distinguish hexadecimal numbers from denary numbers, they can be written in any of the following ways:

- $1C6A_{16}$
- $(1C6A)_{16}$
- $0x1C6A$

Denary to Hexadecimal

Algorithm 1: Divide by 16

1. Draw a table with three columns - one column for denary numbers, one column for the quotients and one column for the remainders.
2. Fill in the denary number in the first row.
3. Divide the denary number by 16 and fill in its quotient and remainder in the same row.
4. If the quotient is 0, proceed to step 5. Otherwise, copy the quotient to the denary number column of the next row and repeat step 3.
5. The equivalent denary number is the remainder column read from the bottom up.

Example

Convert 1899 to hexadecimal

Denary	Quotient	Remainder
1899	118	$11 = B_{16}$
118	7	$6 = 6_{16}$

Denary	Quotient	Remainder
7	0	$7 = 7_{16}$

Hexadecimal to Binary, or Vice Versa

Hexadecimal digit	0	1	2	3	4	5	6	7
Denary equivalent	0	1	2	3	4	5	6	7
Binary equivalent	0000	0001	0010	0011	0100	0101	0110	0111
Hexadecimal digit	8	9	A	B	C	D	E	F
Denary equivalent	8	9	10	11	12	13	14	15
Binary equivalent	1000	1001	1010	1011	1100	1101	1110	1111