Introduction to Networking

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.

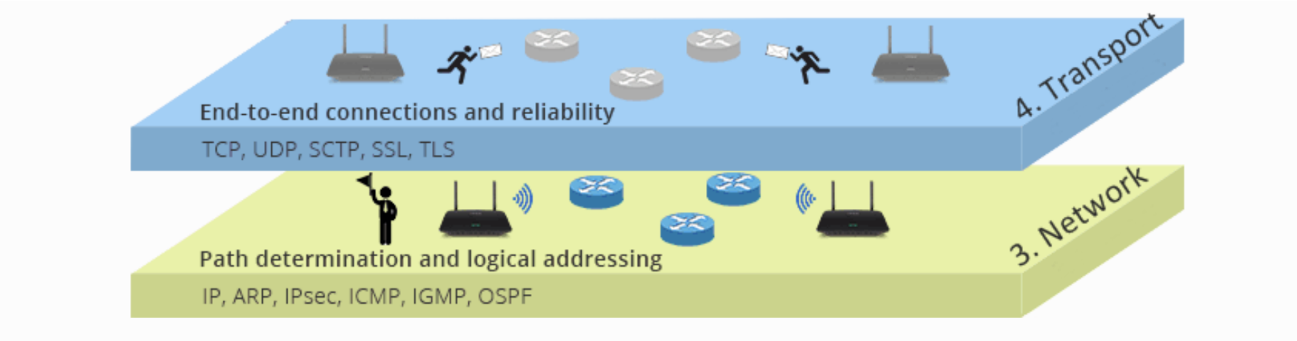
OSI Transport Layer

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.


4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF

TCP/IP Protocol includes:

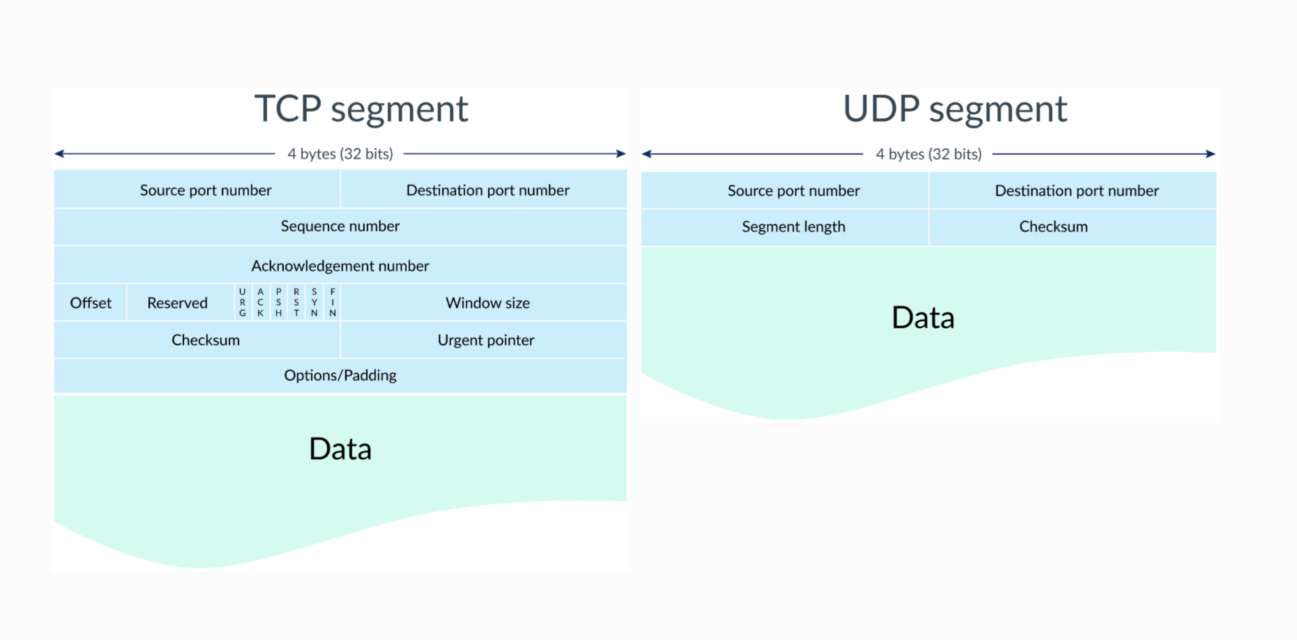
- **HTTP** - transfers web pages from web servers to the client. All web page addresses start with http. An https address is a secure web address which has been encrypted. An https address is used for sites holding bank details and secure information.
- **FTP** - used to transfer large files. It is often 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

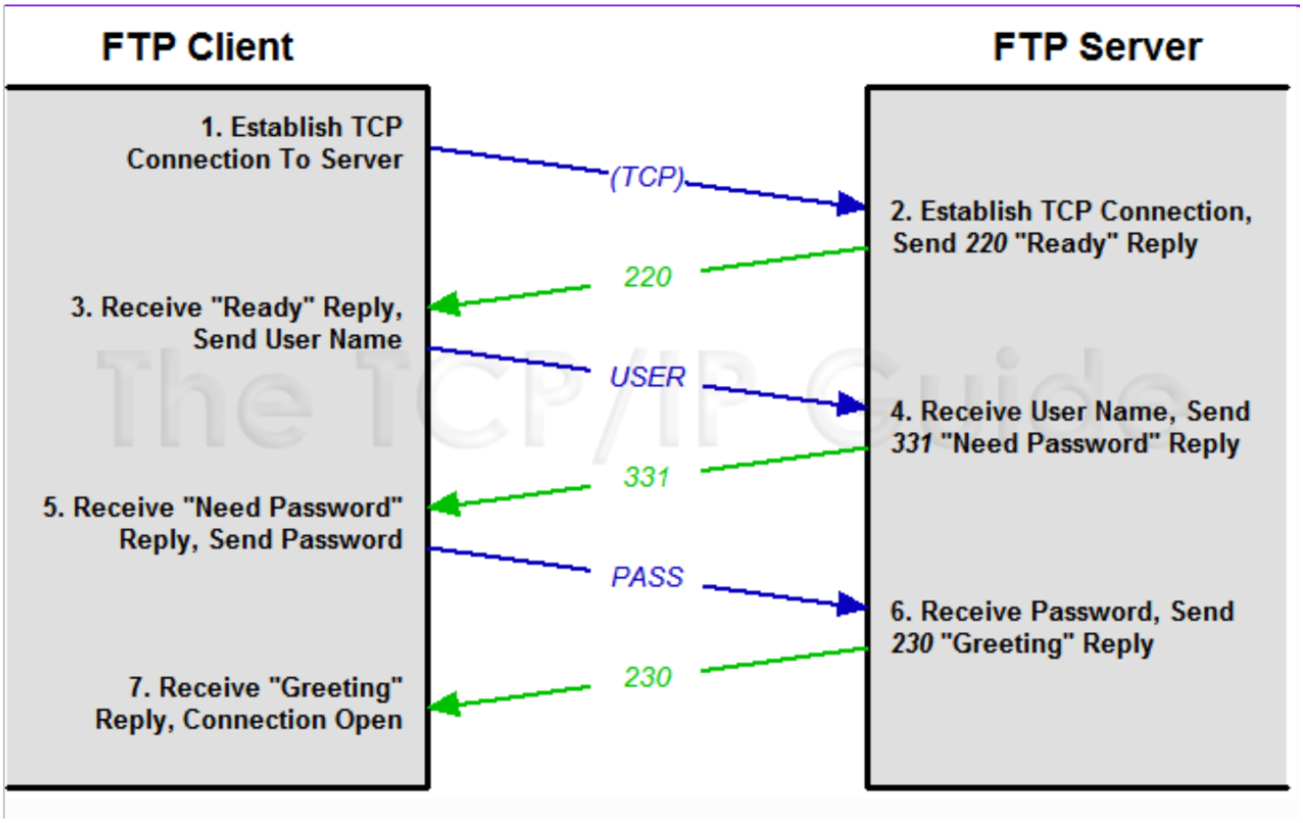
UDP

- 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.


FTP Client
FTP Server
1. Establish TCP Connection To Server
(TCP)
2. Establish TCP Connection, Send 220 "Ready" Reply
220
3. Receive "Ready" Reply, Send User Name
USER
4. Receive User Name, Send 331 "Need Password" Reply
331
5. Receive "Need Password" Reply, Send Password
PASS
6. Receive Password, Send 230 "Greeting" Reply
230
7. Receive "Greeting" Reply, Connection Open
The TCP/IP Guide

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

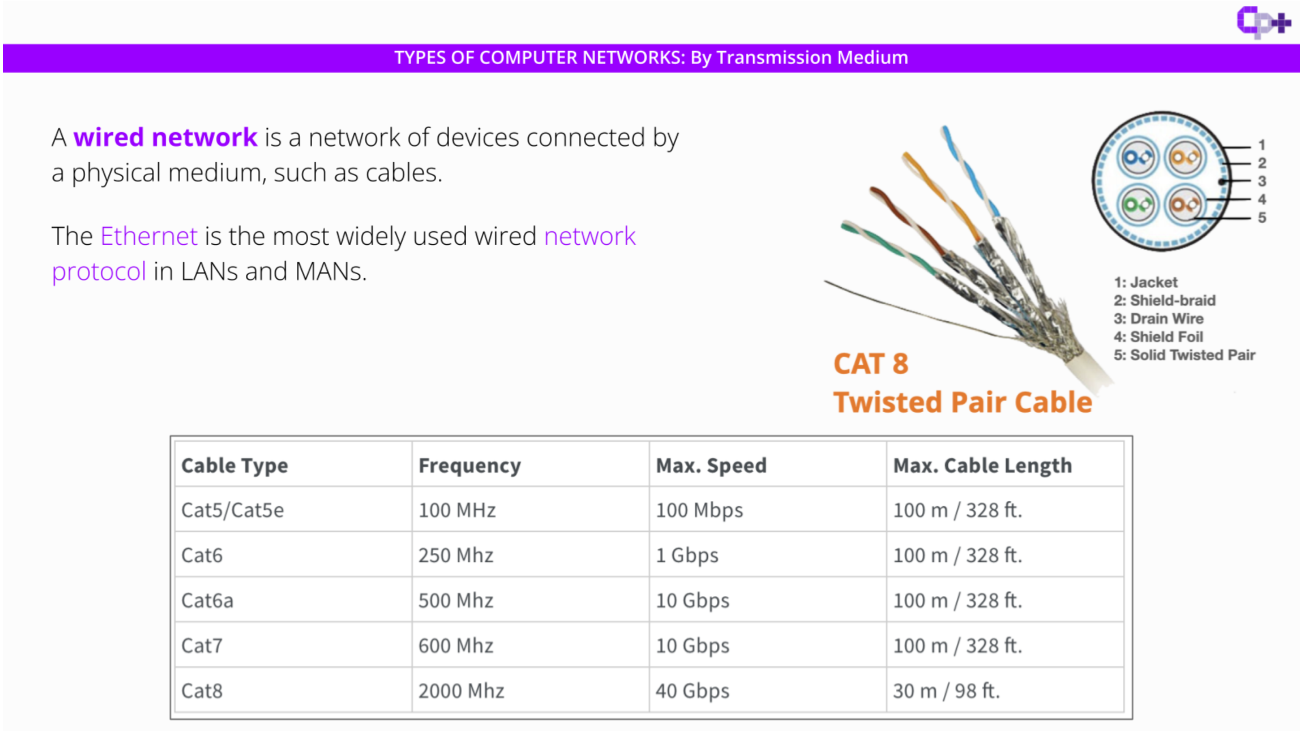
At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resources availability and synchronises 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.



TYPES OF COMPUTER NETWORKS: By Transmission Medium

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**
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

Factor	Wired	Wireless
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

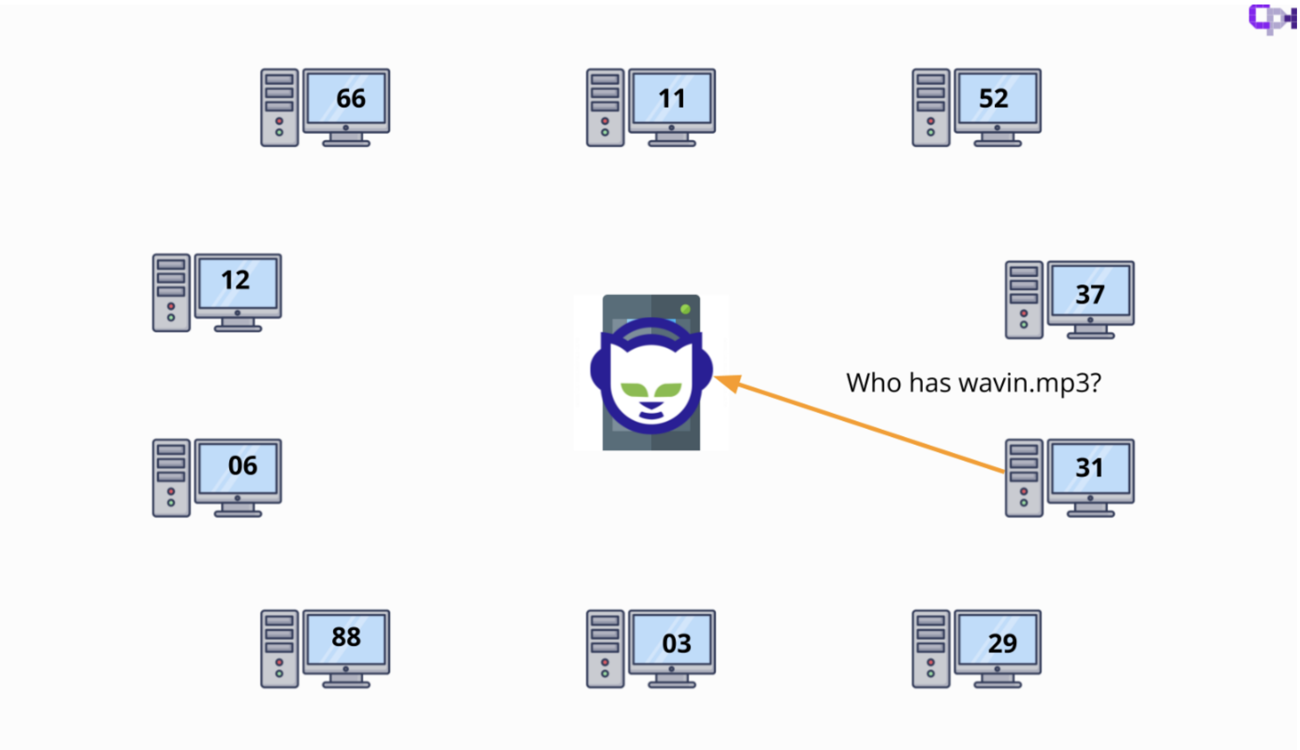
- All computers are considered as equals and the load is distributed among all computers. Each computer in the network is able to act as both a client and a server, communicating directly with other computers

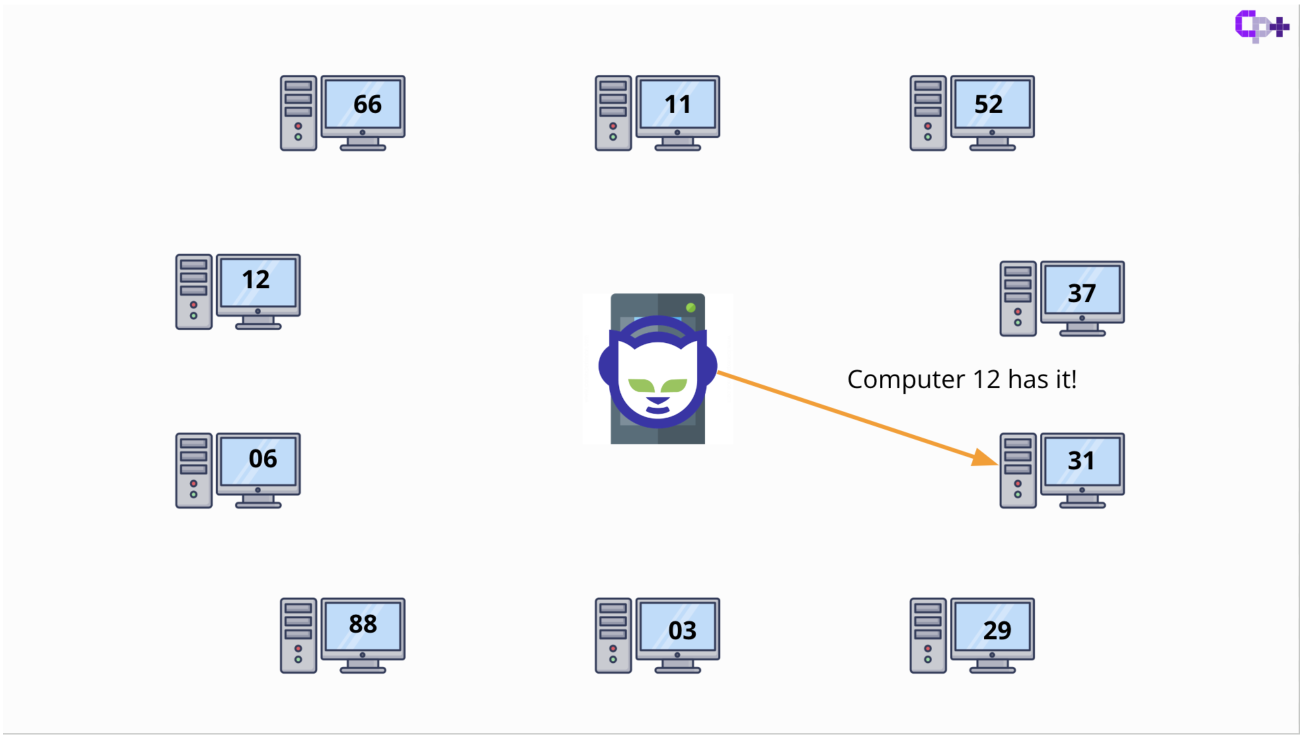
Advantages

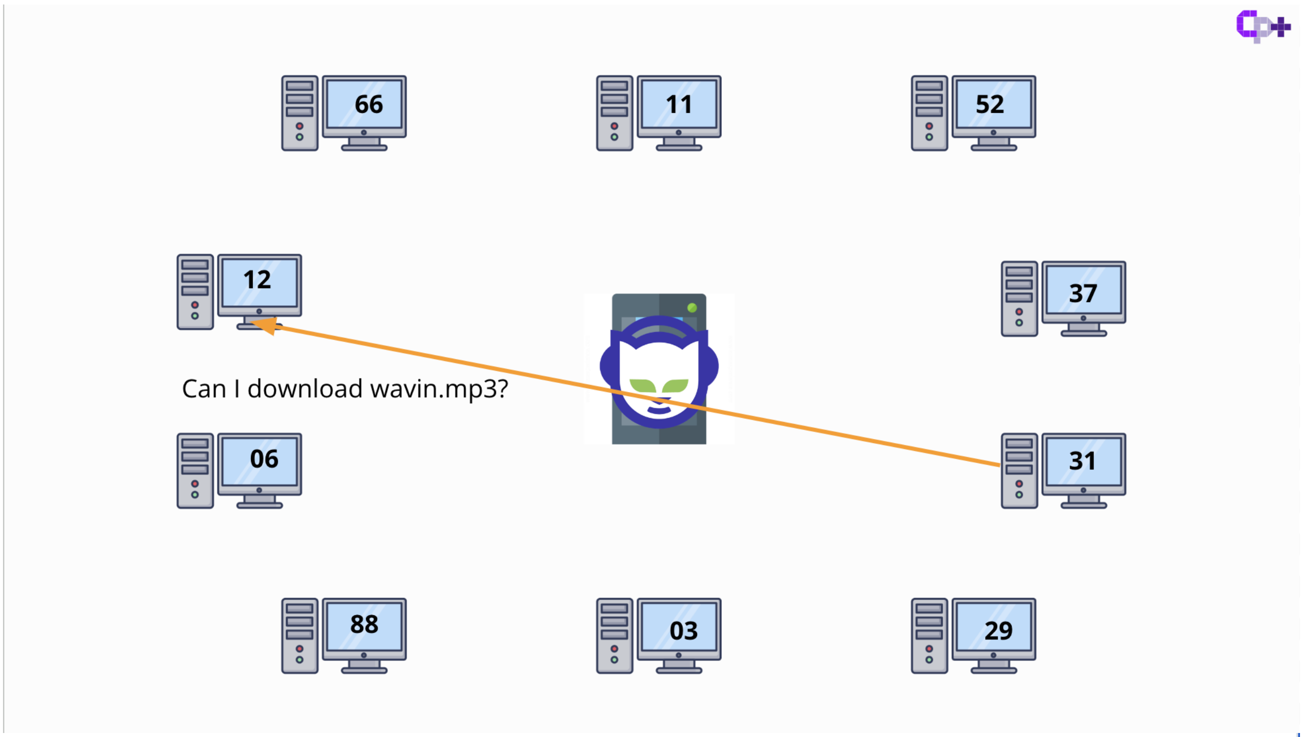
- Cheaper to set up as there is no cost related to dedicated servers
- Easy to set up as no specialised or operating system features are needed.

Disadvantages

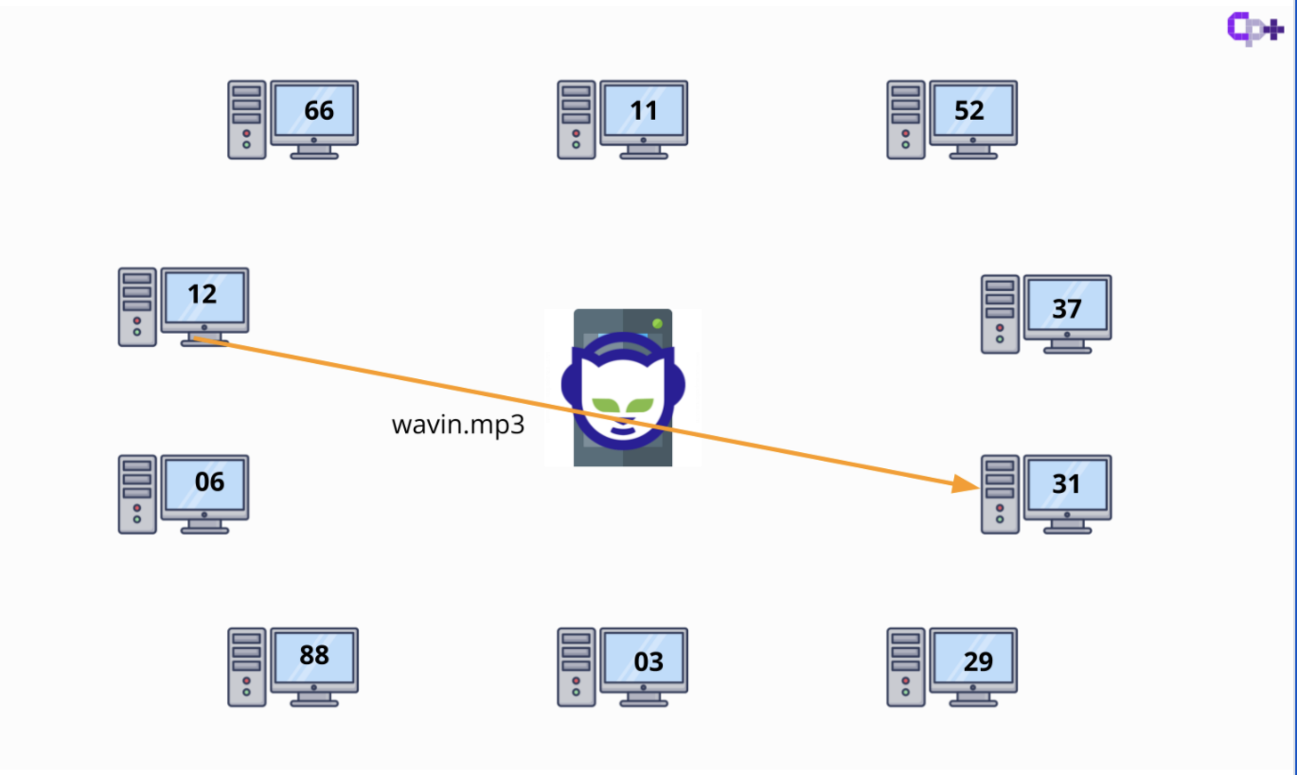
- More effort is required to access and backup resources as they are stored locally within each computer instead of centrally in a server.
- Security is an issue as access rights are not administered by a central server


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

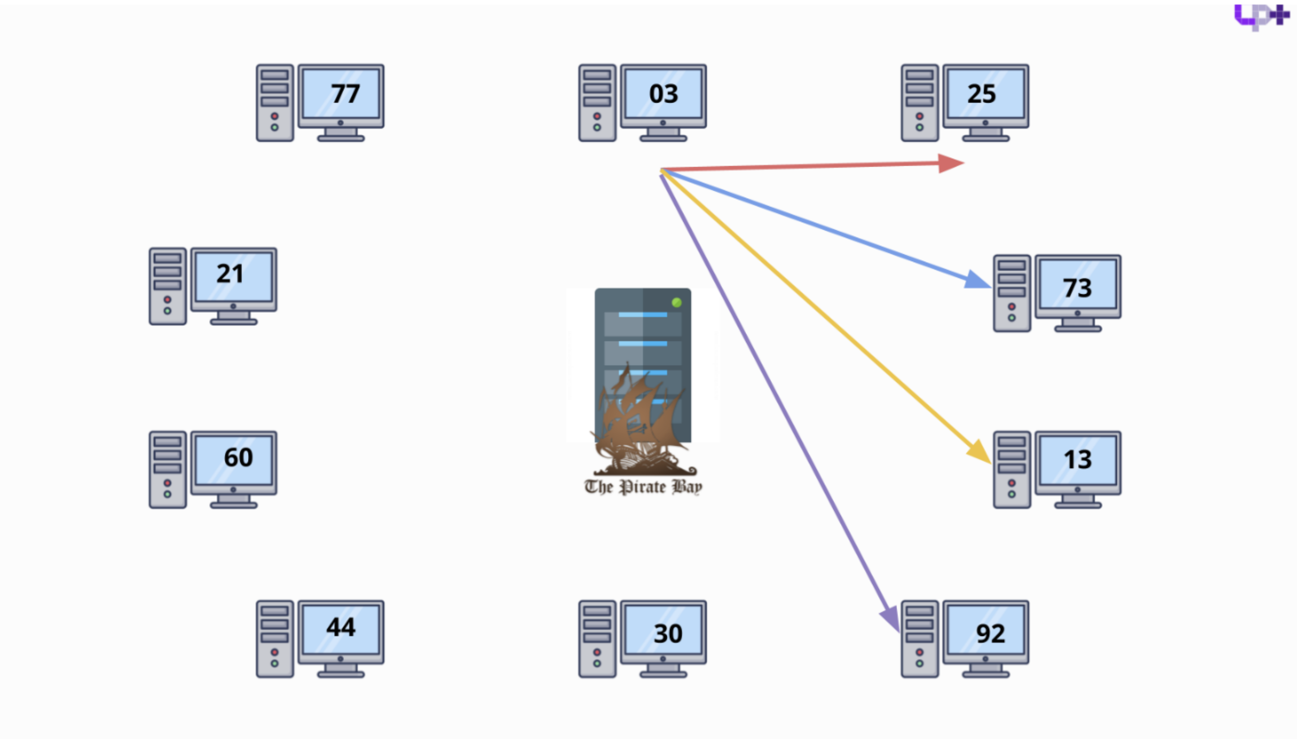

66
11
52
12
37
Computer 12 has it!
06
31
88
03
29



Can I download wavin.mp3?



wavin.mp3



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.
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.

Factor	Client-Server	Peer-to-Peer
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.

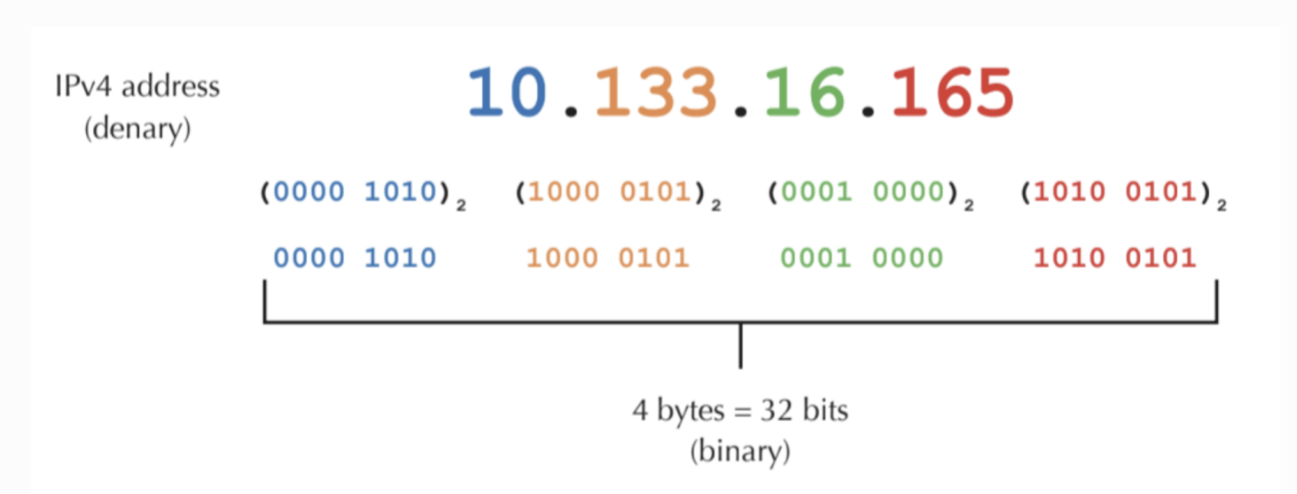
Identifiers

Identifiers

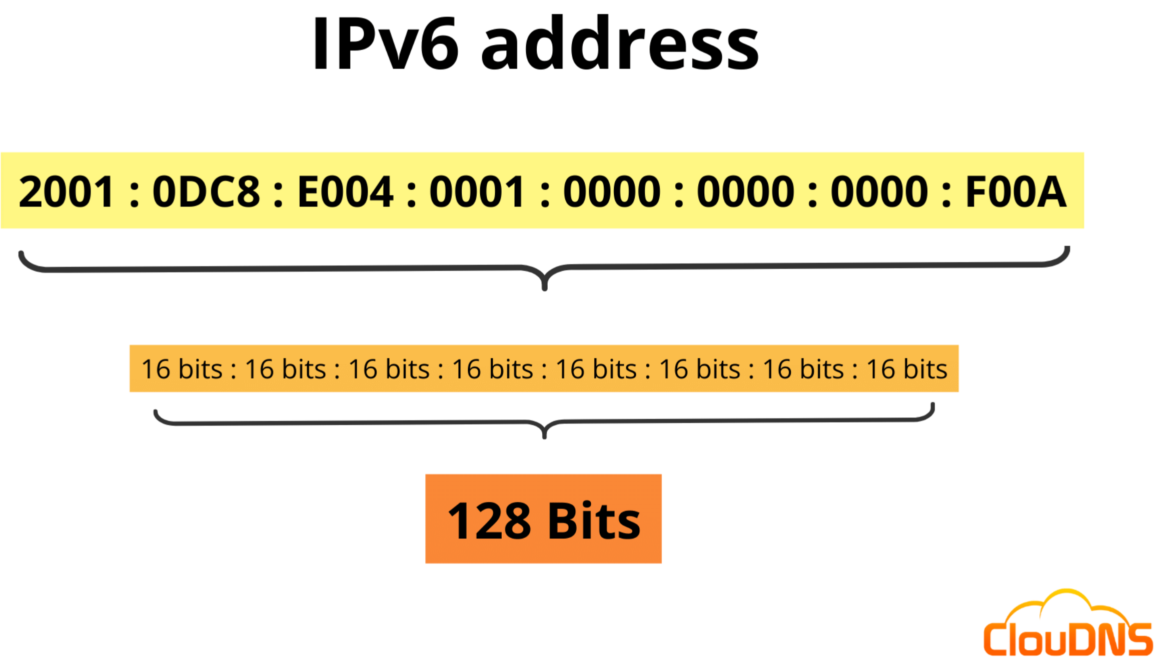
- IPv4 Address
- IPv6 Address
- MAC Address
- Port Number

IPv4 Addresses

Example of an IPv4 address



Example of IPv6 address


IPv6 address
2001 : 0DC8 : E004 : 0001 : 0000 : 0000 : 0000 : F00A
16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits
128 Bits
ClouDNS

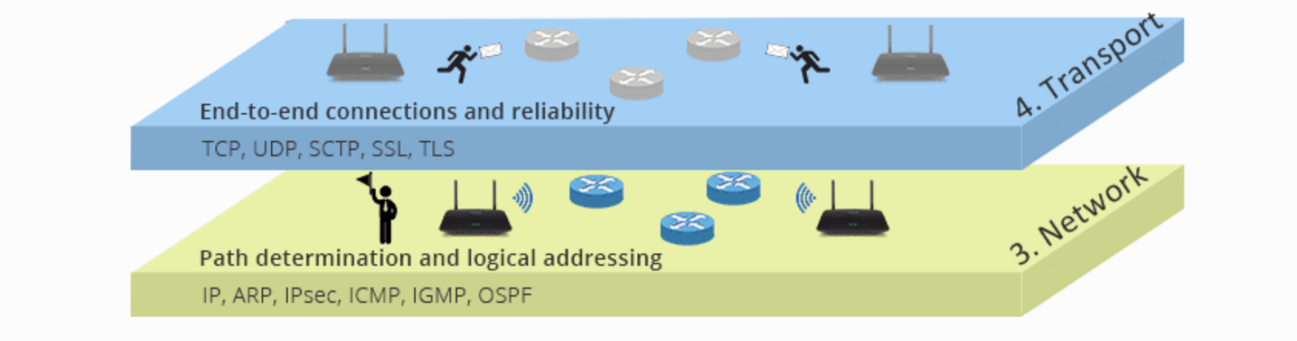
Public vs Private IP Addresses

- 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


4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF

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.

Network Hardware and their Functions

- Network Interface Card
- Network Hub
- Network Bridge
- Network Switch
- Router
- Modem

Network Interface Controller (NIC)

- Provides the hardware interface to **enable the transfer of data** between **a device and a network**. An NIC may connect to a network physically or wirelessly.
- Each NIC also has a unique 48-bit MAC address.

Network Hub

- Device that transmits received packets (even ones from within the network) to all connected devices.

Network Bridge

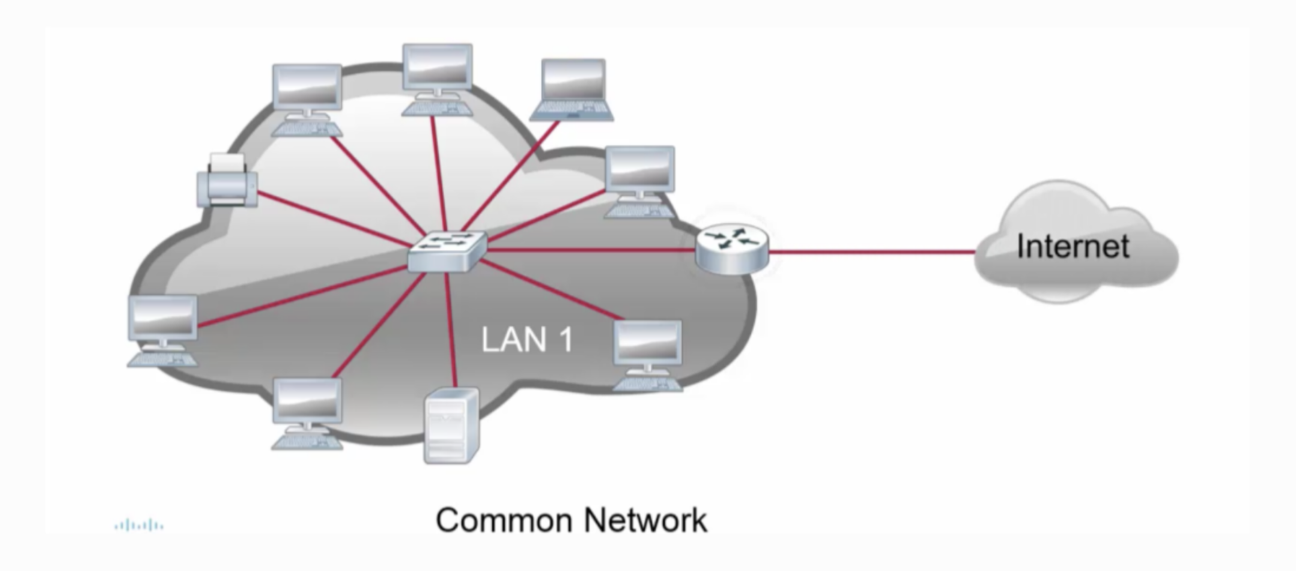
- Device that constructs a single network by connecting two similar networks together.
- Uses MAC addresses to keep track of devices that are connected to each side of the bridge. This lets the bridge intelligently decide whether it should drop or forward the packets that it receives.
- Suppose the bridge receives a packet from computer A. The bridge first examines the destination MAC address stored in the packet's header and devices whether to forward or drop the packet.

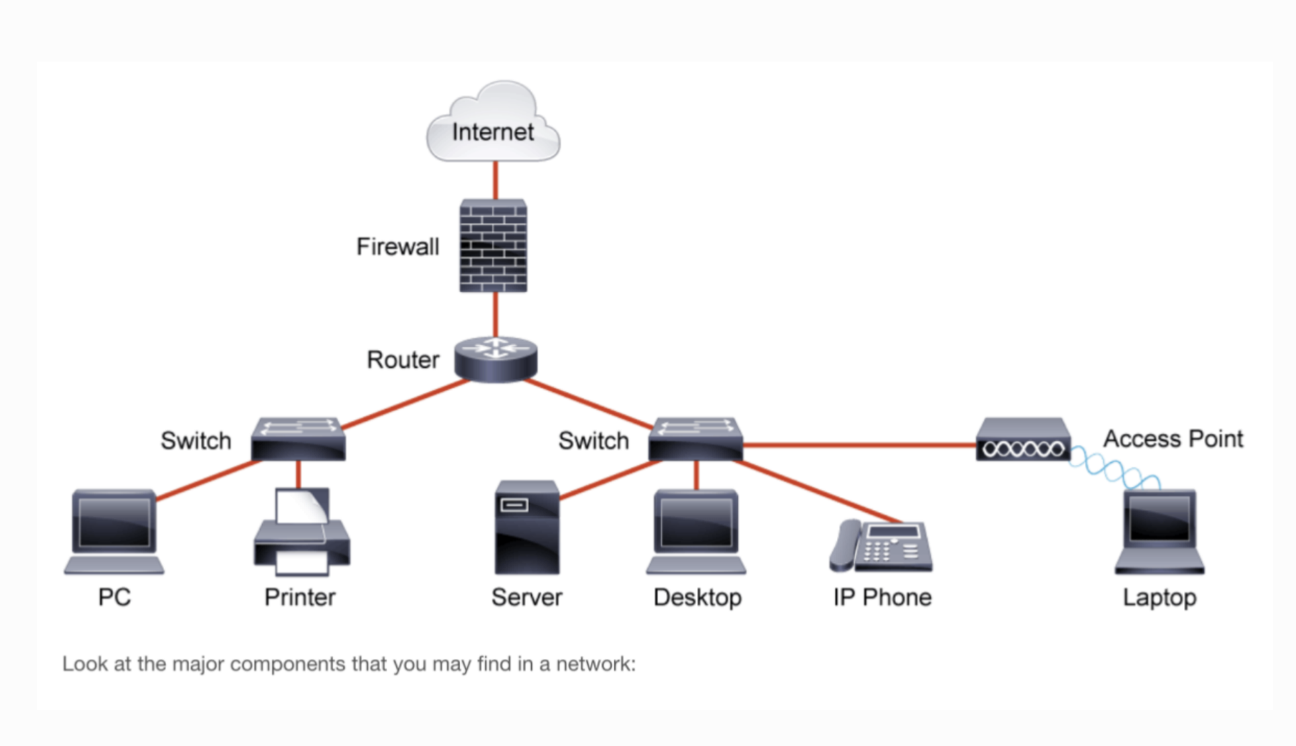
Network Switch

- A network bridge that connects multiple similar networks together.

Router

- Device that forwards packets between separate networks.
- The networks may use different protocols.
- In order for a router to forward packets between different networks using Internet protocols, both the device sending the packet and the device receiving the packet must be identified using IP addresses.





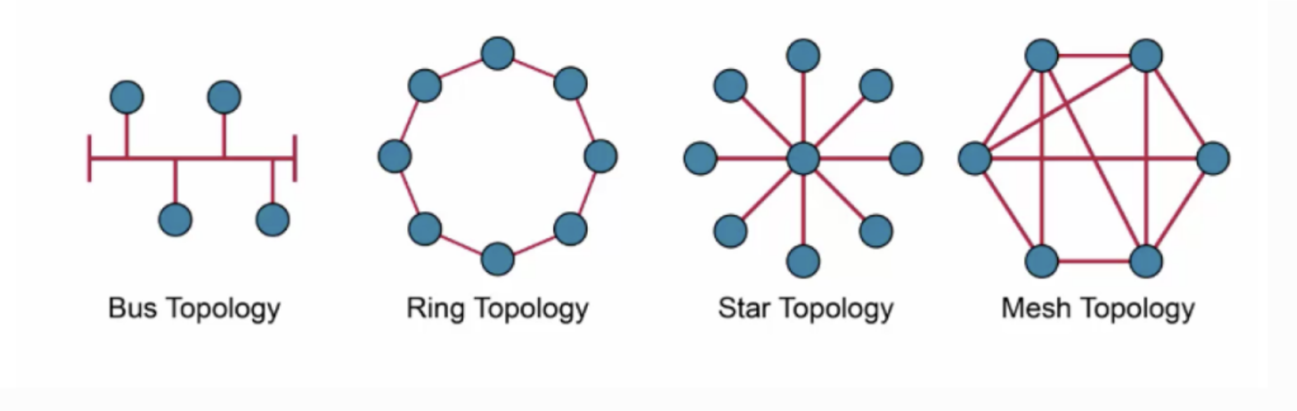
Look at the major components that you may find in a network:

Modem

- Device for connecting devices over a long range, usually used by Internet Service Providers (ISPs).
- But long-range transmission media are typically not designed for transferring digital data (i.e. 0 and 1 bits) that are used by computers. The digital data must be converted to a form suitable for transmission (modulation) and back again (demodulation).
- **Modem** = **mo** dulator + **demo** dulator

Network Topologies

- Bus
- Ring
- Star
- Mesh (+)



Topology: physical layout of the devices on the network.

- Used for both Client-Server and Peer-to-Peer network organisations.
- Used for both Wired and Wireless networks.

Common topologies include:

- Bus Topology
- Ring Topology
- Ring Topology
- Star Topology
- Mesh Topology

Bus Topology

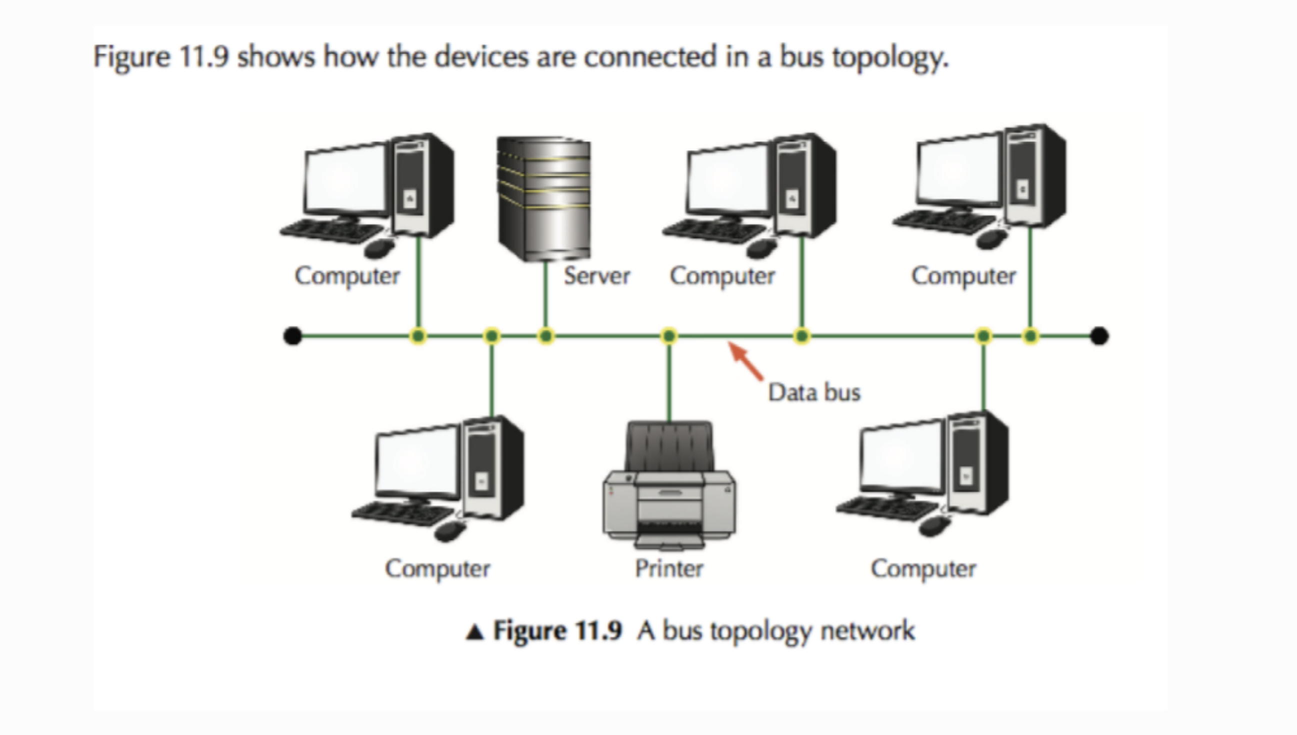


Figure 11.9 shows how the devices are connected in a bus topology.

▲ **Figure 11.9** A bus topology network

Advantages

- Easy and cheap to install as it uses less cabling than other network designs.
- Scalable as new computers can be easily added.
- Can continue to operate even when one of the computers breaks down.
- Works well for small networks.

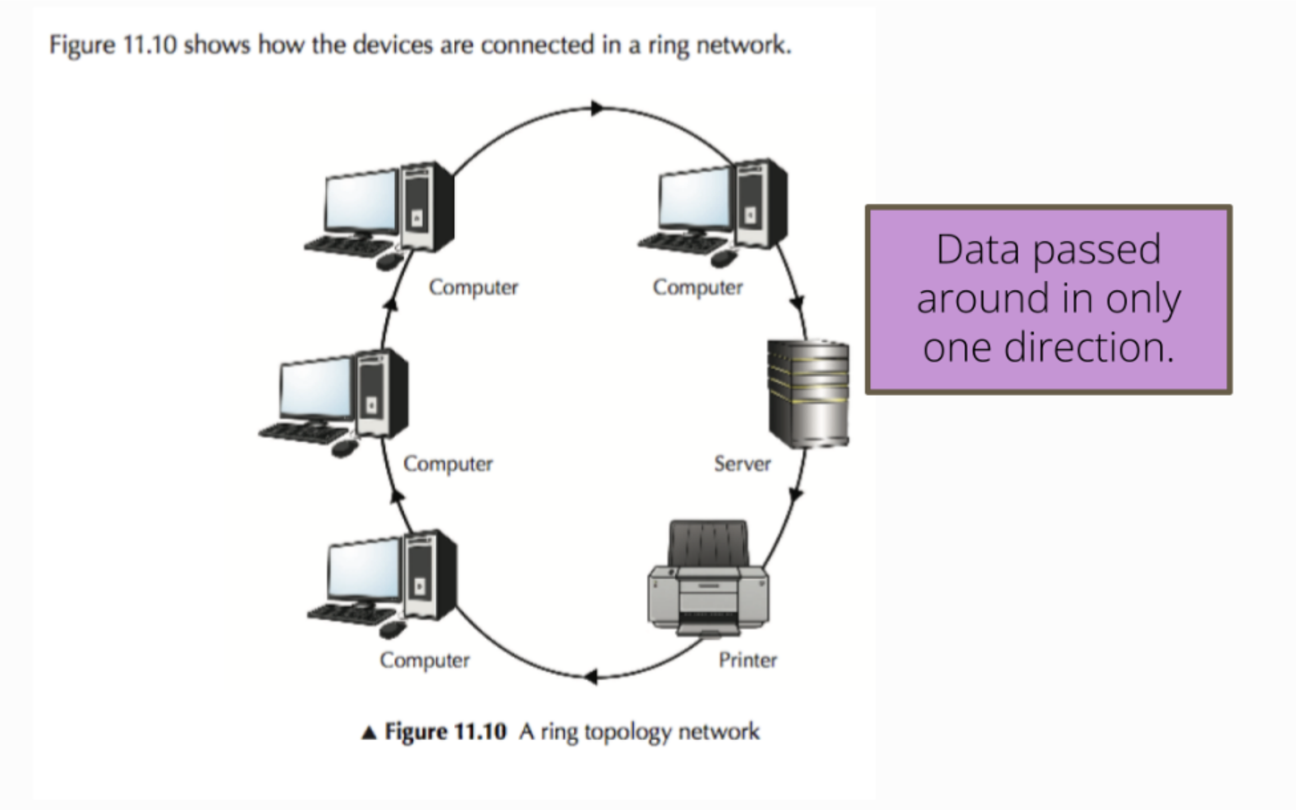
Disadvantages

- A break anywhere along the bus may disable the entire network.
- The size of the network is limited by the capacity and length of the bus.
- A single bus is unsuitable for networks with many computers; performance slows down as the number of computers increase.

Ring Topology

- Data passed around in only one direction.

Figure 11.10 shows how the devices are connected in a ring network.



▲ **Figure 11.10** A ring topology network

Data passed around in only one direction.

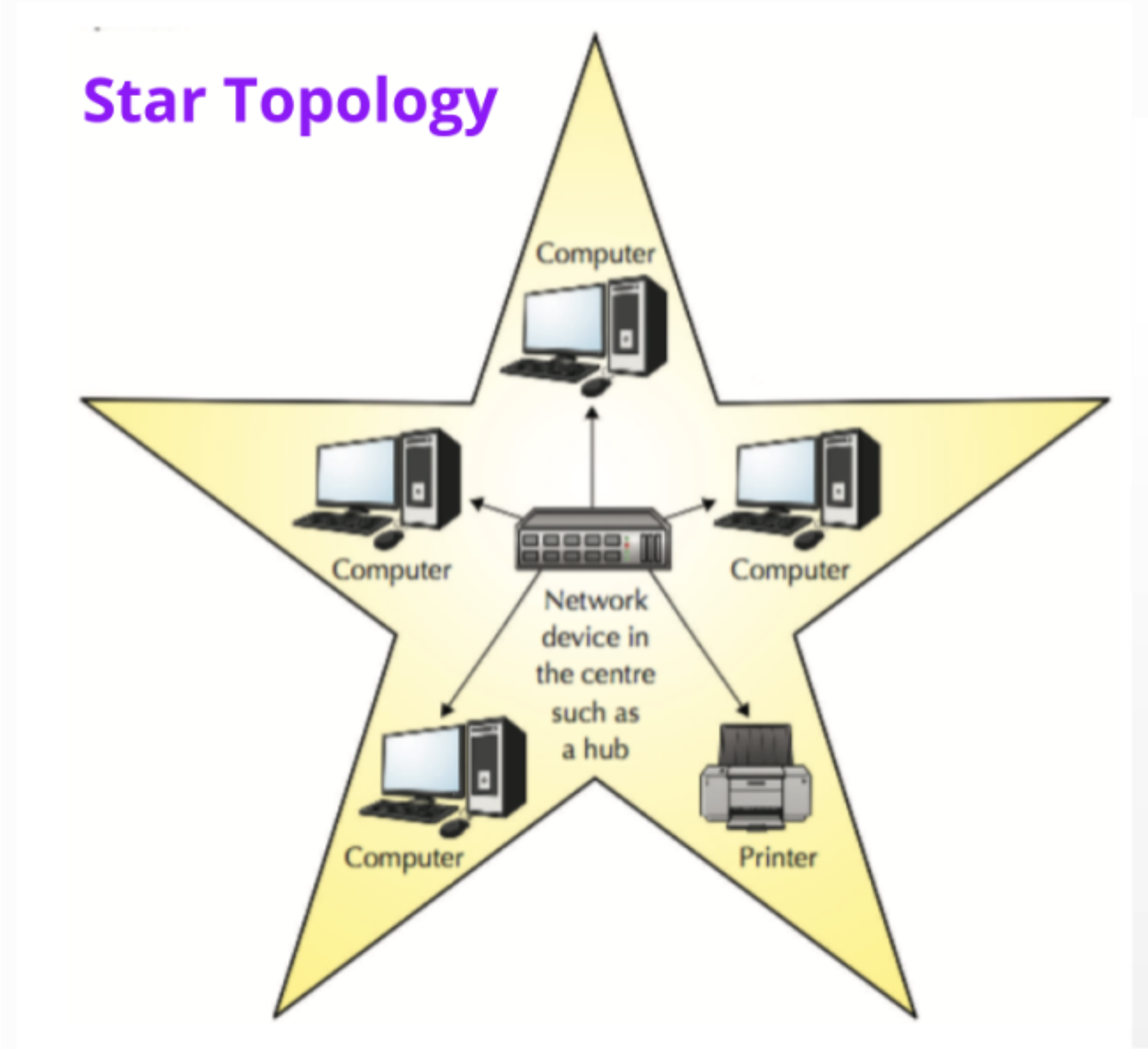
Advantages

- Can operate over larger distances and handle more data than a bus topology.
- Data packets that are sent between two computers will pass through intermediate computers, hence a central server is not required to manage the network.

Disadvantages

- If a computer or cable in the network fails, the entire network may fail as the data cannot be passed on.
- Adding a new computer to the ring network would mean that the whole communication ring needs to be temporarily interrupted.

Star Topology



▲ **Figure 11.11** A star topology network

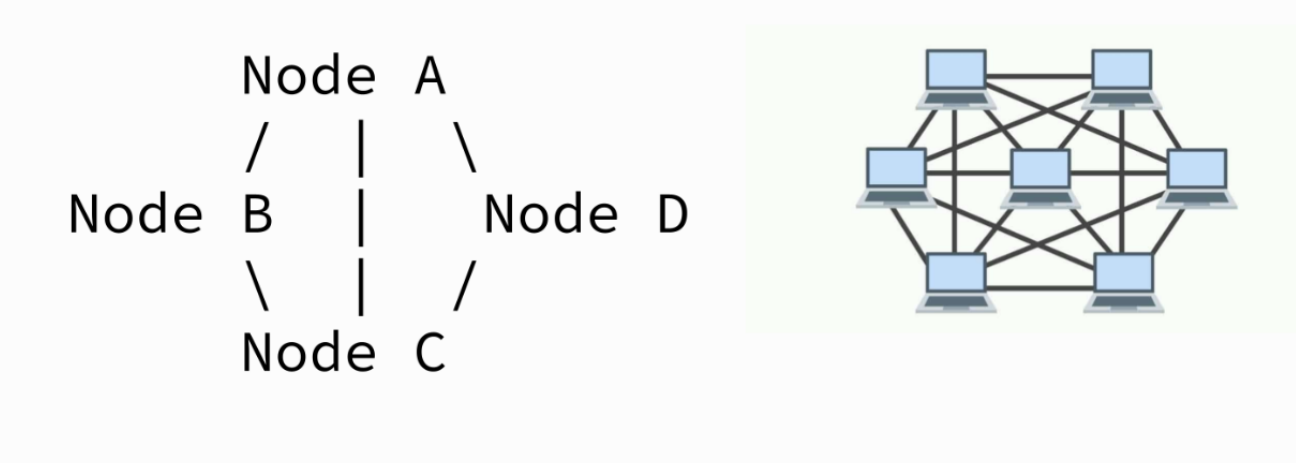
Advantages

- The load on each section of cabling is reduced as each computer uses a separate cable from the rest.
- If a fault occurs at a computer or a cable, it is easy to isolate the fault and do a replacement without affecting the rest of the network.

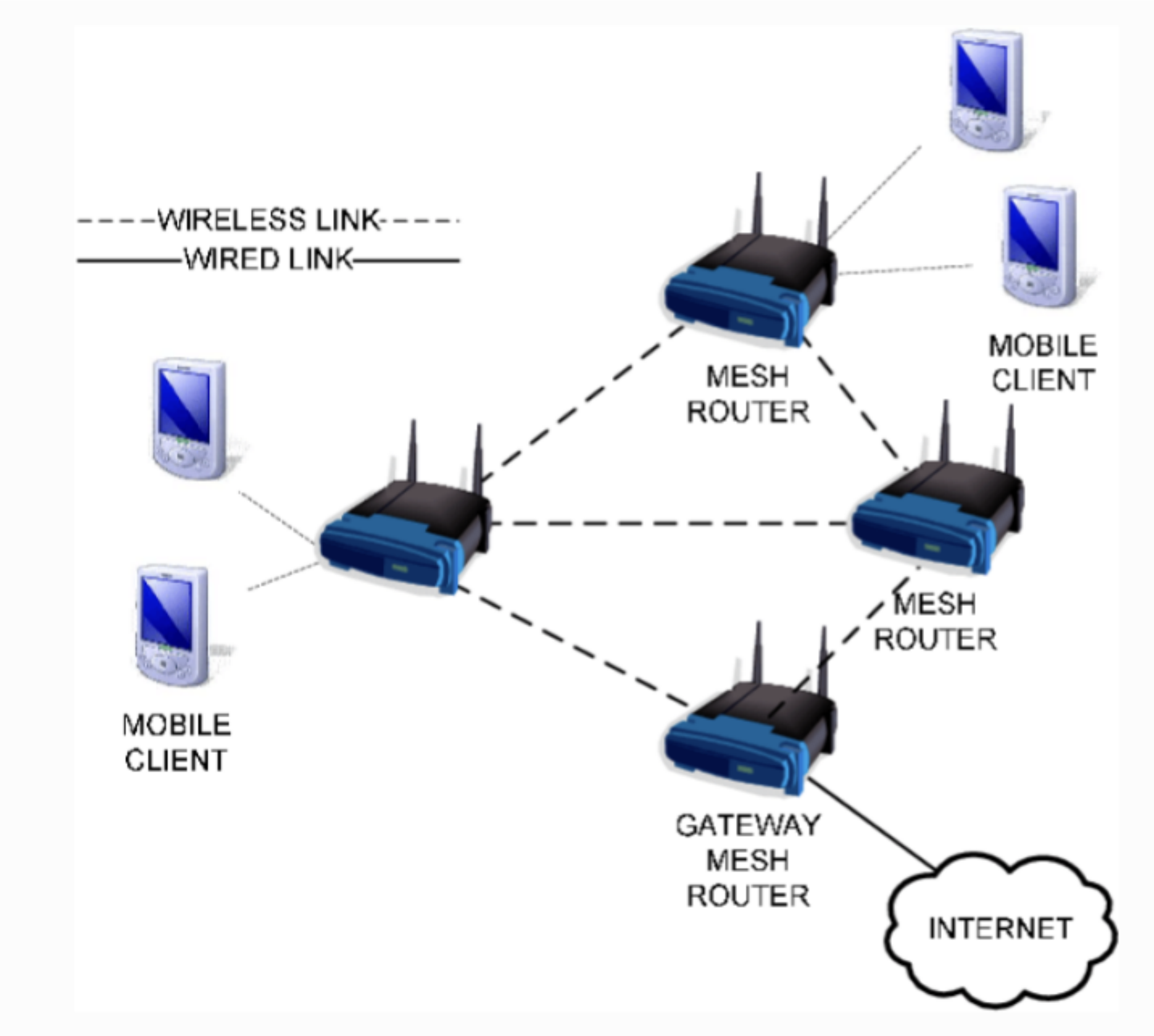
Disadvantages

- Uses more cabling than the other topologies (besides mesh) and hence costs more.
- If the central network device fails, the entire network fails (Single Point of Failure).

Mesh Topology



```
     Node A
     /  |  \
Node B  |   Node D
     \  |  /
     Node C
```



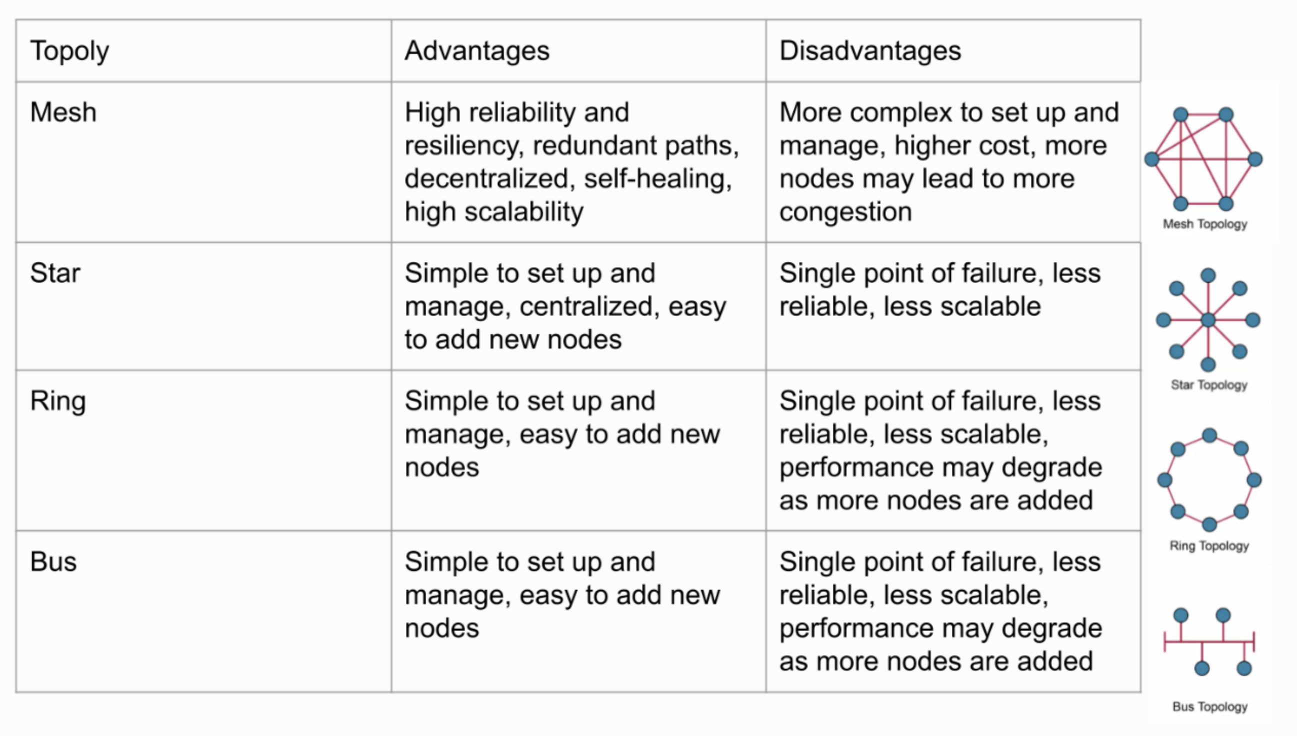
Advantages

- Manages high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

Disadvantages

- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.

- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.



Topoly	Advantages	Disadvantages
Mesh	High reliability and resiliency, redundant paths, decentralized, self-healing, high scalability	More complex to set up and manage, higher cost, more nodes may lead to more congestion
Star	Simple to set up and manage, centralized, easy to add new nodes	Single point of failure, less reliable, less scalable
Ring	Simple to set up and manage, easy to add new nodes	Single point of failure, less reliable, less scalable, performance may degrade as more nodes are added
Bus	Simple to set up and manage, easy to add new nodes	Single point of failure, less reliable, less scalable, performance may degrade as more nodes are added

Task 11.04 Network Topologies

> Jake plans to set up an accountancy consulting business in town. He wants to have a LAN in his office. He has about 100 staff working in the same office while about 20 other staff work from offsite locations such as his clients' offices. The staff needs to share files among themselves and be able to connect to printers. Most of the data being handles is confidential and dates back from 10 years ago to the present. He also has plans to expand his business in the next five years.

Explain why a client-server network is preferred over a P2P network by considering bandwidth, security and storage issues.

Error Checking Methods (Networks)

- Packets of data sent over a network can become lost or corrupted during transmission.

- Noisy Channel: Disturbance in the path when data is carried forwards from sender to receiver.
- When the data is received at the destination, it needs to be checked for errors.
- Note: in the examples in this chapter, we will use packets that are 8 bits long. In reality, the packets are usually larger.

Parity Check

- Error-checking technique which uses a parity bit to detect errors.
- This method is used when transmitting ASCII encoded characters.

Odd Parity System

- All the bits, including the parity bit, will add up to an **odd** number.
- E.g. 1001 0010 (Last bit is the parity bit)
    - If 1011 0010 is received instead, the receiver knows that an error has occurred as the sum of bits is not an odd number

Even Parity System

- All the bits, including the parity bit, will add up to an **even** number.
- E.g. 1001 1010 (Last bit is the parity bit)
    - If 1011 1010 is received instead, the receiver knows that an error has occurred as the sum of bits is not an even number

Limitations of Parity Checks

- If two bits are transposed, then the computer could be fooled into thinking the data is correct and not corrupted.
- If two random bits change state then the system could also be fooled.

Checksum

- A calculated value that is used to determine the integrity of transmitted data.
- Used when transmitting data using the TCP protocol (along with acknowledgements, which safeguard against data that is lost).
- Sum of all bytes in the data is calculated
- If the sum is less than or equal to 255(2^8 – 1), the checksum = sum.
- Else, the checksum = sum mod 256
- If the received data does not match the checksum, then the receiver knows an error has occurred.

Error Correcting Methods

- Able to detect **AND correct** errors in transmission, up to a certain number of errors.

Hamming distance

- The number of bits that differ between two strings
- Used to describe up to how many bits a system is error-detecting/error-correcting
- E.g. '1001 1010' and '1011 1010' have a Hamming distance of 1.
- E.g. '1000 1111' and '0111 0000' have a Hamming distance of 8.

Data Communications [+]

Securing Seven Domains of IT Infrastructure

1. User
2. Workstation
3. LAN
4. LAN to WAN
5. WAN

6. Remote Access
7. System/Application

User Domain

- People and their devices. Strong passwords, access controls, and training.

Workstation Domain

- User computers and OS. Software updates, antivirus, and user privileges.

LAN Domain

- Local network for workstations and servers. Firewalls, intrusion detection, and encryption.

LAN-to-WAN Domain

- Connection between LAN and WAN. VPNs, firewalls, and encryption.

WAN Domain

- Wide area network connecting remote sites and internet. Firewalls, intrusion prevention and content filtering.

Remote Access Domain

- Remote network access. Authentication, access limits, and encryption.

System/Application Domain

- Servers, apps, and data on the network. Access controls, backups, auditing and monitoring.

Advantages and Disadvantages of Networks

Advantages	Disadvantages
Communication: Share instant messages and emails for communication	Risk of data loss: Data may be lost due to hardware failures or errors, hence regular data backups are needed
(Shared) Resources: Make use of shared resources such as printers or files	Initial costs: Costly due to the high setup and equipment costs
(Shared) Software: Software can be stored on the central server and deployed to other computers.	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
(Shared) Storage: Data files can be stored on a central server for ease of access and backup purposes	Server outage: If the server fails, the network will not be able to function, thus affecting work processes.

CIA Triad

- Confidentiality
- Integrity
- Availability

Confidentiality

Safeguarding data confidentiality involves special training for those privy to sensitive documents. Training can help familiarise authorised people with risk factors and how to guard against people with risk factors and how to guard against them.

Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods to prevent users from bending data-handling rules with good intentions and potentially disastrous results. Data encryption is another common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication (2FA) is becoming the norm.

Integrity

These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem. In addition, organisations must put in some means to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash.

Data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.

Availability

This is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a properly functioning operating system (OS) environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important tactics. Redundancy, failover, RAID - even high-availability clusters - can mitigate serious consequences when hardware issues do occur.