Advantages and Disadvantages of Networks

Advantages
- Software and files can be shared.
- Hardware such as printers can be shared
- Users can communicate via email, chat, etc.
- Centralised maintenance and updates.
- Centralised security.
- User monitoring.
- Different users can be given different access rights or permissions.

Disadvantages
- Cost, additional equipment is needed.
- Additional management by specialist staff.
- Spread of malware.
- Potential for hacking.

Types of Network

LAN - Local Area Network
- Confined to a single location
- Owned and maintained by a single organisation
- Used by organisation such as schools and small businesses
- Connected by cables or wireless

WAN – Wide Area Network
- Covers a wide geographical area
- Used by organisations with several different sites such as banks or universities
- Allows all the sites to communicate and share data
- Uses national or international long distance media

The Internet
- A vast WAN covering the entire world
- An Internet Service Provider (ISP) provides access to the Internet.
- Routers provide an interface between the Internet and the customer via the ISP.
- Larger, more powerful routers connect the different components of The Internet.

Wired Networking

Using fibre or coper cable to connect devices in the network together.
Fibre cable provides a faster connection and can cover longer distances.
Advantages:
- Faster data transfer
- Less likely to suffer from interference
- More difficult for unauthorised users to intercept data

Disadvantages:
- Expensive to install or reconfigure
- Harder to move devices so less flexible

Wireless Networking

Using radio signals or infrared light to connect devices in a network together.
Advantages
- Devices can easily be added
- Users can move around freely and stay connected

Disadvantages:
- Signals have a limited range.
- Can suffer from electromagnetic interference from other devices.
- Signals can also be blocked by walls or other objects.
- Each wireless access point

Topic 4 – Networks

The Four Layer TCP/IP Model

Breaks up the process for sending of messages into separate components.
Each component handles a different part of the communication.
Helps to understand the transmission process.
Provides a basis to begin troubleshooting when something goes wrong.
- **Application Layer** – encodes and decodes message using protocols like HTTP or FTP.
- **Transport layer** - breaks down message into pieces called packets. Packets have a packet number. The recipient uses the number to reassemble the packets in the correct order and to see if there are any missing packets.
- **Network layer** - adds the sender and recipient IP address and transmits the message.
- **Data link layer** – provides physical transfer of packets over the network.

Network Protocols

Ethernet - used in wired LANs, covers many standards such as cable types and data transmission speeds.
Wi-Fi - used in wireless LANs.
TCP/IP - Transmission Control Protocol/Internet Protocol. Allows data to be appropriately addressed when transmitting and ensures the integrity of data.
HTTP – Hypertext Transfer Protocol – Web pages
HTTPS - Hypertext Transfer Protocol (Secure) – Secure web pages
FTP – File Transfer Protocol - transmission of files across a network and the internet.
SMTP – Simple Mail Transfer Protocol – Send emails
IMAP – Internet Message Access Protocol – Receive emails
POP3 – Post Office Protocol version 3 – Receive emails

Network Security

Access Control – determines which files, software and systems users have access to.
Users should be restricted to access only the facilities they need for their jobs.
Restrictions limit the actions a user can take, reducing the potential of threats.
Firewall – a tool which monitors traffic going into and out of the network, and either allows or blocks it.
This decision is based on rules, known as the firewall policy.
Can be hardware based or software based.
Hardware firewalls are expensive, but more effective and powerful.
Physical Security - restricting the physical access to important systems and parts of the network.
Important equipment such as servers should be kept in a locked secure room.
Access should only be available to authorised people.
Someone could remove or access the hard disks containing private information or damage equipment.

Identifying Network Vulnerabilities

It is important to identify and fix vulnerabilities before they can be taken advantage of by hackers.
Penetration Testing – determines how resilient a network is against an attack.
Authorised users, sometimes an external company will probe the network for potential weaknesses and attempt to exploit them.
Often carried out using specialist, automated software.
Ethical hacking - attempt to access a network in the same way as a hacker.
They are looking for weaknesses in the security of the network.
Weaknesses can then be fixed.
Might be employed by the business that owns the network being tested or they might work for a security company.

Network Speeds

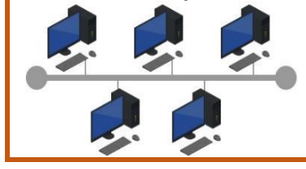
Measured in bits per second.
1 Kbps = 1,000 bits per second
1 Mbps = 1,000,000 bits per second
1 Gbps = 1,000,000,000 bits per second

Working out file transmission speeds
time = size of file (in bits) / network speed (in bits)

Network Topologies

Bus Network
All devices are connected to a single cable (called the bus)
A terminator is at each end of the cable.
Advantages:
- Easy to install extra devices.
- Cheap to install as it doesn't require much cable.

Disadvantages
- If the cable fails or is damaged the whole network will fail.
- Performance becomes slower ad additional devices are connected due to data collisions.
- Each device receives all data, a security risk

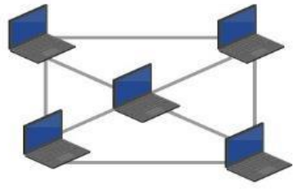


Star Network
All nodes are connected to one or more central switches.
Often used with wireless networks.
Advantages:
- Every device has its own connection so failure of one node will not affect others.
- New devices can be added by simply connecting them to the switch.
- Usually have higher performance as a message is passed only to its intended recipient.

Disadvantages:
- If the switch fails it takes out the whole network.
- Requires a lot of cable so can be expensive.

Mesh Networks
No central connection point, with each device connecting directly to others.
Full mesh networks have every device connected to every other device.
Partial mesh networks have each device connected to several others but not necessarily every other device.
Advantages
- Messages can be received more quickly.
- Messages have many possible routes they can take.
- Multiple connections mean that no device should be isolated
- Each device can talk to more than one node at the same time.
- Devices can be added without interruption.

Disadvantages
- Can be impractical and expensive to setup.
- Require a lot of maintenance



Factors Affecting Network Performance

Bandwidth
- The amount of data that the medium can transfer over a given period of time. Wired networks tend to have more bandwidth than wireless.
- The bandwidth at a Wireless Access Point is shared between all users of that point.
- Different types of traffic have different bandwidth requirements.
- Streaming video requires more bandwidth than sending an email.

Latency
- How long it takes a message to travel across the network.
- Low latency = few delays in transmission, High latency = many delays.
- More delays = longer transmissions.
- Affected by the number of devices on the network and the type of connection.
- Wireless networks usually have higher latency than wired.

Speed
- How fast data can be transferred over the network
- Usually faster for wired connections than wireless.
- Affected by the communication medium used.
- May also be affected by the distance the data must travel, with longer distances resulting in slower speed.

Range
- The physical distance a network can cover.
- Wireless is often used for short range communication.
- Wired is often used for longer distance communication.