PAN (Personal Area Network)

- Personal devices connected by Bluetooth
- Spread over a very small area.
- Used to connect personal devices e.g. smartphone and wireless headphones.
- Uses Bluetooth to connect devices.

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 is the biggest example of a WAN
- Can owned collectively by several organisations, for instance a group of schools

Wireless Networking

- Using radio signals or infrared light to connect devices in a network together.

Advantages	Disadvantages
• Devices can easily be added • Users can move around freely and stay connected	• 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 (WAP) only has so much bandwidth. • Signals can be intercepted by unauthorised users.

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.
- Copper cable is cheaper and easier to work with.

Advantages	Disadvantages
• Faster data transfer • Less likely to suffer from interference • More difficult for data to be intercepted	• Expensive to install or reconfigure • Harder to move devices so less flexible

Email Protocols

- SMTP – Simple Mail Transfer Protocol – used to send email.
- IMAP – Internet Message Access Protocol – controls the download of emails from an email server into an email client application.

Unit 5: Fundamentals of Computer 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.

4) Application Layer

- Encodes and decodes messages.
- Where applications such as browser and email clients operate.
- HTTP, HTTPS, SMTP, IMAP and FTP protocols operate at this layer

3) Transport layer

- Manages the communication between hosts.
- Breaks data down into packets.
- Hosts will agree settings such as the language and size of packets.
- TCP and UDP protocols operate at this layer.

2) Internet layer

- Adds the sender and recipient IP address and transmits the message.
- Routes packets across the network.
- IP Protocol operates at this layer

1) Data link layer

- Provides physical transfer of packets over the network.
- NIC (Network Interface Card) is at this layer
- OS device drivers are at this layer.

Network Security Measures
Encryption

- Turning data into an unreadable format , requiring a key to decrypt it and make it readable again.
- This means that if the data is stolen it cannot be read without the key.
- Data can be encrypted before being sent over a network or when stored.
- Encryption is often used alongside authentication by requiring a username and password to decrypt data and access the key.

Authentication

- Ways to make sure a user is who they say they are.
- Examples include passwords, security dongles and biometric such as fingerprints.
- The most basic security feature and widely used.
- Different levels of authentication are used depending on the security level needed.
- Secure systems require two-factor authentication is now needed, which requires two forms of authentication, such as a fingerprint and password.
- Allows the use of access rights to grant different users access to different systems or areas of a network.

Firewall

- Monitors traffic going into and out of the network, and either allows or blocks it.
- A barrier between trusted and untrusted networks.
- 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.

MAC Address Filtering

- All network adapters have a unique physical address known as a MAC Address.
- This address cannot be changed and allows individual devices on a network to be identified easily.
- Different devices can be blocked or allowed to connect to a network.

Network Protocols

Ethernet

- A family of related protocols which cover how data is sent on wired networks. It is not a single protocol. The protocols include how the hardware is managed, how data is sent and received and how data collisions are handled.

Wi-Fi

- A family of protocols which cover how data is sent through wireless connections. Wi-Fi is a trademark, the generic term for these networks is WLAN. Any device with the Wi-Fi logo uses the Wi-Fi protocols.

TCP - Transmission Control Protocol

- Controls the sending of data.
- Data is broken down into packets which are addressed and tracked through the network to make sure that they arrive at their destination.
- Any packets which don't arrive are resent.
- TCP is more reliable and more widely used than UDP.

UDP – User Diagram Protocol

- Controls the sending of data however but without any tracking.
- Everything is sent once, data which is lost is not resent.
- UDP it is a lot quicker than TCP and is often used in live streams where quality is less important than speed.

IP – Internet Protocol

- Manages the addressing of packets.
- Adds the sender and receiver IP addresses to each packet.
- Works alongside TCP to make sure data is sent securely across The Internet.

HTTP – Hypertext Transfer Protocol

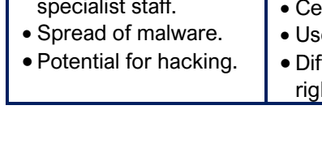
- Responsible for transferring web pages.
- Indicated by http:// at the start of a web address.

HTTPS - Hypertext Transfer Protocol (Secure)

- An encrypted version of HTTP.
- Should be used for websites which send sensitive data such as payment details or passwords.
- Indicated by https:// at the start of a web address.

FTP – File Transfer Protocol - transmission of files across a network and The Internet.

Bus Network



All devices are connected to a single cable (called the bus)

- A terminator is at each end of the cable.

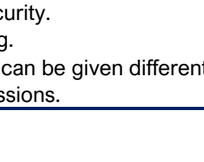
Advantages:

- 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, where a Wireless Access Point or WAP will be the central connection

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.

Networks

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