

Definitions:

LAN: Local Area Network A network of computers and devices, over a single site like a school, where the organisation uses its own cable, it doesn't use third party carriers

WAN: Wide Area Network A network over a wide geographical area, town to town, that uses third party carriers such as cable provided telecommunication companies (BT etc.)

Protocol: A rule or set of rules that govern how data is transmitted over a network.

Networking Advantages:

1 Allows for sharing of resources, printers, internet connections, etc.

2 Improves communication, offers more ways of communication, to multiple locations at once.

Networking Disadvantages:

1 Expensive as additional equipment is often necessary and it can be complex to set up.

2 Connecting to other devices can lower security, as it opens up another channel to your device, viruses can spread more easily.

Hardware Definition & Purpose:

NIC: Network Interface Card—provides device identity and connects device to network.

Switch: Receives and forwards data packets, to specific devices using the device MAC address (intelligent). Sits at the center of a LAN Star topology. Expensive but secure data transmission

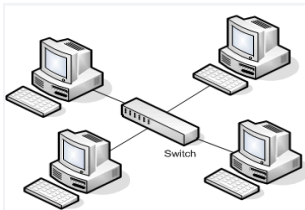
Hub: Receives and forwards data packets, broadcasts to all devices (unintelligent). Sits at the center of a LAN Star topology. Cheap but less secure data transmission

Router: Receives and forwards data packets, to specific networks using the IP address. Sends data down the least congested path. Found on WAN networks like the Internet.

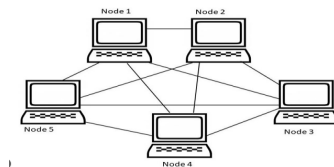
WAP: Wireless Access Point—connects wireless devices to networks.

Twisted Pair: a pair of copper cables twisted together, wrapped in insulation. Data transmitted as electric pulses.

Fibre Optic: a thin glass core (size of human hair) wrapped in insulation. Data transmitted as light. Fast but expensive.

Topologies:**Star Diagram:**

- + Fast and reliable connections as it uses Ethernet connections (wires)
- + Central maintenance and backup is easier due to use of servers
- Expensive to install due to additional equipment and cabling needed
- Central point of failure as STAR topologies use Switches or hubs at their center. If it fails everything stops.

Mesh Diagram:

- + Cheap and easy to set up as they use wireless connections (wifi/bluetooth)
- + No central point of failure, as MESH topologies do not use Switches or hubs
- Slow and unreliable connections as wifi is less reliable than ethernet
- Less secure than Star topologies as Mesh devices are connected to all other devices, hack the device and you have access to all the others.

IP Address: Specifies the location of a device. Provided by the network the device connects to, so it changes as you move from place to place. Made up of denary values separated by dots, each denary value ranges from 0 to 255.

192.168.1

MAC Address: Specifies the identity of a device used on a network. Provided by the device NIC. It doesn't change. Made up of hexadecimal values between 0 and F, separated by colons.

00:1b:63:84:45:e6

DNS Description:

Domain Name System—converts URLs (web addresses) into IP addresses so websites can be found on the Internet.

+ Useful as humans can't easily remember IP addresses but can easily remember catchy website URL addresses.

+ IP addresses change, but URLs stay the same, meaning humans still use the same URL no matter what IP a website has once it has moved to a new location on the Internet.

Competencies:

- I can differentiate between LANs & WANs ☐
- I can state advantages & disadvantages of Star and Mesh topologies ☐
- I can describe Ethernet media types ☐
- I can describe IP and MAC addresses ☐
- I can describe network hardware devices ☐
- I can state what DNS is and why it is useful ☐
- I know why networking is good and bad ☐

Layers:

Network communication is divided by functionality into layers. Each layer is self contained. It serves the layer above it and depends on all the layers below it. See packet switching process below as each of the first 4 steps uses layers, eg: TCP, then IP etc.

Benefits of layers:

Developers can focus in one area of the network

Layers can be changed without affecting other layers.

Standards:

A set of agreed requirements for hardware and software that allows different manufacturers to make compatible products. For example the producers of Ethernet Cables, produce the cable so that it will meet network speed and compatibility standards, users expect cable

Packet Switching:

Process & Layers:

- 1 Application layer—provides software for message creation
- 2 TCP layer—breaks message into packets, adds serial numbers
- 3 IP layer—addresses packets with to/from IP addresses, error checks
- 4 Hardware layers—converts packets for sending over network/BT
- 5 Router stage—routers receive and send packet on, using IP addresses down least congested paths
- 6 Receiving stage—reversal of steps 1-4, error checks take place

Definitions:

HTTPS: HyperText Transfer Protocol Secure—Secure is Asymmetrical Encryption, rules for sending data between browsers and web servers.

FTP: File Transfer Protocol—rules for sending files between servers

POP3: Post Office Protocol—(old) receiving emails, downloading from webserver to your local computer.

IMAP: Internet Message Access Protocol—(new) viewing emails online

SMTP: Simple Mail Transfer Protocol—sending emails via web servers

TCP/IP: Rules for sending data across a network (TCP breaking messages into packets)

The Cloud:

Data warehouses full of hard drives and switches

+ access from anywhere with internet connection

+ Unlimited space / auto backup

- Costs money / subscription

- hackable / needs internet

Network Threats:**Social Engineering:**

Gaining access to networks or data by using humans as the weak security point. Shoulder surfing and Phishing are two examples. Tricking people into revealing security information.

Technological:

Man in the middle (Data interception)

Brute Force (Guessing password combinations)

DDOS (Distributed denial of service), flooding servers with requests to block normal network traffic.

Malware (Worms, Viruses, Ransomware, etc) software based attacks.

Network Threats: Prevention

Passwords (Long, mix of symbols, cases etc)

Encryption (scrambling data into codes using algorithms)

User Access Levels (Using log on details to limit access to network resources, also Permissions that limit what can be done, read/write/execute, once access is granted)

Anti-Malware (Software based security)

Firewalls (data interception and rejection based on IP addresses or keywords)

Penetration Testing (Ethical hacking) to check for leaks in security and to patch them.

SQL Injection:

Using web form input boxes to enter SQL commands to access SQL databases to extract information.

Keywords & Wildcard:

Select, From, Where *

Client Server vs PSP

Clients request data from Servers, Servers grant requests (think browser requesting web pages, also most LANs have servers so uses Client Server, like at school)

P2P— No server, all devices equal access (like a Mesh topology). P2P easy to set up and cheap.