Networking

Network – Devices connected to each other to share information.

Local area network (LAN) = Small, covers limited area. Used in homes

Wide area network (WAN) = Larger, connects multiple LANs, covers cities, countries. E.g Internet

Switch – Connects devices together. Ensures data flows smoothly within LAN.

Router – Directs traffic between different networks. Also connects different networks. E.g computer to internet.

Firewall = Protects networks from unauthorised access. Monitors and controls network traffic.

IP (internet protocol) address = Unique ID for devices on a network. Allows devices to identify and communicate.

2 types: IPv4 and IPv6

IPv4 is limited. IPv6 provides more addresses and has improved security features.

IPv4 = 4 groups x 8 bits = 32 bits total Range= 0-255

IPv6 = 16 group x 8 bits – 128 bits total Range = 0 - 65,535

MAC (media access control) address = Unique hardware-based ID for devices. Operates at data link layer of OSI model. 48 bits

Ports & Protocols

Port = Logical endpoints for communication.

Port for HTTP = 80

Port for HTTPS = 443

Protocols = Rules governing data transmission. Ensures data gets to the right app on your device.

2 main protocols: TCP and UDP

Transmission control protocol (TCP) = Connection-oriented. Ensure all data is delivered correctly and in the right order. Uses include sending files, emails, web.

User datagram protocol (UDP) = Connectionless. Fast but less reliable. Not all data might be sent. Uses include online gaming, streaming, VPNs, DNS.

Open systems interconnection (OSI) model – Conceptual framework that standardises how devices communicate over a network.

7 layers:

1. Application
2. Presentation
3. Session
4. Transport
5. Network
6. Data link
7. Physical

Physical layer – Transmits raw data over a physical medium. E.g cables, signals, hardware.

Data link layer – Ensures data is transferred correctly between network nodes using MAC addresses on a single LAN. E.g ethernet, wi-fi, NIC address

Network layer – Handles logical addressing (IP) and routing across different networks. E.g IP address, routers.

Transport layer – Ensure data is delivered reliably OR quickly using ports. E.g TCP and UDP

Session layer – Established, manages and terminates sessions between apps. E.g NetBIOS

Presentation layer – Translates data so applications can understand it. E.g JPEG, MP3

Application layer – Closest to the user. The applications they use. E.g HTTPS, SSH, DNS

TCP/IP model

1. Application layer
2. Transport layer
3. Internet layer
4. Network access layer

Domain name system (DNS) – Translates human-readable domain names into IP addresses so computers know where to send requests.

DNS components: Nameservers and zone files

Nameservers – Tells the internet where to find your website by mapping your domain name to the right IP address.

2 types: Authoritative and recursive

Authoritative nameservers =Holds DNS records

Recursive nameserver = Queries other nameservers to find the DNS record. Caches info to speed up future queries.

dig ns website.com or dig ns +short website.com = How to find nameservers of a domain

Zone files = File stored on authoritative nameservers that defines all the DNS record for the domain, telling the internet where to find your website.

DNS components: records: Instructions inside a zone file telling the internet how your domain behaves (where to find the website, emails etc). E.g A and AAAA

A records = Maps domain to IPv4 address

AAAA records = Maps domain to IPv6 address

CNAME records = Alias pointing back to main domain

Mail exchange (MX) records = Points to your mail server. Makes email delivery reliable/

TXT records = Stores extra info about domain. Used for security and verification.

How DNS works

DNS resolution = Turns domain names into IP addresses.

DNS hierarchy

1. Root level = points query to the TLD server e.g .com servers
2. Top-level domains (TLDs) = Handles domains under a specific extension such as .com, .org, .net.
3. Second level domains (Authoritative nameservers) = Final source of truth for a domain. Contains all DNS records.
4. Subdomains/hostnames

Domain registrar = A company where you buy your domain name

DNS hosting provider = The company that stores and serves your DNS records

nslookup = Name server lookup. Shows IP address and can show MX record.

dig [ domain ] =Domain information groper. More detailed than lookup.

/etc/hosts file = Local file on computer. Maps domains to IP addresses. Checked before DNS.

How to map domain to local host:

1. nano /etc/hosts
2. Add IP address with website. Save and exit.
3. Flush DNS resolver cache

Routing – Process of finding best paths for data to travel across networks

Routing tables – A GPS for network traffic. Tells every packet the way to reach the IP address.

Importance of routing:

1. Network performance optimisation – reduces latency
2. Ensure reliable application delivery
3. Crucial for managing complex infrastructures

Static vs dynamic routing

Static = Manually configured fixed routes. Do not change unless manually updated by network admin. Great for small, stable networks.

Dynamic routing = Routes are automatically adjusted. Uses routing protocols to find the best path. Scalable and adaptable for large, complex networks.

Routing protocols = Automates best path for data to travel across the network. Uses algorithms that determines the best path.

2 common routing protocols: OSPF and BGP

Open shortest path first (OSPF) = Each router builds its own map and picks the fastest path.

Border gateway protocol (BGP) = Chooses path based on reliability, policies and money agreements.

Subnetting = Dividing a network into smaller networks.

CIDR = Classless inter-domain routing. Writes and manages IP address with a prefix length.

Format = IP address/prefix length

Converting IP addresses into binary

IPv4 address consists of 4 octets. Each octet contains 8 bits.

E.g 192.168.1.1

Calculating subnets

Subnet masks = defines network and host portions

/24 = 24 network bits

Network address translation (NAT) – Lets multiple devices on the same network share one public IP on the internet.

Static NAT – Maps single private IP address to a single public IP address.

Dynamic NAT – Maps private IP address to a pool of public IP addresses.

Port address translation (PAT) = Many private IP addresses share one public IP address.

Network troubleshooting – identify and fix network issues

ping – Test connectivity between devices.

traceroute / tracert – Tracks path data takes to reach destination.

nslookup – Querying DNS to find IP address associated with domain name.