Chapter 21

A network is a collection of **two or more computers** that are connected together for the purpose of sharing resources and data

Why Are Networks Used

to read/write personal files on a central server

to **access shared files** among several users

to download data or updates to computer programs

to **send data to a shared printer**

to **access the Internet**

to **communicate with each other – email, message**

Types of Networks

local area network (LAN) a network that **covers** a relatively **small geographical** area,

wireless local area network (WLAN) **–** radio waves

wide area network (WAN) a network that **covers** a **large geographical** area

personal area network (PAN) network used for data transmission over short distances **– Bluetooth**

Two main models of computer networks

client-server and peer-to-peer

CLIENT-SERVER

In a client-server network there is **at least one server**, which is a **powerful computer** that provides a service or services to the network. **Individual computers** (such as the ones in a typical school computer room) are referred to as the **client computers**. The server will **authenticate the user** (explained later in the unit) and then give the **user access to the files** that he/she has been given permission to access. The server provides services to the clients as required.

A client accesses data or files from a server using the following process:

1 A client will make a connection to the server using its address. The server will know the address of the client because this will be included in the request for a connection.

2 Once the connection has been made, the client will make a service request to the server.

3 If the request is valid, the server will send the requested data to the client using the address identified in step 1

peer-to-peer network can provide a service, such as share some files or provide access to a printer.

instant messaging systems use a peer-to-peer

no central server

lack of records also benefits those people worried about privacy

Network Topologies

four main network topologies - bus, ring, star and mesh

Bus

a single cable / terminator is to absorb signals / prevents them from bouncing back and causing interference

CSMA/CD - Carrier Sense Multiple Access with Collision Detection – check if bus is busy ...

A collision occurs when two or more network devices send a message at the same time, making all the messages unreadable.

ADVANTAGES AND DISADVANTAGES OF THE BUS TOPOLOGY

ADVANTAGES	DISADVANTAGES
Relatively cheap to install since only one cable is needed	Whole network will fail if the cable is cut or damaged
Easy to add extra network devices	Can be difficult to identify where a fault is on the cable
	The more devices that are added to a bus network the slower they run. This is due to only one message being able to be sent at once and because more collisions happen
	All data sent is received by all devices on the network; this is a security risk

Ring

A ring network is a network in which the **cable connects one network device to another in a closed loop**, or ring.

unlike a bus network, there are **no collisions**. Data is passed from one device to the next around the ring **until it reaches its destination**.

ADVANTAGES	DISADVANTAGES
Adding extra devices does not affect the performance of the network	Whole network will fail if the cable is cut or damaged or a device on the network fails
Easy to add extra network devices	Because all the devices in the network are connected in a closed loop, adding or removing a device involves shutting down the network temporarily
	Can be difficult to identify where a fault is on the network
	More expensive to install than a bus network as it requires more cable to complete the ring

Star

each network device is connected to a central point (hub or switch)

star topology is the most widely used

ADVANTAGES AND DISADVANTAGES OF THE STAR TOPOLOGY

ADVANTAGES	DISADVANTAGES
A damaged cable will not stop the whole network from working, just the network device connected to it	If the hub or switch fails, then the whole network will fail
If a switch is used, then the network is efficient as messages are only sent to devices needing them. This also adds to security as not all devices will see a message	Expensive to install due to amount of cable needed and the hub or switch
Easy to locate faults because they will normally only involve one device	
A new device can be added or removed without having to close the network down	

Mesh

There are **two main types** of mesh topology - fully connected and partially connected.

In a **fully connected mesh** network, every network device is connected to every other network device.

In a **partially connected mesh** network, some network devices may be connected to multiple other devices.

Mesh networks can be **wired or wireless**.

In a **wired** network, **very expensive** and **difficult** to implement

Wireless mesh networks don't have the same problems

Mesh networks are **very fault tolerant**.

If a **device or connection fails**, messages are **routed around it**

The **largest** mesh network of all is the **Internet**

ADVANTAGES	DISADVANTAGES
Very fault tolerant, especially in the case of a fully connected mesh network – if one device fails, messages can be re-routed	Difficult and expensive to install wired mesh networks
Very high performance because each network device is likely to be connected to multiple other devices	Can be difficult to manage due to number of connections within the network
In a wireless mesh network each node extends the range of the network	

Wire Vs Wireless

Wired connection methods involve a **physical connection** between the computer and the network

Most **wireless** connections transmit and receive **radio signals**

ADVANTAGES	DISADVANTAGES
Wired connectivity	
Faster than wireless connectivity	Expensive to install and reconfigure
Not easy to intercept or **eavesdrop** on data	Requires many cables at a premises
Less susceptible to interference than wireless connectivity	
Wireless connectivity	
No need for a cable to connect devices or to the Internet	Data transmission speeds can be slower than wired connectivity
Allows users to use their own device	Interference from other wireless devices can adversely affect performance
A wider range of devices can communicate with each other/a network because it is not dependent on having the correct cable	Walls and other physical objects can adversely affect performance
	Data needs to be encrypted (see Unit 3) to prevent eavesdropping or interception

*** communications medium is measured in **bits per second**

*** storage in **kilobytes**

*** Network Data speed = Mbps

*** Storage = MB

Protocol

a protocol is a set of rules that control how communications between devices are formatted and how these communications will be sent/received

A protocol might contain details of:

■how each computer will be **identified**

■what **route** the data will take to get to its destination

■how **errors** will be found and dealt with

■whether each part of a message should be acknowledged as received correctly

■what to do if **data isn't received correctly**

■how the data is to be **formatted**

■how the data is to be **sequenced**

■how the speed of the sender and receiver can be **synchronised**.

Email Protocol

PROTOCOL	DESCRIPTION
SMTP	Simple Mail Transfer Protocol. This protocol is used when sending email through the Internet. It details the format that messages are sent in, what commands email servers should understand and how they should respond to them.
POP3	Post Office Protocol, Version 3. POP3 is the current version of the Post Office Protocol that is used for retrieving email from an email server. Normally email clients using POP3 will connect to the mail server, download any messages and then delete the messages from the server.
IMAP	Internet Message Access Protocol. IMAP allows emails to be accessed using multiple email clients. For example, you might access your email using an email client on your computer, your tablet and your mobile phone. IMAP leaves messages on the server until you delete them. This means that no matter which email client you use, you should see an up-to-date list of your email messages.

Network Protocol

Ethernet is a family of protocols (protocol suit) used in **wired LANs**

physical parts of a network, such as **type of cable and type of connector** to be used,

logical parts, such as how data is **sent and checked** for errors and the speed that data can be transmitted.

TCP provides a reliable connection between computers

The data received is **identical** to the data sent

*** TCP/IP described as a 'protocol suite' rather than a 'protocol stack'.

These two terms are often used as if they are the same.

However, some sources state

that **the suite is the definition of the protocols** and

that **stack is the software implementation of the protocols.**

Table 5.1 TCP/IP Protocol Stack

LAYER	DESCRIPTION
Application	This is the top layer of the stack. It is the layer which interacts with the user to provide access to services and data that is sent/received over a network. Examples of protocols that work at this layer are HTTP, FTP and email protocols.
Transport	This layer manages end-to-end communication over a network. There are two main protocols that operate at this layer – TCP and UDP. (You only need to know about TCP for iGCSE Computer Science.)
Internet	This layer deals with sending data across multiple networks (possibly the Internet), from the source network to the destination network. This is known as routing and is the role of Internet protocol (IP).
Link	This layer controls the transmission and reception of data to/from a local network.

▲ **Table 5.1** The four layers of the TCP/IP protocol stack

Link Layer

This layer is **concerned with transmitting the data** through the local network using the protocols of the specific network, for example **Ethernet**. This is where the **network interface card (NIC)** and the device drivers of the operating system are located.

Checksum

checksum a technique for **finding errors**.

A mathematical formula is applied to the data

It then **compares the checksum**

If the **checksums don't match**, the data is likely to have been **corrupted**.

PROTOCOLS OF THE APPLICATION LAYER

FTP	File Transfer Protocol: the rules that must be followed when files are being transmitted between computers
HTTP	HyperText Transfer Protocol: the rules to be followed by a web server and a web browser when requesting and supplying information. HTTP is used for sending requests from a web client (a browser) to a web server and returning web content from the server back to the client
HTTPS	Secure HTTP: allows for communications between a host and client to be secure. It ensures that all communication between them is encrypted
SMTP	Simple Mail Transfer Protocol: the protocol for sending email messages from client to server and then from server to server until it reaches its destination
POP	Post Office Protocol: used by a client to retrieve emails from a mail server. All of the emails are downloaded when there is a connection between client and server
IMAP	Internet Message Access protocol: unlike POP, the messages do not have to be downloaded. They can be read and stored on the message server. This is better for users with many different devices. This is because they can be read from each other, rather than being downloaded to just one.

▲ **Table 5.2** Some of the protocols of the application layer

Packet

packet a small quantity of data being sent through a network

Data sent using TCP/IP is broken up **into packets**.

A packet **header** contains details of:

- the **sending computer**
- the **recipient computer**
- **how many packets** the data has been split into
- the **number of this particular packet**.

Benefits of Using Networking Layers

■ It makes the **overall model easier to understand** by dividing it into functional parts.

■ Each layer is **specialised to perform** a particular function.

■ The **different layers** can be combined in different ways.

■**One layer** can be developed or **changed without affecting** the other layers.

■It makes it **easier to identify and correct** networking **errors and problems**.

■It provides a **universal standard for hardware and software** manufacturers to follow

Mobile Communications

2G was the **first** to use digital communications / **text messages**

3G increased data transmission speeds to **2mbit/s.** It enabled video calls and downloading and streaming

4G provided much **higher speeds** / popularity of **mobile gaming**

5G, is smarter, faster / peak speeds of **100 Gbps**, 100 times faster than 4G

emerging technologies, such as driverless cars

Chapter 22

NETWORK SECURITY AND ITS IMPORTANCE

Network security covers a wide range of activities that protect data from threats to its **confidentiality**, **correctness** (integrity) and **availability**

1. CONFIDENTIALITY - organisation's computer system often holds data
2. CORRECTNESS - Data is useless unless it is correct.
3. AVAILABILITY - A network is useless if data cannot be accessed when it is needed - DoS

REASONS WHY SECURITY IS IMPORTANT

- required for the running of the organization
- private and confidential
- financially valuable

AUTHENTICATION AND VALIDATION - OQ

Authentication is the process of checking the identity of a user of a computer system or network.

This is often done by validating a username and password against details stored on a central server.

Authentication exist using a PIN fingerprint recognition

Two-factor authentication a *security check* where users have to *type in the code* from a portable hardware device called a 'secure token' or from an *SMS message sent* to their mobile phone

Access control this *decides which users have access to which data*, and what they are allowed to do with it

Many different ways to help secure a network

1. access control,
2. firewalls and
3. physical security.

Access Control

Access control is the **method that controls** whether a particular user will gain access to a particular file.

■ **read-only access** - in this case, the user can **open the file and read its** contents, but not modify the contents or delete the file

■ **read and write access** (modify access) - in this case, the user can **read the file, alter** the contents and then **save** the changes.

Access controls are set up by an organisation's system **administrators**

Firewall

Firewall **sits between the Internet** and the **local internal network**

A firewall **inspects incoming and outgoing data** and uses a set of rules

Rules decide whether to **allow** the data **or not**

Firewall can **customise** the rules

Some examples -

1. stop certain protocols
2. block data coming from or going to certain network addresses
3. stop attempts at hacking the internal network's servers

Firewall can be **software or hardware**

Software firewall installed with some default rules to protect your computer

Business have a **Hardware**- based firewall

Physical security

protecting against locking down theft of equipment / installing a burglar alarm

Electronic lock systems

Entry/exit times can be recorded

CCTV / Biometric

Contemporary Storage and Security (NAS / USB)

NAS

One recently developed system is **network-attached storage** (NAS).

NAS is a **hardware** device

NAS device designed for **home** use could consist of a **single** hard drive

organisation's NAS device consists of **many hard** drives

For **ease of use** rather than being secure

Once a NAS is connected to the Internet it becomes possible for it to be hacked remotely.

Home users often make **mistakes** such as:

- not changing a device's **default password**.
- not updating the **software** running on the NAS

USB

Another widely used storage device is the USB flash drive

USB flash drives are **easy to transport / cheap / very convenient**

Disadvantage is can **find a lost** flash drive and **access** the information /

encrypted USB flash drives are available

Cyber Attack

A cyber-attack is any kind of electronic attack on a computer system, server, network or other IT device.

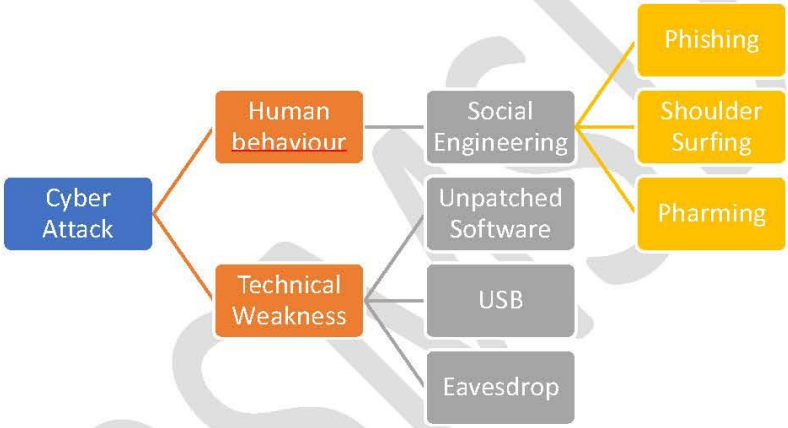
These attacks might be designed to:

■gain access to data

■delete or modify information

■make the system unavailable for use

■physically damage a device



Social Engineering

Attacks that rely on **exploiting human behaviour**

Three common forms - **phishing, shoulder surfing and pharming**

Phishing

A phishing attack is **an attempt to get sensitive, confidential information** such as bank account or credit card

Various forms of phishing - **email** or fake websites

Start with an email

Once the user clicks on a link within the email, a website that looks and acts like the **real website will open.**

when the user **enters** his or her **login** details / they are **passed to the attacker**

Shoulder surfing

gaining access to confidential information **by directly observing a user**, possibly literally looking over their shoulder

Often shoulder surfing happens in **busy** places

Shoulder surfer stands near the cash machine and **sees the user** enter his or her **PIN**

Once the **PIN has been seen**, the **card is stolen**.

The card and PIN can then be used to **withdraw cash**

Pharming

domain names are used to represent IP addresses.

translated back into the IP address by the domain name service (DNS)

If we **have visited** the site before, then this **IP address will be stored on our computer** (in the DNS cache).

The browser will connect **without using the DNS**

receive malware in an email that can change the **IP address of the domain name to a bogus** (fake) one

Malware can also infect the DNS servers / everybody is **directed to the bogus site**

Technical Weaknesses

Unpatched Software

Software is very **complicated** and usually security issues are only found

software **remains vulnerable** (weak).

patches to fix the security issues

USB flash drives

security threat because it **contains malware**

Eavesdropping

means intercepting data being sent to/from another computer system.

person can **eavesdrop on a conversation** without the speakers knowing about it

without actually copying or stealing

Protecting Against Security Weaknesses

*** Security must be considered – design stage - software is to be as safe as possible against cyber attack

Design Stage

Authentication / different users need different levels of access

warnings be issued before allowing users

stored data need to be encrypted

threats will the software face

bad programming practice

write poor quality code and don't consider how safe or secure

pressure might make even a good programmer take shortcuts to meet deadlines.

Two main Types of Code Review

Review by **another** programmer – senior programmer

An automated review - software

Combination of both types

Other Security Measures to Protect from Cyber Attacks

Use an audit trail - a record of activities that have taken place on a computer system

Use secure operating systems - much harder to attack

Provide effective network security - Well-educated technical staff

IDENTIFYING VULNERABILITIES

Ethical hacking

relates to cybersecurity and preventing cyber attacks

'good' hacking - it is looking for weaknesses in software and systems

vulnerabilities can be identified

Once a vulnerability has been found, steps to remove or reduce its impact can be taken.

Penetration testing

to find any weaknesses.

authorised by the organisation and are therefore legal

attacks might be run by employees of the organisation

The pen tester

to gain access to all the systems

looking for technical weaknesses and trying social engineering methods.

pen testing has been completed; a report is usually presented to a senior manager within the organization

Commercial Analysis Tools

use software tools to scan a system for vulnerabilities

vulnerability scanners can be either purchased or hired

look for common issues and alert the user to them.

scan the network from within (internally) or from outside (externally).

Reviews of Network and User Policies

Network Policies

organisation's rules on the use of the network

who is authorised to carry out various activities

how and when patches to software should be applied

access controls

password requirements

security is set up and maintained

what data audit trails should collect

security and maintenance of the network

User Policies

what use of the network is allowed or not allowed

how to report faults, problems and security

Any policies relating to the network should be regularly reviewed

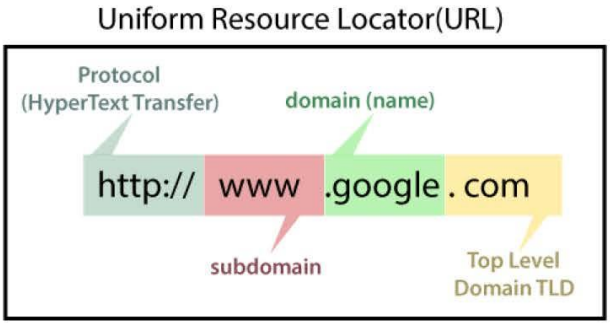
Chapter 23

Internet and WWW

Internet - 'interconnected networks / network of networks / global network / biggest WAN

One of the **services** provided by the **Internet** is the **World Wide Web** (WWW)

The World Wide Web is a **service that runs** on the Internet.



DOMAIN NAME SERVICE (DNS)

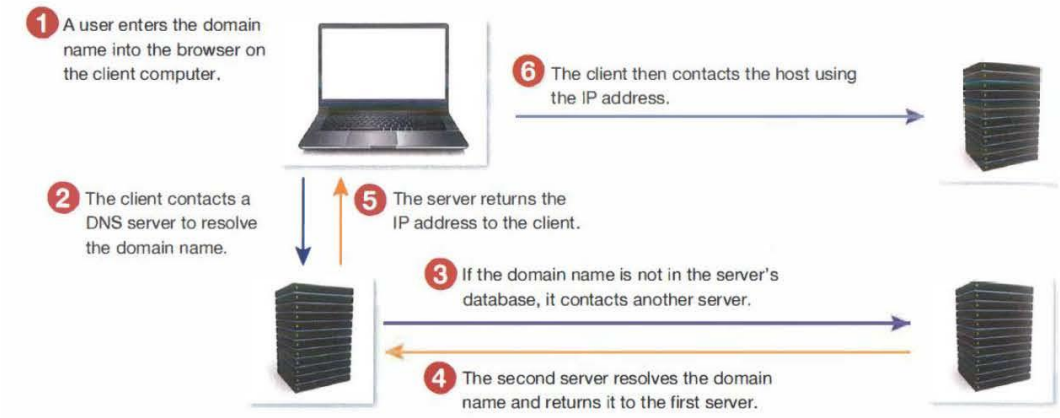
translates domain names into IP addresses

domain names are alphabetical, they're easier to remember

Every time a user **enters** a domain name, (DNS) must **translate** the **name** into the corresponding **IP address**

network is likely to be connected to the **Internet** using **an Internet service provider (ISP)**

ISP is an **organisation** that **provides Internet** connections



▲ **Figure 5.8** Domain name service (DNS)

The **networks** that are a part of the Internet are **linked together** using **routers**.

Router is a piece of networking **hardware** that **forwards packets** between **networks**.

When an Internet-connected computer wants to send data to another whose IP address it already knows the following happens.

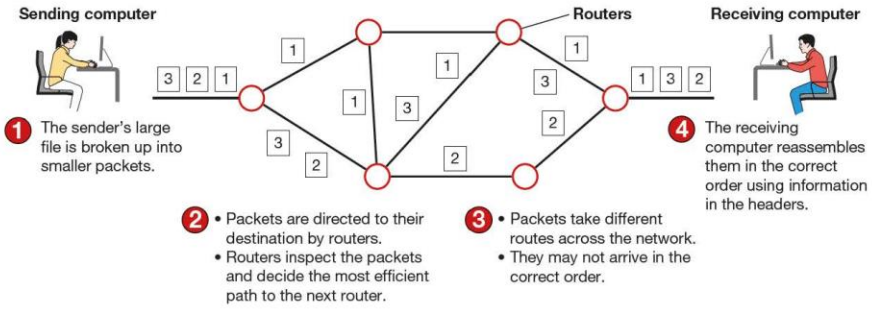
1. The **sending** computer **splits** the **data** into **packets**.
2. Each **packet has a header** that contains the **sender's address**, the **destination address**, the **current packet number** and the **total number of packets** that make up the data.
3. Each **packet** is **sent to** your **ISP**.
4. Your **ISP** will have a **router**. This router will **inspect the packet header** and **decide where** to send the packet **depending on its destination IP** address.
5. The **packet** is likely to **end up at another router**, which will again look at the destination IP address and forward it on. This can **happen many times** before the packet reaches its destination network and intended recipient.
6. **Once a packet reaches its destination**, the receiving computer will put the data back together from the packets. Depending on the protocol being used, the **packets might arrive in the wrong order** and have to be **put back in order** using the information in the packet header.

The **Internet** has **many different services** running on top of it. **Email and the World Wide Web** are two of the most commonly used services to which the Internet provides access.

Services that use the WWW include messaging, file sharing, video conferencing, e-commerce, media streaming, video gaming, cloud storage, health monitoring, the Internet of things.

ACTIVITY 15

1 The diagram should illustrate the process described on pages 233 & 234.



2 The Internet is a mesh network. Mesh networks were discussed earlier in this chapter on pages 209 & 210, including what makes them so fault tolerant.

Internet Protocol (IP) - provides each device or network connected to the Internet with a **unique address**

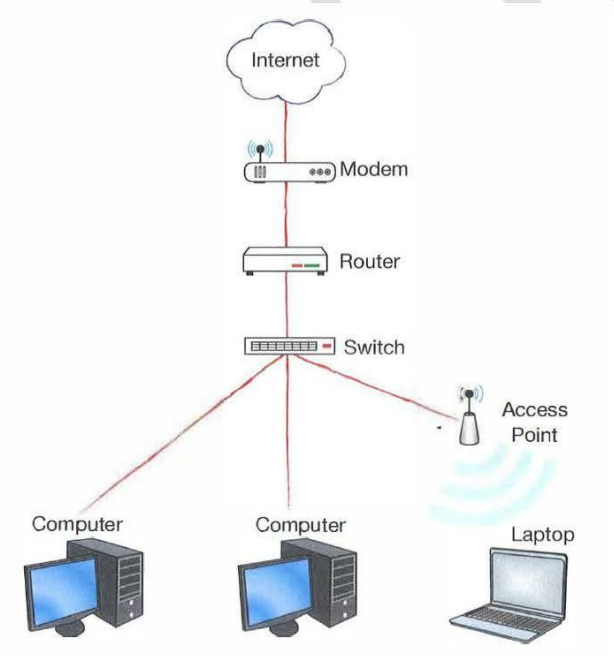
two versions of IP – IPv4 and IPv6

IPv4	**IPv6**
32 bits	128 bits
4 group – 8 bits (0 – 255) 192.168.100.100	8 group – 16 bits (0 – F) 2001:cdba:0000:0000:0000:0000:3257:9652
Dotted Decimal Notation 192.168.1.1	Colon Hexadecimal Notation 2001:cdba:0000:0000:0000:0000:3257:9652
2^32=4294967296 4.3 billion addresses	2^128=3.4028236692094E+38 340 trillion-trillion-trillion addresses

IPv6 was introduced so that **more addresses would be available.**

IPv6 uses 128 bits to create a single unique address on the network.

COMPONENTS NEEDED TO ACCESS THE INTERNET



Switch

used to **link the computers**

messages can be transmitted from one to the other

Switches are 'intelligent'

it can read the destination addresses / send them to only the intended computers

Because they build up a table of all of the addresses

Wireless access points

Allow wireless devices to connect to a wired network using Wi-Fi.

convert data they receive through **cables** into a wireless **signal** and vice versa.

Internet hotspots - similar to switches but cannot direct messages

Routers

are similar to switches – used to **link the several networks**

A **switch** does this within a **single network**, but a **router** does this **across several networks**.

Routers are commonly used in the home / share an Internet connection

Routers can have both cable and Wi-Fi connections.

Modem – Modulator Demodulator

convert the signals in a LAN,

into signals that can be transmitted along the cables provided by the Internet Service Provider (ISP).

type of modem required - depend on the type of cable to the ISP

copper telephone line or cable, carrying electrical signals

fibre-optic cable, carries the signals as light.

Modems are usually combined with routers in a single box as an Internet router