GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols: *Types of Networks*

Key Terminology	BCS Definition
LAN	**Local Area Network:** “Small geographic area. All hardware is owned by the organisation using it. Wired with UTP or fibre optic cable or wireless using routers and Wi-Fi access points.”
WAN	Wide Area Network: “Large geographic area. Infrastructure is hired from telecommunication companies who own and manage it. Connected with telephone lines, fibre optic cables or satellite links.”
Transmission media	“Physical media that can be used to transmit data – e.g., twisted copper cable, fibre optic, etc.”

Thanks to networking technology, we can:

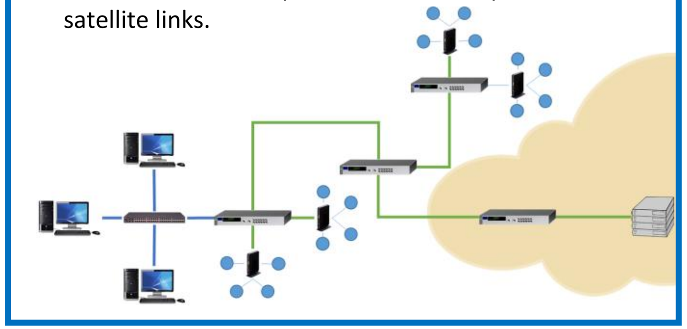
- Transfer files quickly and easily.
- Share peripherals and internet connections.
- Access files from any computer on a network.
- Control security, software updates and backups via a server.
- Communicate with each other via email and social media.

However, networking does have its drawbacks:

- Increased security risk to data.
- Malware and viruses can spread very easily between computers.
- If a server fails, the computers connected to it may not work.
- Computers may run slower if there is a lot of data travelling on the network.

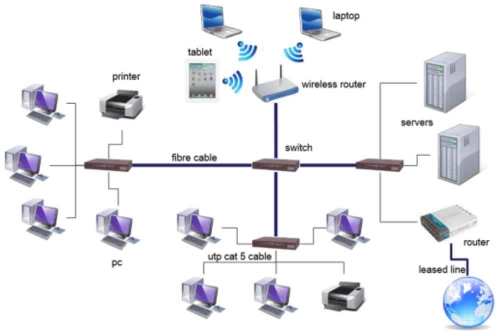
WAN (Wide Area Network)

- Connects LANs together over a large geographical area.
- Infrastructure is leased from telecommunication companies who own and manage it.
- Connected with telephone lines, fibre optic cables or satellite links.



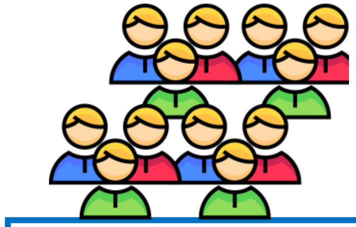
LAN (Local Area Network)

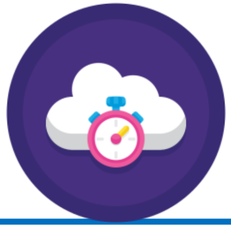
- Covers a single site within a small geographical area.
- All the hardware is owned by the organisation using it.
- Wired with UTP or fibre optic cable or wireless using Wi-Fi.

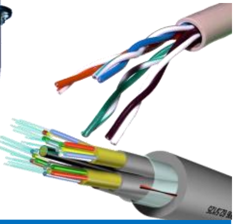


Routers for personal, home use tend to be multi-function, all-in-one devices that act as the:

- Switch
- Router
- Wireless access point







Factors that affect the performance of networks

Bandwidth

- The amount of data that can be sent and received successfully in a specified period of time.
- Not a measure of how fast data travels but how much data can be sent via transmission media.
- Measured in bits per second, often called bit rate.

Numbers of users

- Too many users or devices on the same network can cause it to slow down if there is insufficient bandwidth available.

Transmission media

- Wired connections offer higher bandwidth than wireless connections.
- Fibre optic cables offer higher bandwidth than copper cables.

Error rate

- Less reliable connections increase the occurrence of errors during data transfer.
- Data must be resent until it arrives correctly.
- The quality of a wireless connections depends on the device’s distance from the wireless access point and other environmental factors.
- The quality of the signal provided by copper cables is determined by the grade of the material used – higher-quality cables help to reduce interference.
- The length of the cable is also a factor.

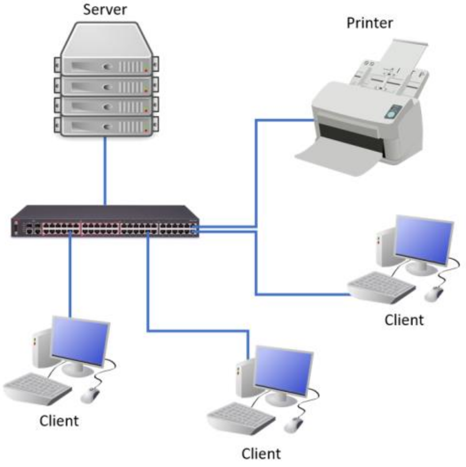
Latency

- The delay between data being transmitted and a user’s device receiving it, latency is caused by bottlenecks in network infrastructure.
- For example, not using switches to appropriately segment network traffic.
- Various pieces of hardware like switches and cables may not operate at the same speed.

GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols:
Client-Server vs Peer-to-peer

Client-server model

- A server controls access and security to one shared file store.
- A server manages access to The Internet.
- A server manages printing jobs.
- A server provides email services.
- A server runs a backup of data.
- A client makes requests to the server for data and connections.

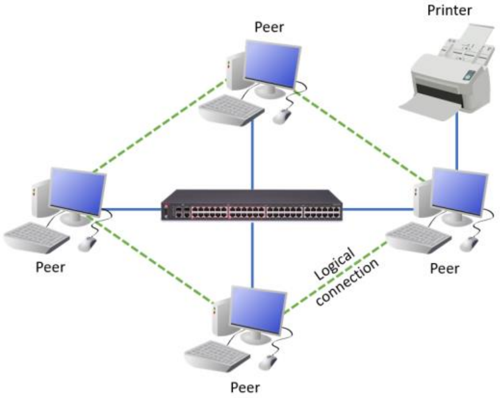


Advantages	Disadvantages
Easier to manage security files.	Can be expensive to setup and maintain.
Easier to take backups of all shared data.	Requires IT specialists to maintain.
Easier to install software updates to all computers.	The server is a single point of failure.
	Users will lose access if the server fails.

Key Terminology	BCS Definition
Client-server network	"A client makes requests to the server for data and connections. A server controls access and security to one shared file store. A server manages access to the internet, shared printers and email services, as well as running data backups."
Peer-to-peer network	"All computers are equal and serve their own files to each other. Each computer is responsible for its own security and backups and usually has its own printer."

Peer-to-peer model

- A peer is a computer on a network, and is equal to all other peers.
- Peers serve their own files to each other.
- Each peer is responsible for its own security.
- Each peer is responsible for its own backup.
- Peers usually have their own printers.
- You can send print jobs to another peer to process, but that peer would need to be switched on to be able to communicate with the connected printer.



Advantages	Disadvantages
Very easy to maintain.	The network is less secure.
Specialist staff are not required.	Users will need to manage their own backups.
No dependency on a single computer.	Can be difficult to maintain a well ordered file store.
Cheaper to set up.	
No expensive hardware required.	

GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols:
Hardware to connect a LAN

Key Terminology	BCS Definition
Wireless access point	"Hardware that allows a Wi-Fi-enabled device to connect to a network."
Router	"A router sends data between networks. It is needed to connect a local area network to a wide area network. It uses the IP address on a device to route traffic to other routers."
Switch	"A switch sends data between computers on a local area network. It uses the NIC address on a device to route traffic."
NIC	**Network Interface Card/Controller:** "Hardware that connects a computer to a network."
Transmission media	"Physical media that can be used to transmit data – e.g., twisted copper cable, fibre optic, etc."

Network interface card / controller

- Every computer connecting to a network will need one of these.
- These days they are not physically separate cards, they are integrated.
- They use a protocol (a set of rules) to determine how the connection should work.
- They allow a device to connect to either a wired or wireless network.

Wireless access point

- Allows wireless enabled devices to connect to a network without cables.
- More convenient.
- They have less bandwidth than a wired connection.
- Security is more of a concern with wireless connections.
- Connection is sometimes not as strong or reliable as wired connections.

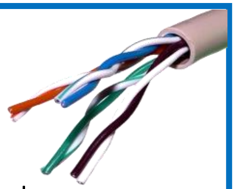
Switch

- Sends data between computers on a LAN.
- They segment the network by forwarding traffic to the correct location.
- Switches learn which devices are connected and understand how to forward traffic in an intelligent way.

Router

- Sends data between networks.
- It creates a WAN from a number of LANs.
- You cannot connect to a WAN without using a router.
- A router uses an IP address (Internet Protocol) to route traffic.

Transmission media:



- **Copper cables (UTP)**
  - Wired connections assure maximum bandwidth, security and reliability.
  - With twisted pair cables the wires are twisted around each other to reduce interference.
  - Normally a set of wires for transmission and receiving.
  - The grade of copper and insulating material affects the quality of the overall cable and therefore the bandwidth.
- **Fibre optic cables**
  - Uses light to transmit data.
  - Cover much longer distances and greater bandwidth than copper.
  - The backbone of The Internet uses fibre optic cables.

GCSE Computer Science Knowledge Organiser
SLR1.3 Computer networks, connections and protocols
The Internet: What is the internet? & The cloud

Key Terminology	BCS Definition
The internet	"A worldwide collection of interconnected computer networks. An example of a WAN – the largest in existence."
The cloud	"Remote servers that store data to be accessed over the internet. Access anytime, anywhere from any device. Automatic backups. Collaborate on files easily."

The internet

- Largest and most well-known Wide Area Network (WAN).
- A collection of interconnected networks spanning the world.
- Not the same as the World Wide Web, which is just a service on the internet.

The cloud

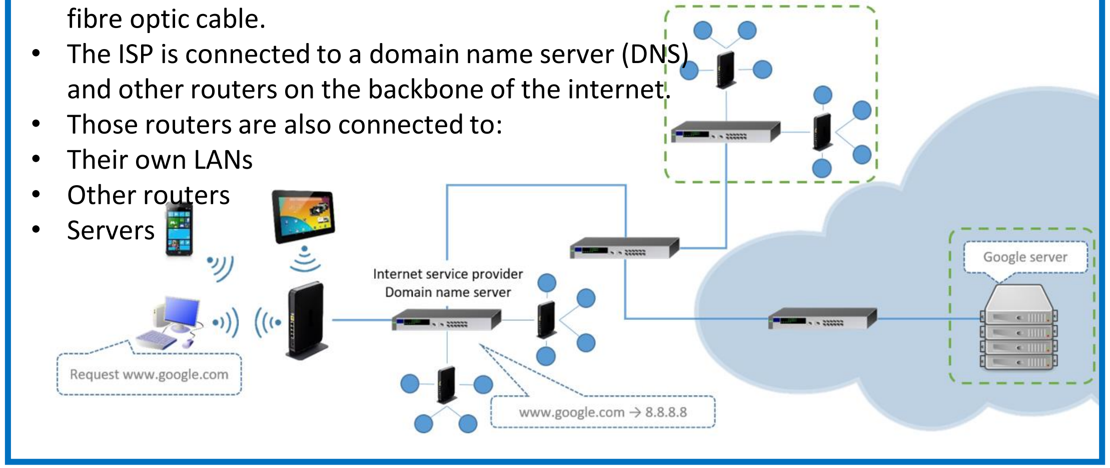
Servers can be used to store data and programs that can be accessed over the internet – this is known as the cloud.

Advantages of the cloud

- Access anytime, anywhere, from any device
- Large storage capacity
- Automatic backup
- Easy collaboration

Internet Structure

- Here is a home network connected via a typical wireless router.
- The router is connected to an internet service provider (ISP), typically via a telephone connection or fibre optic cable.
- The ISP is connected to a domain name server (DNS) and other routers on the backbone of the internet.
- Those routers are also connected to:
- Their own LANs
- Other routers
- Servers



Summary

The internet is a global collection of interconnected networks.

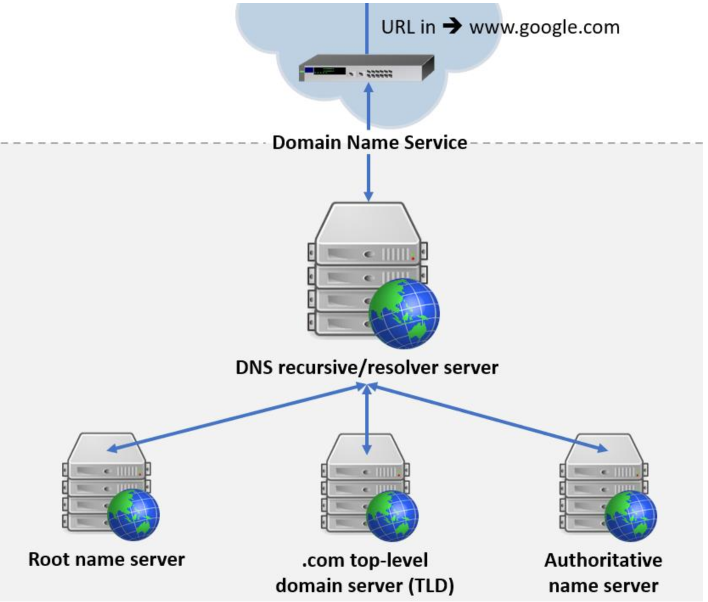
- Web addresses – that are easier for humans to remember – are converted to IP by a DNS resolver server.
- This process is carried out by the Domain Name Service, which is made up of multiple domain name servers.
- Websites are stored on servers dedicated for this purpose – known as hosting.
- Hosted solutions provide 24/7 access, support for multiple users and enhanced security.
- Servers can be used to store data and programs that can be accessed over the internet – this is known as the cloud.
- The cloud provides access to files anytime, anywhere, on any device, as well as automatic backups and collaboration.
- Servers provide services (e.g., web server, web pages, file server, file storage/retrieval).
- Clients request services from a server.

GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols

The Internet: DNS & Web Servers and clients

Domain Name Service

- The Domain Name System (DNS) is like the phonebook of the internet. It translates human-friendly domain names (www.example.com) into numerical IP addresses (192.168.1.1) that computers use to identify each other on the network.
- This process allows users to access websites using easy-to-remember names instead of having to memorise complex numerical addresses.


URL in ➔ www.google.com
Domain Name Service
DNS recursive/resolver server
Root name server
.com top-level domain server (TLD)
Authoritative name server

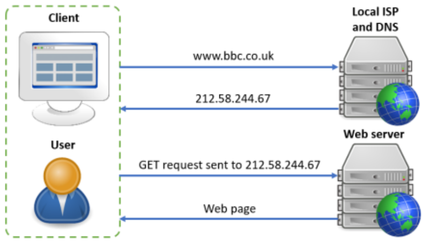
How DNS finds the IP address from the URL:

1. The URL is received by a DNS server.
2. The server queries a root name server.
3. The root server responds with the address of the top-level domain server for .com.
4. The resolver then makes a request to the .com TLD server.
5. The TLD server responds with the IP address of the domain's name server.
6. The recursive resolver sends a query to the domain's name server.
7. The name server returns the IP address of google.com (8.8.8.8) to the resolver.
8. The DNS resolver responds to the web browser with the Google's IP address.

Key Terminology	BCS Definition
DNS	Domain Name System: "The internet equivalent of the phone book. Maintains a directory of domain names and translates them to Internet Protocol (IP) addresses – this is necessary because, although domain names are easy to remember, computers access websites using IP addresses."
Hosting	"Websites stored on dedicated servers. Used for websites that need to be available 24/7, be accessed by thousands of users at a time, be well-protected from hackers and have an IP address that doesn't change."
Web server	"A program that uses HTTP (Hypertext Transfer Protocol) to deliver web pages to users. Page requests are forwarded by a computer's HTTP client. Dedicated computers and appliances may also be referred to as web servers."
Client	"A device that requests and/or uses services from a remote/connected server."

Web servers and clients

- Web servers carry out many functions – the most common are:
- Hosting websites
- Dealing with client requests
- A web page – stored as text (HTML, CSS, JavaScript) – is sent to a browser, which then uses various rules to render it correctly.



1. The client requests a URL via a web browser (e.g., www.bbc.co.uk).
2. The browser sends the domain name to a Domain Name Server (DNS).
3. The DNS maps the domain name to an IP address and returns it to the browser.
4. A GET request for the web page is sent to the web server using its IP address.
5. The requested web page is returned to the client's web browser.

GCSE Computer Science Knowledge Organiser
SLR1.3 Computer networks, connections and protocols
Star and mesh network topologies

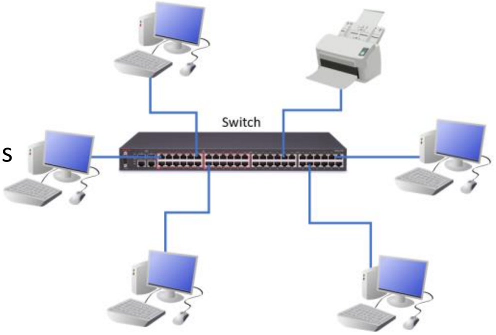
Key Terminology	BCS Definition
Network topology	"The physical or logical arrangement of connected devices on a network – e.g., computers, switches, routers, printers, servers, etc."
Star topology	"Computers connected to a central switch. If one computer fails, no others are affected. If the switch fails, all connections are affected."
Mesh topology	"Switches/routers connected so there is more than one route to the destination – e.g., the internet. More resilient to faults but more cable is required."

Topology
Refers to the way in which the parts of a system are arranged or connected.

In the context of computer networks, topology describes the layout of various elements (such as nodes and connections) in a network

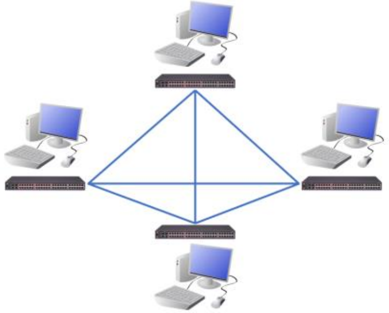
Star network topology

- Most popular type of wired network.
- Central switch.
- All devices connect to the switch.
- The switch is intelligent, ensuring traffic only goes where it is intended.
- If a single cable breaks, only that computer is affected.
- However, the switch is still a serious point of failure.



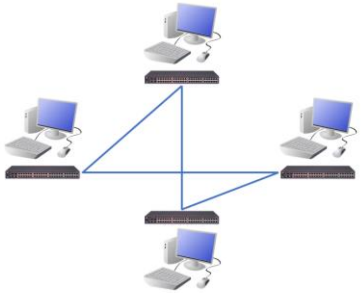
Full mesh network topology

- Every device is connected to every other device.
- If any of the connections break, traffic can be sent via another route.
- More cabling and switch hardware required, which adds to the cost.



Partial mesh network topology

- Multiple routes exist between devices, but every device is not connected to every other device.
- Reduces the amount of hardware compared to a full mesh network.



GCSE Computer Science Knowledge Organiser
SLR1.3 Computer networks, connections and protocols
Modes of connection: wired and wireless

Key Terminology	BCS Definition
Wired connection	"Any computer network that predominantly connects hardware via physical cables – e.g., copper, fibre optic, etc."
Ethernet	"A standard for networking local area networks using protocols. Frames are used to transmit data. A frame contains the source and destination addresses, the data and error-checking bits. Uses twisted pair and fibre optic cables. A switch is used to connect computers."
Wireless connection	"Any computer network that predominantly connects hardware via Wi-Fi, eliminating much of the need for physical cabling."
Wi-Fi	"Wireless connection to a network. Requires a wireless access point or router. Data is sent on a specific frequency. Each frequency is called a channel."
Bluetooth	"A method of exchanging data wirelessly over short distances – much shorter than Wi-Fi. Examples of typical Bluetooth use could be, headphones, car mobiles etc."

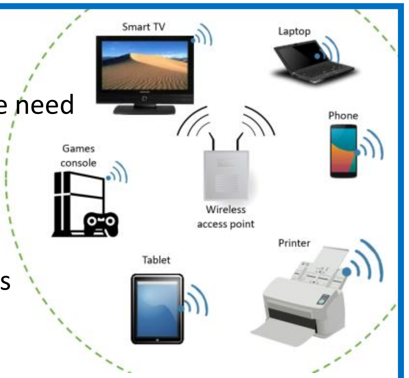
Wireless networks

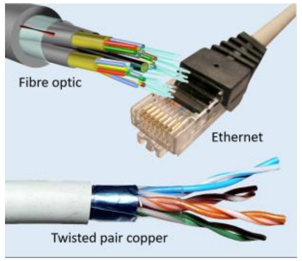
Wi-Fi

- Wireless connections are popular because they are portable and avoid the need for cables.
- However, their bandwidth is lower than that of a wired connection.
- Security is also more of a problem than with wired connections.
- An ever-increasing number of home devices are making use of Wi-Fi.
- Wireless connections are ideal as running lots of cabling through a home is undesirable.

Bluetooth

- Bluetooth is ideal for connecting personal devices.
- However, it has a very short range.
- It can be used to connect things like a wireless keyboard to a computer or wireless headphones to a smartphone.





Ethernet

- A standard for networking technologies.
- Used for communicating on a wired local area network.
- Includes a number of associated protocols (rules for governing communications).
- Provides reliable, error-free, fast communication between two points.
- Originally used in old-style bus networks.
- Still used today in more modern star and mesh networks.
- Data is transmitted in frames, which include:
  - Preamble of bits used to synchronise transmission.
  - Start frame deliminator to signify the start of the data part of the frame.
  - Source and destination MAC address.
  - The actual data.
  - Error-checking information (cyclic redundancy check or CRC).
- User location is limited by the need for a physical cable connection.
- An Ethernet setup relies on lots of cables, connections, ports and physical hardware, raising costs.

Wi-Fi is a common standard for wireless networks:

- Users can move around freely.
- Easier to set up and less expensive.
- More convenient to use.
- Can handle a large number of users.
- Data transfer is much easier.
- Network speeds are lower than with wired networks.
- Relies on signal strength to the wireless access point (WAP).
- Signal can be obstructed by objects or building elements.
- Less secure than wired networks.

Bluetooth is another, more modern standard for wireless networks:

- Ideal for connecting personal devices like Bluetooth-enabled headphones to a smartphone.
- Very short range – around 10 meters
- Low power consumption compared to Wi-Fi.

Wi-Fi	
Range	100 meters
Bandwidth	High
Power consumption	High

Bluetooth	
Range	10 meters
Bandwidth	Low
Power consumption	Low

GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols:

Wireless Encryption

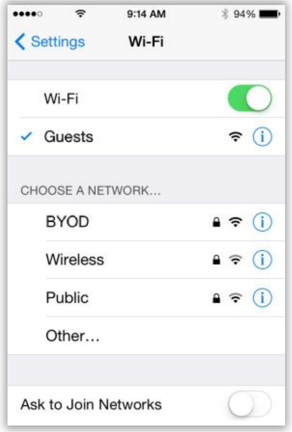
Key Terminology	BCS Definition
Encryption	"Encoding readable data (plain text) into unreadable data (ciphertext). Only the intended recipient can decode the data using a special key. Protects sensitive communications against hacking."

Encryption

Wireless networks are identified with a unique Service Set Identifier (SSID). The SSID must be used by all devices that want to connect to the network and can be set to automatically broadcast to any device in range of a WAP.

Protecting your wireless network:

- The SSID is set automatically, but you can change it if you wish.
- It can also be hidden to make it harder to detect.
- Additionally, it can be secured with a password.



●●●●○ 9:14 AM 94%

< Settings Wi-Fi

Wi-Fi

✓ Guests

CHOOSE A NETWORK...

BYOD

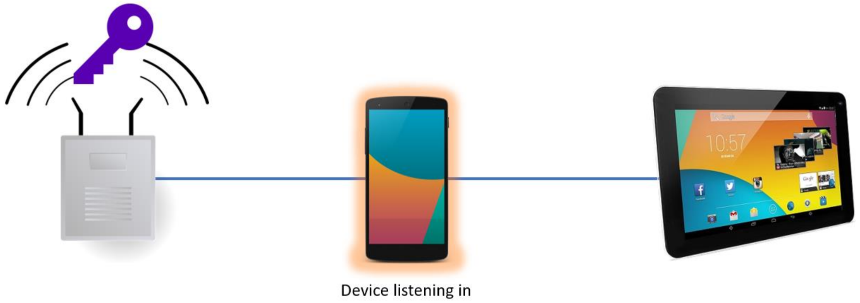
Wireless

Public

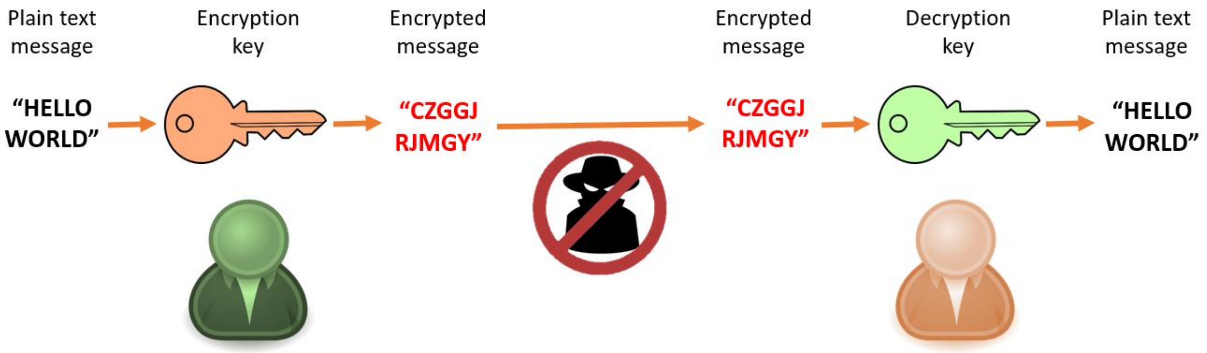
Other...

Ask to Join Networks

Wireless networks broadcast data that must be encrypted in order to be secure – this is done by scrambling the data into ciphertext using a master key created from the network's SSID and password.



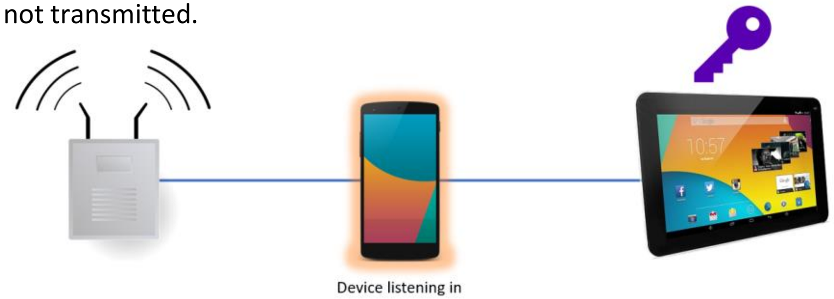
Although wired networks are more secure, encryption can still be used and is often a sensible precaution.



Plain text message → Encryption key → Encrypted message → Encrypted message → Decryption key → Plain text message

"HELLO WORLD" → "CZGGJ RJMGY" → "CZGGJ RJMGY" → "HELLO WORLD"

Data is decrypted by the receiver using the same master key – the key is not transmitted.



Data is decrypted by the receiver using the same master key – the key is not transmitted.

Wireless encryption protocols include WEP, WPA and WPA2. A handshake protocol is used to ensure the receiver has a valid master key before transmission begins.

GCSE Computer Science Knowledge Organiser
SLR1.3 Computer networks, connections and protocols:
IP and MAC Addressing

Key Terminology	BCS Definition
IP address	**Internet Protocol Address:** "A unique string of numbers separated by full stops. Identifies each computer using IP to communicate via a network."
MAC address	**Media Access Control Address:** "Used as a unique identifier for most network technologies including Ethernet and Wi-Fi."

MAC addressing is used to route frames on a local area network (LAN). Each MAC address is unique to every network interface card (e.g., 00:0a:95:9d:68:16).
IP addressing is used to route packets on a wide area network (WAN). There are two versions of IP addresses – IPv4 and IPv6.

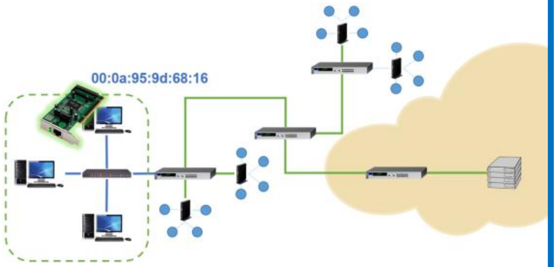
IPv4:
32 bits in size.
Four numbers between 0 and 255 separated with periods (e.g., 69.89.31.212).
A router has a unique WAN-facing IP address and a LAN-facing IP address – this enables a LAN device to have the same IP address as another device on a separate LAN.
IPv4 is being replaced by IPv6 because unique static addresses are running out.

IPv6:
128 bits in size.
Eight groups of four 16-bit hex values separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Media Access Control (MAC)

Every device on a network has a network interface card (NIC)

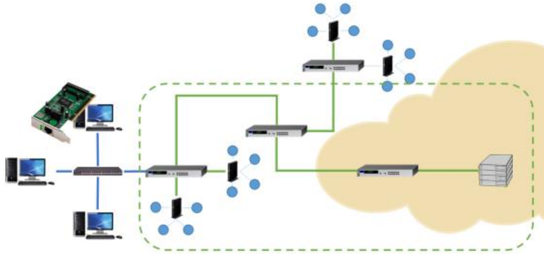
Every NIC has a Media Access Control (MAC) address, which is
used to route frames on a local area network (LAN).



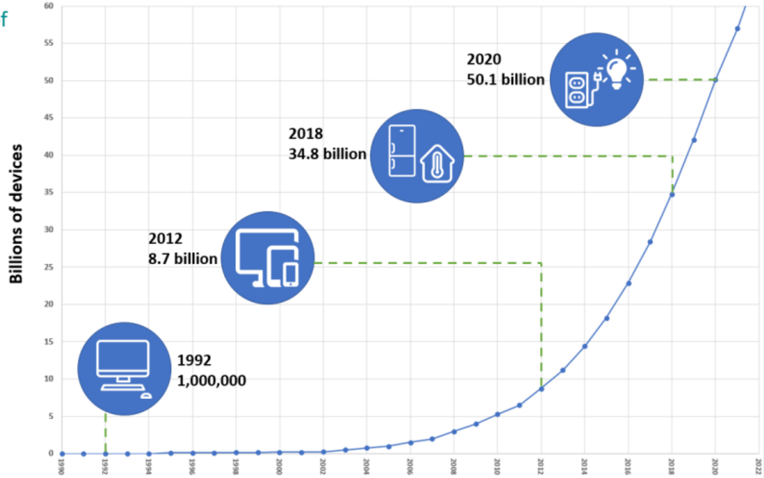
Internet Protocol (IP)

If the LAN is connected to a WAN such as the internet, a different addressing method is required.

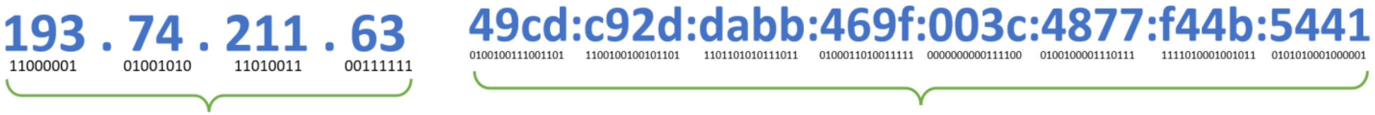
IP addressing is used to route frames on a wide area network (WAN) – with a WAN, we refer to frames as packets.



The Internet of Things (IoT)



IP4 vs IP6



32 bits (4 bytes) in size

128 bits (16 bytes) in size.
Approximately 340 trillion-trillion-trillion combinations

IPv4 format: Four numbers between 0 and 255 separated with periods.

IPv6 format: Eight groups of four 16-bit hex values separated by colons.

IPv4 provides us with approximately 4 billion possible addresses from 000.000.000.000 – 255.255.255.255.

The actual number is slightly lower, as some addresses are reserved for special uses.

GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols:

Standards and Common Protocols

The need for standards
We live in a world where standards are applied inconsistently.
In the field of computer science, standards are vital.

If one device recognises the binary sequence 01000001 as “A”, other devices must also recognise this sequence as “A”.

Without standards, devices connected to LANs and WANs wouldn’t be able to communicate with each other.

- In computer science terms, standards are a set of hardware and software specifications.
- These specifications make it possible for manufacturers and developers to create products and services that can communicate and interact with one another. Standards exist in many areas of computer science – for example:
    - ASCII/Unicode: Character sets
    - IEEE: Computer cables
    - HTML: Web content

Key Terminology	BCS Definition
Standards	“Various rules for different areas of computing. Standards allow hardware and software from different manufacturers to interact with each other.”
Protocol	“A set of rules that allow two devices to communicate.”
TCP/IP	Transmission Control Protocol/Internet Protocol: “TCP provides error-free transmission between two routers. IP routes packets across a wide area network.”
HTTP	Hypertext Transfer Protocol: “A client-server method of requesting and delivering HTML web pages. Used when the information on a web page is not sensitive or personal.”
HTTPS	Hypertext Transfer Protocol Secure: “Encryption and authentication for requesting and delivering HTML web pages. Used in websites that are sending and/or receiving sensitive data (e.g., passwords, bank details).”
FTP	File Transfer Protocol: “Used for sending files between computers, usually on a wide area network.”
POP	Post Office Protocol: “Used by email clients to retrieve email from an email server.”
IMAP	Internet Message Access Protocol: “Used by mail clients to manage remote mailboxes and retrieve email from a mail server.”
SMTP	Simple Mail Transfer Protocol: “Sends email to a mail server.”

Common protocols
Different types of protocols are used for different purposes.
You need to be aware of the basic principles and purposes of the following protocols.

Acronym	Full name	Area/purpose
TCP/IP	Transmission Control Protocol/Internet Protocol	Communication over a LAN/WAN
HTTP	Hypertext Transfer Protocol	Web page requests
HTTPS	Hypertext Transfer Protocol Secure	Web page requests
FTP	File Transfer Protocol	File transfers
POP	Post Office Protocol	Email
IMAP	Internet Message Access Protocol	Email
SMTP	Simple Mail Transfer Protocol	Email

GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols:
Standards and Common Protocols

TCP/IP

- The **Transmission Control Protocol (TCP)** provides error-free transmission between two routers.
- The **Internet Protocol (IP)** routes packets across a wide area network (WAN).
- Together, they make up the TCP/IP protocol stack the foundation of communication over the internet.

HTTP

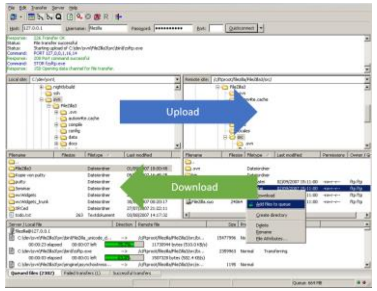
- The **Hypertext Transfer Protocol (HTTP)** is a way for a client and server to send and receive requests, and to deliver HTML web pages.
- It is the fundamental protocol of the World Wide Web (WWW).

HTTPS

- The **Hypertext Transfer Protocol Secure (HTTPS)** is effectively the same as HTTP except it adds in encryption and authentication.
- So it should be used on the web when a website needs to deal with sensitive information such as passwords or bank account details

FTP

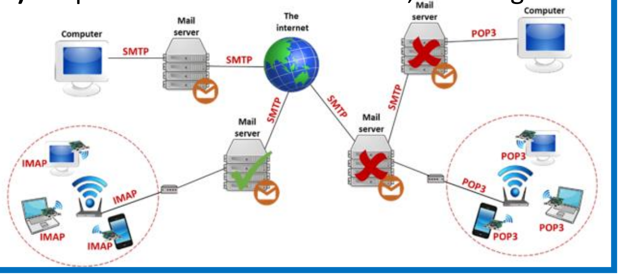
- The **File Transmission Protocol (FTP)** is a protocol used for sending files between computers, typically via a wide area network (WAN).
- People often use FTP clients, software applications that sit on top of the actual FTP protocol.
- Users interact with the program to generate and send the appropriate FTP commands.



Key Terminology	BCS Definition
Standards	"Various rules for different areas of computing. Standards allow hardware and software from different manufacturers to interact with each other."
Protocol	"A set of rules that allow two devices to communicate."
TCP/IP	Transmission Control Protocol/Internet Protocol: "TCP provides error-free transmission between two routers. IP routes packets across a wide area network."
HTTP	Hypertext Transfer Protocol: "A client-server method of requesting and delivering HTML web pages. Used when the information on a web page is not sensitive or personal."
HTTPS	Hypertext Transfer Protocol Secure: "Encryption and authentication for requesting and delivering HTML web pages. Used in websites that are sending and/or receiving sensitive data (e.g., passwords, bank details)."
FTP	File Transfer Protocol: "Used for sending files between computers, usually on a wide area network."
POP	Post Office Protocol: "Used by email clients to retrieve email from an email server."
IMAP	Internet Message Access Protocol: "Used by mail clients to manage remote mailboxes and retrieve email from a mail server."
SMTP	Simple Mail Transfer Protocol: "Sends email to a mail server."

POP/IMAP/SMTP

- Three popular protocols are used in conjunction with mail servers to deal with email.
- Mail servers act like a virtual post office for all incoming and outgoing email.
- **Simple Mail Transfer Protocol (SMTP)** transfers outgoing emails between servers or from an email client to a server.
- **Post Office Protocol (POP)** transfers emails from the mail server to your device, removing them from the server in the process.
- **Internet Message Access Protocol (IMAP)** keeps emails on the mail server, ensuring synchronicity between devices.



GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols:
Concept of Layers

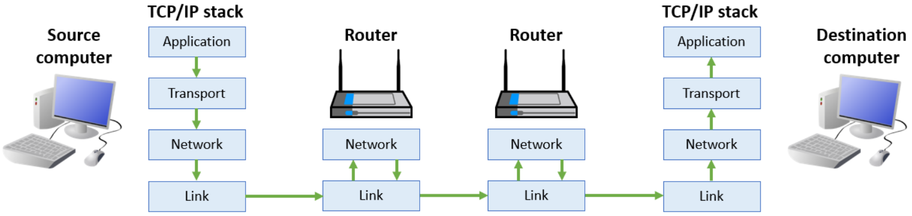
Key Terminology	BCS Definition
Protocol layering	“The concept of protocol rules being built up in layers – the layered protocol stack facilitates the various rules being executed in a defined order.”

The concept of layers
The concept of layering is to divide the complex task of networking into smaller, simpler tasks that work in tandem with each other.

The hardware and/or software for each layer has a defined responsibility, and each layer provides a service to the layer above it.

Advantages of layering

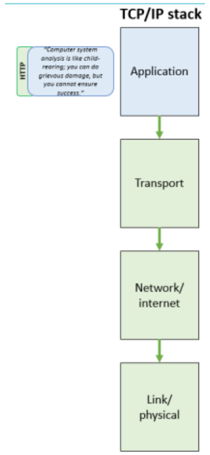
- Reduces the complexity of the problem into manageable sub-problems.
- Devices can be manufactured to operate at a particular layer.
- Products from different vendors will work together.



TCP/IP protocol and the use of layers
TCP/IP is one of the most important protocol stacks in use today.
It is a set of networking protocols, consisting of four layers all working together.
When you communicate via a network, all incoming and outgoing data packets pass up and down through the various layers.

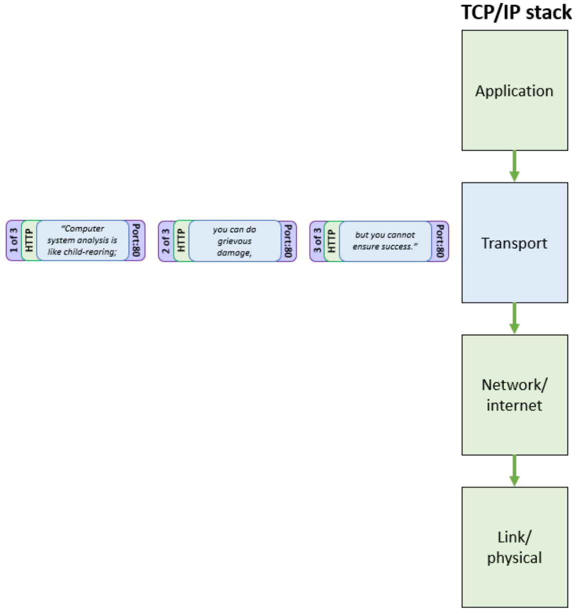
Stages of the TCP/IP Stack
Stage 1 - Application

- We are going to pass this message down through the layers of the **TCP/IP stack** to see what happens to it at each stage before it is sent out to another device via a network.
- The **application layer** uses an appropriate **protocol** relating to whatever application is being used to transmit data.
- This message is being sent via a web browser – so, the list of appropriate **protocols** would include **HTTP, HTTPS, FTP,** etc.


TCP/IP stack
HTTP
“Computer system analysis is like child-rearing; you can do grievous damage, but you cannot ensure success.”
Application
Transport
Network/ internet
Link/ physical

Stages of the TCP/IP Stack
Stage 2 - Transport

- The transport layer uses the TCP part of the stack, which is responsible for establishing an end-to-end connection.
- Once the connection is made, the transport layer splits the data into packets. It adds to each packet:
- Its number/sequence
- The total number of packets
- The port number that the packet should use



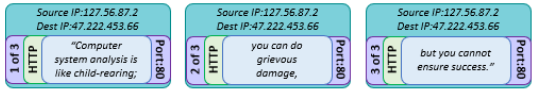
GCSE Computer Science Knowledge Organiser SLR1.3 Computer networks, connections and protocols:

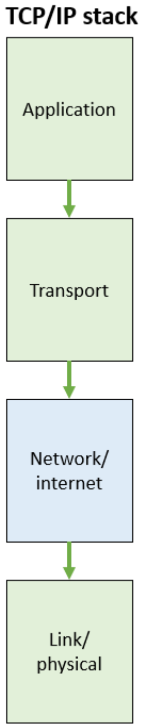
Concept of Layers

Key Terminology	BCS Definition
Protocol layering	“The concept of protocol rules being built up in layers – the layered protocol stack facilitates the various rules being executed in a defined order.”

Stages of the TCP/IP Stack
Stage 3 - Network

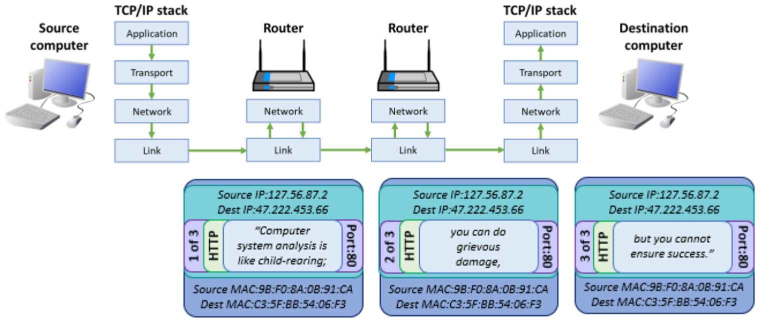
- The network layer use the IP part of the stack, sometimes called the internet layer.
- It adds to each packet:
- Source IP address
- Destination IP address
- All routers operate at this layer. They use the IP address to find out where the packets are heading. We now have what is known as a socket:
- socket = IP address + port
- For example, 127.56.87.2:80.
- We now know:
- The device the packet is being sent to (IP address).
- The application on that device that needs the packet (port).

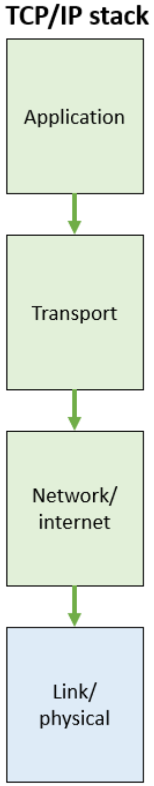




Stages of the TCP/IP Stack
Stage 4 - Link

- The link layer represents the actual physical connection between network devices.
- It is responsible for adding the unique Media Access Control (MAC) address of the:
- Source device
- Destination device
- The MAC address is changed at each hop on the route.


Source computer
TCP/IP stack
Application
Transport
Network
Link
Router
Network
Link
Router
Network
Link
TCP/IP stack
Application
Transport
Network
Link
Destination computer
Source IP:127.56.87.2
Dest IP:47.222.453.66
1 of 3
HTTP
“Computer system analysis is like child-rearing;
Port:80
Source MAC:9B:F0:8A:0B:91:CA
Dest MAC:C3:5F:BB:54:06:F3
Source IP:127.56.87.2
Dest IP:47.222.453.66
2 of 3
HTTP
you can do grievous damage,
Port:80
Source MAC:9B:F0:8A:0B:91:CA
Dest MAC:C3:5F:BB:54:06:F3
Source IP:127.56.87.2
Dest IP:47.222.453.66
3 of 3
HTTP
but you cannot ensure success.”
Port:80
Source MAC:9B:F0:8A:0B:91:CA
Dest MAC:C3:5F:BB:54:06:F3


TCP/IP stack
Application
Transport
Network/ internet
Link/ physical