2.1 NETWORKS INCLUDING THE INTERNET

ZAIN MERCHANT

2.1 Networks including the internet

Candidates should be able to:	Notes and guidance
Show understanding of the purpose and benefits of networking devices	
Show understanding of the characteristics of a LAN (local area network) and a WAN (wide area network)	
Explain the client-server and peer-to-peer models of networked computers	Roles of the different computers within the network and subnetwork models Benefits and drawbacks of each model Justify the use of a model for a given situation
Show understanding of thin-client and thick-client and the differences between them	
Show understanding of the bus, star, mesh and hybrid topologies	Understand how packets are transmitted between two hosts for a given topology Justify the use of a topology for a given situation
Show understanding of cloud computing	Including the use of public and private clouds. Benefits and drawbacks of cloud computing
Show understanding of the differences between and implications of the use of wireless and wired networks	Describe the characteristics of copper cable, fibre-optic cable, radio waves (including WiFi), microwaves, satellites
Describe the hardware that is used to support a LAN	Including switch, server, Network Interface Card (NIC), Wireless Network Interface Card (WNIC), Wireless Access Points (WAP), cables, bridge, repeater
Describe the role and function of a router in a network	
Show understanding of Ethernet and how collisions are detected and avoided	Including Carrier Sense Multiple Access/ Collision Detection (CSMA/CD)
Show understanding of bit streaming	Methods of bit streaming, i.e. real-time and on-demand Importance of bit rates/ broadband speed on bit streaming
Show understanding of the differences between the World Wide Web (WWW) and the internet	
Describe the hardware that is used to support the internet	Including modems, PSTN (Public Switched Telephone Network), dedicated lines, cell phone network
Explain the use of IP addresses in the transmission of data over the internet	Including: • format of an IP address including IPv4 and IPv6 • use of subnetting in a network • how an IP address is associated with a device on a network • difference between a public IP address and a private IP address and the implications for security • difference between a static IP address and a dynamic IP address
Explain how a Uniform Resource Locator (URL) is used to locate a resource on the World Wide Web (WWW) and the role of the Domain Name Service (DNS)	

PRE-READING QUESTIONS

1.
   A. Name the main components that make up a typical computer system.
   B. Tablets and smart phones carry out many of the functions of a desktop or laptop computer. Describe the main differences between the operations of a desktop or laptop computer and a tablet or phone.

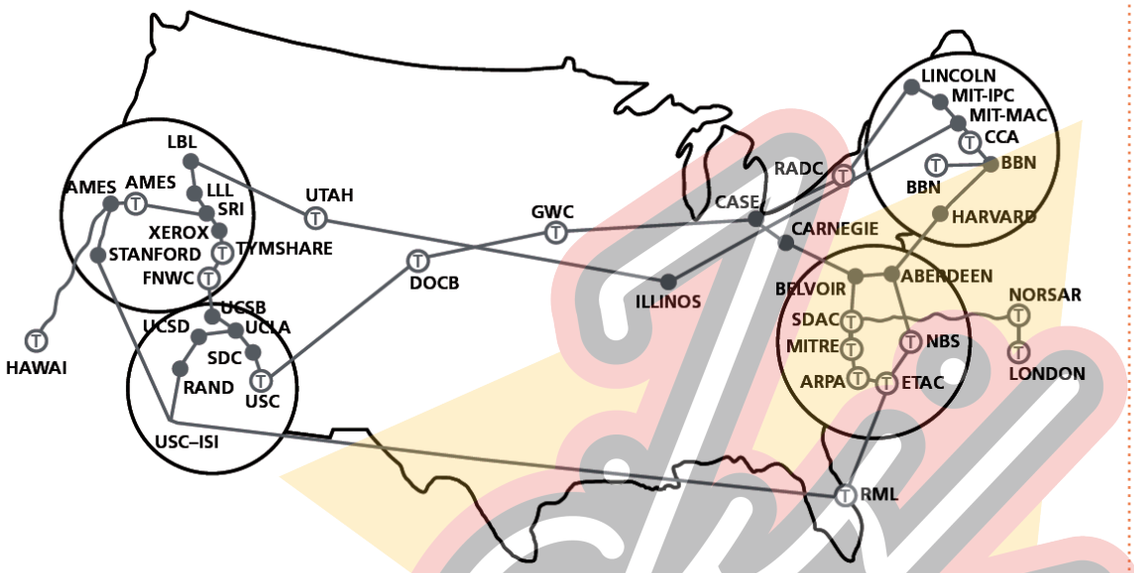
2. When deciding on which computer, tablet or phone to buy, which are the main factors that determine your final choice?

3. Look at a number of computers, laptops and phones and list (and name) the types of input and output ports found on each device.

4. At the centre of all of the above electronic devices is the microprocessor. How has the development of the microprocessor changed over the last ten years?

NETWORKING DEVICES

One of the earliest forms of networking, circa 1970 in the USA, was the Advanced Research Projects Agency Network (ARPAnet). This was an early form of packet switching wide area network (WAN) connecting a number of large computers in the Department of Defense. It later expanded to include university computers. It is generally agreed that ARPAnet developed the technical platform for what we now call the internet.



As personal computers developed through the 1980s, a local network began to appear. This became known as a local area network (LAN). LANs tended to be much smaller networks (usually inside one building) connecting a number of computers and shared devices, such as printers. WANs typically consist of a number of LANs connected via public communications networks (such as telephone lines or satellites). Because a WAN consists of LANs joined together, it may be a private network, and passwords and user IDs are required to access it. This is in contrast to the internet which is a vast number of decentralised networks and computers which have a common point of access, so that anyone with access to the internet can connect to the computers on these networks. This makes it intrinsically different to a WAN.

In recent years, another type of network – a metropolitan area network (MAN) – has emerged. MANs are larger than LANs as they can connect together many small computer networks (e.g LANs) housed in different buildings within a city (for example, a university campus). MANs are restricted in their size geographically to, for example, a single city.

In contrast, WANs can cover a much larger geographical area, such as a country or a continent. For example, a multi-national company may connect a number of smaller networks together (e.g. LANs or MANs) to form a world-wide WAN. This is covered in more detail later.

Here are some of the main benefits of networking computers and devices (rather than using a number of stand-alone computers):

- Devices, such as printers, can be shared (thus reducing costs).
- Licences to run software on networks are often far cheaper than buying licences for an equivalent number of stand-alone computers.
- Users can share files and data.
- Access to reliable data that comes from a central source, such as a file server.
- Data and files can be backed up centrally at the end of each day.
- Users can communicate using email and instant messaging.
- A network manager can oversee the network and, for example, apply access rights to certain files, or restrict access to external networks, such as the internet.

There are also a number of drawbacks:

- Cabling and servers can be an expensive initial outlay.
- Managing a large network can be a complex and difficult task.
- A breakdown of devices, such as the file servers, can affect the whole network.
- Malware and hacking can affect entire networks (particularly if a LAN is part of a much larger WAN), although firewalls do afford some protection in this respect.

NETWORKED COMPUTERS

Networked computers form an infrastructure which enables internal and external communications to take place. The infrastructure includes the following:

HARDWARE

- LAN cards
- routers
- switches
- wireless routers
- cabling

SOFTWARE

- operation and management of the network
- operation of firewalls
- security applications/utilities

SERVICES

- DSL
- satellite communication channels
- wireless protocols
- IP addressing.

Networks can be categorised as private or public.

Private networks are owned by a single company or organisation (they are often LANs or intranets with restricted user access, for example, passwords and user ids are required to join the network); the companies are responsible for the purchase of their own equipment and software, maintenance of the network and the hiring and training of staff.

Public networks are owned by a communications carrier company (such as a telecoms company); many organisations will use the network and there are usually no specific password requirements to enter the network – but sub-networks may be under security management.

WANS AND LANS

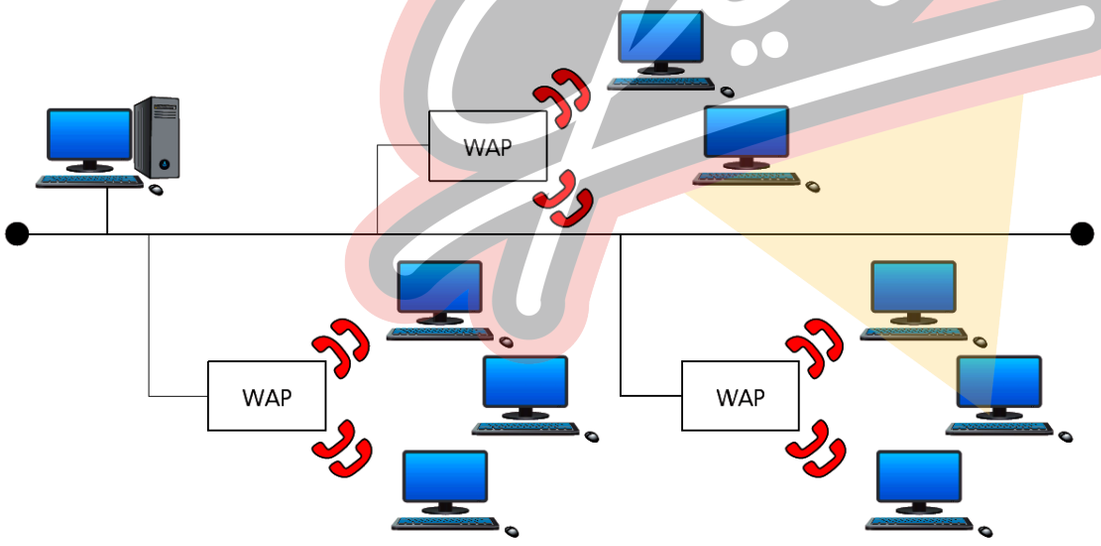
LOCAL AREA NETWORKS (LANS)

LANs are usually contained within one building, or within a small geographical area. A typical LAN consists of a number of computers and devices (such as printers) connected to hubs or switches. One of the hubs or switches is usually connected to a router and/or modem to allow the LAN to connect to the internet or become part of a wide area network (WAN).

WIRELESS LANS (WLANS)

Wireless LANs (WLANs) are similar to LANs but there are no wires or cables. In other words, they provide wireless network communications over fairly short distances (up to 100 metres) using radio or infrared signals instead of using cables. Devices, known as wireless access points (WAPs), are connected into the wired network at fixed locations. Because of the limited range, most commercial LANs (such as those on a college campus or at an airport) need several WAPs to permit uninterrupted wireless communications. The WAPs use either spread spectrum technology (which is a wideband radio frequency with a range from a few metres to 100 metres) or infrared (which has a very short range of about 1 to 2 metres and is easily blocked, and therefore has limited use.

The WAP receives and transmits data between the WLAN and the wired network structure. End users access the WLAN through wireless LAN adapters which are built into the devices or as a plug in module.

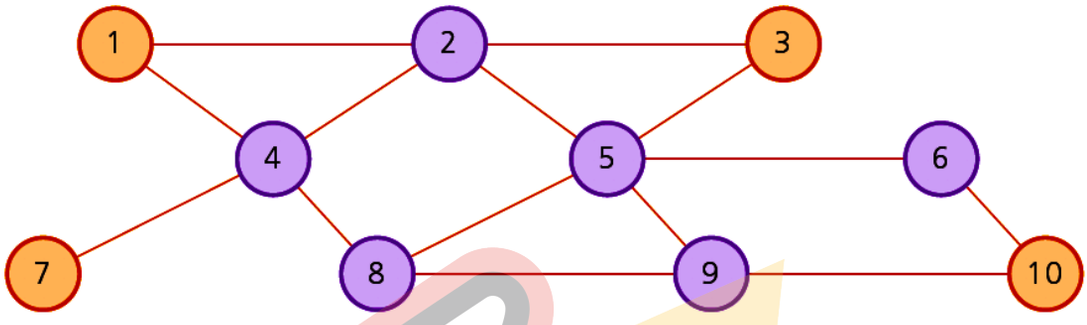


WIDE AREA NETWORKS (WANS)

Wide area networks (WANs) are used when computers or networks are situated a long distance from each other (for example, they may be in different cities or on different continents). If a number of LANs are joined together using a router or modem, they can form a WAN. The network of automated teller machines (ATMs) used by banks is one of the most common examples of the use of a WAN.

Because of the long distances between devices, WANs usually make use of a public communications network (such as telephone lines or satellites), but they can

use dedicated or leased communication lines which can be less expensive and more secure (less risk of hacking, for example).
A typical WAN will consist of end systems and intermediate systems, as shown in figure below. 1, 3, 7 and 10 are known as end systems, and the remainder are known as intermediate systems. The distance between each system can be considerable, especially if the WAN is run by a multi-national company.

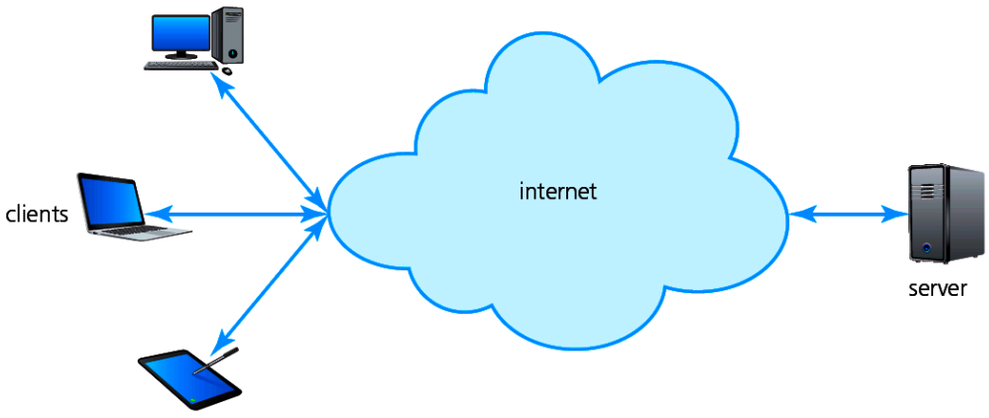


The following is used as a guide for deciding the 'size' of a network:
WAN: 100 km to over 1000 km
MAN: 1 km to 100 km
LAN: 10 m to 1000 m
PAN: 1 m to 10 m (this is not a commonly used term – it means personal area network; in other words, a home system)

CLIENT-SERVER AND PEER-TO-PEER NETWORKING MODELS

We will consider two types of networking models, client-server and peer-to-peer.

CLIENT-SERVER MODEL



Client sends a request to the server and the server finds the requested data and sends it back to the client.

A system administrator manages the whole network; clients are connected through a network; allows data access even over large distances.

- The client-server model uses separate dedicated servers and specific client workstations; client computers will be connected to the server computer(s).
- Users are able to access most of the files, which are stored on dedicated servers.
- The server dictates which users are able to access which files. (Note: sharing of data is the most important part of the client-server model; with peer-to-peer, connectivity is the most important aspect.)
- The client-server model allows the installation of software onto a client's computer.
- The model uses central security databases which control access to the shared resources. (Note: passwords and user IDs are required to log into the network.)
- Once a user is logged into the system, they will have access to only those resources (such as a printer) and files assigned to them by the network administrator, so offers greater security than peer-to-peer networks.
- Client-server networks can be as large as you want them to be and they are much easier to scale up than peer-to-peer networks.
- A central server looks after the storing, delivery and sending of emails.
- This model offers the most stable system, for example, if someone deletes a shared resource from the server, the nightly back-up would restore the deleted resource (this is different in peer-to-peer – see later).
- Client-server networks can become bottlenecked if there are several client requests at the same time.
- In the client-server model, a file server is used and is responsible for
  - ✦ central storage and management of data files, thus enabling other network users to access files
  - ✦ allowing users to share information without the need for offline devices (such as a memory stick)
  - ✦ allowing any computer to be configured as the host machine and act as the file server (note that the server could be a storage device (such as SSD or HDD) that could also serve as a remote storage device for other computers, thus allowing them to access this device as if it were a local storage device attached to their computer).

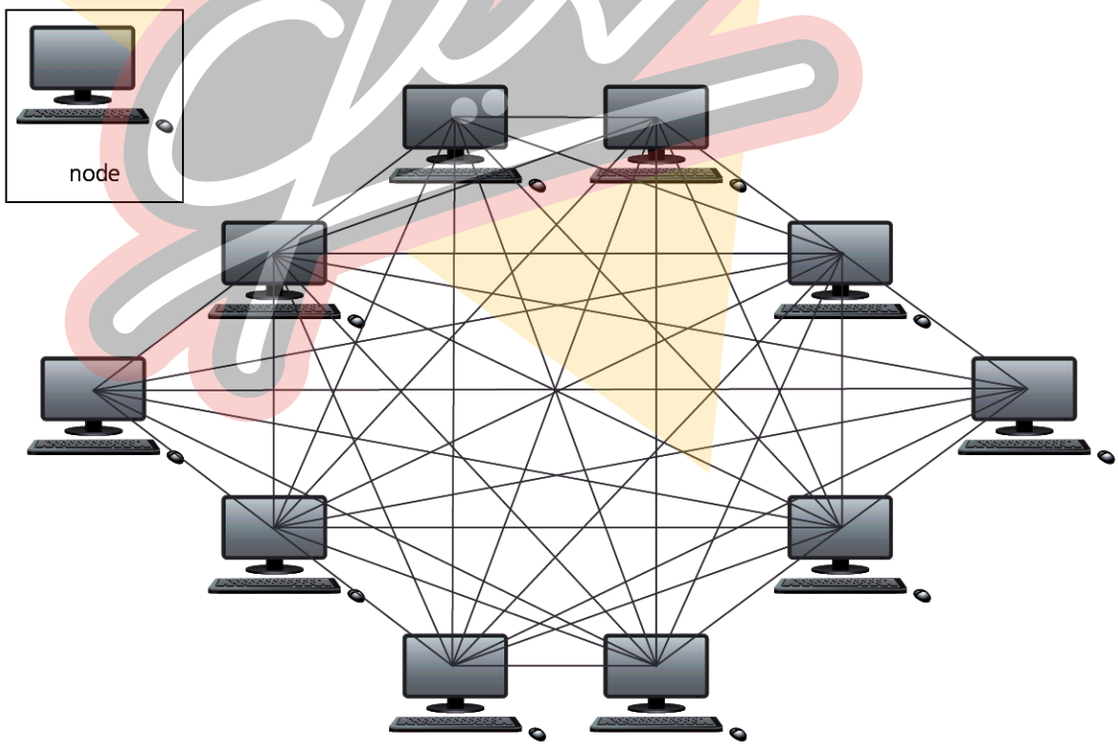
EXAMPLES OF USE OF CLIENT-SERVER NETWORK MODEL

A company/user would choose a client-server network model for the following reasons.

- The company/user has a large user-base (however, it should be pointed out that this type of network model may still be used by a small group of people who are doing independent projects but need to have sharing of data and access to data outside the group).
- Access to network resources needs to be properly controlled.
- There is a need for good network security.
- The company requires its data to be free from accidental loss (in other words, data needs to be backed up at a central location).

An example is the company Amazon; it uses the client-server network model. The user front-end is updated every time a user logs on to the Amazon website and a large server architecture handles items such as order processing, billing customers and data security; none of the Amazon users are aware that other customers are using the website at the same time – there is no interaction between users and server since they are kept entirely separate at all times.

PEER-TO-PEER MODEL



On a peer-to-peer network, each node joins the network to allow

- the provision of services to all other network users; the services available are listed on a nominated 'look up' computer – when a node requests a service, the 'look up' computer is contacted to find out which of the other network nodes can provide the required service

- other users on the network to simply access data from another node
- communication with other peers connected to the network
- peers to be both suppliers and consumers (unlike the client-server model where consumers and resources are kept entirely separate from each other)
- peers to participate as equals on the network (again this is different
- to the client-server model where a webserver and client have different responsibilities).

The peer-to-peer model does not have a central server. Each of the nodes (workstations) on the network can share its files with all the other nodes, and each of the nodes will have its own data.

Because there is no central storage, there is no requirement to authenticate users.

This model is used in scenarios where no more than 10 nodes are required (such as a small business) where it is relatively easy for users to be in contact with each other on a regular basis. More than 10 nodes leads to performance and management issues.

Peer-to-peer offers little data security since there is no central security system. This means it is impossible to know who is authorised to share certain data. Users can create their own network node share point which is the only real security aspect since this gives them some kind of control. However, there are no real authentication procedures.

EXAMPLES OF PEER-TO-PEER NETWORK MODEL

A user would choose the peer-to-peer network model for one or more of following reasons:

- The network of users is fairly small.
- There is no need for robust security.
- They require workstation-based applications rather than being server-based.

An example would be a small business where there is frequent user interaction and there is no need to have the features of a client-server network (for example, a builder with five associated workers located in their own homes who only need access to each other's diaries, previous jobs, skills-base and so on – when the builder is commissioned to do a job they need to access each other's computer to check on who is available and who has the appropriate skills).

THIN CLIENTS AND THICK CLIENTS

The client-server model offers thin clients and thick clients. These can often refer to both hardware and software.

THIN CLIENT

A thin client is heavily dependent on having access to a server to allow constant access to files and to allow applications to run uninterrupted. A thin client can either be a device or software which needs to be connected to a powerful computer or server to allow processing to take place (the computer or server could be on the internet or could be part of a LAN/MAN/WAN network). The thin client will not work unless it is connected at all times to the computer or server. A software example would be a web browser which has very limited functions unless it is connected to a server. Other examples include mobile phone apps which need constant access to a server to work. A hardware example is a POS terminal at a

supermarket that needs constant access to a server to find prices, charge customers and to do any significant processing.

THICK CLIENT

A thick client can either be a device or software that can work offline or online; it is still able to do some processing whether it is connected to a server or not. A thick client can either be connected to a LAN/MAN/WAN, virtual network, the internet or a cloud computing server. A hardware example is a normal PC/laptop/tablet since it would have its own storage (HDD or SSD), RAM and operating system which means it is capable of operating effectively online or offline. An example of software is a computer game which can run independently on a user's computer, but can also connect to an online server to allow gamers to play and communicate with each other.

	Pros	Cons
Thick clients	■ more robust (device can carry out processing even when not connected to server) ■ clients have more control (they can store their own programs and data/ files)	■ less secure (relies on clients to keep their own data secure) ■ each client needs to update data and software individually ■ data integrity issues, since many clients access the same data which can lead to inconsistencies
Thin clients	■ less expensive to expand (low-powered and cheap devices can be used) ■ all devices are linked to a server (data updates and new software installation done centrally) ■ server can offer protection against hacking and malware	■ high reliance on the server; if the server goes down or there is a break in the communication link then the devices cannot work ■ despite cheaper hardware, the start-up costs are generally higher than for thick clients

Thin client software	Thick client software
■ always relies on a connection to a remote server or computer for it to work	■ can run some of the features of the software even when not connected to a server
■ requires very few local resources (such as SSD, RAM memory or computer processing time)	■ relies heavily on local resources
■ relies on a good, stable and fast network connection for it to work	■ more tolerant of a slow network connection
■ data is stored on a remote server or computer	■ can store data on local resources such as HDD or SSD

NETWORK TOPOLOGIES

There are many ways to connect computers to make complex networks. Here we will consider

- bus networks
- star networks
- mesh networks
- hybrid networks.

BUS NETWORKS

A bus network topology uses a single central cable to which all computers and devices are connected. It is easy to expand and requires little cabling. Data can only travel in one direction; if data is being sent between devices then other devices cannot transmit. Terminators are needed at each end to prevent signal reflection (bounce). Bus networks are typically peer-to-peer. The disadvantages of a bus network include:

- If the main cable fails, the whole network goes down.
- The performance of the network deteriorates under heavy loading.
- The network is not secure since each packet passes through every node. The advantages of a bus network include:
- Even if one node fails, the remainder of the network continues to function.
- It is easy to increase the size of the network by adding additional nodes.

In bus network topology, each node looks at each packet and determines whether or not the address of the recipient in the package matches the node address. If so, the node accepts the packet; if not, the packet is ignored.

These are most suitable for situations with a small number of devices with light traffic occurring. For example, a small company or an office environment.

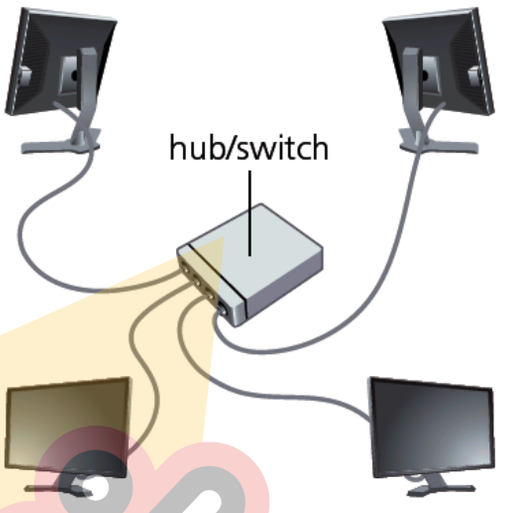
STAR NETWORKS

A star network topology uses a central hub/switch and each computer/device is connected to the hub/switch. Data going from host to host is directed through the central hub/switch. Each computer/device has its own dedicated connection to the central node (hub/switch) – any type of network cable can be used for the connections. This type of network is typically a client-server. The disadvantages of a star network include:

- The initial installation costs are high.
- If the central hub/switch fails, then the whole network goes down. The advantages of a star network include:
- Data collisions are greatly reduced due to the topology.

- It is a more secure network since security methods can be applied to the central node and packets only travel to nodes with the correct address.
- It is easy to improve by simply installing an upgraded hub.
- If one of the connections is broken it only affects one of the nodes.

How packets are handled depends on whether the central node is a switch or a hub. If it is a hub, all the packets will be sent to every device/node on the star network – if the address in the packet matches that of the node, it will be accepted; otherwise, it is ignored (this is similar to the way packets are handled on a bus network). If the central node is a switch, packets will only be sent to nodes where the address matches the recipient address in the packet. The latter is clearly more secure, since only nodes intended to see the packet will receive it.



Star networks are useful for evolving networks where devices are frequently added or removed. They are well suited to applications where there is heavy data traffic.

MESH NETWORKS

There are two types of mesh network topologies: routing and flooding. Routing works by giving the nodes routing logic (in other words, they act like a router) so that data is directed to its destination by the shortest route and can be re-routed if one of the nodes in the route has failed. Flooding simply sends the data via all the nodes and uses no routing logic, which can lead to unnecessary loading on the network. It is a type of peer-to-peer network, but is fundamentally different. The disadvantages of a mesh network include:

- A large amount of cabling is needed, which is expensive and time consuming.
- Set-up and maintenance is difficult and complex.

The advantages of a mesh network include:

- It is easy to identify where faults on the network have occurred.
- Any broken links in the network do not affect the other nodes.
- Good privacy and security, since packets travel along dedicated routes.
- The network is relatively easy to expand.

In flooding, what if one node is compromised. Wouldn't that make mesh network not secure? *

There are a number of applications worth considering here:

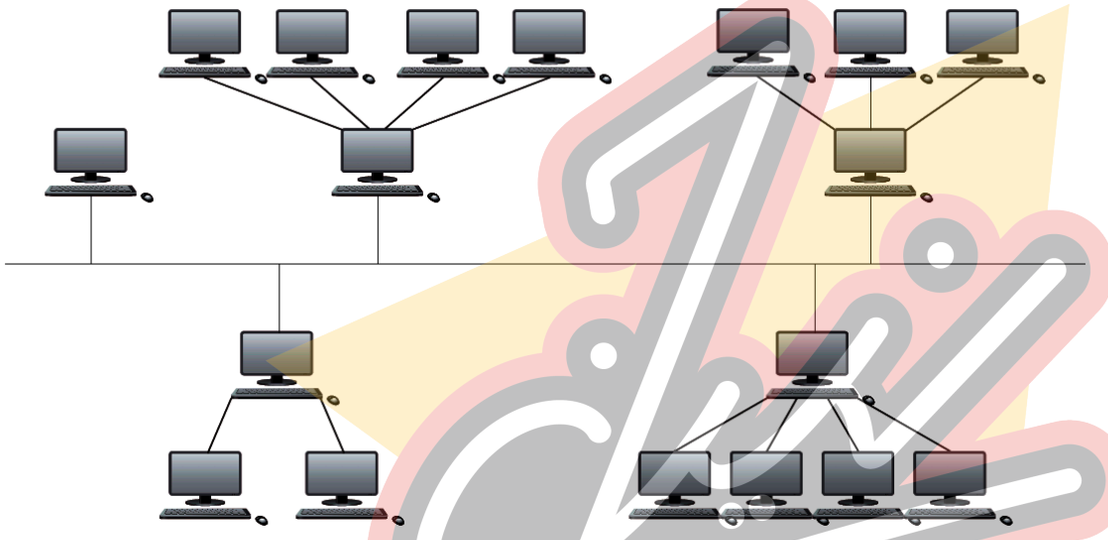
- The internet and WANs/MANs are typical uses of mesh networks.
- Many examples include industrial monitoring and control where sensors are set up in mesh design and feedback to a control system which is part of the mesh, for example
    - ✦ medical monitoring of patients in a hospital
    - ✦ electronics interconnectivity (for example, systems that link large screen televisions, DVDs, set top boxes, and so on); each device will be in a location forming the mesh

- ✦modern vehicles use wireless mesh network technology to enable the monitoring and control of many of the components in the vehicle.

HYBRID NETWORKS

A hybrid network is a mixture of two or more different topologies (bus and star, bus and mesh, and so on). The main advantages and disadvantages depend on which types of network are used to make up the hybrid network, but an additional disadvantage is that they can be very complex to install, configure and maintain.
Additional advantages include:

- They can handle large volumes of traffic.
- It is easy to identify where a network fault has occurred.
- They are very well suited to the creation of larger networks.



Note that the handling of packets in hybrid networks will depend on which of the above topologies are used to make up the hybrid structure.
One of the typical applications of hybrid networks is illustrated by the following example, involving three hotel chains, A, B and C.
Suppose hotel chain A uses a bus network, hotel chain B uses a star network and hotel chain C uses a mesh network.
At some point, all three hotel chains are taken over by another company. By using hybrid network technology, all three hotel chains can be connected together even though they are each using a different type of network. The system can also be expanded easily without affecting any of the existing hotels using the network.
There are many other examples; you might want to explore the various applications for each type of network topology.

PUBLIC AND PRIVATE CLOUD COMPUTING

Cloud storage is a method of data storage where data is stored on offsite servers – the physical storage covers hundreds of servers in many locations.
The same data is stored on more than one server in case of maintenance or repair, allowing clients to access data at any time. This is known as data redundancy. The physical environment is owned and managed by a hosting company.
There are three common systems, public cloud, private cloud and hybrid cloud.
Public cloud is a storage environment where the customer/client and cloud storage provider are different companies.
Private cloud is storage provided by a dedicated environment behind a company firewall. Customer/client and cloud storage provider are integrated and operate as a single entity.
Hybrid cloud is a combination of private and public clouds. Some data resides in the private cloud and less sensitive/less commercial data can be accessed from a public cloud storage provider.
Instead of saving data on a local hard disk or other storage device, a user can save their data 'in the cloud'.

Pros of using cloud storage	Cons of using cloud storage
■ customer/client files stored on the cloud can be accessed at any time from any device anywhere in the world provided internet access is available ■ no need for a customer/client to carry an external storage device with them, or use the same computer to store and retrieve information ■ provides the user with remote back-up of data to aid data loss and disaster recovery ■ recovers data if a customer/client has a hard disk or back-up device failure ■ offers almost unlimited storage capacity	■ if the customer/client has a slow or unstable internet connection, they would have problems accessing or downloading their data/files ■ costs can be high if large storage capacity is required ■ expensive to pay for high download/upload data transfer limits with the customer/client internet service provider (ISP) ■ potential failure of the cloud storage company is possible – this poses a risk of loss of all back-up data

DATA SECURITY WHEN USING CLOUD STORAGE

Companies that transfer vast amounts of confidential data from their own systems to a cloud service provider are effectively relinquishing control of their own data security. This raises a number of questions:

- What physical security exists regarding the building where the data is housed?
- How good is the cloud service provider's resistance to natural disasters or power cuts?
- What safeguards exist regarding personnel who work for the cloud service company? Can they use their authorisation codes to access confidential data for monetary purposes?

POTENTIAL DATA LOSS WHEN USING CLOUD STORAGE

There is a risk that important and irreplaceable data could be lost from the cloud storage facilities. Actions from hackers (gaining access to accounts or pharming attacks, for example) could lead to loss or corruption of data. Users need to be certain sufficient safeguards exist to overcome these risks.

The following breaches of security involving some of the largest cloud service providers suggest why some people are nervous of using cloud storage for important files:

- The XEN security threat, which forced several cloud operators to reboot all their cloud servers, was caused by a problem in the XEN hypervisor (a hypervisor is a piece of computer software, firmware or hardware that creates and runs virtual machines).
- A large cloud service provider permanently lost data during a routine back-up procedure.
- The celebrity photos cloud hacking scandal, in which more than 100 private photos of celebrities were leaked. Hackers had gained access to a number of cloud accounts, which then enabled them to publish the photos on social networks and sell them to publishing companies.
- In 2016, the National Electoral Institute of Mexico suffered a cloud security breach in which 93 million voter registrations, stored on a central database, were compromised and became publicly available to everyone. To make matters worse, much of the information on this database was also linked to an Amazon cloud server outside Mexico.

CLOUD SOFTWARE

Cloud storage is, of course, only one aspect of cloud computing. Other areas covered by cloud computing include databases, networking, software and analytical services using the internet.

Here we will consider cloud software – you can research for yourself how databases and analytical services are provided by cloud computing services.

Software applications can be delivered to a user's computer on demand using cloud computing services. The cloud provider will both host and manage software applications – this will include maintenance, software upgrades and security for a monthly fee. A user will simply connect to the internet (using their web browser on a computer or tablet or mobile phone) and contact their cloud services supplier. The cloud services supplier will connect them to the software application they require.

The main advantages are that the software will be fully tested and it does not need to reside on the user's device. However, the user can still use the software even if the internet connection is lost. Data will simply be stored on the
local device and then data will be uploaded or downloaded once the internet connection is restored.

Cloud-based applications can, therefore, perform tasks on a local device. This makes them fundamentally different to web-based apps which need an internet connection at all times.

WIRED AND WIRELESS NETWORKING

WIRELESS

WI-FI AND BLUETOOTH

Both Wi-Fi and Bluetooth offer wireless communication between devices. They both use electromagnetic radiation as the carrier of data transmission.

Bluetooth sends and receives radio waves in a band of 79 different frequencies (known as channels). These are all centred on a 2.45 GHz frequency. Devices using Bluetooth automatically detect and connect to each other, but they do not interfere with other devices since each communicating pair uses a different channel (from the 79 options).

When a device wants to communicate, it picks one of the 79 channels at random. If the channel is already being used, it randomly picks another channel. This is known as spread spectrum frequency hopping. To further minimise the risks of interference with other devices, the communication pairs constantly change the frequencies (channels) they are using (several times a second). Bluetooth creates a secure wireless personal area network (WPAN) based on key encryption.

Bluetooth is useful when

- transferring data between two or more devices which are less than 30 metres apart
- the speed of data transmission is not critical
- using low bandwidth applications (for example, sending music files from a mobile phone to a headset).

As mentioned earlier in the chapter, Wi-Fi also uses spread spectrum technology. However, Wi-Fi is best suited to operating full-scale networks, since it offers much faster data transfer rates, better range and better security than Bluetooth. A Wi-Fi-enabled device (such as a computer or smart phone) can access, for example, the internet wirelessly at any wireless access point (WAP) or 'hot spot' up to 100 metres away.

As mentioned, wireless connectivity uses electromagnetic radiation: radio waves, microwaves or infrared.

	radio waves	microwaves	infrared	visible light	ultra violet	X-rays	gamma rays
Wave length (m)	10^{2}	10^{-1}	10^{-3}	10^{-5}	10^{-7}	10^{-9}	10^{-11}
Frequency (Hz)	3 MHz	3 GHz	300 GHz	30 THz	3 PHz	300 PHz	30 EHz

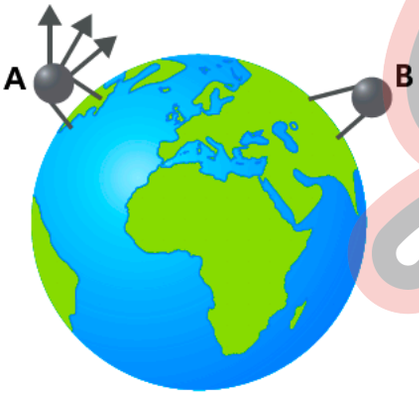
Table below compares radio waves, microwaves and infrared. (Please note: the '>' symbol in the table means 'better than').

Bandwidth	infrared > microwaves > radio waves (infrared has the largest bandwidth)
Penetration	radio waves > microwaves > infrared (radio waves have the best penetration)
Attenuation	radio waves > microwaves > infrared (radio waves have the best attenuation)

Penetration measures the ability of the electromagnetic radiation to pass through different media. Attenuation is the reduction in amplitude of a signal (infrared has low attenuation because it can be affected by, for example, rain or internal walls). Thus, we would expect infrared to be suitable for indoor use only; the fact that it can be stopped by walls is seen as an advantage since this stops the signal causing interference elsewhere. Microwaves seem to offer the best compromise, since they support reasonable bandwidth, and have reasonable penetration and attenuation.

ADDITIONAL NOTES ON THE USE OF SATELLITES

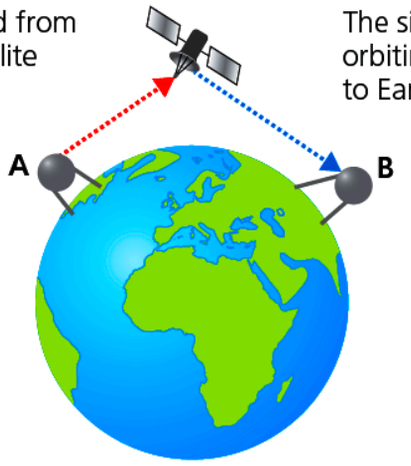
The use of microwaves and radio waves was previously mentioned as a method for allowing Wi-Fi connectivity in networks. These methods are perfectly satisfactory for short distances – the electromagnetic waves carry the signals – but the curvature of the Earth prevents such methods transmitting data globally.



The electromagnetic radiation from antenna A is transmitted but is unable to reach antenna B due to the Earth's curvature.

To overcome this problem, we need to adopt satellite technology:

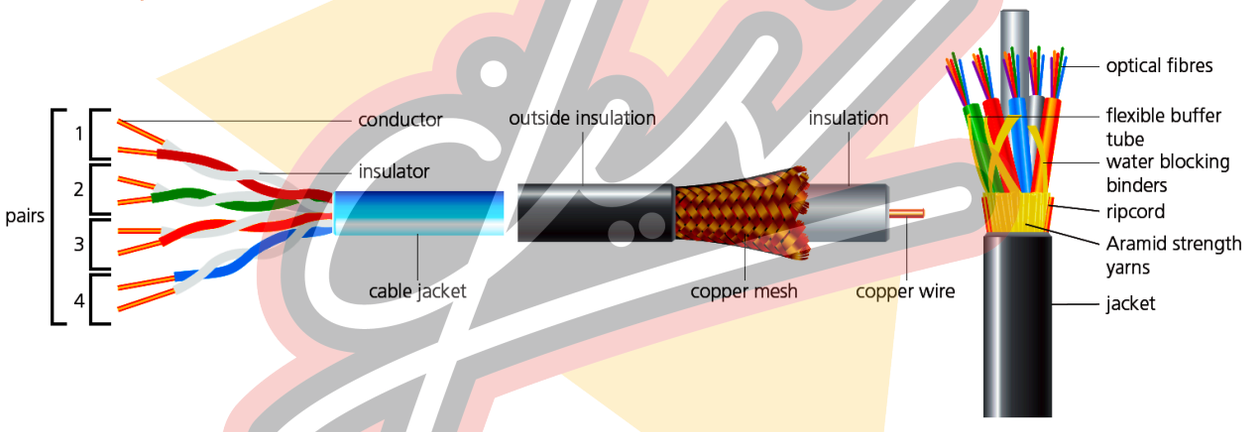
The signal is beamed from antenna A to a satellite orbiting Earth.



The signal is boosted by the satellite orbiting Earth and is then beamed back to Earth and picked up by antenna B.

The communication between antennae and satellite is carried out by radio waves or microwave frequencies. Different frequency bands are used to prevent signal interference and to allow networks spread across the Earth to communicate through use of satellites.

WIRED



There are three main types of cable used in wired networks.

TWISTED PAIR CABLES

Twisted pair cables are the most common cable type used in LANs. However, of the three types of cable, it has the lowest data transfer rate and suffers the most from external interference (such as electromagnetic radiation). However, it is the cheapest option. There are two types of twisted pair cable: unshielded and shielded. Unshielded is used by residential users. Shielded is used commercially (the cable contains a thin metal foil jacket which cancels out some of the external interference).

COAXIAL CABLES

Coaxial cables are the most commonly used cables in MANs and by cable television companies. The cost of coaxial cables is higher than twisted pair cables but they offer a better data transfer rate and are affected less by external interference. Coaxial cables also have about 80 times the transmission capacity of

twisted pair. Coaxial suffers from the greatest signal attenuation, but offers the best anti-jamming capabilities.

FIBRE OPTIC CABLES

Fibre optic cables are most commonly used to send data over long distances, because they offer the best data transfer rate, the smallest signal attenuation and have a very high resistance to external interference. The main drawback is the high cost. Unlike the other two types of cable, fibre optics use pulses of light rather than pulses of electricity to transmit data. They have about 26 000 times the transmission capacity of twisted pair cables.

Fibre optic cables can be single- or multi-mode.

Single-mode uses a single mode light source and has a smaller central core, which results in less light reflection along the cable. This allows the data to travel faster and further, making them a good choice for CATV and telecommunications.

Multi core allows for a multi-mode light source; the construction causes higher light reflections in the core, so they work best over shorter distances (in a LAN, for example).

WIRED VERSUS WIRELESS

Numerous factors should be considered when deciding if a network should use wired or wireless connectivity, as listed below.

WIRELESS NETWORKING

It is easier to expand networks and is not necessary to connect devices using cables.

- Devices have increased mobility, provided they are within range of the WAPs.
- Increased chance of interference from external sources.
- Data is less secure than with wired systems; it is easier to intercept radio waves and microwaves than cables so it is essential to protect data transmissions using encryption (such as WEP, WPA2).
- Data transmission rate is slower than wired networks (although it is improving).
- Signals can be stopped by thick walls (in old houses, for example) and signal strength can vary, or 'drop out'.

WIRED NETWORKING

- More reliable and stable network (wireless connectivity is often subjected to interference).
- Data transfer rates tend to be faster with no 'dead spots'.
- Tends to be cheaper overall, in spite of the need to buy and install cable.
- Devices are not mobile; they must be close enough to allow for cable connections.
- Lots of wires can lead to tripping hazards, overheating of connections (potential fire risk) and disconnection of cables during routine office cleaning.

OTHER CONSIDERATIONS

- If mobile phones and tablets are connected to the network, it will need to offer Wi-Fi or Bluetooth capability.

- There may be regulations in some countries regarding which wireless transmission frequencies can be used legally.
- Permission from authorities and land owners may be required before laying cables underground.
- There are numerous competing signals in the air around us; it is important to consider this when deciding whether to go for wired or wireless connectivity.

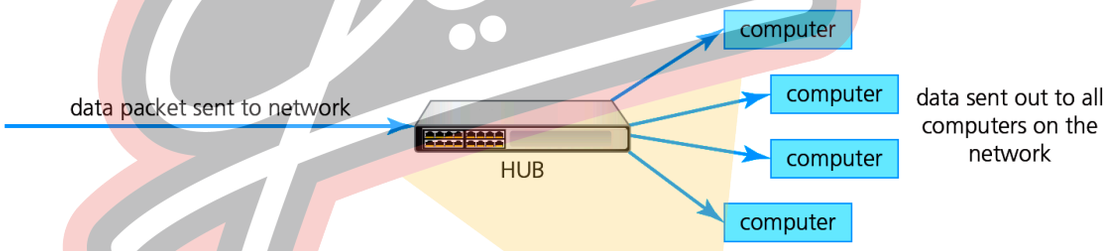
HARDWARE REQUIREMENTS OF NETWORKS

In this section we will consider a number of hardware items needed to form a LAN network and the hardware needed to form a WAN. Please note

- the concept of the WLAN and the hardware needed to support it have been covered in earlier sections
- the hardware items hub and gateway have been included in this section to complete the picture; however, knowledge of these two items is not required by the syllabus.

HUB

Hubs are hardware devices that can have a number of devices or computers connected to them.

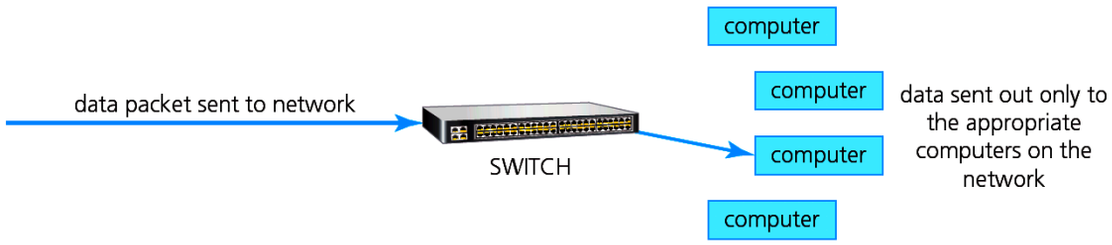


They are often used to connect a number of devices to form a local area network (LAN), for example a star network. A hub's
main task is to take any data packet (a group of data being transmitted) received at one of its ports and then send the data to every computer
in the network. Using hubs is not a very secure method of data distribution and is also wasteful of bandwidth. Note that hubs can be wired or
wireless devices.

SWITCH

Switches are similar to hubs, but are more efficient in the way they distribute the data packet. As with hubs, they connect a number of devices or computers together to form a LAN (for example, a star network).
However, unlike a hub, the switch checks the data packet received and works out its destination address (or addresses) and sends the data to the appropriate

computer(s) only. This makes using a switch a more secure and efficient way of distributing data.



Each device or computer on a network has a media access control (MAC) address which identifies it uniquely. Data packets sent to switches will have a MAC address identifying the source of the data and additional addresses identifying each device which should receive the data. Note that switches can be wired or wireless devices.

REPEATER

When signals are sent over long distances, they suffer attenuation or signal loss. Repeaters are devices which are added to transmission systems to boost the signal so it can travel greater distances. They amplify signals on both analogue (copper cable) and digital (fibre optic cable) communication links.

Repeaters can also be used on wireless systems. These are used to boost signals to prevent any 'dead spots' in the Wi-Fi zone. These devices plug into electric wall sockets and send out booster signals. They are termed non-logical devices because they will boost all signals which have been detected; they are not selective.

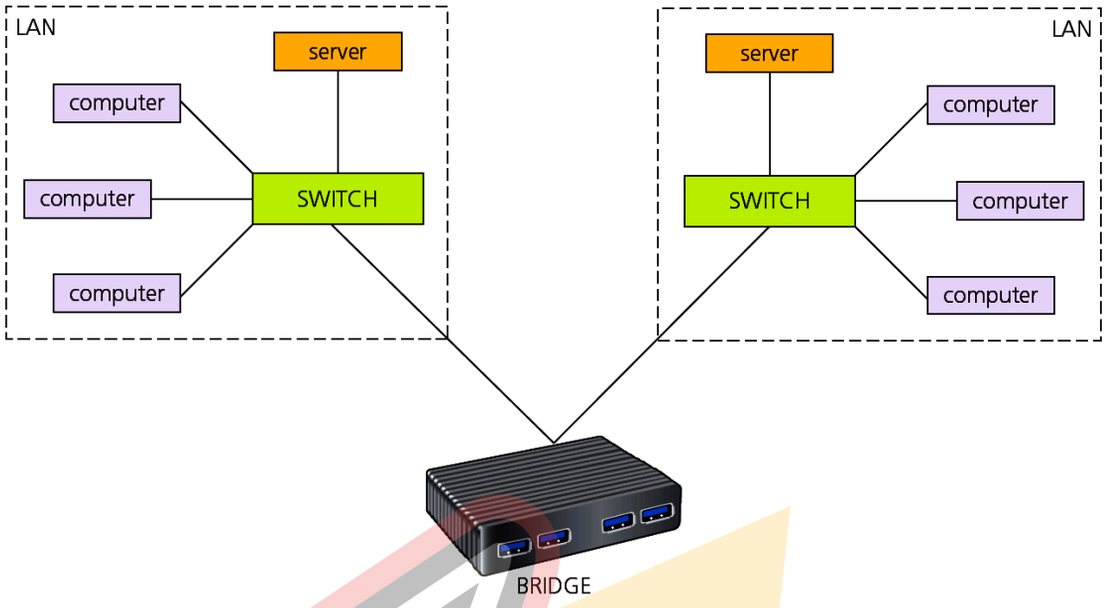
Sometimes, hubs contain repeaters and are known as repeating hubs. All signals fed to the hub are boosted before being sent to all devices in the network, thus increasing the operational range.

There are two main drawbacks of repeating hubs:

1. They have only one collision domain. When the signals are boosted and then broadcast to devices, any collisions which might occur are not resolved there and then. One way to deal with this problem is to make use of jamming signals – while this manages the collisions, it also reduces network performance since it involves repeated broadcasts as the collisions are resolved.
2. The devices are referred to as unmanaged since they are unable to manage delivery paths and also security in the network.

BRIDGE

Bridges are devices that connect one LAN to another LAN that uses the same protocol (communication rules). They are often used to connect together different parts of a LAN so that they can function as a single LAN.



Bridges are used to interconnect LANs (or parts of LANs), since sending out every data packet to all possible destinations would quickly flood larger networks with unnecessary traffic. For this reason, a router is used to communicate with other networks, such as the internet. Note that bridges can be wired or wireless devices.

ROUTER

Routers enable data packets to be routed between the different networks for example, to join a LAN to a WAN. The router takes data transmitted in one format from a network (which is using a particular protocol) and converts the data to a protocol and format understood by another network, thereby allowing them to communicate via the router. We can, therefore, summarise the role of routers as follows. Routers

- restrict broadcasts to a LAN
- act as a default gateway
- can perform protocol translation; for example, allowing a wired network to communicate with a wireless (Wi-Fi) network – the router can take an Ethernet data packet, remove the Ethernet part and put the IP address into a frame recognised by the wireless protocol (in other words, it is performing a protocol conversion)
- can move data between networks
- can calculate the best route to a network destination address.

Broadband routers sit behind a firewall. The firewall protects the computers on a network. The router's main function is to transmit internet and transmission protocols between two networks and allow private networks to be connected.

The router inspects the data package sent to it from any computer on any of the networks connected to it. Since every computer on the same network has the same part of an internet protocol (IP) address, the router is able to send the data packet to the appropriate switch and it will then be delivered using the MAC destination address (see next section). If the MAC address doesn't match any device on the network, it passes on to another switch on the same network until the appropriate device is found. Routers can be wired or wireless devices.

GATEWAY

A gateway is a network point (or node) that acts as an entrance to another network. It is a key point for data on its way to or from other networks. It can be used to connect two or more dissimilar LANs (LANs using different protocols). The gateway converts data packets from one protocol to another. Gateways can also act as routers, firewalls or servers – in other words, any device that allows traffic to flow in and out of the networks. Gateways can be wired or wireless devices.

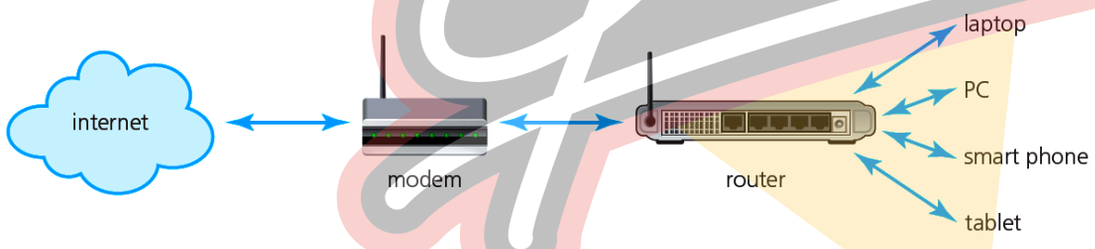
All networks have boundaries so that all communication within the network is conducted using devices such as switches or routers. If a network node needs to communicate outside its network, it needs to use a gateway.

MODEMS

Modern computers work with digital data, whereas many of the public communication channels still only allow analogue data transmission. To allow the transmission of digital data over analogue communication channels we need to use a modem (modulator demodulator). This device converts digital data to analogue data. It also does the reverse and converts data received over the analogue network into digital data which can be understood by the computer.

Wireless modems transmit data in a modulated form to allow several simultaneous wireless communications to take place without interfering

with each other. A modem will connect to the public infrastructure (cable, telephone, fibre-optics or satellite) and will supply the user with a standard Ethernet output which allows connection to a router, thus enabling an internet connection to occur.



While the router will allow the creation of a network in a home, for example, the modem allows for the connection to the external networks

(for example, the internet). Routers and modems can be combined into one unit; these devices have the electronics and software to provide both router and modem functions.

Another example of a modem is a softmodem (software modem), which uses minimal hardware and uses software that runs on the host computer. The computer's resources (mainly the processor and RAM) replace the hardware of a conventional modem.

Routers	Gateways
■ forward packets of data from one network to another; routers read each incoming packet of data and decide where to forward the packet	■ convert one protocol (or data format) to another protocol (format) used in a different network
■ can route traffic from one network to another network	■ convert data packets from one protocol to another; they act as an entry and exit point to networks
■ can be used to join LANs together to form a WAN (sometimes called brouters) and also to connect a number of LANs to the internet	■ translate from one protocol to another
■ offer additional features such as dynamic routing (ability to forward data by different routes)	■ do not support dynamic routing

NETWORK INTERFACE CARD (NIC)

A network interface card (NIC) is needed to allow a device to connect to a network (such as the internet). It is usually part of the device hardware and frequently contains the MAC address generated at the manufacturing stage.

WIRELESS NETWORK INTERFACE CARD/CONTROLLER (WNIC)

Wireless network interface cards/controllers (WNICs) are the same as the more ordinary NICs, in that they are used to connect devices to the internet or other networks. They use an antenna to communicate with networks via microwaves and normally simply plug into a USB port or can be internal integrated circuit plug in.
As with usual NICs, they work on layers 1 and 2 of the OSI model (refer to Chapter 14 for more details). WNICs work in two modes.
Infrastructure mode requires WAPs (wireless access points) and all the data is transferred using the WAP and hub/switch; all the wireless devices connect to the WAP and must use the same security and authentication techniques.
Ad hoc mode does not need to have access to WAPs; it is possible for devices to interface with each other directly.

ETHERNET

Ethernet is a protocol used by many wired LANs. It was adopted as a standard by the Institute of Electrical and Electronic Engineers (IEEE) and Ethernet is also known as IEEE 802.3. A network using Ethernet is made up of:

» a node (any device on the LAN)
» medium (path used by the LAN devices, such as an Ethernet cable)

» frame (data is transmitted in frames which are made up of source address and destination address – the addresses are often the MAC address).

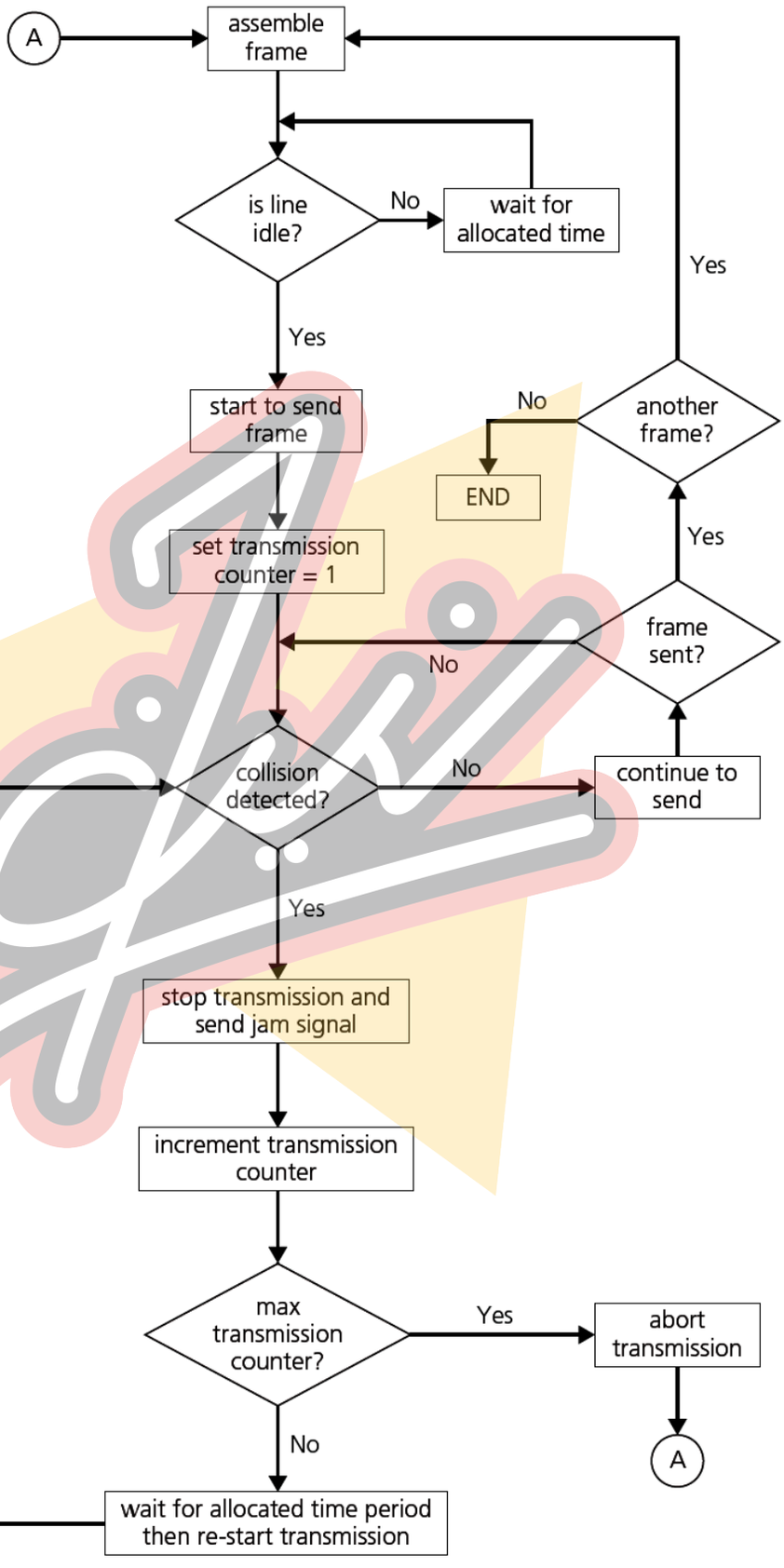
CONFLICTS

When using Ethernet, it is possible for IP addresses to conflict; this could show up as a warning, This may occur if devices on the same network have been given the same IP address; without a unique IP address it is not possible to connect to a network. This is most likely to occur on a LAN where dynamic IP addresses may have been used. Dynamic IP addresses are temporary and may have been assigned to a device on the network, unfortunately, another device using static IP addresses may already have the same IP address. This can be resolved by re-starting the router. Any dynamic IP addresses will be re-assigned, which could resolve the issue.

COLLISIONS

Ethernet supports broadcast transmission (communications where pieces of data are sent from sender to receiver) and are used to send messages to all devices connected to a LAN. The risk is that two messages using the same data channel could be sent at the same time, leading to a collision. Carrier sense multiple access with collision detection (CSMA/CD) was developed to try and resolve this issue. Collison detection depends on simple physics: when a frame is sent it causes a voltage change on the Ethernet cable. When a collision is detected, a node stops transmitting a frame and transmits a 'jam' signal and then waits for a random time interval before trying to resend the frame. CSMA/CD protocol will define the random time period for a device to wait before trying again.

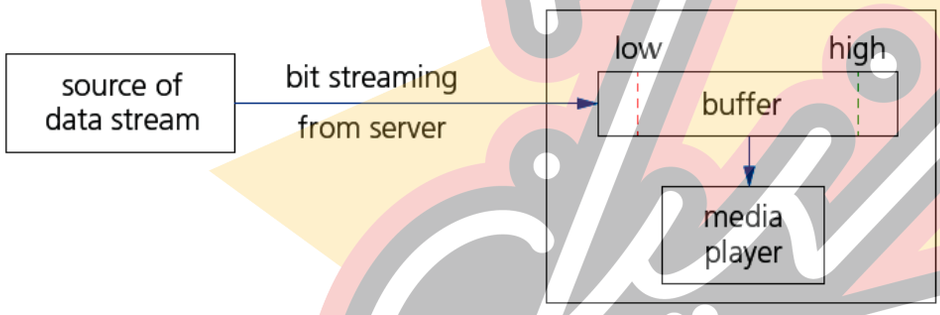
Figure shows how data collisions can be dealt with using transmission counters (which keep track of how many times the collision detection routine has been entered – there will a defined limit as part of the CSMA/CD protocol) and random time periods.


A
assemble frame
is line idle?
No
wait for allocated time
Yes
start to send frame
set transmission counter = 1
collision detected?
No
Yes
stop transmission and send jam signal
increment transmission counter
max transmission counter?
Yes
abort transmission
A
No
wait for allocated time period then re-start transmission
frame sent?
No
Yes
continue to send
another frame?
No
END
Yes

BIT STREAMING

Bit streaming is a contiguous sequence of digital bits sent over the internet or a network that requires a high speed data communication link (such as fast broadband). Since bit streaming often involves very large files (such as video) it is necessary for the files to undergo some data compression before transmission. It is also necessary to have some form of buffering to ensure smooth playback of the media files.

The data transmission rate from the file server (containing the video, for example) to the buffer must be greater than the rate at which data is transmitted from buffer to media player. The larger the buffer, the better the control over the bit rate being sent to the media player. The media player will always check to ensure data lies between a minimum value (often referred to as low water mark) and a maximum value (often referred to as a high water mark). The difference between the two values is usually about 80% of the total buffer capacity. The buffer is a temporary storage area of the computer.



Pros of bit streaming	Cons of bit streaming
■ no need to wait for a whole video or music file to be downloaded before the user can watch or listen ■ no need to store large files on your device ■ allows video files and music files to be played on demand (as required) ■ no need for any specialist hardware ■ affords piracy protection (more difficult to copy streamed files than files stored on a hard drive)	■ cannot stream video or music files if broadband connection is lost ■ video or music files will pause to allow the data being streamed to 'catch up' if there is insufficient buffer capacity or slow broadband connection ■ streaming uses up a lot of bandwidth ■ security risks associated with downloading files from the internet ■ copyright issues

Bit streaming can be either on demand or real time.

ON DEMAND

- Digital files stored on a server are converted to a bit streaming format
- (encoding takes place and the encoded files are uploaded to a server).
- A link to the encoded video/music file is placed on the web server to be downloaded.

- The user clicks on the link and the video/music file is downloaded in a contiguous bit stream.
- Because it is on demand, the streamed video/music is broadcast to the user as and when required.
- It is possible to pause, rewind and fast forward the video/music if required.

REAL TIME

- An event is captured by camera and microphone and is sent to a computer.
- The video signal is converted (encoded) to a streaming media file.
- The encoded file is uploaded from the computer to the dedicated video streaming server.
- The server sends the encoded live video to the user's device.
- Since the video footage is live it is not possible to pause, rewind or fast forward.

THE DIFFERENCES BETWEEN THE INTERNET AND THE WORLD WIDE WEB

There are fundamental differences between the internet and the World Wide Web (WWW).

INTERNET

- The internet is a massive network of networks which are made up of various computers and other electronic devices.
- It stands for interconnected network.
- The internet makes use of transmission control protocol (TCP)/internet protocol (IP).

WORLD WIDE WEB (WWW)

This is a collection of multimedia web pages and other documents which are stored on websites.

- http(s) protocols are written using HyperText Mark-up Language (HTML).
- Uniform resource locators (URLs) specify the location of all web pages.
- Web resources are accessed by web browsers.
- The world wide web uses the internet to access information from servers and other computers.

HARDWARE AND SOFTWARE NEEDED TO SUPPORT THE INTERNET

The fundamental requirements for connecting to the internet are

- a device (such as a computer, tablet or mobile phone)
- a telephone line connection or a mobile phone network connection (however, it is possible that a tablet or mobile phone may connect to the internet using a wireless router)
- a router (which can be wired or wireless) or router and modem
- an internet service provider (ISP) (combination of hardware and software)
- a web browser.

The telephone network system, public switched telephone network (PSTN), is used to connect computers/devices and LANs between towns and cities. Satellite technology is used to connect to other countries (see later).

In recent years, telephone lines have changed from copper cables to fibre optic cables, which permits greater bandwidth and faster data transfer rates (and less risk of data corruption from interference). Fibre optic telephone networks are usually identified as 'fast broadband'. As discussed earlier, high speed broadband has allowed WLANs to be developed by using WAPs.

High speed communication links allow telephone and video calls to be made using a computer and the internet. Telephone calls require either an internet-enabled telephone connected to a computer (using a USB port) or external/

internal microphone and speakers. Video calls also require a webcam. When using the internet to make a phone call, the user's voice is converted to digital packages using Voice over Internet Protocol (VoIP). Data is split into packages (packet switching) and sent over the network via the fastest route.

COMPARISON BETWEEN PSTN AND INTERNET WHEN MAKING A PHONE CALL

PUBLIC SWITCHED TELEPHONE NETWORK (PSTN)

PSTN uses a standard telephone connected to a telephone line.
The telephone line connection is always open whether or not anybody is talking – the link is not terminated until the receivers are replaced by both parties.
Telephone lines remain active even during a power cut; they have their own power source.
Modern phones are digitised systems and use fibre optic cables (although because of the way it works this is a big waste of capacity – a 10 minute phone call will transmit about 10 MB of data).
Existing phone lines use circuit switching (when a phone call is made the connection (circuit) is maintained throughout the duration of the call – this is the basis of PSTN).

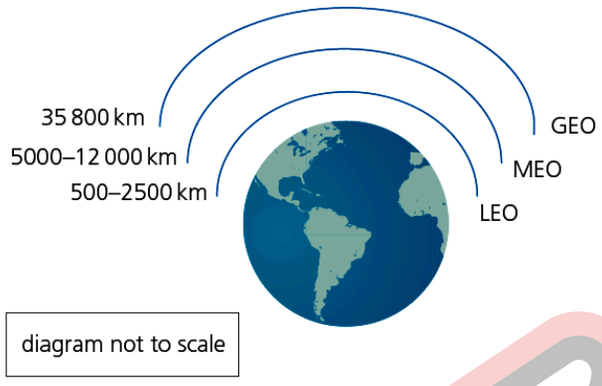
PHONE CALLS USING THE INTERNET

Phone calls using the internet use either an internet phone or microphone and speakers (video calls also require a webcam).
The internet connection is only 'live' while data (sound/video image) is being transmitted.
Voice over Internet Protocol (VoIP) converts sound to digital packages (encoding) which can be sent over the internet.
VoIP uses packet switching; the networks simply send and retrieve data as it is needed so there is no dedicated line, unlike PSTN. Data is routed through thousands of possible pathways, allowing the fastest route to be determined.
The conversation (data) is split into data packages. Each packet contains at least the sender's address, receiver's address and order number of packet – the sending computer sends the data to its router which sends the packets to another router, and so on. At the receiving end, the packets are reassembled into the original state.
VoIP also carries out file compression to reduce the amount of data being transmitted.
Because the link only exists while data is being transmitted, a typical 10 minute phone call may only contain about 3 minutes where people are talking; thus only 3 MB of data is transmitted making it much more efficient than PSTN.

CELLULAR NETWORKS AND SATELLITES

Other devices, such as mobile phones, use the cellular network. Here, the mobile phone providers act as the ISPs and the phones contain communication software which allows them to access the telephone network and also permits them to make an internet connection.

Satellites are an important part of all network communications that cover vast distances. Due to the curvature of the Earth, the height of the satellite's orbit determines how much coverage it can give. Figure shows how satellites are classified according to how high they orbit in relation to the Earth's surface.



Geostationary Earth Orbit (GEO) provide long distance telephone and computer network communications; orbital period = 24 hours

Medium Earth Orbit (MEO) used for GPS systems (about 10 MEO satellites are currently orbiting the Earth); orbital period = 2 to 12 hours

Low Earth Orbit (LEO) used by the mobile phone networks (there are currently more than 100 LEO satellites orbiting the Earth); orbital period = 80 mins to 2 hours

Satellites have the advantage that they will always give complete coverage and don't suffer from signal attenuation to the same extent as underground/undersea cables. It is also difficult to isolate and resolve faults in cables on the sea bed.

IP ADDRESSES

The internet is based on TCP/IP protocols. Protocols define the rules that must be agreed by senders and receivers on the internet. Protocols can be divided into TCP layers. We will first consider internet protocols (IP).

INTERNET PROTOCOLS (IP)

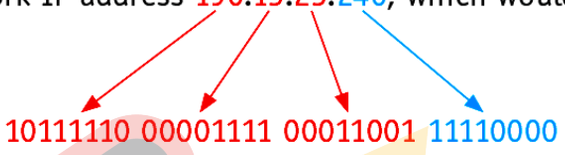
IPV4 ADDRESSING

The most common type of addressing on the internet is IP version 4 (IPv4). This is based on 32 bits giving 232 (4 294 967 296) possible addresses. The
32 bits are split into four groups of 8 bits (thus giving a range of 0 to 255). For example, 254.0.128.77.

The system uses the group of bits to define network (netID) and network host (hostID). The netID allows for initial transmission to be routed according to the netID and then the hostID is looked at by the receiving network. Networks are split into five different classes.

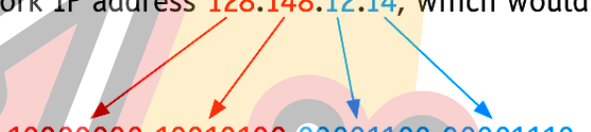
Network class	IPv4 range	Number of netID bits	Number of hostID bits	Types of network
A	0.0.0.0 to 127.255.255.255	8	24	very large
B	128.0.0.0 to 191.255.255.255	16	16	medium size
C	192.0.0.0 to 223.255.255.255	24	8	small networks
D	224.0.0.0 to 239.255.255.255	–	–	multi-cast
E	240.0.0.0 to 255.255.255.255	–	–	experimental

Consider the class C network IP address 190.15.25.240, which would be written in binary as:



Here the network id is 190.15.25 and the host ID is 240.

Consider the class B network IP address 128.148.12.14, which would be written in binary as:



Here the network ID is 128.148 and the host ID is 12.14 (made up of sub-net ID 12 and host ID of 14).

Consider the class A network IP address 29.68.0.43, which would be written in binary as:

Here the network ID is 29 and the host ID is 68.0.43 (made up of sub-net ID 68.0 and host ID of 43).

However, it soon became clear that this IPv4 system provides insufficient address range. For example, a user with a medium sized network (class B) might have 284 host machines and their class B licence allows them 216 (65534; note the value is not 65536 since two values are not assigned). This means several of the allocated host IDs will not be used, which is wasteful.

Classless inter-domain routing (CIDR) reduces this problem by increasing the flexibility of the IPv4 system. A suffix is used, such as 192.30.250.00/18, which means 18 bits will be used for the net ID and the last 14 bits will be used for the host ID (rather than the normal 24 bits and 8 bits for a class C network). The suffix clearly increases the flexibility regarding which bits represent the net ID and which represent the host ID.

IPV6 ADDRESSING

IPv6 addressing has been developed to overcome some of the problems associated with IPv4. This system uses 128-bit addressing, which allows for much more complex addressing structures. An IPv6 address is broken into 16-bit chunks and because of this, it adopts the hexadecimal notation. For example:

A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

Note how a colon (:) rather than a decimal point (.) is used here.

It has been designed to allow the internet to grow in terms of number of hosts and the potential amount of data traffic. IPv6 has benefits over IPv4, it

- has no need for NATs (network address translation)
- removes risk of private IP address collisions
- has built in authentication
- allows for more efficient routing.

ZERO COMPRESSION

IPv6 addresses can be quite long; but there is a way to shorten them using zero compression. For example, 900B:3E4A:AE41:0000:0000:AFF7:DD44:F1FF can be written as:

900B:3E4A:AE41::AFF7:DD44:F1FF

With the section 0000:0000 replaced by ::

The zero compression can only be applied ONCE to an IPv6 address, otherwise it would be impossible to tell how many zeros were replaced on each occasion where it was applied. For example, 8055:F2F2:0000:0000:FFF1:0000:0000:DD04 can be rewritten either as:

8055:F2F2::FFF1:0000:0000:DD04

or as:

8055:F2F2:0000:0000:FFF1::DD04

8055:F2F2::FFF1::DD04 is not a legal way of compressing the original address – we have no way of knowing whether the original address was

8055:F2F2:0000:FFF1:0000:0000:0000:DD04

or

8055:F2F2:0000:0000:0000:FFF1:0000:DD04

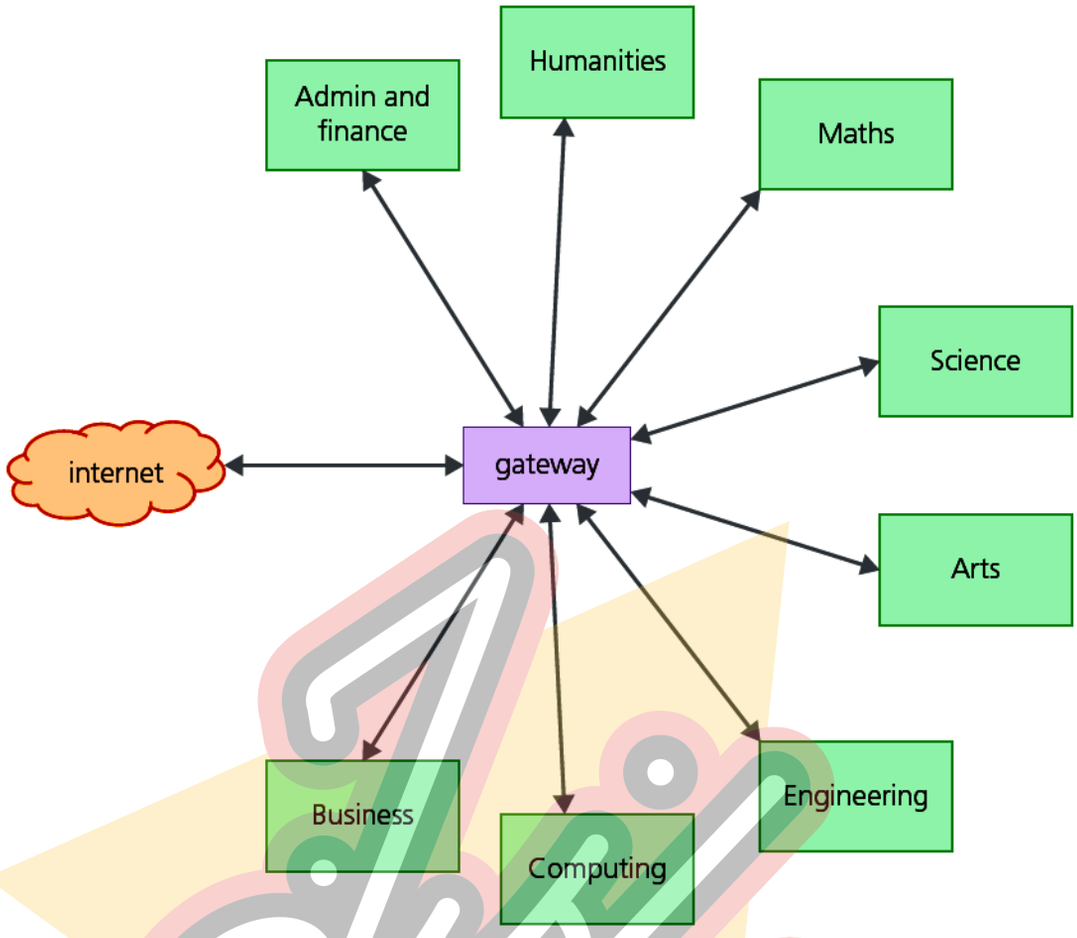
or

8055:F2F2:0000:0000:FFF1:0000:0000:DD04

It would, therefore, be regarded as ambiguous.

SUB-NETTING

CIDR is actually based on sub-netting and the two are similar in many ways. Sub-netting divides a LAN into two or more smaller networks. This helps reduce network traffic and can also hide the complexity of the overall network. Recall that the IP address (using IPv4) is made up of the netID and hostID. Suppose a university network has eight departments and has a netID of 192.200.20 (11000000.11001000.00010100). All of the devices on the university network will be associated with this netID and can have hostID values from 00000001 to 1111110 (hostIDs containing all 0s or all 1s are forbidden). The university network will look something like this:



So, for example, the devices in the Admin and finance department might have hostIDs of 1, 8, 240, 35, 67, 88, 134, and so on, with similar spreads for the other seven departments.
It would be beneficial to organise the netIDs and hostIDs so that the network was a lot less complex in nature. With sub-netting, the hostID is split as follows:
000 00000, where the first 3 bits are netID expansion and the last 5 bits are the hostIDs.
Thus, we have eight sub-nets with the same range of hostIDs.

Department	netID	hostID range
Admin and finance	192.200.20.0	00001 to 11110
Humanities	192.200.20.1	00001 to 11110
Maths	192.200.20.2	00001 to 11110
Science	192.200.20.3	00001 to 11110
Arts	192.200.20.4	00001 to 11110
Engineering	192.200.20.5	00001 to 11110
Computing	192.200.20.6	00001 to 11110
Business	192.200.20.7	00001 to 11110

The devices in the Admin and finance department will have IP addresses
192.200.20.000 00001 to 192.200.20.000 11110
The Humanities department will have IP addresses
192.200.20.001 00001 to 192.200.20.001 11110
And so on for the other departments.
To obtain the netID from the IP address we can apply the AND mask (recall that 1 AND 1 = 1, 0 AND 0 = 0 or 1 AND 0 = 0). Thus, if a device has an IP address of
11000000.11001000.00010100.011 00011
we can apply the AND mask
11111111.11111111.11111111.111 00000
which results in the netID value
11000000.11001000.00010100.011 00000 (or 192.200.20.03)
This is the Science department. Consequently, the whole network is more efficient (for the reasons stated above) and less complex. Compare this to CIDR 192/200/20/0/27, which extends the size of the netID to 27 bits and has a hostID of only 5 bits, but would not reduce the complexity of the network.

PRIVATE IP ADDRESSES AND PUBLIC IP ADDRESSES

Private IP addresses are reserved for internal use behind a router or other NAT device. The following blocks are reserved for private IP addresses.

Class A	10.0.0.0 to 10.255.255.255	16 million possible addresses
Class B	172.16.0.0 to 172.31.255.255	1 million possible addresses
Class C	192.168.0.0 to 192.168.255.255	65 600 possible addresses

Private IP addresses (which are internal value only) allow for an entirely separate set of addresses within a network. They allow access to the network without taking up a public IP address space. However, devices using these private IP addresses cannot be reached by internet users.
Public IP addresses are the ones allocated by a user's ISP to identify the location of their device. Devices using these IP addresses are accessible from anybody using the internet. Public IP addresses are used by

- DNS servers
- network routers
- directly-controlled computers.

UNIFORM RESOURCE SERVICE (URLS)

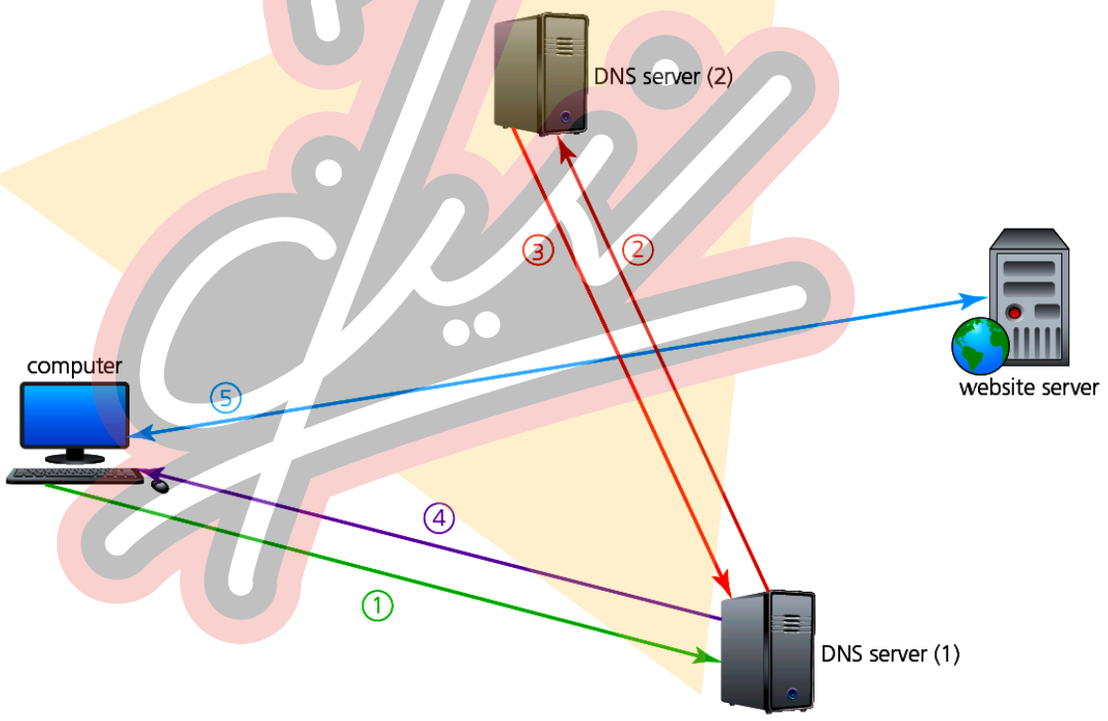
Web browsers are software that allow users to access and display web pages on their screens. They interpret HTML sent from websites and display the results. Web browsers use uniform resource locators (URL) to access websites; these are represented by a set of four numbers, such as 109.108.158.1.
But it is much easier to type this into a browser using the following format:
protocol://website address/path/filename
Protocol is usually http or https
Website address is

- domain host (www)
- domain name (name of website)
- domain type (.com, .org, .net, .gov, and so on)
- (sometimes) a country code (.uk, .de, .cy, .br, and so on).

Path is the web page (if this is omitted then it is the root directory of the website)
Filename is the item from the web page
For example: http://www.hoddereducation.co.uk/computerscience

DOMAIN NAME SERVICE (DNS)

The domain name service (DNS) (also known as domain name system) gives domain names for internet hosts and is a system for finding IP addresses of a domain name. Domain names eliminate the need for a user to memorise IP addresses. The DNS process involves converting a host name (such as www.hoddereducation.co.uk) into an IP address the computer can understand (such as 107.162.140.19).
Often, DNS servers contain a database of URLs with the matching IP addresses.



① The user opens their web browser and types in the URL (www.hoddereducation.co.uk) and the web browser asks the DNS server (1) for the IP address of the website.

② The DNS server can't find www.hoddereducation.co.uk in its database or its cache and sends out a request to DNS server (2).

③ DNS server (2) finds the URL and can map it to 107.162.140.19; the IP address is sent back to DNS server (1) which now puts the IP address and associated URL into its cache/database.

④ This IP address is then sent back to the user's computer.

⑤ The computer now sets up a communication with the website server and the required pages are downloaded. The web browser interprets the HTML and displays the information on the user's screen.

SCRIPTING IN HTML

This section considers HTML scripting using JavaScript and PHP. While this extends beyond the syllabus, it is included here to help you understand how HTML is used to create websites and how web browsers communicate with servers. It is included here for information and to aid understanding.

A user may wish to develop a web application, which is client-server based, on their own computer. To do this they would need to:

- download the necessary server software
- install the application on the chosen/allocated server
- use the web browser on their computer to access and interpret the application web pages.

Each web page would need to be created using HTML. A domain name would have to be purchased from a web-hosting company. The HTML files would need to be uploaded to the server which was allocated to the user by the web-hosting company.

HTML would be used to create a file using tags. For example:

```
<html>
<body>
<p> Example <p/>
[program code]
</html>
```

Between the HTML tags the inclusion of JavaScript or PHP can be used.

JAVASCRIPT

JavaScript (unlike HTML) is a programming language which will run on the client-side. What is the difference between running on the client-side and running on the server-side?

- Client-side – the script runs on the computer, which is making the request, processing the web page data that is being sent to the computer from the server.
- Server-side – the script is run on the web server and the results of processing are then sent to the computer that made the request.

The following short program inputs a temperature and outputs 'HIGH' if it is 200 °C or over, 'OK' if it is 100 °C or over and 'LOW' if it is below 100 °C.

```
<html>
<body>
<p>Enter the temperature</p>
<input id="Temp" value="0"
<button onclick="checkReading()>"Enter</button>
<script>
  function checkReading() {
    var temp, result;
    temp = document.getElementById("Temp").value;
    if (temp >= 200) {
    result = "HIGH"
    } else if (temp >= 100) {
      result = "OK"
    } else {
      result = "LOW"
    }
    alert("The result is " + result)
  }
</script>
</body>
</html>
```

PHP

PHP is another language which can be embedded within HTML. However, when PHP is used it is processed on the server-side. Again, the code will be sandwiched inside HTML and will be stored as a .php file.

The following example is similar to the JavaScript example; again temperatures are input but this time 'H', 'O' and 'L' are output depending on the result. Note that variables begin with $ and are case-sensitive.

```
<?php
  if(isset($ _ GET['temp'])) {
  echo "Result: " . checkReading($ _ GET['temp']);
  } else {
?>
<form action="#" method="get">
  Enter Temp: <input type="text" name="temp" /><br />
  <input type="submit" value="Calculate" />
  </form>

<?php
  }
    function checkReading($inputTemp) {
      $resultChar = "L";
    if($inputTemp >= 200) $resultChar = "H";
    else if($inputTemp >= 100) $resultChar = "O";
    return $resultChar;
  }
?>
```