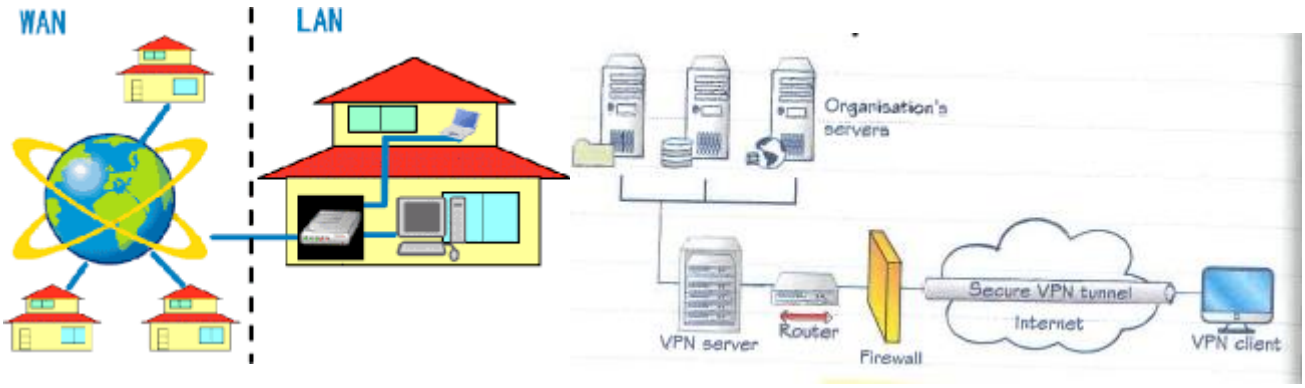
BTEC Level 3

Unit 1: Information Technology Systems

Learning Aim B: Transmitting Data

Knowledge and Assessment Organiser



Student name: .....

Big Question

How is data transferred within IT systems?

Contents

Key command words

Command or term	Definition
Analyse	Learners examine in detail a scenario or problem to discover its meaning or essential features. Learners will break down the problem into its parts and show how they inter-relate. There is no requirement for any conclusion.
Assess	Learners give careful consideration to all the factors or events that apply and identify which are the most important or relevant. Make a judgement on the importance of something.
Calculate	Learners apply some form of mathematical or computational process.
Complete	Learners complete a diagram or process. Can apply to problems/solutions of varying complexity.
Demonstrate	Learners illustrate and explain how an identified computer system or process functions. May take the form of an extended writing response, a diagram or a combination of the two.
Describe	Learners provide an account of something, or highlight a number of key features of a given topic. May also be used in relation to the stages of a process.
Discuss	Learners investigate a problem or scenario showing reasoning or argument.
Draw	Learners represent understanding through the use of a diagram or flowchart.
Explain	Learners denote a series of linked points needed and/or justify or expand on an identified point required.
Evaluate	Learners review and synthesise information to provide a supported judgement about the topic or problem. Typically, a conclusion will be required.
Identify	Learners assess factual information, typically when making use of given stimuli. Requires a single-word or short-sentence answer.
Produce	Learners provide a solution that applies established constructs to a given computing problem.
State, name, give	Learners assess factual information. Requires a single-word or short-sentence answer.
Write	Learners produce a solution, or mechanism used as part of, a solution to a given computing problem.

What is my big question?

How is data transferred within IT systems?

- What are the different types of connectivity?
- What are the different types of networks and there purpose?
- How do the different factors affect the choice of the network?
- What are the issues affecting data transmission?
- What is the difference between lossy and lossless?
- What is bandwidth and latency?

B1: Connectivity

Computers need to transmit data. This can be internally transmitting data between the different components (such as between the CPU and RAM), or it can be externally transmitting data between an IT system and it's peripherals.

In order to transmit data though we need to connect the different devices that need to communicate. This can be done either through physical wires or wirelessly, with different methods providing their own benefits & limitations.

Wired connection methods

Wired methods of connecting devices are any method that uses physical cables to connect between devices, systems or components. Different types of connections rely on widely differing connectors depending on what the signal or data is transmitting.

Wired system connection methods

	Uses	Advantages	Limitations
Cat5	Telephone communications and ethernet networks.	👍 Versatile and widely available. 👍 Cheap compared to other networking options.	👎 Only useful over shorter distances. 👎 More susceptible to interference than other wired techniques such as fibre.
Coaxial	All types of data communication, commonly used in television cabling.	👍 Less susceptible to interference than UTP/STP so works over longer distances. 👍 Cheap, though not as cheap as UTP/STP.	👎 Thickness of cable makes it difficult to work with. 👎 Limited bandwidth.
Fibre optic	Telephone and internet cables, cable television and computer networking.	👍 Improved security as the cable cannot be tapped. 👍 Can be used over long distances. 👍 High data transfer rate.	👎 Very expensive. 👎 Specialist skills needed to install.

Wired device connections

	Uses	Advantages	Limitations
VGA	Analogue connection of video display equipment, such as projectors, CRTs or LCDs.	Universally used on high-resolution display equipment. Low-cost cabling.	Cumbersome cabling. Signal affected over distance (noise). No DRM (digital rights management).
HDMI	Digital connection of both video and sound from devices to display equipment.	Capable of 8k (and beyond) resolution. Used in computing and entertainment.	Limited length. Cabling and technology is more expensive than analogue equivalents such as VGA.
USB/ FireWire	Connecting equipment and peripherals, such as printers, scanners, input devices, cameras.	High speed capability. Backwards compatibility. Can connect multiple devices.	Limited distance. Limited power supply.

Wireless connection methods

Wireless connection methods connect using electromagnetic spectrum. This may be traditional radio waves or eve light waves.

Wireless system connection methods

	Uses	Advantages	Limitations
WiFi	To connect devices wirelessly to local and wide area networks such as the internet.	High data transfer speeds. Good range. Relatively cheap to install.	Can be complex. Security concerns.
3G/4G/ WiMAX	To connect to data networks such as the internet whilst on the move.	Allows true mobility. 4G provides for very fast connection speeds.	Heavy data usage can be costly. Uses public networks.
Satellite broadband	Provides connectivity to remote areas, often rural.	Wide coverage. High speed.	High latency. Subject to weather conditions.
Microwave/ Laser	Allows point-to-point LAN connections between locations.	High speed. No ongoing costs.	Affected by poor weather. High initial cost.

Wireless connections methods for devices

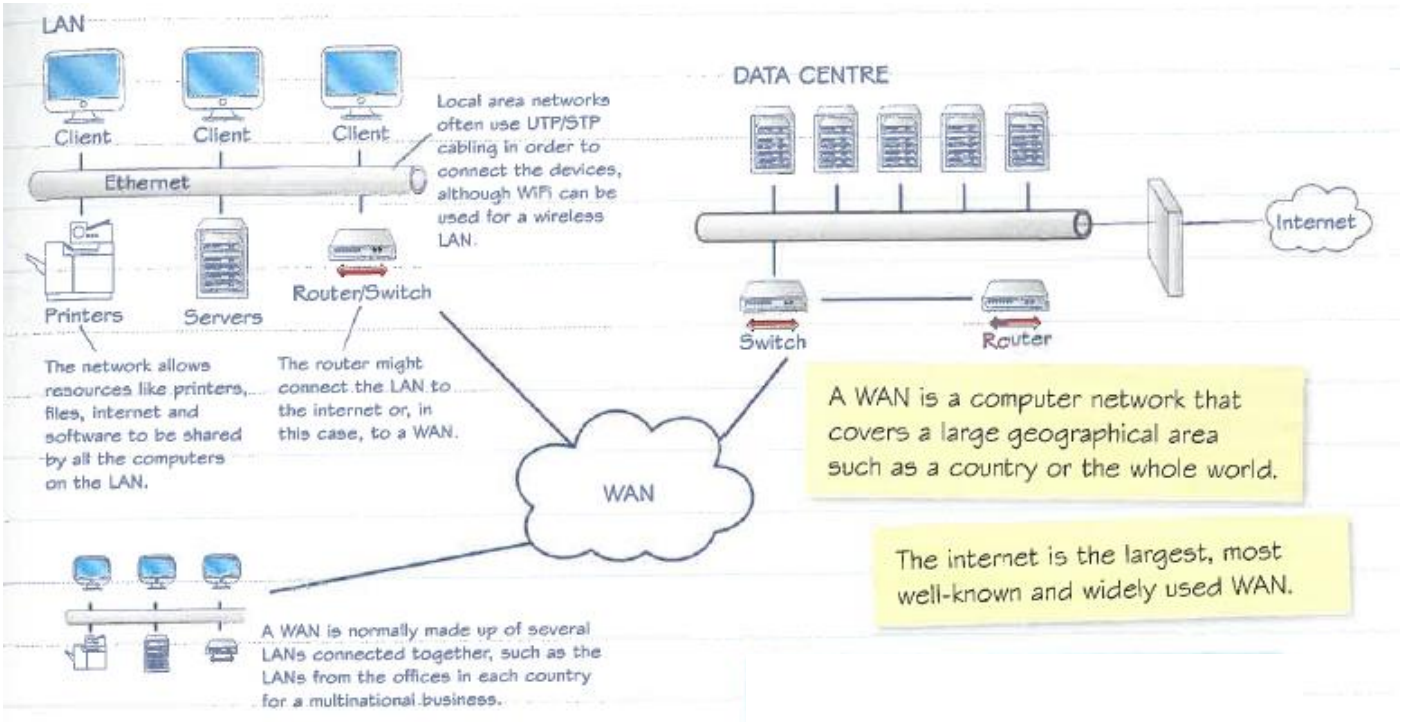
	Uses	Advantages	Limitations
Bluetooth	For pairing devices over short distances, such as wireless headphones, watches, keyboards and mice.	Easy to set up. Low power consumption.	Low data transfer speeds. Very short range.
WiFi Direct	For connecting devices to remote displays.	Can transmit both audio and video. Usually built in to devices.	Limited range. Can affect data connectivity (interference).
WiFi	Allows 'ad-hoc' networks to permit wireless printing/ scanning, for example.	Simple setup. Uses existing WiFi infrastructure.	Using ad-hoc networks can impact connectivity.

B2: Networks

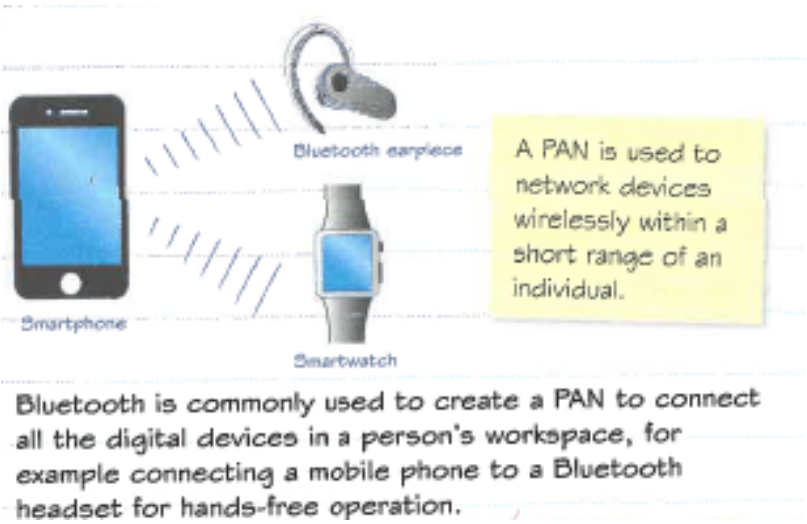
Types of networks

Different types of networks can be defined by their size (personal, local, wide area networks) or by their purpose (virtual private networks).

- Local Area Network Vs Wide Area Network



⇨ Personal area network (PAN)

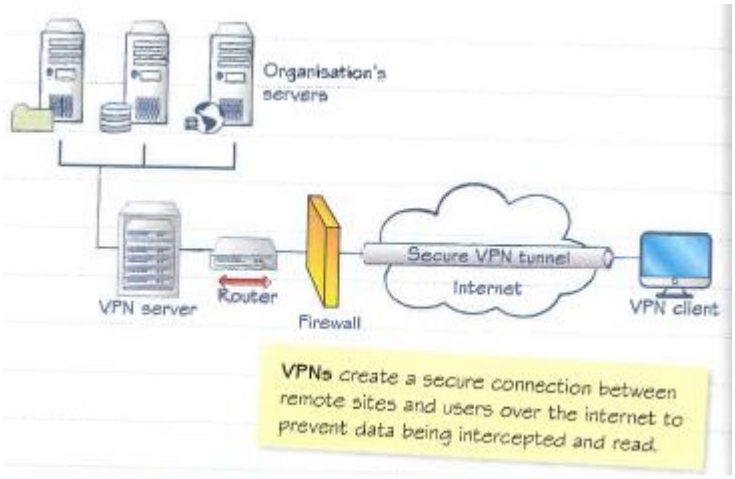


Bluetooth is commonly used to create a PAN to connect all the digital devices in a person's workspace, for example connecting a mobile phone to a Bluetooth headset for hands-free operation.

⇨ Virtual Private Network

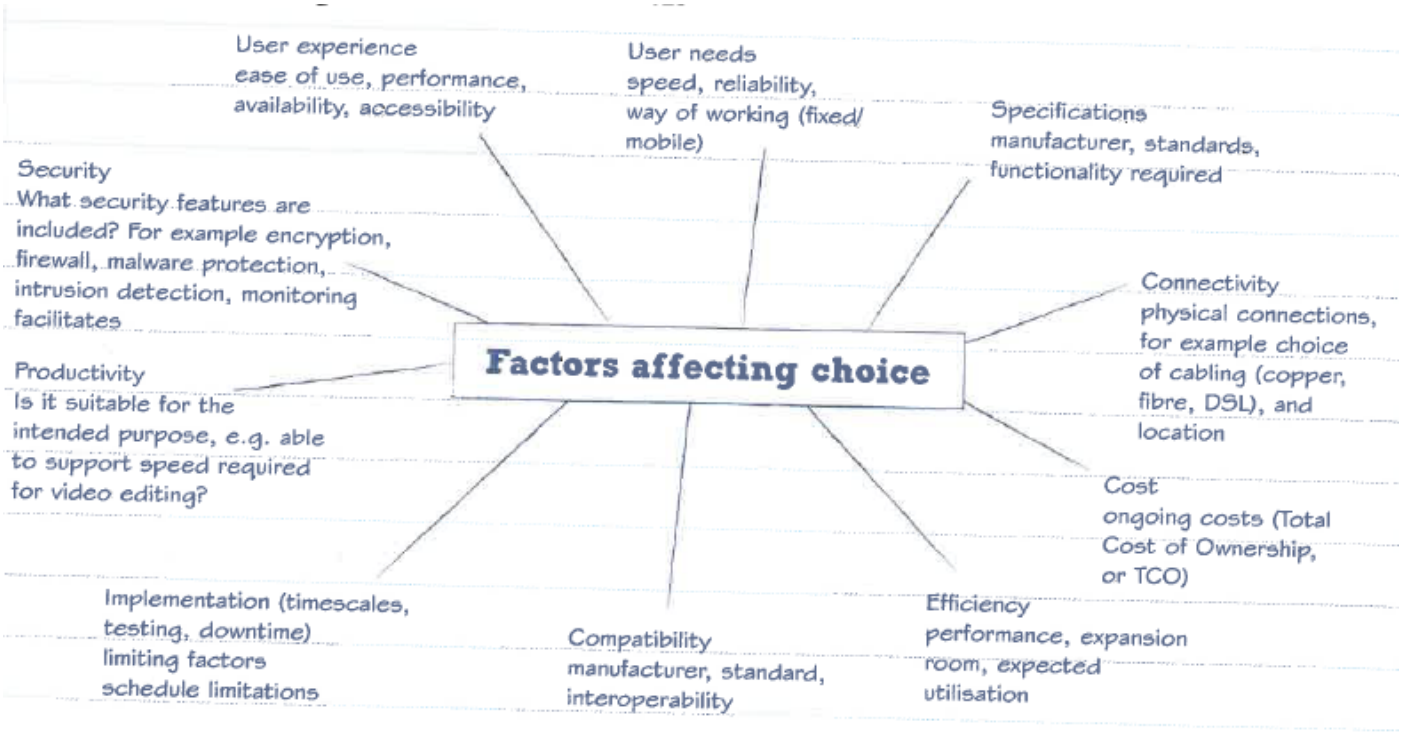
This network technology creates a secure network connection over a public network, usually the internet, by using encryption.

This allows a business to have a secure wide area network without having to pay high costs of constructing the physical network infrastructure, as they can use existing internet infrastructure.



Factor affecting the choice of network

Networks are all around us and are as unique as the users who use them. There are many factors and reasons for selecting the various components that make up a network.



⇨ User Experience

When choosing a network you want it to be accessible to its users. For some people connecting to a network can be a confusing and complex process, especially if they're IT skills are not strong.

Some of the user experience factors include:

- Ease of Use – How simple it is for a user to connect to the network. Hardwired networks are quite simple for most users. WiFi can be made more complex through the use of passwords and special proxy settings.
- Performance – How fast the network is at transferring data. Someone looking to upload and download media files like audio & video will require fast transfer speeds. Someone looking to just access emails needs only relative small speeds.
- Availability – How easily available it is for the users. People living in rural areas, for example, often cannot access fibre optic or mobile broadband services.
- Accessibility – How suitable the network is for access from someone with a disability.

Depending on your user's skills and requirements, each of these factors may have different levels of importance. If you need to transfer large data files then performance is important, if you have poor IT experience then ease-of-use is very important.

⇨ User Needs

This is about what the network is going to be used for. Why is the network required? What tasks are going to be completed using it?

A business, for example, may be creating a network to allow employees to share access to files. Does this need to be in a single building, or across multiple buildings in different cities? This could affect whether a LAN or WAN is needed and therefore the technology required.

Another example may be a home user who needs to tether her laptop to her smartphone in order to share its 4G connection. She would need a simple PAN, using either USB or Bluetooth, rather than an entire LAN setup.

⇨ Specification

This is the specific requirements for the network, in terms of data transfer speed, maximum bandwidth, power consumption & functionality.

This depends closely on the needs of the user and can vary widely. If the network requires file sharing functionality then file server hardware/software will need to be purchased and implemented. If the network will have heavy data transfer requirements then it will need a large maximum bandwidth.

⇨ Connectivity

This is about how the network will be connected to, such as via WiFi or cable broadband.

This is balanced over the user needs for speed, capacity, user experience and reliability. A business that regularly transmits data over the internet between its offices will demand high speeds, capacity and strong reliability.

However, a home user will often prioritise user experience, as they will not have the technical expertise available for setup and maintenance.

⇨ Cost

This is how much the network will cost financially to set up and maintain. There is a huge range of costs depending on the technologies used and this makes it a major consideration.

An example of this is a business that requires a WAN to share confidential data between its offices in different cities. A dedicated private WAN may be ideal but is extremely expensive. Potentially over £1000 per month.

Using a VPN will reduce the costs significantly. You will be paying more like £5 per month per user. While you may not have the same performance or security, this cost saving is often worth it.

⇨ Efficiency

This is about how effectively our network allows us to complete our tasks with as little wastage of resources (such as time and staff).

An example of this would be old-fashioned dial-up networks. The time waiting for the computer to dial-in to the network was wasted time and so was not efficient.

In a workplace using WiFi connections may allow you to work more portably and have less cabling. However, it is also slower and will take longer to log in, browse the web and open files.

In many situations, particularly in business, we need to ensure our network does not prevent us from completing our work efficiently.

⇨ Compatibility

This is about whether the network technology you are using is compatible with the devices connecting to the network.

If you use a tablet or smartphone device for connecting to a network, then using Ethernet cabling for your network would not be wise. This is because most mobile devices do not have Ethernet ports, and so, are not compatible with these devices.

Similarly, using WiFi when your companies' desktop computers do not have wireless networking cards would be hugely wasteful as you'd need to purchase upgrades for all your machines.

⇨ Implementation

This is about the time and ease involved with putting a new network into effect. This might be the time it takes for installing the network, the ease of configuring and testing it or the downtime required when implementing the network.

Some of the implementation factors to consider with a new IT system include:

- Timescales – The time it takes for the new network to be delivered. This involves the lead time with any hardware arriving, the time it takes to install any hardware and the time it takes to configure that hardware.
- Testing – Extensive testing of a network when implemented is required to ensure it works effectively. This might involve checking multiple devices, different services and different locations for example.
- Downtime – The length of time we will be without access to our network services. When implementing the network it may be that the old network services will not be accessible which will lead to business operations halting.

An example where implementation has an impact would be when you select a new home broadband provider. It might be that some ISPs will have a long lead time before they can deliver your modem, or activate the internet in your home. This may have an impact on your choice if you are in a hurry.

⇨ Productivity

This is about how quickly tasks can be completed when making use of the network. This is very important in businesses who rely on their network, as they want staff to complete their work quickly and efficiently.

Network downtime, for example, would have a big impact on productivity as you wouldn't be able to access resources provided over the network while it's down. Often in a business, this can halt productivity almost entirely.

⇨ Security

This is about how safe the network is from security threats, such as hackers. This is particularly important for businesses transmitting data across a country or the whole world.

If a business wants all the employees to have access to certain files that should be confidential to those outside the business, they may share them on a LAN. This is only accessible within the business itself and so is relatively secure.

However, if they needed to have those files accessibility outside of the business office, a LAN would be no use but the internet would be too dangerous as data could be intercepted and misused. So a business may choose a private WAN or use a VPN for greater security.

Network performance factors

The features of a network and its components can affect the performance of an IT system. Every component could potentially slow down your network and thus your IT system performance. For example:

- A servers CPU and memory could be overwhelmed by heavy usage leading to the server crashing. This would prevent access to the services they provide.
- Limited bandwidth in your data transmission method would mean slow data transfer speed. This could case logging in & saving/loading files to take a long time.
- Firewalls used for security on the network can slow down data transfer due to checking packets for threats.
- SOHO (Small Office Home Office) networking equipment being used cannot provide the performance of professional equipment.

We can correct these issues by investing in our network infrastructure and regularly maintaining and updating it, however, this is very costly.

B3: Issues relating to transmission of data

Protocols

These are the rules that define methods of communicating data between two or more digital devices. They ensure that the transmission of data always follows a set procedure. There are different protocols for different applications.

⇨ TCP/IP

Transmission Control Protocol and Internet Protocol are used together as the basic communication language of the internet.

Data is sent over the internet in to broken 'packets' to enable it to be sent more efficiently. Each packet is them reassembled at the destination.

TCP is used to create the packets and reassemble them at the end. Whereas the IP is used to route packets to the intended computer, using the computers IP address.

⇨ Email

SMTP – the Simple Mail Transfer Protocol is used to transfer emails between mail servers. It is also used to transfer email from the client software to the outgoing mail server.

POP3 – the Post Office Protocol 3 is used to retrieve emails from the mail server. It allows us to download messages to our client software for offline reading.

IMAP – the Internet Message Access Protocol is used to retrieve emails from the mail server. Rather than downloading the messages, IMAP syncs them with the mail server.

⇨ Video and video calls

Many companies use their own proprietary protocols for voice and video calls over the internet. Some well-known protocols are:

H.323 – this was one of the first successful VOIP protocols and is recommended by the ITU (International Telecommunication Union). It defines the rules for communicating audio and video over packet switched networks.

SIP – the Session Initiation Protocol is used to create, control and end VOIP connections.

RTP – the Real-time Transport Protocol is designed to transfer audio and video over IP-based networks.

- Webpages

- Security protocols

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are used to ensure that transactions over networks are kept safe. SSL is gradually being phased out and replaced with TLS.

- Secure payment systems

E-commerce is reliant on the ability to pay for goods online securely. The dangers of online bank fraud are well known and still cause some people to avoid purchasing online.

As mentioned in the web page section above, HTTPS allows for the transmission of data securely over the internet. This is used for transmitting bank details to the retailer securely so they can process the transaction.

Some protocols that are used specifically for secure payment systems are:

SET

The Secure Electronic Transaction protocol is a communications protocol that was initially supported by MasterCard & VISA for secure payments. It did not gain much popularity though and isn't in heavy use.

With SET, when a purchase process is started only the purchase order is sent to the merchant website, the card details instead go to the merchant's bank. This will then authorise the payment with the purchaser's bank and the authorisation is returned to the merchant website to complete the transaction.

3D Secure

The 3D Secure protocol is the popular method for secure online payments used by VISA, MasterCard, American Express and most others. It is an XML protocol that uses SSL encryption to ensure data is secure.

During a purchase process, when a user submits their card details for payment, the merchant website will establish if the card is enrolled on 3D secure. If so, the buyer will be directed to a 3D secure page for their own bank to authenticate the buyer. This successful authentication is forwarded to the merchant website who can then send the buyer's card details and the 3D secure authentication to their own bank to authorise the payment.

Transmission Issues

Data transmission is an important part of computer use. It involves sending digital messages between devices in a network, such as LAN or over the internet.

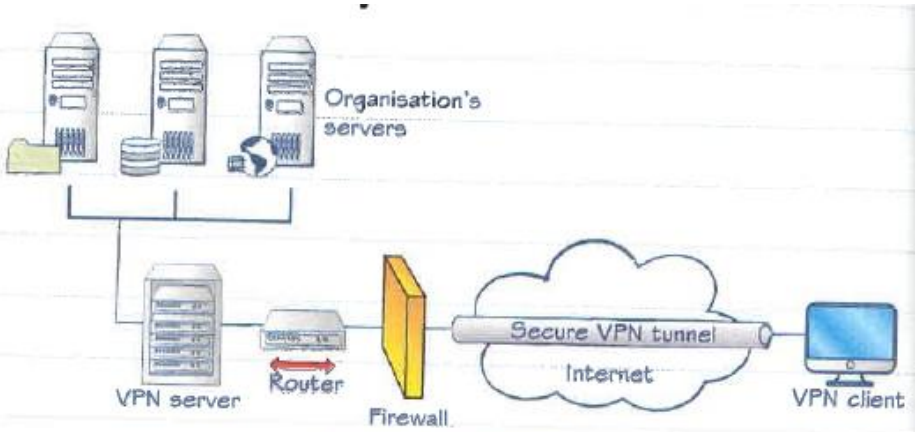
Some of the issues are:

- ⇨ Security consideration

User authentication – usernames and passwords authenticate users who have permission to use a network and prevent unauthorised access by hackers.

Firewalls – these monitor traffic to prevent unauthorised access and dangerous data packets being passed into the system and causing harm.

Encryption – information can be intercepted while being transmitted. Using encryption ensures intercepted data cannot be read. HTTPS is a commonly used method for secure data transmission.



VPNs create a secure connection between remote sites and users over the internet to prevent data being intercepted and read.

Packet sniffers

Packet sniffers are legitimate programs used commonly by network technicians to diagnose problems with a network. However, they can also be used to gain unauthorised access to data.

The packet sniffer will instruct your computer to inspect all data being transmitted over a network, even if it isn't intended for that computer. This might be used to gain passwords or credit cards numbers that have been transmitted over the network.

Spoofing

This is where you get your computer to pretend to be another computer. Every computer connected to the internet is identified by a number and some devices will provide access to services to computers that present a certain number.

By using fake credentials and presenting them to the network they can fool the system into giving access to services meant for another device. This might mean that an attacker will be able to access private and confidential data or even alter or delete that data.

Spoofing can also be used to perform a Denial of Service attack by spoofing IP addresses to make them seem like a legitimate source of data. They can then send masses of data to overload the network making it unusable to the business.

⇨ Bandwidth and latency

Bandwidth and latency

Bandwidth is the rate of data transfer over a network – usually measured in bits per second.

Latency is the time delay for a data packet to transfer to its destination – usually measured in milliseconds.

Bandwidth and latency implications

Browsing the internet doesn't need an instant response so latency isn't a big factor. Bandwidth is an important factor as it affects how long files take to download.

Online gaming needs very low latency as players need a fast response for real-time updates of character movements, etc.

Video calls need low latency and high bandwidth as you need to transfer a lot of data (video and audio), but you also want a fast response to avoid stutter.

⇨ Compression and codecs

Compression

Compression reduces file size so files can be transferred faster. Compression is used for images to be displayed on the Web, video and audio in streaming and VOIP, and documents attached to emails. There are two main types of compression.

- Lossy – data removed during compression is permanently deleted. Commonly used in images, audio and video.
- Lossless – all original data can be recovered when uncompressed. Commonly used for documents.

Codecs

A codec is a program used to compress and decompress video and audio files. This reduces the space they take up on disk and allows fast transfer over a network, such as the internet, for VOIP calls and online streaming.

This leads to a loss of quality in the video or audio – in the resolution, frames per second or both.

Articles for Wider Reading and Flipped Learning

Know it all Ninja

Read through the topics on:

- ⇨ Connectivity
- ⇨ Networks
- ⇨ Issues relating to transmission

Remember to complete the on-line quiz to gain house points and test your knowledge.

https://www.knowitallninja.com/