# Chapter 13

# Networks

# Answering Scheme

## Specimen Paper 3- 2017

1 (a) Award 1 mark for each correct answer up to a maximum of 4.
**Four** from:
The television (TV) programme from the studio is converted to digital data/ modulated onto a carrier wave
The TV signal is sent from the studio to a ground/uplink dish station by high capacity circuit/microwave/fibre optic cable
The signal is uplinked to a geostationary satellite from the ground/uplink dish station
The frequency/channel of the signal is changed ready for downlinking
The viewer's dish is in line of sight of the satellite
The signal is sent from the satellite transponder to viewer's dish
The LNB on the viewer's dish collects signals from the satellite
(A **low-noise block** downconverter (LNB) is the receiving device mounted on satellite dishes used for satellite TV reception, which collects the radio waves from the dish and converts them to a signal which is sent through a cable to the receiver inside the building.)
A cable downlinks the signal to the receiver box
A satellite decoder/set top box processes signals for use by the TV

(b) Award 1 mark for each correct answer up to a maximum of 2.
**Two** from:
Satellite TV can be transmitted with higher data rates so the viewer can watch high-quality audio and video
Satellite TV can be received in most areas so when a terrestrial signal/cable TV is not available TV can still be watched
The viewer has access to hundreds of channels so can view programmes from around the world/many TV stations
The viewer has a greater choice of programmes so can select the ones that are wanted/interesting and discard the channels not wanted

(c) Award 1 mark for each correct answer up to a maximum of 2.
**Two** from:
The initial cost to the viewer is higher because the receiver and satellite dish can be expensive to purchase/install
Viewers will need a separate receiver for each TV set so it can be expensive if more than one TV set is in use
Poor/bad weather can cause the loss of satellite signals/reception so no programmes can be watched in very bad weather
Viewers may have to pay extra/subscriptions to watch some programmes

2 (a) Award 1 mark for each correct answer up to a maximum of 8.
Eight from:
Infrared transmission
Is only effective over short distances so other technologies would be more effective
Can be blocked by walls/obstacles unlike radio waves
... which further limits the range of effectiveness ...
... but does reduce the risk of eavesdroppers outside the network

Can carry a higher bandwidth compared to radio transmission
Relies on line of sight unlike radio transmission

Fibre optic cable
In the long term a one-off installation cost is cheaper than copper cabling Many times more bandwidth per cable than a copper cable
Much larger transmission distance than copper cable which is limited to 100 metres and needs switches to relay signals over this distance
Optical cable transmits data up to 100 km resulting in the need for far fewer network cabinets which means lower cooling costs
Optical cable is immune to external radio frequency or electromagnetic interference, unlike copper which can pick up interference from a number of sources along its run that may degrade the speed considerably
Optical cable does not need lightning protection
In the event of a lightning strike or surge will not damage equipment connected to it
Fibre optic cabling is much lighter than copper, making it easier to transport and install
Initial cost is highly expensive compared to other methods
Optical cable in a LAN requires special expensive network cards
Fitting optical cable requires special training
If an optical cable breaks, local IT technicians may not be able to repair it themselves

Point-to-point laser transmission
Faster data transmission/bit rate
Greater bandwidth
Needs receivers/outlets to relay to stations – cannot transmit directly
Relies on line of sight unlike radio wave transmission
Error rates in data transmission are lower than with radio waves
Can be used for quantum key distribution when using quantum key cryptography unlike radio wave transmission

Radio wave transmission
Can access network resources from any location within the wireless network's coverage area or from any WiFi hotspot
Office-based workers are not limited to working at their desks as with a cabled connection
Wireless networks are more easily expanded with existing equipment, while a cabled network might require additional wiring
Wireless networks eliminate or reduce wiring costs
Radio transmission does not rely on line of sight unlike some other methods

Bluetooth
USB 3.0 interferes with Bluetooth signal
Slowest bit rate of all transmission systems
Obstacles do not affect data transmission/can transmit data through walls unlike infrared transmission
Range is greater than infrared transmission but lower than cabled or laser beam
The required processing power of devices is very low
More limited in the number of devices which can be used

A **mail server** handles and delivers email over a network
A mail server can receive emails from client computers and deliver them to other mail servers
A mail server can also deliver emails to client computers
There are two main types of mail server – outgoing mail servers and incoming mail servers
Outgoing mail servers are known as SMTP (Simple Mail Transfer Protocol) servers
Incoming mail servers are usually either POP3(Post Office Protocol v3) servers or IMAP (Internet Message Access Protocol) servers
A **database server** is a computer in a network used to store databases and retrieve information from them

A database server holds the Database Management System (DBMS) and the databases

It receives requests from the network computers and it searches the database for the selected records ...

... and passes these records back over the network

A database server usually operates in a client-server network where it provides information sought by the client computers

A **proxy server** is a server that acts as a buffer, receiving requests from clients seeking resources from other servers ...

... such as a file, connection, web page, or other resource available from a different server

Usually proxy servers facilitate access to content on the World Wide Web

A proxy server can be used to store/cache frequently visited web sites ...

... when the next user on the network visits the same site the page loads from the proxy server rather than having to search over the internet again ...

... significantly improving access speed for users on the network

A proxy server can be used to control/prevent access to particular websites

A **backup server** enables the backup of data, files, applications and/or databases on a network

A backup server provides backup storage and retrieval services to connected computers, servers or other network devices

A backup server is a server with very large storage capacity

At the scheduled time, the host server connects with the backup server to initiate the data backup process

A **web server** stores, processes and delivers web pages to network users

The communication between client and web server takes place using the Hypertext Transfer Protocol (HTTP)

Web servers most frequently deliver HTML documents which may include images, style sheets and scripts in addition to text content

A web browser makes a request for a specific resource using HTTP and the web server responds with the content of that resource or an error message if unable to do so

(c) Award 1 mark for each correct answer up to a maximum of 6.

**Six** from:

Use of encryption key to scramble/make unreadable the data/files/folders

Only users with encryption key can decrypt the data

Encrypting folders/files containing the data to prevent unauthorised access

Use of encrypted connections via network, e.g. SSL, VPNs

Encryption occurs at the network transfer level (layers 3 and 4) of the OSI model

... using IPsec to create encrypted packets for transmission

Data only encrypted during transmission on network

3 Award 1 mark for each correct answer up to a maximum of 2.

**Two** from:

A padlock is shown by the browser indicating that the data is encrypted during transmission

The URL will show https indicating that a secure connection is being made Browser will display a warning if an invalid digital certificate is received from a website

Browser will display a warning if a mixture of encrypted and unencrypted data is received from a website

Browser address bar changes colour (to green) when using secure connections/extended digital certificates

(b) Award 1 mark for each correct answer up to a maximum of 4.

**Four** from:

Browser initiates a connection to the secure website using https

... using the SSL protocol

Browser uses https to authenticate the website

... by examining the server’s digital certificate and comparing it with that held by certificating authorities

| | |
|---|---|
| | Browser and web server establish a secure connection using public and private keys to generate a session key<br>Transmitted/received data is encrypted using the session key<br>Browser requests user ID and password from Shafiq<br>Browser transmits user ID/password in encrypted form to website |
| 4 | a) Award 1 mark for each correct answer up to a maximum of 2.<br>**Two** from:<br>Biometrics include data about facial recognition/iris recognition/retinal patterns/fingerprints/palm prints stored in computer chips<br>Biometric data are read at point of access and compared to the stored data<br>If the data match then access is allowed/if the data do not match access is not allowed<br>**2**<br>9(b) Award 1 mark for each correct answer up to a maximum of 8. Award a maximum of 6 marks if all points are in favour or all against. 1 mark can be awarded for a reasoned conclusion.<br>*Points in favour of the use of biometrics, e.g.:*<br>Biometric identifiers are unique to individuals<br>... so are more reliable in verifying the identity of an individual<br>Use of biometrics must be difficult to circumvent/traits must be difficult to imitate or substitute<br>... to ensure an appropriate level of security<br>Using biometrics removes the need for user IDs and passwords<br>... eliminating problems with forgotten or lost passwords<br>... eliminating the risk of fraudulent use of another's login details<br>Biometric systems have fast matching speeds to deliver accurate results<br>... so delays in allowing access are minimised<br><br>*Points against the use of biometrics, e.g.:*<br>All people/everyone must have the trait being used for biometrics so the biometric data can be compared/measured on everyone<br>Biometric data must be permanent/does not significantly change over time so algorithm will work over time<br>Biometric data must be measurable/must be easy/quick to acquire the data from an individual so the individual is not inconvenienced/device is accessed quickly<br>Biometric data must be in a form that allows processing/extraction of features for comparison<br>Biometric data may be passed on to third parties/used for other purposes/ raises concerns regarding privacy and the inappropriate use of the data<br>... so individuals may not allow use of their data for this purpose/use of biometrics must be acceptable to participants<br>There is a limit on the number of stored sets of data/maximum number of sets of data and this limits the usefulness of biometrics in large populations/with a large number of users<br>Biometrics rely on the probability of inputs being valid so if the false acceptance rate is set incorrectly imposters can be shown as genuine<br>Failure to detect a match between the input and the (matching) data stored can result in valid inputs being incorrectly rejected and access being improperly denied<br>Failure to capture the biometric data when presented/failing to detect data when correctly presented results in the rejection of genuine readings and access is improperly denied |
| 5 | (a)(i) ***Two*** *from:*<br>*(HDLC is):*<br>High-Level Data Link Control<br>Layer 2 (data link) protocol<br>Connects point-to-point serial devices/leased lines<br>Uses error correction<br>Routers encapsulate HDLC before putting on LAN.<br><br>(a)(ii) ***Two*** *from:*<br>*(Frame relay is):* |

Layer 2 and 3/data link/network layer protocol
Puts data into variable-sized packets/frames
Does not include error-correction/error corrections is done by devices
...can be unreliable
Specifies physical and logical link layers
Used in packet switching
Used on integrated services digital network (ISDN)
Used in permanent virtual circuits (PVC)
Can provide QoS
...worth constant bitrate/emulation of circuit switching.

(b) ***Four*** *from:*
If many people want the OS at once bit torrent is resistant to flash-dot/crowds/website overload/dos/FTP is not resistant to flash-dot/crowds/website overload/dos
Bit torrents can be paused/stopped and restarted/FTP cannot restart if paused, so if interrupted the download has to be done again
Bit torrent makes many small data requests from different IP connections/addresses/FTP is from one IP connection/address so is quicker to download the large OS file
Bit torrent downloads file sections randomly/rarest first/ FTP is sequential download of file sections
Bit torrent can be slow to get up to full speed/FTP achieves full speed as soon as it starts download and can achieve very high download speeds.

6 a) ***Eight*** *from:*
*Advantages:*
A firewall can provide protection to multiple networked computers simultaneously
Firewalls can monitor traffic coming in and going out of a network□
□and produce log files for subsequent analysis
Firewalls can enforce password controls to enter/use the network to try to prevent unauthorised users from gaining access
Firewalls can enforce access policies so that only authorised users can access the network/parts of the network
Firewalls reduce the risk of key logging software sending details to third parties by blocking the access out of the network
*Disadvantages:*
Firewalls are the central point of attack by hackers/potential intruders and once breached there are no further defences
Firewalls can block legitimate process/applications so manual adjustment of settings may be required
□can lead to allowing unwanted access by other processes if not configured by experts
Firewalls are usually incapable of protecting against backdoor Trojans that open ports to send data to third parties who can then access the system
Firewalls do not usually contain malware removal tools.
*Max 6 for all advantages or all disadvantages.*
*1 mark is available for a reasoned conclusion/opinion.*

**8**

2(b) ***Four*** *from:*
Acts as intermediary for client requests for services such as a web page/a file
Provide content filtering to control the content that is accessed/enforce acceptable use policies
Provide user authentication to control web access
Provide detailed logs of user web activity/flag up unacceptable use by employees
Provide links to anti-malware applications to check incoming/outgoing data
Filtering based on URL lists
□DNS blacklists
□based on lists maintained by third party companies
Can provide NAT/anonymity of IP address.

7 **This question to be marked as Level of Response.**

*Evaluation requires that advantages and disadvantages be discussed and weighed up in importance.*

**Level 3 (7–8 marks)**

Candidates will evaluate, in detail, by discussing the advantages and disadvantages of the use of satellites for data communications.
The information will be relevant, clear, organised and presented in a structured and coherent format.
There may be reasoned conclusions/opinions.
Subject specific terminology will be used accurately and appropriately.

**Level 2 (4–6 marks)**

Candidates will evaluate by discussing the advantages and disadvantages of the use of satellites for data communications.
For the most part, the information will be relevant and presented in a structured and coherent format.
There may be reasoned conclusions/opinions.
Subject specific terminology will be used appropriately and for the most part correctly.

**Level 1 (1–3 marks)**

Candidates will describe by giving the advantage(s) and/or disadvantage(s) the use of satellites for data communications.
Answers may be in the form of a list.
There will be little or no use of specialist terms.

**Zero marks:** Response with no valid content.

Answers may make reference to e.g.:

*Advantages:*

satellite communications:

□ easier to setup of mobile communications
□ are more economical than terrestrial communication over long distances
□ is most economical especially for low network traffic demands in remote areas
□ quality of transmitted signal is independent of distance
□ quality of transmitted signal does not depend on location of sending and receiving stations
□ country/owner has control over their own network

*Disadvantages:*

□ huge initial cost of manufacture/launch
□ repair of satellite is almost impossible once it has been launched
□ can be affected by severe weather conditions/very dark clouds
□ can be affected by electromagnetic disturbances/events in space/sun activity
□ annoying time gap/delay between exchange of data reducing the efficiency of satellite communications for data transmission.

8 (a) ***Eight*** *from:*

(Civilian) signals from satellite travel by line of sight to navigation device/ receiver
Use L1/1575.42 MHz in UHF band
Satellites are Low Earth Orbit/LEO
Signal contains ID code of the satellite
...and status/health information
...and current date and time from atomic clock in the satellite
...and almanac data (data that describes the orbital courses of the satellite) about where each GPS satellite is at any point in time
Navigation device/ receiver must lock to (at least) 2 satellites to calculate 2D position (i.e. latitude and longitude)
To 4 or more (usually 4 to 7) satellites to calculate 3D position (i.e. latitude, longitude and altitude/elevation)
Using trilateration techniques
Calculation by finding intersect point by timing the signals from the satellites

**8**

(b) ***Five*** *from:*

| | |
|---|---|
| | Atmospheric/ionosphere/ troposphere delays slowing the satellite signal slows as it passes through the atmosphere<br>Signal multipath errors as the GPS signal is reflected off objects before it reaches the receiver<br>...increases the travel time of the signal<br>Clock errors in the receiver because the built-in clock is not as accurate as the atomic clocks on board the GPS satellites<br>Orbital errors (ephemeris errors) of the satellite's reported location<br>The number of satellites visible may be too few because buildings/terrain/dense foliage may block the signal reception<br>electronic interference can block the signals<br>...causing position errors /no position reading<br>...GPS units usually will not work indoors, underwater or underground<br>Satellite geometry/shading because the relative position of the satellites at any given time is not ideal for signal reception by the receiver<br>...the satellites should be located at wide angles relative to each other<br>...poor geometry occurs when the satellites are located in a line/tight grouping<br>Intentional degradation of the satellite signal by the operator/owner of the satellites<br>...to prevent military adversaries from using the highly accurate GPS signals |
| 9 | ***Eight** from e.g.:*<br>*Benefits of Packet Switching include e.g.:*<br>Makes very efficient use of the network as communication lines are shared<br>Data packets can be routed around unusable nodes/parts of the network so if part of network/node is faulty/not working packets can still reach destination<br>The network only has to expand slowly with increase in users compared to circuit switching<br><br>*Drawbacks of Packet Switching:*<br>The packaging of the data changes each time a packet is switched so there is a time overhead/latency<br>Can cause a problem for time-critical information such as an emergency signal/video streaming<br>Small data packages are inefficiently packaged (e.g. a data package of 600 bytes uses two packets of 512 bytes plus the address information)<br>*Max 6 for all benefits and drawbacks*<br>*1 mark available for a reasoned conclusion/opinion* |

10

| | |
|---|---|
| **Answers/Indicative content Level of Response This question to be marked as a Level of Response.**<br>*Evaluation requires that advantages and disadvantages be discussed and weighed up in importance.*<br>Answers may make reference to e.g.:<br>*Tape-based:*<br>established technology<br>□ huge storage capacity<br>□ serial access<br>□ cheap per GByte<br>□ can be slow to create backup<br>□ can be slow to recover files<br>□ tapes can be fragile<br>□ tapes may not work in different tape drives.<br><br>*Hard disk-based:*<br>□ quick to produce backup<br>□ quick to recover files<br>□ direct access<br>□ cost per GByte varies/can be expensive<br>□ large capacities<br>□ hard disk can fail losing large amounts of data.<br>*'Cloud'-based:*<br>□ off-site technology used so not so vulnerable to on-site disasters<br>□ hardware/maintenance/service costs borne by supplier<br>□ security arranged by supplier<br>□ security of data issues<br>□ unlimited capacity available<br>□ reliable internet connection required<br>□ high bandwidth connection preferred. | **Level 3 (7–8 marks)**<br>Candidates will evaluate in detail the options for creating backups.<br>The information will be relevant, clear, organised and presented in a structured and coherent format<br>There will be a reasoned conclusion/opinion.<br>Subject specific terminology will be used accurately and appropriately.<br><br>**Level 2 (4–6 marks)**<br>Candidates will evaluate the options for creating backups.<br>For the most part, the information will be relevant and presented in a structured and coherent format<br>There may be a reasoned conclusion/opinion.<br>Subject specific terminology will be used appropriately and for the most part correctly.<br><br>**Level 1 (1–3 marks)**<br>Candidates will describe the options for creating backups.<br>Answers may be in the form of a list.<br>There will be little or no use of specialist terms.<br><br>**Level 0 (0 marks)**<br>Response with no valid content. |

11 ***Six** from:*

Audio quality improves with increasing bit rate
...two examples from:
...800 bit/s is minimum for speech to be recognised
32 kbit/s – generally acceptable only for speech
96 kbit/s – generally used for speech/low-quality streaming
128 or 160 kbit/s – mid-range bit rate quality
192 kbit/s – a commonly used high-quality bit rate
320 kbit/s – highest bit rate level supported by the MP3 standard
...lossy compression to reduce bit rate can introduce artefacts
...caused by data/quantisation errors
...distortion of sound
...perceived/heard as 'bubbling/burbling'
...stuttering/jerky/blanks/silences in sound.

12 8(a) ***Four*** *from:*

*(Derived from section 7, sixth principle of Act:*

*‘personal data shall be processed in accordance with the rights of data subjects under this Act’:)*

A right of access to a copy of the information held in their personal data

...told whether personal data is being processed

...given a description of personal data

...given reason(s) for processing

...given details of source of data

A right to object to processing that is likely to cause/is causing damage/distress

A right to prevent processing for direct marketing

A right to object to decisions being taken by automated means

A right (in certain circumstances) to have inaccurate personal data rectified, blocked, erased or destroyed

A right to claim compensation for damages caused by a breach of the Act.

(b) ***Two*** *from:*

Failure to register when required

...and to keep personal data if not registered

...failure to provide accurate information/providing false information when registering

Failure to comply with provisions/stick to reasons for storing data supplied when registering

Processing data if not registered

To fail to provide Data Commissioner with updated address failure to comply with enforcement order

...prohibition notice e.g. not to send data overseas/supply data to third party

...information notice e.g. supplying false information/not all of information

when ordered to do so.

13 ***Eight*** *from:*

Other devices can cause interference

...remove other devices e.g. microwave ovens/cordless telephones on same frequency which can interfere with signal

...WiFi uses 2.4Ghz and/or 5GHz frequency

Ensure that access points do not use same frequencies/channels...

...other access points may use same WiFi channel and interfere with user’s channel

Restrict use of e.g. Bluetooth®

...Bluetooth® signals can cause interference

Restrict use of mobile phones...

...mobile telephone systems can cause interference

Adjust wireless access point settings...

...wireless access point rate control set too high

...results in many retries

Wireless devices can only send or receive but not both at the same time

...effectively cuts the bandwidth in half

give devices with already established connections higher priority

...e.g. video streaming

...other devices appear to have slower access times/data transfer rates

Radio waves are slowed/blocked/’bent’ by objects

...walls/insulation/metal objects may degrade/block WiFi signals so use materials that are transparent to wireless signals

Restrict choice of channels...

...automated channel choice can cause ‘channel hopping’

...too many changes slows access times

Restrict use of ‘legacy’ bands for WiFi

...routers are slower if they have to broadcast on several bands simultaneously

Set access point antennas to optimum position/orientation

...may be set too low/wrong angle/hidden.

14 (a) ***Two*** *from e.g.:*

Default means that this gateway/address is used unless another address is specified
Router/computer node that has details of where to forward data packets
.... if no route known already
Device that passes traffic from local subnet to devices on another subnet

(b) ***Eight*** *from e.g.:*

*Benefits:*
Devices are easier to move around as no wires needed...
...no need to physically connect
...no trailing wires to trip over
Greater productivity by home-workers as they can carry laptop/device with them while doing other tasks
Ease of expansion with new devices as single access point required
...devices can be added without need to add cables/space for connection/additional hubs/switches
...no need to drill holes/damage house fittings/walls for cables
Less expensive than wired connections so no cost of new hubs/switches/sockets/wires
*Drawbacks:*
Security issues so encryption required which may be difficult to set up
Range issues as it is restricted to only 10s of metres from access point
.... physical objects may interfere with signal
.... reduced signal strength as distances from access point increases
Reliability issues
...subject to interference from other wireless devices/electrical items
Speed issues as rate of data transfer is lower than for cabled connections
...may vary during a session leading to poor user experience.
*Max 6 for all benefits or all drawbacks.*
*1 mark is available for a reasoned conclusion.*

15 This question to be marked as a Level of Response.

**Level 3 (7–8 marks)**
Candidates will discuss in detail, giving both benefits and drawbacks, of the use of the use of satellite technology in global positioning systems (GPS).
The information will be relevant, clear, organised and presented in a structured and coherent format.
There will be a reasoned conclusion/opinion.
Subject specific terminology will be used accurately and appropriately.

**Level 2 (4–6 marks)**
Candidates will explain the use, giving a benefit and drawback, of the use of satellite technology in global positioning systems (GPS).
For the most part, the information will be relevant and presented in a structured and coherent format.
There may be a reasoned conclusion/opinion.
Subject specific terminology will be used appropriately and for the most part correctly.

**Level 1 (1–3 marks)**
Candidates will describe, with a least one benefit/ drawback, of the use of the use of satellite technology in global positioning systems (GPS).
Answers may be in the form of a list.
There will be little or no use of specialist terms.

**Level 0 (0 marks):** Response with no valid content.

*Answers may make reference to e.g.:*
*Benefits include:*

Access to satellite signals is available over most of surface of earth unlike signals from terrestrial transmitters

Transmission of GPS signals is not dependent on political boundaries

Satellite signals are accessible over oceans where terrestrial transmissions are difficult to receive due to the long distances from land

Signals are available to anyone who wishes to use them (unless switched off by operator of satellite)

Satellites are vandal-proof/ inaccessible to those who would physically attempt to disrupt their function

*Drawbacks include:*

Requires a large number (c.25 to 35) of satellites to be in orbit to provide adequate coverage of terrain

Cannot easily be repaired if malfunctioning

Requires at least 3, preferably 4, satellites to be visible to / received by GPS receiver to achieve reliable/accurate positioning

Satellite signals are blocked by solid objects/buildings/in tunnels/trees/dense clouds/ snow storms so, in these circumstances, GPS receivers may□

□fail to provide locations

□may provide erroneous locations.

---

16 **(a) Five** *from:*

*Max* ***three*** *(definition) from:*

DNS spoofing is Domain Name System spoofing/Domain Name System cache poisoning

Type of computer hacking

Corrupt data is placed into cache of resolver of DNS/ISP DNS cache so that an incorrect IP address is returned

Network traffic is diverted/redirected to a different computer to that which was requested/to hacker's computer

*Max* ***three*** *(prevention) from:*

DNS server configured to ignore request from other DNS servers that are not directly relevant to the query

Use of secure DNS/public key encrypted/digitally signed data to ensure authenticity of DNS requests

Performing end-to-end validation of DNS requests with HTTPS Defence is at transport layer.

**(b) Five** *from:*

*Max* ***three*** *(definition) from:*

DoS is a Denial of Service attack

Where a computer/system is made unavailable by overwhelming the target system with requests for service

Requests for service are superfluous/have no purpose other than to disrupt/overload the system

Can use many IP addresses/multiple computers/devices to carry out a DoS

*Max* ***three*** *(prevention) from:*

Use of firewall configured to deny incoming packets with IP addresses/ports from identified attackers

Use of tools to analyse incoming data to identify 'spoof'/ unwanted/illegitimate requests

Use of DNS blackhole/routing to re-route IP addresses intended for attacker to non-existent IP address/server

Use of DNS sinkhole to direct traffic to valid IP address for analysis to reject unwanted packets

Use of a specialised/commercial 'cleaning/scrubbing' servers/centre to separate out unwanted traffic from legitimate traffic

Defence is at application layer.

(c) **Four** *from:*

*Max* ***three*** *(definition) from:*

ARP spoofing is Address Resolution Protocol spoofing

To associate/link MAC address of attacker's device to IP address of e.g. default gateway/another network host

Occurs when IP address is resolved to a MAC address
So that traffic is directed to attacker instead of intended host/device
Data frames may be intercepted and modified/prevent traffic movement
*Max* ***three*** *(prevention) from:*
Use of DHCP server configurations to certify that IP addresses are correctly assigned
Use of tools to cross-check ARP resolutions to block incorrect ones
Built into switches/network devices
Configuring the ARP cache in the OS to ignore requests for updates/hard coding the ARP cache in OS to prevent updates.

17 **Eight** *from:*
Locking the room when not in use
□prevents unauthorised access to devices/computers
□requires meticulous logging of who has key to room
□requires strict adherence by users to rules e.g. no unlocking of doors for others to go in
Using swipe cards/ keypads to activate locks
□requires extra items e.g. cards/knowledge of codes
□cards can be stolen/lost and used by others
□codes can be forgotten/told to others
Biometric tests to unlock doors
□via keypads/Voice recognition
□can be time-consuming to collect user data
□needs to be updated regularly as biometric data can change
□can be fooled in various ways e.g. recordings of voice
Bolting computers to the desk
□very secure
□computers not easily moved to other locations
□computers in fixed positions may be difficult to use
Using special pens to mark their postcode/owner details onto the computer/device case
□can allow retrieval of stolen items
□can be a deterrent to thieves
□can deface items preventing resale/reducing asset value
Keeping windows shut/locked/barred - especially if on the ground floor
□prevents thieves from entering
□reduces access to fresh air
Using CCTV video cameras to monitor computer rooms/corridors
□allows surveillance of large areas
□needs constant attendance
Employing security guards to check passes
□effective at preventing unknown people from accessing area
□requires more employees so increases costs
□relies on integrity/honesty of security guard
Positioning screens so passers-by cannot see what is on the screen
□prevents others knowing/discovering the password
□position may be unsuitable for long term use
Type in passwords out of sight of others
□prevents others knowing/discovering the password
□may not be easy to achieve in crowded office/position of keyboard.

18 **Eight** *from:*
Can provide greater bandwidth to provide faster rate of data transfer
Can carry thousands more connections c.f. electrical cable so not so many cables required
Lower signal losses over distance so less need for amplifiers/repeaters so less maintenance
Can span longer distances so is used to cross difficult areas/gaps/seas/oceans
No interaction with other cables as resistant to electrical interference/ground currents
...can be used in areas of high electromagnetic activity
No crosstalk with adjacent cables so no distortion of signals

Lighter in weight so can be more suitable for use in aircraft

No sparks produced if faulty/cut so safer in high risk areas

Resistant to corrosion so less maintenance required

Smaller cable size so can be used in confined spaces

Difficult to ‘hack’/listen/tap into so more secure

Can go around corners/bends unlike laser beams

Can be more expensive to install than copper cables

Specialist test equipment is needed

Specialist tools are required for joining optical fibres

Physical damage is more likely to interfere with signal transmission compared to similar with copper cables

Wildlife prefer the covering of optic fibres for nesting materials compared to those around copper cables

Underwater fibre optic cables are more susceptible to chemical damage than copper ones e.g. hydrogen will degrade them

Cannot have $90_0$ corners unlike copper cables.

*Max six for all positives or all negatives.*

*1 mark available for a reasoned conclusion/opinion.*

19 The more available bandwidth on the connection the higher quality of video that can be streamed

Use of a 3G connection to the internet limits video/streaming to low bit rate of 400 Kb/s

Buffers not filled completely so video pauses/stops/jerky if frames not received fast enough

Provides video of 320 · 240 pixels without apparent stuttering/buffering/ stop-start issues

This will be a poor video/low definition video as seen on the 1024 · 576 screen

Use of a 4G connection with higher bandwidth of c. 15Mbit/s allows video with higher bitrates to be viewed properly

This is 1024 · 576 is possible and this is HD quality

Highest bit rates of 19 / 30 Mbit/s allowing resolutions of up to 1920 · 1080 pixels

Available/can be streamed over Wi-Fi (IEEE 802.1 g) wireless connections....

Which have a maximum of 54 Mbit/s

1920 · 1080 pixels will have to be downscaled for viewing on the smartphone screen

Which may lead to artefacts and loss of quality.

20 **Eight** *from:*

S1 to S6 have their own storage devices for storing whole messages

Message sent in its entirety from source to switch S1

...S1 stores whole message on its storage device

S1 connects to S3 and forwards whole message to S3

...S3 stores whole message on its storage device

...message is deleted from S1

S3 connects to S5 and forwards whole message to S5

...S1 stores whole message on its storage device

...message is deleted from S3

Process repeated between S5 and S6 where message is stored before forwarding to destination

The source and destination of the message are not directly connected

Message can be multiplexed with other messages on network Switches

Method is called ‘message switching’.

(b) **Two** *from:*

Improves/makes more efficient use of bandwidth because the data channels are shared among communication devices

Network congestion can be reduced as messages can be stored temporarily at message switches

Priorities may be used to manage network traffic

Use of broadcast messaging/messages are delivered to multiple destinations makes more efficient use of network bandwidth

Message can be stored until recipient decides to pick it up

| | |
|---|---|
| | Process is transparent to applications the use it. |
| 21 | **Eight** *from:*<br>Geographical area that can be covered is much greater than other broadcasting methods<br>Costs are less over greater distances/areas...<br>No need for terrestrial transmitters to homes<br>Can cover difficult terrain more cheaply<br>Allows greater bandwidth for data transmission...<br>Higher definition for TV/bit rate for radio for higher quality broadcasts<br>More TV/radio channels are possible due to greater capacity<br>Requires users/viewers/listeners to have (suitable) receiving equipment<br>...broadcasters may have a limited audience if few people have satellite receivers<br>...need line of sight view to satellite to be able to receive<br>...need to be professionally installed which takes time and can be costly<br>Satellite technology has a huge setup cost<br>Satellites do not have an unlimited lifespan<br>...may become space junk when lifespan is over<br>Repair of orbiting satellites is almost impossible<br>Signals to ground can be subject to interference/blockage due to weather/other signals<br>Significant delays in signal propagation/travel time of signals/distance from uplink to receiver can cause anomalies e.g. time differences of several seconds in transmissions.<br>*Max six for all positives or all negatives.*<br>*1 mark available for a reasoned conclusion/opinion.* |
| 22 | ***Eight*** *from:*<br>Bandwidth requirements are higher to allow more detail in video images<br>Video-conferencing requires higher resolution video because there are often several people on screen at once<br>Need to see facial features/body expressions of participants clearly<br>One person to another (when video-conferencing) does not require high resolutions<br>High bandwidth (of 2–4 Mbps) would deliver an (H720p) high definition image for multiple participants<br>Low bandwidth (of 512 kbps) would be sufficient for one-to-one videoconferencing<br>Low bandwidth does not allow high definition images so would not be able to properly see the faces of multiple participants<br>High bandwidth would allow higher frame rates/30fps for smooth motion<br>Limited/low bandwidth requires trade-off between resolution and frame rate<br>Resolution priority for displaying slideshows/documents in detail<br>Motion priority for displaying video presentations.<br>*Max 6 for all positives or all negatives.*<br>*1 mark available for a reasoned conclusion/opinion.* |
| 23 | ***Two*** *from:*<br>Each packet takes a different route through the network<br>Each router 'decides' which router to send it onto depending on other network traffic e.g. router A will send some packets to router C and some to D<br>If next router is busy/unavailable<br>If a packet is mis-sent/corrupt en route then re-transmission is requested from originating router<br>Time taken along different routes is not the same<br>Arriving at different times at network H.<br>***(b) Five*** *from:*<br>Each router has a stored lookup table of IP addresses/routes to the next router/network<br>Routing table is stored at control plane of router<br>Routing table used to choose next router/router to which to send packet<br>Static routes B to C to E to G are pre-programmed to show route to destination<br>Dynamic routing protocols build up a table of preferred routes between connected routers/networks<br>B to C to F to G if router E is inefficient/out of action/in heavy demand<br>If destination is unknown router B will send packet to next known router/C or D |

If C/D router does not know destination to H then packet is sent onto next router/E or F.

24 (a) ***Two*** *from:*
*(PPP is)* Point to Point Protocol
Used in (most) dial-up connections
Has link monitoring capability/can log how many errors occur
Can maintain multiple links and enable them to function as single link
Provides authentication via password authentication protocol
(PAP)/challenge-handshake protocol (CHAP)
Requires a username/password to allow dial in to network
(b) ***Eight*** *from:*
Can use multiple email clients simultaneously
Allows use of same email system on mobile devices and PCs at same time
Changes on one device are reflected on other devices connected at same time
Provides multiple mail boxes
Can create/use folders/mailboxes on server
Can copy messages
Email clients stay connected to server
Email messages downloaded as and when they arrive at server
Provides faster response time to emails to recipient compared to POP3
Allows access to sections of message/partial messages/partial fetch
Messages with attachments can be retrieved without downloading the attachment
Can stream content as it is being retrieved
Message state information available
Uses flags stored on server to check whether message has been read/replied to/deleted
Can be seen across connected devices
Server-side searches can be carried out
Email client can search server for email messages using user-defined criteria.

25 **Six** *from:*
Each packet sent by network A takes a different route through the network
Each packet has source/destination address stored in header
Each router has a stored lookup table of IP addresses/routes to the destination (if known)
Routing table is stored at control plane of router
Used to choose next router/router to send packet to
Static routes are pre-programmed to show route to destination B to C to E to G
Dynamic routing protocols build up table of preferred routes between connected networks B to C to F to G if router E is inefficient/out of action/in heavy demand
If destination is unknown router B will send packet to next known router, C or D
If C/D router does not know destination to H then packet is sent onto next router, E or F.
**(b) Six** *from:*
Router D may be not responding
Router D may be in heavy demand
Router D may have failed/be offline
There may a policy set up in router C to over-ride the routing tables so that the packets are not sent to router D
To enforce a QoS for specific services that take precedence over other packets.

> Quality of service (**QoS**) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network. **QoS** controls and manages network resources by setting priorities for specific types of data on the network.

Router C may have more than one set of routing protocols because it is connecting to several different networks at once
Alternative routers may respond quicker/before router D/alternative routes are available sooner than via router D.

26 **Eight** *from:*
Suitable for use in ‘free-space’ i.e. no physical connection medium such as cable or fibre
Infra-red LEDs allow point-to-point optical commnciations
Infra-red LEDs allow high data rates using laser technology
Infra-red LEDs allow relatively inexpensive compared to other radio technologies
Uses pulsing modulation/on-off signals which can restrict rates to low data rates in free space
Suitable for short distance communication between devices (usually only maximum of a few metres)
May not work relaibly when too close together
Line of sight required so objects block the signals
Not subject to interference as much as other radio technologies
Has low power requirements so suitable for use in small/mobile devices/remote controls
Can be more secure than other radio technologies as range is low/easily blocked by objects.
*Max six for all positives or all negatives.*
*1 mark available for a resoned conclusion/opinion.*

27 **This question to be marked as a Level of Response.**

**Level 3 (7–8 marks)**
Candidates will evaluate, giving advantages and disadvantages of, a range of devices, in detail the use of Bluetooth® wireless technology for communication between devices.
The information will be relevant, clear, organised and presented in a structured and coherent format.
There will be a reasoned conclusion/opinion.
Subject specific terminology will be used accurately and appropriately.

**Level 2 (4–6 marks)**
Candidates will explain, with advantages and disadvantages, the use of Bluetooth ® wireless technology for communication between devices.
For the most part, the information will be relevant and presented in a structured and coherent format.
There may be a reasoned conclusion/opinion.
Subject specific terminology will be used appropriately and for the most part correctly.

**Level 1 (1–3 marks)**
Candidates will describe the use of Bluetooth® wireless technology for communication between devices.
Answers may be in the form of a list.
There will be little or no use of specialist terms.

**Level 0 (0 marks)**
Response with no valid content.

*Answers may make reference to e.g.*
Bluetooth® has...
..a range of applications/uses for wireless communications between devices like phones/ headsets/speakers/
..a range of applications/uses for control of communications between devices

*Advantages:*
Bluetooth® requires minimal setup e.g. just a few button presses and (possibly) a 4 digit code so is easy to use/setup or pair/bond devices c.f. other network types
Bluetooth® is low energy technology so suitable for mobile devices
Bluetooth® is standardised so easy to implement/most devices will connect readily
Bluetooth® is standard in a range of devices e.g. smartphones, speakers, headsets
Bluetooth® is not easy to intercept nor will it easily interfere with other device connections

| | |
|---|---|
| | *Disadvantages:*<br>Bluetooth® is short-range<br>Is affected by obstacles/walls that attenuate signals<br>Drains battery power if range is at maximum<br>Bluetooth® – enabled technology can be more expensive than non-enabled devices<br>Bluetooth® has limited bandwidth. |
| 28 | *Command word: Evaluate: discuss the importance of, weigh up, the advantages and disadvantages, judge the overall effectiveness, weigh up your opinions.*<br>This question to be marked as a Level of Response.<br>**Level 3 (7–8 marks)**<br>Candidates will evaluate/explain in detail the benefits and drawbacks of the use of quantum cryptography when transmitting confidential data over public networks.<br>The information will be relevant, clear, organised and presented in a structured and coherent format.<br>There will be a reasoned conclusion/opinion.<br>Subject specific terminology will be used accurately and appropriately.<br>**Level 2 (4–6 marks)**<br>Candidates will explain the benefits and drawbacks of the use of quantum cryptography when transmitting confidential data over public networks.<br>For the most part, the information will be relevant and presented in a structured and coherent format.<br>There may be a reasoned conclusion/opinion.<br>Subject specific terminology will be used appropriately and for the most part correctly.<br>**Level 1 (1–3 marks)**<br>Candidates will describe a benefit and/or drawback of the use of quantum cryptography when transmitting confidential data over public networks.<br>Answers may be in the form of a list.<br>There will be little or no use of specialist terms.<br>**Level 0 (0 marks):** Response with no valid content.<br>*Answers may make reference to e.g.:*<br>Allows use of cryptographic tasks that would be deemed impossible without the use of quantum cryptography, e.g. the guarantee that any interception/viewing/eavesdropping on/disturbance of the data is detected<br>Calculations can be carried out extremely rapidly so much higher bi-length for keys can be used so increasing security of data when encrypted<br>Does not do away with conventional cryptographic keys i.e. a mathematical algorithm is still needed for the actual encryption of the data<br>Uses photons to carry data in terms of their 'spin' which is difficult to control/generate consistently/precise filters to determine the spin are difficult to manufacture/deploy<br>Requires extremely pure fibres to transmit photons intact/undisturbed over anything but short distances – maximum so far is about 60 km/far shorter distance than conventional fibre use can reach<br>Requires a new type/generation of computers to become a viable reality In theory, quantum techniques can break any encryption in a usefully short time. |
| 29 | *Command word: Evaluate: discuss the importance of, weigh up, the advantages and disadvantages, judge the overall effectiveness, weigh up your opinions.*<br>**Eight** *from:*<br>Use of anti-spyware software will prevent spyware being installed<br>May not detect spyware already installed<br>May not detect spyware disguised as legitimate feature of another program/application<br>Use of antivirus software – will detect and remove some spyware but not all, so has limited effectiveness when used on its own<br>Real time scanning of incoming programs/applications/data can provide protection by blocking spyware from entering the system provided the spyware is recognised/in its database/can be analysed to be spyware |

Dedicated anti-spyware can detect and remove spyware provided all areas of system are regularly scanned
Lists of spyware must be up to date
Options may include option to manually delete files if anti-spyware is ‘uncertain’ of status of detected file/data
Spyware may resist attempts to be deleted/uninstalled□
May recreate another running process to reinstall itself once deleted by antispyware software
Using alternative web browsers may prevent spyware being installed as some are more vulnerable than others□
Web browsers are not designed to detect spyware
Using reputable sources for download of software may help prevent spyware being installed
Reputable sources can be ‘infected’
Use of combination of methods is most successful but takes awareness and time to implement
Using a firewall to prevent spyware from returning data to the spyware source
*One mark is available for a valid reasoned opinion/conclusion.*

30 **Eight** *from:*
Packet switching breaks the message into discrete data packets whereas message and circuit may not do so
Packet switching can introduce delays as packets may travel via different routes whereas message and circuit switching do not
Packet and message switching make more efficient use of the capacity of the transmission medium than does circuit switching
Circuit switching keeps the circuit connected for the whole of the duration of the transmission whereas message and switching do not
Circuit switching uses the full bandwidth of the transmission medium whereas message and packet switching do not
Circuit switching can guarantee a higher quality of service compared to the other methods
Message switching can be less secure because messages are stored (temporarily) at nodes
Circuit switching can guarantee a higher level of security of data compared to the other methods
Others can use the same communication channel when packet switching is used whereas this is not possible when message and circuit switching is used.

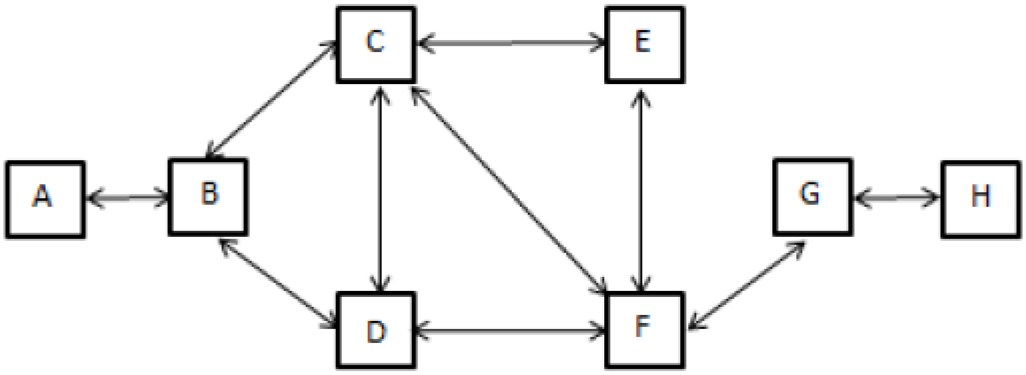
31 **Command word: Evaluate: discuss the importance of, weigh up, the advantages and disadvantages, judge the overall effectiveness, weigh up your opinions.**
*This question to be marked as a Level of Response.*
**Level 3 (7–8 marks)**
Candidates will evaluate, giving advantages and disadvantages, of at least three ways in which physical security can be used in combatting IT crime.
The information will be relevant, clear, organised and presented in a structured and coherent format.
There will be a reasoned conclusion / opinion.
Subject specific terminology will be used accurately and appropriately.
**Level 2 (4–6 marks)**
Candidates will explain giving advantages and disadvantages of at least two ways in which physical security can be used in combatting IT crime.
For the most part, the information will be relevant and presented in a structured and coherent format.
There may be a reasoned conclusion / opinion.
Subject specific terminology will be used appropriately and for the most part correctly.
**Level 1 (1–3 marks)**
Candidates will give advantages / disadvantages of using physical security in combatting IT crime.
Answers may be in the form of a list.
There will be little or no use of specialist terms.

**Level 0 (0 marks):**
Response with no valid content.

*Answers may make reference to e.g.:*
Physical barriers such as wall / doors / bars / use of floors other than ground floor which are cheap and easy to make use of / make use of existing resources which lowers costs
Use of CCTV which can be placed overtly to deter unauthorised persons just by their presence or by a warning / notice that watching is occurring / can be cost effective as a deterrent
Video surveillance can be used to watch large areas with few staff
Physical presence of guards / security staff shows persons that a security system is in operation
... can deal with issues quickly / immediately
Security lighting / automatic lights / sensor-controlled lights can illuminate when persons present to act as deterrent / highlight intruders / warn intruders that they have been seen and these have low cost if e.g. solar powered
Computer devices can be easily / cheaply / quickly fixed / attached to large objects / shelving to deter theft
Physical locks require keys that may be lost / key fobs etc may be lost or stolen / given to unauthorised persons
Combinations to locks can be forgotten

32 **Six** *from:*
Electrical signals converted to light for transmission / converted back to electrical signals after transmission
LED / laser (at node) sends / transmits a light beam / electromagnetic wave along the fibre
Data is modulated onto a carrier wave
Optical fibre connects the nodes / devices
ADC / DAC are used to modulate / demodulate the data onto / off carrier wave
Laser is used where longer distances are to be covered
LED is used where shorter distances are to be covered as it is cheaper than laser
Lasers produce coherent light which can allow greater bandwidth
Receiver is photo detector to convert light into electricity
Uses indium gallium arsenide in photo detector.

33 A suitable diagram could be:



**Three** *from:*
All correct labelled boxes for routers C, D, E, F, G
All correct connecting lines between boxes / routers
All connecting lines shown as double-ended arrows.

(b)(i) (A, B), C/D, F, G, (H). **1**
(b)(ii) **Two** *from:*

shortest route is 5 hops so: 5 x 6 = 30 (time units)
x2 for return, 30 x2 = 60 (time units).

(c)(i) **Two** *from:*
longest route takes 7 hops so: 7 x 6 = 42 (time units)
x2 for return = 84 (time units).
**2**
(c)(ii) **One** *mark for all correct:*
(A, B), D, C, E, F, G (H).
**1**
(d)(i) Between B and G. **1**
(d)(ii) **Two** *from:*
4 hops · 6 = 24
_ 2 = 48 (time units).

34 **(a) Four** *from:*
Provides access (for protocols) to physical / wireless transmission medium
Creates the protocol stack (using its electrical components)

> [The **protocol stack** or network **stack** is an implementation of a computer networking **protocol** suite or **protocol** family. Some of these terms are used interchangeably but strictly speaking, the suite is the definition of the communication **protocols**, and the **stack** is the software implementation of them.]

Allows communications between LANs / WANs (using the protocols it has created)
Provides low level addressing at MAC level
Works at physical and data level of OSI model / OSI layer 1 and 2.
(b) **Seven** *from:*
Accepts data from CPU via internal buses
Converts parallel data stream to linear / serial data stream and vice versa for transmission / after reception to / from transmission medium
Data is sent / received in frames
*When sending:*
NIC is notified that frame has been created by OS in a buffer
NIC accesses / reads buffer / memory directly by DMA
NIC determines address and creates data frame
NIC transmits completed frame to transmission medium
NIC notifies OS that frame has been sent

*When receiving:*
NIC monitors transmission medium for frames
NIC reads frame from transmission medium into buffer using DMA
NIC checks frame contents and calculates checksum to verify integrity of data
NIC interrupts host OS to indicate that a frame has arrived
*Max. 6 if all sending or all receiving.*

35 **Five** *from:*
Cable ensures an uninterrupted connection to the TV
Cable does not suffer from dynamic range limitations as does Bluetooth transmission so (action) movies do not have same impact
Cable does not suffer from limited frequency ranges as does Bluetooth transmission so movie experience can be spoiled
Cable does not need power in the headphones so can be used without preparation when watching movies / unlimited by battery going flat
Bluetooth can suffer from interference from other wireless devices which can spoil the sound (effects) from movie
Bluetooth takes time to process so video and audio are out of sync / lip sync issues spoil the movie experience
Bluetooth headphones can be larger / uncomfortable / heavy due to battery requirements to movie watchers who get tired of using them before end of movie

| | |
|---|---|
| | Bluetooth headphones do not work if battery is flat / needs charging, so cannot listen to sound of movie. |
| 36 | This question to be marked as a Level of Response.<br>**Level 3 (7–8 marks)**<br>Candidates will evaluate, giving both advantages and disadvantages, of the use of anti-virus software in combatting IT crime.<br>The information will be relevant, clear, organised and presented in a structured and coherent format.<br>There will be a reasoned conclusion / opinion.<br>Subject specific terminology will be used accurately and appropriately.<br>**Level 2 (4–6 marks)**<br>Candidates will explain both advantages and disadvantages, of the use of anti-virus software in combatting IT crime.<br>For the most part, the information will be relevant and presented in a structured and coherent format.<br>There may be a reasoned conclusion / opinion.<br>Subject specific terminology will be used appropriately and for the most part correctly.<br>**Level 1 (1–3 marks)**<br>Candidates will describe the use of anti-virus software in combatting IT crime<br>Candidates will explain advantages / disadvantages of the use of anti-virus software in combatting IT crime<br>Answers may be in the form of a list.<br>There will be little or no use of specialist terms.<br>**Level 0 (0 marks):** Response with no valid content.<br>*Answers may make reference to e.g.:*<br>**Advantages**<br>Removes virus / malicious software that could delete / edit / destroy data<br>Protect against spyware to prevent theft of confidential / personal<br>information thus preventing unauthorised access to bank accounts leading to financial loss<br>Can help / may protect against spam / phishing emails thus preventing the divulgence of confidential / personal information<br>Protect against identity theft that may be a result of stolen confidential / personal information<br>Protect against redirection of automatic payments (‘stealware’ or ‘chargeware / affiliate fraud’) to help prevent ’click fraud’<br>Can help protect / stop unwanted / unauthorised use of computer for cryptocurrency mining |
| 37 | **Eight** *from e.g.:*<br>*Data protection laws are needed to address these concerns e.g.:*<br>Personal data is stored on computer systems / in databases which may not be secure<br>Databases are easily edited / searched / accessed (remotely) so data can be seen / manipulated<br>Data can be easily / quickly cross-referenced / correlated by computer systems<br>Computer systems can be networked so data can be accessed from many different locations / shared more easily between users<br>Control over shared data is more difficult to maintain<br>Accuracy of the information may be compromised / difficult to maintain when shared<br>Data can be easily copied to other media / stolen without any trace of the action<br>Data about individuals can be stored without their knowledge so infringing their privacy<br>Keeping records of who / what / when data is accessed are difficult to maintain unless enforced by law. |
| 38 | (a) *Three protocols from e.g.:*<br>FTP/file transfer protocol for uploading data/files/pages to server<br>HTTP/hypertext transfer protocol for accessing web pages<br>HTTPS/hypertext transfer protocol secure for secure data transfer<br>SMTP/IMAP/POP to send/receive emails<br>TCP/IP for packet transmission<br>SSH for secure access to a server/another workstation |

SFTP for secure method of uploading data to a server

SMB for transferring files to a file server

TELNET to connect computers to a switch/router.

(b) *Four from:*

Uses radio waves in 2.4 GHz/5 Ghz frequency ranges/(900 MHz and 3.6/60 GHz frequency bands)

Data frames are modulated onto carrier wave

Spread spectrum used for higher power levels

Two channels used for full duplex exchange of data/most WiFi is half-duplex

WiFi network uses SSID to identify itself

Access point and device must be connected to same WiFi network/SSID to be able to exchange data

Data is encrypted for security during transmission

Devices must use IEEE 802.11 protocols/standards

IEEE 802.11 has a number of variants a/b/g/n/ac(/ad/ah/aj/ax/ay/az) (must have 3 to gain this extra mark)

14 channels on 2.4 GHz which are 5 MHz spaced/device uses channels spaced apart to reduce channel interference.

(c) *Candidates may refer to e.g.:*

***Two** similarities from:*

They are both communication systems

Both use wireless technology

Both have more limited range than cabled networks

Both have limited bandwidth compared to cable networks

***Four** differences from:*

Bluetooth has a shorter range than WiFi

Bluetooth is restricted by solid objects/barriers/walls whereas WiFi can penetrate most barriers to some extent

Bluetooth has a lower bandwidth than WiFi

Bluetooth requires 'pairing' of devices whereas WiFi (often/usually) requires a full log in procedure

Bluetooth data transfer is 'one to one' whereas WiFi facilitates communication between several devices.

39 *Command word: Discuss: give important arguments for and against. Often requires a conclusion.*

This question to be marked as a Level of Response.

**Level 3 (7–8 marks)**

Candidates will evaluate in detail the benefits and drawbacks of the use of copper cables

The information will be relevant, clear, organised and presented in a structured and coherent format.

There may be a reasoned conclusion/opinion.

Subject specific terminology will be used accurately and appropriately.

**Level 2 (4–6 marks)**

Candidates will explain the benefits and drawbacks of the use of copper cables

For the most part, the information will be relevant and presented in a structured and coherent format.

There may be a reasoned conclusion/opinion.

Subject specific terminology will be used appropriately and for the most part correctly.

**Level 1 (1–3 marks)**

Candidates will describe at least one benefit and at least one drawback of the use of copper cables

Answers may be in the form of a list.

There will be little or no use of specialist terms.

**Level 0 (0 marks):** Response with no valid content.

*Answers may include reference to:*

*Benefits:*

Flexible so can be installed almost anywhere/can use 'tight' bends

Can run electrical power along copper cable/Ethernet cable

Can supply power to remote devices e.g. cameras high on buildings do not need separate power supply

Costs of installation are less than for fibre optic cables
NICs that use copper connections are cheaper to buy than those that use e.g. fibre optic
Can provide higher bandwidths than wireless/WiFi
Harder to hack into compared to WiFi

*Drawbacks:*
Can be subject to electrical interference
Must not be run next to mains power cables
Costs of installation are more than for wireless/WiFi
Cannot provide as high bandwidths as fibre optic
Break/lose contact/connection more frequently than fibre optic cables
Easier to connect into by unauthorised users
More of a safety/tripping hazard than WiFi.

40 (a) ***Three*** *from:*
Rapid access to (lost/removed) data/files
Protection of data/files against power loss/failure of main system
Protects against failure of storage system/hard disk
Protects against loss of data from viruses/malware
Protects against failure of OS.

(b) ***Three*** *from:*
Backups will store malware as well as safe data
Backups will not remove malware
Backups will restore data to time before malware infection but latest data will be lost
Backups may not store up to date data if run during office/use hours
Backups take snapshot of data which may change soon after backup is run so some data may not be backed up
Backups can be stolen in their entirety
If not encrypted all data can be stolen/accessed
Backup windows should use system downtime which may be limited to out of hours' time
System performance is reduced when backups are being carried out
Restoration of data after malware infection can be laborious and time consuming
Cost of extra hardware/storage may be excessive.

41 **Six** from:
Acts as gateway between LAN and WAN/internet
Allows use of multiple (internal) IP addresses through one (external) IP address on internet
Many computing devices/computers can be used through one internet connection
Presents single IP address to exterior networks/internet (as number of external IP addresses is limited)
Acts as a central device/node for logging/monitoring of internet access/activity
Acts as a central device/node for filtering of internet access/activity
Controls/requires username and password for internet access/activity
Prevents access to inappropriate material/activities
Acts as a cache for frequently used remote resources
Reduces access times/network traffic over internet connection.

42 a) *Eight from:*
Anti-malware/virus/spyware software to protect against viruses and spyware.
Firewall (software or hardware) to help to prevent unauthorised access to company network
Firewall to help to prevent unauthorised access to files stored by cloud storage provider
Only allow access to company devices/laptops/smartphones
Firewall to enforce company security polices
Firewall to interrogate data packets entering/leaving company networks/cloud storage providers
Firewall works by comparing contents of packets with predetermined/user defined rules
Router to direct data packets to/from internet from/to company network/Cloud storage provider
Router maintains database/list/table of IP addresses to forward packets

Router updates list from other routers as addresses become known to it
Router ranks entries in table according to probability of being correct address for packet to take on its route to destination
Router maintains list/table of other routers to send packet if route is unknown.
X should use encryption to secure the data for transmission
Passwords and user IDs should be required by the access/firewall software before allowing devices to connect/access.
*For 8 marks, must have at least 1 mark from each of firewall, router and encryption.*

(b) *Four from:*
Locations B and C are open to the public/any device can connect so there is no secure connection at these locations
Data may not be encrypted
Location B could be used by hackers using Man in Middle (MIM) to route data through hacker computer
Location B may be susceptible to fake/spoof/unauthorised wireless access points/connections
Location B may be susceptible to intercepting wireless signals from company devices as there is no check on users of cafes/can sit anywhere without reason/identification.

43 **Six** *from:*
Can transmit data long distances along thin fibre optic cables
Laser light is coherent so is not easily lost by dispersion
Can carry vast amounts of data/implement very high bandwidths for data transmission
Can be used in free space/just air so no need for cables
Can be used in a vacuum so can be used between spacecraft
Immune to electromagnetic interference
Increased security as difficult to intercept in fibre/free space
No licence to use is required (for use in free space) in most areas of the world
Can be used to power devices in free space.

44 (a) **Six** *from:*
Use of user ID with password/PIN known only to user
Request random selection of three of the digits of password/PIN
Transaction authentication number sent to customer/generated by code machine held by customer or by number on screen/sent to cell phone of customer □
... OTP/TAN is entered after user ID/password/PIN as next level of authentication □
... OTP/TAN checked against list issued to/held by customer
Use of one-time password generated by a security token
Multi-factor authentication using tokens/sequence of characters
Use of security questions/memorable words plus example
Use of biometrics such as fingerprint/retinal scan
Query use of different devices to log in.

(b) **Six** *from:*
IP security (IPsec) encrypting the data in the packet/encrypting entire packet
Layer 2 Tunnel Protocol (L2TP) and IPsec where L2TP creates the tunnel while IPsec does the encryption
Secure Socket Layer/SSL creates handshake system in conjunction with Transport Layer Security/TLS
Point-to-Point Tunnelling Protocol/PPTP to create a tunnel and encapsulate the data packet
An additional protocol will handle the encryption, e.g. TCP Secure Shell (SSH)
SSH will create the tunnel and carry out the encryption of the tunnel (not the data).

45 (a) *Three from:*

UHD has resolution of 4 times the number of pixels as HD/3840 · 2160 pixels (8.29 megapixels) v. 1920 · 1080 pixels (2.07 megapixels).
UHD has resolution of 4K/4096 · 2160 pixels.
UHD has resolution of 8K/7680 · 4320 pixels (33.18 megapixels)/16 times HD.
Increased dynamic range compared to HD.
Increased colour depth compared to HD.
More LEDs in a given area on screen increase the resolution so there is more detail.

*(b) Eight from e.g.:*

Internet bandwidth of c.25 megabits/sec is required.
Bandwidth required for UHD is not available to all customers/from all internet providers.
Satellite transmissions/signals can provide required bandwidth.
Reduced number of channels will be available unless new satellites are brought into service.
Wireless/mobile telephone/4G networks have restricted bandwidth so cannot provide ultra HD.
Introduction of 5G will make ultra HD available but will require new phones.
Copper cable networks can provide bandwidth/up to 100 Mbit/s as Cat 5 ethernet/Cat 6 1 Gbit/s.
Copper telephone cabling can provide ultra HD.
Distance from exchange is limited as bandwidth reduces over distance.
Fibre optic cables can provide high bandwidth (10 Gbit/s).
Cost of use of fibre to home/installation to home is high.
Fibre to cabinet (FTC) may provide UHD to more homes.
Fibre allows much longer cable runs so may reduce installation costs over long distances from exchange to home.

46 (a) *Six from:*

Different access rights/permissions can be given to different individuals/groups of individuals.
Set up as Access Control Lists.
Works on files/folders/directories.
Permissions on folder/directory may be cascaded down to files contained within.
Files within a folder/directory do not (necessarily) have same permissions as folder/director.
If a permission/access right is not explicitly set, the right is denied.
Read permission allows only viewing of file/directory/folder.
Write permission allows modification of files/deletion/creation/renaming of files (within folder/directory).
Execute permission allows file to run/executed.
Permissions must be set/mandatory if OS is able to run/execute file for user.

(b) *Six from:*

*Advantages of symmetric:*

Symmetric uses keys/same keys for encryption and decryption so that must be shared to access the data so sharing of keys (also) has to be secured.
Symmetric can be less secure because keys have to be shared/confidentiality of shared keys cannot be guaranteed.
Can be very/more secure as (can) use (fixed-size) block encryption rather than encryption of bits/multiple rounds of encryption (which encrypts the encrypted block over and over).
Keys have no special properties so are simple to generate.

*Advantages of asymmetric:*

Asymmetric uses public keys which can be accessed by anyone so no need to send key to specific user.
Asymmetric uses a private/confidential key (known only to owner) so is (very) secure/data can be transferred without danger of public access.
Key size is large/1024 to 2048 bits so security is high.
Keys are reusable saving time/cost for owner.

| | |
|---|---|
| 47 | a) *Four from:*<br>Can use long runs/lengths of cable compared to copper cables.<br>Low signal loss over long distances.<br>Greater tensile strength than copper.<br>Not susceptible to electrical interference.<br>Not susceptible to weather/environmental damage.<br>Can provide very high bandwidth/internet speeds for customers.<br><br>(b) *Three from:*<br>Difficult/require special equipment to splice/join if broken.<br>Loss of signal/light at joins.<br>If bent too much (beyond their limited physical arc) they will break.<br>Special test equipment is often required for testing.<br>Highly susceptible to physical damage/being cut or broken during construction/renovation/building/disturbance works.<br>Data transmission losses often occur when wrapped around curves with small radius. |
| 48 | *Six from e.g.:*<br>Data can be lost/stolen by unauthorised users/hackers using gaining access to storage devices.<br>Data can be stolen by interception of network traffic/capturing of IP packets.<br>Valid user accounts can be abused/accidently cause data loss/damage.<br>Malicious attacks with viruses/trojans/malware that damages/deletes/alters data.<br>Misuse of resources by (unauthorised) persons/devices.<br>Eavesdropping on other users’ activities can enable theft of data/ID.<br>Failure of hardware/software may expose data to loss/theft/damage.<br>No need to have physical proximity to computer to access/can access systems remotely. |
| 49 | *Five from:*<br>Key contents of a Data Protection Act include:<br>1 Personal data should be collected and processed fairly and lawfully.<br>Data subject should be informed about the data being collected.<br>Data subject should be asked for permission to collect it.<br>2 Personal data can be held only for specified and lawful purposes.<br>Data subject should know why data is collected/stored.<br>Law is broken if data is used for other purposes.<br>3 Personal data should be adequate, relevant and not excessive for the required purpose.<br>Only data that is needed can be stored.<br>4 Personal data should be accurate and kept up-to-date.<br>Wrong/inaccurate data must not be stored.<br>Wrong/inaccurate data should be corrected.<br>5 Personal data should not be kept for longer than is necessary.<br>Data must not be kept forever/unreasonable lengths of time/must be destroyed when no longer needed.<br>6 Data should be processed in accordance with the rights of the data subject.<br>Data subjects can inspect the data held about them.<br>Data subjects can insist that incorrect data is amended. |
| 50 | *Eight from:*<br>Maximum number of clients (usually) (voluntarily) restricted (to e.g. 100–200).<br>Number or transmitters/radios/e.g. 4 radios in access point restricts number of clients.<br>Range can be restricted by obstacles/materials that obstacles are made of.<br>Range can be restricted by the height of placement of access point.<br>Range can be restricted by the positioning/direction of antenna(s).<br>Range can be restricted by the presence of other electronic devices in vicinity.<br>Limited number of frequencies are available for data transmission.<br>The number of frequencies available varies in different jurisdictions to avoid interference. |

| | |
|---|---|
| | Large numbers of access points on the same/overlapping frequencies can interfere with each other.<br>Data transmission speed/bandwidth is usually lower/less than wired connection over long distance.<br>Bandwidth of wired can still be high/1000 Mbits/s at 100 m but wireless usually cannot achieve this.<br>Wireless access points have increased security considerations c.f. wired connections so must use password/security keys to connect/join to the access point.<br>Enforced use of passwords can slow down work/frustrate staff when connecting is slow/key is forgotten.<br>Wireless transmissions can be more easily intercepted so data must/should be encrypted.<br>If network key is stolen/publicised, then the key must be changed so every device must reconnect with new key.<br>Additional login details required for guests/temporary workers add to processing requirements in WAP.<br>Security measures add an overhead/slow down processing/data transfer speed.<br>Use of access points may require additional physical/shielding/use of Faraday cages in structure of building to prevent interception of transmissions which increases costs/add structural design complexity/restricts use of mobile connections by users inside the cage. |
| 51 | Eight from:<br>Satellite is in geostationary orbit so appears to be at fixed point above surface of Earth.<br>Must be at certain/correct height/c.37 000 km above equator.<br>Satellite has transmitting dish pointed at Earth.<br>Satellite has transponder(s) which receive(s) and transmit(s) signals (to/from Earth).<br>Receive and transmit signals use different frequencies.<br>Transmit (to Earth) signals are in set range/4–8 and 12–18 GHz range.<br>Horizontal and vertical signal polarisation is used to increase capacity.<br>Digital TV signal is encoded as standard/MPEG-2 TV signal with sound/audio (uplinked from Earth station).<br>TV signal may be encrypted to prevent viewing without paying for service.<br>High definition/ MPEG-4 TV signals with multi-channel sound requires more bandwidth.<br>Receiving dish on Earth is pointed at the satellite in line of sight.<br>Dish has Low Noise Block/LNB at antenna to amplify signal allows use of cheaper cable to receiver.<br>Receiver/TV/set-top box decodes signal into pictures and sounds for display on TV.<br>May include system for decrypting ‘scrambled’ pay TV signal. |
| 52 | *Six from:*<br>Multiple servers/source computers can be/are used without a central server<br>BitTorrent client required on internet-connected computer to implement BitTorrent protocol<br>Protocol works well/effectively over low-bandwidth connections<br>BitTorrent descriptor file is used to describe file being distributed<br>BitTorrent node set up with use of descriptor file and file to be distributed<br>Node becomes seed for download<br>Files made available to others for download by connection to seed/other peers<br>File being distributed is divided into small segments/pieces<br>Segment/piece becomes available to other peers as it is downloaded<br>…original seed/source is relieved of load<br>Every segment/piece is encrypted/protected by a cryptographic hash that can be used to detect changes to ensure file integrity<br>Segments/pieces downloaded in random order/non-sequentially and reordered by BitTorrent client. |
| 53 | *Eight from e.g.:*<br>Enables distribution of internet/network traffic/television and radio signals around home<br>Allows (remote) control of devices/TVs/devices without the need for wired connections<br>Allows use of multiple wireless handsets to use one wired landline so no need for extra lines/connections to landline |

Allows use of wireless doorbells without damage to infrastructure of building/doors
Allows communication without disruption/unsightliness of wires so can be used in historic buildings
Allows multiple devices to connect to central points/internet access points so no need for additional internet connections/ISPs
Allows easy sharing of devices/printers/scanners between computers so no need for complex configuration/setup routines/installations
Allows devices to be moved around/mobility of devices while in use so user can work anywhere
Allows use of (discrete) hearing aids connected to e.g. TV sets so no need for embarrassment of user/high sound volumes that disturb others
Allows use of remote control/monitoring of household appliances when away from home
Allows remote placement of security devices/cameras to avoid tampering/revealing placement position
Can be subject to interference from electronic devices/microwave ovens/fridges so can prove unreliable
Can create security issues if not set up properly so users' personal information can be at risk.
*Must be at least 1 advantage and 1 disadvantage for full marks.*
*One mark available for reasoned opinion/conclusion.*