AQA Computer Science A-Level

4.9.2 Networking

Past Paper Mark Schemes

June 2011 Comp 3

8	(c)		**Reason:** To reduce (network) congestion//improve throughput//*to cut the number of collisions**; **A** faster operation/transmission; **Explanation:** *by cutting the number of collisions**//by reducing the number of stations/computers connected to each section of cabling// because two computers in one segment can communicate at the same time as two computers in another segment; **Note:** * = Do not award two marks for cutting the number of collisions – only award one for either reason or explanation. **Reason:** To improve security; **Explanation:** by localising packet transmission to one segment; **Reason:** To improve reliability; **Explanation:** By limiting effect of cable failure to one segment; **Award marks for either:** • **one reason + explanation** • **two reasons** • **two explanations**	**Max 2**
8	(d)	(i)	Less expensive as reduced cabling requirement; No reliance on central node as data does not all travel through one node; **A** less cabling required without reference to reduced cost if candidate has explained why less cables are needed **A** computer/station for node **Must have explanation as well as advantage for mark**	**Max 1**

8	(d)	(ii)	Improved security as: data only travels down one link // is not sent throughout network // is not sent to all nodes; Improved reliability as if one link fails the other links/nodes are not affected; Speed of link remains constant // speed not affected by number of connections/collisions // faster connection as: no collisions/links not shared; **A** cable for link **R** responses about terminal/computer failure **Must have explanation as well as advantage for mark**	**Max 1**

10	(b)	(ii)	**Step** / **Data/Request Sent** 2 — Printer indicates ready; **A** Yes, Ack 3 — [Computer sends] data; 6 — Printer indicates ready to receive further data; **R** job complete **NE** data received **1 mark** per correct step	**3**

June 2012 Comp 3

8	(a)		System will be storing confidential/personal data (that must be kept securely/safely); Centralised/improved security management // centralised login system // centralised administration // administration will be easier; Centralised backup; Harder for users to change security/sharing settings; Running database from a server will avoid concurrency issues // will avoid problems if two users/computers update (a record in the) database simultaneously; **A** will allow simultaneous updates/access **R** answers that imply that on a peer-to-peer system there would be a separate copy of the database on each workstation Running database from server will ensure that it is always available (as server is unlikely to be turned off) // Files would always be available (as server is unlikely to be turned off); Server (operating system) may allow more simultaneous connections than a workstation // (operating system software on) workstations may not allow enough simultaneous connections for ten users; **NE** the database could be stored on the server **MAX 2**	2

June 2016 AS Paper 2

07	1	**Mark is for AO1 (knowledge)** **Mark as follows:** One of: wireless/network/wireless network Followed by one of: adapter/dongle/card/interface card; **A.** NIC	1
07	2	**Marks are for AO1 (understanding)** MAC address white list/filtering; **A.** description of a whitelist Wireless access points check MAC address of device trying to connect to network against list of allowed addresses; Only devices with an allowed MAC address are able to connect // devices without an allowed MAC address are not able to connect; **DPT** wrong type of address, eg IP address, or no type of address specified **Note for examiners:** refer other plausible methods to team leader	3

07	3	**Marks are for AO1 (understanding)** A network has limited bandwidth; (Preventing some devices from using the network will mean that) more bandwidth available for other devices/users // (preventing some devices from using the network) will decrease network traffic; (Fewer devices on the network means) reduced likelihood of two devices transmitting simultaneously or transmissions interfering with each other/colliding; **Max 2**	2

07	4	**1 mark for AO1 (knowledge) and 1 mark for AO1 (understanding)** **AO1 (knowledge):** **1 mark:** SSID is a (locally unique) identifier for a wireless network; **AO1 (understanding):** **1 mark:** A wireless client must use the same SSID as the one put in the access point to join // which prevents clients from accessing the wireless network unless they are using the same SSID as the access point;	2

07	5	**Marks are for AO1 (knowledge)** Set of rules; that allow two devices to communicate;	2

June 2017 AS Paper 2

08	3	**Marks are for AO1 (understanding)** The SSID/Service Set Identifier of the network will not be visible when trying to connect to a network; this means that only users who know the SSID of the network can try to connect; **A.** name for SSID	**2**

08	4	**Marks are for AO1 (understanding)** A MAC/Media Access Control address is unique to every NIC/Network Interface Card; A white list only allows those MAC addresses that have been authorised to connect to the network // devices whose MAC addresses are not in the white list are not allowed to connect to the network; **A.** Device for NIC **A.** Address for MAC Address **R.** first mark if not clear that MAC address is unique to NIC/device **R.** IP address for MAC address	**2**

June 2017 Paper 2

07		**All marks AO1 (understanding)**	12

Level	Description	Mark Range
4	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response. The response covers all four areas indicated in the guidance below and in at least three of these areas there is sufficient detail to show that the student has an excellent level of understanding of the issues and technologies involved. To reach the top of this mark range, an excellent level of understanding must be shown of all four areas.	10-12
3	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response but the response may only cover two or three of the areas indicated in the guidance below. A good understanding is shown of each of these areas and if only two areas are covered, the coverage of these is excellent.	7-9
2	A limited attempt has been made to follow a line of reasoning by covering at least two of the topic areas in the guidance below. Overall, at least four valid points must have been made which can relate to any of the topic areas in the guidance.	4-6
1	A few relevant points have been made but there is no evidence that a line of reasoning has been followed. The points may only relate to one or two of the four areas from the guidance or may be made in a superficial way with little substantiation.	1-3

Guidance – Indicative Response

1. How it was possible for data to be collected

WiFi signals can travel outside of property // over wide area // limited control over range

Any WiFi receiver in range can read the data packets **NE.** The receiver in the car can read the packets

No need to physically "tap" into a WiFi connection, unlike a cabled connection

A protocol that does not encrypt the transmissions may have been used // unencrypted data sent. **NE.** Network not secure

2. Steps to prevent

Use a protocol that encrypts data transmissions
A. Encrypt the transmission
R. Password protection

Example of secure protocol eg WPA, WPA2

Disable broadcast of SSID to make network harder to identify (Note: Accept this point even though the SSID would be in other data packets)

		Limit power of transmitter so data does not travel outside premises (although in practice this might be hard to achieve) Use cabled network instead of WiFi. **R.** MAC address filtering (as cars were not connecting to networks just intercepting transmissions) **3. Legal and ethical issues** If the data is being transmitted through the air, who does it belong to, if anyone? // Should data transmitted by WiFi be treated like a broadcast (eg TV) or a private communication (eg telephone call)? Is it wrong to intercept data if people freely choose to transmit it wirelessly? **A.** Is it ethical to collect data from people without their permission? Is it legal to intercept data if people freely choose to transmit it wirelessly? What laws apply in this scenario? Is this really hacking? Are the ethics or laws different for intercepting data transmitted wirelessly than by cable? Is there a difference between collecting statistical data eg channel number, signal strength, SSID and collecting the payload data? Was the data just collected or was there an intention to process it as well? What should the company have done when it realised that the data had been collected? // Should the data have been immediately deleted, or kept so that the company could contact and apologise to people it had collected data from? // What should be done with the data now? What should the company have done if it inadvertently discovered evidence of illegal activity in the collected data? Legality/ethicality may depend on the nature of the data gathered // (In the UK) would some of the collected data count as "personal data" (under the Data Protection Act) // could some of the data have been sensitive (accept example eg bank account details, details of minors) **NE.** Data may be private To what extent is the company financially liable for collecting the data? Or any consequences of its use? Could the legal situation be different in different countries where the company operated? Was the collection of data intentional or just an accidental side-effect of a reasonable process? What was done to ensure (existing) policies are followed? Should there have been more oversight of code development? Could intellectual property have been inadvertently stolen? Is it ethical to collect/store information secretly from people // without them knowing? Is it ethical to collect data if there is no (legitimate) purpose for doing so? Were the developers in breach of their contracts with the company / company guidelines?	

		Relevant Legislation Students may name specific pieces of legislation that could have been breached as part of their response. Determining whether or not a breach has actually occurred would probably require more information than is provided in the question and detailed knowledge of the legislation, which is not required by the specification. Therefore, up to **two points** can be given for students naming relevant pieces of legislation that could have been breached, regardless of whether or not this can be ascertained with certainty. Relevant pieces of legislation include: • The Data Protection Act • The Computer Misuse Act • The Regulation of Investigatory Powers Act • The Communications Act Points should be given for assertions that legislation has definitely been breached, even if this is only a possibility in the context rather than a certainty. Responses that reference other legislation should be referred to Team Leaders. **A.** As an alternative to naming the Data Protection Act, a response could instead question whether privacy laws have been breached, or if a breach of privacy has occurred. **4. Lessons** Improved training for developers in what is legal / ethical (accept company needs to improve understanding of legal/ethical issues) Need to review guidelines that developers are expected to follow Need for scrutiny of code / supervision by people outside of development team Developers could be required to check each other's code Developers could be required to log changes made to code and reason Should only collect data that is absolutely necessary // that has a clear purpose // need to review collected data to see why it is being collected and stored // need to fully consider the purpose of any data collection before doing it Could/should remove equipment for Wi-Fi data capture used in cars to collect mapping data. **NE.** Further testing should be carried out unless there is a clear explanation of the mechanism by which testing will check that the software has no additional functionality is described eg inspection of collected data files to verify purpose of contents	

09	2	**All marks AO1 (understanding)** **Physical**: The (physical) layout/arrangement/architecture of the cabling/wiring/connections (between the devices/computers on the network); **A**. The (physical) layout/arrangement/architecture of the devices/computers/network **NE.** How the devices/computers are connected to each other **NE.** "Setup" for layout **NE.** List of topologies eg bus, star **Logical**: How the data/packets flows around a network // architecture of the communication mechanism in a network; **A.** Conceptual way that data moves around a network **A.** The type of protocol used **NE.** How a network operates/behaves	**2**

09	3	**All marks AO1 (understanding)** **Client-server (MAX 2):**	**4**
		Resources stored on the server; **R.** Responses which suggest that everything must be done on the server Clients access resources from server // server provides these resources in response to client requests; **A.** Server provides services to client Centralised / improved security management // centralised login system // centralised administration // administration will be easier; Configuration/setup more complex // configuration/setup requires greater expertise; **Peer-to-peer (MAX 2):** Resources stored on each individual computer/device/peer; Any computer/device/peer can access resources from any other // any computer/device/peer can share resources with any other // files can be distributed across the computers on the network; Each computer/device/peer has equal status // a computer can act as both client and server; Management of security / administration could be more difficult; Computers communicate directly with each other // there is no dependence on a server; **NE.** Computers connected directly to each other, no server ***In both sections, reject points about how computers are connected to each other.*** ***Accept responses that use examples of resources eg files, web pages*** **MAX 4**	

June 2013 Comp 3

5	(b)		Bus (topology/network); **A** Line	1

5	(e)	(i)	Use of Wired Equivalent Privacy/WEP/ WPA/WPA2/WiFi Protected Access; (Strong) encryption of transmitted data // use of Advanced Encryption Standard/AES; **R** encoding Use of Extensible Authentication Protocol/EAP; User/computer must enter/send a passphrase/certificate at start of communication before laptop allowed to connect; **A** key for passphrase **A** only allow password if used in correct context ie for accessing network, not for logging on to a sever or just having a password Access point checks MAC/hardware address of laptop and only allows computers with a MAC/hardware address in a list of approved addresses to connect; **R** IP address Disable broadcast of SSID/identity; Reduce / limit power of transmitter; Use of two/multi-factor authentication;	1

Specimen AS Paper 2

04	1		**Marks are for AO1 (understanding)** **1 mark:** each correct description	4

Label	Description
1	channel idle/not busy // no node transmitting;
2	no acknowledgement received; **NE.** collision occurs
3	acknowledgement received; **NE.** no collision detected
4	(wait for) random period of (time);

04	**2**		**1 mark for AO1 (knowledge) and 2 marks for AO1 (understanding)** **AO1 (knowledge):** **1 mark:** SSID is a (locally unique) identifier for a wireless network; **AO1 (understanding):** **1 mark:** A wireless client must have the same SSID as the one put in the access point to join; **1 mark:** Broadcasting SSID announces publicly your wireless network and can be seen as a security weakness;	3

Specimen Paper 2

04	1	**All marks AO2 (apply)**	12

Level	Description	Mark Range
4	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response. The response covers all four areas indicated in the guidance below and in at least three of these areas there is sufficient detail to show that the student has a good level of understanding of the technologies required. A good level of understanding would be indicated by three substantiated points being made per area. To reach the top of this mark range, a good level of understanding must be shown of all four areas.	10-12
3	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response but the response may only cover three of the areas indicated in the guidance below, with two or three substantiated points being made per area.	7-9
2	A limited attempt has been made to follow a line of reasoning by covering at least two of the topic areas in the guidance below. Overall, at least four valid points must have been made which can relate to any of the topic areas in the guidance.	4-6
1	A few relevant points have been made but there is no evidence that a line of reasoning has been followed. The points may only relate to one or two of the four areas from the guidance or may be made in a superficial way with little substantiation.	1-3

Guidance – Indicative Response

		1. Fridge capturing data from food RFID well suited as completely automatic short-range wireless transmission so no user involvement • tag does not contain a power source but is energised by reader in fridge • this causes wireless transmission of data stored in memory on tag to reader Alternatively, scan barcode/QR code as food put into fridge Barcode less suitable than RFID as only identifies product not use by date and must be manually scanned Problem of how to deal with untagged produce – possible use of voice recognition or touch screen interface Can identify products and potentially track use by dates, but how to work out how much of the product is left – refrigerators redesigned with load cells to weigh items automatically?	

2. Networking technologies

IPv4 does not have a big enough address space for the number of devices, hence introduction of Ipv6

Higher bandwidth Internet connections required for so many devices

- copper-based transmission systems replaced with fibre optic

Need for a standard (application layer) protocol for devices

Security issues with many devices connected to Internet that could be hacked

Would data be communicated to retailers directly from each device or through a server in the home?

Need to consider how to deal with interference between wireless devices, collisions etc with many more devices communicating

3. The data gathered and storage

Automatic collection of data from devices will produce vast amounts of data

This volume of data would be classified as big data

May also be classified as big data due to the velocity of data collection with so many devices

Storage could be cloud based for flexibility or close to processing cores for speed

Velocity at which data generated would make solid state storage appropriate as has fast access speeds but volume of data and lower cost per megabyte of hard disk storage may mean hard disks more likely to be used

Need to consider how long to keep data for in context of

- Storage capacity available
- Complying with relevant laws about privacy

4. Processing

		Volume of data means parallel processing or distributed processing architectures required Volume of data collected makes it unsuitable for processing by traditional relational databases Functional programming is one approach that could be used Functional programming appropriate as works well on parallel processing systems as programs do not specify order of execution Would software that managed contents of the fridge be run as embedded system in fridge or in the cloud / by the retailer? Retailers may develop a standard API to interface with devices	

07	**2**	**All marks AO1 (understanding)** **1 mark for advantage and 1 mark for reason. Must give the advantage to get the reason mark.** **1 mark: (any 1 from)** Improved security; as data only travels down one link // is not sent throughout network // is not sent to all nodes; Improved reliability; as if one link fails the other links/nodes are not affected; **1 mark: (any 1 from)** Speed of link remains constant // speed not affected by number of connections/collisions // faster connection; as no collisions/links not shared; **A.** cable for link **R.** responses about terminal/computer failure	2

<table>
<tr>
<td>07</td>
<td>3</td>
<td>2 marks for AO1 (knowledge) and 4 marks for AO1 (understanding)

<table>
<tr><th>Level</th><th>Description</th><th>Mark Range</th></tr>
<tr><td>3</td><td>A detailed, coherent, description of the basic mechanism that shows a good level of understanding. To score six marks, either the description of the basic mechanism must be comprehensive, or, there may be one or two minor errors or omissions in the description of the basic mechanism but these are compensated for by also describing some aspects of CTS/RTS or the back-off mechanism.</td><td>5-6</td></tr>
<tr><td>2</td><td>An adequate description, including at least three points from the lists below. Some aspects of the basic mechanism may be missed out. The description is logically organised so that it makes sense when read as a whole and therefore demonstrates a reasonable understanding of how the system works.</td><td>3-4</td></tr>
<tr><td>1</td><td>A small number of relevant points</td><td>1-2</td></tr>
</table>
</td>
<td>6</td>
</tr>
</table>

				have been recalled (in this case award one mark per point, up to a maximum of two from lists below). However, the structure of the response, or lack of it, fails to demonstrate an understanding of the mechanism used	

Basic mechanism:

- computer monitors/listens for (data signal)
- if (data) signal present/another transmission in progress then continue to wait
- when no (data) signal present start to transmit
- wait to receive acknowledgement packet (to confirm data received and not corrupted)
- if no acknowledgement received (within reasonable time period) then:
  - wait a random time period
  - then retransmit.

CTS/RTS (if implemented):

- before starting to transmit, computer sends a Request to Send (RTS) to access point
- access point will respond with a Clear to Send (CTS) signal to only one computer at a time
- only the computer that receives the CTS signal will transmit.

Back-off mechanism:

- waiting period is random to reduce likelihood of two computers transmitting at the same time again // to reduce likelihood of another collision
- if a collision occurs again then wait a longer random time before attempting to transmit again
- use of exponential back-off algorithm to determine wait time.