



9.3 The internet part 1 Mark Scheme

Mark schemes

Q1.

Mark is for AO1 (knowledge)

Symmetric: The same key is used to encrypt and decrypt;

A. Sender and receiver use same key

Asymmetric: Different (but related) keys are for encryption and decryption;

A. Sender and receiver use different keys

NE. Symmetric uses one key // asymmetric uses two keys

Max 1

[1]

Q2.

Marks is for AO2 (understanding)

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

[12]

Q3.

	URL	Domain name	IP address	Socket address	Protocol
Telnet					✓
192.168.10.23:80				✓	
http://www.bbc.co.uk	✓				

1 mark - one row correct

2 marks - ALL rows correct

A. Marks other than ticks if intention clear

[2]

Q4.

- (a) To take a required Fully Qualified Domain Name/FQDN and to return an IP address;

To link/map a FQDN to an IP address;

A. domain name for FQDN

R. URL

Max 1

- (b) The (local) computer already has a copy of the needed IP address (in a hosts file);

The (local) computer has a cache of recent DNS queries / answered DNS queries;

A. previously visited site / refreshing a page;

The URL typed in already contains an IP address;

The URL refers to a local resource, e.g., a file on the local computer // localhost // local network;

NE. intranet

Max 2

[3]

Q5.

- (a) (Using an algorithm) to convert a message into a form that is not understandable (without the key to decrypt it);
 (Using an algorithm) to convert a message into a form that is only understandable by the intended parties // can only be read with the correct key;
 (Using an algorithm) to convert a message into cipher text;
NE. Scrambling unless further explanation is provided
NE. Coding
A. "Unreadable" for "understandable"
A. "Data" for "a message"
R. Responses that do not make clear that encryption is a process

- (b) **1 mark** for two or three keys correctly named.
2 marks for all four keys correctly named.

Label	Key Name
①	A's Private Key
②	B's Public Key
③	B's Private Key
④	A's Public Key

A. "Sender" for "A" and "Recipient" for "B" (or similar role descriptions)
 Allow use of same key name more than once and mark correct in the position it is correct (if any).

2

- (c) Two (message) digests are compared // received and recalculated digests compared;

A. "They" for the two message digests

A. "Hash" for "digest"

R. Two messages are compared

1

- (d) To authenticate/confirm identity of sender // to confirm that message was sent by A;

A. Ensures sender is who they say they are

NE. Identify the sender (must be clear that the signature confirms this identity), know who the sender is

To detect if message has been tampered with/altered/changed;

NE. Prevent/stop the message being tampered with

Award marks in part (d) for valid responses to part (d) that are made in part (c).

2

[6]

Q6.

SUBJECT MARKING POINTS:

Internal:

- Student's computer uses subnet mask (and destination/web server's IP address) to determine if destination computer/web server is on same subnet // identify not on same subnet
- Up to two marks from description (in separate section below) of how subnet mask is used
- Packet is sent (from student's computer) to Router (1)
- Router 1 identifies that destination is outside the LAN so forwards packet to router 3/router connected to Internet **A** gateway connected to Internet

External:

- Hierarchical organisation of routers
- Example of hierarchical organisation of routers eg passed up to a national router, transferred internationally and then passed back down a hierarchy
- Path to take selected by each router (not determined at start) **NE**. passed from router to router
- Route may change as a result of eg congestion, technical problems

Either:

- (Possible) repackaging of packet to use different protocol
- Route determined using the (Network ID part of the destination) IP address (**Note:** can infer "IP address" if just "address" is stated, if previously candidate has written about an IP address)
- Use of router tables / criteria to determine next hop / (step of) path
- Router decrementing "time to live" of packet
- Source and destination MAC addresses changed at each router // MAC addresses used for each "hop"

How subnet mask used (MAX 2 points):

- AND operation of subnet mask with student's computer's IP address
- AND operation of subnet mask with web server's IP address
- Result (of AND operation) is the network ID
- Network IDs compared
- If they are the same, then the computers are on the same subnet

A. Interchangeable use of subnet ID and network ID

HOW TO AWARD MARKS:

Mark Bands and Description	
7-8	<i>To achieve a mark in this band, candidates must meet the subject criterion (SUB) and all 5 of the quality of language criteria (QLx).</i> SUB Candidate has covered both internal and external routing in <u>detail</u> and has made at least seven subject-related points. QWC1 Text is legible. QWC2 There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear. QWC3 The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently. QWC4 Sentences (and paragraphs) follow on from one another clearly and coherently. QWC5 Appropriate specialist vocabulary has been used.
5-6	<i>To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).</i> SUB Candidate has covered both internal and external routing, <u>although one may be in more detail than the other</u> and has made at least five subject-related points. QWC1 Text is legible. QWC2 There may be occasional errors of spelling, punctuation and grammar. Meaning is clear. QWC3 The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably

	fluently. QWC4 The candidate has used well-linked sentences (and paragraphs). QWC5 Appropriate specialist vocabulary has been used.
1-4	<i>To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).</i> SUB <u>Candidate may not have covered both internal and external routing, but has covered at least one of them.</u> Up to four relevant points have been made. QWC1 Most of the text is legible. QWC2 There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response. QWC3 The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed. QWC4 Sentences (and paragraphs) may not always be well-connected. QWC5 Specialist vocabulary has been used inappropriately or not at all.
0	Candidate has made no relevant points.

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 4 of the quality of language criteria are met in the lower band. If 4 criteria are not met then drop by two bands.

[8]

Q7.

- (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

(b) **How works (MAX 3):**

All/most processing done by (central) server; **A.** All software run on server
 Keystrokes/mouse clicks/user input transmitted from workstation/terminal to

server over network; **A.** Workstations are just interfaces
 Image/data needed to produce image transmitted from server to terminal over network;
 Applications not installed on (thin client) workstations // all applications on server;
 Operating system loaded by clients from server at boot;

Selection of hardware (MAX 3):

Higher bandwidth network connection required;
 Network must use switch not hub;
 Slower processor /reduced RAM/ no HDD required in workstations;
A. Other examples of limited hardware requirements **A.** 'Dumb terminal'
 Server must have multiple processors/a lot of RAM;
NE. More powerful / less powerful, higher performance / lower performance, cheaper / more expensive
 Accept the opposite of points eg for "Slower processor" accept "a thick client system would need a faster processor".

6

- (c) College network uses a different protocol from the Internet/their ISP // College network does not use TCP/IP;
A. Examples of different protocols/hardware types being used

1

[9]

Q8.

- (a) A numerical label/value assigned to a device;
 A series of four bytes // a 32 bit number;
A. a series of 16 bytes // a 128 bit number;
A. octet as an alternative to byte
R. Internet Protocol

MAX 1

- (b) (i) A set of rules (for communication between devices);

1

- (ii) **HTTP:**
 HTTP is a protocol for accessing websites which are usually available to the general public;

Telnet (MAX 1):

The school does not wish people outside of the school network to remotely login to a school computer // open Telnet port is a security risk;
A. Telnet is an insecure protocol;

2

- (c) **Client server model:**
- User runs a client application to connect to the server/server application // client sends a request to the server
 - Server (performs processing and) sends result back to client

Steps to update server:

- Run the Telnet client on the laptop to connect to the

- company server
- Login to the company server
- Run the FTP client on the company server // use of FTP client to connect to FTP server
- Login to the security update FTP server using username and password
- Download/transfer the required file
- Run the command to install the security update // apply the security update
- Log off from the server // Disconnect from the server

Alternative steps:

- Run the FTP client on the laptop to connect to the security update Server using username and password
- Download/transfer the required file
- Connect to the company FTP server
- Upload the required file from the laptop
- Run the Telnet client to connect to the company server
- Login to the remote server
- Run the command to install the security update // apply update
- Log off from the server // Disconnect from the server

HOW TO AWARD MARKS:

Mark Bands and Description	
5-6	<i>To achieve a mark in this band, candidates must meet the subject criterion (SUB) and all 5 of the quality of written communication criteria (QWCx).</i> SUB Candidate has made at least five mark-worthy points and covers both the client server model and the steps form a logical sequence to update the server. QWC1 Text is legible. QWC2 There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear. QWC3 The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently. QWC4 Sentences (and paragraphs) follow on from one another clearly and coherently. QWC5 Appropriate specialist vocabulary has been used.
3-4	<i>To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the quality of written communication criteria (QWCx).</i> SUB Candidate has made at least three mark-worthy points. QWC1 Text is legible. QWC2 There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.

	QWC3 The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently. QWC4 The candidate has used well-linked sentences (and paragraphs). QWC5 Appropriate specialist vocabulary has been used.
1-2	<i>To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 3 of the 5 quality of written communication criteria (QWCx).</i> SUB Candidate has made a small number of relevant points. QWC1 Most of the text is legible. QWC2 There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response. QWC3 The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed. QWC4 Sentences (and paragraphs) may not always be well-connected. QWC5 Specialist vocabulary has been used inappropriately or not at all.
0	Candidate has made no relevant points.

6

[10]

Q9.

(a)

Situation and Procedure	Authentication	Authorisation	Accounting
A web server generating a log of the IP addresses of computers that have accessed it.			✓ ;
Using a digital signature when sending an e-mail message.	✓ ;		

R. Responses in which more than one column is ticked on a row

A. Responses in which a symbol other than a tick is used

(b) **Virus is (max 2 marks):**

Program that attaches itself to / conceals itself within another program/file;

Self-replicating // program can copy itself; **N.E.** Viruses spread

Has malicious purpose; **A.** Is a type of malware **A.** Examples of malicious purposes

Difference to worm (max 2 marks):

Worm duplicates by exploiting network security weaknesses / across network (whereas virus copies itself by attaching to other files);

Worm is standalone software (whereas virus conceals itself within another file);

Worm replicates without user action (whereas virus relies on user running program to replicate it);

MAX 3

3

(c) Hash/digest produced/calculated from message contents //

(shortened) value calculated from message; **A.** Message is hashed **A.** Message digest created **N.E.** Hash produced Hash encrypted;

A's private key is used for the hash encryption; **N.E.** Uses A's private key

Encrypted hash is known as the (digital) signature;

(Digital) signature is appended to message; **A.** Encrypted hash for digital signature

I. Description of encryption not related to digital signature

MAX 4

4

[9]

EXAM PAPERS PRACTICE

Q10.(a) **Marks are for AO1 (understanding)**

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);

1 mark: each correct description

4

- (b) **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

- (c) **Marks are for AO1 (understanding)**

In coffee shop speed could be limited for each device that is connected // throttling;

In coffee shop more clients connecting to one access point;

In coffee shop connection to Internet might have less bandwidth;

In coffee shop there may be more collisions;

NOTE accept answers made in terms of home

Max 2 marks

MAX 2

[9]

Q11.

- (a) **Marks are for AO1 (knowledge)**

Encryption is the encoding of a message;

conversion of plaintext into ciphertext;

so that other parties cannot read;

message can only be decrypted by the authorised receiver;

Max 2 marks

MAX 2

- (b) **Marks are for AO1 (understanding)**

Greater scrutiny / checking of code;

Weaknesses in the routines can be spotted and publicised;

The security of the routines can be tested / validated by third parties;

Other programmers can learn from the code;

From a philosophical point of view source code should be available;

Might encourage further development of the program;

Max 2 marks

MAX 2

- (c) **Mark is for AO2 (analyse)**

(Large) software libraries have many lines of code;

Cryptography software is complex;

(Open source software) programmers are volunteers;

(Open source software) library has limited funding;

tracing the effect of one line of code is hard / time consuming;

(Heart beat) functionality was not critical to the running of the code // code ran

without any noticeable problems so didn't raise concerns;

Code review (of OpenSSL) was defective;

No-one needed to change this code for two years so they presumed it worked and did not inspect it;
Any 1 from above. Max 1

MAX 1

(d) **Mark is for AO2 (analyse)**

1 mark: Reasons for: Max one
 Detection of illegal activities;
 Monitoring of other states / countries;
 Protection of national interests;

1 mark: Reasons against: Max one
 Invasion of privacy;
 Commercial secrecy;

2

[7]

Q12.

(a) **All marks AO1 (understanding)**

1 mark: A will encrypt the message using **B's public;** key.

1 mark: The message will be decrypted by B using **B's private;** key.

2

(b) **All marks AO1 (understanding)**

1 mark: Detect (unauthorised) changes to message;

1 mark: Authenticate sender's identity // confirm who sent it;

2

[4]

Q13.

(a) SMTP;

Telnet;

A SSH;

Note

For SMTP accept Simple Mail Transfer Protocol

For SSH accept Secure Shell

2

(b) Uniform Resource Locator;

I case

1

(c) 129.12.3.236 // 10.0.1.1 // 81.111.110.1 //
 213.105.114.89 // 62.253.174.77;

I brackets

1

(d) A link between routers might be down / busy and / or a different route is picked;

Routes are determined dynamically as the packet moves from sender to receiver;

A to take the fastest route at that time

NE to travel faster

MAX 1

(e)

	Layer
1	Application (layer)
2	Transport (layer)
3	Network / internet (layer)
4	Link (layer)

1 mark for any two layers correct;

2 marks for all four layers correct;

2

- (f) (Link layer) responsible for network drivers // network cabling // physical connection // changing from one medium to another;

(Link layer) (removes MAC address and) adds MAC address for the next hop;
A hardware address for MAC address

(Network layer) looks at destination IP address;

Router decides on next appropriate hop (after seeing destination IP address);

(Network layer) can split / combine / resize packets if required;

error checking / error detection;
encryption for wireless connections;
tunnelling through a firewall;

MAX 2

[9]

Q14.

- (a) 192.168.0.x (where x is not 0, 2 or 255);

1

- (b) Star (topology);

A Star network

I additional writing that does not talk out the response

1

- (c) Devices are not directly connected to the Internet;
NE all computers on a private network

So that LAN devices cannot be connected to (directly) by computers outside of the LAN / on the Internet // for increased security;

A relevant examples of increased security

Don't need to be allocated by a central authority // would be difficult to organise for each device to have a unique (routable) IP address // easier to allocate if do not need to be unique // (as devices not directly connected to Internet) IP addresses don't need to be globally unique;
NE routable IP addresses globally unique and non-routable only locally unique

Would / May not be enough unique IP addresses for each device to have a routable address // globally more IP addresses would be required if all devices had routable IP addresses // more bits would be required to store an IP address if all devices had routable IP addresses;

MAX 2

2

- (d) AND operation performed using IP address(es) and subnet mask (to produce network IDs / subnet IDs of both desktop computer and FTP server) // Network IDs / subnet IDs / first three octets / bytes / values (in IP addresses) computed using IP address(es) and subnet mask;

To award either of the next two marks, the candidate must have indicated that the subnet mask is used to produce the results that will be compared - even if the method by which the subnet mask is used is incorrect so the first mark has not been awarded.

Network / subnet IDs of both computers / machines compared;
A Results of previous operation compared
A First three octets / bytes / values (in IP addresses) compared
A Award this mark by implication if it is stated what will happen if these two are the same or different

As network / subnet IDs (**A** first three octets / bytes / values / results) differ, desktop computer determines that FTP server is not on same network (so must be communicated with via combined device);

3

- (e) Block / allow (traffic on) specific ports // block specified protocols;
 Block / allow (traffic from) specific IP addresses / domain names;
 Search packets for specific contents / text (and block / allow based on this);
 Act as a proxy server // all traffic to Internet must go via firewall // stops computers on the Internet directly accessing devices on the LAN;
 Stateful inspection // firewall maintains information about current connections and only allows packets relevant to these connections through;
 Identifies unusual behaviour from a host // example of unusual behaviour eg sending an unusually large amount of data;
NE Packet filtering
NE "Data" instead of "packets"
NE Block specific programs connecting to Internet
A Firewall checks packets using rules / criteria for 1 mark if not other marks awarded

MAX 3

3

- (f) *Baseband*
 Whole bandwidth of medium dedicated to one transmission (at a time) // one channel (at a time) // only one computer can send data (at a time) // sends signals with frequencies from 0Hz to a maximum highest frequency;
Broadband
 Bandwidth of medium shared // multiple channels can be carried

(simultaneously) // many computers can send data (simultaneously) // frequency bands assigned to different communications; **TO** multiple wires

MAX 1

1

- (g) More reliable // less susceptible to interference // more stable connection;
Faster transmission speed // higher bit rate // lower latency;

R More secure (not relevant in this instance)

NE Just the word “faster” on its own.

MAX 1

1

[12]

Q15.

- (a) (i) **A** the protocol to be used // secure hyper-text transfer protocol // hyper-text transfer protocol secure;
NE hyper-text transfer protocol
B the FQDN // fully qualified domain name;
A the address of (AQA's) web server
C the path and resource to be returned;
A path / pathname / file path

3

- (ii) uk // .uk ;

1

- (b) (i) To take a required FQDN and to return an IP address;
To link / map a FQDN to an IP address;
A domain name for FQDN
R URL

1

- (ii) The (local) computer already has a copy of the needed IP address (in a hosts file);
The (local) computer has a cache of recent DNS queries / answered DNS queries;
A previously visited site / refreshing a page;
The URL typed in already contains an IP address;
The URL refers to a local resource, e.g., a file on the local computer // localhost ;
NE intranet

MAX 2

- (c) (i) application (layer);
A fourth layer;

1

- (ii) To fetch different parts of the web page that also include an URL;
To fetch a needed image / video / javascript / css / resource;
R transmission error
R network busy

MAX 1

- (iii) Port that is temporarily assigned / only exists for duration of a connection;
Port number automatically allocated // assigned from the TCP / IP stack;
A a port number in range 1024 - 65535

MAX 1

Q16.

Company will need to register / purchase the domain (with an Internet registrar);

DNS records will need to be setup // IP address needs to be linked to domain name
//

www.learncomputing.co.uk set to point to 123.45.67.100;

(Using telnet) company will need to install web-server / ftp-server onto the server;

Web-server configured for root web folder;

These services will need to be started on the server;

Each service will be allocated a port to listen on;

The web server should be set to run on port 80 // FTP set to run on port 21 / 20;

Web pages written in HTML / hyperlinked pages / CSS;

Cascading style sheets / CSS used to control layout / presentation;

upload to the server files using FTP (client);

After the DNS records have propagated around Internet users will be able to access website;

Company may wish to perform some search engine optimization (SEO) to allow user to easily find site;

Mark Bands and Description

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and all 5 of the quality of language criteria (QWCx).

SUB Candidate has made at least five subject-related points.

QWC1 Text is legible.

QWC2 There are few, if any, errors of spelling, punctuation and grammar.
Meaning is clear.

QWC3 The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.

QWC4 Sentences (and paragraphs) follow on from one another clearly and coherently.

QWC5 Appropriate specialist vocabulary has been used.

5-6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB Candidate has made at least five subject-related point.

QWC1 Text is legible.

QWC2 There may be occasional errors of spelling, punctuation and grammar.
Meaning is clear.

QWC3 The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.

QWC4 The candidate has used well-linked sentences (and paragraphs).

QWC5 Appropriate specialist vocabulary has been used.

3-4

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

- SUB** Candidate has made at least one subject-related point.
- QWC1** Most of the text is legible.
- QWC2** There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
- QWC3** The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
- QWC4** Sentences (and paragraphs) may not always be well-connected.
- QWC5** Specialist vocabulary has been used inappropriately or not at all.

1-2

Candidate has made no relevant points.

0 marks

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 4 of the quality of language criteria are met in the lower band. If 4 criteria are not met then drop by two bands.

Max 6

[6]

Q17.

- (a) Data Protection (Act);
- (b) Data should be kept securely;
- (c) Data should be fairly and lawfully processed;
Data should be obtained for specified and lawful purposes. (**A** Data should be processed for limited purposes);
Data should be adequate, relevant and not excessive;
Data should be accurate // kept up to date;
Data should not be kept longer than necessary;
Data should be not transferred to other countries without adequate protection;
Data should be processed in accordance with the rights of the data subjects.

1

1

Max 1

- (d) That data is not being encrypted // data is not being sent securely // that hackers might be able to see personal data;
A the protocol / it is not secure
R website not secure

HTTPS // HyperText Transfer Protocol Secure;

2

- (e) Word processor : General purpose (application software);
Parent portal : Bespoke;
Web server : Special purpose (application software);

3

[8]

Q18.

- (a) (i) Hypertext Markup Language;

1

(ii) Cascading Style Sheet(s);

1

- (b) 2 – RoboEddy Homepage ; **A** minor typos
 3 – font-style ; (must have hyphen)
 4 - /style ; (must have /)
 5 – toptitle ; **R** #toptitle
 6 – class ;
 7 - ul 8 -- / ul (7 + 8 both correct);

NOTES:

Ignore for parts 4,7 and 8

6

[8]

Q19.

- (a) (i) 192.168.0.x where x is not 0 or 255;
 Must be a specific IP address
R addresses that include port numbers
- (ii) 192.168.1.x where x is not 0 or 255;
 Must be a specific IP address
R addresses that include port numbers
- (iii) 192.168.1.y where y is not 0 or 255 and is not the same as x in (ii);
 Must be a specific IP address
R addresses that include port numbers
- (b) Bus (topology / network);
A Line
- (c) 255.255.255.0 / FFFFFFF0 /
 11111111 11111111 11111111 00000000;
- (d) (An operating system that is optimised to) provide (one or more specialised) services to (network) clients;
A description of examples of services e.g. logging on, sharing printers, but just the example of accessing files is not enough as this is in the question. There needs to be additional explanation if files is used as an example, e.g. managing quotas, security of files.
R answers that imply that server does all processing i.e. confusion with thin client
- (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 server 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

- (ii) Longer range // faster transmission speeds // higher bandwidth // more simultaneous connections;
A reverse of points e.g. "Bluetooth only has a short range"
R Bluetooth can only connect two devices at once

1

(f) **SUBJECT MARKING POINT S:**

Internal:

- Student's computer uses subnet mask (and destination / web server's IP address) to determine if destination computer / web server is on same subnet // identify not on same subnet
- Up to two marks from description (in separate section below) of how subnet mask is used
- Packet is sent (from student's computer) to Router (1)
- Router 1 identifies that destination is outside the LAN so forwards packet to Gateway

External:

- Hierarchical organisation of routers
- Example of hierarchical organisation of routers e.g. passed up to a national router, transferred internationally and then passed back down a hierarchy
- Path to take selected by each router (not determined at start) **NE** passed from router to router
- Route may change as a result of e.g. congestion, technical problems

Either:

- (Possible) repackaging of packet to use different protocol (e.g. Gateway may change protocol)
- Route determined using the (Network ID part of the destination) IP address (Note: can infer "IP address" if just "address" is stated, if previously candidate has written about an IP address)
- Use of router tables / criteria to determine next hop / (step of) path
- Router decrementing "time to live" of packet
- Source and destination MAC addresses changed at each router // MAC addresses used for each "hop"

How subnet mask used (Max 2 points):

- AND operation of subnet mask with student's computer's IP address
- AND operation of subnet mask with web server's IP address
- Result (of AND operation) is the network ID;
- Network IDs compared
- If they are the same, then the computers are on the same subnet
A interchangeable use of subnet ID and network ID

HOW TO AWARD MARKS:

Mark Bands and Description

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and all 5 of the quality of language criteria (QLx).

- SUB** Candidate has covered both internal and external routing in detail and has made at least seven subject-related points.
- QWC1** Text is legible.
- QWC2** There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear.
- QWC3** The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
- QWC4** Sentences (and paragraphs) follow on from one another clearly and coherently.
- QWC5** Appropriate specialist vocabulary has been used.

7-8

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

- SUB** Candidate has covered both internal and external routing, although one may be in more detail than the other and has made at least five subject-related points.
- QWC1** Text is legible.
- QWC2** There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
- QWC3** The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
- QWC4** The candidate has used well-linked sentences (and paragraphs).
- QWC5** Appropriate specialist vocabulary has been used.

5-6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

- SUB** Candidate may not have covered both internal and external routing, but has covered at least one of them. Up to four relevant points have been made.
- QWC1** Most of the text is legible.
- QWC2** There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
- QWC3** The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
- QWC4** Sentences (and paragraphs) may not always be well-connected.
- QWC5** Specialist vocabulary has been used inappropriately or not at all.

1-4

Candidate has made no relevant points.

0

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question. If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 4 of the quality of language criteria are met in the lower band. If 4 criteria are not met then drop by two bands.

- (g) Any two points from the list below. Candidate only needs to make one side of point, the other can be implied. Do not award marks for two sides of same point.

Routeable	Non-Routeable
(Globally) unique	Many computers / devices may have same address
Allocated by a central / regional issuing authority (A example)	Not allocated centrally // allocated by a home user / company / ISP
Can be connected to directly <u>over the Internet / from outside private network</u>	Difficult / impossible to connect to <u>over Internet // from outside of network</u>
Owner can be looked up using WHOIS protocol	Owner cannot be looked up using WHOIS protocol

A non-routable IP addresses more secure as cannot be connected to over Internet / from outside network

A can identify location from a routable IP address

2

[18]

Q20.

- (a) WWW (**Max 3 marks**)
 A system of interlinked / hypertext documents;
 Accessed via the Internet;
 Using HTTP protocol;
NE web a collection of web pages

Internet (**Max 3 marks**)
 A network of interconnected computer networks;
A a network of computers;
 Using a globally unique address space;
 Using end-to-end communication protocol // Internet Protocol // "TCP / IP";

Supports a range of application protocols;
A two examples of different protocols;
R "TCP"
R "IP"

Max 4

- (b) Messages split into packets; **A** chunks
 Each packet given destination / source address;

Each packet dispatched to the Internet through a router / gateway;
Packets sent independently;
Packets given a sequence number;
Routers forward packets (until they reach destination);
Path of packet transfer determined by router(s);
Packets reassembled at the destination;

Max 2

(c) **12.23.45.89**

An IP (v4) address (that uniquely identifies a machine on the Internet) // Internet protocol address;

80

A port number // a number that specifies which process on the receiving machine/host to send the data to;
A port;

Denotes that HTTP (server) is recipient of packet // packet is an HTTP packet

2

[8]

Q21.

(a)

Manor School LibraryX
Our favourite genres are: • Science fiction • Suspense • Comedy <u>Discover our Top Ten Books</u>

'Manor School Library' – in title bar;

Line space after 'Our favourite genres are:' with the correct text AND line space after the bulleted list ;

Use of un-ordered list with three bulleted points with correct text;

Hyperlink identified through underlining or clear label with the correct text;

A minor spelling mistakes

Max 3: if any errors in drawing of page (for example font size differences or indenting hyperlink)

4

(b) (i) The text inside the <p> tags/ paragraph will be blue and use the Arial

font //

The text 'Our favourite genres are:' will be blue and use the Arial font;

Candidate needs to talk about text being blue

1

- (ii) #header{ font-size: 36pt; color: green; }

Max 2 if ; separator missing between 36pt and color

1 mark - #header {} // div {} // div#header{} ;

[Not contents]

1 mark – for color: green;

1 mark – for font-size: 36pt;

Note: color must be spelt without the u

For green accept #00xx00 where xx in range 01 to FF

3

[8]

Q22.

- (a) (i) To manage / control / execute commands on a remote machine;

A remote access / login

A a clear example of remote management

NE remote viewing

R remote desktop

1

- (ii) Enable files on one host / computer / client to be copied to another host / computer / server;

To manage files on a remote computer / server;

A to upload / download / transfer files

NE “sharing”

NE load a file

NE transfer data

1

- (iii) To retrieve / fetch (stored) email;

To check for new emails;

A access / download / receive

R sending

TO any mention of sending

NE just “email”

1

- (b) (i) 192.168.3.205 // 74.125.4.148 // 208.43.202.29;

1

- (ii) 80 // 25 // 58539 // 57458 // 57459;

I colons

1

- (iii) 192.168.3.205:80 //

192.168.3.205:25 //74.125.4.148:58539 //

208.43.202.29:57458 // 208.43.202.29:57459 ;

1

- (c) Servers might be in another room / site / cupboard / inaccessible ;
Servers might not have a keyboard / monitor installed ;

Can manage multiple servers from one machine;
 Servers can be managed outside of work hours / from anywhere;
 It would be quicker (**A** more convenient) (to manage from her machine than visit the servers) // better time management;
 Server rooms are often uncomfortable places for people to work in;
NE she does not need to go to the servers

Max 2

[8]

Q23.

- (a) (Using an algorithm) to convert a message into a form that is not understandable
 (without the key to decrypt it);
 (Using an algorithm) to convert a message into a form that is only understandable
 by the intended parties // can only be read with the correct key;
 Converting a message into cipher text;
NE scrambling unless further explanation is provided
A “unreadable” for “understandable”
A “data” for “a message”

Max 1

- (b) (i) B will not be able to decrypt it // A's private key would be needed to decrypt it // only A could decrypt it; (as ...)
 Only A has access to A's private key // B cannot access A's private key;

Max 1

- (ii) As A's public key is available to anyone;
 Anybody could decrypt it;

Max 1

- (c) **Subject-related points:**

Purpose:

To authenticate/confirm identity of sender // that message was sent by A // To detect if message has been tampered with/changed;

How used:

*¹ Hash / digest produced/calculated from message // (shortened) value calculated from message;

A message is hashed

A message digest created

*¹ Hash encrypted with A's private key;

*¹ Encrypted hash is known as the (digital) signature;

*² (Digital) signature is appended to message;

A transmitted with message

A even if stated or implied that this is done after the encryption of the message using B's public key

A hash or digest

A encrypts message and signature with B's public key;

A without reference to signature but **TO** if clear from order of statements or what candidate has written that the signature is not encrypted with B's public key

B decrypts message and signature with B's private key;

A without reference to signature

B decrypts (digital) signature using A's public key (to reveal hash);

B reproduces/recalculates hash from received message;

A re-hashed

A creates new digest

*³If received hash matches reproduced hash then message has not been tampered with // identity of sender is authenticated;

A Data for message

A Digest, checksum for hash

A Encrypted hash / Encrypted digest for signature

A Example of hashing method e.g. MD2/4/5/6, SH0/1/224/256/384/512

*¹ = as an alternative to these three points, allow one mark for the idea that the digital signature is calculated from/hashed from/a digest of the message

*² = only award this mark if there is previously the concept of the hash or signature being produced.

*³ = can only be awarded if there is clear concept that the comparison is to a recalculated hash

Only one mark should be awarded for the purpose. Other marks must come from how the digital signature is used.

The purpose mark could be implicit in the how used mark and should be awarded if it is.

It is acceptable for steps to be missed out.

Accept responses with message sent from B to A if it is clear that this is what the candidate has done.

How to award marks:

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and all 5 of the quality of language criteria (QWCX).

SUB	Candidate has covered both the purpose and the use of digital signatures, and has made at least five subject-related points including both creation and use. <u>To get 6 marks, the answer must include reference to the encryption of the message digest/hash using A's private key.</u>
QWC1	Text is legible
QWC2	There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear
QWC3	The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
QWC4	Sentences and (paragraphs) follow on from one another clearly and coherently.
QWC5	Appropriate specialist vocabulary has been used.

5–6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QWCx).

SUB	Candidate has provided a description of some parts of the process and has made at least three subject-related points.
QWC1	Text is legible.
QWC2	There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
QWC3	The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
QWC4	The candidate has used well-linked sentences (and paragraphs).
QWC5	Appropriate specialist vocabulary has been used.

3–4

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QWCx).

SUB	Only one or two relevant points have been made.
QWC1	Most of the text is legible.
QWC2	There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
QWC3	The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
QWC4	Sentences (and paragraphs) may not always be well– connected.
QWC5	Specialist vocabulary has been used inappropriately or not at all.

1–2

Candidate has made no relevant points.

0

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 4 of the quality of language criteria are met in the lower band. If 4 criteria are not met then drop by two bands.

[6]

Q24.

- (a) To examine the destination of each packet;
To forward packets from one network to another;
To manage congestion;
Choose an appropriate forwarding route;
Route packets according to destination IP address;
Store incoming packets temporarily;
Change link address in packet;
To store/make use of a routing table;
A data instead of packets
R information / signals

Max 2

- (b) SMTP;
POP(3);
IMAP(4);
A full names of the protocols above
A ESMTP // SMAP // LMTP // QMTP

Max 1

- (c) **Key Points of Subject Criteria**
Concept that data passed up/down between layers;
A by example – just one needed but must be correct
NE just describing the layers in the correct order

Application layer selects appropriate protocol for the communication // protocol mentioned by example (POP / HTTP);
Application layer is to interact with the user via the email client / web browser;

Transport Layer:

Transport layer establishes end to end communication // Transport layer establishes a virtual path // TCP layer establishes connection between client and server;
Destination and source application level client/server identified by port numbers;

TCP layer uses these port numbers to route reassembled requests/responses to correct application layer client/server;
 TCP layer splits and reassembles requests/responses into packets/from packets;
 Packets are numbered by transport layer;
 Transport layer deals with error control (acknowledgements/retransmission);

Network layer adds source and destination IP addresses; Routers use destination IP addresses to route packets to destination // network layer involved with packet routing;

Link layer adds source and destination hardware/Ethernet/Link layer/MAC addresses;
 Link layer destination and source addresses change from link to link;
 Link layer moves packets between 2 internet hosts;
 Link layer deals with physical connection/cabling;
A Link layer includes network card / drivers;

Network layer strips IP address (when receiving) // Link layer strips MAC address (when receiving);
 Server uses received source IP address to know where to send response;

Server uses received client port number to know to which instance of application layer client to send response to;
 Servers use well-known ports;
 Client port numbers come from the dynamic range;
 Packets of Email client/server and Web browser/Web server travel independent paths;
 Packets of Email client/server and Web browser/Web server share links//intermingled on links;

Combination of IP address and Port = Socket / described;

Note: Accept answers where candidate uses the IP addresses and ports indicated in the figure to match up with statements above

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QWCx).

- | | |
|------|--|
| SUB | Candidate has made at least 5 valid points covering. |
| QWC1 | Text is legible. |
| QWC2 | There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear. |
| QWC3 | The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently. |
| QWC4 | Sentences and paragraphs follow on from one another clearly and coherently. |
| QWC5 | Appropriate specialist vocabulary has been used. |

5-6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QWCx).

- | | |
|------|--|
| SUB | Candidate has made at least 3 valid points. |
| QWC1 | Text is legible. |
| QWC2 | There may be occasional errors of spelling, punctuation and grammar. Meaning is clear. |
| QWC3 | The candidate has, in the main, used a form and style of writing |

- appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
- QWC4 The candidate has used well-linked sentences and paragraphs.
- QWC5 Appropriate specialist vocabulary has been used.

3-4

To achieve a mark in this band, candidates must meet the subject criterion (SUB). The quality of language should be typified by the QWCx statements.

- SUB Candidate has provided at least one point from the above.
- QWC1 Most of the text is legible.
- QWC2 There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response..
- QWC3 The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
- QWC4 Sentences and paragraphs may not always be well-connected or bullet points may have been used.
- QWC5 Specialist vocabulary has been used inappropriately or not at all.

1-2

Candidate has not made reference to any of the points above.

0

[9]

Q25.

- (a) An ISP sells clients Internet access/connection; Provides users with access to Internet backbone;
R provides an Internet service

Max 1

- (b) Clients may have broken Copyright, Designs and Patents Act;
Digital Economy Act;
R Copyright, Copyright Act

Max 1

- (c) Data which relate to a living individual who can be identified from that data // data about a living identifiable person;

1

- (d) (i) ISP has (potentially) broken Data Protection Act (by not securing personal data);

1

- (ii) (Clients have potentially misused / hacked their ISP's computer system) therefore clients have broken the Computer Misuse Act;
R they may have broken the law

1

[5]

Q26.

(http means) Hypertext transfer protocol (will be used) // this is the protocol / set of rules (that will be used)

A "The protocol" as a BOD mark on this occasion but just the word "protocol" as NE.

R format

(www means) Resource/web page/web site/URL is part of the world wide web // on a web/virtual server;

NE world wide web on its own

(uk means) Country the site is registered in;

A organisation / company based in UK

NE site in the UK, country on its own

[3]

Q27.

- (a) (i) 192.168.0.x where x is not 0 or 255;

1

- (ii) 192.168.2.x where x is not 0 or 255;

1

- (b) 255.255.255.0;

1

- (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

- (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

- (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

- (e) Below are some example security threats and measures, but they are only examples. Award marks for all reasonable security threats and appropriate measures.

Threats:

Virus	Malicious self-replicating programs which attach to other programs
Spam	Unsolicited junk email
Worm	Malicious self-replicating programs which replicate across networks using security vulnerabilities
Remote Login	Ability to login to a computer via Internet A "hacking" if explained
Trojan	A malicious program hidden inside another program // masquerading as another program
Phishing	Attempts to get users to divulge personal information
Pharming	Misdirecting users to a fake website by changing DNS entries
Spyware	Program that collects information from a user's computer without user knowing
Denial of Service Attack	Repeated requests/pings from the Internet could overwhelm (parts of) the network.

Threats must be described not simply named.

Measures:

Use a secure operating system

Regularly install security patches/upgrades for software

Use virus checking software + some explanation of what this will do

Keep virus definitions up to date

Use anti-spyware software + some explanation of what this will do

Use of firewall to control traffic between private network and Internet // explanation of how firewall might work

Use of spam filter in email package

Enable web browser features to detect Pharming

Restrictions on which websites users can visit

White lists/black lists

Enforce strong passwords

Encryption of data during transmission

Authentication of user/computer attempting remote login using digital certificate//smart card//security code generating device

Log files
 Network manager keeps informed about latest threats // network manager
 trains users about threats

*Measures must be appropriate to security issues described.
 More than one measure can be used for the same threat.*

How to award marks:

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and all 5 of the quality of language criteria (QLx).

SUB	Candidate has described 2 security threats and 3 appropriate measures OR 3 security threats and 2 appropriate measures. To get 6 marks answer must include 3 threats and appropriate measures.
QL1	Text is legible
QL2	There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear.
QL3	The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
QL4	Sentences and paragraphs follow on from one another clearly and coherently.
QL5	Appropriate specialist vocabulary has been used.

5–6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB	Candidate has described at least 2 security threats and described 1 or more appropriate security measures OR candidate has named (but not described) some security threats and has described 3 or more security measures
QL1	Text is legible
QL2	There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
QL3	The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
QL4	The candidate has used well-linked sentences and paragraphs.
QL5	Appropriate specialist vocabulary has been used.

3–4

To achieve a mark in this band, candidates must meet the subject criterion (SUB). The quality of language should be typified by the QLx statements.

SUB	Candidate has described at least 1 security threat and may or may not have described some appropriate security measures OR candidate has named at least one security threat and has described 1 or 2 security measures.
QL1	Most of the text is legible.
QL2	There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
QL3	The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
QL4	Sentences and paragraphs may not always be well-connected or bullet points may have been used.
QL5	Specialist vocabulary has been used inappropriately or not at all.

1–2

Candidate has made no relevant points.

0

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 3 of the quality of language criteria are met in the lower band. If 3 criteria are not met then drop by two bands.

6

[13]

Q28.

- (a) Number of signal changes per second // rate at which signals can change; A voltage changes for signal changes as BOD

1

- (b) (i) Each signal level / signal change represents two bits (of data)/more than one bit (of data) // channel supports four / more than two different signal levels/voltages // use of modulation/coding technique e.g. phase modulation
NE Send more than one bit at a time

Must be clear that there are more than two signal levels

1

(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

- (c) Baseband – whole bandwidth of medium dedicated to one channel at a time // only one computer can send data at a time // sends signals with frequencies from 0Hz to a maximum highest frequency.

Suitable for LAN – lower cost electronic components (accept examples) // simpler hardware // good performance at low cost

NE cheaper

Broadband – bandwidth of medium shared so multiple channels can be carried simultaneously // many computers can send data simultaneously // frequency bands assigned to different communications. **TO** multiple wires
Suitable for WAN – expensive to install / maintain communications media over long distance // many more devices/people needs to communicate // more cost effective to share medium.

How to award marks:

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 5 of the 5 quality of language criteria (QLx).

SUB Candidate has described both baseband and broadband and has explained

	accurately why at least one of these is appropriate to the context.
QL1	Text is legible.
QL2	There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear.
QL3	The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
QL4	Sentences and paragraphs follow on from one another clearly and coherently.
QL5	Appropriate specialist vocabulary has been used.

3–4

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB	Candidate has described both broadband and baseband but may not have explained why they are suitable.
QL1	Text is legible
QL2	There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
QL3	The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
QL4	The candidate has used well-linked sentences and paragraphs.
QL5	Appropriate specialist vocabulary has been used.

2

To achieve a mark in this band, candidates must meet the subject criterion (SUB). The quality of language should be typified by the QLx statements.

SUB	Candidate has only described one of baseband or broadband.
QL1	Most of the text is legible.
QL2	There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
QL3	The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
QL4	Sentences and paragraphs may not always be well-connected or bullet points may have been used.
QL5	Specialist vocabulary has been used inappropriately or not at all.

1

Candidate has made no relevant points.

0

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 3 of the quality of language criteria are met in the lower band. If 3 criteria are not met then drop by two bands.

4

[9]

Q29.

- (a) Provides reliability of transmission // check transmission successful;
Error detection and correction // error handling
A either detection or correction;

Acknowledgement of received packets;
 Retransmission of packets if necessary;
 Flow control / congestion avoidance / congestion management;
 Packet sequencing;
 Adding TCP headers;
 Pass data to correct process in application layer;
 Allocates port numbers;
 Dividing data into packets / reassembles data from packets; **NE** "chunks", transports packets
 Connection establishment / maintenance;
 Creation of virtual circuits // creating an end-to-end connection;

Max 2

- (b) HTTP/ HTTPS/ SMTP/ POP3/ Telnet / SSH;
 The above are only the most common examples.
 Students may provide alternatives and these should be checked.

1

- (c) Network (layer);
A IP (layer)

1

[4]

Q30.

- (a) (aqa.org.uk) domain name;
R FQDN (courses / computing.html) path name // location of file / resource / object / document // path of file / resource / object / document;
NE file name

2

- (b) A set of (agreed) rules / codes / signals (for data exchange between systems);
 Agreed standard for communication between computer systems;

Max 1

- (c) Both use the same protocol;
 Both are client-server based;
 Both have a similar purpose // both used to share information / data / resources; **A** access
 Both use TCP / IP;
 Both are accessed through the use of a URL;
 Concept that web pages can be accessed through a web browser on either system // use of same software;

Max 2

- (d) Easier to remember a FQDN or converse for IP address i.e.
 IP addresses are less memorable;
 FQDN can identify (to a human) what a site is whereas an IP address cannot // easier to understand;

Max 1

[6]

Q31.

- (a) (i) Hypertext Transfer Protocol;
A Hypertext as two words

1

- (ii) HTTPS is secure;
 HTTPS (usually) uses port 443, HTTP (usually) uses port 80/Use different port numbers;
 HTTPS uses SSL/Secure Socket Layers;
 HTTPS is encrypted;
R encoded
 Servers using HTTPS must have a public key certificate;
 HTTPS allows authentication of client/users/machines//allows access to be restricted to certain clients/users/machines;
A Reverse of answers e.g. HTTP is not secure etc.

Max 1

- (iii) A description of any website which could reasonably require secure data transmission;
R URLs of specific websites
R Social networking sites
R Bank website **NE**
R online shopping without concept of transaction **NE**

1

- (b) Port that is temporarily assigned/only exists for duration of a connection;
 Port number automatically allocated // assigned from the client's TCP/IP stack;
A Port number 1024 – 4095

Max 1

- (c) Communication initiated by clients;
 Clients must know which port number to connect to // (Server) port number must be known by client (before communication with server starts) // So client can select service;
 Particular port numbers are used to provide a particular service
 // **A** Example of specific well known port number with its use;

Max 2

[5]

Q32.

- (a) The protocol // This resource uses file transfer protocol;

1

- (b) Address of (ftp) server // Fully Qualified Domain Name;
A FQDN
R Domain name

1

- (c) Pathname/location of file/page/resource // Description of file structure;
R Filename

1

[3]

Q33.

- (a)

	URL	Domain Name	IP Address	Protocol

(i) http://www.guineas.co.uk	✓			
(ii) 212.58.251.195			✓	
(iii) guineas.co.uk		✓		

1 mark for each correctly placed tick

R Answers with more than one tick on a row.

3

- (b) To translate/convert/resolve domain names into IP addresses;
A FQDN for domain name
 Answer must have the CONCEPT of an action
NE To store the domain names and IP Addresses
NE To access the web page without knowing the IP address
NE To link the domain name to the IP address

1

[4]

Q34.

- (a) **Similarity:**
 Use same protocols
A example eg. TCP/IP HTTP;
 Similar facilities available
A example e.g. email, web site;
 Use of same software to access information
A example e.g. web browser.
 Similar purpose – sharing information, improved communication;
 Both client/server systems;
NE Both use protocols
NE Both are networks

1

Difference:

Internet publicly available vs intranet only accessible within company/by employees / private;
 Internet use of public telecommunications network vs intranet may use private network;
 Intranet more secure than the Internet;
R Need password for intranet
R Global vs Local

Must state both sides of difference

Must be clear that difference is stated the correct way round

1

- (b) (i) Set of rules / agreed codes;
 Agreed standard for communication between computer systems;

1

(ii)

Layer	Function
-------	----------

Application	Gives applications access to the network; A Examples of applications
Transport/TCP	Provides reliability of transmission / check transmission successful; Error detection and correction / error handling A either detection or correction Acknowledgement of received packets; Retransmission of packets if required; Flow control / Congestion avoidance / congestion management; Packet sequencing; Adding TCP headers; Pass data to correct process in application layer; Allocation of port numbers; Divided data into packets / reassembling data from packets; Connection establishment / maintenance; Creation of virtual circuits;
Network/Internet/IP	Routing; Adds addressing info; Adds source and destination <u>IP</u> addresses;
Link/ Data Link/ Physical	Physical interface with medium/cable; Mapping of IP to MAC addresses; A Hardware address Conversion of IP datagrams to network frames; Adds Ethernet / MAC addresses; Adds header / trailer;

1 mark for each correct layer name

1 mark for each correct function associated with the correct layer

EXAM PAPERS PRACTICE

4

[7]

Q35.

- (a) (i) the protocol used
// this is the hypertext transfer protocol;
- (ii) address of Aqa's World Wide Web server;
R domain name
- (iii) the path / location of the file / resource;
OR description of folder structure;

1

1

1

[3]

Examiner reports

Q1.

Just over half of students correctly explained that symmetric encryption used one key for both encryption and decryption whereas asymmetric used different keys for each process. Some responses lost marks through lack of clarity, for example by stating that asymmetric used two different keys without indicating that one was used for encryption and the other for decryption. A small number of students confused the topic with asynchronous and synchronous communication.

Q2.

This question required students to write an extended response that covered a number of different areas of the specification. Responses often covered the aspects of how the owners could have protected their networks and what legal and ethical issues might have arisen well but neglected the aspect of how it was possible for the data to be collected and were not specific enough with regard to how the company's practices might have changed as a result of the incident.

With regard to how the data was collected, examiners were looking for students to recognise that WiFi signals could travel over a wide area and that any WiFi receiver in range could read the data from these packets. Few students made these points, but a reasonable number identified that the data may not have been encrypted or that an outdated encryption protocol such as WEP might have been used.

Good responses recognised that an appropriate measure to prevent the data from being collected would have included encrypting the data using a protocol such as WPA2. In the question's context, measures such as enforcing a MAC address whitelist or using a firewall were not appropriate as the cars were simply collecting information that was being transmitted; they were not trying to connect to the wireless access points. Some students referred to adding a password to the network which was not a strong enough point to be mark worthy; they failed to identify that the "password" they were referring to would actually be used to make a key for an encryption system.

Students are not required to have knowledge of specific legislation for this specification, but should have an understanding of issues around areas of ethical and legal concern such as privacy, data protection, copyright and hacking. Nevertheless, mention of specific relevant legislation was considered mark worthy. Relatively few students took the opportunity to really discuss the legal and ethical issues. For example: given that the data was being transmitted freely through the air, would accessing it really count as hacking, given that the functionality involved was added by a small number of developers, were they or the company responsible for it, would the nature of any offences committed depend upon the type of data collected, did it matter if the data collection was intentional or accidental? Students should be encouraged to consider this sort of reflection when answering this type of question.

Most students recognised that the company needed to have better oversight of the development process but many made general statements about this and did not suggest specific measures that might be taken to improve their practices, such as introducing third-party review of code or improved training of developers on legal and ethical issues. Points relating to testing were not considered mark worthy unless it was explicitly stated that the testing would be focussed on ensuring that the software had no additional functionality or that the data collected by the cars was all relevant to the intended purpose of the system.

Some students appeared to have completely misunderstood the scenario and wrote at considerable length about the rights and wrongs of companies using cars to take photographs in public places rather than about interception of WiFi signals. Students need to ensure that they are answering the question asked rather than a question that they might have prepared for.

Q8.

Students appear to be developing further their understanding of networking. It was pleasing to see well written responses for part (b) where students could clearly describe why HTTP requests need to be accepted by a firewall and Telnet request denied. Linking HTTP to a need to be able to browse websites was a commonly seen answer. Those students who linked HTTP to being able to browse the Internet did not secure the mark. Telnet appears to be a less known protocol to students but answers discussing the potential problems of allowing remote control of computers inside the school were seen.

Part (c) was answered well and the majority of students secured 3 or more marks. Strong answers clearly described the client-server model and then explained the process of applying the security patch to the company server. A group of students went off in a slightly wrong direction by talking about downloading the security update from a website rather than a FTP server. A few students, who perhaps did not fully understand the question, responded by just talking about the TCP/IP layers and what they are used for. Students who secured high marks could clearly describe the use of an FTP client to connect to the FTP server to allow the update to be downloaded. They then appreciated the need to Telnet across to the company server, login and then apply the update. It was possible to secure full marks for the question by either downloading the update to David's laptop and then uploading to the company server or by remotely connecting to the company server and then downloading the update directly to that server.

Q9.

This question was about various aspects of computer security.

Part (a) was very well answered with the vast majority of candidates correctly identifying that a web server log was a method of accounting and a digital signature was a form of authentication.

In part (b), most candidates were able to demonstrate a good understanding of computer viruses, explaining that they were malicious, self-replicating programs that attached themselves to other programs. Understanding of worms was less good, with many candidates failing to recognise that the key feature of a worm is that it distributes itself over a network by exploiting security weaknesses. Many candidates confused worms with Trojans or believed that the distinction between a worm and virus related to the actions that they might take on an infected computer rather than their method of spread.

The use of digital signatures, covered in part (c) has been asked about before, and was fairly well understood. Many full mark responses were seen. Even candidates who did not achieve many marks mentioned key terms, suggesting that they had some degree of understanding. Some candidates went on to explain parts of the process that were not asked about on this paper, such as how the entire message might be encrypted or how the digital signature would be authenticated by the recipient. It is important that candidates read the question being asked so that they do not waste time writing material that cannot achieve marks.

Q13.

The first part of this question looked at identifying protocols in a different way and it was

pleasing to see that students could identify a protocol from a screenshot of it being used. Most students spotted that the first one was linked to email and answered with either POP3, SMTP or just email. As the information provided gave details of an email being prepared and sent the actual protocol was SMTP.

The second screenshot proved to be a little bit harder but it was still pleasing to see that a group of students spotted it as either Telnet or SSH. The answer of 'remote login' was not awarded a mark but did show some understanding.

Part (b) proved harder than expected with less than half of students securing the mark. The acronym URL was probably known by the majority of students but it was clear that not many could actually provide the answer uniform resource locator.

It was pleasing to see that students could provide reasons for why traceroute might show different hops. Good answers included the idea that links might be busy or down for some reasons or considered the actual role of the router in deciding which route to send individual packets. The idea that 'a different route was taken' was deemed as not enough in trying to explain why.

Part (f) allowed students to explain the role of the router and those that read the question carefully tended to answer well. It was also clear that some students just quoted the roles of each layer without thinking in terms of an actual router.

Q14.

This question was about networking.

For part (a) students had to identify an appropriate IP address. This was satisfactorily tackled with just under two thirds of students achieving the mark. Common mistakes were to give an IP address that started with the same three octets as the IP address assigned to Port Y of the router instead of Port X, to use 0 as the last octet and to give a three-octet IP address.

Over three quarters of students correctly identified the physical topology as being a star in part (b).

The most frequently seen correct response to part (c) related to the increased security offered by the use of non-routable IP addresses. Other good responses related to the limited number of routable IP addresses available using IPv4, and the difficulty of allocating these to devices. Over half of students achieved one mark, but few went on to achieve both the available marks.

For part (d) students had to explain how the subnet mask was used. Explanations were poor and only a quarter of students achieved any marks at all. Good responses explained that the subnet mask was logically ANDed with the destination IP address to produce the subnet ID of the destination. The same process was repeated with the source IP address and subnet mask to produce the subnet ID of the source. These two subnet IDs were then compared and if they were different (as was the case in the example) then the data would have to be sent to the router instead of directly to the destination. Common misconceptions were that the data was passed around the network until it found a computer where it matched the subnet ID, that the subnet mask was capable of doing things itself, and that the mask was a form of security.

For part (e) students had to describe how a firewall worked. Many responses were superficial, referring only to the data being checked, without explaining against what criteria; just over half of students achieved at least one mark, but very few achieved more than this. Appropriate methods that might be used included using an IP address blacklist,

blocking specific ports, inspecting the contents of packets and stateful inspection. Some students erroneously believed that a firewall could perform essentially the same function as virus checking software.

Part (f) was about the difference between baseband and broadband. Just under half of students achieved this mark, and the most common mark worthy response explained that baseband carried one channel over the whole bandwidth of a medium whereas broadband divided the bandwidth up into a number of channels. There was some confusion with parallel and serial transmission and a small number of students, though fewer than when this topic was previously asked about, responded that broadband was faster.

Part (g) was well answered with three quarters of students achieving a mark. The most commonly cited reason was the faster speed of transmission when using a cable or increased reliability, both of which were relevant to streaming television pictures.

Q15.

- (a) This part was based around a given URL and asked candidates to identify parts of this URL and then to state the top-level domain. Questions have been asked previously about breaking down a URL into parts and candidates generally made a good attempt at answering this. It should be noted that the question asked candidates to 'describe' and this would generally mean that an answer should be formed into a sentence rather than just one or two words. The protocol section is understood by a lot of candidates but the FQDN (fully qualified domain name) does seem to cause problems. The distinction between a domain name and a fully qualified domain name does appear to be an area of weakness at the moment.
- (b) This part asked questions around the Domain Name System (DNS) and it is clear that a certain group of candidates have a good understanding of what DNS is and how it works whilst others have no awareness of this topic. This is an area that would hopefully be taught with students actually performing name lookup queries and considering how domains are registered and settings propagated around the Internet. Candidates with an awareness of this topic could explain that the DNS server would respond to a domain name query with the IP address currently allocated to that domain name. They could then also identify a situation when a DNS query would not need to be sent. It was pleasing to see an understanding of DNS results being cached on a local computer and even seeing some candidates talking about a hosts file. It was also common to see answers such as moving to another page on the website or another page / resource on the same domain. A few candidates seem to think that the DNS server holds the actual web pages and returns those to the client or that it is the DNS server that then connects you to a website. It was decided that a resource being on an intranet was not an acceptable answer on its own for part (ii) as some kind of DNS query might need to be sent or what the candidate was trying to express was covered elsewhere in the mark scheme. We also decided that IP was not enough for IP address for part this part of the question. Candidates that answered that a DNS sever returns an IP or that you would not need to send a DNS query if you entered an IP did therefore not secure marks.
- (c) This part was based around HTTP GET requests and it was pleasing to see that a group of candidates could clearly apply their understanding to these question parts.
 - (i) This part was answered correctly by the majority of candidates and it was clear that it was understood that a browser would be operating in the application layer.

- (ii) Weaker candidates could not supply the correct name of any of the TCP / IP layers. It was pleasing to see that candidates understood that an initial HTTP GET request could just return a HTML file and when processed this might need more HTTP GET requests to retrieve necessary resources such as images, javascript and CSS files to display a web page.
- (iii) This part proved hard for candidates to secure a mark and a lot just described a port number and not a client port number therefore not describing what made it a client one. It was pleasing to see the correct answer of a temporary port number being supplied for the duration of a connection being supplied by a few candidates. There does seem to be some confusion around client port numbers with candidates indicating that it can identify a machine on a local network or that the server actually supplies the number to the client.

Q16.

This question was concerned with the registering of a domain name and the setting up of a server to provide web pages. Most students used the provided terms to structure their answers and it was pleasing to see the understanding that they had with regard to this process.

Weaker answers stated what each of the terms meant rather than linking it into the process of registering and creating a website on a server. It was clear that some students had experience of performing these tasks themselves as their answers described the steps with a good amount of detail. The majority of students understood that the domain name would need to be registered but there was confusion over the setting up of DNS records. The setting up of software / services on a server is clearly something that students do not particularly understand. Giving students access to a server, or a device such as a Raspberry Pi, so that they can install software and turn services on and off would provide an ideal experience for students to answer questions of this type. It was pleasing to see students provide the correct port numbers for appropriate services and to notice that the server would need to have both FTP and web server software installed. A few students even correctly identified the packages that could be used by mentioning Apache and Filezilla, with a clear understanding of the distinction between server and client software.

Q17.

The majority of students correctly identified that the first part of this question concerned the Data Protection Act. Students did struggle, however, to identify the principle required for part (b) and then to name another for part (c). It was common to see statements about certain activities for protecting data rather than stating actual principles. Part (b) was looking for the idea of data security and some students correctly identified the difference between internal and external security. The common answers for part (c) included keeping data up to date and not keeping data longer than necessary.

The majority of students correctly identified that HTTPS would be the preferred protocol for transmitting this data and over 60% secured the second mark for this question part with the common answer of HTTP not being a secure protocol. There appears some confusion over what HTTPS actually is and answers such as 'the website could be hacked' or 'the website is not secure' did not gain marks. At this level we would encourage students to appreciate that HTTPS is a protocol involving the encryption of data transmitted between two devices for the purpose of making the transmission secure but the protocol doesn't imply that all of the data on a website is actually secure.

Part (e) was answered well by students with the majority scoring 2 or 3 marks. Mistakes included identifying the web server software as either an operating system or a utility

program. It seems possible that students do not have experience of servers and how they operate.

Q18.

The HTML / CSS question proved to be easier than last year when the format was slightly different. It was pleasing to see how many students could provide correct answers to question part (a) but it is to be noted that it was not as high as expected with only 60% providing 'hypertext mark-up language' for part (a)(i).

Part (b) proved to be a good discriminating question with students gaining the whole range of marks. The majority of students secured 3 or 4 marks out of the 6. Common mistakes included students not understanding the difference between an ordered and un-ordered list or just providing `<p>` and `<p>` for the list section. The marks had to be syntactically correct to be awarded. For example, `#toptitle` was not the correct answer for missing item 5 because the `#` is omitted from id selectors when the tag is referenced in the body section of the HTML.

Q19.

Part (a) was well answered, with the majority of candidates achieving all three marks. Common mistakes were to give IP addresses made up of three octets instead of two, to give a value of zero for the Host ID or to include a port number in an IP address.

For part (b), the overwhelming majority of candidates recognised that this was a bus topology.

For part (c), candidates who knew the correct format of a subnet mask almost always got the right answer but quite a lot of candidates appeared not to know what a subnet mask was at all.

Part (d) was poorly answered, with only about a third of candidates achieving the mark. Many candidates confused a Server Operating System with either a Network Operating System or a Thin Client System. Candidates needed to recognise that a Server Operating System was optimised to allow the server to efficiently deliver services to clients on the network. Well explained examples were also creditworthy, but the example of just loading files was not sufficient as this was given in the question.

A good awareness was shown in part (e)(i) of how to maintain the security of a WiFi network. Answers such as the use of WEP / WAP, disabling the broadcast of the SSID and the use of a MAC whitelist were common. A more problematic answer, offered by many candidates, was the use of a password to connect to the network. This answer was credited if the examiner understood that the "password" was in fact a passphrase entered to encrypt the data on the WEP / WAP connection, but it was not credited if the answer could be interpreted as a logon system. Candidates need to be aware that the passphrase entered is not a password checked against a database of valid passwords but instead, it is used to calculate the encryption keys that will be used for data transmission. Candidates also need to be aware of the meaning of important keywords in a question such as "describe". A single word or very brief response is unlikely to be creditworthy if a question has asked for a description of something.

Part (e)(ii) was very well answered, with the most popular answer relating to the relative ranges of WiFi and the most common implementation of Bluetooth class. The most common misconception was that only two Bluetooth devices could connect together at once.

Part (f) asked about routing a packet of data from a computer on a LAN to a web server

across the Internet. Candidates were expected to explain how the packet would be routed both internally on the LAN and externally on the Internet. Almost all of the mark scheme points were made by some candidates, but very few candidates individually made enough of them. Generally, the routing of packets externally on the Internet was dealt with more successfully than routing on the LAN.

Very few candidates explained how the subnet mask would have been used by the student's computer to identify that the destination web server was not on the same segment as it was, and therefore the packet would first be sent to Router 1. Pleasingly, most candidates recognised that the packet would then be sent on to the gateway but many did not achieve the mark for this point because they failed to explain that this was done because the destination computer was outside of the LAN.

External routing was generally better covered, with candidates explaining how the destination IP address would be used to pass the packet between routers in a hierarchical fashion. A small number of candidates recognised that routing decisions were made by each router (using a routing table) and also explained the distinction between how the IP addresses and MAC addresses would be used.

Common mistakes were to explain about the use of the TCP / IP stack or how packets were formed or to discuss the use of CSMA / CD. These points were not usually wrong, but did not address the question.

For part (g), approximately half of the candidates achieved at least one mark comparing routable and non-routable IP addresses, but few achieved both. Good responses referred to uniqueness, who would issue the IP addresses and whether or not they could be directly reached across the Internet.

Some candidates stated that it was not possible to connect directly to a non-routable IP address. This was not creditworthy as it is possible to connect directly to such an address if you are on the same network. Candidates needed to make clear that they meant "across the Internet" to achieve the mark. Other common mistakes were to give opposing sides of the same point and to confuse the comparison between routable and non-routable IP addresses with comparing static and dynamic IP addresses.

Q20.

Describing the differences between the WWW and the Internet demonstrated that there are still some students who do not understand the role of the Internet. It was common to see the idea that the WWW was the main focus rather than being an application that uses the connections provided by the Internet. Students who scored full marks provided a good description of the Internet and the WWW and highlighted factors such as the protocols used.

Part (b) allowed students to mention that a message is split into packets and this is how many secured at least one mark. It was clear that students have a better understanding of routing but that this is still an area that could be improved.

The majority of students secured both marks in part (c). Students were not awarded a mark for just stating 'IP' and it was necessary to write at least 'IP address' to secure the mark.

Q21.

Part (a) was answered well by students. Weaker students did not show the spacing that would be present between the block tags. Other students either numbered the list or did not place any bullet points on them and lost the ability to secure one of the marks.

Students do need to be encouraged to produce neat diagrams and the labelling of blank spaces and hyperlinks makes the awarding of marks a lot easier.

Describing the effect of the style rule in part (b)(i) had most students realising that the font would be changed to Arial and the text colour blue, but some forgot to link this either to the text on the web page or the <p> tag so it was not clear which text would be affected.

The majority of students could correctly write 'color:green' for part (b)(ii) but to then add in the other required elements was a slightly harder challenge. Not many students appeared to know the syntax for an ID selector. It was also surprising to see a few students drop marks by writing 'color:blue' which demonstrates a poor reading of the question.

Q22.

Part (a) of the question started by asking students to identify a use of a collection of protocols. The majority of students could correctly identify a use for FTP and it was obvious that this was a well known protocol. Students, however, struggled with both Telnet and POP3. Whilst the majority of students knew that POP3 was concerned with e-mail, this was not considered to be creditworthy as students should be aware of the difference between POP3 and SMTP. Students who did identify that POP3 was concerned with retrieving e-mail from a server were rewarded with the mark. It would be beneficial for students to have access to working with these common protocols so that they can gain a feel of their use.

The first few parts of (b) were answered well by students. Most secured the mark for IP address and port, but providing a socket came out as the hardest of the three parts. The most common incorrect answer for port was 37 with students picking this out from a different column of the figure. In a similar fashion, it was common to see a variety of items taken only from the figure as a guess at socket.

The last part of question was answered well with the majority of students gaining at least one mark. A wide variety of answers were seen across the marking period. Popular answers included the servers being off-site and the point that it would save time being able to access the servers from a desktop rather than travelling to them. Students who realized that the servers might be able to be managed from anywhere with an Internet connection were also awarded a mark.

Q23.

Part (a): This question part asked for a definition of encryption (using an algorithm and a key to convert message data into a form that is not understandable without the key to decrypt it). Approximately three quarters of students were able to provide a suitable definition.

Part (b)(i): This question part was well answered, with most students recognising that B would not have A's private key so could not decrypt the message. Some students did not understand the asymmetric nature of the process and so wrote responses that assumed that if A's public key was used to encrypt the data, the same key would need to be used to decrypt it.

Part (b)(ii): This question part was far less well answered than part (b)(i). The correct answer was that this would be insecure as A's public key, which would be used for decryption, is available to anyone. As in the previous part, some students lost marks because they did not recognise the asymmetric nature of the encryption. The response that, "anyone with A's public key could decrypt the message" was not considered to be enough for the mark as it did not make clear that everyone could get this key.

Part (c): This question part required students to explain the purpose of a digital signature and how digital signatures are used. Approximately three quarters of students were able to explain the purpose. More disappointingly, less than half were able to describe how digital signatures were used. Nevertheless, students who knew the topic provided excellent, detailed explanations. The most commonly made mistakes were: to be confused between the hash and the digital signature; to believe that the digital signature was attached to the end of the original message after the original message was encrypted rather than before; and to provide an unclear description of how the hash would be regenerated at the receiver and compared to the transmitted hash. Some students confused a digital signature with a digital certificate. The quality of written communication of almost all responses was satisfactory.

Q24.

When describing the role of a router it was common for weaker students simply to point out that it, 'routes information,' and, 'passes information from the client to the server.' Answers tended to be vague perhaps indicating that this is currently an area of subject matter that is not particularly well known. Students who identified that a router forwards packets from one network to another and who stated that it inspected the destination IP address were awarded the marks.

It was pleasing to see that the majority of students could name a protocol associated with e-mail. Incorrect answers included Telnet, FTP and HTTP but the majority correctly answered with SMTP or POP.

When describing the TCP/IP stack it was clear that the stronger students could place a few points into each of the layers and they were rewarded with high marks. It was common for weaker students to mix points up between layers or to fail to provide enough information.

Q25.

Whilst most students provided answers for part (a), it was quite common to see the stem of the question simply repeated. The answer, 'an ISP provides an Internet service,' was not enough to secure a mark. Students secured the mark by describing how an ISP supplies a connection or access to the Internet to their clients.

It is usual for question papers to now ask students to state the full name of a law and a few students lost marks in question by not following this instruction.

The answer of simply, 'copyright,' is not enough to secure a mark and this led to around half of all students securing a mark for part (b).

The term 'personal data' has appeared on past papers and it is still evident that students struggle to define this well enough to secure the mark. We are looking for personal data from which it is possible to identify a living individual.

Question part (d) asked students to identify two further laws and the majority of students secured both marks. More students secured the mark for identifying the Data Protection Act over the Computer Misuse Act. Occasionally students answered with 'Data Misuse Act' or 'Computer Protection Act' which perhaps identifies that they have heard about the laws but are not able to state the names correctly.

Q26.

In this question candidates were asked to identify parts of a URL; questions of this type have been asked on similar papers in the past. Most candidates secured one mark by

identifying that the http part refers to the protocol being used. Candidates who simply answered, 'protocol,' were not awarded the mark as the question did ask them to explain what each part meant.

Understanding that the www part of a URL refers to the name of a machine (virtual or otherwise) that is being accessed was not so well known. Good candidates realized that this machine would be on the World Wide Web and answered accordingly. Candidates who simply stated that www stands for World Wide Web did not secure a mark. Some candidates tried to define the World Wide Web, rather than answering the question itself which referred to a URL. Candidates continue to think that the 'uk' refers to sites being hosted or based in the UK. This isn't necessarily true, a website could be hosted anywhere in the world and still use 'uk'. The 'uk' indicates that the domain has been registered in the UK.

Q27.

Part (a)(i), ii: Approximately two-thirds of candidates responded with an appropriate IP address for each of these question parts. However, as in 2010, a small but significant minority of candidates gave answers that could not possibly be IP addresses.

Part (b): The correct subnet mask was 255.255.255.0. Approximately half of the candidates identified that this was the case.

Part (c): Answers to this question part covered a range of issues: security, reliability and throughput. The most common correct response explained that there would be a reduction in the number of collisions. Candidates needed to ensure that their explanations were sufficiently detailed to achieve both marks.

Part (d)(i): This topic was reasonably well understood, with candidates explaining that cabling costs would be lower as a single cable would run around the entire network. A small but surprising number of candidates believed that a bus network would be faster because only one cable was involved.

Part (d)(ii): There were many good responses, covering issues relating to reliability, security and speed. The most common error was to state that a star topology was more reliable because the failure of a single computer would not affect the others. Rather, it is the limited effect of the failure of a single cable that would improve reliability.

Part (e): Most candidates managed to write lengthy responses to this question part. The quality of these answers was quite variable, with some candidates demonstrating an extensive understanding of network security when connected to the Internet whilst other responses were quite superficial. When answering this type of question candidates need to make sure that they address the entire question. Some candidates lost marks by focussing only on the security measures that the network manager could put in place, either ignoring or only briefly mentioning the threats to which these would be responses. To achieve marks, candidates needed to describe the threats and measures, not simply name them.

Q28.

Part (a): The baud rate is the number of signal changes per second that can be supported by a transmission medium. Approximately half of the candidates stated this correctly, but some defined the bit rate instead.

Part (b)(i): The bit rate can be higher than the baud rate if more than two different signal levels are supported so that more than one bit can be encoded in each signal change. This was recognised by some, but not many, candidates. A commonly held misconception was that the bit rate could be higher than the baud rate if the data being transmitted

contained consecutive bits of the same value – for example, transmitting three 1s followed by a single 0 would only need one signal change.

Part (b)(ii): This question part was well answered, with the vast majority of candidates getting two of the three marks. Most candidates correctly explained the first two missing steps but got the last one wrong. The final stage in the handshake should have been that the printer indicates it is again ready to receive. Many candidates mistakenly believed that the printer indicated that the data had been received or was being printed instead.

Part (c): Candidates showed only a limited understanding of baseband and broadband, with just over a third scoring and marks. Many clearly had little idea what the terms meant and were just guessing based on their general knowledge of “broadband” and knowing what the terms LAN and WAN mean. Those that did achieve some marks often made quite superficial points, usually about the number of communication channels, rather than demonstrating a sound technical understanding of how the two systems differed in their method of operation.

Q29.

Part (a) was answered poorly by the majority of candidates. The role of the transport layer does not seem to be understood to the depth required with candidates producing vague responses. Many candidates used only the diagram to state that the transport layers pass data to and from the other layers which was not enough to gain credit. Some candidates were also confused about the role of each layer, with many stating that IP addresses or MAC addresses were added by the transport layer, when these are functions of other layers. The majority of candidates who secured marks described data being split into packets and the idea of packet sequencing. Better candidates were also aware of the transport layer assigning port numbers.

Part (b) was well answered by the majority of candidates. Common answers were HTTP, HTTPS, Telnet and SMTP. A few candidates identified applications; for example e-mail, rather than protocols, and therefore did not secure the mark.

Part (c) divided the candidates. Many incorrectly stated that a router operated in the link layer. To actually route a packet the router needs to look at IP addresses and therefore operates in the network layer.

Q30.

Although this question has been asked before, candidates struggled to secure full marks for part (a).

Often candidates answered with one or two words, rather than using a full sentence which the question required since it asked for a description. The majority of candidates correctly identified the domain name, but a few still confused this with a Fully Qualified Domain Name (FQDN). Instead of describing the second part it was common to see a candidate state only ‘path’ and therefore not secure the mark. Candidates should be encouraged to use full sentences when the question asks for a description.

Part (b) was answered well by the majority of candidates. A few candidates stated only ‘a rule’, but this was not accepted. It is pleasing to see more candidates use a fuller answer including the communication aspect.

The majority of candidates scored 1 mark for part (c) with only a few securing the second mark. The idea that both an intranet and the Internet use the same protocols is well known, but a few candidates did not secure the mark with an answer stating only that “they both use protocols”. A number of candidates stated only that they were networks or connected computers, but this was not creditworthy.

The majority of candidates secured the mark for part (d) by stating that a FQDN is easier to remember. A few candidates talked themselves out by describing a FQDN as also containing the IP address.

Some candidates responded that using a FQDN was faster when this is not true as the client will need to search for the IP address using DNS. A few candidates also wrote about using a FQDN as being more secure than using an IP address, but this was also not creditworthy.

Q31.

This question concerned the HTTP and HTTPS protocols and for the first time included questions about the use of ports. The former parts were answered very well with the question about the difference between HTTP and HTTPS being especially well described. However, the same cannot be said about the other two parts of the question on ports, which is a new topic. These were answered very poorly with only a very few candidates gaining full marks. The answers given were often vague and, on the whole, this showed that this part of the specification was not at all well known.

Q32.

The question asked candidates to describe the three labelled parts of a URL. Surprisingly this was also not very well answered – at least in terms of candidates gaining full marks. The idea of a protocol and the file and pathname were usually well known but the middle part was seen to be correct. Answers to part C often failed to gain a mark because the candidates gave either the file or the path, but not both parts of the expected answer and so did not gain credit for half an answer.

Q33.

Part (a) was very successfully answered. The vast majority of candidates could distinguish between an IP address, Domain Name and URL and gained full marks. Only a handful of candidates failed to score any marks.

For part (b) many candidates had some idea what a Domain Name Server (DNS) did but often described this poorly. The majority simply stated that it stored the appropriate URL and IP address combinations and left it at that, they did not go on to mention its active role in translating the URL into an IP address. Common incorrect answers were of the form that the Domain Name is easier to remember than an IP address. There was also a lot of confusion about the DNS being the preferred way of ensuring all web servers etc. had a unique URL so servers would be able to find requested sites i.e. candidates were describing Domain Name Registration services.

Q34.

This question was poorly answered. Many candidates simply stated that the Internet and an intranet were both networks, which was not enough to gain credit. Valid similarities included the use of common protocols and provision of access to similar services. A mistaken belief, widely held, was that an intranet would only be available on a LAN or within a small area. Candidates may form this opinion based on their own practical experiences of a college intranet, but large companies have global intranets that can be accessed worldwide. Many candidates lost marks by only stating one side of a difference, such as that an intranet was private, without making clear that they understood that in contrast the Internet was publicly accessible.

Most candidates were able to give a definition of a protocol or to describe one in sufficient detail to be worthy of credit. Some gave examples of protocols, which by themselves were

not creditworthy.

There were a lot of very good responses to the question about the TCP / IP protocol stack. Many candidates were able to name two stack layers and to give examples of layer functions. The most common errors were to name the Transport layer as the Transfer layer and the Data Link layer as the Data layer.

Q35.

Although not a new topic, candidates continue to have difficulty understanding what the different parts of a Uniform Resource Locator represent. `http://` tells the browser which protocol to use; www.aqa.org.uk is the address of AQA's World Wide Web server; `/ qual / gce / computing_new.php` is the file path of the resource.

