01.1 Explain **two** differences between a LAN and a WAN

[4 marks]

One mark per explanation point, such as:

- A WAN is a Wide Area Network that links more than one remote geographical site/location to another;
- A LAN is a Local Area Network that links together devices that are within one site\location;
- The speed of data transmission across a LAN is likely to be higher than across a WAN;
- WANs are typically public networks (and so data encryption is likely to be used);
- LANs (may not need data encryption) as they are typically private;
- LANs typically carry less traffic than WANs; This is because the number of users on a LAN can be controlled by the administrator whereas public WANs could have an unlimited number of users;
- LAN Connections are generally more reliable as they are under the control and maintenance of the network administrators;
- On a WAN it is possible that heavy traffic, peak usage times, viruses, weather or physical damage could affect the connection reliability;
- WANs are typically under shared ownership;
- LANs are typically owned by a single person or organisation;

01.2 State two examples where a PAN might be used.

[2 marks]

Any valid example, uch as bluetooth speaker or headphones (1 mark only for both), game controller, to transfer files, connect devices to play games, connect phone to car audio system, mouse/keyboard/trackpad/printer etc… (1 max)

02.1 Explain the purpose of the Internet Protocol (IP)

[2 marks]

Any two of: Relays data across network boundaries / defines how to address and route each packet / to make sure it reaches the right destination.

02.2 Explain the purpose of the SMTP and IMAP protocols.

[2 marks]

One mark for each:

IMAP – used by e-mail software to retrieve e-mail messages from a mail server. Allows the manipulation of messages – deleting messages, storing them in folders etc... – on the mail server.

SMTP – enables users to send (and receive) email messages. Allows e-mail messages to be sent between servers, allowing messages to be sent to someone using a different mail server

02.3 Place the HTTP, FTP and TCP protocols in their correct layer of the TCP/IP stack

[3 marks]

Layer	**Protocol(s)**
Application layer	HTTP, FTP
Transport layer	TCP

03 Many computer users make use of wireless networks, either as their main network or when they are using mobile devices.

Discuss the advantages and disadvantages of using wireless networks.

[6 marks]

Level 3 (5-6 marks): explain at least three advantages and disadvantages clearly related to users
Level 2: (3-4 marks): some explanation of two or three issues with some advantages and disadvantages related to users
Level 1 (1-2 marks): some valid points made, probably not well related to users. Only advantages or disadvantages.

Example points:

Advantages	**Disadvantages**
ease of connection	speed of connection slower
ability to roam/move around	speed reduces the further from router
connection to public wifi	interference from other devices
lack of cables	risk of hacking/intercepting data
ease of connecting multiple users, eg. guests	other people may be able to use
cheap/easy to set up. Easy to use on a temporary basis – eg. at a meeting or convention	need for data encryption
	connection not as stable or reliable as wired network

04 Using free to access public wireless networks creates ethical, legal and data privacy issues.

Explain **three** issues that computer users and network providers should be aware of in this situation.

[6 marks]

Level 3 (5-6 marks): explain three issues clearly related to users and providers
Level 2: (3-4 marks): explain two or three issues with some relation to either users or providers
Level 1 (1-2 marks): some valid points made, probably not well related to users of providers

Example points:

- Websites – need to restrict access to inappropriate websites
- Time – limit amount of time, they may not want to provide indefinite access or may want to charge for access after the time limit has expired.
- Preventing file sharing and illegal sharing\use of copyrighted materials.
- Accountability – identification of users and actions on a network by preventing anonymous access.
- Prevention of illegal activities such as terrorism and fraud.
- The responsibility to keep children safe and protected.
- Responsibility to keep users (customers) data safe and secure. Risk that data may be recorded and used for marketing etc…
- Spoofing of websites, phishing. Responsibility of organisation to put some kind of protection in place, eg filtering of known fraudulent sites. Risk of malware or other risk to hardware
- Recording of private messages or details if not encrypted.
- Recording of usernames and passwords that the user may also use to access other systems.
- Responsibility of organisation to secure their systems from possible attack.