4.a.i.) An SMTP server allows the *sending* of e-mail, it accepts e-mails from a mail client program and forwards them to the destination mail host. An SMTP server is optional on a network, required only if e-mail is to be sent.

4.a.ii.) A domain name server maps human readable machine names to network addresses, both locally on the network and possibly across a wider area such as the internet. If the network has no internet connection the use of a DNS server is optional, as a “hosts” file could be used instead.

4.a.iii.) A POP3 server allows the *receiving* of e-mail by an e-mail client program, from the users mailbox on the POP3 host. A POP3 server is optional if there is no e-mail service required on the network.

4.a.iv.) A caching web proxy server makes requests for web resources on behalf of the client programs on the local network, and will also cache some of those resources locally for improved performance. It also allows a single internet network address to be shared by all of the clients on the local network. Such a server is optional, as each client could connect to internet web hosts if required.

4.b.) A message integrity protocol is a means of ensuring that a message has not been altered during transmission. They use a “one-way” mathematical function that can be applied to the plaintext of the message to produce a number, but the number cannot be used to regenerate the message. In addition, the resulting number (also known as a message digest) will have to be encrypted in some way, as anyone tampering with the message could also generate the corresponding message digest. An example of a message digest algorithm is MD5, and the PGP2 e-mail system provides a complete message integrity service.

4.c.) JPEG compression can be used to reduce the storage required for photographic images, often by quite a large amount, although this achieved by loosing some information from the image in the fine detail. The amount of compression can be controlled by the users although images that are compressed too much will suffer from “blocky” effects in which some areas of the picture have no tonal variation. Even images that are set to maximum quality will suffer some small losses in quality as the conversion process described below loses some colour information through averaging.

JPEG compression works by converting the image from colour components (e.g. RGB) to separate “luminance” and “chrominance” components. The parameters for this conversion are dependent on the sensitivity of the human eye to particular colours and some colour information is lost through averaging. The resulting information is then split into blocks and each is transformed into the frequency domain by using a discrete co-sine transform (DCT). The DCT coefficients are then quantised, and the level of quantisation can be adjusted by the user to determine the amount of compression achieved. The coefficients for each block are then run-length encoded, and the blocks themselves are Huffman encoded to achieve further space reductions.

5.a.) A “Firewall” is used to protect an internal network from an external network (such as the internet) which is assumed to be “insecure”. It does this by limiting the types of connections that are allowed both into and out of the internal network, this is known as packet filtering. They can for example restrict access to internal hosts based on their IP address and port number. More advanced firewalls may also monitor the state of each network connection to detect other types of attack such as source routing or IP spoofing.

Firewalls do not however protect internal networks from application vulnerabilities such as forged e-mail addresses or redirected web pages. They will also not protect networks that have other means of access to them, such as dial-in modems or wireless access points. They must also be set up correctly to meet the needs of the internal users and for example, must ensure that all unneeded services are turned off or made inaccessible.

5.b.i.) Network address translation is a means of sharing one internet (IP) address amongst all of the hosts on an internal network. IP packets from the internal network destined for the internet are intercepted by the NAT gateway and sent onwards using the gateways own IP address. The gateway uses the TCP port number to route returning IP packets to the correct internal host. They provide security by hiding the internal network address from the outside world.

5.b.ii.) A Proxy server makes application level requests on behalf of internal network clients. There must be one proxy server for each application to be supported, for example HTTP, FTP or ICQ. Local network clients are not allowed to access internet hosts providing these applications directly must connect to the proxy server. This allows the organisation to restrict the types of external applications provided, and by requiring authorisation on the proxy server can also restrict (and monitor the use of) these applications on a per-user basis.

5.b.iii.) A Virtual Private Network creates a secure IP level connection across an insecure network such as the internet. It does this by sending encrypted “internal” IP packets inside normal “public” IP packets. These are decoded at each end of the connection. They allow an external user, for example with a laptop in a hotel room, to connect and use all the facilities of the internal network over the internet in a secure fashion.

5.c.i.) HTTP is the protocol used between web servers and web browser clients. It allows the client to request resources and the server to return that resource, or an appropriate error message.

5.c.ii.) MIME is used to show the type of a resource, i.e. the format of the data, for example text/html or application/msword. It is used for example in HTTP and SMTP transfers to show the type of data in the resource and how that data is encoded.

5.c.iii.) HTML is a data format describing the layout and content of web pages.

5.d.) A web browser will make an HTTP request to a web server, including the name of the resource it wishes to obtain as a URL (Uniform Resource Locator). The web server will send a reply, also using the HTTP protocol. Included in this reply will be information about the MIME type of the resource. For a web page the MIME type will be “text/html”. The web browser will recognise this type and know that the resource is an HTML formatted web page. It will read the HTML data, interpret the HTML “tags” and display the resulting web page to the user.