# Homework 4 TCP/IP Answers

# A file is being transferred between two computers across a network.

1. Identify a protocol that could be used to transfer this file [1]

File transfer protocol (FTP)

HyperText Transfer Protocol (HTTP)

1. The network uses TCP/IP as shown below



The numbers represent the layers of the TCP/IP stack. Name the layers
in the table below: [4]

|  |  |
| --- | --- |
| **Label** | **Layer** |
| 1 | Application |
| 2 | Transport |
| 3 | Network |
| 4 | Link |

1. Data packets travel from router to router on layers 3 and 4. As this happens, their headers change. Explain the changes with reference to IP and MAC addresses. [5]

1 mark for each:

A packet is received by the router whose MAC address at the Link Layer was specified by the router from which it received the packet

The router removes the MAC addresses at the Link layer; and passes the packet to the Network Layer

The Network Layer looks up the destination IP address in the routing table; and passes the packet back to the Link Layer

The Link Layer sends the message to the next router

# A self-employed accountant runs his own business from a small office. He has an email server that he uses to communicate with his clients. A firewall is also used.

1. Identify **one** protocol and its associated port that he can use to read email
held on this server. [2]

POP3; 110;

IMAP; 143;

1. The accountant also uses his smartphone to access emails. He finds that emails he reads in the office do not appear on his phone. Explain why this is. [2]

The office computer accessing the emails is likely using POP3;

POP3 downloads emails from server and then removes them;

1. A section of the company firewall log is displayed on the accountant’s computer.

Firewall blocked access to resource at 84.134.4.128:80

Firewall granted access to resource at 84.134.4.128:22

From the log above, give an example of the following:

1. Port number 80 or 22 [1]
2. IP Address 84.134.4.128 [1]
3. Socket 84.134.4.128:80 or 84.134.4.128:22 [1]
4. Firewall settings currently restrict access to HTTP. Describe how Secure Shell could be used to circumvent this restriction and provide additional security. Your answer should include what makes SSH a secure connection. [3]

An SSH connection on port 22 is used to access a remote computer;

Port 22 must not be blocked by the firewall;

SSH creates an encrypted tunnel between the two communicating points;

The remote computer can then be used to communicate through HTTP ports; and transfer the data back through the SSH tunnel to the client computer;

Data can be transferred and, if intercepted, cannot be read;

SSH uses private/public keys for encryption;

 [Total 20 Marks]