**Communication networks Coursework 1**

1. 1. The company has asked me to come up with a plan for their network that allows for the controlling of smart mugs. They will need to have a website set up that can sell products and provide customers with a secure way to pay, a way to send emails to customers, internet access to multiple computers, storage for these computers and a way for employees to remotely access the computers.

I have assumed that the customer support on their website would be an instant messaging programme. Another assumption I’ve made is the company doesn’t have a budget when picking the hardware, they need to set up the network.



|  |  |
| --- | --- |
| **Requirement** | **Description** |
| The system must be useable 99% of the time 24 hours a day | This requirement considers the reliability and accessibility of the system. Having the system be very reliable and be accessed 24 hours a day is important for a growing business so they can gain trust from their customers. |
| The system must allow users to access the network remotely | In the client brief it stated that the employees must be able to work remotely and therefore accessing the network not from the office is important. |
| The system must allow users to send and receive emails to/from anyone | Once again in the client brief it stated that the employees must be able to communicate with customers via emails. This is important for the company because it builds a strong customer service to further develop the business |

* 2. For the company I would recommend a Cisco SG350-10 10-port Gigabit Managed Switch. This is a good level switch for a small to medium company allowing for 10 different high-speed connections. It has multiple built in security features such as IGMP snooping, this is useful for high bandwidth usage such as uploading large files. This switch is also at the cheaper end at only £136 which is very cost effective for the company

The 2nd product I would recommend is Synology RT2600ac. This is a great router for a small to medium business because it has 4 gigabit ports built in, 800mbps 2.4GHz Wi-Fi and 1.73gbps 5GHz Wi-Fi for if you’re in close range to the router. It also has 4x4 MIMO Omni-directional high-gain dipole for both 2.4 and 5GHz Wi-Fi allowing for long range Wi-Fi across multiple offices. It also has many built in security features such as intrusion prevention, denial-of-service protection and firewall management meaning the business will be secured from multiple different attacks. It is also very reasonably priced at only £200.

* 1. One limitation that my system would have is there is only 14 gigabit ports on the router and switch. This limits the company to only 14 connected computers. They have plans to expand from 5 employees so if they go over 14, they’ll need to by another switch.

Another limitation would be the size that the Wi-Fi can reach. This is especially limited by the material the walls are made out of, if the walls of the offices are super thick and reinforced then the range the Wi-Fi can reach is very limited. This can be worked around with Wi-Fi range extenders or Powerline adapters which can be purchased at a reasonable cost.

* 1. A distributed denial of service attack is a type of attack where a server is overwhelmed with more traffic than it can handle, this leads to the server crashing. Once the server is down it is often easier for an attacker to get control of the network uploading malicious code. Or the attacker can hold the server hostage and only stop the attack in return for money. These types of attacks are mainly done on websites, so can be prevented, in most cases, by purchasing website security for a well-known company. This is best for a small company because otherwise they need to hire another person to look after the cyber security side of the business, which would cost a lot more than a subscription.

1. 1. I would use the Telnet protocol because in the brief the company made it clear that they need employees to be able to work remotely, and telnet achieves this by allowing people to remotely connect to a host

The 2nd protocol I would use would be the Simple Mail Transfer Protocol (SMTP). This is because they company, said in the brief that they want to communicate with customers via e-mail.

* 1. For Telnet the work station would be used to type in the commands to connect to the sever, and the router

For SMTP

* 1. One security issue of the Telnet protocol is not encrypted which means that anyone with access to the TCP/IP packet flow between the host and client can read what’s being sent.

One security issue with the use of SMTP is it transfers the messages in the email in a plaintext format. This means that there is no encryption and can be intercepted easily.

<https://www.ssh.com/ssh/telnet>