Table of Contents:

1. Introduction:………………………………………………………………………………………………………..…………Page 2

1.1 Executive Summary…………………………………………………………………………………………...Page 2

2. Acknowledging TCP/IP and OSI models:.…………………………………………………..…………………….Page 2

2.1 What mechanics are in effect in the model……..…………………………………………………Page 2

3. WAN technologies: ……………………………………………………..………………………………………………...Page 2

3.1 Synopsis of WAN technologies……………………………………………………………….………....Page 2

3.2 Introduction of media types……………………………………………………………………………...Page 2

3.3 Table: Comparison of media: Synopsis, Speed, Security and Cost………………………Page 3

3.4 Conclusion of media types………………………………………………………….………………..……Page 4

4. Communication within the Infrastructure: …………………………………………………………….….…..Page 4

4.1 IP addressing scheme & requirement for subnets………………………………….………...Page 4

4.2 Tables displaying site’s IP addressing scheme: ……………………………………………..…..Page 5

4.2.1 Table: Manchester IP addressing scheme……………………………………………..Page 5

4.2.2 Table: Birmingham IP addressing scheme……………………………………………..Page 5

4.2.3 Table: York IP addressing scheme……………………………………………………….…Page 6

5. VLAN discussion: …………………………………………………………………………………………………………..…Page 6

5.1 Requirement for VLAN………………………………………………………………………………………..Page 6

5.2 Implementing inter-VLAN routing…………………………………………………………………….…Page 6

6. Communication between networks: ………………………………………………………………………….……Page 7

6.1 RIP discussion………………………………………………………………………………………………..……Page 7

6.2 Table: external IP addresses………………………………………………………………………….…….Page 7

6.3 Configuring RIP………………………………………………………………………………………………..….Page 7

6.4 NAT/PT discussion………………………………………………………………………………………….…Page 7

6.5. Configuring NAT/PT……………………………………………………………………………….…….……Page 8

7. Security within the infrastructure: ……………………………………………………………………….………….Page 8

7.1 MAC port security……………………………………………………………………………………..….…….Page 8

7.2 VLAN security……………………………………………………………………………….……………………..Page 8

8. Conclusion: …………………………………………………………………………………………………….……….………Page 8

9. Bibliography: …………………………………………………………………………………………………………..………Page 9

1. Introduction:

1.1 Executive Summary

An eSports company based in Manchester wish to expand their company and their infrastructure to Birmingham, whilst upgrading their current infrastructure in their Manchester and York site, due to the fact that their current network is outdated and underperforming. All of their sites need to be identical internally and should possess the same external links, so the new infrastructure should be appropriate and compatible for all the sites.

1. Acknowledging TCP/IP and OSI models:

2.2 What mechanics are in effect in the model

Firstly, a networking expert would distinguish the different layers of the TCP/IP and OSI models and how their applicable to the company’s infrastructure. They would learn that this company’s infrastructure requires work on internet accessing, which is layer 1 and Layer 1+2 (network access and physical + data link layer) on the models respectively (Edwards, J. and Bramante, R., 2009) [[5]](#_9.__). Additionally, IP addressing and subnetting; these being layer 2 and 3 (Internet and Network layers on the respective models). As well as the exchanging of packets and messages over a network, layer 3 and 4 (TCP and UDP on the transport layer of the respective models). (Samain, J. et al.,2017) [[14]](#_9.__)

1. WAN technologies:

3.1 Synopsis of WAN technologies

With this information, the networking expert should understand that each site should be identical but independent of each other, so each site will be a LAN (local-area-network) connecting to each other, forming a WAN (wide-area-network). Therefore it’s imperative to work on the Layer 1 protocol of the TCP/IP and layer 1 +2 of the OSI model (network access and physical + data link respectively) in order to improve the media/connection between the sites and ISP to prioritise and uphold the quality of the live streaming as well as general communications (Goralski, 2008) [[6]](#_9.__) (Vachon, B., Graziani, R. (2008) [[19]](#_9.__). The network expert will need to determine the best media for cross-site communication, respecting the fact that the 20Mbps from the DSL link is insufficient.

3.2 Introduction of media types

There is a limited number of media, and their advantages and disadvantages will be expressed in the table below. Only cable media will be considered since it’s generally much faster than wireless media, since it isn’t encumbered by unexpected and unnecessary traffic.

3.3 Table: Comparison of media: Synopsis, Speed, Security and Cost

|  |  |  |  |
| --- | --- | --- | --- |
|  | Twisted Pair | Coaxial Cabling | Fiber-Optic Cabling |
| Examples & Description | UTP (Unshielded Twisted Pair) – wires are just twisted together, STP (Shielded Twisted Pair) – individual pair of wires are wrapped in foil and then wrapped again for double protection. Both are terminated with a RJ-45 connector. (Oliviero, A. and Woodward, B., 2014) [[12]](#_9.__) | Coaxial Cable – solid stranded copper surrounded by insulation which is then surrounded by a copper mesh and outside insulation. Terminated with N-series type, F-series type or BNC connector.  (Ruytenberg, T., Webb, A. and Zivkovic, I. 2020) [[13]](#_9.__) | SMF (Single mode Fiber) – single small core that carries single ray of light shot from laser technology, and MMF (Multimode Fiber) – larger single core that carries light pulses (1+ ray of light) shot from LED emitters. Terminated with splicing and standard connectors; straight-tip, subscriber-connector, Lucent connector, Duplex multimode connector.  (Syvridis, D. et al., 2005) [[16]](#_9.__) |
| Material | Copper | Copper | Glass |
| Speed & Bandwidth | UPT – 10 Mbps up to 10 Gbps 200 Mhz. SPT – 10 Mbps up to 100 Mbps. | 10 Mbps up to 100 Mbps. | SMF – 10 Mbps up to 100 Gbps. MMF – 10 Mbps to 10 Gbps. |
| Distance & Attenuation | Maximum cable length of UTP is 100 metres. Maximum cable length of STP is 100 metres too. Attenuation increases at these lengths so a signal regeneration device is mandatory. | Maximum cable length is 500 metres. Likewise a regeneration device is necessary to decrease attenuation. | SMF can run significantly longer distances than MMF; SMF – 40 kilometres and MMF – 550 metres. This is because the single beam of light in SMF has less dispersion than the MMF’s multiple beams of light, which ultimately result in loss of signal strength. |
| Security/Endurance | UTP is susceptible to EMI (electromagnetic interference) and RFI (radio frequency interference) and crosstalk which can all distort and corrupt the data, STP has minimal susceptibility to EMI and RFI and crosstalk due to its braided foil shields. Both are made of twisted copper and insulated so they can endure more damage than fiber-optic. | Coaxial is less susceptible to EMI and RFI than twisted pair media. It’s still susceptible to crosstalk but less likely than twisted pair media. Due to its insulation and mesh, it is the most durable media. | Completely immune to EMI and RFI and crosstalk. Since it’s made of thin strands of glass, a fragile material, so it can more easily be damaged than other media types.  (Agrawal, G.P. 2010) [[1]](#_9.__) |
| Training Required | Minimal training required to install and maintain it. | Minimal training required to install and maintain it. | Trained professionals are required to install and maintain |
| Cost | Cheap media, UTP being slightly cheaper than STP. | Cheap media, but more expensive than twisted pair. | Most expensive media, MMF being pricier. |

3.4 Conclusion of media types

A networking expert will compare the statistics of the media and obviously determine fiber-optic as the best media choice. However, they will ultimately have to make a decision based on the company’s budget, and fiber-optic will be incredibly expensive. If the company wishes to have the most superior internet access, cross-site communication and streaming quality and have the budget to support this then the networking expert will deem fiber-optic as the best media choice, but if they don’t have a budget to support this then a mixture of fiber-optic and the other media will be viable e.g., fiber-optic to connect the sites to each other and the ISP, with other media within each site’s network. This will still improve cross-site communication and host streaming substantially.

4. Communication within the Infrastructure:

4.1 IP addressing scheme & requirement for subnets

Each site will have their own IP addressing scheme which will be issued by the DHCP configured on the site’s routers. Each site will then have their IP address subnetted to relieve network congestion to prevent performance deterioration as well as to secure each department. The networking expert will determine the appropriate subnet mask, so that all departments have a subnet that can host all of their devices (Mogul, J., 1985) [[10]](#_9.__). They will deem that a subnet mask of /27 (255.255.255.224) is suitable because; 8 subnets will be available, meaning each department will have their own subnet, even the Manchester site that has 2 additional departments, and each subnet will have 32 hosts, meaning that every device can be hosted (Tarkaa, N.S., Iannah, P.I. and Iber, I.T., 2017) [[17]](#_9.__). The 30 competitor machines will be split into 3 blocks of 10 machines, therefore each block will be assigned their own subnet. This is to minimise the amount of hosts on each subnet, because assigning all 30 machines to one subnet would eliminate the possibility of scalability, since 2 address are automatically reserved for the network ID and broadcast ID.

4.2 Tables displaying site’s IP addressing scheme:

4.2.1 Table: Manchester IP addressing scheme

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Subnet (Department) | Number of Hosts | Subnet Address | Subnet Mask | First Usable Address | Last Usable Address | Broadcast Address | Number of Unused IP Addresses |
| Admin Machines | 10 | 172.16.0.0/27 | /27 | 172.16.0.1/27 | 172.16.0.30/27 | 172.16.0.31/27 | 20 |
| Competitor Machines: A | 10 | 172.16.0.32/27 | /27 | 172.16.0.33/27 | 172.16.0.62/27 | 172.16.0.63/27 | 20 |
| Competitor Machines: B | 10 | 172.16.0.64/27 | /27 | 172.16.0.65/27 | 172.16.0.94/27 | 172.16.0.95/27 | 20 |
| Competitor Machines: C | 10 | 172.16.0.96/27 | /27 | 172.16.0.97/27 | 172.16.0.126/27 | 172.16.0.127/27 | 20 |
| Laser Printer | 4 | 172.16.0.128/27 | /27 | 172.16.0.129/27 | 172.16.0.158/27 | 172.16.0.159/27 | 26 |
| Server Class Machines | 20 | 172.16.0.160/27 | /27 | 172.16.0.161/27 | 172.16.0.190/27 | 172.16.0.191/27 | 10 |
| Management Machines | 10 | 172.16.0.192/27 | /27 | 172.16.0.193/27 | 172.16.0.222/27 | 172.16.0.223/27 | 20 |

4.2.2 Table: Birmingham IP addressing scheme

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Subnet (Department) | Number of Hosts | Subnet Address | Subnet Mask | First Usable Address | Last Usable Address | Broadcast Address | Number of Unused IP Addresses |
| Admin Machines | 10 | 172.17.0.0/27 | /27 | 172.17.0.1/27 | 172.17.0.30/27 | 172.17.0.31/27 | 20 |
| Competitor Machines: A | 10 | 172.17.0.32/27 | /27 | 172.17.0.33/27 | 172.17.0.62/27 | 172.17.0.63/27 | 20 |
| Competitor Machines: B | 10 | 172.17.0.64/27 | /27 | 172.17.0.65/27 | 172.17.0.94/27 | 172.17.0.95/27 | 20 |
| Competitor Machines: C | 10 | 172.17.0.96/27 | /27 | 172.17.0.97/27 | 172.17.0.126/27 | 172.17.0.127/27 | 20 |
| Laser Printer | 4 | 172.17.0.128/27 | /27 | 172.17.0.129/27 | 172.17.0.158/27 | 172.17.0.159/27 | 26 |

4.2.3 Table: York IP addressing scheme

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Subnet (Department) | Number of Hosts | Subnet Address | Subnet Mask | First Usable Address | Last Usable Address | Broadcast Address | Number of Unused IP Addresses |
| Admin Machines | 10 | 172.18.0.0/27 | /27 | 172.18.0.1/27 | 172.18.0.30/27 | 172.18.0.31/27 | 20 |
| Competitor Machines: A | 10 | 172.18.0.32/27 | /27 | 172.18.0.33/27 | 172.18.0.62/27 | 172.18.0.63/27 | 20 |
| Competitor Machines: B | 10 | 172.18.0.64/27 | /27 | 172.18.0.65/27 | 172.18.0.94/27 | 172.18.0.95/27 | 20 |
| Competitor Machines: C | 10 | 172.18.0.96/27 | /27 | 172.18.0.97/27 | 172.18.0.126/27 | 172.18.0.127/27 | 20 |
| Laser Printer | 4 | 172.18.0.128/27 | /27 | 172.18.0.129/27 | 172.18.0.158/27 | 172.18.0.159/27 | 26 |

5. VLAN discussion:

5.1 Requirement for VLAN

A networking expert would certainly utilise and integrate VLANs into each site’s network in order to reduce broadcast traffic, since communication will only be forwarded to other devices in the same VLAN (Xiaowei, J., Zhimin, L. and Wenlong, 2019) [[21]](#_9.__), and eliminate the need for additional equipment e.g., routers and switches, since a VLAN is deployed on the site’s existing switch, thus saving money and ensuring network flexibility/scalability. This will be executed by assigning a VLAN to each subnet within the site thus creating a VLAN for each department in the network.

5.2 Implementing inter-VLAN routing

An inter VLAN mechanic will be implemented as well, so communication will be possible between devices in different VLANs. The mechanic is incredibly beneficial, because communication will only occur within the same VLANs, this prevents unnecessary communication within the site’s network. However, inter VLAN routing will enable the possibility of communication between devices in different VLANs when needed, consequently reducing traffic (Odi, A.C., Nwogbaga, N.E. and Chukwuka, N.O., 2015.) [[11]](#_9.__). This will be executed on the router, after the expert creates DHCP pools and assign the VLAN’s their subnet network, their default gateway and their DNS.

6. Communication between networks:

6.1 RIP discussion

Communication will be enabled between each site by configuring RIP (Routing Information Protocol) on the site’s routers. RIP is a protocol that is specifically used by routers to exchange routing information on a network, by determining the efficient way to route the data. (Hedrick, C., 1988) [[7]](#_9.__)

6.2 Table: external IP addresses

Each site is given their own external IP address between each other: These being:

|  |  |
| --- | --- |
| Site | External IP address |
| Manchester – Birmingham | 175.101.0.0/16 |
| York – Birmingham | 175.102.0.0/16 |
| Manchester – York | 175.103.0.0/16 |
| Manchester - ISP | 172.104.0.0/16 |

6.3 Configuring RIP

The routers are given an IP address from the networks above, respective of what site they belong to. Since each router is connected to each other, each router will have 2 external IP address added to their RIP, plus their respective internal IP address network. Essentially, this allows the routers to recognise the networks they are communicating with e.g., Manchester’s device pings Birmingham’s device; communication is successful because the internal networks are recognised by the routers. (C. G. Dumitrache, G. Predusca, L. D. Circiumarescu, N. Angelescu and D. C. Puchianu, 2017)[[4]](#_9.__)

Only the Manchester network has communication with the ISP, so the expert will only connect the Manchester router to the ISP. The Manchester connection to the ISP will be configured statically for performance and security reasons. Less bandwidth is consumed because no route calculation is needed, communication will only occur in the given route and due to the fact that the static route won’t be advertised over the network, it results in better network security. (Black, U. D., Black, U. N. 2000) [[3]](#_9.__)

6.4 NAT/PT discussion

However, to enable communication to the ISP, NAT/PT (Network Address Translation/Port Address Translation) will need to be implemented because the site’s networks are operating with private IP addresses whereas the ISP uses public IP addresses (Tsirtsis, G. and Srisuresh, P., 2000) [[18]](#_9.__) . The NAT protocol maps private IP addresses to a public IP address before transferring information, so communication between a private network and a public one is successful. (Wing, D., 2010) [[20]](#_9.__)

6.5. Configuring NAT/PT

NAT is configured by creating access control lists, a network traffic filter mechanic that can grant or deny access to a destination (Suman, S. and Agrawal, E.A., 2016) [[15]](#_9.__). In this case, the expert will want to grant the site access to the ISP, so access control lists are created for the site’s VLANs and granted permission to the router-ISP connection. ‘Nat inside’ will be enabled on all the VLANs inside the network whilst ‘NAT outside’ will be enabled on the router-ISP connection, effectively allowing the private IP addresses to be translated to public ones.

7. Security within the infrastructure:

7.1 MAC port security

The networking expert will apply sticky MAC port security to all the switches in the site’s infrastructure. The feature dynamically learns the device’s MAC address that’s are connected to it and retains this information(McMillan, 2018) [[8]](#_9.__). It has both security and performance inferences, because only ‘learnt’ devices are given the privilege of forwarding packets, thus preventing unknown devices from forwarding packets and potentially preventing an attack.

7.2 VLAN security

As expressed above, VLANs serve security purposes too, because traffic is filtered, therefore if a device is compromised, it prevents it from infecting the entire network. (Ashraf, Z. and Yousaf, M., (2016)[[2]](#_9.__)

8. Conclusion:

In conclusion, the overall infrastructure has been improved greatly by prioritising efficiency by implementing protocols and mechanics that focus on relieving network congestion and reducing bandwidth consumption by filtering out unnecessary and unwanted traffic as a result of VLANs, which simultaneously provides substantial security to the network due to the prevention of packets/traffic being forwarded outside of their department or even introduced in the first place thanks to MAC port security.

## 9. Bibliography:

[1] Agrawal, G.P. (2010). *Fiber-optic communication systems*, fourth edition. 4th ed. New York: Wiley. doi:10.1002/9780470918524. Pp. 36-44

[2] Ashraf, Z. and Yousaf, M., (2016). *SECURE INTER-VLAN IPv6 ROUTING: IMPLEMENTATION & EVALUATION*. Pakistan: Science International, *28*(3). Pp 3007-3012

[3] Black, U. D., Black, U. N. (2000). *IP Routing Protocols: RIP, OSPF, BGP, PNNI, and Cisco Routing Protocols*. Switzerland: Prentice Hall PTR. Pp 117-120

[4] C. G. Dumitrache, G. Predusca, L. D. Circiumarescu, N. Angelescu and D. C. Puchianu, (2017). *Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer*, Romania: IEEE. doi: 10.1109/ISEEE.2017.8170694. pp. 1-6

[5] Edwards, J. and Bramante, R. (2009). *Networking self-teaching guide: OSI, TCP/IP, LANs, MANs, WANs, implementation, management, and maintenance*. 1st ed. Hoboken: Wiley. pp. 435-436

[6] Goralski, W., 2008. *The Illustrated Network: How TCP/IP Works in a Modern Network*. 2nd ed. Morgan Kaufmann, pp.33-46.

[7] Hedrick, C., (1988). *Routing information protocol*. United States, New Jersey: RFC 1058, Rutgers University. Pp 2-4.

[9] McMillan, T 2018, *CCNA Security Study Guide : Exam 210-260*, John Wiley & Sons, Incorporated, Newark. Available from: ProQuest Ebook Central. pp. 143-144

[10] Mogul, J., (1985). *Internet standard subnetting procedure*. United States: RFC Editor. Doi: <https://doi.org/10.17487/RFC0950>. Pp 1-11

[11] Odi, A.C., Nwogbaga, N.E. and Chukwuka, N.O., (2015). *The Proposed Roles of VLAN and Inter-VLAN Routing in Effective Distribution of Network.* Nigeria: Ebonyi State University. International Journal of Science and Research, (7), pp.2608-2615.

[12] Oliviero, A. and Woodward, B., 2014. *Cabling: the complete guide to copper and fiber-optic networking*. John Wiley & Sons. pp 9-13.

[13] Ruytenberg, T., Webb, A. and Zivkovic, I. (2020). *‘Shielded‐coaxial‐cable coils as receive and transceive array elements for 7T human MRI’*, Magnetic resonance in medicine, 83(3), pp. 1136–1137. doi:10.1002/mrm.27964.

[14] Samain, J. et al. (2017). *‘Dynamic Adaptive Video Streaming: Towards a Systematic Comparison of ICN and TCP/IP’*, IEEE transactions on multimedia, 19(10). doi:10.1109/TMM.2017.2733340. pp. 2166-2169

[15] Suman, S. and Agrawal, E.A., (2016). *IP traffic management with access control list using cisco packet tracer*. Int. J. Sci. Eng. Technol. Res, *5*(5), pp 1556-1560.

[16] Syvridis, D. et al. (2005). *‘Chaos-based communications at high bit rates using commercial fibre-optic links’*, Nature, 438(7066), pp. 343–346. doi:10.1038/nature04275.

[17] Tarkaa, N.S., Iannah, P.I. and Iber, I.T., (2017). *Design and simulation of local area network using cisco packet tracer*. The International Journal of Engineering and Science, *6*(10), pp.63-77.

[18] Tsirtsis, G. and Srisuresh, P., (2000). *RFC2766: Network Address Translation-Protocol Translation (NAT-PT)*. United States: RFC Editor. DOI: <https://doi.org/10.17487/RFC2766>. Pp 4-13.

[19] Vachon, B., Graziani, R. (2008). *Accessing the WAN, CCNA Exploration Companion Guide*. United Kingdom: Pearson Education. Pp 3

[20] Wing, D., (2010). *Network address translation: Extending the internet address space*. IEEE internet computing, *14*(4), doi: [10.1109/MIC.2010.96](http://dx.doi.org/10.1109/MIC.2010.96) pp.66-70.

[21] Xiaowei, J., Zhimin, L. and Wenlong (2019). *‘Application of Routing Communication Between VLANs in A Layer 3 Switch’*, IOP conference series. Materials Science and Engineering, 569(3). pp. 1-2