London South Bank University

School of Engineering
Electronic and Computer
Systems Engineering

Assignment

for

Data Communications and Computer Networks

EEE_5_DCN

Student ID: 3909995

Module Leader: Zhanfang Zhao

Table of Contents

Contents

Abstract

London – Liverpool network development (Design and Implementation, Maintenance)
By Alexandru-Mihai Sava, School of Engineering (London, United Kingdom), Lecturer Zhanfang Zhao, London South Bank University

A reliable London-Liverpool network system must include a secure communication solution to prevent potential foreign devices from accessing the contents of one department. The construction of the system must be in accordance with current standards to ensure increased longevity through the possibility of upgrading and maintaining over time.

The report targets to design and implement a network system for both London and Liverpool location based on Managing and Technical Director's requirements. Their main priority is separating employee departments from company servers, as well as configuring firewalls to control and manage the traffic flow from outside at peak times.

The final design demonstrates the ability of developing and implementing small networks based on the application of basic knowledge in the field.

Introduction

As a company grows its business, solution providers play a leading role in the network design projects needed to update the client's existing network and expand it to accommodate additional users or workloads. Vendors have commoditized their network products, allowing solution providers to implement powerful network elements that would have been cost prohibitive just a few years ago. According to Stephen J. Bigelow, Senior Technology Editor. Published on 27 Oct 2008 Network design considerations checklist for providers. SearchITChannel website.

The scope of this report is improving the networks both at London and Liverpool based on their business needs. The most important consideration in any network design project is identifying the client's business problem. Network design is less about technologies and components, and more about meeting clients' network technology goals and business objectives. According to Stephen J. Bigelow, Senior Technology Editor. Published on 27 Oct 2008 Network design considerations checklist for providers. Problem identification. SearchITChannel website.

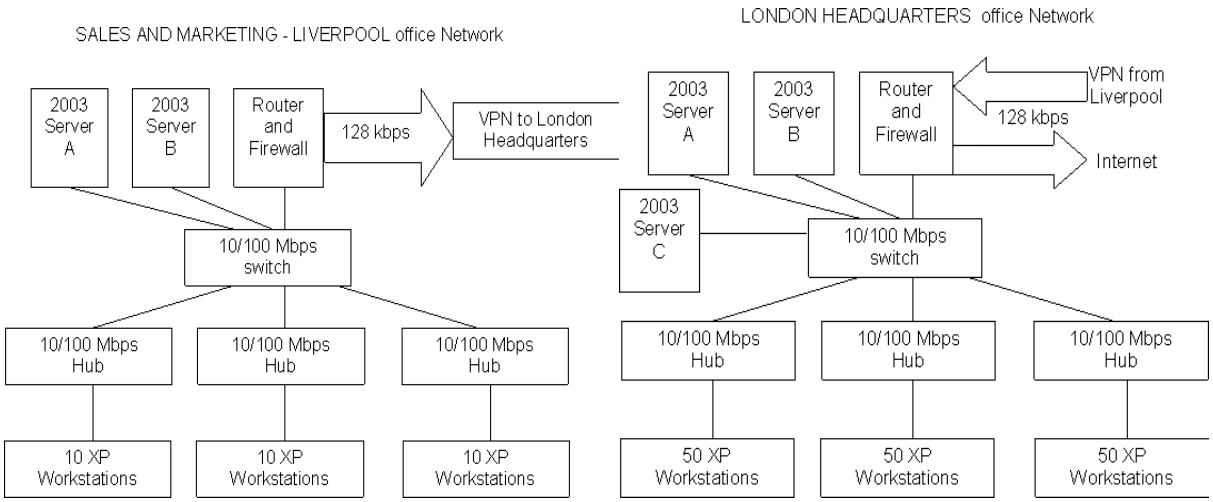
During the meeting with the Managing Director and Technical director of the company, several requirements were raised in attention such as updating the security infrastructure between their departments, including a secure communication link between the two locations of the company. Furthermore, the directors are keen to get the full control of certain corporate information on their servers and strictly control the access in such a manner that only senior management staff can get directly access.

Incontestably, their main priority is establishing security measures to ensure safe exchanges of information via internet between locations. In this case, a physical firewall on both locations is necessarily needed to hide all the local data network from the outside world while permitting the organization to access the Internet smoothly. A VPN configuration of the company's router would be mandatory to allow Liverpool and London access their files from the servers and when Liverpool occasionally streams videos to London Headquarters.

That all being said, one approach would be configuring the switches to create the department VLANs first, following by setting up the firewalls and VPN IPsec tunneling connections between businesses. Once the high-priority tasks are completed, then I would like to focus researching on adding extra security layers such as a Domain Controller Server to store the authentication credentials when an employee from one department logs in to their computer, allowing them to access IT resources if they only successfully log on. Besides, for the VPN connection in the London Headquarters, an authorization server should be included as when the Liverpool streams to London, they would need to authenticate with their credentials to be able to connect on the VPN infrastructure.

Initials Design and Further Meetings

Before the post-implementation process, a list of detailed requirements need to be established from Directors to be able choosing the best approach of designing a final solution. Their initial network topology includes the VPN connection from Liverpool to London, but there are no specifications of how it should be implemented on their system. The same case is for configuring VLANs on the switch in boh locations, no indications whatsoever of which ports or how many of them should be allocated to one departament if they wish to expand their business in the near future by adding new departaments or servers, or even such other devices like printers, analog phones and so on. In the Liverpool office network, there are only two servers available, A and B, and based on their current requirements one of them should be and exchange mail server (SMTP) for the departaments to interchange emails with the inside network, along with the outside Internet and Headquarters office. The other one should be an file sharing server (FTP) as Liverpool office works with a lot of clips for their marketing and sales purposes that need to get stored somewhere safe where only authorized personel can access, modify, delete, share or edit the content. The same should be for the London office servers, one SMTP server for emails and one FTP server for file sharing and storing, but for the third one, there are much more possibilities of what is its exact purpose. As Liverpool office connects via VPN to London Headquarters, it is importat to understand what protocol is the VPN using, and based on this information, the server can be either a domain controller server or a authorization server for VPN authentification and access token.



When arranging further meetings with the Directors of both locations, the following aspects should be clarified. First, when configuring the VPN access from Liverpool, I would like to know what their needs are and how the virtual connection will be used to implement the most appropriate protocol and cut additional costs of maintenance over time. VPNs has two main categories: site-to-site or remote access. The remote access is a layer 3 VPN connectivity and the traffic information between the offices is shared with the Internet Service Provider (ISP). This type of connection does not include any configurations on their inside

office routers as the tunneling takes place inside the service provider's router. This technique is easier to implement, and it is less costly, and for a such small company I would opt this option compared to layer 2 VPN. Layer 2 VPN or point to point tunneling protocol is one of the first versions of the VPN in the early days of the internet, but it became less dependable over time due to their high demand of often maintenance as this is under control of the management office, requiring dedicated servers to operate. Although it might be safer as this type of VPN does not get involved with the ISP, a special team is required in both locations to check and control the traffic, raising the maintenance costs that can be avoided if using the newer VPN layer. Depending on their budget and how sensitive their data is, is the Director choice to choose either layer 3 ISP VPN or layer two fully in their control VPN.

As for the firewall and internal router, their configuration can be updated based on VLAN creation. However, firewalls require large amount of maintenance to certify that the network integrity remains maintained and efficient. This may not be a major problem for years to come but hiring a specialist once every several years is certainly required as an outdated firewall could put the local network at risk.

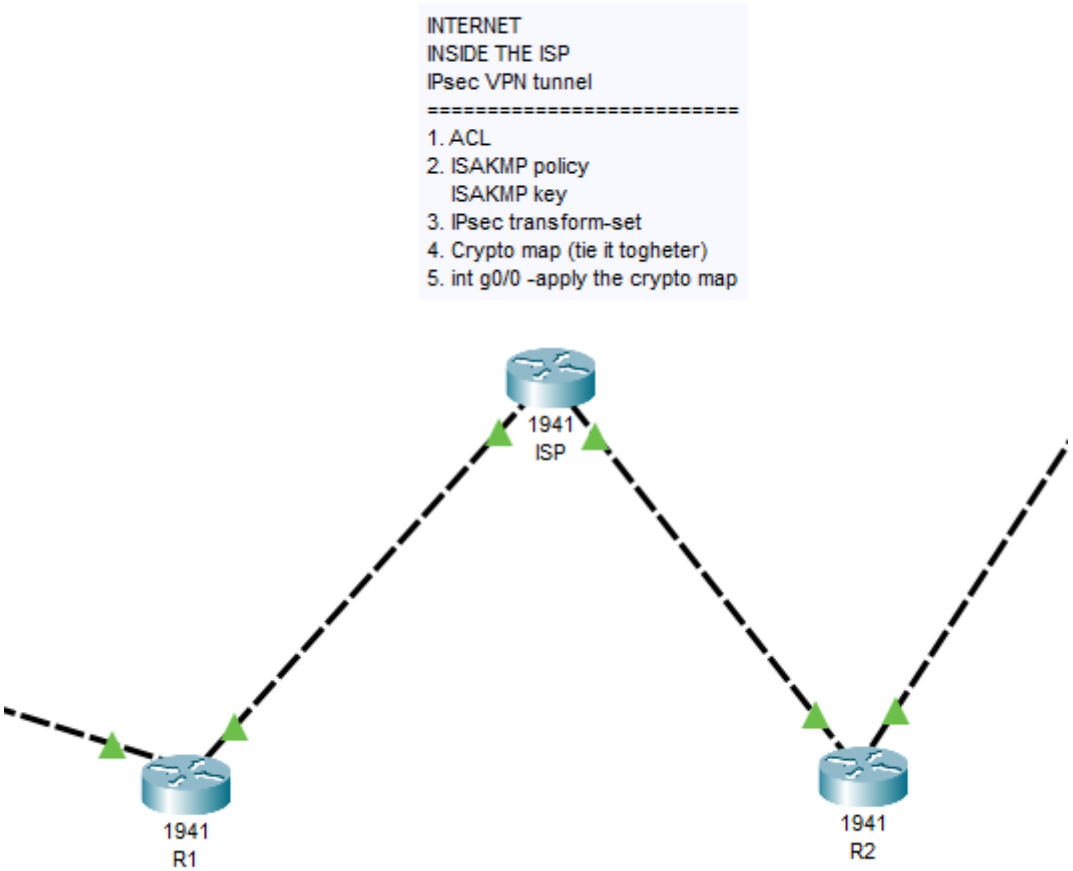
With given the circumstances for the initial network design taking care of, it would be useful to know the budget the company is willing to spend on buying equipment for the expansion of their network in an even more secured LAN environment. If the Directors agree to allocate ore to their budget, a Domain Controller Server in both locations would be included, allocating users with a work/business account to log in before starting working. These Domain Controller Servers or simply DNS servers will cover all the devices inside the LAN to get accessed by only having a valid account. A worker failing to register to his work account will result in not being able to access the company's files. It is recommended to include and additional Domain Controller Server as it provides redundancy and eliminates the possibility of a system crash during peak times when more than 80% of the employee are currently working, exchange emails or share files.

Another important aspect to ask the Director is how many users per network wants to keep. Personally, for this current network, I would split it in four networks with the subnet class of 26 as there are no more than 60 workstations for each department. If the Director wants to add more than sixty workstation per department, a new network must be configured and assigned to another VLAN. Based on the decision of the Director, an optimal subnetting for the local LAN would be applied. Lastly, based on this, I would ask to allocate more money into the budget to buy an additional switch for both locations to separate the servers from users. This will increase the security even more with now having the servers separated physically (a dedicated switch only for them) and virtually (VLAN). This will become useful if they want to buy other devices such as printers or analog phones for Liverpool Sales and Marketing departments as these will be included in a secured VLAN, connected to the servers' switch.

After attending to the final meeting with the Directors, they agreed to allocate more money in their budget, meaning both networks will feature Domain Controller Servers, printers especially for Sales and Marketing department and additional switches to separate the Servers/Printers from Users/Workstations.

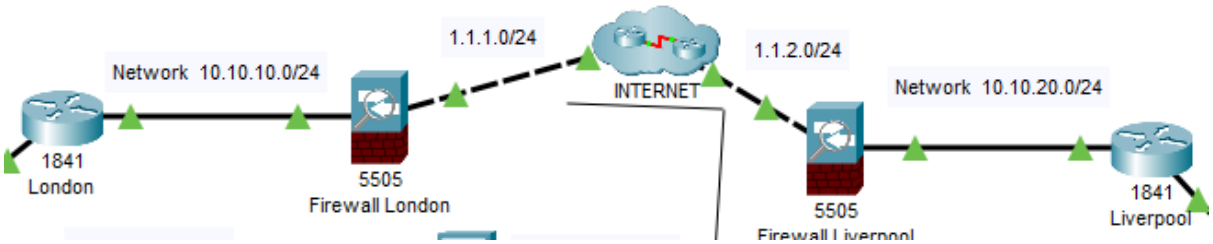
Design and Implementation

Considering all the details the Directors proposed during these meetings, it is attainable to achieve a solution to their security communication problem, starting from the initial designed network, following with the post-implementation process of adding and configuring the new devices. The emphasis will be on performing the connection between the IPsec router located in the London ISP router (R1) and Liverpool ISP router (R2), both connected to WAN which is another ISP that establish the internet connection for London and Liverpool. This step would be know as setting up the VPN connection from Liverpool to London and vice-versa using IPsec tunneling technology.



IPsec tunneling represents the layer 3 VPN which is done inside the ISP routers. The company can request to their ISP to enable such feature which comes to an additional cost. The first step is to enable the tunneling is allowing an access list (ACL) to permit the traffic from R1 flowing to R2 and vice-versa. ACL acts similarly as a firewall by creating lists of IP addresses to either permit or deny their traffic inside or outside their interface. Once the ACL is configured and flow between the router is permitted, the Internet Security Association and Key Management Protocol (ISAKMP) needs to be enabled the 1941 Cisco Routers. Any Cisco Routers older than 1941 do not support this feature, therefore no VPN can be

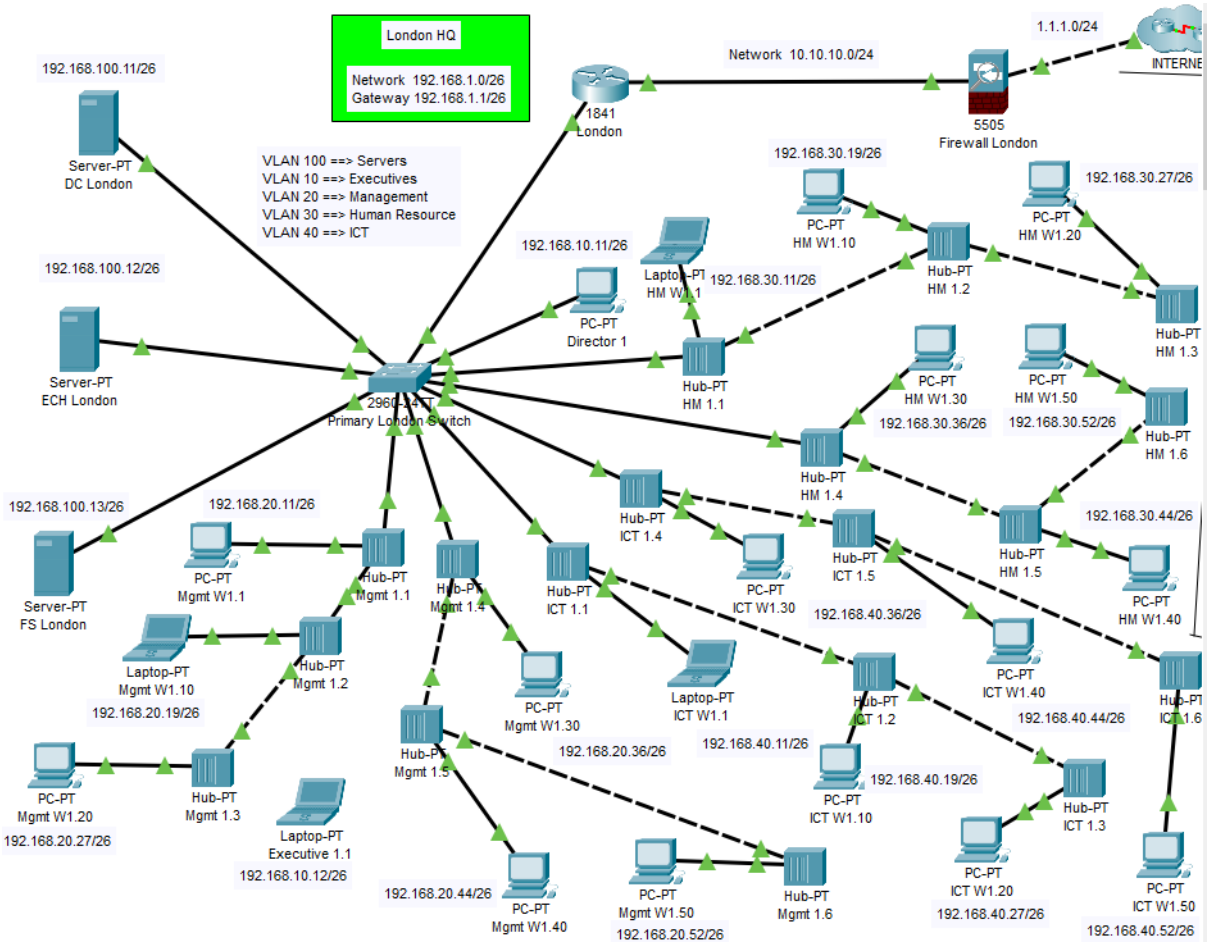
configured on them. ISAKMP, also called IKE (Internet Key Exchange), is the negotiation protocol that allows hosts to agree on how to build an IPsec security association. According to Cisco Press. Published on 3 Oct 2017. IPsec VPN. Cisco Press website. In this configuration, both routers get the crypto isakmp policy is set on ten, having authentication pre-share in group 5 with an encryption aes 256. The isakmp crypto key is ensured by the policy by default, but during the configuration it important to point out towards which IP address the isakmp policy and key should be applied. Upcoming step is connecting their crypto map by showing the tunneling path based on how many peer addresses is travelling through. As an example, from R1 to R2 the IP travels under one peer address which is the interface address of the destination router R2. With the crypto map created on both routers, it must get applied on the corresponding interface on where the communication is performed to turn on the VPN connection between London and Liverpool public network addresses. For such small or medium sized companies, having a public IP address with a prefix size of twenty-four is extremely expensive and not needed. An appropriate example of a public class A IP address for London would be 1.1.1.0/30 with a range of usable hosts 1.1.1.1 and 1.1.1.2 and a broadcasting address of 1.1.1.3; for Liverpool would be 1.1.2.0/30 with a range of usable hosts 1.1.2.1 and 1.1.2.2 and a broadcasting address of 1.1.2.3. During the packet tracer implementation, the 24-prefix size was used to evaluate the connectivity links with the internet.



The next priority on the list to implement the security solution is setting up the physical firewall connections from the inside local and global to outside global and local. From the London perspective, the inside local is the LAN where the servers and workstations are functionating together, all of them connected to Internal Router, then connected to firewall and inside global is the firewall connection with the London ISP. Firewall acts like a security gate, it is responsible of analyzing the packages that come from the outside Internet and inspect if they are in the access list or not to access the LAN. It also translates the private IP addresses to the owned public one when the internet is accessed from the inside. For our organization being able communicate with each other, the firewalls need to be configured to such an extent that permits access to the Liverpool private IP address only. To achieve this, both need to enable the ACL and permit their public IP addresses any type of traffic (TCP, ICMP, UDP etc.). Following next, an object network named NAT London, respectively Liverpool needs to be created and include the subnet type of their public IP address and enable NAT protocol into a dynamic interface from inside to outside. With NAT enabled and configured, the NAT overload translation (PAT) can be realized by selecting the access list that permits the inside entry of all private IP address and guide it to the interface port directly connected to the Internet that has the one private IP address. Finally, a routing path table for all inside networks of the LAN must guide to the inside local port of firewall which comes from the Internal router and another routing path table for the outside network that the company owns for both locations.

Inside the London Headquarters building, and Intern Router (Black) called London manages all the LAN traffic, routing either inside other VLANs or towards the firewall to outside Internet and Liverpool office depending on the needs. The London LAN is composed of five different VLANs, all of them created inside Primary London Switch. The switch has a total of

twenty-six ports, 24 fast and 2 gigabit ethernet ports. As one of them will be used for trunking to establish communication between VLANs via a layer three device, which in this case is the Router London, remaining with 25 available ports. Based on company's requirements, there are going to be 5 VLANs for servers and other end devices, Executives which are the Technical and Managing Directors with the senior staff, Management department, Human Resource department and ICT department.



Each department from London Headquarters has fifty active workstations, all connected to one hub which then goes into the switch. However, the packet tracer simulation tool features hubs up to ten ports maximum, hence multiple hubs would be used. They only support half-duplex communication, meaning in technical terms, one device's traffic can sometimes collide with other device's traffic causing delays and network slowdowns. This particularly happens when they are multiple devices connected simultaneously. Their big advantage is the cost, they are a lot more less expensive than a switch, thus for such network and budget, this is going to be the solution to connect all fifty workstations for each department.

To reduce the connectivity slowdowns and delays of the hubs, every hub should be connected to one of the switch's ports and not between them. If multiple hubs relate to each other, then going into the switch and there are a considerable number of workstations connected to the hub's ports, the Internet connection starts decreasing dramatically as it gets closer to the last hub. Therefore, how the hubs are connected in my simulation topology above (3 hubs each of them connected to each other) is not dependable when the workers of one department expects an important email or exports a large file towards the storing server. The solution while implementing the design in a real environment is to connect all the

department hubs to the corresponding VLAN they belong in.

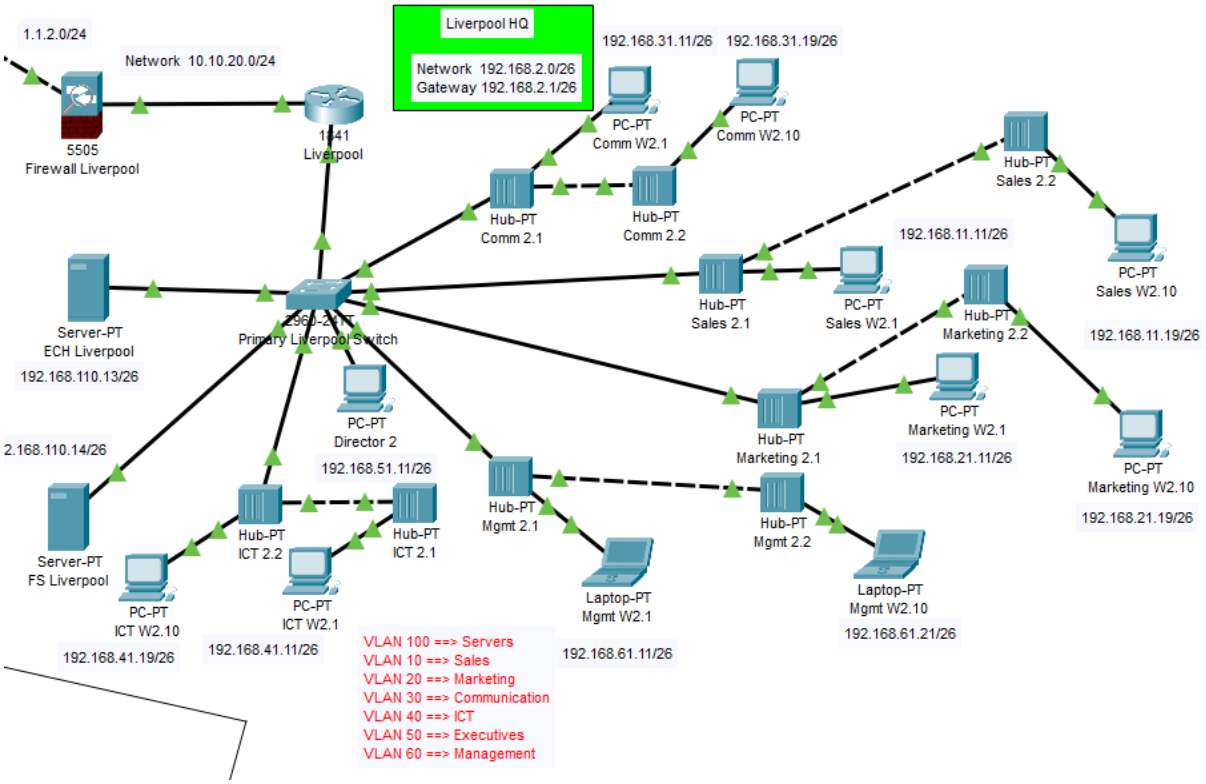
Each VLAN gets assigned with 5 ports from the switch, resulting in using all the available ones. The VLAN 100 named Servers gets the Fast Ethernet ports 0/2 to 0/6, VLAN 10 named Executives gets the Fast Ethernet ports 0/7 to 0/11, VLAN 20 named Management gets the Fast Ethernet ports 0/12 to 0/16, VLAN 30 named Human Resource gets the Fast Ethernet ports 0/17 to 0/21 and, finally, VLAN 40 named ICT gets the Fast Ethernet ports 0/22 to 0/24 and the remaining two Gigabit ports. By inserting one hub (a hub has 10 ethernet ports) in every available port of a VLAN, this results a total of 50 available ports for the VLAN, being exactly the number of ports needed to connect the 50 computers. If the company wishes to expand their department and add more computers, it is either connecting and additional hub to another one, but it is not recommended, or buying another switch and create additional VLANs.

The subnetting of the network is intuitive and easy to understand, but it is not that simple to implement to other devices when they join the network as there is no DHCP server configured. The reason I have not configured an DHCP server is due to the fact I want the full control of their routing path, especially now when the VLANs were created. In other words, I want every department/VLAN differ from each other by looking at their unique class B IP address and differ every user/worker from one to another inside one department by having a unique class C IP address. Certainly, these IP addresses are fully controlled by the router which owns for the entire LAN the private IP address of 192.168.0.0 to reduce the costs as the firewall converts to the public address owned by the company. Moreover, the LAN IP address prefix size is 26 with the subnet mask of 255.255.255.192, because there are no more than 60 users/devices per department, thus the remaining 3 network addresses with their usable host range addresses can be used when the company has the resources to expand their business and create other LANs for other purposes.

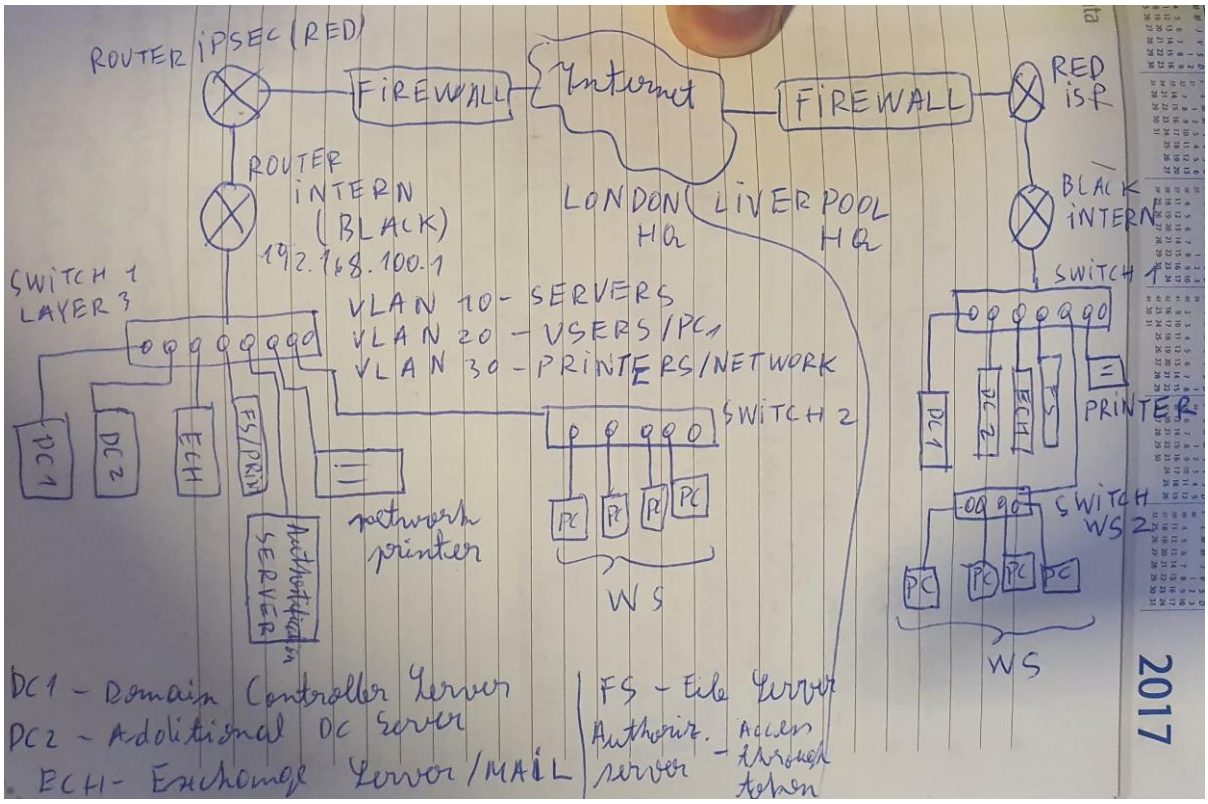
The rule of assigning static IP addresses to newer devices is accordingly: the LAN network IP address is 192.168.0.0/26 with the default gateway to router 192.168.1.1 and DNS server for London 1.1.1.1; once the global settings are applied, based on what VLAN interface is the device is connected to, the IP address template is: **192.168.<VLAN ID no.>.<device available no.>**. For instance, Management Worker 1.1 is going to be assigned with the static IP address of 192.168.20.11/26 as it belongs to VLAN 20, up to the 50th Management worker with the IP address of 192.168.20.52/26.

As for the servers, for each specified name of its purpose, that service is getting activated. By default, a server can have multiple services active in the same time, but this will slighty reduce its performance compared to being focused on only providing one service. For the File sharing and storage server,the Trivial File Transfer Protocol (TFTP) as well as the File Transfer Protocol (FTP) will be enabled. With the requirements from the Directors, only the senior management staff will be able to write and read. The workers from every departament they can only upload files via TFTP command, leaving the Directors to review what they exported and delete, modify, rename and all the other permissions. All of these exchanges between the client pc and server is protected through a user authentification. Based on their account, they are granted certain permission for the server. For the Exchange email server, both SMTP and POP3 protocols will stay enable, as SMTP sever allows the user to send the email from their device and store it or forward it to another SMTP server based on the domain name and destination address, remaining that POP3 to organize the emails stored in the server and forward them to the correct user.

Shifting the attention to the Liverpool office network, the configurations explained above is adapted for their department requirements.

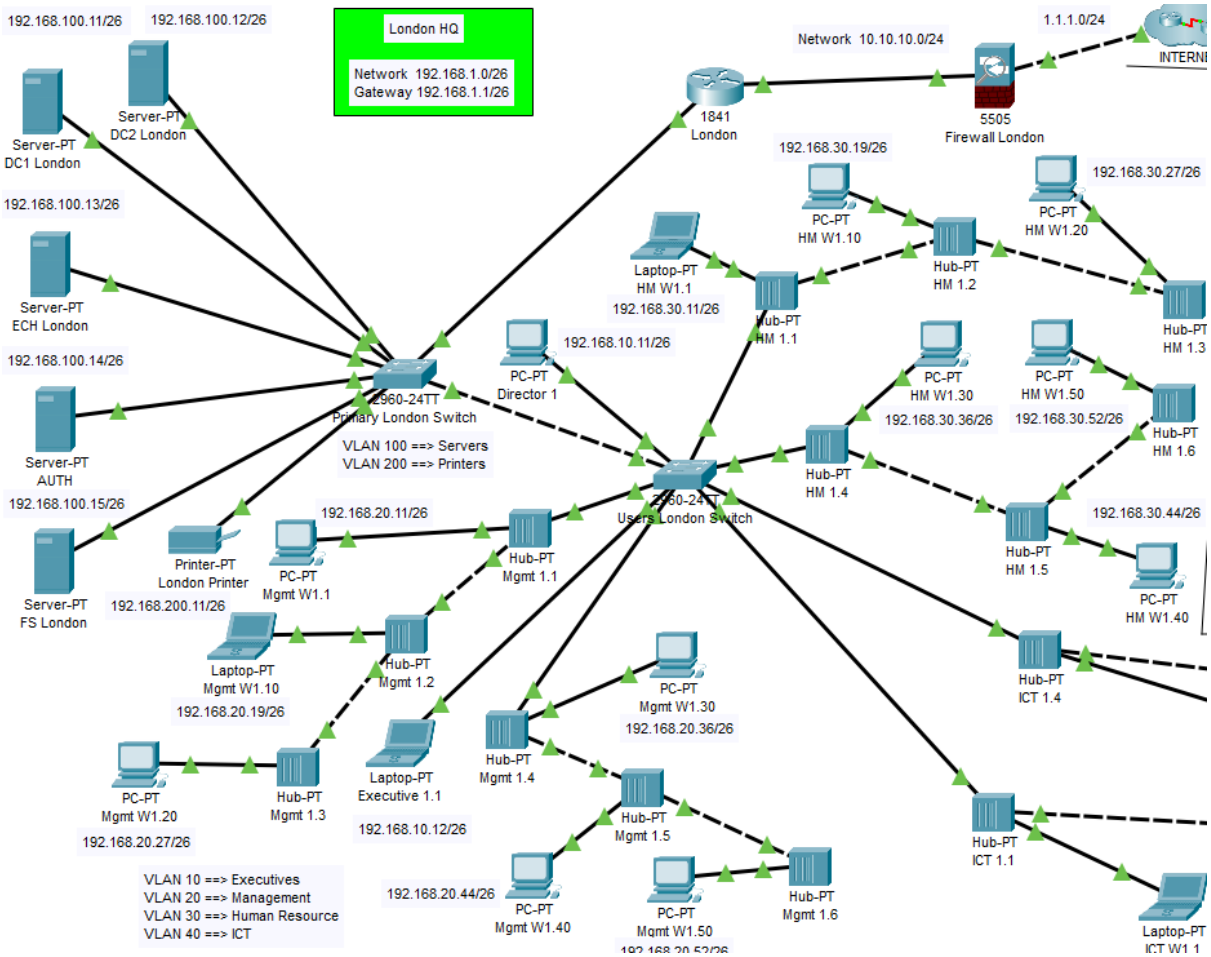


With the initial implementation configurations finished, the networks can receive their update of improving the stability and adding extra layers of security. Below, it is the illustration of post-implementation design. Domain Controller Servers are included in both London and Liverpool locations, together with printers when the company require to print documents. Moreover, an Authorization Server will provide the VPN users with a token to register.



When buying another switch to include in a network, there are 2 options available. The first one is buying a multilayer switch as showed in my design and configure the INTER-VLANing communication through its additional layer or buying a normal switch like the one already owned and configure the INTER-VLANing communication through the router using dot1Q encapsulation protocol. Multilayer switch is much more recommended for complex networks, because ensures an increased and secured longevity over time with a decreased probability of a network instability or crash. Buying another normal layer 2 switch requires enabling of the VLANs Trunking Protocol (VTP) which can manage substantial amounts of VLAN domains, but in case if something goes wrong during the maintenance configuration, the whole LAN system may become unstable and crash. VTP is only recommended for small network environments; its old architecture protocol is not suitable for bigger network environments where devices can be often replaced with new ones.

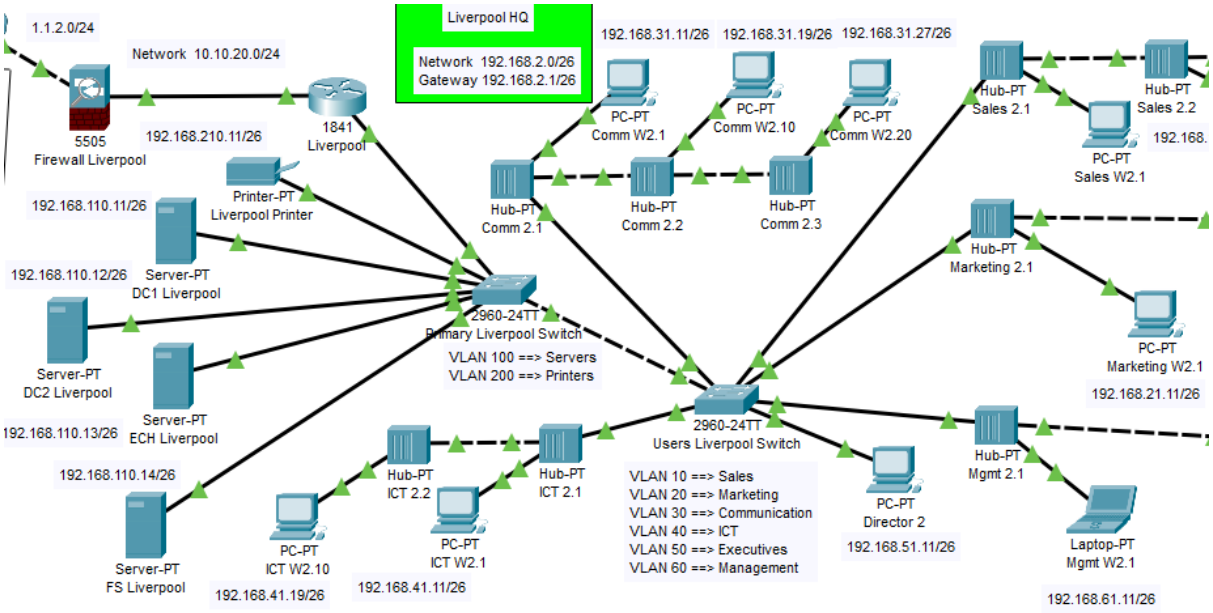
In an attempt to simulate the network to make sure the new design works, the VTP configuration will be used, but in the real network environment the multilayer switch is getting bought as it costs the same as a normal one.



The Primary Switch London provides 3 major VLANs: VLAN 100 the servers, VLAN 200 the printers or any other analog devices and the trunked connection to Users London Switch. With this separation, the Liverpool office users connected via VPN will get access only to the servers as the firewall sets the path of the outside towards them. The only server they will access first is the Authorization Server which will issue a token to the user who accessed the network, verify their identity and grand free roam to other servers if they have permissions. For the technical director who has the 192.168.10.11/26 IP address has granted access everywhere as a static ACL route for his address has been issued for all servers. He does

not require token to connect via VPN to Liverpool as the firewalls recognize his translated private IP address (he gets a unique public IP address when his private one gets through NAT).

The Liverpool network gets the similar upgrade in terms on switching. The Primary Liverpool switch includes the servers and printers, and the Users Liverpool Switch all the departments where the workers conduct their activities.



The Domain controller servers from both locations require regular maintenance to ensure the integrity of the users' accounts within the company. This may include to check every user's data authentication is kept safe and cleared occasionally after the Director analyzed their activity to avoid flooding the server with unnecessary outdated information.

Costs and Maintenance

The cost of the implementation may vary depending on where the devices are bought, including taxes or transport fees. The following prices are taken from the "Attributes" tab of each device from the packet tracer network topology. Both locations will need additional hubs to meet the criteria of including the specified number of workstations per department. London office will require 15 hubs in total to include all the 150 workstations from the network, meanwhile Liverpool office will only need 7 for its total of 30 workstations. One hub, according to packet tracer, costs 20 dollars by default. In total, around 440 dollars is going to

be spend for both offices. As for the switches, servers, and printers, both locations will need to feature one multilayer switch and printer, and two new servers for domain control. Occasionally, the multilayer switch can reach to a huge price depending on what features are included, but for this company a 3560-24PS multilayer switch will be enough satisfy the network needs, and it comes at the same price as a regular one, 1500 dollars. Adding up the price of one server, 2000 dollars, multiplied by four as both locations need an extra of two, a total of 8000 dollars. Two printers are 3000 dollars, set default by packet tracer.

Adding every device up, that would be a total of 14440 dollars, converted to Great Britain pound, around 11775 pounds for the networking devices. As it was mentioned, this price can be even higher or lower based on the market and the location from where are bought.

As for the public IP network address, there is an hourly fee of owning such one. One public network address is charged around 0.004 dollars per hours, resulting in a total of 0.008 dollars per hour for the two public network addresses (1.1.1.0/30 and 1.1.2.0/30).

In terms of further maintenance and upgradation, regular network audits can ensure compliance to the network security policies by preventing unauthorized intruders inside the firewall, routers, and servers. These periodic scans should be as frequent as possible, as once every two weeks or less by authorized IT engineers. One aspect of extreme high importance during an audit is updating the routers and firewalls to the latest patch available from the manufacturer, as malwares and malicious data adapt to newer infrastructures, putting the outdated devices in big danger of becoming targets of such attacks. After the network devices get the latest patch, the IT maintenance engineer needs to merge the older configuration with a new one by changing the encryption and password details to use the up-to-date protocol standards. According to SMB Technology. Published on 25 Aug 2012. Maintaining Network Security. Shaw Technology website. Some of the details were taken from here.

Project Management and Planning

Throughout meetings with managing and technical directors, multiple targets and requirements of great interest were established with a focus on updating the security structure of the network in both locations, so that the company can perform their corporate activities in a safe environment. The first meeting took place on 15th of March, where the directors introduced the stage of both networks at that time, explaining their purpose within the company. As their concern was updating both network to a more secure and reliable system, I received a series of requirement specifications to include while planning for a strategy. All requirements are to be accomplished by the deadline of 13rd of May as the Directors mentioned.

Considering that Directors mentioned a start and an end for their networks to be upgraded, I

will arrange my schedule in such a manner that the solution is implemented in packet tracer by the deadline, remaining for client's IT department to implement it in the real environment. When planning a network installation, there are six phases to take into consideration:

- Gathering information on the project's scope and existing infrastructure. In my case, I require to arrange more meeting with the client to understand what they really want to achieve.
- Making purchasing decisions. After getting sufficient intel about their network goals, I will make the appropriate decisions of what is required to buy based on research.
- Ordering equipment eight weeks prior from the deadline to have enough time to install, configure and assess the devices behavior along with the existing network.
- Configuring and installing the new equipment, then evaluating its connectivity and functionality.
- Gaining client feedback and acceptance.
- Informing the client's IT department for ongoing maintenance and support.

According to Greg Schaffer. Published on 23 Feb 2009 8:00 GMT. Project Management for Networking Greeks. Break down project work. Computer World website. Some of the ideas in the bullets were taken from here.

I proposed another meeting with the directors on 22nd of March to establish detailed requirements for what they want to expect and how much they are willing to spend if it is the case of buying new devices. After getting all the information needed, following week at the last meeting with the directors on 29th of March, I introduced my plan of action indicating the steps are going to be followed by the IT team when they will have to implement the network in the real environment, as well as the cost of the new devices and necessary maintenance at the end. With the agreement of the directors, I ordered the equipment on behalf of the company, with the expectation of get it delivered by next month.

Meanwhile, I worked of projecting the networking updates on packet tracer. Within the first week of April (5th to 12th), I simulated the initial design before update, applying the VPN, firewall configurations and subnetting both networks, following by the succeeding week (12th to 19th) to write in my report the progress and let the directors know the project's status. On the third week of April (19th to 26th), it was time to upgrade the network by adding the devices that were about to arrive and configure them so that the IT department can easily maintain and add newer devices in the future. As the task was much heavier than the previous, the final updated design was finished around 6th of May. On 10th of May, I presented my updated network project in front of the directors, giving the impression that it is ready for the real-world implementation.

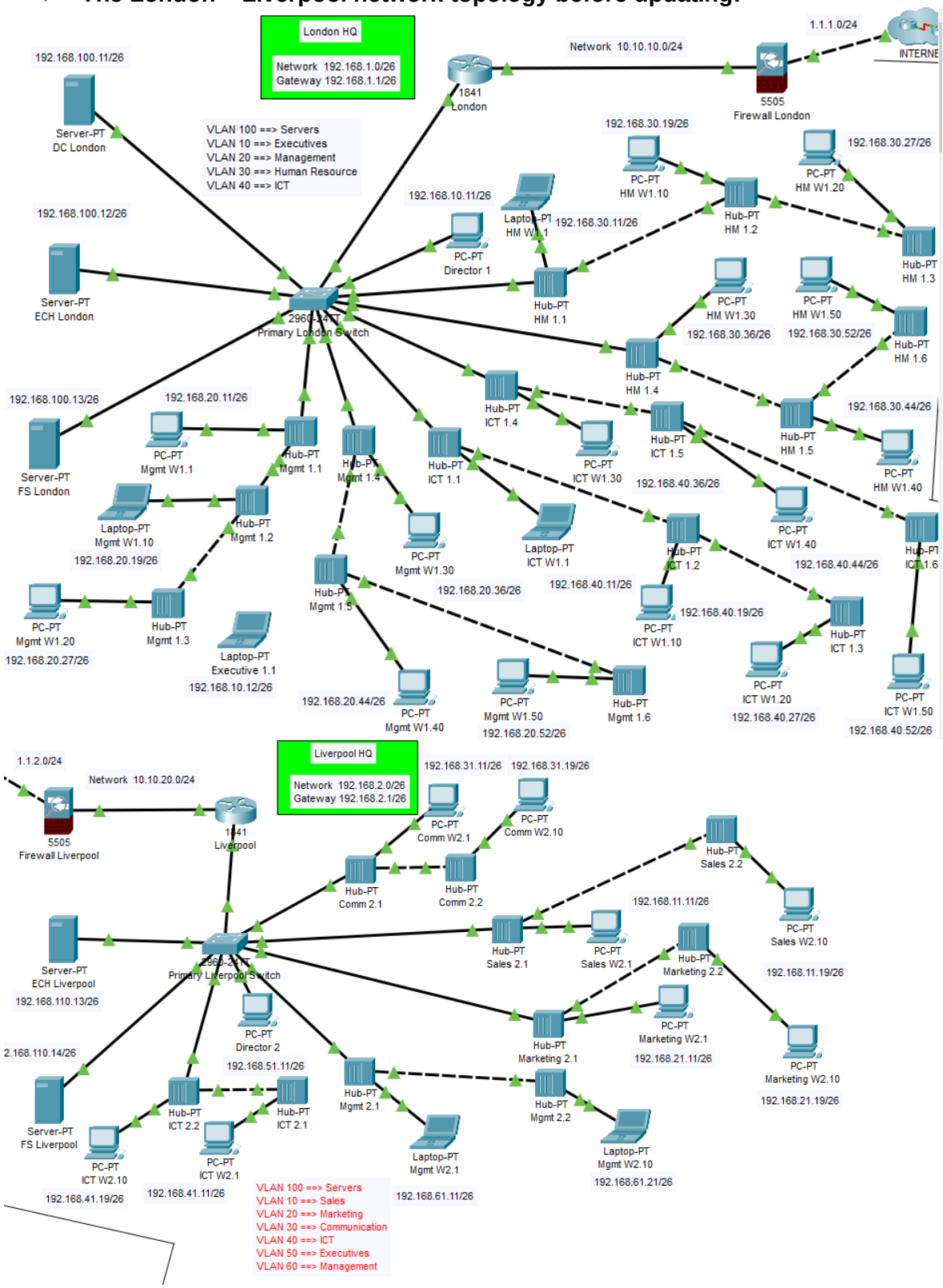
Discussion and Conclusion

The final network design can be enhanced in various techniques, such as replacing the firewall infrastructure or creating their own VPN source to get full control of their flow of data and hide it while pass through the ISP. During the simulation on packet tracer, I tried to include as much reliable configuration as possible, based on the knowledge accumulated during the labs. A substantial challenge was implementing the VPN infrastructure through the ISP and then configuring the firewalls to allow certain addresses from outside to access the local network. Not only it was extremely difficult not having the necessary knowledge to configure such devices, but their adaption within my network made it almost impossible, because if one protocol is not configured correctly, the whole system might go down.

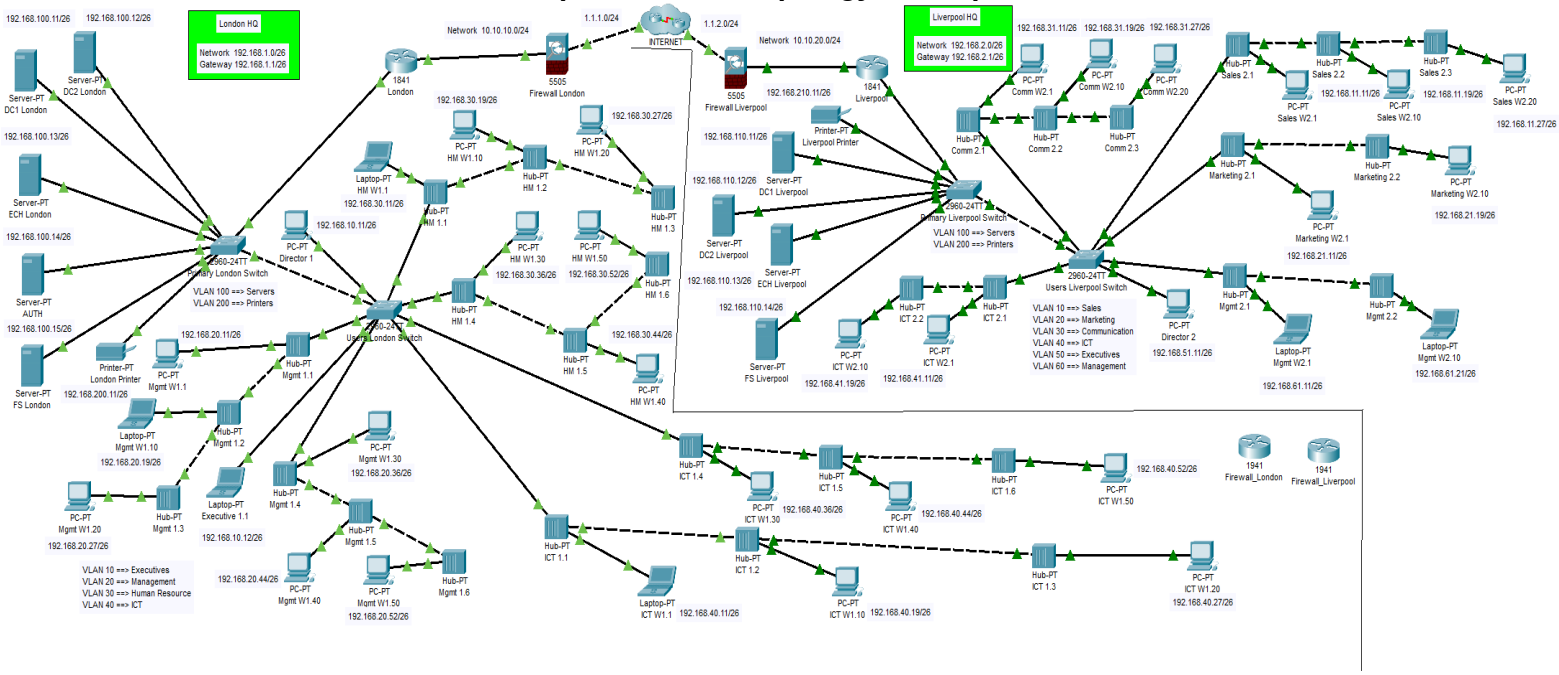
My goal for this network was to include as many security features as possible to meet the client's expectations, but since I encountered some devices limitations through packet tracer and not being able to properly configure them, I decided to release my updated network design as it is. Many improvements and optimizations with the required maintenance can be made from this point, but the main part is that this assignment taught me how it feels like to work for a company and how to plan an efficient strategy to deliver the best possible product for my client, based on my knowledge in the field.

Appendix

- **The London – Liverpool network topology before updating:**



- **The London – Liverpool network topology after update:**



- **The packet tracer simulation files can be reviewed and downloaded from my Google Drive (there are 2 files – "initial" is before update and "post" is after):** https://drive.google.com/drive/folders/1hupyJLpJyNgMAvxJQvLA6KjDNeC9M2r6?usp=sharing

References

- Laboratory materials including subnetting, routering, Inter-VLAN communication and general knowledge of using CLI commands.
- Lecture Notes and Assignment sheet.
- According to Stephen J. Bigelow, Senior Technology Editor. Published on 27 Oct 2008 Network design considerations checklist for providers. SearchITChannel website: https://www.techtarget.com/searchitchannel/feature/Network-design-considerations-checklist-for-providers
- According to Stephen J. Bigelow, Senior Technology Editor. Published on 27 Oct 2008 Network design considerations checklist for providers. Problem identification. SearchITChannel website: https://www.techtarget.com/searchitchannel/feature/Network-design-considerations-checklist-for-providers
- According to Cisco Press. Published on 3 Oct 2017. IPsec VPN. Cisco Press website. https://www.ciscopress.com/articles/article.asp?p=2803868

- According to SMB Technology. Published on 25 Aug 2012. Maintaining Network Security. Shaw Technology website: https://www.shawtechnology.com/maintaining-network-security/
- According to Greg Schaffer. Published on 23 Feb 2009 8:00 GMT. Project Management for Networking Greeks. Break down project work. Computer World website: https://www.computerworld.com/article/2550814/project-management-for-networking-geeks.html

- Research was realized while reading these websites:
- https://yourbusiness.azcentral.com/five-things-considered-designing-network-11153.html
- https://www.logitrain.com.au/blog/network-design-steps.html
- https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/#:~:text=to%20VPN%20tunneling.-,The%20Three%20Main%20Types%20of%20VPNs,site%20VPNs%20for%20corporate%20purposes.
- https://blog.symquest.com/questions-ask-before-designing-business-network-environment
- https://computernetworking747640215.wordpress.com/2019/11/22/how-to-configure-an-ftp-server-in-packet-tracer/
- https://www.geeksforgeeks.org/difference-between-network-address-translation-nat-and-port-address-translation-pat/
- https://ipwithease.com/layer-2-vs-layer-3-vpn/
- https://kalaharijournals.com/resources/141-160/IJME_Vol7.1_159.pdf
- https://www.calculator.net/ip-subnet-calculator.html
- https://www.youtube.com/watch?v=uau3uiETdqY (Domain Controller explanation)
- https://www.youtube.com/watch?v=qij5qpHcbBk (NAT explained)
- https://www.youtube.com/watch?v=2-Dq0GlBka0 (IP outside and inside explained)

- During the simulation through packet tracer, these tutorials were used:
- https://www.youtube.com/watch?v=yBgWpU1-lX0 (NAT configuration)
- https://www.youtube.com/watch?v=lLbn6Ag0dd4 (TFTP server configuration)
- https://www.youtube.com/watch?v=Mk5WUsHOK0Y (FTP server configuration)
- https://www.youtube.com/watch?v=Mk5WUsHOK0Y (Firewall configuration)
- https://www.youtube.com/watch?v=Z7LwU6H5IGE (IPsec tunneling configuration)
- https://www.youtube.com/watch?v=ZefJNVr7AAU (STMP/POP3 configuration)