ECE 407 Final Report

Alan Palayil

ECE 407

TA: Ziru Chen

Team Members: Matthew Ostrowski, Nikhil Aditya Chaganti, Ravishankar Natarjan

ABSTRACT

Throughout the project I were tasked to set up the overall topology for 4 integrated LANs into a WLAN. The 4 LANs consisted of Company A, Company B, Company C, and Company D. Within doing this many of the fundamentals of networking will be established. This includes- setting up routers, setting up all the fundamental servers (DHCP, DNS, FTP, WEB, EMAIL), using switches, establishing a wireless router for guest connections, etc. Though understanding the concepts of these devices is one thing, to physically configure the devices and all their connections is another. Using this project, it is essential I understand the practice of the device to ensure an efficient network throughout. Although many things were deemed successful there were certain obstacles which were encountered were discussed within the group and resolved through further practices and studies.

INTRODUCTION

To begin our exploration into network as described in the problem statement, it is essential to understand the background as to which this work exists. Something very essential to this project is understanding the DHCP server. DHCP is Dynamic Host Configuration Protocol. It is a client/server protocol which may automatically provide an IP host with its IP address and other related configuration information such as the subnet mask, default gateway, DNS server, etc. Essentially a DHCP server was used to auto-assign IP addresses on PCs and phones for the departments. Although there are a few ways to use DHCP for our report, I used the departments head router to do so. Another fundamental of our topology was grouping together the DNS/FTP to a switch then the WEB/EMAIL servers to a different switch which was connected to the router going out to the WLAN. I did this as the DNS/FTP servers are internal servers defined specifically for each of the companies or universities. Rather than the WEB/EMAIL servers which are external servers. I want other companies to be able to access the web and email servers of another LAN through the WLAN. Another fundamental to our topology was having a main router in the center of all LANs. This was used for traffic flow of the companies. It is the crossroads to get anywhere you want in the topology. Essentially it is the center for the extended star topology of each of the LANs. This is essential to ensure that all packages may get to any given location within the company.

SYSTEM DESIGN

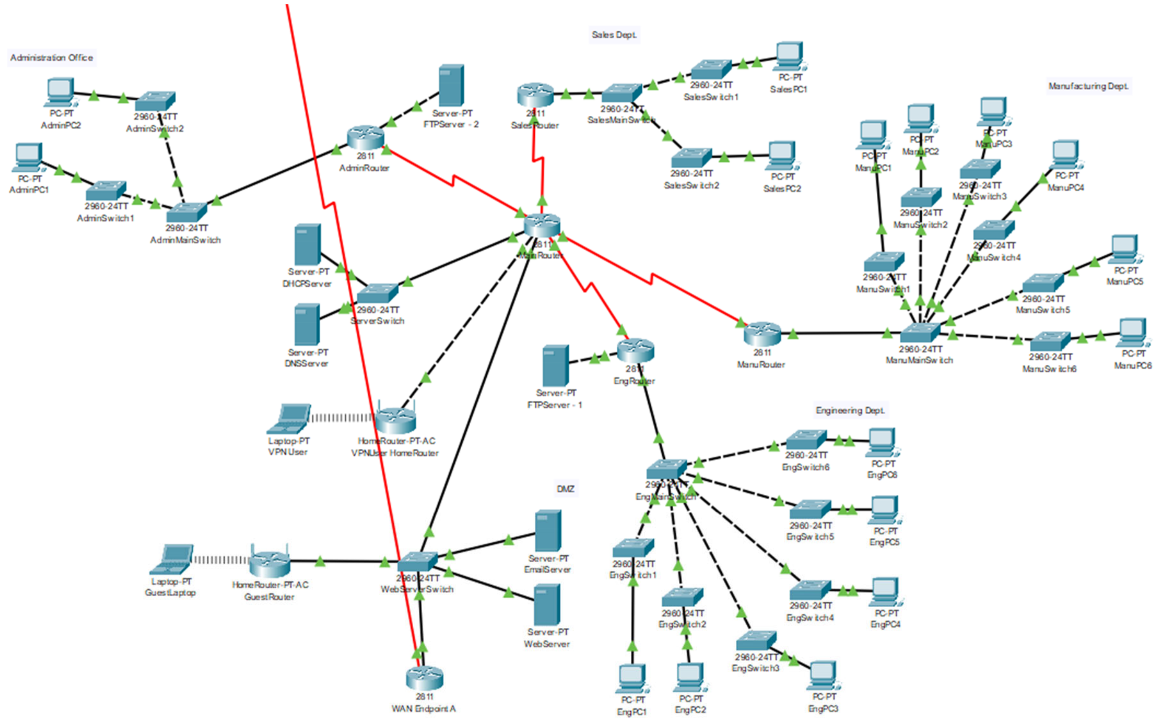
For the basic topology of our overall project, I have a WLAN which holds a line topology, connected the 4 LANs, Company A, Company B, Company C and Company D. Each of these LANs follow an extended star topology which branches from a main router connected to the department routers, a switch which holds the DNS/FTP servers, and a switch which holds the WEB/EMAIL servers along with a connection to the head router of the WLAN for the company. Within all the companies, the central router is also connected to a wireless router which acts as the guest WLAN for the companies. Within our LANs for the companies, I used routers as the DHCP server for the departments. I had to properly divide the DHCP to account for the IP range of the company described in problem statement. For example, Company D had a range from **216.244.158.0** to **216.244.167.255**. Within this range I had the router of the engineer's department establish an IP range from **216.244.158.0-216.244.158.254** for the PCs and phones using static IP addressing and DHCP. Similarly, I divided up the other departments in all companies. The configuration of addressing tables for each company may be seen in the tables listed in the Appendix at the end of the report.

It is also to be noted that for each of the departments I diluted down the overall number of PCs and phones (if needed). Although on the cisco packet tracer itself these numbers of the actual PCs are diluted down, the configuration and set up can handle the actual number of persons in the department, guests on WLAN, etc.

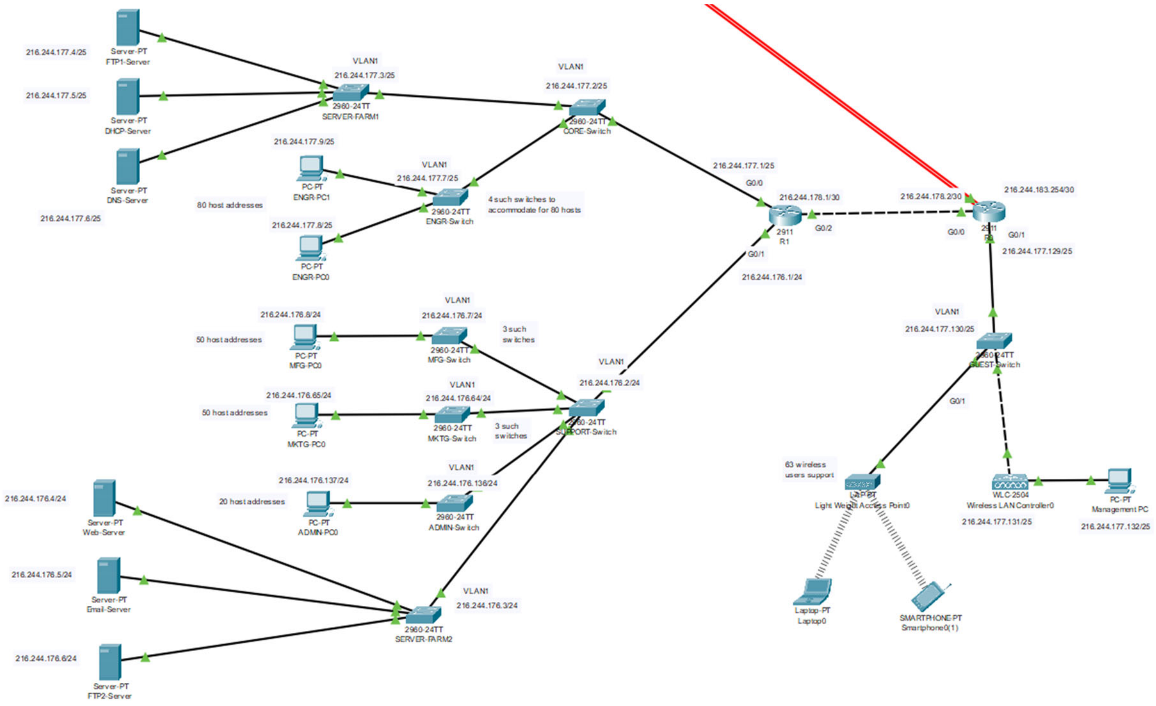
IMPLEMENTATION

Below you will see screenshots of our actual implementation into the cisco packet tracer:

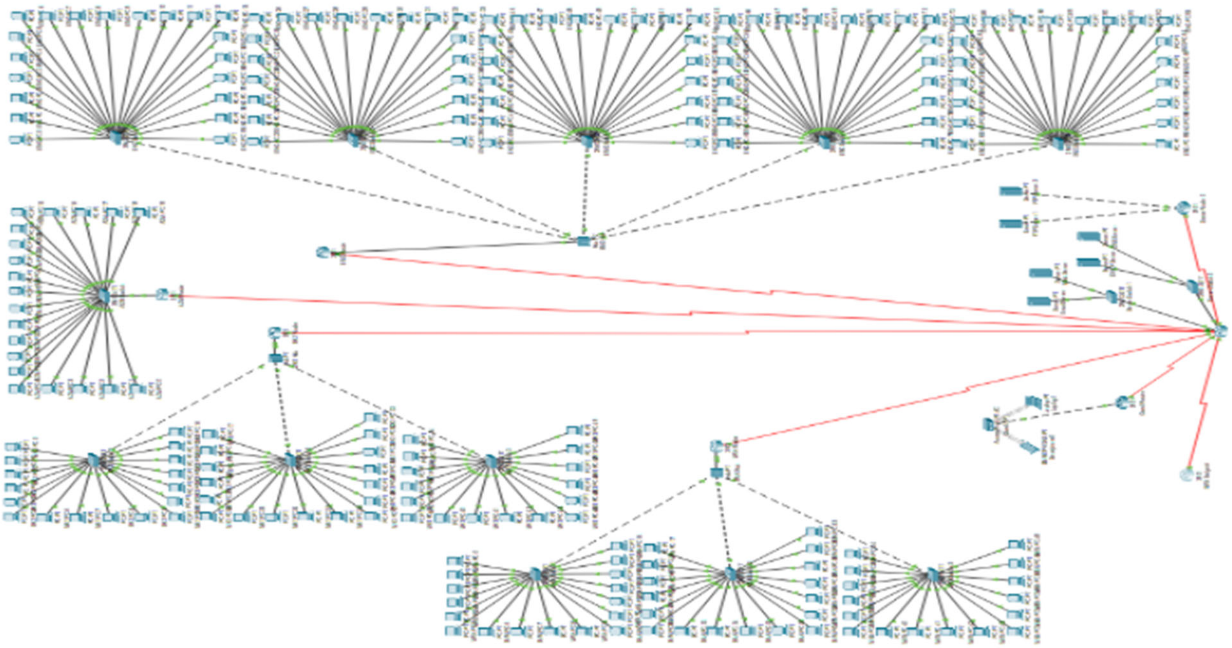
Implementation of Company A (Nikhil Chaganti):



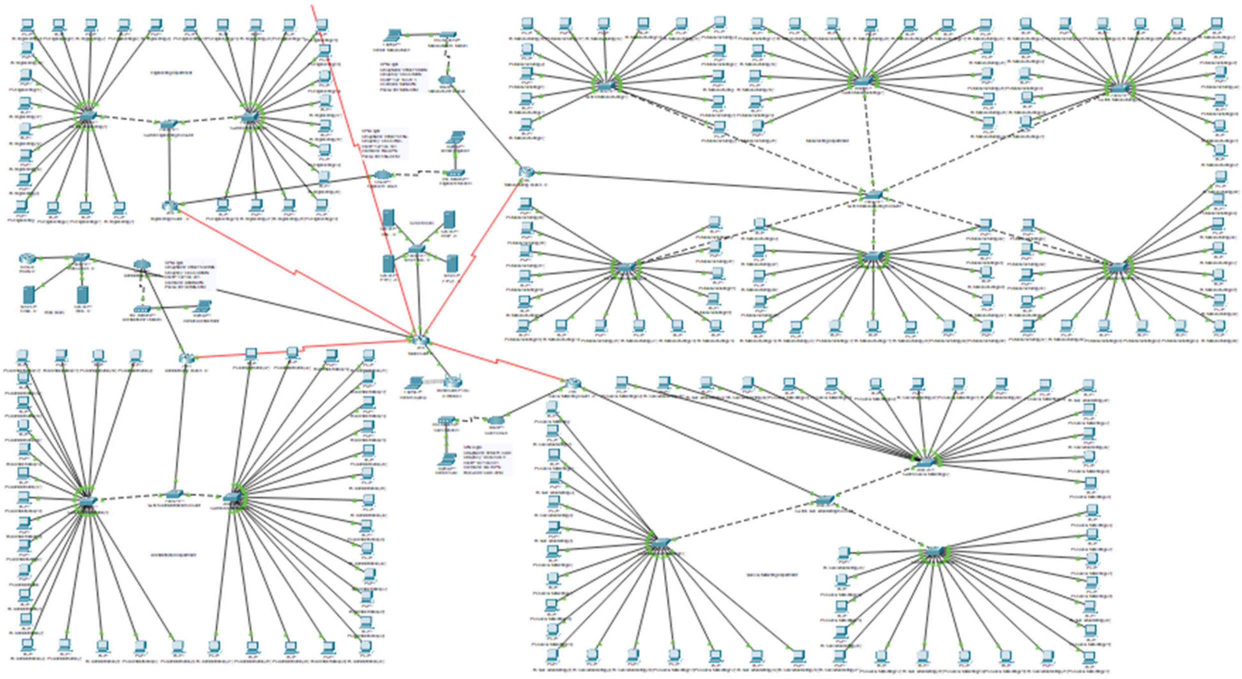
Implementation of Company B (Ravishankar Natarajan):



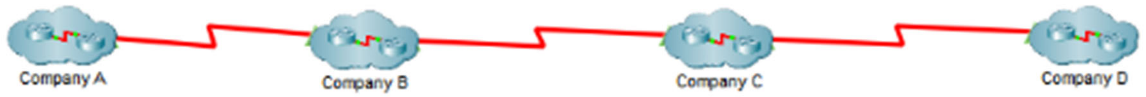
Implementation of Company C (Matthew Ostrowski):



Implementation of Company D (Alan Palayil):



Overall Topology of Network:



RESULTS AND DISCUSSION

1. You should justify every design decision in terms of optimality.

   I worked on assigning IP addresses through DHCP, but I was facing issues every time I started the file again. So each department's PCs are assigned statically and to display DHCP assignment, I have implemented it on the VPN IP addressing. All servers are properly able to communicate within the network of each LAN. Although I did not test it for each PC individually, I tested on one PC per department to ensure that they are able to access the FTP server (when needed). ACL is implemented in each of the department's routers to have the restricted list within to have the router restrict it at the beginning before the department tries to communicate with a restricted server. I also ensured that PC's are able to access the DNS server and Web server under the Web browser service and properly receive information from the web pages which have been created. For the emailing service, I signed into the email server, sent out a sample email, and properly received it from another PC in the network. I replied and this was properly received on the original sender. For the guest WLAN, I was properly able to connect to the wireless router and get dynamically routed an IP address on the network. From here the device was properly configured into the extended star topology of the LAN. All PCs were statically assigned. Finally for the VPN, I used the following config- aaa, isakmp, and crypto to set it up. I made a sample cloud for a remote employee to sign into their department remotely with the given VPN credentials.

1. Include a snapshot of your network topology from cisco packet tracer.

   For the basic topology of our over WAN, I have 4 LANs, Company A, Company B, Company C and Company D connected using the RIPv2. Each of these LANs follow an extended star topology which branches from a main router connected to the department routers, a switch which holds the DNS/FTP/DHCP servers, and a switch which holds the WEB/EMAIL servers along with a connection to the head router of the WLAN for the company. While selecting the routing implementation to use, I discussed how static routing is a form of routing in which a router uses a manually configured routing entry instead of data from dynamic routing traffic. In certain cases, a network administrator manually configured static routes by adding entries to a routing table, although this is not always the case. Static paths, in contrast to dynamic routing, are set and do not change when the network is changed or reconfigured. It is worth noting that on a router, both dynamic and static routing are typically used to optimize routing efficiency and provide backups if dynamic routing information is not shared. Within our network I used RIP v2 to connect all the central components to the main routers. RIP v2 is helpful in that it keeps track of the closest router for each destination address. I manually input the networks which the packets can transmit over, and it does the rest.

Our network in Cisco Packet Tracer is outlined within the IMPLEMENTATION subsection of this report.

1. Explain in detail the following concepts, and reflect how they influence your design decisions:

. Functions of switches, hubs, routers, access points.

Throughout our network I used switches and routers but did not find a use in hubs or access points. Switches were used for many purposes throughout our design. They were used to manage traffic to each company, used to connect to the WLAN, assigned DHCP, etc. Overall, they were good for integrating end devices into our network overall. Switches use layer 2 switching to send and receive messages from the connected hosts, in most cases of our network, the routers. They can cache addresses which speeds up forwarding decisions. They also served as a connection point to end devices from our DHCP routers. Although in most cases you only see one switch connected to the DHCP router per department, note that there would be many more if I were not diluting down the number of employees. I did not use hubs as I dynamically assigned IP addresses and our main router was used as a relay router. I do not use an access
point although I use a wireless router to act as one, which also dynamically assigns an IP into our network.

a. Collision domains, broadcast domains.

The Collision domain helps to allow traffic to flow forward and backward. Although the Broadcast domain is a type of domain where traffic may flow all over the network. Along with that in the Collision domain, all the devices have access to other devices of other IP subnets. Although the broadcast domain is never limited to the specific IP subnet for all types of IP broadcasts. Within the collision domain packet collision occurs as multiple devices transmit data on a single wire link. While the broadcast domain uses a switched environment to broadcast, so no collision occurs although this may result in slower speeds.

a. Static routing, dynamic routing, and selective routing algorithms.

Static routing is a form of routing in which a router uses a manually configured routing entry instead of data from dynamic routing traffic. In certain cases, a network administrator manually configured static routes by adding entries to a routing table, although this is not always the case. Static routing is the case that I used with employees of University Z, while the rest was typically assigned with DHCP. Static paths, in contrast to dynamic routing, are set and do not change when the network is changed or reconfigured. It is worth noting that on a router, both dynamic and static routing are typically used to optimize routing efficiency and provide backups if dynamic routing information is not shared. Within our network I used RIP v2 to connect all the central components to the main routers. RIP v2 is helpful in that it keeps track of the closest router for each destination address. I manually input the networks which the packets can transmit over, and it does the rest.

1. Please describe the detail traffic flow when the following action is taken

. An employee in the engineering department pings the FTP server 1 of his/her own company.

If an employee in the engineering department pings the FTP server 1 of his/her own company, first the ARP request would go out which also uses STP to find the proper destination. The path will then originate from that PC to the switch which holds that department's PC connections, from that switch it goes to the engineering department's router, at the router there is an IP check by ACL for department's restriction and after it goes through the list and from that it goes to the main router of the company, then to the server hub, and finally into the FTP Server 1. It will then acknowledge this and send it back.

a. An employee in the engineering department pings the FTP server 2 of his/her own company/university.

If an employee in the engineering department pings the FTP server 2 of his/her own company, first the ARP request would go out which also uses STP to find the proper destination. The path will then originate from that PC to the switch which holds that department's PC connections, from that switch it goes to the engineering department’s router, at the router there is an IP check by ACL for department’s restriction and after it goes through the list and from that it responds back to the employee’s PC that it doesn’t have access to the FTP Server 2 and fails to ping FTP Server 2.

a. An employee in the administration department pings the web server of his/her own company.

If an employee in the administration department pings the web server of his/her own company, first the ARP request would go out which also uses STP to find the proper destination. The path will then originate from that PC to the switch which holds that department's PC connections, from that switch it goes to the administration department’s router, at the router there is an IP check by ACL for department’s restriction and after it goes through the list and from that it goes to the main router of the company, then to the server hub, and finally into the web server. It will then acknowledge this and send it back.

a. An employee in the administration department pings the web server of another company.

The traffic flow from our topology would go as follows if the network has already sent out the ARP signal and a path is known. Suppose an employee from Company C is pinging the web server of Company D. It would go from that user’s PC to the switch which holds that departments PC connections, from that switch to the administration department router, from that router to the main router of Company C which would pass it onto the web server switch of the company, after this it would go to the WLAN C router to WLAN D router of Company D. It would then go from the Company D Router to the web server switch which ends up being passed to the Company D web server. It then acknowledges this and responds back in a reverse path.

1. Explain why and how VPNs provide a secure tunnel between LANs?

Once an employee is outside the LAN, the employee doesn’t have access to the servers. A VPN encrypts the packets at the originating point, often hiding the data and information about that employee's originating IP address. The VPN server at some destination point, decrypting the data. In the company’s VPN it’s characterized by the same organization controlling both endpoints of the VPN. I implemented the VPN through AAA server which has Authentication, Authorization, and Accounting. The ISAKMP protocol is a framework for dynamically establishing security associations and cryptographic keys in an Internet environment. This framework defines a set of message flows (exchanges) and message formats (payloads). ISAKMP defines a generic payload for key exchange information. Using the IPsec and static crypto map, the define the policy of the data flows and the crypto peer to which that traffic needs to go. Thus, providing a secure tunnel between the remote user and LANs.

CONCLUSION

Overall, the experience of this lab report ensured that I understood the material previously mentioned in the practices. I had to ensure that I understood all the fundamentals and, in a way, take it a step further to show how these individual concepts all relate. For example, within setting up the DNS server, I implemented that within the DHCP so that not only were the IP addresses auto assigned but also a proper trace back to the DNS server itself. This project ensured that I took the fundamentals of all the practices and were able to build it into something from scratch. I was forced to look at the problem statement at hand and think about the best way to connect four companies which further had specifications within them. Although obstacles persisted throughout the project -some I was able to fix, others left for future studies. I deem that they are essential in the learning experience to encounter as they encourage us to further our research and see how to deal with these issues at hand, just like the real world. For example, when establishing the connections for Company D departments, within the building of the topology into the actual implementation of it into cisco packet tracer, networking fundamentals were utilized in whole throughout this whole project.