Sell Sell It LTD Networking Configuration

TNE10006

Sujin Jeong
Nicholas Anzellotti 101623877
Jared Speake

Company Information

Sell Sell It, is a small company that is requiring 5 VLANS. One of these will be a dedicated management VLAN used for switch and router management. The other 4 will be designated to Retail, Housing, Apartments and rental divisions respectively. The network topology needs to be a relevant LAN design including the use of a single distribution switch and 2 access point switches, each of which will hold 2 of the VLAN connections. The switches will be configured to use EtherChannel Bundling for redundancy and PVST+. The distribution switch will be forced to be the root bridge of the current configuration.

As this is a business with a reasonably large distribution network security is imperative and port security will be implemented on all switches. Following this a logical port allocation to quickly recover from faults will be applied ensuring that the switches are configured in a way that is simple for maintenance teams.

Subnetting Information:

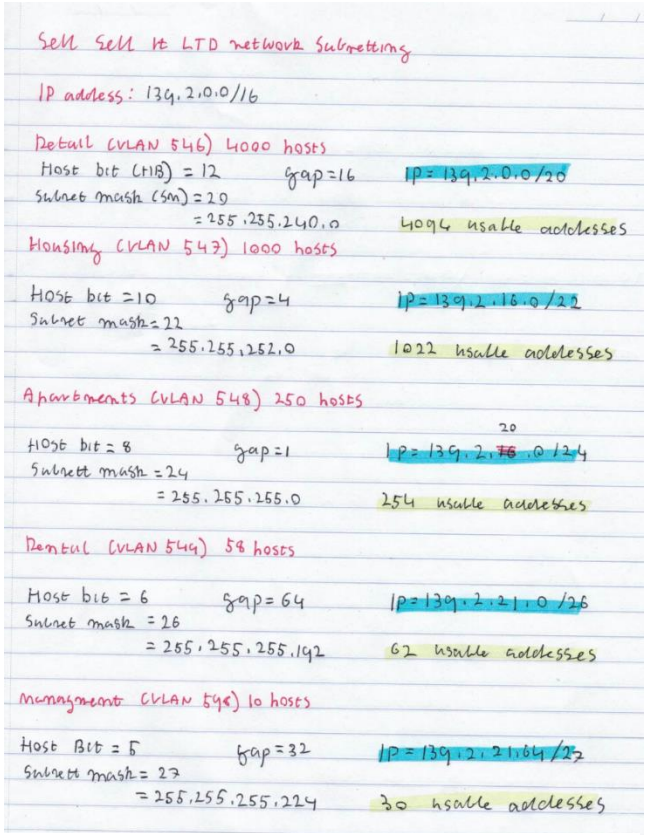

Figure 1: Subnetting Work

In order to subnet the current network properly we first had to analyze the number of nodes that are connecting to each VLAN and then properly allocate the subnets to sit within the IP Given. For this study the IP 139.2.0.0/16 was assigned to the team. This is a class B network which have us a wide range of addresses to work with if the company every requires to expand in the future. VLAN 546 held the department for **Retail** the number of hosts required were 4000. To ensure that we had over the amount that was needed we used the host bit of 12. This gave us 4094 usable addresses that we could assign for the VLAN. This gave us a subnet mask of /20 for retail and holding the default

IP of 139.2.0.0/20. Secondly the Housing VLAN was established. This VLAN required 1000 hosts so the host bit of 10 was selected. This gave us 1022 usable hosts for the VLAN. Adding on the gap then gave the **Housing** VLAN an IP of 139.2.16.0/22. Thirdly the apartment VLAN was established. This VLAN required 250 hosts so a host bit of 8 was selected allowing for 254 usable hosts. Adding the gap yet again gave the **apartments** VLAN an IP of 139.2.20.0/24. Finally, the last public VLAN was the rental VLAN. This required a use of 58 hosts. To ensure that there would be enough a Host Bit of 6 was selected. This allows for 62 usable hosts and presented the **Rental** IP to be 139.2.21.0/26.

The management VLAN was configured with scalability in mind. While the original plans were to attribute only 10 hosts for scalability reasons, we applied a much larger subnet providing over double the amount of usable IP's. We used a Host Bit of 5 allowing for 30 usable IP addresses. This will allow the network to expand and still maintain this management subnet for over double the amount of hosts present. Applying this gave the **Management** an IP of 139.2.21.64/27

Routing Table:

Name	IP Address	Subnet Mask
Retail (VLAN 546)	139.2.0.0/20	255.255.240.0
Housing (VLAN 547)	139.2.16.0/22	255.255.252.0
Apartments (VLAN 548)	139.2.20.0/24	255.255.255.0
Rental (VLAN 549)	139.2.21.0/26	255.255.255.192
Management (VLAN 598)	139.2.21.64/27	255.255.255.224

Logical Topology:

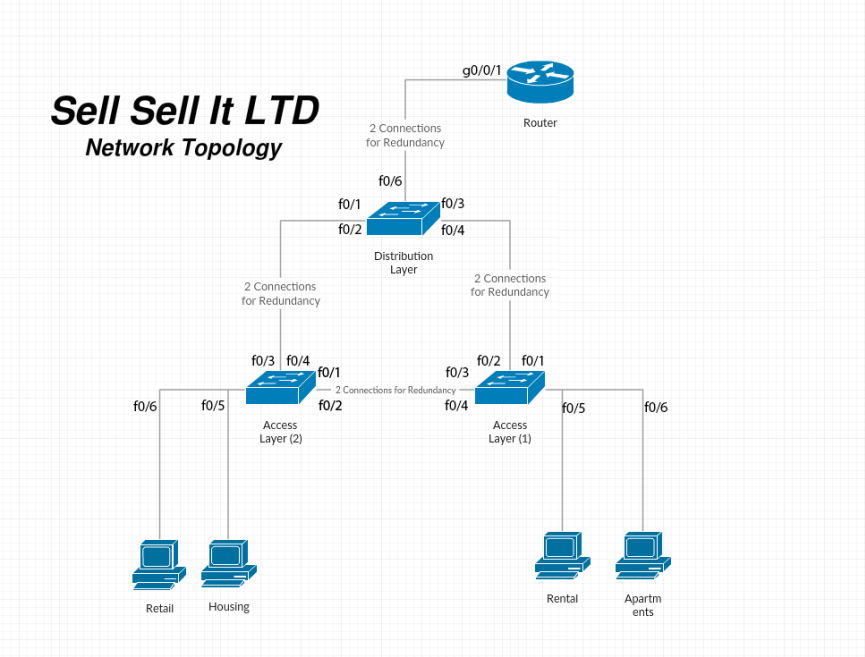

Figure 2: Logical Topology

Design Discussions:

Port allocation was a very important point for the development of this network. It was important that the network was easily maintainable and can be repaired and troubleshooted quickly if an error was to occur. While we did implement further solutions to mitigate errors from happening, we wanted to ensure that from a base level port allocation was easy and made sense to the maintenance team and ensured that no ports were “randomly” allocated. As such the logical topology in figure 2 was created. The basic outlook of the port allocation is that the first 4 ports of each switch are dedicated to connections with other switches. This way if a cable was to be a fault it can easily be identified from the first 4 switchports if the fault was to be at the switches. The connections are also in numeric order. In order to achieve redundancy two links would need to be connected as such the f0/1 and f0/2 ports would be connected to ensure that it is as simple as possible for maintenance. Following this all other ports that were not in use were shutdown to avoid any physical connections to the switches or routers.

Secondly, we wanted to implement a form of **security** for the switches and routers. Port security was the first area of concern for this. For each switch we applied a "sticky" form of port security. This would ensure that each time a new MAC address connects to the switch that it is saved to the switches NVRAM. This is configured to hold a max amount of 3 MAC addresses. If the maximum is exceeded, then the port will shut itself down to prevent further intrusion, this is configured for all 4 switchports as well as 5 and 6 for the access switches as they have nodes connected to them. While this couldn't be configured for the router to avoid any bruit force attacks to the router a timeout was set. The current timeout will allow for a max of 5 wrong guesses in 60 seconds before locking out the user for 60 seconds.

Remote Management:

While having physical security measures is important, we also had to implore the use of SSH to ensure that we could remotely access our switches and routers through any SSH client on the network. To do this a new user was created on all the switches and routers. To further ensure that the security of this server is not breached the passwords for both the router and switches remain different. They are presented as follows:

Device	Username	Password
Switches (DL1,AS1,AS2)	Sell-Sell-It	labpassword
Routers (R1)	Sell-Sell-It	SellSellItRouter

While these passwords do not follow a normal naming convention they remain different enough to ensure that only authorized users can access a specific device.

Spanning Tree:

Spanning tree is a protocol that runs on bridges and switches nominating which ports to disable and enable to avoid loops within the network. The network topology proposed made use of a distribution layer switch along with two access level switches. This meant that a large amount of bandwidth would be filtered along the distribution switch, so it was imperative that both links f0/1-4 remained active to ensure the shortest path to the router. To ensure this, the Distribution Layer switch (DL1) was configured to be the root bridge, this ensured that both links would remain active to both access point switches.

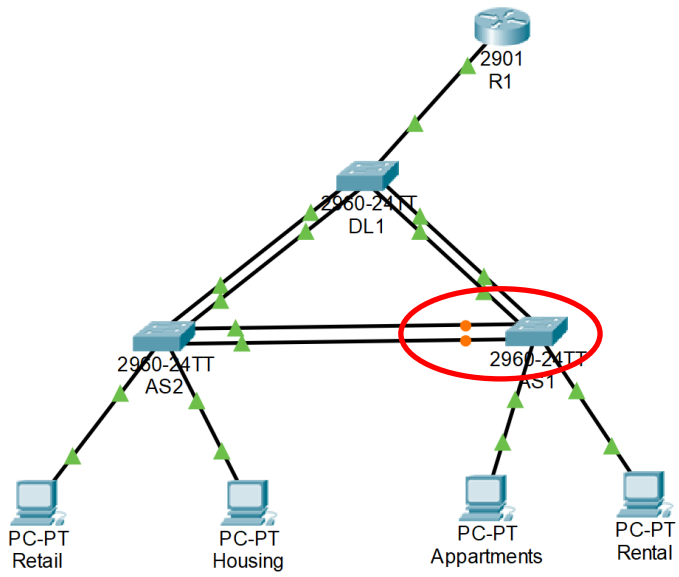

Figure 3: Spanning Tree Config

The links that were shut down by the spanning tree protocol to prevent these loops within the network were the links between the access layer (AS1 & AS2) switches. To achieve this allocation the priority of the distribution layer switch was set higher than the access layer switches so that in the "election" process the distribution switch would always remain the root bridge. Testing of this configuration is show later within this report.

Redundancy & EtherChannel

The final design oversight required was the use of redundancy and speed for the network. Both were implemented using "EtherChannel Bundling". The theoretic implementation of this technique meant that theoretically we would achieve double the bandwidth by attaching two physical connections to each switch and configuring them as a single logical interface, however this isn't always the case. This wouldn't necessarily double the throughput as data can only be sent as fast as the data is received this includes errors in communication, latency and specific layer 3 protocols being used. To enable ether channeling bundling first two "virtual" connections would need to be created at each switch. This was done according to the topology in figure one and three. Two physical connections were applied to each switch and each of these were configured as one logical (virtual) interface. In doing this we enabled redundancy over both physical connections. If one physical connection or cable was to fail the nodes connected to the switch would not fail as there would be a second physical connection supporting the data transfer. However, if a link logical link was to completely fail (Figure 4) the Spanning tree protocol would then enable the block ports

between the access switches as another fallback to avoid minimal downtime of the network. While this will however create a much higher traffic flow over one logical link it will avoid downtime while maintenance can troubleshoot the issue.

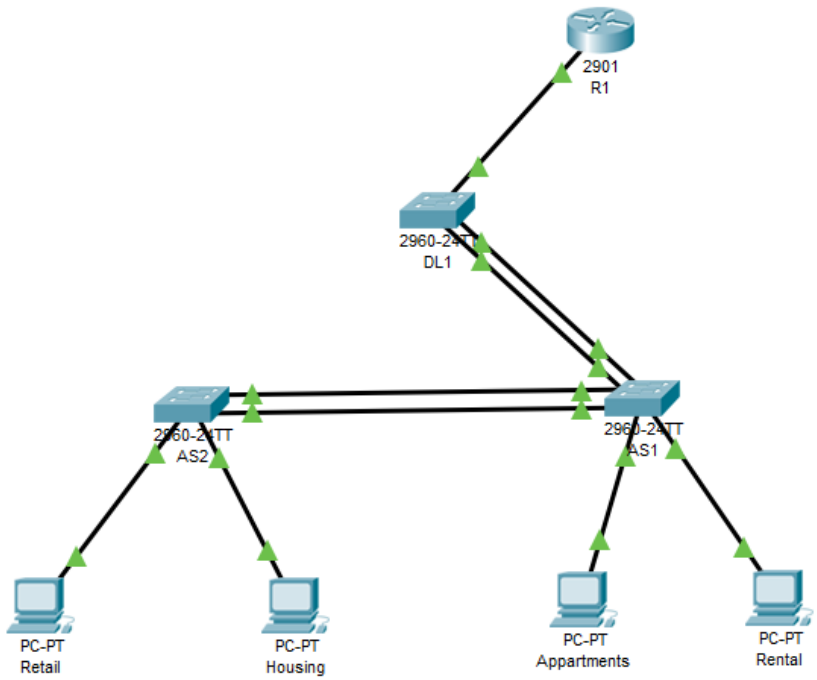

Figure 4: Redundant Link Config