Sell Sell It LTD Networking Configuration

TNE10006

Sujin Jeong 102442426
Nicholas Anzellotti 101623877
Jared Speake 102088752

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:

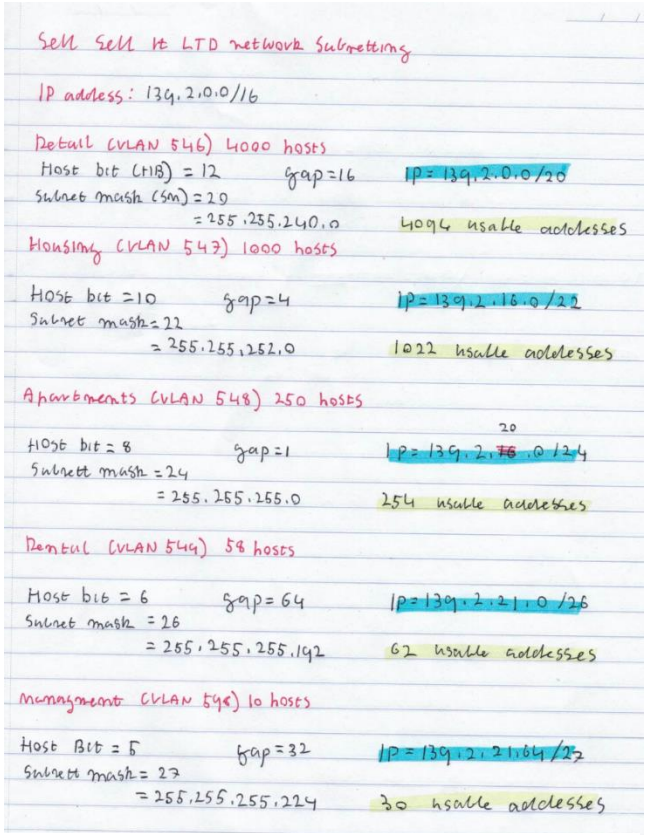


Figure 1: Subnetting Work

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:

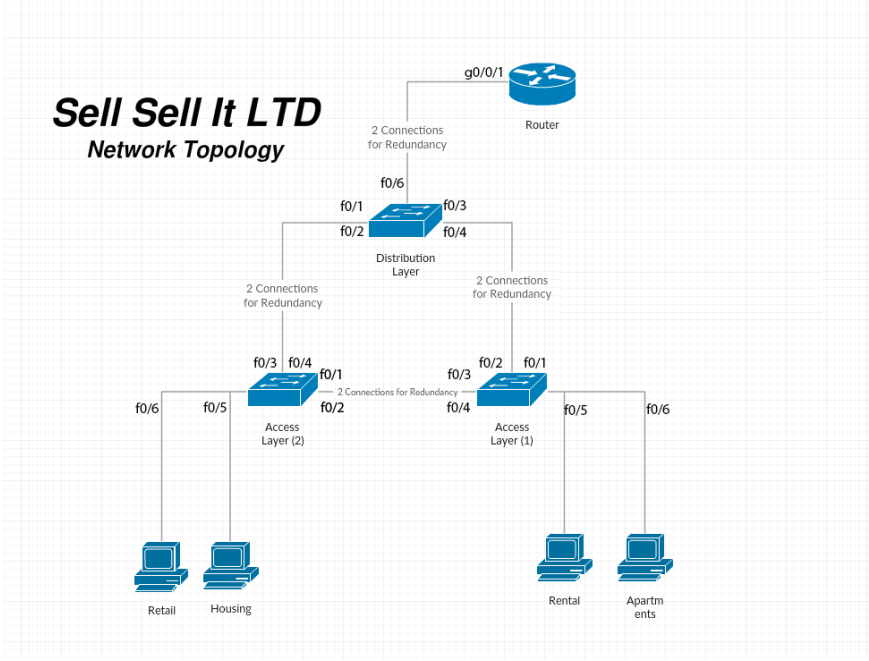


Figure 2: Logical Topology

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.

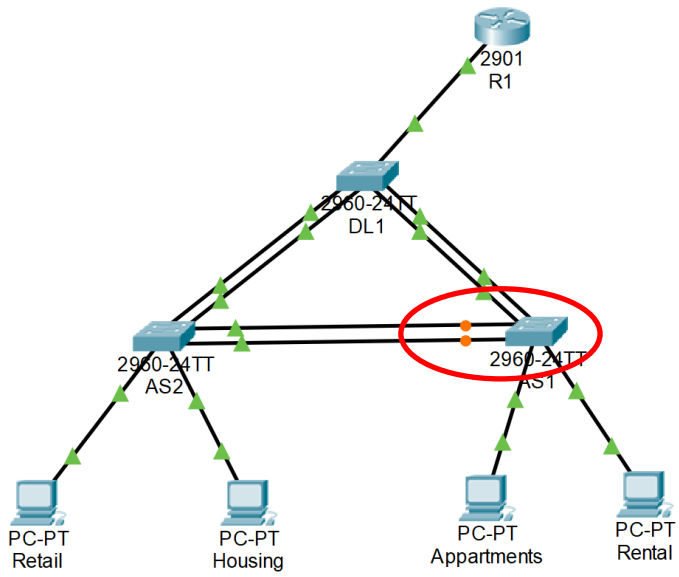


Figure 3: Spanning Tree Config

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.

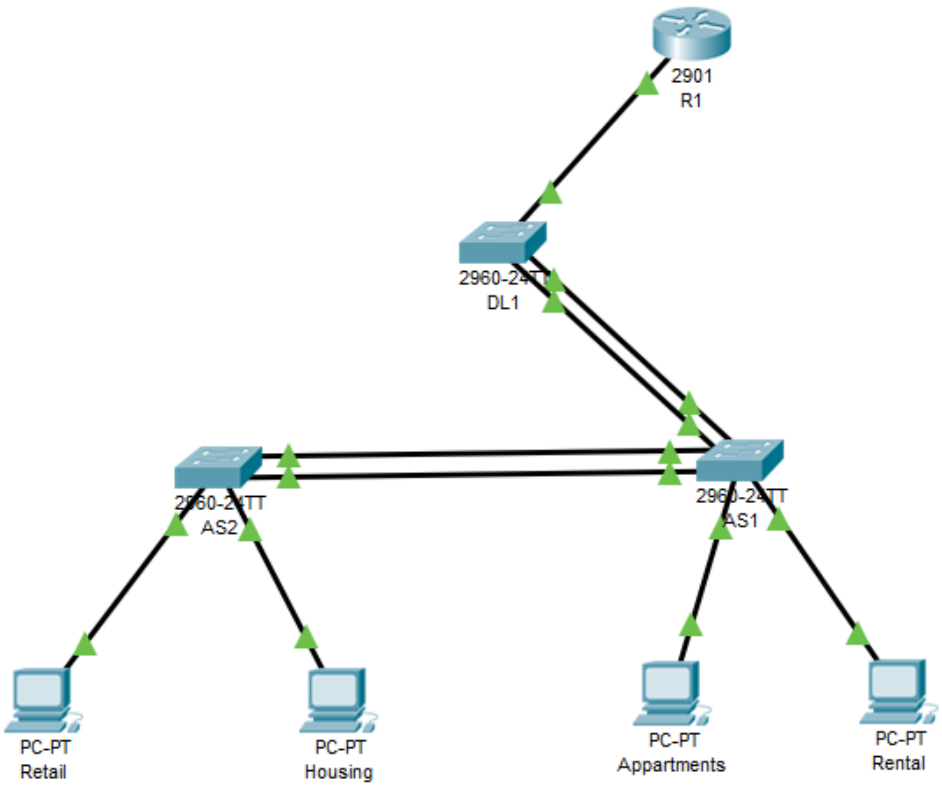


Figure 4: Redundant Link Config

Device Configuration Info

Device	Hostname	Interface Descriptions, Security, MOTD	Usernames	Passwords
Access Switch 1	AS1	-F0/1-6→ 3 MAC addresses set to sticky with a shutdown violation enabled. -Unused ports shutdown -MOTD = "Sell Sell It Access Switch 1 Contains apartments and rental hosts authorized access only"	Sell-Sell-It	EXEC Mode= labpassword SSH = labpassword
Access Switch 2	AS2	-F0/1-6→ 3 MAC addresses set to sticky with a shutdown violation enabled. -Unused ports shutdown - MOTD = " Sell Sell It Access Switch 2 Contains Housing and Retail Hosts Authorized Access only"	Sell-Sell-It	EXEC Mode= labpassword SSH = labpassword
Distribution Switch	DL1	-F0/1-6→ 3 MAC addresses set to sticky with a shutdown violation enabled. -Unused ports shutdown -MOTD= " Sell Sell it Distribution Switch 1 Authorized access only"	Sell-Sell-It	EXEC Mode= labpassword SSH = labpassword
Router	R1	Interface descriptions: -g0/0.546 = RetailVLAN -g0/0.547 = HousingVLAN -g0/0.548 = AparetmentVLAN -g0/0.549 = RentalVLAN -g0/0.598 = ManagementVLAN - Login block applied for 60 seconds if 5 attempts are undertaken with 60 seconds MOTD = "Sell Sell It Router Authorized Personal Only"	Sell-Sell-It	EXEC = labpassword SSH = SellSellItRouter

Testing Protocol

OVERALL NETWORK FUNCTIONALITY

Upon the completion of building the network we used the ping command to test connectivity to all hosts in the network. Starting with the router, every end device was checked for connection with the intent of proving a properly configured network. We used a table to systematically ping every address from each device which is provided below

TEST 1		Apartments	Retail	Rental	Housing	R1	DL1	AS1	AS2
Router(R1)		✓	✓	✗	✓	✓	✓	✗	✗
Switch (DL1)		✓	✓	✗	✓	✓	✓	✓	✓
Switch (AS1)		✓	✓	✗	✓	✓	✓	✓	✓
Switch (AS2)		✓	✓	✗	✓	✓	✓	✓	✓

Figure 5: Connectivity Table

Our initial test revealed a lack of connection with the rental departments end device. This would require further investigation. As the rest of the network was working correctly, we decided the end device in question must have a fault.

```
R1#ping 139.2.16.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.16.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

R1#ping 139.2.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#ping 139.2.21.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.66, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/1/5 ms

R1#ping 139.2.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#139.2.21.68
Trying 139.2.21.68 ...Open

[Connection to 139.2.21.68 closed by foreign host]
```

```
AS2#ping 139.2.21.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.66, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

AS2#ping 139.2.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

AS2#ping 139.2.21.65

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.65, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

AS2#ping 139.2.21.67

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.67, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms

AS2#
```

Figure 6: Ping Command Being Ran From R1 And AS2 Revealing error with Rental End Device.

By running the **arp – a** command on each of the end devices it was revealed that an IP address had been removed from the Rentals Department, resulting in no connection with that host. This was resolved and the table was again executed, this time revealing full network connectivity.

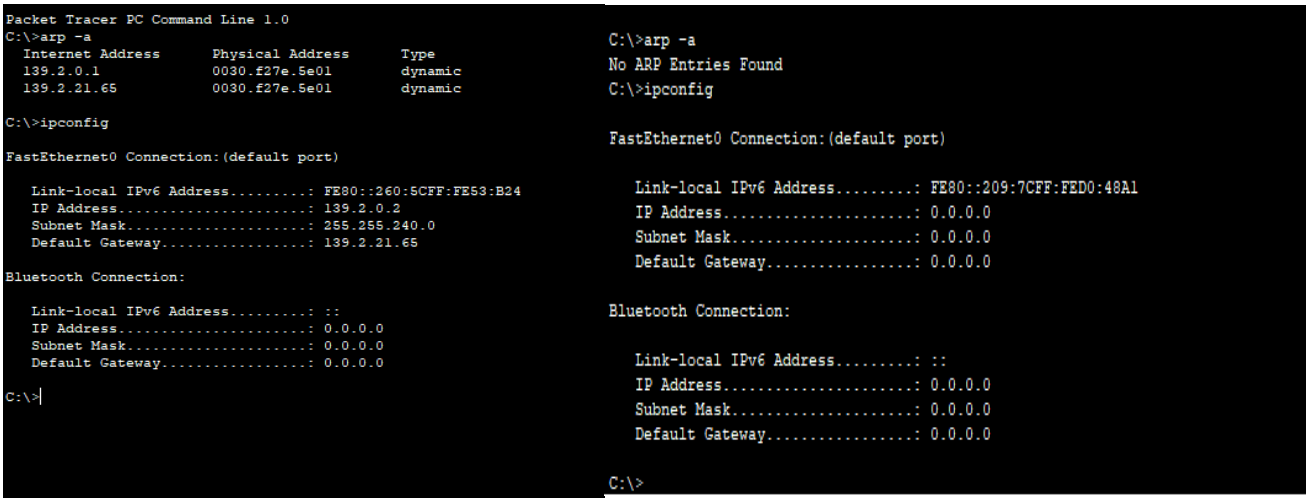


Figure 7: Arp-A Command Being Used On End Devices Showing A Problem With Rentals.

Once the issues was resolved, the ping command was again implemented using the table, revealing a fully operational network and giving us a platform to further test the more intricate parts of the network.

TESTING PROTOCOL FOR REDUNDANT LINKS

Implementing redundancy protects the network from a single point a failure by increasing the availability of devices in the network topology. We chose to create two lines of connection between switches as a way of inputting redundancy in our network.

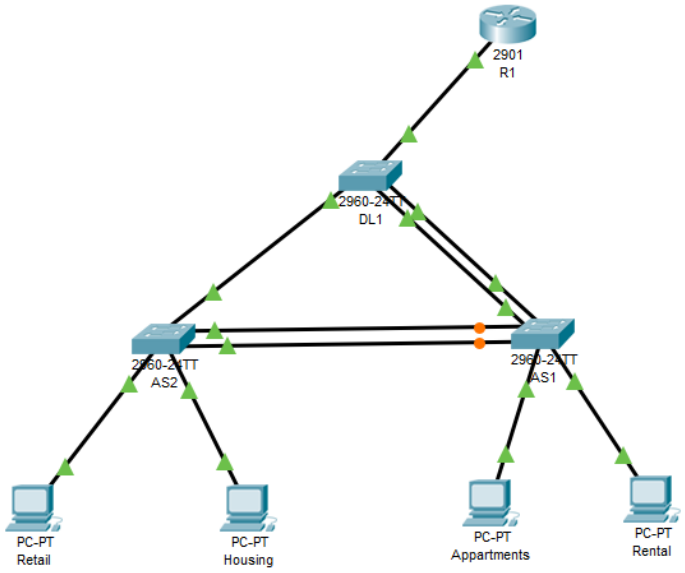


Figure 8: Image: Example Removal Of Link From As2 To DL1

With two lines of connection between each device, our network should always be able to send packets even if one line is damaged or disconnected. To test this theory, once the network was built, we systematically removed points of connection.

With one line disconnected we once again used the ping command from the Router to each end device to see the to see if there was still connectivity. The results, captured below, show that all packets reached their desired destination therefore the redundancy protocol had been implemented and the second connection had been used as means of delivering the packet.

```
R1>ena
Password:
R1#ping 139.2.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/3 ms

R1#ping 139.2.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.0.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms

R1#ping 139.2.16.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.16.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms

R1#ping 139.2.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/10 ms
```

Figure 9: : Ping Command Being Implemented After Removal Of Connection Between As1 And Ds1

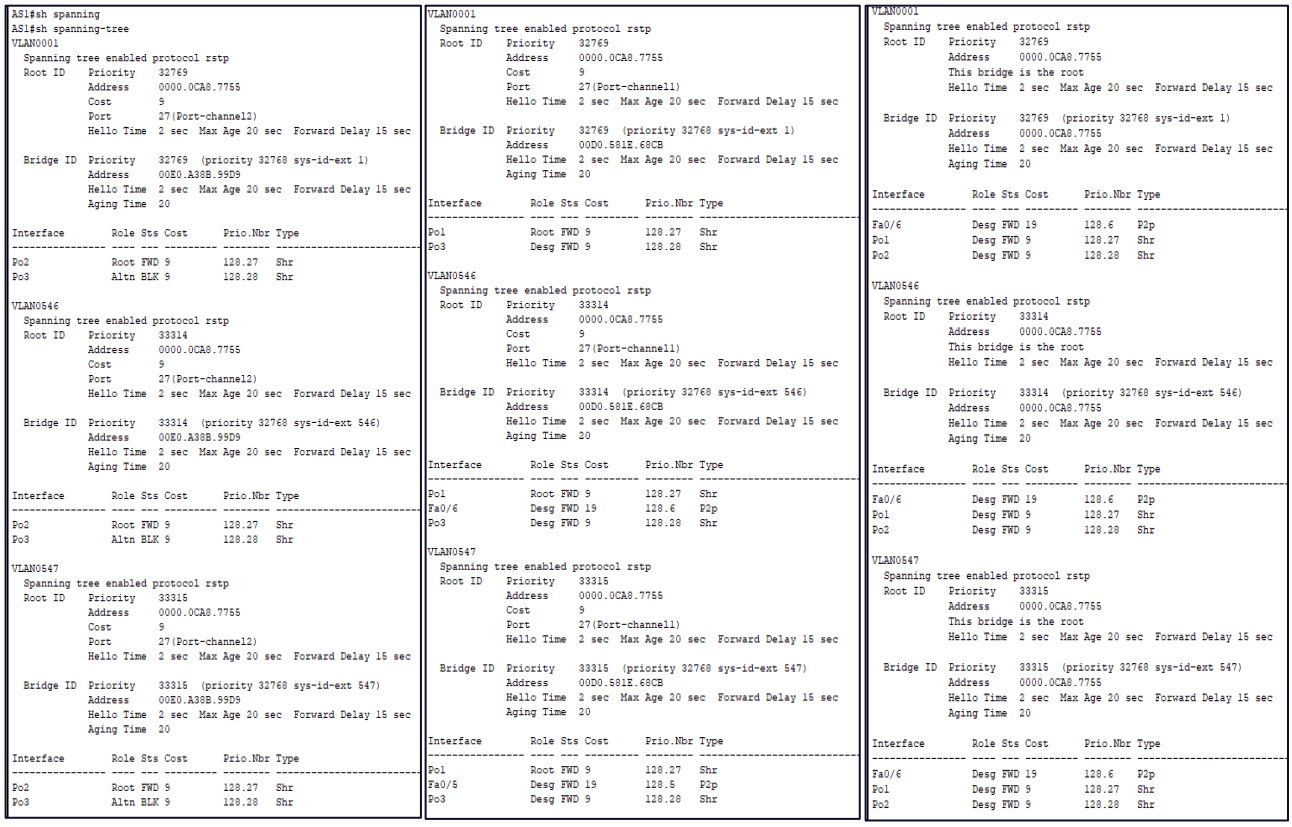
This testing procedure was then implemented on all lines to all switches, to check our redundancy was evident across the network.

TESTING PROTOCOL FOR SPANNING TREE

A drawback feature of the implementation of two lines of connection for physical redundancy between each switch is the possibility of packets getting stuck in loops or duplicates frames **occurring**.

The Spanning Tree protocol is a layer 2 loop avoidance mechanism for redundant links that ensures there is only one logical path between destinations on the network. It intentionally blocks any redundant path that could cause a loop.

To test this**,** we used the show spanning-tree command on all three switches while everything was connected to observe the election process of the root bridge.



```
AS1#sh spanning
AS1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00E0.A38B.99D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Root FWD 9         128.27   Shr
Po3              Altn BLK 9         128.28   Shr

VLAN0546
  Spanning tree enabled protocol rstp
  Root ID    Priority    33314
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33314  (priority 32768 sys-id-ext 546)
             Address     00E0.A38B.99D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Root FWD 9         128.27   Shr
Po3              Altn BLK 9         128.28   Shr

VLAN0547
  Spanning tree enabled protocol rstp
  Root ID    Priority    33315
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33315  (priority 32768 sys-id-ext 547)
             Address     00E0.A38B.99D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Root FWD 9         128.27   Shr
Po3              Altn BLK 9         128.28   Shr
```

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.581E.68CB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 9         128.27   Shr
Po3              Desg FWD 9         128.28   Shr

VLAN0546
  Spanning tree enabled protocol rstp
  Root ID    Priority    33314
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33314  (priority 32768 sys-id-ext 546)
             Address     00D0.581E.68CB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 9         128.27   Shr
Fa0/6            Desg FWD 19        128.6    P2p
Po3              Desg FWD 9         128.28   Shr

VLAN0547
  Spanning tree enabled protocol rstp
  Root ID    Priority    33315
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33315  (priority 32768 sys-id-ext 547)
             Address     00D0.581E.68CB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 9         128.27   Shr
Fa0/5            Desg FWD 19        128.5    P2p
Po3              Desg FWD 9         128.28   Shr
```

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0CA8.7755
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0000.0CA8.7755
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po1              Desg FWD 9         128.27   Shr
Po2              Desg FWD 9         128.28   Shr

VLAN0546
  Spanning tree enabled protocol rstp
  Root ID    Priority    33314
             Address     0000.0CA8.7755
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33314  (priority 32768 sys-id-ext 546)
             Address     0000.0CA8.7755
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po1              Desg FWD 9         128.27   Shr
Po2              Desg FWD 9         128.28   Shr

VLAN0547
  Spanning tree enabled protocol rstp
  Root ID    Priority    33315
             Address     0000.0CA8.7755
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33315  (priority 32768 sys-id-ext 547)
             Address     0000.0CA8.7755
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po1              Desg FWD 9         128.27   Shr
Po2              Desg FWD 9         128.28   Shr
```

Figure 10: Show Spanning-Tree Command On All 3 Switches Revealing DS1 As Allocated Root Bridge.

Following this we completely disconnected DL1 from AS1 and reran the spanning tree protocol to see the changes in the output. Our results showed that STP was implemented and the blocked ports were reopened allowing frames to be passed to the router even though there is major line of connection missing.

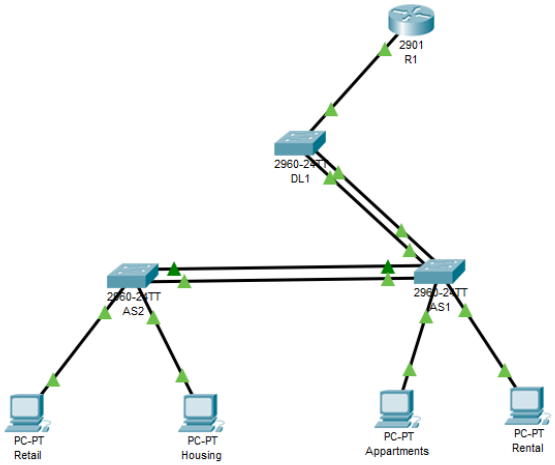


Figure 11 shows our test scenario implemented with the disconnection of lines between DL1 an AS1

```
AS1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00E0.A38B.99D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Root FWD 9         128.27   Shr
Po3              Desg FWD 9         128.28   Shr

VLAN0546
  Spanning tree enabled protocol rstp
  Root ID    Priority    33314
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33314  (priority 32768 sys-id-ext 546)
             Address     00E0.A38B.99D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Root FWD 9         128.27   Shr
Po3              Desg FWD 9         128.28   Shr

VLAN0547
  Spanning tree enabled protocol rstp
  Root ID    Priority    33315
             Address     0000.0CA8.7755
             Cost        9
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33315  (priority 32768 sys-id-ext 547)
             Address     00E0.A38B.99D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Root FWD 9         128.27   Shr
Po3              Desg FWD 9         128.28   Shr
```

```
AS2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0CA8.7755
             Cost        18
             Port        28(Port-channel3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.581E.68CB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po3              Root FWD 9         128.28   Shr

VLAN0546
  Spanning tree enabled protocol rstp
  Root ID    Priority    33314
             Address     0000.0CA8.7755
             Cost        18
             Port        28(Port-channel3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33314  (priority 32768 sys-id-ext 546)
             Address     00D0.581E.68CB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po3              Root FWD 9         128.28   Shr

VLAN0547
  Spanning tree enabled protocol rstp
  Root ID    Priority    33315
             Address     0000.0CA8.7755
             Cost        18
             Port        28(Port-channel3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33315  (priority 32768 sys-id-ext 547)
             Address     00D0.581E.68CB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5            Desg FWD 19        128.5    P2p
Po3              Root FWD 9         128.28   Shr
```

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0000.0CA8.7755
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0000.0CA8.7755
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po2              Desg FWD 9         128.28   Shr

VLAN0546
  Spanning tree enabled protocol rstp
  Root ID    Priority    33314
             Address     0000.0CA8.7755
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33314  (priority 32768 sys-id-ext 546)
             Address     0000.0CA8.7755
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po2              Desg FWD 9         128.28   Shr

VLAN0547
  Spanning tree enabled protocol rstp
  Root ID    Priority    33315
             Address     0000.0CA8.7755
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33315  (priority 32768 sys-id-ext 547)
             Address     0000.0CA8.7755
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po2              Desg FWD 9         128.28   Shr
```

Figure 12: sh spanning-tree command issued post removal of connection show reorganization of blocked ports.

Finally we again issued the ping command from from each of the end switches to the router to prove that packets would still be delivered and that the spanning tree protocol was being implemented. The results showed that there was still a connection although the packets where taking a while longer to be delivered.

```
AS2#ping 139.2.21.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.66, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

AS2#ping 139.2.21.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.66, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

AS2#ping 139.2.21.65

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 139.2.21.65, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

AS2#
```

Figure 13: Ping Command Issued Post Removal Of Connections From AS2 To R1

Finally we issued the ping command from the end devices connected to AS2 just to confirm there is connectivity right throughout the network.

```
Pinging 139.2.21.65 with 32 bytes of data:

Reply from 139.2.21.65: bytes=32 time<1ms TTL=255
Reply from 139.2.21.65: bytes=32 time=1ms TTL=255
Reply from 139.2.21.65: bytes=32 time<1ms TTL=255
Reply from 139.2.21.65: bytes=32 time=3ms TTL=255

Ping statistics for 139.2.21.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 139.2.21.66

Pinging 139.2.21.66 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 139.2.21.66: bytes=32 time<1ms TTL=254
Reply from 139.2.21.66: bytes=32 time<1ms TTL=254

Ping statistics for 139.2.21.66:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 139.2.21.66

Pinging 139.2.21.66 with 32 bytes of data:

Reply from 139.2.21.66: bytes=32 time<1ms TTL=254
Reply from 139.2.21.66: bytes=32 time=1ms TTL=254
Reply from 139.2.21.66: bytes=32 time<1ms TTL=254
Reply from 139.2.21.66: bytes=32 time<1ms TTL=254

Ping statistics for 139.2.21.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure 14: Ping Command Issued From End Devices Retail To R1

TESTING PLAN FOR ETHERCHANNEL BUNDLING

As we had previously connected two lines between switched to allow for redundancy in our network it made sense to also implement **EtherChannel** bundling where the two physical links will act as one logical link and provide twice the bandwidth two each connection in the network. It also provides us with extra redundancy as you will still have connection from layer to layer if a line is damaged just with a **diminished** bandwidth.

To test the **EtherChannel** bundling is implemented we ran the **EtherChannel** summary command on each switch to firstly display the summary information about **EtherChannel's**.

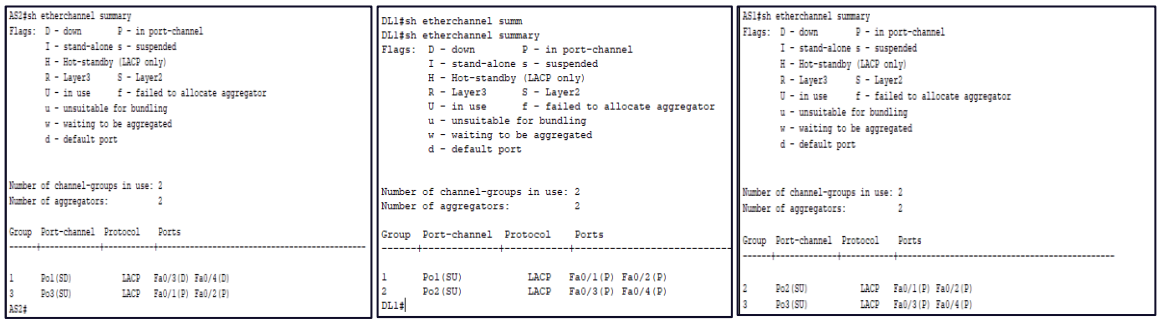


Figure 15: Etherchannel Summary Command On Each Switch

Then we ran the sh interface port number command on all switches to confirm the line were running at their expected bandwidth.

Figure 16: sh int p0/1 on AS1

Finally, we again ran sh interfaces range on the switches again but this time with port lines disconnected to view the decrease in bandwidth to half of the original output. This proving the EtherChannel bundling has been implemented.

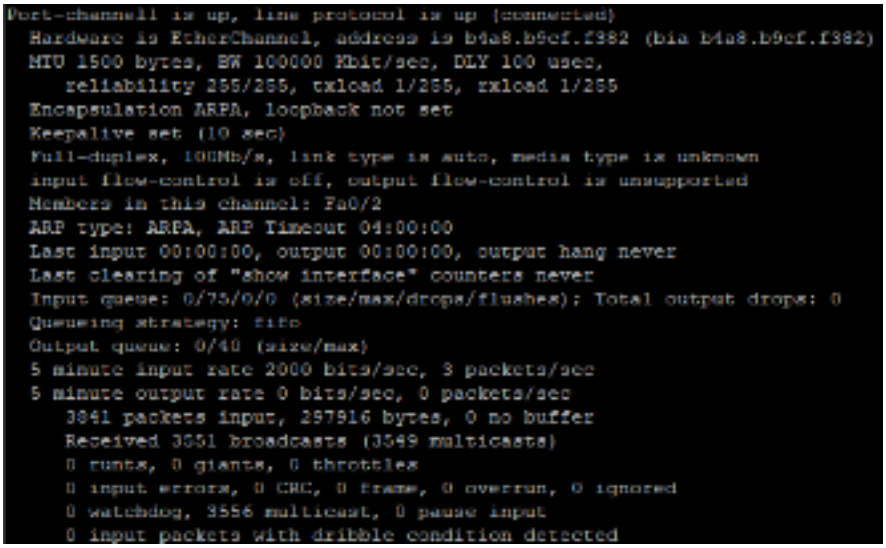


Figure 17: sh int p0/1 on AS1 with connection removed

Conclusion

The solution to the problem presented includes various security techniques that would be valued in a business as big as “Sell Sell It” to avoid physical and virtual threats to any business integral data. To ensure that the network reaches minimal downtime redundant links have also been configured along with EtherChannel bundling to provide a theoretical double in bandwidth speeds for the hosts that are connected. Scalability has also been included presenting by the physical topology allowing for a second distribution switch to be added to increase both bandwidth and potential available hosts for future requirements. Furthermore, the Management VLAN was expanded allowing for over double the amount of hosts available for future network upgrades.