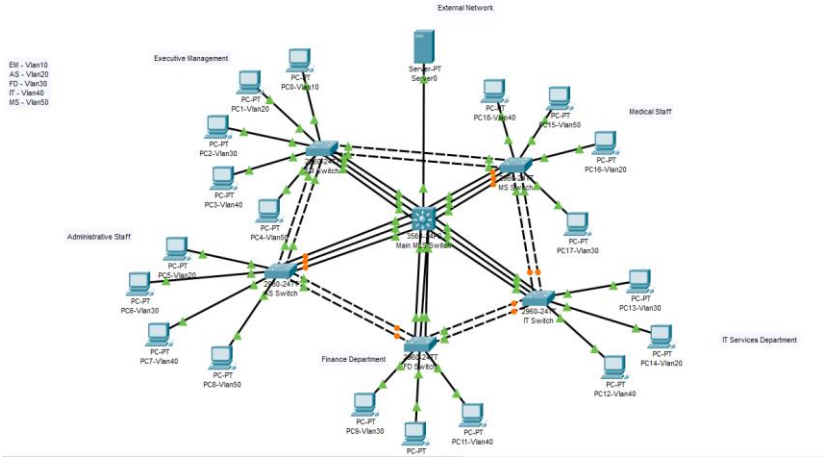
MetroHealth

Hosptial Headquarters

Prototype LAN Design



Adam Romanowicz

C00297492

IT Management

Requirement 1: Departmental Segmentation Using Vlans

To achieve departmental segmentation each department has a vlan associated with it. In the prototype vlans 10,20,30,40 and 50 were used for the departments Executive Management, Administrative Staff, Finance Department, IT Services and Medical Staff. In the topology each switch is associated with a particular department as the hospital is segmented into 5 areas, however, other employees from other departments are present in each area as well e.g IT Service end users are present in each area for hospital efficiency and departmental co-operation. Vlan 98 is an unused interface vlan, it is used for extra security as trunklines will not allowed traffic tagged with this vlan to pass through, all interfaces assigned to Vlan 98 is also shut down. Vlan 99 is the management vlan and is used for remote connectivity to the switches command line interface via ssh. Vlan 100 is the native vlan used by trunklines to allow untagged traffic to pass through. The default vlan 1 has been shutdown and is not used in the design.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   Executive_Management              active    Fa0/20
20   Administrative_Staff              active    Fa0/21
30   Finance_Department                active    Fa0/22
40   IT_Services                       active    Fa0/23
50   Medical_Staff                     active    Fa0/24
98   Unused                            active    Fa0/6, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Gig0/1, Gig0/2
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Requirement 2: Inter-Vlan Communication and External Connectivity

To achieve inter-vlan communication trunklines between switches have been used, each trunkline also has a filter to what vlan tagged traffic is allowed to pass through them for additional security. The tag is changed in the MLS which has SVIs set up for each vlan with ip addresses configured on each to act as each individual vlan's default gateway e.g traffic with vlan 10 tags that are being sent to a vlan 40 end user get their vlan 10 tag removed and a vlan 40 tag added on so the vlan 40 end user device does not drop the frame. External connectivity was achieved via the MLS with a router port configured (no switchport) and ip routing turned on. An ip address was configured onto this interface and acts as a default-gateway which allows external traffic enter the network.

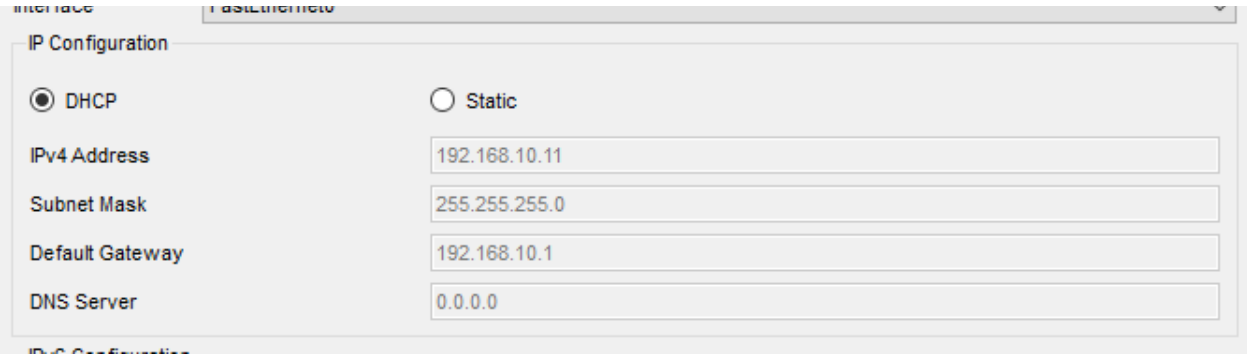
```
!
interface Vlan10
 description SVI for Executive_Management
 mac-address 0007.ecb2.ce01
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 description SVI for Administrative_Staff
 mac-address 0007.ecb2.ce02
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 description SVI for Finance_Department
 mac-address 0007.ecb2.ce03
 ip address 192.168.30.1 255.255.255.0
!
interface Vlan40
 description SVI for IT_Services
 mac-address 0007.ecb2.ce04
 ip address 192.168.40.1 255.255.255.0
!
interface Vlan50
 description SVI for Medical_Staff
 mac-address 0007.ecb2.ce05
 ip address 192.168.50.1 255.255.255.0
!
interface Vlan99
 description Management vlan for ssh traffic and ip address for remote connection into switch
 mac-address 0007.ecb2.ce06
 ip address 192.168.99.16 255.255.255.0
!
interface Vlan100
 description Native vlan for untagged traffic across trunklines
 mac-address 0007.ecb2.ce07
 ip address 192.168.100.1 255.255.255.0
!
```

```
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      100
Po2         on           802.1q         trunking      100
Po3         on           802.1q         trunking      100

Port        Vlans allowed on trunk
Po1         10,20,30,40,50,99-100
Po2         10,20,30,40,50,99-100
Po3         10,20,30,40,50,99-100

Port        Vlans allowed and active in management domain
Po1         10,20,30,40,50,99,100
Po2         10,20,30,40,50,99,100
Po3         10,20,30,40,50,99,100

Port        Vlans in spanning tree forwarding state and not pruned
Po1         10,20,30,40,50,99,100
Po2         10,20,30,40,50,99,100
Po3         10,20,30,40,50,99,100
```

Requirement 3: IPv4 Addressing with Dynamic Allocation

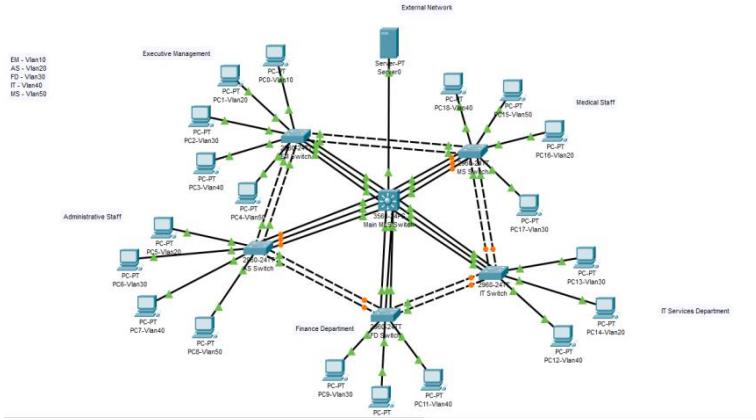
Each vlan has its own IPv4 network address pool where necessary; the vlan number is used in the IPv4 address to make it clear what vlan the ip is a part of; the addressing scheme is as follows: 192.168.XX.XX /24 e.g vlan 10 addresses would be 192.168.10.11, 192.168.10.12, etc. Dynamic allocation for scalability and ease of network management is achieved using DHCP which is enabled and configured on the MLS. Excluded addresses for departmental vlans are 192.168.XX.1-192.168.XX.10; this is done for later use by IT management if needed e.g static ip address for a DNS server. DHCP leases ip addresses for each end user on each of the 5 departments in the topology with each vlan having its own default-gateway.

```
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp excluded-address 192.168.50.1 192.168.50.10
!
ip dhcp pool EM-VLAN
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
ip dhcp pool AS-VLAN
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
ip dhcp pool FD-VLAN
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
ip dhcp pool IT-VLAN
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
ip dhcp pool MS-VLAN
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
```



Requirement 4: Network Redundancy for High Availability

Network redundancy is achieved by having additional connections to each switch with at least 3 connections to 3 other switches at a time. STP prevents any logical loops this topology might cause. EtherChannel is another additional step in achieving redundancy with departmental switches having 2 cable EtherChannels connecting to other departmental switches; those switches then connect to the Main MLS with 3 cable EtherChannels, this is done for redundancy and higher bandwidth to the core switch as all frames going in and out of the network plus inter-vlan frames are passing through the MLS. Any disruption in the topology can be mitigated by the additional connections e.g a cable being broken/unplugged in an EtherChannel will not break the other connection(s) in that channel; if all connections in the EtherChannel are broken the topology can still mitigate this via STP by unblocking other connections effectively going around the disruption.




```
interface Port-channel1
 description EtherChannel for f0/4,f0/11 and f0/12
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,40,50,99-100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 description EtherChannel for f0/3,f0/9 and f0/10
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,40,50,99-100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 description EtherChannel for f0/2,f0/7 and f0/8
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,40,50,99-100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel4
 description EtherChannel for f0/5,f0/13 and f0/14
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,40,50,99-100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel5
 description EtherChannel for f0/1,f0/15 and f0/16
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,40,50,99-100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

Requirement 5: Network Device Security and Hardening

To increase security this topology includes various precautions to prevent unauthorized access to the network; this includes trunkline vlan filtering e.g only allowing certain vlans pass through the trunkline (10,20,30,40,50,99-100), password upon login, ssh users and login passwords (telnet access disabled) for secure and encrypted remote access, enable privilege password, encrypted passwords using service-encryption and unused interfaces being put on an unused vlan that cannot cross trunklines and those interfaces being turned off.

```
service password-encryption
!
hostname Main
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
username administrator secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
banner motd ^CUnauthorized access is prohibited!^C
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
```

```
98   Unused                           active    Fa0/6, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Gig0/1, Gig0/2
```

```
!
interface FastEthernet0/10
 description Unused switch interface which is turned off
 switchport access vlan 98
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 description Unused switch interface which is turned off
 switchport access vlan 98
 switchport mode access
 shutdown
!
interface FastEthernet0/12
 description Unused switch interface which is turned off
 switchport access vlan 98
 switchport mode access
 shutdown
```

```
EA#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      100
Po2         on           802.1q         trunking      100
Po3         on           802.1q         trunking      100

Port        Vlans allowed on trunk
Po1         10,20,30,40,50,99-100
Po2         10,20,30,40,50,99-100
Po3         10,20,30,40,50,99-100

Port        Vlans allowed and active in management domain
Po1         10,20,30,40,50,99,100
Po2         10,20,30,40,50,99,100
Po3         10,20,30,40,50,99,100

Port        Vlans in spanning tree forwarding state and not pruned
Po1         10,20,30,40,50,99,100
Po2         10,20,30,40,50,99,100
Po3         10,20,30,40,50,99,100
```