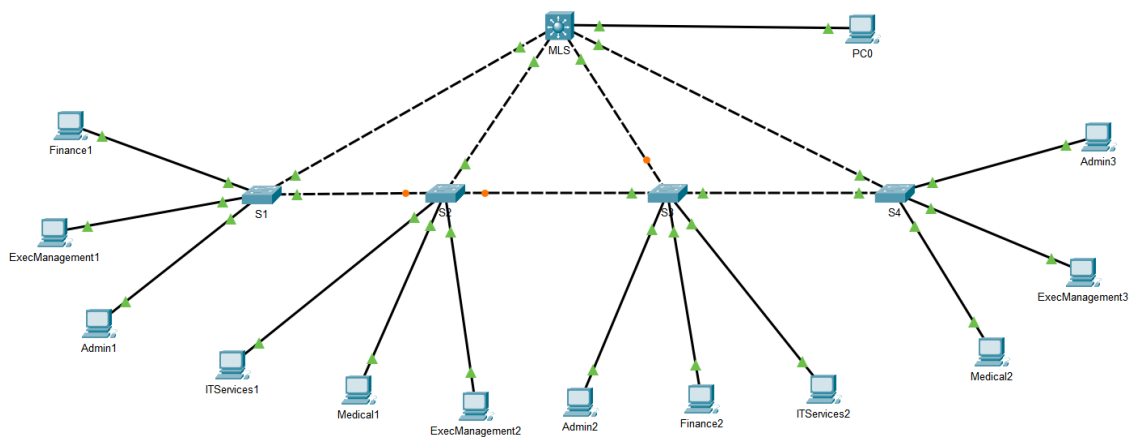


LAN Design Report

MetroHealth Hospital Headquarters

I designed a scalable and secure LAN for MetroHealth Hospital's new headquarters. This report will explain my design choices and how I created a network to support all departments to ensure security and redundancy.



The above topology is the network I designed. I chose to use the Layer 3 switch to achieve Inter-VLAN routing. I chose this as opposed to Router-on-a-Stick as it is more cost effective, faster routing speeds, and more scalable if the hospital expanded to over 50 VLANs.

Departmental Segmentation using VLANs

As the hospital has five departments, Executive Management, IT Services, Administration, Finance, and Medical Staff, I set up five data VLANs to segment the traffic between each department. Not every department is in the same area, so I configured trunk ports between each switch to ensure that the departments could communicate across broadcast domains.

After creating all the VLANs on each switch, I assigned them to the ports that the PCs in the relevant department were connected to.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	Executive-Management	active	Fa1/1
20	Administrative-Staff	active	Fa2/1
30	Finance-Department	active	Fa3/1
40	IT-Services-Department	active	
50	Medical-Staff	active	
60	Unused	active	Fa4/1, Fa5/1, Fa7/1
99	Management	active	
100	Native	active	
150	VOICE	active	

Inter-VLAN Communication and External Connectivity

To achieve inter-VLAN communication between each department, I set up trunk lines between each switch.

```
S1#show int trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    100
Fa6/1     on        802.1q         trunking    100

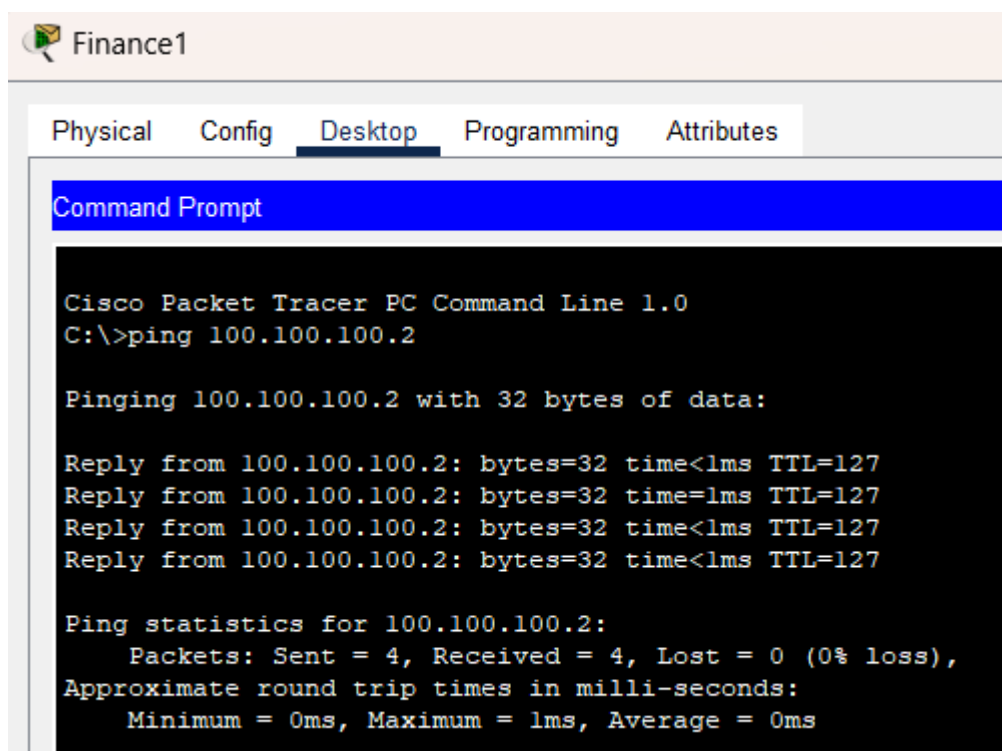
Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa6/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,40,50,60,99,100,150
Fa6/1     1,10,20,30,40,50,60,99,100,150

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,40,50,60,99,100,150
Fa6/1     1,10,20,30,40,50,60,99,100,150
```

On S1, Fa0/1 is connected to S2 and Fa6/1 is connected to the MLS. The native VLAN on these and all other trunk line in the network is 100, to ensure untagged traffic can make it through the trunk lines and to the correct destination.

To communicate with outside network devices, I have connected a PC to the MLS with an IP address outside of the hospitals LAN. The IP address assigned to the MLS port is also the default gateway of the PC. With these configurations, all devices in the network can ping the outside PC, ensuring external network connectivity.



IPv4 Addressing with Dynamic Allocation

I used DHCPv4 to assign IPv4 addresses to my end devices and network devices. The addressing scheme I used was:

VLAN 10: 192.168.10.0

VLAN 20: 192.168.20.0

VLAN 30: 192.168.30.0

VLAN 40: 192.168.30.0

VLAN 50: 192.168.50.0

I used the MLS as my DHCPv4 server by enabling 'ip routing' on the device. This saves the need for a separate, dedicated server.

```
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 VLAN1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.2
ip dhcp pool VLAN2
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.2
ip dhcp pool VLAN3
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.2
ip dhcp pool VLAN4
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.40.2
ip dhcp pool VLAN5
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
 dns-server 192.168.50.2
!
!
ip routing
```

I excluded the first 10 addresses of each VLAN to be kept for things such as printers and servers. I then set up the pool for each VLAN and addresses such as the network address and default gateway. After this, DHCP was fully set up and ready to assign IPv4 addresses to my devices.

<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.40.14
Subnet Mask	255.255.255.0
Default Gateway	192.168.40.1
DNS Server	192.168.40.2

This PC in VLAN 40 was successfully assigned an IPv4 address in that range.

Network Redundancy for High Availability

In the topology above, I have a connection from each Layer 2 switch to the Layer 3 switch, so that if one connection goes down, there is still other ways for each device to communicate. The 5 data VLANs are all located on different switches, so if one switch was to fail, the entire department isn't down, and rather just one PC.

Network Device Security and Hardening.

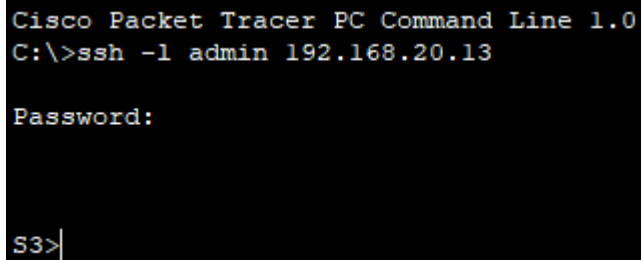
As the first step in security, each switch has encrypted passwords on the console and enable modes. For simplicity in this demonstration, I have configured all passwords as 'cisco', although this would not be a secure password in a real application of this network.

```
service password-encryption
!
hostname S2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
```

Any unused ports are assigned to an unused VLAN (VLAN 60 – Unused) and shutdown to prevent any unwanted connections without the network administrator's permission.

```
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
```

To facilitate remote connections to the network, I have implemented SSH. This is much more secure than Telnet, as the data is sent encrypted. To access the network via SSH, the user must have a username and password that has been set up by the administrator.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.20.13

Password:

S3>|
```