Evan Dunphy Student Number: C00303467

LAN Design for MetroHealth Hospital Headquarters

MetroHealth

Devoted to Hope, Health, and Humanity

Contents

INFO 2

TOPOLOGY 3

PORT CONNECTIONS 5

VLAN DESIGN 6

INTER VLAN ROUTING 8

IP ADDRESSING 9

REDUNDANCY 11

SECURITY MEASURES 13

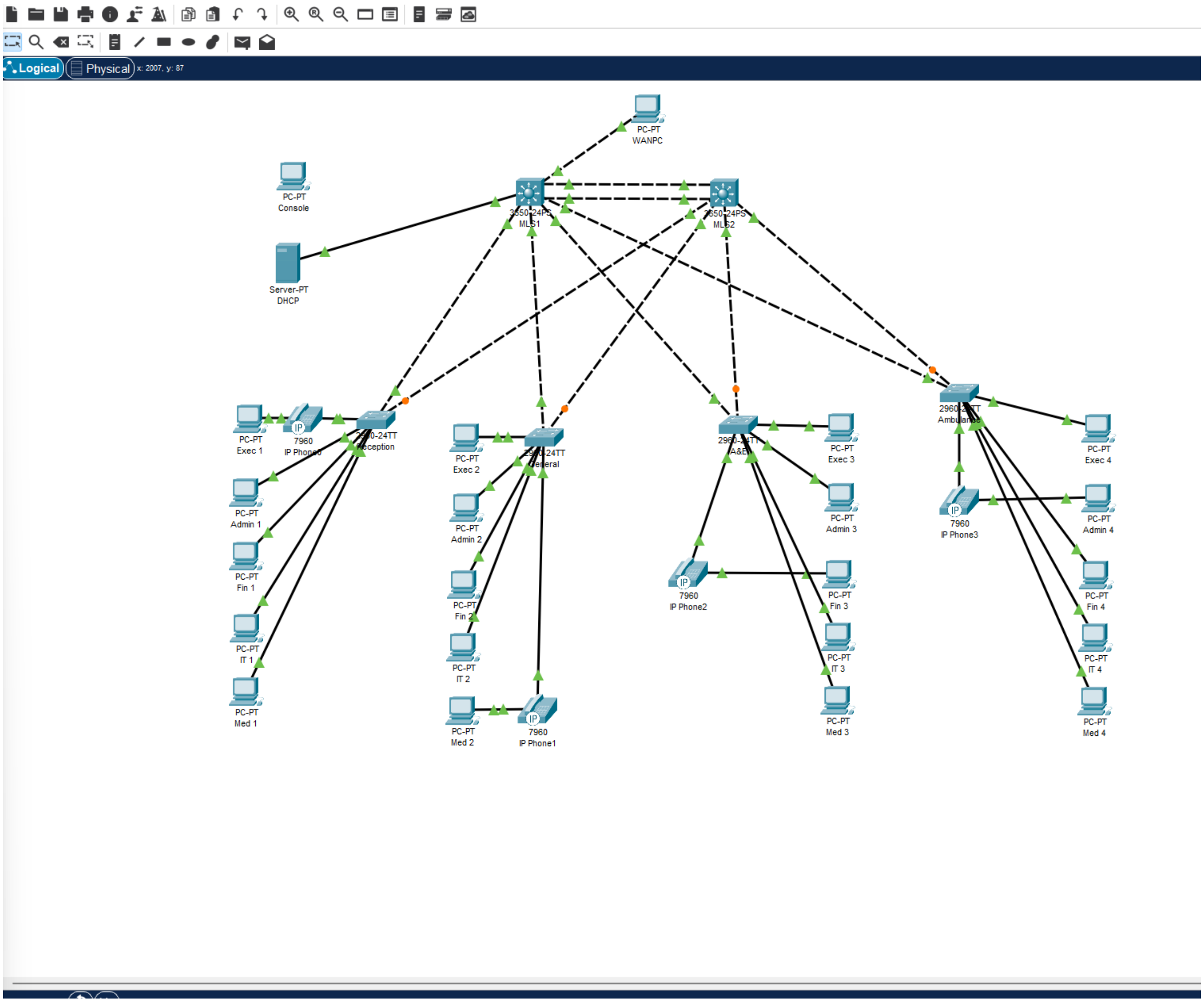
INFO

MetroHealth Hospital, a leading healthcare provider, is expanding its headquarters to manage multiple clinics and departments. A high-performance Local Area Network (LAN) is required to support critical operations such as patient care, administrative functions, and medical services.

I have designed a LAN prototype for the MetroHealth Hospital that fits all the necessary criteria. The prototype was made with Cisco packet tracer. The prototype file is contained in the same email as this report.

Due to limitations in cisco packet tracer the full extent of the LAN could not be created and simulated.

TOPOLOGY



The LAN contains 2 Multilayer Switches (MLS). MLS1 is active on layer 3 and facilitates communication between the VLANs in the LAN and routes traffic to and from the External Network, MLS2 is not active on layer 3 and does not route traffic from VLAN to VLAN and acts as a normal layer 2 switch in the topology.

Should MLS1 fail, MLS2 can be configured to actively route frames from VLAN to VLAN. MLS2 is a backup for MLS1, however we are using it in the topology to keep costs down as MLS's are very expensive hardware.

Every area in the hospital has a switch to connect end devices to, and each switch is connected to both MLS1 and MLS2. Each switch is configured with multiple VLANs for each department in the hospital. Due to the limitations of cisco packet tracer the switches have 24 fast ethernet ports and only 2 gigabit ethernet ports. In a real-world situation, the switches would have more total ports and all ports would be at least gigabit ports.

Ip phones are installed on the LAN to allow for real time conversation between areas in the hospital, such as when an ambulance arrives and needs to notify A&E of a patient in need of urgent care.

A server is on the network to provide services such as DHCPv4, DHCPv6, DNS and any other services necessary. In the simulated prototype the server only provides the DHCPv4 service.

I choose not to add IP printers to the topology as I believe most printers will be connected directly to the user PCs and the standalone printers in the MetroHealth hospital would be for X-ray, MRI scans and other specialized services that need specific types of printers that cisco packet tracer does not provide.

All switches are connected to at least 2 other switch devices, providing frames with multiple paths to travel to their destination. Should one path fail there is another path to travel. These connections create physical loops in the LAN, however with STP implemented these loops are logically blocked. MLS1 is designated to be the root bridge in the STP set up making all frames travel through it as a priority.

An Ether channel link is set up between MLS1 and MLS2 to guarantee high latency. Due to cisco packet tracer's limitations, Ether channel between the switches and the MLSs could not be established but in a real-world situation Ether channel would be set up.

A console line is set up in the server room for when SSH remote access fails for troubleshooting issues with the switches and MLSs configurations.

PCs are connected to switches in each area for members of staff, patient and guest visitors in the MetroHealth hospital can connect to the LAN and the internet. Each PC is connected to a specific port on the switches to assign them to different VLANs.

PORT CONNECTIONS

The port connections for each MLS and Switch are listed in the tables below.

MLS1				
PORT	**TYPE**	**SHUT**	**DEVICE TO**	**ALLOWED VLANs**
G1/0/1	TRUNK	OPEN	RECEPTION	ALL
G1/0/2	TRUNK	OPEN	GENERAL	ALL
G1/0/3	TRUNK	OPEN	A%E	ALL
G1/0/4	TRUNK	OPEN	AMBULANCE	ALL
G1/0/5-24	ACCESS	SHUT	N/A	2
G1/1/1-2	TRUNK	ETHER	MLS2	ALL
G1/1/3	ACCESS	OPEN	DHCP	5
G1/1/4	ROUTER	OPEN	WAN	N/A

MLS2				
PORT	**TYPE**	**SHUT**	**DEVICE TO**	**ALLOWED VLANs**
G1/0/1	TRUNK	OPEN	RECEPTION	ALL
G1/0/2	TRUNK	OPEN	GENERAL	ALL
G1/0/3	TRUNK	OPEN	A%E	ALL
G1/0/4	TRUNK	OPEN	AMBULANCE	ALL
G1/0/5-24	ACCESS	SHUT	N/A	2
G1/1/1-2	TRUNK	ETHER	MLS1	ALL
G1/1/3	ACCESS	SHUT	N/A	N/A
G1/1/4	ROUTER	OPEN	WAN	N/A

RECEPTION, GENERAL, A&E, AMBULANCE				
PORT	**TYPE**	**SHUT**	**DEVICE TO**	**ALLOWED VLANs**
F0/1	ACCESS	OPEN	EXEC PC	10
F0/2	ACCESS	OPEN	ADMIN PC	20
F0/3	ACCESS	OPEN	FIN PC	30
F0/4	ACCESS	OPEN	IT PC	40
F0/5	ACCESS	OPEN	MED PC	50
F0/6-24	ACCESS	SHUT	N/A	2
G0/1	TRUNK	OPEN	MLS1	ALL
G0/2	TRUNK	OPEN	MLS2	ALL
VLAN90	ROUTER	OPEN	NA	N/A

VLAN DESIGN

VLANs were used in the LAN to segment the network to ensure security, management efficiency and traffic isolation. Each VLAN is assigned to a specific department in the MetroHealth hospital. Four types of VLAN are being used in the LAN. Data, Voice, Native and Management VLAN types. The management VLAN type is used solely for management traffic to allow SSH access into the switches. The native VLAN type is used for trunk links between each of the switches. The data VLAN type is used for user generated traffic. All traffic on a single data VLAN is only able to be sent to and from end devices on the same VLAN. By assigning ports to a specific VLAN the LAN is split into many smaller LANs logically which creates broadcast domains for each specific VLAN.

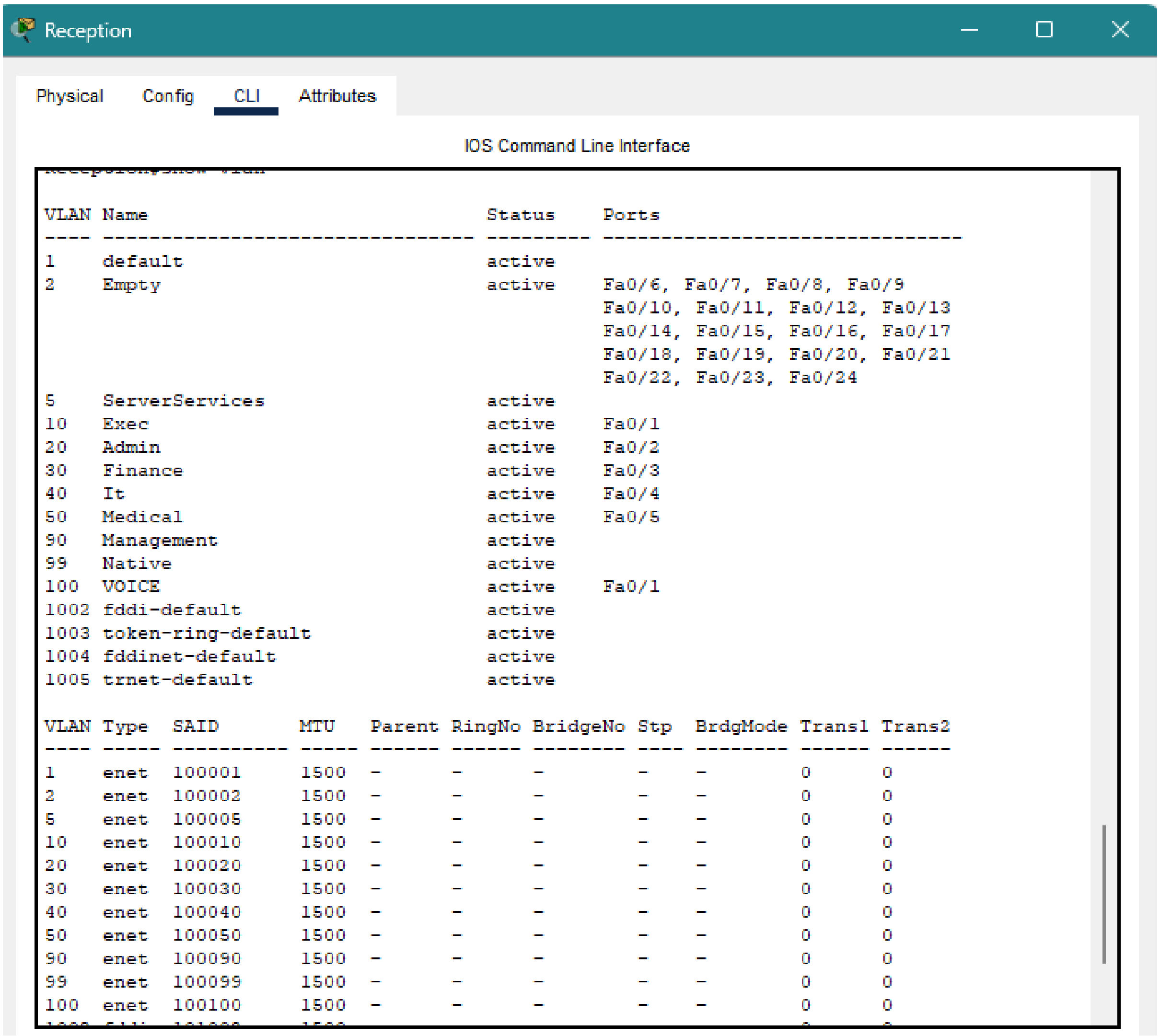
As a security measure the Empty VLAN was created to put unused ports in. ServerServices was created for dedicated server connections to provide services such as DHCP and DNS.

Exec was created as a data VLAN for the Executive Management group. Admin was created as a data VLAN for the Administrative Staff. Finance was created as a data VLAN for the Finance Department. IT was created as a data VLAN for the IT Services Department. Medical was created as a data VLAN for the Medical Staff.

Management was created to allow for ssh access to each switch. Native was created to be the native VLAN for each switch instead of VLAN 1. VOICE was created to allow IP phones to be in the topology. VOICE is a voice VLAN that is configured specifically for voice communication. The VOICE VLAN is configured with quality of service to guarantee effective voice communication.

VLANS	
ID NUMBER	**NAME**
2	Empty
5	ServerServices
10	Exec
20	Admin
30	Finance
40	It
50	Medical
90	Management
99	Native
100	VOICE

In the prototype only the VLANs above have been created, however in the real implementation many more VLANs would be created for all the departments in the hospital needed and other VLANs for guest visitors and patients, etc.



```
Reception#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
2    Empty                            active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
5    ServerServices                   active    
10   Exec                             active    Fa0/1
20   Admin                            active    Fa0/2
30   Finance                          active    Fa0/3
40   It                               active    Fa0/4
50   Medical                          active    Fa0/5
90   Management                       active    
99   Native                           active    
100  VOICE                            active    Fa0/1
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
90   enet  100090     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
```

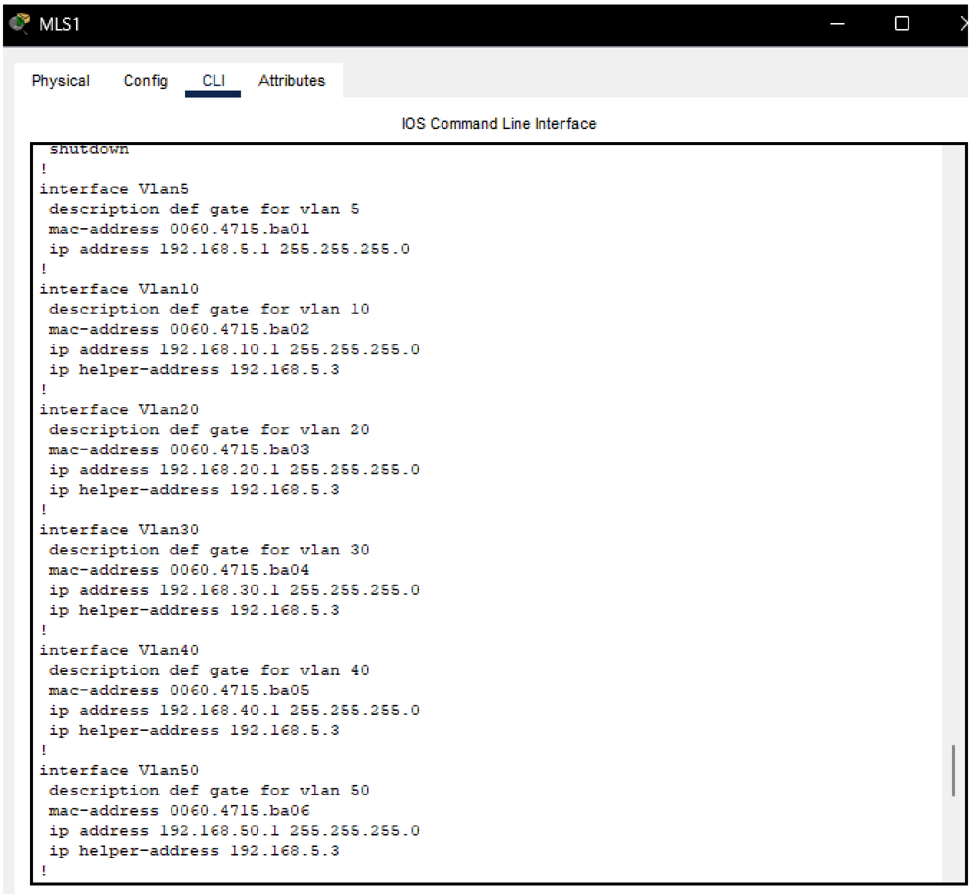
INTER VLAN ROUTING

Inter VLAN routing is implemented on the LAN to allow data from devices on one VLAN to be sent to devices on other VLANS.

The MLS creates Svi's to act as default gateways for each VLAN and has IP routing enabled; this allows end devices on each VLAN to communicate with end devices on other VLANs.

SVI IP SCHEME		
VLAN & SVI NAME	**IP ADDRESS**	**SUBNET MASK**
ServerServices	192.168.5.1	/24
Exec	192.168.10.1	/24
Admin	192.168.20.1	/24
Finance	192.168.30.1	/24
It	192.168.40.1	/24
Medical	192.168.50.1	/24
Management	192.168.90.1	/24
VOICE	192.168.100.1	/24

The MLS was chosen to provide inter VLAN routing over other methods because of its many advantages. Due to the size of MetroHealth, we need an unknown large amount of VLANs a MLS is the most scalable implementation of inter VLAN routing. A MLS with routing enabled and SVI's is also the fastest method of Inter VLAN routing. Choosing this option allows for future growth of the MetroHealth hospital and for high network speed in the current implementation of the LAN.



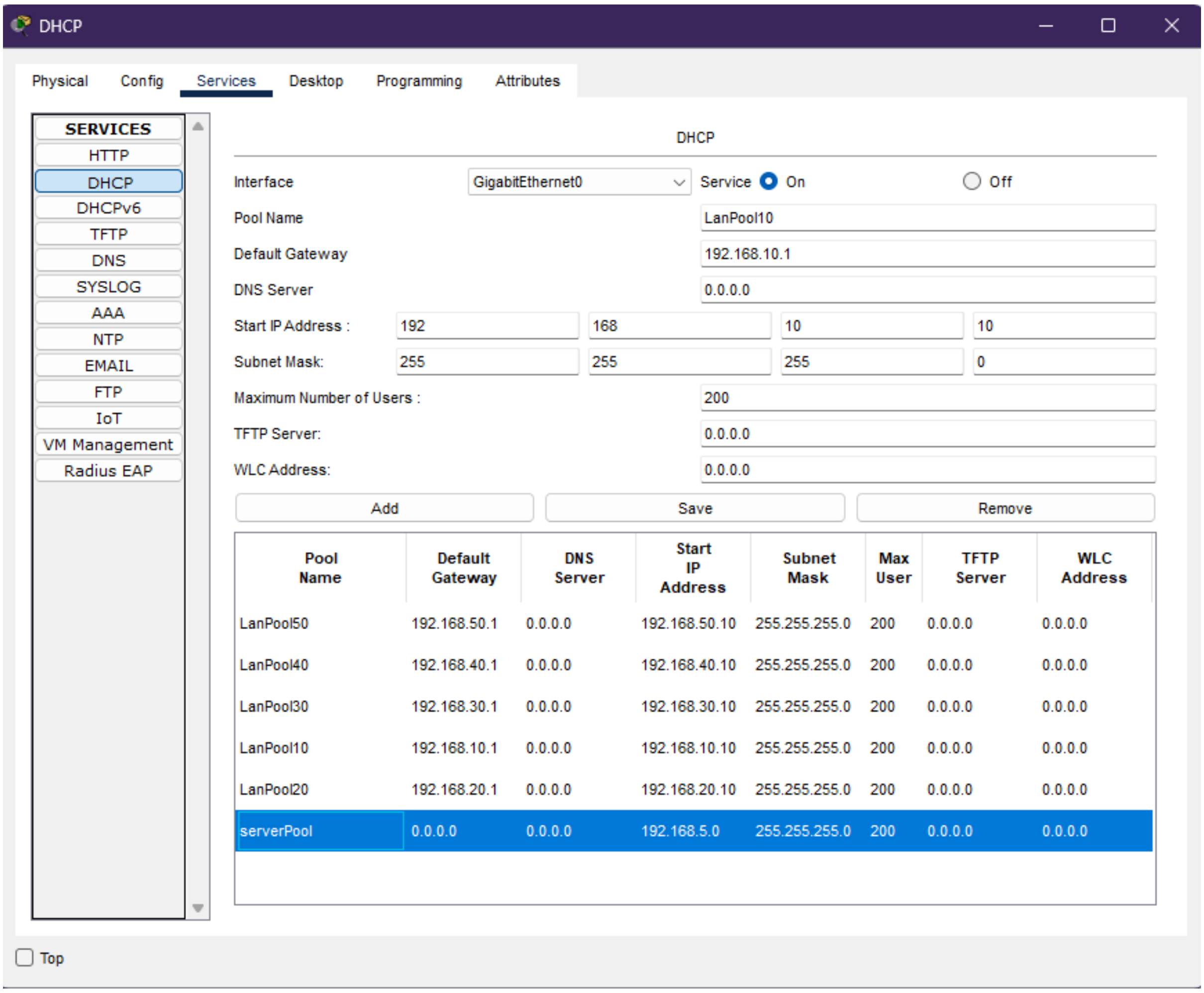
```
 shutdown
!
interface Vlan5
 description def gate for vlan 5
 mac-address 0060.4715.ba01
 ip address 192.168.5.1 255.255.255.0
!
interface Vlan10
 description def gate for vlan 10
 mac-address 0060.4715.ba02
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.5.3
!
interface Vlan20
 description def gate for vlan 20
 mac-address 0060.4715.ba03
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.5.3
!
interface Vlan30
 description def gate for vlan 30
 mac-address 0060.4715.ba04
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 192.168.5.3
!
interface Vlan40
 description def gate for vlan 40
 mac-address 0060.4715.ba05
 ip address 192.168.40.1 255.255.255.0
 ip helper-address 192.168.5.3
!
interface Vlan50
 description def gate for vlan 50
 mac-address 0060.4715.ba06
 ip address 192.168.50.1 255.255.255.0
 ip helper-address 192.168.5.3
!
```

IP ADDRESSING

A DHCP server is used in the LAN to provide each user PC with a dynamically assigned Ip address corresponding to the VLAN it is on, it also provides the PC with the default gateway for that VLAN. An IP address and default Gateway are essential for each PC and allows them to communicate with other PCs on the LAN, servers, other network devices and the internet.

DHCP POOLS		
ID	**IP RANGE**	**DEFAULT GATEWAY**
10	192.168.10.2-255	192.168.10.1
20	192.168.20.2-255	192.168.20.1
30	192.168.30.2-255	192.168.30.1
40	192.168.40.2-255	192.168.40.1
50	192.168.50.2-255	192.168.50.1

LAN pools are created on the server to assign an IP address in a range of IP addresses to PCs on a specific VLAN. The default gateway is also a part of each LAN pool and is given out to the PCs. Certain IP addresses are excluded from the LAN pools that are or will be assigned to other devices that need unchanging IP addresses.



DHCP

Interface: GigabitEthernet0
Service ● On ○ Off
Pool Name: LanPool10
Default Gateway: 192.168.10.1
DNS Server: 0.0.0.0
Start IP Address : 192 168 10 10
Subnet Mask: 255 255 255 0
Maximum Number of Users : 200
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
LanPool50	192.168.50.1	0.0.0.0	192.168.50.10	255.255.255.0	200	0.0.0.0	0.0.0.0
LanPool40	192.168.40.1	0.0.0.0	192.168.40.10	255.255.255.0	200	0.0.0.0	0.0.0.0
LanPool30	192.168.30.1	0.0.0.0	192.168.30.10	255.255.255.0	200	0.0.0.0	0.0.0.0
LanPool10	192.168.10.1	0.0.0.0	192.168.10.10	255.255.255.0	200	0.0.0.0	0.0.0.0
LanPool20	192.168.20.1	0.0.0.0	192.168.20.10	255.255.255.0	200	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.5.0	255.255.255.0	200	0.0.0.0	0.0.0.0

An IP helper address is assigned to each SVI on MLS1 to allow PCs on different VLANs to contact the DHCP server and receive an IP address and Default Gateway.

Static IP addresses are assigned to some of the network devices. All the switches have a manually assigned IP address in the range of 192.168.90.1 to 192.168.90.255 with a subnet mask of /24. Dynamic addresses would not be suitable for the switches as having a different IP address for each switch at different times would lead to confusion, accessing each switch and maintaining the network.

The DHCP server has a static IP address, so the IP helper address on MLS1 can allow the PCs to contact the DHCP server.

Each of the IP phones have IP addresses statically assigned. This was chosen to make sure that a person could always contact the same Ip phone. I was unable to assign the IP addresses to the IP phones in the topology as I do not understand how to configure the Ip phones in cisco packet tracer.

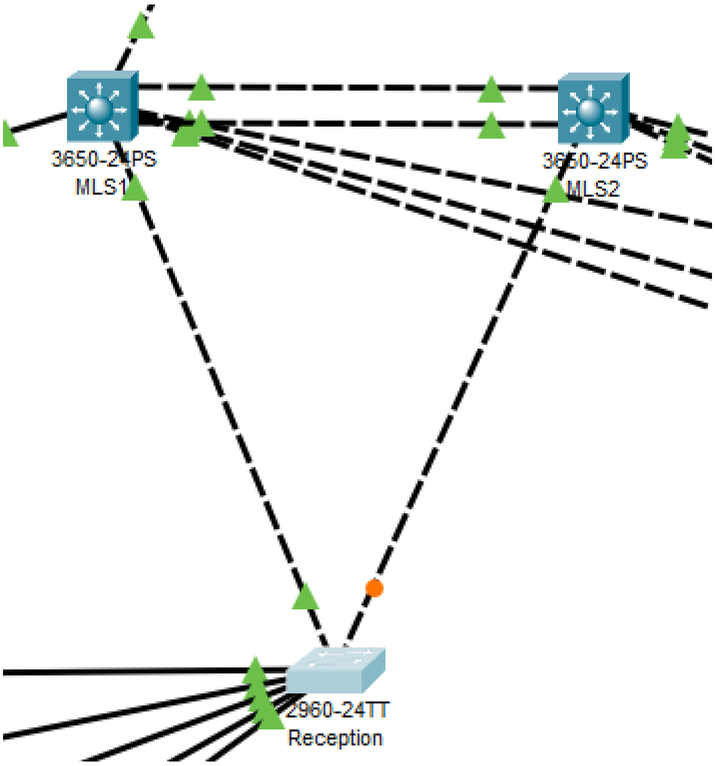
STATIC IP		
DEVICE	**IP**	**SUBNET MASK**
MLS1	192.168.90.1	/24
MLS2	192.168.90.2	/24
Reception	192.168.90.3	/24
General	192.168.90.4	/24
A&E	192.168.90.5	/24
Ambulance	192.168.90.6	/24
DHCP	192.168.5.3	/24
Ip phone 0	192.168.100.3	/24
Ip phone 1	192.168.100.4	/24
Ip phone 2	192.168.100.5	/24
Ip phone 3	192.168.100.6	/24
WAN PC	192.168.254.2	/30
MLS WAN PORT	192.168.254.1	/30

REDUNDANCY

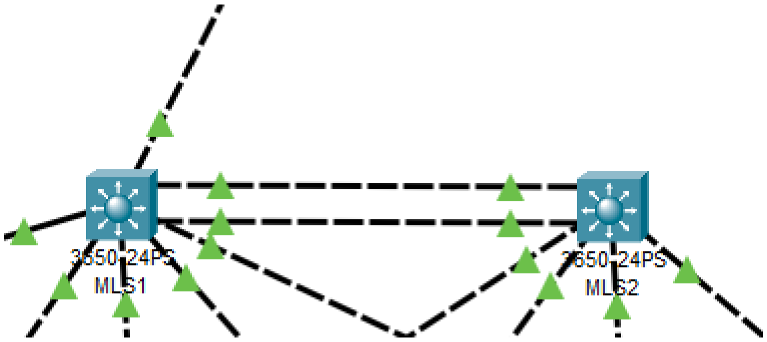
To provide high availability and redundancy in the network every switch is connected to at minimum two other switches. This provides the ethernet frames being sent from switch to switch at least two paths to travel to their destination. This creates physical loops in the LAN which could cause broadcast storms. STP is implemented in the LAN which allows us to use these loops effectively. STP logically blocks one port from the switch when a loop occurs. STP will unblock the closed port if the other port no longer works. This ensures frames from the switch can still be delivered to its destination.

In this prototype STP is implemented with MLS1 being the root bridge, which makes all network traffic flow through it as a priority. This is used to decide the shortest path to MLS1 and the port on each switch that has the longest path to MLS1 is blocked.

SPANNING TREE PROTOCOL	
DEVICE	**BRIDGE ID**
MLS1	Primary
MLS2	Secondary
RECEPTION	Default Value
GENERAL	Default Value
A&E	Default Value
AMBULANCE	Default Value



Ether Channel is also implemented it then LAN. Ether channel groups connections of the same speed allowing them to be used together to create one channel of higher speed. This provides quicker data travel on the LAN. In this prototype only one Ether channel is setup between MLS1 and MLS2. If the prototype is chosen as the LAN used by the MetroHealth hospital all connections between switches will be Ether channel.


3650-24PS
MLS1
3650-24PS
MLS2

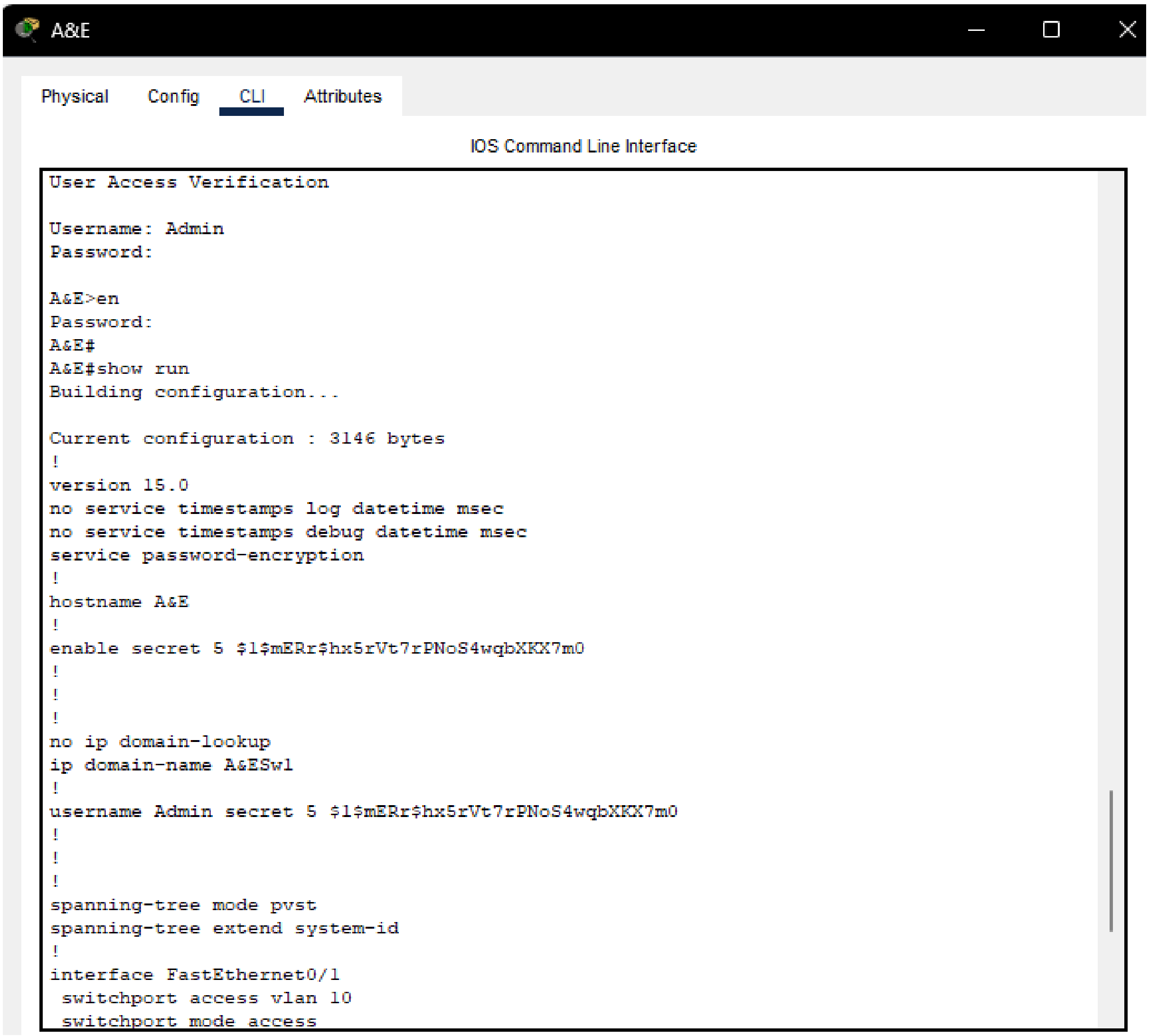
SECURITY MEASURES

Several security measures were implemented in the prototype to prevent unauthorized access to network devices. This protects the devices from attacks, ensuring the availability of services.

Local accounts and configuration mode passwords are set on all network devices to secure from unauthorized access. A username and password are necessary to access all the network devices privileged Exec mode and configuration files. All console, VTY and auxiliary lines to the network devices require a local account and password to access the device. All passwords are encrypted so they are not in plain text in the configuration files. In the prototype all passwords are cisco, however in the real-world implementation of the LAN, passwords will be much stronger and password rules will be implemented.

I added local accounts to the switches with a privilege level of 15, which should allow said user to be in privileged exec mode from login, however in cisco packet tracer whenever I created these accounts and restarted the switches the users privilege level would be set to 5 instead of 15. This made me add the password for the privileged exec mode on all the switches as a security measure. This issue is present on all the layer 2 switches but does not affect the MLSs.

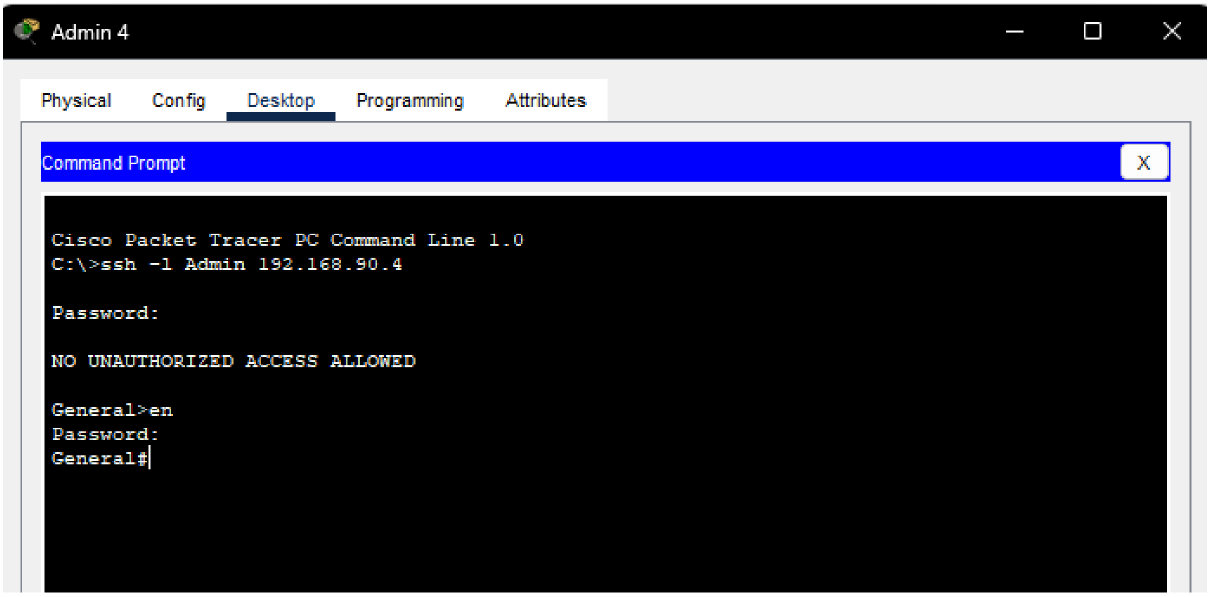
SECURITY		
Name	**Password**	**Privilege**
Admin	cisco	15
enable secret	cisco	15



```
User Access Verification

Username: Admin
Password:

A&E>en
Password:
A&E#
A&E#show run
Building configuration...

Current configuration : 3146 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname A&E
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
no ip domain-lookup
ip domain-name A&ESw1
!
username Admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
```

SSH has been implemented on the LAN to allow remote access to each of the switches and MLSs. SSH packets are encrypted so if an attacker gets the packets, they can't easily understand it. SSH is the only remote access protocol that is allowed to access the switches and MLSs all other methods have been disabled due to their insecurities such as Telnet being plain text. Each network device has been given a domain name to generate the encryption key to allow SSH access.

SSH	
Device	**Domain name**
MLS1	MLS1
MLS2	MLS2
RECEPTION	RecSw1
AMBULANCE	AmbSw1
A&E	AESw1
GENERAL	GenSw1

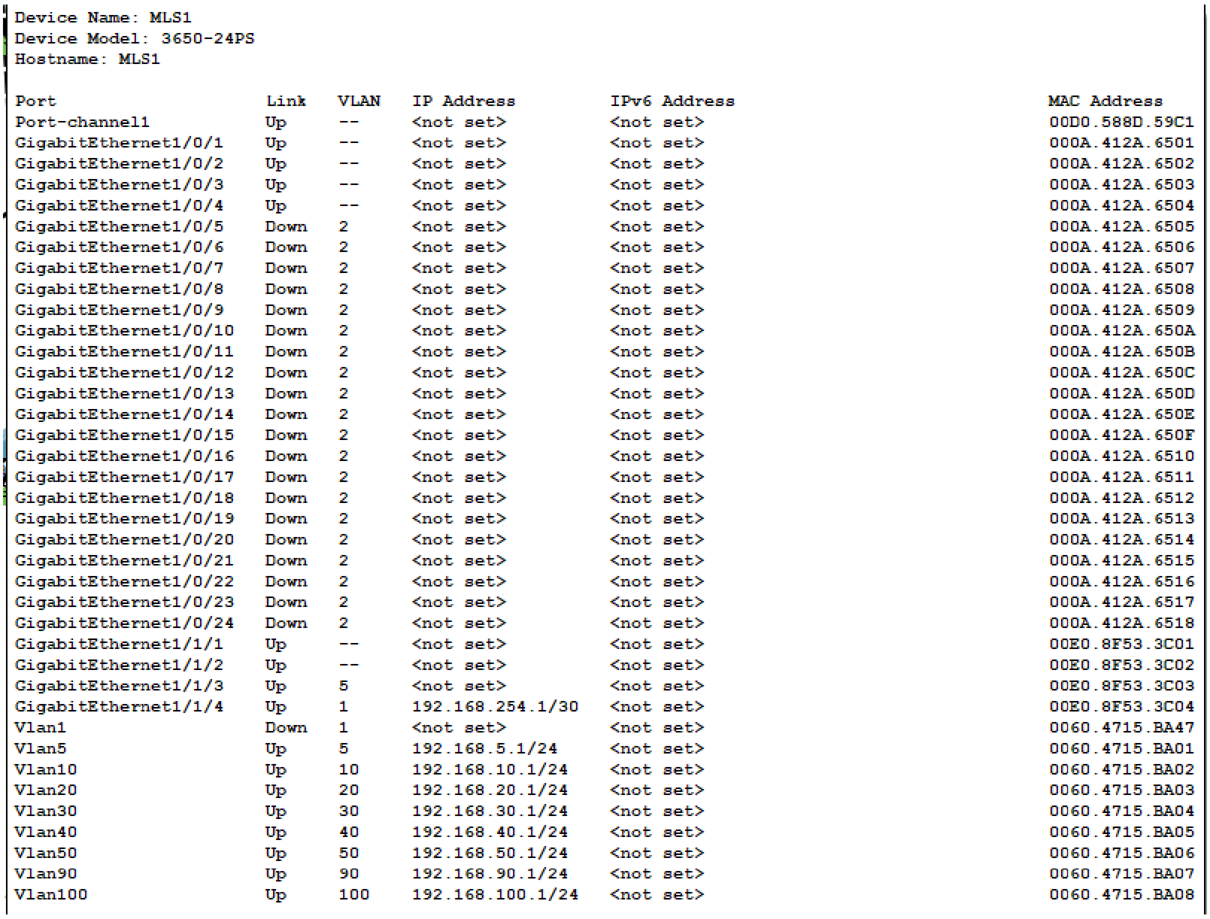


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Admin 192.168.90.4

Password:

NO UNAUTHORIZED ACCESS ALLOWED

General>en
Password:
General#
```

A Banner message is implemented on the login screen of all network devices to notify any person trying to access the device that if they are not authorized to access the device, they are punishable by the law. In the prototype the banner message is an example, however in the real-world implementation of the banner message, the legal department will be consulted for the exact wording in the message to deter and notify attackers.

The port-to-port connections on the switches are statically made into trunk ports disabling DTP to make it harder for attackers to access User Data on the LAN, the VLANs that can send frames through those ports are also set at this time, only allowing data from the necessary VLANS to travel through these ports.

Ports that are not being used to connect devices have been shut off and moved to the empty VLAN. This adds security to the LAN by making attackers unable to connect to the LAN through these ports.



```
Device Name: MLS1
Device Model: 3650-24PS
Hostname: MLS1

Port                    Link   VLAN   IP Address        IPv6 Address                              MAC Address
Port-channel1           Up     --     <not set>         <not set>                                 00D0.588D.59C1
GigabitEthernet1/0/1    Up     --     <not set>         <not set>                                 000A.412A.6501
GigabitEthernet1/0/2    Up     --     <not set>         <not set>                                 000A.412A.6502
GigabitEthernet1/0/3    Up     --     <not set>         <not set>                                 000A.412A.6503
GigabitEthernet1/0/4    Up     --     <not set>         <not set>                                 000A.412A.6504
GigabitEthernet1/0/5    Down   2      <not set>         <not set>                                 000A.412A.6505
GigabitEthernet1/0/6    Down   2      <not set>         <not set>                                 000A.412A.6506
GigabitEthernet1/0/7    Down   2      <not set>         <not set>                                 000A.412A.6507
GigabitEthernet1/0/8    Down   2      <not set>         <not set>                                 000A.412A.6508
GigabitEthernet1/0/9    Down   2      <not set>         <not set>                                 000A.412A.6509
GigabitEthernet1/0/10   Down   2      <not set>         <not set>                                 000A.412A.650A
GigabitEthernet1/0/11   Down   2      <not set>         <not set>                                 000A.412A.650B
GigabitEthernet1/0/12   Down   2      <not set>         <not set>                                 000A.412A.650C
GigabitEthernet1/0/13   Down   2      <not set>         <not set>                                 000A.412A.650D
GigabitEthernet1/0/14   Down   2      <not set>         <not set>                                 000A.412A.650E
GigabitEthernet1/0/15   Down   2      <not set>         <not set>                                 000A.412A.650F
GigabitEthernet1/0/16   Down   2      <not set>         <not set>                                 000A.412A.6510
GigabitEthernet1/0/17   Down   2      <not set>         <not set>                                 000A.412A.6511
GigabitEthernet1/0/18   Down   2      <not set>         <not set>                                 000A.412A.6512
GigabitEthernet1/0/19   Down   2      <not set>         <not set>                                 000A.412A.6513
GigabitEthernet1/0/20   Down   2      <not set>         <not set>                                 000A.412A.6514
GigabitEthernet1/0/21   Down   2      <not set>         <not set>                                 000A.412A.6515
GigabitEthernet1/0/22   Down   2      <not set>         <not set>                                 000A.412A.6516
GigabitEthernet1/0/23   Down   2      <not set>         <not set>                                 000A.412A.6517
GigabitEthernet1/0/24   Down   2      <not set>         <not set>                                 000A.412A.6518
GigabitEthernet1/1/1    Up     --     <not set>         <not set>                                 00E0.8F53.3C01
GigabitEthernet1/1/2    Up     --     <not set>         <not set>                                 00E0.8F53.3C02
GigabitEthernet1/1/3    Up     5      <not set>         <not set>                                 00E0.8F53.3C03
GigabitEthernet1/1/4    Up     1      192.168.254.1/30  <not set>                                 00E0.8F53.3C04
Vlan1                   Down   1      <not set>         <not set>                                 0060.4715.BA47
Vlan5                   Up     5      192.168.5.1/24    <not set>                                 0060.4715.BA01
Vlan10                  Up     10     192.168.10.1/24   <not set>                                 0060.4715.BA02
Vlan20                  Up     20     192.168.20.1/24   <not set>                                 0060.4715.BA03
Vlan30                  Up     30     192.168.30.1/24   <not set>                                 0060.4715.BA04
Vlan40                  Up     40     192.168.40.1/24   <not set>                                 0060.4715.BA05
Vlan50                  Up     50     192.168.50.1/24   <not set>                                 0060.4715.BA06
Vlan90                  Up     90     192.168.90.1/24   <not set>                                 0060.4715.BA07
Vlan100                 Up     100    192.168.100.1/24  <not set>                                 0060.4715.BA08
```