CS215

DATA COMMUNICATIONS AND MANAGEMENT

ASSIGNMENT 2

Group Members:
Vishant Chand (S11219214)
Shanesh Dewan (S11219250)
Fadheel Shah (S11219454)
Avnit Kumar (S11220543)


```
Switch>en
Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/2
10   Sales                             active    Fa0/1, Fa0/2, Fa0/3
20   HR                                active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
30   Finance                           active    Fa0/8, Fa0/9, Fa0/10
40   IT                                active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
50   Servers                           active    Fa0/15, Fa0/16, Fa0/17
60   Management                        active    Fa0/18, Fa0/19, Fa0/20
70   Printers                          active    Fa0/21, Fa0/22
80   PrinterServer                     active    Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

"VLANs are like coffee cups. You pour the data in, and it doesn't spill into anyone else's cup. Unless, of course, you mess up the trunking, and then it's coffee everywhere!"

Table of contents

Contents

Introduction

Overview:

This assignment aims on designing and implementing a secure network infrastructure for the XYZ Corporation using VLANs(Virtual LANs) for the specified departments . The company has decided to do a network upgrade or expansion which requires efficient IP addressing allocation using VLSM (Variable Length Subnet Mask) and better security implementations using ACLs (Access Control Lists). The corporation also requires all IP addresses to be distributed dynamically to different devices in a subnet using DHCP (Dynamic Host Configuration Protocol).

Objectives:

- Calculate the IP ranges for all departments specified based on their hosts requirements using VLSM(Variable Length Subnet Mask)
- Implement VLANs, DHCP, and inter-VLAN routing (router on a stick) to allow communication between different VLANs.
- Implement ACL (Access Control Lists) based on the security policies.
- Create a working network simulation in packet tracer meeting all requirements.

VLSM Calculation and IP Addressing

VLSM Working

Department	IPs/Hosts
Sales	50
HR	30
Finance	15
IT	10
servers	10
management	5
printers	5
print server	10

	128	64	32	16	8	4	2	1
bits (Power)	7	6	5	4	3	2	1	0

Step 1:

- Network given:
  172.16.0.0/16

- 172 – first octet is between 128 – 191, the address is Class B

Step 2:
default subnet mask for class be is 255.255.0.0
Default subnet mask for class B in binary is:
1111 1111. 1111 1111. 0000 0000. 0000 0000

Step 3:
Identify the largest network
Sales with 50 IP address

To accommodate 50 IP addresses
Usable IP Address = (2^n) – 2
N = 6, since 2^6 = 64

64 – 2
= 62

We require 50 Addresses and 62 is supplied.

Step 4:
Identify the new subnet mask
Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 6 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1100 0000
New subnet in decimal: 255.255.255.192
New subnet in CIDR: /26

Step 5:
Calculate update
Update = 256 – last octet of change
256 – 192 = 64

Step 6:
Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26	1 – 62	172.16.0.63

Repeat steps 3 to 6 until finished:

Second largest network
HR with 30 IP Addresses

To accommodate 30 IP addresses

Usable IP Address = (2^n) – 2
N = 5, since 2^5 = 32

32 – 2 = 30

We require 30 addresses and 30 is supplied

Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 5 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1110 0000
New subnet in decimal: 255.255.255.224
New subnet in CIDR: /27

Calculate update
Update = 256 – last octet of change
256 – 224 = 32

Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26	1 – 62	172.16.0.63
172.16.0.64 /27	65 – 94	172.16.0.95
172.16.0.96		

Third largest network
Finance with 15 IP Addresses

To accommodate 15 IP addresses
Usable IP Address = (2^n) – 2
N = 5, since 2^5 = 32

32 – 2 = 30

We require 15 addresses and 30 is supplied

Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 5 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1110 0000
New subnet in decimal: 255.255.255.224
New subnet in CIDR: /27

Calculate update
Update = 256 – last octet of change
256 – 224 = 32

Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26	1 – 62	172.16.0.63
172.16.0.64 /27	65 – 94	172.16.0.95
172.16.0.96 /27	97 – 126	172.16.0.127
172.16.0.128		

fourth largest network

IT with 10 IP Addresses

To accommodate 10 IP addresses
Usable IP Address = (2^n) – 2
N = 4, since 2^4 = 16

16 – 2 = 14

We require 10 addresses and 14 is supplied

Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 4 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1111 0000
New subnet in decimal: 255.255.255.240
New subnet in CIDR: /28

Calculate update
Update = 256 – last octet of change
256 – 240 = 16

Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26	1 – 62	172.16.0.63
172.16.0.64 /27	65 – 94	172.16.0.95
172.16.0.96 /27	97 – 126	172.16.0.127
172.16.0.128 /28	129 – 142	172.16.0.143
172.16.0.144 /		

fifth network

servers with 10 IP Addresses

To accommodate 10 IP addresses
Usable IP Address = (2^n) – 2
N = 4, since 2^4 = 16

16 – 2 = 14

We require 10 addresses and 14 is supplied

Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 4 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1111 0000
New subnet in decimal: 255.255.255.240
New subnet in CIDR: /28

Calculate update
Update = 256 – last octet of change
256 – 240 = 16

Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26	1 – 62	172.16.0.63
172.16.0.64 /27	65 – 94	172.16.0.95
172.16.0.96 /27	97 – 126	172.16.0.127
172.16.0.128 /28	129 – 142	172.16.0.143
172.16.0.144 /28	145 – 158	172.16.0.159
172.16.0.160		

sixth network
management with 5 IP Addresses

To accommodate 5 IP addresses
Usable IP Address = (2^n) – 2
N = 3, since 2^3 = 8

8 – 2 = 6

We require 5 addresses and 6 is supplied

Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 3 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1111 1000
New subnet in decimal: 255.255.255.248
New subnet in CIDR: /29

Calculate update
Update = 256 – last octet of change
256 – 248 = 8

Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26	1 – 62	172.16.0.63
172.16.0.64 /27	65 – 94	172.16.0.95
172.16.0.96 /27	97 – 126	172.16.0.127
172.16.0.128 /28	129 – 142	172.16.0.143
172.16.0.144 /28	145 – 158	172.16.0.159
172.16.0.160 /29	161-166	172.16.0.167
172.16.0.168 /		

seventh network

printer with 5 IP Addresses

To accommodate 5 IP addresses
Usable IP Address = (2^n) – 2
N = 3, since 2^3 = 8

8 – 2 = 6

We require 5 addresses and 6 is supplied

Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 3 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1111 1000
New subnet in decimal: 255.255.255.248
New subnet in CIDR: /29

Calculate update
Update = 256 – last octet of change
256 – 248 = 8

Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26	1 – 62	172.16.0.63
172.16.0.64 /27	65 – 94	172.16.0.95
172.16.0.96 /27	97 – 126	172.16.0.127
172.16.0.128 /28	129 – 142	172.16.0.143
172.16.0.144 /28	145 – 158	172.16.0.159
172.16.0.160 /29	161-166	172.16.0.167
172.16.0.168 /29	169-174	172.16.0.175
172.16.0.176 /		

Eighth network

Print Server with 5 IP Addresses

To accommodate 5 IP addresses
Usable IP Address = (2^n) – 2
N = 3, since 2^3 = 8

8 – 2 = 6

We require 5 addresses and 6 is supplied

Default subnet mask: 1111 1111. 1111 1111. 0000 0000. 0000 0000
Reserve 3 bits from the right and turn the remaining into 1's.
New subnet mask: 1111 1111. 1111 1111. 1111 1111. 1111 1000
New subnet in decimal: 255.255.255.248
New subnet in CIDR: /29

Calculate update
Update = 256 – last octet of change
256 – 248= 8

Update Networking list

network	Usable Ip range	Broadcast address
172.16.0.0 / 26 sales	1 – 62	172.16.0.63
172.16.0.64 /27 HR	65 – 94	172.16.0.95
172.16.0.96 /27 finance	97 – 126	172.16.0.127
172.16.0.128 /28 IT	129 – 142	172.16.0.143
172.16.0.144 /28 Server	145 – 158	172.16.0.159
172.16.0.160 /29 Management	161-166	172.16.0.167
172.16.0.168 /29 Printers	169-174	172.16.0.175
172.16.0.176 /29 Print Server	177 - 182	172.16.0.183

Configurations

VLAN Configuration

```
enable
configure terminal

vlan 10
name Sales
exit

vlan 20
name HR
exit

vlan 30
name Finance
exit

vlan 40
name IT
exit

vlan 50
name Servers
exit

vlan 60
name Management
exit
```

```
vlan 70
name Printers
exit

vlan 80
name Print_Server
exit

interface range fa0/1 - 3
switchport mode access
switchport access vlan 10
exit

interface range fa0/4 - 7
switchport mode access
switchport access vlan 20
exit

interface range fa0/8 - 10
switchport mode access
switchport access vlan 30
exit

interface range fa0/11 - 14
switchport mode access
switchport access vlan 40
exit

interface range fa0/15 - 17
```

```
switchport mode access
switchport access vlan 60
exit

interface range fa0/18 - 20
switchport mode access
switchport access vlan 50
exit

interface range fa0/21 - 22
switchport mode access
switchport access vlan 70
exit

interface range fa0/23 - 24
switchport mode access
switchport access vlan 80
exit

interface gigabitEthernet 0/1
switchport mode trunk
switchport trunk allowed vlan all
exit
```

DHCP pool configuration

```
enable
configure terminal

ip dhcp pool Sales
network 172.16.0.0 255.255.255.192
default-router 172.16.0.1
dns-server 8.8.8.8

ip dhcp pool HR
network 172.16.0.64 255.255.255.224
default-router 172.16.0.65
dns-server 8.8.8.8

ip dhcp pool Finance
network 172.16.0.96 255.255.255.224
default-router 172.16.0.97
dns-server 8.8.8.8

ip dhcp pool IT
network 172.16.0.128 255.255.255.240
default-router 172.16.0.129
dns-server 8.8.8.8

ip dhcp pool Servers
network 172.16.0.144 255.255.255.240
default-router 172.16.0.145
dns-server 8.8.8.8
```

```
ip dhcp pool Management
network 172.16.0.160 255.255.255.248
default-router 172.16.0.161
dns-server 8.8.8.8

ip dhcp pool Printers
network 172.16.0.168 255.255.255.248
default-router 172.16.0.169
dns-server 8.8.8.8

ip dhcp pool Printer_Server
network 172.16.0.176 255.255.255.248
default-router 172.16.0.177
dns-server 8.8.8.8

end
write memory
```

Router on a stick configuration

```
enable
configure terminal

interface gigabitEthernet 0/0/0
 no shutdown
 exit

interface gigabitEthernet 0/0/0.10
 encapsulation dot1Q 10
 ip address 172.16.0.1 255.255.255.192
 exit

interface gigabitEthernet 0/0/0.20
 encapsulation dot1Q 20
 ip address 172.16.0.65 255.255.255.224
 exit

interface gigabitEthernet 0/0/0.30
 encapsulation dot1Q 30
 ip address 172.16.0.97 255.255.255.224
 exit

interface gigabitEthernet 0/0/0.40
 encapsulation dot1Q 40
 ip address 172.16.0.129 255.255.255.240
 exit

interface gigabitEthernet 0/0/0.50
 encapsulation dot1Q 50
```

```
 ip address 172.16.0.145 255.255.255.240
 exit

interface gigabitEthernet 0/0/0.60
 encapsulation dot1Q 60
 ip address 172.16.0.161 255.255.255.248
 exit

interface gigabitEthernet 0/0/0.70
 encapsulation dot1Q 70
 ip address 172.16.0.169 255.255.255.248
 exit

interface gigabitEthernet 0/0/0.80
 encapsulation dot1Q 80
 ip address 172.16.0.177 255.255.255.248
 exit

end
write memory
```

Access Control Lists (ACL) configuration

```
Extended IP access list HR->FINANCE
    10 deny ip 172.16.0.64 0.0.0.31 172.16.0.96 0.0.0.31
    20 permit ip any any

Extended IP access list SALES->IT
    10 deny ip 172.16.0.0 0.0.0.63 172.16.0.128 0.0.0.15
    20 permit ip any any

Extended IP access list IT->FINANCE
    10 deny ip 172.16.0.128 0.0.0.15 172.16.0.96 0.0.0.31
    20 permit ip any any

Extended IP access list DENY-ACCESS-TO-SERVERS
    10 deny ip 172.16.0.0 0.0.0.63 172.16.0.144 0.0.0.15
    20 deny ip 172.16.0.64 0.0.0.31 172.16.0.144 0.0.0.15
    30 deny ip 172.16.0.96 0.0.0.31 172.16.0.144 0.0.0.15
    40 permit ip any any

Extended IP access list ALLOW-PRINTER-TO-PRINTSERVER
    10 permit ip 172.16.0.168 0.0.0.7 172.16.0.176 0.0.0.7

Extended IP access list SERVER->DHCPSERVER
    10 deny ip 172.16.0.0 0.0.0.63 172.16.0.144 0.0.0.15
    20 deny ip 172.16.0.96 0.0.0.31 172.16.0.144 0.0.0.15
    30 deny ip 172.16.0.64 0.0.0.31 172.16.0.144 0.0.0.15
    40 permit ip any any

Extended IP access list IP->ROUTER
    10 permit ip 172.16.0.128 0.0.0.15 172.16.0.0 0.0.0.63
```

```
    20 deny ip 172.16.0.0 0.0.0.63 172.16.0.128 0.0.0.15
    30 permit ip 172.16.0.128 0.0.0.15 host 172.16.0.129
    40 permit ip any any

Extended IP access list ACCESS-TO-SALES
    10 permit ip 172.16.0.128 0.0.0.15 172.16.0.0 0.0.0.63
    20 permit ip any any

Extended IP access list ACCESS-TO-HR
    10 permit ip any any

Extended IP access list FINANCE->ROUTER
    10 permit ip 172.16.0.96 0.0.0.31 host 172.16.0.97

interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 172.16.0.1 255.255.255.192
 ip access-group ACCESS-TO-SALES out

interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 172.16.0.65 255.255.255.224
 ip access-group ACCESS-TO-HR out

interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 172.16.0.97 255.255.255.224
 ip access-group FINANCE->ROUTER out

interface GigabitEthernet0/0/0.40
```

```
 encapsulation dot1Q 40
 ip address 172.16.0.129 255.255.255.240
 ip access-group IP->ROUTER out

interface GigabitEthernet0/0/0.50
 encapsulation dot1Q 50
 ip address 172.16.0.145 255.255.255.240
 ip access-group SERVER->DHCPSERVER out

interface GigabitEthernet0/0/0.60
 encapsulation dot1Q 60
 ip address 172.16.0.161 255.255.255.248

interface GigabitEthernet0/0/0.70
 encapsulation dot1Q 70
 ip address 172.16.0.169 255.255.255.248

interface GigabitEthernet0/0/0.80
 encapsulation dot1Q 80
 ip address 172.16.0.177 255.255.255.248
 ip access-group ALLOW-PRINTER-TO-PRINTSERVER out
```

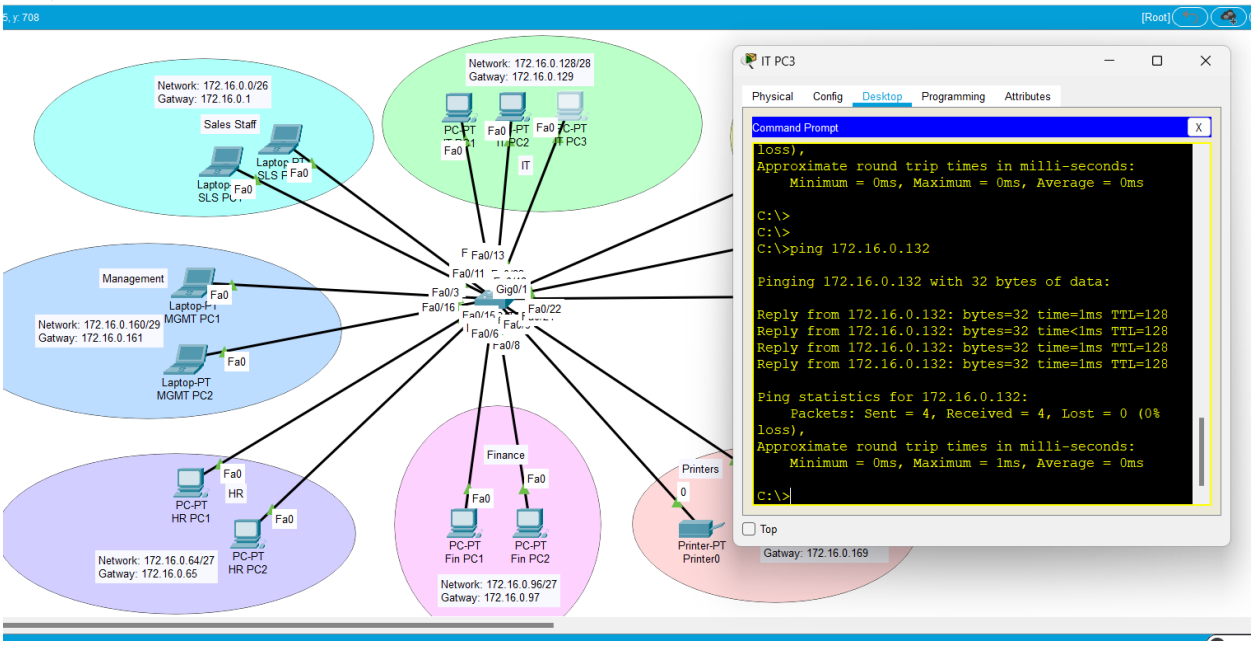
Connectivity Test Results

VLAN Connectivity

- VLANs created and assigned to specific ports.

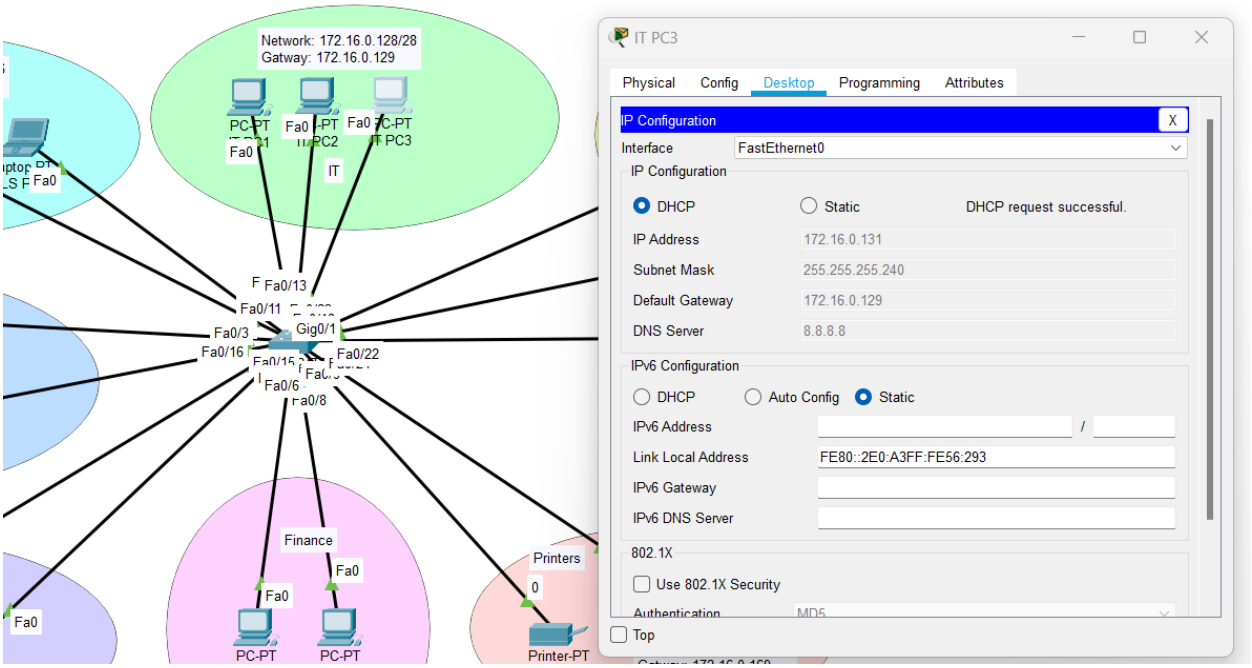
```
Switch>en
Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/2
10   Sales                             active    Fa0/1, Fa0/2, Fa0/3
20   HR                                active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
30   Finance                           active    Fa0/8, Fa0/9, Fa0/10
40   IT                                active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
50   Servers                           active    Fa0/18, Fa0/19, Fa0/20
60   Management                        active    Fa0/15, Fa0/16, Fa0/17
70   Printers                          active    Fa0/21, Fa0/22
80   Print_Server                      active    Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

- Successful ping between devices on the same VLAN (IT).



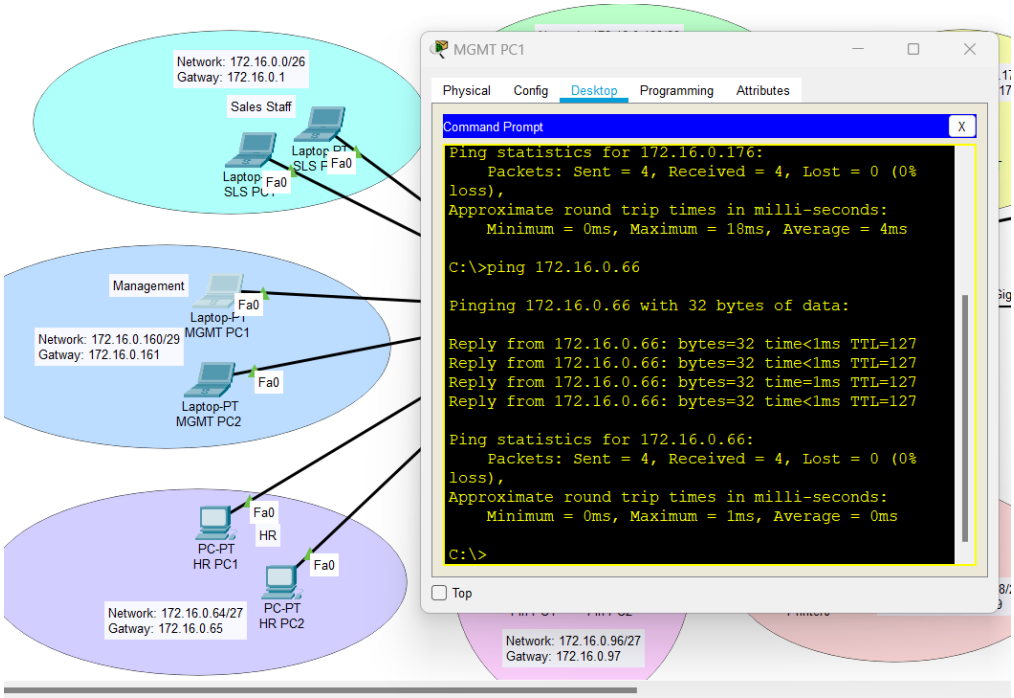
DHCP Functionality

- Devices are getting their IP addresses dynamically through DHCP



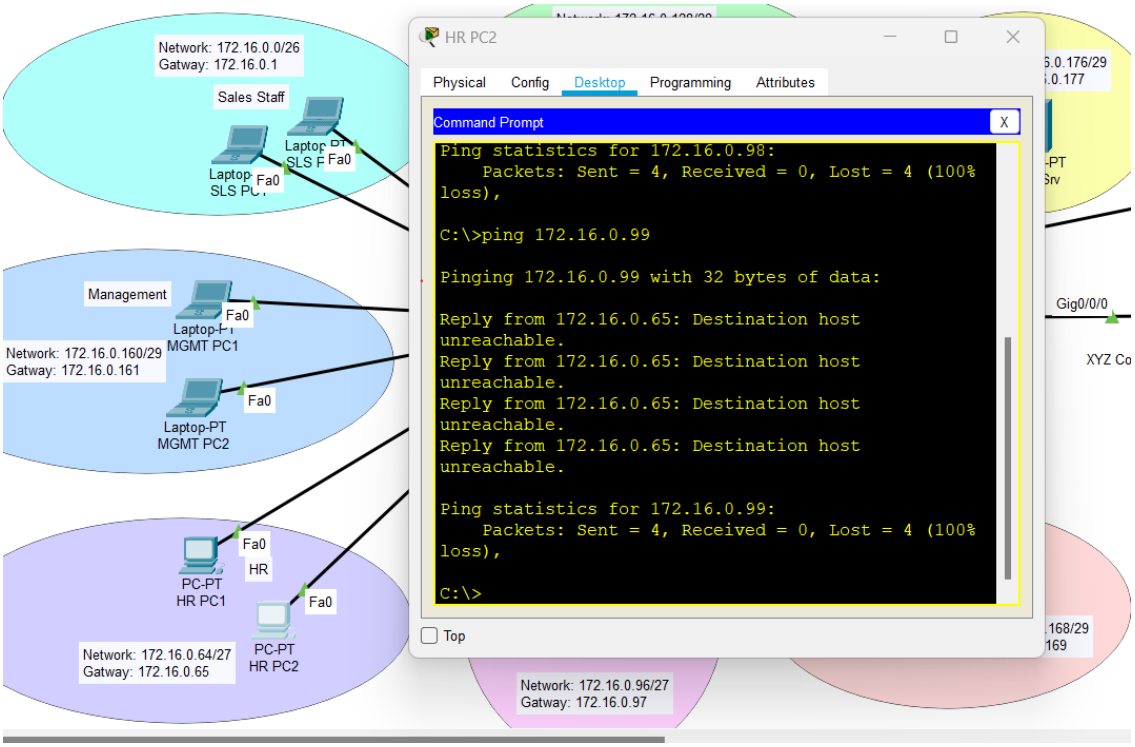
Router on a Stick Verification

- Successful ping between Management & HR (Different VLANs)

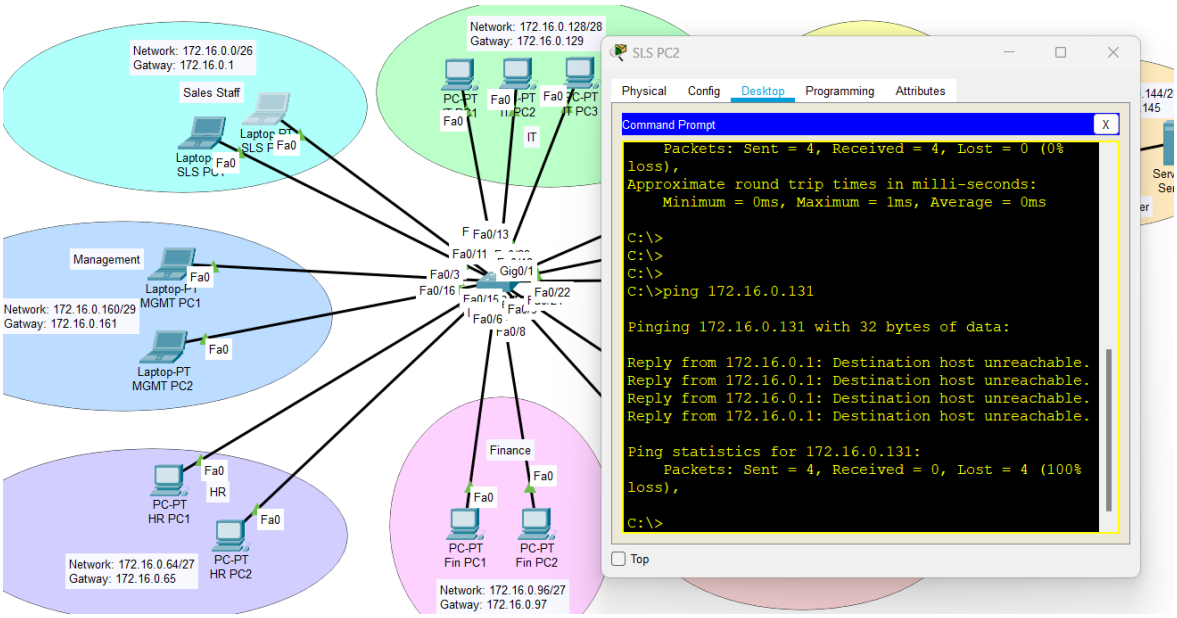


ACL Verification

- HR staff should not have access to Finance data. Implement an ACL to deny HR access to Finance VLAN.

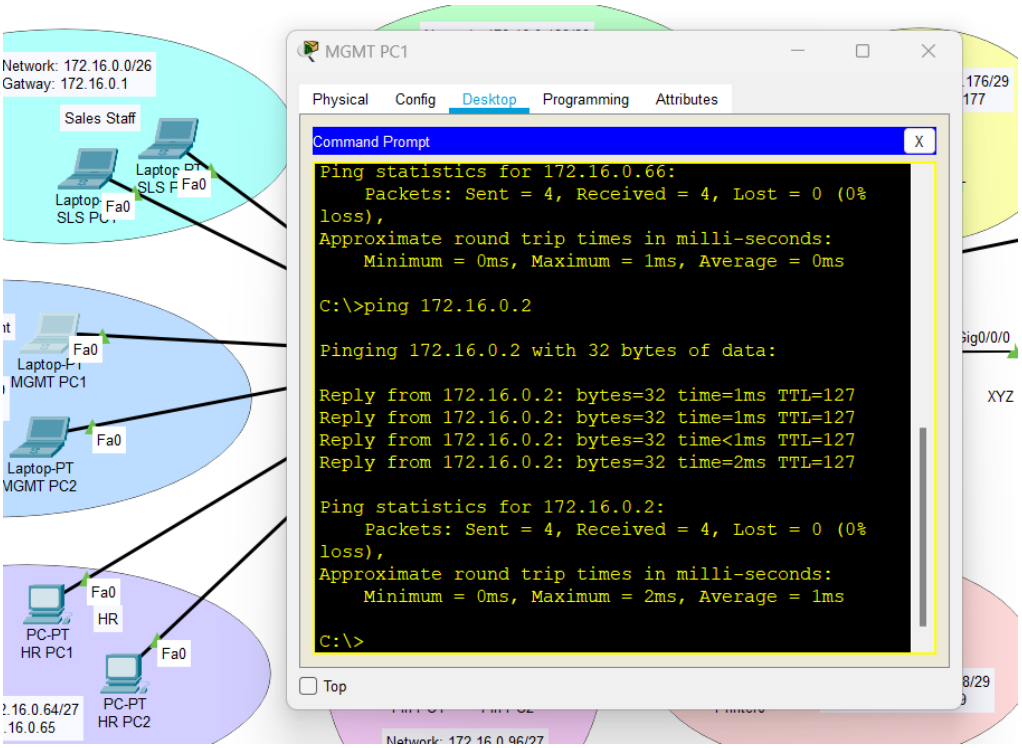


- Sales staff should not have access to IT resources. Implement an ACL to deny Sales VLAN access to the IT VLAN.

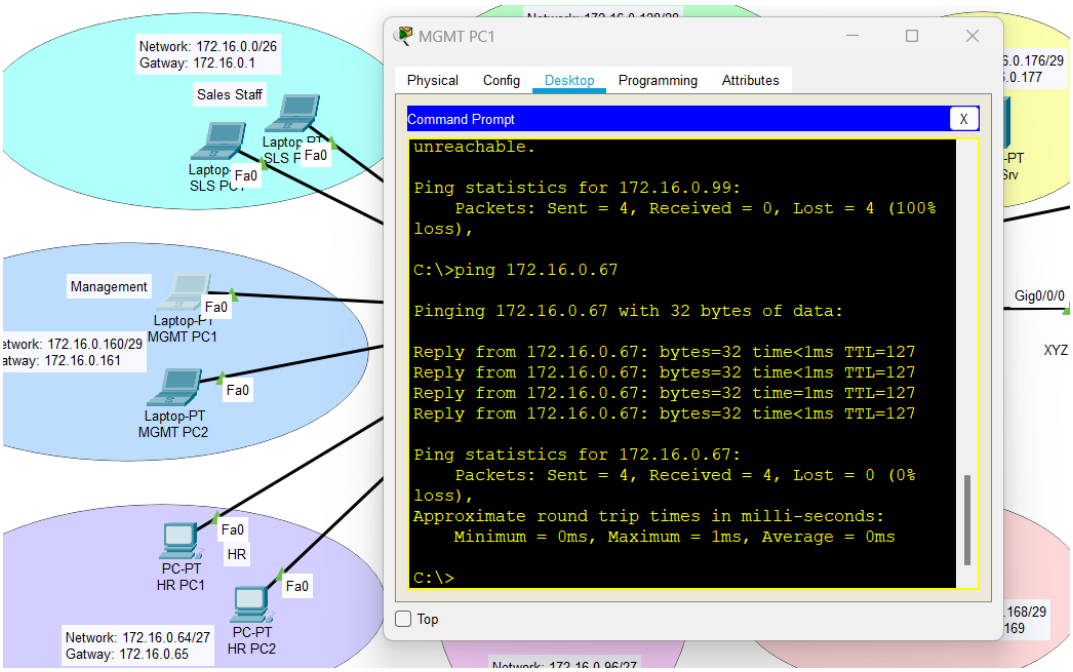


- Management will have full access to all departments. Create an ACL that permits traffic from the Management VLAN to all other VLANs.

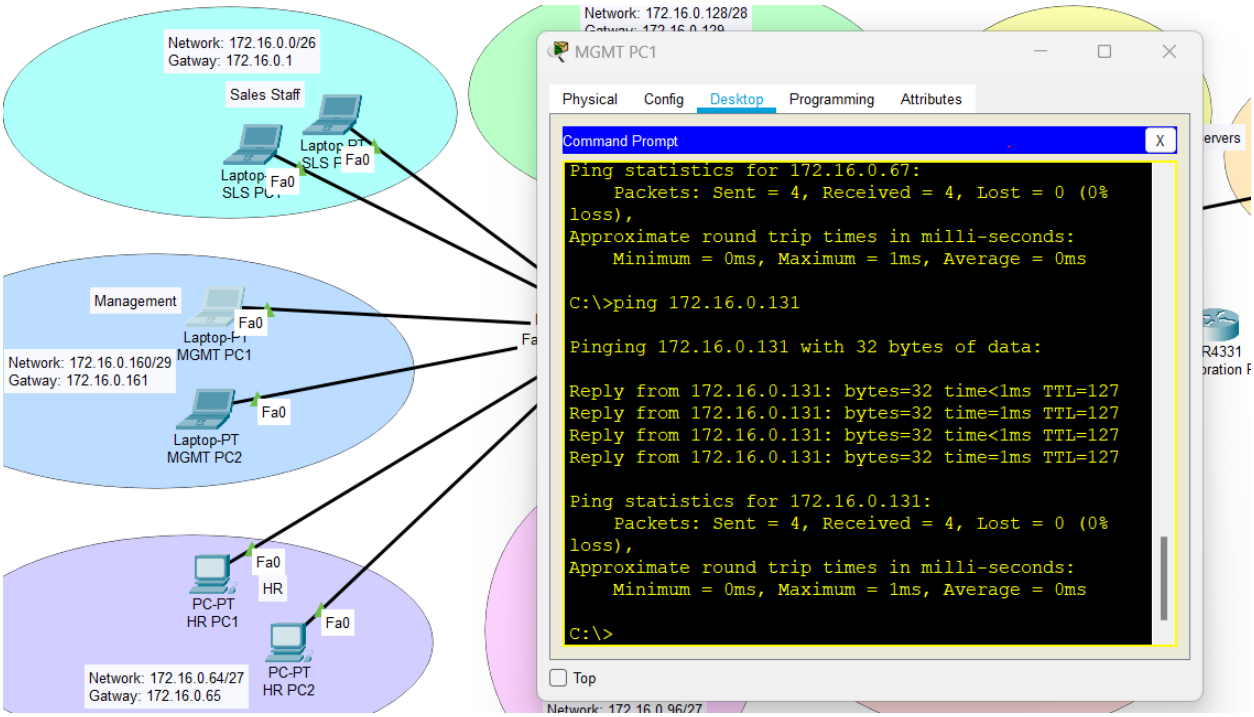
Management to Sales Staff



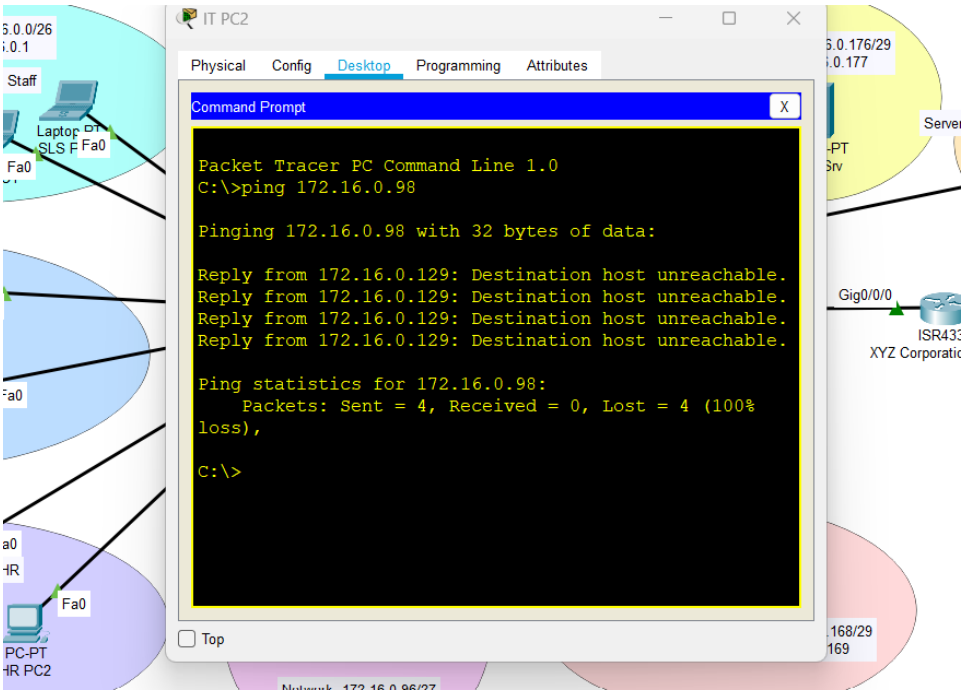
Management to HR



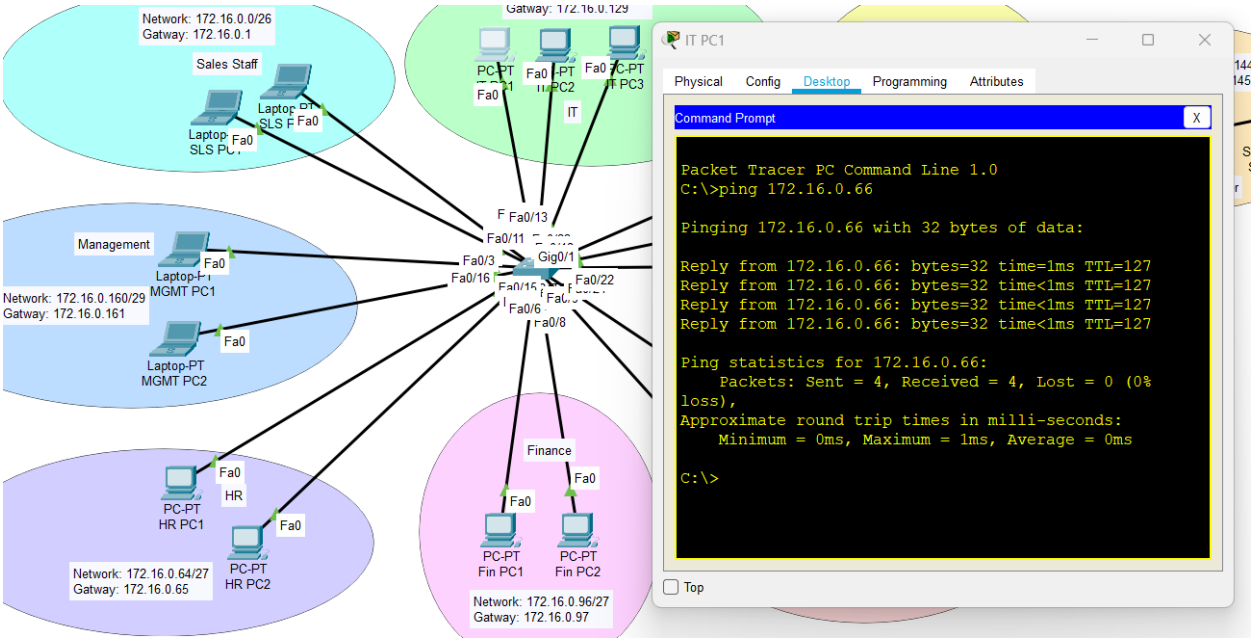
Management to IT



- Implement an ACL that denies IT VLAN access to Finance VLAN while allowing access to Sales and HR.

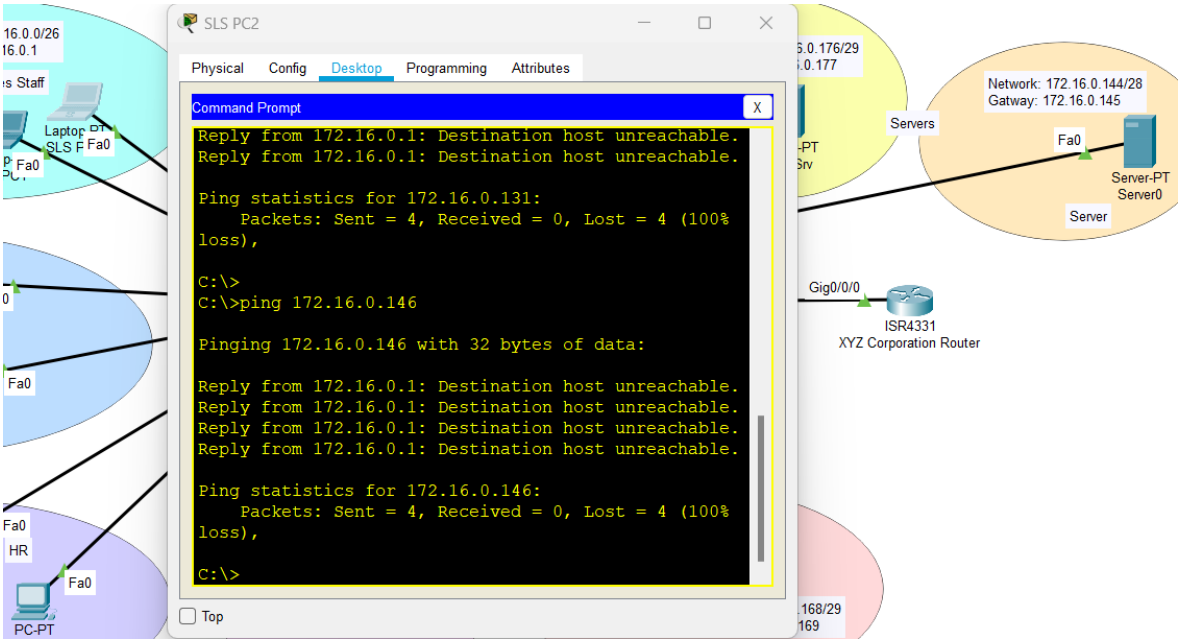


IT can access HR

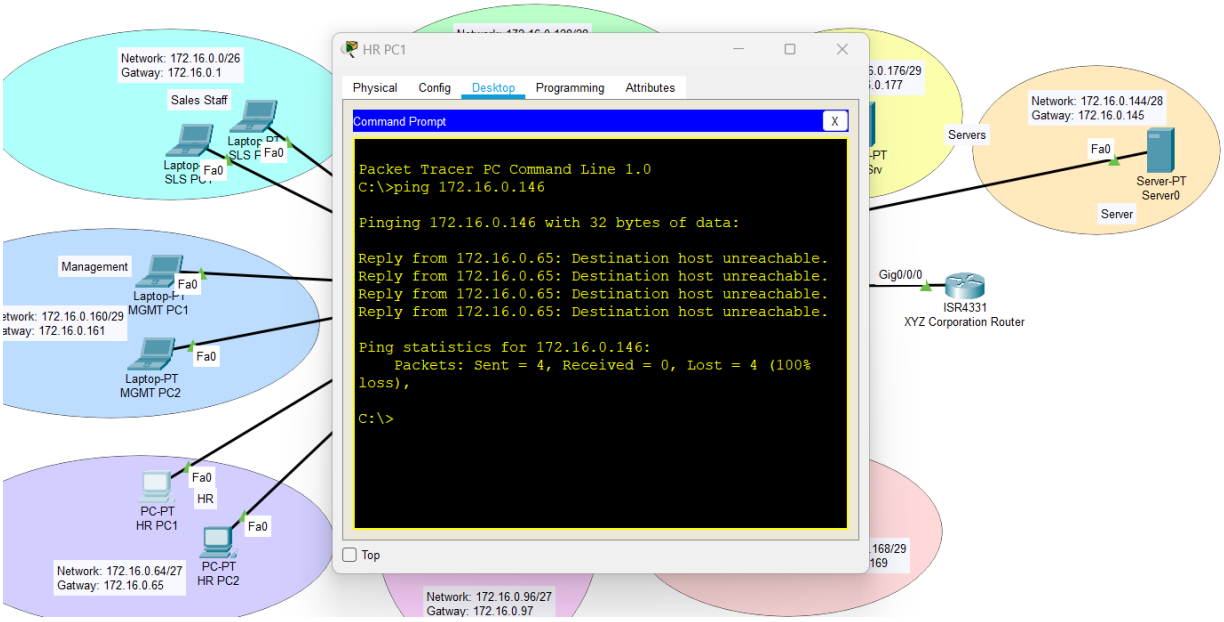


- Sales, HR, and Finance can access servers, which they should not. i.e. Only the Management and IT VLANs should be allowed to access the Servers VLAN. Deny access to all other VLANs.

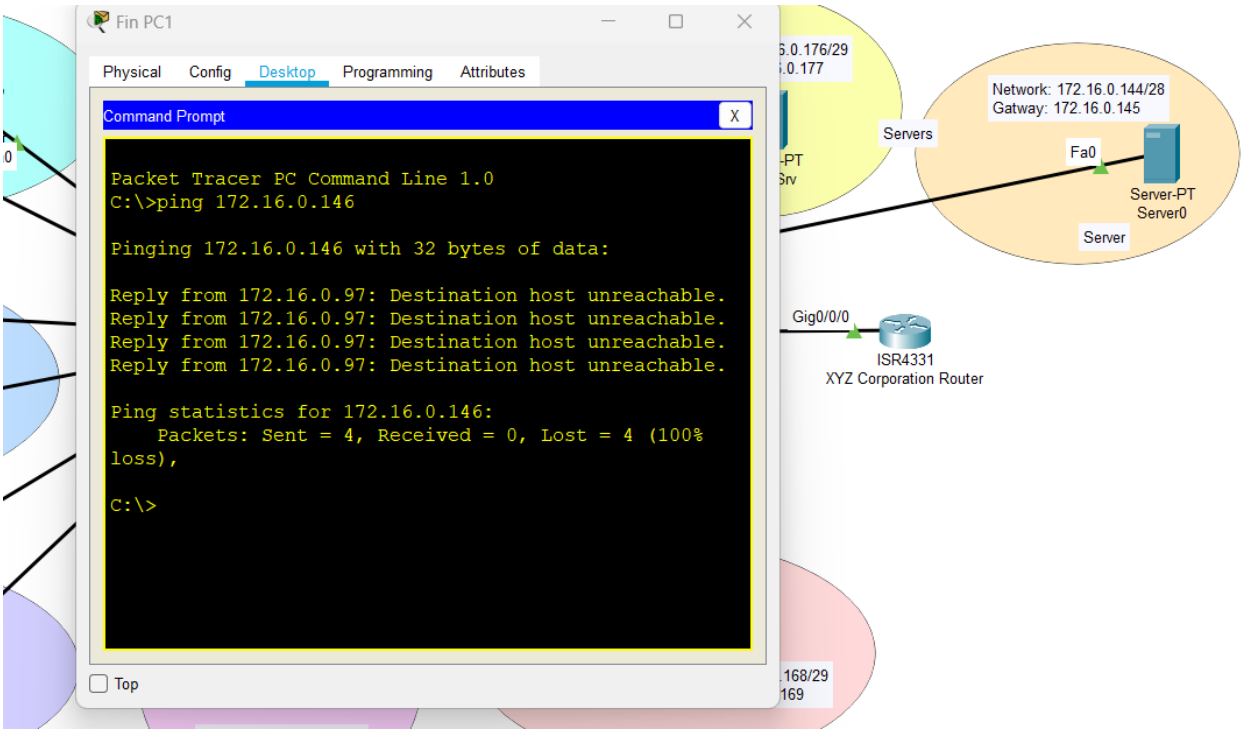
Sales cannot access Servers VLANs



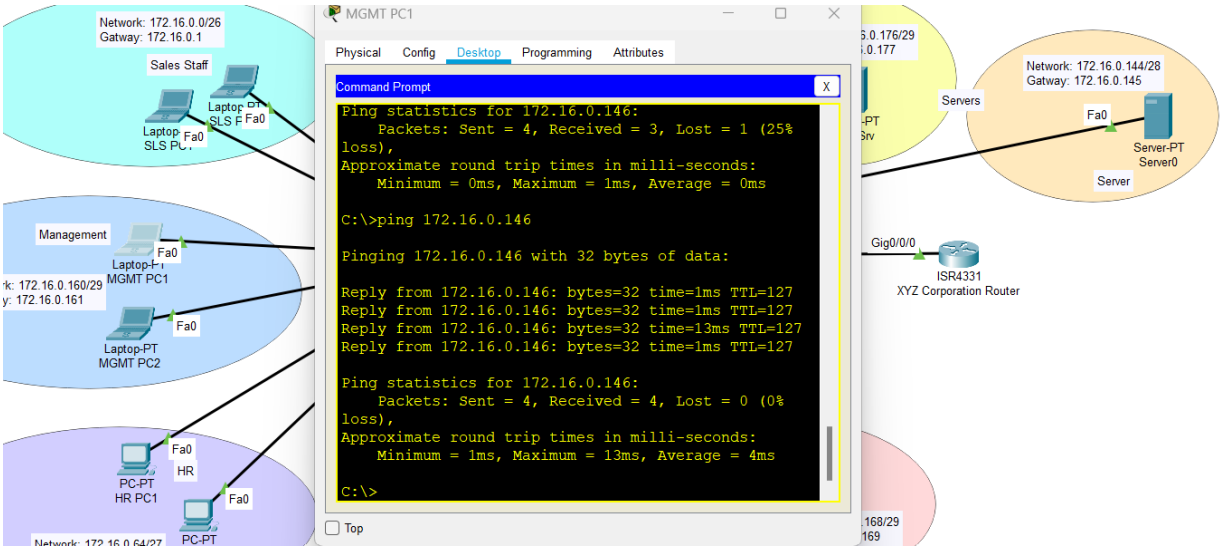
HR cannot access Servers VLANs



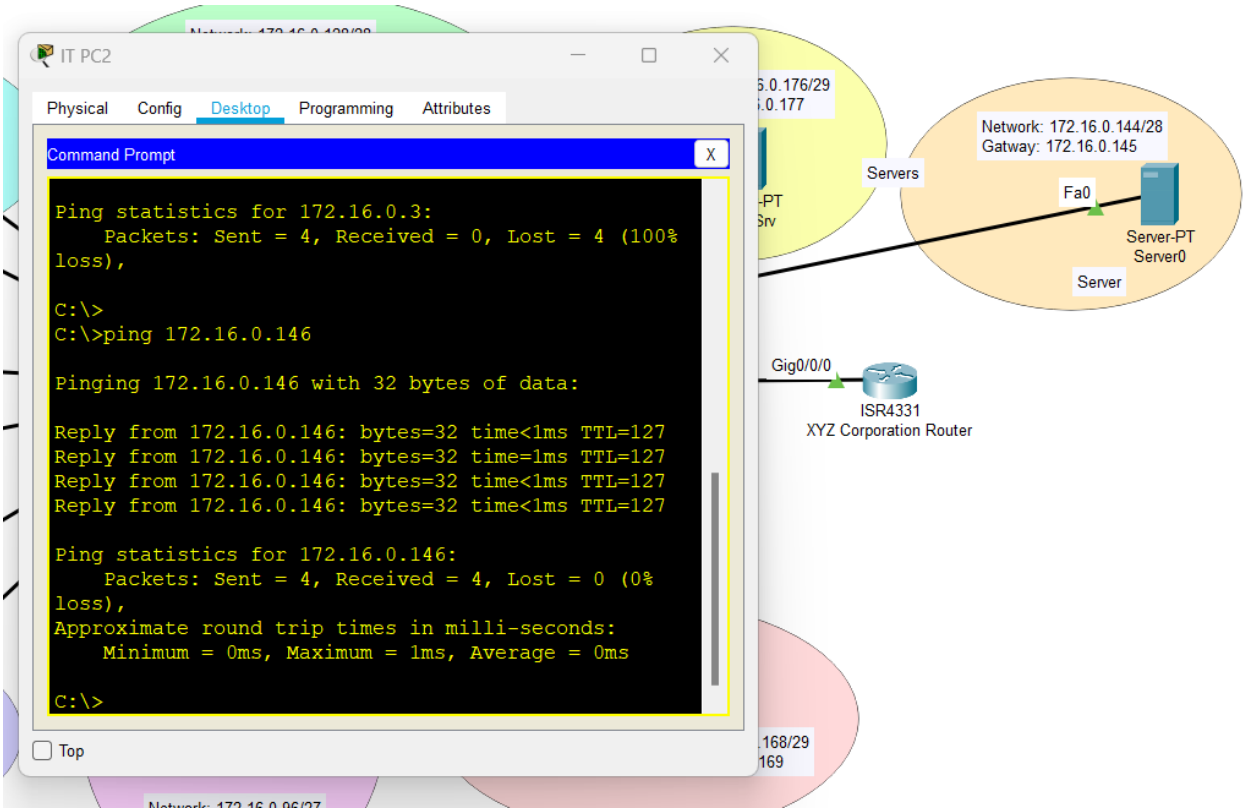
Finance cannot access Servers VLANs



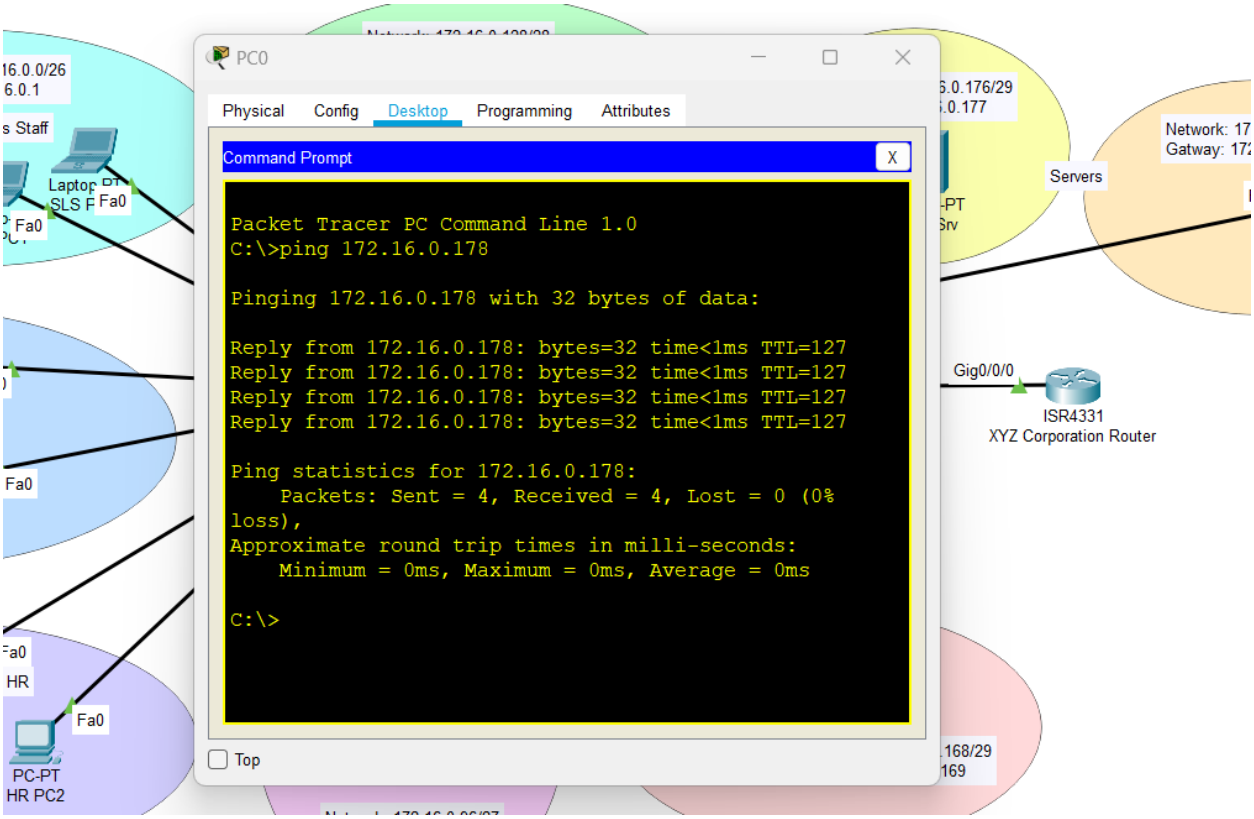
Management can access Servers VLANs



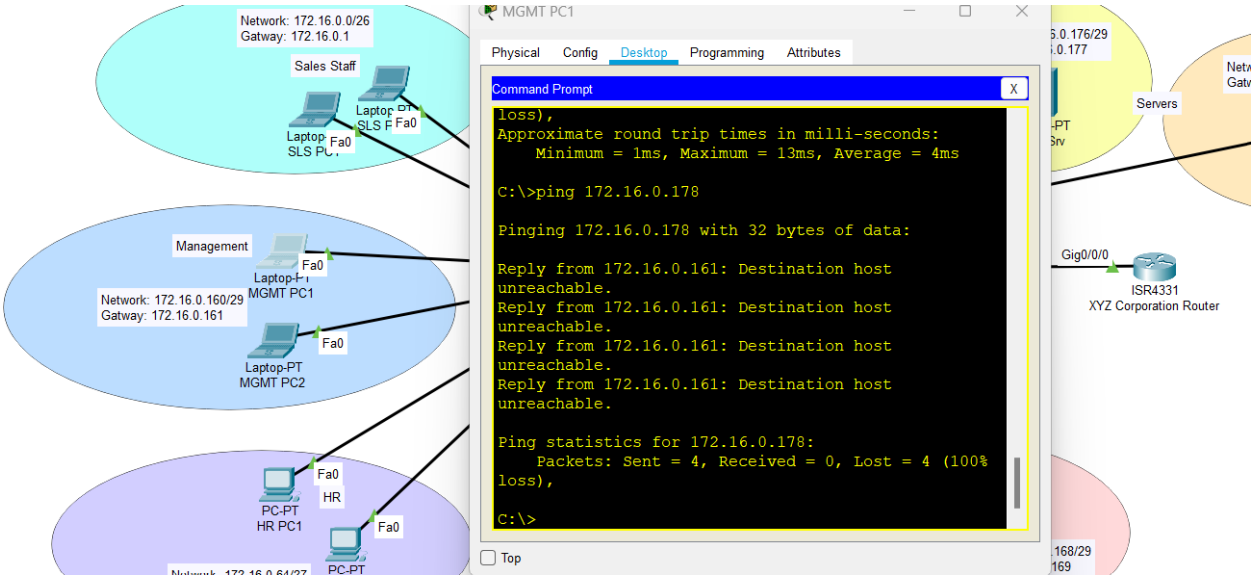
IT can access Servers



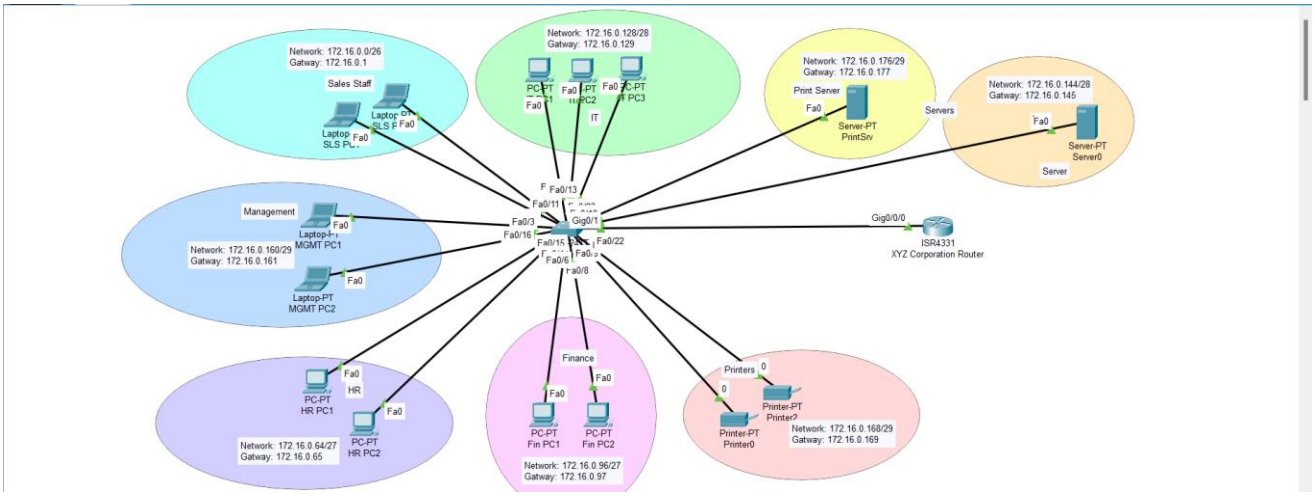
Print Server can only communicate with Printers.(To test for connectivity between printer and print server we place a PC and ping to the Print Server)



Other departments like Management cannot access Print Server



Network Design



Network Requirements met:

- All departments are in a separate VLAN
- IP allocation is done through VLSM
- IP are assigned dynamically through a DHCP pool
- Inter VLAN routing to allow communication between devices on different VLANs
- ACL rules are implemented
- Print server can only be accessed by Printer VLAN.

Documentation Requirements met:

- Show all calculations for VLSM
- All tables are filled
- All configurations used for VLAN, DHCP, router, and ACL are shown
- Connectivity test results
- Brief explanation on ACL and VLSM.

Security Considerations

how ACLs are used to secure the network

ACL(Access Control Lists) are a set of rules that controls which traffic is permitted to access the network. ACLs are configured in the router or a layer 3 switch, these security policies are implemented by the network administrator where specific IP addresses, subnets or services are either permitted or denied.

ACLs contribute towards:

- Traffic filtering: based on security policies implemented, unauthorized devices cannot communicate with devices on other networks. This will help keep sensitive data protected from unauthorized acc.
- Restrict VLAN Access: Implementing ACLs on a router can help isolate VLANs which will protect data as well as improve network performance.
- Monitoring: ACLs can also assist network administrators to log and monitor activities on the suspicious activity on the network, this prevents the risk of cyberattacks.

IP Optimization Using VLSM

how VLSM optimizes the IP address allocation:

VLSM(Variable Length Subnet Mask)- is a subnetting technique used when designing a network where it allows network administrators to create subnets with different subnet masks.

VLSM optimizes the IP allocation by:

- Efficient IP usage: when using VLSM, it allows only the required number of IP addresses to be used based on the host requirements of each network segments. This eliminates IP addresses from being wasted compared to when using FLSM(Fixed Length Subnet Mask)
- Better flexibility: VLSM allows network administrators to design IP addressesing schemes on varying subnet sizes based on the requirements of hosts.

Conclusion

In conclusion, the requirements for the network design was met by calculating the IP addresses based on the hosts for each departments. VLSM helps in a more optimized and efficient subnetting technique and allows for more flexibility. All IP addresses were allocated to different devices through a configured DHCP pool. VLANs were implemented to allow network segregation and better network performance. Furthermore, to allow for better security in the network we had to configure ACLs(Access Control Lists) to control which traffic can enter a subnet and which devices can communicate with each other. This is crucial to prevent sensitive information for the company from being exploited by hackers. A fully functional network was then designed in packet tracer with few limitations when configuring as it is not similar to a configuring a real physical networking equipment, however, all the necessary features were implemented, and connectivity tests were conducted .