

Cisco IOS Configuration and Network Analysis

DCCN2 Assignment 1

● Successful	PC11	PC0
● Successful	PC10	PC3

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Network_Department
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Software_Department
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Technical_Department
Switch(config-vlan)#exit
Switch(config)#exit

```

Submitted By,

U.Anogan - SA23523128

Contents

Introduction3

Task 1: VLAN Configuration4

Task 2: Variable-Length Subnetting (VLSM) and Classless IP Addressing 11

Task 3: Port Security Configuration 19

Task 4: DHCP Configuration on Routers25

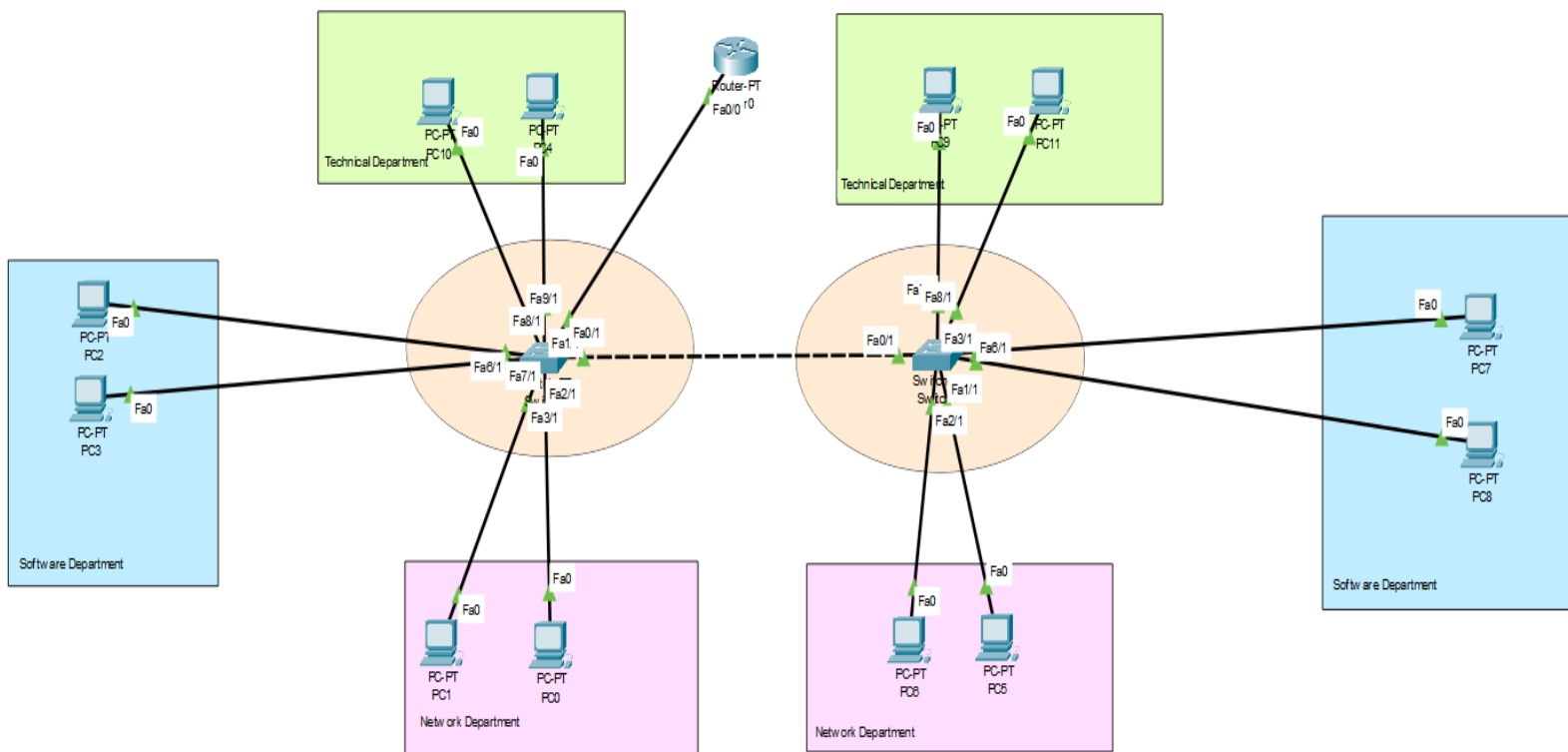
Task 5: Network Analysis using Wireshark29

Conclusion.....34

Introduction

In today's interconnected world, small to medium-sized enterprises (SMEs) require robust network solutions to facilitate communication across various departments while ensuring security and efficiency. This assignment involves configuring a network for a fictional SME using Cisco IOS, focusing on five critical tasks: VLAN configuration, Variable-Length Subnet Masking (VLSM) for efficient IP addressing, port security implementation, DHCP configuration for dynamic IP assignment, and network analysis using Wireshark.

The primary objective is to design and implement a secure network infrastructure that accommodates departmental communication needs while maintaining traffic isolation.



Task 1: VLAN Configuration

➤ Objective

To create VLANs for different departments, assign switch ports to VLANs, and enable inter-VLAN routing to allow communication between departments while maintaining isolation unless explicitly allowed.

1. Switch and PC Setup:

- ✓ Created two switches: PT Switch 0 and PT Switch 1.
- ✓ Connected 6 PCs to each switch (12 PCs total).
- ✓ Connected PT Switch 0 and PT Switch 1 using a trunk link.

2. VLAN Creation:

- ✓ VLAN10 (Network Department) for PCs: PC0, PC1, PC5, PC6.
- ✓ VLAN20 (Software Department) for PCs: PC2, PC3, PC7, PC8.
- ✓ VLAN30 (Technical Department) for PCs: PC4, PC9, PC10, PC11.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Network_Department
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Software_Department
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Technical_Department
Switch(config-vlan)#exit
Switch(config)#exit
```

- Connected PT Switch 0 and PT Switch 1 using a trunk link.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#switchport trunk allowed vlan 10,20,30
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Fa1/1     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     10,20,30
Fa1/1     10,20,30

Port      Vlans allowed and active in management domain
Fa0/1     10,20,30
Fa1/1     10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none
Fa1/1     10,20,30

Switch#
```

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     10,20,30

Port      Vlans allowed and active in management domain
Fa0/1     10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     30
```

3. Switch Port Assignments:

✓ PT-Switch0

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 2/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet 3/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet 6/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface FastEthernet 7/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface FastEthernet 8/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa1/1, Fa4/1, Fa5/1
10	Network_Department	active	Fa2/1, Fa3/1
20	Software_Department	active	Fa6/1, Fa7/1
30	Technical_Department	active	Fa8/1, Fa9/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

✓ PT-Switch1

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa4/1, Fa5/1
10	Network_Department	active	Fa1/1, Fa2/1
20	Software_Department	active	Fa3/1, Fa6/1
30	Technical_Department	active	Fa7/1, Fa8/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

✓ Show VTP Status (PT-Switch0)

- vtp mode server

```
Switch#show vtp status
VTP Version                : 1
Configuration Revision      : 6
Maximum VLANs supported locally : 255
Number of existing VLANs    : 8
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xCE 0x99 0xCB 0x95 0x7F 0x12 0x8E 0x26
Configuration last modified by 0.0.0.0 at 3-1-93 00:07:04
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp domain IT
Changing VTP domain name from NULL to IT
```

✓ Show VTP Status (PT-Switch1)

- vtp mode client

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp domain IT
Domain name already set to IT.
Switch(config)#vtp domain UOB
Changing VTP domain name from IT to UOB
Switch(config)#00:16:49 %DTP-S-DOMAINMISMATCH: Unable to perform trunk negotiation on
port Fa0/1 because of VTP domain mismatch.

Switch(config)#vtp domain IT
Changing VTP domain name from UOB to IT
Switch(config)#exit
Switch#
%SYS-S-CONFIG_I: Configured from console by console

Switch#show vtp status
VTP Version                : 1
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 8
VTP Operating Mode          : Client
VTP Domain Name             : IT
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x54 0x88 0x8D 0x5B 0xF1 0x69 0xD6 0x72
Configuration last modified by 0.0.0.0 at 3-1-93 00:07:04
```

4. Router Configuration

- ✓ interface FastEthernet0/0.1
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.248
exit
- ✓ interface FastEthernet0/0.2
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.248
exit
- ✓ interface FastEthernet0/0.3
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.248
exit

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.248
Router(config-subif)#exit
Router(config)#interface FastEthernet0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.248
Router(config-subif)#exit
Router(config)#interface FastEthernet0/0.3
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.248
Router(config-subif)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/0.1	192.168.10.1	YES	manual	administratively down	down
FastEthernet0/0.2	192.168.20.1	YES	manual	administratively down	down
FastEthernet0/0.3	192.168.30.1	YES	manual	administratively down	down
FastEthernet1/0	unassigned	YES	unset	administratively down	down
Serial2/0	unassigned	YES	unset	administratively down	down
Serial3/0	unassigned	YES	unset	administratively down	down
FastEthernet4/0	unassigned	YES	unset	administratively down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down

- ✓ interface FastEthernet 0/0
- ✓ no shutdown

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

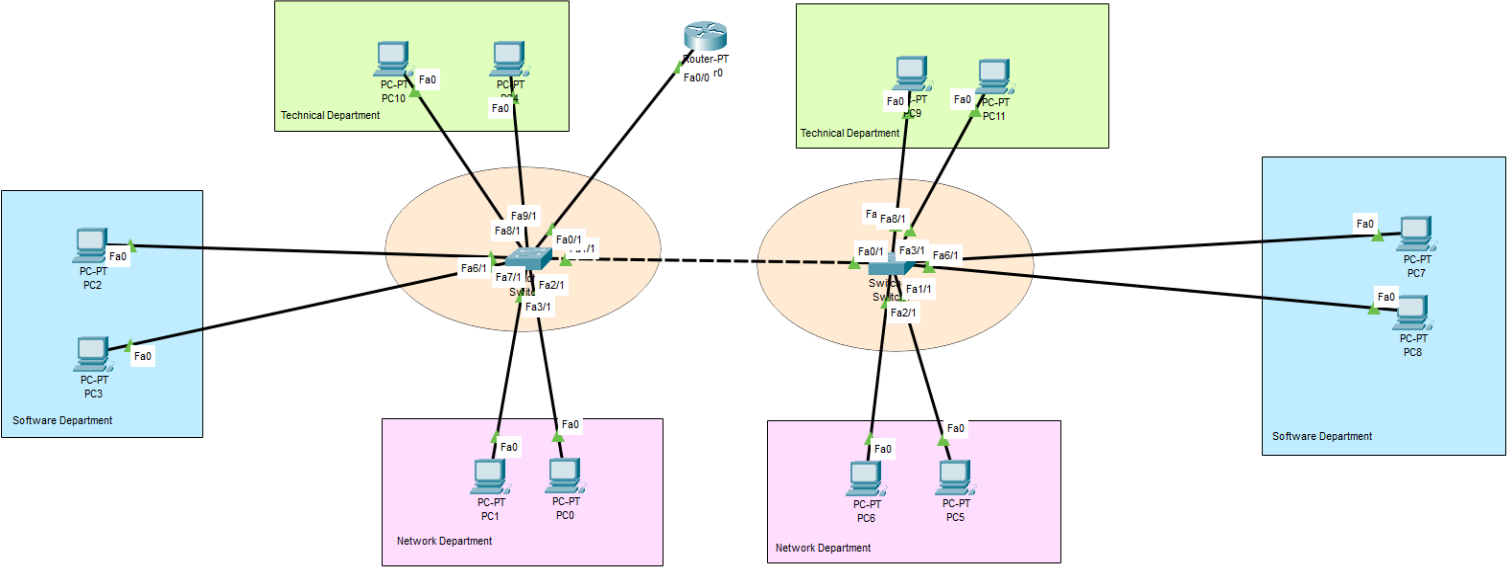
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
```

5. Testing Inter-VLAN Communication:

- Multiple packets were sent to test communication across different VLANs. The following packets were successfully transmitted. Some examples are as follows,
- From PC0 in the Network Department (VLAN10) to PC7 in the Software Department (VLAN20).
 - From PC6 in the Network Department (VLAN10) to PC10 in the Technical Department (VLAN30).
 - From PC3 in the Software Department (VLAN20) to PC1 in the Network Department (VLAN10).



Time: 01:38:30

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC7	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC6	PC10	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC3	PC1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC11	ICMP		0.000	N	3	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC7	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC6	PC10	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC3	PC1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC11	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC11	PC0	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC10	PC3	ICMP		0.000	N	5	(edit)	(delete)

Task 2: Variable-Length Subnetting (VLSM) and Classless IP Addressing

➤ Objective

To design an efficient IP addressing scheme using VLSM to ensure no IP address wastage and assign IP addresses to the PCs in each VLAN.

✓ Subnet Design:

- Based on the number of PCs per VLAN, a /29 subnet was chosen, providing 6 usable IP addresses per VLAN, which meets the requirement for 4 PCs in each VLAN.
- The following IP ranges were allocated:

❖ VLAN10: 192.168.10.0/29

❖ VLAN20: 192.168.20.0/29

❖ VLAN30: 192.168.30.0/29

✓ IP Address Allocation:

❖ VLAN 10:

- Network: 192.168.10.0
- Router: 192.168.10.1
- PCs: 192.168.10.2 - 192.168.10.5
- Broadcast: 192.168.10.7

❖ VLAN 20:

- Network: 192.168.20.0
- Router: 192.168.20.1
- PCs: 192.168.20.2 - 192.168.20.5
- Broadcast: 192.168.20.7

❖ VLAN 30:

- Network: 192.168.30.0
- Router: 192.168.30.1
- PCs: 192.168.30.2 - 192.168.30.5
- Broadcast: 192.168.30.7

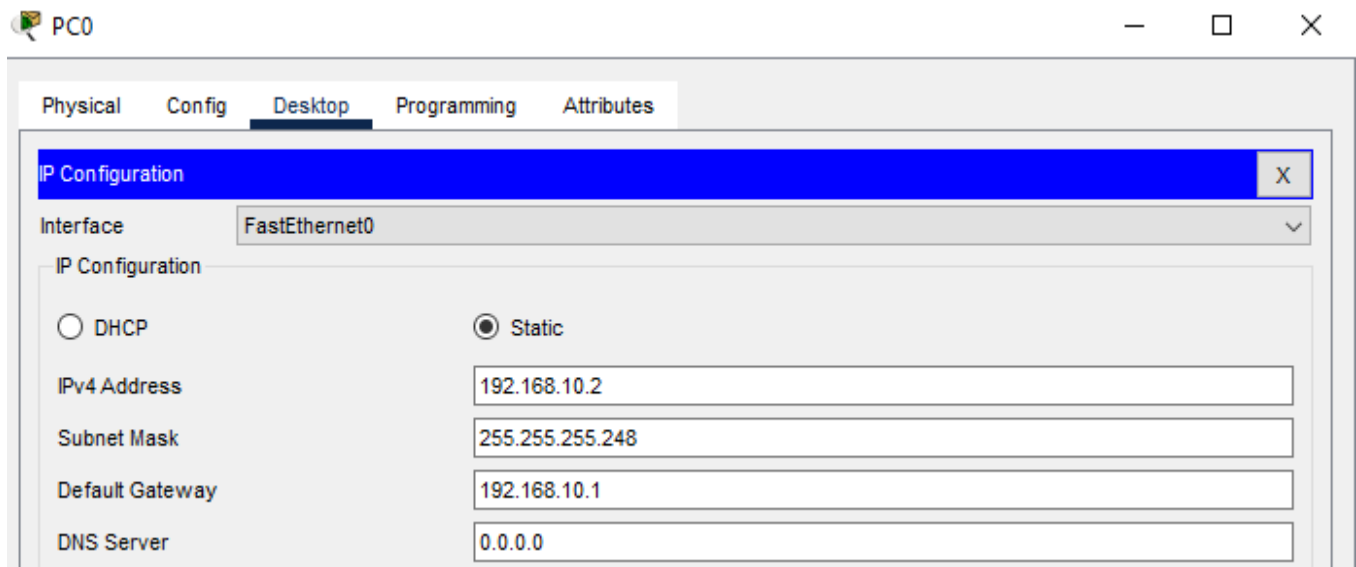
✓ PC Configuration:

- Assigned IP addresses, subnet masks (255.255.255.248), and default gateways (router subinterfaces) to all PCs.

IP address configuration screenshots for the PCs

VLAN 10 (PCs)

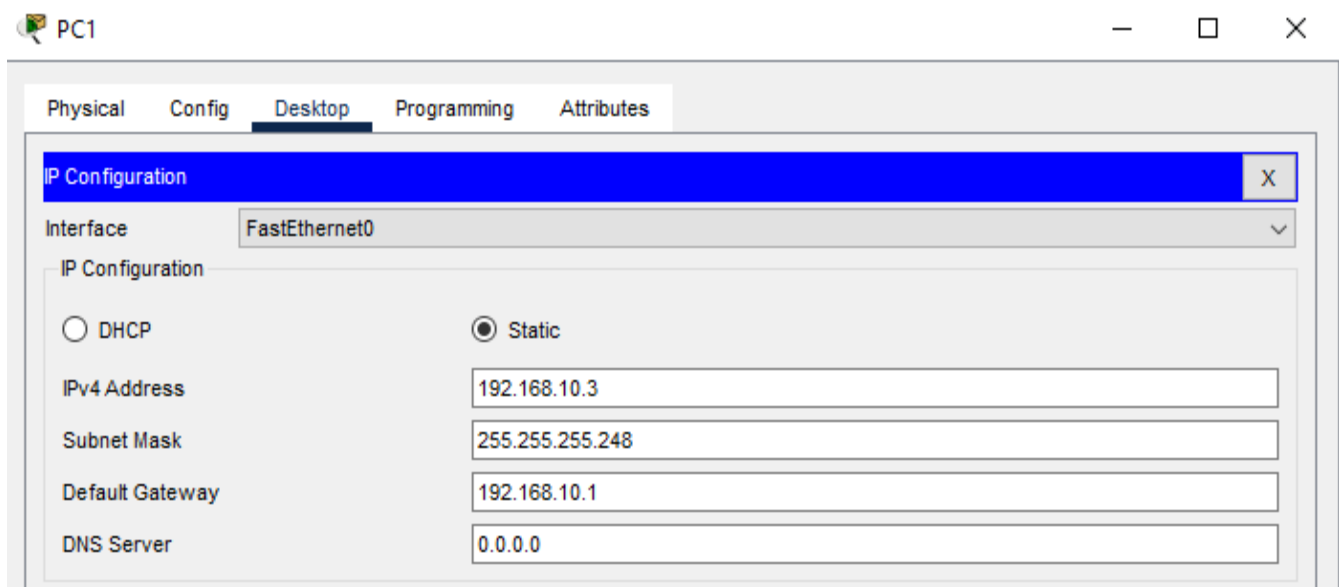
✓ PC0



The screenshot shows a window titled "PC0" with a tabbed interface. The "Desktop" tab is selected, and the "IP Configuration" window is open. The "Interface" dropdown is set to "FastEthernet0". Under "IP Configuration", the "Static" radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.248
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

✓ PC1



PC1

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

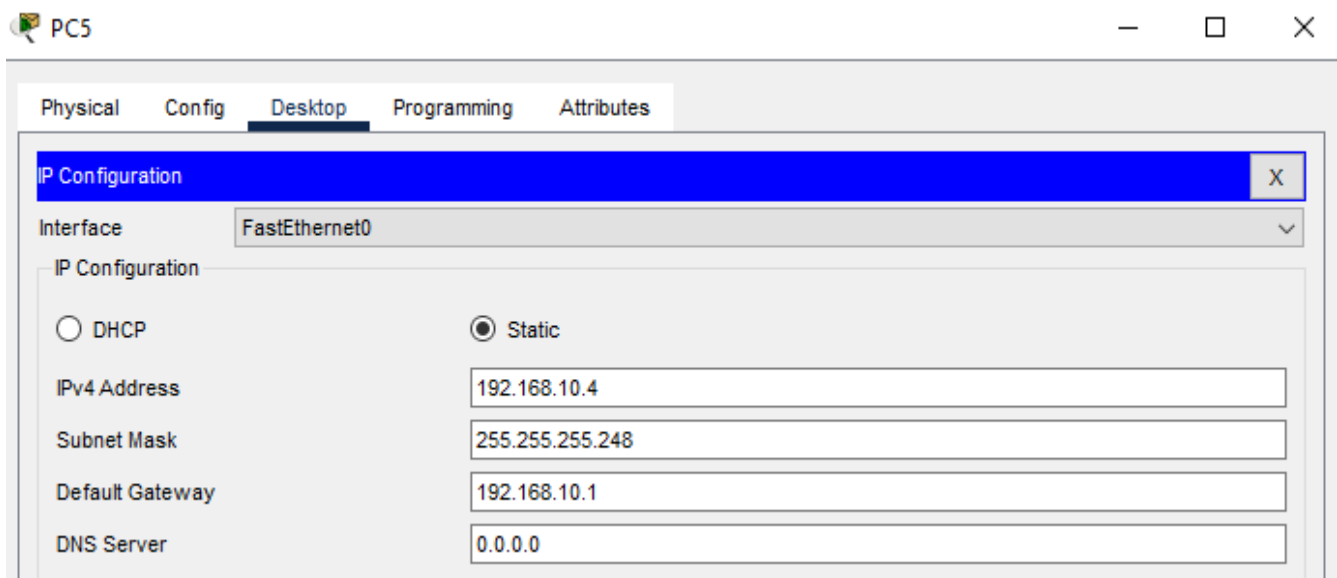
IPv4 Address: 192.168.10.3

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.10.1

DNS Server: 0.0.0.0

✓ PC5



PC5

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

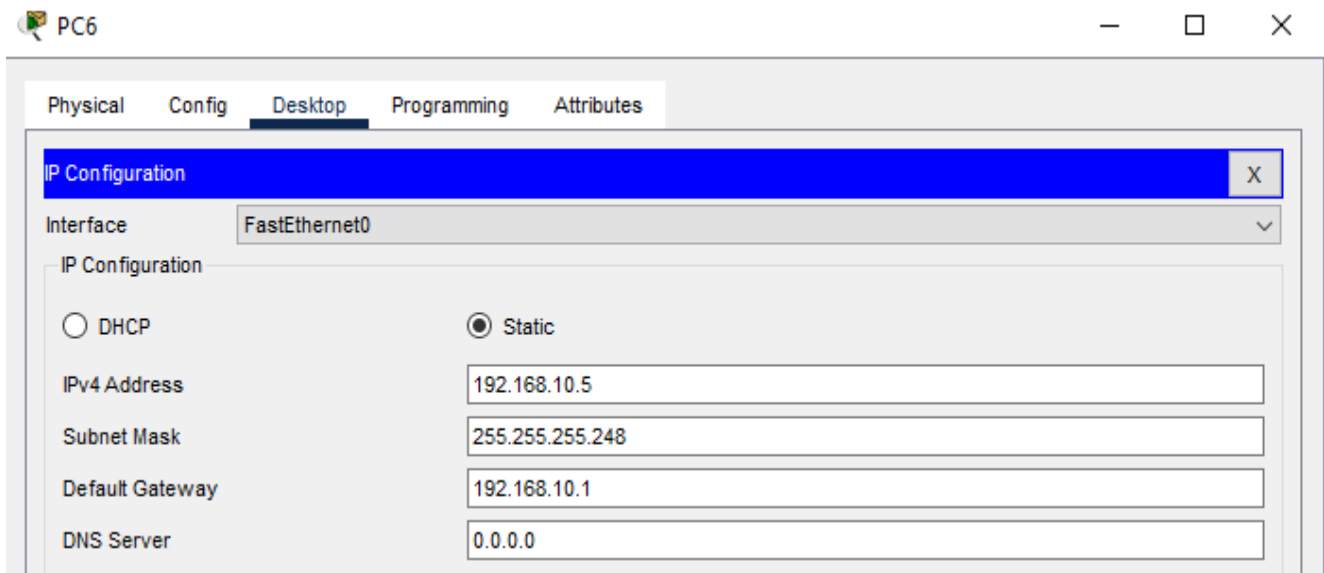
IPv4 Address: 192.168.10.4

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.10.1

DNS Server: 0.0.0.0

✓ PC6



PC6

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.10.5

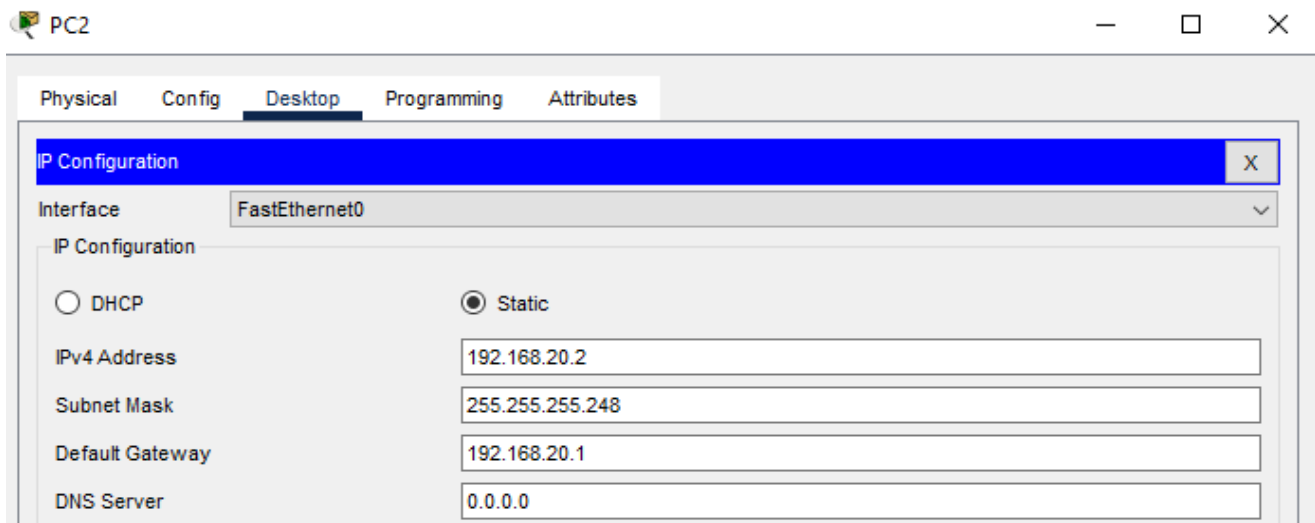
Subnet Mask: 255.255.255.248

Default Gateway: 192.168.10.1

DNS Server: 0.0.0.0

VLAN 20 (PCs)

✓ PC2



PC2

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

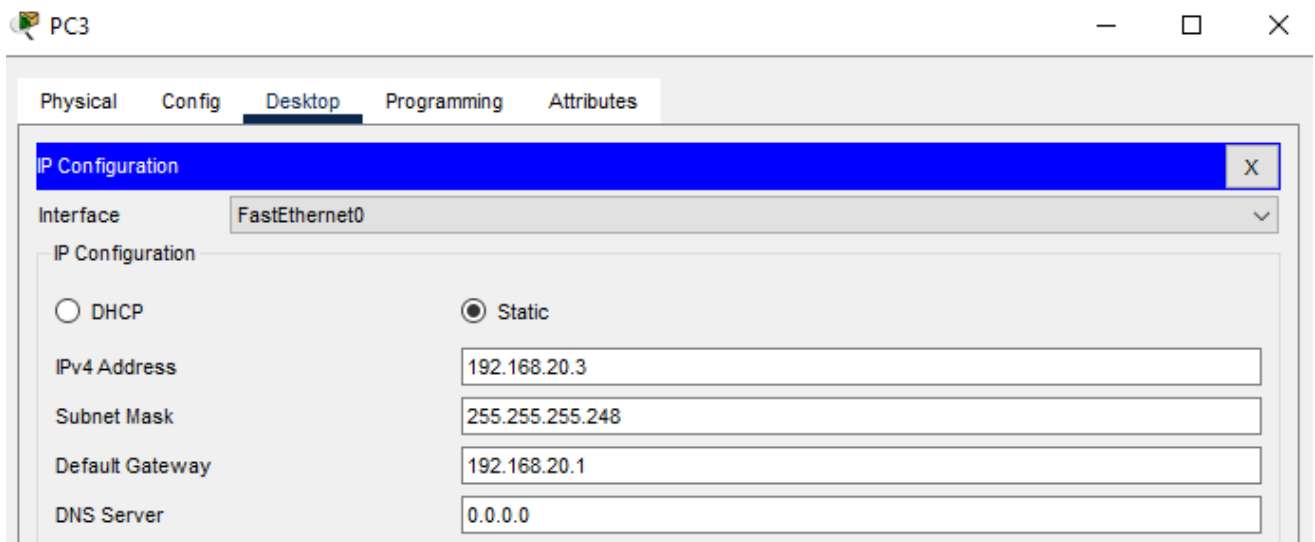
IPv4 Address: 192.168.20.2

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.20.1

DNS Server: 0.0.0.0

✓ PC3



PC3

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

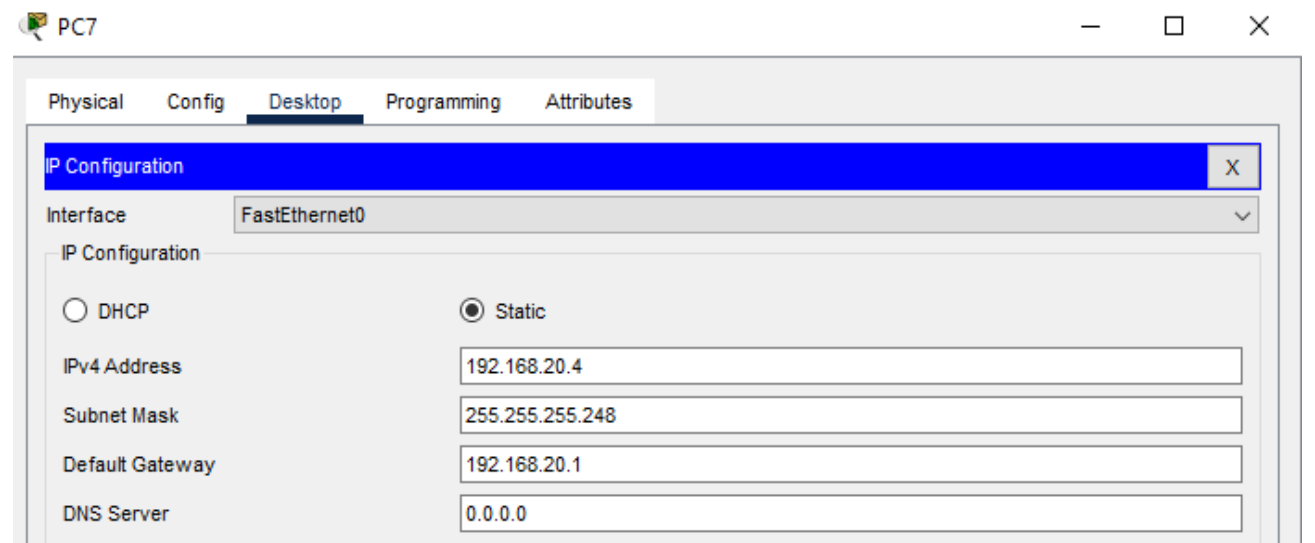
IPv4 Address: 192.168.20.3

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.20.1

DNS Server: 0.0.0.0

✓ PC7



PC7

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

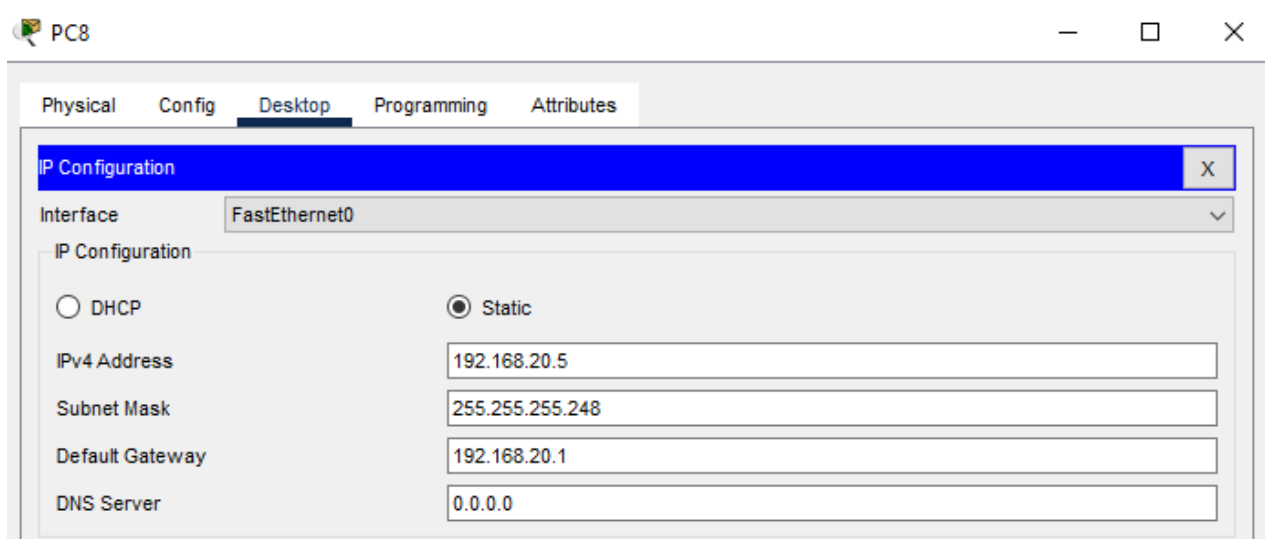
IPv4 Address: 192.168.20.4

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.20.1

DNS Server: 0.0.0.0

✓ PC8

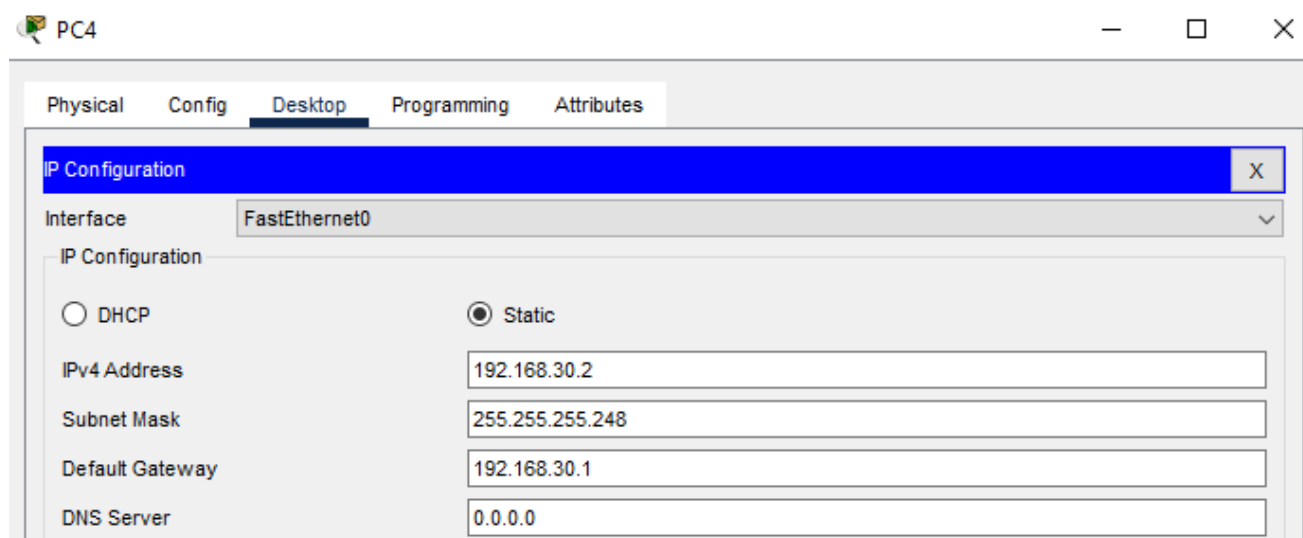


The screenshot shows the configuration window for PC8. The 'Desktop' tab is selected, and the 'IP Configuration' section is highlighted. The interface is set to 'FastEthernet0'. The IP configuration is set to 'Static' with the following values:

Field	Value
IPv4 Address	192.168.20.5
Subnet Mask	255.255.255.248
Default Gateway	192.168.20.1
DNS Server	0.0.0.0

VLAN 30 (PCs)

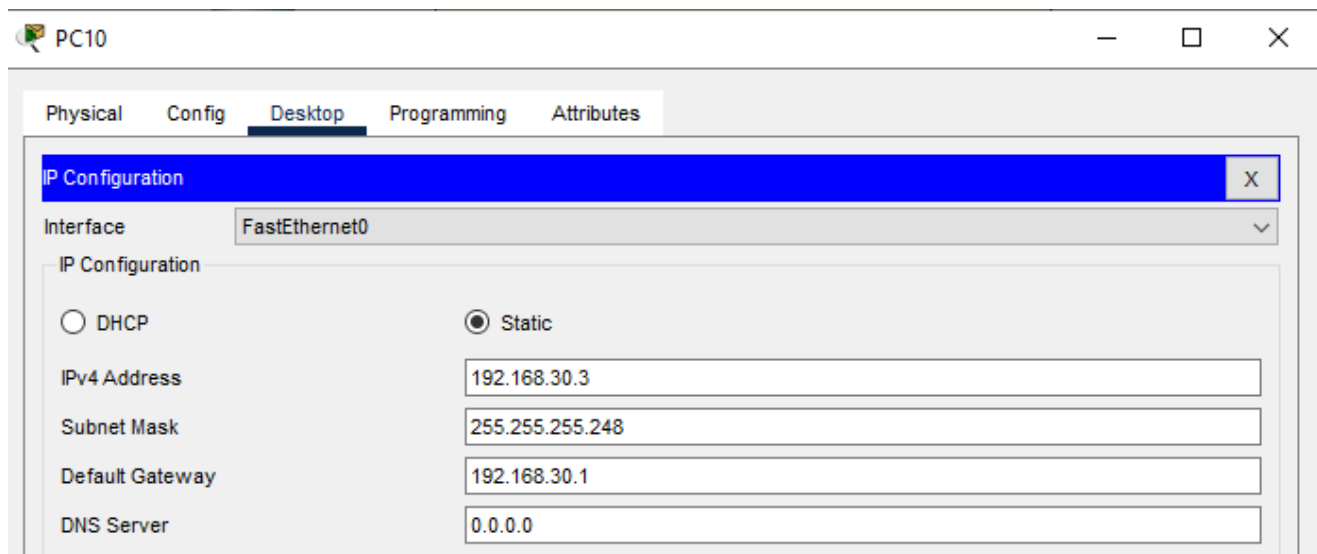
✓ PC4



The screenshot shows the configuration window for PC4. The 'Desktop' tab is selected, and the 'IP Configuration' section is highlighted. The interface is set to 'FastEthernet0'. The IP configuration is set to 'Static' with the following values:

Field	Value
IPv4 Address	192.168.30.2
Subnet Mask	255.255.255.248
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

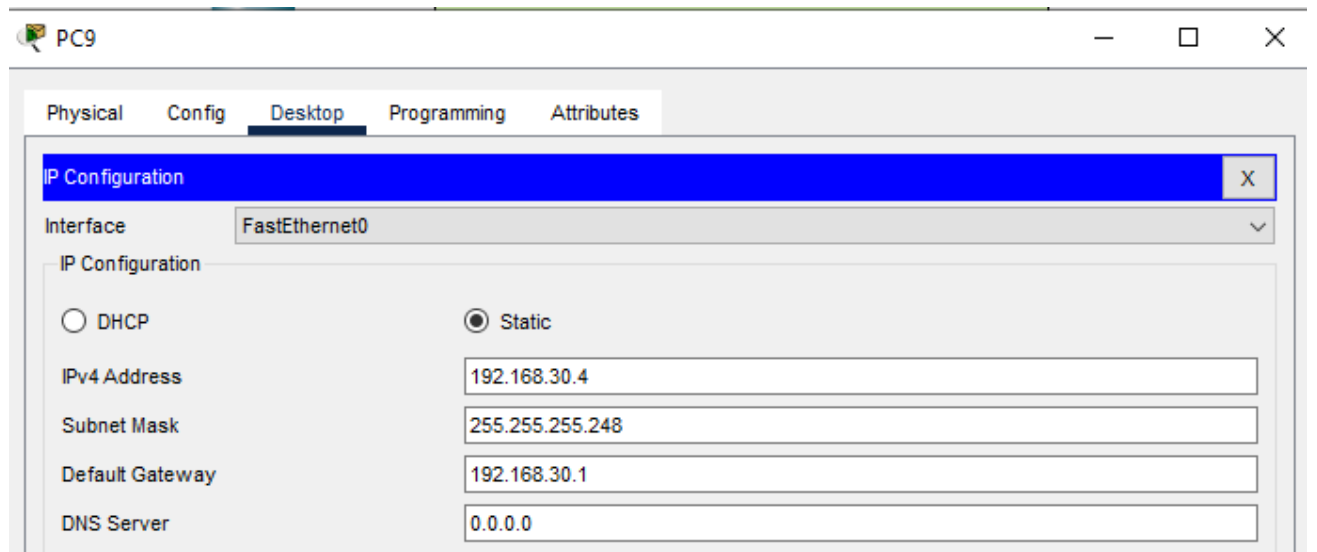
✓ PC10



The screenshot shows the configuration window for PC10. The 'Desktop' tab is selected. The 'IP Configuration' section is highlighted in blue. The 'Interface' dropdown is set to 'FastEthernet0'. The 'IP Configuration' section shows the 'Static' radio button selected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are filled with the values 192.168.30.3, 255.255.255.248, 192.168.30.1, and 0.0.0.0 respectively.

Interface	Value
FastEthernet0	
IP Configuration	
DHCP	<input type="radio"/>
Static	<input checked="" type="radio"/>
IPv4 Address	192.168.30.3
Subnet Mask	255.255.255.248
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

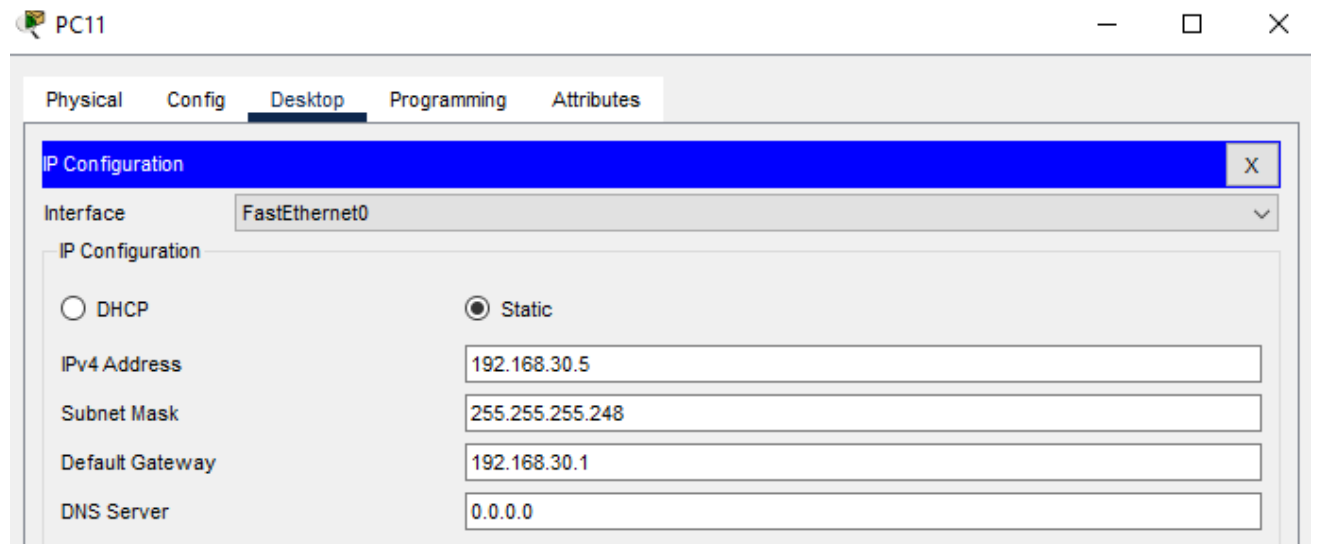
✓ PC9



The screenshot shows the configuration window for PC9. The 'Desktop' tab is selected. The 'IP Configuration' section is highlighted in blue. The 'Interface' dropdown is set to 'FastEthernet0'. The 'IP Configuration' section shows the 'Static' radio button selected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are filled with the values 192.168.30.4, 255.255.255.248, 192.168.30.1, and 0.0.0.0 respectively.

Interface	Value
FastEthernet0	
IP Configuration	
DHCP	<input type="radio"/>
Static	<input checked="" type="radio"/>
IPv4 Address	192.168.30.4
Subnet Mask	255.255.255.248
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

✓ PC11



The screenshot shows the configuration window for PC11. The 'Desktop' tab is selected. The 'IP Configuration' section is highlighted in blue. The 'Interface' dropdown is set to 'FastEthernet0'. The 'IP Configuration' section shows the 'Static' radio button selected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are filled with the values 192.168.30.5, 255.255.255.248, 192.168.30.1, and 0.0.0.0 respectively.

Interface	Value
FastEthernet0	
IP Configuration	
DHCP	<input type="radio"/>
Static	<input checked="" type="radio"/>
IPv4 Address	192.168.30.5
Subnet Mask	255.255.255.248
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

IP address configuration screenshots for the Router

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.248
Router(config-subif)#exit
Router(config)#interface FastEthernet0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.248
Router(config-subif)#exit
Router(config)#interface FastEthernet0/0.3
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.248
Router(config-subif)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/0.1	192.168.10.1	YES	manual	administratively down	down
FastEthernet0/0.2	192.168.20.1	YES	manual	administratively down	down
FastEthernet0/0.3	192.168.30.1	YES	manual	administratively down	down
FastEthernet1/0	unassigned	YES	unset	administratively down	down
Serial2/0	unassigned	YES	unset	administratively down	down
Serial3/0	unassigned	YES	unset	administratively down	down
FastEthernet4/0	unassigned	YES	unset	administratively down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

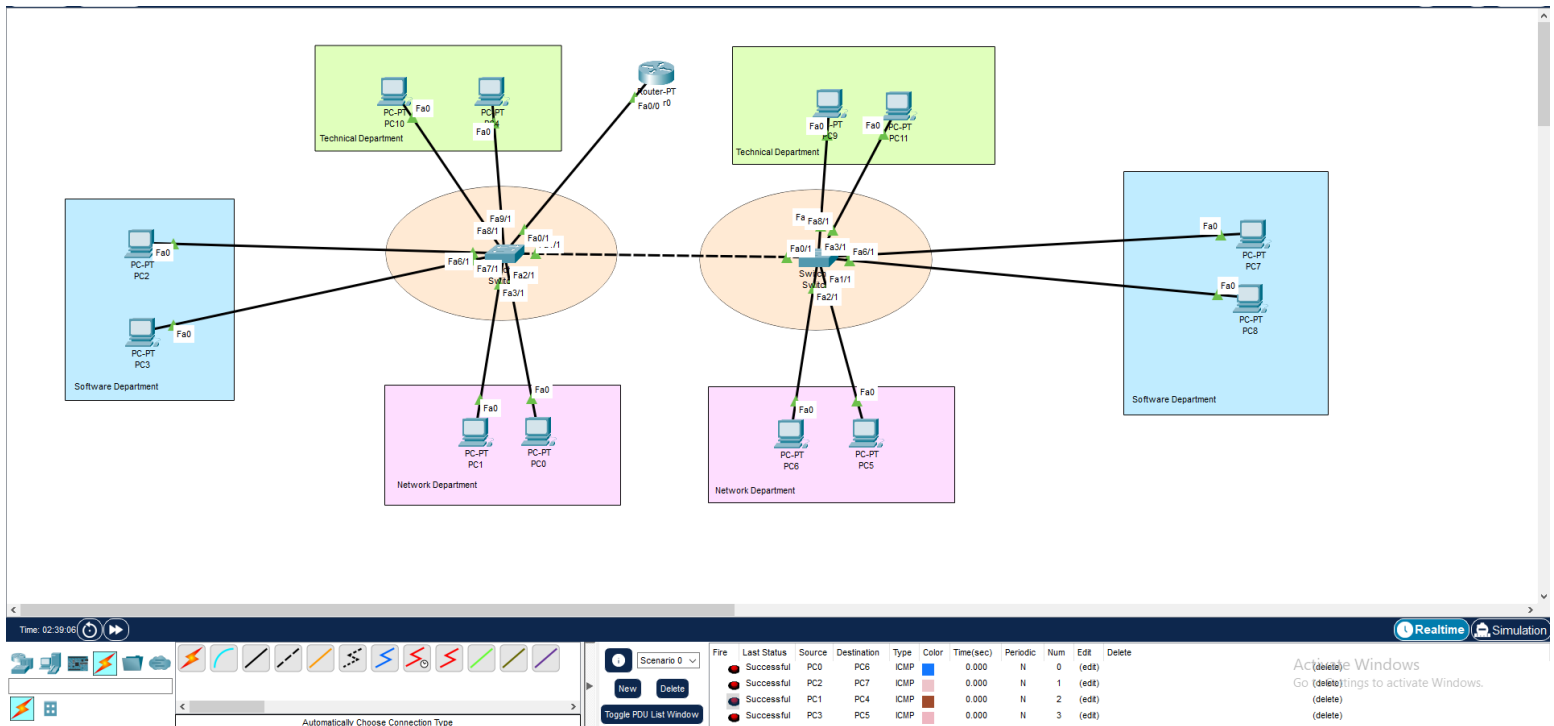
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
```

✓ Testing Subnetting:

- Confirmed proper routing and communication across the subnets by testing communication between devices in the same and different VLANs. Some examples are as follows,
 - From PC0 in the Network Department (VLAN10) to PC6 in the Network Department (VLAN10).
 - From PC3 in the Software Department (VLAN20) to PC5 in the Network Department (VLAN10).



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC6	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC7	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC4	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC3	PC5	ICMP		0.000	N	3	(edit)	(delete)

Task 3: Port Security Configuration

➤ Objective

- To improve network security, Task 3 required configuring and implementing port security on specific ports for both Switch 0 and Switch 1.
- Port security was applied to one port from each VLAN (VLAN 10, VLAN 20, and VLAN 30) on both switches, limiting each port to only one device by limiting the number of MAC addresses.
- The violation mode was set to shutdown, which means that if an unauthorized device connects, the port is automatically disabled.
- The configuration was tested by connecting unauthorized devices (such as laptops) to the secured ports.
- The switch's behavior was monitored to verify that the security violation count increased and the ports went into a shutdown state, protecting the network from unauthorized access.

PT Switch0

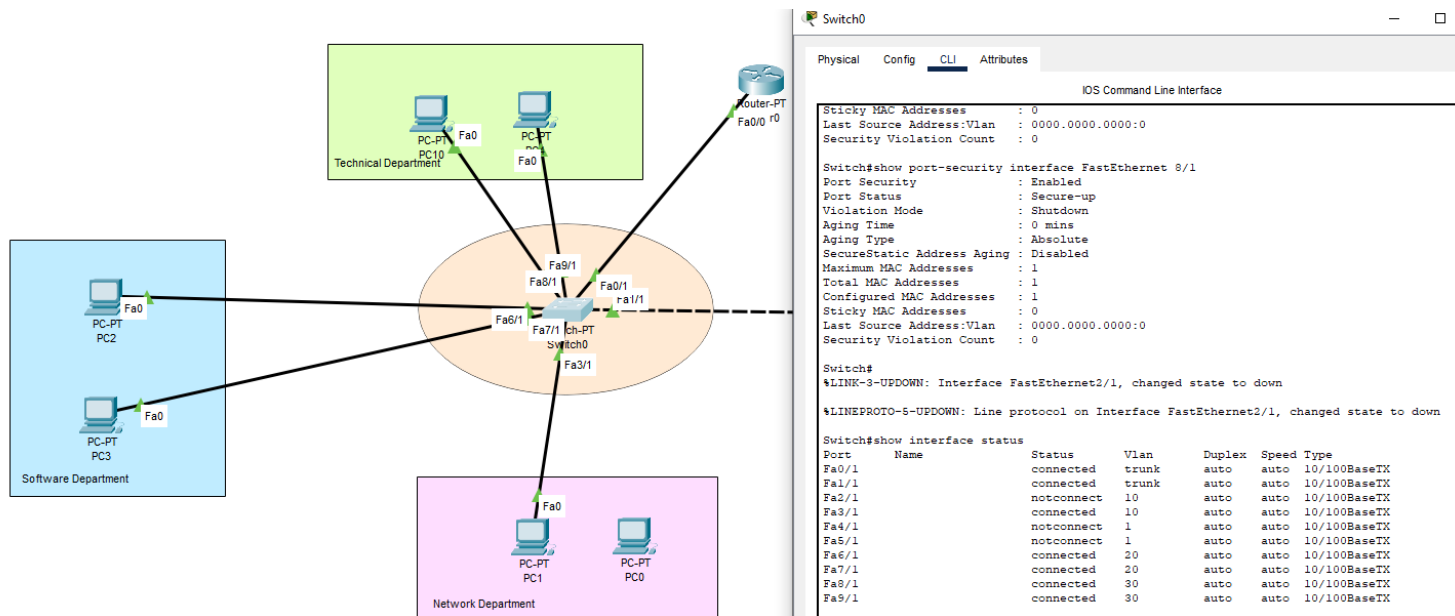
```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 2/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0001.63DB.64B4
Found duplicate mac-address 0001.63db.64b4.
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#interface FastEthernet 6/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0050.0FC9.01C5
Found duplicate mac-address 0050.0fc9.01c5.
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#interface FastEthernet 8/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 00E0.F766.A144
Found duplicate mac-address 00e0.f766.a144.
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

```
Switch#show port-security interface FastEthernet 2/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

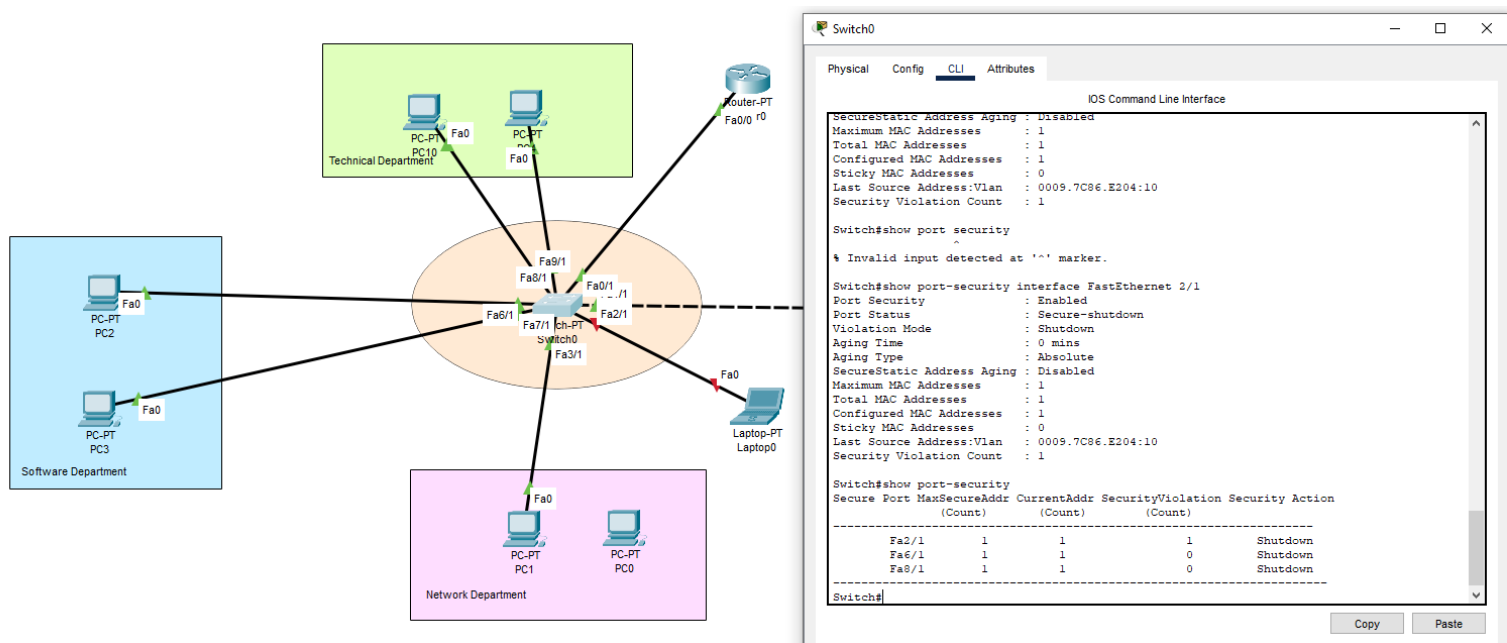
```
Switch#show port-security interface FastEthernet 6/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

```
Switch#show port-security interface FastEthernet 8/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

✓ Screenshot of Authorized Device Removal



✓ Unauthorized Device Connected to Port



✓ Status after Removing Authorized Device and Connecting Unauthorized Device

```

Switch#show port-security interface FastEthernet 2/1
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0009.7C86.E204:10
Security Violation Count : 1

Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
-----
Fa2/1 1 1 1 Shutdown
Fa6/1 1 1 0 Shutdown
Fa8/1 1 1 0 Shutdown

```

PT Switch1

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 000A.4115.07B9
Found duplicate mac-address 000a.4115.07b9.
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#interface FastEthernet 3/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0030.F284.8287
Found duplicate mac-address 0030.f284.8287.
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#interface FastEthernet 7/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0000.0CAC.C30C
Found duplicate mac-address 0000.0cac.c30c.
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

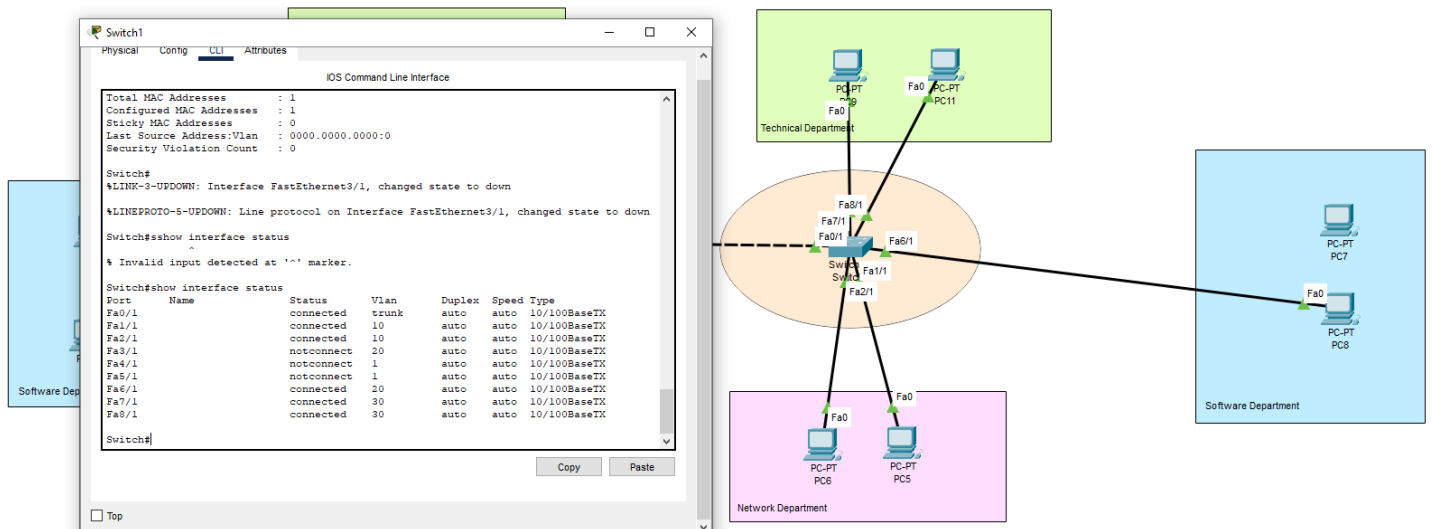
Switch#write memory
Building configuration...
[OK]
Switch#
```

```
Switch#show port-security interface FastEthernet 1/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

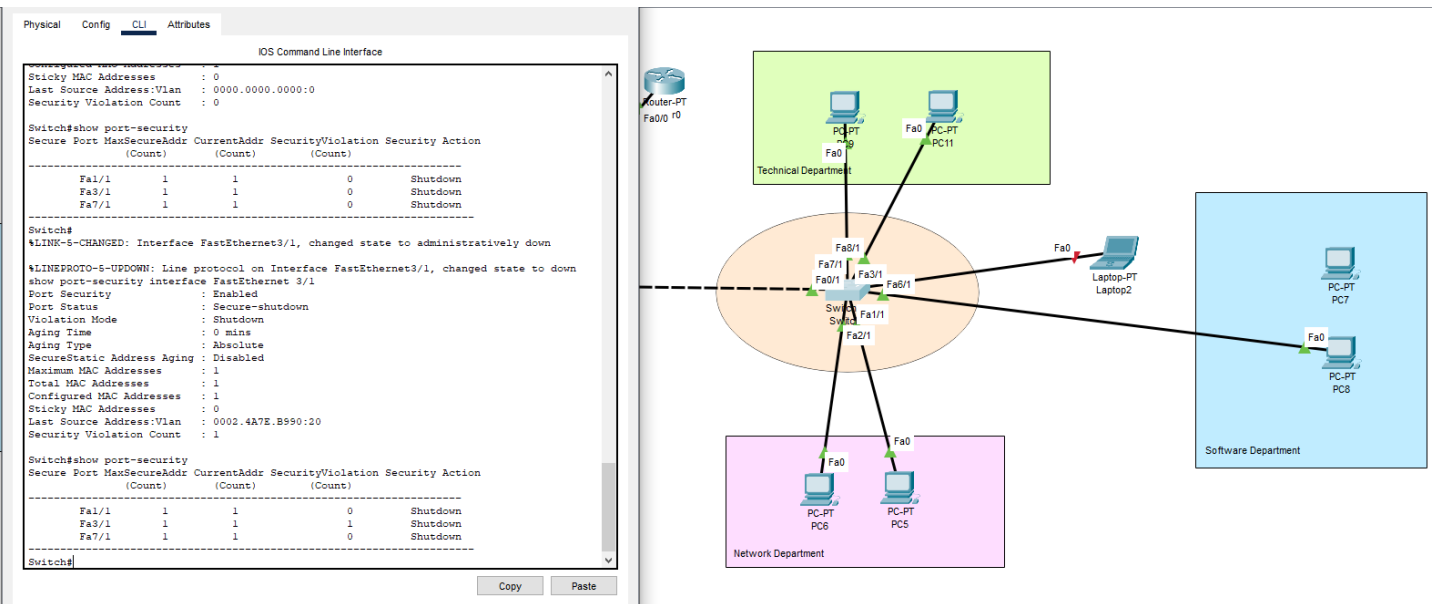
```
Switch#show port-security interface FastEthernet 3/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

```
Switch#show port-security interface FastEthernet 7/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

✓ Screenshot of Authorized Device Removal



✓ Unauthorized Device Connected to Port



✓ Status after Removing Authorized Device and Connecting Unauthorized Device

```
show port-security interface FastEthernet 3/1
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0002.4A7E.B990:20
Security Violation Count : 1
```

```
Switch#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa1/1	1	1	0	Shutdown
Fa3/1	1	1	1	Shutdown
Fa7/1	1	1	0	Shutdown

Task 4: DHCP Configuration on Routers

➤ Objective

The goal of Task 4 is to configure Dynamic Host Configuration Protocol (DHCP) on the router, enabling automatic IP address assignment for devices in each VLAN. This will allow end devices like PCs, laptops, and other networked devices to dynamically receive IP addresses and other network configurations such as subnet masks and default gateways from the DHCP server configured on the router.

➤ Define a DHCP Pool for Each VLAN:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool Network_Department
Router(dhcp-config)#network 192.168.10.0 255.255.255.248
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool Software_Department
Router(dhcp-config)#network 192.168.20.0 255.255.255.248
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool Technical_Department
Router(dhcp-config)#network 192.168.30.0 255.255.255.248
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.10.1
Router(config)#ip dhcp excluded-address 192.168.20.1
Router(config)#ip dhcp excluded-address 192.168.30.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
```

➤ DHCP Configuration Challenges

- ✓ To ensure proper segmentation, each VLAN's switch ports were configured separately. On the router, DHCP pools were created for each VLAN, containing the network address, default gateway, and DNS settings. This setup was designed to make it easier to assign dynamic IP addresses to connected devices.

✓ PT-Switch0

```
Switch#show vlan brief
```

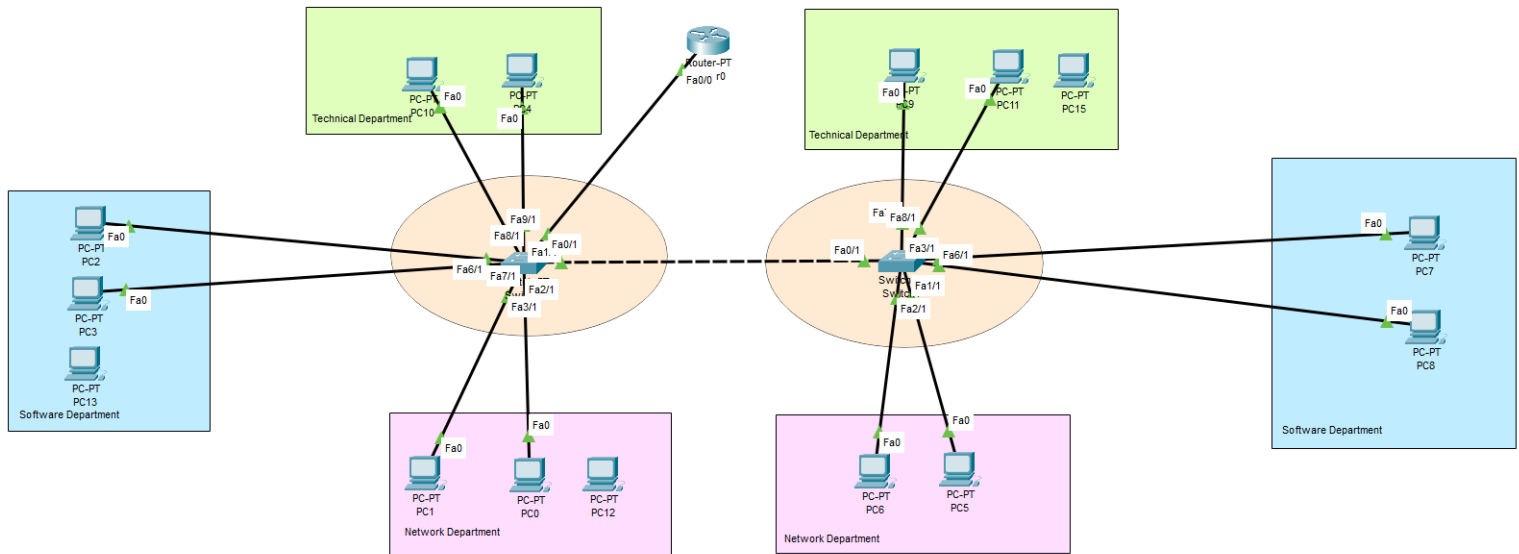
VLAN	Name	Status	Ports
1	default	active	
10	Network_Department	active	Fa2/1, Fa3/1, Fa4/1
20	Software_Department	active	Fa5/1, Fa6/1, Fa7/1
30	Technical_Department	active	Fa8/1, Fa9/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

✓ PT-Switch1

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa5/1
10	Network_Department	active	Fa1/1, Fa2/1
20	Software_Department	active	Fa3/1, Fa6/1
30	Technical_Department	active	Fa4/1, Fa7/1, Fa8/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

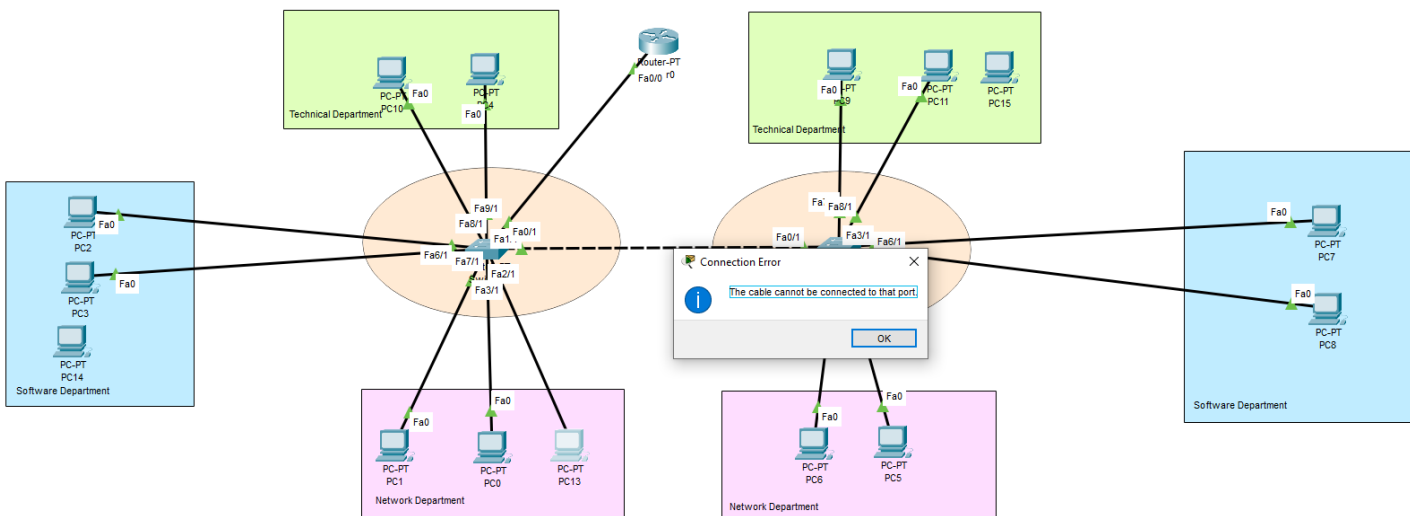
- ✓ New PCs (PC12, PC13, and PC14) were added to the network. Each PC was configured to operate in DHCP mode to automatically request an IP address upon connection to the respective switch ports assigned to their VLANs.



- ✓ Despite successful configurations, persistent connectivity issues arose, preventing the PCs from communicating with the DHCP server.

✓ Specific problems included:

- Connection Error: The cable cannot be connected to that port.



- Devices failing to obtain IP addresses, despite being set to DHCP mode.
- Although the router was configured with the appropriate DHCP settings for each VLAN, the connection between the switch and the PCs remained problematic, hindering the demonstration of DHCP functionality.

✓ Verification of DHCP Configuration

- To confirm that the DHCP settings were correctly applied, I executed the command: *Router# show ip dhcp pool*

```
Router>enable
Router#show ip dhcp pool

Pool Network_Department :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 6
  Leased addresses                  : 0
  Excluded addresses                : 3
  Pending event                    : none

  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  192.168.10.1       192.168.10.1 - 192.168.10.6    0 / 3 / 6

Pool Software_Department :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 6
  Leased addresses                  : 0
  Excluded addresses                : 3
  Pending event                    : none

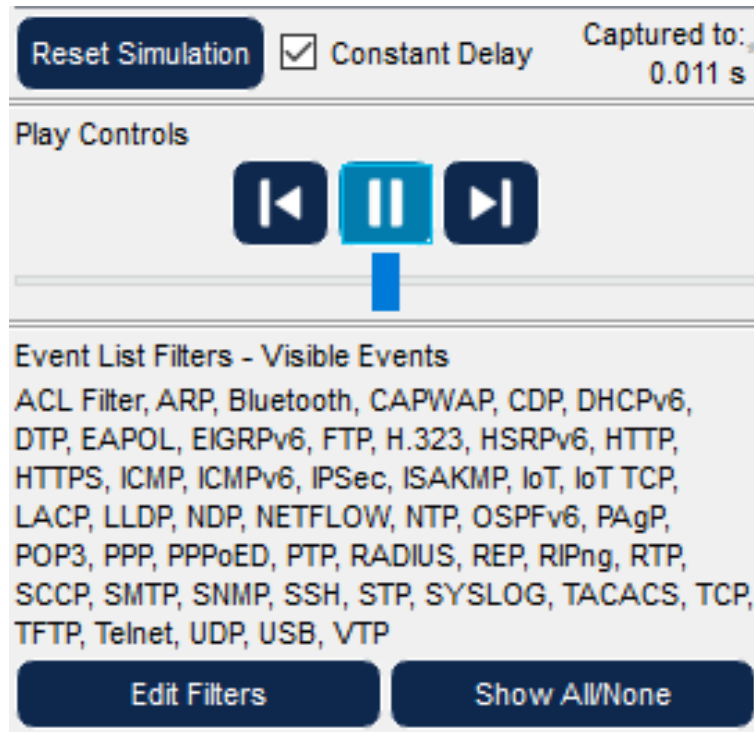
  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  192.168.20.1       192.168.20.1 - 192.168.20.6    0 / 3 / 6

Pool Technical_Department :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 6
  Leased addresses                  : 0
  Excluded addresses                : 3
  Pending event                    : none

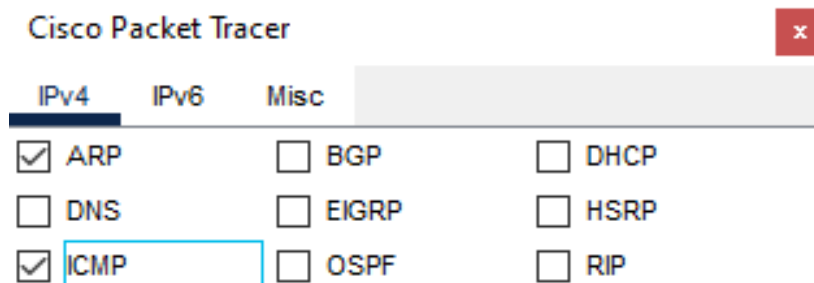
  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  192.168.30.1       192.168.30.1 - 192.168.30.6    0 / 3 / 6
Router#
```

Task 5: Network Analysis using Wireshark

- ✓ In Cisco Packet Tracer, switch from Real-Time Mode to Simulation Mode. This will allow you to control and monitor packet flow across the network



- ✓ Click on the Edit Filters button, and select only ARP and ICMP protocols. This will limit the captured traffic to ARP resolution and ICMP ping requests/replies.



- ✓ Perform actions such as pinging between devices (e.g., from PC0 to PC7 and PC4 to PC1) to generate ICMP traffic.

```
C:\>ping 192.168.20.4

Pinging 192.168.20.4 with 32 bytes of data:

Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



```
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:





Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time=2ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

- ✓ As packets flow through the network, they will appear in the Simulation Panel.

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device		
	0.000	--		
	0.000	--		
	0.001	PC0		
	0.001	PC4		
	0.002	Switch0		
	0.002	--		
	0.003	Switch0		
	0.003	Router0		
	0.004	Router0		
	0.004	Switch0		
	0.005	Switch0		
	0.005	Switch1		
	0.006	PC1		
	0.006	PC7		
	0.007	Switch0		
	0.007	Switch1		
	0.008	Router0		
	0.008	Switch0		
Visible	0.009	Switch0		
Visible	0.009	Router0		

- ✓ In the Event List of the Simulation Panel, observe each packet’s status (Success, Failed, or Discarded). Clicking on individual packets will display detailed information about the source, destination, and protocol, verifying if the communication was successful.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC7	ICMP		0.000	N	0	(edit)	
	Successful	PC4	PC1	ICMP		0.000	N	1	(edit)	

➤ Limitations of Cisco Packet Tracer for Wireshark Captures

- Wireshark cannot analyze network traffic because Cisco Packet Tracer is a simulation tool that cannot generate real packets for capture. As a result, it cannot support live packet capturing.
- When you host in real time, you can effectively capture network traffic using Wireshark.
- Sample ICMP Capture are as follows,

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
356	19.147291	172.16.0.27	172.16.0.3	ICMP	218	Destination unreachable (Port unreachable)
508	20.518357	172.16.0.27	40.99.9.178	ICMP	112	Destination unreachable (Port unreachable)
546	20.885339	172.16.0.27	172.16.0.2	ICMP	249	Destination unreachable (Port unreachable)
3555	38.849630	172.16.0.27	172.16.0.3	ICMP	273	Destination unreachable (Port unreachable)
5627	41.592952	172.16.0.27	172.16.0.2	ICMP	172	Destination unreachable (Port unreachable)
9046	167.777654	172.16.0.27	103.102.166.224	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 9048)
9048	167.822013	103.102.166.224	172.16.0.27	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=57 (request in 9046)
9066	168.792469	172.16.0.27	103.102.166.224	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 9068)
9068	168.837434	103.102.166.224	172.16.0.27	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=57 (request in 9066)
9083	169.802746	172.16.0.27	103.102.166.224	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 9084)
9084	169.847653	103.102.166.224	172.16.0.27	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=57 (request in 9083)
9099	170.814671	172.16.0.27	103.102.166.224	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 9100)
9100	170.859630	103.102.166.224	172.16.0.27	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=57 (request in 9099)

> Frame 9068: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{E7C4F94B-B36D-4273-A31D-FD243AA00B69}	
▼ Ethernet II, Src: Fortinet_09:00:02 (00:09:0f:09:00:02), Dst: LCFCElectron_c6:ab:05 (e8:80:88:c6:ab:05)	
> Destination: LCFCElectron_c6:ab:05 (e8:80:88:c6:ab:05)	
> Source: Fortinet_09:00:02 (00:09:0f:09:00:02)	
Type: IPv4 (0x0800)	
[Stream index: 17]	
> Internet Protocol Version 4, Src: 103.102.166.224, Dst: 172.16.0.27	
▼ Internet Control Message Protocol	
Type: 0 (Echo (ping) reply)	
Code: 0	
Checksum: 0x5559 [correct]	
[Checksum Status: Good]	
Identifier (BE): 1 (0x0001)	
Identifier (LE): 256 (0x0100)	
Sequence Number (BE): 2 (0x0002)	
Sequence Number (LE): 512 (0x0200)	
[Request frame: 9066]	
[Response time: 44.965 ms]	

0000	e8 80 88 c6 ab 05 00 09 0f 09 00 02 08 00 45 00E.
0010	00 3c 97 33 00 00 39 01 30 1c 67 66 a6 e0 ac 10	..<3..9. 0.gf....
0020	00 1b 00 00 55 59 00 01 00 02 61 62 63 64 65 66UY.. ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

✓ **Expected Output for ICMP Traffic**

No	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.2	192.168.20.4	ICMP	64	Echo (ping) request id=0 seq=1
2	0.000005	192.168.20.4	192.168.10.2	ICMP	64	Echo (ping) reply id=0 seq=1
3	0.000010	192.168.30.2	192.168.10.3	ICMP	64	Echo (ping) request id=0 seq=1
4	0.000015	192.168.10.3	192.168.30.2	ICMP	64	Echo (ping) reply id=0 seq=1

✓ **Expected Output for ARP Filter**

No	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.2	Broadcast	ARP	42	Who has 192.168.20.4? Tell 192.168.10.2
2	0.000005	Broadcast	192.168.20.4	ARP	42	192.168.20.4 is at 00:11:22:33:44:55
3	0.000010	192.168.30.2	Broadcast	ARP	42	Who has 192.168.10.3? Tell 192.168.30.2
4	0.000015	Broadcast	192.168.10.3	ARP	42	192.168.10.3 is at 00:AA:BB:CC:DD:EE

Conclusion

In this assignment, a comprehensive network design was successfully completed, involving the configuration of VLANs, implementation of DHCP, and analysis of network traffic using Cisco Packet Tracer and Wireshark. The network comprised three VLANs representing different departments: the Network Department (VLAN 10), the Software Department (VLAN 20), and the Technical Department (VLAN 30). Each VLAN was configured with appropriate IP addressing and routing settings, enabling efficient communication among connected devices.

Numerous difficulties were faced, especially when setting up DHCP and capturing traffic in Wireshark. Devices that had the correct DHCP settings started to have problems getting IP addresses, which required careful troubleshooting to ensure proper functionality.

Furthermore, live packet capturing limitations in Cisco Packet Tracer made it difficult to perform a thorough analysis of network traffic. To verify inter-VLAN communication, numerous tests were run, configurations were fine-tuned, and all settings were confirmed. While expected ARP and ICMP packets were anticipated based on my configurations, not all of the desired data could be captured due to limitations in the simulation environment.

In the end, this experience improved knowledge of DHCP functionality, network design principles, and the significance of careful troubleshooting for efficient network management.