VLAN Segmentation Using Cisco Packet Tracer

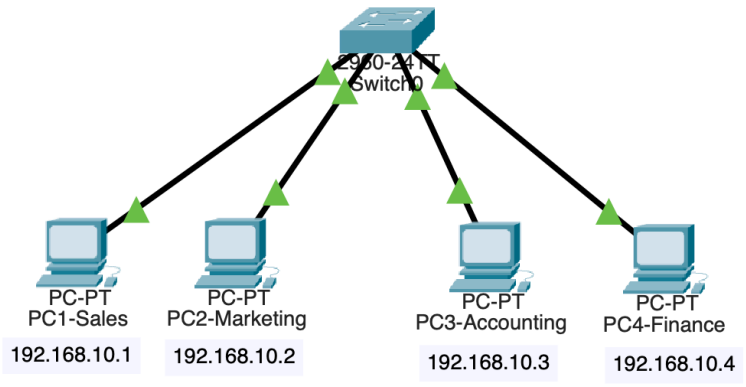
Name: Duc Anh Pham
Date: January 14, 2026
Home Lab: CompTIA Network+

Lab Description

This lab demonstrates network segmentation using Virtual Local Area Networks (VLANs) on a single switch in a home lab environment. A Cisco switch named **HomeLab** was set up to support four departments: **Sales, Marketing, Accounting, and Finance**.

Each department was assigned its own VLAN to improve network organisation, enhance security, and separate network traffic. Although all devices are connected to the same physical switch, VLAN configuration ensures that each department operates within its own isolated broadcast domain.

The lab was completed using **Cisco Packet Tracer**, focusing on Layer 2 switching concepts commonly used in enterprise and home lab networks.



Lab Objectives

The objectives of this lab are to:

- Understand the purpose and benefits of VLANs for network segmentation
- Create and name VLANs on a Cisco switch
- Assign switch ports to VLANs according to departmental roles
- Verify VLAN configuration and port membership
- Demonstrate logical separation of network traffic on a single switch
- Apply enterprise networking concepts in a home lab environment

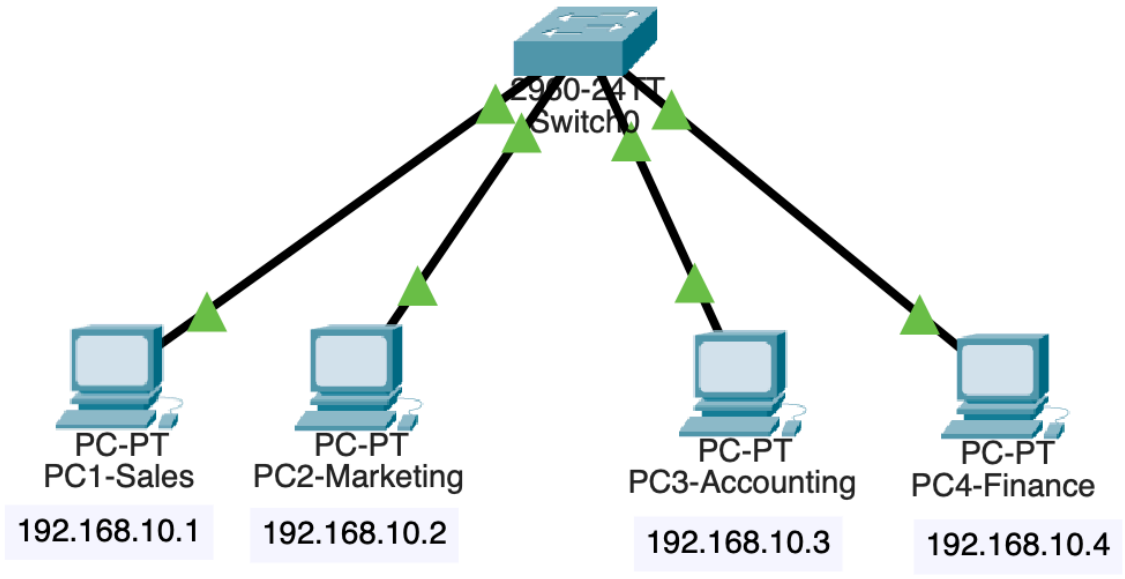
Lab Implementation

Step 1: Network Topology Setup

A basic network topology was created using **Cisco Packet Tracer**. One switch named **HomeLab** and four PCs were added to the workspace. Each PC represents a different department: Sales, Marketing, Accounting, and Finance.

All PCs were connected to the switch using **copper straight-through cables** with the following port assignments:

- **PC1 (Sales)** → FastEthernet0/1
- **PC2 (Marketing)** → FastEthernet0/2
- **PC3 (Accounting)** → FastEthernet0/3
- **PC4 (Finance)** → FastEthernet0/4



Step 2: IP Address Configuration

Each PC was manually assigned an IPv4 address in the same subnet to allow initial communication testing:

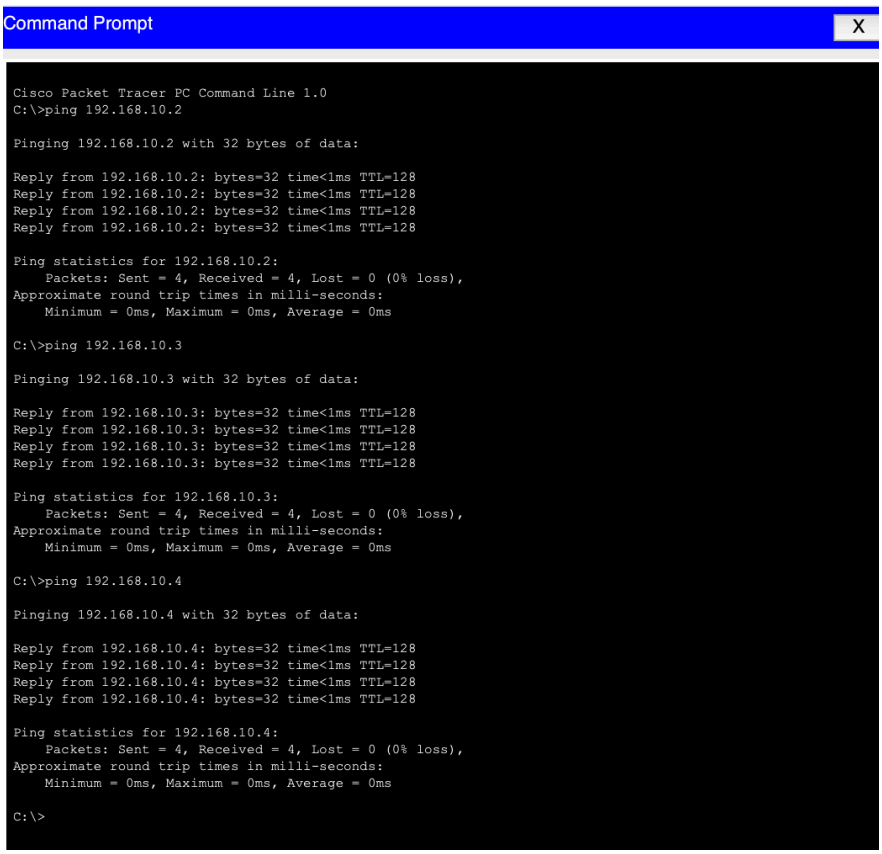
- **PC1:** 192.168.10.1
- **PC2:** 192.168.10.2
- **PC3:** 192.168.10.3
- **PC4:** 192.168.10.4

The subnet mask used for all PCs was **255.255.255.0**.

Step 3: Connectivity Verification

After IP configuration, connectivity between all PCs was tested using the **ping** command. Each PC successfully pinged the other three PCs, confirming that all devices could communicate with each other before VLAN segmentation was applied.

This step establishes a baseline network state, demonstrating that all devices are initially part of the same broadcast domain.



Step 4: Switch Access and Default Configuration Verification

After confirming end-device connectivity, the Cisco switch was accessed through the **Command Line Interface (CLI)** to begin configuration.

Before making any changes, the default switch state was verified to ensure the network was functioning correctly:

- The existing VLAN configuration was checked to confirm that only the default VLANs were present.
- The MAC address table (CAM table) was examined to verify that the switch had successfully learned the MAC addresses of all connected PCs on their respective ports.

These verification steps confirmed that the switch was operating normally and that all devices were communicating within the same default broadcast domain prior to VLAN segmentation.

```
Switch>
Switch>
Switch>en
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, 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
                                                Gig0/1, Gig0/2
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
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

```
Switch#show mac-
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.435e.5678    DYNAMIC     Fa0/1
   1    0001.64ed.0dca    DYNAMIC     Fa0/3
   1    0002.17a2.679d    DYNAMIC     Fa0/2
   1    0003.e428.0b0c    DYNAMIC     Fa0/4
Switch#
```

Step 5: Switch Identification and VLAN Creation

Once the default configuration was verified, initial switch configuration began.

First, the switch hostname was changed to **HomeLab** for easier identification and management.

Next, four VLANs were created to logically separate the network based on departmental roles:

- **VLAN 2 – Sales**
- **VLAN 3 – Marketing**
- **VLAN 4 – Accounting**
- **VLAN 5 – Finance**

Each VLAN was assigned a descriptive name to clearly reflect its department. This step establishes the foundation for network segmentation by creating separate broadcast domains on the same physical switch.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname HomeLab
HomeLab(config)#vlan 2
HomeLab(config-vlan)#name Sales
HomeLab(config-vlan)#vlan 3
HomeLab(config-vlan)#name Marketing
HomeLab(config-vlan)#vlan 4 Accounting
                    ^
% Invalid input detected at '^' marker.

HomeLab(config-vlan)#vlan 4
HomeLab(config-vlan)#name Accounting
HomeLab(config-vlan)#vlan 5
HomeLab(config-vlan)#name Finance
```

Verification

After creating and naming the VLANs, the configuration was verified by checking the VLAN table on the switch. The verification confirmed that:

- All four VLANs were successfully created
- VLAN IDs and names matched the intended department assignments
- The VLANs were active and ready for port assignment

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, 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
                                                 Gig0/1, Gig0/2
2    Sales                             active
3    Marketing                         active
4    Accounting                        active
5    Finance                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 6: Assigning Switch Ports to VLANs

After successfully creating and verifying the VLANs, switch ports were assigned to their respective VLANs based on departmental roles.

Each PC-connected port on the **HomeLab** switch was configured as an access port and assigned to the appropriate VLAN:

- **FastEthernet0/1 → VLAN 2 (Sales)**
- **FastEthernet0/2 → VLAN 3 (Marketing)**
- **FastEthernet0/3 → VLAN 4 (Accounting)**
- **FastEthernet0/4 → VLAN 5 (Finance)**

Configuring the ports as access ports ensures that each connected device belongs to a single VLAN and prevents unintended VLAN traffic.

```
HomeLab#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HomeLab(config)#inter
HomeLab(config)#interface f0/1
HomeLab(config-if)#switchport mode access
HomeLab(config-if)#switchport access vlan 2
HomeLab(config-if)#exit
HomeLab(config)#interface f0/2
HomeLab(config-if)#switchport mode access
HomeLab(config-if)#switchmode access vlan 3
                          ^
% Invalid input detected at '^' marker.

HomeLab(config-if)#switchport access vlan 3
HomeLab(config-if)#exit
HomeLab(config)#interface f0/3
HomeLab(config-if)#switchport mode access
HomeLab(config-if)#switchport access vlan 4
HomeLab(config-if)#exit
HomeLab(config)#interface f0/4
HomeLab(config-if)#switchport mode access
HomeLab(config-if)#switchport access vlan 5
HomeLab(config-if)#exit
HomeLab(config)#
```

Verification

After assigning the ports, the configuration was verified by checking the VLAN-to-port mapping on the switch. The verification confirmed that:

- Each port was assigned to the correct VLAN
- No ports remained incorrectly associated with the default VLAN
- The switch ports were active and correctly segmented

This step completes the logical network segmentation by enforcing VLAN separation at the switch port level.

```
HomeLab(config)#do show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, 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
                                                 Gig0/1, Gig0/2
2    Sales                             active    Fa0/1
3    Marketing                         active    Fa0/2
4    Accounting                        active    Fa0/3
5    Finance                           active    Fa0/4
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

HomeLab(config)#
```

Step 7: Post-Segmentation Connectivity Testing

After assigning switch ports to their respective VLANs, connectivity tests were performed to validate network segmentation.

Each PC attempted to ping the other three PCs located in different VLANs. The ping tests were **unsuccessful**, confirming that devices in separate VLANs could no longer communicate with one another.

This result is expected behaviour, as VLANs create separate broadcast domains. Without inter-VLAN routing configured, traffic between VLANs is blocked at the switch level.

The successful failure of these ping tests verifies that VLAN segmentation has been implemented correctly and that departmental network isolation is functioning as intended.

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Final Lab Conclusion

This lab successfully demonstrated how Virtual Local Area Networks (VLANs) can be used to logically segment a network using a single physical switch. By placing devices from different departments—Sales, Marketing, Accounting, and Finance—into separate VLANs, network traffic was effectively isolated even though all devices were connected to the same switch.

Initial connectivity testing confirmed that all PCs could communicate when operating in the default VLAN. After VLAN creation and port assignment, post-segmentation ping tests failed as expected, verifying that inter-VLAN communication was blocked without routing configuration. This confirms that each department operates within its own broadcast domain.

Through this lab, foundational skills in switch configuration, VLAN implementation, and network verification were developed. The concepts demonstrated in this home lab reflect real-world enterprise networking practices and highlight the importance of network segmentation for improved security, performance, and manageability.