



VLAN

Complete Notes CCNA to CCIE

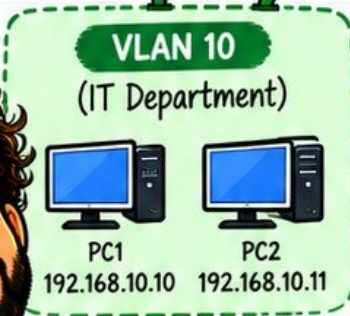
- ✓ Concepts
- ✓ Configuration
- ✓ Trunking
- ✓ Inter-VLAN
- ✓ Troubleshooting
- ✓ Commands
- ✓ Diagrams
- ✓ Real-world Examples

- ✓ Theory + Diagrams
- ✓ Step-by-Step Configs
- ✓ CCNA to CCIE Level
- ✓ Real Scenarios
- ✓ Interview Points

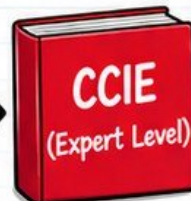
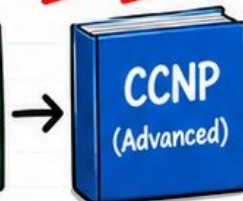
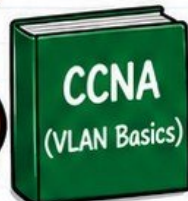


Same Switch
Different Networks

Better Segmentation
More Security
More Control



"Same Infrastructure
Multiple Networks
That's VLAN!"



- What You'll Learn?**
- ✓ What is VLAN?
 - ✓ Types of VLAN
 - ✓ Access & Trunk Ports
 - ✓ VLAN Configuration
 - ✓ Inter-VLAN Routing
 - ✓ VTP, DTP, Native VLAN
 - ✓ Troubleshooting VLAN
 - ✓ Practical Examples
 - ✓ CCNA to CCIE Concepts



1 What is VLAN?

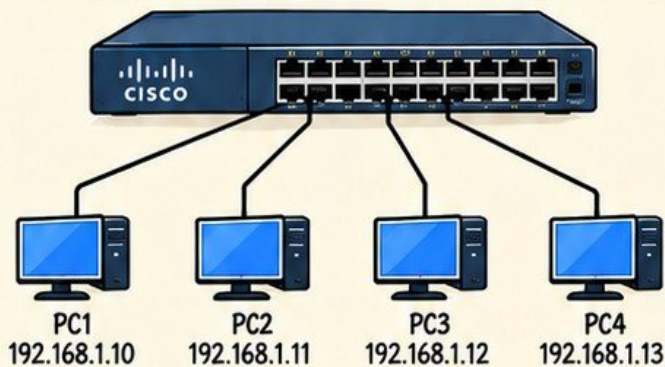
- **VLAN (Virtual Local Area Network)** is a **logical separation** of a physical network into multiple broadcast domains.
- It allows multiple networks to run on the same physical infrastructure.
- Each VLAN is like an independent LAN with its own broadcast domain.
- Helps in better segmentation, security and bandwidth utilization.

2 Why Do We Use VLAN?

- **Segmentation** – Separate departments or users.
- **Security** – Isolate sensitive data.
- **Reduce Broadcast Traffic** – Smaller broadcast domains.
- **Better Network Management** – Easy to manage.
- **Cost Saving** – Multiple networks on same hardware.
- **Flexibility** – Users can be moved easily between VLANs.
- **Improved Performance** – Less unnecessary traffic.

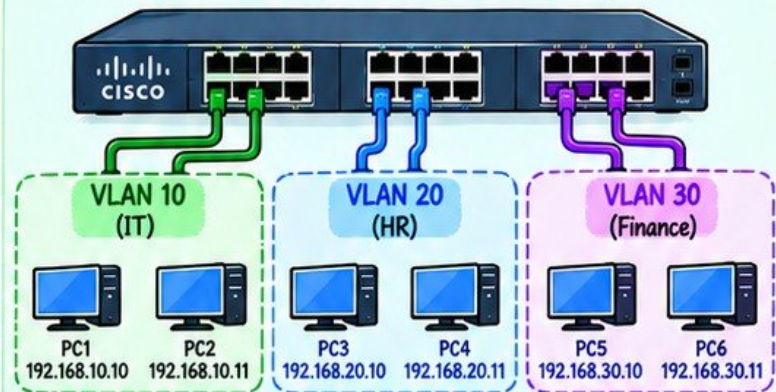
3 Traditional Network vs VLAN Network

Traditional Network (Without VLAN)



- All devices in same broadcast domain
- No separation between departments
- More broadcast traffic
- Less secure

VLAN Network (With VLAN)



- Multiple broadcast domains on same switch
- Separate departments
- Less broadcast traffic
- More secure and organized

4 Key Terms

Term	Description
VLAN	Logical network segment on a switch.
Broadcast Domain	A group of devices that receive broadcast traffic.
Trunk	Carries multiple VLANs between devices.
Access Port	Port that belongs to a single VLAN.
Trunk Port	Port that carries multiple VLANs using 802.1Q tagging.
VLAN ID	A unique number (1-4094) to identify a VLAN.
Native VLAN	VLAN used for untagged traffic on a trunk link.

5 VLAN ID Range

Range	Name	Usage
0	Reserved	Cannot be used
1	Default VLAN	Default management VLAN
2 – 1001	Normal VLANs	Commonly used for users and departments
1002 – 1005	FDDI/Token Ring	Legacy (not used)
1006 – 4094	Extended VLANs	Supported on most modern switches

In real networks, different types of VLANs are used for different purposes.
Understanding VLAN types is important from **CCNA to CCIE** level.

1 Data VLAN

- Used for normal user data traffic
- Assigned to user ports (Access Ports)
- Example: VLAN 10, 20, 30 for different departments



2 Default VLAN

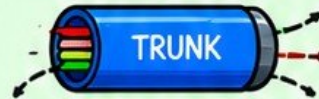
- **VLAN 1** is default on Cisco switches
- All ports are in **VLAN 1** by default
- Should not be used for production (security risk)



Avoid using VLAN 1 for user traffic!

3 Native VLAN

- Used on trunk ports for **untagged traffic**
- Frames without VLAN tag are placed in **Native VLAN**
- Default Native VLAN is **VLAN 1** (but should be changed)

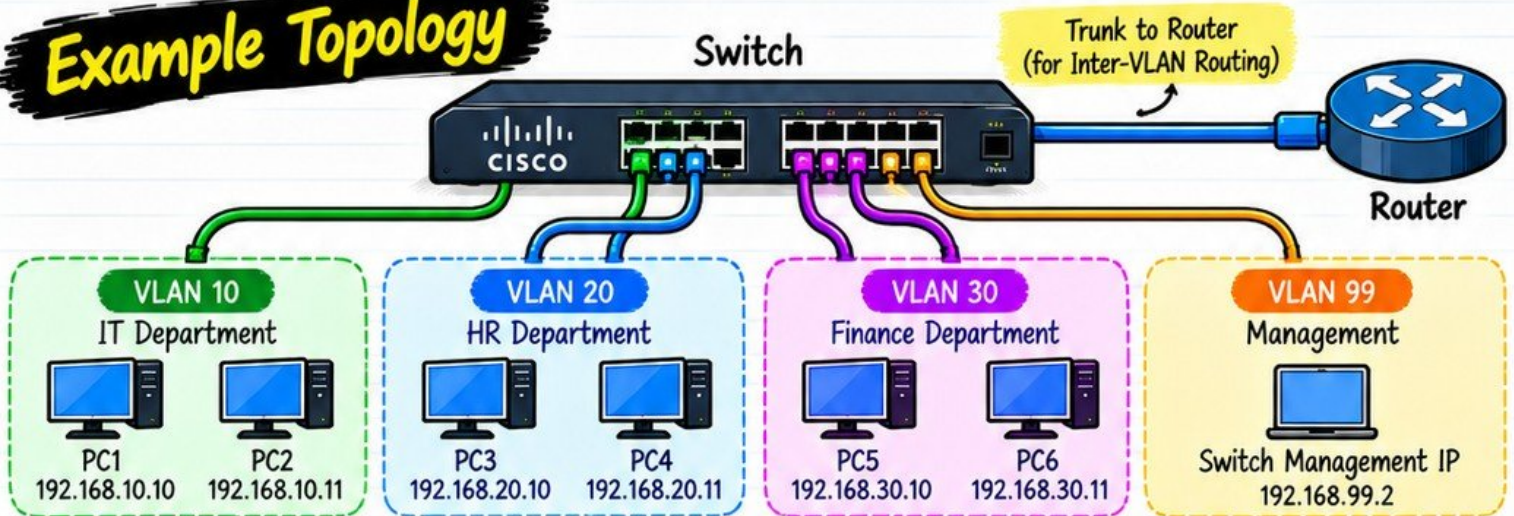


4 Management VLAN

- Used for device management (Switch, Router, Firewall, etc.)
- Separate from user traffic for security
- Example: **VLAN 99**



Example Topology



Quick Summary:

- ✓ Data VLAN → User traffic
- ✓ Default VLAN → VLAN 1 (avoid)
- ✓ Native VLAN → Untagged traffic on trunk
- ✓ Management VLAN → Device management
- ✓ Use separate VLANs for better security, performance and management.



Different VLANs...
Different Purposes!



VLAN Trunking allows **multiple VLANs** to be carried over a **single physical link** between network devices (switch to switch, switch to router, switch to firewall, etc.).

What is Trunk?

- A trunk link is a link between two network devices that carries traffic for **multiple VLANs** using VLAN **tagging (802.1Q)**.

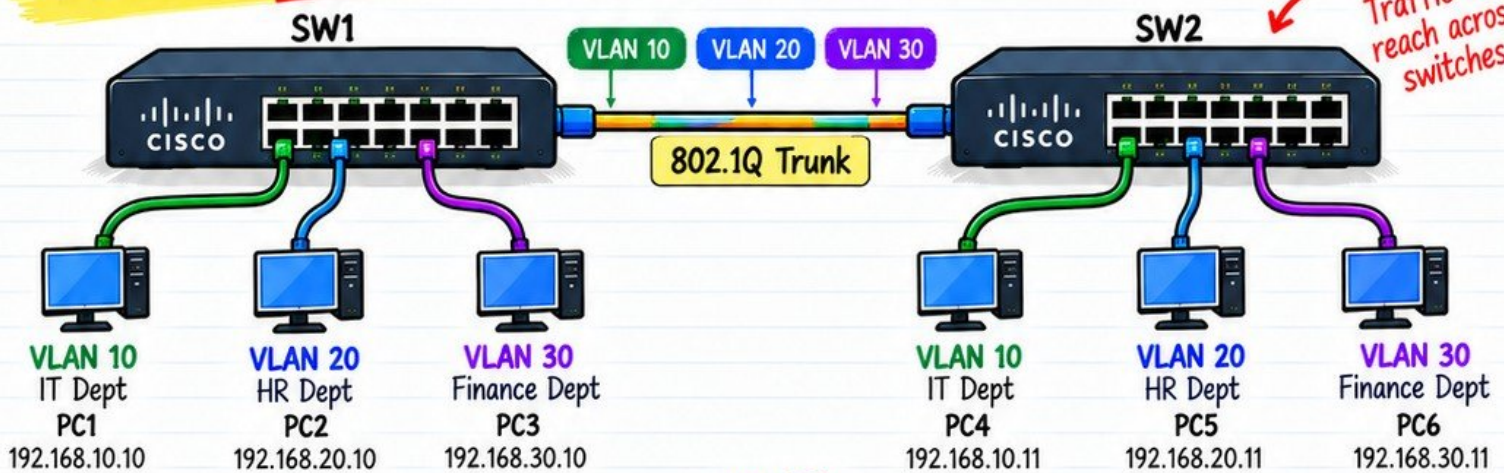
Key Points:

- ✓ Uses **802.1Q** tagging
- ✓ Carries **multiple VLANs**
- ✓ Used between switches, switch to router (Router-on-a-Stick), switch to firewall, etc.
- ✓ One physical link, **many VLANs**
- ✓ Native VLAN is used for **untagged traffic**

Where Trunk is Used?

- ✓ Switch to Switch
- ✓ Switch to Router (Inter-VLAN Routing)
- ✓ Switch to Firewall
- ✓ Switch to Load Balancer
- ✓ Any device that needs multiple VLANs

Trunk Link Example (Switch to Switch)



Frame Format

Preamble	SFD	Destination MAC	Source MAC	802.1Q Tag	Type/Length	Data	FCS
7 Bytes	1 Byte	6 Bytes	6 Bytes	4 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

802.1Q Tag Details

TPID (0x8100)	Priority (PCP)	DEI (CFI)	VLAN ID (VID)
16 bits	3 bits	1 bit	12 bits

VLAN Tag (802.1Q adds 4 bytes)

VLAN ID Range:
0 - 4095

- 0 and 4095 : Reserved
- 1 : Default VLAN
- 2 - 1001 : Normal VLANs
- 1002 - 1005 : Reserved (for FDDI/Token Ring)

Native VLAN

- ✓ Frames from native VLAN are sent **without 802.1Q tag**.
- ✓ Default native VLAN is 1.
- ✓ Should be **changed for security reasons**.



Try to use an **unused VLAN** as native VLAN (e.g. 999).



Inter-VLAN Routing allows communication between different VLANs. Since VLANs are in different **broadcast domains**, a Layer 3 device (Router or L3 Switch) is required for inter-VLAN communication.

What is Inter-VLAN Routing?

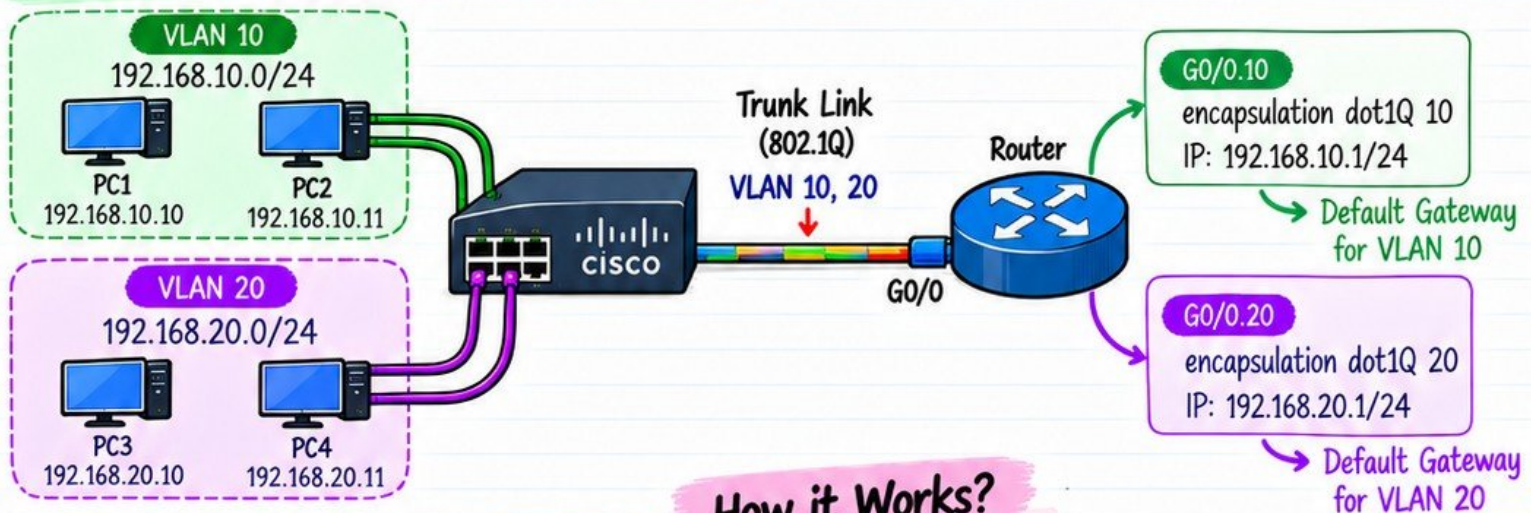
- ✓ VLANs are separate networks.
- ✓ By default, they **cannot communicate** with each other.
- ✓ Inter-VLAN Routing enables communication between VLANs using a **Layer 3 device** (Router or L3 Switch).
- ✓ Each VLAN has its own **default gateway** (SVI or Sub-interface).



Methods of Inter-VLAN Routing

- 1 Router-on-a-Stick (ROAS)**
Single physical link with trunk and sub-interfaces on router.
- 2 Layer 3 Switch (SVI)**
Using Switched Virtual Interfaces (SVI) on L3 switch.
- 3 Multiple Physical Interfaces**
Separate physical interface for each VLAN (not preferred).

Method 1: Router-on-a-Stick (ROAS)



Router Sub-interface Configuration (Cisco IOS)

```
Router(config)# interface g0/0
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# interface g0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit

Router(config)# interface g0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
```

How it Works?

- 1 Switch trunk forwards VLAN tagged traffic to router.
- 2 Router sub-interfaces handle each VLAN.
- 3 Router routes traffic between VLANs.
- 4 Devices use router sub-interface IP default gateway.

Pros & Cons of ROAS

- ✓ **Advantages:**
 - Cost effective (single link)
 - Simple setup
 - Works on routers with 802.1Q
- ✗ **Disadvantages:**
 - Single physical link (bandwidth bottleneck)
 - Router becomes single point of failure
 - Not ideal for high traffic environment

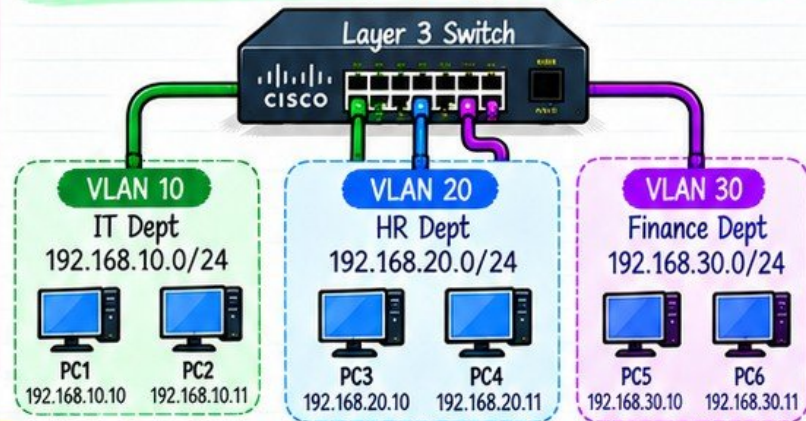


A Layer 3 Switch can perform inter-VLAN routing using **Switched Virtual Interfaces (SVI)**. Each VLAN has a **Gateway (SVI)** on the L3 switch, which enables communication between VLANs.

What is SVI?

- ✓ Switched Virtual Interface (SVI) is a Layer 3 interface on a **Layer 3 switch**.
- ✓ Acts as the default gateway for the VLAN.
- ✓ Enables inter-VLAN routing without an external router.
- ✓ Each VLAN has its own SVI with an IP address.

Inter-VLAN Routing Topology (Using L3 Switch)



Configuration on Layer 3 Switch (Cisco IOS)

- ```
Switch(config)# vlan 10
Switch(config-vlan)# name IT
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name HR
Switch(config-vlan)# exit
Switch(config)# vlan 30
Switch(config-vlan)# name FINANCE
Switch(config-vlan)# exit

! Create SVI for each VLAN
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 30
Switch(config-if)# ip address 192.168.30.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

! Enable IP routing
Switch(config)# ip routing
```

SVI =  
Default Gateway  
for each VLAN

## Verification Commands

Switch# **show ip interface brief**

| Interface | IP-Address   | OK? | Method | Status |
|-----------|--------------|-----|--------|--------|
| Vlan10    | 192.168.10.1 | YES | manual | up/up  |
| Vlan20    | 192.168.20.1 | YES | manual | up/up  |
| Vlan30    | 192.168.30.1 | YES | manua  | up/up  |

Switch# **show vlan brief**

| VLAN | Name    | Status | Ports            |
|------|---------|--------|------------------|
| 10   | IT      | active | Gi1/0/1, Gi1/0/2 |
| 20   | HR      | active | Gi1/0/3, Gi1/0/4 |
| 30   | FINANCE | active | Gi1/0/5, Gi1/0/6 |

## Testing Inter-VLAN Communication

- PC1 (VLAN 10) → ping 192.168.20.10 ✓ Success
- PC1 (VLAN 10) → ping 192.168.30.10 ✓ Success
- PC3 (VLAN 20) → ping 192.168.10.10 ✓ Success
- PC5 (VLAN 30) → ping 192.168.10.10 ✓ Success

## Limitations

- Not suitable for very large or complex networks (use dedicated router/Firewall).
- Consumes L3 switch resources (CPU, memory).
- Advanced features like NAT, VPN may not be available.
- Use proper ACLs for security between VLANs.

## Key Points

- Each VLAN has a **unique SVI** with IP address.
- Enable **'ip routing'** on L3 switch.
- SVIs act as **default gateway** for VLAN.
- No external router required.
- Works at **high speed** (hardware-based routing).
- Commonly used in enterprise networks and data centers.

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol that manages VLANs across multiple switches in a network. It helps maintain a consistent VLAN database.

## What is VTP?

- ✓ Shares VLAN information across switches.
- ✓ Reduces manual configuration on each switch.
- ✓ Works over trunk links only.
- ✓ Uses VTP domain to identify the same network.
- ✓ Only VLAN information is shared (not interfaces, STP, etc.).



## VTP Modes

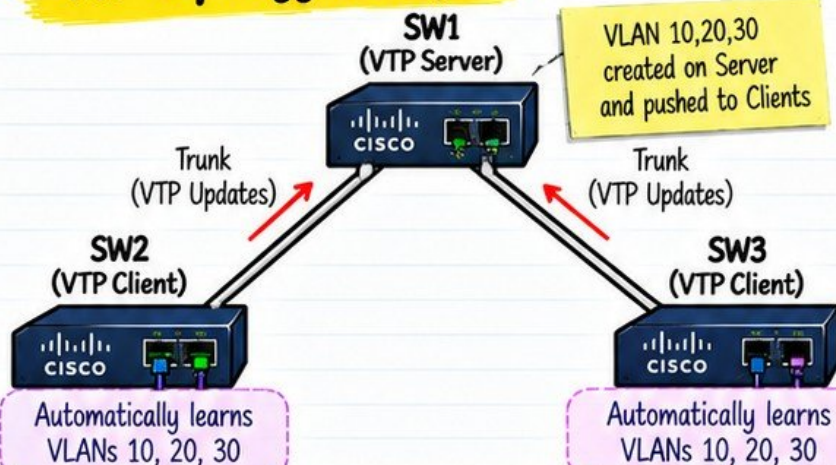
- 1 Server**
  - Can create, modify and delete VLANs.
  - Sends VLAN updates to clients.
  - Stores VLAN database in NVRAM.
- 2 Client**
  - Cannot create, modify or delete VLANs.
  - Receives VLAN updates from server.
  - Stores VLAN database in RAM only (lost after reload).
- 3 Transparent**
  - Does not participate in VTP updates.
  - Can create, modify and delete local VLANs (not advertised).
  - Forwards VTP updates to other switches.



## VTP Components

- ✓ **VTP Domain**  
(Switches must be in same domain to share VLANs)
- ✓ **VTP Version**  
(Version 1, 2 or 3)
- ✓ **VTP Mode**  
(Server / Client / Transparent)
- ✓ **VTP Password**  
(Optional, for security)
- ✓ **VTP Revision Number**  
(Increments with each change)

## VTP Topology Example



## Basic VTP Configuration (Server)

```

Switch(config)# vtp domain TECHNETWORKK
Switch(config)# vtp mode server
Switch(config)# vtp password cisco123
Switch(config)# vtp version 2

! Create VLANs (will be advertised to clients)
Switch(config)# vlan 10
Switch(config-vlan)# name IT
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name HR
Switch(config-vlan)# vlan 30
Switch(config-vlan)# name FINANCE

```



## Client Configuration

```

Switch(config)# vtp domain TECHNETWORKK
Switch(config)# vtp mode client
Switch(config)# vtp password cisco123
Switch(config)# vtp version 2

! VLANs will be learned automatically from the server.

```



## Verify VTP Status

```

Switch# show vtp status
VTP Version : 2
Configuration Revision : 5
Maximum VLANs supported : 255
Number of existing VLANs : 4
VTP Operating Mode : Server
VTP Domain Name : TECHNETWORKK
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled

```



## Show VLANs Learned

```

Switch# show vlan brief
VLAN Name Status Ports
1 default active Gi1/0/1
10 IT active
20 HR active
30 FINANCE active

```



## Important:

- Always use same VTP domain and version.
- Use VTP password for security.
- In large networks, consider using VTP Transparent mode to avoid accidental VLAN deletion.

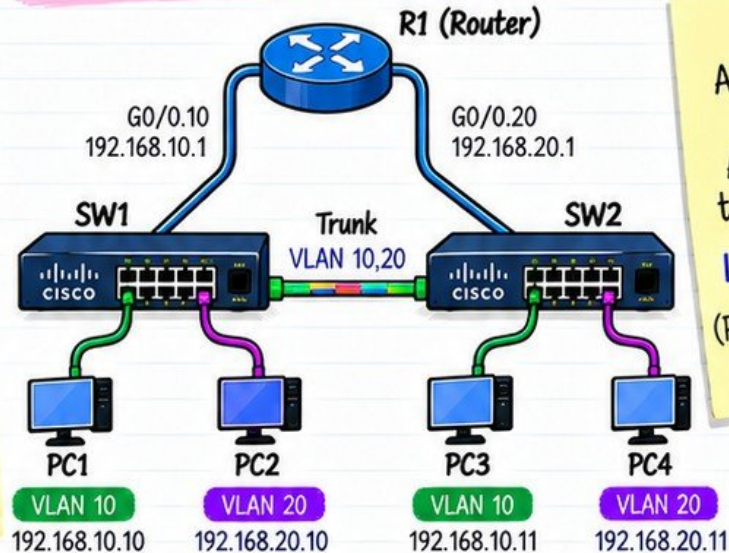


VLAN issues are very common in real networks. Here are common problems, their causes and solutions.  
These troubleshooting steps are important from **CCNA to CCIE** level.

## Common VLAN Issues

- 1 PC not getting IP in VLAN
- 2 VLAN not working on trunk
- 3 Cannot ping between VLANs
- 4 VLAN missing in VTP database
- 5 SVI down / not reachable
- 6 Wrong VLAN assigned on port
- 7 Inter-VLAN routing not working
- 8 VLAN allowed list mismatch
- 9 Native VLAN issues (stp, mismatch)
- 10 VLAN exists on one switch only

## Example Topology (for troubleshooting)



Always follow a  
Systematic  
Approach while  
troubleshooting:  
**L1 → L2 → L3**  
(Physical → VLAN → Routing)

## Useful Show Commands

| Purpose                     | Command (Cisco IOS)                                 |
|-----------------------------|-----------------------------------------------------|
| Check VLANs on switch       | <code>show vlan brief</code>                        |
| Check trunk status          | <code>show interfaces trunk</code>                  |
| Check switchport config     | <code>show interfaces &lt;int&gt; switchport</code> |
| Check VTP status            | <code>show vtp status</code>                        |
| Check MAC address table     | <code>show mac address-table vlan &lt;id&gt;</code> |
| Check interface status      | <code>show ip interface brief</code>                |
| Check STP status (per VLAN) | <code>show spanning-tree vlan &lt;id&gt;</code>     |
| Check DHCP (if SVI is used) | <code>show ip dhcp binding</code>                   |
| Check configuration         | <code>show running-config   section vlan</code>     |

## Sample Troubleshooting Scenarios

- 1 **PC not getting IP in VLAN**
  - Check correct VLAN assigned on access port
  - Verify cable, port status
  - Check DHCP server or SVI IP
  - Use: `show vlan brief`, `show interfaces <int> switchport`
- 2 **VLAN not working on trunk**
  - Verify trunk is up and VLAN allowed
  - Check native VLAN mismatch
  - Use: `show interfaces trunk`
  - Ensure VLAN exists on both switches
- 3 **Cannot ping between VLANs**
  - Check if inter-VLAN routing is configured (Router or L3 Switch)
  - Verify SVI IP and status (up/up)
  - Check routing, ACL, firewall
  - Use: `show ip interface brief`

## Verification Checklist

- ✓ VLAN exists on all required switches
- ✓ Access ports are in correct VLAN
- ✓ Trunk links are up and allowing required VLANs
- ✓ SVI is up and reachable
- ✓ Inter-VLAN routing is enabled (if required)
- ✓ No ACL blocking the traffic
- ✓ VTP domain/version/password match (if using VTP)
- ✓ STP is stable (no unexpected blocking)

## Debugging Tips

- Check physical connectivity first
- Use show commands to verify VLAN and trunk status
- Make sure VLAN exists end-to-end
- Verify SVI IP and routing
- Check for ACL or firewall rules
- Look for native VLAN mismatch
- Use ping and tracert for testing
- Compare running-config between switches

## Common Mistakes

- ✗ VLAN not created on all switches
- ✗ Access port left in default VLAN 1
- ✗ VLAN not allowed on trunk
- ✗ Native VLAN mismatch
- ✗ SVI in shutdown state
- ✗ Wrong VTP domain or version
- ✗ Inter-VLAN routing not configured
- ✗ ACL blocking inter-VLAN traffic

VLANs help in network segmentation, but proper security practices are required to prevent unauthorized access, **VLAN hopping** and other **Layer 2 attacks**.



## Why VLAN Security is Important?

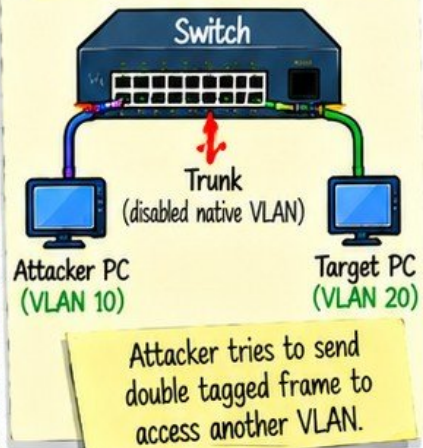
- ✓ Prevents unauthorized access between departments.
- ✓ Reduces broadcast traffic and attacks.
- ✓ Protects against Layer 2 attacks like VLAN Hopping.
- ✓ Helps in compliance and data protection.
- ✓ Enables better control using ACLs, Firewall and Security Policies.



## Common VLAN Security Threats

- 1 **VLAN Hopping**  
(DTP, double tagging)
- 2 **Unauthorized Access**  
to VLAN
- 3 **VLAN Spoofing**  
(Changing VLAN ID)
- 4 **MAC Flooding**  
(Exhaust switch MAC table)
- 5 **ARP Spoofing**  
(within same VLAN)
- 6 **STP Manipulation**  
(priority attack, root bridge)

## VLAN Hopping Example



### 1 Disable Unused Ports

```
Switch(config)#
interface range f0/10 - 24
switchport mode access
switchport access vlan 999
shutdown
description Unused_Port
```

Put unused ports in a dummy VLAN and shutdown to prevent unauthorized access.

### 2 Disable DTP (Dynamic Trunking Protocol)

```
Switch(config)#
interface g0/1
switchport mode access
switchport nonegotiate
switchport access vlan 10
```

Disable DTP to prevent attackers from forcing a trunk and performing VLAN hopping.

### 3 Use a Dedicated Native VLAN

```
Switch(config)#
interface g0/1
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30
```

Never use VLAN 1 as native VLAN. Use a dedicated and unused VLAN (e.g. 999).

### 4 Limit Allowed VLANs on Trunk

```
Switch(config)#
interface g0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
```

Allow only required VLANs on trunk to reduce attack surface.

### 5 Enable Port Security

```
Switch(config)#
interface f0/5
switchport mode access
switchport access vlan 10
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
```

Prevents unauthorized devices from connecting and stops MAC flooding attacks.

### 6 Use ACLs Between VLANs



Router / L3 Switch

```
ip access-list extended HR-ACL
deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
permit ip any any
```

```
interface vlan 10
ip access-group HR-ACL in
```

Use ACLs on Layer 3 devices to control traffic between VLANs.

### 7 Enable DHCP Snooping

```
Switch(config)#
ip dhcp snooping
ip dhcp snooping vlan 10,20,30
interface g0/1
ip dhcp snooping trust ! (trusted port to DHCP server)
```

Prevents rogue DHCP servers and DHCP attacks.

### 8 Enable Dynamic ARP Inspection (DAI)

```
Switch(config)#
ip arp inspection vlan 10,20,30
interface g0/1
ip arp inspection trust
```

Prevents ARP spoofing attacks within VLAN.



VLANs are one of the most important topics from **CCNA to CCIE**. They help in network segmentation, improve security, reduce broadcast traffic and make the network easy to manage.



### Complete VLAN Recap

- 1 What is VLAN? (Logical segmentation)
- 2 VLAN ID (1-4094, 1 & 1002-1005 reserved)
- 3 Access Port (Single VLAN)
- 4 Trunk Port (Multiple VLANs)
- 5 Inter-VLAN Routing (ROAS / SVI)
- 6 VTP (Server / Client / Transparent)
- 7 VLAN Trunking (Tagging 802.1Q)
- 8 VLAN Security (Best Practices)
- 9 Troubleshooting (Common issues)
- 10 Real-World Use Cases (Enterprise)

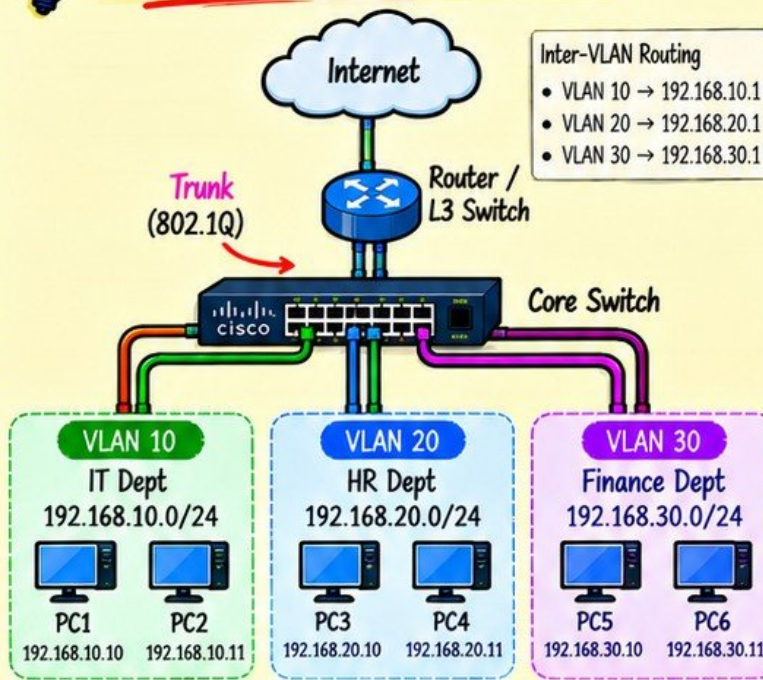


### Key Takeaways

- ✓ VLANs separate networks and reduce broadcast traffic.
- ✓ Each VLAN has its own broadcast domain.
- ✓ Use trunk links for inter-switch VLAN communication.
- ✓ Use SVI or Router-on-a-Stick for inter-VLAN routing.
- ✓ VTP helps in VLAN management across switches.
- ✓ Use proper security best practices (disable unused ports, port-security, DTP, DHCP snooping, etc.).
- ✓ Always follow a systematic troubleshooting approach.
- ✓ Plan VLANs as per business requirements.
- ✓ VLANs are widely used in enterprise networks, data centers and campus environments.



### Real-World Enterprise Example



### Best Practices for VLAN Design

- ✓ Plan VLAN ID and IP addressing properly.
- ✓ Use meaningful VLAN names (IT, HR, Finance, etc.).
- ✓ Disable unused switch ports.
- ✓ Use port-security to prevent unauthorized access.
- ✓ Disable DTP on access ports.
- ✓ Implement ACLs between VLANs for security.
- ✓ Use VTP only if required (otherwise Transparent mode).
- ✓ Monitor VLANs using SNMP, Syslog and NMS.



### Next Steps (Level Up)

- CCNA Level** → Learn basic VLAN, Trunk, Inter-VLAN Routing and VTP.
- CCNP Level** → Advanced VLAN Design, Troubleshooting, VTP, Security and Enterprise Scenarios.
- CCIE Level** → Large Scale VLAN Design, Multi-Site, High Availability, Security, Automation and Real-World Architectures.

“VLANs are the foundation of a well-designed and secure network.”  
- Technetworkk



Save This Post  
For Future Reference

