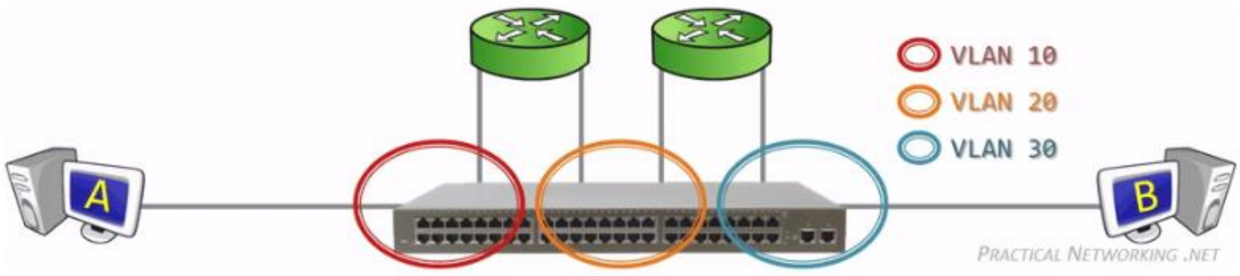
Understanding VLANs – The Complete Guide

Virtual LANs (VLANs) are the backbone of modern network segmentation. They allow multiple logical networks to exist on a single switch, giving **better performance, security, and control**.
Let's dive deep into **what VLANs are, their types, commands, advantages, and real-world use cases.**



What is a VLAN?

A **VLAN (Virtual Local Area Network)** is a logical network created inside a switch to segment devices into smaller, isolated groups, regardless of their physical location.

- Without VLANs, all devices connected to a switch belong to **one broadcast domain**, meaning **every broadcast packet is sent to all devices** – which causes unnecessary traffic and potential security risks.
- With VLANs, devices can be grouped **logically** (e.g., HR VLAN, IT VLAN, Guest VLAN), and **broadcasts stay within their own group**.

Example:

If HR is assigned VLAN 10, Finance VLAN 20, and IT VLAN 30, traffic from HR won't reach Finance unless a router or Layer 3 switch routes it.

Advantages of VLANs

- **Security:** Sensitive data from one department is isolated from others.
- **Reduced Broadcast Traffic:** Each VLAN forms its **own broadcast domain**, preventing unnecessary flooding.

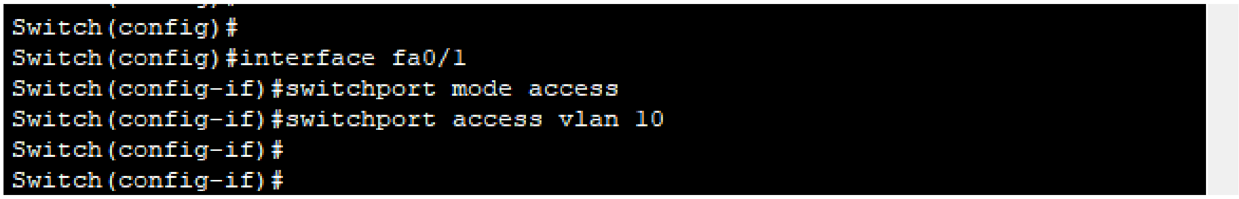
- **Better Performance:** Segmentation ensures that only relevant devices receive traffic.
- **Flexibility:** Devices from different floors or buildings can share the same VLAN.
- **Easier Management:** Network administrators can logically group devices without rewiring.
- **Scalability:** Adding or moving devices to another VLAN is just a configuration change.

VLAN Ports – Access vs. Trunk

1. Access Ports

- Connects **end devices** like PCs, printers, and IP phones.
- Assigned to **one VLAN only**.
- All untagged traffic entering or leaving the port belongs to that VLAN.

Example Command:



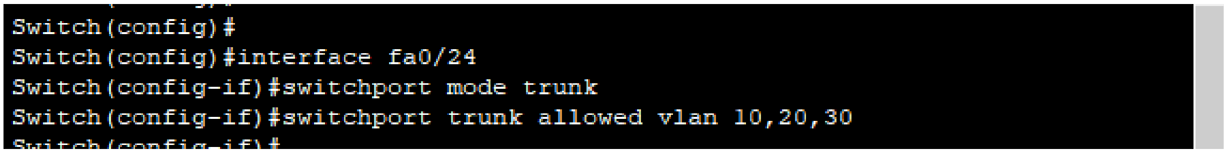
```
Switch(config)#
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
Switch(config-if)#
```

Use Case:
HR employee's PC is connected to a switch port assigned to VLAN 10 (HR VLAN).

2. Trunk Ports

- Carry traffic from **multiple VLANs** across switches or to routers.
- VLANs are identified by **802.1Q tags** (except for the native VLAN).
- Essential for networks with multiple VLANs spanning across different switches.

Example Command:



```
Switch(config)#
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30
Switch(config-if)#
```

Use Case:
A trunk port connects Switch A and Switch B, allowing VLAN 10 (HR), VLAN 20 (Finance), and VLAN 30 (IT) to communicate between both switches.

Single Broadcast Domain

- A VLAN **limits broadcasts to devices within that VLAN only**.
- Without VLANs, a broadcast (e.g., ARP requests) would flood the entire network.
- **Benefit:** Network efficiency improves because broadcasts do not overwhelm devices in other VLANs.

Example:
A broadcast from a PC in VLAN 10 is **never sent** to VLAN 20 or 30.

VLAN ID: Normal and Extended Range

Normal Range VLAN IDs

- **1 to 1005** (default range).
- Widely used in traditional networks.
- VLAN 1 is the **default VLAN** (avoid using it for data traffic).

Extended Range VLAN IDs

- **1006 to 4094.**
- Used in **large-scale enterprise or service provider networks**.
- Stored in a different database (requires VTP version 3 or transparent mode).

Why Extended VLAN Range?

- In large networks or data centers, 1005 VLANs may not be enough.
- Extended VLANs allow **thousands of isolated networks** for tenants, servers, or clients.

Types of VLANs

1. Data VLAN

Definition:

A **Data VLAN** (also called user VLAN) carries **regular network traffic** generated by user devices (PCs, laptops, IoT, printers). It is the most **common VLAN type**.

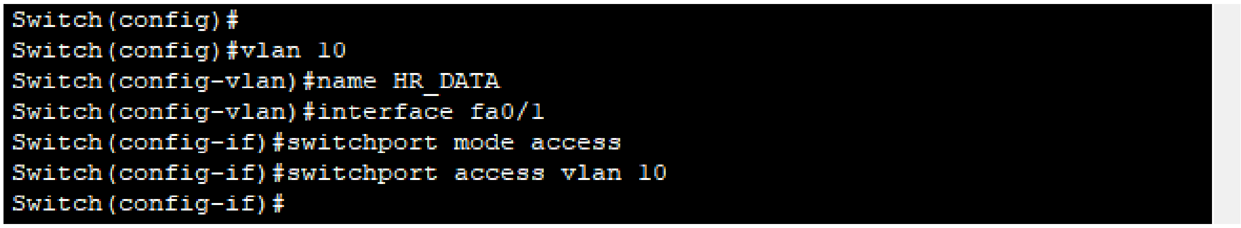
Key Points:

- Does not include voice or management traffic.
- Can be mapped to specific groups or departments.
- Helps **separate user data** from sensitive or high-priority traffic.

Use Case:

- VLAN 10 for HR, VLAN 20 for Finance, VLAN 30 for IT.
- Each department is isolated, reducing unnecessary traffic between them.

Example Configuration:



```
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name HR_DATA
Switch(config-vlan)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
```

Real-World Example:

In a hospital, VLAN 10 might carry traffic for patient record systems (HR & staff PCs), while VLAN 20 handles financial systems. This ensures **data confidentiality** and prevents misrouting of sensitive data.

2. Voice VLAN

Definition:

A **Voice VLAN** is dedicated to **VoIP (Voice over IP)** traffic. It ensures **low latency**, **minimal jitter**, and **high-quality calls** by prioritizing voice packets using **QoS (Quality of Service).**

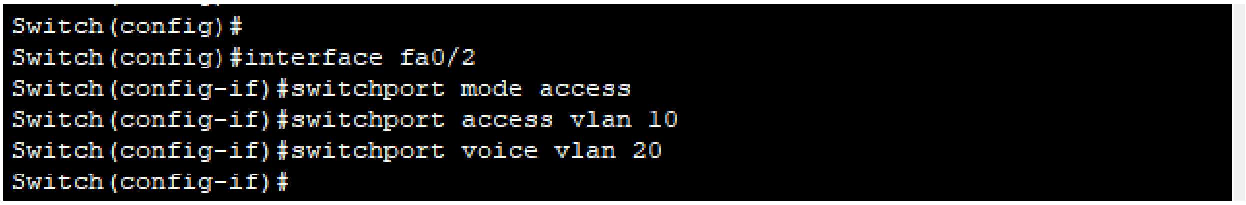
Key Points:

- IP phones often share the same physical port with a PC.
- The switch separates the **voice VLAN** from the **data VLAN** on the same port using tagging.
- Ensures that voice traffic is **prioritized over data** (using DSCP or CoS marking).

Use Case:

- VLAN 20 for IP phones in an office network.
- Port Fa0/1 might carry **data on VLAN 10** and **voice on VLAN 20** simultaneously.

Example Configuration:



```
Switch(config)#
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 20
Switch(config-if)#
```

Real-World Example:

Call centers and corporate offices always configure **Voice VLANs** to ensure **crystal-clear VoIP calls** even during heavy data traffic.

3. Default VLAN

Definition:

By default, all switch ports are assigned to **VLAN 1**. This is known as the **Default VLAN.**

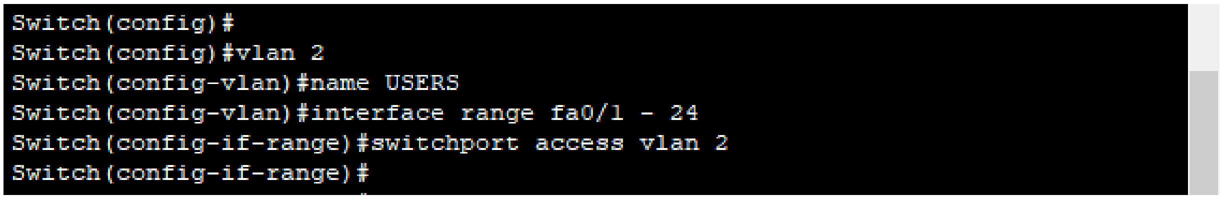
Key Points:

- Default VLAN carries **control plane protocols** like CDP, VTP, STP by default.
- **Best Practice:** Do not use VLAN 1 for user traffic due to security risks.

Use Case:

- Use VLAN 1 only for basic switch initialization, then move devices to other VLANs.

Example Configuration:



```
Switch(config)#
Switch(config)#vlan 2
Switch(config-vlan)#name USERS
Switch(config-vlan)#interface range fa0/1 - 24
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#
```

4. Native VLAN

Definition:

The **Native VLAN** is the VLAN that carries **untagged traffic** on a trunk port. By default, VLAN 1 is the native VLAN.

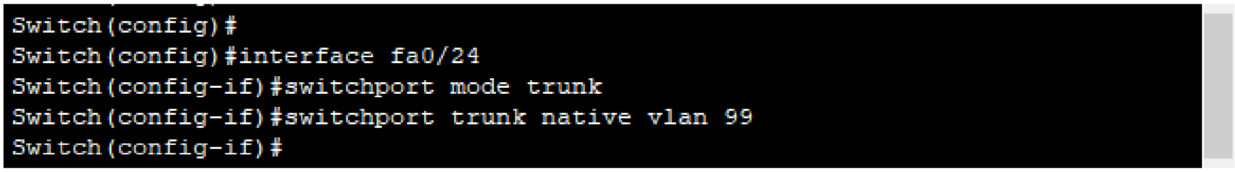
Key Points:

- Untagged traffic (e.g., control frames) is placed in the native VLAN.
- **Best Practice:** Change native VLAN from 1 to another unused VLAN for security.

Use Case:

- When a device does not support tagging (untagged frames), they are automatically assigned to the native VLAN.

Example Configuration:



```
Switch(config)#
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#
```

5. Management VLAN

Definition:

A **Management VLAN** is used exclusively for **device management traffic** (Telnet, SSH, HTTP, SNMP).

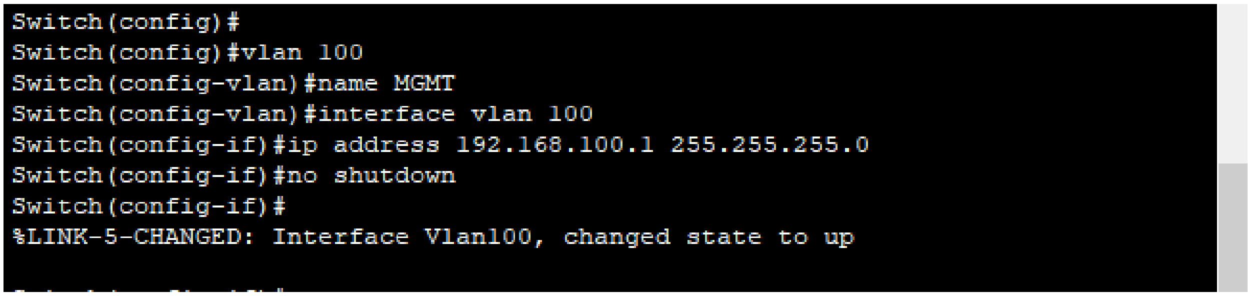
Key Points:

- Usually separate from data VLANs for **security and monitoring.**
- A switch's management IP is assigned to this VLAN.

Use Case:

- VLAN 100 is reserved for network administrators to remotely manage switches/routers.

Example Configuration:

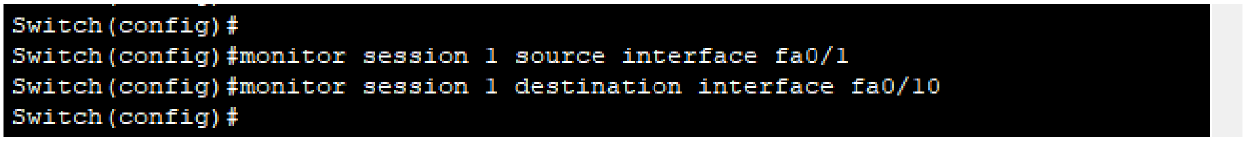


```
Switch(config)#
Switch(config)#vlan 100
Switch(config-vlan)#name MGMT
Switch(config-vlan)#interface vlan 100
Switch(config-if)#ip address 192.168.100.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up
```

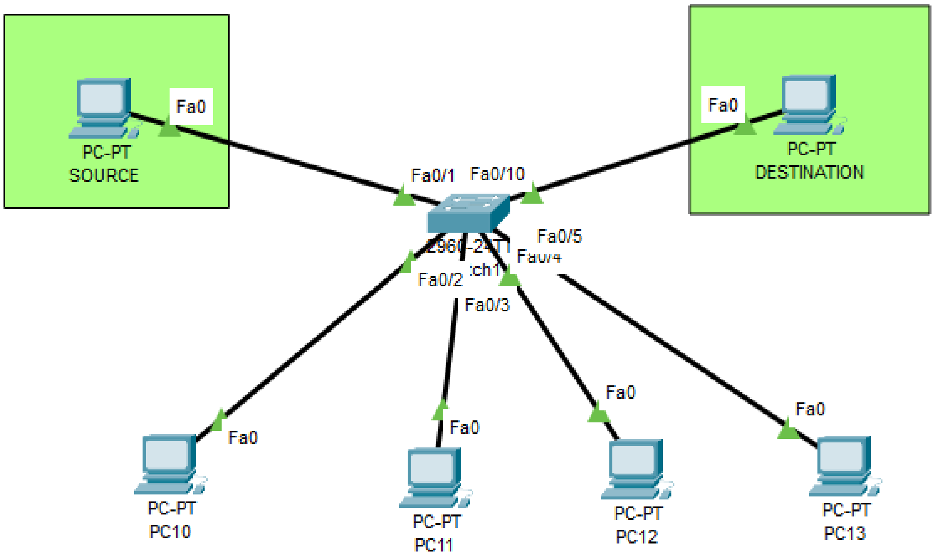
6. SPAN VLAN (RSPAN VLAN)

Definition:

SPAN is a **port mirroring feature** on a switch that copies network traffic from one or multiple **source interfaces (or VLANs)** to a **destination interface** for monitoring.
It's often used with **Wireshark, intrusion detection systems (IDS), or network analyzers** for troubleshooting or security analysis.



```
Switch(config)#
Switch(config)#monitor session 1 source interface fa0/1
Switch(config)#monitor session 1 destination interface fa0/10
Switch(config)#
```



Key Points:

- **Source Port (Fa0/1 in the image):** The interface whose traffic you want to monitor.
- **Destination Port (Fa0/10 in the image):** The interface connected to a monitoring device (e.g., a laptop running Wireshark).
- **SPAN VLANs:** Used to extend monitoring capabilities across multiple switches (RSPAN).

- **Traffic Direction:** You can monitor **inbound**, **outbound**, or **both directions** on a port.

Use Cases:

1. **Network Troubleshooting:**
   - Analyze slow network traffic or packet drops by capturing the data directly.
2. **Security Monitoring:**
   - IDS/IPS tools monitor suspicious traffic by receiving a copy from a SPAN port.
3. **Performance Analysis:**
   - Helps IT teams review live traffic patterns, bandwidth usage, or detect anomalies.

How SPAN Works (Based on Image):

- **PC Source (Fa0/1):** This PC's traffic is mirrored.
- **PC Destination (Fa0/10):** This PC captures mirrored traffic using packet capture tools like **Wireshark**.
- Other PCs (PC10, PC11, PC12, PC13) are unaffected by SPAN but continue normal communication.

Step-by-Step SPAN Configuration

1. Enter Global Configuration Mode

```
Switch> enable
Switch# configure terminal
```

2. Define the SPAN Session and Source Port

```
Switch(config)# monitor session 1 source interface fa0/1
```

- This tells the switch to monitor all traffic **inbound and outbound** on Fa0/1.

Optional Direction Control:

- Only incoming: monitor session 1 source interface fa0/1 rx
- Only outgoing: monitor session 1 source interface fa0/1 tx

3. Define the Destination Port

```
Switch(config)# monitor session 1 destination interface fa0/10
```

- This port should be connected to your **analysis PC** (running Wireshark).

4. Save the Configuration (Optional)

```
Switch(config)# end
Switch# write memory
```

How to Verify SPAN

Use the following command:

```
Switch# show monitor
```

It will display the active SPAN session with details about the **source and destination ports.**

Real-World Scenario Example:

- **IT Security Team:** Sets up SPAN to monitor all traffic from the finance VLAN to look for suspicious packets.
- **Network Engineer:** Uses Wireshark on the destination port to capture all packets sent/received by a server under troubleshooting.

Key Considerations for SPAN:

- The **destination port cannot forward traffic** while SPAN is active; it is dedicated to capturing traffic.
- Excessive SPAN sessions on a busy switch may cause **performance degradation** because of the additional load.
- Use **RSPAN** (Remote SPAN) if you need to monitor traffic across multiple switches, by creating a special VLAN dedicated for mirrored traffic.

7. Private VLAN (PVLAN)

Definition:

A **Private VLAN** allows devices in the same VLAN to be **isolated from each other** but still connect to a **shared gateway.**

Key Points:

- Consists of:
  - **Primary VLAN** (main VLAN).
  - **Secondary VLANs:**
    - **Isolated VLANs:** Devices cannot talk to each other.
    - **Community VLANs:** Devices can talk to each other but not to other groups.

Use Case:

- **Data centers or hosting providers** where multiple clients share the same network but must remain **isolated for security.**

Real-World Example:

In a hosting environment, each customer VM is isolated but can reach the router/firewall for internet access.

VLAN Types Summary Table

VLAN Type	Purpose	Example Scenario
Data VLAN	User traffic	HR/Finance traffic segregation
Voice VLAN	Prioritized voice traffic	Call centers, VoIP phones
Default VLAN	Factory default VLAN 1	Switch initialization
Native VLAN	Untagged traffic on trunk	Non-802.1Q devices
Management VLAN	Device management	SSH/Telnet/SNMP for switches
SPAN/RSPAN	Traffic monitoring	Wireshark analysis
Private VLAN	Device isolation	Data centers, hosting

Why VLAN Types Matter

- Each VLAN type solves a **specific problem**: security, performance, management, or monitoring.
- Without proper VLAN planning, **networks become flat**, vulnerable, and inefficient.