



Chapter 8 - Implementing Ethernet Virtual LANs (VLANs)



1. Virtual LAN (VLAN) Concepts

A VLAN (Virtual Local Area Network) divides a single physical network (switch) into multiple logical networks.



Key idea:

Without VLANs → all devices are in one broadcast domain.

With VLANs → each VLAN is its own broadcast domain.

Example:

If a switch has 3 VLANs:

- VLAN 10: Sales

- VLAN 20: HR

- VLAN 30: IT

Each group's traffic stays separated – even though they use the same switch.



Benefits of VLANs:

- Improves security (departments are isolated)

- Reduces broadcast traffic
 - Makes network management easier
 - Allows logical grouping of users (not based on physical location)
-

2. Creating Multiswitch VLANs Using Trunking

VLAN Tagging Concepts

When VLANs extend across multiple switches, we need a way to identify which VLAN a frame belongs to.

That's where VLAN tagging comes in.

A trunk link carries traffic from multiple VLANs between switches.

- Each Ethernet frame is tagged with its VLAN ID (called 802.1Q tag).
- Switches read the tag to know which VLAN the frame belongs to.
- Normal access ports (for PCs) carry only one VLAN and no tags.

802.1Q and ISL VLAN Trunking Protocols

There are two main trunking protocols:

1. IEEE 802.1Q (modern and standard)

- Adds a 4-byte VLAN tag into the Ethernet frame.
- Has a native VLAN (frames sent without tags).

2. ISL (Cisco proprietary, old)

- Encapsulates the entire frame (rarely used now).

 Today, CCNA focuses only on 802.1Q.

 3. Forwarding Data Between VLANs

The Need for Routing Between VLANs

- Devices in the same VLAN can communicate directly (Layer 2).
- Devices in different VLANs cannot communicate unless there is routing (Layer 3).

That's because each VLAN is its own subnet.

Routing Packets Between VLANs with a Router

Two main methods:

1. Router-on-a-Stick

- *One physical router interface.*
- *Subinterfaces (one per VLAN) with different IP addresses.*
- *Connected to the switch via a trunk link.*
- *Example:*

■ *VLAN 10 → 192.168.10.1/24*

■ *VLAN 20 → 192.168.20.1/24*

2. Layer 3 Switch (Multilayer Switch)

- *Performs routing internally (faster).*
 - *Uses SVIs (Switch Virtual Interfaces) for each VLAN.*
-

4. VLAN and VLAN Trunking Configuration and Verification

Creating VLANs and Assigning Access VLANs to an Interface

To create and assign VLANs on a Cisco switch:

```
Switch# configure terminal
```

```
Switch(config)# vlan 10
```

```
Switch(config-vlan)# name Sales
```

```
Switch(config)# interface fastEthernet 0/1
```

```
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport access vlan 10
```

VLAN Configuration Example 1: Full VLAN Configuration

Includes:

- Creating VLANs
- Naming VLANs
- Assigning ports
- Verifying with `show vlan brief`

VLAN Configuration Example 2: Shorter VLAN Configuration

- Quick creation and port assignment
(Less detailed but faster setup)

VLAN Trunking Protocol (VTP)

- Cisco protocol that helps distribute VLAN info to all switches automatically.
- Works in three modes:
 1. Server - can create/delete VLANs (shares info)
 2. Client - receives VLAN info from server
 3. Transparent - does not share VLANs, keeps local only
- VTP domain name must match between switches.

VLAN Trunking Configuration

```
Switch(config)# interface g0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)# switchport trunk native vlan 99
```

Verify:

show interfaces trunk

show vlan brief



5. Implementing Interfaces Connected to Phones

Data and Voice VLAN Concepts

Cisco IP phones have two VLANs:

- Voice VLAN: for phone traffic (VoIP)
- Data VLAN: for the PC connected through the phone

Each phone port on a switch carries both VLANs using 802.1Q tags.

Data and Voice VLAN Configuration and Verification

Example:

```
Switch(config)# interface fa0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport voice vlan 20
```

-  The switch tags voice traffic (VLAN 20) and leaves data traffic (VLAN 10) untagged.

Summary: IP Telephony Ports on Switches

- One port = two VLANs (data + voice)
 - Better performance and quality for VoIP
 - Must configure both VLANs correctly
-

6. Troubleshooting VLANs and VLAN Trunks

Common issues and how to fix them:

Confirm the Correct Access VLAN Is Assigned

Check:

`show interfaces switchport`

Make sure the port has the correct VLAN number.

Access VLANs Undefined or Disabled

If a VLAN doesn't exist → traffic won't pass.

Create it with `vlan <id>`.

Mismatched Trunking Operational States

If one side is trunk and the other is access → link won't carry multiple VLANs.

Check with `show interfaces trunk`.

The Supported VLAN List on Trunks

Make sure both switches allow the same VLANs on the trunk:

`switchport trunk allowed vlan 10,20,30`

Mismatched Native VLAN on a Trunk

If the native VLAN (untagged traffic) doesn't match → you'll see errors.

Make sure both sides have the same:

`switchport trunk native vlan 99`



Final Summary (Easy to Remember)

Topic	Key Points
VLANs	Separate broadcast domains on a single switch
Trunking (802.1Q)	Carries multiple VLANs between switches
Routing Between VLANs	Needed for inter-VLAN communication
VTP	Shares VLAN info between Cisco switches
Voice VLANs	Separate VLAN for VoIP phones
Troubleshooting	Check VLAN assignments, trunk status, and native VLANs