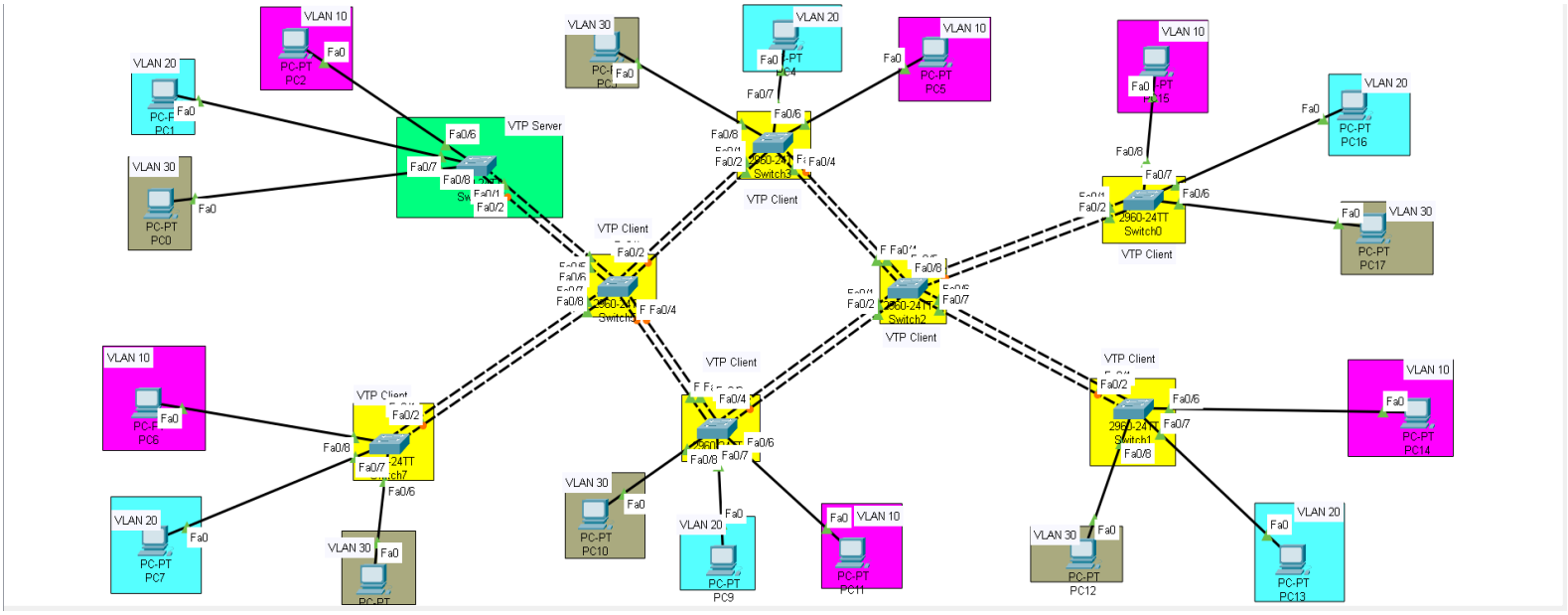
Switching Concepts



VLAN and EtherChannel Configuration Summary

In this topology, we created **three VLANs (10, 20, and 30)** from the **VTP server**.
Each link between the switches is configured as a **Port-Channel using EtherChannel**, which enhances bandwidth and redundancy between switches.

Every PC is assigned to its corresponding VLAN:

- **VLAN 10** → Assigned to PC1
- **VLAN 20** → Assigned to PC2
- **VLAN 30** → Assigned to PC3

With this setup, **devices can only communicate within the same VLAN** because there is **no Inter-VLAN routing** configured in this topology.
(Unlike other topologies where a Layer 3 device, such as a router or L3 switch, handles VLAN-to-VLAN communication.)

I recommend you understand the requirements and implement it on your own wish you the best 😊

Base Switch Configuration

The following configuration is applied to **all switches** in the topology to ensure consistent basic settings and secure remote access.

Configuration Steps

Switch> enable

Switch# configure terminal

Switch(config)# hostname <Name>

Switch(config)# no ip domain-lookup

Switch(config)# enable secret Admin123

! Configure console access

Switch(config)# line console 0

Switch(config-line)# password admin123

Switch(config-line)# login

Switch(config-line)# logging synchronous

Switch(config-line)# exec-timeout 2

Switch(config-line)# exit

! Configure VTY (Telnet/SSH) access

Switch(config)# line vty 0 15

Switch(config-line)# password admin123

Switch(config-line)# login

Switch(config-line)# logging synchronous

Switch(config-line)# exec-timeout 2

Switch(config-line)# exit

! Encrypt all plain-text passwords

Switch(config)# service password-encryption

! Save the configuration

Switch(config)# end

Switch# write memory

Configuration Notes

- no ip domain-lookup prevents the switch from trying to resolve mistyped commands as hostnames.
- logging synchronous ensures log messages don't interrupt command input.
- exec-timeout 2 automatically logs out inactive sessions after **2 minutes** for security.
- service password-encryption encrypts all passwords stored in the running configuration.

What Is EtherChannel?

EtherChannel is a Cisco technology that allows you to **bundle multiple physical Ethernet links** into one **logical link** (called a **Port-Channel**).
All the member interfaces act as a single interface from both the switch and device perspective.

It provides:

- **Higher bandwidth** (sum of all member links)
- **Redundancy** (if one link fails, traffic continues through the others)
- **Load balancing** (traffic is distributed across links based on a hashing algorithm)

Example Concept

If you connect **Switch A** and **Switch B** with 4 × 1 Gbps links:

- Without EtherChannel → Spanning Tree (STP) would **block 3 links**, using only 1.
- With EtherChannel → The 4 links **act as one 4 Gbps logical link**, and **STP sees it as one port** (so no blocking).

Why It Exists

EtherChannel was designed to **overcome STP limitations** — before EtherChannel, adding redundant physical links caused loops and blocking by STP.

Now:

- STP sees the **Port-Channel** as **one interface**.
- Inside that Port-Channel, **EtherChannel balances the traffic** and **recovers from failures**.

EtherChannel Modes

- You can form an EtherChannel in **three ways:**

Mode	Protocol	Description
PAgP	Cisco proprietary	Port Aggregation Protocol — negotiates EtherChannel between Cisco devices
LACP	IEEE 802.3ad standard	Link Aggregation Control Protocol — works between multi-vendor devices
Static (On)	None	Manually groups ports; no negotiation

Mode Combinations

Side A	Side B	Result
On	on	Channel forms (static)
desirable	auto	Channel forms (PAgP)
Active	passive	Channel forms (LACP)
Auto	auto	No channel
passive	passive	No channel

We need to configure the EtherChannel first so when we make the trunk interfaces for VTP we already made our port Channel

Common EtherChannel Rules

1. All member interfaces **must have identical configuration**:
    - Speed and duplex

    - VLAN membership
    - Trunk/access mode
    - Native VLAN
2. Mismatched settings cause the channel to **fail** or **suspend**.
3. EtherChannel can work in:
    - **Layer 2** mode → for VLANs and trunking
    - **Layer 3** mode → for routed ports (no switchport)

EtherChannel and STP

- STP runs **once per Port-Channel**, not per link.
- If one physical link fails, STP **doesn't need to recalculate** — the Port-Channel stays up.

Troubleshooting Tips

show etherchannel summary

show interfaces port-channel1

show lacp neighbor

show pagp neighbor

Common issues:

- Speed/duplex mismatch
- VLAN mismatch
- Wrong mode combinations
- Misconfigured trunk/access settings
- Mixing different interface types (e.g., Gigabit and FastEthernet)

EtherChannel Configuration

Step 1: Identify Interfaces for the Port-Channel

Before configuring EtherChannel, determine which interfaces on each switch will participate in the **Port-Channel**.
For example:

- On **Switch 1**, use interfaces **GigabitEthernet0/1** and **GigabitEthernet0/2**
- On **Switch 2**, use interfaces **GigabitEthernet0/1** and **GigabitEthernet0/2**

These interfaces will be bundled together to form a single logical link — the **Port-Channel**.

LACP Configuration (IEEE 802.3ad)

LACP is an **open standard protocol** used to automatically bundle multiple physical links into a single logical link for redundancy and load balancing.

Active Side Configuration

Switch# enable

Switch# configure terminal

Switch(config)# interface range fastEthernet0/1 - 2

Switch(config-if-range)# channel-group 1 mode active

Switch(config-if-range)# exit

Switch(config)# interface port-channel1

Switch(config-if)# switchport mode trunk

Switch(config-if)# exit

Switch# write memory

Passive Side Configuration

Switch# enable

Switch# configure terminal

Switch(config)# interface range fastEthernet0/1 - 2

Switch(config-if-range)# channel-group 1 mode passive

Switch(config-if-range)# exit

Switch(config)# interface port-channel1

Switch(config-if)# switchport mode trunk

Switch(config-if)# exit

Switch# write memory

PAgP Configuration (Cisco Proprietary)

PAgP is Cisco's proprietary protocol for aggregating links into an EtherChannel.
It automatically negotiates bundling between switches when both sides support it.

First Side (Auto Mode)

Switch# enable

Switch# configure terminal

Switch(config)# interface range fastEthernet0/1 - 2

Switch(config-if-range)# channel-group 2 mode auto

Switch(config-if-range)# exit

Switch(config)# interface port-channel2

Switch(config-if)# switchport mode trunk

Switch(config-if)# exit

Switch# write memory

- **Second Side (Desirable Mode)**

Switch# enable

Switch# configure terminal

Switch(config)# interface range fastEthernet0/1 - 2

Switch(config-if-range)# channel-group 2 mode desirable

Switch(config-if-range)# exit

Switch(config)# interface port-channel2

Switch(config-if)# switchport mode trunk

Switch(config-if)# exit

Switch# write memory

Verification

After configuration, verify the EtherChannel status with the following command:

Switch# show etherchannel summary

Configure VTP:

Determine the VTP Server

What Is VTP (VLAN Trunking Protocol)?

VTP (VLAN Trunking Protocol) is a **Cisco proprietary Layer 2 protocol** that helps manage **VLAN information consistently across multiple switches** in the same domain.

It allows you to:

- Create, delete, or rename VLANs **once** on a central switch (the **VTP Server**).
- Automatically propagate these VLAN changes to all other switches in the same **VTP domain**.

Purpose of VTP

Without VTP:

- You'd have to **manually create VLANs on every switch** in your network.
- That means lots of work and a higher chance of configuration errors.

With VTP:

- VLANs are **centrally managed** and automatically synchronized across trunk links.

How It Works

VTP messages are sent over **trunk links** using **Layer 2 multicast frames**.

Each VTP message includes:

- **VTP domain name** (must match across switches)
- **Configuration revision number**
- **List of VLANs**
- **VTP version**

Switches compare the **revision number** to decide which VLAN database is newer:

- If a switch receives an update with a **higher revision number**, it overwrites its local VLAN database with the new one.

VTP Modes

Mode	Description	Can Create VLANs?	Can Advertise VLANs?	Saves VLANs to NVRAM?
Server	Central VLAN database; sends updates to others.	Yes	Yes	Yes
Client	Receives VLANs from server; cannot create or delete.	No	Yes (forward only)	No
Transparent	Doesn't participate in VTP, forwards messages but keeps its own VLANs.	Yes (local only)	Yes (forwards only)	Yes
Off (v3 only)	Ignores and doesn't forward VTP messages.	Yes	No	Yes

VTP Versions

Version	Description
VTPv1	Basic version, supports normal VLANs (1–1005) only.
VTPv2	Adds support for Token Ring VLANs, transparent mode improvements, and consistency checks.
VTPv3	Major upgrade — supports extended VLANs (1006–4094), MST, better authentication, and role-based security (primary server concept).

Basic Configuration Example

On the Server:

Switch(config)# vtp domain LAP-LOCAL

Switch(config)# vtp mode server

Switch(config)# vtp version 2

Switch(config)# vtp password MySecret123

On the Client:

Switch(config)# vtp domain LAP-LOCAL

Switch(config)# vtp mode client

Switch(config)# vtp password MySecret123

On the Transparent Switch:

Switch(config)# vtp mode transparent

VTP Revision Number

Each time you make a VLAN change on a **VTP Server**, it **increments the revision number by 1**.

When another switch receives a VTP update:

- If its revision number is **lower**, it updates its VLAN database.
- If it's **higher**, it **ignores** the update.

Dangerous Scenario (Common in Labs/Production):
If you connect a switch with a **higher revision number** but an **empty VLAN database**, it can **erase VLANs across the entire domain**.

Solution: Always reset the revision number before connecting a switch to production:

delete flash:vlan.dat

reload

VTP Pruning

VTP pruning reduces unnecessary VLAN traffic on trunk links.

Without pruning:

- Broadcast, multicast, and unknown unicast traffic for all VLANs go over all trunks.

With pruning:

- Switch only sends traffic for VLANs that have **active ports** on the downstream switch.

Enable it with:

vtp pruning

Common Issues:

- Connecting a lab switch with a **higher revision number** can **wipe VLANs**.
- In multi-vendor networks, VTP doesn't work (Cisco proprietary).

Best Practices:

1. Use **VTP Transparent mode** in most environments.

2. Manually configure VLANs (safer, especially in production)
3. Always set the **domain name and password**.
4. **Erase vlan.dat** before connecting any reused switch.
5. Use **VTPv3** if you must use VTP — safer and more controlled.

Verify VTP Status

Use the following command to check the current VTP mode, domain, and configuration revision number:

Switch# show vtp status

Key fields to note:

- **VTP Operating Mode:** Server / Client / Transparent
- **VTP Domain Name:** Must match across all switches
- **Configuration Revision:** Increases when VLAN changes occur
- **Number of Existing VLANs:** Confirms successful propagation

---

Create VLANs on the VTP Server

VLANs are always created on the **VTP Server**, which then distributes them to all switches operating as **VTP Clients** in the same domain.

Switch# configure terminal

Switch(config)# vlan 10

Switch(config-vlan)# name HR

Switch(config-vlan)# vlan 20

Switch(config-vlan)# name ICT

Switch(config-vlan)# vlan 30

Switch(config-vlan)# name Finance

Switch(config-vlan)# exit

Switch# write memory

Verify VLAN Database

To confirm that the VLANs were created successfully, use:

Switch# show vlan

Verify VLAN Propagation on Clients

When you open any **VTP Client switch** and execute:

Switch# show vlan

Assign Access Ports to VLANs

Use the following commands to assign interfaces to their appropriate VLANs:

Switch# configure terminal

Switch(config)# interface range fastEthernet0/1 - 5

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

Switch(config-if-range)# switchport access vlan <VLAN_ID>

Switch(config-if-range)# exit

Switch# write memory

Replace <VLAN_ID> with the VLAN number (e.g., 10, 20, or 30) based on which department or network segment each PC belongs to.

Configure IP Addresses on PCs

Assign an IP address to each PC that belongs to the same VLAN subnet.
For example:

VLAN	Network	Example PC IP	Description
10	192.168.10.0/24	192.168.10.10	HR Department
20	192.168.20.0/24	192.168.20.10	ICT Department
30	192.168.30.0/24	192.168.30.10	Finance Department

Verify VLAN Communication

- **Ping between PCs in the same VLAN → Success**
- **Ping between PCs in different VLANs → Fail**

This is expected because **Inter-VLAN routing is not configured** in this topology — only Layer 2 switching is in effect.

Restrict VLAN Traffic on Trunk

To **block a specific VLAN (e.g., VLAN 20)** from traversing a trunk link, use the following command:

Switch(config)# interface port-channel1

Switch(config-if)# switchport trunk allowed vlan except 20

Switch(config-if)# exit

Switch# write memory

This command allows **all VLANs except VLAN 20** to pass through the trunk link.

Important Concept: What VTP Actually Does

VTP only propagates VLAN information — not port configurations.

That means:

- VLAN 10 (and all other VLANs) will be **created automatically** on all switches in the same **VTP domain**.
- But **VTP will not configure access ports** like switchport access vlan 10.
  You still need to configure those **manually or with a script/template**.