Configuring and Verifying VLANs

VLAN - A **Virtual Local Area Network** is a logical subdivision of a switch that allows devices in different physical locations to be grouped into the same broadcast domain. This improves network segmentation, security, and efficiency.

Default VLAN - By default, all switch ports belong to **VLAN 1**. This VLAN cannot be deleted or disabled. It is used for management and control-plane traffic unless otherwise configured.

- **Cannot be turned off**

Standard VLAN Range - VLANs **1–1005**

Where are VLANs stored by default using VTP?

- Stored in the **vlan.dat** file under flash (default)
- Known as **Server/Client Mode**
- VLAN numbers can go above 1005 with newer versions of VTP (e.g., VTPv3)

Where are VLANs stored when using Transparent Mode?

- VLAN information is stored in the **running configuration**
- VLAN numbers can go above 1005 in this mode

Switchport (Enable) - The **switchport command** is used to configure a switch port as either an **access port** (assigned to a single VLAN) or a **trunk port** (carrying multiple VLANs). By default, most switch ports operate in Layer 2 mode with switchport enabled.

Voice Requirements

- Bandwidth per call depends on codec, sampling rate, and Layer 2 media:
  - **Jitter** less than 30 ms
  - **Delay** less than 150 ms
  - **Packet loss** less than 1%
  - Voice traffic is marked with an **802.1p CoS (Class of Service) value of 5**

802.1q - An IEEE standard that defines how VLAN tags are inserted into Ethernet frames. It adds a **4-byte VLAN tag** between the source MAC and EtherType/length fields, allowing multiple VLANs to be carried over a single trunk link.

- **802.1p** - A standard for **Layer 2 QoS marking** (Class of Service) that prioritizes traffic by assigning values (0–7) in the VLAN tag header. Value **5** is typically reserved for voice traffic to ensure low latency and jitter.

Commands to Remember

```
switchport access vlan 20 – Ensure you never become a trunk port. This is used on an endpoint device where it will never become a trunk.
switchport voice vlan 200
```

- VLAN numbers above are examples only, shown for command structure.

Configuring and Verifying Trunks

Trunk - A switch port configured to carry traffic for multiple VLANs simultaneously. Each frame is tagged (using **802.1q**) so that devices know which VLAN the traffic belongs to.

- A trunk can be formed:
  - From a switch to a switch
  - From a switch to a router (router-on-a-stick)
  - From a virtualization host/PC NIC to a switch (when supporting VLAN tagging)

When data is sent to the default gateway across a trunk port, it must be tagged. This is done using the **802.1q standard**, which adds a **4-byte VLAN tag** to the Ethernet frame.

- Tag consists of:
  - Tag Protocol Identifier (TPID)

- User Priority (802.1p, CoS)
- Canonical Format Indicator (CFI)
- VLAN ID (VID)

ISL (Inter-Switch Link) - A Cisco-proprietary VLAN tagging protocol, now **deprecated**. Do not use ISL in modern networks; always use **802.1q**.

Dynamic Trunking Protocol (DTP) - A Cisco-proprietary protocol that negotiates trunking automatically between two switch ports.

- DTP can dynamically form trunks based on port configuration.
- Default behavior varies by switch model and IOS version.
- **Best practice:** Disable DTP and manually configure trunk links.
  - Use the interface command:

`switchport nonegotiate – This would be used to turn of DTP on a trunk`

	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

If one side of a trunk is configured for **ISL** and the other side is configured for **802.1q**, this is considered an **encapsulation mismatch**.

- Result: The trunk will fail, and VLAN traffic will not pass between the switches.
- **Best Practice:** Always use **802.1q**, as ISL is Cisco-proprietary and deprecated.

	Dynamic Auto	Dynamic Desirable	Trunk	Trunk Nonegotiate	Access
Dynamic Auto	Access	Trunk	Trunk	Limited Connectivity	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Limited Connectivity	Access
Trunk	Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Trunk Nonegotiate	Limited Connectivity	Limited Connectivity	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Limited Connectivity	Acc

Filtering VLANs

Allow only specific VLANs to communicate across a trunk.

```
switchport trunk allowed vlan 10,20,200
```

- Retyping the command with a different VLAN number will **overwrite** the list.
- Use the **add** keyword to include more VLANs without overwriting:

```
switchport trunk allowed vlan add 60
```

- Use `/?` for command options.

PVID (Port VLAN ID)

- **PVID** is the VLAN ID assigned to untagged frames arriving on a trunk port.
- In Cisco terminology, this corresponds to the **Native VLAN**.

- All untagged frames received on a trunk are associated with the VLAN specified as the PVID.

Native VLAN

- Native VLAN frames are carried over the trunk **untagged**.
- The default Native VLAN is **VLAN 1**.
- Native VLAN must match on both ends of the trunk.
    - A mismatch may cause traffic from different VLANs to merge, leading to security issues.

Best Practice: Change the Native VLAN to an unused VLAN ID to reduce risk.

VLAN Trunking Protocol (VTP)

- **VTP** is a Cisco-proprietary protocol used to manage VLAN configurations across multiple switches.
- VLANs are created on a **VTP server**, and changes are advertised to **VTP clients** in the same VTP domain.
    - **Default Settings:**
        - Mode: **Server**
        - Version: **1**
        - Domain: **Null** (not set)
- VTP helps maintain consistency of VLAN information, but can also cause issues if misconfigured (e.g., accidentally deleting VLANs).

VTP Modes:

- **Server** – Can create, modify, and delete VLANs; propagates updates.
- **Client** – Cannot create or delete VLANs; receives updates from the server.
- **Transparent** – VLANs are stored locally and not advertised; still forwards VTP messages.
- **Off (VTPv3 only)** – Disables VTP entirely.

Configuration Revision

- A **Configuration Revision Number** is an integer that increments each time a VLAN database change is made on a VTP server.
- Switches in the same VTP domain compare their revision numbers:
    - The switch with the **higher revision number** propagates its VLAN database to others.
- **Risk:** A rogue device with a higher revision number could overwrite the production VLAN database.

VTP Versions

- **VTPv1** – Original version; supports normal VLANs (1–1005).
- **VTPv2** – Adds support for Token Ring VLANs and consistency checks; backward-compatible with v1.
- **VTPv3** – Supports extended VLAN range (1–4094), introduces authentication enhancements, adds support for MST (Multiple Spanning Tree), and allows a **Primary Server** concept.

Primary vs Secondary Server (VTPv3):

- **Primary Server** – The only device that can make VLAN database changes.
- **Secondary Servers** – Forward VLAN information but cannot change it.
- Prevents accidental overwrites.

VTP Pruning

- **VTP Pruning** reduces unnecessary VLAN traffic on trunk links by restricting broadcast, multicast, and unknown unicast traffic to only the switches that have active ports in that VLAN.

- Available only in **Client** and **Server** modes.

Inter-VLAN Routing

- Each VLAN has a unique IP subnet.
- A **Layer 3 device** (router or multilayer switch) is required to forward traffic between VLANs.

Subinterfaces

- A **Subinterface** is a logical interface on a router's physical interface that allows routing for multiple VLANs using **802.1q encapsulation**.
- Commonly used with **Router-on-a-Stick**.

Example Configuration:

```
interface g0/0
 no shutdown

interface g0/0.10
 encapsulation dot1Q 10 native
 ip address 192.168.10.1 255.255.255.0

interface g0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
```

SVI (Switch Virtual Interface)

- An **SVI** is a virtual Layer 3 interface on a switch, representing a VLAN.
- Used for inter-VLAN routing on multilayer switches or for switch management.

Example Configuration:

```
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
 no shutdown

interface vlan 99
```

```
 ip address 192.168.99.1 255.255.255.0
 no shutdown

! Change Native VLAN on trunk
interface g0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 99

ip routing
```

Routed Ports

- A **Routed Port** is a physical switch port configured to act like a router interface.
- It does not belong to a VLAN and operates purely at **Layer 3**.
- Useful for point-to-point connections between switches or between a switch and a router.

Command to Convert a Port to a Routed Port:

```
interface g0/1
 no switchport
 ip address 192.168.1.1 255.255.255.0
 no shutdown
```

First Hop Redundancy Protocol (FHRP)

- **Definition:** A set of protocols that provide **gateway redundancy** by allowing multiple routers or multilayer switches to work together to present a **single virtual default gateway** to hosts on a LAN.
- Purpose: Ensures that if the active router fails, another router automatically takes over without interrupting end-host connectivity.

Common FHRP Protocols:

- **HSRP (Hot Standby Router Protocol)** – Cisco proprietary.
    - Virtual MAC Format (HSRPv1): **0000.0C07.ACXX**
        - `0000.0C` – Cisco OUI
        - `07.AC` – HSRP identifier

        - XX – Group number (in hex, 0–255)
    - Virtual MAC Format (HSRPv2): **0000.0C9F.FXXX**
        - `0000.0C` – Cisco OUI
        - `9F.F` – HSRP v2 identifier
        - XXX – Group number (in hex, 0–4095)
- **VRRP (Virtual Router Redundancy Protocol)** – Open standard.
    - Virtual MAC Format: **0000.5E00.01XX**
        - `0000.5E` – IANA OUI
        - `00.01` – VRRP identifier
        - XX – VRID (Virtual Router ID, 1–255)
- **GLBP (Gateway Load Balancing Protocol)** – Cisco proprietary; adds load balancing features.
    - Virtual MAC Format: **0007.B400.XXYY**
        - `0007.B4` – Cisco OUI for GLBP
        - `00` – Reserved
        - XX – GLBP group number (1–1024)
        - YY – AVF (Active Virtual Forwarder) number (0–3)

How it Works:

- End devices are configured with the **virtual IP address** of the gateway.
- Routers in the FHRP group elect an **Active/Standby** (HSRP) or **Master/Backup** (VRRP) device.
- If the active router fails, a backup device quickly takes over using the same **virtual IP** (and associated virtual MAC).

Benefit: Provides **high availability** and prevents a single point of failure at the default gateway level.

GARP (Gratuitous ARP)

- **Definition:** A type of ARP message that a device sends for its **own IP address** rather than requesting another device's MAC.
- **Purpose:**
  - Updates the ARP tables of other devices with the sender's IP-to-MAC mapping.
  - Detects **IP address conflicts** (duplicate IPs on the network).
  - Used in **FHRP failover events** so that hosts update their ARP cache with the new active router's MAC address.
- **How it Works:**
  - A device broadcasts an ARP request or reply stating: *"Who has this IP? I do."*
  - This forces all devices on the subnet to refresh their ARP cache with the sender's MAC address.

Example Use Case:

- When an HSRP standby router becomes active, it sends a **GARP** to update all hosts so they associate the **virtual IP** with the new router's MAC address.