



VLANs & 802.1Q Trunking

Use this when: you split a switch into separate networks, carry them between switches on a trunk, or route between them.

🔧 The 802.1Q tag: 4 bytes added on a trunk

IEEE 802.1Q

Dest MAC 6 bytes	Source MAC 6 bytes	TPID 0x8100 16 bits: "tagged"	PCP 3: priority	DEI 1	VLAN ID 12 bits: 1 to 4094	Type 2	Payload data	FCS 4
----------------------------	------------------------------	---	------------------------------	-----------------	--------------------------------------	------------------	------------------------	-----------------

Access port: one VLAN, no tag **Trunk:** many VLANs, each tagged **Native VLAN:** the one sent untagged (default 1)

📋 VLAN numbers

1	Default; can't delete. Don't use for users.
2 to 1001	Normal range, your VLANs
1002 to 1005	Reserved (Token Ring, FDDI)
1006 to 4094	Extended range

🔧 Does a trunk form? (DTP)

Default: dynamic auto

	AUTO	DESIRABLE	TRUNK	ACCESS
auto	No	Yes	Yes	No
desirable	Yes	Yes	Yes	No
trunk	Yes	Yes	Yes	Mismatch

🔧 Configure

Access port · trunk port

```
vlan 10
 name SALES
interface g0/1
 switchport mode access
 switchport access vlan 10
 switchport voice vlan 150 ! IP phone
```

```
interface g0/24
 switchport mode trunk
 switchport nonegotiate ! no DTP
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150
 switchport trunk allowed vlan add 30
```

🔧 Route between VLANs

```
! router on a stick
interface g0/0.10
 encapsulation dot1q 10
 ip address 192.0.2.1 255.255.255.192
```

```
! layer 3 switch (SVI)
ip routing
interface vlan 10
 ip address 192.0.2.1 255.255.255.192
 no shutdown
```

show vlan brief	VLANs and access ports
show interfaces trunk	Trunks, native, allowed
show interfaces g0/1 switchport	Mode of one port

🔧 Stop VLAN hopping

⚠️ **DANGER** Ports left in dynamic mode let an attacker negotiate a trunk. Set **access** or **trunk** plus **nonegotiate**.

⚠️ **CAUTION** Use an unused native VLAN (999) and the same one on both ends.

⚠️ **CAUTION** **allowed vlan 30** replaces the list. Use **add**.

🔧 Trunk down? Check

Native VLAN	Same on both ends? CDP logs a mismatch
Allowed list	Is the VLAN on both trunks?
VLAN exists	Created on the far switch too?



● One VLAN = one subnet

● **auto + auto** = no trunk

● Shut unused ports, park them in an unused VLAN