# VLANs Cheat Sheet — Reference Tables



## VLANs — General

| |
|---|
| Logical segmentation of a physical network |
| IEEE 802.1Q — industry standard tagging |
| Cisco ISL — legacy, Cisco proprietary (deprecated) |
| VLANs operate at Layer 2 (Data Link) |
| Each VLAN = separate broadcast domain |
| Inter-VLAN routing requires Layer 3 device |
| VLANs stored in flash: vlan.dat file |
| Max VLANs: 4094 (12-bit VID field) |
| VLAN 0 and 4095 reserved — cannot be used |
| Supported on switches and routers (subinterfaces) |

## VLAN Ranges

| | |
|---|---|
| **VLAN 1** | Default VLAN — all ports assigned; cannot delete |
| **VLAN 2-1001** | Normal range — stored in vlan.dat |
| **1002-1005** | Reserved (FDDI/Token Ring) — cannot delete |
| **1006-1024** | Extended — some IOS versions only |
| **1025-4094** | Extended range — requires VTP transparent/off |
| **VLAN 4095** | Reserved — cannot be used |

## VLAN Types

| | |
|---|---|
| **Default** | VLAN 1 — factory default for all ports |
| **Data** | Carries user-generated traffic |
| **Voice** | Dedicated VLAN for VoIP QoS |
| **Management** | In-band switch management access |
| **Native** | Untagged on 802.1Q trunk (default VLAN 1) |
| **Private** | PVLAN — isolated / community / promiscuous |

## Port / Interface Types

| | |
|---|---|
| **Access** | Carries one VLAN — untagged — end devices |
| **Trunk** | Carries multiple VLANs — tagged (802.1Q) |
| **Voice** | Access + voice VLAN on same port (Cisco) |
| **Routed** | L3 port — no VLAN — used with SVIs |
| **Tunnel** | QinQ — 802.1ad — double tagging |

## 802.1Q Tag Structure

| | |
|---|---|
| **TPID** | 0x8100 — identifies 802.1Q frame |
| **PCP** | 3 bits — Priority Code Point (CoS/QoS) |
| **DEI** | 1 bit — Drop Eligible Indicator |
| **VID** | 12 bits — VLAN ID (0-4095) |
| **Frame size** | Max 1522 bytes (standard 1518 + 4B tag) |
| **Native VLAN** | NOT tagged on trunk — must match both ends |

## DTP Switchport Modes

| | |
|---|---|
| **auto** | Become trunk if neighbour is desirable/trunk |
| **desirable** | Actively negotiate trunk — sends DTP frames |
| **trunk** | Unconditionally trunk — sends DTP frames |
| **access** | Unconditionally access — no DTP |
| **nonegotiate** | No DTP frames — use with static trunk/access |

## VTP Modes & Key Fields

| | |
|---|---|
| **Server** | Creates/modifies/deletes VLANs — default mode |
| **Client** | Receives VTP updates — cannot modify VLANs |
| **Transparent** | Forwards VTP but uses own vlan.dat |
| **Off** | Does not participate in VTP at all |
| **Domain** | Must match for VTP to synchronise |
| **Revision** | Higher revision wins — DANGER: reset before add |
| **Pruning** | Removes unused VLANs from trunks |

## Inter-VLAN Routing

| | |
|---|---|
| **Router-on-a-Stick** | One physical link — subinterfaces per VLAN |
| **Subinterface** | int Gi0/0.10 — encapsulation dot1q 10 |
| **SVI** | Switch Virtual Interface — L3 switch |
| **SVI syntax** | interface vlan 10 |
| **L3 switch** | ip routing + SVI per VLAN |
| **Native VLAN** | encapsulation dot1q 10 native |

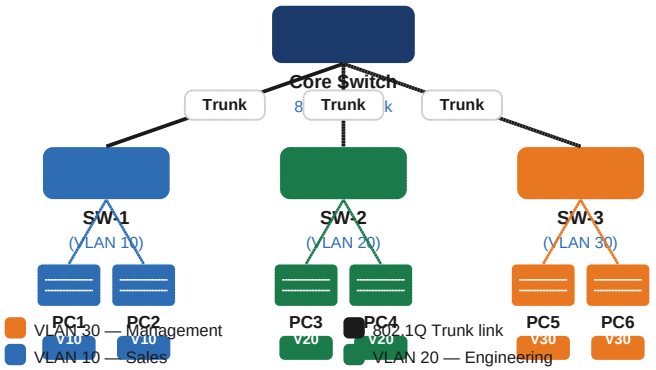
## Key Cisco IOS Commands

```
vlan <id>
  name <name>
interface <intf>
  switchport mode access
  switchport access vlan <id>
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk native vlan <id>
  switchport trunk allowed vlan <list>
  switchport trunk allowed vlan add <id>
  switchport nonegotiate
  switchport voice vlan <id>
vtp mode server | client | transparent | off
vtp domain <name>
vtp password <pass>
vtp pruning
show vlan brief
show interfaces trunk
show vtp status
show interfaces <intf> switchport
```

## VTP Revision Number Warning

Adding a VTP Server with higher revision number will overwrite ALL VLAN configs on the domain!
Always reset revision: change domain name or set to transparent first.

## VLAN Network Topology (Access & Trunk)

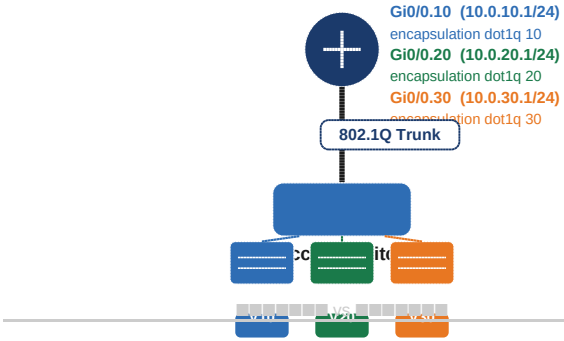



### Trunk Configuration Key Points

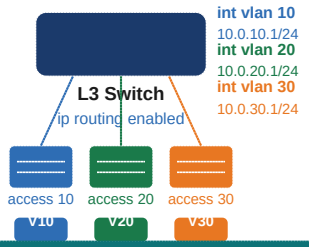
Native VLAN must match on BOTH ends — mismatch = CDP warning.
Use switchport nonegotiate to disable DTP on trunk ports.
Restrict trunk: switchport trunk allowed vlan 10,20,30.
Double-tagging attack: native VLAN != user VLAN (use VLAN 999).
Verify: show interfaces trunk shows allowed, active, forwarding.

## Inter-VLAN Routing (Router-on-a-Stick & L3 Switch)

### Method 1: Router-on-a-Stick (single physical link)




### Method 2: L3 Switch with SVIs (preferred in enterprise)




### Router-on-a-Stick vs L3 Switch SVI

ROAS: Simple, cheap — single link = bottleneck at scale.
SVI: Wire-speed routing in hardware — enterprise standard.
SVI needs ip routing globally + SVI per VLAN.
ROAS needs subinterface + encapsulation dot1q <vlan> .

## 802.1Q Frame & VLAN Tag Structure

**Standard Ethernet Frame (no VLAN tag — access port)**

| Dst MAC | Src MAC | EtherType | Payload | FCS |
|---|---|---|---|---|
| 6B | 6B | 2B | 46-1500B | 4B |

**802.1Q Tagged Ethernet Frame (trunk port — 4 bytes inserted)**

| Dst MAC | Src MAC | TPID | PCP | DEI | VID | EtherType | Payload | FCS |
|---|---|---|---|---|---|---|---|---|
| 6B | 6B | 0x8100 | 3b | 1b | 12b | 2B | 46-1500B | 4B |

**802.1Q Tag Field Detail (4 bytes total)**

| TPID | PCP | DEI | VID |
|---|---|---|---|
| Tag Protocol ID<br>0x8100 = 802.1Q<br>2 bytes | Priority Code Point<br>0-7 CoS/QoS marking<br>3 bits | Drop Eligible Indicator<br>1 bit | VLAN Identifier<br>0-4095 (12 bits)<br>4094 usable |

**QinQ Double Tagging (802.1ad — outer + inner tag)**

| Dst MAC | Src MAC | Outer TPID | Outer VID | Inner TPID | Inner VID | EtherType | Payload | FCS |
|---|---|---|---|---|---|---|---|---|
| 6B | 6B | 0x88A8 | S-Tag | 0x8100 | C-Tag | 2B | Var | 4B |

**VLAN ID Range Summary**

| | |
|---|---|
| 0 | Reserved — used internally by 802.1Q |
| 1 | Default VLAN — all ports assigned, no delete |
| 2-1001 | Normal range — VTP propagated, stored vlan.dat |
| 1002-1005 | Reserved legacy (FDDI/Token Ring) |
| 1006-4094 | Extended range — VTP off/transparent only |
| 4095 | Reserved — not usable |

### Native VLAN — Security Best Practice

Native VLAN is sent UNTAGGED on a trunk port.
Mismatch = traffic lands in wrong VLAN — security risk.
Best practice: set native VLAN to unused VLAN (e.g. 999).
Trunk: switchport trunk native vlan 999