

MAG212 CYBER

NETWORK ENGINEERING · SWITCHING MASTERCLASS · 2026

ULTIMATE CHEAT SHEET / CCNA · CCNP · IT ADMINISTRATORS

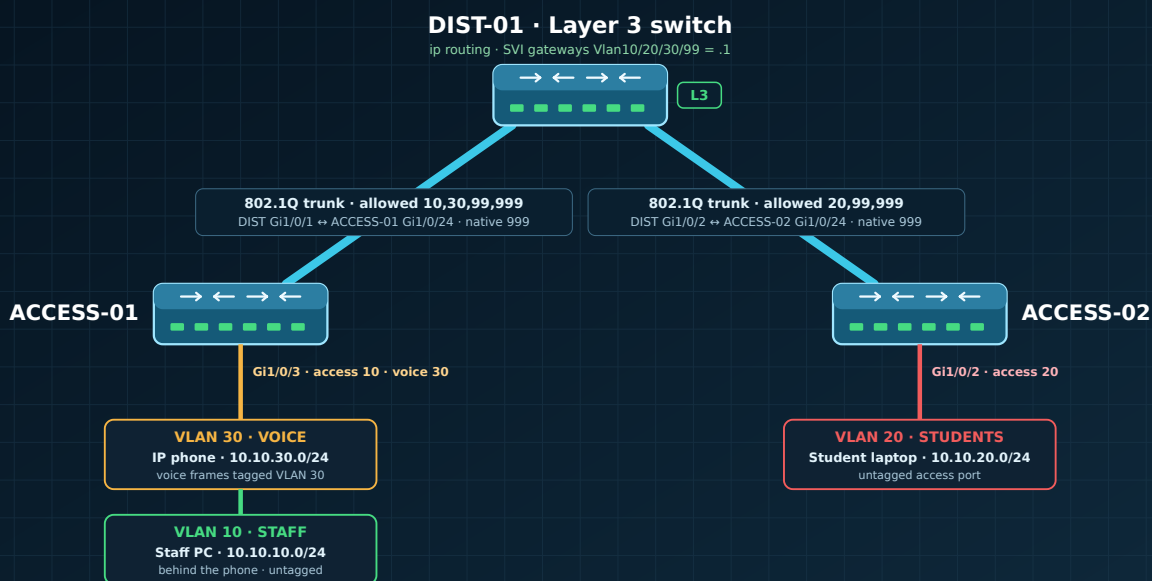
VLANs Ultimate Cheat Sheet

802.1Q Trunking · Access & Voice Ports · SVIs · Inter-VLAN Routing · VTP · Security · Troubleshooting

Published by MAG212 CYBER · Technical education edition

MAG212 CYBER · VLAN CAMPUS LAB

802.1Q trunks · access and voice ports · SVI gateways on a Layer 3 distribution switch · lab addressing



VLAN 99 · MANAGEMENT · 10.10.99.0/24

Management SVI on every switch, carried on both trunks · VLAN 999 = dedicated unused native VLAN on both trunks

Lab convention: All addresses below are original private lab values. The diagram matches the configurations below: trunk allowed lists, native VLAN 999, the voice port on ACCESS-01 Gi1/0/3 and the student port on ACCESS-02 Gi1/0/2. Interface numbering assumes Cisco Catalyst IOS XE hardware; adapt it to your switch model.

01 / VLAN essentials at a glance

Term	Meaning	Example
Access VLAN	Unmodified endpoint Ethernet frames belong to one data VLAN	Staff PC on VLAN 10
Voice VLAN	Phone traffic may be tagged on a host-facing port while PC traffic is untagged	PC VLAN 10 / voice VLAN 30
802.1Q trunk	Transports multiple VLANs over one physical link by using an 802.1Q tag	Access-to-distribution uplink
Native VLAN	Default untagged VLAN on an 802.1Q trunk, unless platform-wide native tagging is enabled	VLAN 999 dedicated unused
SVI	Switch virtual interface serving as Layer 3 gateway when routing is enabled	Vlan10 / 10.10.10.1
VTP	Cisco protocol that can propagate VLAN database changes	Use transparent/off where appropriate

02 / Original network design & addressing

VLAN	Name	Network	Gateway SVI	Example location
10	STAFF	10.10.10.0/24	10.10.10.1	ACCESS-01 Gi1/0/3 (PC behind the phone)
20	STUDENTS	10.10.20.0/24	10.10.20.1	ACCESS-02 Gi1/0/2
30	VOICE	10.10.30.0/24	10.10.30.1	ACCESS-01 Gi1/0/3
99	MANAGEMENT	10.10.99.0/24	10.10.99.1	Switch management SVIs
999	NATIVE-UNUSED	No user subnet	None	Native trunk VLAN

03 / Create the VLANs on the switches

```
configure terminal
vlan 10
  name STAFF
vlan 20
  name STUDENTS
vlan 30
  name VOICE
vlan 99
```

```
name MANAGEMENT
vlan 999
name NATIVE-UNUSED
end
show vlan brief
```

Why: The switches must recognize each VLAN locally. A trunk allow-list does not create the VLAN; it only controls which VLAN tags are permitted across that uplink.

04 / Access ports: one data VLAN

```
! ACCESS-02 – student laptop on Gi1/0/2
configure terminal
interface GigabitEthernet1/0/2
description STUDENT-LAPTOP
switchport mode access
switchport access vlan 20
spanning-tree portfast
spanning-tree bpduguard enable
no shutdown
end
show interfaces GigabitEthernet1/0/2 switchport
```

Expected result: An ordinary untagged host joins VLAN 20. PortFast is only for verified end-device interfaces; BPDU Guard can disable the port if switch BPDUs appear.

05 / Access port with separate voice VLAN

```
! ACCESS-01 – phone with PC behind it
configure terminal
interface GigabitEthernet1/0/3
description STAFF-PHONE-PLUS-PC
switchport mode access
switchport access vlan 10
switchport voice vlan 30
spanning-tree portfast
spanning-tree bpduguard enable
no shutdown
end
```

Data uses VLAN 10; a compatible IP phone tags voice frames for VLAN 30, commonly using LLDP-MED/CDP information. Supply DHCP scope/relay and QoS policies separately for real deployments.

06 / Manual 802.1Q trunk — both ends

ACCESS-01 / uplink Gi1/0/24

```
interface GigabitEthernet1/0/24
description TRUNK-T0-DIST-01
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 10,30,99,999
switchport nonegotiate
no shutdown
```

DIST-01 / downlink Gi1/0/1

```
interface GigabitEthernet1/0/1
description TRUNK-T0-ACCESS-01
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 10,30,99,999
switchport nonegotiate
no shutdown
```

Both ends of a trunk must match: the same native VLAN (999, a dedicated unused VLAN) and the same allowed list. Configure the second trunk, DIST-01 Gi1/0/2 to ACCESS-02 Gi1/0/24, the same way with 20,99,999 on both ends.

Modern fixed-802.1Q Catalyst platforms may not support `switchport trunk encapsulation dot1q`. Do not paste the old command unless your switch actually offers encapsulation selection.

07 / Layer 3 switch: SVI gateways and inter-VLAN routing

```
! DIST-01 (multilayer switch)
configure terminal
ip routing
interface Vlan10
description STAFF-GATEWAY
ip address 10.10.10.1 255.255.255.0
no shutdown
interface Vlan20
description STUDENT-GATEWAY
ip address 10.10.20.1 255.255.255.0
no shutdown
interface Vlan30
description VOICE-GATEWAY
ip address 10.10.30.1 255.255.255.0
no shutdown
interface Vlan99
description MANAGEMENT-GATEWAY
```

```

ip address 10.10.99.1 255.255.255.0
no shutdown
end
show ip interface brief | include Vlan
show ip route connected

```

SVI line protocol generally requires the VLAN to exist and have an active Layer 2 forwarding path (or qualifying autostate conditions). By default, a Layer 3 switch with `ip routing` can route between connected VLANs; use ACLs/firewall policy to restrict access.

08 / Restrict students from staff network

```

! Example only: deny Student-to-Staff, permit other IPv4
ip access-list extended STUDENT-IN
deny ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255
permit ip 10.10.20.0 0.0.0.255 any
interface Vlan20
ip access-group STUDENT-IN in
!
show ip access-lists STUDENT-IN

```

This is only an illustrative ACL—not a complete school segmentation policy. It allows other destinations (including management) unless additional explicit denies are added. In production, build and test a least-privilege matrix and account for IPv6 separately.

09 / VTP: decide before enabling

Mode	Behavior	Operational note
Server	Creates and advertises VLAN database updates	Misconfiguration can affect an entire VTP domain
Client	Receives VLAN database information from upstream	Manual local VLAN creation may be restricted
Transparent	Uses locally controlled VLAN configuration, while VTP message handling varies by version	Practical choice for independently managed switches
Off (where supported)	Disables VTP participation/forwarding	Check device support

```

! Example – configure independently managed VLANs
vtp mode transparent
show vtp status

```

VTP v3 offers different controls and safer revision handling than v1/v2; still confirm design and change control before using centralized VLAN propagation.

10 / Troubleshooting — what to run and why

Command	What it proves
<code>show vlan brief</code>	VLANs are present and access ports are assigned
<code>show interfaces trunk</code>	Trunk state, native VLAN, allowed/active/forwarding VLANs
<code>show interfaces Gi1/0/24 switchport</code>	Administrative versus operational trunk state
<code>show mac address-table dynamic vlan 20</code>	Source MAC learning within VLAN 20
<code>show spanning-tree vlan 20</code>	STP forwarding versus blocking on VLAN 20
<code>show ip interface brief</code>	SVI addresses and up/down status
<code>show ip route connected</code>	Connected VLAN routes on the Layer 3 switch
<code>show ip dhcp snooping</code>	Whether DHCP snooping is active and on which VLANs

Case A: VLAN 20 users on ACCESS-02 cannot reach their gateway

Check: the port is in VLAN 20, the VLAN exists on both switches, the trunk is forwarding VLAN 20, DIST-01 Vlan20 is up/up, and clients have correct subnet/mask/gateway. **Fix:** align both trunk allowed-lists and check STP, DHCP, and SVI state.

Case B: One access switch displays native VLAN mismatch

Check: `show interfaces trunk` on both ends. **Fix:** set the same dedicated native VLAN and align tagging expectations; investigate before suppressing warnings.

Case C: Same-VLAN works but different VLANs cannot talk

Check: `ip routing`, SVI operational status, default gateways, ACL directions, routing/firewall policies. **Fix:** correct gateway/SVI/policy, not trunk settings by default.

11 / VLAN security checklist

- Disable unused ports and park them in an unused VLAN; document exceptions.
- Set access ports explicitly and avoid dynamic trunk negotiation where not needed.
- Limit trunks to necessary VLANs; match both sides and use a dedicated native VLAN.

- Apply PortFast and BPDU Guard only to verified endpoint interfaces.
- Enable DHCP Snooping and Dynamic ARP Inspection where compatible; define trusted uplinks carefully.
- Use 802.1X or MAC authentication policies for user/device identity, with tested fallback handling.
- Protect management VLAN access with ACLs, AAA, SSH, and a dedicated administration path.
- Separate sensitive segments using ACLs or stateful firewalls; VLANs by themselves are not security boundaries.

12 / Practice questions & explained answers

Q1. A switch access port is in VLAN 20. Does it add 802.1Q tags to a normal PC's frames?

Answer: Normally no. Frames to/from a conventional host on an access port are untagged; the switch tracks VLAN association internally.

Q2. Why is a trunk allowed VLAN list not enough to create end-to-end connectivity?

Answer: The VLAN must exist and be active on the relevant switches, STP must permit forwarding, and a valid Layer 3 gateway/policy must exist where routing is required.

Q3. A PC can ping another device on VLAN 10 but not a device in VLAN 20. What changes?

Answer: Inter-VLAN connectivity requires a Layer 3 routing function (SVIs or router-on-a-stick), correct host gateways, and policies that permit the traffic.

Q4. How does a voice VLAN differ from a second trunk between switches?

Answer: It is a special host-facing arrangement allowing a capable phone to send tagged voice frames while the attached PC generally sends untagged data; it is not a general-purpose switch-to-switch trunk.

Q5. Which command quickly reveals a missing allowed VLAN?

Answer: `show interfaces trunk`. Compare both ends, the VLAN existence table, and the VLANs currently forwarding through STP.

Q6. Why should you avoid blindly enabling VTP server mode?

Answer: Central propagation of VLAN database updates can introduce unintended changes across multiple switches. Choose VTP architecture deliberately and verify version/domain/revision behavior.

13 / Sources & further reading

This is an original MAG212 CYBER guide. The three-switch campus lab, diagram, security checklist and troubleshooting cases were written independently and checked against current Cisco Catalyst documentation and the IEEE standard.

- [Cisco IOS XE — Configure VLAN Trunking](#)
- [RFC 3069 — VLAN Aggregation for Efficient IP Address Allocation \(background\)](#).
- [IEEE 802.1Q overview](#)

Older ISL encapsulation and the `switchport trunk encapsulation dot1q` command are historical/platform-specific; this guide uses fixed 802.1Q trunks. Example configs are for training and need change-control validation before production use.

MAG212 CYBER • Learn / Cheat Sheets • VLAN Ultimate Cheat Sheet • Original educational illustrations and configuration examples