

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

VLANs, trunks & MAC learning

01 / Quick reference and concepts

Follow one endpoint VLAN across access ports, trunks and the gateway without confusing link state with forwarding.

Cisco Catalyst IOS XE and Juniper EX/QFX. Junos configuration differs between ELS and non-ELS; this guide uses inspection commands.



Verify the same VLAN at every hop. A physical uplink can be up while VLAN 30 is absent or blocked.

Check	Access port	Trunk / uplink
VLAN identity	Assigned access VLAN	Allowed, active and forwarding VLAN
Tagging	Usually untagged endpoint	802.1Q; native handling must match
MAC learning	Client on expected port	Client follows expected uplink
Gateway	Client resolves its gateway	Gateway interface and return path

What to understand first

- A VLAN is a Layer 2 broadcast domain. Access and trunk describe interface behavior; routing between VLANs requires an L3 gateway and the relevant policy.
- A trunk has several distinct tests: negotiated/configured mode, VLAN permission, VLAN existence and spanning-tree forwarding. Passing the first does not prove the others.
- Native VLAN and untagged handling must match the design on both ends. Junos native-vlan-id and interface-mode placement depend on model and configuration style.
- MAC tables learn source addresses from traffic and age entries out. An absent MAC can mean an idle endpoint, wrong VLAN or missing frames, rather than a broken switch.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

VLANs, trunks & MAC learning

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show interfaces GigabitEthernet1/0/1 switchport
show interfaces trunk
show mac address-table vlan 30
show spanning-tree vlan 30
```

Inspect: Follow VLAN 30 through allowed, active and forwarding lists; trace the client MAC.

Junos EX/QFX

Read-only operational

```
show ethernet-switching interfaces
show vlans
show ethernet-switching table
show spanning-tree interface
```

Inspect: Compare VLAN membership, learned MAC location and STP state. Output details vary by release.

Illustrative trunk evidence

Illustrative teaching example, not captured device output.

```
Uplink state: up
Configured allowed VLANs: 10,20,30
Active VLANs:           10,20
Client VLAN:             30
```

- VLAN 30 is permitted but not active in this simplified example. Check VLAN existence and the intended configuration on both switches.
- Do not overwrite the whole allowed-VLAN list to repair one entry; review the approved change and existing traffic first.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

VLANs, trunks & MAC learning

03 / Troubleshooting and acceptance

1. Record endpoint MAC, VLAN, port and gateway; generate one controlled application attempt.
2. Verify access VLAN and physical errors at the endpoint port.
3. Follow the MAC and VLAN hop by hop, checking trunk permission and STP forwarding at both ends.
4. Once the gateway is reached, move to ARP, routing and firewall/session checks.
5. Retest another VLAN sharing the uplink to detect unintended impact.

Common mistakes

- Equating trunk status with carriage of every VLAN.
- Copying ELS stanzas directly into a non-ELS switch or vice versa.
- Changing native VLANs on one end or replacing an allowed list blindly.

Acceptance checks

- Expected VLANs traverse the uplink and unintended VLANs do not.
- MACs learn on the expected paths without unexplained movement.
- Gateway and real client applications pass on each affected VLAN.

Primary references

[Cisco IOS XE VLAN trunks](#)[Junos ELS MAC table](#)[Junos spanning-tree monitoring](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)