

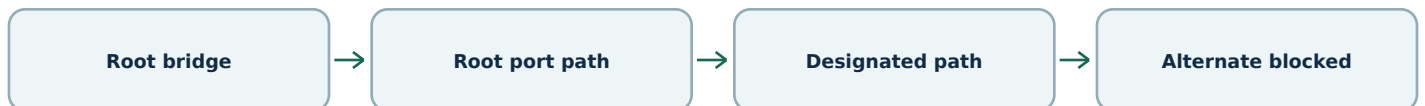
SWITCHING | REV 2.0 | REVIEWED 2026-10-10

STP, RSTP & MST field reference

01 / Quick reference and concepts

Interpret root election and port roles, distinguish expected blocking from a fault and check MST boundaries.

Layer 2 STP variants on Catalyst IOS XE and Junos. Per-VLAN, common-tree and MST interoperability must be designed explicitly.



This is a role-reading sequence, not a physical topology. Each non-root bridge selects a root port; alternate paths can be intentionally non-forwarding.

Item	Interpretation	Operational check
Root election	Lowest bridge ID wins	Priority plus system-ID extension / MAC
Root port	Best path toward root	Compare cost and tie-breakers
Designated	Selected port for segment	Normally forwards when converged
Alternate	Other path to root	Discarding can be healthy
RSTP states	Discarding / learning / forwarding	Role and state are different
Classic timers	Hello 2s / max age 20s / delay 15s	Defaults, not a convergence guarantee
MST region	Name, revision, VLAN mapping	Must agree for same region

What to understand first

- Root placement should follow the intended traffic design. An accidental low bridge priority can move the root and redirect traffic without a physical link failure.
- Classic STP uses blocking, listening, learning and forwarding states; RSTP combines non-forwarding states as discarding and uses rapid transition mechanisms where applicable.
- Edge/PortFast settings are for intended endpoint edges. BPDU Guard and root protection serve different purposes; investigate their trigger before restoring a port.
- MST maps VLANs into instances. A mismatch in name, revision or mapping creates a region boundary even when the cables and VLAN lists match.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

STP, RSTP & MST field reference

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 spanning-tree summary
show spanning-tree vlan 30
show spanning-tree inconsistentports
show spanning-tree mst configuration
```

Inspect: Check root identity, role/state, inconsistent ports and the actual MST mapping.

Junos

Read-only operational

```
show spanning-tree bridge
show spanning-tree interface
```

Inspect: Inspect root ID, root port, costs and role/state. Match the output to RSTP, MSTP or VSTP in use.

Illustrative role/state observations

Illustrative teaching example, not captured device output.

```
Root ID: distribution switch A
Uplink 1: Root / Forwarding
Uplink 2: Alternate / Discarding
Root changes during incident: 0
```

- A non-forwarding alternate can be correct loop prevention. Confirm the topology before trying to make both uplinks forward.
- If the expected root changes repeatedly, investigate BPDUs, link instability and unauthorized switches.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

STP, RSTP & MST field reference

03 / Troubleshooting and acceptance

1. Identify the intended and actual root for the affected VLAN/instance.
2. Compare roles and states on both ends of the suspected segment.
3. Review topology changes, error counters and protection-triggered ports with timestamps.
4. For MST, compare region parameters and VLAN-to-instance mappings exactly.
5. Use a planned redundancy test; verify reconvergence and application recovery before closing.

Common mistakes

- Disabling STP to make a blocked link pass traffic.
- Applying edge settings to an inter-switch link without the intended design.
- Assuming all vendors run an identical per-VLAN tree by default.

Acceptance checks

- Actual roots and region boundaries match the design.
- No unexplained inconsistent ports or sustained topology-change bursts.
- Approved link-failure test meets the application recovery target.

Primary references

[Cisco IOS XE spanning tree](#)[Junos spanning-tree monitoring](#)[Junos show spanning-tree bridge](#)

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](#)