🧩 Chapter 9 – Spanning Tree Protocol (STP) Concepts

🌐 1. STP and RSTP Basics

The Need for Spanning Tree

Switches flood broadcast and unknown unicast frames.
If there are redundant links, a loop can occur ⟶ frames circulate forever ⟶ network crash.

✅ STP (Spanning Tree Protocol) prevents loops in a Layer 2 network.

What Spanning Tree Does

STP:

- Detects loops
- Blocks redundant links
- Keeps only one active path between switches
- Automatically re-enables blocked links if the main link fails

🧠 Goal: create a "loop-free logical topology," even if physical links are redundant.

⚙️ 2. How Spanning Tree Works

The STP Bridge ID and Hello BPDU

- Bridge ID (BID) = priority + MAC address (unique ID of each switch).
- Switches exchange BPDU (Bridge Protocol Data Units) every 2 seconds to share information.
- Hello BPDU messages are used to elect the Root Bridge.

Electing the Root Switch

- The Root Bridge is the "center" of the network tree.
- Election rules:
    1. Lowest Bridge ID wins.

2. If priorities are equal, lowest MAC address wins.

✅ Set root manually:

spanning-tree vlan 1 root primary

Choosing Each Switch's Root Port

- After the root is elected, every non-root switch selects one port with the lowest path cost to reach the root.
- That port becomes the Root Port (RP).
- STP uses path cost values (based on link speed):
  - 100 Mbps → 19
  - 1 Gbps → 4
  - 10 Gbps → 2

Choosing the Designated Port on Each LAN Segment

- On each LAN segment, one switch port becomes the Designated Port (DP) — the port that sends frames toward the root.
- The other port (if any) becomes blocked to avoid loops.

Configuring to Influence the STP Topology

You can control which switch becomes root by setting its priority:

Switch(config)# spanning-tree vlan 10 priority 4096

🧠 Lower number = higher priority (default is 32768).

📊 3. Details Specific to STP (and Not RSTP)

STP Activity When the Network Remains Stable

- The network has one Root Bridge.
- Root ports and designated ports stay in forwarding state.
- Redundant ports stay blocked.

STP Timers That Manage STP Convergence

- Hello Time: 2 seconds (Root sends BPDUs)
- Forward Delay: 15 seconds (time to move between states)
- Max Age: 20 seconds (how long to wait before deciding the root is dead)

Changing Interface States with STP

Ports go through five states:

1. Blocking – listens only for BPDUs
2. Listening – prepares to forward, no data yet
3. Learning – starts building MAC address table
4. Forwarding – sends and receives data
5. Disabled – administratively down

🕑 Convergence can take 30–50 seconds in traditional STP.

⚡ 4. Rapid STP (RSTP) Concepts

Comparing STP and RSTP

- RSTP (802.1w) is a faster version of STP.
- Converges in a few seconds instead of 50+.
- Uses port roles and handshakes for faster recovery.

RSTP and the Alternate (Root) Port Role

- Root Port (RP): best path to root.
- Alternate Port: backup path if RP fails (quick switch).
- Designated Port (DP): forwards frames for that LAN.
- Backup Port: secondary DP on same segment.

RSTP States and Processes

RSTP simplifies STP's five states into three:

1. Discarding (blocking + listening combined)
2. Learning
3. Forwarding

✅ Result: much faster convergence.

RSTP and the Backup (Designated) Port Role

- Backup Port is a non-forwarding port that can quickly take over if the designated port fails.

RSTP Port Types

1. Edge Port: directly connected to an end device (like a PC).
2. Point-to-Point Port: between two switches.
3. Shared Port: connected to a hub (rare now).

🧰 5. Optional STP Features

EtherChannel

Combines multiple physical links into one logical link for redundancy + speed.

- STP treats it as one single link, preventing loops.
- Configuration example:

```
interface range g0/1 - 2
channel-group 1 mode active
```

PortFast

- Used for access ports (PCs) to skip STP states.
- Port goes immediately to forwarding.
- Should not be used on switch-to-switch links.

```
interface f0/10
spanning-tree portfast
```

BPDU Guard

- Works with PortFast.
- If a BPDU is received on a PortFast port → port is shut down (to prevent loops).

`spanning-tree bpduguard enable`

BPDU Filter

Two uses:

1. On PortFast ports: prevents BPDUs from being sent or received (to stop accidental loops).
2. On trunks: can be used to disable STP entirely on a port (rare).

`spanning-tree bpdufilter enable`

Root Guard

- Prevents another switch from trying to become the root bridge.
- If it receives better BPDUs, the port goes into root-inconsistent state.

spanning-tree guard root

Loop Guard

- Protects against unidirectional link failures that might cause loops.
- Keeps a port in loop-inconsistent state if BPDUs stop arriving.

spanning-tree guard loop

🧾 Final Summary (Easy Table)

Concept	Description	Key Command
STP	Prevents Layer 2 loops	spanning-tree vlan X
BPDU	Control message for STP	Sent every 2s
Root Bridge	Central switch of STP	spanning-tree vlan X root primary
Root Port	Best path to root	auto-selected
RSTP	Faster version of STP	IEEE 802.1w
PortFast	Instant forwarding on access ports	spanning-tree portfast
BPDU Guard	Protects PortFast ports	spanning-tree bpduguard enable
Root Guard	Prevents fake roots	spanning-tree guard root
Loop Guard	Prevents loops due to link failure	spanning-tree guard loop
EtherChannel	Combines multiple links	channel-group X mode active

---