Days 20, 21, 22: Spanning Tree Protocol

CCNA 200-301 Study Guide: Layer 2 Switching and Spanning Tree Protocol

1.0 The Critical Need for Spanning Tree Protocol (STP)

In modern networks, redundancy is a necessity for high availability. However, redundant physical links at Layer 2 create a lethal risk: switching loops. Unlike Layer 3 packets, which have a Time-to-Live (TTL) field to kill a packet if it circles too long, Layer 2 Ethernet frames have no expiration mechanism.

The Consequences of a Loop

1. Broadcast Storms: A single broadcast frame is duplicated endlessly, consuming all bandwidth and crashing switch CPUs.
2. MAC Table Instability (MAC Flapping): The switch sees the same source MAC appearing on different ports simultaneously, causing its forwarding logic to fail.
3. Duplicate Frame Delivery: A host receives multiple copies of the same unicast frame, causing application errors.

The Metaphor: Think of STP as a Tree Pruner. It looks at a messy, circular bush of redundant wires and "prunes" (blocks) specific branches so that only a single, logical tree remains where every leaf (host) has exactly one path to the root.

2.0 Core Mechanics of Legacy STP (IEEE 802.1D)

STP creates a loop-free topology by electing a single reference point called the Root Bridge.

2.1 The Root Bridge Election

The switch with the numerically lowest Bridge ID (BID) is elected the Root Bridge.

$$Bridge\ ID = Bridge\ Priority + Extended\ System\ ID\ (VLAN\ ID) + MAC\ Address$$

- Default Priority: 32,768 (must be changed in increments of 4,096).
- Tie-breaker: If priorities are equal, the switch with the lowest MAC address wins.
- Outcome: All ports on the Root Bridge are Designated Ports (DP) and are in a forwarding state.

2.2 STP Path Cost

Each non-root switch finds the "cheapest" path to the root based on cumulative link costs.

Link Speed	802.1D Cost (Legacy)	802.1w Cost (Rapid)
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2,000

2.3 STP Port Roles

1. Root Port (RP): The single port on a non-root switch with the lowest cost to the Root Bridge.

2. Designated Port (DP): The port on a segment that provides the best path to the Root. One DP per segment.
3. Non-Designated Port: A port that is Blocking to prevent a loop.

3.0 STP Port States and Convergence

To prevent loops while calculating the topology, 802.1D uses a timer-based approach.

State	Forward Data?	Learn MACs?	Notes
Blocking	No	No	Listens for BPDUs.
Listening	No	No	15s delay. Determining roles.
Learning	No	Yes	15s delay. Building the MAC table.
Forwarding	Yes	Yes	Fully operational.

- Total Convergence Time: 30–50 seconds. This delay is the primary weakness of legacy STP.

4.0 Rapid Spanning Tree Protocol (RSTP - 802.1w)

RSTP is the modern standard. It replaces slow timers with a Proposal-Agreement Handshake, allowing for sub-second convergence.

4.1 RSTP Enhancements

- Discarding State: Combines the legacy Blocking and Listening states.
- Alternate Port: A pre-calculated backup for the Root Port. If the RP fails, the Alternate Port goes to forwarding immediately.
- Backup Port: A backup for a Designated Port (rare, used with hubs).

- Edge Ports: Ports connected to end devices (PCs). They transition to forwarding immediately.

5.0 The STP Security Toolkit

To prevent accidental loops or malicious Root Bridge hijacking, use these standard features:

- PortFast: Configured on access ports (PCs/Servers). Bypasses Listening/Learning to prevent DHCP timeouts.
- BPDU Guard: If a port with BPDU Guard receives a BPDU (indicating someone plugged in a switch), it puts the port in err-disabled state.
- Root Guard: Prevents a downstream switch from becoming the Root Bridge.
- Loop Guard: Prevents loops caused by unidirectional link failures (e.g., fiber strands failing).

6.0 Configuration and Verification Commands

6.1 Configuration

Set the mode to Rapid PVST (Recommended)

Switch(config)# spanning-tree mode rapid-pvst

Set the Root Bridge (Method 1: Macro)

Switch(config)# spanning-tree vlan 10 root primary

Set the Root Bridge (Method 2: Priority)

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

Configure Access Port security

Switch(config)# interface g0/1

Switch(config-if)# spanning-tree portfast

Switch(config-if)# spanning-tree bpduguard enable

6.2 Verification

Command	Purpose
show spanning-tree	General overview of roles, costs, and Bridge IDs.
show spanning-tree vlan <id>	STP status for a specific VLAN.
show spanning-tree summary	High-level look at states and global features.

7.0 Key Takeaways Summary

1. STP prevents loops by logically blocking redundant paths.
2. Election is based on the Lowest Bridge ID.
3. Legacy STP (802.1D) is too slow (30-50s); RSTP (802.1w) is the standard.
4. Security: Always use PortFast + BPDU Guard on all user-facing ports to protect the topology.

Revision #1
Created 2026-03-14 19:26:50 UTC by Tony Utter
Updated 2026-03-14 19:27:09 UTC by Tony Utter