Spanning Tree Protocol (STP) Workbook

A Hands-On Guide to PVST+, RSTP, and MSTP

Mehdi JAFARI ZADEH

Date: January 21, 2025

Contents

Chapter 1

Introduction

1.1 Purpose and Audience

Welcome to the **Spanning Tree Protocol (STP) Workbook**. This resource is designed for students and IT professionals who want hands-on practice with the various flavors of STP, such as PVST+, RSTP, and MSTP. By working through the material, you'll build a solid foundation in both the theoretical and practical aspects of Spanning Tree deployment.

- **Who Should Use This Workbook?**
  - Networking learners familiar with **basic Ethernet switching** and **VLAN fundamentals**.
  - Network engineers or administrators looking to strengthen or refresh their STP expertise.
- **What Topics Are Covered?**
  - Core concepts and functions of STP.
  - Configuration steps and relevant commands.
  - Practical lab exercises to reinforce concepts.
  - Advanced discussions of load balancing, security enhancements, and recommended practices.

1.1.1 Prerequisites

Before diving into this workbook, you should have:

- **General CLI experience**: Ability to move between different switch configuration modes (e.g., global config, interface config).
- **IP addressing and subnetting knowledge**: Comfort with IPv4/IPv6 addresses, subnet masks, and interface configurations.
- **Basic VLAN skills**: Understanding VLAN creation, VLAN assignment, and trunk port setup.

1.2 How to Use This Workbook

The workbook is divided into sections that build on each other. Each section features an introduction to theoretical concepts, followed by configuration examples, and concludes with exercises to apply what you've learned.

1. **Theory**: Explains the principles and objectives of each topic.
2. **Command References**: Highlights relevant commands for each concept.

3. **Hands-On Exercises**: Lets you configure and test STP in different scenarios.

4. **Answer Key (at the end)**: Provides detailed solutions and reasoning for the exercises.

Note. *Attempt each exercise on your own first. Use the answer key only as a reference after you've tried to solve the tasks. Experimentation and troubleshooting enhance your understanding of STP and develop valuable problem-solving skills.*

Revisit earlier sections if you find yourself unclear on any points; each new topic often depends on earlier fundamentals. By following this structure, you'll deepen your theoretical knowledge while also learning practical configuration and troubleshooting skills for real-world STP deployments.

Chapter 2

STP Fundamentals

2.1 Redundancy and the Need for STP

2.1.1 Redundancy in Switched Networks

Enterprise networks often implement **redundant connections** between switches to boost reliability and uptime. While extra links improve resilience, they also risk creating **Layer 2 loops**.

What Are Layer 2 Loops?

A Layer 2 loop occurs when multiple paths exist between the same devices and broadcast or certain multicast/unicast frames end up circulating indefinitely. This leads to:

- **Broadcast Storms**: Excessive broadcast traffic overwhelms links and switch CPUs.
- **MAC Table Instability**: Switches repeatedly update their MAC address tables with conflicting data, causing incorrect forwarding.
- **High CPU Usage**: Switches become inundated as they struggle to handle the repeated frames and table updates.

2.1.2 How STP Breaks Loops

The **Spanning Tree Protocol** (as defined in IEEE 802.1D, and later improved in additional standards) systematically identifies and **disables certain ports** in a redundant topology. This ensures there is only one logical path to any segment, forming a "tree" without loops. If a primary path fails, STP rapidly recalculates the topology and activates a previously blocked port to restore connectivity.

2.2 STP Concepts and Terminology

2.2.1 Bridge ID and Root Bridge

- **Bridge ID (BID)**: Unique to each switch, consisting of a **bridge priority** and a **MAC address**.
- **Root Bridge**: The switch with the **lowest BID** acts as the logical hub for the network's spanning tree. All other switches calculate their best path to this root.

2.2.2 Port Roles

- **Root Port (RP)**: On non-root switches, this port leads **directly** to the Root Bridge via the path with the lowest cost.

- **Designated Port (DP)**: One per segment, it forwards traffic away from the Root Bridge. Determined by the lowest path cost and then by BID if there's a tie.
- **Non-Designated/Blocked Port**: Any port not chosen as a DP or RP remains blocked to prevent loops in the network.

2.2.3 Port States (802.1D STP)

1. **Blocking**: Receives BPDUs but does not forward frames.
2. **Listening**: Prepares to participate in forwarding; listens for BPDUs but discards data frames.
3. **Learning**: Learns MAC addresses but still does not forward data frames.
4. **Forwarding**: Actively sends and receives data and BPDUs.
5. **Disabled**: Port is shut down or otherwise administratively disabled.

Note. *Rapid STP (RSTP) and MSTP simplify these states to Discarding, Learning, and Forwarding.*

2.2.4 BPDU (Bridge Protocol Data Unit)

BPDUs carry critical STP information (Bridge ID, root path cost, timers, etc.) between switches. They enable the election of the Root Bridge, selection of port roles, and detection of topology changes.

2.2.5 Path Cost

- **Path Cost** indicates link desirability. Common defaults: 10 Mbps = 100, 100 Mbps = 19, 1 Gbps = 4, 10 Gbps = 2.
- Lower cost implies a more preferred path.

2.3 STP Timers

Three key timers govern the speed and reliability of STP convergence:

1. **Hello Time (default 2 seconds)**
   - How often the Root Bridge sends out BPDUs.
2. **Forward Delay (default 15 seconds)**
   - Duration the port remains in Listening and Learning states before transitioning to Forwarding.
3. **Max Age (default 20 seconds)**
   - Time a switch will retain a received BPDU before considering it invalid.

Note. *Tweaking timers can accelerate or slow down convergence. Misconfiguration can lead to instability.*

2.4 Root Bridge Election

When STP launches, all switches initially assume they can be the root and send out BPDUs with their own Bridge ID. Through BPDU exchanges:

1. Switches compare **Bridge IDs**.
2. The lowest Bridge ID wins the **Root Bridge** title.

3. Non-root switches compute their route cost to the Root.
4. Each switch designates one **Root Port** with the smallest cost path to the Root.
5. Every segment has one **Designated Port** (lowest cost/BID).
6. Other ports become **blocked** to avoid loops.

2.4.1 Tie-Breakers

If two switches have the same priority, the switch with the lower **MAC address** wins. For a given switch's Root Port selection, if path costs are equal, the decision continues with comparing sending BIDs or port IDs.

2.5 Basic STP Configuration

Below are examples using a Cisco CLI, though specifics may differ by device model or vendor.

2.5.1 Setting the STP Mode

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

Note. ***PVST+*** *is Cisco's Per-VLAN Spanning Tree enhancement, but classic STP and PVST+ share similar fundamental mechanics.*

2.5.2 Configuring the Root Bridge

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

Lower priority = higher likelihood of becoming Root. Multiples of 4096 are commonly used.
Alternatively:

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

This automatically adjusts the priority so that your switch takes over as root for VLAN 10.

2.5.3 PortFast on Edge Ports

PortFast allows access ports (toward end-user devices) to bypass Listening/Learning:

```
Switch(config-if)# spanning-tree portfast
```

Caution: Only enable on ports connected to **end devices**, never inter-switch trunk ports.

2.5.4 Verification

Use these commands to check STP status:

```
Switch# show spanning-tree
Switch# show spanning-tree vlan 10
Switch# show spanning-tree detail
```

These commands provide details on the Root Bridge, port roles, costs, and configured timers.

2.6 Exercises

Exercise 2.1: Observing a Basic Topology

- **Objective**: Watch STP elect a root automatically.
- **Setup**:
  - Connect three switches (A, B, and C) in a triangle.
  - Verify STP is active.
- **Tasks**:
  1. Power up and let STP converge (30–60 seconds).
  2. Use `show spanning-tree` on each switch to find:
     - The Root Bridge.
     - Root Ports vs. Designated Ports.
     - Any blocked ports.
  3. Review each switch's **Bridge ID**.
- **Challenge:**
  - Why was the winning Root Bridge selected?
  - If a tie occurred, what resolved it?

Exercise 2.2: Forcing a Root Bridge

- **Objective**: Manually set which switch becomes root.
- **Setup**: Same three-switch triangle.
- **Tasks**:
  1. On **Switch B**, run:

     ```
     spanning-tree vlan 10 priority 4096
     ```

  2. Verify via `show spanning-tree vlan 10` that Switch B is now the root.
  3. Check port role changes.
- **Challenge:**
  - How would you make Switch A root for VLAN 20?
  - Why is it advantageous to assign different root switches for different VLANs?

Exercise 2.3: Using PortFast and BPDU Guard

- **Objective**: Speed up edge port convergence and protect against loops.
- **Setup**: Switch A with two access ports connected to two PCs (PC1, PC2).
- **Tasks**:
  1. Enable PortFast on the PC-connected interfaces.
  2. Enable BPDU Guard on those interfaces:

```
interface range FastEthernet0/1 - 2
  spanning-tree portfast
  spanning-tree bpduguard enable
```

3. Unplug and reconnect the PCs; note the instant Forwarding state.

- **Challenge:**
  - What happens if you link another switch to a PortFast + BPDU Guard port?

Exercise 2.4: Adjusting Path Costs

- **Objective**: Change STP paths by modifying interface cost.
- **Setup**: Reuse the three-switch triangle.
- **Tasks**:
  1. Identify the current Root Bridge.
  2. On a non-root switch, increase or decrease the cost on one trunk interface:

```
interface <port>
  spanning-tree cost <value>
```

  3. Verify via `show spanning-tree` that a different Root Port was selected.

- **Challenge:**
  - Why might changing interface cost be preferable over adjusting switch priorities in certain designs?

Summary and Next Steps

At this stage, you should be comfortable with the **basic principles of STP**—from why we need it to how it operates and is configured. The next section explores **STP variants (PVST+, RSTP, MSTP)**, diving into improvements in convergence speed, scalability, and flexibility.

Note. *Don't rush forward until you've mastered the fundamentals. Repetition and experimentation in a lab environment are key to truly understanding STP's behavior.*

Chapter 3

STP Fundamentals

3.1 Redundancy and the Need for STP

...

3.2 STP Concepts and Terminology

...

Chapter 4

STP Variants (PVST+, RSTP, MSTP)

4.1 PVST+

...

4.2 Rapid Spanning Tree Protocol (RSTP)

...

4.3 Multiple Spanning Tree Protocol (MSTP)

...

Chapter 5

Advanced STP Tuning and Security

5.1 PortFast

...

5.2 BPDU Guard

...

5.3 Root Guard and Loop Guard

...

Chapter 6

Monitoring and Troubleshooting

6.1 Key Show Commands

...

6.2 Common STP Problems

...

Chapter 7

Practical Lab Scenarios

7.1 Scenario 1: Single-VLAN STP

...

7.2 Scenario 2: Multi-VLAN + PVST+

...

7.3 Scenario 3: Rapid STP (Rapid PVST+)

...

7.4 Scenario 4: MSTP with Four VLANs

...

7.5 Scenario 5: Security Hardening

...

Chapter 8

Additional Resources

8.1 Official Documentation

...

8.2 Books and Study Guides

...

8.3 Online Articles and Videos

...

8.4 Lab Simulation Tools

...

8.5 Design and Best Practices

...