Alqalam Journal of Medical and Applied Sciences. 2025;8(4):2950-2955
https://doi.org/10.54361/ajmas.2584126

Original article

Analysis of RSTP Synchronization Performance and Its Security Features in Simulation Networks

Malak Almagoz[1]*, Nuredin Ahmed[2]

[1]*Department of Information Technology, Libya Academy for Graduate Studies, Tripoli, Libya*
[2]*Department of Computer Engineering, University of Tripoli, Tripoli, Libya*
Corresponding Email. *malakalmagoz2000@gmail.com*

Abstract
This study focuses on the design and implementation of an experimental network composed of three interconnected switches in order to analyze the performance of the Rapid Spanning Tree Protocol (RSTP). The protocol was applied to examine its role in preventing switching loops and controlling port states to ensure overall network stability. The network topology and all configurations were implemented using the Cisco Packet Tracer simulation tool, where RSTP was enabled, a root bridge was selected, and access ports were configured using PortFast, BPDU Guard, and Root Guard to improve convergence speed and enhance security. In addition, Root Guard was applied on inter-switch links to preserve the stability of the spanning tree structure. A link failure scenario was simulated to observe the protocol's behavior during topology changes and to evaluate its ability to quickly restore connectivity through an alternative path. The results demonstrated that RSTP operated efficiently, successfully prevented loop formation, and maintained continuous network stability. Furthermore, the study examined the convergence behavior of RSTP during topology changes caused by link disconnection, confirming its effectiveness in rapidly reconstructing network paths.
Keywords. Rapid Spanning Tree Protocol, Spanning Tree Protocol, BPDU Guard, Root Guard.

Introduction

Rapid Spanning Tree Protocol (RSTP) is an advanced network protocol developed from the traditional Spanning Tree Protocol (STP), designed to provide high availability and loop-free connectivity within Ethernet networks. This paper reviews network design, protocol configuration, implementation steps, testing procedures, and protocol behavior analysis. RSTP is considered one of the most significant improvements introduced to overcome the limitations of the traditional STP, which is known for its slow reconvergence process when network failures occur. RSTP enhances network performance by enabling rapid reconfiguration of the topology upon link failure, allowing traffic to switch to an alternative path within seconds. This capability is particularly important in modern networks where downtime must be minimized. Despite the widespread adoption of RSTP in many organizations and enterprises, several practical implementations still lack clarity regarding protocol activation, port role transitions, and failure recovery mechanisms when a link is disconnected. This gap highlights the need for practical simulation-based studies that clearly demonstrate RSTP behavior.

Previous studies published between 2021 and 2025 indicate that most research related to the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) has primarily focused on theoretical analysis or performance comparisons between STP and its variants. Many of these studies emphasized protocol efficiency and convergence behavior without presenting a clear practical or simulation-based model that can be directly applied in educational or training environments. In contrast, the present study proposes an integrated practical simulation model for designing a network with redundant paths and evaluating RSTP behavior within a reproducible simulation environment using Cisco Packet Tracer [1]. This approach extends beyond purely theoretical discussions by providing detailed configuration steps and analyzing port roles, including root, designated, and alternate ports, before and after topology changes. Furthermore, several previous works did not adequately address port protection mechanisms such as PortFast, BPDU Guard, and Root Guard within the context of RSTP deployment [2,3].

The current study incorporates these security features as essential components to enhance network stability and prevent unintended topology changes. Existing literature also reports that traditional STP convergence time typically ranges between 30 and 50 seconds following a link or node failure, whereas RSTP significantly reduces convergence time to a few seconds or even milliseconds, depending on network topology and port configuration parameters [7]. By combining practical simulation, convergence analysis, and security feature evaluation, this study addresses gaps identified in previous research and provides a comprehensive applied model for RSTP analysis.

This study was conducted to design and implement a practical simulation model that demonstrates RSTP configuration and deployment using Cisco Packet Tracer, to analyze port roles—including root, designated, and alternate ports—before and after topology changes, to evaluate protocol behavior and the effectiveness of security features during link failure scenarios, and to provide a reproducible educational model that supports learning and practice for network engineering students and practitioners.

Received*: 25-10-2025 -* ***Accepted****: 19-12-2025 -* ***Published****: 28-12-2025*

Methodology

Research Approach

This research methodology employs a case study approach based on simulation of the Rapid Spacing Tree Protocol (RSTP) using Cisco Packet Tracer, a network simulation tool widely used in academic and professional training settings. This simulation approach was chosen because it provides a controlled and reproducible environment suitable for educational purposes and allows for repeated testing without physical hardware limitations. It is important to clarify that this study is based on network simulation, not real-world experimentation. Cisco Packet Tracer is a network simulator that mimics the behavior of actual network devices and protocols. This distinction from real-world experimentation (which requires physical hardware) is crucial for ensuring the accuracy of the methodology in the Analysis Stage.

Simulation Setup

The simulation topology consists of three managed switches with the following specifications, as shown in Table 1.

Table 1. Simulation Environment Specifications

Parameter	Configuration	Purpose
Switch Models	Catalyst 2960 series (simulated)	Standard enterprise switch
Link Speed	FastEthernet (100 Mbps)	Port cost calculation (default: 19)
Number of Switches	3 switches	Demonstrates multi-switch topology
Redundant Paths	1 backup links	Tests convergence mechanisms
Protocol Version	RSTP (802.1w)	Rapid reconvergence capability

Bridge Priority Configuration in RSTP

The root Bridge is Determined Based on The Lowest Bridge Priority Value. If The Priorities are Equal, as in our practical experience with three keys, where the priority of each key was 32769, the root bridge is chosen based on the lowest MAC address. Therefore, key number 1 was chosen as the root bridge because it has the lowest MAC address of the three, as shown in (Table 2) below.

Table 2. RSTP Priority Configuration for Root Bridge Selection

Switch	Priority Value	Role	Mac Address
Switch 0	32769	Tertiary Bridge	0090:0CBA:B312
Switch 1	32769	Root Bridge	0000:BD45:4443
Switch 2	32769	Secondary Bridge	0060:3EC6:19B7

Study phases

The study was conducted in three phases: In the first phase, the fundamentals of the Spanning Tree Protocol and loop prevention mechanisms were reviewed. Network requirements were defined, including redundancy, loop prevention, and convergence speed. The RSTP port role assignment algorithms were analyzed, and the implementation of security features was planned. In the second phase, the network topology was constructed in Cisco Packet Tracer. RSTP was enabled on all switches, and switch priorities were configured for root bridge selection. Port protection mechanisms were implemented, including PortFast on terminal ports, as well as BPDU Guard and Root Guard on uplink ports. Finally, the initial system state was documented. In the third phase, connection verification was performed through ping tests to ensure end-to-end communication across the network. Link failure scenarios were simulated by disconnecting specific links to observe the protocol's response. The output of global spanning tree commands was captured and analyzed following topology changes, providing insight into the updated network state. Protocol convergence time and port role transitions were evaluated to assess the efficiency of RSTP in maintaining stability and redundancy.

Figure 1 illustrates the system design stages, beginning with the project objectives and requirements analysis stage and progressing to the preparation of the topology and the selection of appropriate devices. Then, the root bridge device is identified, and the port roles are planned according to RSTP standards. Necessary protection is included to prevent loopbacks and secure the network. Finally, a network and link failure test plan is developed to verify the design's readiness before implementation.

Received*: 25-10-2025 -* ***Accepted****: 19-12-2025 -* ***Published****: 28-12-2025*

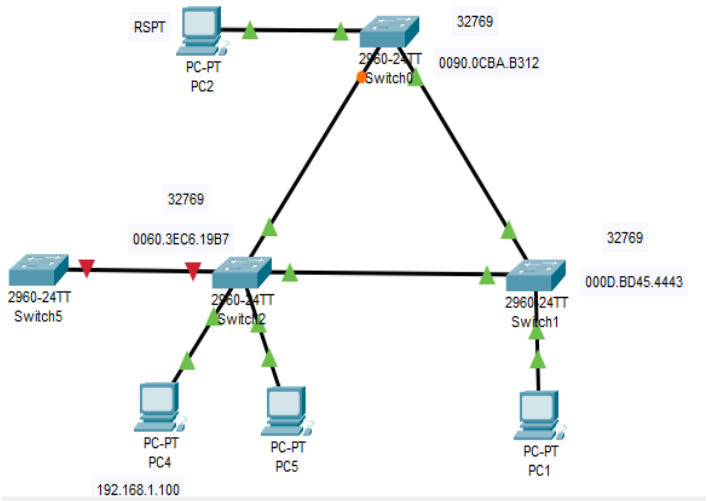

Figure 1. Final Network Topology Implemented for RSTP Simulation

Results

This section presents the results obtained after implementing the network, responding to it, and activating the RSTP protocol within the Packet Tracer environment. This section included three basic phases: connection testing, status checking, and link failure testing.

Connectivity Verification

Network connectivity was verified via ping tests between all connected devices. The process was confirmed to be responsive, and the RSTP protocol established correct routing paths without loops, enabling normal network connectivity. Subsequently, all test devices achieved full packet delivery with acceptable latency, confirming the protocol's functionality.

Initial Network State (Before Link Failure)

The initial spanning tree configuration established the following topology: Switch 1 (Root Bridge) with its spanning-tree output, Switch 0 with the spanning-tree output shown in Table 5, and Switch 2 with its spanning-tree output.

Table 3. Switch 1 Spanning Tree Information (Root Bridge)

Parameter	Value
Bridge ID Priority	32769
Bridge Address	0000:BD45:4443
Root Bridge ID	32769 (Self - this is the root)
Root Port	None (this switch is the root)
Hello Time	2 seconds
Max Age	20 seconds
Forward Delay	15 seconds

Table 4. Switch 1Port Information (All Ports Designated)

Interface	Type	Role	Status
FastEthernet 0/2	P2P	Designated	Forwarding
FastEthernet 0/3	P2P	Designated	Forwarding
FastEthernet 0/24	P2P	Designated	Forwarding

Table 5. Switch 0 Spanning Tree Information

Parameter	Value
Bridge ID Priority	32769
Bridge Address	0090.0CBA.B312
Root Bridge ID	32769 (Switch 0)
Root Port	FastEthernet0/2
Hello Time	2 seconds
Max Age	20 seconds
Forward Delay	15 seconds

Received*: 25-10-2025 -* ***Accepted****: 19-12-2025 -* ***Published****: 28-12-2025*

Table 6. Switch 0 Port Information

Interface	Type	Role	Status
FastEthernet 0/24	P2P	Designated	Forwarding
FastEthernet 0/1	P2P	Alternate	Forwarding
FastEthernet 0/2	P2P	Root	Blocked

Table 7. Switch 2 Spanning Tree Information

Parameter	Value
Bridge ID Priority	32769
Bridge Address	0060.3E8C.1987
Root Bridge ID	32769(Switch 0)
Root Port	FastEthernet 0/3
Hello Time	2 seconds
Max Age	20 seconds
Forward Delay	15 seconds

Table 8. Switch 2 Port Information (Initial State)

Interface	Type	Role	Status
FastEthernet 0/3	P2p	Root	Forwarding
FastEthernet 0/1	P2p	Designated	Forwarding
FastEthernet 0/23	P2p	Designated	Forwarding
FastEthernet 0/24	P2p	Designated	Forwarding

Analysis of initial state

The initial topology correctly reflects RSTP behavior. Switch 1, with the lowest MAC address (0000:BD45:4443), is elected as the root bridge, and all of its ports remain in the forwarding state. Switch 0 and Switch 2 each maintain one root port (FastEthernet 0/1) to ensure connectivity with the root. On Switch 0, FastEthernet 0/1 is blocked as an alternate port, serving as a backup path. Similarly, on Switch 2, FastEthernet 0/3 is blocked as the alternate port. This configuration effectively prevents loops while maintaining redundancy.

Network state after link failure

A link failure was simulated by disconnecting the connection between Switch 0 and Switch 2. The protocol rapidly reconverged, activating the alternate path via Switch 1, as illustrated in the following figure. Switch 1 remained unchanged and continued to function as the root bridge. The post-failure states of Switch 1 and Switch 2 are presented below, with Switch 2 undergoing a critical transition in port roles to restore connectivity.

Table 9. Switch 1 Post-Failure State

Parameter	Value
Bridge ID Priority	32769
Root Bridge ID	32769 (Self)
Root Port	None

Table 10. Switch 0 Ports After Link Failure

Interface	Type	Role	Status
FastEthernet 0/3	P2P	Designated	Forwarding
FastEthernet 0/24	P2P	Designated	Forwarding

Table 11. Switch 0 Post-Failure State

Parameter	Value
Bridge ID Priority	32769
Root Bridge ID	32769
Root Port	FastEthernet 0/1

Received*: 25-10-2025 -* ***Accepted****: 19-12-2025 -* ***Published****: 28-12-2025*

Following the failure of the connection between Switch 0 and Switch 1, the following transitions were observed. The previously blocked port on Switch 0 (Fa0/1) transitioned to the forwarding state and assumed the role of the root port. Similarly, the previously blocked port on Switch 2 (Fa0/1) also transitioned to forwarding mode, providing an alternate path to maintain connectivity. As a result, the alternative route through Switch 0 became the preferred forwarding path. Overall, network connectivity was preserved through the redundancy built into the topology, demonstrating RSTP's ability to rapidly restore availability after a link failure.

Table 12. Switch 1 Ports After Link Failure (Alternate Path Activated)

Interface	Type	Role	Status
FastEthernet 0/24	P2P	Designated	Forwarding
FastEthernet 0/1	P2P	Root	Forwarding

Table 13. Switch 2 Post-Failure State

Parameter	Value
Bridge ID Priority	32769
Root Bridge ID	32769
Root Port	FastEthernet 0/03

Table 14. Switch 2 Ports After Link Failure (Path Recalculation)

Interface	Type	Role	Status
FastEthernet 0/3	P2p	Root	Forwarding
FastEthernet 0/1	P2p	Designated	Forwarding
FastEthernet 0/23	P2p	Designated	Forwarding
FastEthernet 0/24	P2p	Designated	Forwarding

Convergence behavior

Although simulation-based measurements do not provide precise millisecond-level time data, the state transitions visualized in Cisco Packet Tracer software demonstrated near-instantaneous changes in port role upon link failure detection. In a production network, RSTP convergence typically occurs within one to three seconds in standard network topologies, compared to 30–50 seconds in traditional STP protocols [7].

Discussion

The Spanning Tree Protocol (STP) is one of the most essential protocols in Ethernet networks, as it prevents the formation of loops that can significantly degrade network performance. However, in large and complex network environments, STP becomes inefficient due to its slow response to topology changes, particularly during link failures or the addition of new switches. This limitation often results in extended network downtime, a challenge that has been widely reported in previous studies [7].

Rapid Spanning Tree Protocol (RSTP) was introduced as a major improvement over STP to address these limitations by significantly reducing convergence time. While traditional STP typically requires between 30 and 50 seconds to reconverge after a failure, RSTP can restore network connectivity within a few seconds. This finding is consistent with existing literature that highlights the faster convergence behavior of RSTP compared to STP under various network conditions [7]. Reduced convergence time is a critical factor in determining overall network efficiency and reliability.

In the RSTP framework, the root bridge is selected based on bridge priority values, allowing network administrators to control traffic flow and network stability through deliberate configuration. In this study, priority values were intentionally set to achieve optimal root bridge selection, which contributed to efficient data forwarding and network stabilization. Furthermore, the use of PortFast and BPDU Guard on access ports enhanced network performance and security by accelerating the transition of ports to the forwarding state and preventing unintended topology changes. Similar approaches have been discussed in previous research, emphasizing the importance of these features in maintaining stable and secure network operations [5][6]. Despite the advantages offered by RSTP, certain challenges may still arise when deploying the protocol in large-scale network environments.

Conclusion

The findings of this paper demonstrate that the Rapid Spanning Tree Protocol (RSTP) is a fundamental networking protocol for network stability and infrastructure. It mitigates the impact of link failures that could cause a complete network outage. The protocol is characterized by its ability to efficiently explain and

Received*: 25-10-2025 -* ***Accepted****: 19-12-2025 -* ***Published****: 28-12-2025*

process paths, effectively prevent loops, and maintain connectivity across redundant paths. RSTP also offers rapid topological adaptation and quick connectivity in case of link failure without affecting inter-device communication. Furthermore, it recognizes root bridges and assigns different port roles. The effectiveness of RSTP in regulating data freedom and appropriate paths has been demonstrated. Security settings such as Root Guard, PortFast, and BPDU Guard contribute to network security. Therefore, this study focuses on designing a network based on RSTP principles, one that is scalable and provides key performance across a wide range of variables, while also prioritizing security and software efficiency. This study represents a practical model that can be adopted in new network management and security designs.

Conflict of interest. Nil

References

1. EhabBooks. Rapid Spanning Tree Protocol (RSTP) overview. Available from: https://www.ehabbooks.com/?p=5082. Accessed 2025 Nov 9.
2. Accuenergy. Rapid Spanning Tree Protocol (RSTP): overview and operation. Available from: https://www.accuenergy.com/support/reference-directory/rapid-spanning-tree-protocol-rstp/. Accessed 2025 Mar 10.
3. Al-Qudah S. Applying reliability solutions to a cooperative network. Int J Adv Eng Technol. 2021;1(2):1–6.
4. Liu X, Zhang Y. Performance evaluation using Spanning Tree Protocol, Rapid Spanning Tree Protocol, Per-VLAN Spanning Tree, and Multiple Spanning Tree. Int J Comput Netw Commun. 2023;15(3):45–58.
5. Al-Hammadi A, Yousuf M. Spanning Tree Protocol (STP)-based computer network performance analysis under BPDU configuration attacks and root bridge takeover using linear regression. Int J Comput Netw Inf Secur. 2023;15(2):32–41.
6. Chien C. Spanning Tree Protocol (STP) and its application in network design. J Netw Comput Appl. 2003;27(3):161–169.
7. Pratapnaidu A, Maneesha MVR. Fast recovery from link failures in Ethernet networks. Int J Res Mod Eng Emerg Technol. 2024;12(1):45–52.

Received: *25-10-2025* - ***Accepted***: *19-12-2025* - ***Published***: *28-12-2025*