Araid Journal of Science and Technology (AJST)
Higher Institute of Science and Technology-Al Shmokh

مجلة الرائد للعلوم والتقنية
المعهد العالي للعلوم والتقنية - الشموخ

Received: 26 May 2026 | Accepted: 18 June 2026 | Published online: 30 June 2026

Comparative Review of STP, RSTP, and PVST Protocols: Loop Prevention in Layer 2 Networks

Azzam Nasr*, Nuredin A. S. Ahmed**
*Department of Information Technology, Libya Academy for Graduate Studies, Tripoli, Libya
**Department of Computer Engineering, University of Tripoli, Tripoli, Libya
azzammans20@gmail.com , nu.ahmed@uot.edu.ly

ABSTRACT

Ethernet switching technologies remain the underlying foundation of local area networks (LAN) since they provide scalable and efficient communication as well as cost-effectiveness between network devices in the modern world today. However, redundant Layer 2 paths introduce the risk of switching loops which may contribute to broadcast storms, duplicate fame transmission and media access control (MAC) network instability. In order to address such challenges, a wide range of loop prevention protocols have been developed while preserving network redundancy. Among these protocols are, the Spanning Tree Protocol STP, Rapid Spanning Tree Protocol RSTP and Per-VLAN Spanning Tree PVST.

Therefore, this study adopts a comparative analytical review methodology to evaluate these protocols based on operational principles, convergence speed mechanisms, scalability, redundancy management, VLAN support, load balancing capability, performance characteristics, security considerations and enterprise suitability. The study further examines some rising technologies such as multiple spanning tree protocol MSTP, Transparent Interconnection of lots of Links TRILL and EVPN-VXLAN.

The findings reveal that although STP provides a reliable foundation for loop prevention, its slow convergence makes it unsuitable for modern latency sensitive networks. RSTP significantly improves network recovery times via rapid convergence mechanisms, whereas PVST and Rapid PVST + provide enhanced traffic engineering and load balancing through VLAN spanning tree instances. The study concludes that modern enterprise and data center environments increasingly adopt multi-path layer 2 technologies that address the currently inherent limitations associated with the traditional spanning tree based approaches.

Key words: STP, RSTP, PVST, Layer 2 networks, Ethernet switching, loop prevention, VLAN, redundancy, MSTP, EVPN-VXLAN.

1. INTRODUCTION

The increasing growth of modern enterprise networks has become a fundamental requirement for reliability and fault tolerant communication infrastructures. Therefore, Ethernet technology has been viewed as the most prevailing networking standard because of its high availability, simplicity, scalability and operational continuity. [1] [2] .

To ensure network continuity, administrators very often deploy redundant links between switches providing alternative communication paths and backup during device or link failures. However, although redundancy supports fault tolerance, it can also contribute to the potential of layer 2 forwarding loops. [3] [1].

Unlike layer 3 IP networks, Ethernet switching does not involve a time-to-live TTL mechanism that is capable of addressing frame lifetime. As a result, Ethernet broadcast and other unknown frames may circulate in topologies carrying redundant paths. [4].This issue can result in serious network instability via broadcast storms, multiple frame duplication, MAC address table instability and excessive bandwidth consumption. These problems can lead to network congestion and complete service outages. To overcome these challenges, certain mechanisms are needed to prevent loops while maintain network redundancy. For instance, the Spanning Tree Protocol STP introduced by the IEEE was initially developed by Radia Perlman as standardized solution for preventing loops under IEEE 8.2.1D. This STP mechanism produces a loop-free logical topology through selectively blocking redundant links and thereby preserving physical redundancy during failover. [3] [5].

Overtime, subsequent advanced mechanisms have emerged such as Rapid Spanning Tree Protocol RSTP and vendor specific implementations such Per-VLAN Tree PVST and Rapid PVST+ to address the performance limitations and weaknesses of STP. Therefore, this paper provides a comparative analytical review of STP, RSTP and PVST, with the emphasis on their operational mechanisms, convergence characteristics, scalability, security considerations and suitability for modern networking environments. The paper also reviews new rising alternative technologies such as MSTP, TRILL, and EVPN-VXLAN which largely substitute for the traditional spanning tree approaches.

1.2 Research Gap

Although various studies focus on spanning tree technologies individually, limited comparative review studies comprehensively evaluate STP, RSTP and PVST simultaneously with emphasis on convergence performance, scalability, VLAN traffic engineering security implications and emerging Layer 2 alternative technologies. Therefore, this comparative study attempts to address this gap through a structured comparative analytical review.

1.3 Academic Contribution

This study contributes to existing literature on networking by providing a structured comparative analytical review of traditional and modern Layer 2 loop prevention technologies while integrating operational analysis, security evaluation, scalability

considerations and new emerging enterprise networking trends within a unified framework.

2.Reseach Methodology

2.1Reserach Design

This study adopts a comparative analytical review methodology rather than a simulation or experimental approach. The purpose is to critically compare STP, RSTP and PVST approaches according to their operational principles, convergence characteristics, scalability, redundancy and their suitability for enterprise networking.

2.2 Literature selection criteria

The reviewed sources were selected according to the following criteria:

1.Relevance to Layer 2 loop prevention and Ethernet switching

2.Inclusion of IEEE standards and Cisco implementation guides.

3. Availability of technical comparisons involving STP, RSTP, PVST, MSTP, TRILL or EVPN-VXLAN.

4. Preference for peer reviewed articles, RFCs, IEEE publications and some recognizing networking textbooks.

5. Inclusion of both classical and modern studies relate to enterprise networking.

However, sources lacking technical relevance or insufficient were excluded.

2.3 Comparison Framework

These protocols were compared based on some technical criteria. These criteria include: convergence speed, loop prevention efficiency, VLAN support, scalability, load balancing capability CPU and memory usage, administrative complexity, security implications and enterprise suitability. These criteria directly influence network reliability, operational stability and redundancy management.

2.4 Evaluation Metrics

The protocols were comparatively evaluated employing qualitative and technical indicators extracted from the reviewed literature in this area. The main metrics included network recovery time, traffic optimization capability, redundancy usage efficiency, CPU and memory overhead, VLAN traffic engineering flexibility, security resilience and scalability in enterprise environments.

2.5 Analytical Approach

This study used descriptive and analytical comparison methods to evaluate Root bridge election, Port roles and state transitions, convergence mechanisms, redundancy management, traffic forwarding behavior, security vulnerabilities, enterprise deployment suitability. The study further examined emerging technologies such as MSTP, TRILL and EVPO-VXLAN.

2.6 Scope of the study

This study does not implement laboratory simulations or packet–level experiments. As a result, the findings are derived from previously published technical and academic literature review. Therefore, the study should be interpreted as a comparative theoretical and operational review.

3. Literature review

3.1 Spanning Tree Algorithms

The operational framework of Spanning Tree based protocols is derived from graph theory an distributed systems algorithms. The spanning tree approach is a collection of links that connects all nodes in a network without causing cycles while eliminating redundant paths that may create loops. In Ethernet switching, these algorithms convert a physically redundant topology into a logically loop free form while still preserving backup communication paths. [1] [4].

Spanning tree protocols operate by exchanging Bridge Protocol Data Units BPDUs, enabling switches to collectively identify network topology information without relying on centralized control. By using distributed computation, switches select a Root Bridge, determine the lowest cost forwarding paths and identify redundant links that should be placed into a blocking or discarding state. [1] [4].

This election process involves three key stages:

1- Root Bridge Election
2- Root Port Selection
3- Designated Port Selection.

Each switch is assigned a Bridge ID (BID) consisting of a bridge priority value and a MC address. The switch with the lowest numerical BID is selected as the Root Bridge. Subsequently, non-root switches calculate the lowest cost path to the Bridge Root and designate the forwarding ports accordingly.[5] Perlman, R. (1985).

3.2 Understanding layer 2 loops

In order to understand the significance of loop prevention mechanisms, it is necessary to examine how Ethernet switching functions. Ethernet switches forward frames based on the destination of MAC addresses stored within dynamically learned forwarding tables. This associates MAC addresses with specific physical ports. When a frame arrives with an unknown destination MAC address the frame is flooded out of all interfaces except the ingress interface port. [1] [2].

In redundant layer 2 topologies, this frame flooding can cause forwarding loops. Broadcast frames that are replicated across many redundant links may continuously circulate between switches resulting in exponential traffic amplification. [4].

3.3 Effects of layer 2 loops

Layer 2 loops can severely disrupt Ethernet network operations. There are major conditions associated with layer 2 loops:

1. Broadcast storms: These broadcast and unknown frames are repeatedly replicated and forwarded across redundant links. This excessive traffic consumes network bandwidth and processing resources which can cause network outages. [4].
2. MAC Address Instability: switches frequently relearn MAC addresses from different interfaces. As a consequence, this instability prevents accurate frame

forwarding causing MAC flapping and unstable forwarding behavior throughout the network [2].

3. Duplicate Frame Delivery: although frames may traverse multiple redundant paths at the same time, end devices may receive multiple copies of the same Ethernet frame resulting in protocol instability and application inconsistencies and communication errors in the network. [1] [5].
4. Network Congestion: excessive traffic resulted from network loops can saturate switch ports and exhaust CPU resources causing network wide service degradation and disruption of network services.

Collectively, the severity of these conditions makes loop prevention an essential priority in any redundant switch networks. Therefore, spanning tree protocols can reduce these challenges by selectively blocking redundant ports through transforming physical mesh topology into a logically loop free one with the emphasis on preserving backup paths for redundancy. [3]

What is a layer 2 loop?

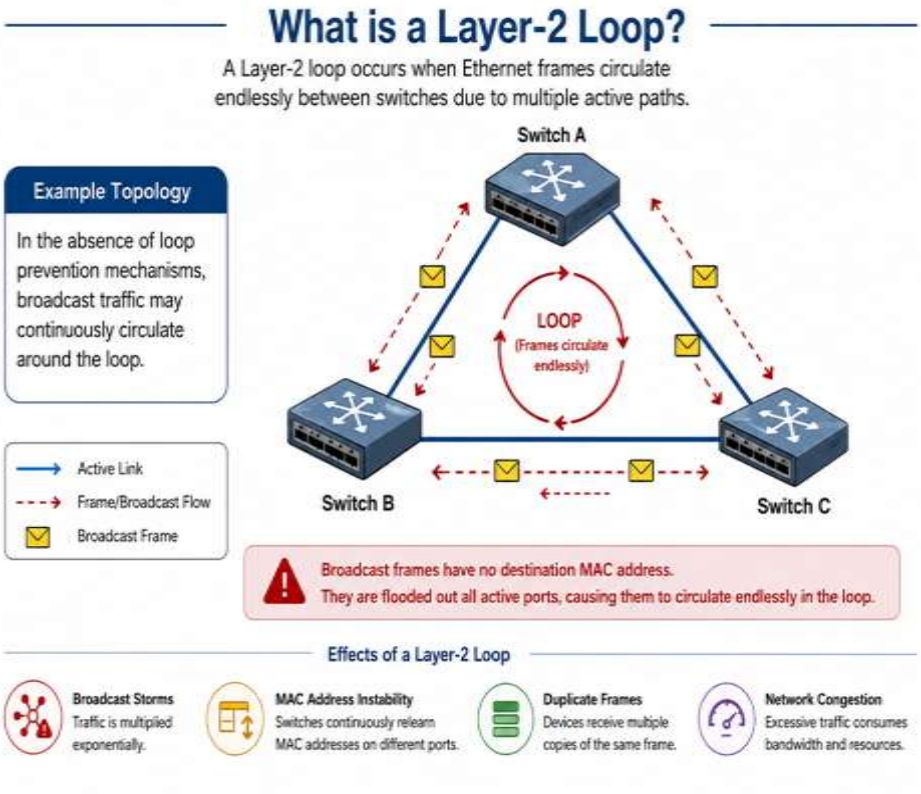


Figure 1: a layer 2 loop.

A layer 2 loop occurs when the Ethernet frames circulate endlessly between switches because multiple paths remain active simultaneously.
Examples of topologies:

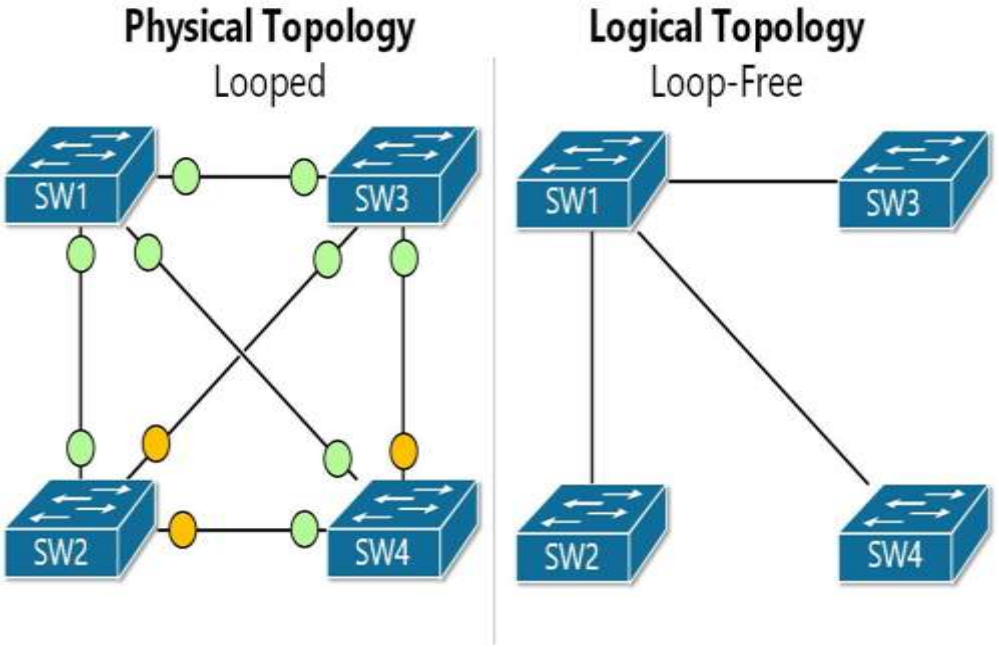


Figure 2: Examples of topologies

In case loop prevention mechanisms are absent, broadcast traffic continues circulating indefinitely around the loop.

4. Protocol analysis

4.1 Spanning Tree Protocol STP

4.1.1 Overview

This STP protocol was standardized under IEEE 802.I to construct a loop free topology while preserving redundant physical links for fault tolerance. It prevents layer 2 loops by selectively blocking redundant paths.[6].

4.1.2 STP operation

This protocol operates through four key mechanisms :

- Root Bridge Election.

The switch with the lowest Bridge ID value becomes the Root Bridge. Bridge ID consists of Bridge Priority and MAC Address. [3].

- Root Port Selection.

Each non- root switch selects a Root Port that provides the least-cost path toward the Root Bridge. [1] [2].

- Designated Port Selection

Each network segment elects a Designated Port that is responsible for forwarding traffic. [3][5].

- Blocking Redundant Ports

Ports that are not selected as Root Ports or Designated Ports enter the blocking state to prevent loops

4.1.3 STP Port States

Five operational port states defined by STP

Table 1: STP Port States

State	Function
Blocking	Prevents forwarding
Listening	Processes BPDUs
Learning	Learns MAC addresses
Forwarding	Actively forwards traffic
Disabled	Inactive

4.1.4. Limitations of STP

One of the primary limitations of STP is its slow convergence. It depends on several timer mechanisms, such as Hello Timer, Forward Delay Timer, and Max Age Timer. During the occurrence of topology changes, ports progress sequentially through the listening and learning states before reaching forwarding traffic mode. As a result, convergence generally requires around 30 and 50 seconds. Although this delay was acceptable in earlier Ethernet networks, these delays are unsuitable for modern real time applications that demand rapid fault recovery. [7].

4.2 Rapid Spanning Tree Protocol RSTP

4.2.1 Overview

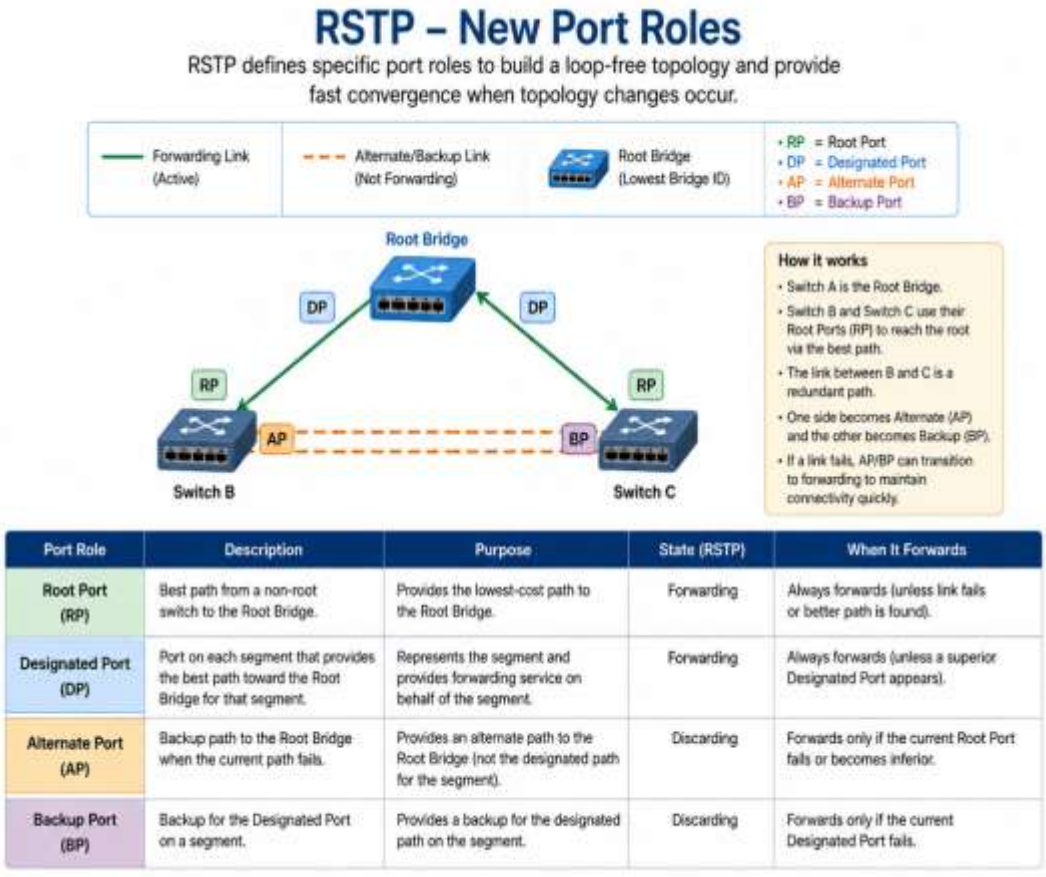
Rapid Spanning Tree Protocol RSTP which was standardized under IEEE 802.1W was developed to address the convergence limitations of the traditional STP and to improve convergence speed while preserving backward compatibility. [3].

4.2.2 New Port Roles

Rapid Spanning Tree Protocol RSTP introduces additional port roles to speed failover operations.

Table 2: New Port Roles

Port Role	Description
Root Port	Best path toward root
Designated Port	Active forwarding port
Alternate Port	Backup path to root
Backup Port	Backup designated path



Port Role	Description	Purpose	State (RSTP)	When It Forwards
Root Port (RP)	Best path from a non-root switch to the Root Bridge.	Provides the lowest-cost path to the Root Bridge.	Forwarding	Always forwards (unless link fails or better path is found).
Designated Port (DP)	Port on each segment that provides the best path toward the Root Bridge for that segment.	Represents the segment and provides forwarding service on behalf of the segment.	Forwarding	Always forwards (unless a superior Designated Port appears).
Alternate Port (AP)	Backup path to the Root Bridge when the current path fails.	Provides an alternate path to the Root Bridge (not the designated path for the segment).	Discarding	Forwards only if the current Root Port fails or becomes inferior.
Backup Port (BP)	Backup for the Designated Port on a segment.	Provides a backup for the designated path on the segment.	Discarding	Forwards only if the current Designated Port fails.

Figure 3: RSTP. New Port Roles

4.2.3 Port States

RSTP simplifies the five STP state model into three operational states as follows:
Table 3: RSTP Port States

State	Function
Discarding	Blocks traffic
Learning	Learns MAC addresses
Forwarding	Forwards traffic

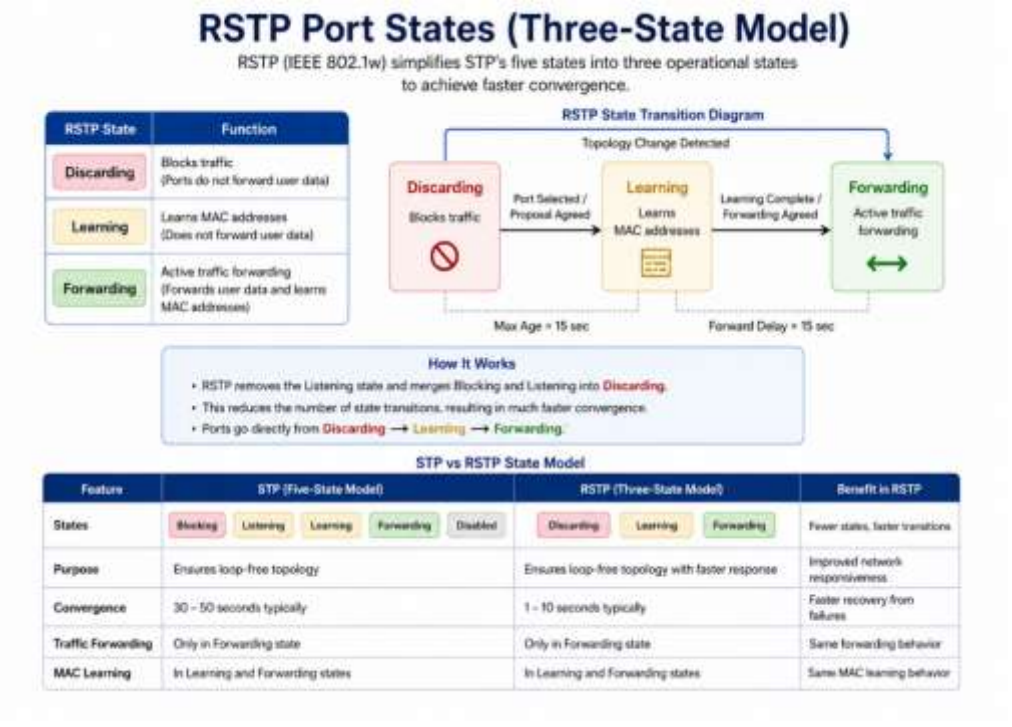


Figure 4: RSTP Port States

4.2.4 Limitations of RSTP

RSTP introduces several enhancements and support that can significantly reduce convergence time. RSTP introduces proposal and agreement process, edge ports, alternate ports, and immediate forwarding on point to point links. [6].

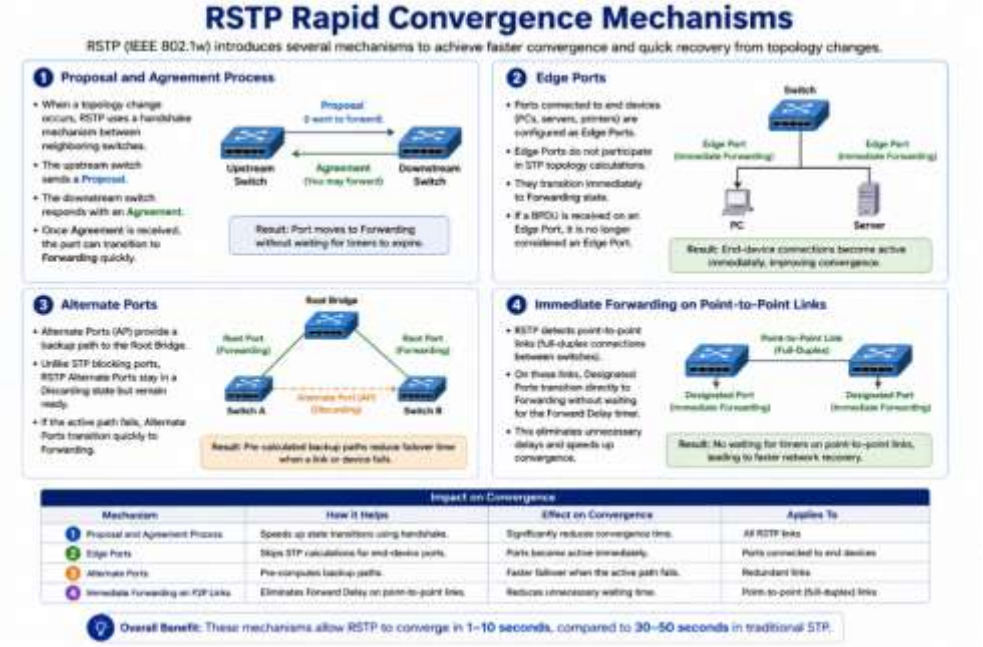


Figure 5: RSTP Rapid Convergence Mechanism

Unlike STP, RSTP increases complexity, greater processing requirements that STP and limited load balancing capabilities. RSTP actively negotiates topology changes between adjacent switches allowing convergence to operate within seconds instead of tens of seconds.

4.3 Per-VLAN Spanning Tree (PVST)

4.3.1 Overview

Per-VLAN Spanning Tree (PVST) is a Cisco propriety extension that creates an independent spanning tee instance for each VLAN.

4.3.2 Operational characteristics

Unlike STP and RSTP which function using a single spanning tree topology for all VLANs, PVST enables different VLANs to follow different forwarding paths. This design improves traffic distribution and optimizes bandwidth usage in enterprise networks containing multiple VLANs. [9] [8].

Per-VLAN Spanning Tree (PVST) is a Cisco propriety extension that creates an independent spanning tee instance for each VLAN. In contrast to STP and RSTP which function using a single spanning tree topology for all VLANs, PVST enables different VLANs to follow different forwarding paths. This design improves traffic distribution and optimizes bandwidth usage in enterprise networks containing multiple VLANs. [9] [8].

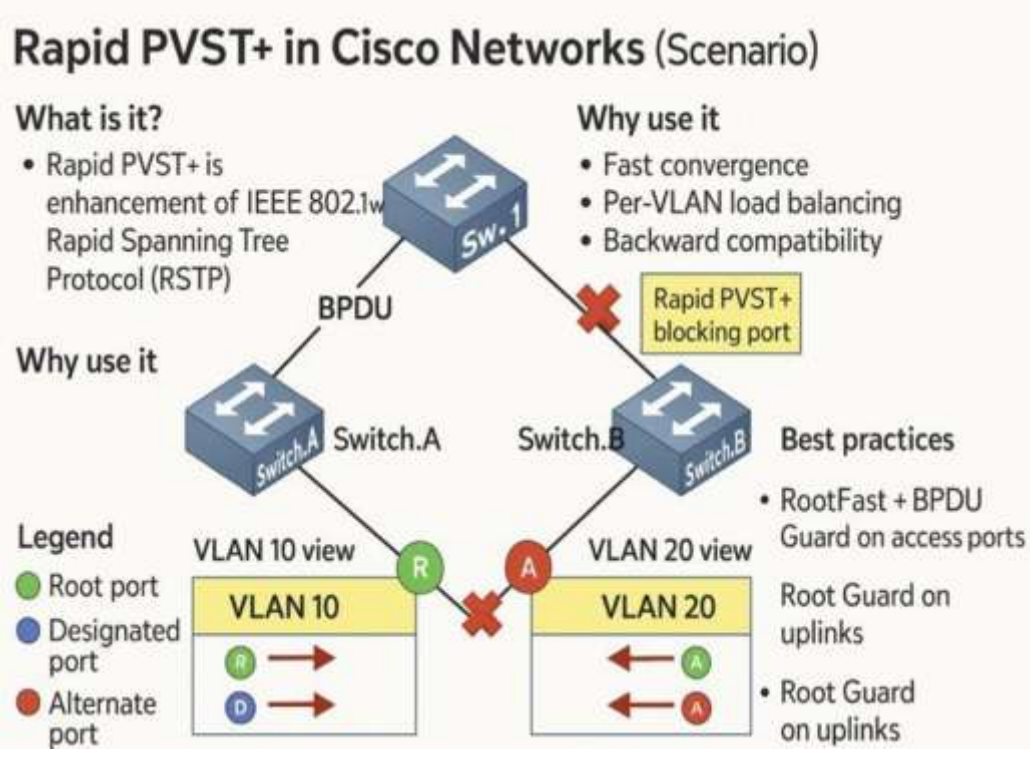


Figure 6: Rapid PVST+ in Cisco Networks.

Rapid PVST+ enables administrators to assign different Root Bridges to different VLANs as follows:

Table 4: Rapid PVST+ in Cisco Networks

VLAN	Root Bridge
VLAN 10	Switch A
VLAN 20	Switch B
VLAN 30	Switch C

As illustrated in the table above, this distribution allows traffic from separate VLANs to use different redundant links which improves traffic balancing and network efficiency.

Rapid PVST+ combines RESTP convergence mechanisms with Per-VLAN spanning tree operation. Each VLAN enjoys rapid failover and independent path optimization that is capable of rapid convergence and VLAN specific traffic engineering.

4.3.3 Limitations of PVST

Despite its flexibility, betted loading and improved bandwidth usage , PVST introduces various operational challenges. These include higher usage of CPU, higher memory consumption, greater administrative complexity and vendor dependence.

5.Security Considerations

Although spanning tree protocols are primarily designed for loop prevention, they also pose some key security challenges. STP and its related protocols do not implement native authentication mechanisms for Bridge Protocol Data Units BPDUs. As a result, a malicious attacker can inject superior BPDUs into the network and illegitimately assume the role of Root Bridge causing traffic interception, network instability or denial of service conditions. [9] [4].

In order to reduce these venerable risks, modern enterprise networks implement supplementary protection mechanisms including:

Table 5: Security implications

Security Feature	Function
BPDU Guard	Disables ports receiving unexpected BPDUs
Root Guard	Prevents unauthorized root bridge elections
Loop Guard	Protects against unidirectional link failures
Port Fast	Enables rapid forwarding on edge ports

As illustrated in the table above, these mechanisms significantly improve spanning tree security and operational stability.

6.Comparative analysis of SPT, RSTP & PVST

The following table outlines the key differences between Spanning Tree Protocol SPT, Rapid Spanning Tree Protocol RSTP and Per-VLAN Spanning Tree Protocol in terms of their technical characteristics and network performance.

6.1 Technical comparison

Table 6: Technical Comparison

Feature	STP	RSTP	PVST
Standard	IEEE 802.1D	IEEE 802.1w	Cisco Proprietary
Convergence	30–50 sec	1–10 sec	1–10 sec
VLAN Support	No	No	Yes
Load Balancing	Limited	Moderate	Excellent
Resource Usage	Low	Medium	High
Scalability	Moderate	High	Very High
Enterprise Suitability	Low	High	Very High

6.2 Performance comparison

Table 7: Performance Comparison

Performance Metric	STP	RSTP	PVST
Network Recovery Speed	Slow	Fast	Fast
CPU Utilization	Low	Medium	High
Traffic Management Efficiency	Poor	Moderate	Excellent
Redundancy Usage	Limited	Improved	Excellent
Suitability for Enterprise Networks	Moderate	High	Very High

To sum up, STP provides a simple and resource-efficient solution, but its slow time convergence can limit network performance. RSTP supports convergence speed and scalability which makes it more suitable for modern networks, PVST offers the highest level of traffic management and VLAN flexibility but it requires more processing resources and higher administrative complexity.

Overall, the selection between these protocols mainly depends on network size, vendor compatibility and performance needs. Small organizations may still operate

STP, whereas medium to large enterprises typically achieve better performance and scalability with RSTP or PVST+.

7.Emerging alternative Technologies

Modern data center environments largely employ technologies that can eliminate many limitations linked to spanning tree protocols.

7.1. Multiple Spanning Tree Protocol MSTP

multiple spanning tree protocol MSTP defined under IEEE 802, 1S, is an advanced protocol developed to improve network scalability and efficiency. It can also create a separate spanning tree instance or each VLAN, MSTP allows multiple VLANs to be combined into a single spanning tree instance, making it a practical solution in modern networking. IEEE Standards Association. [10] [11].

7.2. TRILL

Transparent interconnection of lots of links TRILL is a modern layer 2 networking approach developed to address the problems of traditional spanning tree protocols. TRILL allows all network links to remain active simultaneously allowing efficient layer 2 multipathing and improved bandwidth usage. It also supports active-active forwarding to improve network performance, redundancy and load balancing across multiple paths. TRILL reduces wasted network resources and offers more rapid transmission and fault recovery which makes it highly suitable for large enterprise settings. [12] [13].

7.3. EVPN-VXLAN

This modern network technology involves visualization that is largely adopted in modern data center environments due to its high scalability and flexibility. It operates through combining VPN (EVPN) with Virtual LAN (VXLAN) which enable efficient layer 2 an layer3 connectivity across large scale networks. This technology supports active-active forwarding by allowing multiple network paths to function simultaneously for improved redundancy and load balancing. [14]

8. Findings

This study found that all three protocols successfully prevent Layer 2 switching loops while preserving redundancy. However, these three protocols significantly differ in their functions regarding convergence speed, scalability, VLAN flexibility, traffic optimization and enterprise suitability.

STP provides a stable and standardized mechanism for preventing loops through Root Bridge election and redundant port blocking but suffers from slow convergence, which may range between 30 and 50 seconds during topology changes. RSTP substantially improves failover performance and operational responsiveness. PVST

provides superior VLAN traffic engineering and load balancing but introduces greater resource overhead and administrative complexity.

The findings further reveal that modern enterprise environments increasingly prefer technologies such as MSTP, TRILL and EVPN-VXLAN because these technologies aim at addressing several limitations regarding traditional spanning tree approaches by enhancing active -active forwarding, multipathing, higher scalability and improved redundancy usage. Despite the role of this evolution, STP protocols continue to remain relevant because of their maturity, simplicity, interoperability and wide implementation within Ethernet infrastructures.

Additionally, the study findings identify a number of security issues linked to spanning tree technologies especially the absence of native authentication regarding BPDU messages. Consequently, contemporary networks widely implement additional security mechanisms including BPDU Guard, Root Guard, Loop Guard and Port Fast to protect against malicious topology manipulation and to improve operational stability.

9. Discussion of findings

The findings of this comparative study indicate that while STP, RSTP and PVST effectively prevent Layer 2 switching loops, they significantly differ in convergence speed, scalability, VLAN support and suitability for modern enterprise networking. These findings are therefore consistent with the existing literature on Ethernet switching and loop prevention technologies.

This comparative review confirms that STP provides a standardized and reliable mechanism for preventing loops through Root Bridge election and redundant port blocking. This finding therefore supports the works of Perlman (1985) and IEEE 802.1D Standard (IEE Standard Association, 2004) who established STP as the fundamental protocol for the creation of loop free Layer 2 topologies. However, its relatively slow convergence time (30-50 seconds) limits its effectiveness in modern networking which requires rapid fault recovery. This limitation is also supported by Kozierok (2005).

Furthermore, the findings demonstrate that RSTP significantly improves network performance by reducing its convergence time to a few seconds through rapid transition mechanisms and traditional port roles. This finding is in agreement with IEEE 802.1w and is similar to the study of Saadat and Khedr (2016) who reported that RSTP improves network availability and operational efficiency while preserving compatibility and traditional STP.

Moreover, the analytical review shows that PVST offers the greatest flexibility by creating separate spanning tree instances foe each VLAN which allows improved traffic distribution and load balancing. These findings are therefore consistent with Cisco Systems (2022, 2023) which emphasize that Rapid PVST+ improves bandwidth usage and traffic engineering in VLAN based enterprise networks. However, this review confirms that these advantages are accompanied by higher CPU usage, memory consumption and configuration complexity.

The study further found another important result concerning security. Although spanning tree protocols effectively prevent loops, they remain vulnerable to BPDU manipulation because they lack native authentication mechanisms. This finding

therefore supports the study of Convery (2004) and Saadat and Khedr (2016) who recommended implementing security features such as BPUD Guard, Rot Guad, Loop Guard and PortFast to improve network resilience and protect against malicious topology changes.

Another final finding indicated in this review is that enterprise and data center environments are increasingly adopting advanced technologies such as MSTP, TRILL, and EVPN-VXLAN to address the limitations found in traditional spanning tree protocols. This conclusion therefore aligns with IEEE 802. 1Q (2018), Eastlake et al (2014), and Jha (2025) who found that such technologies support active-active forwarding, improved scalability, and more efficient utilization of redundant network paths.

Overall, the findings of the study demonstrate that although STP remains suitable for small and less complex networks, RSTP provides a more effective solution for most enterprise environments due to its rapid convergence and operational efficiency. PVST offers the highest VLAN flexibility in Cisco based infrastructures whereas emerging alternative technologies are increasingly becoming the most suitable choice for large scale and modern network architectures.

10. Conclusion

This comparative analytical review evaluated STP, RSTP, and PVST technologies as essential in layer 2 loop prevention in Ethernet switching environments.

The study confirmed that traditional SPT remains a reliable and standardized framework for loop prevention. However, its slow time convergence affects its effectiveness in latency sensitive and highly dynamic networks.

The study found that RSTP significantly improves network responsiveness through introducing rapid time convergence and quick failover capabilities, which makes it more feasible and appropriate for modern enterprises that need higher availability and reduced recovery times.

Moreover, the study found that PVST and Rapid PVST+ extend spanning tree functions through VLAN specific spanning tree instances that support load balancing, bandwidth usage and traffic engineering. Despite the role of PVST in providing superior flexibility and performance, it also introduces greater processing overhead, memory usage and configuration complexity compared to STP and RSTP.

Furthermore, the study established that security remains a critical aspect of spanning tree implementation as unauthorized BPDU manipulation can compromise network stability. As a result, modern enterprise networks depend on certain mechanism for data protection including BPDU Guard, Root Guard, Loop Guard and Port Fast to support network resilience and maintain operational security.

Overall, RSTP remains one of the most recommended spanning tree technologies used for modern enterprise network environments because of its rapid time convergence, improved fault recovery and its operational efficiency. Within Cisco based infrastructures using extensive VLAN segmentation, Rapid PVST+ provides enhanced traffic

improvement and higher administrative flexibility. Although the future direction of layer 2 networking largely prefers advanced multipath technologies such as MSTP, TRILL and EVPN-VXLAN which aim to eliminate several inefficiencies linked to traditional spanning tree approaches while supporting scalable and active – active networking design.

Refeences

[1] S. Tanenbaum and D. J. Wetherall, Computer Networks, 6th ed. Pearson Education, 2021.

[2] J. Doyle and J. Carroll, Routing TCP/IP, Volume 1, 2nd ed. Cisco Press, 2005.

[3] IEEE Standards Association, IEEE 802.1D-2004: IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges. IEEE, 2004.

[4] S. Convery, "Hacking Layer 2: Fun with Ethernet Switches," Black Hat USA Briefings, 2004.

[5] R. Perlman, "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN," ACM SIGCOMM Computer Communication Review, vol. 15, no. 4, pp. 44–53, 1985.

[6] M. Saadat and M. Khedr, "A Survey of Spanning Tree Protocol Security Vulnerabilities and Countermeasures," International Journal of Computer Science and Information Security, vol. 14, no. 5, pp. 412–421, 2016.

[7] C. Kozierok, The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference. San Francisco, CA, USA: No Starch Press, 2005.

[8] Cisco Systems, Rapid PVST+ Configuration Guide, IOS-XE Release 17.x. Cisco Press, 2022.

[9] Cisco Systems, Spanning Tree Protocol (STP) Enhancements: PortFast, UplinkFast, BackboneFast, Loop Guard, and Root Guard. Cisco Press, 2023

[10] IEEE Standards Association, IEEE Standard 802.1Q-2018: IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks. New York, NY, USA: IEEE, 2018.

[11] IEEE Standards Association, IEEE 802.1s-2002: IEEE Standard for Information Technology—Multiple Spanning Trees. IEEE, 2002.

[12] D. Eastlake, M. Zhang, P. Agarwal, R. Perlman, and D. Dutt, "Transparent Interconnection of Lots of Links (TRILL) Protocol," IETF RFC 7177, May 2014.

[13] P. Unbehagen, J. Jeffree, P. Ashwood-Smith, C. Fedyk, A. Bragg, N. Unbehagen, and G. Mihail, "Shortest Path Bridging IEEE 802.1aq Overview," 2012.

[14] C. Jha, "VXLAN/BGP EVPN for Trading: Multicast Scaling Challenges for Trading Colocations," International Journal of Computational and Experimental Science and Engineering (IJCESEN), vol. 11, no. 3, pp. 53–61, 2025. doi:10.22399/ijcesen.3478.