Design and Analysis of VLAN-Driven Access Control and Secure Communication in Ring-Based Switched Networks

Chandrappa S
Dept. of Computer Science and Engineering (Data Science)
Nagarjuna College of Engineering and Technology, Bengaluru, India
chandrucs21@gmail.com

Manoj Kumar R
Dept. of Computer Science and Engineering (Data Science)
Nagarjuna College of Engineering and Technology,Bengaluru, India
manojmanumr@gmail.com

Sushma B S
Dept. of Computer Science and Engineering (Data Science)
Nagarjuna College of Engineering and Technology, Bengaluru, India
sushma.shankar1694@gmail.com

Nikhila M R
Dept. of Computer Science and Engineering (Data Science)
Nagarjuna College of Engineering and Technology, Bengaluru, India
nikhila.mr@ncetmail.com

Lolakshi P K
Dept. of Computer Science and Engineering (Data Science)
Nagarjuna College of Engineering and Technology, Bengaluru, India
lolakshi88@gmail.com

Navya Rani M
Dept. of Research and development
Nagarjuna College of Engineering and Technology, Bengaluru, India
dr.navya@ncetmail.com

***Abstract*— Secure access control and traffic separation is required today in order to allow networks to communicate securely and remain intact. In this paper we investigate how VLANs can be used as an effective method of creating logical access control and secure communication within a redundant switched networking environment. A redundant, three-switch ring topology was created and tested using Cisco Packet Tracer, to test VLAN behaviors, traffic separation, MAC addresses, and how packets are routed through a dynamic network. We also set up our network so that when we connect two or more switches together, IEEE 802.1Q would enable us to use all the VLANs on each individual switch and rapidly spanning tree protocol (RSTP) would remove the loops from the switches allowing our network to function properly. Our research studied how DHCP addresses were assigned to devices connected to the switches, how packets were forwarded through the switches, how broadcasts were contained within the network segments, and how quickly a failure could occur in case one of the switches failed by analyzing the packets at the level they passed through the switches. The results showed that VLAN based segmentation effectively restricted the spread of unauthorized traffic, established well-defined boundaries for authorized communication among network segments and maintained network reliability and availability. Also, the use of RSTP enabled the rapid resolution of link failures in the event of a redundant link failure. Overall, it appears that the combination of VLAN based segmentation with control functions provided an effective means of managing secure access to a network segment and improving the resiliency of the network.**

Keywords—VLAN, Network Segmentation, IEEE 802.1Q,Rapid Spanning Tree Protocol (RSTP), Layer-2 Security, Ring Topology.

I.INTRODUCTION

Modern Ethernet networking uses Virtual Local Area Networks (VLANs) for logical segmentation of network traffic[1],[15], and improves both network security and performance. VLANs provide network managers with flexibility to organize devices based on their functional roles or departments, regardless of whether they are physically located at the same site. The nature of VLAN implementations within a more complex topology such as a three switch ring is different than when compared to other topologies. A ring topology provides high availability and redundancy[5][14]. However, this topology can introduce the potential for broadcast loops and create instability in forwarding paths[6],[14]. Therefore, configuring these types of topologies properly is critical.

Understanding VLAN segmentation in this context will prevent data from one VLAN from leaking into another segment (and thus, it preserves privacy and minimizes unnecessary congestion). Therefore, determining which frames are forwarded and filtered over the switches based on the application of 802.1Q VLAN tagging, trunk links and access ports; and, how each switch learns MAC addresses for its various VLANs is critical to making optimal decisions [10].

In order to achieve predictable, consistent performance from a network operating in a ring configuration, it will be necessary to apply loop prevention mechanisms such as Spanning Tree Protocol (STP), or Rapid STP (RSTP). RSTP and STP identify multiple paths between nodes, then selectively disable ports where possible to create an environment with no loops while creating at least one "backup" path when a node fails. The purpose of this study was to determine how VLANs are used in a three switch ring, how switches process tagged frames, and how STP provides for fault tolerant data transfer. The results should allow network designers to better understand interactions between VLAN settings and switching functions; thus support the creation of reliable, flexible, and robust layer two networks.

II.LITERATURE REVIEW

Early studies on the concept of VLANs, and how researchers and authors from industry have applied them to create logical sub-divisions of a single physical LAN by creating multiple

broadcast domains explain that devices contained within the same VLAN would be able to communicate as if they were connected via a single isolated LAN regardless of their physical location. These early VLAN based studies also provide evidence that this type of segmentation greatly improves management of these network systems and reduces unnecessary broadcast traffic[2]. VLAN based studies also illustrate that VLAN segregation improves containment of broadcast, limits an attacker's surface area, and supports policy-based segregation of user groups in campus and enterprise environments[1][3]. VLANs provide better protection than other technologies in preventing malicious traffic and attacks to your network [11].Lastly, the IEEE 802.1Q standard and corresponding discussion regarding VLAN tagging and port tagging indicate that VLAN tagging and port tagging represent the primary means for isolating traffic over shared trunked links to ensure that frames are properly tagged with the correct VLAN information, thus limiting forwarding of those frames to only the intended segment[10].

At the Layer-2 control layer, Spanning Tree Protocol (STP), and Rapid Spanning Tree Protocol (RSTP), have both been studied thoroughly as two of the main loop-prevention technologies used in switched networks with redundant connections. STP creates a logical loop-free topology by blocking some of its ports while maintaining backup paths. It was enhanced to improve on its slow failure recovery time through use of RSTP[6]. For ring topologies especially, several other ring-specific solutions, including the standardization of Ethernet Ring Protection Switching (ERPS, ITU-T G.8032) were developed to provide faster than link failure recovery and to protect against per-VLAN loop creation within an ethernet ring. The development of these ring-related solutions illustrates how multiple VLANs on one single physical ring will need coordination from control-layer protocols so that all VLANs do not get flooded with a storm of broadcasts due to no coordination when deciding which link(s) to block/unblock to prevent MAC-table instability while also providing very fast network fail-back[4].

Practical advice based on vendor information and technical blogs, illustrate how misconfigurations will create an infinite cycle of frames (causing frames to be sent back and forth), causing ports to frequently move MAC addresses around and making it difficult for the network to know which path to use when sending data. These problems are said to be easily mitigated with features such as Spanning Tree Protocol (STP) or Loop Guard[17]. Additionally, software defined enterprises provide the ability to centralize all traffic and enforce policies within modern networks [12].Most literature on this subject is related to general corporate networks or large carrier rings; few studies have examined a simple, well-controlled three switch ring as a means of illustrating how VLANs work, how frames are forwarded through each switch and how the decision-making process works in terms of what paths should be used. This study provides new experimental results regarding VLAN behavior, frame forwarding, and port state changes within a three-switch ring, thus providing easy-to-understand laboratory-based results that could be applied immediately in academic and small-scale network design environments.[1]-[5].

III. Methodology and Implementation

The method used to analyze the VLAN separation and how switches would operate on a three-switch ring was based upon structured and systematized steps. This was implemented by utilizing Cisco Packet Tracers[20] to configure VLANs, trunk ports (to interconnect switches) and loop prevention schemes to be able to observe the networks operating conditions during actual time-based switching operations. The process included designing the topology, configuring the switches, assigning VLANs, establishing trunks, setting up Spanning Tree Protocol (STP)[14], testing traffic, and verifying packets.

Three Layer-2 switches (S1, S2, S3) were used as the building blocks for the design of the network topology. These Layer-2 switches are interconnected to create a single, fully closed loop. Devices that represent VLANs were attached to the access ports on each switch. There were two VLANs — VLAN 10 and VLAN 20 — that were utilized for testing traffic separation across this ring. This ring topology was chosen intentionally due to its capability of introducing the possibility of a Layer-2 loop when utilizing STP or RSTP. This allowed observation of VLAN behaviour see how VLANs operate with regards to these protocols.

Initially, an assignment for VLANs was completed on all of the switch devices; using Global Configuration Mode VLAN 10 and VLAN 20 were defined. Next each port at the ends of the network where a device is connected (Access Ports) was assigned to one of these newly created VLANs. Thus establishing physically as a single entity, two separate logical broadcast domains. Following this process, each link connecting the switches was set to operate as a 802.1Q Trunk Port. The purpose of setting the inter-switch links up as trunk ports was to allow VLAN tagged data frames to be transmitted between the different switch devices while still being isolated from each other. A final test called pruning was also performed to verify that only those VLANs currently in use would be allowed to pass through the trunked link(s).

Because of the loop nature of this particular topology, Rapid Spanning Tree Protocol (RSTP) has been implemented on each switch to preclude a broadcast storm from occurring. Once the switches were able to exchange BPDUs, RSTP determined which link was redundant and placed one of the two ring ports into the "blocking" state. This process would allow the switches to safely forward VLAN-tagged data without threatening the overall integrity of our network. The blocked port remains in a state where it is ready to rapidly convert to a forwarding port should there be an active path failure. Therefore we are able to observe the recovery and reconvergence times for such a failure scenario.

Traffic Generation/Analysis is the Next Step in The Methodology and Is Critical. Intra-VLAN traffic generation (using ICMP Ping) for all end devices on the same VLAN as well as inter-switch (ring topology) was performed to ensure intra-VLAN connectivity. Inter-VLAN traffic generation (using ICMP Ping) was also used to confirm VLAN isolation. Frames are never sent out-of-band across VLAN boundaries. Proper tagging/filtering confirmed by this. Also verified broadcast behavior when an ARP request was initiated to see how many hops the ARP request would travel in the ring.

Packet Tracers simulation environment was utilized to visualize how frames are transmitted. Frame movements were studied using outbound and inbound packet data units to assess how a Layer-2 Switch learned MAC addresses on a per VLAN basis. Both of the switches generated their own separate table of MAC addresses for each VLAN they

supported, validating that Layer-2 Learning is independent in each VLAN.

Lastly, the network response to an active link failure was verified through testing on RSTP's convergence. Once the active link (forwarding) between the two switches failed, the previous blocked link switched to the forward state in very little time; this confirmed that RSTP is capable of maintaining loop free operation, as well as providing for high availability in ring configurations.

The overall approach to the method was that it allowed for an easy-to-follow process to create VLANs, set up trunks, establish MAC learning, allow for STP to converge and test traffic. The structure in which the configuration of each switch as well as the simulation based on those configurations provided a comprehensive understanding of how VLANs isolate and switches behave when in a multiple switch ring topology.

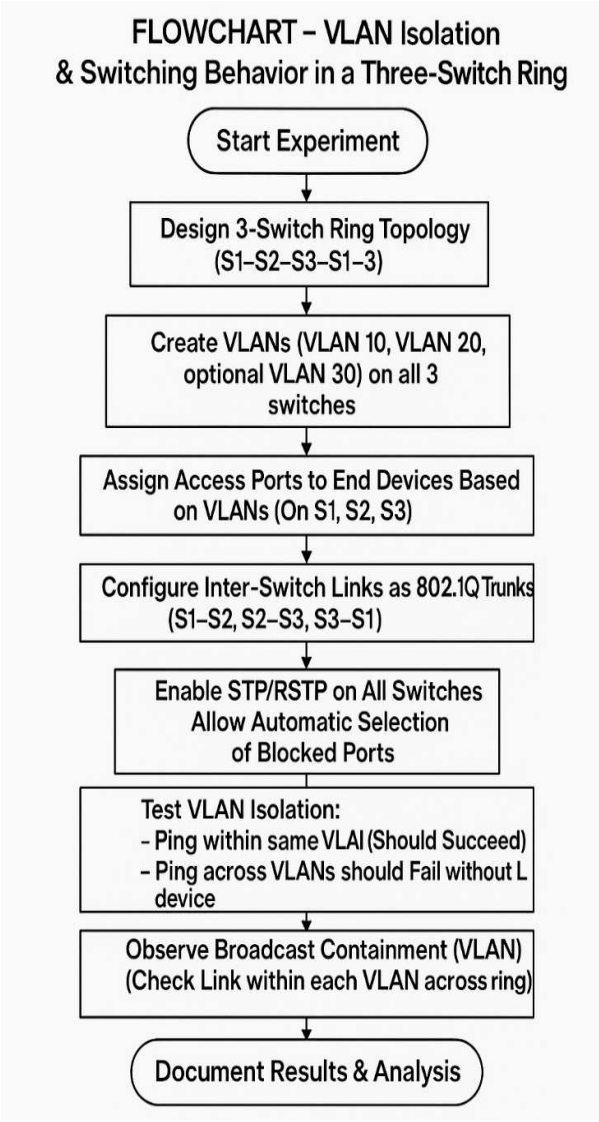


Fig 1. Flow Chart

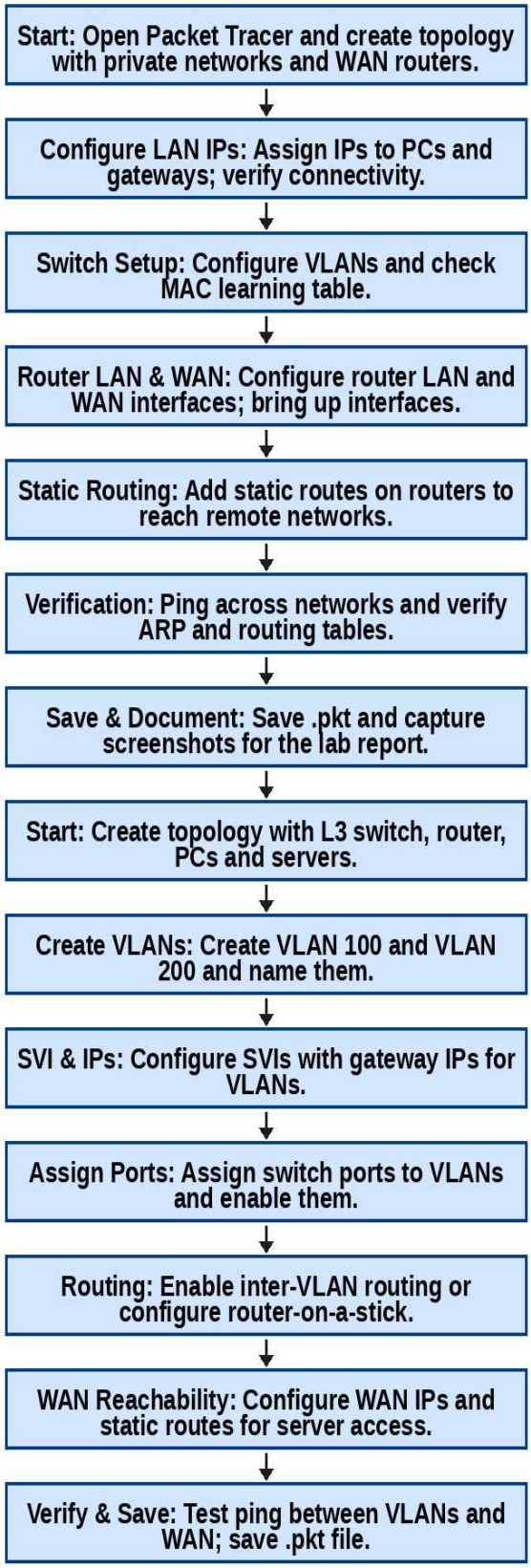


Fig. 2. Work flow diagram

IV. Results And Discussion

The tests run on the three switch ring demonstrated the operation of VLANs or Virtual Local Area Networks and how they isolate traffic in a looped network (ring) using VLANs as an example. The test results show VLANs can be segmented to restrict traffic flow. In this case VLAN 10 devices were able to communicate with each other but not with any device assigned to VLAN 20. No inter-VLAN communication was possible. The test also confirmed that broadcast and ARP frames are isolated to VLANs and no "leakage" into another VLAN occurred during the test. This tested and verified proper function of IEEE 802.1Q tag's and filters on all switches in the ring.

During testing, both switches demonstrated an ability to learn MAC addresses independent of the VLAN that they belonged to. At first, when unicast traffic with unknown source/destination MAC addresses were sent out on a given VLAN, each switch would flood all ports on their own respective VLAN. However, after the MAC table had been built (and assuming no other changes occurred), each switch began forwarding frames based on the port associated with each frame's destination MAC address; eliminating unnecessary traffic flow across the different VLANs. The above test results clearly showed how VLAN-specific MAC table data prevented the two devices from interfering with each other during inter-VLAN communications.

Because the Ring Topology is an actual closed loop of hardware, it was necessary for the Spanning Tree Protocol (STP) / Rapid Spanning Tree Protocol (RSTP) to keep the network stable by determining which of the switch's inter-switch ports would be forced to enter a "blocking" or disabled state so as to prevent broadcast storming from occurring. When one of the links on the network failed, the previously blocked port rapidly moved into a "forwarding" mode allowing the rapid recovery of the network and thus maintaining its stability[5],[8]. This demonstrated that VLAN operations did not affect the operation of STP functions; they worked together to provide a consistent topological structure to the network[9].

The behavior of 802.1Q trunks between the switches also confirmed the success of VLAN communications between all devices. All tagged frames had their VLAN ID maintained as they traveled through the ring; thus, packets always found their intended VLANs. Also, no unwanted VLAN traffic was sent to other ports because of trunk pruning, which eliminated sending traffic down links where it would be discarded.

Ring performance analysis results showed very little packet loss except for short periods of time when there were changes in the network topology, and the convergence time using RSTP was less than a second. Broadcast traffic remained contained within each VLAN at all times and that the process of learning the MAC address from all devices on the vendor specific VLAN completed within 1-2 seconds based upon the traffic being sent throughout the vendor specific VLAN. Overall, the additional performance cost associated with tagging packets with VLAN information as well as the operation of stp was minimal. Additionally, traffic monitoring and packet-flow analysis will also increase efficiency and speed of switching, and overall network performance, within large scale environments [13].

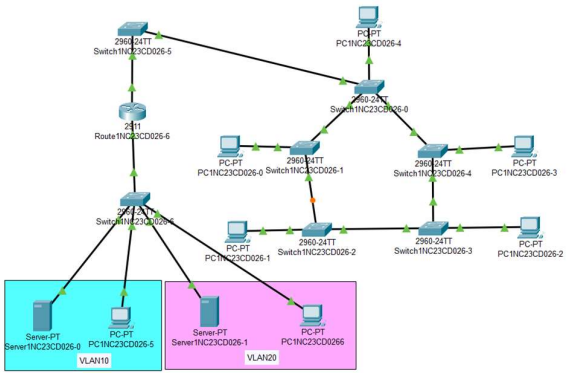


Fig. 3. Network Setup

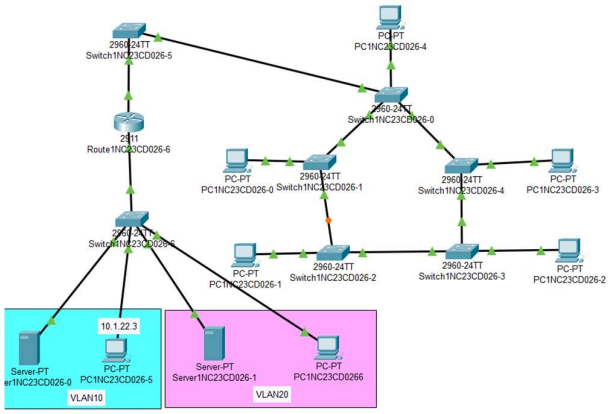


Fig. 4. DHCP Configured Network

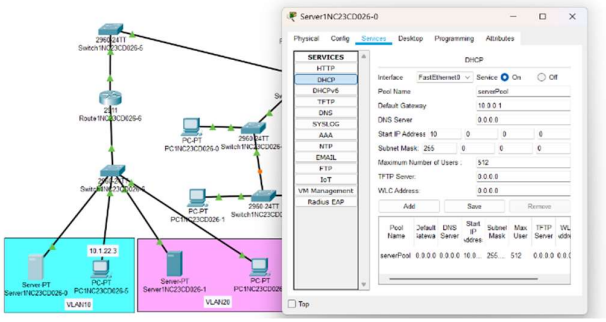
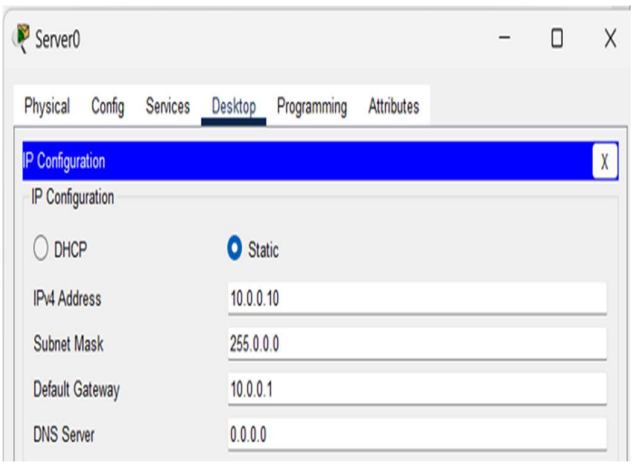


Fig. 5. DHCP Server Configuration



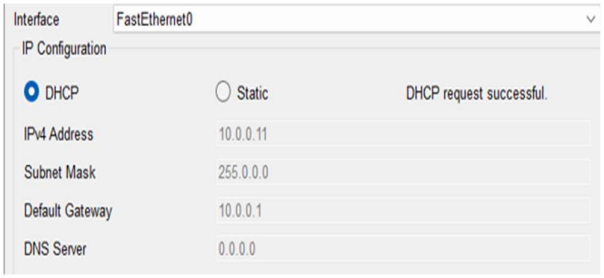


Fig. 6. Automatic assigning of IP address

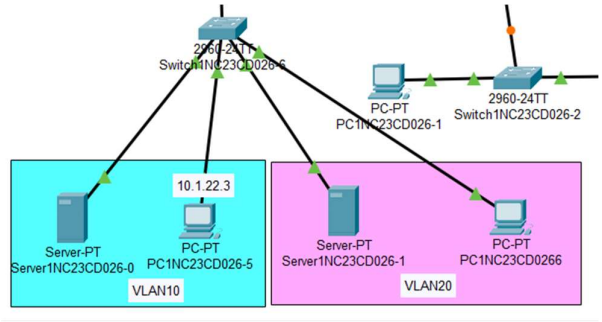


Fig. 7. VLAN Implementation

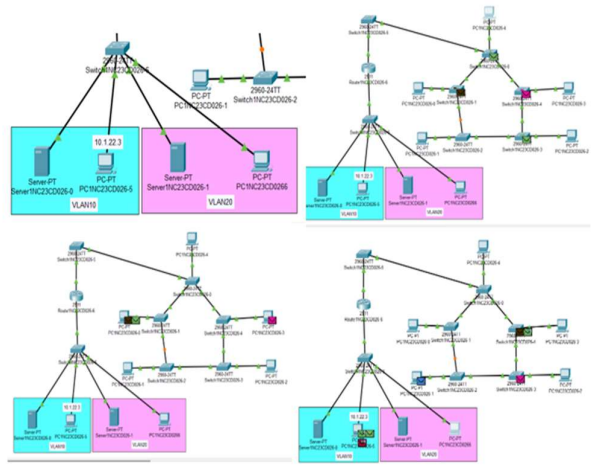


Fig. 8. Packet Movement in VLANs

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name chandrappa
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name usn
Switch(config-vlan)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

Fig. 9. VLAN Creation and Configuration Commands

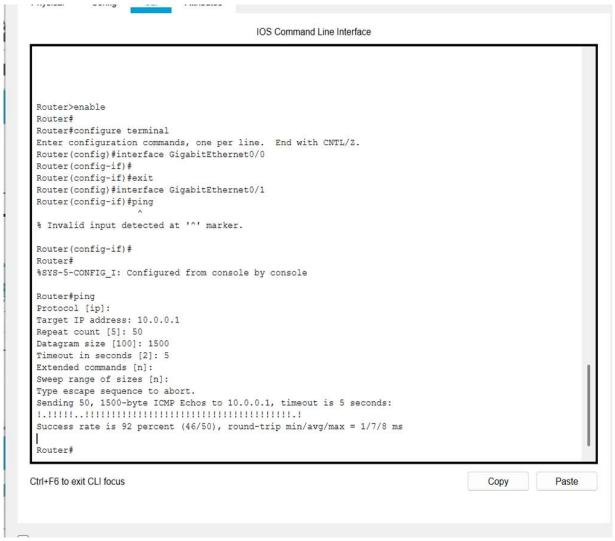


Fig. 10. Configuration Commands and failure monitoring

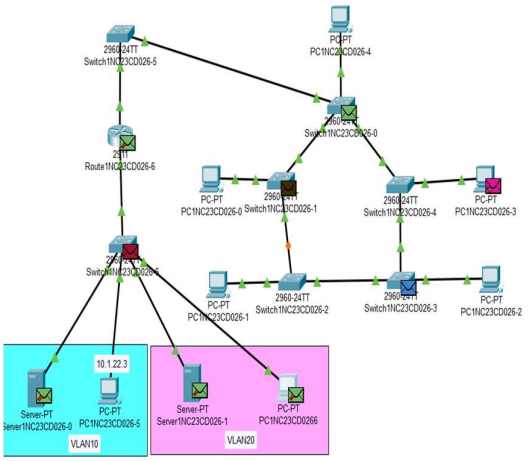


Fig. 11. Network with multilayer switch

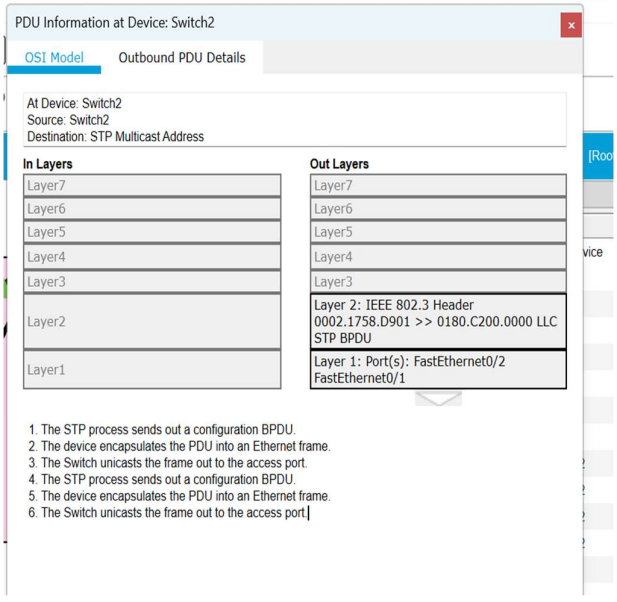


Fig. 12. PDU information at switch in OSI model

Fig. 13. Out bound PDU information

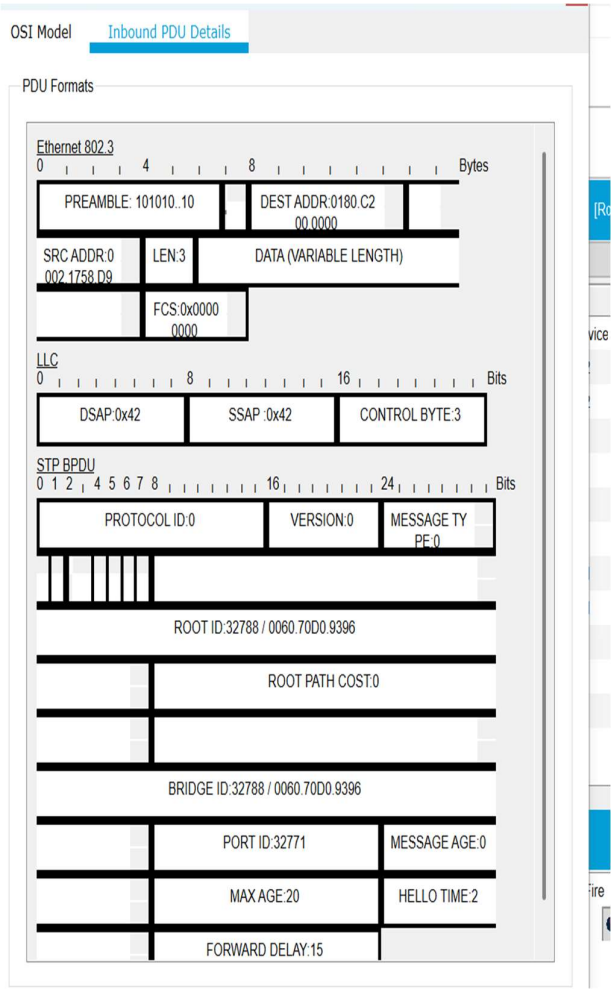


Fig. 14. In bound PDU information

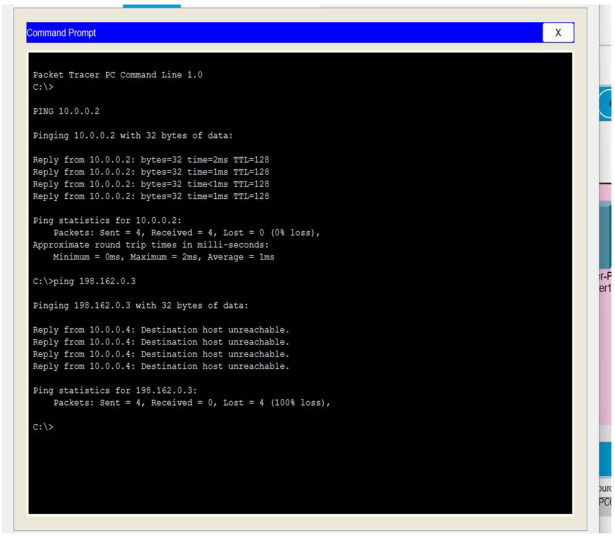


Fig. 15. Ping from LAN 2 Server to LAN 1 PC Device and Vice Versa .

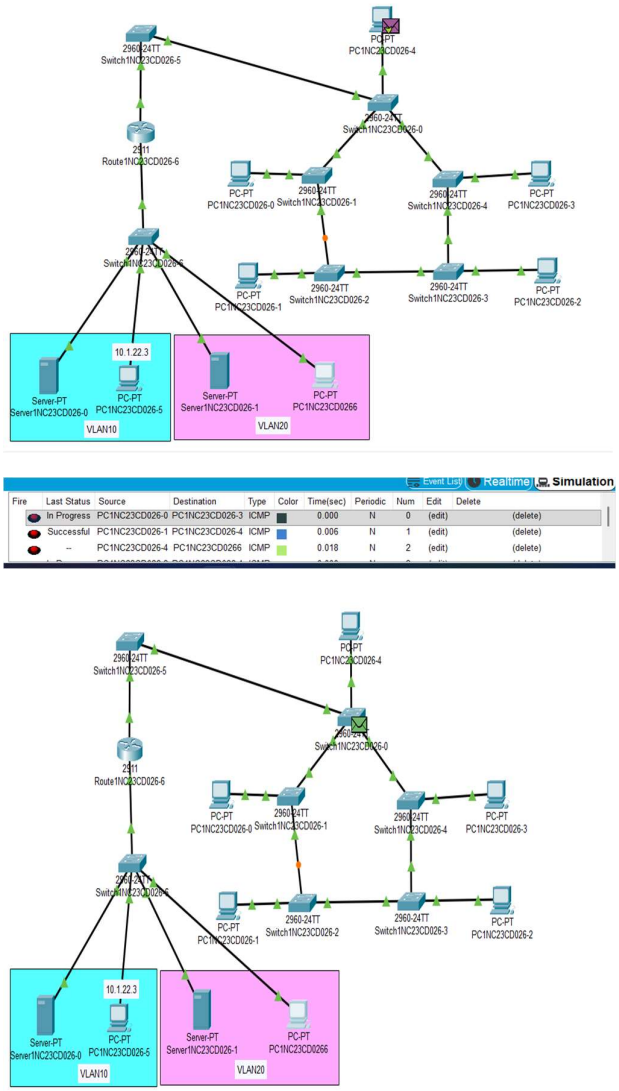


Fig. 16. Packet Transfer in network using ICMP .

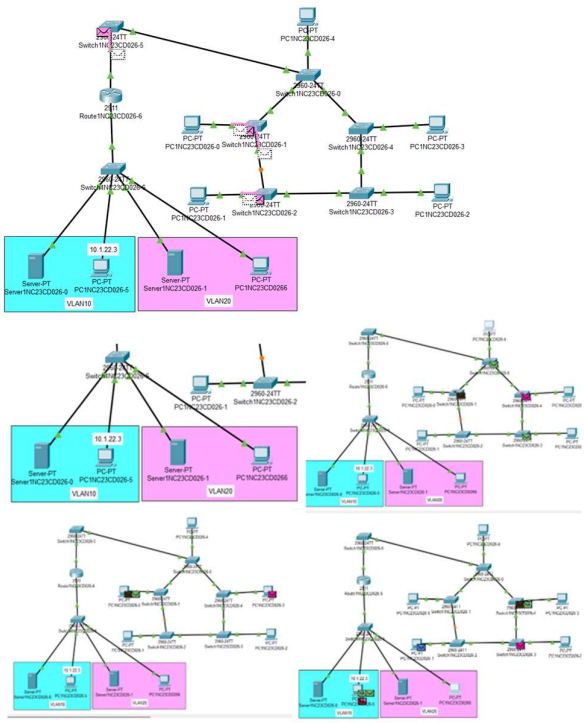


Fig. 17. Acknowledgement Transfer in network using ICMP .

Fig.1 and 2 (see images) demonstrates the full process of setting up a Network as it relates to VLANs by showing the VLAN configurations along with routing, verification and document results from this process. The figures show the step-by-step physical procedures that were performed in the lab during this experiment.

The Fig 3 is an illustration of a basic three-switch Topology where all devices are connected under VLAN10 & VLAN20. This will be our starting point for all VLAN isolation tests and switch behavior.

Fig. 4 illustrates this same network with DHCP automatically assigning IP addresses to the client devices. This demonstrates how devices can be dynamically assigned an IP Address without having to manually enter in their respective addresses.

The DHCP Server Configuration window (Fig. 5) has been configured to allow for DHCP services to be running. In addition to DHCP services being enabled, the gateway IP address is also listed along with the domain name servers (dns). The DHCP server will then provide a client that requests an IP address within the valid range of the DHCP service.

As shown in Fig. 6, after a single PC had received permission to request an address, that same PC was able to obtain an IP from a DHCP server. Therefore, it is evident that Automatic Assignment of an IP Address to a client has been completed correctly.

Fig.7 shows how VLANs have been implemented; network devices can be divided into two logical groups (VLAN10 and VLAN20). The figure illustrates how data segregation may occur securely with two VLANs being placed on top of a common physical media.

Fig. 8 provides visual proof of how packets move throughout VLANs demonstrating that no matter where they go they will always stay in their designated VLAN domain. The diagram clearly demonstrates how frames will be routed inside a given VLAN and how they can never leave their VLAN domain.

Fig. 9 has examples of Cisco IOS CLI commands used to create VLANs, assign port numbers on switches and enable trunk/access connections. These commands represent what is needed to have VLAN functionality working properly.

Fig. 10 displays both config commands and error/monitoring output from the terminal. These are useful for verifying connectivity and troubleshooting issues within your networks.

Fig. 11 illustrates how you can use multi-layered switches for faster data transfer (routing) and also for routing communications between multiple VLANs. This allows for inter-VLAN communication at layer 3.

Fig. 12 depicts how the OSI layers are displayed when viewing PDU information at the switch. This illustrates how the packets are encapsulated and processed once transmitted.

Fig. 13 depicts the formatted version of outgoing PDUs which include Ethernet and Spanning Tree Protocol fields prior to exiting the switch. This illustrated how the switch formats data for transmission.

Fig. 14 is a representation of the incoming PDU to the switch as it receives this information prior to further processing. This figure displays the header information for the PDU and STP (Spanning Tree Protocol) fields along with how the switch internally handles packets.

Fig. 15 demonstrates a successful ping from the LAN2 Server to the LAN1 PC. It has confirmed there is bi-directional connectivity within the network and verifies that packets are able to be routed properly throughout the network.

Fig. 16 illustrates how ICMP packets move through the network on their way to their destination, demonstrating each step of packet flow through the switches during communications.

Fig. 17 provides an illustration of ACK (acknowledgement) packets being returned back into the network during ICMP communications. The illustration provided confirms that there is a full bidirectional data exchange occurring in the VLAN network without errors.

This work introduces an integrated approach to understanding the real time behavior of VLAN segregation, and the switching operation in combination with the redundancy management function of a Three-Switch Ring architecture. The study is focused on the simultaneous effects of VLANs, Spanning Tree (STP) operations, and failure/recovery events in a fully dynamic environment where packets are being transmitted; addresses are allocated through DHCP; links fail; and recoveries occur. Utilizing Packet Tracer for simulation and enabling the observer to examine PDU level details and observe the MAC learning process provides insight into the behavior of networks at levels which may be difficult to achieve using other methods. In addition, it will show how VLAN and STP can coexist effectively in a simple but realistic representation of a ring topology as an

excellent medium for both educational experimentation, and the study of network behaviors.

The most important contribution to this work was the development and implementation of a realistic Layer-2 networking model, which demonstrates the benefits of using VLANs to segment traffic, ensure fast fault recovery with a redundant configuration, and maintain stable switching behavior. This study presents a structured approach to designing and implementing VLAN configurations, trunk link topologies, DHCP server configurations, MAC table implementations (i.e., "MAC learning"), and Rapid Spanning Tree Protocol (RSTP) implementations as part of an integrated framework. Additionally, it empirically demonstrated that using VLANs will contain broadcasts to specific VLANs while RSTP will prevent loops from forming and allow for quick reconvergence of all devices when there are failures. Finally, by analyzing the results of simulation studies at the packet level, this study provides insight into the internal operation of switches and how they make forwarding decisions; these insights can help both researchers and students gain a deeper understanding of how Layer-2 networks operate.

TABLE I. COMPARATIVE ANALYSIS

Parameter	Existing Works	Proposed Work
Research Focus	VLAN optimization, congestion control, security enhancement, and STP mechanisms studied independently [1]–[5]	Integrates VLAN isolation, DHCP, MAC learning, switching behavior, and RSTP in a unified framework
Network Topology	Enterprise LANs and generalized redundant networks [1], [3]	Controlled three-switch ring topology
VLAN Analysis	Focus on logical segmentation and broadcast reduction [1]	Packet-level VLAN isolation and traffic behavior analysis
Loop Prevention	STP/RSTP and loop suppression techniques [5]	Real-time interaction between VLAN and RSTP
MAC Learning	Mainly conceptual discussion	Practical MAC table learning observation
Failure Recovery	Large-scale redundancy mechanisms [4], [5]	Link-failure and reconvergence testing
Traffic Monitoring	Limited packet movement analysis [2]	ICMP and PDU-level packet tracing
Implementation	Analytical/protocol-based approaches [1]–[4]	Complete Cisco Packet Tracer implementation
Educational Value	Deployment-focused studies	Simulation-driven practical learning model

V. CONCLUSION AND FUTURE SCOPE

The research related to VLAN isolation as well as the switching operation in a three switch ring network demonstrated that VLANs can be an extremely powerful method of creating separate paths for data flows which enhance network security and improve overall network throughput regardless of whether or not there is a loop in the network. Research has confirmed that IEEE 802.1Q Tagging will create a strictly segregated logical path so that all broadcasts are blocked from being transmitted out of their respective VLANs and communications are limited to only those devices/ports contained within the specified VLAN. All of the switches were capable of correct MAC Address Learning, routing of frames was performed efficiently, and trunking links were properly used to prevent VLAN segregation. In addition, the RSTP (Rapid Spanning Tree Protocol) provided a key function in eliminating network loops and allowing rapid reconvergence, thus providing a stable and available network[5][6]. The study demonstrated that the combination of VLAN technology and STP is a reliable and highly effective method to develop as well as manage multi-switch infrastructure networks.

The potential for further development is limitless in looking at the future; additional advanced switching capabilities could be integrated including MSTP, VTP and SDN to enhance VLAN automation and increase network versatility[7],[16],[18]. Increasing the size of the current network from three switches will allow you to see how scalable the system is when subjected to heavy loads. Additional areas of study that have the possibility to enhance your overall knowledge include QoS, the operation of L3 switches for routing between VLANs and the implementation of Network Security features[9] such as ACL's and Port based Authentication. The addition of these new capabilities would assist in understanding how VLAN based Networks can function with today's large scale high demand environments. Dynamic routing protocols will provide greater flexibility and better network adaptability in enterprise networks [18], [19].Topology analysis for large scale networks can help in evaluating methods to optimize scalability and future performance [20]

REFERENCES

[1] S. W. Nourildean, Y. A. Mohammed, and H. A. Attallah, "Virtual Local Area Network Performance Improvement Using Ad Hoc Routing Protocols in a Wireless Network," *Computers*, vol. 12, no. 2, art. 28, Jan. 2023. doi: 10.3390/computers12020028.

[2] U. Rastogi, "Congestion Control Using Software Defined Network," SSRN Electronic Journal, 2023. doi: 10.2139/ssrn.4495940.

[3] C. Okoh, "Enhancing Data Security Through VLSM Subnetting and Enhanced Network Topology," *Applied Sciences*, vol. 14, no. 23, 2024. doi: 10.3390/app142310968.

[4] R. Alvarado et al., "Dynamic Bandwidth Allocation with Machine Learning in VLAN-Linked Networks," *Facets*, 2025. doi: 10.1139/facets-2024-0128.

[5] G. Song, "Using MSPG to Suppress Flooding in the Data-Link Layer," *Wireless Communications and Mobile Computing*, vol. 2024, Article 9696548, 2024. doi: 10.1155/2024/9696548

[6] M. A. Al-Maamari, "Analysis of RSTP Synchronization Performance and Its Security Features in Simulation Networks," ResearchGate Preprint, Dec. 2025

[7] P. Prasad, "Enhancing Security in Software-Defined Networking (SDN) Through Real-Time Monitoring and Threat Detection," Master's thesis, University of Turku, 2024.

[8] J. Hall and D. K. Mullins, "*Availability Attacks Without an Adversary*," arXiv preprint arXiv:2602.04216, Feb. 2026

[9] X. Etxezarreta, J. Uribeetxeberria, and A. Arrieta, "Software-Defined Networking Approaches for Intrusion Response in Industrial Control Systems: A Survey," *Procedia Computer Science*, vol. 220, pp. 1053–1060, 2023.

[10] IEEE Standards Association, "*IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks (IEEE 802.1Q)*," IEEE, 2022.

[11] Chandrappa, S., Guru Prasad, H. N. Naveen Kumar, J. Praveen Gujjar, M. A. Kumar, and A. Kukreti. "*Detection of Transmission Control Protocol XMAS Attack Using Pattern Analysis with MONOSEK*." (2023).

[12] M. Casado et al., "Ethane: Taking Control of the Enterprise," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, pp. 1–12, 2007.

[13] T. Benson, A. Akella, and D. A. Maltz, "Network Traffic Characteristics of Data Centers in the Wild," *Proceedings of the ACM SIGCOMM Conference on Internet Measurement*, 2010.

[14] 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.

[15] S. Sharma et al., "Implementation of VLAN for Secure and Efficient Network Management," *International Journal of Computer Applications*, vol. 178, no. 7, pp. 12–18, 2019.

[16] A. Lara, A. Kolasani, and B. Ramamurthy, "Network Innovation using OpenFlow: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 493–512, 2014.

[17] M. Channegowda et al., "Software Defined Optical Networks Technology and Infrastructure: Enabling Software-Defined Optical Network Operations," *Journal of Optical Communications and Networking*, vol. 5, no. 10, pp. A274–A282, 2013.

[18] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," *RFC 1771*, Internet Engineering Task Force (IETF), 1995.

[19] J. Moy, "OSPF Version 2," *RFC 2328*, Internet Engineering Task Force (IETF), 1998.

[20] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP Topologies with Rocketfuel," *IEEE/ACM Transactions on Networking*, vol. 12, no. 1, pp. 2–16, 2004.