Current Journal of Applied Science and Technology

Volume 42, Issue 2, Page 43-51, 2023; Article no.CJAST.95226
ISSN: 2457-1024
(Past name: British Journal of Applied Science & Technology, Past ISSN: 2231-0843, NLM ID: 101664541)

Technical Supplement for Network Control

Omamoke Layefa [a*], Japheth Bunakiye Richard [b], Egbure, John Yinembele [a] and Ofualagba Mamuyovwi Helen [c]

[a] Department of Mathematics/ Computer Science, Faculty of Basic and Applied Sciences, University of Africa, Toru-orua, Sagbama, Bayelsa State, Nigeria.
[b] Department of Mathematics/ Computer Science, Faculty of Sciences, Niger Delta University, Amassoma, Bayelsa State, Nigeria.
[c] Department of Computer Science, Delta State Polytechnic Otefe-Oghara, Delta State, Nigeria.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/CJAST/2023/v42i24055

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/95226

Original Research Article

Received: 10/11/2022
Accepted: 16/01/2023
Published: 16/02/2023

ABSTRACT

Networking in computer science is the connection of two or more computers electronically with the sole aim of data or peripheral sharing. As the computers and peripherals connected to a network increases, using routers and switches alone is no longer reliable to contain broadcast traffic. Therefore this research employed VLAN technology to improve the performance of an extended star network topology by dividing a single switching network into a number of overlaying virtual networks called VLANs that can accommodate various functionalities, security needs and easy administration. For Inter-VLAN routing, a layer 3 switch that support 802.1Q trunking on a fast Ethernet or GigabitEthernet interface was used. This study is conducted using a white-box approach and the waterfall methodology to design, simulate and compare. After configuration, it was seen that the presence of failure in the main network is abstracted from the network users as the VLANS is configured logically to access and share resource with systems on all blocks. Subsequently, A ring

**Corresponding author: E-mail: layefa.ekereke@uat.edu.ng;*

topology can be introduced to the system were each block will have a backup switch and can serve as a backup for the block nearest to it. Also a Dual ISP can be introduced to provide steady internet access.

Keywords: VLAN; Router; Switch; Star Topology; IP address.

1. INTRODUCTION

Computer Network can be seen as the connection of two or more computers electronically with the sole aim of data, information or peripheral sharing. There are numerous advantages of networking of computers, they include performance efficiency, data/information manageability, security and cost effectiveness as it enables resource sharing between users not necessarily within a visible space [1]. Switches and Router are devices used to enable data transfer from one place to another using different technology such as a radio waves or wire.

A Local Area Network (LAN) is a network of computers located within a virtually accessible space or single broadcast domain or within a short distance usually at home, offices buildings or school. WAN is a network that covers wider area than LAN and usually covers cities, countries and the whole world. Several major LAN can be connected together to form a WAN [2-5]. As several devices can be connected to a network, it is important to ensure that data does not collide at some point when this device attempt to use data channel simultaneously. William [6] used a set of rules called carrier sense multiple access/collision detector to detect and prevent data collision in networks. Also Andrew [7] developed Virtual Local Area Networks (VLANs) as an improved solution to using routers to contain broadcast traffic.

According to Kattepur et al. [8] Virtual local area network (VLANs) is the process of partitioning a single physical LAN into smaller logical LANs, VLAN reduces the broadcast domain, improve security and performance and are ideal for separating and managing large networks. A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment [9-11]. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging [12-14].

VLANs are able to be created and packets are easily moved through those VLANs with the help of trunk port, a trunk port is a port configured on a network switch that allows data to flow across a network node for multiple virtual local area networks [15,16].

Some random issues averagely faced in network here in University of Africa include;

1. Physical connectivity issues
2. Duplicate static IPs
3. Configuration conflicts
4. Destruction of Fibre cables due to on-going construction
5. Faulty patch cords
6. Device failure e.g. switch

Based on recent happening and observations (January to June, 2022) on university of Africa network set-up, we observation that in an average monthly base, at least a node in the network must experience a downtime either due to switch failure, configuration issues or breakage in the internal lines connecting to the node. And until this node is traced and issue treated, the network supply to all computers attached to such node will be down. This calls for a more efficient network model necessary to enable sharing of information across clients/offices.

1.1 Aim

The purpose of this research is to develop an advanced star network topology by Configuring a VLANs supplement on different switches within the network to reduce network downtime, reduce bridge in data communication and add security measures to increase network/data security.

1.2 Objectives

To achieve the above stated aim, extra lines will be added to the existing lines running through

each node and firewall will be added to the entire network as a protective measure against cyber-attacks and unauthorized persons and this will mitigate the frequently experienced problems mentioned across the network to the barest minimum.

2. REVIEWED LITERATURES

According to Huchao et al. [17], Network topology is the description of the arrangement of nodes (e.g. networking switches and routers) and connections in a network is often represented as a graph. No matter how identical two organizations are, no two networks look exactly the same. Network topologies outline how devices are connected together and how data is transmitted from one node to another.

A Logical network topology is a conceptual representation of how devices operate at particular layers of abstraction. Logical topology basically describes the configuration aspect of any topology, how the IP addresses are assigned, how data is expected to move from one device to another, how trunk port, access port VLANs are assigned on a network while A Physical topology details how devices are physically connected [18,19]. The different types of topologies that enterprise networks have built on today include; Bus topology, Ring topology, Star topology, Mesh topology, and Tree topology. Hybrid topology includes merging two or more network topology for greater efficiency.

VLANs is an acronym for Virtual local area networks, VLANs are becoming very important as network complexity has exceeded the capacity of a typical local area networks (LAN) [20]. In essence, a VLAN is a collection of devices or network nodes that communicate with one another as if they made up a single LAN, when in reality they exist in one or several LAN segments. In a technical sense, a segment is separated from the rest of the LAN by a bridge, router, or switch, and is typically used for a particular department [21-24]. This means that when a workstation broadcasts packets, they reach all other workstations on the VLAN but none outside it. Types of VLAN includes; Port-Based VLAN, Protocol based VLAN and MAC Based VLAN.

VLANs reduce the incidence of collisions and decrease the number of network resources wasted by acting as LAN segments. Data packets sent from a workstation in a segment are transferred by a bridge or switch, which will not forward collisions but will send on broadcasts to every network devices. For this reason, segments are called “collision domains” because they contain collisions within the bounds of that section. However, VLANs have more functionality than even a LAN segment because they allow for increased data security and logical partition. Remember, a VLAN acts as a single LAN although it only makes up a segment. This means that the broadcast domain of a VLAN is the VLAN itself, rather than each network segment. Additionally, the partitions do not have to be defined by the physical location of the network devices. They can be grouped instead by department, project team, or any other logical organizational principle [25].

VLAN provides the following advantages:

1. Solve broadcast problem
2. Reduce the size of broadcast domains
3. Allow user to add additional layer of security
4. Make device management easier
5. Allow us to implement the logical grouping of devices by function instead of location

Al-Hamiri, et al [26] did a simulation that show that VLAN overcome LAN networks in terms of bandwidth and security. This has been done by reducing the throughput in both sending and receiving levels to the confidential servers. The VLAN has also reduced the broadcast domain which results in a high-power efficiency. Moreover, the VLAN network technology has been proved to have lower values of delay in transferring files and packets than LAN network technology.

Modern technology is essential for all healthy, economic, and educational sectors. Using modern technology involves high-performance networks in terms of Quality of Services (QoS) parameters such as delay, throughput, bandwidth, response time and security.

There are five (5) basic VLAN types:

1. The Port base allows network administrators to manually designate VLANs for each switch port without the need to frequently update the network infrastructure.
2. Mac address-based VLAN assigns VLANs depending on the source MAC addresses of the packets. The Security and adaptability of network administrator would not have to update the configuration of

VLANs even if the users regularly move their physical location

3. IP subnet-based VLANs can be assigned to devices based on their IP subnets using IP subnet-based VLAN. It will function well for a public network when there is a larger need for mobility, simpler management, and less of a need for security. When a user's IP changes, this technology enables them to automatically join a new VLAN ID.
4. Protocol-based VLAN can assign VLANs in accordance with the protocol types and frame encapsulation formats when used for a network with several protocols.
5. Policy-based VLAN can combine policies, such as combinations of MAC addresses and IP addresses can be used to assign VLANs. Network security and flexibility will be significantly improved through the combination of rules to provide inter-VLAN access control.

The need for inter-VLAN routing became paramount since broadcast packets are limited in the same VLAN, host in different VLANs are unable to directly communicate with each other in layer 2. Connections can be done with a router with each VLAN needing one physical port, sadly because of the high cost and poor scalability this type of routing is rarely used. It is called inter-vlan routing with separate physical interfaces.

Router on the stick is done using one physical interface to achieve traffic forwarding between VLANs using this type of VLAN routing. The router can receive frames with VLAN tags on the trunk interface from the connected switch after configuring the connection between the two devices as a trunk link. The router can then pass the routed packets out to destinations with VLAN tags over the same interface.

3. DESIGN AND SIMULATION

3.1 Methodology Used

In this research we present a study characterizing VLAN usage in a large-sized network like campus or enterprise (Table 1). Our study is conducted using a white-box approach, involving data such as router configuration, files obtained from network operators, and through interactive interactions with them. Our study also uses the waterfall methodology to design, simulate and compare the new developed VLAN aided network topology with the existing non VLAN network.

3.2 Design and Simulation

Packet tracer was used as a network simulator for the entire project, Micro soft word was used for documentation of the work, , line VTY 0-4 is a virtual port used to get Telnet or SSH access to the device, DHCP POOL is a built in server that automatically assigns IP address to devices connected to it, Service Set Identifier (SSID), IP Network Address Translator (IP NAT) that enables unregistered IP addresses to connect to the internet and one on one interview/discussion was done to get information about the current network architecture used.

The current University of Africa network examined used an extended star topology which connects two different campuses together, the network architecture allows these two campuses to be connected on same network but separated by VLANs, VLAN where used to segment the entire network which makes it easier to manage. All VLANs are added to a trunk port which manages the VLANS, every host or client on the network belongs to a particular VLAN and all hosts on the network is connected to a central manageable switch.

As seen in Fig. 1, each block has a single line running through it which potentially renders the line useless peradventure something happens to that line and there is no security technology embedded into the network. The system only uses VLANS for information sharing and network management issues arising from time to time. Hence the entire network is not secured, not fault tolerable as failure by any line causes a halt in internet supply to computers connected to that switch.

The VLANs enhanced network is an improved version of the existing system, It is focused mainly on security, network control and using VLANS to serve as redundancy in case of network failure in any block in the campus, it also has extra fiber optic lines running to all main blocks (switches) which will serve as backup peradventure any line fails. Port based VLAN was used in the configuration process of the separate VLANs.

Fig. 2, shows fibre optic lines added to each of the previously existing lines which will serve as backup lines for internet access.

Fig. 3, show all configured VLANS and IP addresses assigned to each VLAN on the new system.

Table 1. Logical configuration of new system/design

S/N	VLAN name	Address	Gateway	IP Range
5	Block A	192.168.5.0/24	192.168.5.1	192.168.5.1-192.168.5.254
6	Block B	192.168.6.0/24	192.168.6.1	192.168.6.1-192.168.5.254
7	Block C	192.168.7.0/24	192.168.7.1	192.168.7.1-192.168.5.254
8	ICT HUB	192.168.8.0/24	192.168.8.1	192.168.8.1-192.168.5.254
9	ICT	192.168.9.0/24	192.168.9.1	192.168.9.1-192.168.5.254
10	LAB	192.168.10.0/24	192.168.10.1	192.168.10.1-192.168.5.254
11	BURSARY	192.168.11.0/24	192.168.11.1	192.168.11.1-192.168.5.254
12	LIBRARY	192.168.12.0/24	192.168.12.1	192.168.12.1-192.168.5.254
13	HOSTEL	172.16.13.0/22	192.168.13.1	192.168.13.1-192.168.5.1022
14	CAMERA	192.168.14.0/24	192.168.14.1	192.168.14.1-192.168.5.254
15	UAT WIFI	172.16.15.0/22	172.16.15.1	172.16.15.1-172.16.15.1022
16	JAMB CBT	172.16.16.0/23	172.16.16.1	172.16.16.1-172.16.16.508
17	SERVERS	192.168.17.0/24	192.168.17.1	192.168.17.1-192.168.17.254

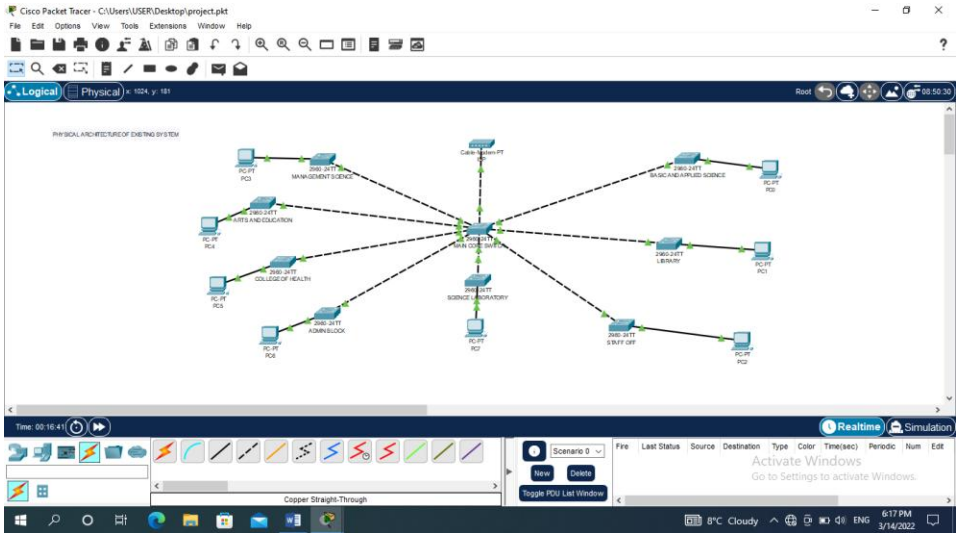

Fig. 1. Physical architecture of University of Africa network topology

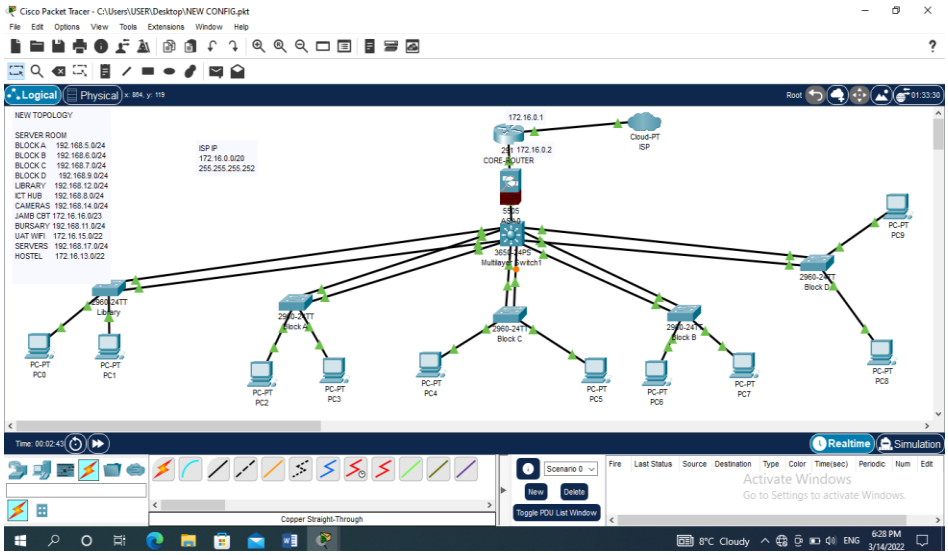

Fig. 2. Physical architecture of VLANs enhanced network

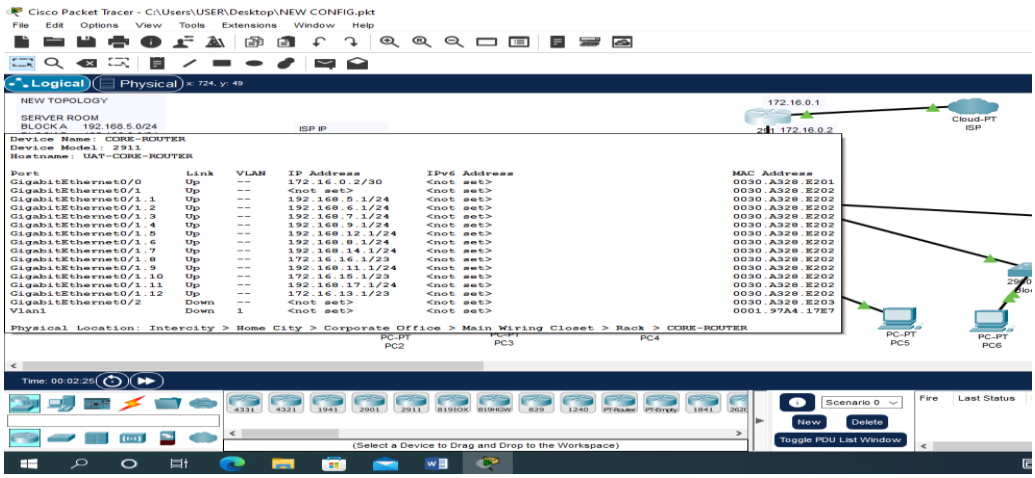

Fig. 3. Shows a run-down of all VIANS configured on the VLANs enhanced network

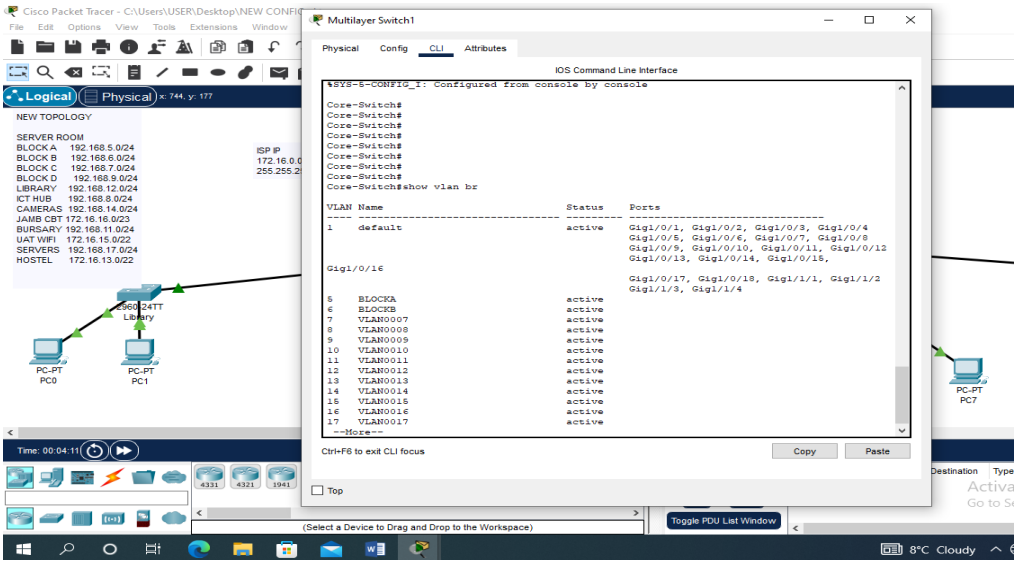

Fig. 4. Shows VLANS on the core switch

Fig. 4 shows all VLANS on the main core manageable switch.

Fig. 5 shows two different VLANS configured on same switch. VLANS were improved upon to facilitate access right to some essential units that have their own servers. Fig. 6 shows a Successful Communicating between two computers on same VLAN but not on same place.

4. DISCUSSION

a. Fibre optic lines were added to each of the previously existing lines which will serve as backup lines, as seen in Fig. 2. The network users are not aware of any network failure (abstraction), data sharing, internet access and peripheral sharing continues via VLAN. Only the network administrator is aware of the network failure and tries to fix the issue.

b. VLANS were improved upon to facilitate access right to some essential units that have their own servers. As seen in Fig 5 VLAN 12 belongs to library, FAST ETERNET PORT 2 was configured so as to communicate with any client that have access to that port on VLAN 12S. VLANS was also improved upon to serve as backup for internet access.

c. The firewall serves as a protective measure against any unauthorized access and various cyber-attacks like malware, ransom ware etc. it is strategically placed immediately after the main router because, any request or packets coming in and going out of the network must pass through the firewall as shown in Fig. 2.

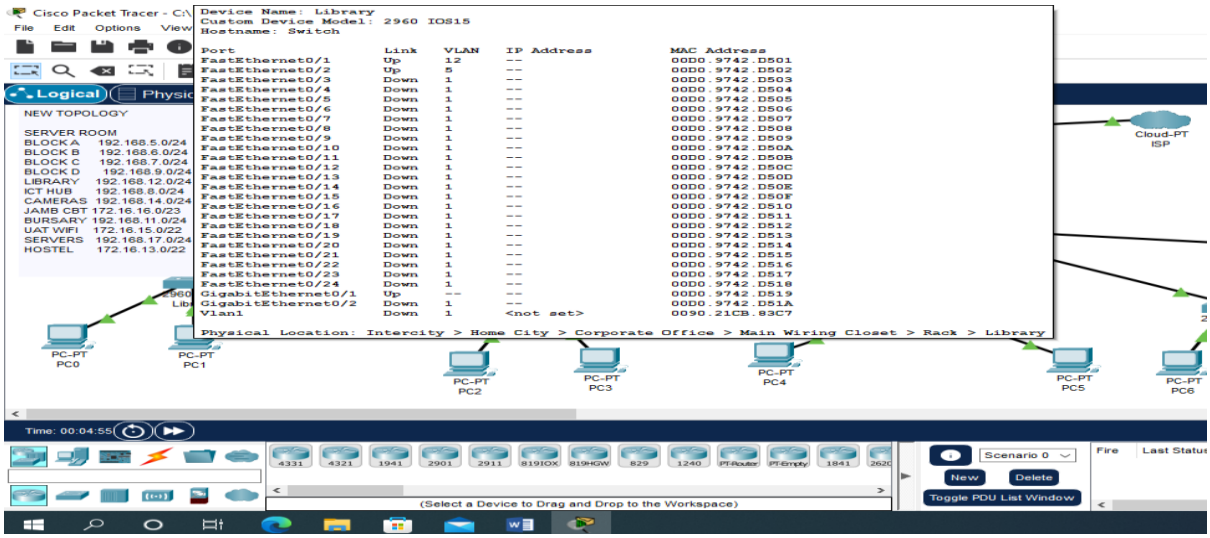

Fig. 5. Shows two separate VLANS being configured on one switch

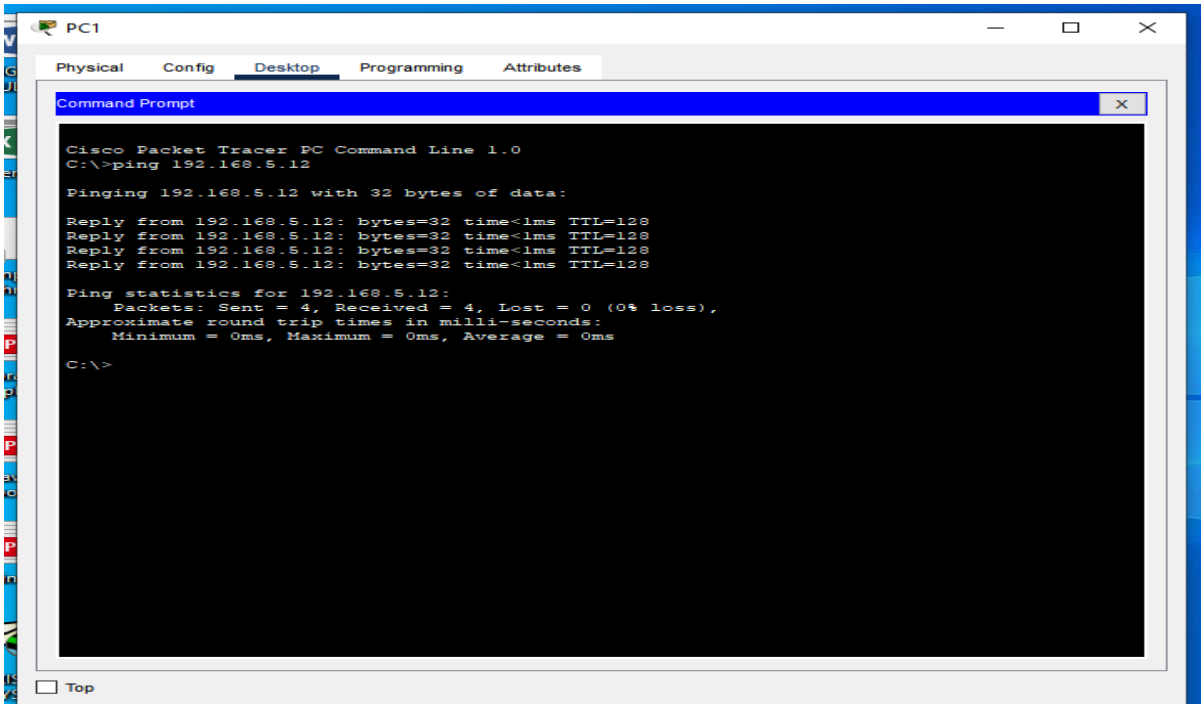

Fig. 6. Successful status of two systems communicating with each other on same VLAN physically apart

5. CONCLUSION

VLANs and trunks played a vital role in improving the efficiency and security of an enterprise network. When properly utilized, VLANs and trunks provide flexibility as seen in Fig. 3, all VLANS that are configured on the new system, stability, and ease of troubleshooting. it enabled resource sharing as seen in Fig. 4 in the presence of failure in the main network, 2 VLANS are configured on the library core switch VLAN 5 belongs to Block A while VLAN 12 belongs to Library, for the of resource sharing a system physically connected on the Library switch is configured logically to access and share resource with systems on block A because they are on same VLAN.

6. FUTURE WORK

A ring topology can be introduced to this system were each block will have a backup switch and

can serve as a backup for the block nearest to it. Also a Dual ISP can be introduced to provide steady internet access.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Grant TJ. Network topology in command and control. Advances in Information Security, Privacy, and Ethics. IGI Global. 2014:228-250.
2. Fatta G. Presti G, Lo Re G. Computer network topologies: Models and generation tools; 2022.
3. Fu Wei, Lu Ai. VLAN technology application research based on campus network security. Applied Mechanics and Materials. 2012:220-223.
   Available:www.scientific.net/AMM.220-223.2945
4. Groth D, Toby S. Network+ study guide, Fourth Edition. Sybex Inc; 2005.
   ISBN 0-7821-4406-3
5. Garimella P. Yu-Wei S, Nan Z, Rao S. Characterization study of VLANs in a campus network; 2022.
6. William Stallings. Data and computer communications". Prentice Hall PTR, Pearson Education, (Eighth Edition); 2010.
7. Andrew S. Tanenbaum. "Computer networks", Prentice Hall PTR, Pearson Education; 2010.
8. Kattepur A, David S, Mohalik S. Model-based reinforcement learning for router port queue configurations. Intelligent and Converged Networks. 2021;2:177-197.
9. Tang A, Kakarla S, Beckett Ryan, Zhai E, Brown Matt, Todd M, Tamir Y, Varghese G. Campion: Debugging router configuration differences. 2021:748-761.
10. Tutsch Dietmar, Hommel Günter. MLMIN: A multicore processor and parallel computer network topology for multicast. Journal of Computing & Operations Research. 2008;35:3807-3821.
11. Zhang Yong-Ku, Song Li-Ren. Campus network security model study. Proceedings of SPIE - The International Society for Optical Engineering; 2011.
    Available:http://www.cse.wustl.edu/jain/cis78897/ftp/virtuallans/index.html
12. Alani Mohammed. Domestic router functions configuration; 2017.
    DOI: 10.1007/978-3-319-54630-8_2
13. Anjum A, Pasha A. A brief view of computer network topology for data communication and networking. International Journal of Engineering Trends and Technology. 2015;2(2): 319-324.
14. CCNA study guide, CCNA Routing and Switching, Cisco systems Mega Guide, CCNA 2013:640-802.
15. Pawar Swati, Nirmal Ankita, Borade Swapnali, Badgujar Pallavi, Ugale Vivek. Network design for college campus. 2020;7:323-326.
16. Ran Deling. Design and Planning of University Campus Network. Journal of Physics: Conference Series. 2020; 1533:022109.
    DOI: 10.1088/1742-6596/1533/2/022109
17. Huichao M, Guoliang L, Chunyu W. Campus Network planning and design. Journal of Computer Hardware Engineering. 2018;12(9).
18. Andrews T, David J, Wallal P. Computer Networks, Fifth Edition; 2011.
19. Liu Dale, Barber Brian, Di Grande Luigi. Configuring Cisco Routers; 2009.
    DOI: 10.1016/B978-1-59749-306-2.00008-7
20. Hossain MT, Mondal M. Implementing VLAN & VPN for an organization; 2020.
21. Heping Pu, Pengxi Li, Shiwen Long. Study on the application of MAC-based VLAN and multi-domain authentication in the Campus Network Management; 2013.
22. Jiang Ning, Shan Liancheng. Application of MAC-based VLANs for mobile office in campus area network. 2008:1029–1032.
23. Kabir Md. Design a VLAN (Virtual Local Area Network) based network; 2020.
    DOI: 10.13140/RG.2.2.29163.57120
24. Prof. Dharminder Kumar. Overview of System Analysis & Design
25. Shukla N, Dashora Y, Tiwari M. Design of computer network topologies: A vroom inspired psychoclonal algorithm. Applied Mathematical Modelling. 2013;37:888–902.
26. Al-Hamiri Mohammed, Al-Khaffaf Dhurgham. Performance evaluation of

campus network involving VLAN and broadband multimedia wireless networks using OPNET modeler. TELKOMNIKA (Telecommunication Computing Electronics and Control). 2021;19:1490-1497.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/95226