*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 20, Issue 6, Ser. I (Nov – Dec 2025), PP 11-17*
*www.iosrjournals.org*

# Evolving Technology To Advance Campus Networks - Providing Secured And Reliable Communication Amidst Facilitated Scaling

Jinadu Olayinka T., Owa Victor K. And Sunday Femi
*Department Of Computer Science, Rufus Giwa Polytechnic P.M.B 1019, Owo, Nigeria*
*Department Of Accountancy, Rufus Giwa Polytechnic P.M.B 1019, Owo, Nigeria*

***Abstract***
*Networking has evolved over the decades, leading to improved interactions with modern information technology devices and applications. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) have facilitated network automation, encompassing more secured deployments and flexible management. SDN promoted hardware independence, while virtualization's open ecosystem evolves cloud computing. Software-controlled networks promoted centralized management and resource optimization. Though, campus network spans several kilometers basking on Wireless Local Area Network (WLAN) model. LAN storms remained an issue as network scales. Broadcast domain deteriorates data communication security, even with fiber-optic-connected substations. Consequently, virtualizing the network infrastructures became expedient to primarily isolate broadcast domain; reduce overheads; and also optimize resources. Virtual LAN technology was implemented to securely advance network scaling and communicate with greater efficiency. deteriorates as network scales. Using selected departments as case study, ad-hoc point-to-point topology, connecting substations with central service was configured. Fibre-optic facilitated trunks, linking Faculty substation with others within 100 to 300 meters. VLAN port tagging was configured over 24-port Mikrotik switch and simulated using enterprise Network Simulator Package. Performance measured includes virtualized bridging, IP-address and inter-VLAN routing, with significant improvement in secured traffic management. Ping statistics showed improved communication accuracy. While VLAN tagging ensured traffic isolation, trunking enabled multiple VLANs share same switch. Traffics from different VLANs were easily differentiated using dot1q protocol implementation. VLAN techniques facilitated logical segmentation, enhanced throughputs, with secured communication amidst desired scalability. An overall efficiency of improved performance, secured access control and reduced overheads were offered as enhancements to the campus network services.*

***Keywords:*** *Access control, Dot1q, NFV, SDN, Trunking, VLAN*

---

Date of Submission: 01-11-2025 Date of Acceptance: 10-11-2025

---

## I. Introduction

Computer networking is achieved with group of devices connected with each other through any of the transmission media, wired or wireless. Wired connectors, including fiber-optics, twisted pairs or coaxial are characterized with fast and reliable data transmission (Jacoby, 2020). Connecting end user devices - computers, printers, scanners, camera, fax machines and others for switching is achieved over layer-2 (L2) device. Layered network provides services by enabling each component send and receive data based on layered functionalities described in Kurose and Rose (2017) and upheld in HuaweiTech (2022). Essentially, computer networking enables data exchange and resource sharing among interconnected devices using layered protocols. Various protocols are specified to guide information transmission over physical or wireless technologies.

Computer network consists of nodes and links. Nodes can be physical or virtual machines. Described in Amazon (2025), node is essentially a single-instance virtual machine and fundamental unit of computing power within Amazon Web Service (AWS). They are basic building blocks for various AWS services including data storage, computations or application hosting. Thus, network nodes, which serves either as data communication equipment (DCE) or data termination equipment (DTE), use links as transmission media in frame and packet forwarding.

Significantly, DCE (switch, modem or hub) or DTE (printer, computers, servers) actively participate in networking based on standardized protocol while transmitting over the physical (cable wires, optical fibers) or wireless (free space) links. Sending and reception of electronic data through links is pre-determined and provisioned in deployed architectures. Fibre-optic link is more accurate in carrying data across large campuses because of the ever-increasing traffic and transmission speeds requirements (Fibreoptic, 2025).

## II. Theoretical Background

Technically, Mano (1993) described computer architecture as the structure and behaviour of various functional modules and how they interact. By extension, network architecture defines and includes specifications for physical components, functional/logical organization, protocols and procedures required in networking. Generally, computer networks are based on standards provided by ISO, IEEE and other allied organizations. These standardizations enable functional organization of computer networks expressed as topologies, describing connection patterns of communicating nodes. Tanenbaum and Wetherall (2011) earlier remarked that topology of many wired LANs, built from point-to-point (P2P) links are based on *Ethernet* (IEEE 802.3) standard. Stallings (2014) also described IEEE 802 as the most widely-used standard for Ethernet family, with WLAN and virtually bridged LANs as members. Working groups are provided for each area (IEEE 802WG).

Campus network, characterized as LAN or WLAN consists of physically connected devices and Ethernet technology implemented as media access connection protocol. Typically, campus networking is achieved with layer-1 devices connected over layer-2 switches. Although, three types of packets (unicast, multicast and broadcast) are enabled over a LAN infrastructure, switches transmit packets in broadcast domain, enabling all end-users access to transmission. Packets with multicast address is transmitted on LAN segment using MAC-level multicast addresses. Also remarked in Stallings (2014), multicasting within single LAN scope, using Ethernet (IEEE 802) and other LAN protocols, is straight forward because user members (multicast group) recognize multicast address and accepts packet. Thus, LAN enables peer communication among faculty members and other administrators, with access control provided by packet transmission mode.

Virtual Local Area Networking (VLAN) concept enables splitting of devices at data link layer into logical units. Generally, layer-3 devices isolate broadcast domain caused by L2 switches. Geeks (2023) also explained that VLAN technology divides broadcast domain of the L2 switches. VLAN identification, achieved using 'tags' and VLAN tagging, is an integral part of networks of all sizes. IEEE 802.1Q standard, developed by the Institute of Electrical and Electronics Engineering (1998) defined Virtual Bridged Local Area Networks (VLANs) as structure supported on enterprise-grade security appliances, access points or series switches.

The 802.1Q tags, called Dot1q are added to Ethernet frames to identify VLAN membership. Thus, VLAN tag is a 32 bits (4 bytes) information, representing VLAN ID with 12bits; TPID protocol with 16bits; (16bits); priority PCP with (3 bits) and Drop indication (DEI) with 1bit. VLAN IDs are configured directly on networks.

VLAN tagging helps network devices identify which VLAN a frame belongs. VLAN creates small-sized sub-networks that are relatively easier to manage. Consisting of logical grouping of devices, and regardless of their physical location, VLAN segments LAN into multiple virtual networks, creating distinct broadcast domains within the single physical network (HuaweiTech, 2020). Logical segmentation, achieved provides campus networking efficiency and optimized resource usage, including APS, dedicated servers and other infrastructures. Switch ports with same attributes are grouped, tagged and managed in same VLAN as port group to ensure access control (HuaweiTech, 2022).

With campus network consolidation, layered function subsists in LAN resource-sharing. Devices in same domain receives all broadcast packets, to characterize visible treat of data insecurity. Using VLAN, separate broadcast domains are created. Hosts not linked from same switch are easily grouped since VLAN membership is configured through software (Wikipedia, 2025). Technically specified in (CiscoTech (2020) and HuaweiTech (2020), VLAN identification help tag network frames for simplified management and inter-VLAN routing is required to forward packets between VLANs.

Virtualization concept provides for consolidation of network infrastructures. Network virtualization, which combines physical network resources into single software-based entity, allowed for more efficient and flexible network management (Wikipedia, 2025). Decoupling network functions from physical hardware, virtualization also enables creation of multiple virtual switches on physical infrastructures, including L2 switches and L3 routers among others. VLAN technique enables logical traffic segmentation via attended software networking. Multiple virtual switches are created on one physical switch to achieve resource utilization. Virtualized switches are effectively managed using capabilities of software defined networking (SDN) and real-time programmability (Jinadu and Aliu, 2018).

Lumen (2025) described SDN as network virtualization architecture, enabling multiple switches to be combined into a single intelligent switch. The model makes entire network visible such that security threats are enabled to be addressed holistically in real-time using software-based controls. Using well-defined application programming interface (API), SDN effectively separates data and control functions, making the execution of policies centralized.

**Justification for the Research**

With the recent proliferation of higher educational institution creation in Nigeria and most campuses beginning from the scratch, there is need to put in place, essential information technology infrastructures that are

compatible with the intelligent age. So, considering the sky-rocketing costs of new installations and upgrades, both beginners and existing campuses need to leverage on new technology to scale network service provisions for their stakeholders and as well optimize available resources. The new technique, using VLAN will enable optimization through virtualization.

Although, L2 switch, an essential building block in Ethernet LANs and indispensable component in campus networking is easily affordable, it belongs to only one broadcast domain. Forwarding both broadcast and multicast packets over every switch port of multiply-connected switch introduces switching loop into networks. Switching loop develops into broadcast storm within seconds and entire network traffic is choked off. Also, Spanning Tree Protocol (STP) topology defined and developed by IEEE802.1D to prevent broadcast storms was inefficient as observed in Balchunas (2014) too. So, with switching loops, broadcasts forward traffic endlessly using same ports, making broadcast domain a persistent issue limiting scalability. New protocol will isolate and prioritize traffic, reduce broadcast traffic and congestion bottlenecks.

In addition, despite broadcast and multiple unicast transmissions easily enabled in LAN transmission, they generate unnecessary copies of source packet, leading to congestion and flooded transmissions. Similarly, multicasting done within on single LAN segment is easy using IEEE 802 or other LAN protocols, but it becomes big issue in Internet environment as routers connect each other over high-speed links. Inter-VLAN routing will resolve this issue and enable access to wide area networks. Implementing VLAN trunking will facilitate transmission of traffics from multiple VLANs over same trunk link.

Also, connectivity over optic-fibre is more accurate in transmitting higher gigabits of data. A choice for fibre-optic communication became expedient as voice, video and multimedia traffics characterized ever-growing campus networks and even upcoming ones.

The choice to use Huawei's Versatile Routing Platform as the software to implement the networking function is due to its universal acceptance and compatibility with other vendors. Also, VRP's compatibility with Application Programming Interfaces (APIs) enables interaction with network management, control and data plane handling in agreement with SDN conceptualization. The API allow device configuration and monitoring functions (HuaweiTech, 2020).

Lastly, as packets with multicast address are transmitted on LAN segment using MAC-level multicast addresses, potential security risks are experienced. Using VLAN tagging, traffics are differentiated and prioritized to enable secured access controls. The software-based controls also offered simplified and efficient management. Virtualized architecture in VLAN design, supported by adaptive packet switching will enable flexibility and enhance scalability.

**Knowledge gaps**

The following knowledge gaps will be filled:

(i) design of point-to-point topology using virtualized switches; access and trunk links; and
(ii) implementation of VLAN protocol IEEE 802.1q using simulation; and
(iii) evaluation of network performance.

**Expected contribution to knowledge**

After carrying out this study, the following would be added to knowledge:

(i) high-speed transmission on fibre-optic connection links for fast speed packet switching
(ii) virtualized switch made to provide logical segmentation and broadcast traffic isolation
(iii) NFV and SDN models fused in software-based packet switching to eliminate hardware latency
(iv) measurement of network performance - VLAN summary, ARP table, mac-address generation etc.
(v) connectivity and performance tests using VRP and ping tools
(vi) analysis of ping statistics

## III. Materials And Methods

Materials required for this research are enterprise Network Simulator Package (eNSP); Versatile Routing Platform (VRP); Virtual Box; Wireshark and the Ping tool.

To implement IEEE 802.1Q protocol on campus LAN, we attempted capturing a LAN topology with connected devices around the central ICT complex and Faculty of Applied Science (FAS) in Rufus Giwa Polytechnic, Owo, Nigeria. Though, FAS is within 1km distance to the ICT, it was a newly constructed building housing many departments. These departments, though consisting different user groups are expectedly demanded to be served necessary applications from the central ICT.

To this end, 24-port Mikrotik switches were installed in FAS-Workstation (FAS-WKS) and linked, using 24/84/96 cores fibre-optic cables with configured *Routerboard Mikrotik* 1100AHX4, at the central ICT. An optical network terminal (ONT), which serves as connection point (endpoint of fibre optic cable), provided fibre-to-the-

premises and was made to reside within the installed FAS-WKS 16-U device. ONT was finally connected to FAS-LAN via Ethernet switch ports, to enable access to high-speed Internet provided on campus.

***Simulation Setup***

Using enterprise Network Simulator package, the following scenarios were analyzed and translated to data communication requirement analysis for FAS-LAN:

(i) each department within FAS-LAN designed to run on separate subnets
(ii) faculty main office subnet created to house an application server
(iii) software laboratory featuring multiuser environment for SWD to run on separate subnet
(iv) access points and Internet of Things (IoT) devices in NCC laboratory run on another subnet
(v) trunk link between COM and STA departments provides common data to many user-groups etc.

***Planning the VLAN***

Various subnets of FAS-LAN segments were respectively determined based on stated scenario captured into topology design presented in Fig. 1(a). Each subnet was assigned appropriate Internet Protocol (IP) address and unique VLAN identification (VLAN IDs). Pools of VLAN tags were created between 2 and 4095.

For this research, VLAN 10, 20, 30 were respectively created on switches representing COM and STA departments. Each switch was customized to serve three categories of user-groups via three subnets as shown in Table 1. Versatile Routing Platform (VRP) was used for the configuration. Shown in Table 1, are data for ports configuration; VLAN ID and IP address assigned to each VLAN representing created user-groups.

Table 1. Data for VLAN network setup

| User Group | VLANID | Port-Group | Link Type | IP Address |
|---|---|---|---|---|
| HOD/Exam Officer | VLAN 10 | 1 - 8 | Access | 192.168.1.1 198.168.1.4 |
| Staffers | VLAN 20 | 7 - 17 | Access | 192.168.2.1 192.168.2.5 |
| Students | VLAN 30 | 18 - 24 | Access | 192.168.3.1 192.168.3.6 |
| SW_COM | VLAN 10 20 30 | 1 - 24 | Trunk | 192.168.1.2 192.168.2.2 192.168.3.2 |
| SW_STA | VLAN 10 20 30 | 1 - 24 | Trunk | 192.168.1.3 192.168.2.3 192.168.3.3 |

Upon the determination of parameters to use, and configuration data planned for each segment, network topology designed is presented in Fig. 1(a) while VID and ports are summarized in Fig. 1(b).

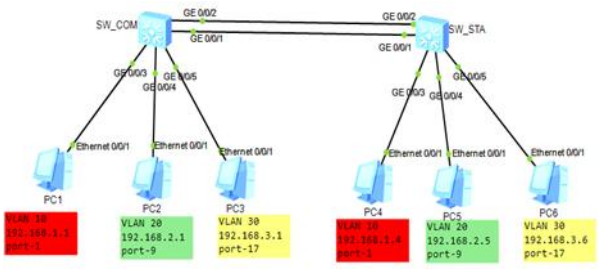
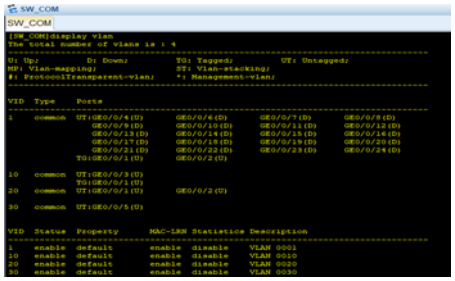



Fig. 1(a) Topology design for VLAN processes




(b) VID and Ports summary

VID and port summary was obtained running initial test using *display vlan* on SW-COM. Three new vlans with native *vlan 1* as default were reported created, making total VLAN 4. Links setup were analyzed and summarized (as *TG* or *UT* representing *Tagged* or *Untagged*). Other configurations for packet transmission were applied.

***Switch port configuration***

Configuration steps for VLAN tagging on SW_COM and SW_STA switches were based on algorithm:

1. SW>System view
2. Create VLANs
3. Port link-type set on interface view – access/trunk
4. Default VLAN set for access/trunk – pvid vlan[]
5. Set list for link to allow-pass
6. Configure IP using interface IP addr mask
7. Quit

VLANs were created in batches and access ports configured for individual devices within user-group. VLAN ID and IP address were also assigned to user-groups for routing functions.

Trunk port was configured between the two switches to enable carriage of multiple VLAN traffics (see Appendix). Code segment on each SW VLAN included configuration on *int g0/0/1* and *int g0/0/2* respectively, indicating *port link-type trunk;* list set *port trunk pvid [vlan no]* and passage *port trunk allow-pass [vlan no]* procedures.

***Inter-VLAN routing***

To enable communication between users in different VLANs, Router (R) was configured to handle traffics from many VLANs using coded line segment on router for inter-VLAN communication. Implementing Wide Area Networking (WAN) point-point-protocol (PPP), which cannot identify VLAN packets as they move between different VLANs is enabled using 'VLANIF' command configured on R via interface linking R.

[Router]int g0/0/6
[Router-gigabitEthernet]vlan-if
[Router-gigabitEthernet-vlan-if]vlan 10
[Router-gigabitEthernet-vlanif-10]ip addr  mask etc

Configuring each *vlanif* on the router enables processing of frames from vlans. On sending packets, the frame tags would be removed and PPP WAN protocol will be able to process the packets.

***VLAN dot1q termination***

Configuring *VLANIF* was the approach used to terminate dot1q implementation in segments. Sub-interface configuration of *g0/0/1.1* on SW-STA terminates VLAN tagging as frames are received on *vlan 10.*

[SW-STA] int g0/0/1.1
[SW-gigabitEthernet-g0/0/1.1]dot1q termination vlan 10

***Tests and Measurements***

On VRP, network parameters were measured from performances based on implemented VLAN dot1q protocol, both in *System-view* and *User-view* modes using these commands:

[SW]display arp
[SW]display mac-addr
[SW]display vlan
PC>ping destination ip-address

Results obtained from running *arp* on *SW-COM* is shown in Fig. 2(a) while IP address assignment on created *vlanif* is shown on Fig. 2(b). MAC address detected was displayed against each switch as resolved by protocol confirmatory command *arp.* Created VLANs were displayed with assigned switch ports and their summary. *Vlanif* enables inter-VLAN communication via VLAN 20. Other information regarding the network performance including maximum number of allowed VLAN on each switch as 4095 is captured. Performance reports from both *User-view* and *System-view* confirmed separation of broadcast domain on each switch (SW-COM or SW-STA) into 3 isolated logical segments. Other PC simulation results are attached as Appendix.

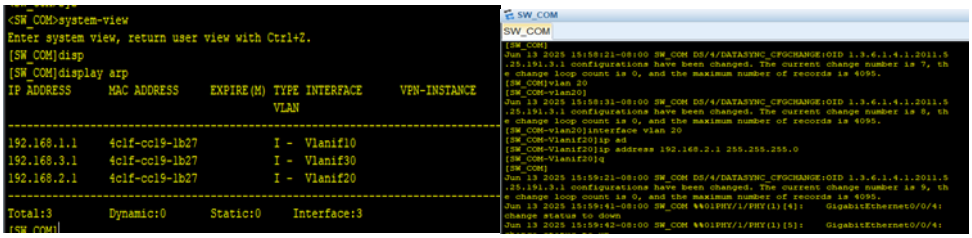



Fig. 2
(a) result using *arp* protocol
(b) assigned IP address on VLAN 20

## IV. Results And Discussion

Displayed parameters from running the address resolution protocol, *arp* provided a mapping of active hosts on the network, resolving assigned IP address with dynamically detected MAC address.

List of created *VLANs* and the running links were displayed. Interface marked with *U* signifies UP and active (running). Five active links were detected (*int g0/0/1 – g0/0/5*). Marking on the interfaces with *TG* indicates *Tagged* frames and *UT* denotes *Untagged* frames.

Connectivity tests with *Ping* tool carried out in *User-view* confirmed logical separation of broadcast domain on SW. Hosts' connectivity tests were carried out between hosts in same user-group, suggesting same VLAN membership and between hosts in different VLAN using IEEE 802.1Q protocol. Traffic transmission success to hosts in same VLAN are shown in Fig. 4(a-c) while traffic transmission to users in different VLAN are also reported in Fig. 4(d-f). These and other tests are included in the Appendix.

***Analysis of ping statistics***

Shown in Fig. 5 is the ping statistics displayed on connected hosts. 5 packets were transmitted in 5 sequences between PC4 and PC1 with an average round-trip time (RTT) of 90ms, being in same VLAN. Also, PC5 connected with PC2 to transmit 5 packets on average RTT of 78ms. However, no transmission was enabled between PC4 (VLAN 10) and PC2 (VLAN 20) and between PC5 (VLAN 20) and PC1 (VLAN 10).

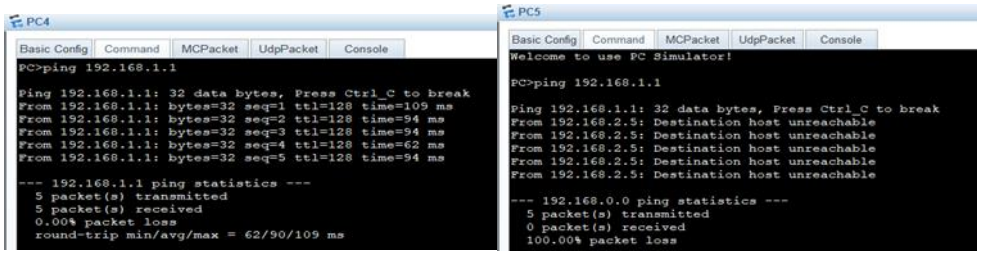



Fig. 5 Ping statistics (a) connection established (PC4 - PC1) (b) connection failed (PC5 and PC1)

***Deductions from the measurements and statistics***

(i) *arp,* address resolution protocol implemented as gratuitous arp to avoid duplicate IP address
(ii) *MAC* address dynamically detected and resolvedly mapped with IP address
(iii) *Interface* type connected between switches was trunked
(iv) *VLAN ID,* corresponding to each subnet host was displayed
(v) *VLANs* dot1q was terminated on gateway with 'VLANIF' command

Trunk port enable access to multiple VLANs on same link. Use of trunk (as hybrid) link between switches offered simplified technique to manage multiple VLANs on the shared link. Also, single or multiple VLAN membership with options to define 'tag' or 'untag' for specific VLAN was provided flexibility.

Point-to-point topology connected nodes directly and VLANs provided broadcast domain separation on both switches. Representing multiple smaller logical partitions of the broadcast domain, VLAN provides security filtering of transmitted traffics. Similarly, creating the logical partitions on virtualized SW-COM and SW-STA switches signifies broadcast domain isolation and elimination of all associated bottlenecks.

Security policies were enabled on created logical networks and administrator boundary provided for connected hosts. Device types' grouping into PC, AP, Printers, Camera, Tablets etc. for varying security policies and different QoS was projected. VLAN assignment in this research was port- and IP subnet-based. Total configured VLANs, ports with link status (tagged or untagged) and active gigabitEthernet (GE) links indicated with 'UP'. VLAN assignment based on protocols is projected for further studies.

## V. Conclusion And Recommendation

VLAN technology is vendor-neutral and applicable in any campus network, medium or large. Port-based or IP subnet-based VLAN assignment offers simplified and flexible network management. Traffic prioritization provided enhanced security and regulated access control through its encapsulation. There were improvements in resource utilization as virtualized bridging were provided.

No additional costs on infrastructure to scale network service to new departments. Evolving technology of *dot1q* facilitated reduced overheads, improved network efficiency and performance stability. VLAN tagging forward frame to appropriate VLANs efficiently while trunking enable multiple VLANs transmit over shared links. This made resource utilization evident using trunk port configuration on virtualized switches.

Demonstrated communication throughputs and resource optimization characterized network transmission efficiency. Isolation of broadcast traffic domains validated dot1q protocol as an efficient technology for network segmentation and enhanced security. Restricted access provided via network segmentation contributed to service reliability. Congestion was eliminated and isolated traffics securely transmitted while network scales.

Finally, dot1q technology exhibited greater benefits of security and service reliability in networking. LAN broadcast traffics were isolated and differentiated using software control. Thus, a resultant logical segmentation and flexible management, which provided secured data communication amidst network scaling

visibly became evident. Therefore, *dot1q* technology is recommended for implementation on campuses that require WLAN service upgrade and secured wireless service.

## References


[1]. Amazon Web (2025). What Are Nodes In AWS? Available In Https://Doc.Aws.Amazon.Com. Retrieved June 5, 2025.
[2]. Balchunas A. (2014). Spanning Tree Protocol (STP). Accessed From Www.Routeralley.Com. Retrieved May 21, 2025.
[3]. Cisco Tech (2020). Vlans Explained: CCNA 201-301. Available In Www.Youtube.Org. Retrieved June 10, 2025.
[4]. Fibreoptic Systems (2025). Available In Https://Www.Fibreoptic.Com. Accessed May 21, 2025.
[5]. Geeks Forgeeks (2023). What Is Virtual LAN? Available In Www.Geeksforgeeks.Org. Retrieved June 10, 2025.
[6]. Huawei Technologies (2020). Data Communication Notes. Available In Www.Huawei.Com. Retrieved June 5, 2025.
[7]. Huawei Technologies (2022). HCIA Data Communication V1. Available In Www.Huawei.Com/En/#/. Retrieved 30-5-25.
[8]. IEEE 802WG (1998). IEEE 802.1Q. Available In Www.Google.Com. Retrieved June 10, 2025.
[9]. Jacoby, Mitch (2020). Guide To Fibre Optics And Premises Cabling. The Fibre Optics Association.
[10]. Jinadu Olayinka And Aliu Abass (2018). Reconfigurable Communication System With Dynamic Capacity Increase: Model To Containing Congestible Traffics. International Journal Of Engineering And Future Technology (IJEFT), UAE, 15(3):11-21. Www.Ceser.In/Ceserp/Index.Php/IJEFT/
[11]. Kurose James F. And Rose Keith W. (2017). Computer Networking: A Top-Down Approach. 7th Ed. Pearson.
[12]. Lumen Technologies (2025). Software-Defined Networking Benefits. Available In Www.Lumen.Com. Retrieved 10-5-25.
[13]. Mano Morris M. (1993) Computer System Architecture. 3rd Ed. Pearson
[14]. Stallings W. (2014). Data And Computer Communication. 10th Ed. Pearson.
[15]. Tanenbaum Andrew S. And Wetherall David J. (2011) Computer Networks. 5th Ed. Prentice Hall, Pearson.
[16]. Wikipedia (2025). What Is VLAN? Available In Https://En.Wikipedia.Org. Retrieved June 10, 2025.