International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

A Survey of Emerging Techniques for Large Networks of Virtual Local Area Networks (VLANs) with Benefits and Limitations

Ajas Shaik*

Department of Information Technology

Received 01 Dec 2024, Accepted 20 Dec 2024, Available online 23 Dec 2024, **Vol.14, No.6 (Nov/Dec 2024)**

Abstract

The numerous benefits of wireless communication have led to its meteoric rise in popularity as a network type, yet there have been numerous obstacles to enhancing its performance. An alternative method that allows a network administrator to construct a logical network out of a physical network is VLAN, which stands for Virtual Local Area Network. Thus, VLANs are fundamental technology for enhancing network performance, capacity and security. VLANs are a means of breaking large networks into smaller broadcast domains, managing broadcast traffic, controlling congestion, and providing increased levels of security. This paper explores the emerging techniques in managing and optimising VLANs within large-scale network environments. VLANs are essential for improving network performance, security, and scalability by the logical segmentation of networks into smaller, isolated broadcast domains. This survey also outlines trends in future VLAN technologies such as Software Defined Networking (SDN), VXLAN, and Big Data and Analytics. Also, the paper covers the uses, advantages, and disadvantages of VLANs, including enhanced security, scalability, and economy, though admitting to issues of VLAN configuration difficulty and security threats. In the paper, the authors discussed the future trends including the integration of multi-cloud, network slicing coupled with 5G, and integration of blockchain for VLAN security.

Keywords: *Virtual Local Area Networks, Emerging Techniques, Scalable Network Architecture, limitations, future directions.*

Introduction

Whether for government agencies, commercial companies, or educational institutions, especially universities, the value and additional benefits of network infrastructure are clear in today's globalised society. It helps accomplish significant objectives, including increased productivity, efficiency, knowledge acquisition, and teamwork. An effective network design and a strong technological foundation are prerequisites for the university's planned expansion of information technology. Computer networking allows the modern world to share data across systems, regardless of physical location, by following predefined protocols that allow different systems to communicate in various ways to accomplish common goals[1].

VLANs are core to current network implementation since they allow the subdivision of large networks into micro sectors based on performance, security, and scalability needs[2]. With the increases in the complexities of network environments, conventional VLAN architectures are capable of handling dynamic and large-scale implementations at a strain[3].

*Corresponding author's ORCID ID: 0000-0002-0038-6957
DOI: https://doi.org/10.14741/ijcet/v.14.6.11

Such evolution has led to the creation of new techniques that are effective in large VLAN networks, which include automation, Software Defined Networking (SDN)[4], and Advanced Virtual Networks [5]. The importance of VLANs is based on the features associated with the separation of traffic, limitation of broadcast domains, and multiple opportunities for network control[6].

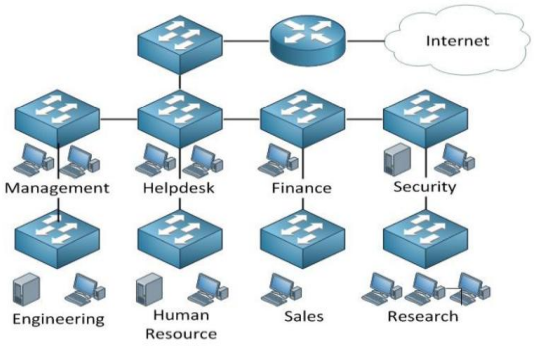

Fig.1 Virtual local area network

However, adding the concept of VLANs to networks to include larger networks posed challenges like the challenges of managing the VLAN address space[7], developing consistency in VLAN configuration and

achieving the best performance. Prospective techniques have been developed to overcome these challenges with the help of recent enhancements in two areas generally – the hardware and the software and protocols[8]. Figure 1 shows the overview of virtual local area networks.

Emerging techniques for large networks of Virtual Local Area Networks (VLANs) focus on improving scalability, security, and efficiency in managing complex network environments. Traditional VLANs are thus becoming more capable of dealing with larger amounts of traffic and a wide range of applications as organisations use more cloud computing, the Internet of Things, and virtualisation technologies. An extensive review of VLANs is given in this study, with an emphasis on their function in contemporary network architecture, especially in large-scale environments. It discusses the concept and use of VLAN, specifically the VLAN's capacity to enhance the performance, scalability and security of the network through the division of traffic into unique broadcast domains. The paper also briefly explores fresh emerging concepts in VLAN, such as SDN, VXLAN and artificial intelligence for VLAN management. Also the study also considers the opportunities and challenges of VLAN as well as its effects on network security and performance. Last but not least, it is important too to discuss future development scenarios of the VLAN technology, including multi-cloud VLAN, Network slicing with 5G and implications of blockchain technology on VLAN network security.

The following research is organised as follows: an overview of VLAN discussed in Section II; Section II provides the emerging techniques for large networks in VLAN; Section III gives the scalable network architecture; Section IV provides the VLAN security threats, then Section V to VIII provide the benefits, limitations and future directions, Section IX provide some existing work on VLAN with various tools and techniques, Section X is last provide the conclusion of this paper.

Overview Of Virtual Local Area Networks (VLAN)

The LAN's blueprint in abstract form is called a virtual LAN. A VLAN may use a portion of a single switch's ports or portions of ports from several switches. Systems on a single VLAN on a single network do not, by default, view traffic from other VLANs on the same network [9].

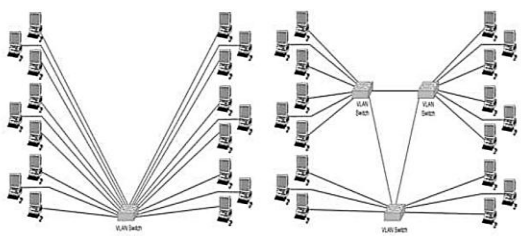

Fig.2 (a) single switch VLAN (b) multi switch VLAN

Network speed and scalability may be enhanced via VLANs' broadcast control feature, which eliminates superfluous broadcast traffic. Security enables administrators to create access lists that logically divide individuals and departments, allowing them to regulate traffic among VLANs. Figure 2 (a) represents single-switch VLAN, and figure 2 (b) represents multi-switch VLAN.

Through the removal of the network's physical borders, VLANs enable a user or device to leave from any location. Frequently, virtual local area networks can be used to isolate the user network from the server network. The main campus of UniversitéLumière de Bujumbura uses virtual local area networks. There are a variety of network weaknesses based on the standard flat LAN architecture, where each user is part of a single broadcast domain.

VLAN Architecture

The development of virtual local area networks allows for the erasure of several issues. A layer 2 switch capable of supporting the VLAN protocol is required for the creation of VLANs. It is an often-held belief among novices in the networking industry that all it takes to "enable" VLANs on a network is the installation of a little piece of software on each client or switch. That is not the case; instead, your Cisco system would benefit from VLAN switches, such as Cisco Catalyst switches [10]. Your switch must be compatible with VLANs when you buy it; otherwise, you won't be able to set them up. VLANs include millions of computations and necessitate specific hardware that is constructed into the switch [11]. Each VLAN is established on a separate network, which is a switch. Network broadcasts are automatically blocked from any switch ports that aren't part of the same VLAN. This is the rationale for a VLAN having In today's vast networks, networks play a crucial role in aiding segmentation, and firewalls that are poorly designed might worsen the difficulty created by applications that rely heavily on broadcast signalling. Figure 3 displays the VLAN infrastructure, which adds a new dimension to network architecture and creates several new issues for administrators.

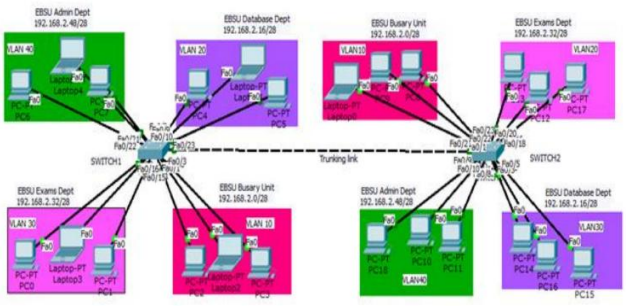

Fig.3 VLAN Infrastructure

Applications of VLANs

The following research applications of VLANs are[12]:

Performance enhancement: As LAN communication rates rise, routers that use software to transfer data become a bottleneck. This bottleneck is eliminated by using switches instead of routers.
Implementation of virtual workgroups: It is easy to group all the individuals working on a single project into a single VLAN since workstations may be transferred from one VLAN to another simply by adjusting the settings on switches. This will make it easier for them to collaborate and exchange resources.
Greater flexibility: Users may keep working inside the same VLAN even if they switch desks or just move their laptops across the office, provided the VLANs are configured correctly. When routers physically split a network, this becomes considerably more difficult.
Ease of partitioning off resources: Network administrators can create separate VLANs for servers and other devices to which they want to restrict access.
Reduced cost: The cost of the arrangement is decreased by employing switches on the VLAN to construct broadcast domains instead of costly routers.
Security: Broadcasting sensitive information via a network exposes the network to a number of hazards and threats. By limiting access to the network data to users who are authorised, VLANs can lessen the likelihood that an intruder would obtain access. Additionally, VLANs may be used to govern broadcast domains, set up firewalls, restrict access, and notify network management in the event of an external assault.

Emerging Techniques for Large Networks in Vlan

Network managers may conceptually divide huge networks into smaller, more manageable groupings independent of their actual location using VLANs. As enterprise networks continue to grow and evolve, managing a large-scale network of VLANs becomes increasingly complex. Emerging techniques are aimed at improving scalability, security, automation, performance, and overall network efficiency. Below are some key techniques and trends that are shaping the management and optimisation of VLANs in large networks[13].

Software-Defined Networking (SDN) and VLANs

A new paradigm in network administration known as software-defined networking (SDN) has recently evolved. By decoupling the network's control plane and data plane, software-defined networking makes network programmability and centralisation possible [14].
Centralized Management: This means that through SDN, the administrators can manage several VLANs in the entire network topology from a single controller. This helps to simplify its features, thus making it possible to deploy new VLANs in the shortest time possible.
Dynamic VLAN Assignment: In SDN, dynamic VLAN can be configured depending on the role, type of equipment, or application necessity. This assists in massaging resources, and it eases the reconfiguration of the network.
Improved Network Visibility: SDN based controllers are more advantageous because they allow for easier inspection of VLAN traffic patterns and are capable of Traffic Flow Control.

VLAN Aggregation and Stacking

VLAN aggregation, as well as stacking, enables multiple VLANs to be combined and form one logical configuration. That is especially important for big networks where it helps to decrease the number of VLANs to be managed and monitored [15][16].
VLAN Stacking: This entails managing the many VLANs in a single unit, hence reducing the burdens of managing every VLAN separately.
Trunking Protocols: Advanced trunking protocols like IEEE 802.1Q and Link Aggregation Control Protocol (LACP) are used to aggregate VLAN traffic, improving bandwidth utilisation and redundancy.

Segment Routing (SR) for VLAN Traffic

Segment routing is a method that enables traffic steering in a network domain as well as the assignment of traffic pathways. Today, it is actively used in large VLAN networks because it facilitates traffic engineering here [17].
Traffic Optimization: SR lets the network administrator define the exact route that traffic should take through the VLANs and brings a certain efficiency to the manner in which VLAN traffic transverses a network.
Reduced Complexity: Unlike traditional MPLS (Multiprotocol Label Switching), SR doesn't require complex label-switching tables, making it easier to scale and manage.

Virtual Extensible LAN (VXLAN) for Scalable VLANs

VXLAN is an encapsulation technology that enables the creation of highly scalable Layer 2 networks over Layer 3 infrastructures[18]. It is commonly used in data centres and cloud environments to extend VLANs across geographically dispersed locations.
Greater Scalability: VXLAN enables the creation of up to 16 million unique logical networks (compared to the 4,096 VLAN limit in traditional 802.1Q VLANs), which is essential for large-scale deployments.
Data Center Integration: VXLAN is a VLAN that can be easily incorporated into cloud and virtualised data centers in particular, extending VLAN across diverse geographical locations.

VLAN Monitoring and Analytics with AI/ML

Advanced analytics powered by AI and ML are becoming indispensable tools for managing large-scale VLAN networks.

Traffic Analysis: AI-supported network monitoring tools can scan VLAN traffic and possible compliance issues, inefficiencies, or security risks much earlier than small and isolated manual checks.
Predictive Maintenance: It is even possible to send alerts when certain VLANs are likely going to fail or perform relatively poorly, thereby taking preventive measures to stabilise the network.

Zero Trust Networking (ZTN) and VLAN Isolation

Zero Trust Network Architecture (ZTNA) [19] is a new approach to security that does away with the need for traditional perimeter defences and instead relies on continuous identification verification to give access to resources.
VLANs in Zero Trust: With VLANs aligned to Zero Trust policies, network segmentation is achieved by coupling it with identity-based access control. In that way, if there is a security breach, only individuals or items that are permitted to gain entry to the crucial VLANs will receive permission to do so, and the risk of early transfer will be minimised.
Micro-Segmentation within VLANs: ZTNA principles also enhance the use of granular security controls within VLANs, enabling policies to be set as finely as the workload or user as opposed to reposting on conventional network-based separation.

Scalable Architecture of Network

For organisations to manage growing data loads, integrate new devices, and enable future growth, a network design that can be easily scaled is crucial. The scalable network design is depicted in Figure 4 [20].

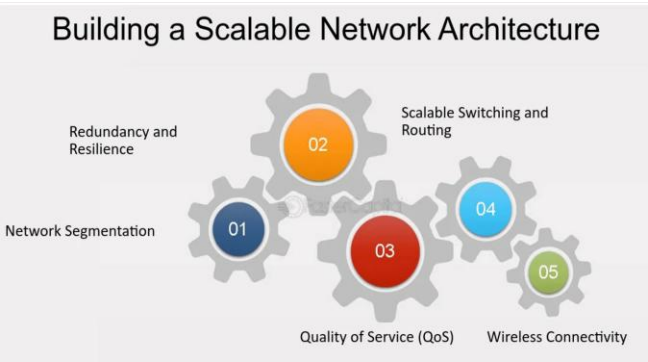

Fig.4 Scalable Network Architecture

The following are important factors to take into account while creating a scalable network architecture:
Network Segmentation: Reduce liability and increase throughput by properly dividing up your network. By using SDN or VLANs, you can create different networks within the organisation for different devices or departments. Limitation of access in networks helps to minimise traffic volume, prevents hacking and other violations, and improves the operation of a network overall.
Redundancy and Resilience: For the network to be highly available and hence minimise its downtime, ensure that there are duplicated cables and devices. Some examples of such technologies are link aggregation, redundant power sources and fail-over mechanisms. Redundancy is a form of creating a backup for a network so that it will still be functional in case one connection or device is lost.
Quality of Service (QoS): Applications and services are critical to any network and must be used to determine the priority order of traffic flows. QoS allows for provisioning of delay and amount through a network based on policies in place. This ensures that no matter how congested the network becomes, definitely mission-critical applications such as VoIP or video conferencing will have to be prioritised and allowed to have proper network usage.
Scalable Switching and Routing: Equip your network with high-performance routers and switches, so purchase routers and switches. It is advisable to attempt to select instances that can be further substituted for the modular additions or stacking, those that can handle more transactions and increase the complicated path records. Therefore, it becomes possible for your network architecture to handle the growth of your firm.
Wireless Connectivity: Mobile environments are growing, and constant networking is getting more important due to the necessity of using various technologies in working spaces. It should be your network has adequate capacity and coverage to support wireless access points when that is needed. For higher speed, higher capacity and compatibility for many devices, consider technology such as Wi-Fi 6 (802.11ax).

Vlan Security Threats

VLANs have been used by network managers to provide a layer of security and isolation for data protection. VLAN tagging, however, was not intended as a security feature. This should be considered while putting VLANs into place in order to accomplish security. The phrase "VLAN hopping" is commonly used to describe any way that a malicious device might transmit packets to a VLAN port that it ordinarily would not be authorised to access [21].

Furthermore, if a hostile device knows the target system's MAC address, it can defeat the protection of a VLAN. Attackers posing this severe risk to VLAN security would need inside information about the devices they are aiming at and where they are located [22]. As soon as an attacker has the MAC address, they can add the target device's static address to their system's local ARP cache. Despite the devices' separation into different VLANs, this enables them to communicate directly with one another[23].
VLAN Hopping: The second is related to VLAN tagging, in which the attackers direct packets to the unauthorised VLAN ports. This makes devices that are

malicious gain entry to VLAN segmentation and be able to access secured VLANs.

MAC Address Spoofing: They attach themselves to the intended resources using the knowledge they possess by assigning fake MAC addresses. Through Arp cache, they configure a static MAC address, which allows direct communication between computers in different VLANs.

Insider Threats: That is why anyone who knows the VLAN of the network can easily penetrate the network without authorisation.

Double Tagging Attacks: There is when an attacker prepares packets with two VLAN tags to avoid going through switches to get to other VLANs.

Inter-VLAN Routing Exploits: The faulty setup of old routers or Layer 3 devices can lead to VLANs and their traffic being plainly visible to the Internet.

Man-in-the-Middle (MITM) Attacks: Any switch has the capability of VLAN isolation, and if the switching devices are not protected against ARP poisoning or DHCP spoofing attacks, VLAN may be exposed to MITM attacks.

Switch Spoofing: A misconfiguration of VLANs can bring vulnerability to the network by setting un-tagged ports or having default VLANs.

Inadequate VLAN Configuration: Some VLAN misconfigurations, including untagged port VLANs and default VLANs, are easily prone to unauthorised access.

Benefits Of Virtual Local Area Networks (VLANs)

It is not ideal for sensitive information to be accessible to unauthorised persons via broadcast on a local area network since the network only has one broadcast domain, and all traffic between workstations on the network follows that [24]. Additionally, network collisions might occur if the broadcast is not well confined. Consequently, routers are typically used by network managers to prevent broadcasts from exiting a business network[1].

A router's processing time for incoming data is often longer and more costly than that of a switch. VLANs emerged as a replacement for traditional methods of limiting broadcast traffic on LANs by utilising VLAN topologies and employing routers for broadcast filtering and address summarisation, respectively, to control the flow of traffic.

Security

An increase in network safety is achieved by VLANs. The administrators of the network may manage every user and port in a virtual private network that spans several broadcast domains. It is now far more difficult for an attacker to sniff a network simply by connecting a workstation to any port on a switch.

Creating Workgroups

It is possible to isolate a group of users that require an exceptionally high level of security by creating a virtual local area network that prevents communication between users outside of the network. This implies that any department inside a company may be made independent of the others.

Scalability

Network transfers, modifications, and additions are effortlessly accomplished by configuring a port in the appropriate virtual local area network and designating hosts to the same VLAN traffic employing a packet sniffer. Every port and all resources that a VLAN is permitted to utilise are within the control of the network administrator. VLANs are instrumental in limiting sensitive traffic that originates from a department within an organisation.

Cost effective

Reducing the need for more costly network equipment, such as switches and routers, may save money for a company. Additionally, VLANs can improve network performance by directing more effective use of resources and bandwidth.

Easy Troubleshooting

Many network issues can arise from using VLANs to partition users and resources, but these issues can be quickly and easily resolved by tracing the hosts to their respective VLANs.

Integrity

Users are logically organised based on their functions, and VLANs are not reliant on the users' physical or geographic locations. Therefore, it is possible to handle university data without compromising it, particularly for institutions with branches.

Broadcast Control

The creation of several virtual LANs, which constantly grow the number of broadcast domains while lowering their size, allows for control over broadcast network administration.

Limitations Of Virtual Local Area Networks (VLANs)

VLANs have their own drawbacks, which are mentioned below. Need special hardware software or switch support Improved security Easy to implement and configure Scalability Lowers transmission delays Cost effective These challenges relate to implementation, management, and performance of the networks, especially for a large network.

Complex Configuration and Management: There are certain complexities involved with VLANs; getting the configurations wrong can really create havoc on a network.

Security Vulnerabilities: Prone to VLAN hopping attacks, which is a menace to a network.

Hardware Dependency: Some protocols are incompatible with regular switches or routers and may demand an upgrade of the company's network equipment.
Single Point of Failure: This is because switch failures can affect and or completely suspend communication for all the connected devices in the VLAN.
Increased Latency: However, to implement Inter-VLAN routing in large networks some delays are usually observed.
Inter-VLAN Communication Costs: VLAN routing is used in layer 3 routing, which increases the processing of the switch.
Bandwidth Overhead: Network variations require several tasks, especially when trunk lines have VLAN tagging capabilities, which takes more bandwidth and might cause traffic jams.
Troubleshooting Challenges: Any complex VLANs take more time to isolate the problem.
Incompatibility Issues: VLAN implementation across the different layers of the various brands of quality hardware may not fully interconnect.
Human Error: Incorrect settings or poor distributions lead to exclusion or intrusions of the device.

Future Directions of Virtual Local Area Networks (VLANs)

As networking technologies continue to evolve, the role and implementation of VLANs are expected to undergo significant changes. With the rise of cloud computing, SDN, AI, and 5G, VLANs will adapt to new trends that enhance network scalability, security, performance, and management. Below are key future directions and trends for VLANs:

Integration with SDN and Network Automation

Nowadays, VLAN will be revolutionised by SDN as it provides freedom and flexibility in programming. By use of SDN controllers [25], VLANs will be dynamically created, updated, and deleted with reference to policy engines, thus enhancing the scalability, flexibility, and accuracy of VLAN management in large and diverse networks. This will resolve many issues with network management, making the processes faster, including deployment and real-time adjustments.

Multi-Cloud and Hybrid Cloud VLAN Integration

When multi-cloud and hybrid cloud models have become common in organisations, VLANs shall spread across multiple clouds [26]. These technologies, such as VXLAN, will help VLANs to interconnect seamlessly across cloud providers and also across the in-house physical infrastructure to enhance secure and efficient communication across data centers.

Adoption of VXLAN for Scalability

The advantages of VXLAN are notable from the following points: VXLAN will replace VLAN as the best solution for network segmentation at scale. This will be especially helpful in highly virtualised environments and big data centers, enabling organisations to grow their networks without hitting traditional VLAN challenges.

AI and ML in VLAN Management

The primary aspects of VLAN in which AI and ML will be instrumental include flow traffic modulation, anomaly detection, and self-healing mechanisms. AI-powered prognostics will anticipate network loads and offer security threats that will allow for interventions to be made before system downtime occurs.

Zero Trust Networking (ZTN) and VLAN Security

To enhance the level of security and control over the access that devices have to resources in a network, VLANs will interact with ZTNA [24]. This high level of micro-segmentation will reduce the risk of VLAN shenanigans as Zero Trust pushes for consistent micro-segmentation, which will verify users every time they attempt to access files in their same VLAN.

5G and VLANs for Network Slicing

5G technology will introduce network slicing, where VLANs will play a key role in isolating and managing different types of traffic for specific applications, such as IoT, autonomous vehicles, and augmented reality[27]. This will ensure each slice gets the necessary resources, security, and performance, particularly in highly dynamic environments.

Blockchain for VLAN Security and Transparency

Blockchain technology will enhance VLAN security by providing decentralised validation of network traffic. It will offer an immutable audit trail for network activity, improving security, integrity, and compliance, especially in sensitive environments where data transparency and accountability are crucial.

Literature of Review

Virtual local area networks have been the subject of several academic recommendations. Prior research has focused on how virtual local area networks (VLANs) affect LAN performance and security; however, this study delves further into how VLANs affect wireless network management and performance improvement, as well as how routing protocols can boost wireless network performance.

Gentile et al. (2024) examined the impact of different types of overlay networks on the performance of VPNs and optical networks (ONs), including RTT and bandwidth, while connecting many hosts inside the same data centre, between data centres in the same building, or across the Internet. Instead of the usual

Docker, LXC, or Podman containers, these networks link individual KVM instances. Where encrypted channels, such as VTI, are not yet available, the second analysis creates several unencrypted channels, and the last analysis wraps overlay traffic using IPsec (Transport mode). A comprehensive collection of traffic simulation campaigns demonstrates the achieved results[28].

Li et al. (2024), provide a solution that makes use of VLAN and VxLAN many-to-one mapping, mandating that all traffic originating from inside the data centre must pass via the VxLAN gateway. Including network aggregation and traffic visualisation in your thorough review will help us determine how well our micro-segmentation technique worked. Expand upon introducing micro-segmentation by incorporating an improved algorithm for asset behaviour. The system builds behavioural profiles using the past traffic of internal network assets; this allows for the quick detection of suspicious conduct and the prompt implementation of countermeasures. Cloud data centre security may be greatly improved with the use of this algorithm, as empirical findings show that it is quite good at spotting suspicious activity in intranet assets[29].

Madavarapu et al. (2023), suggested network offers a solution for data flow according to the demand, which is necessary for the EDS applications' network paths. Electronic data interchange is now fully protected thanks to the deployment of the suggested VLAN in a Cisco environment, which satisfies all requirements. All of these rollouts have been a smashing success, and the EDD platform for safe data sharing across two separate local networks has been fine-tuned[30].

Nourildean, Mohammed and Attallah (2023), used the Riverbed Modeller simulation to examine the VLAN in various circumstances inside a wireless network utilising three ad hoc routing techniques. An important downside of VLAN, according to the research, is that it significantly reduces performance while simultaneously reducing network latency and data. It was possible to enhance the network's latency and throughput using ad hoc routing algorithms, such as AODV, DSR, and OLSR. As further research into ways to enhance the latency and throughput of any network, the results showed that these ad hoc routing techniques enhanced the performance of WSN[31].

Alani and Al-Sadi (2023), investigates related works on dynamic tunnelling with SD-WAN, classifies them by research goal into practicable categories, and presents the most common SD-WAN tunnelling applications, specifically virtual local area network. Finally, this paper's extensive literature review shows that SDN link failure research dominates. This class uses SD-WANs' stronger networking and ability to fix most communication issues. The controller might swiftly recover by switching to a pre-computed backup path in case of a fault. Dynamic VLAN Open-flow Software-defined WAN Virtual LAN The CC BY-SA license makes this article open access[32].

Romansky (2022), explores a potential avenue for an optimised network architecture design, delving into topics such as the requirements for setting up VLANs, the organisation of a demilitarised zone for open access, and the intricacies of creating a VPN. They present a structural approach for designing optimal network architectures with clearly defined sequential phases[33].

Chen, Yan and Qiu (2020), the smart grid's use of VLAN technologies is the primary focus of this article. This paper proposes a three-layer switched VLAN that partitions the distributed smart grid data management system into independent subsystems with well-defined logical communication units, based on an examination of the fundamental features of smart grid management. Due to this fact that clients and servers in service-based VLANs are often in the same VLAN, the tests presented in this article show that routing is unnecessary for around 10% of the communications that occur randomly across VLANs, a figure that remains relatively constant between 0% and 4%. The routing budget is reduced for VLANs based on conventional policies as the maximum number of hosts in a given VLAN grows[34].

Rodríguez et al. (2020) explore the possibility of using Evolutionary Algorithms (EAs) to determine the bare minimum of VLANs and the memberships that go along with them that are required to facilitate secure and reliable network communication. Greater solutions feature fewer VLANs and greater security; a hybrid Pareto-based fitness measure is devised to rate alternative VLAN solutions, as the problem involves a multi-objective search. Regardless of the situation, such as an increase in the number of linked devices or a decrease in the number of necessary VLANs, the simulation results show that this method can reliably identify short and secure VLAN groups[35].

Below is a summary Table I of the related works in VLAN technology and its applications, which organises the information by author, year, focus, methodology, key findings, technologies, challenges and future work.

Table 1 Summary of the related work based on Emerging Techniques for Large Networks of Virtual Local Area Networks (VLANs

Author(s) & Year	Focus	Methodology	Key Findings	Technologies	Challenges	Future Work
Gentile et al. (2024)	Network performance of VPNs and overlay	Analysed RTT and bandwidth variations with different	Explored KVM-based networks and compared performance of unencrypted and IPsec-	VPN, KVM, IPsec, Overlay Networks	Impact of encryption on network performance	Further optimisation of encrypted traffic in

	networks	overlay network types	encrypted overlay traffic, revealing key performance impacts.			overlay networks.
Li et al. (2024)	Micro-segmentation in data centres using VLANs and VxLAN	Proposed many-to-one mapping of VLAN and VxLAN traffic with cost-effective implementation	Achieved secure, cost-effective micro-segmentation; introduced an algorithm for detecting abnormal internal network behaviour.	VLAN, VxLAN, Micro-Segmentation, Traffic Visualization	Scalability of micro-segmentation; compatibility of protocols	Implementing the algorithm in large-scale cloud environments.
Madavarapu et al. (2023)	Secure VLAN deployment for Electronic Data Interchange (EDI) applications	Deployed VLAN in a Cisco environment, tested with four different methods	Successfully deployed VLANs with optimised security for EDI using methods like time division multiplexing and user-defined frames.	VLAN, EDI, Time Division Multiplexing, Cisco Environment	Ensuring end-to-end security for EDI traffic across networks	Explore more secure methods for multi-party EDI exchanges.
Nourildean, Mohammed and Attallah (2023),	Impact of VLANs on wireless networks with ad hoc routing protocols	Simulated VLAN performance with AODV, DSR, and OLSR ad hoc routing protocols	VLAN adoption reduced delay and throughput; ad hoc routing protocols improved wireless sensor network performance.	VLAN, Wireless Networks, AODV, DSR, OLSR	VLAN-induced overhead in wireless networks	Testing VLAN performance in more diverse wireless network scenarios.
Alani and Al-Sadi (2023)	Dynamic tunneling with SD-WAN and VLANs	Review of SD-WAN tunnelling applications related to VLANs	Identified VLAN management, multi-VLAN setups, and SD-WAN for fault recovery as key research areas in SD-WAN tunnelling.	SD-WAN, VLAN, Dynamic Tunneling, OpenFlow, SDN	Link failure recovery and dynamic path optimisation	Investigating SD-WAN protocols for automated VLAN management.
Romansky (2022)	Optimised VLAN network architecture, DMZ and VPN setup	Proposed structural model for VLANs and VPN setup in network architecture	Designed an optimised network model for VLAN configuration and VPN integration, with an emphasis on security and accessibility.	VLAN, VPN, DMZ, Network Architecture	Securing network layers and optimising design for large-scale networks	Extending the model for cloud-based and hybrid environments.
Chen, Yan and Qiu (2020)	Application of VLANs in smart grid management	Designed a three-layer switched VLAN for distributed smart grid systems	Showed that VLANs reduce network congestion and improve data processing efficiency in smart grids.	VLAN, Smart Grid, Network Optimization	Addressing congestion in large-scale grid systems	Expanding the VLAN model to cover real-time data in smart grids.
Rodríguez et al. (2020)	Evolutionary Algorithms (EAs) for optimising VLAN number and security	Used hybrid Pareto-based fitness measure to optimise VLANs for connectivity and security	Demonstrated that EAs can optimise VLAN grouping to minimise the number of VLANs while ensuring security and connectivity.	VLAN, Evolutionary Algorithms, Optimization	Balancing security and connectivity with minimal VLANs	Investigating EA applications for large, dynamic networks.

Conclusion

VLAN is a logical network segment within a physical network that allows devices to be grouped together based on their function, regardless of their physical location, essentially creating separate broadcast domains within a single network, improving performance and security by managing traffic more efficiently. In conclusion, VLANs are essential for modern network design, offering improved performance, security, and scalability by logically segmenting networks into smaller broadcast domains. They provide benefits such as cost savings, easier management, and enhanced security but also present challenges like configuration complexity and security vulnerabilities. Emerging technologies, including Software-Defined Networking (SDN), VXLAN, and AI, are enhancing VLAN capabilities, enabling more dynamic, secure, and scalable networks. As network requirements grow, VLANs will continue to evolve, integrating with technologies like Zero Trust and blockchain to address future demands for flexibility, security, and performance. Future innovations will likely address current limitations, making VLANs even more efficient and robust for tomorrow's networking challenges.

References

[1] Y. A. Makeri, G. T. Cirella, F. J. Galas, H. M. Jadah, and A. O. Adeniran, "Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement On Network Security For Enterprise," *Int. J. Adv. Netw. Appl.*, 2021, doi: 10.35444/ijana.2021.12604.

[2] G. P. Pal and S. Pal, "Virtual Local Area Network (VLAN)," *Int. J. Sci. Res. Eng. Technol.*, 2013.

[3] A. F. Gentile, P. Fazio, and G. Miceli, "A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and

Mobile Scenarios," *Telecom*, 2021, doi: 10.3390/telecom2040025.
[4] A. Lara, A. Kolasani, and B. Ramamurthy, "Simplifying network management using Software Defined Networking and OpenFlow," in *2012 IEEE International Conference on Advanced Networks and Telecommunciations Systems, ANTS 2012*, 2012. doi: 10.1109/ANTS.2012.6524222.
[5] R. Camacho and E. Inga, "State of Art, Cognitive Radio for Virtual Network Operator on Advanced Metering Infrastructure," *IEEE Lat. Am. Trans.*, 2015, doi: 10.1109/TLA.2015.7332134.
[6] K. Dixit, P. Pathak, and S. Gupta, "A new technique for trust computation and routing in VANET," in *2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*, 2016. doi: 10.1109/CDAN.2016.7570944.
[7] S. Gupta and A. Mathur, "Enhanced flooding scheme for AODV routing protocol in mobile ad hoc networks," in *Proceedings - International Conference on Electronic Systems, Signal Processing, and Computing Technologies, ICESC 2014*, 2014. doi: 10.1109/ICESC.2014.60.
[8] V. G. Nguyen and Y. H. Kim, "SDN-based enterprise and campus networks: A case of VLAN management," *J. Inf. Process. Syst.*, 2016, doi: 10.3745/JIPS.03.0039.
[9] E. P. Ruaya and M. V. M. Buladaco, "Virtual Local Area Network (VLAN) Network Design for NEMSU- Administration Building," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 11, no. 6, pp. 294–298, Dec. 2022, doi: 10.30534/ijatcse/2022/101162022.
[10] A. Mehdizadeha, K. Suinggia, M. Mohammadpoorb, and H. Harun, "Virtual Local Area Network (VLAN): Segmentation and Security," *Proc. Third Int. Conf. Comput. Technol. Inf. Manag.*, 2017.
[11] C. O. Agwu, N. E. Nwogbaga, and C. N. Ojiugwo, "The Proposed Roles of VLAN and Inter-VLAN Routing in Effective Distribution of Network Services in Ebonyi State University," *Int. J. Sci. Res.*, 2013.
[12] V. Rajaravivarma, "Virtual local area network technology and applications," in *Proceedings of the Annual Southeastern Symposium on System Theory*, 1997. doi: 10.1109/ssst.1997.581577.
[13] S. D. Krothapalli, X. Sun, Y. W. E. Sung, S. A. Yeo, and S. G. Rao, "A toolkit for automating and visualizing VLAN configuration," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2009. doi: 10.1145/1655062.1655075.
[14] D. Álvarez, P. Nuño, C. T. González, F. G. Bulnes, J. C. Granda, and D. García-Carrillo, "Performance Analysis of Software-Defined Networks to Mitigate Private VLAN Attacks," *Sensors*, 2023, doi: 10.3390/s23041747.
[15] C. Cheng, Q. Huang, and L. Wang, "A Study of VLAN aggregation implementation," *Wuhan Ligong Daxue Xuebao (Jiaotong Kexue Yu Gongcheng Ban)/Journal Wuhan Univ. Technol. (Transportation Sci. Eng.*, 2005.
[16] X. Li and C. Cheng, "Discuss on VLAN stacking in packet network," in *2009 International Symposium on Intelligent Ubiquitous Computing and Education, IUCE 2009*, 2009. doi: 10.1109/IUCE.2009.131.
[17] V. Pereira, M. Rocha, and P. Sousa, "Traffic Engineering with Three-Segments Routing," *IEEE Trans. Netw. Serv. Manag.*, 2020, doi: 10.1109/TNSM.2020.2993207.
[18] R. Davoli and M. Goldweber, "VXVDE: A switch-free VXLAN replacement," in *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*, 2015. doi: 10.1109/GLOCOMW.2015.7414109.
[19] Sahil Arora and Apoorva Tewari, "Zero trust architecture in IAM with AI integration," *Int. J. Sci. Res. Arch.*, vol. 8, no. 2, pp. 737–745, Apr. 2023, doi: 10.30574/ijsra.2023.8.2.0163.
[20] Y. J. Wu, J. X. Liang, H. Zhang, Z. W. Lin, Y. Ma, and Z. Tian, "Programmable virtual network instantiation in IaaS cloud based on SDN," *J. China Univ. Posts Telecommun.*, 2013, doi: 10.1016/S1005-8885(13)60234-4.
[21] O. Okoro, E. A. Edim, O. A. Ofem, E. Essien, I. O. Obono, and B. P. Tawo, "Improving security in a virtual local area network," *J. Theor. Appl. Inf. Technol.*, 2022.
[22] M. A. Hossain, H. Miah, R. Ahmed, and S. Anower, "Secure Inter-VLAN routing in multi branches office network," *Int. J. Commun. Inf. Technol.*, 2023, doi: 10.33545/2707661x.2023.v4.i2a.65.
[23] G. Leischner and C. Tews, "Security through VLAN segmentation: Isolating and securing critical assets without loss of usability," *Interface*, 2008.
[24] R. Bishukarma, "Scalable Zero-Trust Architectures for Enhancing Security in Multi-Cloud SaaS Platforms," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1308–1319, 2023, doi: 10.48175/IJARSCT-14000S.
[25] Y. Zhou, Y. Wang, J. Yu, J. Ba, and S. Zhang, "Load balancing for multiple controllers in SDN based on switches group," in *19th Asia-Pacific Network Operations and Management Symposium: Managing a World of Things, APNOMS 2017*, 2017. doi: 10.1109/APNOMS.2017.8094139.
[26] R. Bishukarma, "Optimising Cloud Security in Multi-Cloud Environments : A Study of Best Practices," *TIJER – Int. Res. J.*, vol. 11, no. 11, pp. 590–598, 2024.
[27] B. Patel, V. K. Yarlagadda, N. Dhameliya, K. Mullangi, and S. C. R. Vennapusa, "Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering," *Eng. Int.*, vol. 10, no. 2, pp. 117–130, 2022, doi: 10.18034/ei.v10i2.715.
[28] A. F. Gentile, D. Macrì, E. Greco, and P. Fazio, "Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment," *Futur. Internet*, vol. 16, no. 8, 2024, doi: 10.3390/fi16080283.
[29] D. Li, Z. Yang, S. Yu, M. Duan, and S. Yang, "A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology," *Futur. Internet*, vol. 16, no. 9, 2024, doi: 10.3390/fi16090320.
[30] J. B. Madavarapu, F. H. Mohammed, S. Salagrama, and V. Bibhu, "Secure Virtual Local Area Network Design and Implementation for Electronic Data Interchange," *Int. J. Adv. Comput. Sci. Appl.*, 2023, doi: 10.14569/IJACSA.2023.0140701.
[31] 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*, 2023, doi: 10.3390/computers12020028.
[32] T. O. Alani and A. M. Al-Sadi, "Survey of optimizing dynamic virtual local area network algorithm for software-defined wide area network," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 21, no. 1, p. 77, Feb. 2023, doi: 10.12928/telkomnika.v21i1.24249.
[33] R. Romansky, "An approach for optimized architectural design of virtual local area network," *Commun. Cogn.*, 2022, doi: 10.57028/c55-119-z1025.
[34] R. Chen, M. Yan, and Z. Qiu, "Application of Virtual Local Area Network Technology in Smart Grid," in *Advances in Intelligent Systems and Computing*, 2020. doi: 10.1007/978-3-030-43306-2_9.
[35] A. P. Rodríguez, E. W. Fulp, D. J. John, and J. Cui, "Using evolutionary algorithms and pareto ranking to identify secure virtual local area networks," in *GECCO 2020 Companion - Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion*, 2020. doi: 10.1145/3377929.3398089.