Enhancing Data Center Performance using Virtual Extensible LAN (VXLAN) EmergingTechnology

Adel Ali Eluheshi[1] ; Zahra Abdalla Elashaal[2] ; Asra Abobker Alazragh[3] .

1- Libyan Academy, Tripoli, Libya
dept. of Electrical and Computer Engineering
adel.eluheshi@academy.edu.ly

2- University of Tripoli, Tripoli, Libya
Faculty of Faculty of Information Technology,
z.elashaal@uot.edu.ly

3- Libyan Academy, Tripoli, Libya
dept. of Electrical and Computer Engineering
eabalazragh@gmail.com

Abstract

As more and more people turn to the cloud for their personal and professional purposes, cloud computing has become essential for the majority of users. Given the increased demand for cloud virtualization, the datacenter needs to be able to accommodate more virtual machines (VMs) that are housed on its servers. A datacenter employing old technology may accommodate up to 4096 VLANs, which would restrict the number of tenants it could serve. Spanning-Tree Protocol (SPT) is used by VLANs to remove loops, or duplicates, which block half of the routes and waste available bandwidth. The Virtual Extensible LAN (VXLAN), an emerging technology, must be used from there. It permits network seg- mentation similar to that of regular VLANs without obstructing traffic or reducing scalability. This study outlined both established and novel approaches and then clarified how to use them for data center topology. It also covered the drawbacks of utilizing conventional technologies. The benefits of cutting-edge technology and its superior influence on datacenter bandwidth utilization. To demonstrate how the new technology enhances data center performance, these technologies were lastly replicated using the Eve emulator.

Keywords: Cloud virtualization, Virtual machines, Professional purposes,Cloud computing, Eve emulator, LAN, VXLAN, SPT.

1 Introduction

LANs are physical networks used for computer sharing and information ex- change. They were first created in the 1960s for research institutes, colleges, and universities. Virtual LAN (VLAN) technology divides LANs into multiple broadcast domains, allowing logical isolation among tenants. VXLAN technology, which uses UDP port 4789, allows Layer 2 overlay networks to communicate. VXLANs can extend Layer 3 networks, enabling data centers or cloud environments to be isolated. VXLANs also provide resilient routing algorithms for bandwidth usage and network performance optimization [8, 9, 12]. Research by Talvinder, Varun, and Satish investigates how virtual private cloud services may be provided using both established and new technologies in DC networking topologies. They emphasize the difficulties with standard VLANs and the significance of EVPN and VXLAN in managing big tenant networks. The research by Dennis and Sai examines the development of carrier cloud networking while addressing issues with restricted virtual machine mobility, scalability limitations, and non-optimized forwarding. They talk about improved scalability, efficient L3 routing, LISP, and VXLAN as solutions. Both researches are theoretical and have not been put into practice [2, 12].

1.1 Problem Statement

Due to the widespread adoption of cloud computing for both personal and business purposes, cloud computing is growing in popularity. Data centers must thus provide additional room for virtual machines (VMs) on servers. VLANs enable up to 4096 VLANs (12-bit VLAN IDs), which logically separate tenants, lessen broadcast traffic, and enhance network security. However, because VLANs only o er 4094 VLAN IDs, which is insufficient for data centers with a large number of VMs, they are limited in their potential to scale. Additionally, because of the Spanning-Tree Protocol (SPT), VLANs can block pathways and result in bandwidth loss.

1.2 proposed solution

Emerging technology (VXAN), which enables network segmentation without blocked pathways and restricted scalability, is required to overcome these problems. VXLAN offers higher scalability with a 24-bit segment ID, allowing up to 16 million VXLAN segments for high-number virtual machines in datacenters or cloud networks. It also maximizes bandwidth utilization by using Layer 3 equal-cost multipath (ECMP) routing instead of Spanning-Tree Protocol (SPT), which disables nearly half of available paths in the network. So, the question here is, how VXLAN enhances the utilization of Bandwidth based on Equal-cost multi-path routing (ECMP) in network.

1.3 Research Methodology

Reviewing the fundamentals of VLAN and VXLAN technology, designing and configuring a network utilizing both classic VLAN and emerging VXLAN scenarios, contrasting the advantages and advancements of VXLAN, and debating the distinctions between emerging and traditional technology are the objectives of this study. The implementation was made by using emulation software.

2 VLAN Technology

VLAN technology divides a physical LAN into multiple groups, enabling hosts to interact directly as in Figure 1. This simplifies administration and adapts to network changes. VLANs can group networks logically, even if physical locations are separated. They reduce congestion on large LANs [6].

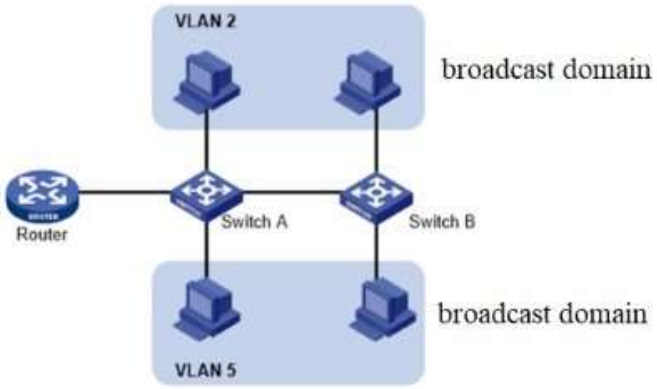
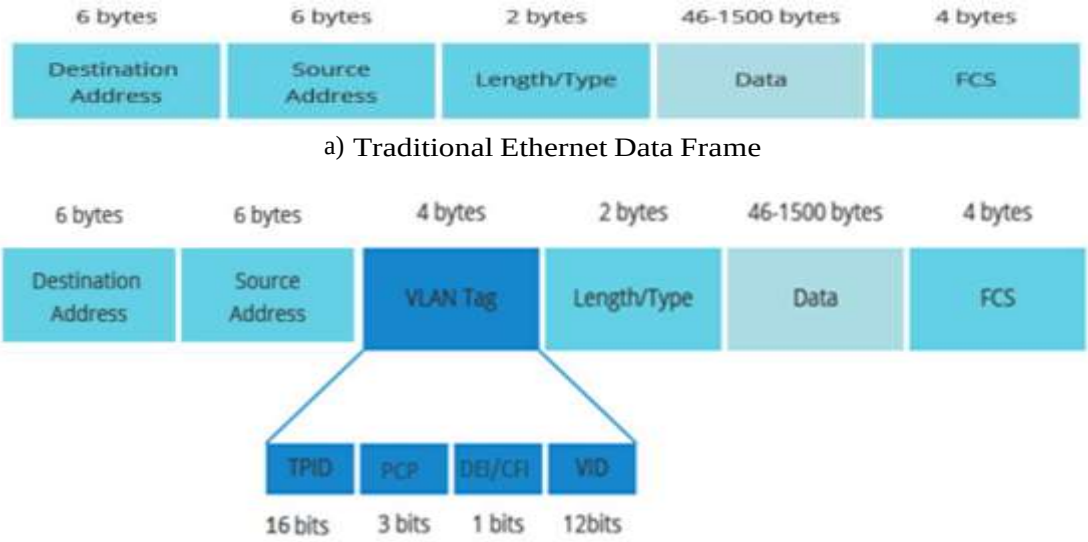


Figure 1: VLAN Multiple Broadcast Domain

2.1 VLAN Ethernet Frame

Layer 2 switches identify VLAN frames by inserting a VLAN Tag into data link layer encapsulation. Sincoskie invented this concept, tagging each frame with a color, now known as IEEE 802.1Q. VLANs create network traffic split over multiple networks [7].

Figure 2 shows the VLAN Tag is a 4-byte add to an Ethernet frame header, containing the Tag protocol identifier (TPID), Priority code point (PCP), Drop eligible indicator (DEI), and VLAN identifier (VID).



a) Traditional Ethernet Data Frame

b) VLAN Data Frame

Figure 2: Data Frames

It coordinates frames between dispersed VLANs across switches using the VLAN tag communication mechanism. In a network with 90 VLAN ports, two switches A and B are set as "tagged" member ports of VLAN 90 as shown in Figure 3. A tagged frame is delivered to switch A, and if it's compatible with that VLAN, it's correlated with that VLAN.

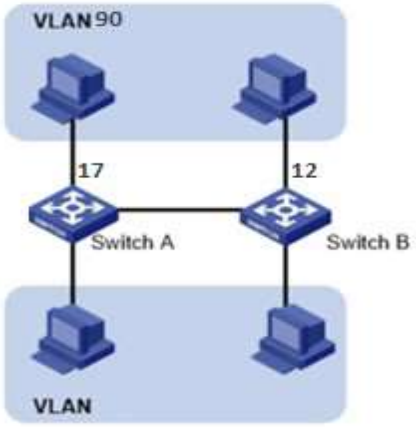


Figure 3: VLAN Tag working

2.2 VLAN Types and its Connections

The implementation of VLANs, including port-based VLANs, MAC-based VLANs, and IP subnet-based VLANs as following:

- VLANs are network interfaces that allow devices to be connected in two ways: VLAN-aware and VLAN-unaware. Port-based VLANs allow for manual configuration on switch ports, making them suitable for small networks without regular infrastructure changes.
- MAC address-based VLANs assign MAC addresses to VLANs, keeping a table of related VLAN memberships on each switch.
- IP subnet-based VLANs assign VLANs according to devices' IP subnets, suitable for public networks with mobility, simplified management, and lower security demands [13].

VLANs can be used in two ways: VLAN-aware devices understand VLAN memberships and formats, and access links belonging to a single VLAN. Trunk links connect switches and can handle multiple VLAN traffic.

2.3 Spanning Tree Protocol (STP) (IEEE 802.1D)

Switch topology monitoring (STP) is a Layer 2 switching protocol that pre- vents switch loops by creating a single path tree structure through the network. STP uses a root bridge as a reference point to identify redundant paths and block redundant links. Switches send Bridge Protocol Data Units (BPDUs), as shown in Figure 4, to multicast addresses every 2 seconds, selecting the best link towards the root for forwarding and blocking other redundant links. The Root Bridge is the switch with the lowest Bridge ID, with the non-Root Bridge considering one port as a ROOT PORT (RP) with less cost.

VLAN technology reduces broadcast domain size and allows logically connected devices to act as their own networks. It can support up to 4096 VLANs. (12-bit VLAN ID). However, STP technology may not realize full network capacity due to traffic restrictions.

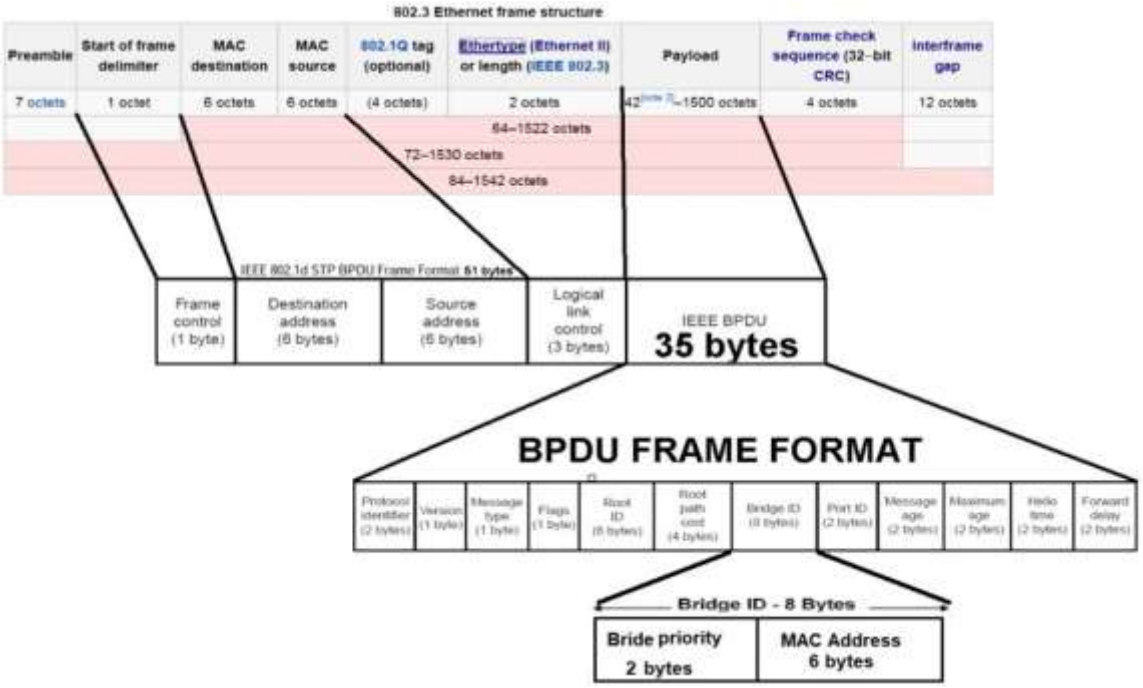


Figure 4: STP and BPDU frame

3 VXLAN Technology

The Internet Engineering Task Force (IETF) defines VXLAN, or virtual extensible local area network, as an extension of network virtualization over Layer 3 technology. It is the industry standard overlay technology for creating data center networks because it can adapt to the demands of multi-tenancy and dynamic virtual machine immigration. Using a tunneling technology called VXLAN, de- vices can build a tunnel across an IP network through which user-side traffic can be encapsulated and forwarded as shown in Figure 5. Before transferring a Layer 2 Ethernet frame over a Layer 3 network, it encapsulates it in a UDP packet [11].

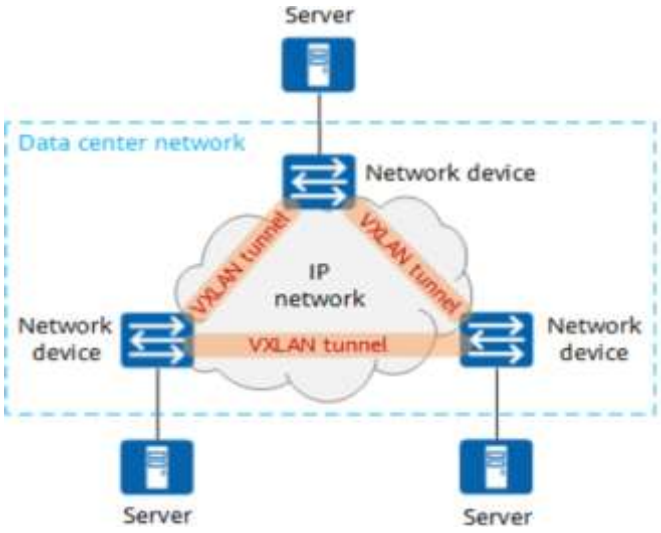


Figure 5: VXLAN tunnel

VXLAN can provide data center networks with greater scalability when the number of tenants increases

quickly, and many tenants need to be isolated. It can make use of every network path that is available to handle high data traffic volumes. For VXLAN tunneling, as shown in Figure 6, two networks are needed: an overlay that represents a logical network and an underlay that represents a physical network in charge of packet transfers [5]. In summary, VXLAN is a popular overlay technology that enables dynamic virtual machine (VM) immigration and multi-tenancy in data center networks. It is supported by Cisco Nexus switches and can provide layer2 connectivity extension across the Layer3 boundary.

3.1 Control and Data Planes

Control and data planes are crucial in network communication, explaining how packets travel through the network. Control planes handle data processing, while data planes describe how devices forward packets. The Management Plane includes local device management traffic, while the Data Plane is high-speed.

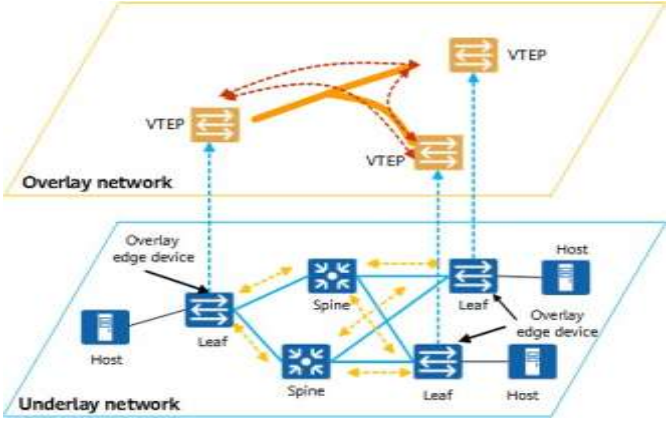


Figure 6: Overlay and Underlay networks.

path through the device. VXLAN encapsulation is a significant aspect of net- work traffic, with VTEPs adding several new headers as seen in Figure 7 [4].

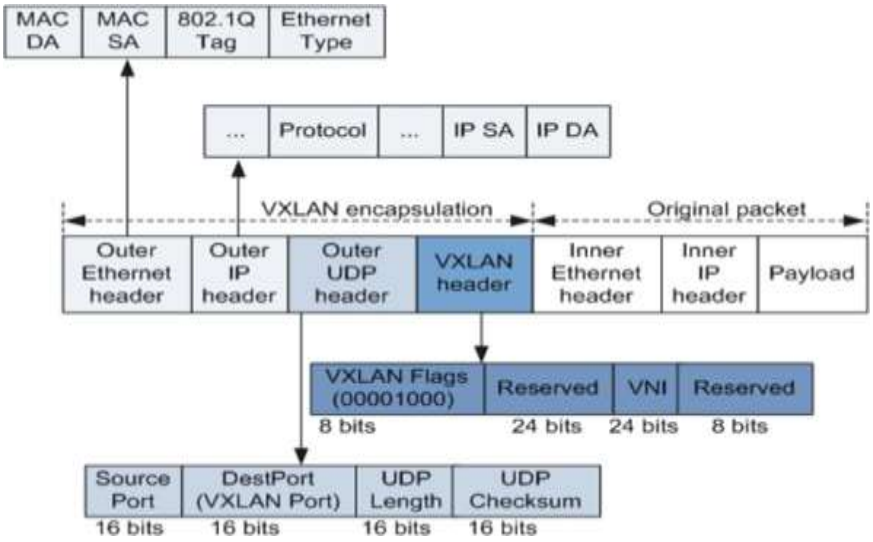


Figure 7: VXLAN Headers

The VXLAN header consists of four parts: Reserved (8 bits), VNI (24 bits), Reserved (24 bits), and Flags (8 bits). Outer UDP header uses a destination port of 4789 and a random source port, while Outer IP header includes VXLAN source and destination addresses. Outer MAC headers include MAC DA

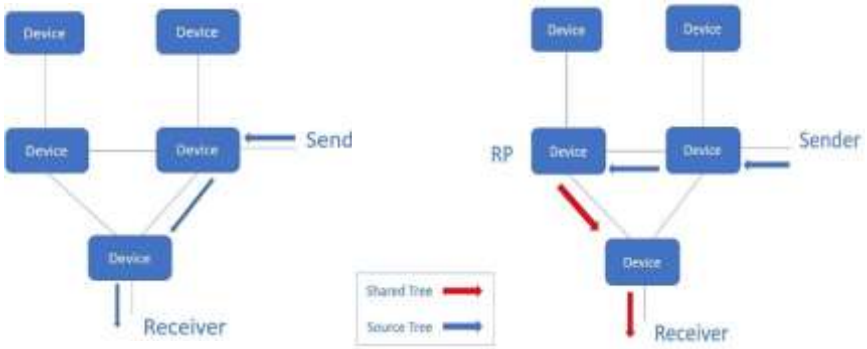
(destination MAC address) and MAC SA (source MAC address).

VXLAN definitions include VXLAN Tunnel Endpoint (VTEP), Virtual Net- work Identifier (VNI), and Network Virtualization Edge (NVE). VTEPs map VLAN segments to VXLAN segments in tenants' end devices, perform VXLAN encapsulation and decapsulation, and can support up to 16 million segments. NVEs are overlay interfaces in Cisco equipment used to de ne VTEPs [4]. So that control and data planes are essential in network communication, with VXLAN encapsulation plays a crucial role in ensuring efficient network traffic.

3.2 VXLAN Operates

The VXLAN tunneling protocol encapsulates Layer 2 Ethernet frames in Layer 3 UDP packets, creating virtualized Layer 2 subnets. Each subnet is uniquely identified by a VXLAN network identifier (VNI). The VXLAN tunnel endpoint (VTEP) handles packet encapsulation and decapsulation. VXLAN with flood and learning behavior uses Any-source multicast (ASM) Protocol Independent Multicast for multicast functionality. Protocol-Independent Multicast (PIM) is a group of multicast routing protocols for IP networks, allowing one-to-many and many-to-many data distribution [1][3].

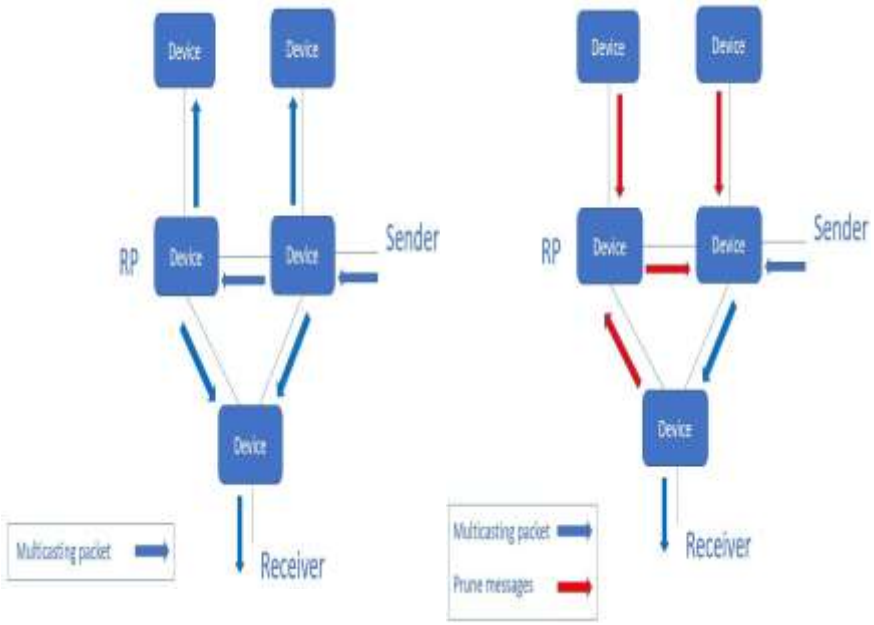
Multicast forwarding uses Reverse Path Forwarding (RPF) to avoid floods and loops in networks. To send multicast traffic, a state and multicast distribution tree are needed. The shortest path minimizes latency while maintaining state information for every source. As shown in Figure 8, shared distribution trees use a Rendezvous Point (RP) to limit resources and minimize overhead [10].



a) Source Distribution Tree b) Shared Distribution Tree

Figure 8: Source and Shared Distribution Tree

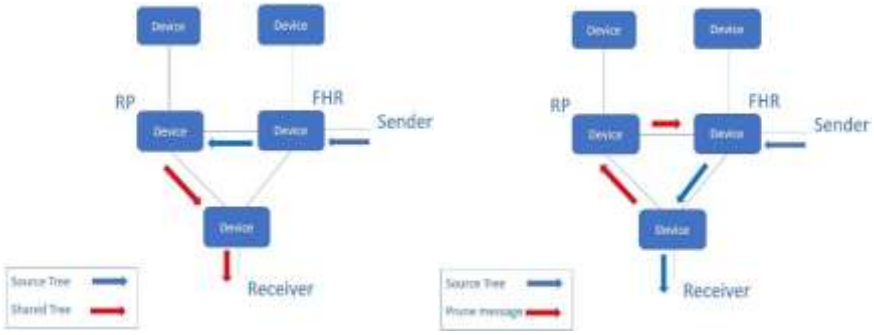
Protocol Independent Multicast (PIM) is a group of multicast routing protocols with two modes: sparse and dense. PIM dense floods traffic, allowing devices not interested to remove themselves as shown in Figure 9, and prunes traffic after 4 minutes. PIM-SM is a mode where multicast traffic is only sent when requested. It operates using the Rendezvous Point (RP), as the router shown in Figure 10. The mode starts with an IGMP Join message from the receiver device to the first hop router (FHR), then sends a PIM Join to the RP. The RP decapsulates the packet and creates an SPT.



a) PIM-DM Flooding b) PIM-DM Pruning

Figure 9: PIM-DM Flooding and Pruning

So VLAN, a classic network isolation solution, offers tenant isolation of 4096, but VXLAN creates virtual tunnels between switches, enabling dynamic virtual machine migration.



a) PIM Sparse, source and shared tree b) SPT Switchoverg

Figure 10: PIM Sparse, source and shared tree and SPT Switchover

4 Implementation and Results

This study contrasts traditional (VLAN) and developing (VXLAN) technologies using two scenarios, shows how to implement both using the same topology, and explores the distinctions between the two. The Emulated Virtual Environment (EVE-NG) platform, which enables companies to construct virtual proof-of- concepts and training environments, was used to set up the work environment. VMware ESXi was developed as a virtual machine that ran without an operating system directly on system hardware. Four Cisco Nexus 9000v switches and four PCs at the access layer were used to set up the network.

4.1 Simulation Topology Used

The study employs a spine-leaf architecture in a data center network topology, consisting of two switching layers, spines and leafs. Leaf switches aggregate server traffic and connect directly to the spine, while

spine switches interconnect all leaf switches as indicated in Figure 11. The Nexus 9000v Switch serves as spines and leaf switch.

4.2 VLAN Implementation

The simulation involves applying VLAN technology in a topology, using Port- based VLANs (interface-based VLAN) type and assigning VLANs for each switch via port. The topology includes SPINEs and LEAFs, with links connected to end devices in ACCESS mode and links connecting directly into the SPINEs or core network in TRUNK mode. All links in SPINE switches are set in TRUNK mode. To verify the VLAN settings, the command is applied to all nodes. The LEAF-1 and LEAF-2 have four interfaces, two belonging to both VLANs 100 and 200, connected to SPINE switches as trunk links. The SPINE-1 and SPINE-2 have two interfaces, both belonging to VLANs 100 and 200, connected to LEAF switches as trunk links, as indicated in Figure 11. The STP Election Process, shown in Table 1, begins when switches are turned on for the first time, defining which switch is the ROOT bridge.

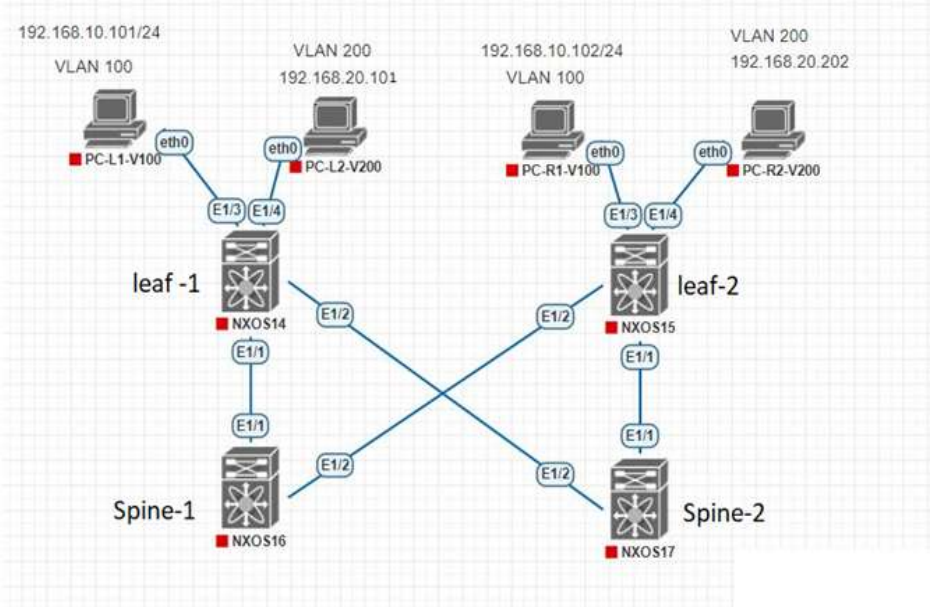


Figure 11: spine-leaf topology architecture

The network device with the lowest MAC address in the VLAN becomes the Root Bridge.

Table 1: STP Election Process

Name	Name	Most Significant bits of MAC Address	Root
LEAF 1	NXOS 14	50b6	No
LEAF 2	NXOS 15	5082	No
SPINE 1	NXOS 16	50f0	No
SPINE 2	NXOS 17	501b	Yes

4.3 VXLAN Implementation

The second part of the simulation involves applying VXLAN technology in the topology shown in Figure 12. The topology will be used for VLAN implementation, starting with configuring PCs, then encapsulating the upper section into an overlay network (VTEPs), and finally encapsulating the lower section into an underlay network.

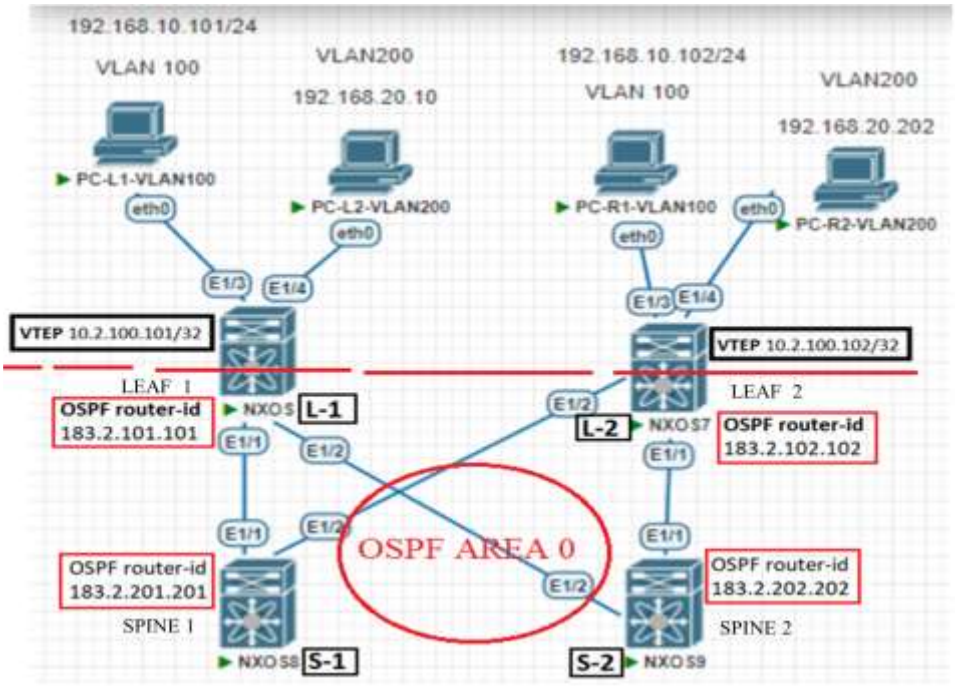


Figure 12: VXLAN Topology with Overlay and Underlay network.

4.3.1 Overlay Network

To configure VTEPs, which encapsulate classical frames to VXLAN packets, create a VTEP in each LEAF node as an NVE interface (Virtual Interface). Enable features in each LEAF, as indicated in the Table 2, create VLAN 100 and 200, map VLAN 100 to VNI 101000 and 200 to VNI 202000 using the vn-segment command, create a loopback 100 in each LEAF, advertise in OSPF AREA 0, and create a virtual interface (NVE interface) representing a VTEP.

Set the links connected to PCs as access mode, with interfaces Ethernet1/3 connected to VLAN 100 and Ethernet1/4 connected to VLAN 200.

Table 2: Features Purpose

Feature	Purpose
interface-VLAN	Enables VLAN interface mode. That connects a VLAN on the device to the Layer 3 router engine on the same device
vn-segment-vlan-based	Mapping VLANs to VXLAN
nv overlay	Enables VXLAN

4.3.2 Underlay Network

The configuration of an underlay network (layer-3) is described, utilizing the OSPF protocol as the routing protocol. The OSPF and PIM features are enabled, and the IP's transporter belongs to the single OSPF AREA 0. The PIM multicast routing protocols must be configured on all interfaces in nodes belonging to the underlay network, both physical and virtual.

Table 3: The Interfaces' IP

Node	IP	Interfaces
LEAF 1	183.2.101.101	Loopback 0 for E1/1 and E1/2
LEAF 2	183.2.102.102	
SPINE 1	183.2.201.201	
SPINE 2	183.2.202.202	

As shown in Table 3, a loopback 0 is created in all nodes, and the same IP is set as router-id to provide a unique identity to the OSPF Router. The same IP is set to physical interfaces via the IP Unnumbered feature, which con- serves network and address space. Multicast functionality is needed for VXLAN (flood and learning) behavior, and Any-source multicast (ASM) Protocol Inde- pendent Multicast- Sparse Mode (PIM-SM) is used. PIM Sparse Mode requires a Rendezvous Point (RP) to connect the ow source to the switch next to the receiver. Anycast RP methods are used to create RP. Two SPINEs are configured to provide RP service, creating unique loopbacks (unique-IP) in SPINE 1 and SPINE 2, and creating a shared-IP loopback 200 on both SPINEs, as in Figure 13. These IPs are advertised in the IGP (OSPF) and set as members in RP-anycast. The final step involves each device in the infrastructure learning the identity of the RP IP, advertising the shared-IP loopback 200 as the RP of the multicast environment in all nodes LEAFs and SPINEs.

The command "Switch Show vxlan interface" was applied to LEAFs node for VXLAN verification, confirming the correct setting. LEAF-1 and LEAF-2 have four interfaces, with the only one belonging to the overlay network, identifying VXLAN.

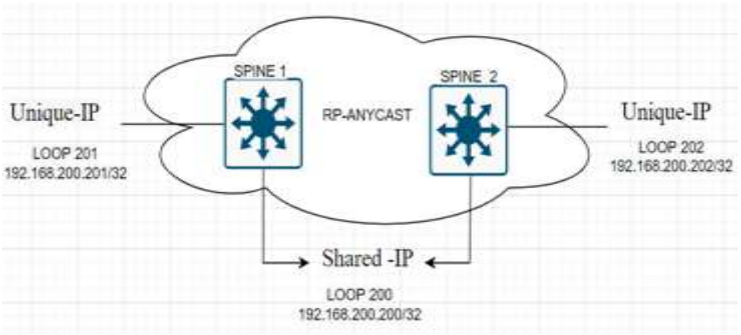


Figure 13: RP-anycast

4.4 The Scenarios

The study compared VLAN and VXLAN technologies using two scenarios:

- Ping between PCs in the same (VLAN/VXLAN) topology, and monitoringtraffic routes and paths,
- Dropping one path between LEAF and SPINE, and monitoring networkupdates.

4.4.1 VLAN Scenarios

The previously scenarios applied to the configuration of VLAN technology as:

VLAN PCs pinging Scenario After pinging from PC-L1 to PC-R1 which belong VLAN 100 to the architecture displayed in Figure 11. The traffic entering the network (LEAF-2/NXOS15) is monitored through interfaces E1/1 and E1/2. The traffic passes through interface E1/1 in LEAF2, with LEAF 1 taking the path as the traffic route. There is no traffic in interface (E1/2) in LEAF2, indicating that the path linked to this interface has been blocked. This is due to SPINA 2 being selected as the ROOT in the network, causing a loss in available bandwidth. The reason for this is the use of VLAN using STP.

The packet inspection on the (LEAF 2) reveals that the Ethernet section of the packet contains the MAC address of PC-L1 and the IP version 4 configuration of PC-R1. The 802.1Q virtual LAN section displays the VLAN tag, but the priority and DEI are not set. The ID set 100 represents VLAN 100. When the packet arrives at PC-R1, the section of 801.1Q virtual LAN disappears, as the LEAF 2 removes the trunk

header before forwarding the packet. The PC has no knowledge about VLAN TAG and VLAN in general.

VLAN Path Dropping Scenario: The text describes a process to drop the path between LEAF-1 and SPINE-2 in E1/2, as shown in Figure 14, and monitor traffic coming to (leaf-2) in E1/1 and E1/2. The first step involves cutting the path and shutting down the interface. After the shutdown, traffic starts falling asE1/2 is the only route in the topology. However, the other path remains blocked, and the root bridge status of SPINE 1 and SPINE 2 remains unchanged.

4.4.2 VXLAN Scenarios

The two scenarios applied to the configuration of VXLAN technology was:

VXLAN PCs pinging Scenario: The ping traffic from PC-L1 to PC-R1 in VLAN 100 is monitored through interfaces E1/1 and E1/2 in LEAF-2/NXOS15 as shown in Figure 12. The traffic is transferred using OSPF, which takes advantage of Layer 3 equal-cost multipath (ECMP) of available paths. The traffic sequence separates between both paths, with E1/2 passing the request of packet sequence number 99 and E1/1 passing the replay of packet sequence number 99. This load balance ensures the best use of bandwidth utilization, as routing protocols allow traffic to be balanced between both paths. This is an advantage of using routing protocols.

The packet inspection reveals that it arrived on LEAF 2 at interface E1/2 before being transferred to PC-R1. The Ethernet section displays the MAC address of SPINE 1, represented as a Source MAC, and the Destination MAC as LEAF 2. The Virtual extensible Local Area Network section displays the VXLAN header, VXLAN 10100 as VNI, with only the LEAFs (VTEPs) known about VXLAN VN-segment. The Internet Protocol Version section represents the IP of LEAF 1 with loopback 100 as Source IP and LEAF 2 with loopback 100 as Destin IP. The Ethernet sections display the MAC address of PC-L1, and the IP version 4 section shows the IP of PC-L1 and PC-R1. The UDP destination port of VXLAN is set by default at 4789.

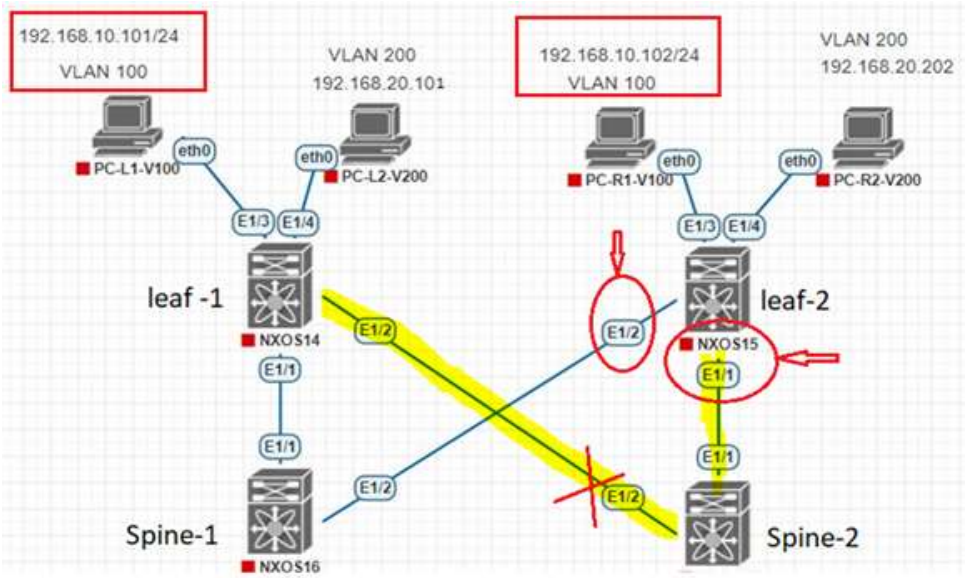


Figure 14: dropping the path in VLAN.

VXLAN Path Dropping Scenario: To monitor traffic coming to (leaf-2) in E1/1 and E1/2, cut off the path between LEAF-1 and SPINE-1 in E1/1 and E1/1, and shutdown the interface as shown in Figure 15. After shutdown, traffic will stop passing through interface E1/2 in LEAF 2. All traffic will be loaded to the second path interface E1/1 in LEAF 2. The last sequence received in interface E1/2 is a sequence 149-

request, where the replay-149 sequence received in interface E1/1. Despite one path being down, traffic passes normally without packet loss and the topology remains available and stable, unlike the situation with VLAN.

VXLAN technology offers higher scalability with a 24-bit segment ID, enabling up to 16 million VXLAN segments for high numbers of virtual machines in datacenters or cloud networks. It can support up to 4096 VLANs, unlike VLAN's 12-bit ID. VXLAN packets are transferred using OSPF, which takes advantage of Layer 3 equal-cost multipath (ECMP) routing to use all available paths, unlike Spanning-Tree Protocol (SPT) which disables half of available paths.

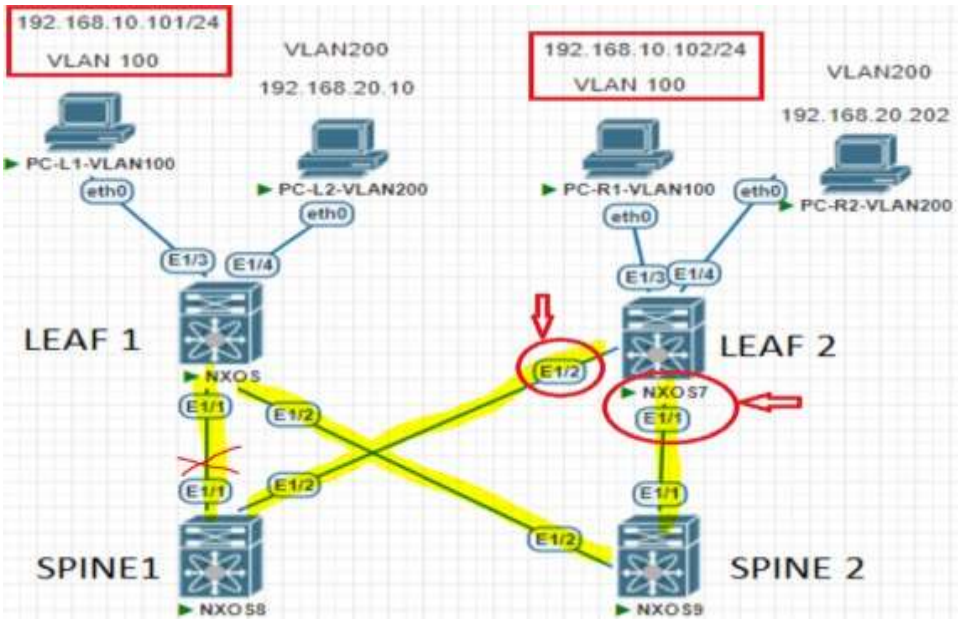


Figure 15: dropping the path in VXLAN.

5 Conclusion

The application of cutting-edge technology to data centers to boost efficiency is examined in this paper. To illustrate their benefits, it contrasts conventional VLAN and virtual VXLAN networks. Despite being small and fixed Layer 2 virtual networks, VLANs is a type of classical network isolation technology that can accommodate up to 4096 tenants; nonetheless, they are unable to allow large- scale dynamic virtual machine migration. By creating virtual tunnels between switches, VXLANs enable the data center network to be virtualized into a sizable Layer 2 virtual switch that can surpass the 802.1Q 4096 VLAN limit without compromising network stability. Using MAC-in-UDP encapsulation and tunneling, VXLANs can overlay numerous subnets over a data center infrastructure, extending layer 2 subnets across layer 3 network infrastructure. In order to take advantage of Layer 3 equal-cost multipath ECMP routing and guarantee ideal bandwidth utilization, they can also employ OSPF, BGP, or IS-IS protocols.

6 Future work

It is advised that future research that looking into Ethernet VPN (EVPN), another kind of VXLAN technology, for data center connectivity. VXLAN technology functions in the data plane of overlay

networks, while EVPN serves as the control plane. In EVPN VXLAN, the underlay employs eBGP as the routing protocol.

References

[1] Andrew Adams, Jonathan Nicholas, and William Siadak. Protocol inde- pendent multicast-dense mode (pim-dm): Protocol speci cation (revised). Technical report, 2005.

[2] Dennis Cai and Sai Natarajan. The evolution of the carrier cloud network- ing. In 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, pages 286 291. IEEE, 2013.

[3] Bill Fenner, Mark Handley, Hugh Holbrook, and Isidor Kouvelas. Pro- tocol independent multicast-sparse mode (pim-sm): Protocol speci cation (revised). Technical report, 2006.

[4] A Shaji George and AS Hovan George. A brief overview of vxlan evpn. Ijireeiceinternational Journal of Innovative Research in Electrical, Elec- tronics, Instrumentation and Control Engineering, 9(7):1 12, 2021.

[5] Bhoopendra Kumar, Sanjay Kumar Dhurandher, and Isaac Woungang. A survey of overlay and underlay paradigms in cognitive radio networks. In- ternational Journal of Communication Systems, 31(2):e3443, 2018.

[6] Jhansi Bharathi Madavarapu, Firdous Hussain Mohammed, Shailaja Sala- grama, and Vimal Bibhu. Secure virtual local area network design and implementation for electronic data interchange. International Journal of Advanced Computer Science and Applications, 14(7), 2023.

[7] Abbas Mehdizadeha, Kevin Suinggia, Mojtaba Mohammadpoorb, and Har- lina Haruna. Virtual local area network (vlan): Segmentation and security. In The Third International Conference on Computing Technology and In- formation Management (ICCTIM2017), volume 78, page 89, 2017.

[8] Larry L Peterson and Bruce S Davie. Computer networks: a systems ap- proach. Elsevier, 2007.

[9] Saravanan Ramesh. Securing VXLAN-based overlay network using SSH tunnel. University of Delaware, 2017.

[10] Alessandro Russo, Renato Lo Cigno, and Izhak Rubin. Protocol in- dependent multicast: From wired to wireless networks. In 2013 In- ternational Conference on Computing, Networking and Communications (ICNC), pages 610 615. IEEE, 2013.

[11] Faisal Shahriar, S Newaz, Syed Zahidur Rashid, Mohammad Azazur Rah- man, and Muhammad Foyazur Rahman. Designing a reliable and redun- dant network for multiple vlans with spanning tree protocol (stp) and fast hop redundancy protocol (fhrp). In Proc. Int. Conf. Ind. Eng. Oper. Manag, volume 2018, pages 534 540, 2018.

[12] Talvinder Singh, Varun Jain, and G Satish Babu. Vxlan and evpn for data center network transformation. In 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1 6. IEEE, 2017.

[13] Yogesh Yadav and Piyush Yadav. Virtual local area network. 2013.