Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Comparative Evaluation of VXLAN with Traditional Overlay Network Protocols

Hasan A. Saeed, Shavan Askar, Zhalla Soran, Dilshad Khoshnaw
hasan.saeed@epu.edu.iq, shavan.askar@epu.edu.iq
Information System Engineering, Technical College of Engineering, Erbil Polytechnic University, Erbil, 44001, Iraq

Article Information

Submitted : 21 Mar 2024
Reviewed: 25 Mar 2024
Accepted : 8 Apr 2024

Keywords

Underlay & Overlay network, VXLAN-EVPN, VXLAN-LISP

Abstract

This article examines various network virtualization technologies, including Virtual Extensible LAN (VXLAN), as well as overlay network protocols such as VXLAN-EVPN (Ethernet VPN) and VXLAN-LISP (Locator/Identifier Separation Protocol). These protocols play a crucial role in improving the scalability and flexibility of big cloud computing infrastructures. While each of these technologies can be employed to expand a Layer 2 connection across an already established network, they possess unique qualities and applications. The objective is to offer a comprehensive comprehension of these technologies and their suitability in diverse network contexts. VXLAN-EVPN has higher performance in terms of encapsulation speed and reduced packet overhead, rendering it highly suitable for high-speed and large-scale deployments. Conversely, VXLAN-LISP demonstrates superior network latency and interoperability, offering benefits in multi-tenant and geographically distributed networks. VXLAN can be combined with other widely used overlay network protocols, including Generic Network Virtualization Encapsulation (GENEVE), Stateless Transport Tunneling (STT), and Network Virtualization using Generic Routing Encapsulation (NVGRE). The objective is to offer a comprehensive comprehension of these technologies and their suitability in diverse network contexts.

A. Introduction

VXLAN-EVPN is a network architecture that enhances Layer 2 connectivity by overlaying a virtual network in addition to an existing physical network. VXLAN is an open standards technology that enables the interconnection of VXLAN networks using an existing infrastructure. EVPN multihoming enables the connection of a Layer 2 device or an end host device to multiple leaf switches in the VXLAN network, ensuring redundancy. BGP EVPN MAC learning is a control-plane mechanism based on factors (MPBGP) that enables the discovery of remote VTEPs and the advertisement of MAC address and MAC/IP information. EVPN serves as a control plane for VXLAN, aiming to minimize network flooding and handle scalability concerns. It is frequently employed in the implementation of data centers on a big scale.[1]. VXLAN-LISP integrates the VXLAN overlay technology with the LISP control plane. It offers a resolution for the scalable and efficient movement and freedom from location constraints in corporate networks. VXLAN-LISP decouples the identification (ID) of a device from its location (Locator), enabling seamless mobility of devices across various locations without the need to modify their IP addresses. It is frequently employed in enterprise campus networks.[2]

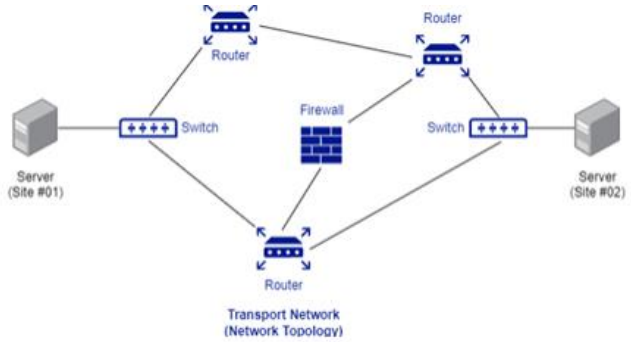

Figure-1 Underlay network

1. Underlay Network

An underlay network refers to the tangible framework that serves as the basis for the virtual network. The network infrastructure comprises switches, routers, and other networking hardware responsible for facilitating the transmission of data packets between physical devices. The primary purpose of the underlay network is to expeditiously and effectively transmit data packets, prioritizing low latency and high performance. In figure-1 [1], conventional routing protocols such as OSPF or BGP are employed to ascertain the most efficient route between devices, thereby further optimizing performance. The underlay network serves as a dependable and expandable base for the virtual overlay network, guaranteeing the timely and efficient delivery of data packets.[2], [3].

1.1 Underlay Networks At Layer 2

The VLAN specifications are called into doubt in reference [4]. It permits the establishment of many LANs utilizing a single physical Ethernet connection. The bridges-switches in each VLAN are configured to offer unicast and broadcast connectivity. To enable these functions, VLAN tags are added into the Ethernet

frame. The network's VLAN-aware component analyzes these messages based on the tag fields. The VLAN tag consists of a 16-bit Tag Protocol Identifier (TPID) and a 16-bit Tag Control Information (TCI) that includes a 3-bit Priority Code Point (PCP), a single bit for the Drop Eligible Indicator (DEI), and a 12-bit VLAN-Identifier (VID). As a result, 4096 VLANs are possible [5].

1.2 Underlay Networks at Layer 3

The Internet is a Type 3 infrastructure network. For managing routes within an autonomous system (AS), the Open-Shortest-Path-First (OSPF) or Intermediate System to Intermediate System (IS-IS) protocol is used, whereas the Border-Gateway-Protocol (BGP) is used for transferring and connecting routes between AS. MPLS networks are a sort of historical underlay WAN technology that runs between Layers 2 and 3 of the network stack[6,7]

B. Overlay Network

An overlay network is a logical network that is constructed on top of an existing underlay network. The system is engineered to possess adaptability and expandability, enabling administrators to generate and oversee virtual networks as required. An overlay network is formed by enveloping data packets with supplementary headers that designate the virtual network. Administrators can utilize this feature to customize virtual networks that extend across multiple physical devices, including the ability to create virtual networks that are separate from the physical network structure. The overlay network's adaptability and scalability make it an effective tool for managing intricate data center environments. The overlay network has the capability to segregate traffic, establish tailored network structures, and ensure secure connectivity among several departments.[2], [8].Overlay networks, in essence, refer to logical networks that are built on top physical network, as seen in Figure-2 [7]. The Internet a superimposed layer constructed on top of the telephone network. The use of overlays involves the implementation of a decision-making process that is generally necessary in distributed applications. Every node in the overlay network is also present in the underlying physical network. However, the connections between the overlay nodes are established through the use of tunneling.Tunneling facilitates the transmission of packets from one endpoint to another. Overlay-networks facilitate the exploration of new internet protocols and the expansion of Internet functionality and features. BitTorrent is prime such as of peer-2-peer networks constructed utilizing overlay. [9].

	Underlay Network	Overlay Network
Protocols	Ethernet, IP, routing protocols, etc.	VXLAN, GRE, IPSec, etc.
Scalability	Hard to scale, less flexible than the overlay network	Easier to scale (more flexible) than the underlay network
Control	Mostly, hardware-based network traffic orchestration	Software-based network traffic orchestration
Encapsulation	Traditional layer 2, 3, and 4 (OSI) packets encapsulation	Requires extra encapsulation than the traditional headers
Flow	Traffic traverses network function devices	Traffic traverses virtual links in overlay nodes

Table 1

Overlay Transport Virtualization (OTV) is a method that separates the logical network from the physical network. This is achieved by using tunneling techniques and encapsulating traffic within IP packets, enabling it to cross layer 3 boundaries. Various protocols, such as VXLAN, NVGRE, and STT, utilize this technique as proposed standards by the IETF. While there are some differences among these protocols, they all employ a 24-bit identifier, allowing for over 16 million potential networks. In each case, the endpoints are part of a virtual network, regardless of their location in the underlying physical network.[5].

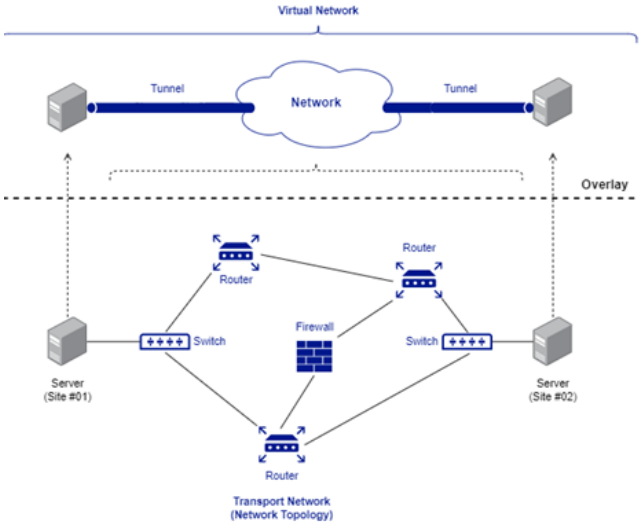

Figure-2 Overlay Network

C. Virtualizing Data Paths

3.1 Generic-Routing-Encapsulation (GRE)

Generic-Routing-Encapsulation (GRE) it is a protocol that encapsulates and transports network-packets over an IP network. Tunnels GRE is a protocol used in tunneling, which enables the transmission of packets overIP-based network by encapsulating and forwarding them. It offers connectivity to a diverse range of network-layer protocols. GRE was initially developed to facilitate the transportation of NoNroutable legacy protocols, such as Internetwork Packet Exchange (IPX), over an IP network. Nowadays, it is predominantly employed as an overlay for both IPv4 and IPv6. GREtunnel serve various purposes, as illustrated in figure-3.[2] They can be utilized to route traffic through a firewall or an ACL, to establish connections across separate networks, and can even act as a makeshift solution for flawed routing systems. Their primary utility is in their ability to establish Virtual-Private-Network (VPN)[10].

When a router encapsulates a packet for a GREtunnel, it extra header information is appended (referred to as encapsulation) to the packet. This added information includes the IP address of the remote endpoint as the destination. The new IP header enables the packet to be directed between the two tunnel endpoints without examining the payload of the packet. Once the packet arrives at the remote location

IP-Sec (InternetProtocol-Security)

IP-Sec (InternetProtocol-Security) is a network protocol that provides security for Internet Protocol (IP) communications. Internet-Protocol-Security (IP-Sec) is a collection of protocols that ensuring the security of IP communications at the network layer, as defined by the Internet Engineering Task Force (IETF). [3] IPSec is a security system that currently applies to all Internet communication. It offers the ability to certify data integrity, identify data origins, and defend against retransmission. The IPSec system employs three core security protocols: Authentication Header (AH), Encapsulation-Security-Payload (ESP), and Internet Key Exchange (IKE)[5]

Tunnel mode: This mode involves the encryption of the entire original packet and the addition of a newSet of IPsec headers. These additional a headers serve the purpose of routing the packet and also offer overlay functionality. The term "Authentication Header" refers to a security protocol used to provide authentication and integrity for IP packets in computer networks.

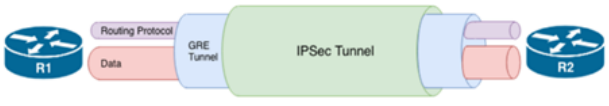

Figure-3

Transport mode: Provides encryption and authentication just for the packet payload. This mode lacks overlay functionality (ESP) and performs routing based on the original IP headers.[11]

ESP, or Encapsulating Security Payload, offers data confidentiality, authentication, and safeguards against packet replay attacks by hackers. In general, the term "payload" refers to the data without any additional information, such as headers. However, when discussing ESP (Encapsulating Security Payload), the payload specifically refers to the portion of an original packet that is surrounded by IP-sec heade. of user's text is "[12,13]".

D. Virtualization Network

Network virtualization, in its current form, is intricately connected to the development of contemporary datacenters. These datacenters consist of numerous commodity servers that collaborate to tackle computational tasks.

4.1 VXLAN (Virtual-Extensible LocalArea-Network)

VXLAN, short for virtual Extensible LAN, is a network virtualization technology. Its objective is to address the challenges related to scalability. This process allows for the encapsulation of layer 2 frames, which are based on the Media-Access-Control (MAC) protocol, into User-Datagram-Protocol (UDP) datagrams at layer 4. The encapsulation is done using port 4789, which is the designated port for UDP Virtual Extensible LAN (VXLAN) communication. This technology allows for the extension of a layer 2 network across an IP network. Server virtualization allowed the creation of several virtual machine (VM) instances, each with its own unique MAC address. This led to a significant increase

in the number of (MAC) address tables into switched Ethernet-networks, which were necessary to provide communication across hundreds of VMs. The user's text is [4]. Deploying virtual machines (VMs) of the data center setting and organizing them in groups necessitates the use of numerous virtual local area networks (VLANs). It addresses the challenges that may arise while servicing a large number of tenants and handling MAC traffic across logical IP tunnels. Figure-4 [15] depicts the format of a VXLAN frame. The inclusion of fields other than the standard 5-tuple is required for VXLAN-based flow classification. To simplify communication between two tenants, cloud overlay network traffic based on VXLAN employs a unique network-identifier (VNI) value. To communicate with other tenants, of each tenant creates a dynamic overlay-network. The VNI field consists of 24 bits and has the capacity to identify up to 16 million VXLAN segments. To effectively monitor VXLAN based overlay network traffic, it is crucial to detect the VNI value.

Figure **4** Typical flow pattern based on 5-tuple and new flow pattern for VXLAN based on 6-tuple

Table-2 MP-BGP EVPN control plane for VXLAN offers the following

1	The ability to build a VXLAN overlay network that is more robust and scalable
2	Support for multi-tenancy
3	Control plane learning for end host Layer 2 and Layer 3 accessibility information
4	Minimizes network flooding through protocol-driven host MAC/IP route distribution
5	Provides integrated routing and bridging
6	ARP suppression to minimize unnecessary flooding
7	Optimal east-west and north-south traffic forwarding
8	Peer discovery and authentication to improve security

As a result, the VXLAN-based 6 tuple flow flow pattern is introduced. It denotes a collection of six field values. The standard flow key pattern has been enhanced with a new VNI key field, yielding a unique 6 tuple VXLAN-based flow pattern. This pattern includes the following fields: source IP address, source port number, destination IP address, destination port number, protocol, and the newly added VNI field. If any field changes, a new flow is generated. Figure 3 displays the recently accepted 6-tuple VXLAN flow pattern. Each flow is accompanied by an entry that contains non-critical information such as start and end times, total number of packets, and total bytes. All current network traffic flows are tracked by the flow cache.[4]For a broadcast traffic such as an ARP request, the local Virtual Tunnel Endpoint (VTEP) add the VXLAN header of the packet and sends the frame to all hosts that are part of the Virtual Network Identifier (VNI). The receiver VTEP, which has the destination host belonging to the same VNI, removes the encapsulation and handles it as unicast traffic. The process of encapsulating the packet leaving the switch to a destination host is illustrated in figure 5.[15]

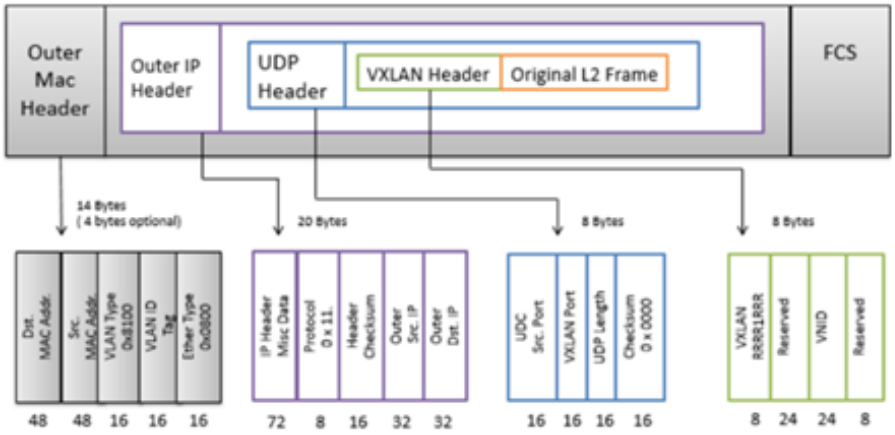

Figure -5 **VXLAN-Network- Identifier**

4.1.1 VXLAN-Network- Identifier (VNI)

VXLAN-Network- Identifier (VNI) is a numerical value used to identify a VXLAN network.

VLAN ID, with a capacity of 12 bits, supports a maximum of 4000 VLANs. In contrast, VXLAN utilizes a 24-bit VXLAN network identifier (VNI), enabling the coexistence of up to 16-million VXLAN segments (sometimes referred to as overlay-networks) inside in the same infrastructure. The VXLAN shim header contains the location of the original inner MAC frame that was generated by an endpoint. Figure-6 illustrates the utilization of the Virtual Network Identifier (VNI) to facilitate the division of Layer 2 and Layer 3 data flow.[7]

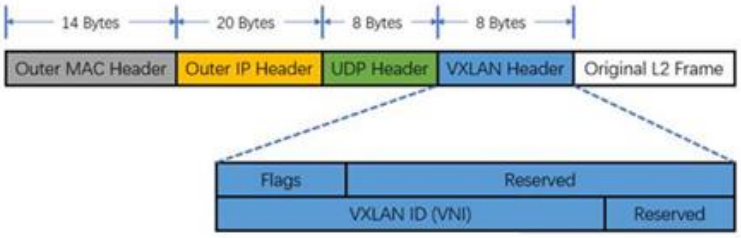

Figure-6 VXLAN Header

4.1.2 VXLAN Tunnel-EndPoint (VTEP)

The VXLAN TunnelEndPoint (VTEP) is the point where VXLAN encapsulation occurs. It is coupled to a traffic source, which can be either a stand-alone server or a virtual machine.[9]

The VXLAN standard specifies VXLAN is a data plane protocol, but it does not specify VXLAN control plane. This allows it to be used of any control plane, such as VXLAN with LISP control plane[7]

4.2 MP-BGP-EVPN

MP-BGP Ethernet-Virtual-Private-Network (EVPN) serves as control protocol specifically designed to VXLAN. Prior to the introduction of EVPN, VXLAN overlay networks functioned using a flood-and-learn architecture. In this specific paradigm, the process of acquiring knowledge about end-host information and discovering VTEPs is solely dependent on data-plane operations, without the involvement of a control protocol for distributing endHost reachability information across VTEPs. MP-BGP-EVPN modifies this is a specific model. The control-plane learning to the endHosts is established at the rear of remote VTEPs. The system provides both control-plane and data-plane separation, together with a consolidated control-plane for Layer2 and Layer3 communication in a VXLAN overlay-network. Table2 displays the utilization of MP-BGP-EVPN for VXLAN, which provides a decentralized control plane solution that significantly improves the capability to construct and connect SDN overlay networks [16].

4.3 NVGRE

NVGRE (Network Virtualization Generic Routing Encapsulation)VLANs have the capability to span over distributed networks, encompassing both layer 2 and layer 3. The NVGRE standard was jointly proposed by Microsoft, Arista, Intel, Hewlett-Packard, Dell, and Broadcom. NVGRE and VXLAN are both network virtualization protocols that aim to provide a multitude of virtual local area networks for subnets using encapsulation and tunneling technology. While they serve the same purpose and have similar practical applications, there are differences in their transmission protocols, data packet formats, transmission modes, and fragmentation methods[5]

4.4 MP-BGP EVPN with VXLAN

MP-BGP EVPN is a control protocol specifically designed with VXLAN, which is a net-virtualization technology. Prior to the introduction of EVPN-VXLAN overlay networks functioned using a flood-learn architecture. In this specific architecture, the process of acquiring end-host information and discovering VTEPs is done through the data plane, without the use of a control protocol to distribute end-host reachability information between VTEP. MP-BGP EVPN modifies this specific model. It enables the end hosts to learn the control-plane in the remote VTEPs. The system provides both control-plane and (data plane) separation, together with a consolidated control plane for Layer-2 and Layer-3 communication in a VXLAN overlay-network. BGP-EVPN, designed for VXLAN, provides a decentralized (control-plane) solution that significantly improves the capability to construct and link SDN overlay-networks [16].The VXLAN network can be partitioned into two distinct segments. The initial component comprises the physical equipment, whereas the subsequent component encompasses the software protocols employed. A VXLAN network comprises an overlay and an underlay, which collectively enable the functioning of the VXLAN network. The overlay utilizes the BGP-EVPN and VXLAN protocols, with the MP-BGP EVPN overlay being employed to disseminate the IP and MAC address details of the end hosts.[17]

4.5 Spine and Leaf Switches

Spine switches serve as the intermediary nodes that connect all the leaf switches. The switches facilitate the transmission of data between the leaf switches

and do not possess knowledge of the destination addresses. The spine switches offer redundancy to the network by enabling numerous paths to connect the leaf switches in a figure-8 configuration.[18].Leaf switches are the network nodes that establish connections with host or access devices. A leaf switch, positioned at the network's periphery, is alternatively referred to as an edge or Network Virtualization Edge (NVE). The figure displayed is in the shape of an eight. Inter-host communication between devices on different leaf switches is facilitated by routing the traffic through a spine switch. Leaf switches act as Virtual Tunnel Endpoints (VTEPs) in a VXLAN network, responsible for both encapsulating and decapsulating data. The number 18 is enclosed in square brackets[18].

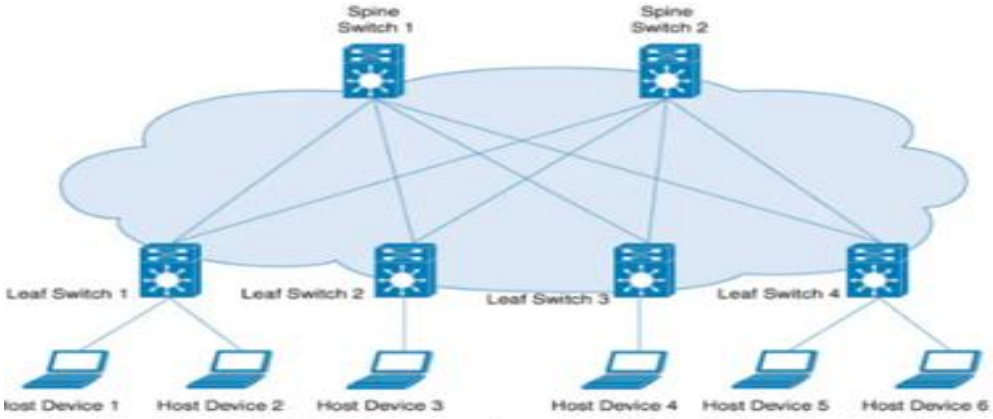

Figure-8 spine and leaf

4.6 Advantages of (EVPN) with (VXLAN)

EVPN optimizes MAC learning by utilizing BGP to communicate MAC and IP address data, resulting in a streamlined process of acquiring MAC addresses throughout the VXLAN fabric.Service Integration: EVPN facilitates the smooth incorporation of Layer 3 services, such as routing and MPLS VPN services, allowing for effective deployment and administration of services[14-17]

4.7 Locator-ID Separation Protocol (LISP)

The LISP map protocol acts as the LISP overlay-network's control-plane. LISP's control-plane is constructed using the LISP Alternative-Logical-Topology (ALT), which is based on the BGP[19]. LISP distinguishes between the identity of the host and location. is creates new structure. The IP-address is broken into 2-parts: the EndPoint Identifier (EID) and the Routing Locator (Routing Locator) (RLOC). Endpoint Identifiers can be IP addresses from both IPv4 and IPv6 (EID). As a result, no changes to the current foundation of the Internet's architecture and protocol stack are required, as shown in Figure-9 [12]. In order to implement LISP, the architecture must include the following additional components. The Ingress Tunnel Router (ITR) is responsible for associating the source EID with its associated RLOC, as well as associating the location EID with the Entrance Tunnel Router's RLOC. The ITR does this by sending map-requests to the map-resolver. Following that, it encloses the source and destination EIDs and RLOCs within the packet header and transmits it using the specified route. The 2.Egress-Tunnel-Router (ETR) sends map-register requests to the map-server on a regular basis.

[10], [20] When the system receives a map request, it sends a response to lTR. In addition, as part of its other functions, it can decapsulate LISP packets. The 3.Map server processes and aggregates registration requests based on EID prefixes. In addition, it has a mapping database. A partial mesh connection connects the 4.Map Resolver to the Alternative-Logical-Topology. It decodes TTR-map requests from their enclosed form and sends them to ETR. The 5.ALT router receives and broadcasts EID prefixes. 6.Proxy TTR: builds a database that connects non-LISP sites to their associated lTR. The Egress-Tunnel-Router (ETR) function for non-LISP sites is implemented by the 7-Proxy ETR[21-24].

4.7 Transparent-Interconnection-Lots-Links (TRILL)

Transparent-Interconnection-Lots-Links (TRILL) refers to a networking protocol that enables efficient and transparent communication between multiple network links.TRILL is a standard established with the Internet-Engineering Task Force (IETF). TRILL guarantees the computation and adoption of new shortest paths at the Ethernet level whenever update is produced by a topology or ink-state changes. This eliminates the performance and routing efficiency limitations associated with spanning tree protocols [22]. Devices that implement TRILL are referred to as Routing Bridges (RBridges). The TRILL data plane is responsible for encapsulating and incoming packets to the TRILL network and sending them to a destination layer-2 location (is egress RBridge). This is supplemented by a largely out-of-band control-plane that distributes a mapping information [22].

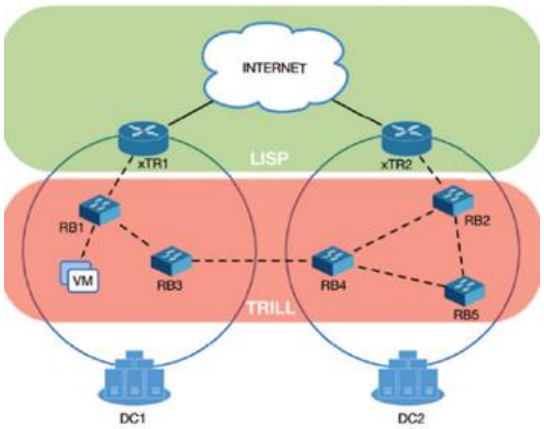

Figure - 9 TRILL-LISP

The TRILL-LISP protocols have a similar approach in how they link the end-point identifier (such as an Ethernet or IP address) to a routing locator (such as an egress-RBridge or egress-tunneling router, respectively). This capability is particularly intriguing when there is a requirement for smooth VM migration at data-link and network-layers.[23]

4.7 Fabric-Path

Fabric-Path is a networking technology that provides a loop-free and scalable solution for data center environments. Links are direct connections between two points. The leaf switches have the task of encapsulating the Ethernet frames

received from the CE network and de-encapsulating the FabricPath frames received from the FabricPath core, before forwarding them to the destination CE domain. The IS-IS protocol is utilized for layer 2 routing within the FabricPath domain and between spine switches. The primary objective of utilizing IS-IS is to calculate the Shortest Path Tree (SPT) among all FabricPath nodes. Using IS-IS in the core network has numerous benefits. One distinguishing feature is the utilization of an independent layer 3 transport, which is integrated into the CLNS stack. IP is unnecessary at the core of a layer 2 topology. Furthermore, IS-IS possesses inherent extensibility due to the presence of the Type-Length-Value (TLV) field. The field in question contains many attributes, such as IP route, metric value, and MPLS traffic engineering, which are encoded and included in IS-IS updates. The FabricPath protocol is utilized to propagate the FabricPath switch ID, forwarding path tags, and facilitate the exchange of control plane information. This enables IS-IS to construct the shortest path tree for leaf and spine switches[25-29].

4.8 VXLAN with SDN

SDN-basedsoftware-defined network and VXLAN Visual networks and cloud computing networks greatly enhance the implementation of new services and have become a fundamental infrastructure provider in the digital society. VXLAN, a network scheme that overlays Layer 2 over Layer 3, is widely used in cloud computing networks. Despite partially addressing the capacity limitation of its predecessor, virtual local area network (VLAN), VXLAN still faces challenges such as excessive signaling overhead during multicast and interrupted communication with migrating virtual machines (VMs)[30-33].

Functionalities	SDN Based VxLAN	Traditional VxLAN
Tenant Management	Real-time supervision	Manual Configuration
VM Dilatation	Automatical configuration	Manual Configuration
Fault Detection	Enhanced capability by global information	Difficult to locate the fault
New Service	Flexible deployment in the intelligent center	Inevitable hardware configuration modifications
VM Migration	Proactive or Paasive	Manual Configuration
Load Balancing	Automatical detection	Some simple mechanism.

Table 3

E. Conclusion

VXLAN-EVPN is utilized in network virtualization for distinct objectives.VXLAN and EVPN are both utilized in network virtualization, however they serve different .VXLANEVPN is commonly used in data center networks for multitenancy and multisite connectivity, providing a scalable and efficient solution.VPN reduces flooding by using BGP to exchange MAC and IP address information, allowing for efficient learning of MAC addresses throughout the VXLAN fabric. VXLAN allows the establishment of virtual Layer 2 networks over Layer 3 infrastructure, whereas LISP offers a scalable routing architecture with effective mobility management. VXLAN and LISP when used together, is used in enterprise campus networks for mobility and location independence, providing a flexible option for device movement across several locations. VXLAN can be combined with other widely used overlay network protocols, including Generic

Network Virtualization Encapsulation (GENEVE), Stateless Transport Tunneling (STT), and Network Virtualization using Generic Routing Encapsulation (NVGRE).

F. References

[1] Z. Zhao, F. Hong, and R. Li, "SDN Based VxLAN Optimization in Cloud Computing Networks," IEEE Access, vol. 5, pp. 23312–23319, Oct. 2017, doi: 10.1109/ACCESS.2017.2762362.

[2] "Cisco Press CCNP and CCIE Enterprise Core Official Cert Guide," 2020.

[3] T. Muhammad, "Overlay Network Technologies in SDN: Evaluating Performance and Scalability of VXLAN and GENEVE," 2021.

[4] D. H. Abdulazeez and S. K. Askar, "A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture Within the Fog-Cloud Environment," in IEEE Access, vol. 12, pp. 39936-39952, 2024.

[5] Fady Samann, and Shavan Askar, "Examining the Use of Scott's Formula and Link Expiration Time Metric for Vehicular Clustering" Computer Modelling in Engineering and Sciences, 2024.

[6] Itika Sharma, Sachin Kumar Gupta, Ashutosh Mishra, Shavan Askar, "Synchronous Federated Learning based Multi Unmanned Aerial Vehicles for Secure Applications" Scalable Computing: Practice and Experience, Volume 2, No. 3, 2023.

[7] O. Ghazali and S. Khurram, "Enhanced IPFIX flow monitoring for VXLAN based cloud overlay networks," International Journal of Electrical and Computer Engineering, vol. 9, no. 6, pp. 5519–5528, 2019, doi: 10.11591/ijece.v9i6.pp5519-5528.

[8] M. S. M. Sudrajat, D. Perdana, and R. M. Negara, "Performance analysis of VXLAN and NVGRE tunneling protocol on virtual network," Bulletin of Electrical Engineering and Informatics, vol. 6, no. 3, pp. 295–300, Sep. 2017, doi: 10.11591/eei.v6i3.622.

[9] Gustavo D. Salazar-Chacón, Andy R. Reinoso García, "Segment-Routing Analysis: Proof-of-Concept Emulation in IPv4 and IPv6 Service Provider Infrastructures", 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp.1-7, 2021.

[10] N. M. Mosharaf, K. Chowdhury, R. Boutaba, and D. R. Cheriton, "A Survey of Network Virtualization," 2008.

[11] T. Singh, V. Jain, and S. Babu, "VXLAN and EVPN for Data Center Network Transformation."

[12] Society of Digital Information and Wireless Communications and Institute of Electrical and Electronics Engineers, 2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP) : 21-23 July 2016.

[13] Lukas. Krattiger, David. Jansen, and Shyam. Kapadia, Building data centers with VXLAN BGP EVPN : a Cisco NX-OS perspective.

[14] Diana Hayder Hussein; Shavan Askar, "Federated Learning Enabled SDN for Routing Emergency Safety Messages (ESMs) in IoV Under 5G Environment", IEEE Access, Volume 11, 2023.

[15] Media Ali Ibrahim; Shavan Askar, "An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm", IEEE Access, Volume 11, 2023.
[16] Harikumar PallathadkaManipur, Sarmad Jaafar, Shavan Askar, Essam Q. AL. Husseini, Barno Sayfutdinovna Abdullaeva, Noor Hanoon Haroon, "Scheduling of Multiple Energy Consumption in The Smart Buildings with Peak Demand Management", International Journal of Integrated Engineering, Vol. 15, No. 4, 2023.
[17] F. De Turck, IEEE Communications Society, and Institute of Electrical and Electronics Engineers, Proceedings of the 2020 IEEE Conference on Network Softwarization : NetSoft 2020 : Bridging the gap between AI and network softwarization: 29 June-3 July 2020 - Virtual Conference.
[18] F. De Turck, IEEE Communications Society, and Institute of Electrical and Electronics Engineers, Proceedings of the 2020 IEEE Conference on Network Softwarization : NetSoft 2020 : Bridging the gap between AI and network softwarization: 29 June-3 July 2020 - Virtual Conference.
[19] Omar Shirko; Shavan Askar , "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking" IEEE Access, Volume 11, 2023.
[20] Dezheen H. Abdulazeez; Shavan K. Askar, "Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment" IEEE Accesss Volume 11, 2023.
[21] Fady E. F. Samann; Shavan Askar, "Estimating The Optimal Cluster Number For Vehicular Network Using Scott's Formula" 2022 4th International Conference on Advanced Science and Engineering (ICOASE).
[22] S. Ramesh, S. K. Bohacek, and K. E. Barner, "SECURING VXLAN-BASED OVERLAY NETWORK USING SSH TUNNEL," 2017.
[23] A. S. George and A. S. H. George, "This work is licensed under a Creative Commons Attribution 4.0 International License A Brief Overview of VXLAN EVPN," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, vol. 9, pp. 2321–5526, 2021, doi: 10.17148/IJIREEICE.2021.9701.
[24] E. Ekblad and M. Rehnberg, "Analysis of the security of a VXLAN network Analys av säkerheten för ett VXLAN-nätverk."
[25]https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/configuration_guide/vxlan/b_176_bgp_evpn_vxlan_9500_cg/configuring_spine_switches_in_a_bgp_evpn_vxlan_fabric.html.
[26] Institute of Electrical and Electronics Engineers., International Federation for Information Processing., and IEEE Communications Society., IEEE/IFIP NOMS'14 : IEEE/IFIP Network Operations and Management Symposium : Krakow, Poland, 5-9 May 2014.
[27] H. Pu, Y. Wang, and X. An, "Safety Protection Design of Virtual Machine Drift Flow in Cloud Data Center Based on VXLAN Technology," Journal of Computer and Communications, vol. 08, no. 08, pp. 45–58, 2020, doi: 10.4236/jcc.2020.88005.

[28] V. S. Mentor and K. Cheema, "Project title: An analysis on network virtualization protocols and technologies by."
[29]S. Kiran and K. Jasti, "SYSC 5801 Advanced Topics in Computer Communication Locator/ID Separation Protocol (LISP) and Applications."
[30] Nafees Zaman; Ahmad Abu Saiid; Md Arafatur Rahman; Shavan Askar; Jasni Mohamad Zain , "A Data-Intelligent Scheme Toward Smart Rescue and Micro-Services", IEEE Access Volume 11, 2023.
[31] Fady E. F. Samann; Siddeeq Yousif Ameen; Shavan Askar, "Fog Computing in 5G Mobile Networks: A Review" 2022 4th International Conference on Advanced Science and Engineering (ICOASE).