Data Center Lab Using VxLAN Data Plane and BGP-EVPN Control Plane

2023 4th International Conference on Data Analytics for Business and Industry (ICDABI) | 979-8-3503-6978-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICDABI60145.2023.10629438

Mohammed Elmadani
Information Technology Faculty
Misurata University, Libya
m09191141@it.misuratau.edu.ly

Salem Omar Sati
Information Technology Faculty
Misurata University, Libya
salem.sati@it.misuratau.edu.ly

***Abstract*—Virtual Extensible Local Area Network is an overlay technology that allows smart encapsulation of layer two through layer three. It provides the extension of Virtual Local Area Network domains, allowing the original addressing of virtual hosts through the data centers and cloud computing networks. Furthermore, The traditional three-layer model data center architecture can be abandoned with a more efficient topology, known as Spine and Leaf. The Spine and Leaf topology offers low latency and high bandwidth, which are crucial for high-performance computing and cloud environments. Moreover, by incorporating VXLAN technology with the Spine and Leaf architecture, it will provide an effective network topology, which considers the demands of modern data center networks. This paper introduces the VxLAN Multiprotocol Border Gateway Protocol, Ethernet Virtual Private Network (MP-BGP EVPN), and provides a practical implementation using the Free Range Router with docker containers in a GNS3 environment.**

***Index Terms*—Border Gateway Protocol, Virtual eXtensible Local Area Network, Spine and Leaf, Ethernet Virtual Private Network, Control Plane.**

I. Introduction

Virtual Extensible Local Area Network (VxLAN) provides the best solution, especially for an address challenges faced by traditional data center networks [1]. VxLAN provides the solution for data center networks to scale, by simplifying network architecture for the virtualized environment of modern data centers [2]. VxLAN solves the problems that concern VLAN identification and tagging according to IEEE 802.1q standard. This standard uses 12 bit VLAN identifier which limits the number of supported VLANs to a maximum of 4,096. This tag field of 12 bits in the VLAN frame leads to big issues in large-scale data centers and public clouds. There is also the issue of virtual machine migration between different subnets or different data centers. As VLAN works only in layer 2 Ethernet collision domain it causes the virtual machine to not be routed between different subnets or two data centers. VxLAN is the solution of tunneling protocol that extends layer two over layer three, This solution enables the virtual machine to be migrated to a different subnet or data center, VxLAN header fields add 24 bit virtual network identifier to overcome the limitation of VLAN 12 bit tagging. However VxLAN is data plane learning that follows the behavior of flood and learn approach, which has the same issues that impact on the traditional Ethernet. When the network scale grows the broadcast domain increase which impact the entire network's performance and scalability. This performance degradation is not desirable in a data center environment. BGP-EVPN provides the best solution by distributing reachability information for VxLAN tunnels. Which enables the creation of large-scale layer two domains for cloud and data centers. Furthermore, it supports visualization and virtual machine migration [3]. VxLAN is a technology that addresses issues related to the deployment of Spanning Tree Protocol (STP) for redundancy at layer two. By eliminating the need for the STP protocol and its associated issues at layer two, VXLAN allows for better scalability and faster convergence, and by utilizing Equal-Cost Multipath (ECMP) routing technologies, this enables the use of all available links between switches, improving network performance [4], [5]. This paper will focus on MP-BGP and EVPN solutions for data centers. The contribution of the paper is building a test bed for MP-BGP, EVPN, and VxLAN using GNS3 and FRRouting (FRR) [6]. This testbed shows how it's used to distribute reachability information through the use of Route Type Two and Route Type Three in NLRI messages. It also uses the open-source software image FRR which is a Linux image to enable VxLAN EVPN features. The paper is organized using the following sequence. Section II demonstrates the related papers and research on the topic. In Section III, the paper provides the concepts of MP-BGP protocol and EVPN address family. Section IV gives the architecture of VxLAN Header encapsulation. The paper introduces the concept of Free Range Routing (FRR) protocol suite in Section V. Section VI shows the steps of installation and configuration using the GNS3 simulator for VxLAN BGP-EVPN lab implementation. Finally, Section VII gives the paper's conclusion and directions for future work.

II. Related Works

VxLAN technology is considered an overlay network. There are many papers study the topic of VxLAN such as [7] which shows the latest technology of VxLAN solution through data centers with EVPN control plane, It concludes that VxLAN has a faster convergence, performance, and scalable when deploying the MP-BGP control plane. The paper [4] presents the new architecture with its related protocols for the control plane and the data plane. Modern data centers usually deploy

Fat-Tree as a topology with multipath routing. To get full features of such topology, the paper suggests deploying specific routing protocols called Multi-path routing as a solution for data center communication. The paper [8] provides a review of several solutions for data centers' interconnecting environments. The paper shows a deep study and analysis of the advantages and disadvantages of different reviewed solutions. The paper [9] presents the use of overlay technology with VxLAN tunnels. This solution is deployed to balance traffic between data centers, the load balancing is implemented using the data plane of the SDN network. The contribution of the paper is the load balancer in overlay networks based to minimize the delay. The paper [10] proposes a new SDN-based VxLAN architecture. this architecture show how can deploy a smart controller to improve the multicast and facilitate the virtual machine migration. While the paper [11] explains what is VxLAN and how the technology is deployed for a cloud and data center infrastructure. It shows the flexibility of managing physical resources anywhere in data center networks. On the other hand, it demonstrates the virtual machine's place of shared Layer two connectivity among VxLAN. The paper [12] shows that VxLAN provides an encapsulation approach that builds the overlay network. It concludes that VxLAN can be deployed in data centers interconnecting virtual machines. The paper [13] shows a VxLAN proof-of-concept emulation by deploying the open networking paradigm. It also confirms that the solution can be implemented by two mechanisms of the Lightweight Network Virtualization and Ethernet VPN for large scale networking. The paper [14] describes how Shortest Path Bridging and EVPN can be combined to provide a large-scale distributed data center network. It shows how multicast protocol can enhance backbone network efficiency.

This paper will build a lab with open-source tools, and provide knowledge of how VxLAN can be used with BGP, by inspecting its messages. This lab will be used to test the performance of VxLAN in scenario where multiple data centers are connected with each other.

III. Multi-Protocol Border Gateway Protocol (MP-BGP)

MP-BGP is an extension of IP version 4 Border Gateway Protocol [15] that multiplexes different address families. It associates Network Layer Reachability Information into a single BGP peering session, enabling VPN services via a single session. The protocol uses Route Distinguishers (RDs) to differentiate between routes and provides unique identities for tenants via a Route Target (RT) attribute. A route can be added to a Virtual Routing and Forwarding (VRF) for routing traffic, which is received from respective sites by having a specific RT property associated with it. VxLAN is data plane technology [2] and in order to implement control plane, Ethernet Virtual Private Network (EVPN) was introduced, EVPN is an extension of MP-BGP and it is used to exchange MAC addresses, VTEP (VXLAN Tunnel Endpoint) information of the participated devices. EVPN can be used in conjunction with VXLAN to provide multitenancy in a data center environment. In the context of data centers, EVPN with VXLAN enables the creation of scalable, efficient, and flexible Layer 2 and Layer 3 connectivity between geographically dispersed data centers. It simplifies the deployment and management of virtualized workloads, increases network agility, and supports workload mobility.

MP-BGP, EVPN determines a new sub-address family called the EVPN address family which is considered as a L2VPN address family. This address family has also introduced EVPN NLRI. This EVPN NLRI specifies the following route types of VxLAN EVPN. When these routes are advertised between the connected EVPN peers, VxLAN tunnels are automatically established between peers, and host addresses are learned. The main route types of EVPN are as follows:

1) *Type 2 route* This type is considered as MAC/IP route. This route is used to advertise the MAC or physical address, ARP protocol entry, and layer three routing information of hosts.
2) *Type 3 route* This type is considered as inclusive multicast route. This route is used for the dynamic discovery of VTEPs. It is also used for dynamic connecting of VxLAN tunnels.
3) *Type 5 route* This type is considered as an IP prefix route. This route is used to distribute the information of the imported external routes or routing information of hosts.

The MAC/IP advertisement route (Type 2) is one of the most important EVPN routes. The function of this route is to inform other network devices of the location by advertising its MAC address and any associated IP addresses. For host mobility support with keeping the devices connected even when they move from one location to another, this form of EVPN route is employed. The distribution list for ingress replication is created using EVPN route type 3. Also, this route is known as the "inclusive multicast Ethernet tag route". When a VNI is configured at the VTEP, then route type 3 is generated and delivered to all ingress replication of connected VTEPs. By deploying this, each VTEP is made aware of every other remote VTEP. Another crucial route type in EVPN is the IP Prefix Advertisement Route (Type 5). This route is employed to promote IP prefixes that can be accessed over the network. This route can be helpful, especially for promoting IP subnets between data centers. Therefore, equipment in one data center can talk to devices in another data center.

IV. VxLAN Header Encapsulation

The VxLAN header contains several fields, including a unique VxLAN Network Identifier (VNI). This identifier is used to distinguish different VXLAN networks. When the packet reaches its destination, the VXLAN header is removed and the original packet is forwarded to the destination. Other network virtualization technologies, such as Generic Routing Encapsulation (GRE) and Stateless Transport Tunneling (STT), are quite similar to the behavior of the VxLAN header encapsulation process. However, VxLAN has some advantages over these technologies, such as support for multicast and unicast traffic, a bigger VNI space (16 million unique IDs), and more. The fact that VxLAN header encapsulation might increase packet overhead is one of its drawbacks. In high-speed networks, where even a little bit of extra overhead can significantly affect performance, this can be very problematic. To limit this problem, some hardware manufacturers have created specialized

VxLAN tunneling hardware that can encapsulate data at wire speed [16]. VxLAN adds 50 bytes (assuming VLAN tagging is not used in the inner frames that are encapsulated) are equal to 8 bytes (VXLAN header), 8 bytes (UDP header), 20 bytes (IPv4 header), and 14 bytes (outer L2 header) [2]. Clients which utilize VLAN tagging must add 4 bytes, making a total of 54 bytes.

V. Free Range Routing (FRR)

FRR [6] provides an IP routing suite. Its role in a networking service is to exchange Routing Information Base (RIB) with other routers, it makes routing decisions, and it informs other layers of these decisions. FRR registers routing decisions into the kernel, allowing the kernel make the corresponding forwarding and routing decisions. In addition based on the dynamic routing. FRR supports layer three configurations, including static routes and router advertisements. It has fewer layers two functionality. FRR runs on operating systems such as Linux and BSDs. Traditional routing software works as a single process program, It provides complete routing protocol functionalities. FRR is a suite of daemons of software which are working together to construct the routing table. Each supported protocol is programmed in its daemon, and these daemons are connected to a main daemon of Zebra, this daemon is responsible for routing decisions and manages the data plane. This architecture of FRR allows for high resiliency since a software error in one FRR daemon will not impact the others. It is also flexible because of its modularity which makes it easy to add a new daemon to the FRR suite. FRR is an internet routing protocol suite for Linux platforms. It implements the most common protocols such as Opens Shortes Path First (OSPF), MP-BGP, EVPN, VxLAN.

VI. VxLAN BGP-EVPN Implementation

Vxlan is an overlay network and it deploys the BGP-EVPN as the control plane for the transport of layer two frames. Regardless of whether these frames are bridged at Layer Two or routed at Layer Three. When a Virtual Network Interface (VNI)is created it will have its own Route Distinguisher (RD) and set of Import/Export rules for Route Targets (RT).

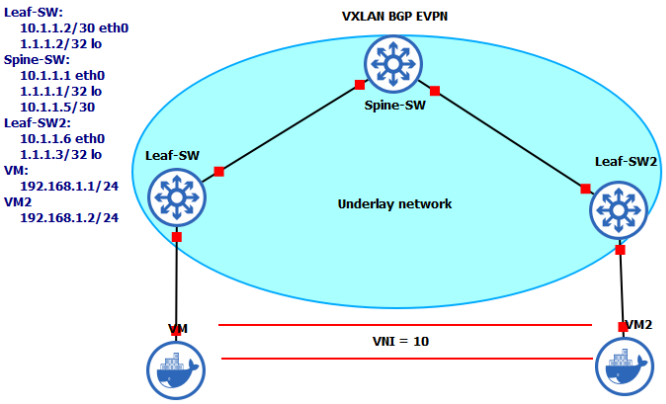

Fig. 1. The topology used for simulation in GNS3.

The topology used to demonstrate the implementation of VxLAN BGP-EVPN using FRR is shown in Figure 1. This topology consists of three FRRs and two hosts. The topology uses FRR which is a free and open-source internet routing protocol suite for Linux operating systems. It has two functions, one will use Linux commands to configure the VxLAN tunnel interface and bridge interface. The other function will be the routing mechanisms and MP-BGP EVPN implementation using the VTY shell (vtysh) command, It gives all FRR daemons combined as a single daemon or session. The lab in Figure 1 runs the FRR router as a Linux image which runs through the docker container in the GNS3 emulator. The virtual machines act as hosts and are also docker containers that running Alpine Linux distribution.

```
Spine-SW# conf terminal
Spine-SW(config)# interface eth0
Spine-SW(config-if)# ip address 10.1.1.1/30
Spine-SW(config-if)# ip ospf area 0
Spine-SW(config-if)# exit
Spine-SW(config)# interface eth1
Spine-SW(config-if)# ip address 10.1.1.5/30
Spine-SW(config-if)# ip ospf area 0
Spine-SW(config-if)# exit
Spine-SW(config)# interface lo
Spine-SW(config-if)# ip address 1.1.1.1/32
Spine-SW(config-if)# ip ospf area 0
Spine-SW(config-if)# exit
```

Fig. 2. OSPF configuration.

```
Spine-SW# show ip ospf route
============ OSPF network routing table ============
N    1.1.1.1/32           [0] area: 0.0.0.0
                          directly attached to lo
N    1.1.1.2/32           [10000] area: 0.0.0.0
                          via 10.1.1.2, eth0
N    1.1.1.3/32           [10000] area: 0.0.0.0
                          via 10.1.1.6, eth1
N    10.1.1.0/30          [10000] area: 0.0.0.0
                          directly attached to eth0
N    10.1.1.4/30          [10000] area: 0.0.0.0
                          directly attached to eth1

============ OSPF router routing table =============

============ OSPF external routing table ===========
```

Fig. 3. Routing corresponding to the underlay network.

The topology consists of two leaf switches and one spine switch as demonstrated in Figure 1. The scenario will deploy VxLAN EVPN. The leaf switches will be configured VTEPs, these switches will encapsulate and decapsulate the VxLAN tunnel header. Where the spine switch will participate only in the dynamic routing process. The underlay network will use OSPF to provide underlay connectivity, the configuration is shown in Figure 2. To allow VTEPs to exchange EVPN routes between them we use BGP in the loopback interface to advertise EVPN Route Type Two and Route Type Three. The routing table is shown in Figure 3 resulting from the configuration of OSPF. The OSPF configuration for enabling the connectivity at the underlay network. OSPF implementation is based on

a single area (Area 0) which is the backbone area. Figure 4 illustrates creating a bridge interface and VxLAN interface in Linux based on the FRR routing. Assigning the VxLAN tunnel interface and the physical interface that connected the end host to the bridge. This lets hosts connect to the bridge interface to allow communication between virtual machines. This communication will be across different physical hosts using a container over a VxLAN overlay. The bridge interface enables the exchange of traffic between the two networks or hosts. This connectivity is done by serving as a logical link between physical network interfaces and VxLAN tunnels.

```
/usr/lib/frr # ip link add br0 type bridge
/usr/lib/frr # ip link set br0 up
/usr/lib/frr # ip link add vxlan10 type vxlan id 10 dstport 4789
/usr/lib/frr # ip link set vxlan10 up
/usr/lib/frr # brctl addif br0 vxlan10
/usr/lib/frr # brctl addif br0 eth1
```

Fig. 4. VxLAN configuration in leaf switches.

```
Leaf-SW(config)# router bgp 1
Leaf-SW(config-router)# neighbor 1.1.1.1 remote-as 1
Leaf-SW(config-router)# neighbor 1.1.1.1 update-source lo
Leaf-SW(config-router)# address-family l2vpn evpn
Leaf-SW(config-router-af)# neighbor 1.1.1.1 activate
Leaf-SW(config-router-af)# advertise-all-vni
Leaf-SW(config-router-af)# exit-address-family
```

Fig. 5. EVPN configuration on leaf switches.

Figure 5 illustrates MG-BGP EVPN configuration on leaf switch by using Layer Two VPN address family. The configuration specifies neighbor peer or BGP speaker. It also advertises all VNI. The advertise-all-VNI command must be used to enable EVPN for a BGP instance. This setting shows how to configure an FRR router to use EVPN. MP-BGP protocol as an extension for BGP protocol is configured on the loopback interface.

```
Leaf-SW# show bgp l2vpn evpn
BGP table version is 6, local router ID is 1.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[EthTag]:[ESI]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1.1.1.2:2
*> [2]:[0]:[48]:[46:3f:f3:86:3f:45]
                    1.1.1.2                              32768 i
                    ET:8 RT:1:10
*> [3]:[0]:[32]:[1.1.1.2]
                    1.1.1.2                              32768 i
                    ET:8 RT:1:10
Route Distinguisher: 1.1.1.3:2
*>i[2]:[0]:[48]:[ae:86:63:a1:3d:70]
                    1.1.1.3                  0    100      0 i
                    RT:1:10 ET:8
*>i[3]:[0]:[32]:[1.1.1.3]
                    1.1.1.3                  0    100      0 i
                    RT:1:10 ET:8
```

Fig. 6. EVPN Route Type 2 and Route Type 3 advertisement.

Figure 6 illustrates the advertising of EVPN Route Type Two and Route Type Three between leaf switches. Using the command "show bgp l2vpn evpn", to check the MAC and IP addresses, where these are advertised via BGP EVPN. MAC addresses of the two virtual machines are shown in Figure 6. The last octet of the MAC address of the virtual machine (VM2) is 70. On the other side, the last octet of MAC address of the virtual machine (VM) is 45. Figure 6 shows that there are two MAC addresses advertised using the BGP EVPN control plane as a Route type two message. Using a Wireshark capturing tool, it is possible to capture how the MP-BGP protocol delivers keep-alive control messages. These keep-alive control messages are used to test the underlay network connectivity between nodes. BGP relies on Transmission Control Protocol (TCP) to establish a reliable communication channel between routers as peers or speakers. In the BGP protocol, routers use keep-alive messages to discover BGP neighbors and establish peer relationships with other routers as shown in Figure 7, these messages are brief data packets, which confirm that BGP peers can interact with one another.

20 60.003235	10.1.1.1	224.0.0.5	OSPF	82 Hello Packet
21 62.922031	10.1.1.2	224.0.0.5	OSPF	82 Hello Packet
22 63.827542	1.1.1.2	1.1.1.1	BGP	85 KEEPALIVE Message
23 63.834367	1.1.1.1	1.1.1.2	BGP	85 KEEPALIVE Message
24 63.834929	1.1.1.2	1.1.1.1	TCP	66 38167 → 179 [ACK]

Fig. 7. BGP and OSPF messages.

Based on the Wireshark capture tool it can be observed that the MP-BGP update message carries EVPN information to the other leaf switch, by inspecting Subsequent Address Family Identifier (SAFI) code 70 which indicates that the router using EVPN extension as shown in Figure 8.

```
> Path Attribute - MULTI_EXIT_DISC: 0
> Path Attribute - LOCAL_PREF: 100
> Path Attribute - ORIGINATOR_ID: 1.1.1.2
> Path Attribute - CLUSTER_LIST: 1.1.1.1
> Path Attribute - EXTENDED_COMMUNITIES
v Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 126
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 103
  v Path attributes
    v Path Attribute - MP_REACH_NLRI
      > Flags: 0x90, Optional, Extended-Length, Non-transitive, Complete
        Type Code: MP_REACH_NLRI (14)
        Length: 44
        Address family identifier (AFI): Layer-2 VPN (25)
        Subsequent address family identifier (SAFI): EVPN (70)
      > Next hop: 1.1.1.3
        Number of Subnetwork points of attachment (SNPA): 0
      > Network Layer Reachability Information (NLRI)
    > Path Attribute - ORIGIN: IGP
    > Path Attribute - AS_PATH: empty
    > Path Attribute - MULTI_EXIT_DISC: 0
    > Path Attribute - LOCAL_PREF: 100
    > Path Attribute - ORIGINATOR_ID: 1.1.1.3
    > Path Attribute - CLUSTER_LIST: 1.1.1.1
    v Path Attribute - EXTENDED_COMMUNITIES
      > Flags: 0xc0, Optional, Transitive, Complete
        Type Code: EXTENDED_COMMUNITIES (16)
        Length: 16
      v Carried extended communities: (2 communities)
        > Route Target: 1:10 [Transitive 2-Octet AS-Specific]
        > Encapsulation: VXLAN Encapsulation [Transitive Opaque]
```

Fig. 8. MP-BGP update message.

The MP_REACH_NLRI is a path attribute field used to advertise a feasible route to a BGP peer. Also, it permits the router to advertise the network layer address to the destination listed in NRLI. This message originated by one leaf switch to the other to advertise EVPN messages A new Address Family Indicator/Subsequent Address Family Indicator (AFI/SAFI) is defined for EVPN: l2vpn (25) /evpn (70). For two BGP speakers

to exchange EVPN Network Layer Reachability Information (NLRI), they must negotiate the EVPN BGP capability at the start of the BGP session to ensure that both peers can support such NLRI. Where AFI/SAFI is used by EVPN when deploying MP-BGP, as BGP update messages. This message has a specific path attribute to identify what type of protocol is advertised with this message. These defined numbers are registered with the IANA organization to ensure BGP and EVPN standardization. MP-BGP extension can be used with any following protocols IPv4 and IPv6 in addition to L2VPN. Figure 9 shows the additional 50 bytes added during VxLAN encapsulation to the original header, VXLAN uses UDP with the destination port 4789, while the source port is calculated using the hash algorithm as a result of the original Ethernet frame, A VxLAN header is appended to the original Layer two frame before it is encapsulated in a UDP-IP packet according to the MAC-in-UDP encapsulation.

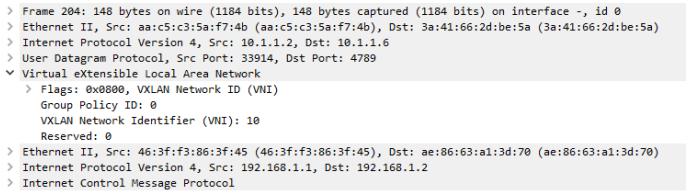

Fig. 9. VxLAN Header Encapsulation.

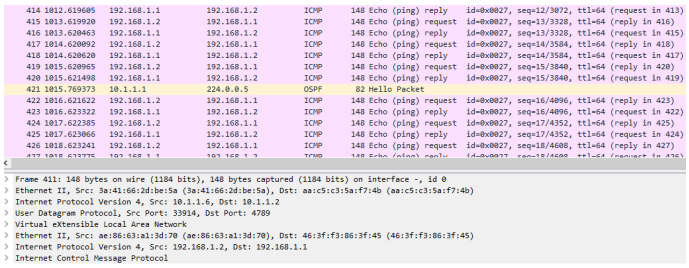

Fig. 10. Test connectivity between VMs.

Figure 10 demonstrates a successful communication between the two Virtual machines, as the Request and Replay messages of Internet Control Message Protocol (ICMP) shown.

VII. Conclusion and Future Work

The limitation of Layer two Ethernet networks and VLANs has been overcome by the VxLAN BGP-EVPN technology. This is done using separating the logical or overlay network from the underlying physical infrastructure, VxLAN implementation with BGP-EVPN provides a scalable solution to construct large-scale virtual networks. This solution provides flexibility and visibility in the network. VxLAN BGP-EVPN solution enables the creation of virtual connected hosts via networks that connect several data centers. The concept of VxLAN overlays is based on using MP-BGP for the signaling control plane and EVPN for MAC address distribution over the data plane. This paper proposes VxLAN and BGP-EVPN labs for testing and education, especially in the field of data centers. Furthermore, this technology provides a basis for cloud integration and multi-site connectivity. The lab implemented using FRR routing suite in GNS3 emulator. The VxLAN BGP-EVPN lab helps designers and administrators to test some scenarios of data center interconnecting (DCI) and its advantages might help developers improve cloud and data center clustering. Moreover, the lab helped to understand the concept of virtualization and virtual machine migration In future work, the authors plan to use the lab test bed for analyzing some of the VxLAN issues such as MTU size and its impact on the Data Center Interconnecting (DCI).

Acknowledgment

The authors would like to thank the staff of the Communication and Network Department of Information and Technology faculty at Misurata University. Furthermore, the authors thank the University of Bahrain for organizing this conference.

References

[1] M. Mahalingam, D. G. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright, "Virtual extensible local area network (VXLAN): A framework for overlaying virtualized layer 2 networks over layer 3 networks," *RFC*, vol. 7348, pp. 1–22, 2014.

[2] E. F. Naranjo and G. D. Salazar Ch, "Underlay and overlay networks: The approach to solve addressing and segmentation problems in the new networking era: Vxlan encapsulation with cisco and open source networks," in *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)*, 2017, pp. 1–6.

[3] D. A. S. GEORGE and A. H. George, "A brief overview of vxlan evpn," *Ijireeiceinternational Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, vol. 9, no. 7, pp. 1–12, 2021.

[4] A. Radoi and C. Rîncu, "Integration of data center network technologies vxlan, bgp, EVPN," in *14th International Conference on Communications, COMM 2022, Bucharest, Romania, June 16-18, 2022*. IEEE, 2022, pp. 1–5.

[5] S. M. Haider Bokhari, "Overview and design of vxlan," vol. 1, p. 6, 11 2016.

[6] L. FOUNDATION, "FRRouting Project," https://frrouting.org/ , 2017, accessed: 2023-05-20.

[7] T. Singh, V. Jain, and G. S. Babu, "Vxlan and evpn for data center network transformation," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2017, pp. 1–6.

[8] L. Alberro, A. Castro, and E. Grampín, "Experimentation environments for data center routing protocols: A comprehensive review," *Future Internet*, vol. 14, no. 1, p. 29, 2022.

[9] E. A. Alvarado-Unamuno and J. E. Arizaga-Gamboa, "Design and implementation of traffic balancer over overlay networks with vxlan tunneling," in *Technologies and Innovation - 7th International Conference, CITI 2021, Guayaquil, Ecuador, November 22-25, 2021, Proceedings*, ser. Communications in Computer and Information Science, R. Valencia-García, M. Bucaram-Leverone, J. del Cioppo-Morstadt, N. Vera-Lucio, and E. Jácome-Murillo, Eds., vol. 1460. Springer, 2021, pp. 125–139.

[10] Z. Zhao, F. Hong, and R. Li, "SDN based vxlan optimization in cloud computing networks," *IEEE Access*, vol. 5, pp. 23 312–23 319, 2017.

[11] K. Wanguhgu, "VXLAN: extending networking to fit the cloud," *login Usenix Mag.*, vol. 37, no. 5, 2012.

[12] S. Pallagatti, G. Mirsky, S. Paragiri, V. P. Govindan, and M. Mudigonda, "Bidirectional forwarding detection (BFD) for virtual extensible local area network (VXLAN)," *RFC*, vol. 8971, pp. 1–9, 2020.

[13] G. Salazar-Chacon and L. Marrone, "Open networking for modern data centers infrastructures: Vxlan proof-of-concept emulation using lnv and evpn under cumulus linux," in *2022 IEEE Sixth Ecuador Technical Chapters Meeting (ETCM)*. IEEE, 2022, pp. 1–6.

[14] D. Allan, J. Farkas, P. Saltsidis, and J. Tantsura, "Ethernet routing for large scale distributed data center fabrics," in *2013 IEEE 2nd International Conference on Cloud Networking (CloudNet)*, 2013, pp. 164–169.

[15] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol extensions for BGP-4," *RFC*, vol. 4760, pp. 1–12, 2007.

[16] C.-G. Lim, S.-M. Pahk, T.-I. Kim, and J.-H. Lee, "Design and implementation of hardware accelerated vtep in datacenter networks," in *2015 17th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2015, pp. 745–748.