IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

A Brief Overview of VXLAN EVPN

Dr. A. Shaji George[1], A. S. Hovan George[2]

Masters IT Solutions, Chennai, Chennai, Tamil Nadu, India[1,2]

Abstract: The purpose of this paper is to provide network professionals with a common need to comprehend how to use VXLAN networks within their own organizations to release the entire potential of modern networking. Whilst interested network administrators shall acquire the most advantages from such content, the information contained within this research paper might be of use to each IT professional involved in network technologies. Aspects in this paper examine how VXLAN EVPN provides a solution to network challenges that have overwhelmed the entire industry for many years, and how to implement constructs that are usually observed in traditional networks thanks to this new technology. This research paper explores VXLAN EVPN, starting with an introductory stage, achieving a good understanding of terms and concepts as well as progressing via implementations through a single data center to several data centers. The following paper also refers design and the integration of Layer4-Layer7 network services, co-existence along with brownfield environments, operation, as well as maintain a VXLAN EVPN. At the conclusion of this paper, the reader will have a strong foundation of VXLAN EVPN and an understanding of real-world use instances that can be instantly used to help in the development of a strategy to effectively shift to next-generation data center with this new technology.

Keywords: VXLAN, EVPN, BGP EVPN, Layer4-Layer7 Services, MP-BGP EVPN, Multi-POD & Multi-Site, Cloud Networking, Datacenter networks, Network Virtualization.

I. INTRODUCTION

IT is constantly evolving in the direction of a cloud consumption model. This transformation influences how the applications have been developed and implemented, steering evolution in data center infrastructure design to satisfy these shifting requirements [1,2]. As the basis of the modern-day data center, the network should also play a part in this evolution while at the same time gathering the growing demands of server virtualization as well as new microservices-based architectures [3,4]. This requires a new model that must provide the following areas: i) **Flexibility** to permit workload flexibility throughout any floor tile in any location. ii) **Resiliency** to sustain service standards even in unsuccessful conditions (improved fault separation). iii) **Multi-tenancy** facilities and better capacity segmentation. iv)**Performance** to deliver for sufficient bandwidth and predictable latency, autonomous of scale for the most demanding workloads. v) **Scalability** from the small environments to the cloud-scale while keeping the above traits [5]. As a consequence, modern data center networks have been evolving from the traditional hierarchical designs to horizontal direction orientated spine-leaf architectures along with hosts and services distributed across the network. Such networks are capable of supporting the more and more widespread east-west traffic flows experienced in modern applications. Additionally, there remain clustering technologies and virtualization techniques that need Layer 2 proximity. Evolving user requirements and application prerequisites suggest a different method that is straightforward, and much more agile. The simplicity of provisioning and speed are currently critical performance measurements for data center network infrastructure which supports physical, virtual, as well as cloud environments without endangering scalability or security. These are the major drivers for the industry to see Software Defined Network (SDN) solutions. The VXLAN Fabric with BGP EVPN control plane offers a scalable, flexible as well as easy-to-manage solution to meet the growing needs of cloud-based environments. The subsequent paper also describes the design as well as the integration of Layer4-Layer7 network services, co-existence in conjunction with brownfield environments, operation, as well as maintain a VXLAN EVPN. In this paper, we explained the ideas of VXLAN EVPN and the issue it has been designed to solve. At the conclusion of this paper, the reader will have a powerful foundation of VXLAN EVPN and the knowledge of real-world use instances that could be instantly used to contribute to the development of a strategy to effectively shift to the next-generation data center with this new technology.

II. AN OVERVIEW OF VXLAN EVPN

It has been several years since; Network segmentation has been provided by VLANs in data center networks as a de-facto standard. Standardized as IEEE 802.1Q, VLANs leverage conventional loop prevention methods like Spanning Tree Protocol that not only enforces restrictions on network design as well as resiliency, although it will result in ineffective use of available network links owing to the blocking of redundant paths, which is necessary to ensure a

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

loop-free network topology [6,7]. VLANs also utilize a 12-bit VLAN identifier to respond to Layer 2 segments, thus enabling the addressing of through to a practical limit of around 4,000 VLANs. With the expansion of large, multi-tenant data centers and increasingly complex IT infrastructure, VLANs have become a major limiting factor to IT departments and cloud providers in modern data center networks. Modern data centers need a development from the shackles of traditional Layer 2 networks. leading manufacturers recommended the Virtual Extensible LAN (VXLAN) standard towards the IETF as a solution for the data center network challenges presented by traditional VLAN technology as well as the Spanning Tree Protocol [8,9]. At the heart, VXLAN offers advantages of flexible workload placement, greater scalability of Layer 2 segmentation, as well as a connection to the extension throughout the Layer 3 network boundary [10]. Though, with not an intelligent control plane, and due to its flood and learn behavior, VXLAN has its limits. Multi-Protocol Border Gateway Protocol (MP-BGP) established new Network Layer Reachability Information (NLRI) to take both Layer 2 MAC and Layer 3 IP information at the same moment [11]. By allowing the merged set of MAC and IP information that is available for forwarding decisions, improved routing and switching across a network becomes viable as well as the need for flood and learn behavior that limits its capacity to scale. An extension that allows BGP to transport Layer 2 MAC and Layer 3 IP information will be called EVPN (Ethernet Virtual Private Network) [12,13].

The following are some of the advantages provided by VXLAN EVPN solutions:

1	Standards-based Overlay (VXLAN) with standards-based control plane (BGP)
2	Facilitation of Software-Defined-Networking (SDN)
3	Layer 2 MAC and Layer 3 IP information distribution by control plane (BGP)
4	Leverages Layer 3 ECMP – all links forwarding – in the underlay
5	Integration of physical and virtual networks with hybrid overlays
6	Forwarding decision based on scalable control plane (minimizes flooding)
7	Integrated Routing/Bridging (IRB) for Optimized Forwarding in the Overlay
8	Significantly larger namespace in the overlay (16M segments)

Source: Cisco Blog [14]

Table 1 Advantages provided by VXLAN EVPN solutions

III. THE PURPOSE OF VIRTUAL EXTENSIBLE LAN (VXLAN) OVERLAY

A Network overlays are a method that is used in modern data centers to build an adaptable infrastructure over an intrinsically static network through virtualizing the network. Instead Of going into the specifics of the way in which overlays work, the challenges facing them, as well as the solutions to overlay obstacles, it is worth spending a while to understand why conventional networks are therefore unchanging [15]. Since networks were originally developed, there had been no such thing as an application transferring from one place to another whilst it has been in use. As a consequence, the initial architects of TCP/IP were using the IP address as both the identification of a device as well as its location on the network. This has been a quite reasonable thing to accomplish as both the computer and their applications are not moving, or at the very least they did are not moving very quickly or very frequently [16]. At Present in the state-of-the-art data center, applications are frequently installed on virtual machines (VMs) or else containers. The virtual application workload may be extended across several locations. The application endpoints (Virtual Machines, containers) may also be mobile amongst different hosts. Their identity (IP addresses) doesn't indicate their location. Owing to the rigid pairing of an endpoint's location with its identity within the conventional network model, an endpoint might need to change its IP address to specify the new location once it progresses. This breaks down through the seamless mobility model needed by the virtualized applications [17]. Consequently, the network needs to evolve from the static model to a more flexible one in order to constantly provide assistance to communications among application endpoints irrespective of wherever they are. One method is to distinguish between the identification of an endpoint from its physical position on the network so the sites can be modified at will without violating the communications to an endpoint. This is a place where overlays are coming into the picture [18].

An overlay receives the initial message sent through an application and encapsulates it along with the location it wants to be delivered to before it is sent across the network. Once the communication comes at its ultimate destination, it remains decapsulated and delivered as wanted [15,19,20]. The identities of the devices (applications) communicating are in the initial message, and the sites are located in the encapsulation, hence dividing the location from the identity. This encapsulation, as well as decapsulation, is carried out on a per-packet basis and thus must be done extremely

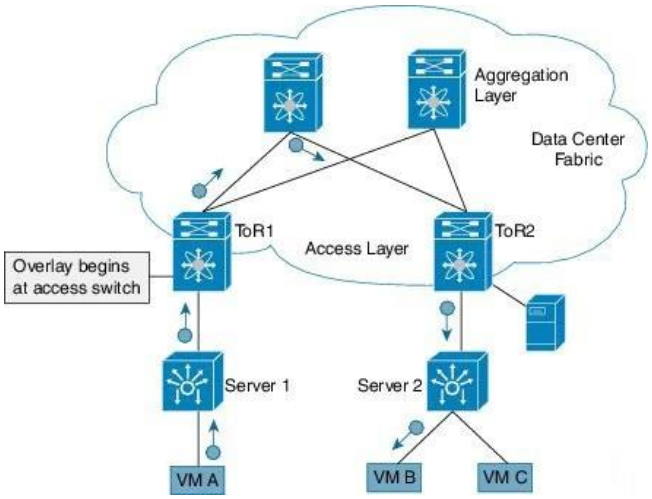
IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701



Source: Cisco.com
Fig. 1 VXLAN Overlay

quickly and efficiently. At Present, in accordance with the market research, roughly 60-70% of all the application workloads are virtualized, though, over 80% of servers currently in use do not run a hypervisor. Obviously, every data center is a unique mix of servers that run virtualized workloads vs. non-virtualized workloads cover the whole spectrum. Every network solution used for the data center should address this mix [15]. The suggested Virtual Extensible LAN (VXLAN) standard in accordance with the IETF as a solution to the data center network challenges presented by conventional VLAN technology. The VXLAN standard offers for the flexible workload placement and the higher scalability of Layer 2 segmentation that is needed by the present application demands [21].

VXLAN is designed to deliver the identical Ethernet Layer 2 network services such as VLANs are doing today, but with higher extensibility as well as flexibility [15]. Applying VXLAN technologies through the network will provide the following advantages to each workload in the relevant data center [21]:

1	Flexible arrangement of any workload in each and every rack throughout and between data centers
2	Decoupling between the physical and virtual networks
3	Large Layer 2 network to give workload mobility
4	Centralized Management, provisioning, and automation, from a controller
5	Scaling, Performance, agility, and streamlining operations
6	Improved utilization of available network paths in the fundamental infrastructure

Source: VXLAN Overview [21]
Table 2 Advantages provided by VXLAN technologies

IV. AN EXPLANATION OF WHY A CONTROL PLANE IS NEEDED

Once implementing an overlay, there are three main tasks that need to be achieved. First Of All, there should be a system to forward packets across the network. Conventional networking mechanisms remain effective for this [22,23]. Secondly, there should be a control plane in which the location of an appliance or application may be looked up and the outcome used in order to encapsulate the packet so that it could be forwarded to the target [24,25]. Thirdly, there has to be a way to upgrade the control plane in such a way that it is always correct [15]. Obtaining the false information in the control plane might result in packages that are sent to the wrong location and presumably dropped [26]. The first assignment, forwarding the packet, is something that network equipment has constantly delivered. Reliability, Performance, cost, as well as supportability, are basic considerations for a network that should similarly be applied to both the physical and overlay networks respectively [27]. The second task, control plane lookup, and encapsulation are actually a problem of performance as well as capacity. If these tasks were performed in software, they will consume important CPU resources and then add the latency as compared to hardware solutions. The third element of an overlay is the means through which the changes to the control plane will be updated through all the network elements. This

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

updating is a true challenge and a worry for all the data center administrators because of the potential for the application effect from packet loss when the control plane malfunctions [28,29].

V. THE VXLAN CONTROL PLANE

VXLAN as the overlay technology does not offer several of mechanisms in place for scale and fault tolerance which other networking technologies have been developed and are currently taking for granted [30]. In VXLAN networks, every switch creates a database by using the locally connected hosts. The mechanism is necessary so that more switches find out more about those hosts. In a conventional network, there is absolutely no mechanism to distribute this information [31,32]. The sole control plane formerly available as a data plane-driven model referred to as flood and learn. For the host to be accessible, its information needs to be flooded through the network. Ethernet networks have operated through this weakness for years [33,34]. Although the demand for scalable networks rises, the consequences of flood and learn will have to be mitigated. For VXLAN overlay, a control plane is mandatory which is capable of distributing the Layer 2 and Layer 3 host accessibility information within the network [35]. Initial implementations of VXLAN did not have the ability to carry Layer 2 network accessibility information, hence, Ethernet VPN (EVPN) extensions have been added to Multi-Protocol BGP (MP-BGP) to bring this information [36,37].

VI. THE EVPN CONTROL PLANE

An overlay involves a mechanism to find out which end host device stands behind which overlay edge device. VXLAN natively works on a flood as well as learn mechanism where broadcast, an unidentified unicast and multicast (BUM) traffic in a specific VXLAN network will be sent over the IP core to each VTEP which has a membership in the appropriate network. IP multicast is used to transmit traffic across the network. The receiving VTEPs decapsulates a packet and, based on the interior frame, operate Layer 2 MAC learning. The internal source MAC address that is learned versus the outer source IP address equivalent to the source VTEP. In this manner, reverse traffic is unicasted in the direction of the formerly learned end host [36,37,38,39]. The disadvantage of the flood and learn mechanism remains that it does not permit scalability through a VXLAN network. In order to address this problem, a control plane is used to control the MAC address learning and VTEP discovery [36,37]. In BGP EVPN VXLAN deployments, Ethernet Virtual Private Network (EVPN) will be used as the control plane. EVPN control plane offers the capability to exchange the two MAC address and IP address information. EVPN utilizes Multi-Protocol Border Gateway Protocol (MP-BGP) as a routing protocol to deliver reachability information relating to the VXLAN overlay network, involving endpoint IP addresses, endpoint MAC addresses, and subnet reachability information. BGP EVPN distribution protocol enables mapping information that will be built through the tunnel edge devices in the site-identity mapping database [38,39,40,41].

VII. OVERVIEW OF MP-BGP EVPN CONTROL PLANE

Based on IETF RFC 7342, MP-BGP EVPN is a control protocol for VXLAN. Overlay networks in VXLAN operated based on a flood-and-learn architecture before EVPN was introduced. In this particular model, end-host information learning, as well as VTEP discovery, remain both data-plane based, without control protocol for distribution end-host reachability information between VTEPs. MP-BGP EVPN alters this particular model. It establishes control-plane learning for the end hosts in the back of remote VTEPs. It offers control-plane as well as data plane separation as well as a unified control plane for the two layers, Layer 2 and Layer 3 sending in a VXLAN overlay network. MP-BGP EVPN intended for VXLAN offers a distributed control plane solution that greatly enhances the ability to build and interconnect SDN overlay networks [21,42,43,44].

MP-BGP EVPN control plane for VXLAN offers the following advantages:

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

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

Source: Cisco.com [5,8,11,21,45]
Table 3 MP-BGP EVPN control plane for VXLAN Advantages

VIII. THE EVOLUTION OF THE ETHERNET VPN (EVPN) CONTROL PLANE

The ongoing implementation of the EVPN control plane is concentrating on providing scalable data center Fabrics along with mobility as well as segmentation. Since EVPN control plane implementations become more and more complete, the EVPN control plane can address further use cases like Data Center Interconnect. The entire theoretical description of the EVPN control plane can be caught in a sequence of Internet drafts which are being worked upon at the IETF [41,48]. A common specification of EVPN adapts use instances outside the Data Center Fabric, containing Layer 2 DCI [46]. In order to correctly address the Data Center Interconnect. prerequisites, the EVPN control plane implementation should be extended to include the multi-homing feature that is specified in the EVPN specification to deliver failure containment, site-awareness, loop protection, as well as optimized multicast replication [47,48].

IX. FUNDAMENTAL CONCEPTS: BASIC UNDERSTANDING OF THE TECHNOLOGY AND HOW IT WORKS.

Throughout the networking world, an overlay network is a virtual network running at the top of physical networking infrastructure. A physical network offers an underlay function, providing the connectivity as well as services necessary to support the virtual network examples delivered through the overlay. A virtual network that makes it possible for an independent set of network services that will be offered irrespective of the underlay infrastructure, although such services could be the same. As a good example, it will be possible to deliver Layer 2 connectivity services at the top of a Layer 3 network infrastructure through an overlay network. A very common instance of this will be the VPLS service provided across a carrier's MPLS infrastructure [55,56]. The overlay network usually provides transport of network traffic among tunnel endpoints at the top of the underlay by encapsulating and decapsulating traffic among tunnel endpoints. Tunnel-endpoint can be delivered via a physical device on the network and perform tunnel encapsulation/decapsulation in the hardware [57]. It can also be virtual, along with the tunnel endpoint process that is running in a hypervisor. Hardware-based tunnel endpoint offers a higher performance by utilizing hardware-based forwarding although has fewer flexibility implementing new functionality. On the other hand, a software endpoint offers increased flexibility although at the cost of limited performance [54].

X. VXLAN: A BASIC OVERVIEW

Network overlays are generated by encapsulating traffic as well as tunneling it across a physical network. The VXLAN tunneling protocol encapsulates L2 Ethernet frames in L3 UDP packets. Virtual Extensible LAN (VXLAN) allows virtual L2 subnets or segments which can span an underlying physical L3 network [46,51,53]. Throughout a VXLAN overlay network, every Layer 2 subnet or segment is distinctively identified through a virtual network identifier (VNI). A VNI segments traffic in the same manner that a VLAN ID segments traffic. As is the case for VLANs, endpoints inside the same virtual network are able to communicate directly with one another. Endpoints in various virtual networks require an appliance that supports inter-VXLAN routing, which is usually the router or a high-end switch [42,49,51]. An entity that performs VXLAN encapsulation, as well as decapsulation, is referred to as a VXLAN tunnel endpoint. Every VXLAN tunnel endpoint is usually allocated to a unique IP address [50,52,53].

XI. EVPN: A BASIC OVERVIEW

Ethernet VPN (EVPN) is a standards-based protocol that provides a virtual multipoint bridged connection between different domains across an IP as well as the IP/MPLS backbone network. EVPN allows continuous multitenant, adaptable services which can be expanded on demand [46,58,59]. EVPN is an expansion to BGP which enables the network to take both L2 MAC and L3 IP information at the same time to improve routing and switching decisions. Such control plane technology utilizes Multiprotocol BGP (MP-BGP) intended for MAC and IP address at the endpoint distribution, where MAC addresses are considered to be routes. EVPN allows devices acting like virtual tunnel endpoints (VTEPs) to exchange reachability information among themselves regarding their endpoints [58]. EVPN offers multipath forwarding as well as redundancy via an all-active model. An access layer can be connected between two or more distribution devices as well as forward traffic-utilizing all of the connections. If the access link or distribution device fails, traffic flows from the access layer in the direction of the distribution layer that uses the remaining active links. For the traffic in the opposite direction, remote distribution devices update their forwarding tables to transmit traffic toward the remaining active distribution devices attached to the multihomed Ethernet segment [8,21,58].

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

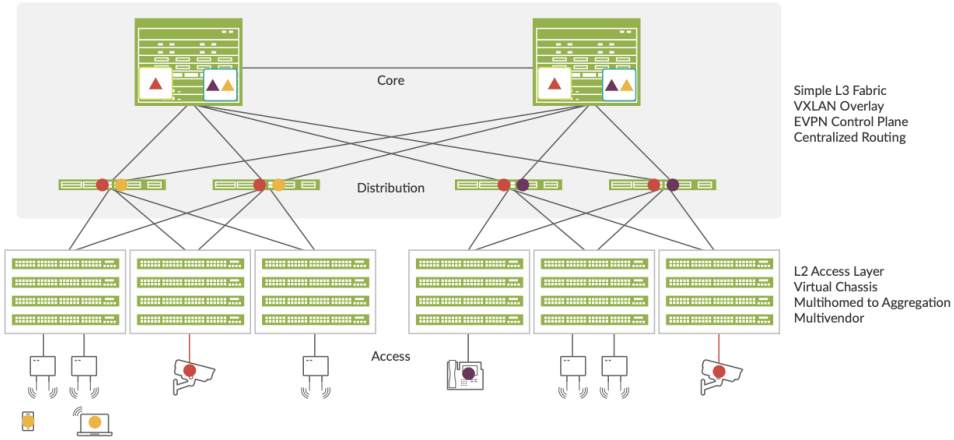
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

XII. IN THE ENTERPRISE OF EVPN-VXLAN

An EVPN-VXLAN-based campus architecture allows for enterprises to easily add additional core, distribution, and access layer devices to an ever-increasing business without needing to redesign together with a new set of devices to upgrade the architecture [46,61,62,63].

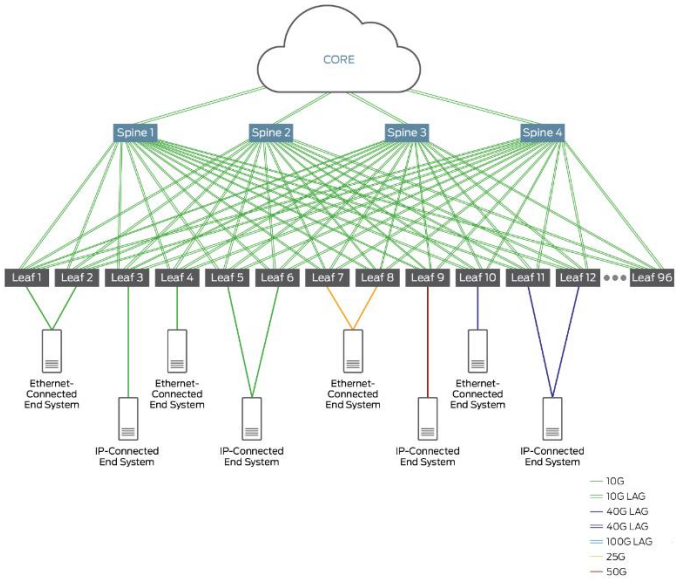


Source: juniper.net
Fig. 2 EVPN-VXLAN-based campus architecture

Furthermore, enterprises can use a common set of policies as well as services throughout campuses in conjunction with support for Layer 2 and Layer 3 VPNs. By utilizing a Layer 3 IP-based underlay together with an EVPN-VXLAN overlay, campus network operators will be able to deploy much larger networks than remain otherwise accessible with traditional Layer 2 Ethernet-based architectures [46,61,62,63,64].

XIII. EVPN-VXLAN IN THE DATA CENTER

The latest data centers that are running on the scale usually use an IP fabric architecture with EVPN-VXLAN overlay.



Source: juniper.net
Fig. 3 Data center fabric architecture

The IP fabric allows you to collapse conventional networking layers in the two-tier spine-and-leaf architecture that is optimized for large-scale environments. This extremely interrelated Layer 3 network serves as an underlay to offer high resiliency as well as low latency throughout the network and could be easily scaled off horizontally as needed.The EVPN-VXLAN overlay is sitting on top of the IP fabric, allowing you to expand and interconnect your Layer 2 data

IJIREEICE
ISSN (Online) 2321-2004
ISSN (Print) 2321-5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
Vol. 9, Issue 7, July 2021
DOI 10.17148/IJIREEICE.2021.9701

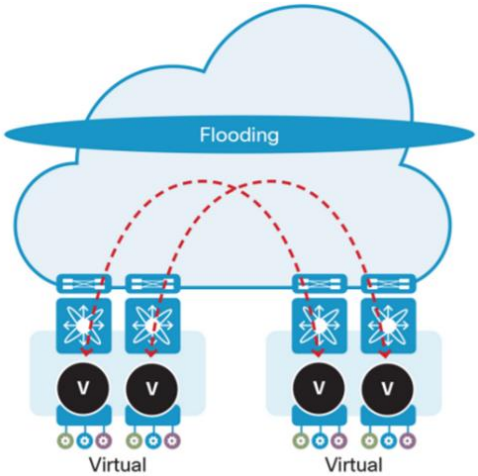
center domains as well as place endpoints (like the servers or virtual machines) anywhere within the network, even across data centers [61,65].

XIV. INTRODUCTION OF SOFTWARE OVERLAYS

Server virtualization has changed the manner in which the data centers are operated, and the overwhelming majority of data centers these days implement it to a certain extent. Though, making the assumption that those data centers run solely virtualized workloads will be a mistake. Numerous organizations still utilize mainframes, for instance. Furthermore, new applications which do not require server virtualization are going into the major stage, like cloud-based software which makes use of Linux containers, or modern scale-out applications for example the Big Data, that deliver operational advantages and scale without the requirement of a hypervisor. Though VXLAN is a common overlay concept that is commonly deployed across the network, it is occasionally linked with server virtualization and hypervisors. This section explains the strengths and weaknesses of implementing VXLAN on virtualized hosts, and how to achieve the greatest benefit out of this technology, taking into account the fact that one of the primary reasons for the interest in VXLAN is its openness, which prevents vendor lock-in (vendor or hypervisor) [66].

XV. HOST-BASED OVERLAY OVERVIEW

Server virtualization provides significant benefits such as more flexibility and agility in delivering computing services within the data center. Networking to the hypervisor is traditionally provided through VLAN transport, and there is a recent trend to introduce host based VXLAN overlays to enhance the agility and automation of the network layer.



Source: Cisco.com
Fig. 4 Host-Based Overlay

The host-based overlay usually runs between the host VTEPs over IP transport and provides the simplicity of deployment and automation capability, enabling the server team to be able to provide virtual networking essential services without the need to engage the network team. This capability to automate networking directly by the Virtual Machine Manager (VMM) as a software-only overlay frequently results in a sub-optimal network solution that does not take into consideration the wider aspects of operations, integration, as well as performance for the network as a whole. Due to the lack of correlation between overlays and underlays, the network team has to spend extra time troubleshooting in addition to the CPU impact introduced by host-based overlays. In connection with the CPU impact, the overall performance of a software VTEP is reliant on the CPU and memory that is available in the hypervisor. Some implementations run the VTEP function in kernel space, while others run it in userspace. Either option should deliver the essential packet processing necessary for efficient application delivery [67]. Following solutions usually struggle to provide line-rate throughput even with hardware assistance on the server NIC. Furthermore, host-based overlay network solutions are primarily concentrated on networking for virtual servers without consideration for physical workloads or any other existing services internal or external to the data center. Connectivity to both the physical servers as well as resources outside the virtual network usually requires gateways, both in software or hardware that needs to be integrated into the physical network [68]. In brief, when assessing the host-based overlay solutions, it is important to take into account the broader commercial and technical implications for the data center comprising licensing cost, performance penalty, compute operating expense, additional gateway infrastructure requirements, as well as the impact on network operations.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

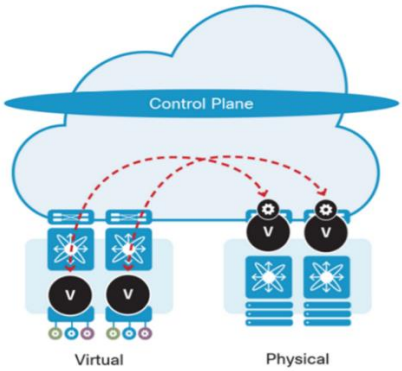
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

XVI. HYBRID OVERLAYS ALONG WITH VXLAN EVPN

As discussed earlier, pure host-based overlays give slight value to data centers, although there are situations where a hybrid approach might be able to solve some challenges or use cases. Service Providers have extremely particular requirements about network management and operations including i)A mix of hardware and software VTEPs is supported ii) Integration along with the hypervisor layer iii) multi-vendor fabric support iv) Underlay and overlay are operated by different teams. Hybrid VXLAN overlays comprise the two host-based software VTEPs and switch-based hardware VTEPs. A unified operational and management model is required to integrate the two kinds of VTEP jointly. Virtual Topology System (VTS) is an instance of such a solution.

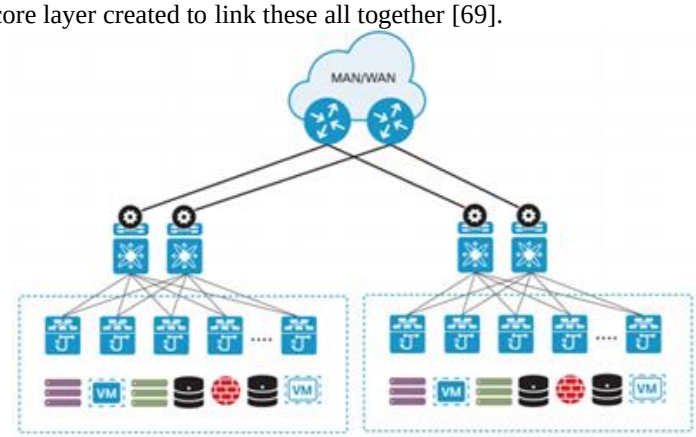


Source: Cisco.com
Fig. 5 Hybrid Overlays

Virtual Topology Systems (VTS) provisions hardware and software VTEPs. The ability to integrate a VXLAN software-based VTEP allows the deployment of the VXLAN technology on top of legacy network hardware or to complement hardware-based VTEP deployments. The Virtual Topology Controller (VTC) is the single point of management for hybrid overlays to configure, manage and operate a VXLAN Fabric with an MP-BGP EVPN control plane. The management layer supports integration with hypervisors such as VMware vSphere or Openstack / KVM so that network constructs can be directly provisioned from the hypervisor User Interface. The northbound REST APIs enable integration with third-party tools. The control plane is represented by a virtualized IOS-XR router to provide integration with MP-BGP EVPN and advertise reachability information to the software VTEP itself over an API. The software VTEP named Virtual Topology Forwarder (VTF) provides VXLAN encapsulation capability in the hypervisor.

XVII. SINGLE-POD VXLAN DESIGN

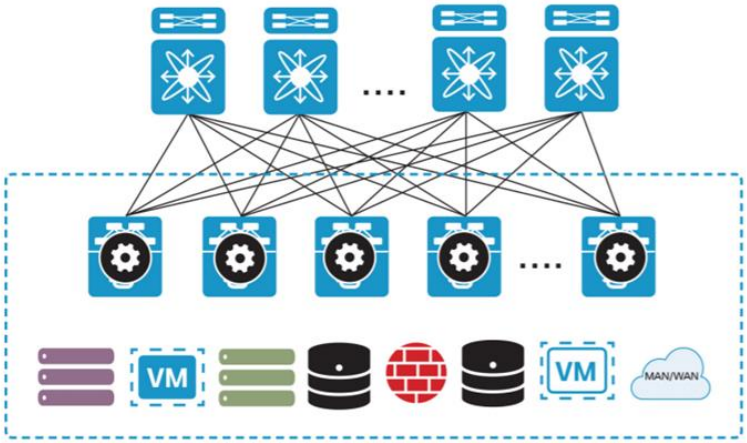
In the classic hierarchical network designs, Layer 2 and Layer 3 functionality are provided by access and aggregation layers together as building blocks for data center connectivity. In the smaller data center environments, a single building block would be scalable enough to meet the entire demand for connectivity and performance. Such as the environment scales to fulfill the enhanced demands of the larger data center, this building block is usually replicated along with an additional core layer created to link these all together [69].



Source: Cisco.com
Fig. 6 Hierarchical Network Design

IJIREEICE
ISSN (Online) 2321-2004
ISSN (Print) 2321-5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
Vol. 9, Issue 7, July 2021
DOI 10.17148/IJIREEICE.2021.9701

These building blocks are usually referred to as a Point of Delivery, or POD, and to enable reliable, modular scale as the environment expands. While you are designing VXLAN Fabric, a single-POD also identifies a single VXLAN Fabric-based upon a scalable spine-leaf architecture as shown in the illustration below [70].



Source: Cisco.com
Fig. 7 VXLAN Fabric

A single VXLAN POD can scale to hundreds of switches as well as thousands of ports that will meet the requirements of several enterprise data center environments; though, to encounter more sophisticated or larger-scale requirements, the VXLAN POD can be replicated in the shape of a multi-POD design. In a standard deployment with multiple data center locations, these VXLAN Fabrics, whether single or multi-POD-based, shall be deployed together like a multi-site VXLAN design. Equally, the multi-POD and multi-site deployment types are described in more detail in the multi-POD and multi-site Designs section [71].

XVIII. AN OVERVIEW OF LAYER4-LAYER7 SERVICES AND DEPLOYMENT DEVICE TYPES

A VXLAN Fabric offers Layer 2 and Layer 3 connectivity; though, extra services are necessary for the data center. Such services are provided by dedicated appliances physical or virtual and need a connection to the fabric. Those are the dedicated functions that shall be referred to as Layer4-Layer7 services. Traditional hierarchical network models link Layer4-Layer7 services at an aggregation layer. Within a VXLAN Fabric, Layer4-Layer7 appliances can be linked to any leaf switch or connected to a dedicated leaf pair referred to as a “service leaf". There are several different connectivity possibilities for physical and virtual appliances.

Layer4-Layer7 Device Types: Depending upon the requirements, multiple Layer4-Layer7 services can be implemented to offer a complete network and service function stack. These features include the following: i) Stateful Layer 4 firewalling: There are several organizations that implement network security through dedicated firewalls with complex firewall policies. The firewall policies permit or deny communication between different organizational or application tiers. Firewalls are also capable of performing other functions such as Network Address Translation (NAT). ii) Application Firewalls: Today, most attack vectors are focused on the application. The attacks leverage standard TCP ports to exploit application vulnerabilities. SQL Code Injection and Cross-Site Scripting are examples. Application-level firewalls can be used to protect against these modern attacks. iii)Intrusion Detection (IDS) / Intrusion Prevention (IPS): The solution detects attacks and helps prevent systems from being compromised. In addition, it prevents a compromised system from initiating suspicious network activity. Ping sweeps and port scans are examples of network reconnaissance. iv) WAN Optimization: The objective of this service will be to enhance the user experience through methods such as optimization of the TCP stack, compression, as well as content caching. v)Application Delivery Controllers (ADC): The ADC incorporates server load balancing, SSL offloads as well as other application functionality. ADCs may be deployed on their own or in tandem with other service nodes [5].

Some Layer4-Layer7 appliance vendors may incorporate several of the above-mentioned categories into a single product such as FW and IPS. Additionally, another frequently used term is a service chain, when multiple Layer4-Layer7 appliances are implemented in a sequence, such as WAN optimization, FW, and ADC [5,8].

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

XIX. THE REASON FOR DEPLOYING MULTI-POD AND MULTI-SITE

An increasingly competitive, globally connected business environment puts enormous pressure on organizations to ensure the continuous availability of critical business applications. As digital strategies drive innovative new business opportunities, these organizations are looking for IT infrastructures that can support these new application infrastructures by offering agility, performance, and availability. When you build the IT infrastructure to provide support for these business-critical environments, the modern-day data center deployments need geographic diversity and scale, guaranteeing the ability to provide rapid scale, high-performance, and "constantly on" availability. As a result, data center networks have been building built as scalable, highly available network fabrics that are distributed across multiple data centers, whether separated within or across a metro area, or across the globe [5,8].

Reason for Deploying Multiple PODs

The best possible way to efficiently scale a system is through modularity. Any monolithic architecture will only grow to a certain point, after which inefficiencies will appear. A data center is an example of a system that requires a flexible way to scale the network infrastructure. Frequently a data center build-out starts in a single room and later expands across multiple rooms. Besides scale, physical facility and infrastructure layouts can be another motivation for multi-POD designs. Multi-POD designs fit very well in situations where a physical location is partitioned across multiple rooms with limited cabling but maintaining end-to-end Layer 2 and Layer 3 connectivity is still required. Any service within one POD can be made available to any other POD within this multi-POD topology. As an instance, consider a high availability (HA) cluster being implemented at a single physical location but spread throughout different rooms due to the site's local HA capabilities different Power Distribution Unit - PDU, Uninterruptible Power Supply - UPS, etc [5,8,10].

Reason for Deploying Multiple Sites

Modern latest data center environments need to meet the requirements for the high availability in a data center and across geographically distributed DC infrastructure. This kind of distributed architecture offers several advantages for highly available application delivery. Applications may be delivered into an active/active or active/standby deployment model and form the basis for effective business continuity or disaster recovery strategy. There are many factors that determine the relevance and design of the multi-site data center environment including physical limitations for example the site location and the requirements for geographical diversity. Other factors include bandwidth and service availability for the infrastructure such as dark fiber or wavelength service, as well as the latency which might affect application performance. These considerations determine the Recovery Point Objective (RPO) and The Recovery Time Objective (RTO) for application availability. In contrast to single-site deployment, the networking solution for multiple locations should also address the need to keep a level of separation. Any occasion whether planned or unplanned has an impact on one site should not spread to any other site as it would impact overall application availability. When deploying a network infrastructure based on VXLAN EVPN, the consistent delivery of Layer 2, Layer 3 and IP multicast services must be maintained. Together, these allow for the delivery of distributed application architectures and geographically dispersed clustered infrastructure to support highly available storage access and compute virtualization.

Design criteria to be taken into consideration for such deployments include i) Physical Connectivity: In many instances, given the limitations set forth above, the accessibility of connectivity services can be limited. As an instance, dark fiber or wavelength services availability can be limited or cost-prohibitive over large distances, while a routed Layer 3 or MPLS service can be easily available at a feasible price point. The design should take into account the need to allow for multiple connection categories ranging from high bandwidth dark fiber through to bandwidth-constrained service provider-delivered Layer 3 services. ii) Fault Isolation: While connecting multiple separate network environments altogether, the risk of a failure event transmitting between sites dramatically increases unless controls will be applied to limit the control plane and data plane activity. Examples are the selection and configuration of control plane protocols such as BGP, and the control or restriction of data plane activity such as ARP suppression/spoofing and storm control. Based upon these criteria, the multi-site solution must provide a suitable set of features and functionality necessary to meet the specific demands of a specific deployment.

XX. CONCLUSIONS

In light of the evolution of cloud technology and the benefits of multi-tenancy, the fundamental requirement of network architecture has entirely changed. It is now necessary to achieve seamless business continuity via multi-data centers across locations. It has been necessary to enhance existing technologies and implement new technologies with lots of new functionality and features. Based on the analysis of emerging technologies, this research paper focuses on the latest capabilities of VXLAN, EVPN, Data Centers infrastructure as per the requirements and requirements analysis for the

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

industry. By studying this research paper, network professionals will be able to design the Data Center with the latest state-of-the-art technologies. Based on our study, Modern Data Centers are experiencing multiple infrastructure problems due to high demand from users and a large volume of traffic flowing across their networks. Many of them can be solved with VXLAN and EVPN. Researchers within the field of networking are presenting the research paper in order to help network professionals gain knowledge of new technologies and introduce them to VXLAN and EVPN techniques for designing a data center. VXLAN EVPN is thoroughly examined in this paper, beginning with the introductory stages, gaining a clear understanding of the terms and concepts, and moving through scenarios from single data centers to multiple data centers. Additionally, the paper discusses the design and integration of L4-L7 network services, coexistence with brownfield environments, and how to build, operate, and maintain VXLAN EVPNs. Readers will walk away from this paper with a solid understanding of VXLAN EVPN and a grasp of real-world use cases that can be utilized immediately to aid in identifying a successful strategy to implement a next-generation data center with this new technology.

REFERENCES

[1]. TECHNATIVE- Why today's evolving data center needs composability- APRIL 23,2020- by Marten Terpstra- https://technative.io/why-todays-evolving-data-center-needs-composability/
[2]. Cisco-What Is a Data Center-https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html.
[3]. https://blogs.juniper.net/en-us/enterprise-cloud-and-transformation/evpn-and-the-future-of-data-centers - EVPN and the Future of Data Centers- May 7, 2019- by Michael Bushong.
[4]. IASA -Data Center Design- by Brice Ominski- ITAP Consultant – Microsoft https://itabok.iasaglobal.org/itabok3_0/data-center-design/
[5]. https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/nexus9000/sw/vxlan_evpn/VXLAN_EVPN.pdf
[6]. INFOSEC- VLAN network segmentation and security- chapter five [updated 2021]- May 24, 2021 by Tom Olzak- https://resources.infosecinstitute.com/topic/vlan-network-chapter-5/
[7]. NERDYNAUT- Segmenting LANs using Virtual Local Area Networks (VLAN)- February 24, 2019- Shehan Marasinghe. https://www.nerdynaut.com/segmenting-lans-using-virtual-local-area-networks-vlan
[8]. Cisco- VXLAN EVPN Multi-Site Design and Deployment White Paper- May 5, 2021- https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-739942.html.
[9]. ethernuno- Open-Source Knowledge- CCNP SWITCH 300-115 – Part 1.3 Configure and verify VLANs- by ethernuno on 19/11/2015- https://ethernuno.wordpress.com/2015/11/19/ccnp-switch-300-115-part-1-3-configure-and-verify-vlans/
[10]. Cisco - Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide, Release 5.2.x- https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/lxvpn/configuration/guide/b-l2vpn-cg52xasr9k/b-asr9k-l2vpn_chapter_01011.html
[11]. https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/nexus9000/sw/vxlan_evpn/VXLAN_EVPN.pdf
[12]. SPEAK NETWORK SOLUTIONS | by Jack Wang | March 21st , 2016| SDN, Virtualization| https://www.speaknetworks.com/what-is-cisco-aci-fabric/
[13]. Cisco - Virtual Extensible LAN and Ethernet Virtual Private Network- January 19,2018 Document ID: 212682 https://www.cisco.com/c/en/us/support/docs/lan-switching/vlan/212682-virtual-extensible-lan-and-ethernet-virt.html
[14]. Cisco Blogs - Data Center VXLAN/EVPN: Standards based Overlay with Control-Plane- Lukas Krattiger- February 5, 2015- https://blogs.cisco.com/datacenter/vxlanevpn-standards-based-overlay-with-control-plane
[15]. Cisco Blogs- ACI Design Principles: The role of SDN Overlays in Application Centric Deployments – Part 1- Shashi Kiran- February 28,2014
[16]. https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address
[17]. Cisco - Cisco Application Centric Infrastructure (ACI) - Endpoint Groups (EPG) Usage and Design- Document ID:1595263694155376- https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731630.html
[18]. DZone- Cloud Zone- A Glossary of 37 Modern Data Center Terms You Need to Know- by Rob Whiteley · May. 18, 17 · Cloud Zone · Analysis
[19]. https://docs.oracle.com/cd/E19455-01/806-0916/6ja85398n/index.html
[20]. https://www.sparkpost.com/resources/email-explained/email-message-flow-sending-delivery/
[21]. Cisco - VXLAN Overview: Cisco Nexus 9000 Series Switches- November 6, 2013, Document ID:1476825831111564 - https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-729383.html
[22]. Netwrix Blog - Network Security Devices You Need to Know About - Jeff Melnick
Published: January 22, 2019, October 3, 2019- https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/
[23]. https://datatracker.ietf.org/doc/html/rfc5245
[24]. NetworkStatic | Brent Salisbury's Blog- GoBGP – A Control Plane Evolving Software Networking- MAR 29, 2016, by BRENT SALISBURY in IN THE LAB, PROGRAMMING- https://networkstatic.net/gobgp-control-plane-evolving-software-networking/
[25]. AfterAcademy- Amit Shekhar- Co-Founder @AfterAcademy- 4 Mar 2020 - https://afteracademy.com/blog/what-is-data-encapsulation-and-de-encapsulation-in-networking
[26]. Cisco- Control Plane Policing- December 5, 2006 - https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/cpp.html
[27]. https://en.wikipedia.org/wiki/Reliability_engineering
[28]. https://www.liveaction.com/resources/tips-and-tricks/packet-loss-impact/
[29]. https://en.wikipedia.org/wiki/Software-defined_networking
[30]. Network Direction- https://networkdirection.net/articles/routingandswitching/vxlanoverview/
[31]. https://en.wikipedia.org/wiki/Computer_network
[32]. PC & NETWORK DOWNLOADS VXLan – What Is it & Quick Tutorial Marc Wilson 10/12/2020 https://www.pcwdld.com/vxlan
[33]. https://www.open.edu/openlearncreate/mod/oucontent/view.php?id=129584&printable=1
[34]. https://www.lantronix.com/resources/networking-tutorials/ethernet-tutorial-networking-basics/
[35]. https://www.juniper.net/us/en/research-topics/what-is-evpn-vxlan.html
[36]. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-12/configuration_guide/vxlan/b_1612_bgp_evpn_vxlan_9500_cg/bgp_evpn_vxlan_overview.html#id_126791

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9701

[37]. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/vxlan/configuration/guide/b_NX-OS_VXLAN_Configuration_Guide/configuring_vxlan_bgp_evpn.html
[38]. Cisco -BGP EVPN VXLAN Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches) https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-12/configuration_guide/vxlan/b_1612_bgp_evpn_vxlan_9500_cg/bgp_evpn_vxlan_overview.html#id_126945
[39]. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-9/configuration_guide/lyr2/b_169_lyr2_9500_cg/configuring_vxlan_bgp_evpn.html
[40]. https://support.huawei.com/enterprise/ru/doc/EDOC1100055055/64f9ec04/understanding-evpn
[41]. https://www.arista.com/en/um-eos/eos-evpn-overview
[42]. Cisco -Deploy a VXLAN Network with an MP-BGP EVPN Control Plane White Paper- June 29, 2015, Document ID:1571251013146951- https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white-paper-c11-735015.html
[43]. Data Center Dope VXLAN MP-BGP EVPN Part 1- October 14, 2015, by matt pinizzotto
[44]. https://support.huawei.com/enterprise/en/doc/EDOC1100168670
[45]. https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKDCN-3040.pdf
[46]. https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/nce-evpn-vxlan-campus-primer.html
[47]. https://datatracker.ietf.org/doc/html/draft-snr-bess-evpn-loop-protect-00
[48]. Nokia Ethernet VPN (EVPN) for integrated layer 2-3 services by Greg Hankins , Jorge Rabadan 2 Jun 2014
[49]. https://www.arubanetworks.com/faq/what-is-evpn-vxlan/
[50]. https://koo.seeduwaambo.online/juniper-vxlan-configuration-example.html
[51]. https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/8/html/networking_guide/openstack_networking_concepts
[52]. https://networkdirection.net/articles/routingandswitching/vxlanoverview/
[53]. https://networklessons.com/cisco/ccnp-encor-350-401/introduction-to-virtual-extensible-lan-vxlan
[54]. https://docs.microsoft.com/en-us/azure-stack/hci/concepts/plan-software-defined-networking-infrastructure
[55]. https://docs.docker.com/network/overlay/
[56]. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/layer2/7x/b_5600_Layer2_Config_7x/config_vxlans.html
[57]. https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html
[58]. https://docplayer.net/201610384-Configuring-an-evpn-vxlan-fabric-for-a-campus-network-with-erb.html
[59]. https://docs.nvidia.com/networking-ethernet-software/cumulus-linux-37/Network-Virtualization/Ethernet-Virtual-Private-Network-EVPN/
[60]. https://wiki2.org/en/Virtual_private_network
[61]. https://www.juniper.net/us/en/research-topics/what-is-evpn-vxlan.html
[62]. https://www.infradata.com/resources/what-is-evpn-vxlan/
[63]. https://www.electronicsmedia.info/2018/07/02/juniper-networks-delivers-evpn-vxlan-fabric-connect-enterprise-data-center-campus-networks/
[64]. https://support.huawei.com/enterprise/en/doc/EDOC1100141248/eebc9ffc/overall-design
[65]. https://marconiwireless.world/data-center-networking
[66]. https://www.infoq.com/articles/virtualization-intro/
[67]. https://www.arubanetworks.com/techdocs/VSG/docs/040-dc-design/esp-dc-design-020-network-design/
[68]. Nuagenetworks-from Nokia- Network Virtualization: Overlay and Underlay Design by Dimitri Stiliadis, Jul 16, 2013
[69]. https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white-paper-c11-737022.html
[70]. https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737855.html
[71]. https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html