Ethernet Virtual Private Networks
for
Integrated, Scalable
Layer 2 and Layer 3 VPN Services

Contents

Broadband Forum White Paper
MR-350
February 2016

1 Overview and Introduction

Ethernet Virtual Private Networks (EVPN) deliver a wide range of benefits—including greater network efficiency, reliability, scalability, mobility and policy control—that directly impact the bottom line of service providers and enterprises alike. This white paper provides an overview of EVPN, including its features and benefits.

As customers expand their networks and move to use Network Function Virtualization (NFV) an integrated service interface that provides both Layer 3 as well as Layer 2 VPN services and lets the customer choose either one or both becomes very appealing.

Carriers are constantly faced with the challenge of providing enhanced services to their customers in a cost effective manner. Layer 3 IP Virtual Private Networks (VPN) and Layer 2 Ethernet VPN services are established technologies for VPN service delivery in the carrier environment. Both approaches have strengths and limitations in addressing different market segments and this makes it desirable for carrier customers to combine them in solutions and therefore for a carrier to offer both. In such situations an integrated approach to providing these services gives an enhanced experience to the customer as well as reduces operational cost to the customer and provider.

2 Ethernet Virtual Private Networks (EVPN)

EVPN is a next generation technology that was created to address the limitations of legacy Ethernet Layer 2 VPN and address new requirements. EVPN can already provide the MEF E-LAN service and standardization is in progress to support E-Line and E-Tree services. EVPN introduces control-plane based learning of MAC addresses. This enhances scalability and provides a mechanism to apply policies. The control-protocol chosen is Multiprotocol BGP (MP-BGP) and this underpins a scalable and resilient architecture that is similar to the proven architecture of IP VPNs.

Broadband Forum TR-224 describes the architecture and requirements to develop a solution for Carrier Ethernet services using MPLS using VPLS and VPWS. Broadband Forum TR-350 describes the architecture for those same services using EVPN, improving scalability and resiliency while simplifying operations.
This paper provides:

- A short background of IP and Ethernet VPNs
- An overview of the EVPN technology and architecture
- Business drivers that propel EVPN

3 IP VPN and Ethernet VPN Services

Enterprises have used connectivity services provided by service providers as the primary connectivity mechanism to interconnect their sites. Over time these connectivity services have been based on different technologies. In the past, circuit switched private line, frame relay and ATM-based services were more prevalent. In the last decade, connectivity services based on IP, Ethernet and MPLS infrastructure have become widely available and deployed to gain network efficiency and convergence of multiple services over the same network.

Provider provisioned Layer 3 and IP VPN services are a popular choice to connect the various sites of an enterprise due to their ability to connect a large number of sites regionally, nationally or globally in an efficient manner. Service providers have implemented the IP VPN service using a MP-BGP/MPLS based IP VPN architecture to interconnect the IP subnets within the different sites of the customer's network infrastructure. Routing, reliability and Quality of Service (QoS) are also managed by the service provider. The IP VPN service provides the foundation on which other value added services such as voice, video conferencing and unified communications are built.

Carrier Ethernet services (or Provider Provisioned Layer 2 VPN Ethernet services) are the other widely available connectivity option. Ethernet has long been a ubiquitous technology choice in the campus due to its cost-effectiveness. Carrier Ethernet services provide the benefit of performance-assured standardized services and have become a popular choice to interconnect LANs across sites that run bandwidth-intensive applications. They provide customers the flexibility to design their own routed network and also provide transport to carry legacy application protocols (e.g. IBM's SNA). Ethernet VPN services have been implemented by many service providers using the MPLS based L2VPN architecture.

4 Evolving Industry Deployments

The widespread deployment of IP VPNs has proven the BGP MPLS-based architecture and produced a deep operational expertise in many carriers' operational teams. The ease, with which a large number of globally distributed remote sites can be connected, has resulted in distribution of the technology expertise across the carriers' operational staff. This has also produced a broad range of well-developed operational procedures that a carrier can use effectively in many deployment scenarios.

The operations for the customer's IT teams have been simplified by the carrier managing the routing for the IP VPN service. According to IDC's 2015 white paper 42% of US business respondents across company size segments utilize network-based IP VPNs. At the same time the cost-effectiveness of Carrier Ethernet services have made it a popular choice especially for high bandwidth applications, e.g. healthcare organizations sharing patient x-rays and medical imaging records between multiple hospital locations. The IDC white paper [1] analyses the trend and business drivers for choosing the best enterprise VPN solutions. The specific choices of Layer 2, Layer 3 or some combination of both are based on application and vertical segments and tradeoffs between the Layer 2 and Layer 3 VPN limitations and/or leveraging their strengths.

Both the Layer 3 and Layer 2 connectivity mechanisms have many common characteristics. The support for multiple Classes of Service (CoS) has enabled the deployment of applications such as voice and video. The integrated VPN solution provides a "mix and match" of the VPNs that can be tailored to best suit any application. An integrated solution provides the best of both services and provides an optimized WAN service. According to the IDC white paper 46% currently deploy both L2 and L3 VPN services.

5 New VPN Requirements

Service Providers and enterprises alike are facing shortcomings in current Layer 2 VPN technologies, especially with the relentless growth of cloud-originated content, video, real-time traffic and inter-data center traffic. Scale, performance and traffic management have become more business critical than ever, driving the need for next-generation Layer 2 VPN technology. Network operators need a VPN solution that:

- Scales to the largest deployments; (e.g., Data Center)
- Maximizes bandwidth through active load balancing;
- Minimizes latency for optimal user experience;
- Speeds service recovery and restoration;
- Reduces configuration and operations overhead; and
- Provides an integrated Layer 2 and Layer 3 VPN solution that efficiently routes traffic in a mixed Layer 2/Layer 3 environments.

6 What is EVPN and Why is it a Recommended Solution?

E-Line, E-LAN, and E-Tree services provide an Ethernet virtual connection between two or more sites. E-Line is a point-to-point (P2P) service, whereas E-LAN and E-Tree provides a point-to-multipoint (P2MP). These services can be implemented on MPLS-based infrastructure using TR-224 architecture and requirements.

[1] *Choosing the Best Enterprise IP VPN or Ethernet Communication Solution for Business Collaboration, IDC, 2015*

While VPLS and VPWS technologies have been a boon to Service Providers and enterprises alike, each has shortcomings that impede business operations and burden IT staff with configuration and operations tasks. Consequently, IETF has developed EVPN, a next-generation, standards-based VPN technology for interconnecting Layer 2 domains that also offers integrated Layer 3 gateway functionality.

EVPN provides network virtualization to support multiple customers over a common MPLS infrastructure. Provider edge devices (PEs) implement multiple EVPN instances to provide virtual Layer 2 bridged connectivity between customer edge devices (CEs), which can be a host, a router or a switch.

EVPN supports different tunnel types, but most implementations use MPLS infrastructure as depicted in Figure 1. By leveraging MPLS, EVPN inherits benefits such as fast-reroute and MPLS CoS. Additionally; EVPN PEs can be connected over an IP infrastructure using MPLS over GRE or VXLAN tunneling. VXLAN, which emerged as a data-plane encapsulation method for data centers with an IP fabric, can also be used in a WAN to carry Layer 2 frames over a pure IP infrastructure.

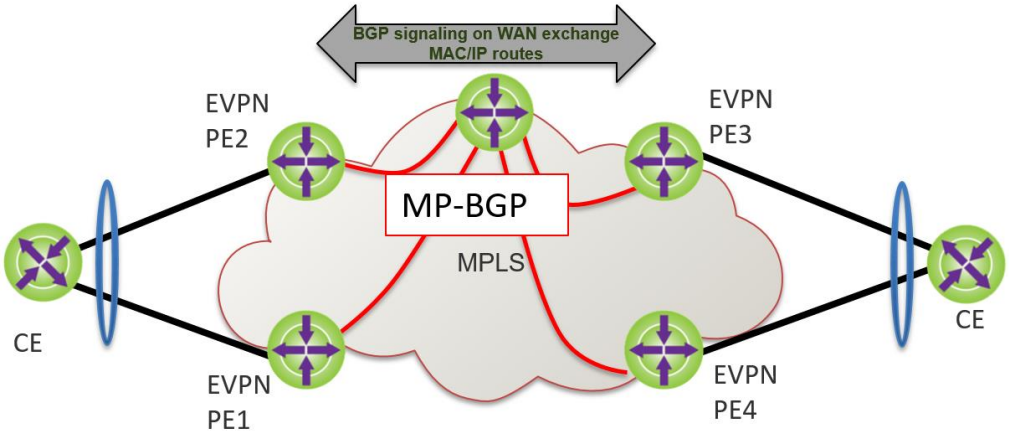


Figure 1: EVPN for next-generation Ethernet services on MPLS.

EVPN is similar to VPLS in the data plane—for example, both implement MAC learning to establish reachability between various Layer 2 devices. A key difference is that EVPN uses the control plane rather than the data plane to communicate MAC and IP address reachability between PEs. EVPN uses multi-protocol BGP (MP-BGP) to distribute MAC routes and their IP bindings. This allows operators to implement very fine-grained control over MAC route distribution and thereby offer more sophisticated Layer 2 VPN services than has been possible to date.

From a deployment perspective, EVPN offers service providers three customer connectivity options for delivering rich service interfaces to their clients: VLAN based, VLAN Aware Bundle and VLAN Bundle. These service interfaces are consistent with Metro Ethernet Forum-defined services and offer easy migration of these services onto new EVPN infrastructure for even richer service interfaces.

More importantly, EVPN addresses the shortcomings of VPLS and other Layer 2 services. These shortcomings, and how EVPN resolves them, are highlighted below.

7 Improved Network Efficiency

VPLS and other Layer 2 VPN services rely on learning MAC addresses in the data plane at every PE device in a packet's path. VPLS emulates the broadcast domain of a LAN over MPLS infrastructure. Consequently, broadcast MACs are always flooded, e.g. ARP/ND, and all participating ingress PE routers make separate copies of each broadcast or multicast packet to send to all other PE routers that are part of the same extended VPLS-based LAN.

In a large Layer 2 VPN, for example, replication overhead can be significant for each ingress router and its attached core-facing links. Service providers and enterprises need interconnect technologies that minimize the flooding of multi-destination frames.

EVPN is similar to IP VPNs and uses MP-BGP in the control plane to advertise MAC and IP reachability information. For example, PEs use MP-BGP to advertise the MAC addresses learned from their connected CEs, along with an MPLS label, to other PEs. Essentially, remote PE routers don't need to learn MACs in the data plane because the EVPN control plane supplies that information. As a result, EVPN greatly reduces flooding in the network with unknown unicast traffic, provides greater control over the MAC learning process, and gives operators the ability to apply policies, such as restricting who learns what. Additionally, since MAC routes include MAC address and their IP bindings, ARP/ND flooding is also minimized as PEs can locally support proxy-ARP/ND for remote hosts.

And by making use of IP VPN-like forwarding, based on MAC routes, the PEs do not need to maintain point-to-point pseudo wires between all PEs in the network core. Moreover, EVPN supports the concept of aliasing, which allows a PE to advertise a MAC route associating it to an Ethernet Segment. This allows a remote PE to load balance traffic among all the PEs connecting to that Ethernet Segment instead of forwarding just to the PE that advertised the MAC route, thus achieving better bandwidth utilization of the core network and edge links.

8 Integrated Layer 2/Layer 3 Functionality

Because VPWS and VPLS operate at Layer 2, they require Layer 3 gateway functionality to allow inter-subnet (inter VLAN) traffic. Even when the traffic is local—for example, when both the subnets (VLANs) are on the same PE—traffic must be routed via a Layer 3 gateway. Layer 3 gateway solutions typically require special configuration, which is an operational burden, and traffic flows aren't always optimal. On the other hand, a pure Layer 3 solution can create issues for intra-subnet traffic, such as not being able to extend the subnet across sites.

EVPN's integrated routing and bridging (IRB) functionality supports both Layer 2 and Layer 3 connectivity between edge nodes along with built-in Layer 3 gateway functionality. By adding both host and gateway MAC and IP address information in MAC routes as well as IPv4/IPv6 prefixes in IP-Prefix routes, EVPN provides optimum forwarding for both intra-subnet and inter-subnet within and across data centers for unicast as well as multicast traffic. This functionality is especially useful for service providers that offer Layer 2 VPN, Layer 3 VPN or direct Internet access services and want to extend all these services to provide cloud services to existing customers.

9 Resiliency and High Availability

Data volumes continue to escalate, which makes running the network in active/standby mode increasingly more expensive. It is critical for IT to maximize utilization of all links between data centers. That includes the ability to establish multi-homed connections, even between multiple PE routers, and to load balance across those connections. In addition to better link utilization, multi-homed connections also offer better resiliency and reliability against the potential failure of one connection or node.

Current L2VPN technologies only support single-active multi-homing and thus cannot use available physical bandwidth by load balancing among all connected local PEs. EVPN supports both single-active and all-active multi-homing for Layer 2 and Layer 3 traffic along with load balancing. With support for both all-active per-service and all-active per-flow multi-homing, EVPN enables optimal load balancing across peering PEs.

High availability (HA) is crucial for any network service, and is especially critical for data center interconnection where traffic volumes are very large. For availability, VPLS relies on the underlying MPLS capabilities such as Fast Reroute (FRR). While these MPLS FRR mechanisms aid in boosting network availability, Layer 2 shortcomings

pose their own challenges to HA. For example, the lack of all-active multi-homing in VPLS makes it difficult to achieve sub-50 milliseconds service restoration in the case of an edge node or edge link failure.

The rapid increase in virtualized applications has led to an increase in the volume of MACs that must be handled by the network. For large service providers and enterprises, there can be hundreds of thousands of MAC addresses supported across interconnected sites. If a node or link fails, need to relearn a high number of MACs in the broadcast domain can slow network re-convergence, which leads to data loss and in turn negatively affects application performance.

To ensure rapid recovery after a failure, enterprises and service providers need all-active multi-homing. Network re-convergence must also be independent of the number of MAC addresses learned by the PE. EVPN support for all-active multi-homing is a key HA enhancement.

In addition, EVPN defines a mechanism to efficiently and quickly signal remote PEs with the need to update their forwarding tables when a connectivity failure occurs. Withdrawal of the Ethernet Segment (ES) route allows for the mass withdrawal of MAC addresses whose reachability has been affected due to loss of that particular link.

10 Reducing the Provisioning Pain

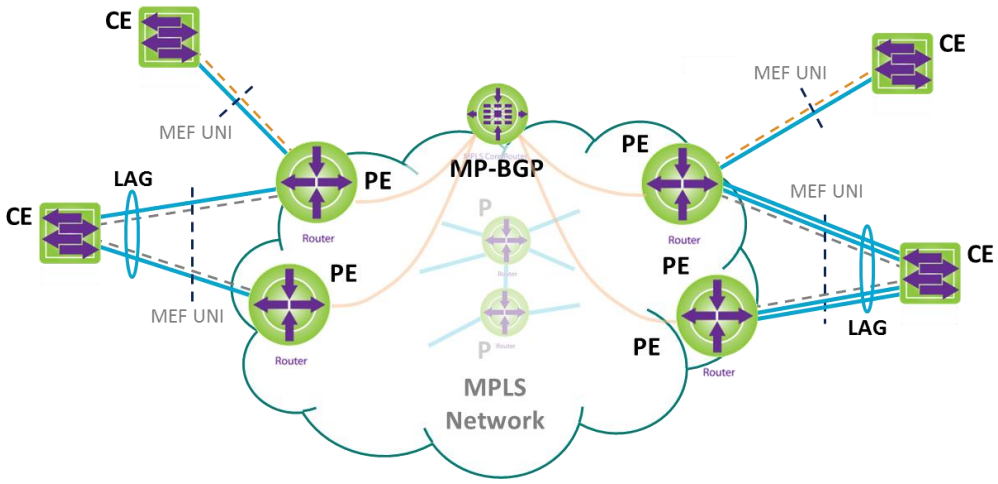
Although VPLS supports BGP-based auto-discovery, provisioning VPLS still requires that network operators specify various network parameters on top of the access-side Ethernet configuration. This provisioning overhead adds to operational expenses. In addition, VPLS has no provision for administrative control over MAC distribution, which limits an operator's ability to maximize MAC address operational efficiency.

EVPN's support for BGP-based policies gives operators better administrative control, including fine-grained, policy-driven control on route advertisement and consistent policy-based forwarding for Layer 2 traffic. EVPN's IP VPN-like policy control also allows for more efficient, feature-rich E-LAN and E-Line services and enhanced, customized services for end users. Additionally, by providing a single technology for both Layer 2 and Layer 3 VPNs, EVPN simplifies deployment and can seamlessly interoperate with Layer 2 VPNs and IP VPNs.

All of the characteristics mentioned above ideally suit EVPN technology for data center interconnection, Layer 2 VPNs, and integrated Layer 2/Layer 3 VPN applications.

11 Next Generation E-LINE/ E-LAN /E-TREE Use Case

E-Line, E-LAN, and E-Tree based on EVPN overcomes the shortcomings of current offerings of these services by providing integrated Layer 2/Layer 3 connectivity, native support for multi-homing, and network resiliency between edge nodes. EVPN builds on widely deployed BGP VPLS and IP-VPNs technologies, protecting investments in MPLS infrastructure, as well as the existing knowledge base.



EVPN Properties	Benefit for Next-Generation L2VPN Use Case
Support for all active multi-homing	All-active support allows operators to efficiently use all links at the same time.
Rich policy-based services	EVPN's support for BGP-based policies gives operators better administrative control, including granular, policy-driven control on route advertisement and consistent policy-based forwarding for L2 traffic.
Integrated Layer 2 / Layer 3 services	Efficient integration of Layer 2 services with IP-VPN and internet services allows more connectivity options for applications. Different VLAN handoff options allow rich customizable services.
Common provisioning for all services	By providing a single, consistent technology for both Layer 2 and Layer 3 VPNs, EVPN simplifies deployment and can seamlessly interoperate with Layer 2 VPNs and IP VPNs.
High availability	Given enterprises' reliance on cloud based services, high availability at the network level has become table stakes for next-generation E-Line, E-LAN, and E-Tree services. Built in high availability protects them from traffic loss caused by link or node failure.

12 EVPN Business Bottom Line

For service providers and enterprises alike, EVPN's features and benefits translate directly to the bottom line:

Reduced Capex: EVPN allows fuller utilization of each CE-PE link to offer higher bandwidth as well as improved resiliency, thus reducing the need for standby connections. For example, all-active multi-homing and load balancing maximize bandwidth while features such as IRB and MAC learning help boost efficient utilization of network resources. By building on existing technologies, EVPN lets operators upgrade their current MPLS and VPLS infrastructure to the newer EVPN-based service infrastructure with as little as a simple software upgrade—completely protecting customers' capital investments and thereby reducing CapEx.

Lower OpEx: EVPN reduces operations overhead by making it possible to use a single control plane to support both Layer 3 and Layer 2 VPNs, simplifying deployment. In addition, EVPN's IRB functionality reduces configuration overhead and simplifies data center operations. Likewise, EVPN gives operators fine-grained, policy-driven administrative control for greater efficiency. Additionally, by building on existing IP VPN and BGP VPLS technologies, EVPN allows operators to utilize their knowledge base without having to retrain people on completely new technology. All these improvements and reuse options help reduce operators' operational expenditures.

Revenue-enhancing services and greater service flexibility: EVPN lets service providers offer feature-rich E-LAN, E-Line and E-Tree services and easily expand their service interfaces. For example, providers that already offer Layer 2 VPN/VPLS and Layer 3 VPN services over an IP/MPLS network can easily use EVPN's IRB feature to provide cloud, storage and other services. Customers benefit from the ability to get advanced services—including integrated Layer 2/Layer 3 services, sophisticated service topologies via BGP policies, multi-homing and load balancing—at cost lower than of VPLS and IP VPNs services offered separately.

Improved customer satisfaction: EVPN's HA features, such as link-level and node-level redundancy; ensure fast failover and convergence times so customers get uninterrupted access to applications and services. Likewise, EVPN lets operators ensure customer privacy; with EVPN, network operators can carefully control how network information is distributed and processed and isolate groups of devices, ensuring that the traffic sharing their network remains private.

13 Summary and Ongoing EVPN Work

By addressing the shortcoming of current Layer 2 VPN offerings and allowing flexible integration of Layer 3, EVPN provides a solid foundation to a growing number of data center interconnection, mobile infrastructure, IoT, private cloud, and other E-LINE/E-LAN/E-Tree use cases.

The published TR-350 addresses E-LAN, which is the most common service type provided by EVPN. E-LAN provides multipoint to multipoint connectivity to customers with multiple sites, such that all sites appear to be on the same local area network.

Ongoing EVPN related work in Broadband Forum includes Phase 2 of TR-350 to add E-Line service type. This service type embodies all characteristics of a point to point service.

Phase 2 of the architecture also includes the E-Tree service, which is of interest to both service providers as well as enterprise where a multicast like tree is needed for content distribution, e.g. IPTV.

Phase 2 of TR-350 will also address additional issues such as EVPN interoperation with existing L2VPN technologies.

Those interested in the ongoing work are encouraged to contact Broadband Forum at info@broadband-forum.org.

14 Acknowledgements

Editors: Rao Cherukuri, Juniper Networks; Greg Mirsky, Ericsson.
Contributors: Guiu Fabregas, Alcatel-Lucent; Sriganesh Kini, Ericsson; Disha Chopra, John E Drake, Sachin Natu, Juniper Networks
Routing and Transport Area Director: David Sinicrope, Ericsson

15 About the Broadband Forum

The Broadband Forum is the industry's defining body for LAN/WAN architecture design, implementation, management and certification testing for technologies, both existing and emerging, in the Broadband market. Our work encompasses best practices for global networks, enables new revenue-generating service and content delivery, establishes technology migration strategies, engineers' critical device, service & development management tools, in the home and business IP networking infrastructure. Broadband expertise is sourced from more than 150 manufacturers and service provider companies. The Forum has published over 200 globally adopted standards over the last 24 years. Activity levels driven by the emergence of ultra-fast connectivity, IoT, NFV and SDN and the new Broadband 20/20 initiative have seen contribution levels rise to more than 1200+ in the last 12 months. The Broadband Forum's free technical standards and white papers can be found at broadband-forum.org. Twitter @Broadband_Forum.

