less packet overheads, better customer isolation

forwarding information can be learned through the data plane, best approach when customer wants all the routing and policy governance under its management control, Usually, L2VPNs offer lower operational cost and higher compatibility than L3VPNs, as tunnelled L2VPNs are conceptually simpler than L3VPNs

L2 MPLS VPN – forwards based on the L2 address of the L2 PDU. The L2 PDU is encapsulated in the transport protocol (MP-LS). The VPN can provide point-to-point (AToM) or LAN type multipoint service (VPLS). Something to remember about these types of VPN is that L2 forwarding information is learned though the data plane (for VPLS), similar to standard switch MAC learning. The control plane does not get involved in distributing L2 forwarding information. This means traffic from unknown MAC addresses is initially flooded, until return traffic is received across the pseudowire and the destination MAC is learned. Point-to-point L2 VPNs don't need to learn MAC information as they just forward out of the other port/pseudowire (they only have two interfaces per device).

L3 MPLS VPN – forwards based on the L3 address of the L3 PDU. The L3 PDU is encapsulated in the transport protocol (MPLS). With MPLS VPN, MP-BGP is used to distribute L3 forwarding information between sites for routes within the VPN.

Layer-2 VPNs defined by L2VPN operate over pseudowires (PWs) as defined by the PWE3 WG or over IP or MPLS PSN tunnels. A L2VPN emulates a "native" service over a PSN that is adequately faithful to, but may not be entirely indistinguishable from the native service itself. Further, following in the "edge-to-edge" nature of the service, the L2VPN WG will not define any mechanisms which exert control over the underlying PSN. When necessary it may, however, recommend or require the use of existing PSN QoS and path control mechanisms between the PEs which provide the L2VPN connectivity.

Nowadays, L2VPNs like VPLS are becoming popular among service providers because they support multipoint communication and have robust security features. As an L2 solution, VPLS has a zero-hop delay at the core of the network. Therefore, VPLS can achieve lower latencies and better jitter performance than L3VPNS. Furthermore, VPLS also provides the ability to add new sites without the need to reconfigure service provider equipment or the local equipment at existing sites. For these reasons, VPLS networks are now becoming attractive in many enterprise applications such as DCI (Data Centre Interconnect), Voice over IP (VoIP) and videoconferencing services.

Virtual Private LAN Services (VPLS) is a shared packet switched network that provides multiple PW connections. VPLS delivers layer 2 services across a WAN that emulates an Ethernet LAN in all aspects. All sites connected through VPLS appear to be on the same LAN, irrespective of the locations of the sites. This network establishes a private connection, as only CE devices belonging to the same VPLS can participate in the connection. The functioning of VPLS is similar to that of a LAN. CE devices that are members of same VPLS instance can interact and communicate with each other, as if they were communicating over a LAN, using the Service Provider’s network.

Usually, L2VPNs offer lower operational cost and higher compatibility than L3VPNs, as tunnelled L2VPNs are conceptually simpler than L3VPNs [6]. The lower provisioning cost of VPLS can be attributed to its optimal resource utilization.

VPLS is an easy way of provisioning an L2VPN. Moreover, VPLS is preferred because of some of its features, like protocol independence and cost-effective operational properties [7] [8]. The primary motive behind VPLS is to connect companies that operate at a global scale as if they are networked on the same Local Area Network (LAN). VPLS offers multipoint-tomultipoint Ethernet connectivity over a Multi-Protocol Label Switching/ Internet Protocol (MPLS/ IP) network [9]. In other words, VPLS merges MPLS and IP technology with Ethernet components, which rectifies the issues of Ethernet technology. Initially, VPLS architecture was proposed as a flat architecture, which worked well for small to medium scale networks [9]. But for more extensive networks, flat architectures faced major scalability issues in both data and control planes because of the requirement of a full mesh of PWs. To resolve this issue, a Hierarchical VPLS (H-VPLS) architecture was proposed. The H-VPLS architecture provides a viable solution to the scalability issue by decreasing the number of PWs. Initially, MPLS was used to implement VPLS since it had issues like the discovery of neighbours, scalability, and security. Thereafter, two standard implementations were proposed: (i) Border Gateway Protocol (BGP) for auto-discovery and signaling [10], and (ii) Label Distribution Protocol (LDP) for signaling [11]. These two architectures provided automatic neighbour discovery and signaling solutions, but security remained one of the biggest bottlenecks for VPLS.

The introduction of SDN in VPLS is a recent evolution in this series of advancements [14], [15]. Software-Defined VPLS (SD-VPLS) offers improved tunnel management, enhanced security, and better scalability.

On the one hand, globalization requires networks to be more secure, scalable and agile. These requirements have led to the advent of SDN, which is a new paradigm that allows software networks [37]. On the other hand, VPLS is one of the leading technologies for connecting business enterprises. Thus the use of SDN in the realm of VPLS is expected to enhance the capabilities of VPLS. More specifically, SDN can be applied in VPLS to enhance security, scalability and make the network more programmable, which increases flexibility and agility. So, one of the recent technological advancements in the field of VPLS is SD-VPLS.

In this use case virtually separate paths were created to isolate the traffic flow between the end points. For this Virtual Private LAN Service (VPLS) was implemented in this Use case. The goal was to connect multiple end-points in an OpenFlow network, creating isolated L2 broadcast overlay networks. While legacy technologies require the manual configuration of multiple devices in the network, VPLS tries to make the process easier for network operators. Hosts that get connected together can send in either untagged or VLAN tagged traffic, using either the same or different VLAN IDs. Two different VPLS were created, first, blue VPLS connecting Host H1 with Server 1 and second, red VPLS connecting Host H2 with Server 2 as observed in following figure.

VPLS on IP network

L2VPN service

Chart

Description automatically generated

Chart

Description automatically generated

Chart

Description automatically generated

Chart

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Chart, line chart

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Xxxxxxxxxxx with h1,h2, s1 and s2

Chart, radar chart

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

A screenshot of a video game

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated