# VPLS VPNs

# From Wikipedia, the free encyclopedia

**Virtual Private LAN Service** (**VPLS**) is a way to provide [Ethernet](https://en.wikipedia.org/wiki/Ethernet)-based multipoint to multipoint communication over [IP](https://en.wikipedia.org/wiki/Internet_protocol_suite) or [MPLS](https://en.wikipedia.org/wiki/MPLS) networks. It allows geographically dispersed sites to share an Ethernet [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) by connecting sites through [pseudowires](https://en.wikipedia.org/wiki/Pseudowire" \o "Pseudowire). The term 'sites' includes multiplicities of both servers and clients. The technologies that can be used as pseudo-wire can be [Ethernet over MPLS](https://en.wikipedia.org/wiki/Carrier_Ethernet#Ethernet_over_MPLS), [L2TPv3](https://en.wikipedia.org/wiki/L2TPv3) or even [GRE](https://en.wikipedia.org/wiki/Generic_Routing_Encapsulation). There are two [IETF](https://en.wikipedia.org/wiki/IETF) standards track [RFCs](https://en.wikipedia.org/wiki/Request_for_Comments) ([RFC 4761](https://tools.ietf.org/html/rfc4761) and [RFC 4762](https://tools.ietf.org/html/rfc4762)) describing VPLS establishment.

VPLS is a [virtual private network](https://en.wikipedia.org/wiki/Virtual_private_network) (VPN) technology. In contrast to L2TPv3, which allows only [point-to-point](https://en.wikipedia.org/wiki/Point-to-point_(telecommunications)) layer 2 tunnels, VPLS allows any-to-any (multipoint) connectivity.

In a VPLS, the [local area network](https://en.wikipedia.org/wiki/Local_area_network) (LAN) at each site is extended to the edge of the provider network. The provider network then emulates a [switch](https://en.wikipedia.org/wiki/Network_switch) or [bridge](https://en.wikipedia.org/wiki/Network_bridge) to connect all of the customer LANs to create a single bridged LAN.

VPLS is designed for applications that require multipoint or broadcast access.

## Mesh establishment

Since VPLS emulates a LAN, full mesh connectivity is required. There are two methods for full mesh establishment for VPLS: using [Border Gateway Protocol](https://en.wikipedia.org/wiki/Border_Gateway_Protocol) (BGP) and using [Label Distribution Protocol](https://en.wikipedia.org/wiki/Label_Distribution_Protocol) (LDP). The "control plane" is the means by which [provider edge](https://en.wikipedia.org/wiki/PE_router) (PE) routers communicate for auto-discovery and signalling. [Auto-discovery](https://en.wikipedia.org/wiki/Virtual_Private_LAN_Service#PE_auto-discovery) refers to the process of finding other PE routers participating in the same VPN or VPLS. Signalling is the process of establishing pseudowires (PW). The PWs constitute the "data plane", whereby PEs send customer VPN/VPLS traffic to other PEs.

BGP provides both auto-discovery and signalling. The mechanisms used are very similar to those used in establishing Layer-3 MPLS [VPNs](https://en.wikipedia.org/wiki/VPN). Each PE is configured to participate in a given VPLS. The PE, through the use of BGP, simultaneously discovers all other PEs in the same VPLS, and establishes a full mesh of pseudowires to those PEs.

With LDP, each PE router must be configured to participate in a given VPLS, and, in addition, be given the addresses of other PEs participating in the same VPLS. A full mesh of LDP sessions is then established between these PEs. LDP is then used to create an equivalent mesh of PWs between those PEs.

An advantage to using PWs as the underlying technology for the data plane is that in the event of failure, traffic will automatically be routed along available backup paths in the service provider's network. Failover will be much faster than could be achieved with e.g. [Spanning Tree Protocol](https://en.wikipedia.org/wiki/Spanning_Tree_Protocol) (STP). VPLS is thus a more reliable solution for linking together Ethernet networks in different locations than simply connecting a [WAN](https://en.wikipedia.org/wiki/Wide_area_network) link to [Ethernet switches](https://en.wikipedia.org/wiki/Network_switch) in both locations.

VPLS has significant advantages for both service providers and customers. Service providers benefit because they can generate additional revenues by offering a new [Ethernet](https://en.wikipedia.org/wiki/Ethernet) service with flexible bandwidth and sophisticated service level agreements (SLAs). VPLS is also simpler and more cost effective to operate than a traditional service. Customers benefit because they can connect all of their sites to an [Ethernet](https://en.wikipedia.org/wiki/Ethernet) [VPN](https://en.wikipedia.org/wiki/VPN) that provides a secure, high speed and homogenous network. Moreover, VPLS provides a logical next step in the continuing evolution of Ethernet from a 10 Mbit/s shared LAN protocol to a multi-Gbps global service.

## Label stack

VPLS MPLS packets have a two-label stack. The outer label is used for normal MPLS forwarding in the service provider's network. If BGP is used to establish the VPLS, the inner label is allocated by a PE as part of a label block. If LDP is used, the inner label is a virtual circuit ID assigned by LDP when it first established a mesh between the participating PEs. Every PE keeps track of assigned inner label, and associates these with the VPLS instance.

## Ethernet emulation

PEs participating in a VPLS-based VPN must appear as an Ethernet bridge to connected [customer edge](https://en.wikipedia.org/wiki/Customer_edge) (CE) devices. Received Ethernet frames must be treated in such a way as to ensure CEs can be simple Ethernet devices.

When a PE receives a frame from a CE, it inspects the frame and learns the CE's MAC address, storing it locally along with LSP routing information. It then checks the frame's destination MAC address. If it is a broadcast frame, or the MAC address is not known to the PE, it floods the frame to all PEs in the mesh.

Ethernet does not have a [time to live](https://en.wikipedia.org/wiki/Time_to_live) (TTL) field in its frame header, so loop avoidance must be arranged by other means. In regular Ethernet deployments, Spanning Tree Protocol is used for this. In VPLS, loop avoidance is arranged by the following rule: A PE *never* forwards a frame received from a PE to another PE. The use of a full mesh combined with [split horizon](https://en.wikipedia.org/wiki/Split_horizon) forwarding guarantees a loop-free broadcast domain.

## Scalability

VPLS is typically used to link a large number of sites together. Therefore, Scalability is an important issue that needs addressing.

### Hierarchical VPLS

VPLS requires a full mesh in both the control and data planes; this can be difficult to scale. For BGP, the control plane scaling issue has long been addressed, through the use of [route reflectors](https://en.wikipedia.org/wiki/Route_reflector) (RRs). RRs are extensively used in the context of Internet routing, as well as for several types of VPNs. To scale the data plane for multicast and broadcast traffic, there is work in progress to use [point-to-multipoint](https://en.wikipedia.org/wiki/Point-to-multipoint) LSPs as the underlying transport.

For LDP, a method of subdividing a VPLS VPN into two or three tiered hierarchical networks was developed. Called **hierarchical VPLS** (**HVPLS**), it introduces a new type of MPLS device: the **multi-tenant unit** (**MTU**) switch. This switch aggregates multiple customers into a single PE, which in turn needs only one control and data plane connection into the mesh. This can significantly reduce the number of LDP sessions and LSPs, and thus unburden the core network, by concentrating customers in edge devices.

HVPLS (LDP) may also be used to join two VPLS mesh structures together. Without using HVPLS, every node in each VPLS mesh must become meshed with all nodes in the other VPLS mesh. However, with HVPLS, the two meshes can essentially be joined together at certain locations. Techniques such as redundant pseudowires can provide resiliency in case of failures at the interconnection points.

### MAC addresses

Since VPLS links multiple Ethernet broadcast domains together, it effectively creates a much larger broadcast domain. Since every PE must keep track of all [MAC addresses](https://en.wikipedia.org/wiki/MAC_address) and associated LSP routing information, this can potentially result in a large amount of memory being needed in every PE in the mesh.

To counter this problem, sites may use a router as the [CE](https://en.wikipedia.org/wiki/Customer_Edge) device. This hides all MAC addresses on that site behind the CE's MAC address.

PE devices may also be equipped with [content-addressable memory](https://en.wikipedia.org/wiki/Content-addressable_memory) (CAM), similar to high-end Ethernet switches.

An alternative mechanism is using MAT (MAC Address Translation).[[1]](https://en.wikipedia.org/wiki/Virtual_Private_LAN_Service#cite_note-1) However, at the time of writing this, there aren't vendors providing MAT functionality.

### PE auto-discovery

In a VPLS-based VPN with a large number of sites, manually configuring every participating PE does not scale well. If a new PE is taken into service, every existing PE needs to have its configuration adjusted to establish an LDP session with the new PE. Standardisation work is in progress to enable auto-discovery of participating PEs. Three implementations are being worked on:

### LDP

The LDP method of PE auto-discovery is based on that used by the Label Distribution Protocol to distribute labels across P and PE routers within a single autonomous system.

### BGP

The BGP method of PE auto-discovery is based on that used by [Layer-3 MPLS VPNs](https://en.wikipedia.org/w/index.php?title=Layer-3_MPLS_VPN&action=edit&redlink=1) to distribute VPN routes among PEs participating in a VPN. The BGP4 Multi-Protocol (BGP-MP) extensions are used to distribute VPN IDs and VPN-specific reachability information. Since IBGP requires either a full mesh of BGP sessions or the use of a route reflector, enabling the VPN ID in a participating PEs existing BGP configuration provides it with a list of all PEs in that VPN. Note that this method is for auto-discovery alone; LDP is still used for signalling. The method of establishing VPLS with BGP described above accomplishes both auto-discovery and signalling.

### RADIUS

This method requires ALL PEs to be configured with one or more [RADIUS](https://en.wikipedia.org/wiki/RADIUS) servers to use. When the first CE router in a particular VPLS VPN connects to the PE, it uses the CE's identification to request authentication from the RADIUS server. This identification may be provided by the CE or may be configured into the PE for that particular CE. In addition to a username and password, the identification string also contains a VPN name and an optional provider name.

The RADIUS server keeps track of all PEs that requested authentication for a particular VPN and returns a list of them to the PE requesting authentication. The PE then establishes LDP sessions to every PE in the list.

## VPLS Configuration

Below is sample of VPLS configuration.

Here goes VPLS config

Here goes VPLS config

Here goes VPLS config

Configuration VPLS Configuration