

PPVPN Working Group

Internet-Draft

Expiration Date: 21 Aug, 2002

Loa Andersson
Tove Madsen
Utfors AB

21 February, 2002

PPVPN Terminology
<[draft-andersson-ppvnp-terminology-00.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at:
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at:
<http://www.ietf.org/shadow.html>.

Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

The provider provisioned VPN solutions has attracted a great deal of interest. Memos proposing different and overlapping solution have been discussed on the PPVPN mailing list and in the Working Group meetings. This has lead to a development of a partly new set of concepts used to

INTERNET-DRAFT

[draft-andersson-ppvnp-terminolgy-00.txt](#)

21.02.02

Andersson

Expires Aug 2002

[Page 2]

describe the set of VPN services. To a certain extent there are more than one term covering the same concept and sometimes the same term covers more than one concept. The terminology needs to be made clearer and more intuitive. This document seeks to fill at least part of the need.

Contents

| | | |
|--------------|--|-----------|
| <u>1.</u> | Introduction..... | <u>3</u> |
| <u>2.</u> | Terminology..... | <u>4</u> |
| <u>3.</u> | Virtual Private services..... | <u>4</u> |
| <u>3.1</u> | Virtual Private Network (VPN)..... | <u>4</u> |
| <u>3.2</u> | Layer 2 VPN (L2VPN)..... | <u>5</u> |
| <u>3.3</u> | Virtual Leased Line Service (VLLS)..... | <u>5</u> |
| <u>3.4</u> | Layer 3 VPN..... | <u>5</u> |
| <u>3.5</u> | Pseudo Wire (PW)..... | <u>5</u> |
| <u>3.6</u> | Virtual Private LAN Service (VPLS)..... | <u>5</u> |
| <u>3.7</u> | Virtual Private Switched Network (VPSN)..... | <u>6</u> |
| <u>3.8</u> | Virtual LAN (VLAN)..... | <u>6</u> |
| <u>3.9</u> | Transparent LAN Service (TLS)..... | <u>6</u> |
| <u>4.</u> | Building blocks..... | <u>6</u> |
| <u>4.1</u> | Customer Edge device (CE)..... | <u>6</u> |
| <u>4.1.1</u> | Device based CE naming..... | <u>7</u> |
| <u>4.1.2</u> | Service based CE naming..... | <u>7</u> |
| <u>4.2</u> | Provider Edge (PE)..... | <u>8</u> |
| <u>4.2.1</u> | Device based PE naming..... | <u>8</u> |
| <u>4.2.2</u> | Service based PE naming..... | <u>8</u> |
| <u>4.2.3</u> | Distribution based PE naming..... | <u>9</u> |
| <u>4.2.4</u> | Examples of PE naming..... | <u>9</u> |
| <u>4.3</u> | Core..... | <u>10</u> |
| <u>4.3.1</u> | Provider router (P)..... | <u>10</u> |
| <u>5.</u> | Functions..... | <u>10</u> |
| <u>5.1</u> | Endpoint discovery..... | <u>10</u> |
| <u>5.2</u> | Flooding..... | <u>10</u> |
| <u>5.3</u> | MAC address learning..... | <u>10</u> |
| <u>5.3.1</u> | Qualified learning..... | <u>11</u> |
| <u>5.3.2</u> | Unqualified learning..... | <u>11</u> |
| <u>5.4</u> | Signalling..... | <u>11</u> |
| <u>6.</u> | "Boxes"..... | <u>11</u> |
| <u>6.1</u> | Aggregation box..... | <u>11</u> |
| <u>6.2</u> | Customer Premises Equipment (CPE)..... | <u>11</u> |
| <u>6.3</u> | Multi Tenant Unit (MTU)..... | <u>11</u> |
| <u>7.</u> | Packet Switched Network (PSN)..... | <u>12</u> |

| | | |
|---------------------|--|--------------------|
| 7.1 | Route Distinguisher (RD)..... | 12 |
| 7.2 | Route Target (RT)..... | 12 |
| 7.3 | Tunnel..... | 12 |
| 7.4 | Tunnel multiplexor..... | 12 |
| 7.5 | VC label..... | 13 |
| 7.6 | Inner label..... | 13 |
| 7.7 | Virtual Channel (VC)..... | 13 |
| 7.8 | VPN Routing and Forwarding (VRF)..... | 13 |
| 7.9 | Virtual Forwarding Instance (VFI)..... | 13 |
| 8. | Acknowledgements..... | 13 |

[1.](#) Introduction

There are a comparatively large number of memos being submitted to the PPVPN and PWE3 working groups that all addresses the same problem space, provider provisioned virtual private networking for end customer. The memos address a wide range of services, but there is a great deal of commonality among the proposed solutions.

This has lead to a development of a partly new set of concepts used to describe this set of VPN services. To a certain extent there are more than one term covering the same concept and sometimes the same term covers more than one concept. The terminology needs to be made clearer and more intuitive.

This document seeks to fill at least part of the need and proposes a foundation for a unified terminology for the PPVPN working group; in some cases the parallel concepts within the PWE3 working groups is used as references.

[2.](#) Summary for Sub-IP Area

[2.1](#) Summary

This draft outlines a terminology that is possible to apply across all the WG documents processed by PPVPN WG. It addresses the key concepts valid for both L2 and L3 VPNs.

2.2 Where does it fit in the Picture of the Sub-IP Work

This work fits squarely in the PPVPN box.

[2.3](#) 3.3. Why is it Targeted at this WG

The WG is chartered with developing L2 and L3 VPNS. This draft specifies a terminology for that area.

[2.4](#) Justification

The WG should consider this document as it creates a starting point for a WG terminology that will help to create a coherent view of all the PPVPN specifications.

[3.](#) PPVPN Terminology

The concepts and terms in this list are gathered from Internet Drafts sent to the PPVPN mailing list. The focus is on terminology and concepts that are specific to the PPVPN area, but this is not strictly enforced, e.g. there are concepts and terms within the PWE3 and MPLS areas that are closely related. We've tried to find the earliest use of terms and concepts in Internet Drafts sent to the PPVPN working group.

The document is structured in four major sections. [Section 4](#) lists the different services that has been/will be specified, [Section 5](#) lists the building blocks that is used to specify those services, [section 6](#) lists the functions needed in those services and [section 7](#) list some typical devices used in customer and provider networks.

[4.](#) Provider Provisioned Virtual Private Network services

In this section we define the terminology that relates the set of service to solutions specified by the PPVPN working group. The concept "pseudo wire" that belongs to the PWE3 working group is included for reference purposes. For requirements for provider provisioned VPNs see [\[15\]](#).

[4.1](#) Virtual Private Network (VPN)

VPN is a generic term that covers the use of a public or private network to create groups of users that is separated from other network users and may communicate among them as if they were on a private network. The level of separation is possible to enhance e.g. by end-to-end

encryption, this is however outside the scope of PPVPN working group charter. For further discussions on IP based VPNs see [7].

In this document "VPN" is also used as a generic name for all services listed in [section 4](#).

[4.2](#) Layer 2 VPN (L2VPN)

See Virtual Private Wire ([section 4.3](#)).

[4.3](#) Virtual Private Wire (VPW)

A Virtual Private Wire (VPW) service is a point-to-point circuit (link) connecting two Customer Edge devices (see [section 5.1](#)). The link layer used to connect the CE devices to the provider network can be any link layer type, e.g. an ATM VCC, a Frame Relay circuit or Ethernet. The CE devices can be routers, bridges, switches or hosts. In some implementations a set of VPWs is used to create a multi-site L2VPN network. An example of a VPW solution is described in[2].

A VPW differs from a VPLS ([section 4.6](#)) in that the VPLS is multipoint to multipoint.

[4.4](#) Layer 3 VPN

A L3VPN is solutions, that interconnects several sets of hosts and routers and allows them to communicate based on L3 addresses, see [11].

[4.5](#) Pseudo Wire (PW)

The PWE3 working group within IETF specifies the pseudo wire technology. A pseudo wire is an emulated point-to-point connectivity over a packet switched network that gives the possibility to interconnect two nodes with any L2 technology. The PW shares some of the building blocks and architecture constructs with the point to multipoint solutions, e.g. PE and CE. An early solution for PWs is described in [5]. Encapsulation formats readily used in VLLS, VPLS and PWs is described in [6].

[4.6](#) Virtual Private LAN Service (VPLS)

A VPLS is a provider service that emulates the full functionality of a traditional Local Area Network. A VPLS makes it possible to interconnect several LAN segments over a packet switched network (PSN) and makes the remote LAN segments behave as one single LAN. For early work on defining a solution and protocol for a VPLS see [4], [12] and .

In a VPLS the provider network emulates a learning bridge and forwarding decision are taken based on MAC addresses or MAC addresses and VLAN tag.

[4.7](#) Virtual Private Switched Network (VPSN)

A VPSN is the same as a VPLS.

[4.8](#) Virtual LAN (VLAN)

A VLAN is a way of separating traffic on a LAN, e.g. between different departments within a company. IEEE 802.1Q defines how to mark an Ethernet frame with a tag that may be used to create user groups on a LAN.

[4.9](#) Transparent LAN Service (TLS)

A TLS is the same as a VPLS.

[5.](#) Building blocks

Starting with specifications of L3VPNs, e.g. the 2547 specification [[9](#)] and [[10](#)] and Virtual Routers [[13](#)], a way of describing the building blocks and allocation of functions in VPN solutions was developed. In this section we generalize these concepts to a set of concepts that is valid for all the specifications developed by the PPVPN WG. The building blocks are often in day-to-day talk treated as if it were a single physical box, common for all services. However, for different reasons this is to over-simplify. Any of the building blocks could be implemented across more than one physical box. How common the use of such implementations will be is beyond the scope of this document.

[5.1](#) Customer Edge device (CE)

A CE is the name of the device with the functionality needed on the customer premises to access the services specified by the PPVPN working group.

There are two different aspects that need to be considered in naming CE devices. One could start with the type of device that is used to implement the CE (see [section 4.1.1](#)). It is also possible to use the service the CE is used to implement and come up with a set of prefixed CEs, (see [section 4.1.2](#)).

It is common practice to use "CE" to indicate any of these boxes, since it is very often unambiguous in the specific context.

5.1.1 Device based CE naming

[5.1.1.1 Customer Edge Router \(CE-R\)](#)

A CE-R is a router in the customer network interfacing the provider network. There are many reasons to use a router in the customer network, e.g. in a L3VPN using private IP addressing this is the router that is able to do forwarding based on the private addresses. Another reason to require the use of a CE-R on the customer side is that one want to limit the number on MAC-addresses that needs to be learnt in the provider network.

A CE-R could be used to access both L2 and L3 services.

[5.1.1.2 Customer Edge Switch \(CE-S\)](#)

A CE-S is a service aware L2 switch in the customer network interfacing the provider network. In a VLLS or a VPLS it is not strictly necessary to use a router in the customer network, a layer 2 switch might very well do the job.

[5.1.2 Service based CE naming](#)

The list below is just examples and it will be extended as the number of services increases.

[5.1.2.1 L3VPN-CE](#)

An L3VPN-CE is the device or set of devices on the customer premises that attaches to a provider provisioned L3VPN, e.g. a 2547bis implementation.

[5.1.2.2 VLLS-CE](#)

A VLLS-CE is the device or set of devices on the customer premises that attaches to a provider provisioned vlls.

[5.1.2.3 VPLS-CE](#)

A VPLS-CE is the device or set of devices on the customer premises that attaches to a provider provisioned vpls.

5.2 Provider Edge (PE)

A PE is the name of the device or set of devices at the edge of the provider network with the functionality that is needed to interface the customer. PE, without further qualifications, is very often used for naming the devices since it is made unambiguous by the context.

In naming PEs there are three aspects that we need to consider, the service they support, whether the functionality needed for service is distributed across more than one device and the type of device they are build on.

[5.2.1](#) Device based PE naming

Both routers and switches may be used to implement PEs, however the scaling properties will be radically different depending which type of equipment that is chosen.

[5.2.1.1](#) Provider Edge Router (PE-R)

A PE-R is a L3 device that participates in the PSN (see [section 8](#)) routing and forwards packets based on the routing information.

[5.2.1.2](#) Provider Edge Switch (PE-S)

A PE-S is a L2 device that participates in e.g. a switched Ethernet taking forwarding decision packets based on L2 address information.

[5.2.2](#) Service based PE naming

[5.2.2.1](#) L3VPN-PE

An L3VPN-PE is a device or set of devices at the edge of the provider network interfacing the customer network, with the functionality needed for a L3VPN.

[5.2.2.2](#) VPW-PE

A VPW-PE is a device or set of devices at the edge of the provider network interfacing the customer network, with the functionality needed for a VPW service.

5.2.2.3 VPLS-PE

A VPLS-PE is a device or set of devices at the edge of the provider network interfacing the customer network, with the functionality needed for a VPLS.

[5.2.3](#) Distribution based PE naming

For scaling reasons it is in the VPLS case sometimes desired to distribute the functions in a VPLS-PE across more than one device, e.g. is it feasible to allocate MAC address learning on a comparatively small and in-expensive device close to the customer site, while participation in the PSN signalling and set up of PE to PE tunnels are done by routers closer to the network core.

When distributing functionality across devices a protocol is needed to exchange information between the Control PE (see [section 5.2.3.1](#)) and the Forwarding PE (see [section 5.2.3.2](#)).

[5.2.3.1](#) Control PE

The Control PE is the device to which the signalling and control functions are allocated when a VPLS-PE is distributed across more than one box.

[5.2.3.2](#) Forwarding PE

The forwarding PE is the device to which the functions needed to take forwarding or switching decision at the ingress of the provider network.

[5.2.4](#) Examples of PE naming

[5.2.4.1](#) Layer 2 PE (L2PE)

L2PE is the joint name of the devices in the provider network that implement L2 functions needed for a VPLS or a VLLS.

[5.2.4.2](#) Logical PE (LPE)

The term Logical PE (LPE) originates from [8] and is used to describe a set of devices used in a provider network to implement a VPLS. In a LPE VPLS functions are distributed across small devices (PE-Edges/Forwarding PE) and devices attached to a network core (PE-Core/Control PE). In an LPE solution the PE-edge and PE-Core can be interconnected by a switched

Ethernet transport network(s) or uplinks. The LPE will appear to the core network as single PE. In this document the devices that constitutes the LPE is called Control PE and Forwarding PE.

[5.2.4.3 VPLS Edge \(VE\)](#)

The term VE originates from [1] and is used to describe the device used by a provider network to hand off a VPLS to a customer. In this document the VE is called a Forwarding PE.

[5.3 Core](#)

[5.3.1 Provider router \(P\)](#)

The P is defined as a router in the core network that does not have interfaces directly towards a customer. Hence a P router does not need to keep VPN state and is VPN un-aware.

[6. Functions](#)

In this section we have grouped a number of concepts and terms that has to be performed to make the VPN services work.

[6.1 Endpoint discovery](#)

Endpoint discovery is the process by which the devices that are aware of a specific VPN service will find all customer facing ports that belong to the same service.

The requirements on endpoint discovery and signalling are discussed in [3].

[6.2 Flooding](#)

Flooding is a function related to L2 services; when a PE receives a frame with an unknown destination MAC-address, that frame is send out over (flooded) every other interface.

[6.3 MAC address learning](#)

MAC address learning is a function related to L2 services; when PE receives a frame with an unknown source MAC-address the relationship between that MAC-address and interface is learnt for future forwarding purposes.

6.3.1 Qualified learning

In qualified learning, the learning decisions at the Forwarding PE is based on the customer Ethernet frame's MAC address and VLAN tag, if a VLAN tag exists. If no VLAN tag exists, the default VLAN is assumed.

[6.3.2 Unqualified learning](#)

In unqualified learning, learning is based on a customer Ethernet frame's MAC address only.

[6.4 Signalling](#)

Signalling is the process by which the PEs that have VPNs behind them exchange information to set up PSN tunnels and tunnel multiplexors. This process might be automated through a protocol or the done by manual configuration. Different protocols may be used to establish the PSN tunnels and exchange the tunnel multiplexors.

[7. "Boxes"](#)

We list a set of boxes that will typically be used in an environment that supports different kinds of VPN services.

[7.1 Aggregation box](#)

The aggregation box is typically an L2 switch that is service un-aware and is used only to aggregate traffic to more function rich points in the network.

[7.2 Customer Premises Equipment \(CPE\)](#)

The CPE equipment is the box that a provider places with the customer. It serves two purposes ; giving the customer ports to plug in to and making it possible for a provider to monitor the connectivity to the customer site. The CPE is typically a low cost box with limited functionality and in most cases not aware of the VPN services offered by the provider network.

[7.3 Multi Tenant Unit \(MTU\)](#)

An MTU is typically an L2 switch placed by a service provider in a building where customers of that service provider are located.

8. Packet Switched Network (PSN)

A PSN is the network through which the tunnels supporting the VPN services are set up.

[8.1](#) Route Distinguisher (RD)

A Route Distinguisher is an 8-byte value that together with a 4 byte IPv4 address identifies a VPN-IPv4 address family. If two VPNs use the same IPv4 address prefix, the PEs translates these into unique VPN-IPv4 address prefixes. This ensures that if the same address is used in two different VPNs, it is possible to install two completely different routes to that address, one for each VPN.

[8.2](#) Route Target (RT)

A Route Target attribute can be thought of as identifying a set of sites, or more precisely a set of VRFs (see [section 8.8](#)). Associating a particular Route Target with a route allows that route to be placed in all VRFs that are used for routing traffic received from the corresponding sites.

A Route Target attribute is a BGP extended community used in [\[9\]](#) and [\[14\]](#). A Route Target community is used to constrain VPN information distribution to the set of VRFs. A route-target can be perceived as identifying a set of sites, or more precisely a set of VRFs (see [section 8.8](#)).

[8.3](#) Tunnel

A tunnel is connectivity through a PSN that is used to send traffic across the network from one PE to another. The tunnel provides separation of traffic belonging to one customer from traffic belonging to another. How the tunnel is established depends on the tunnelling mechanisms provided by the PSN, i.e. the tunnel could be based on the IP-header or an MPLS label.

[8.4](#) Tunnel multiplexor

A tunnel multiplexor is an entity that is sent with the packets traversing the tunnel to make possible to decide to which instance of a service a packet belongs and from which sender it was received. In [\[2\]](#) the tunnel multiplexor is formatted as an MPLS label.

8.5 VC label

In an MPLS enabled IP network a VC label is an MPLS label, used to identify traffic within a tunnel that belongs to a particular VPN, i.e. the VC label is the tunnel multiplexor in networks that uses MPLS labels.

8.6 Inner label

See VC label [section 8.5](#).

8.7 Virtual Channel (VC)

A VC is transported within a tunnel and identified by its tunnel multiplexor. A virtual channel is identified by a VCI (Virtual Channel Identifier). In the PPVPN context a VCI is a VC label or tunnel multiplexor and in the Martini case it is equal to the VCID.

8.8 VPN Routing and Forwarding (VRF)

In networks running 2547 VPN's [\[9\]](#) PE routers maintain VRF's. A VRF is a per-site forwarding table. Every site to which the PE router is attached is associated with one of these tables. A particular packet's IP destination address is looked up in a particular VRF only if that packet has arrived directly from a site, which is associated with that table.

8.9 Virtual Forwarding Instance (VFI)

A VFI is a virtual layer 2 forwarding instance that serves one single VPLS. Forwarding done by a VFI is based on MAC addresses and VLAN tags, and possibly other relevant information on a per VPLS basis. The VFI is allocated to VPLS-PE or in the distributed case to the forwarding PE.

8.10 Virtual Router (VR)

A Virtual Router (VR) is software and hardware based emulation of a physical router. Virtual routers have independent IP routing and forwarding tables and they are isolated from each other, see [\[13\]](#).

9. Acknowledgements

Much of the content in this document is based on discussion in the PPVPN design teams for "auto discovery" and "l2vpn".

Authors' Contact

Loa Andersson
Utfors AB
Rönsundavägen 12, PO Box 525
SE-169 29 Solna, Sweden
phone: +46 8 5270 5038
loa.andersson@utfors.se

Tove Madsen
Utfors AB
Rönsundavägen 12, PO Box 525
SE-169 29 Solna Sweden
phone: +46 8 5270 5040
tove.madsen@utfors.se

References

- [1] Kompella, K et.al "[draft-kompella-ppvpn-dtls-01.txt](#)" Work in progress, Internet Draft, November 2001.
- [2] Kompella, K et.al "MPLS-based Layer 2 VPNs" [draft-kompella-ppvpn-l2vpn-01.txt](#), Work in Progress, November 2001.
- [3] Squire, M "[draft-squire-ppvpn-vpn-discovery-reqts-00.txt](#)" VPN Discovery Discussions and Options, Work in Progress, November 2001.
- [4] Kompella, V, Lasserre, M et.al. "Transparent VLAN Services over MPLS" [draft-lassere-vkompella-ppvpn-tls-02.txt](#), Work in progress, November 2001.
- [5] Martini, L, et.al "[draft-martini-l2circuit-trans-mpls-05.txt](#)", Work in progress, Internet Draft, February 2001.
- [6] Martini, L et.al "[draft-martini-l2circuit-encap-mpls-01.txt](#)", Work in Progress, Internet Draft, February 2001.
- [7] Gleeson, B et.al. "A Framework for IP Based Virtual Private Networks" [rfc 2764](#), February 2000.
- [8] Ould-Brahim, H et.al "VPLS/LPE L2VPNs: Virtual Private LAN Services using Logical PE Architecture" [draft-ouldbrahim-l2vpn-lpe-01.txt](#), Work in Progress, Internet Draft, November 2001.
- [9] Rosen, E et.al. "BGP/MPLS VPNs", [rfc2547](#), March 1999.

INTERNET-DRAFT

[draft-andersson-ppvpn-terminology-00.txt](#)

21.02.

- [10] Rosen, E et.al. "BGP/MPLS VPNs", [draft-ietf-ppvpn-rfc2547bis-01.txt](#), Work in Progress, Internet Draft, January 2002.
- [11] Callon, R., et al., "A Framework for Provider Provisioned Virtual Private Networks", [draft-ietf-ppvpn-framework-04.txt](#), Work in Progress, Internet Draft. July 2001.
- [12] Augustyn, W., et.al., "Requirements for Virtual Private LAN Services (VPLS)", [draft-augustyn-vpls-requirements-01.txt](#), Work in Progress, Internet Draft, February 2002.
- [13] Ould-Brahim H., et al., "Network-based IP VPN using Virtual Routers", [draft-ietf-ppvpn-vr-00.txt](#), Work in Progress, Internet Draft, July 2001.
- [14] Ould-Brahim H, et al., "Using BGP as an auto-discovery mechanisms for network-based VPNs", [draft-ietf-ppvpn-bgpvpn-auto-02.txt](#), Work in Progress, Internet Draft, January 2002.
- [15] Carugi, M., et al., "Service requirements for Provider Provisioned Virtual Private Networks", <[draft-ietf-ppvpn-requirements-03.txt](#)>, Work in Progress, Internet Draft, December 2001.

This document expires on 21 Aug, 2002.