Virtual Private Network: Layer 2 Solution

Giorgio Sadolfo
giorgiosadolfo@fastwebnet.it
What is virtual private network?

• A virtual private network (VPN) allows the provisioning of private network services for an organization or organizations over a public or shared infrastructure such as the Internet or service provider backbone network (Cisco).
Virtual Private Network: An Overview

Virtual Private Networks (VPNs)

Provider Provisioned VPNs (PPVPNs)

Site-to-Site

Layer 1 VPNs (L1VPN) - GMPLS

- Point-to-Point (P2P) (VPWS) (F: VLLS)

Layer 2 VPNs (L2VPN)

- Multipoint-to-Multipoint (M2M)

Layer 3 VPNs (L3VPN)

- Compulsory Tunnel Mode / NAS-Initiated
- Voluntary Tunnel Mode / Client-Initiated

Remote Access

Layer 3 VPNs (L3VPN)

- L2F
- PPTP
- L2TPv2/v3
- PE-Based
  - BGP/MPLS RFC4364/2547bis Style
  - Virtual Router (VR) Based

Customer Provisioned VPNs

Remote Access

Site-to-Site

- IPsec
- GRE
- IP-in-IP

IPsec
- L2TPv3
- GRE
- IP-in-IP

PPTP
- L2TPv2/v3
- IPsec
- SSL/TLS

CE-Based

TDP/LDP/RSVP Signalled LSPs

- IPsec
- L2TPv3
- GRE
- IP-in-IP

Draft Martini (AToM) L2 Transport Based
Type of virtual private network

- **SITE to SITE**: Site-to-site VPNs provide an Internet-based WAN infrastructure to extend network resources to branch offices, home offices, and business partner sites.
  - Reliable and high-quality transport of complex, mission-critical traffic, such as voice and client server applications
  - Simplified provisioning and reduced operational tasks for network designs
  - Integrated advanced network intelligence and routing for a wide range of network designs
**Type of virtual private network**

- **REMOTE ACCESS**: Remote access VPNs extend almost any data, voice, or video application to the remote desktop, emulating the main office desktop. With this VPN, you can provide highly secure, customizable remote access to anyone, anytime, anywhere, with almost any device.

  - Create a remote user experience that emulates working on the main office desktop
  - Deliver VPN access safely and easily to a wide range of users and devices
  - Support a wide range of connectivity options, endpoints, and platforms to meet your dynamic remote access needs
VPN Layer 2: Overview

- **Layer 2 site-to-site VPNs** (L2VPN) can be provisioned between switches, hosts, and routers and allow data link layer connectivity between separate sites.
- Communication between customer switches, hosts, and routers is based on Layer 2 addressing, and PE devices perform forwarding of customer data traffic based on incoming link and Layer 2 header information:
  - MAC address;
  - Frame Relay;
  - Data Link Connection Identifier [DLCI];
  - and so on.
There are two categories of provider provisioned L2VPN:

- **Point-to-point (P2P) circuit-based VPNs** also known as Virtual Private Wire Service (VPWS) VPNs and are constructed using, for example, Draft Martini (MPLS) or L2TPv3 pseudowires (emulated circuits).
Layer 2 VPN

There are two categories of provider provisioned L2VPN:

- **Multipoint-to-multipoint (M2M) VPNs** M2M VPNs come in two varieties:
  - Virtual Private LAN Service (VPLS) VPNs
  - IP-Only LAN Service (IPLS) VPNs
Virtual Private LAN Service: VPLS

Virtual private LAN service (VPLS) is a way to provide Ethernet based multipoint to multipoint communication over IP/MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudo-wires. (Wikipedia)

• VPLS is also know as:
  • Transparent LAN Service (TLS)
  • E-LAN
VPLS Actors

- The **CE (Customer Edge)** device is a router or switch located at the customer’s premises; it can be owned and managed by the customer, or owned and managed by the service provider. It is connected to the PE through an Attachment Circuit (AC).
- The **PE (Provider Edge)** device is where all the VPN intelligence resides, where the VPLS originates and terminates, and where all the necessary tunnels are set up to connect to all the other PEs. As VPLS is an Ethernet layer 2 service, the PE must be capable of Media Access Control (MAC) learning, bridging and replication on a per-VPLS basis.
- The **IP/MPLS core network** interconnects the PEs; it does not really participate in the VPN functionality. Traffic is simply switched based on the MPLS labels.
VPLS: Setting Up

The basis of any multipoint VPN service (IP VPN or VPLS) is the full mesh of MPLS tunnels (Label Switched Paths [LSPs], also called outer tunnels).

• Label Distribution Protocol LDP
• Resource Reservation Protocol – Traffic Engineering (RSVP-TE)
VPLS: Setting Up

For every VPLS instance, a full mesh of inner tunnels (PWs) is created between all the PEs that participate in the VPLS instance.
VPLS: Implementation type

- **Auto-Discovery**: What method is used that enables multiple provider edge routers (PE) participating in a VPLS domain to find each other?
- **Signaling**: What protocol is used to set up MPLS tunnels and distribute labels between PEs for packet demultiplexing purpose?

<table>
<thead>
<tr>
<th>VPLS Implementation Model</th>
<th>Discovery</th>
<th>Signaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 4761 (BGP-based VPLS)</td>
<td>BGP</td>
<td>BGP</td>
</tr>
<tr>
<td>RFC 4762 (LDP-based VPLS)</td>
<td>None</td>
<td>LDP</td>
</tr>
</tbody>
</table>
How does VPLS work?

Creating the pseudo wires:
Three PWs need to be created, each consisting of a pair of unidirectional LSPs or virtual connections. For VC-label signaling between PEs, each PE initiates a targeted LDP session to the peer PE and communicates to the peer PE what VC label to use when sending packets for the considered VPLS. The specific VPLS instance is identified in the signaling exchange using a service identifier.

Fig. 2  Pseudo wire signaling

- PE1 → PE2: For Svid 101 Use VC label pe 2-1
- PE2 → PE1: For Svid 101 Use VC label pe 1-2
- PE1 → PE3: For Svid 101 Use VC label pe 3-1
- PE3 → PE1: For Svid 101 Use VC label pe 1-3
- PE3 → PE2: For Svid 101 Use VC label pe 2-3
- PE2 → PE3: For Svid 101 Use VC label pe 3-2
How does VPLS work?

MAC learning and packet forwarding:

- PE2 receive a packet from M3 but it doesn’t know the destination of M1: flood the packet;
- PE1 learns from VC label pe2-1 that M3 is behind PE2; it stores this information in the FIB for Svc-id 101 (PE3 does the same);
- PE1 strips off label pe2-1, does not know the destination M1 and floods the packet on ports 1/1/1:100 and 1/1/1:200; PE1 does not flood the packet to PE3 because of the split horizon rule;
- M1 receives the packet.
How does VPLS work?

The Packet Format:
VPLS: Test Bed

VPLS step by step:
1. Setting up PE’s loopback
2. Setting up IP/MPLS provider backbone
   • Enable BGP (or LDP)
   • Enable RSVP
   • Enable OSPF
3. Setting up the VPLS instance
VPLS: Setting up the PE

ROUTER-ID e AS-NUMBER
• Set routing-options router-id 10.0.0.1
• Set routing-options autonomous-system 50

Loopback
• Set interfaces lo0 unit 0 family inet address 127.0.0.1/32
• Set interfaces lo0 unit 0 family inet address 10.0.0.1/32 primary
VPLS: IP/MPLS backbone

Interface inside the provider network
• Set interfaces ge-0/0/1 unit 0 family inet address 40.0.0.1/32
• Set interfaces ge-0/0/1 unit 0 family mpls

MPLS and TUNNEL
• Set protocols mpls interface ge-0/0/1
• Set protocols mpls interface lo0.0
• Set protocols mpls label-switched-path PE1-PE2 to 10.0.0.2

RSVP
• Set protocols rsvp interface ge-0/0/1
• Set protocols rsvp interface lo0.0
**VPLS: IP/MPLS backbone**

**BGP**
- Set protocols bgp group IBGP type internal local-address 10.0.0.1 neighbor 10.0.0.2
- Set protocols bgp group IBGP family l2vpn signaling
  - *Enable the signaling*
- Set protocols bgp local-as 50
  - *Enable MP-BGP flow*
VPLS: IP/MPLS backbone

**OSPF**

- Set protocols ospf
  area 0.0.0.0
  interface ge-0/0/1
- Set protocols ospf
  area 0.0.0.0
  interface lo0.0
- Set protocols ospf
  traffic-engineering
VPLS: IP/MPLS backbone

PE-CE interface

• Set interface ge-0/0/2
  encapsulation ethernet-vpls
• Set interface ge-0/0/2 unit 0 family vpls

ETHERNET-VPLS: Directly connect with ethernet cable
VLAN-TAGGING: trunk Q-in-Q between CE and PE
VPLS: Define an instance

VPLS Instance

- Set routing-instance VPLS instance-type vpls
- Set routing-instance VPLS protocols vpls site-range 5 site SITE01 site-identifier 1
- Set routing-instance VPLS protocols vpls no-tunnel-services
- Set routing-instance VPLS route-distinguisher 30.0.0.1:1
- Set routing-instance VPLS vrf-target target:50:1
- Set routing-instance VPLS instance-type vpls interface ge-0/0/2
EXTENDED COMMUNITIES: (19 bytes)
  Flags: 0xc0 (Optional, Transitive, Complete)
    Type code: EXTENDED_COMMUNITIES (16)
    Length: 16 bytes
  Carried Extended communities
    UnknownRoute Target: 50:1
  UnknownLayer 2 Information: Unknown, Control Flags: none, MTU: 0 bytes
    Encapsulation: Unknown
    Control Flags: Control Word not required, Sequenced delivery not required
    MTU: 0 bytes
MP_REACH_NLRI (32 bytes)
  Flags: 0x90 (Optional, Non-transitive, Complete, Extended Length)
    Type code: MP_REACH_NLRI (14)
    Length: 28 bytes
    Address family: Layer-2 VPN (25)
    Subsequent address family identifier: VPLS (65)
  Next hop network address (4 bytes)
    Next hop: IPv4=10.0.0.2 (4)
  Subnetwork points of attachment: 0
Network layer reachability information (19 bytes)
  RD: 30.0.0.1:1, CE-ID: 2, Label-Block Offset: 1, Label-Block Size: 8, Label Base 262145 (bottom)
VPLS: 2^ Scenario

SITE1

SITE2

LAN1 40.0.0.0/29
LAN2 40.0.0.8/29
LAN3 40.0.0.16/29
LAN4 40.0.0.24/29
LAN5 40.0.0.32/29

LAN2 - 40.0.0.18
LAN3 - 40.0.0.25
LAN4 - 40.0.0.34
LAN5 - 40.0.0.33

PE 1 J2320
PE 2 J2320

CE 1
CE 2

ge-0/0/2
ge-0/0/2

AS 50
route-distinguisher 30.0.0.1:1;
vrf-target target:50:1;
site-range 5

Tagged VPLS instance as:
vlans-vpls - vlanid 600
H-VPLS: Hierarchical VPLS

VPLS BGP based:
• Route reflector solution
H-VPLS: Hierarchical VPLS

VPLS LDP based:
• Hub-Spoken solution
H-VPLS: Hierarchical VPLS

H-VPLS enables VPLS to span multiple metro networks. A spoke connection is used to connect each VPLS between the two metros. In its simplest form, this could be a single tunnel LSP. A set of ingress and egress PW labels is exchanged between the border PE devices to create a PW for each VPLS instance to be transported over this LSP.
References

- RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling, January 2007;
- Wei Luo, Layer 2 VPN Architectures, Cisco Press, March 2005;
- Luc De Ghein, MPLS Fundamentals, Cisco Press, November 2006;
- Mark Lewis, Comparing, Designing, and Deploying VPNs, Cisco Press, March 2006;
- Zhuo (Frank) Xu, Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services, Alcatel - Lucent SRA, January 2010;