Network working group
Internet Draft
Intended status: Informational
Expires: September 2011

R. Gu
J. Dong
M. Chen
Q. Zeng
Huawei Technologies
Z. Liu
China Telecom

March 7, 2011

Analysis of Virtual Private LAN Service (VPLS) Deployment

draft-gu-l2vpn-vpls-analysis-00.txt

Abstract

This document analyses the deployment of typical VPLS network with existing solutions, and discusses the features of each solution. In addition, this document indicates that the advantages of the existing VPLS mechanisms may be integrated to achieve easier and more efficient VPLS provisioning.

Table of Contents

1. Introduction

Virtual Private LAN Service (VPLS), also known as Transparent LAN Service and Virtual Private Switched Network Service, is a Layer 2 Service that emulates LAN service across a Wide Area Network (WAN) [RFC4664]. The primary motivation behind Virtual Private LAN Services (VPLS) is to provide connectivity between geographically dispersed customer sites across the service provider network, as if they were connected using a LAN.

Recently VPLS has become quite popular, and will be deployed in more and larger networks. Also, since there has been much progress in network convergence, whereby multiple kinds of customer services, such as VPLS and IP VPN [RFC4364] etc., would be carried over a single, consolidated IP/MPLS network.

Currently there are some options to deploy VPLS services, and operators need to choose the most suitable technology according to their requirement and the work load in network deployment and operation.

This document analyzes the deployment of typical VPLS network with existing solutions, and discusses the features of each solution. In addition, this document indicates that the advantages of the existing VPLS mechanisms may be integrated to achieve easier and more efficient VPLS provisioning.

2. Deployment of VPLS Network

This section describes the operation of a VPLS network with existing solutions. General topology of a VPLS network is shown in Figure 1. There are N PEs in the network, and V VPLS instances are deployed in the network.

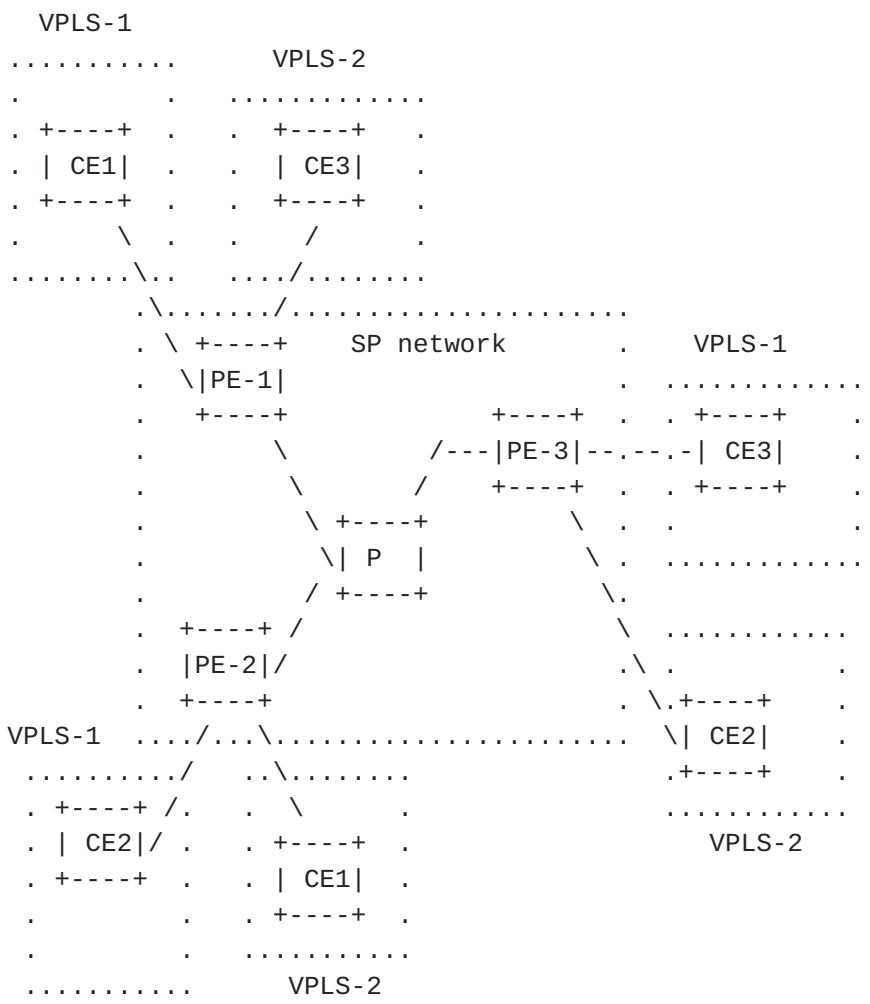

Figure 1. General topology of VPLS network

2.1. Deployment Considerations of LDP based VPLS

[RFC4762] describes the control plane of signaling pseudowire labels for VPLS service using Label Distribution Protocol (LDP).

For LDP signaling, full-mesh targeted LDP sessions need to be established among VPLS PEs. For a network with N PEs, there would be N*(N-1) targeted LDP sessions. If N is large, the deployment would be configuration intensive. Besides, [RFC4762] does not provide mechanism for membership auto-discovery, by default the identities of all the remote pseudowire endpoints in each VPLS instance need to be manually configured on each PE. Thus if a new site or a new PE is added to one VPLS, configurations of all the other PEs need to be updated. Besides, in large scale VPLS networks, the overhead of maintaining full meshed N*(N-1) LDP sessions would be an issue.

While this could be alleviated by Hierarchical VPLS (H-VPLS), the expense is additional complexity in provisioning and operation.

When using LDP based mechanism to deploy a VPLS network, one unique VPLS Identifier needs to be assigned for each VPLS instance.

Section 3.2.2 of [RFC6074] specifies BGP based Auto-Discovery (BGP-AD) mechanism for VPLS service. This mechanism can be combinely used with LDP based VPLS signaling, which would reduce the overhead of PW endpoint configuration, and even the establishment of targeted LDP sessions may be automatically triggered by BGP auto-discovery.

However, when BGP-AD is used with LDP signaling, in addition to BGP sessions established for membership auto-discovery, it is still required to set up fully meshed targeted LDP sessions for pseudowire signaling, regardless of whether the LDP sessions are manually configured or automatically established. Thus in this case operators need to deploy and maintain both BGP and targeted LDP to offer VPLS services. And the signaling overhead in this case would be higher than both LDP signaling without BGP-AD and BGP based VPLS in [RFC4761].

Using LDP based VPLS signaling, the pseudowire labels are allocated "on-demand" for each remote endpoints in each VPLS instance, thus label resources are utilized efficiently.

MAC Address Withdrawal mechanism is defined in LDP based VPLS to expedite removal of MAC addresses in some topology changes. And status information of the pseudowires can be exchanged using mechanism in [RFC4447]. These features could make operation and maintenance of VPLS more efficient and convenient.

2.2. Deployment Considerations of BGP based VPLS

[RFC4761] describes the BGP based auto-discovery and signaling mechanism for VPLS.

BGP based VPLS mechanism combines VPLS membership auto-discovery and signaling into a single BGP Update message, which achieves quite low signaling overhead and allows operational convergence with IP VPN.

The control plane of BGP based VPLS could inherit the scalability mechanism from BGP, thus full meshed signaling sessions among VPLS PEs can be avoided by deploying route reflectors [RFC4456]. Each PE can just establish one BGP session with route reflector.

To deploy a BGP based VPLS service, operator needs to assign a unique VE-ID for each PE in given VPLS instance. As VE-IDs cannot be generated automatically and requires coordination among all the PEs in the same VPLS, this may introduce management burden to operators, especially in multi-area and multi-AS scenarios. Similar to IP VPN, Route Targets are used to identify different VPLS instances.

The pseudowire discriminators are advertised in form of label blocks. Although this avoids the control plane load of sending individual label signaling messages to each remote PE, the use of label block is based on idea of "allocate in advance" and "over-provisioning" and in many cases the allocation of label resources may be not quite efficient compared with "on-demand" label allocation for each discovered remote endpoint. Besides, the size of label block allocated could be impacted by VE-IDs of remote PEs, which makes the management more complicated, and exposes a potential security issue. An example of VE-ID assignment and label block allocation is described as below:

For ease of VE-ID management and future network expansion, operator may assign a set of blocks of VE-ID for different regions of the network, as shown in Figure 2, VE-ID 1-100 are assigned to region 1, and VE-ID 101-200 are assigned to region 2. According to the mechanism in [RFC4761], in order to establish VPLS pseudowire with a PE in region 2, say the VE-ID is 102, PE1 needs to allocate a label block with the size of at least 102, even if in the beginning only less than 10 PEs are deployed in each region. If the number of VPLS instances V in the network is large, the amount of labels wasted altogether may not be neglectable.

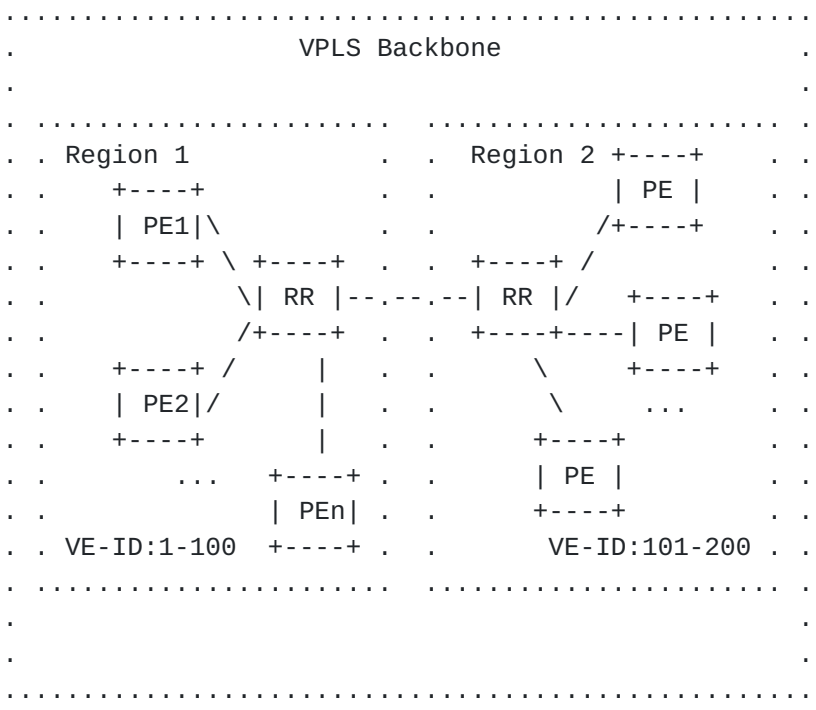

Figure 2. An Example of VE-ID Assignment

Currently BGP based VPLS does not provide mechanisms of MAC address withdrawal and pseudowire status notification.

3. Comparison of Existing VPLS Solutions

As analyzed in section 2, both LDP based and BGP based VPLS solutions have some advantages and disadvantages. These are summarized in Table 1.

VPLS service provisioning consists of membership discovery and pseudowire signaling. VPLS membership can be either manually configured, or auto-discovered through BGP auto-discovery mechanism. According to Table 1, it is obvious that BGP-AD is an important feature which significantly reduces the overhead of manual provisioning in LDP based VPLS, with the expense of coexistence of two control plane protocols and additional signaling sessions and messages. BGP based VPLS combines auto-discovery and signaling into a single Update message at the cost of potential waste of label resources.

While VPLS provides multipoint service, the underlying infrastructure is full-mesh point-to-point pseudowires. Thus the on-

demand label allocation mechanism in LDP signaling could provide better efficiency in label resource utilization.

Regarding the control plane scalability, the big challenge with LDP VPLS is maintenance of full-mesh targeted LDP sessions, while in BGP VPLS this problem can be easily solved with route reflection.

Some service providers may have already deployed IP VPN service in their networks which uses BGP as signaling protocol, and plan to provide VPLS service in the same network, in this case they may prefer to deploy VPLS using the same technology as IP VPN to simplify service provisioning and network operation.

VPLS Solution	Advantages	Disadvantages
LDP VPLS without BGP-AD	1.on-demand label allocation 2.MAC withdrawal and PW status notification mechanism	1.manual provisioning 2.full mesh T-LDP session 3. non-convergence with IP VPN operation
BGP VPLS	1.convergence with IP VPN 2.membership auto-discovery 3.scalability with use of RR 4.minimal signaling overhead	1.VE-ID management 2.waste of label resource 3.lack of MAC withdrawal and PW status notification
LDP VPLS with BGP-AD	1.membership auto-discovery 2.on-demand label allocation 3.MAC withdrawal and PW status notification mechanism	1.overhead of two control plane protocols 2.full mesh T-LDP session

Table 1. Comparison of existing VPLS solutions

To simply VPLS service provisioning, BGP based auto-discovery would becomes a mandatory feature. The concerns about LDP based VPLS with BGP-AD may be the scalability issue and burden of full-mesh targeted LDP sessions. While control plane of BGP based VPLS is more scalable and achieves convergence with IP VPN, inefficiency in label resource utilization and complexity in VE-ID management may influence operators' choice.

Actually there may be one solution which integrates the advantages and avoid those disadvantages:

a. BGP-AD in [RFC6074] is used for membership auto-discovery.

b. After auto-discovery of members in each VPLS, instead of establishing targeted LDP sessions, the BGP sessions which are already established for BGP-AD can be re-used to execute signaling functions in a similar way to LDP VPLS, i.e. using BGP to perform on-demand pseudowire label allocation, MAC address withdrawal and pseudowire status notification.

In this way, the VPLS provisioning could be simplified by BGP-AD, and there would be no need of setting up any targeted LDP session in the VPLS network. Label resource could be allocated efficiently and the complexity of VE-ID management would be avoided. BGP is the only control plane protocol and the operation convergence with IP VPN can be achieved. Detailed specification about extensions for this solution would be described in a separate document and is outside the scope of this document.

4. Security Considerations

This document does not change the security properties of VPLS.

5. IANA Considerations

There is no IANA action required by this draft.

6. Acknowledgments

The authors would like to thank ... for their valuable suggestions and comments to this document.

7. References

7.1. Normative References

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RFC4456] Bates, T., Chen, E., and R. Chandra, "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)", RFC 4456, April 2006.

[RFC4664] Andersson, L. and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, September 2006.

[RFC4761] Kompella, K. and Y. Rekhter, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling", RFC4761, January 2007.

[RFC4762] Lasserre, M. and V. Kompella, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", RFC4762, January 2007.

[RFC6074] Rosen, E., Luo, W., Davie, B. and V. Radoaca, ''Provisioning, Autodiscovery, and Signaling in L2VPNs'', RFC6074, January 2011.

[RFC4447] Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

Authors' Addresses

Rui Gu
Huawei Technologies Co.,Ltd.
Huawei Building, No.3 Xinxi Rd.,
Hai-Dian District
Beijing, 100085
P.R. China
Email: gurui@huawei.com

Jie Dong
Huawei Technologies Co.,Ltd.
Huawei Building, No.3 Xinxi Rd.,
Hai-Dian District
Beijing, 100085
P.R. China
Email: jie.dong@huawei.com

Mach(Guoyi) Chen
Huawei Technologies Co.,Ltd.
Huawei Building, No.3 Xinxi Rd.,
Hai-Dian District
Beijing, 100085
P.R. China
Email: mach.chen@huawei.com

Qing Zeng
Huawei Technologies Co.,Ltd.
Huawei Building, No.3 Xinxi Rd.,
Hai-Dian District
Beijing, 100085
P.R. China
Email: zengqing@huawei.com

Zhihua Liu
China Telecom
109 Zhongshan Ave., Guangzhou
510630, China
Email: zhliu@gsta.com