Network Working Group Tissa Senevirathne
Internet Draft (Force10)
Document: draft-tsenevir-bgp-l2vpn-02.txt Loa Andersson
Category: Informational (Utfors AB)

May 2002

Auto-Discovery of VPLS Membership and Configuration Using BGP-MP

Status of this Memo

1. Abstract

Membership and configuration discovery is a key component in Layer 2 VPN infrastructure. This document presents use of BGP-MP extensions for VPLS Membership and configuration discovery. More specifically, this document adapts generic VPN discovery methods presented in [2] for VPLS Membership and Configuration discovery.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [3].

Placement of This Memo in Sub-IP Area

RELATED DOCUMENTS:

WHERE DOES IT FIT IN THE PICTURE OF THE SUB-IP WORK

PPVPN

WHY IS IT TARGETED AT THIS WG

PPVPN WG charter specifies explicitly to consider BGP-VPN services, more specifically based on RFC 2547. In addition WG charter includes Virtual Private LAN Services (VPLS) and VPN auto-discovery.

JUSTIFICATION

Layer 2 VPN services are gaining popularity in emerging metro services infrastructure. Ability to automatically discover configuration and membership information enables metro service providers to manage large VPLS networks easily. Absence of such auto-discovery leads to manual configuration of VPLS services. Such manual configuration is not only tedious and less flexible, but also increases administrative costs.

3. Introduction

Ability to automatically discover configuration and membership information enables metro service providers to manage large VPLS networks easily. Absence of such auto-discovery leads to manual configuration of Layer 2 VPN services. Such manual configuration is not only tedious and less flexible, but also increases administrative costs.

The VPN service introduced in [4] is widely used to provide Layer 3 VPN services by service providers. As Layer 2 VPN becomes available, the same providers may be required to provide both Layer 2 and Layer

3 VPN services. Ability to use the same set of control protocols to provide two classes of VPN not only provide flexibility but also allow investment protection and migration from one class to another or co-offering.

In this document we define specific details required to implement VPLS membership and configuration discovery using methods out lined

in [2]. The architecture and requirements for VPLS can be found in [5] and [6].

In this document we assume readers are familiar with terminology and concepts used in [2] [4] [5] [6].

4. VPLS Membership and Configuration discovery

When providing VPLS services, participating PE devices are required to obtain key parameters such as; end-points or membership information and VLAN(usage) information.

End-points or Membership information

PE devices that participate in a given VPLS are defined by common membership information. A given PE device MAY support more than one VPLS.

VLAN span (usage)

VLAN span provides a sub-scope within the VPLS. VLAN may span over a subset of end-points.

5. BGP-MP encoding for VPLS discovery

. Encode VPLS-ID (L2-VPN-ID) using VPN-ID extended community [2].

. Use Extended Communities Attributes to specify the VLAN information applicable to given VPLS-ID.

5.1 Encoding of NLRI

5.1.1 Layer 2 VPN AFI

[2] specifies a common AFI for auto-discovery of Layer 2 VPN. This AFI is common to all models of Layer 2 VPN. Actual value of the Layer 2 VPN AFI [TBD].

5.1.2 VPLS SAFI

SAFI 0x[TBD] is used to denote that NLRI is related to VPLS auto-discovery.

5.1.3 Encoding NLRI for VPLS

NLRI carries IP address of the PE device that is advertising the discovery information. VPLS auto-discovery NLRI is a 8 byte Route Distinguisher (RD). IP address of the PE is encoded as part of the NLRI.

Route Distinguisher

The Route Distinguisher for VPLS is coded as follows.

Type field - 4 bytes
Value field û 4 bytes

Type field
  The value of the type field indicates that it carries the IP address of the PE device.

  Type field = 0x0001 indicates that the RD carries IPV4 address of the PE device.

  All other values in Type field are reserved.

Value field

  IP address - 4 bytes.

5.2 Encoding VLAN extended communities attribute

A new extended community is used to carry the VLAN information. This attribute is transitive across the autonomous system boundary. The value for TYPE field for extended community attribute will be assigned by IANA. Assigned number subfield contain the 12 bit VLAN id pre-pended with required zero (0). Filtering based on VLAN and VPN-ID extended community attributes allow a PE device to accept or reject VLAN based on local policies.

6.0 Further discussion

When Layer 2 VPNs PE devices are connected to more than one service provider the AS number in the RD is used to uniquely identify the Layer 2 VPN membership.

7. Security Considerations

Security issues relevant to Layer 2 VPN are discussed in [6] and Security issues relevant to use of 2547bis are discussed in [4].

8. References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Ould-Brahim, H , et. al, Using BGP as an Auto-Discovery Mechanism for Network-based VPNS.

3 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

4 Rosen, E., et.al., BGP/MPLS VPNs, RFC 2547, March 1999.

5 Senevirathn, T., et.al, Requirements for Network Based Layer 2 VPN, Work in Progress, May 2001.

6 Senevirathne, T., et.al., A Framework for Virtual Metropolitan Internetworks (VMI), Work In Progress, February 2001.

9. Acknowledgments

Increasing popularity of Layer 2 VPN services motivated us to publish this work. We wish to acknowledge valuable comments and suggestions provided by Eric Rosen and Yakov Rekhter.

10. Author's Addresses

Tissa Senevirathne
Force10 Networks
1440, McCarthy Blvd, Milpitas, CA
Phone: 408-965-5103

Email:
tsenevir@hotmail.com m

Loa Andersson
Utfors AB

Full Copyright Statement