Network Working Group
Internet Draft
Document: draft-squire-ppvpn-vpn-discovery-reqts-00.txt

Matt Squire
Hatteras Networks

November 2001 Expires May 2002

VPN Discovery Discussions and Options

Status of this Memo

Abstract

VPNs are a common service being offered by providers. The PPVPN WG is tasked with defining a limited number of solutions to support the interoperable deployment of VPN services. As part of this effort, a design team was tasked with defining the requirements of PPVPN discovery proposals, to analyze if additional discovery schemes are needed, and to characterize potential solutions to the problem. This draft is the output of that design work. Consensus was not reached on the solution characteristics. However, this draft attempts to capture the discussions and positions of the design team exchanges.

1 Introduction

VPNs come in many shapes and sizes. In [MARTINISIG], as an example, an emulated VC consists of two LSPs (Label Switched Paths), one in each direction. Each endpoint initiates the setup of the LSP that carries packets in the "incoming" direction. In order for the

signaling to proceed, each endpoint has apriori knowledge of
(a) the address of the other endpoint, and
(b) a VC id.

On a given emulated VC, the same VC id must be used for both LSPs.

In this context, "apriori knowledge" simply means information that must be known prior to the initiation of signaling. The draft [MARTINISIG] provides one example of how to use signaling in establishing a VPN. The information required as apriori knowledge may differ depending on the signaling protocol and assumptions.

In the context of PPVPN, discovery is the process by which a PE learns the required apriori knowledge.

1.1 Specification of Requirements

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.

2 Necessity of a Solution

There are currently two proposals for performing VPN endpoint discovery. The two methods can be characterized as BGP and multicast. RFC 2547 (and related work) define mechanisms to use BGP multi-protocol extensions to include VPN information in the BGP routing information. Discovering which PE equipment is in which VPNs can then be determined by querying the routing tables.

RFC 2917 defines how multicast can be used to discover VPN membership. Each VPN is assigned a specific multicast address. This address implicitly defines a communication channel to all VPN members over which members can determine the unicast address of other PE equipment in that VPN.

Current PPVPN discovery methods have been developed as part of particular deployment solutions. The BGP and multicast approaches introduced above were specifically developed for discovery of L3VPNs in BGP or multicast enabled networks. Most members of the design team believe that there are contexts where additional discovery mechanisms are needed. Some members are firmly opposed to this belief.

PPVPN discovery is only one part of the PPVPN solution. As there are currently multiple models and architectures for PPVPN solutions, including virtual routers, overlay L3 networks, Layer2 VPNS, etc., one must consider particular discovery solutions in the context of the PPVPN architectures for which they are intended.

3 Requirements

There was consensus from the design team on many requirements for a VPN discovery protocol. However, there was contention over the exact interpretation of the requirements. This following list summarizes the requirements while later subsections discuss where these requirements are in dispute.

Any VPN discovery process or protocol must satisfy the following requirements.

- It MUST support inter-provider VPNs.
- It MUST be possible to deploy the auto-discovery scheme in a manner which prevents unauthorized access and allows authentication of the source
- It MUST respond to VPN membership changes in a timely fashion (see 3.1)
- It SHOULD limit VPN information to only those PEs involved in that VPN.
- It MUST provide VPN endpoint information consisting of at last the IP address of associated PE equipment, and MAY be extendible to provide additional information (see 3.2).

3.1 Timely Fasion

The responsiveness of VPN discovery to membership changes is hotly contested. Although faster is always better, the main question is how fast is fast enough? When a PE is added to a VPN (or deleted for that matter), how quickly must the other PE equipment in that VPN notice the change?

The two positions put forward by the design team and captured by this document are rougly:
a) "Routing" time frame.
b) "Provisioning" time frame.

This document does not attempt to exactly quantify the two possibilities. However, it should be clear that (a) is a more stringent requirement than (b). As a rough quantification, (a) is usually measured in seconds, while (b) is measured in minutes.

3.2 Extended Discovery or Signaling

There are two different ways of viewing the VPN discovery process. It could be viewed as a limited process where each member learns enough about other members of the VPN to complete VPN signaling. Alternatively it could be viewed as this limited process, plus the VPN signaling.

The VPN signaling is required to exchange parameters of a more or less dynamic nature, e.g. information used to dynamically distribute MPLS labels set up LSP tunnels and VC LSP's.

The point of contention centers on the boundary between discovery and signaling. It is clear that, at a minimum, each PE device must know the IP address of other PE devices that serve a VPN. The question then becomes whether the IP address enough information. The two conflicting positions are

---

a) Yes. All additional information should be exchanged via the signaling protocol.
b) No. It should be required to support additional information that may be a prequesite for signaling.

It is clear that the initialization process must be extensible to new parameters and features, the question lies in where those parameters are added.

4 Conclusion

Being an IETF design team, we have realized our responsibility to not reach consensus.

The design team was able to reach consensus on some of the VPN discovery requirements. These are described in Section 3. However, there was intense contention on several key issues as described outlined in Sections 3.1 thru 3.2. As a result, we can conclude that any one PPVPN discovery solution is unlikely to satisfy all providers, developers, and scenarios.

5 Referenc

[RFC2026] S. Bradner, "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2547] E. Rosen & Y. Rekhter, "BGP/MPLS VPNs," RFC 2547, March 1999.

[RFC2917] K. Muthukrishnan & A. Malis, "A Core IP MPLS VPN Architecture," RFC 2917, September 2000.

[MARTINISIG] L. Martini, et al., "Transport of Layer 2 Frames over MPLS," draft-martini-l2circuit-trans-mpls-08.txt, Work in Progress.

6 Acknowledgments

This draft is the result of collaborative effort of the PPVPN discovery design team. The members of that design team are:

Loa Andersson (Utfors)
Ron Bonica (MCI)
Juha Heinanen (Song Networks)
Jim Luciani (Crescent Networks)
Dave McDysan (WorldCom)
Dave Meyer (Sprint)
Hamid Ould-Brahim (Nortel Networks)
Yakov Rekhter (Juniper Networks)
Eric Rosen (Cisco)
Tissa Senevirathne (Force 10 Networks)
Matt Squire (Hatteras Networks)

All members made valuable contributions to this effort.

7 Author's Addresses

Matt Squire
Hatteras Networks
639 Davis Drive
Research Triangle Park, NC 27709
Email: msquire@hatterasnetworks.com