Network Working Group
Tony Li
INTERNET DRAFT Juniper
Networks

# CPE based VPNs using MPLS

<draft-li-mpls-vpn-00.txt>

Status

This document is an Internet Draft. 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 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 a "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

## 1.0 Abstract

This document describes a proposed architecture for the construction of Virtual Private Networks (VPNs). This proposal differs from [1] and [2] in that the functionality of the VPN is shared by the Customer Premises Equipment (CPE). Multi-Protocol Label Switching (MPLS) is used as a tunneling mechanism across the ISP network.

## 2.0 Introduction

A VPN is a mechanism that allows one or more sites to exchange packets. It differs from traditional Internet connectivity in that:

- The address space used by the VPN sites might not be global

- The VPN sites require secure communications, possibly including payload privacy and protocol level privacy

- Sites might interact with multiple VPNs and with the Internet simultaneously

- The ISP might perform traffic engineering on the structure of the

VPN
to ensure consistent service to the VPN participants

This proposal differs from those found in [1] and [2] in that it allows the VPN site to maintain physical security over the cryptographic equipment used to encrypt its data. This security level is likely to be necessary for any site with a serious interest in security. The implication is that a VPN site need not trust the Internet Service Provider (ISP) to ensure data privacy, only to provide data transit.

This proposal uses BGP as the primary mechanism for information distribution and assumes that RSVP or LDP is used as the signaling mechanism for the MPLS domain.

## 3.0 Theory of Operation

In this architecture, BGP information is exchanged between the CPE and the ISP's border router so that the CPE can indicate (a) its presence in the network and (b) the set of VPNs that the CPE would like to participate in.

This information is possibly (but not necessarily) filtered by the ISP and then passed on to other sites. Sites wishing to connect to the VPN initiate an MPLS label-switched path (LSP) with other members of the VPN.

If the creation of the LSP is allowable according to the policies established for the VPN, the connection is established and the sites that initiated the LSP have connectivity through the LSP. Transit service is provided by encapsulating packets in an MPLS tunnel. The ISP is responsible for delivering the packets to the designated site within the network. The ISP is not responsible for providing security for the VPN, but it might provide access control information on the distribution of information about the VPN itself.

The specification of the policies for VPN membership and the mechanisms for determining policy compliance are beyond the scope of this document.

Because an LSP can be modeled as a (half-duplex) point-to-point link, the topology of the VPN can be a full mesh between sites. Alternately, a sparse topology can be constructed based on the policy established by the CPE. This allows the participants in the VPN to determine the optimal tradeoff between administrative overhead and optimized routing between sites.

For scalability reasons, providing VPN services is done at the site level. Individual users wishing to access the VPN must do so through a VPN member site. Users not physically present at a VPN member site

may access the VPN by first accessing a VPN member site using a mechanism such as Mobile IP [3].

## 4.0 VPN advertisement

To advertise membership in the VPN, the CPE uses BGP. The CPE advertises a host route (/32 prefix) in BGP. The address that is advertised is the IP address of the CPE equipment itself. This address is taken from the ISP's address space and can be globally unique. The remainder of the address space within a site can be local, and the CPE can provide NAT functionality to separate the address space of the site from the global Internet and/or the remainder of the VPN. [4]

To identify the VPN, each VPN is given a unique identifier. This identifier is a 16-bit number, assigned by the ISP. The CPE advertises this number as part of the BGP communities attribute by advertising a community in which the most significant 16 bits are the ISP's Autonomous System (AS) number and the least significant 16 bits are the VPN identifier. This BGP community number is already allocated to the ISP for local use by the ISP. Additional VPN identifiers can be allocated either by acquiring another AS number or by use of one of the locally scoped communities.

The ISP's border router is the first router to receive the VPN advertisement from the CPE. At this point, the ISP can filter or otherwise examine the advertisement to ensure that it complies with the ISP's policies. For example, the ISP might wish to sell VPN services at an extra charge. The ISP could discard VPN advertisements from customers that had not subscribed to the VPN service. Further, if the ISP helps to administer membership in the VPN, the ISP optionally could discard advertised communities that the site did not actually participate in.

For VPN advertisements that are accepted by the ISP, BGP naturally propagates them to other BGP speakers attached to the ISP and thus to other CPE devices. Note that the ISP can easily construct policy such that a CPE receives only the BGP advertisements that the ISP selects, such as those from other members of the VPN and the default route. This would avoid having the CPE carry full routing. Further, the ISP can easily filter out VPN advertisements, thus protecting the default-free Internet routing table from the introduction of unnecessary routes.

The receiving CPE can authenticate the BGP advertisements that it receives, discarding any that fail the authentication test.

## 5.0 Establishing LSPs

When a CPE receives a VPN advertisement, it can decide to create a VPN connection to the advertiser. The CPE is under no obligation to connect to all possible members of the VPN. The creation of VPN LSPs is a function of the VPN participants and the ISP. For example, a common topology today is a star, in which an enterprise has a central site and many remote sites. In general, the remote sites communicate only with the central site. Thus, it makes sense for the remote sites to establish an LSP only back to the central site rather than forming a full mesh of LSPs between VPN participants. Such a policy could be configured into the remote site's CPE.

If a site does decide to initiate a VPN LSP to another VPN participant, it does so by using an MPLS signaling protocol to set up the LSP. Currently, both RSVP and LDP are possible candidate signaling protocols for MPLS. The modifications discussed in this document could reasonably be applied to both protocols.

When a site is establishing an LSP, it uses its signaling protocol to indicate that it would like an LSP. It uses the address of the CPE device at the opposite end of the LSP to indicate the destination of the LSP. In addition, the CPE attaches the VPN identifier, a time stamp, and a signature for security purposes.

Because the ISP participates in the signaling protocol, it has the ability to filter out setup requests for the VPN that do not coincide with the ISP's policies. This helps to ensure that access to VPN services is enforced at the LSP level. In addition, the ISP has the ability to perform traffic engineering on the LSP setup request. Work on traffic engineering is currently in progress, but it is reasonable to expect that an explicit route could be computed by the ISP's border router and attached to the setup request. This allows the ISP to place VPN traffic on appropriate facilities to ensure appropriate service levels for the VPN.

After passing the entry border router, the LSP setup propagates through the ISP's network in a manner similar to any other traffic-engineered LSP.

When the LSP setup request is received by the destination CPE, it is again authenticated and can be rejected (using the appropriate signaling protocol mechanisms) if it fails the authentication check or violates the destination CPE's configured policies. If it is accepted, the CPE completes the setup request as it normally would within the signaling protocol. As part of the acknowledgment of the setup, the destination CPE also can attach a series of prefixes to its acknowledgment. These prefixes represent reachability information that the destination CPE allows the originating CPE to reach using that LSP.

When the originating CPE system receives the acknowledgment, it can, depending on its configured policies, install the prefixes in its forwarding table and it also can inject those prefixes into its local routing. Note that these prefixes are determined by configuration and do not constitute a routing protocol in and of themselves. No mechanisms are provided here to ensure loop freedom or optimality of route computation for prefixes exchanged using the signaling protocol. Sites wishing to have a routing protocol run on top of the VPN are not precluded by this architecture, but no special provisions are made for (or are required by) such situations. Similarly, multicast can be supported on the VPN by running normal multicast routing protocols across the VPN.

## 6.0 Acknowledgments

The author would like to thank Johna Johnson, Aviva Garrett, and Lisa Bourgeault for her comments and Yakov Rekhter for his generous contributions to this work.

## 7.0 References

[1] J. Heinanen, et. al, "VPN support with MPLS," <draft-heinanen-mpls-vpn-01.txt>, March 1998.

[2] D. Jamieson, et. al, "MPLS VPN Architecture," <draft-jamieson-mpls-vpn-00.txt>, August 1998.

[3] C. Perkins, "IP Mobility Support," RFC 2002, October 1996.

[4] K. Egevang & P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May 1994.

## 8.0 Author's Address

Tony Li
Juniper Networks, Inc.
385 Ravendale Dr.
Mountain View, CA 94043
Email: tli@juniper.net
Fax: +1 650 526 8001
Voice: +1 650 526 8006