Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

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 draft documents 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 "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This memo describes how provider provisioned Virtual Private LAN Service (VPLS) can be implemented using DNS and LDP for PE discovery and label distribution.

1. Introduction


An advantage of a DNS/LDP based solution for provider based VPNs is that it doesn’t require BGP implementation or configuration complexity in the PE routers and can be easily deployed also in inter-AS cases where the VPN sites are attached to PEs in more than one AS. Another advantage of DNS is that it has been in wide use for years and can thus be deployed without any new standardization.
effort. See [2] for more discussion on the use of DNS for VPN discovery.

A similar DNS/LDP based solution can also be applied to provider based Virtual Circuit and Virtual Router VPNs.

2. Addition of Sites

2.1 Configuration Actions

DNS/LDP based VPLS is very easy to provision. Only the following two configuration actions are needed when a new site (CE device) is added to a VPN:

(1) If the PE device (PE for short) does not previously connect any sites of this VPN, the IP address (A record) of the PE is added to DNS under domain name

\[
\text{vpn-name}.\text{domain}
\]

The label "vpn-name" uniquely identifies the VPN within "domain", which belongs to the administrative "owner" of the VPN. An example of the domain name of a VPN is bobsVpn.serviceProvider.net.

(2) The "interface" of the PE to which the site is connected to is configured to belong to the VPN. This is done by specifying the domain name and type of the VPN. This document covers the case where the type of the VPN is "LAN".

Note that also in the case of a multi-provider VPN, the administrative "owner" of the VPN is the single body that operates the master DNS server for the VPN zone. The "owner" of a VPN MAY choose to make all updates to the zone data of the VPN by itself or MAY allow other providers to dynamically update the zone data.

2.2 Protocol Actions

After the above configuration actions, the following protocol actions take place in sequence at the PE of the new site if the PE of the new site doesn’t previously connect site(s) of the VPN:

(1) The PE of the new site checks that its own IP address has become available in the DNS under the domain name of the VPN.

(2) The PE of the new site queries DNS for IP addresses of the other (remote) PEs of the VPN.
(3) The PE of the new site establishes an LDP session with each of the remote PEs unless one already exists.

(4) The PE of the new site sends a Label Mapping Message to each of the remote PEs that advertises a label to be used when a remote PE sends packets to the sites of the VPN at the PE of the new site. Each such label MUST uniquely identify at the PE of the new site both the VPN and the sending PE.

The Label Mapping Message uses the following VPN ID FEC TLV:

```
+-------------------------------+-------------------------------+
<table>
<thead>
<tr>
<th>VPN ID TLV</th>
<th>Address Family</th>
<th>VPN ID Length</th>
</tr>
</thead>
</table>
+-------------------------------+-------------------------------+
| Domain name of the VPN padded with spaces to the next four octet boundary + |
| ...                  |               |               |
+-------------------------------+-------------------------------+
```

Element type name: VPN ID
Type: TBD by IANA
Address Family: set to zero
VPN ID Length: Variable

The following protocol actions take place in sequence at a PE when it receives a Label Mapping message from another PE:

(1) The PE checks from the DNS that the other PE belongs to the VPN of the Label Mapping Message and that it itself has at least one site in that VPN. If not, the PE responds to the Label Mapping Message with a Label Release Message and no other protocol actions take place at the PE.

(2) The PE checks if it already has a label for the VPN and PE of the Label Mapping Message. If so, the PE responds to the Label Mapping Message with a Label Release Message and no other protocol actions take place at the PE.

(3) The PE checks if it already has itself advertised a label to the other PE for the VPN of the Label Mapping Message. If not, the PE sends a Label Mapping Message to the other PE to be used when the other PE sends packets to the sites of the VPN at the PE. The advertised label MUST again uniquely identify at the PE both the VPN and the other PE.
If the PE of the new site already connects site(s) of this VPN, no protocol actions take place at either the PE of the new site or at the remote PEs.

3. Removal of Sites

3.1 Configuration Actions

The following configuration actions are needed when an existing site (CE device) is removed from a VPN:

1. If the site to be removed is the last site of the VPN at the PE, the IP address of the PE is removed from DNS under the domain name of the VPN.

2. The site is removed from the VPN by unconfiguring the VPN from the "interface" of the PE to which the site is connected to.

3.2 Protocol Actions

After the above configuration actions, the following protocol actions take place at the PE of the removed site if the removed site was the last site of the VPN at the PE:

1. The PE checks that its IP address does not anymore exist in the DNS under the domain name of the VPN.

2. The PE removes any existing labels of the VPN that it had advertised to the remote PEs by sending them a Label Withdraw Message.

In addition to processing the Label Withdraw Message, the following protocol actions take place when a PE receives a Label Withdraw Message from another PE:

1. The PE removes the label that it had advertised to the other PE for the VPN of the Label Withdraw Message by sending it a Label Withdraw Message.

2. If there is no remaining need to keep the LDP session up between the PE and the other PE, the PE MAY terminate the LDP session with the other PE.

4. Failure Recovery

If a PE looses its LDP session with another PE having site(s) in a common VPN, the PE releases the label it has advertised to the other PE for this VPN. The PE then tries to re-establish the LDP session.
until (a) the session gets established or (b) this PE or the other PE no longer have site(s) in this VPN. Once the LDP session gets established, the PE advertises to the other PE a label to be used to send packets to the site(s) of the VPN at this PE as described in section 2.2.

When a PE recovers from a crash, it adds each of the configured VPN site(s) to their respective VPN(s) as described in section 2.2.

5. Exponential Back-off Behavior

If any protocol action does not succeed immediately, the normal behavior is that the PE keeps on trying with exponential back-off until the action either succeeds or becomes invalid due to a change in VPN configuration. If the protocol action fails for an implementation specific prolonged period of time, the PE SHOULD notify the "owner" of the VPN about the problem via a management action.

6. Data Plane

The PEs that host the sites of a VPN act as fully connected learning bridges.

When PE A needs to forward an Ethernet packet to PE B, PE A encapsulates the Ethernet packet into a label stack entry [4] as described in [5]. The label of the label stack entry is the one that PE B has advertised to PE A for this VPN. The optional control word MUST NOT be used.

PE A then sends the resulting frame to PE B in any available tunnel, such as a HIP, GRE, IPSec, VLAN, or MPLS. The selection of the tunneling protocol is outside the scope of this memo.

7. DNS Zone Update Latency

In order to make addition and removal of VPN PEs as fast as possible, it is important to try to minimize the latency of VPN zone updates. This can be achieved by turning on DNS NOTIFY [6] in the master server for each VPN zone and/or by configuring refresh times of VPN zones small, e.g., zero.

8. DNS Message Size

Correct operation of directory/LDP based VPNs requires that IP addresses of all PE routers of a VPN fit into a single DNS response. As described in [7], if a PE receives a response that has the Truncated Header bit (TC) set, it MUST ignore that response, and
query again, using a TCP connection that will permit larger replies.

9. Security Considerations

Security of directory/LDP based VPNs depends on security of the directory (DNS), LDP, and the tunneling protocol(s). Security of LDP is covered in the security section of [3]. Also the various tunneling protocol specifications have their own security sections.

Regarding DNS security, the important issues related to this memo are security of zone transfers, security of possible dynamic updates, as well as integrity and authentication of DNS queries and responses. In case of dynamic updates, it is RECOMMENDED that secure dynamic updates [8] are used. Security of zone transfers as well as integrity of queries and responses are addressed by DNS extensions [9] and [10].

No DNS extensions exist for providing confidentiality for queries or responses. It is thus possible that if a party knows the domain name of a VPN, the party can find out the IP addresses of PE routers that connect sites of that domain. Depending on the situation, that may or may not be an acceptable security risk.

In a single-provider VPN, DNS servers that host VPN zones can be easily fire-walled from all public access. Another way to prevent outside parties from accessing VPN information is to use DNS access lists that allow VPN zone related queries only from trusted PE routers.

Acknowledgements

I would like to thank Joel Halpern of Longitude Systems and Matt Squire of Hatteras Networks for their constructive comments on an earlier versions of this memo.

References


Author’s Address

Juha Heinanen
Song Networks, Inc.
Hallituskatu 16
33200 Tampere, Finland
Email: jh@song.fi

Full Copyright

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS
IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK
FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT
LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT
INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR
FITNESS FOR A PARTICULAR PURPOSE.