Network Working Group
Internet Draft
Expiration Date: February 1999

S. Pegrum
D. Jamieson
M. Yuen
A. Celer
Nortel (Northern Telecom) Ltd.
August 1998

VPN Point to Multipoint Tunnel Protocol (VPMT)
draft-pegrum-vmmt-01.txt

Status of this Memo

This draft obsoletes draft-pegrum-vmmt-00.txt

Abstract

For many carrier's, the implementation of Virtual Private Network (VPN) services using current IP Tunneling technology is problematic because of onerous configuration requirements. The VPMT is an protocol for the dynammic distribution of VPN information throughout a shared network, which in turn allows the automatic formation of point to multi-point tunnels between VPN routers.

The method described in this internet draft is intended for single AS where the AS administrator is a trusted third party. Traffic seperation is maintained between VPNs.

Table of Contents

1. Introduction

For the purposes of this document, a VPN shall be considered to consist of a grouping of private routers that use a shared tunneled backbone. It is assumed that multiple VPNs use the shared backbone.

Private routers that are members of the same VPN form a peer group. The members of the peer group communicate with each other over a logical shared broadcast medium which is actually the tunnelled backbone simulating a shared broadcast medium for each VPN peer group.

In common tunnel implementations, tunnels are point to point connections where the endpoints are statically configured by the network operator. The VPMT protocol dynamically distributes connection information (tunnel endpoints) between VPN peers throughout a shared network, to allow dynamic establishment of a point to multi-point tunnels. The VPN connection information could include multi-cast information allowing the establishment of multi-point to multi-point tunnels.

Each VPN is identified by a 32 bit VPN identifier (VPNID) that is unique in the shared network, but common to all the routers which belong to the same VPN. Suggested format of the VPNID is 16 bits of AS number and 16 bits VPN number. It is assumed that VPN does not cross boundaries of the AS.

Each VPN peer (router) belonging to a VPN is identified by a 32 bit peer VPN identifier (PEERID) that is unique in the private network, but does not have to be unique in the shared network. This information is not propagated in the network.

The VPN peer connectivity is achieved in two steps:

* discovering the peers in the shared network
* establishment of communication channels between peers

This protocol deals with the dynamic VPN peer discovery in shared network. Suggestions on how to establish the communication channels between peers are given in Section 5.

1.1 Terminology

There is no new terminology introduced by this draft.

2. Address Assignment

Each VPN peer would have assigned a number of addresses as following:

* IP address in shared network -
  In case of non-multicast enabled shared network this address is to be used as a source or destination address in all VPN peer discovery messages.
  In case of the multicast enabled network it is the group multicast address to which the VPN peer belongs.
  This address can also be used to establish VPN peer to peer communication channels, if it is not-multicast address.

* IP address in shared network - (optional)
  This address is being used to establish communication channels between VPN peers, if the VPMT messaging is isolated from the VPN data traffic.

* multiple private IP addresses -
  These addresses are used to establish configuration of the private address space (network).
  The tunnel is not established between two end-points if advertised private interfaces do not belong to the same sub-net.
  There has to be at least one private address assigned to the VPN peer.

3. Routing Updates

No routing information is exchanged between the shared and private networks. Routing updates from the shared network are blocked and not transmitted into the private networks. Conversely, private network updates, even though they are tunnelled across the shared network, are not transmitted into the shared network routing domain.

The VPN peer processes only routing information received from the peer which belong to the same VPNID.

4. VPN Peer Discovery

The VPMT protocol allows VPN peer discovery to run in multicast and non-multicast enabled networks.

New VPN peers joining the VPN immediately issues a VPN Peer Solicitation message to trigger advertisements from other routers on the VPN. In addition, each VPN router periodically issues a VPN Advertisement Message to ensure that VPN integrity is maintained Advertisements are not meant to provide blackhole detection. The Layer 2 tunnel protocol and the VPN routing protocol provide blackhole detection.

After discovering VPN peers connectivity between them is established. The VPN peer configuration information is used by the implemented Layer 2 Tunneling protocol to establish connectivity between VPN peers. The Layer 2 tunneling protocol carries full responsiblity of management of setting-up and tearing down peer connectivity.

ARP entries on VPN peers are refreshed when processing the VPN Advertisement messages received from VPN peers.

4.1 VPN Peer Discovery Algorithm

The algorithm for discovering peers in the shared network for both multicast and non-multicast enabled networks is the same.

Step 1.
Provision set of addresses specified in Section 2 for the VPN peer, and unique VPNID for the VPN .

Provision the following:

1) for multicast enabled networks - multicast address where solicitation and advertisement message are sent
2) for non-multicast enabled networks - provision set of known addresses where the solicitation and advertisement message are sent.

This draft does not deal with the automatic discovery of carrier network configuration for non-multicast enabled networks.

Step 2.
When VPN peer joins the shared network it issues the VPN Solicitation Message which includes the full information about the peer. This message is sent to known address(es).
The acknowledgement to that message comes in the form of a VPN Advertisement Message which contains remote VPN peer configuration data.

Step 3.
On receiving of the VPN Advertisement Message, the following checks are performed:

1) VPNID is checked; in case that the VPNID of the remote peer does not match VPNID of the receiver, the message is not processed
2) each private (address, mask) pair is compared with own private (address, mask) pair; for private interfaces that belong to the same sub-net, the connectivity can be eastablished . The method of setting up-the connectivity depends on the Layer 2 tunneling implementation
3) in case that the peer connectivity is to be established, the shared address of the peer is stored

   It is an implementation detail if the shared address of the peer should be stored in case that the private interfaces do not belong to the same sub-net.

Step 4.
If the VPN peer does not receive any responses for its VPN Solicitation Message, the message is periodically re-sent. The value of the period is provisionable and set by the network administrator.

If peer connectivity is established, the VPN Solicitation message will not be resent.

Step 5.
VPN Advertisement message is sent in two scenarios:

1) as a reply to the peer VPN Solicitation Message
2) periodically sent to known multicast address or set of known destinations

An algorithm to change the advertisement frequency can be implemented in order to lower the requirements on the bandwidth for the messages in stable carier network. The frequency of updates is indicated in the advertisement message generated by the VPN peer.

Step 6.
If the VPN peer disconnects from the network, no action is performed. It is up to Layer 2 tunneling protocol to tear down the connection.

4.2 Multicast Enabled Shared Networks

In multicast enabled shared networks, each VPN peer is required to join the multicast group that is provisioned for its associated VPN.

After joining the multicast group, the VPN peer executes a VPN Peer Router Discovery protocol described in Section 4.1 on that multicast group.

The messages are a combination of VPN discovery and address resolution. The VPN discovery is meant to be a security measure to ensure that all routers that belong to this multi-cast group belong to the same VPN (have the same VPNID). This is intended to guard against configuration errors only. It is assumed that the shared network is secure.

After discovering a VPN peer, the connectivity between them is established by the layer 2 tunneling protocol.

4.3 Non-Multicast Enabled Shared Networks

In non-multicast enabled shared networks, the VPN peer discovery algorithm descibed in Section 4.1 is used.
The destination address to send the VPN Solicitation and Advertisement Message can be one of the following:

* broadcast address instead of a multicast group address
* set of known unicast addresses

If the broadcast address is being used, the limit on the number of broadcast addresses in the network may impose additional VPN peer discovery message processing in order to separate peer configuration data. In this case it is advisable to use separate IP address to establish communication channels between VPN peers.

If the set of unicast addresses is being used, the originating VPN peer would push VPN Solicitation and Advertisement messages to all known destinations. The further refinement of the protocol is an implementation concern.

To propagate peer discovery information in the network the following methods can be used:

1. ICMP messages

2. OPAQUE LSAs
3. TCP connection established between known destinations
4. use of multicast addresses in the network

In Section 6, an example using the ICMP message implementation is given.

5. Peer Conectivity

Peer connectivity phase is responsible for the following:

1) in case that connectivity between peers can be established (same VPNID and interface(s) belong to the same sub-net(s), it handles all actions necessary to create tunnel via carrier backbone (network)
2) in case that connectivity between peers cannot exist anymore, it carries all actions necessary to remove the tunnel via carrier backbone (network)
3) based on the layer 2 media used to esatblish peer connectivity, there can be periodical verification of the tunnel state. This functionality is separate from VPN Peer Discovery phase.

The communication of data between VPN peers througout carrier network can be carried using separate layer 2 media. The following methods of encapsulating VPN data can be used:

1. IP in IP tunnel
2. MPLS
4. IPSec
5. Frame Relay SVCs

This draft does not discuss the options of the peer connectivity establishement and maintenance.

6. Peer Discovery Using ICMP Messages

In this section, the example is given on the use of the ICMP Peer Discovery message to identify VPN peers in order to set-up the connections between them. A new message type is being proposed, which includes all necessary data to identify the peer and set-up the connection.

6.1 Message Formats

The message formats follow standard ICMP type messages. The IP Header is not shown in the diagrams below.

The VPMT protocol proposes to define new ICMP message type VPN Peer

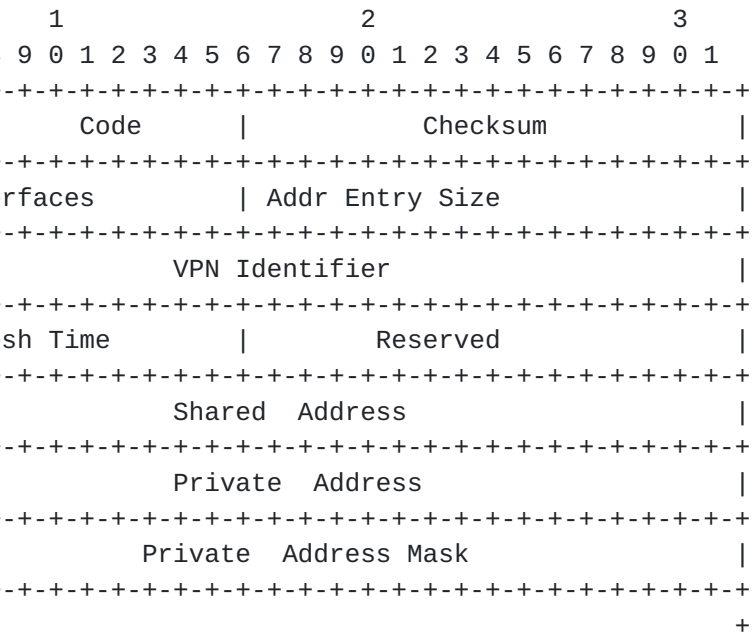
Discovery for messages to dynamically discover VPN peers.
For the VPN ICPM Peer Discovery message the following codes are assigned:

* 1 - VPN solicitation message; this message will invoke the VPN Adverisement message to be sent by the receiving router
* 2 - VPN advertisement message; this message is not acknowledged in any way by the receiving router

The VPN ICMP Peer Discovery message format includes VPN configuration information.

The diagram below illustrates the message format for IPv4 only addresses.

VPN ICMP Peer Discovery Message



IP Header Addresses:

Destination Address:	Shared Network IP Address of the VPN peer; in case of the multicast enabled network it is the group multicast address to which the VPN peer belongs
Source Address:	Shared Network IP Address of the VPN peer

ICMP Fields:

Type:	VPN ICMP Peer Discovery
Code:	value {1, 2}; where: 1 - VPN Solicitation Message

	2 - VPN Advertisement Message
Checksum:	16 bit one's complement of entire message
S (shared)	1 bit format of the shared address: 0 - complies with IPv4 1 - complies with IPv6
P (private)	1 bit format of the private (address,mask) pair: 0 - complies with IPv4 1 - complies with IPv6
Num Interfaces:	14 bit containing number of VPN private interfaces included in this message; interface is desfined by (address, mask) pair
Addr Entry:	Size of (address,mask) pair in 32 bit words
VPN Identifier:	32 bits containing VPNID shared between VPN peers
Refresh Time:	2 bytes of refresh time interval in seconds
Reserved:	2 bytes
Shared address:	VPN peer address in the shared network this address may differ from the source address in IP header. This address specifies communication channel end-point on the source VPN peer.
Private Address:	IP address of the interface to the private network
Private Address Mask:	mask associated with the IP address of the interface to the private network

6.2 IPv6 Compliance

The VPMT protocol can be used in IPv6 . The message format remains the same with respect to fields, however the size of the following fields will, optionally, expand from 32 bits to 128 bits:

* Shared address
* Private address
* Prefix length for the private address mask

The following fields in the ICMP Peer Discovery message will be used to specify the format of the address and appropriate mask:

* shared :
  - 0 - IPv4 format
  - 1 - IPv6 format
* private :
  - 0 - IPv4 format
  - 1 - IPv6 format

The behaviour of the protocol remains unchanged.

7. Summary

VPMT addresses several problems:
- Dynamic VPN endpoint configuration
- Support of Multi-point to Multi-point tunnels
- Security against network operator misconfiguration
- Ensures private network isolation

The VPMT protocol allows for scalable VPN solutions using a common shared infrastructure.

8. Security Considerations

This protocol requires the shared network to be secure and trusted.

The method is intended for a single AS where the AS administrator is a trusted third party.

9. References

[1] S. Deering, Editor, "ICMP Router Discovery Messages", RFC 1256, Xerox PARC, September 1991 [2] S. Hanks et al., "Generic Router Encapsulation", RFC 1701, NetSmiths Ltd & Cisco Systems, October 1994

9. Author's Address

Scott Pegrum
Nortel (Northern Telecom), Ltd.
PO Box 3511 Station C
Ottawa ON K1Y 4H7
Canada

EMail: spegrum@Nortel.ca

Dwieght Jamieson
Nortel (Northern Telecom), Ltd.
PO Box 3511 Station C
Ottawa ON K1Y 4H7
Canada

EMail: djamies@Nortel.ca

Matthew Yuen
Nortel (Northern Telecom), Ltd.
PO Box 3511 Station C
Ottawa ON K1Y 4H7
Canada

EMail: myuen@Nortel.ca

Alicja B. Celer
Nortel (Northern Telecom), Ltd.
PO Box 3511 Station C
Ottawa ON K1Y 4H7
Canada

EMail: aceler@nortel.ca