                  Virtual Private Networks Identifier

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   Virtual Private IP networks may span multiple Autonomous Systems or
   Service Providers. There is a requirement for the use of a globally
   unique VPN identifier in order to be able to refer to a particular
   VPN (see section 6.1.1 of [1]). This document proposes a format for
   a globally unique VPN identifier.

1. Introduction

   As the Public Internet expands and extends its infrastructure
   globally, the determination to exploit this infrastructure has led to
   widespread interest in IP based Virtual Private Networks. A VPN
   emulates a private IP network over public or shared infrastructures.
   Virtual Private Networks provide advantages to both the Service
   Provider and its customers. For its customers, a VPN can extend the
   IP capabilities of a corporate site to remote offices and/or users
   with intranet, extranet, and dialup services. This connectivity
   should be achieved at a lower cost to the customer with savings in
   capital equipment, operations, and services.   The Service Provider
   is able to make better use of its infrastructure and network
   administration expertise offering IP VPN connectivity and/or services
   to its customers.

   There are many ways in which IP VPN services may be implemented. The
   IP based VPN framework document [1] identifies four types of VPN to
   be supported: Virtual Leased Lines, Virtual Private Routed Networks,

Virtual Private Dial Networks, and Virtual Private LAN Segments. In
addition, numerous drafts and white papers outline methods to be used
by Service Providers and/or Service Provider customers to enable this
service. Solutions may be customer based or network based. Network
based solutions may provide connectivity and services at layer 2
and/or layer 3. The devices involved in enabling the solution may be
Customer Premises Equipment (CPE), Service Provider Edge equipment,
Service Provider Core equipment, or some combination of these.

While the various methods of VPN service implementation are being
discussed and debated, there are two points on which there is
agreement:

  Because a VPN is private, it may use a private address space which
  may overlap with the address space of another VPN or the Public
  Internet.

  A VPN may span multiple IP Autonomous Systems (AS) or Service
  Providers.

The first point indicates that an IP address only has meaning within
the VPN in which it exists. For this reason, it is necessary to
identify the VPN in which a particular IP address has meaning, the
"scope" of the IP address.

The second point indicates that several methods of VPN service
implementation may be used to provide connectivity and services to a
single VPN. Different service providers may employ different
strategies based on their infrastructure and expertise. It is
desirable to be able to identify any particular VPN at any layer and
at any location in which it exists using the same VPN identifier.

2. Global VPN Identifier

The purpose of a VPN-ID is to identify a VPN. This identifier may be
used in various ways depending on the method of VPN service
implementation. For example, the VPN-ID may be included:

  - In a MIB to configure attributes to a VPN, or to assign a physical
    or logical access interface to a particular VPN.

  - In a control or data packet, to identify the "scope" of a private
    IP address and the VPN to which the data belongs.

It is necessary to be able to identify the VPN with which a data
packet is associated. The VPN-ID may be used to make this
association, either explicitly (e.g. through inclusion of the VPN-ID
in an encapsulation header [2]) or implicitly (e.g. through inclusion

of the VPN-ID in a ATM signalling exchange [3]). The appropriateness
of using the VPN-ID in other contexts needs to be carefully
evaluated.

There is another very important function that may be served by the
VPN identifier. The VPN identifier may be used to define the "VPN
authority" who is responsible for coordinating the connectivity and
services employed by that VPN. The VPN authority may be the Private
Network administrator or the primary Service Provider. The VPN
authority will administer and serve as the main point of contact for
the VPN. The authority may outsource some functions and
connectivity, set up contractual agreements with the different
Service Providers involved, and coordinate configuration,
performance, and fault management.

These functions require a VPN that is global in scope and usable in
various solutions. To be a truly global VPN identifier, the format
cannot force assumptions about the shared network(s). Conversely, the
format should not be defined in such a way as to prohibit use of
features of the shared network. It is necessary to note that the
same VPN may be identified at different layers of the same shared
network, e.g. ATM and IP layers. The same VPN-ID format and value
should apply at both layers.

The methods of VPN-ID usage are beyond the scope of this memo.

3. Global VPN Identifier Format Requirements

   The VPN Identifier format should meet the following requirements:

    - Provide a globally unique VPN Identifier usable across
      multiple Service Providers.
    - Enable support of a non-IP dependent VPN-ID for use in
      layer 2 VPNs.
    - Identify the VPN Authority within the VPN Identifier.

4. Global VPN Identifier Format

   The global VPN Identifier format is:

     3 octet VPN authority Organizationally Unique Identifier [4]

   followed by

     4 octet VPN index identifying VPN according to OUI

```
0 1 2 3 4 5 6 7 8
+-+-+-+-+-+-+-+-+
| VPN OUI (MSB) |
+-+-+-+-+-+-+-+-+
|    VPN OUI    |
+-+-+-+-+-+-+-+-+
| VPN OUI (LSB) |
+-+-+-+-+-+-+-+-+
|VPN Index (MSB)|
+-+-+-+-+-+-+-+-+
|   VPN Index   |
+-+-+-+-+-+-+-+-+
|   VPN Index   |
+-+-+-+-+-+-+-+-+
|VPN Index (LSB)|
+-+-+-+-+-+-+-+-+
```

The VPN OUI (IEEE 802-1990 Organizationally Unique Identifier) [4]
identifies the VPN authority. The VPN authority will serve as the
primary VPN administrator. The VPN authority may be the
company/organization to which the VPN belongs or a Service Provider
that provides the underlying infrastructure using its own and/or
other providers' shared networks. The 4 octet VPN Index identifies a
particular VPN serviced by the VPN authority.

5. Security Considerations

   This document defines the format of the global VPN identifier without
   specifying usage. However, the association of particular
   characteristics and capabilities with a VPN identifier necessitates
   use of standard security procedures with any specified usage.
   Misconfiguration or deliberate forging of VPN identifier may result
   different breaches in security including the interconnection of
   different VPNs.

6. References

   [1] Gleeson, Heinanen, Lin, Armitage, Malis, "A Framework for IP
       Based Virtual Private Networks", Work in Progress.

   [2] Grossman, D. and J. Heinanen, "Multiprotocol Encapsulation over
       ATM Adaptation Layer 5", RFC 2684, September 1999.

   [3] "MPOA v1.1 Addendum on VPN Support", ATM Forum, af-mpoa-0129.000,
       August, 1999, Bernhard Petri, editor, final ballot document.

   [4] http://standards.ieee.org/regauth/oui/index.html

7. Authors' Addresses

Barbara A. Fox
Lucent Technologies
300 Baker Ave, Suite 100
Concord, MA   01742-2168

Phone: +1-978-287-2843
EMail: barbarafox@lucent.com

Bryan Gleeson
Nortel Networks
4500 Great America Parkway,
Santa Clara, CA   95054

Phone: +1-408-855-3711
EMail: bgleeson@shastanets.com

8. Full Copyright Statement

Acknowledgement