Internet Engineering Task Force
INTERNET-DRAFT

Expires December 2003

J. Sumimoto
NTT
M. Carugi
Nortel Networks
(Co-editors)

J. De Clercq
Alcatel
A. Nagarajan
Consultant
M. Suzuki
NTT

June 27, 2003

Guidelines of Applicability Statements for PPVPNs
<draft-ietf-l3vpn-applicability-guidelines-00.txt>

Status of this Memo

Abstract

This document plays a role of guidelines to assist development of applicability statements for each specific Layer 2 and Layer 3 PPVPN approach. It provides a check-list which consists of metrics, each of which is intended to clearly point out what must be evaluated and written in each approach specific applicability statement document.

1. Introduction

The term Provider Provisioned Virtual Private Network (PPVPN) refers to Virtual Private Networks (VPNs) for which the service provider participates in management and provisioning of the VPN. PPVPNs can be classified into various PPVPN types based on their characteristics, and requirements for PPVPNs are described in three separate documents, [GEN REQTS], [L3 REQTS], and [L2 REQTS]. This document extracts metrics directly relating to protocols/mechanisms out of provider/service/engineering requirements for PPVPNs described in the three requirements documents so as to make approach specific applicability statements significant. The extracted metrics in this document form a check-list, each of which is intended to clearly point out what must be evaluated and written in each approach specific applicability statement document. Detailed description with regard to the metrics is out of scope of this document. Section 2 reviews taxonomy of PPVPN types for which metrics are listed in this document. Section 3 provides list and outline of metrics. Section 4 is for security considerations, Section 5 is for acknowledgement and section 6 is for references.

2. Taxonomy of PPVPNs

The terminology used in this document is defined in [TERMINOLOGY].

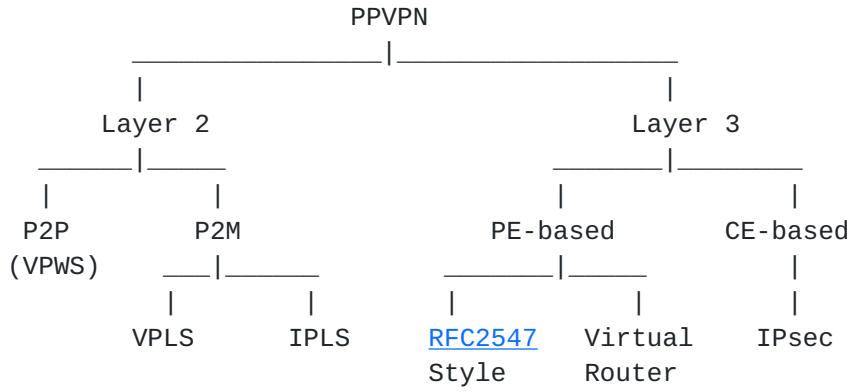

Figure. 2.1 PPVPN taxonomy

The figure above presents taxonomy of PPVPN approaches. Note that CE-based Layer 2 PPVPNs may also be further classified as point-to-point (P2P) or point-to-multipoint (P2M), and P2M PPVPNs may also be further classified as Virtual Private LAN Service (VPLS) and IP-only LAN-like Service (IPLS). Definitions for layer 3 PPVPNs can be obtained from [L3 FWK] and definitions for layer 2 PPVPNs can be obtained from [L2 FWK].

3. List and outline of metrics for evaluating each PPVPN approach

This section provides list and outline of metrics generic to L3 and L2 PPVPN approaches (in Section 3.1), specific to L3 PPVPN approaches (in Section 3.2) and specific to L2 PPVPN approaches (in Section 3.3). Each L3 PPVPN approach is to be evaluated by using both generic and L3 specific metrics. Similarly, each L2 PPVPN approach is to be evaluated by using both generic and L2 specific metrics. In this document, AS stands for Applicability Statements.

3.1 Generic metrics

This section provides metrics generic to layer 3 and layer 2 PPVPN approaches.

3.1.1 Isolated exchange of routing and data information

Each specific AS document must clarify whether and how the following attributes are implemented by the concerned PPVPN approach.

- Isolated data forwarding (mandatory)

- Isolated routing (i.e. constrained distribution of reachability to only VPN sites)
  (Internal topology of VPN should not be visible to the shared public network (Internet))

3.1.2 Security

Each specific AS document must clarify whether and how the following attributes of user security are supported by the concerned PPVPN approach.

- Confidentiality

- Integrity

- Authentication

- Replay attack prevention

Additionally, each specific AS document must clarify how the following security attributes with regard to setup/operation are protected by the concerned PPVPN approach.

- Protocol attacks

- Unauthorized access

- Tampering with signaling

3.1.3 Tunneling

Each specific AS document must clarify the following attributes.

- Kind of supported tunneling techniques
- Tunnel termination points

3.1.4 QoS

Each specific AS document must clarify if the following types of QoS are supported or not, and how they are supported.

- Intserv/RSVP (Customer usage/Provider usage)
- Diffserv (Customer usage/Provider usage)
- Point to point
- Point to cloud

3.1.5 Auto-discovery

Each specific AS document must clarify

- Whether any mechanism are supported or not

  If supported, it must also clarify the following attributes.

- Kind of mechanism
- What is discovered by the mechanism
- Information exchanged by the mechanism

3.1.6 Scalability

With regard to each of the following factors, each specific AS document must clarify (1) what resource is pressed by the factor (e.g. VFI's table size) and (2) how (in what order) is the resource pressed? (E.g. O(n) or O(n^2) or ...). VFI stands for Virtual Forwarding Instance, and VSI stands for Virtual Switching Instance (for more detail, see framework documents).

- Number of VPNs
  (Especially, influence toward VFI/VSI's table size / number of tunnels should be considered.)

- Number of sites
  (Especially, influence toward VFI/VSI's table size / number of tunnels should be considered.)

- Number of routes per VPN

- Rate of configuration changes / impact of adding new site
  (Especially, influence toward increase of controlling traffic / average convergence time should be considered.)

- Number of users per VPN

- Number of addresses per VPN

- Number of PEs and/or CEs

- Number of VRFs/VRs and interfaces per PE (for only PE-based L3 VPN approaches),
  (Especially, influence toward processing overhead of a PE should be considered.)

- Number of tunnels

3.1.7 Management

Each specific AS document must clarify (1) whether each of the following aspects of management are supported or not by the concerned PPVPN approach, and (2) how they are supported.

- Configuration/Provisioning
  VPN membership, tunnels, network access, routing protocols, etc.

- Performance/SLA
  Monitoring/Accounting states and statistics.

- Security
  Access control, authentication, etc.

- Fault
  Detection, localization, and corrective actions.

- Customer Management
  Capabilities of customers to view the topology, operational state, order status, and other parameters associated with their VPN

3.1.8 Traffic types

Each specific AS document must clarify whether and how the following

types of traffic are supported or not.

- Unicast or point-to-point

- Multicast or point-to-multipoint

- Broadcast

3.1.9 Temporary access

Besides permanent access which is mandatory to all PPVPN approach, each specific AS document must clarify (1) whether supported or not, and (2) how to support,

- Temporary access

3.1.10 Migration impacts

Each specific AS document must clarify

- Functions required to be added to legacy devices from the customers' and providers' point of view.

3.1.11 Interworking

Interworking scenarios among different solutions providing PPVPN services is highly desirable. If any constraints exist in a PPVPN approach, the corresponding specific AS document must show the constraints and their influence.

3.2 Metrics specific to L3 PPVPN approaches

This section provides metrics specific to L3 PPVPN approaches. Each specific L3 PPVPN approach must be checked by these L3 specific metrics as well as generic metrics provided in the former sections.

3.2.1 Addressing

Each specific AS document must clarify whether overlapping customer IP addresses in different VPNs are supported or not.

3.2.2 IP Routing Protocol Support for Customer

At least the following protocols must be supported between CE and PE routers, or between CE routers: static routing, IGP, such as RIP, OSPF, IS-IS, and BGP. If there exists any restriction in a PPVPN approach, it must be described in the specific AS document concerning the PPVPN approach.

3.2.3 Core network requirements

Each specific AS document must clarify the following attributes of concerned PPVPN approach.

- Routing protocols applicable to SP network routing

- Core router awareness of mechanisms used

3.3 Metrics specific to L2 PPVPN approaches

This section provides metrics specific to L2 PPVPN approaches. Each specific L2 PPVPN approach must be checked by these L2 specific metrics as well as generic metrics provided in the former sections. VPLS stands for Virtual Private LAN Service (for more detail, see [L2 FWK]).

3.3.1 Scope/Accuracy of Emulation

Each specific AS document must clarify the following attributes of concerned PPVPN approach.

- Difference between L2 VPN protocol and specification at customer interface and existing native protocols and specification (if exists)

3.3.2 Addressing

Each specific AS document must clarify

- Whether overlapping customer L2 addresses in different VPNs are supported or not

- Whether overlapping VLAN IDs for different customer are supported or not (in case of VPLS supporting VLANs)

3.3.3 Loop Prevention of L2 topology

Each specific AS document must clarify

- Whether any mechanism are supported or not. (Especially, is STP supported?)

  If any mechanism supported, it must also clarify the following attributes.

- Kind/scope of the mechanism. (Especially, is STP supported? Is Split horizon scheme over mesh topology adopted?)

3.3.4 Packet re-ordering

Each specific AS document must clarify the following attributes.

- Possibility of packet re-ordering

- Influence of packet re-ordering

3.3.5 Minimum MTU

Each specific AS document must clarify the following attributes.

- Support of MTU specified for the layer 2 technology
  (including consistency with inserting VLAN tag)

- Guarantee of prohibition of frame fragmentation

3.3.6 Support for MAC Services (only for VPLS)

Each specific AS document must clarify whether MAC services (see the following examples) are supported or not by the concerned PPVPN approach.

- Filtering of frames

- Flooding

- Creation of address table

- Aging of address table

If any constraints exist in a PPVPN approach, the corresponding specific AS document must show the constraints and their influence.

3.3.7 Scalability

L2 specific scalability metrics are listed in this section. For generic scalability metrics, see section 3.1.6.

Each specific AS document must clarify scalability concern specific to L2 VPN control protocol including signaling. Especially, scalability concern caused by use of STP must be clarified in case of VPLS.

4. Security considerations

There are no additional security considerations besides those already described in this document.

5. Acknowledgments

The authors of this document would like to acknowledge the suggestions and comments received from the entire Layer 3 Applicability Statement Design Team formed in the ppvpn WG. Besides the authors, the members of the design team include Luyuan Fang, Paul Knight, Dave McDysan, Thomas Nadeau, Olivier Paridaens, Yakov Rekhter, Eric Rosen, Chandru Sargor, Benson Schliesser, Cliff Wang and Rick Wilder.

6. References

6.1 Normative References

[GEN REQTS] Nagarajan, A., "Generic Requirements for Provider Provisioned VPN," Work in Progress.

[L3 REQTS] Carugi, M. et al., "Service Requirements for Provider Provisioned Virtual Private Networks," work in progress.

[L2 REQTS] Augustyn, W., Serbest, Y., et al., "Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks", work in progress

[TERMINOLOGY] Andersson, L., Madsen, T., "PPVPN Terminology", work in progress.

6.2 Informative References

[L3 FWK] Callon, R. et al., "A Framework for Provider Provisioned Virtual Private Networks," work in progress.

[L2 FWK] Andersson, L., et al., "L2VPN Framework", work in progress.

[IPsecVPN AS] De Clercq, J. et al., "Applicability Statement for Provider Provisioned CE-based Virtual Private Networks using IPsec," work in progress.

[VR AS] Nagarajan, A. et al., "Applicability Statement for Virtual Router-based Layer 3 PPVPN approaches," work in progress.

[2547BIS AS] Rosen, E. et al., "Applicability Statement for VPNs Based on rfc2547bis," work in progress.

7. Authors' address

Junichi Sumimoto (Co-editor)
NTT Information Sharing Platform Labs.

3-9-11, Midori-Cho
Musashino-Shi, Tokyo 180-8585 Japan
Email: sumimoto.junichi@lab.ntt.co.jp

Marco Carugi (Co-editor)
Nortel Networks S.A.
Parc d'activites de Magny - Les Jeunes Bois - Chateaufort
78928 YVELINES Cedex - FRANCE
Email: marco.carugi@nortelnetworks.com

Jeremy De Clercq
Alcatel
Fr. Wellesplein 1, 2018 Antwerpen, Belgium
Email: jeremy.de_clercq@alcatel.be

Ananth Nagarajan
Consultant
Email: ananth@maoz.com

Muneyoshi Suzuki
NTT Information Sharing Platform Labs.
3-9-11, Midori-cho,
Musashino-shi, Tokyo 180-8585, Japan
Email: suzuki.muneyoshi@lab.ntt.co.jp