White Paper: The Opportunities for Multi-Domain VPN services in GÉANT

Authors: Xavier Jeannin, Karl Meyer

Date: 16 May 2014

Table of Contents

1. Summary 3
1.1. VPN vs Private Networks 3
2. GÉANT VPN services positioning 6
2.1. VPN Service Portfolio 6
2.2. Service Summary 6
3. Difference between GÉANT VPN services 9
4. User Audience 10
4.1. Use Cases for GÉANT MD-VPN 10
5. GÉANT MD-VPN Benefit Summary 12
6. Appendix 1 MD-VPN service Outline technical description 13
6.1. End-to-End service 13
6.2. VPN multiplexing feature 13
6.3. VPN-Proxy 13

1. SUMMARY

The use of TCP/IP networking is now virtually ubiquitous, with virtually every application and system using the core networking technology to help intercommunication. Without the global acceptance of TCP/IP and the core underlying technologies, it is unlikely that the levels of collaboration in the Research and Education community would have been possible.

For the majority of users the open, best efforts, minimal network level security operation of IP networking are sufficient. The high performance networks delivered by NRENs and GÉANT offer levels of capacity, speed and reliability that were unimaginable 10 years ago and the development of application and protocol level security and encryption provides privacy and security for the majority of applications.

However for a significant number of applications and projects there exists a need to provide enhanced levels of assurance and performance in addition to those provided by standard IP connectivity. It is this type of application that Virtual Private Networks (VPNs) - using either Layer3 IP connectivity or Layer 2 services have been developed for.

For many advanced projects or virtual organisations VPNs offer a solution to their national and international connectivity requirements and these services offer a valuable opportunity for GÉANT to demonstrate value add in the marketplace. Layer 2 based connectivity services are also in demand for scientific research projects

1.1. VPN vs “Private” Networks

VPNs offer an intermediate between fully “private” networks and the use of shared IP networking.

Within a private network each new site or location (or even system) requires a new separate private circuit to be used (either as a physical circuit or a Layer 2 virtual circuit). As the number of sites connected increases then the complexity and cost of these circuits rises exponentially. Even when using virtual L2 Point to Point circuits, the complexity and support costs increase as the number of sites increases.

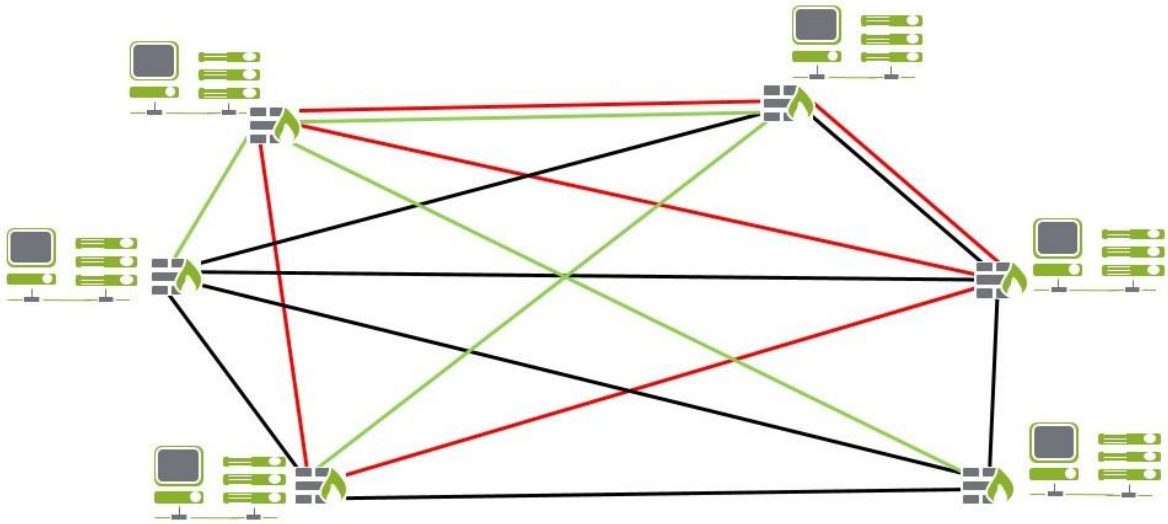

Figure 1 – provisioning of multiple private network infrastructures (either physical circuits or L2 virtual circuits)

In addition to the cost and complexity of the network comes the delays in connecting sites and the need to manage multiple service contracts. This is of particular importance when sites need to be connected only for short periods of time or may require low levels of performance for most of the time and rarely need higher performance. The over-specifying of network capacity can create substantial additional costs for projects and may prevent some organisations taking part in research due to lack of funding.

Virtual private networks reduce the barriers to entry for these projects and increase the flexibility of networking.

By using a common core network platform and logically separating traffic on a shared physical connection it is possible to provide a service functionally equivalent to private networking whilst maximizing the utilization of existing network provisioning.

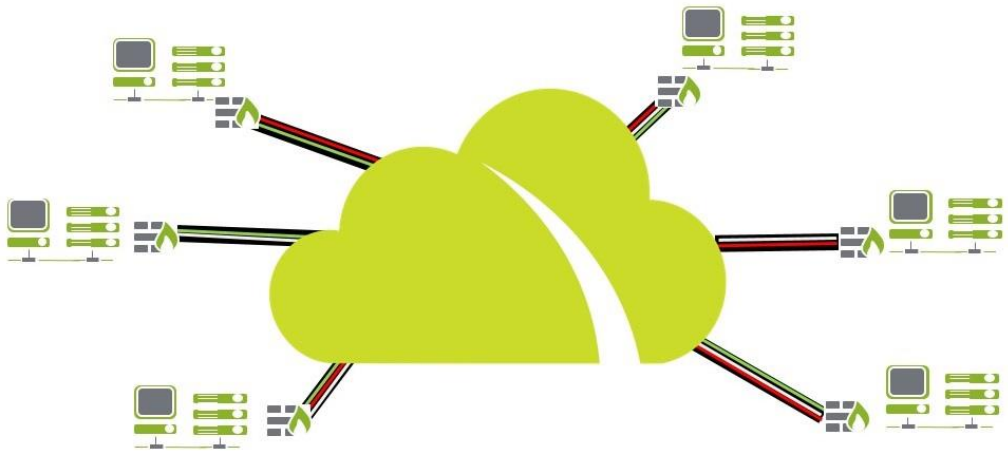

Figure 2 – Provisioning of multiple VPN services using IP backbone infrastructure

Because the connectivity is shared and is only logically isolated the services can be increased in capacity or decreased on an as required basis.

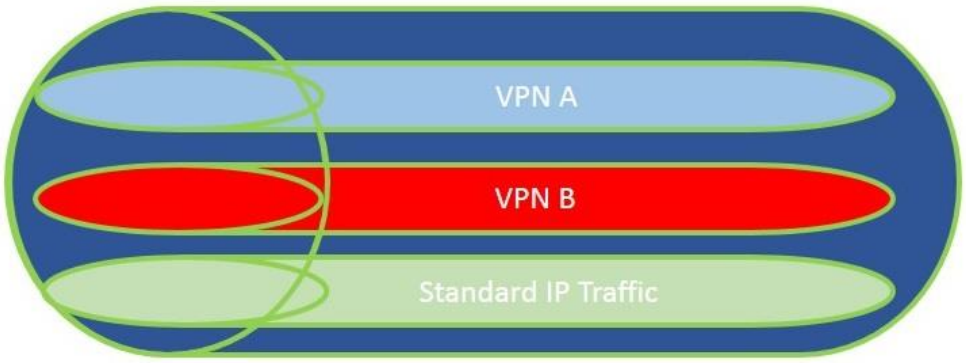

Figure 3 – Bandwidth sharing across shared IP resource

Benefits summary;

- IP networks are shared by all the users and so are “public”
- Private (point to point) networks have hardware and circuits dedicated solely to their users
- A Virtual Private Network (VPN) – either L3 or L2, uses shared hardware and circuits but is logically divided rather than physically separated (making it virtual)
- A VPN gives the flexibility of a shared network with most of the privacy and performance of a private network.

It is for these key reasons that VPN services are considered to be a core element of the value added services portfolio of GÉANT and the NRENs.

2. GÉANT VPN SERVICES POSITIONING

The marketplace for VPN services in the R&E sector is wide and diverse with requirements ranging from point-to-point high capacity services, through hub and spoke network configurations and multi-site peer-to-peer requirements and any combination and permutation of connectivity. Therefore it is necessary to consider the provision of different service models for VPN provisioning to support the full spectrum of user requirements.

2.1. VPN Service Portfolio

GÉANT proposes to offer a range of VPN services focused on a set of user needs. By dividing the spectrum of user scenarios into clearly defined (though overlapping) services it will be possible to ensure maximum support for the users. This customer focus is essential to maintain the end user service ethos of GÉANT and the NRENs. These services will share some core provisioning and support frameworks to maximise the return on investment in application and software development and reduce support overhead.

The decision to provide a degree of service feature overlap between different service offerings is a considered and deliberate approach. Without some level of service overlap there would exist the potential risk that some, currently unknown, user requirement could not be met by the GÉANT portfolio. The aim therefore is to ensure that a service or combination of services will meet the user needs rather than having to constrain the user requirement to fit within a subdivided service portfolio.

The three top level service divisions will be

- GÉANT Plus
- GÉANT L3-VPN
- GÉANT MD-VPN

These services provide a connectivity among project participants dispersed across multiple locations via the GÉANT and NRENs networks. These services as all services delivered by GÉANT fall in a scope of user to user connectivity, meaning that the service delivered will be not used by NRENs directly but delivered by the NRENs or the Regional Network (RN) to end-users.

It is important to note that, from the end-users point of view, these services delivered seamlessly from end-to-end. They differ from the NREN point of view in the way that they are co-delivered by GÉANT and the NREN and service demarcation points.

2.2. Service Summary

L3VPN service

The L3VPN GÉANT service aims to allow the deployment of L3VPN multi-domain within the NREN domains. The service is delivered in IP packets form over dedicated BGPs peering on the NREN interface and requires a manual configuration on side of the NREN interface for each L3VPN and for each involved NREN.

GÉANT plus service

GÉANT Plus offers point to point layer 2 connectivity (i.e. Point-to-Point L2VPN). It is delivered in 802.1q packet form over dedicated VLANs on the NREN interface.

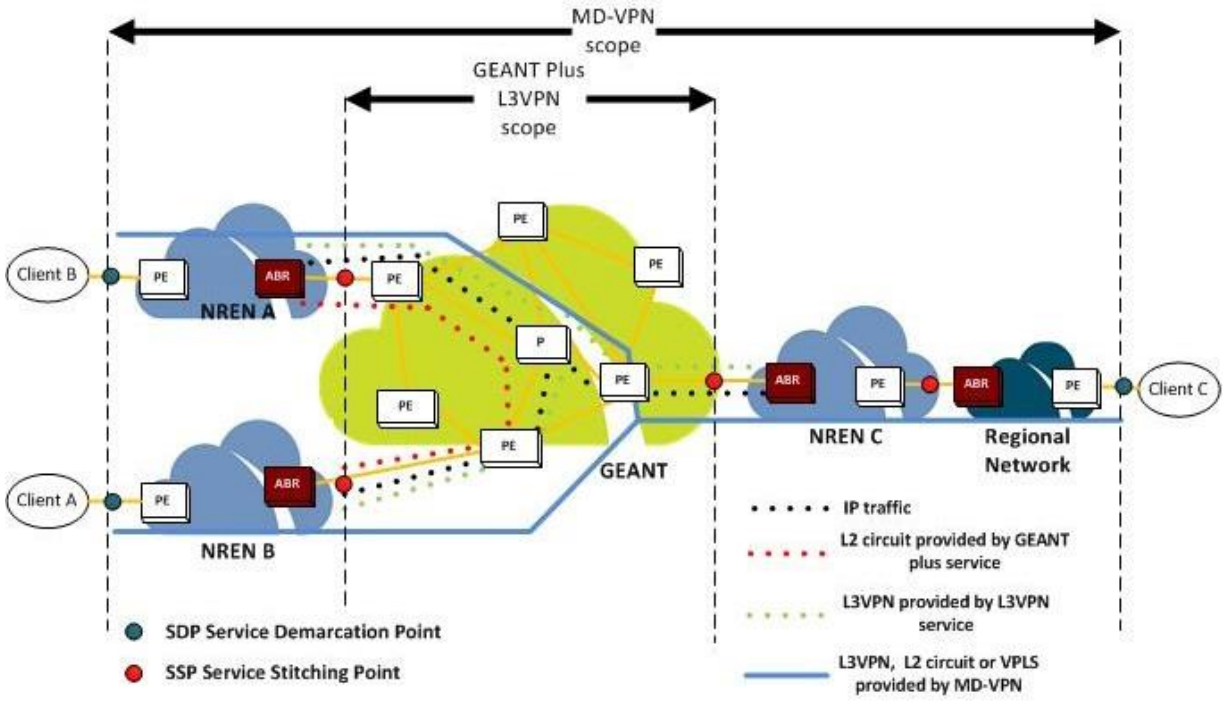

Figure 4- GÉANT VPN services

GÉANT MD-VPN service

The GÉANT MD-VPN service is designed to offer a range of end services across a common delivery platform. The services will include**:**

- **L3VPN,**
- **P2P-L2VPN (L2 P2P circuit),**
- **MP-L2VPN (VPLS).**

In contrast to the L3VPN and GÉANT Plus services, MD-VPN is delivered jointly with NRENs with a service demarcation point which is extended to the boundary between the end user and the host NREN.

MD-VPN will offer an end-to-end service through the use of “Service Stitching Points” (SSPs) these will be located at the interface between the GÉANT network and the NREN and will provide the interface between the networks.

Across the GÉANT network, the MD-VPN service will deliver MPLS packet over a BGP labeled Unicast peering on the NREN interface. The SSP will provide access to all services supplied by the MD-VPN service and is set-up once. Due to the configuration of the Unicast BGP peering, NRENs are then free to create as many end user VPNs as required, without any new configuration between them and GÉANT needed. This greatly simplifies the process of VPN creation and allows for a highly scalable implementation and support process.

Service Demarcation

GÉANT plus and L3VPN deliver their service at the border of GÉANT whereas MD-VPN aims to provide the service at end user site (end-to-end service).

“Out of Area” VPNs

One of the primary limitations of VPNs has always been the difficulty in connecting the “out of area” sites that are served by non-participating networks. Often these outlying sites have been so difficult to connect that the overall business case for the VPN fails.

MD-VPN has been designed to enable these sites to be connected into the overall VPN platform in a cost effective manner.

This uses a VPN-Proxy to act as a gateway point into the MD-VPN service for NRENs that are not MPLS enabled.

Through this proxy, the MD-VPN is able to deliver both L3VPN and point-to-point layer 2 circuit services (i.e. Point-to-Point L2VPN) and the proxy acts as the service demarcation point for the VPN service.

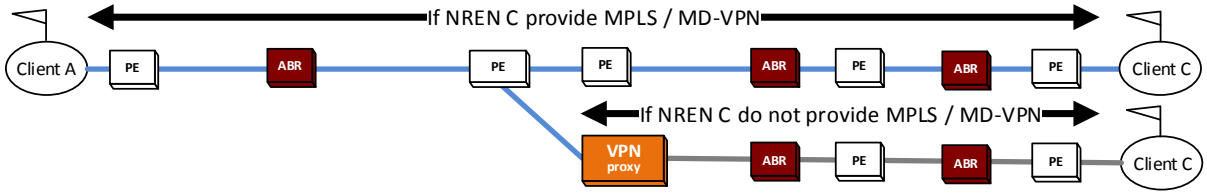

Figure 5 - VPN-Proxy usage in MD-VPN service

3. DIFFERENCE BETWEEN GÉANT VPN SERVICES

All three GÉANT VPN services operate using the same VPN over MPLS platform and are delineated by the usage, scope and service demarcation points. The following table details the delivery and implementation differences between the VPN services

Service***	GÉANT Plus	GÉANT L3VPN	GÉANT MD-VPN
Scope – service delivery demarcation	GÉANT Border	GÉANT Border	**End-to-End**
How the service is delivered to the NRENs?	On NREN interface 802.1q – (VLAN)	Over NREN IP service interface	On NREN interface MPLS or with VPN-Proxy: IP, 802.1q – (VLAN)
Implementation	Manual configuration for each circuit / P2P L2VPN	Manual configuration at each connection points of the VPN	**Endpoint configuration only**
GÉANT Implementation time	Delivered on an existing interface 5 days and 10 weeks on a new interface	Delivered on an existing interface 5 days and 10 weeks on a new interface	**Automatic for subscribed NRENs** – NREN endpoint delivery subjtect to NREN scheduling
Robustness	Automated re-routing and recovery	Automated re-routing and recovery Backup access possible	Automated re-routing and recovery Backup access possible
High Capacity	up to 100Gbps		
Reliability	up to 99.999% availability		up to 99.999% availability*
QoS and Bandwidth guarantee	Best effort Possible with dedicated interface	Best effort Possible with dedicated interface	Best effort **

* *Reliability expected, not proofed so far, still in pilot phase*

** *Bandwidth guarantee will be studied during GN4, same constraints are expected than for L3VPN and GÉANT Plus*

*** *As GÉANT Plus and L3VPN services deliver the service at GÉANT border. In order to compare these three services, this comparison takes in consideration only the GÉANT part of the MD-VPN service.*

4. USER AUDIENCE

The three services are targeted at different audience types and can deliver a variety of end-user benefits.

Features	GÉANT Plus	GÉANT L3VPN	GÉANT MD-VPN
Layer 3 VPN Facility		X	X
Point-to-point circuits / P2P L2VPN	X		X
Multi-Point L2VPN / VPLS			X

GÉANT Plus can be used to deliver P2P circuit – P2P L2VPN

- If the service has to be delivered strictly at the border of the GÉANT;
- If one NREN does not want to use MD-VPN according to their network policy;
- If MD-VPN is not available.

L3VPN can be used to deliver L3VPN

- If the project require that the service is delivered strictly at the border of the GÉANT but if only few points require a delivery at GÉANT border the MD-VPN with VPN-Proxy could be better;
- If MD-VPN is not available.

MD-VPN can be used to deliver P2P-L2VPN (L2 P2P circuit), MP-L2VPN (VPLS), L3VPN

- As MD-VPN is cheaper and offer a faster deployment, it should be preferred when he is available. Even if one NREN is not available, the VPN-Proxy can allow it to let the other partners of the VPN to use MD-VPN.

MD-VPN is able to provide the same services as GÉANT Plus and GÉANT L3VPN but with the benefit of removing the need for manual configuration between GÉANT, NRENs and RN. This reduces delivery lead time and operating, support and implementation cots for NRENs, RNs and GÉANT.

GÉANT plus and GÉANT L3VPN deliver their service between NRENs whereas MD-VPN aims to deliver the service at the border between NRENs and end users. MD-VPN is not designed to deliver at the service the border of GÉANT. Therefore the continued use and support of GÉANT Plus and GÉANT L3VPN is recommended to provide clear delineation between end use and NREN focused services. In addition, because MD-VPN requires close technical collaboration between NRENs and between NRENs and GÉANT and extends the Service Demarcation Points to the boundaries of third party networks this could lead to some NRENs being initially unwilling to take part in the service. This will then further the need to maintain GÉANT Plus and GÉANT L3VPN services to support these NRENs and their users.

4.1. Use Cases for GÉANT MD-VPN

There is a wide scope for GÉANT MD-VPN use, from the long-term infrastructure with intensive network usage to quick point-to-point services for a conference demonstration. The following cases give examples of how GÉANT MD-VPN can be used to support R&E collaboration;

- **International Collaboration** - Universities, labs and all scientific projects based on international collaboration will benefit from the use of GÉANT MD-VPN services as the end-to-end service demarcation and the ability to support “out of area” connections improve ease of use. LHCONE, ITER and CONFINE are examples of success. Future Internet projects are also target users for GÉANT MD-VPN using proxy services to provide outreach.
- **Ad hoc P2P connections** - For example conference demonstrations or P2P data transport between sites needed only rarely and only for short periods of time. The rapid deployment of VPNs will enable such projects to take advantage of the service whereas the time for deployment of earlier services would have been prohibitive.
- **Distributed Infrastructure Services -** Cloud service providers, Grid and HPC centres could offer services across VPNs to increase service assurance and to separate traffic flows for management and (possibly) billing purposes
- **Scientific Infrastructure –** GÉANT MD-VPN is ideally suited to hub and spoke network structures enabling access to centralised infrastructure projects. Also distributed networking for remote sensors could benefit from higher levels of assurance offered by VPNs
- **Education –** Ad hoc and semi-permanent VPNs can provide linkages between school and campus networks in a clearly separated manner. This can be used to support outreach projects and collaboration.
- **Transparent Transport Services** - As GÉANT MD-VPN can provide a transparent data transport, it can be used by high level network services like SDN, BoD and in general by future internet projects**.**

5. GÉANT MD-VPN BENEFIT SUMMARY

GÉANT MD-VPN as an addition to the GÉANT connectivity services portfolio is an essential added value services for GÉANT, NRENs and end users. It provides an enhancement to the offerings to end-users by providing a “seamless” VPN experience across multiple NRENs further improving international collaboration and enabling a wide range of innovative uses for the network infrastructure.

The benefits to NRENs for adopting this service can be summarised as:

- **OPEX saving** thanks to its VPN multiplex feature and by avoiding manual configuration between NRENs and GÉANT, and between NRENs and RNs;
- **NO CAPEX** is required as it relies on the reuse of standard features already available in NREN routers;
- **Differentiation** - NRENs provides an original service that cannot be provided by commercial telecoms as GÉANT MD-VPN is based on collaboration between domains – This provides a value add for NRENs in comparison to local telco organisations.
- **Assurance** - MD-VPN offers a safer environment for education and research network
    - Mitigate the risk by providing a closed network for science collaboration;
    - Save security CAPEX (avoiding firewall) and OPEX on end-users site;
    - High network performance by avoiding firewall usage;
- **Flexibility** – GÉANT MD-VPN offers a new way for the NRENs to propose a bundle of useful services that covers a wide scope of their user needs
    - Reduced lead time to provision services assists ad hoc and short period projects.
    - All types of site can be connected, using multiple access and solutions.

6. APPENDIX 1 MD-VPN SERVICE OUTLINE TECHNICAL DESCRIPTION

MD-VPN service **provides a bundle of services:**

L3VPN, P2P-L2VPN (L2 P2P circuit) (Kompella or Martini), MP-L2VPN (VPLS).

6.1. End-to-End service

MD-VPN is delivered jointly with NRENs. In the standard usage way of MD-VPN, GÉANT delivers to NRENs VPNs over MPLS at a Service Stitching Point (SSP). The GÉANT MD-VPN delivered MPLS packet over a BGP peering on the NREN interface. Then the NRENs deliver the VPNs to the end-users at a Service Demarcation Point (SDP).

The service can be extended in order to reach the end-users by building a new SSP between NRENs and regional networks (RN). **GÉANT MD-VPN is a seamless infrastructure**, all the NREN domains crossed are transparent. For instance, if a VPN is created between a RN in France and Finland (FUnet), the NRENs RENATER, GÉANT and NORDUnet are completely transparent for French RN and FUnet.

6.2. VPN multiplexing feature

The SSP provides access to all services supplied by MD-VPN and **is set-up only once** thanks to a new BGP peering (Labeled Unicast) over the NREN interface.

The NRENs are then free to create as many VPNs as they want, without any new configuration between them and GÉANT reducing OPEX for NRENs and GÉANT. The only configuration required to deliver a new VPN to the end-users is made on the edge routers, and thus the lead time for delivering a multi-domain VPN is very short

6.3. VPN-Proxy

Thanks to the VPN-Proxy, GÉANT MD-VPN service is also capable to deliver L3VPN in IP packets form over dedicated BGPs peering and point to point layer 2 circuit (i.e. Point-to-Point L2VPN) in 802.1q packets form over dedicated VLANs (as L3VPN and GÉANT plus service).

VPN provided by MD-VPN can be stitched with external VPN like it is usually done with L3VPN and GÉANT plus service.

The usage of VPN-Proxy allows to connect NRENs that are non MPLS enabled but we lose where it is used, the MD-VPN advantages (VPN multiplexing and seamless infrastructure).

Thanks to VPN-Proxy, we are able to connect all types of all site, so it is not required that all client sites need to be connected to a MD-VPN NREN to deploy a VPN thanks to MD-VPN service.

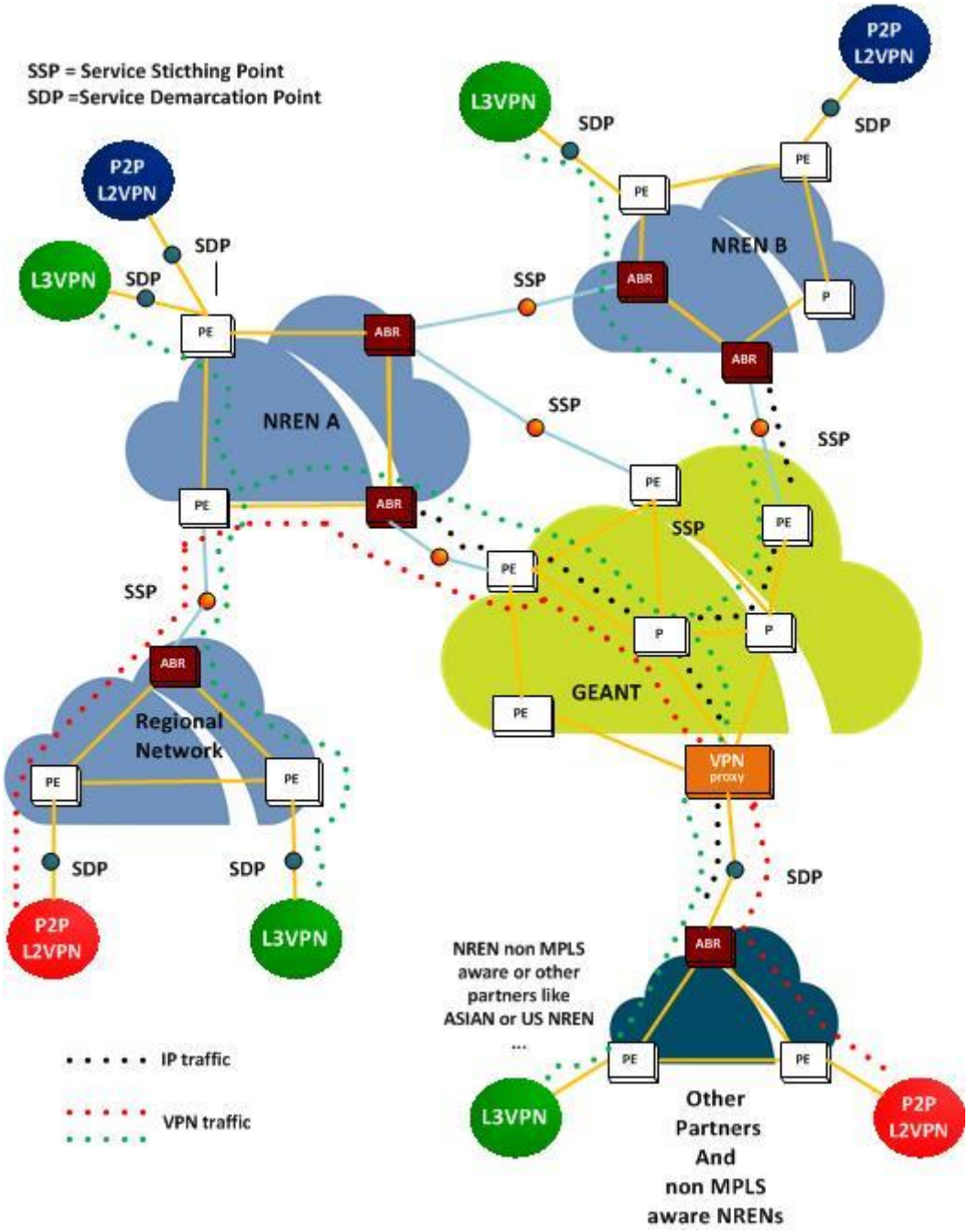

Figure 6: MD-VPN service summary

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of DANTE and can under no circumstances be regarded as reflecting the position of the European Union.