11-10-2013

Deliverable D7.1 (DS3.3.1): MDVPN Service Architecture

Deliverable DS.3.3.1

Contractual Date:	30-09-2013
Actual Date:	11-10-2013
Grant Agreement No.:	605243
Work Package/Activity:	SA3
Task Item:	3
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	RENATER
Document Code:	GN3PLUS13-400-47
Authors:	Tomasz Szewczyk (PSNC), Xavier Jeannin (RENATER), Jovana Palibrk (AMRES), Bojan Jakovljevic (AMRES), Thomas Schmid (DFN), Carlos Friaças (FCCN), Pavle Vuletic (AMRES), Dusan Pajin (AMRES)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Abstract: The GN3plus Multi-Domain Virtual Private Network (MDVPN) service will deliver seamless private interconnection of two or more networks across multiple network domains (typically GÉANT and NREN backbones). This will allow the users of the IPv4/IPv6 (or Layer2) networks to work as if their networks are coupled together. This document describes what the MDVPN service plans to offer, as well as the service delivery terms.

Table of Contents

Executive Summary

This document describes the future GN3plus Multi-Domain Virtual Private Network (MDVPN) service that will be offered over a joint service domain (typically GÉANT and NREN backbones). The objective of GN3plus SA3, Task 3 is to deploy a pilot version of the service by the end of the GN3plus project (March 2015). Taking into account the dependency of service deployment on NRENs' and GÉANT's operational agenda (and the difficulty to foresee this), the progress of this task will enable quick and wide deployment. The document's aim is to describe what the service offers and the terms of service delivery. In order to address the needs of different readers, this document provides an overview of the service, service features, service provider agreement, service specification and technical specification of the service.

The MDVPN service is to be provided for educational and research organisations or projects that need private network connectivity across multiple domains, such as multiple service provider networks (NRENs). At the time of writing this report (September 2013), the GN3plus MDVPN service is able to deliver L2VPN (point-to-point) and L3VPN (multi-point) very quickly across multiple network domains. This allows the users of the IPv4/IPv6 (or Layer 2) networks to work as if their networks are directly coupled.

The use of VPN improves end-user performance and security, and facilitates scientific collaboration. LHCONE and LHCOPN project experience suggests that VPN usage improves user performance, and increases the scientific/researcher network exchange between NRENs and GÉANT. As MDVPN is very flexible and fast to deliver to end users, there will be a wide scope for MDVPN use, from the long-term infrastructure with intensive network usage to quick point-to-point for a conference demonstration. As a result, the success of MDVPN should be assessed by the number of created VPNs as well as the network throughput.

The MDVPN service requires deployment to the VPN transport service, which will be delivered by GÉANT to transport a VPN from one domain (NREN) to another. Thanks to their high flexibility, the MDVPN and VPN transport service are able to cope with the heterogeneous infrastructures that cooperate to deploy service instances across several domains. The deployment of these two services is expected be quick, as these two services are based on Internet standard (RFC) and do not require new resources, because existing routers and links can be used to provide the service.

Introduction: Using this Document

This document describes the MDVPN service that is jointly offered by specific GÉANT partners. The service definition for end-to-end connectivity services offered to the end-user is described by five main components:

- A **general service description** (GSD) (Section 1) explains the service in a way that users who have little or no knowledge of networks may find it easy to understand. This description can be forwarded by the NRENs to any customer they may wish to announce the service to or included in marketing and promotional material.
- A **service functionality description** (SFD) (Section 2) explains what is included as part of the service offering. This information is typically needed by the NOC managers and operational staff at the institutions that need the service.
- An **operational level agreement** (OLA) (Section 3) is an agreement between a minimum of two domains, describing the goal of the MDVPN service.
- A **service level specification** (SLS) (Section 4) carefully analyses the service, and the SLS specifies the boundaries for the technical parameters of the service. This information is important to the NOC managers and operational people and institutions (end users) that need the service. Certain high-level parameters of the SLS may be used in the GSD, where these are of most interest to the user.
- A **technical service specification** (TSS) (Section 5) that describes the infrastructure and the supporting services that are needed to run the service. The infrastructure and supporting services are placed in either a joint service provider category or in an individual provider category, to clarify the responsibilities of the different participants. The infrastructure and supporting service blocks are further decomposed into smaller components, where needed.
- A **glossary** of defined acronyms and further **references** may also be found at the end of this document.

1 General Service Description (GSD)

The GN3plus MDVPN service delivers seamless, private interconnection of two or more networks across multiple network domains. This allows the users of the IPv4/IPv6 (or Layer2) networks to work as if their networks are coupled.

A typical scenario would be one where an organisation seeks to connect a number of sites from different physical locations as if they were in the same physical location, to enable the organisation to access the same level of security. This security improvement enables high network performance by avoiding deep firewall inspection, such as the case with standard IP. This scenario is achievable by using the MDVPN service jointly offered by a set of networks in the GN3plus service area. Another example of MDVPN service usage is connectivity between clusters, grids, cloud centres and parts of HPC centres, allowing them to form virtual resources or provide services for research projects. The MDVPN service will be very useful for international end-user (researchers) collaboration, especially to support data exchange and cooperation on a daily basis.

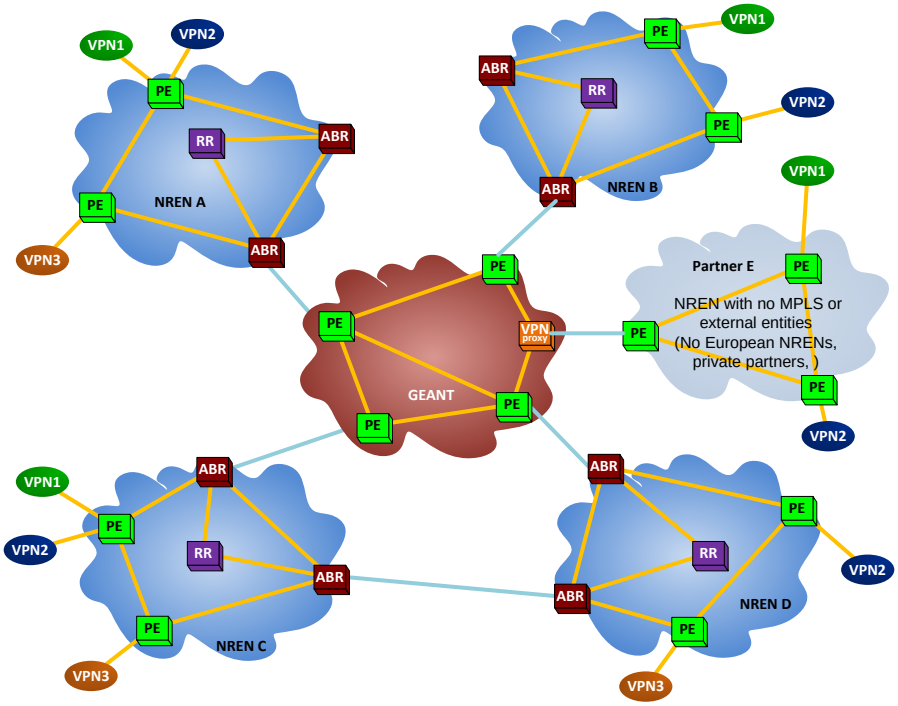

Figure 1: MDVPN service

The MDVPN service also guarantees that the data of VPN Z users cannot be delivered to sites outside of the VPN Z, and that sites or machines outside of the VPN Z are unable to join machine that are in the VPN Z. The data is kept private between the different instances of the service (i.e. VPN X, Y, Z…), i.e. the content sent back and forth between the different sites of the VPN Z is accessible only to the virtual private network Z. This is achieved by isolating the MDVPN customer data flows from any other traffic, standard IP traffic and traffic of other MDVPN customers. In addition, it provides more advanced routing options and together with bandwidth, guarantees more flexible solutions for HPC centres.

The capacity of the MDVPN service can be adjusted to accommodate different user requirements, allowing both small- and large-scale offices to seamlessly interconnect.

The service is offered collaboratively by GÉANT and a set of adjacent domains (NRENs or external partners) that adhere to the service. These joint networks form a multi-domain area where the service is provided (GN3plus service area). One of the advantages of the service is that it uses well known and standardised protocols and technologies, which are available on many routing and switching platforms. This expands the scope of the service on (almost) all NRENs.

The service is designed for situations where users need a dedicated and independent network for transfer of data (IP or native Ethernet traffic) between two or more end points. This is typically the case if the user premises are spread over a large geographical area. The service is always enabled, meaning that once established, no further operations are needed on a daily basis. The service offers high security in the sense that the carried traffic is isolated from other traffic. It should be noted that the traffic is isolated at the logical layer and not necessarily at the physical layer. It means that the core networks will carry data from multiple users, but there will be no ‘crosstalk’ between these traffic streams. From the users’ perspective, each instance of the service is a virtual private network. Hence MDVPN service is an ‘umbrella’ infrastructure, which enables participating NRENs to provide VPN services for end users.

The MDVPN service is a joint service delivered by NRENs and GÉANT. This leads to the fact that in order to deliver the service to the end user, the NRENs only need to subscribe to the GÉANT VPN transport service once. Then the NRENs can open their MDVPN service instances for their users. The users subscribe to MDVPN NREN service as many times as an L3VPN or L2VPN is needed.

The joint service provider actively participates in exchange of control traffic exchanged between end user sites (for example, appropriate routing protocol can be enabled between end user router and NREN router).The service is monitored by the NRENs delivering it, and the NREN to which an end user is connected is a unique point of contact, thereby ensuring a fast response to failures. In addition, a service support structure (Infrastructure Support Team, Service Desk) is established for problem resolution and other means. Thanks to the peer model of the service, the NREN can provide advanced monitoring and troubleshooting support.

2 Service Functionality Description

2.1 MDVPN in a Nutshell

A typical MDVPM scenario is that of a user group or organisation spread geographically into smaller sites within the GN3plus service area. Each geographically separate office needs to be connected with other sites in the same user group. This is illustrated in Figure 2, below.

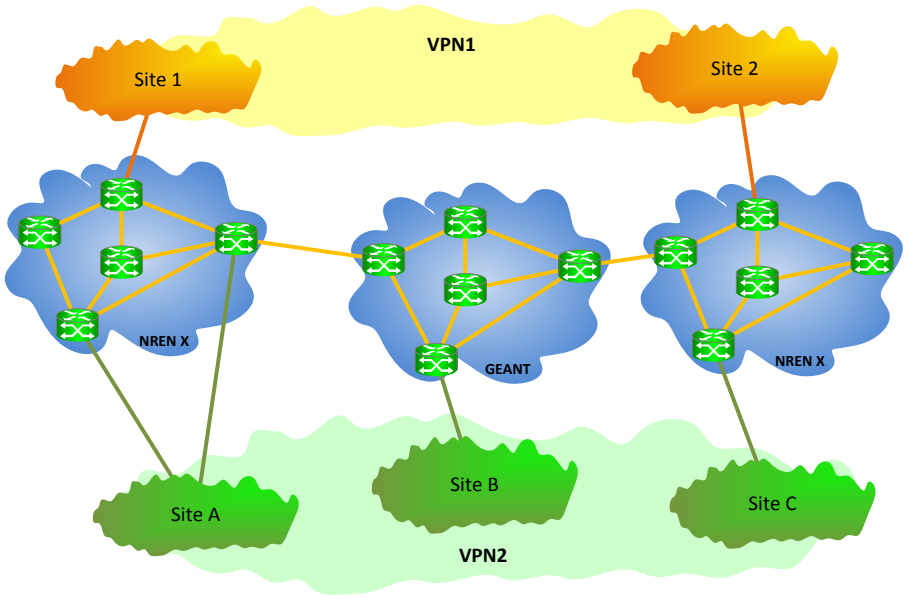

Figure 2: MDVPN service overview

The middle row of Figure 2, above, illustrates three, independent domains that deliver the MDVPN service to two different user groups labelled VPN1 (orange) and VPN2 (green). One of main advantages of the MDVPN service is that the user-group clouds can be connected to the GN3plus service area, illustrated by the middle row (blue clouds) by a number of different technologies, ranging from dedicated private lines to logical lines delivered by local service providers or universities. The network elements within the GN3plus service domain are configured to exchange traffic between the VPNs with the same colour, which make it appear as if they were connected to the same local network. The MDVPN service may be offered with local redundancy, as indicated for VPN2 in the NREN X domain. Here, two different connections are used to carry the traffic into the provider (NREN) network. The appropriate signalling protocols, will assure redundancy over loop-free network. MDVPN supports cross-border fibre between two NRENs in order to improve the service reliability. If the site is not directly connected to

a NREN, the NREN can use any appropriate technologies to deliver the service, in particular, the same technologies used in MDVPN.

The MDVPN service can be very useful when researchers (end users) wish to exchange data between different departments or labs located anywhere in the GN3plus service area, and cooperate on a daily basis. **One of this service's advantages is that it does not always require new network resources, because existing routers and links can be used to provide the service.**

2.2 Service Functionality Description

The MDVPN service delivers private Layer2/Layer 3 connectivity between user premises by means of MPLS based VPN solutions. Typical examples of multi-domain VPNs are shown below in Figure 3.

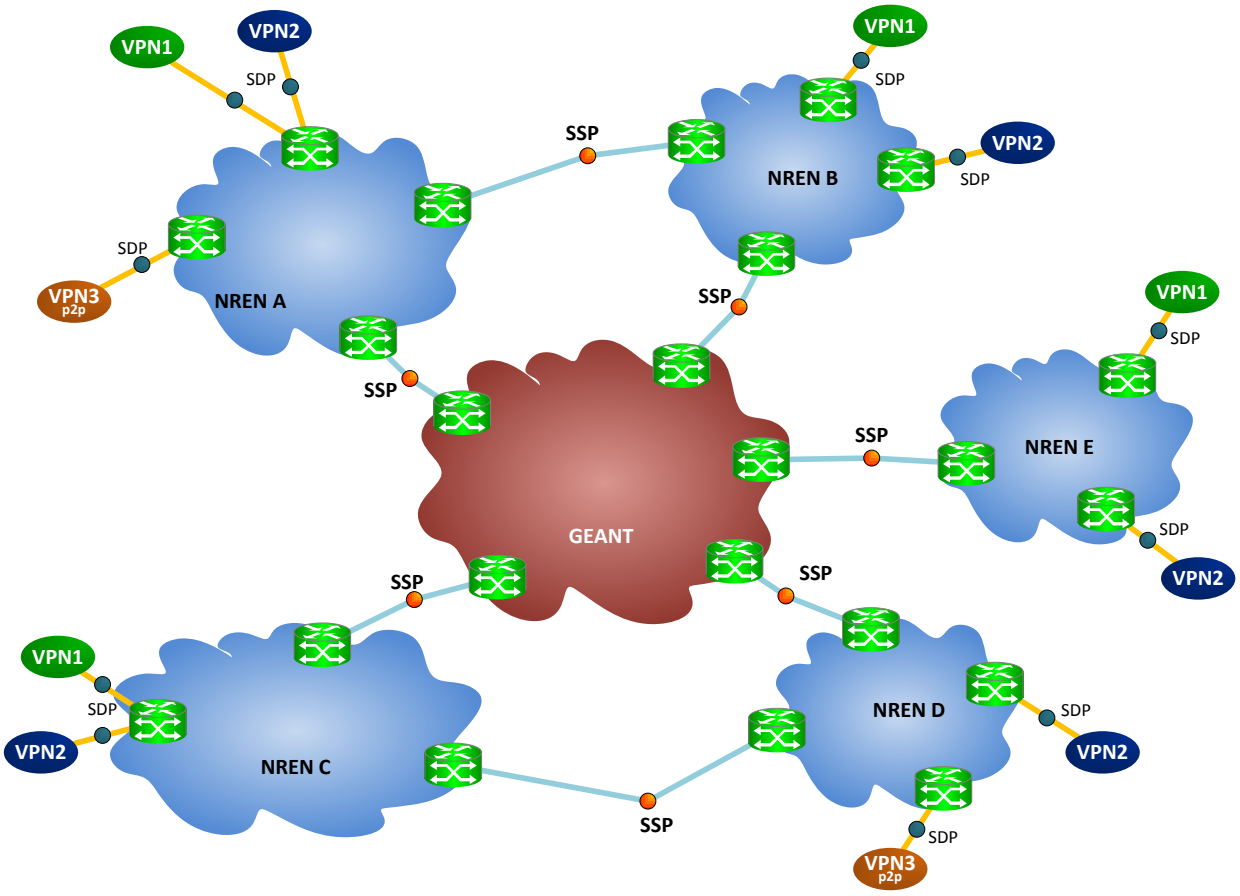

Figure 3: Multi-domain VPNs example

As shown on Figure 3 many end-user sites can be geographically distributed and connected to different networks. However, if the sites are located in the GN3plus service area, they are still able to form private networks and exchange traffic.

In the GN3plus service domain, service solutions such as MDVPN are offered by multiple networks, which make it necessary to peer VPN information at the borders between NREN networks. These peering points are referred to as Service Stitching Points (SSPs) in the GN3plus MDVPN service architecture. The Service Demarcation Points (SDPs) are the end points where the service is terminated for the end users in the GN3plus service architecture.

The MDVPN service is offered in response to an end-user request (end users are defined as the direct customers of the domains that provide the MDVPN service). The end-user specifies the endpoints (SDPs) of the service, located at the edges of the federated domain. These points are located at the interfaces of PE devices found at the edge of the joint service domain. The NRENs will provide a map of inter-domain connectivity (SSP) and list of SDPs to the end user. The list of SDPs will change as long as new sites are connected or sites withdraw from the VPN, therefore, it is up to the end user to maintain a list of allowed connected sites. According to an updated list, NRENs will provide the list of inter-domain connectivity (SSP) to the end user.

MDVPN supports cross-border fibre between two NRENs to ensure greater service reliability and network flexibility. In order to provide the MDVPN service to sites that are not directly connected to an NREN, the NREN can use any appropriate technologies to deliver the service. Like GÉANT, an NREN can deploy a VPN transportation service (CoC). However, the scenario where a NREN will provide VPN transportation for another NREN that is already connected to GÉANT VPN transportation has yet to be tested and analysed in detail. Therefore, it is not recommended for the NRENs to implement it for the first deployment of MDVPN.

Each NREN will use its own subscription approach for its end users, although the NRENs involved in MDVPN service need to exchange several pieces of information in order to be sure that the service is appropriately delivered.

As the service is not enabled as a default, NRENs can subscribe to GÉANT's VPN transport service. The GÉANT VPN transport service will transport the L2VPNs or L3VPNs that the NRENs want to inject into the service. It is possible to use a subinterface or a dedicated interface to access to the GÉANT VPN transport service, in the form of an SSP. The subscribing NREN will also specify the maximum amount of bandwidth that will be dedicated for use by this service.

2.3 Service Options

The MDVPN service can deliver differentiated functionalities, depending on end-user requests:

- IPv4 routed transport (IPv4 L3VPN)
- IPv6 routed transport (IPv6 L3VPN)
- Hybrid routed transport (IPv4/IPv6 L3VPN)
- Point-to-Point Ethernet (Virtual Leased Line)

Moreover, a detailed analysis of multipoint Ethernet service (VPLS) will be conducted in order to add this service to the GÉANT's portfolio of services later, if the conclusions of this analysis are positive and if a use case is identified.

2.4 Service Parameters

The end-user that requests the service must also specify parameters of the VPN as listed below:

- Bandwidth allocated for each SDP (site to be connected) and bandwidth required for transport between particular SDPs
- Interface type (for example Ethernet, ATM, POS)

- MTU size requirements
- Any required network redundancy (dual homing)
- Layer3 routing protocol (for example static routing, OSPF, BGP) – if applicable.

It must be noted that in case of sending several data flows from several sites to one specific site, the bandwidth reserved for this site will be shared.

2.5 Acceptable Use Policy (AUP)

The acceptable use policy (AUP) for this service defines acceptable practices relating to the use of MDVPN service provided over joint network infrastructure by the end users that have gained access to the MDVPN through SDPs. The AUP will require that by using the MDVPN service, the end user acknowledges that s/he is responsible for compliance with the AUP. The MDVPN service is designed to provide connectivity for educational and research activities.

The MDVPN shall not be used for any unlawful activities or in connection with any criminal or civil violation and the Services shall in all cases be used in compliance with applicable law.

An end user may not attempt to gain unauthorised access to, or attempt to interfere with or compromise the normal functioning, operation or security of, any portion of the Joint Network Infrastructure.

Users are entirely responsible for maintaining the confidentiality of their password and account information.

AUP violation by end users or NRENs will result in a warning, and if no proper justification (or feedback) is supplied, access to the service can be terminated.

3 Operational Level Agreement

3.1 Goals and Objectives

The following text provides an example Operational Level Agreement ('OLA' or 'Agreement') between **GÉANT** and **NRENs or between a NREN and another NREN** for the provisioning of IT services required to support and sustain the MDVPN service. The objective of the service is to provide a basis and framework for the delivery of high-quality services that meet the needs of the NRENs' end users. Note that an OLA is contracted once for all the VPNs that can be set-up.

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT service support and delivery to the end-user(s) by the service provider(s).

The **goal** of this Agreement is to obtain mutual agreement for IT service provision between the service provider(s) (i.e. GÉANT and the NRENs) in order to deliver MDVPN service instances.

The **objectives** of this Operational Level Agreement are to:

- Provide clear reference to MDVPN service ownership, accountability, roles and/or responsibilities
- Present a clear, concise and measurable description of MDVPN service provision to the stakeholders and end users.

3.2 Stakeholders

The following service provider(s) will be used as the basis of the Agreement, and represent the **primary stakeholders** associated with this OLA:

- VPN transport provider: GÉANT
- VPN provider(s): all NRENs taking part into the MDVPN service.

3.3 Beginning Date, Duration and Periodic Review

This Agreement is valid from the -XX- (to be filled by NRENs) and is valid until further notice. This Agreement should be reviewed at a minimum –XX- (to be filled by NRENs) times per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

Business Relationship Manager: GÉANT
Review Period: Yearly (example)
Previous Review Date: 01-01-2014 (example)
Next Review Date: 01-01-2015 (example)

3.4 Service Agreement

3.4.1 Service Scope

The following Services are covered by this Agreement:

- Multi-Domain Virtual Private Network (MDVPN).
- GÉANT Multi-Domain Service Desk (MDSD) for MDVPN.
- NREN Service support for MDVPN.

3.4.2 VPN Provider Requirements

VPN Provider responsibilities and/or requirements in support of this Agreement include:

- Connection of the end users to the VPN service instance required by the end users.
- Deliver VPN data of MDVPN to end users.
- Meeting response times associated with service-related incidents.
- Appropriate notification to transport VPN provider, other VPN Providers and end users for all scheduled maintenance.
- Providing service availability in its point-of-presence (PoP) to the transport VPN provider, other VPN Providers and end users.
- Providing usage accounting for MDVPN service instances to all service partners, through the MDVPN MDSD.

3.4.3 VPN Transport Provider Requirements

VPN transport Provider responsibilities and/or requirements in support of this Agreement include:

- Transport the VPNs (Multi-Point L3VPN, Point-to-Point L2VPN) of VPN providers.

- Meeting response times associated with service-related incidents by using the MDVPN Multi-Domain Service Desk (MDSD), provided by DANTE/GÉANT.
- Appropriate notification to all MDVPN service members for all scheduled maintenance.
- Providing usage accounting of MDVPN Service Stitching Points (SSPs).

3.4.4 Service Assumptions

Assumptions related to in-scope services and/or components include:

- Changes to services will be communicated and documented to all stakeholders.

3.5 Service Management

3.5.1 Service Availability

The service availability is defined as the service instance availability measured individually between SDPs for delivering the service. This availability is a function of:

- The Transport VPN service availability, which is defined by the service availability between SSPs.
- The availability of each VPN, which is delivered by VPN provider. At VPN provider level, this availability is measured between the internal SDPs (NREN internal path for VPN) and between the SDPs and the VPN provider's SSP (NREN).

3.5.2 Service Provisioning and Trouble Management

VPN providers manage:

- An end user's initiation / termination / change request to the service, according to their own user request process.
- Problems/issues related to this service, which are detected or reported by the end users.

The VPN transport provider manages:

- The VPN provider initiation / termination / change request.
- Any problems/issues related to this service, either internally detected or reported by VPN providers to GÉANT.

4 Service Level Specification

The MDVPN service allows NRENs (GÉANT is considered as a NREN) delivering multi-domain VPN service (multi-point L3VPN, point-to-point L2VPN) to end users. The MDVPN service requires another service, the VPN transport service that allows transporting all the multi-domain VPNs setting-up within MPVPN service from one domain (NREN) to another domain.

In the SLS section, the VPN transport service and MDVPN service are analysed. As a multi-domain service, MDVPN requires a deeper analysis of the role and relationships of the actors (end-users, VPN providers, VPN transport providers) in order to define the operation for the MDVPN service.

Then SLS specifies the quality parameters for the MDVPN service. SLS specifies a set of parameters, depending on SDPs' and SSPs' configuration and conduit transport parameters. Some of these parameters are mandatory.

4.1 VPN Transport Service

The GÉANT network provides the VPN transport service for the NRENs (transparently transporting the NRENs' VPNs). In the future, NRENs could also provide this service. The relationship between the NRENs and the VPN transport service provider (i.e. GÉANT) is a classical service provider (GÉANT) and users (NRENs) relationship. Therefore, this service will follow the standard rule of GÉANT service operation (subscription, withdraw, etc…). The NREN will subscribe to this service for the maximum amount of required bandwidth, which should exceed the sum of bandwidth required by the NREN's VPN that use this Service Stitching Point (SSP). The list of SSPs should also be provided by the NREN to GÉANT, noting the type of interface (dedicated interface or subinterface).

4.2 Modelling the MDVPN Service

In order to achieve a good level of quality for the MDVPN service, all necessary business processes required for the transition, operation, supporting, maintenance and continual improvement of the service need to be clearly defined. The aim of this phase in development of the MDVPN service is to highlight processes and procedures used in order to improve the capabilities of the GÉANT Multi-domain Service Area providing MDVPN service.

The Multi-Domain Virtual Private Network (MDVPN) service is the core service[1] provided to users. As described in Section 1, the MDVPN service will be offered collaboratively by GÉANT and participating European NRENs. Both NRENs and GÉANT will offer and deliver parts of a jointly provided service to users across Europe. GÉANT will provide the enabling service – Transport VPN (see Section 5.1.3.1) that is needed in order to deliver core MDVPN service. Transport VPN service that GÉANT provides to the NRENs will be invisible to the end users of the MDVPN service. NRENs will provide the VPN service–MDVPN service to the users across Europe.

Regardless of the complex structure of the GÉANT Multi-domain Service Area, where the MDVPN service will be provided, end-users of the service should not notice any difference in the organisation and performance of the service support and delivery. All necessary procedures and processes important for the operation of service and needed to fulfil end-user requests must be developed by a joint effort of SA3 T3, GÉANT operational team and an NREN's team (service provisioning, request fulfilment, problem management, performance management, etc.). It is also important that the organisational complexity of the service provider should not have a negative impact on delivery and performance of the provided service.

Inter-domain information exchange and organisation are extremely important for the MDVPN service, and must be clearly and precisely defined to reflect both end-user requirements and the multi-domain nature of the GÉANT-NREN environment. The exact form of this exchange will be confirmed pending GÉANT operational feedback. Successful service implementation and application are the main focus of SA3 T3 effort, however, as MDVPN is a typical IT service, this focus must extend beyond the operational aspects of service lifecycle, to include, for instance, service positioning and advertisement (although these are outside of the remit of SA3, T3).

The results of GN3 JRA2 T1 – Control and Management group [GN3 D.J2.1.1] are used for modelling and defining the business processes necessary to establish and for the operations of the MDVPN service. This task proposed GÉANT-NREN business process architecture, a set of business processes used for multi-domain network service support within the GÉANT Multi-domain Service Area. The business model created from these results, planned to be ready by end-January 2014, will take into account the two distinct levels that are characteristic of this service: multi-domain VPN service and VPN transport service. This proposal is mainly derived from the standard TMF Business Framework (the enhanced Telecom Operations Map - eTOM) [GB921D] and consists of a selected subset of eTOM business processes and new processes responsible for the inter-domain interaction unique to the GÉANT-NREN environment.

4.2.1 MDVPN Main Entities

In order to properly define the MDVPN business process architecture, it is important to clearly identify the main entities/actors that will be included in the service delivery. Business processes are defined to align with the service provider that provides a well-defined set of services to its end-users using its subset of Network Resources. The provider may also have a range of suppliers and partners required for service provision.

The following entities will be included in the MDVPN's business process architecture:

End-users are the focus of the MDVPN's business objectives. The following types of end-users could potentially use the service:

[1] ITIL definition – Core services deliver the basic outcomes desired by the user.

- **Campuses** and **Institutions**: Education and research campuses and/or other public institutions such as libraries and hospitals that have access to the GÉANT network through their NRENs.
- **Projects**: Research and technology projects have specific networking requirements to facilitate their project's collaboration needs, and these are typically met by the project's host institutions (which are, in turn, connected to the local NREN and through that, to the GÉANT network).

In order to properly define different business processes workflows, it is important to understand the end-user/service provider relationship. End-users are associated with groups/projects, the organisation of which may vary between member institutions. The MDVPN service must be flexible enough to cope with the range of end-users' organisations (note: the organisation of the end-user groups/projects is outside of the scope of this paper). The initiating institution will request the service on behalf of its NREN's group/project, due to language barriers and contractual obligations between NRENs and their institutions.

A **service provider** is an organisation supplying services to one or more end-users. The service provider of the MDVPN service is the set of NRENs participating in delivery of the MDVPN service. The MDVPN service will be listed in the NRENs' service portfolios and offered along with services that are local to the NREN.

In order to facilitate the delivery of the MDVPN service, GÉANT must provide the Transport VPN service. The Multi-domain Service Desk (MDSD)[2] will also be supporting the service for all NRENs that will participate in its provisioning. In this context, the GÉANT network will be one of the suppliers to NRENs in providing the MDVPN service.

Partners are those with whom the service providers (NRENs) co-operate in a shared organisation area. In the context of the MDVPN service, regional networks partner the delivery of the service to the end-users in the case where the end-users are not directly connected to the service provider (NREN).

4.2.2 MDVPN Main Functions and Roles

In addition to the business processes, it is essential to clearly define the specific functions, roles and responsibilities for successful MDVPN service management. The same person can act in different roles, and delegation of roles between domains is also possible.

A function could be defined as a team or group of people and the tool or other resources used by the group to carry out one or more processes or activities. [ITIL] In the context of the MDVPN service, the next function could be recognized by the following components:

- **MDVPN Service Desk** – The Service Desk is a vital part of a service provider organisation, and should be the single point of contact for users on a day-to-day basis. It is responsible for dealing with a variety

[2] The Multi-Domain Service Desk (MDSD) is a GÉANT-provided service which centralises and simplifies the provision of support services to NRENs participating in multi-domain services. The MDSD is the single point of contact for NRENs who require information or assistance with respect to the multi-domain services. The MDSD is staffed by experienced NOC Engineers based in the GÉANT Network Control Centre (NCC), who are knowledgeable about the GÉANT environment and services.

of service activities, including: incident handling, issue escalation to problem management staff, manage users service and change request, handling communication with users, etc.

The MDVPN service desk needs to be decentralised, taking into account the multi-domain nature of the service provider. Since the provider of the MDVPN services is a set of NRENs, the MDVPN service desk will be a set of local NRENs' service desks (1st level NREN NOC) or parts of NRENs' SDs devoted to the MDVPN service. Every domain (NREN) inside GÉANT's Multi-domain Service Area will provide support to their user community. User group/project member institution will contact and communicate the local NREN service desk (1st level NREN NOC) for every question or request regarding the MDVPN service.

Regardless of the overall MDVPN service desk structure, users should be in no doubt about how to seek help if they need assistance. Contact information of all NREN service desks will be provided and well publicised.

- **MDVPN service operational management** – Operational management refers to the group, department or team responsible for performing day-to-day operational activities, ensuring that a device, system or process is actually running or working. The stability of the IT infrastructure and consistency of IT services is a primary concern of operational management.

  The MDVPN operational management function will be responsible for the ongoing management and maintenance of the NRENs' network infrastructure to ensure delivery of the agreed level of the MDVPN services to the users. It is the 2nd level support for the MDVPN service users. The MDVPN operational management group will be decentralised and will be composed from participating NRENs NOCs (2nd and 3rd level NREN NOCs). However, some level of synchronisation between NRENs' NOCs needs to be implemented.

  The GÉANT MDSD could have a synchronisation role between NRENs' NOCs. MDSD could improve communication and leverage documentation and information exchange between NRENs' NOCs. MDSD is needed to ensure consistency and uniform service quality across all participating domains.

- **MDVPN service technical management** – Technical management refers to the groups, departments or teams that provide technical expertise and overall management of the IT infrastructure and services.

  The MDVPN technical management is responsible for the design and development of technical architecture and performance standards for the MDVPN service. It is responsible for specifying the operational activities performed as part of MDVPN operational management. The MDVPN technical management provides high-level support during incidents and with problem resolution. It is responsible for continual service improvement activities and ensures that all system and operating documentation is up to date and complete.

  The GN3plus SA3 T3 MDVPN group takes the role of MDVPN service technical management. It is responsible for coordination of all the MDVPN service design activities, processes and resources and ensures the consistent design of architecture, technology, processes, information and metrics for the MDVPN service. In order to ensure sustainability of the MDVPN service, if the service gains a significant number of users, a similar task should be included in subsequent GÉANT projects.

  A role could be defined as a set of responsibilities, activities and authorities assigned to a person or team [ITIL]. All roles within service management require specific skills, attributes and competences from the people involved to enable them to work effectively and efficiently. Roles are not job titles. One person or team may have multiple roles, but one role could be carried out by a number of people or teams. In the context of the MDVPN service, the following roles have been identified:

- **MDVPN Product Manager/Service Owner** – Accountable for the overall delivery of the MDVPN service, and representing the service across the GÉANT Multi-domain Service Area, The Product Manager: ensures that the service delivery and support meets the users' requirements, identifies service improvements, works with GÉANT's business relationship management to understand and translate user requirements (big project support, etc.) into activities, measures or service components, works on the design and improvement of business processes workflows, and ensures that are service level agreements (SLSs) and operating level agreements (OLAs) are performed as agreed. The MDVPN Product manager role is consistent with the GN3plus Product Management role, defined in GN3plus Product Lifecycle Management.

- **MDVPN Service Operation Manager** – Working with the MDVPN Product Manager on planning and coordination of all process activities, the Service Operation Manager ensures that all activities are carried out as required, monitors and reports on process performance, assists with the resolution of performance-related, availability-related and capacity-related incidents and problems associated with the MDVPN service, and ensures that all service components, applications and resources are properly configured to proactively monitor the MDVPN service instance.

- **MDVPN Service Instance Architect** – Responsible for the overall design coordination and planning of an MDVPN service instance, the Service Instance Architect ensures appropriate documentation of the MDVPN service instance (overall design, architecture, topology etc.) is produced using agreed standards, methods and tools, and is kept up to date and available to all involved parties in service delivery.

- **MDVPN Service Level Manager** – Monitors and measures the MDVPN service performance achievements, reports on service levels, holds reviews with customers and identifies required improvements. Analyse service infrastructure and service instance availability and quality over time.

Properly defined and assigned roles will ensure that all operational activities inside business processes will be carried out on agreed levels, and that clear responsibility is assigned for these activities. This will contribute to improved efficiency in delivering of the MDVPN service.

4.2.3 MDVPN Inter-Domain Relationship

Unlike the commercial environment, multi-domain network services are provided in the GÉANT environment without commercial or user/supplier relationships between service-providing domains (NRENs). Service users are residing in the NREN domains and all participating NREN domains are jointly involved in all phases of service provisioning. This concept is also applied to the MDVPN service. NREN domains that participate in delivering the MDVPN service are autonomous in the control and management of the network resources they own and keep full control over them (loosely coupled federated model). It is not possible for a network element in Domain A to be controlled from Domain B.

The business processes architecture which could be used to represent the delivery of MDVPN service inside GÉANT Multi-domain Service Area is presented in the following Figure 4.

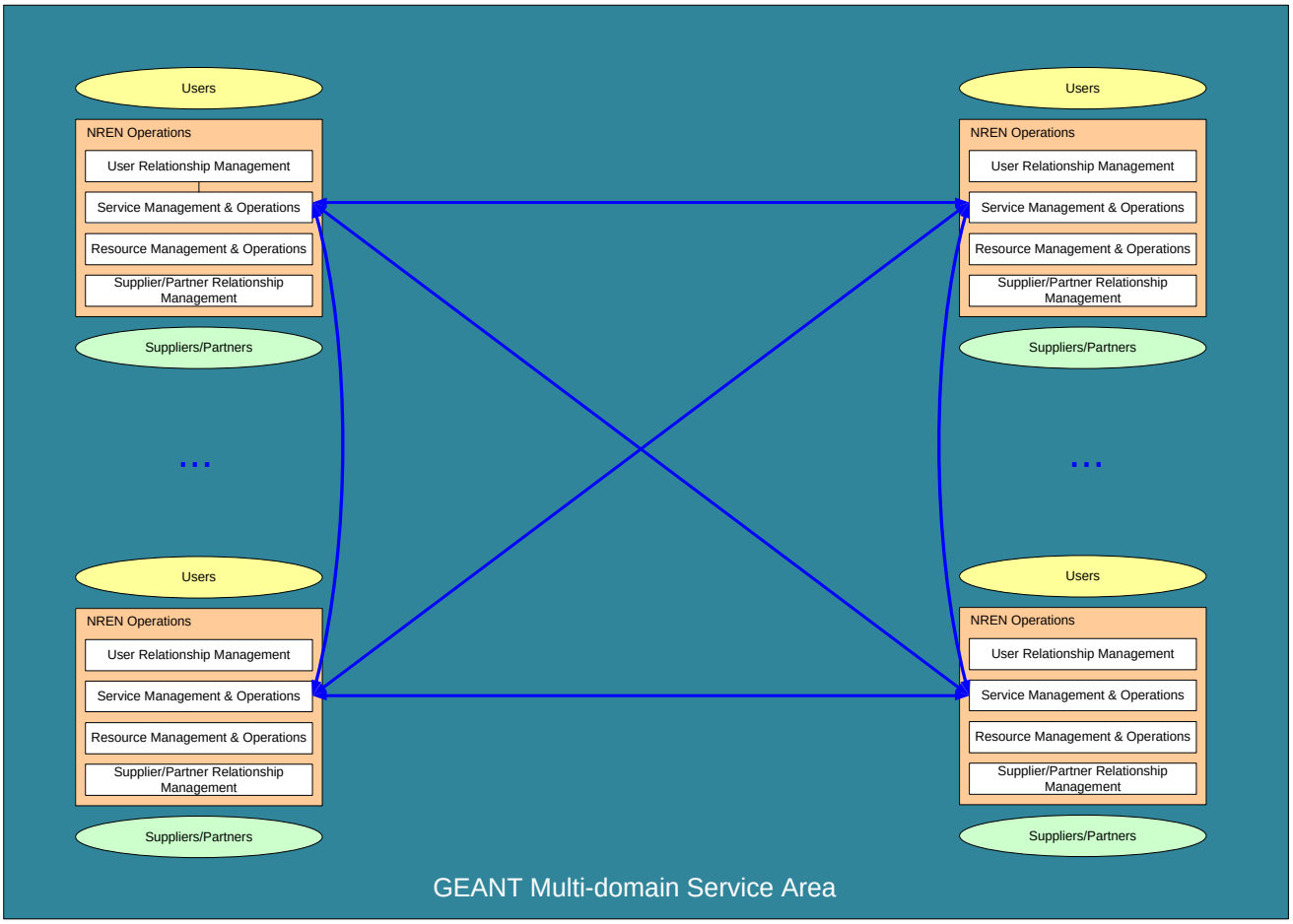

Figure 4: The MDVPN business processes architecture

MDVPN users reside in two or more of the NREN domains participating in the MDVPN service instance. User relationship management must exist in all NREN domains because, as previously stated, the end institution that is asking for a service is requesting it from its own NREN. Supplier/Partner Relationship Management is also needed in all participating domains, as all of the participating NRENs manage the relationship with their own telecoms providers, networking equipment vendors and GÉANT/DANTE during the service provisioning phase. All domains directly serving end users must support the full set of Operations Area business processes.

4.2.4 MDVPN Business Process Decomposition

To be able to clearly define inter-domain relationships inside the GÉANT Multi-domain Service Area, the service architecture must be further decomposed on different business processes when delivering the MDVPN service. The definition of business processes defined for GÉANT multi-domain service environment is out of scope of this document. Elements of it may be found in “Information Schemas and Workflows for Multi-Domain Control and Management Functions” [GN3 DJ2.1.1]. It also represents Level 2 decomposition of eTOM business processes in the Operations area and the Multi-domain Service interaction process, unique for multi-domain service environments. Detailed descriptions of all these processes can be found in [GN3 DJ2.1.1].

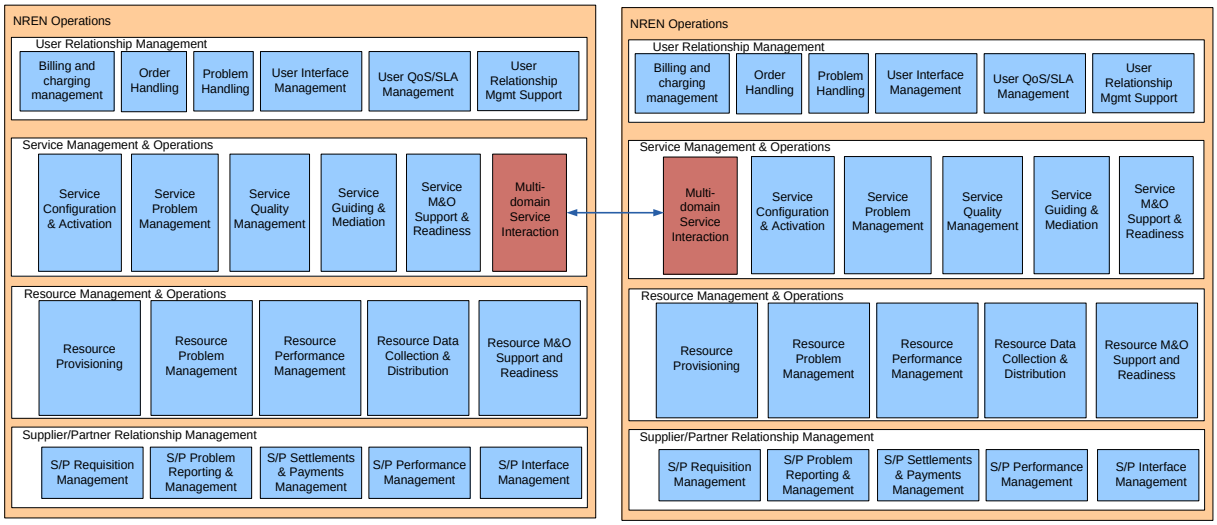

Figure 5: Business process decomposition for NREN to NREN interaction [GN3 DJ2.1.1]

4.3 Service Management

A MDVPN service desk should be available for the coordination of a number of associated activities. The MDSD (GÉANT Multi Domain Service Desk) and local (NRENs) NOCs will be used to provide support for the service. It is important that this service is well integrated to NREN NOC operation, as it may require advanced troubleshooting coordination with GÉANT and other NRENs.

4.3.1 The VPN Transport Service Provisioning Workflow

GÉANT/DANTE provides the VPN transport service for the NRENs. In the future, the NRENs could also provide this service. The NREN should request any subscription to a VPN transport service via a web interface. The NREN requests should be handled by the MDSD. The information, the procedure and the form will be discussed between MDVPN service technical management group and the MDSD. Two cases should be taken in consideration: whether the NREN supports or does not support MPLS technology.

4.3.2 MDVPN Business Process Workflows

The MDVPN business process workflows will propose the order in which business processes should be executed, and how NRENs and potentially MDSD interact and exchange information with each other in order to accomplish important activities needed to deliver the MDVPN service (e.g. service provisioning, problem management etc.). These workflows could be used in a later phase of the service lifecycle as a basis for the design and development of MDVPN business-process-supporting tools. The rigorous representation of process workflows should adhere to the TMF template for process flow representation (see examples in [GB921F]). Descriptions of MDVPN process flows can be found in the ongoing work of GN3plus SA4 T3 task [DS4.3.1]. This document describes process flows in a less rigorous way in order to focus more on the process itself and the role of various functions in it, and less on standardised process names and TMF specifications.

The workflows described below assume that NRENs satisfy some prerequisites. The most important prerequisite is an NREN's subscription and membership to the GÉANT Transport VPN service. The GÉANT Transport VPN service will enable participating NRENs to collaboratively provide MDVPN service to their users and to deliver new connectivity to them. Technical aspects of accession to the GÉANT Transport VPN service are presented in Sections 5.2.1 and 5.2.2.

Every participating NREN will ensure that all information, materials, systems and resources regarding the MDVPN service is available to the local NREN Service desk (part of MDVPN Service desk) to support users.

4.3.2.1 *The MDVPN Service Provisioning Workflow*

When end-users request an instance of MDVPN service i.e. a new multi-domain VPN, it is crucial that the MDVPN service achieves the following objectives:

1. Guarantee that the process of provisioning a new multi-domain VPN will be managed and monitored until the end of the process (success or failure).
2. The provisioning request should be as easy as possible for the end-users. As end–users could be disconcerted by a simple form, a specific help could be provided by the NRENs.
3. The set-up duration (i.e. duration between the request and the end of provisioning process) should be minimised; the objective in case of multi-domain multi-point VPN is that two end-points will be quickly connected in order that end-users can start their first tests as quickly as possible.

The Multi-Domain Service Provisioning workflow described in document "Information Schemas and Workflows for Multi-Domain Control and Management Functions" (see Section 4.2 in [GN3 DJ2.1.1]) illustrates the business process interaction for general multi-domain service provisioning, regardless of the technologies used and the type of service provisioned. This model will be used as a basis to describe composite MDVPN service provisioning workflow, which shows the whole set and order of business processes required for completing the provisioning process. Process flow is illustrated below in Figure 6.

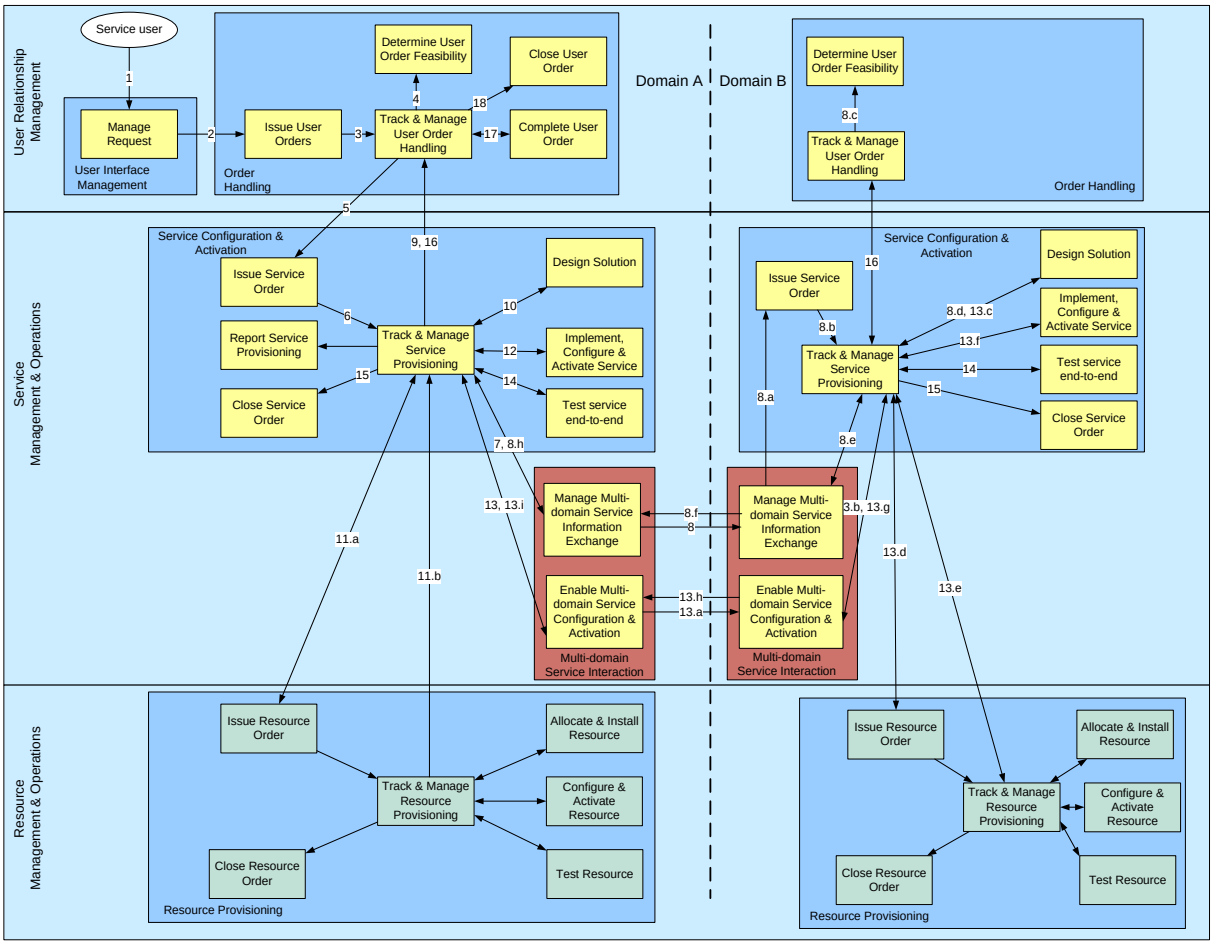

Figure 6: VPN Service provisioning workflow

End-user Group/Project Request

The MDVPN Service Provisioning workflow starts with end-users group/project request for the provisioning of the new multi-domain VPN service instance. The MDVPN service request for an end-user group/project could be submitted by any end-user group/project member institution that is authorised by the other partners in that end-user group (Authorised Member Institution - AMI). AMI will submit MDVPN service request to the Service Desk of local NREN to which AMI is connected. AMI will provide all necessary information important for full description of end-users group/project MDVPN service request.

End users' requests will precede each NREN's request processing. In some cases, the end-users could request the MDVPN service from GÉANT, for instance, a project would like to have a unique point of contact within the GÉANT network.

The initiator NREN receives the AMI service request for provisioning of the new MDVPN service instance. This will be performed according to the existing local NREN rules (e.g. phone call, service portal, e-mail etc.) for their users. All the necessary MDVPN service request details (e.g. user order description, service order end-point addresses, contact details, etc.) are captured, and further status of service request is managed (monitoring the service provisioning procedure, updating existing user order, modifying the user order status etc.). The local

NREN that received the MDVPN service request from AMI is called the initiator NREN, and as such, will be responsible for further management of the MDVPN service instance activation (i.e. multi-domain VPN activation).

The initiator NREN Service Desk will create a record of the relevant request information and the user order (e.g. ticket in ticketing system of initiator NREN, new request on the NREN service portal etc.) aimed for documentation purposes. It will also check if all the necessary information about the user group/project service order is provided, according to the requirements defined by the **MDVPN technical management group**.

A crucial point for management of the service and the provisioning is the communication channel between end-users, VPN providers and VPN transport provider. A tool that will easily create the two following email lists is necessary to manage a multi-domain VPN (for instance VPN-ASTRO) (availability, setting-up, change management, etc.)

1. List of NRENs involved in the VPN for all communication between NRENs (debugging, provisioning, …); for instance VPN-ASTRO-VPN-providers@MDVPN.dante.net
2. List of end-user institutions and NRENs for all communication between institutions and NRENs related to all network operation within the multi-domain VPN (maintenance announce, site unavailability, …), for instance VPN-ASTRO-operation@MDVPN.dante.net

Feasibility and Availability Assessment

The issued end-user order will require a feasibility assessment in all NREN domains, which are listed in initiating a service request. This task is undertaken by the initiator NREN Service Desk.

The initiator NREN Service Desk checks if the AMI is authorised to use this particular service, and in cooperation with the initiator NREN NOC, whether the technical conditions for access to service are met. The initiator NREN initiates a validation procedure with all participating NREN domains involved in the request, to check the availability and/or the feasibility of providing and supporting the requested the MDVPN service instance in their own domains.

In accordance with the information provided in the end-user order, the initiator NREN NOC needs to generate a service order. This may be done in a number of ways (end-user orders might have non-technical descriptions, not follow agreed terminology), including, by filling a predefined service order template document or web form on some MDVPN central repository location (e.g. file server, web portal, MDSD knowledge base, etc.). The **MDVPN technical management group** will define strict procedures on the recording/tracking of service orders. The service order could be sent to a peer's domains by an e-mail list (for instance VPN-ASTRO-VPN-providers@MDVPN.dante.net) or through MDVPN's central repository notification (e.g. web-based portal, central ticketing system, etc.).

All NREN NOCs that receive the service order will check the availability of the MDVPN service and the feasibility of this request in their domain. Every peer domain will collect the necessary information and send the initiating NREN the request. This could be done through the e-mail list, or through updating the MDVPN central repository location (e.g. file server, web portal, MDSD knowledge base, etc.) or in any other way as defined by the **MDVPN technical management group.** When the information from all peer domains about the availability and/or the feasibility of providing and supporting the MDVPN service is received, the initiator NREN Service Desk will update the status of the service order record and inform AMI. If all participating NRENs confirm availability and/or the

feasibility of providing and supporting the MDVPN service to all member institutions of a user group/project, AMI will be informed that the user order is accepted and pass the request to the design, configuration and activation phase.

If one of the participating NRENs does not confirm availability of the MDVPN service, AMI will be informed that the user order is not accepted, a partial deployment could be done and the user group/project request updated.

The **MDVPN technical management group** will define the maximum duration in which the participating NRENs have to check availability of the MDVPN service and provide answers to the AMI and the initiator NREN. These two durations should also be included in the OLA agreement.

In the later stage of development of the MDVPN service, checking the availability of the MDVPN service could be automated through the use of a repository of service portfolios, service instances in use and domain capabilities in the Federated Service Inventory (FSI).

MDVPN Service Instance Design, Configuration and Activation

When the user order is confirmed, in the general case, all NRNENs will follow their own procedures to activate the VPN in their domain, so it only requires configuration of the VPN. The configuration process also uses information obtained in the service order report and the standard design guidelines defined by **MDVPN technical management group.** Each peer NREN only designs the intra-domain part of the MDVPN service instance (i.e. local IP address range, NREN PE–CPE routing protocol, etc.).

The **Service Instance Architect** could also be consulted to define the technical and administrative parameters (Route Target 5.2.3.1, unique service instance identifier, etc.) needed for the functioning of the MDVPN service instance.

After successful installation and configuration, all NRENs will confirm that the VPN is implemented to the initiator NREN/domain of the results (e.g. notification via e-mail list - for instance VPN-ASTRO-VPN-providers@MDVPN.dante.net, updating status on MDVPN service central repository, etc.).

MDVPN Service Instance Testing and Closure of Service Request

When receiving notification of each peer NREN domain's initiator, the NREN triggers the testing of the service. If the testing of the requested MDVPN service instance is successful, the initiator NREN will inform the end-users using the email list (for example, VPN-ASTRO-operation@MDVPN.dante.net) of the progress of the deployment. The progress is reported on the ticket, and once all the NRENs have provided the VPN, the initiator NRENs will change the status of the service order to 'activated', and could initiate the Close Service Order process.

The initiator NREN will update the MDVPN service repository with the data from the installed service instances and inform the AMI that the MDVPN service instance is configured and activated according to the request.

Once the user order is finalised, the initiator NREN Service Desk changes the status of an open ticket to closed. It is also possible for the service to have a partial start before all sites are connected (as the case with L3VPN, where all sites will not be ready at the same time).

Monitoring of Service Provisioning Workflow

The Report Service Provisioning process will continuously monitor the status of service orders, provide notifications of any changes, and provide management reports to the MDVPN Operational manager/MDVPN Service Level Manager during the MDVPN Service Provisioning workflow. The activities inside the Report Service Provisioning process could be implemented using the e-mail list of which the MDVPN Operational manager/MDVPN Service Level Manager is a member, or through the 'watcher' role inside Central MDVPN Ticketing system, etc. Carrying out activities within this process will ensure that all parties involved in MDVPN Service Provisioning workflow are responsible and adhere to the obligations defined in the OLA agreement.

The **MDVPN Technical Management Group** will define which information from the provisioning process needs to be documented, how this data/documents will be available in later phases of the service lifecycle, who will be responsible for management of these documents, etc.

4.3.3 Service Problem Management Workflow

4.3.3.1 *VPN Transport Service Request Problem Management Workflow*

For the VPN transport service, all requests from the NREN to DANTE should be made through the GÉANT Multi-Domain Service Desk (MDSD). DANTE commits to provide the same quality of response to NRENs as offered for its IP service. An interface for problem reporting should be available for the NRENs to allow send/receive notifications about potential disruption of the service to the MDSD.

Consequently, the same parameters and values as for the IP service are applied to the MDVPN, to determine if the NREN request for problem resolution is handled correctly.

4.3.3.2 *MDVPN Service Request Problem Management Workflow*

NRENs will provide to the end users, the same quality of response to users requesting assistance for a problem/issue with MDVPN instances as offered for their regular IP service. The standard NOC procedures used for IP interworking can be used to support the MDVPN service. An NREN can escalate issues to GÉANT or other NRENs as part of the troubleshooting/problem resolution process.

Consequently, the same parameters and values used for the IP service can also be used to determine if the end-user request for problem resolution is handled correctly.

The GÉANT Multi-Domain Service Problem Management workflow described in "Information Schemas and Workflows for Multi-Domain Control and Management Functions" (see Section 4.3 in [GN3 DJ2.1.1]) illustrates the business process interaction for general user-reported, multi-domain service problem management regardless of which type of service is having a problem. This model will be used as a basis to describe the composite MDVPN service user-reported problem management workflow. Process flow is schematically shown in Figure 7.

For this workflow, it is assumed that the user/member institutions of the MDVPN service instance will contact their local NREN service desk (part of MDVPN Service Desk) to report any problems in MDVPN service instance.

It is assumed that every NREN will provide the necessary topological information important for general MDVPN service instance delivery and problem management to other participating NRENs. Technical documentation related to the MDVPN service instance will be available at the central MDVPN Service repository to all participating NRENs. (e.g. MDVPN Knowledge Base integrated in GÉANT MDSD Knowledge Base, MDVPN wiki platform, MDVPN web portal, etc.)

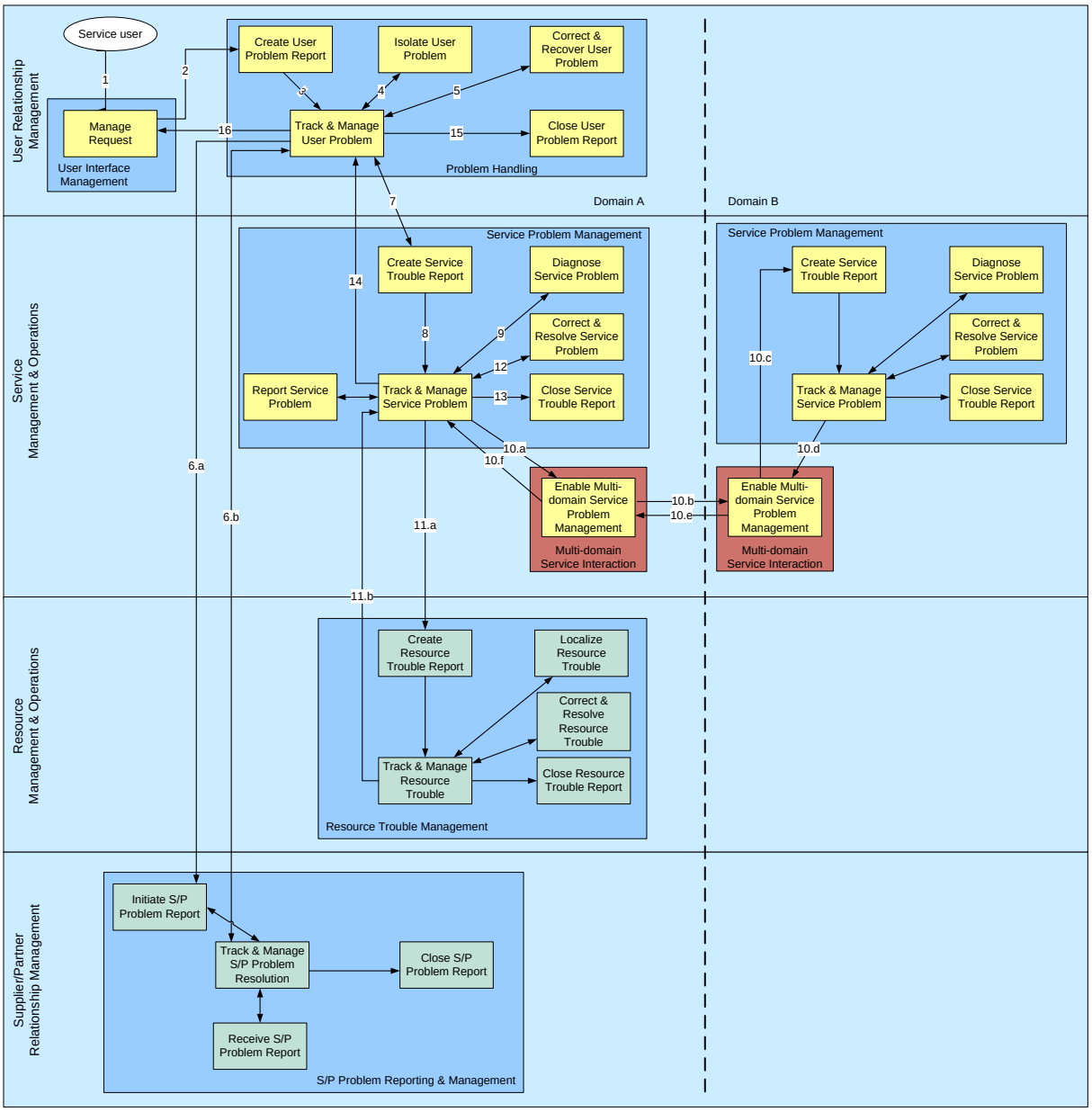

Figure 7: MDVPN Service user-reported problem management workflow

End-user Problem Report

The MDVPN Service end-user-reported problem management workflow starts when end-user reports a problem with the MDVPN service instance. Every participating institution of the MDVPN service instance could report a

problem in delivery of service and request a resolution from the local NREN Service Desk. The local NREN Service Desk is responsible for collecting the required problem-related data (e.g. user problem description, MDVPN service instance ID, contact details, authentication information, etc.). Problem reporting will be performed according to the existing local NREN rules (e.g. phone call, service portal, e-mail etc.) for their users.

The local NREN Service Desk extracts and transfers captured information from the user problem request and creates a record of provided information (End-user Problem Report) for later problem solving (e.g. trouble ticket in local NREN ticketing system, etc.).

User Problem Isolation and Recovery Activities

The local NREN Service Desk will isolate the user problem and eventually identify its root cause (e.g. is the problem in the service domain of the MDVPN service, caused by the improper use of the MDVPN service by the user, or is it caused by a problem linked to the underlying services, etc.).

After successful isolation of the root cause of a problem, the local NREN Service Desk must inform the Service Desks of other involved partners (participating NRENs, GÉANT, Regional Network) regarding the problem. This MDVPN service problem notification will improve the efficiency of issue resolution inside the MDVPN service instance, and will inform participating NREN domains about the existence of problems in the functioning of service. Notification could be sent to the operation VPN e-mail list. Notification form, structure and all information that needs to be included in a message will be defined by the MDVPN Technical Management Group.

Once the user problem is isolated, the local NREN Service Desk process triggers correction and recovery activities. Objective of these activities is to restore MDVPN service to a normal operational state as efficiently as possible. Depending on the root cause of problem, activities may include educational interaction with end-users to ensure correct usage of the MDVPN service, initiating request to enabling services supplier for restoration and recovery or identification of restoration activities inside the MDVPN service instance operation management processes.

The MDVPN service is provided in a specific and complex GÉANT Service Area environment, where the Transport VPN service (enabling service for core MDVPN service) is managed by GÉANT/DANTE. If the user problem is caused by a problem linked to the Transport VPN service, the local NREN will initiate a request to the GÉANT NCC for restoration and recovery of the Transport VPN service, and will further coordinate, track and manage GÉANT/DANTE problem resolution activities. The GÉANT/DANTE will inform all NREN domains about cause of problem and estimated time for resolution through the GÉANT MDSD function.

Service Problem Diagnostics and Resolving Activities

If the end-user's problem is caused specifically by the MDVPN service, the local NREN Service Desk creates a Service Problem/Trouble Report (e.g. change trouble ticket owner from Service Desk to 2nd level NREN NOC, open a trouble ticket on the Central MDVPN Ticketing system or create a new item on the Central MDVPN Service Repository, etc.). The local NREN NOC will further co-ordinate necessary activities in order to guarantee that all tasks are finished at the appropriate time and in the appropriate sequence.

The local NREN NOC performs diagnostics, tests and various audits against specific MDVPN service instances in order to detect the root cause of the service problem. During diagnostics, the NREN NOC will use MDVPN Service Instance documentations (e.g. maintained centrally on the MDVPN Service repository or maintained

locally by every participated NREN, etc.), which contain the necessary information about the service instance (topology information, participating domains, IP addressing, etc.) and developed MDVPN general monitoring tools. The local NREN NOC will update the Service Problem Report during and after the root cause has been identified. After diagnosing the service problem, all participating NRENs have to be informed about the cause of problem and status of the Service Problem Report.

The service problem can be caused by a problem in some of the underlying services. In this case, the local NREN NOC initiates trouble reports for the underlying services and continues to monitor the progress of their resolution.

If the diagnosed service problem process shows that the problem is located in other domains, the local NREN NOC creates the appropriate Service Trouble Report in those domains involved in the provisioning of the service instance. (e.g. e-mail notification on mailing list, e-mail notification to the peer NREN domain, trouble ticket in Central MDVPN ticketing system, etc.). This, in turn, will trigger the creation of Service Problem Report in the peer domains.

Peer NREN NOCs will coordinate actions for resolving the service problem in the remote domains. Once the problem is solved in the peer domain, peer NREN NOC will inform the NREN NOC in the originating domain of the results of troubleshooting and recovery activities.

Regardless of the nature of the MDVPN service failure, the local NREN NOC will resolve or be informed about successfully resolving the underlying cause of issue. This will restore the MDVPN service instance to a normal operational state.

Closure of User/Service Problem Report

After the successful resolution of the service problem, the local NREN NOC triggers the closing of the Service Problem report (e.g. updates the status of open trouble ticket at Central MDVPN Ticketing system, notifies peer NRENs regarding the resolution, etc.). The local NREN Service Desk initiates the closing of the User Problem Report (e.g. close trouble ticket in local NREN Ticketing system etc.) and informs the user's institution about repair and restoration activities and successful resolution.

Monitoring of Problem Management Workflow

The Report Service Problem process will continuously monitor the status of service trouble report, provide notifications of any changes and provide management reports (i.e. reports about the problem that occurred, the root cause and the activities carried out for restoration) to the MDVPN Operational manager/MDVPN Service Level Manager during the MDVPN Service Problem Management workflow. The activities inside the Report Service Problem process could be implemented using the e-mail list where the MDVPN Operational manager/MDVPN Service Level Manager is a member, or through the 'watcher' role inside the Central MDVPN Ticketing system, etc. Carrying out activities within this process will ensure that all parties involved in Problem Management workflow will take responsibility and adhere to the obligations defined in the OLA agreement.

4.3.4 Termination / Change Management

Changes to the existing service instances or termination of service instances have to be coordinated with the service desks (the NREN's NOC and MDSD). The service desks coordinate the integration of monitoring information (for example, maintaining the weathermap service).

4.3.5 VPN Log for Accounting

The provisioning of VPN for the end users is within the scope of the NRENs, nevertheless, the NRENs should provide to DANTE data about L3VPN and L2VPN instances that were set-up during each quarter. The purpose of this log is to help DANTE to show the usefulness of this service, by publishing overall usage figures.

4.4 Service Availability Target

Service availability is defined as the availability of the service instance measured individually between SDPs for delivering the service. i.e., if one of the SDPs fail in a multi-site VPN, the availability of the service should be reduced. Because of chain topology between SDPs, each NREN should make every effort to provide this parameter in their domain at highest level. It is strongly recommended that each NREN offers availability higher than **98%**. Multi-homing of end user sites together with multiple paths in multi-domain network, is recommended in order to increase network redundancy and thus availability.

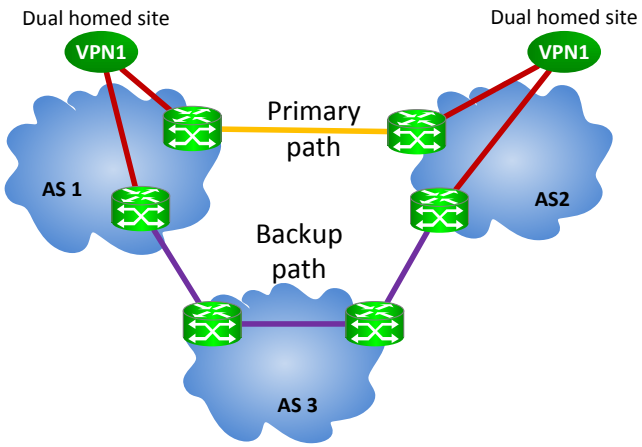

Figure 8: Multi-homed end user site and redundant paths in multi-domain networks

In scenario presented in Figure 8 AS 3 must be aware of rerouting traffic from services provided by AS 1 and AS2.

4.5 Service Capacity Target

There are a number of dependencies when working with service capacity. First, the delivered capacity depends on NRENs; the specified capacity of the service (as per user request) shall be delivered within the following limitations:

- Capacity between any two SDPs should be delivered with 99% throughput for capacities up to 1Gbps.
- Capacity between any two SDP should be delivered with 95% throughput for capacities up to 10Gbps.

The computation could be done over a period of one month, every month. The above results can be achieved, assuming that no other traffic is forwarded from/to those two SDPs. If the above limits are not delivered, the service will be considered as out of service/degraded performance.

Second, because all the VPNs are merged at the SSP, the delivered capacity also depends on SSP capacity deployed between a NREN and GÉANT and between NRENs. The SSP capacity must be great enough to allow lossless traffic exchange for the services it is used for.

A key issue relating to capacity, which must be solved, is traffic policing and traffic bursts. The devices installed on both sides can use different mechanisms to perform traffic policing. The differences may be related to the current value of the bandwidth limitation (rate-limit) applied to the SSP (interface) and the way in which the traffic amount is calculated. These parameters are platform related, so it is not possible to provide strict values for all devices.

General recommendations for SSPs are:

- Egress traffic shaping.
- The ingress rate limit together with burst value should be applied in the agreement with a neighbouring NREN.
- Traffic scheduling according to ToS/DSCP marking could be applied to egress SSP.

General recommendations for SDPs are:

- The ingress rate limit should be applied on SDPs.
- The values for burst size should be adjusted to individual requirements of each service.
- Traffic scheduling according to ToS/DSCP marking could be applied to egress SDP.

The above recommendations are not obligatory for participating domains, but should be carefully considered before deploying an MDVPN service, as they ensure the requested bandwidth (or capacity) end to end is delivered from the joint service provider.

4.6 Conduit Parameters

The MDVPN service requires that some parameters remain unchanged across domains. These parameters include the Maximum Transmission Unit (MTU) and capacity.

In order to avoid segmentation and reassembly, the end user should specify the minimum acceptable value of the MTU for IP packets, which will be transferred between sites.

The second conduit parameter is capacity, which defines data rate for the end user transmission on each SDP. Additionally, the end user should specify bandwidth required for transport between particular SDPs. In order to avoid data loss, the QoS mechanism can be applied on the SDPs and SSPs.

Parameter	Description	Value	Default
MTU	The requested Minimum Transmission Unit, including the header bytes (but not the preamble and the FCS)	At SDP: 1500 bytes (up to 9180 bytes if available) At SSP: Jumbo Frame should be allowed, 9180 bytes	By default, the MTU will be set to 1500 octets for IP packets and presented to the end user. The end user can request to setup MTU for maximum available size.
SSP Capacity	The rate of bits that will be accepted at the ingress point, in terms of Mbps.	Should meet summary requirements for all services provided over SSP	Physical interface capacity
SDP Capacity	The rate of bits that will be accepted at the ingress point, in terms of Mbps	100 Mbps to 10 Gbps in 50 Mbps increments	*<100 Mbps>*
Inter SDPs traffic rates	The rate of bits that will be sent between pair of SDPs	100 Mbps to 10 Gbps in 50 Mbps increments	*<100 Mbps>*

Table 1: GN3plus MDVPN service supported conduit parameters

Note that the SSP can be setup on a physical interface connecting two NRENs. This interface can be shared between many services provided by NREN (for example commodity IP, BoD, and MDVPN). The capacity allocation on physical interface should allow meeting all requirements for all services.

For multipoint VPN service, the end user should describe the required and estimated traffic flow sizes between SDPs. This will help to ensure appropriate capacity in the NREN's core network and on SSPs. In case the end user is not able to determine traffic flow, the NRENs should provide capacity for worst-case of traffic distribution between all SDPs' Technical Service Specification.

5 Technical Service Specification

5.1 Service Architecture

The MDVPN service is reliant upon MPLS technology. It is also built on well known, standard-based signalling protocols. Thanks to this approach, the service architecture, operation and maintenance should be clear and straightforward for NREN staff aware of VPN technologies.

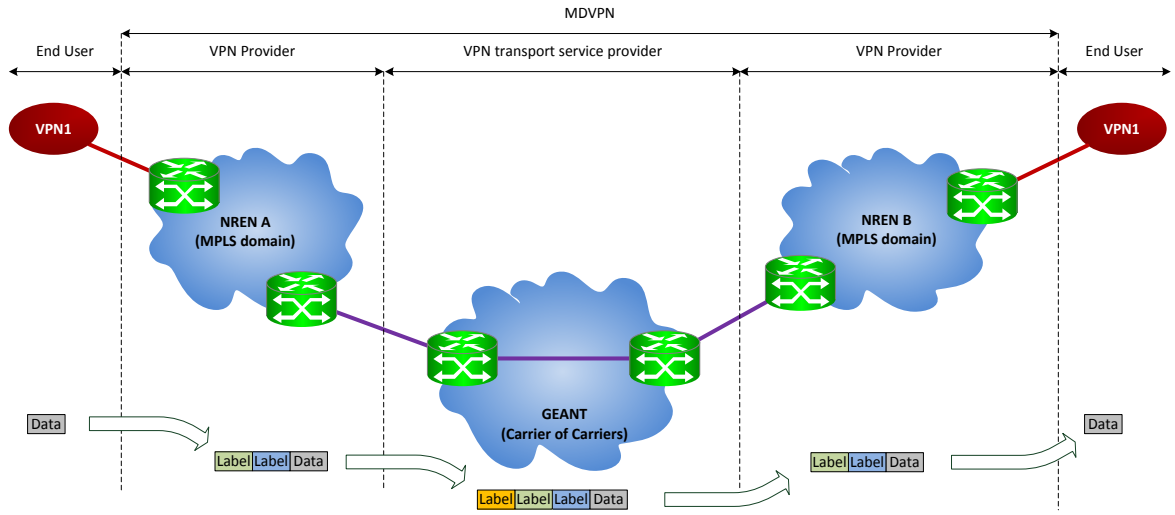

Figure 9: MDVPN service concept

Figure 9 shows the general concept of using MPLS technology to deploy the MDPVPN service. Note that it only covers the basic concept of data delivery for end users. All technical details are given in this chapter.

5.1.1 Operation Modes

The MDVPN service is capable to operate in two modes, depending on the interconnection type between NRENs:

- VPN multiplexing
- Back to back

In general, the VPN multiplexing mode assumes that NRENs are connected with SSP supporting MPLS technology and label exchange protocols are shared among all VPNs. When using Back-to-Back mode, the VPN

instances are connected on SSP with dedicated logical subinterfaces (or dedicated physical interface) without support for MPLS switching. Additionally, in case of L3VPN, individual BGP sessions are required between neighbouring VPN instances, providing prefix exchange inside each VPN network.

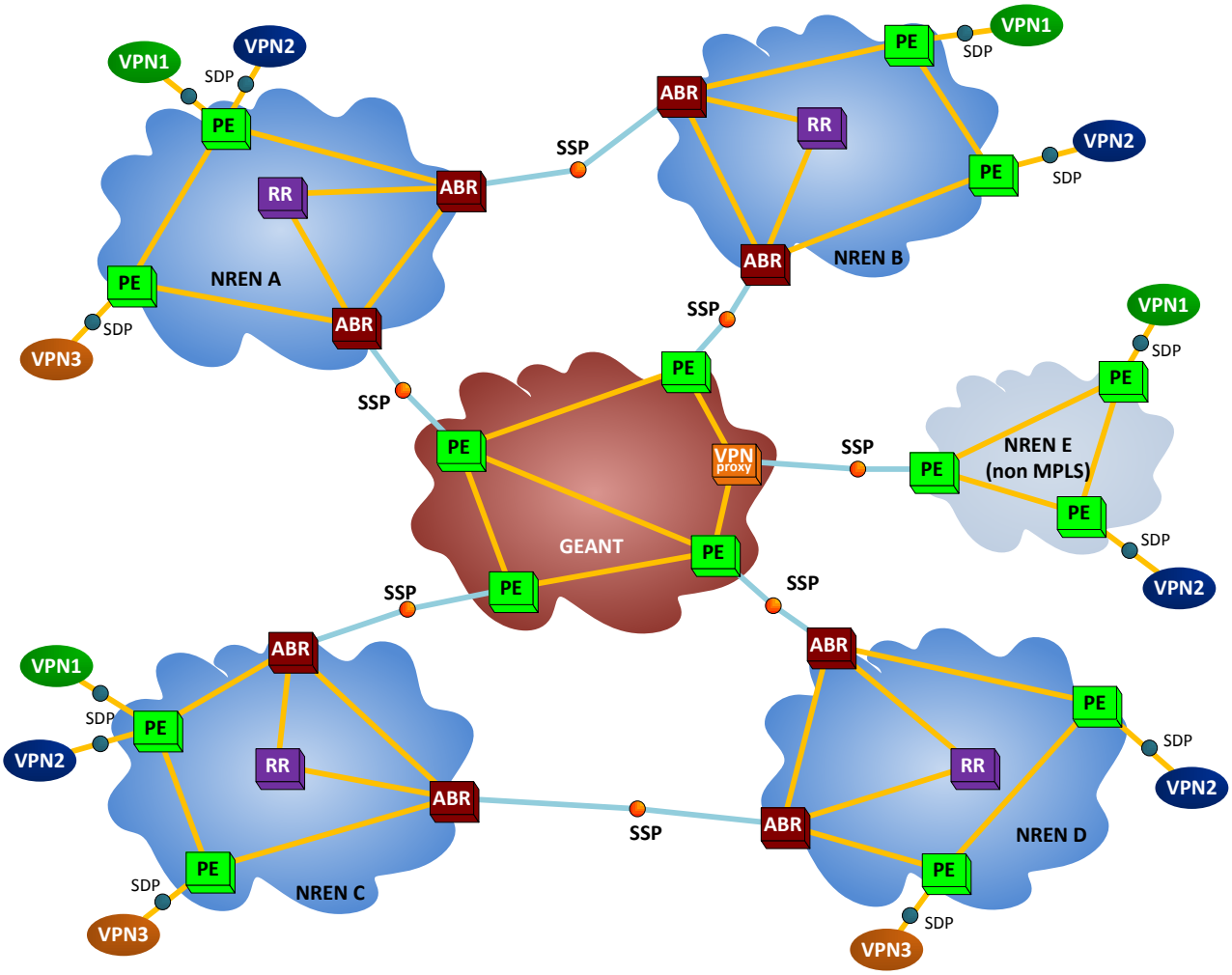

Figure 10: MDVPN service overview

5.1.1.1 *VPN Multiplexing*

This mode requires that participating NRENs support MPLS switching on SSP (labelled unicast peering). However, within the GÉANT network, the **Carrier of Carriers** (CoC) service will be provisioned, providing transparent transport of VPN traffic.

5.1.1.2 *Back to Back*

This mode is designed for NRENs that do not support MPLS switching on SSP. In order to allow them to participate in the MDVPN federated service infrastructure, these VPNs must be **stitched to the service in Back-to-Back mode (Option A RFC 4364)**. This means that on SSP, each VPN that a NREN would like to transport,

has its own subinterface identified with a service delimiter (e.g. VLAN ID). The traffic and signalling for a particular VPN is exchanged over this subinterface, and typically, a standard BGP protocol with VPN extension will be enabled for each VPN instance.

5.1.2 Control Plane Architecture

For the MDVPN service, two key signalling elements must be properly setup:

- Signalling for multi-domain MPLS path between PE routers.
- Signalling for VPN labels (and prefixes, if it results from the service properties) exchange between PE routers.

The main goal of the first element is to provide PE with the label it should use in order to reach other PEs (to which remote site of VPN network is connected to). The signalling architecture for multi-domain MPLS path between PE routers is the same for all MDVPN service options (L2/L3 VPNs). This is possible because of the independence of the payload carried in MPLS packets. It is sufficient to establish a single transmission path that can be used to reach other PEs, in order to send over it different kinds of traffic (e.g. IPv4, IPv6 packets or Ethernet frames).

For that purpose, the labels allowed to reach a particular PE must be exchanged between domains. This will be achieved by using BGP labelled unicast protocol between NRENs and GÉANT. Note that this process is independent from a label exchange mechanism used inside a NREN network.

The main goal of having a second signalling element is to provide PE with labels, which will be used in order to differentiate VPN traffic and assign it to the appropriate VPN instance. The signalling architecture used for VPN labels exchange can differ depending on preferences of particular NRENs. The labels for all services can be exchanged with BGP protocol. For some services (L2VPNs) it can be done using the LDP protocol.

Figure 11 shows the signalling elements needed in order to provide data transmission between two end-user sites in case of routed services (L3VPN).

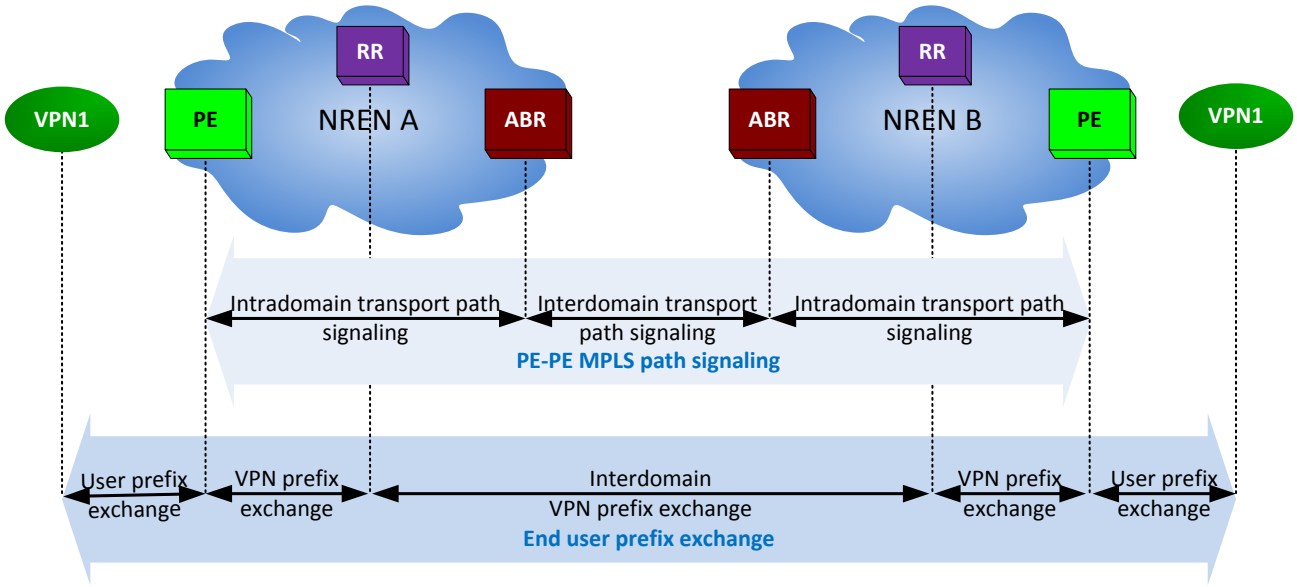

Figure 11: MDVPN service signalling architecture (L3VPN case)

Figure 12 Shows signalling elements needed in order to provide data transmission between two end-user sites in case of L2 services (VLL/VPLS), if LDP is used. In this case, it is possible to use direct signalling between PE routers in order to setup an L2 transmission service.

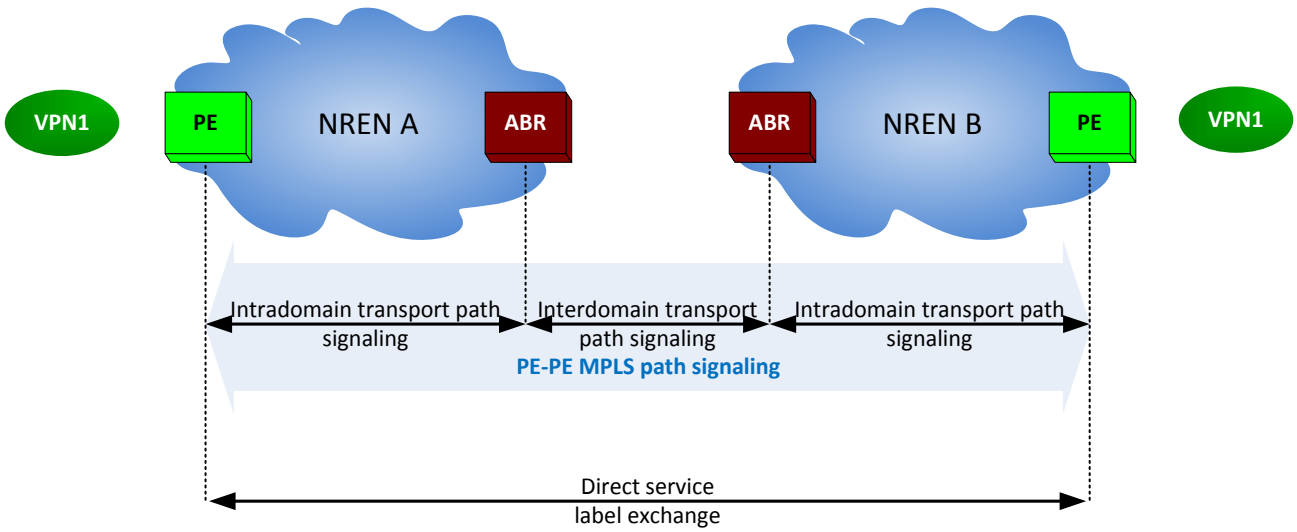

Figure 12: MDVPN service signalling architecture (L2VPN case)

5.1.2.1 *Signalling Transport Path*

In a MPLS environment, it is important for each PE router to know the label that should be used in order to reach another PE. In a single domain, this is usually achieved by using one of label distribution protocols (e.g. LDP or

RSVP). However, in a multi-domain environment, other mechanisms must be used in order to assure security and scalability. These requirements are met by BGP labelled-unicast protocol.

The main goal of using BGP labelled-unicast protocol as a basis for the MDVPN service is the **distribution of labels for all PE routers** in all domains used to provide services for end users. Be aware that a PE's label will change according to domain.

The mechanism is called BGP labelled unicast and is described in RFC3107. In this case, BGP is used to distribute a route to a particular PE, along with an MPLS label that is mapped to that route. The label mapping information for a particular route is 'piggybacked' in the same Multiprotocol BGP-4 Update message that is used to distribute the route itself.

Label mapping information is carried as part of the NLRI in the Multiprotocol Extensions attributes. The AFI indicates the address family of the associated route. For the NLRI containing a label, a SAFI value 4 is used.

Note that on Figure 10 the link between NREN and GÉANT is established between ABR (NREN site) and PE (GÉANT site). This is explained in Section 5.1.3.

5.1.2.2 *Signalling VPNs*

When the PE router knows the label to reach other PEs, it is required to exchange additional labels (L3VPN and L2VPN labels), used to differentiate particular services. These service labels can be exchanged between PEs using different mechanisms.

One of the most popular is the BGP protocol, which can support label exchange for L3VPN and L2VPN services. Using the BGP protocol allows NRENs to re-use some existing policies already implemented for IPv4/IPv6 routing. It also introduces high scalability solutions such as **Route Reflectors**. Therefore, the only supported protocol for L2VPN and L3VPN label exchange is BGP.

However, in case of simple L2 services, the LDP protocol can be used for service label exchange. The service labels are exchanged between PEs using **targeted LDP sessions**, making the solution very intuitive and simple.

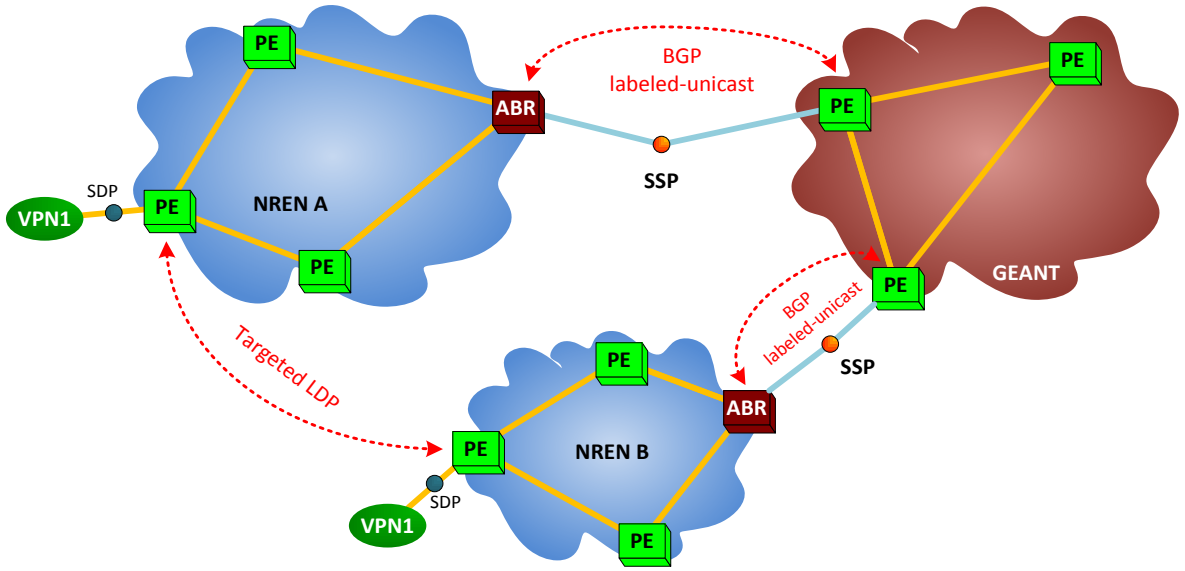

Figure 13 Label exchange in MDVPN service (using LDP protocol for L2 VPN services)

5.1.3 GÉANT Domain

In order to enable the MDVPN service, at least two NREN networks must be connected. This can be a direct connection or, as in most cases, through the GÉANT network.

The GÉANT network will provide transparent transmission and signalling exchange for any MDVPN service participant. Additionally, GÉANT will provide resources that will enable transatlantic cooperation and a means of connecting NRENs that currently don't support MPLS technology.

5.1.3.1 *GÉANT Carrier of Carriers*

In general, NRENs in Europe are connected together through the GÉANT network. In order to improve GÉANT's, a Carrier of Carriers (CoC) VPN will connect resources of NRENs who have joined the MDVPN service.

The Carrier of Carriers is an interprovider VPN solution, built upon the following standards:

- RFC 3107, Carrying Label Information in BGP-4
- RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 5601, Pseudowire (PW) Management Information Base (MIB)
- RFC 5603, Ethernet Pseudowire (PW) Management Information Base (MIB)
- RFC 6368, Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs).

The key difference in terms of multi-domain interoperability for CoC is that, in the GÉANT network, the dedicated VPN network will be provisioned in order to connect several NRENs. Hence, the BGP-labelled unicast session between a NREN and GÉANT will be established not as an ABR-ABR (AS Border Router) session but as ABR-

PE session. Simply, the NREN network will function as a CoC VPN end user. This approach introduces a hierarchy which maintains great network flexibility and a peer model in NREN cooperation.

5.1.3.2 *VPN Proxy*

Deploying a CoC solution in the GÉANT network would, in theory, prevent GÉANT from providing MDVPN services for end users directly connected to the GÉANT network or to connect NRENs that do not support MPLS and BGP labelled unicast.

In order to overcome this limitation, a proxy system will be defined, which will provide access to the Carrier of Carriers VPN. This system is called VPN proxy. It will be implemented as dedicated hardware or logical system within GÉANT network.

The VPN proxy will be connected to the CoC VPN as a regular NREN network. The only difference is that it will use an iBGP labelled session (instead of eBGP). This is because both systems (CoC PE and VPN proxy) will be configured with the same AS number. However, thanks to the CoC VPN, the VPN proxy will not interfere with GÉANT systems outside the VPN.

The end users connected directly to GÉANT, which can be partners outside the GÉANT service area or NRENs connected in back-to-back mode, will peer directly with the VPN proxy. The VPN proxy will then provide MPLS transmission to other members.

5.1.3.3 *VPN Route Reflector (VR)*

The labels for particular VPN services provisioned with BGP protocol, will be exchanged between domains through a VPN Route Reflector (VR). The VR will be provisioned on two VPN proxy systems and peer with all participating NRENs through a multihop eBGP session.

The main role of the VR is to redistribute to all participating NRENs all VPN prefixes without changing the next-hop. Note that the VR is not a regular route reflector (such as the case in an iBGP scenario). It will maintain external multihop BGP sessions to NRENs.

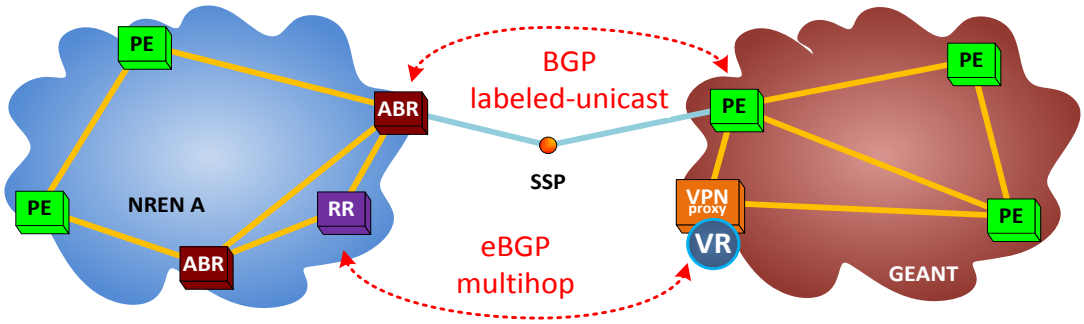

Figure 14 Label exchange for MDVPN service (using BGP protocol)

5.1.4 Domain Borders

5.1.4.1 *Service Demarcation Points (SDPs)*

There will be at least one Service Demarcation Point for each VPN site. During the service setup phase it is necessary to list all SDPs, along with the required bandwidth. Keep in mind the required bandwidth depends on the VPN's data flow, for instance, several sites can send their traffic to one site. The parameters of underlying (Layer 2) technology must be defined before setting up the SDP for MDVPN service. An example of typical options set for Ethernet interfaces is:

- Untagged interface
- Single tagged interface
- Double tagged interface.

Note: Multiple SDPs can exist on the same physical router interface. For example, different VLAN IDs can be used to provide services for multiple-end users connected to the router through a Layer 2 switched infrastructure. Moreover, in order to extend the service's scope, it is strongly recommended to consider sharing SDPs together with the BoD service.

Additionally, in case of a Layer 3 VPN, the routing protocol for SDP can be selected. It is possible to use a dynamic routing protocol or static routing on SDP. In order to avoid routing information redistribution, it is recommended to use the same routing protocol inside a MDVPN service instance across all sites.

It is also recommended for NRENs to set rate limits on ingress interface (SDP) in order to avoid network overload by unwanted (uncommitted) traffic. The end user should be notified and the use of egress traffic shaping (and queuing based on ToS/DSCP tags) is recommended.

It is **not recommended** to set rate limits on an egress interface (SDP) in order to avoid traffic loss. It is recommended to use egress traffic shaping and queuing based on ToS/DSCP tags.

5.1.4.2 *Service Stitching Points*

The Service Stitching Points (SSPs) connect participating domains and provides data exchange for multi-domain services. SSPs differentiate neighbouring domains (for example, NREN networks). It must be noted that domains are free to use equipment and transport technologies of any kind, only with the assumption that they will be able to carry end user traffic and maintain appropriate signalling protocols. This makes SSPs very sensitive to the type and characteristics of transported traffic. In general, two types of SSPs can be used:

- **SSP with MPLS technology and BGP labelled unicast protocol enabled (VPN multiplexing).** This SSP can use existing a peering interface between two domains (NRENs) in order to exchange end user traffic and signalling information (PE routers loopback addresses). This is described in Figure 15, below.

- **SSP with back-to-back VPN connectivity**. These SSPs directly connect a particular L3VPN instance defined in one domain (NREN) to an appropriate instance defined in a neighbouring NREN. Routing information is exchanged with BGP protocol session established for each VPN instance (Option A).

Service delimiter (e.g. VLAN ID) is required on SSPs using back-to-back connectivity, in order to allow differentiation between many service instances. This scenario is illustrated in Figure 16.

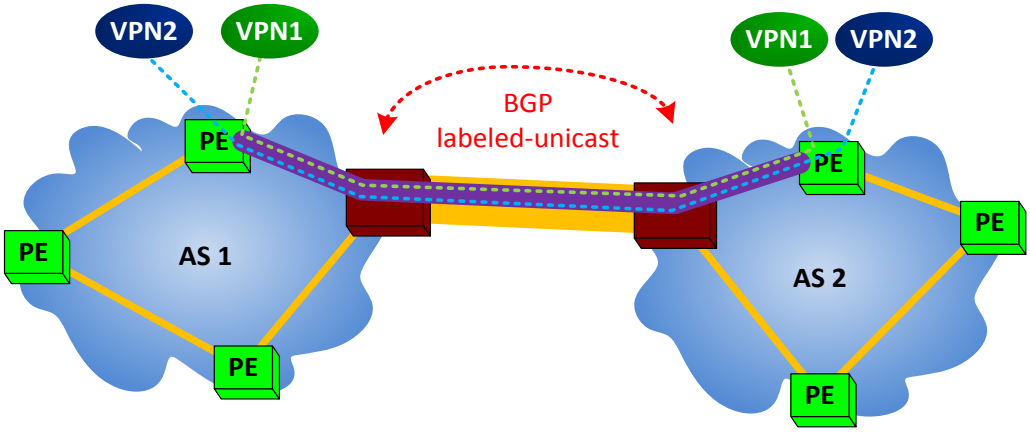

Figure 15 SSP with MPLS technology (VPN multiplexing)

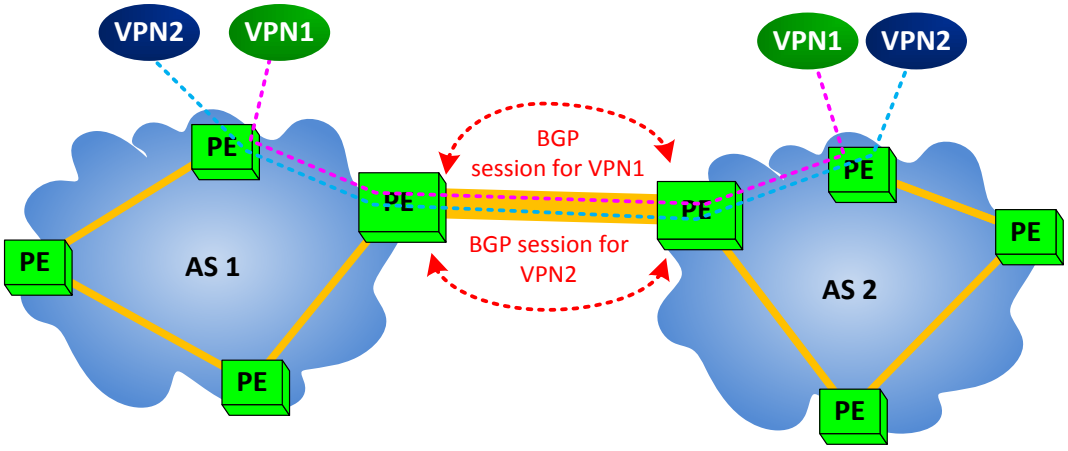

Figure 16 SSP with back-to-back connectivity

5.2 Service Operation and Maintenance

5.2.1 Joining the MDVPN Service Area (VPN multiplexing)

5.2.1.1 *SSP setup*

SSPs will be setup according to standard NOC procedures used by NRENs and GÉANT. During the setup phase, it is required to provide appropriate resources that will be used by the service. Appropriate bandwidth should be provisioned in each domain.

In order to setup an SSP (in VPN multiplexing mode), the following steps should be taken:

1) Establish and verify an L2 link (on physical interface or logical subinterface).
2) Assign IPv4 addresses for that link (usually /30 subnet).
3) Allow labelled packet on the interface.
4) Establish BGP labelled unicast session:
    a. Exchange AS numbers
    b. Enable next-hop mapping for IPv6 (if wanted/needed).

Once the eBGP-labelled unicast session is established, the interface and BGP session status, should be added to monitoring systems by each NOC.

5.2.1.2 *VPN Label Exchange Setup*

In general, it is strongly recommended to use the VPN Route Reflector (VR) in order to exchange VPN labels with NRENs. However, it is also possible to establish direct eBGP multihop sessions between NRENs by partners exchanging the following set of parameters:

- Loopback interface IP address
- AS number
- Supported address families for exchanged prefixes (IPv4 unicast VPN by default)
- Prefix limit (if applied).

Additionally, partners may exchange community values and their purpose.

Once the eBGP multihop session is established, each NOC should add it to monitoring systems.

5.2.2 Joining the MDVPN Service Area (Back-to-Back)

In order to setup a SSP (in back-to-back mode), the following steps should be taken:

1. Establish and verify an L2 link (on physical interface or logical subinterface).
2. Assign IP addresses for that link. In most cases the IP addresses will belong to a particular VPN instance, so it should be assigned by end user technical staff, in order to avoid conflict (overlapping).
3. Establish BGP session:
    a. Exchange AS numbers.

Once the eBGP session is established, the interface and BGP session status should be added to monitoring systems by each NOC.

5.2.3 Maintaining the Service

5.2.3.1 *Route Target Management*

For L3VPN, the NRENs should coordinate themselves in order to be able to choose a unique route target. It is recommended that the originating NREN will assign a globally unique RT by using its AS number or a public IP

address as part of the RT. Additionally, the Route Target database should be maintained to allow one-to-one matching between the name of the L3VPN and Route Target, (GÉANT/DANTE could be the appropriate institution for this task). This will be very useful for all NOCs involved in any service instance troubleshooting. The route target used and its match with L3VPN should be published by DANTE on a website.

The RT Constrained Route Distribution (RFC 4684) should be used. This functionality allows PE routers to import only prefixes for which there is an importing VRF. So it improves the quality of the deployment as it detects RT misconfiguration. It also avoids waste of processing power on VR and PE devices. With this feature VR will send only wanted VPNv4/v6 prefixes to PE routers. It could also be useful to configure RTC for the connection between NREN RR and NREN PE routers.

5.2.3.2 *Monitoring the Service*

Monitoring a multi-domain VPN service instance is difficult because of three major issues:

- Decentralised network management
- VPN traffic isolation
- VPN is transparent for VPN transport provider (GÉANT).

In a multi-domain environment, each participant uses independent hardware platforms and management systems. Despite availability of well-known protocols such as SNMP or NETCONF, it is not possible to access all network elements involved in a particular service delivery. This makes the network view incomplete from a single management system point of view. At present, there are no mature distributed management systems that could provide appropriate functionality.

One of the features of the VPN service is traffic isolation, which excludes the ability to perform advanced active measurements for a particular VPN instance. In order to provide a highly reliable multi-domain VPN service, it is possible to use existing tools and procedures, to provide a wider view of the service. Some sampling mechanism (e.g. IPFIX, sFlow) could also be used in order to collect more detailed data.

Moreover, the state of the protocols enabled on SDPs and SSPs should be monitored.

Day-to-day monitoring

MDVPN monitoring is performed in order to detect problems that may affect the service level specification or that can lead to service degradation. The day-to-day monitoring data should help the service provider in mitigating/solving those deteriorations.

A live state of accessibility regarding each PE must be available. A specific L3 VPN instance (‘ping_VPN’ instance) will be setup on all PEs, and it is strongly recommended that participating NREN join this ‘ping_VPN’ instance. This VPN will be used for diagnostic purposes and can help to troubleshoot issues in underlying infrastructure (MPLS forwarding and/or signalling). The NREN should provide at least a single IP address that can be used for simple ICMP tests (ping/traceroute). A central tool (kind of smokeping) must also be installed in order to check the availability of the PE through the ‘ping_VPN’.

NRENs may also want to install some active measurement equipment and share the results with other participants (e.g. those using PerfSonar).

A VPN Reflector will be deployed and will centralize the L3VPN routes of NRENs that want to use it. A Looking Glass service for the VPN Reflector will help to troubleshoot the VPNs signalling (route announcement and reception).

Statistics Monitoring

The VPN transport provider (GÉANT) is not able to distinguish the different VPNs. Thus at GÉANT level, only SSP availability and usage (throughput statistics) will be provided. The traffic carried by a particular VPN instance can be monitored, at least at interface (SDP) level. It is up to the NREN to provide statistics on their SDP. NRENs and GÉANT cannot provide a general view of VPN usage, so it will be the responsibility of end users to decide if it is necessary, and which tool they will use.

The MDVPN technical management group and MSDS will detail the different statistics that should be collected at SSP level and at SDP level. They will also explain how it should be published (where and who can access to it).

5.2.3.3 *Topology Service*

It will be useful, either for end user access or for day-to-day monitoring, to be able to know the location of the service access points, based on a list of Points of Presence (PoP) within the NRENs where the service is available. Therefore, the NRENs must provide a list of their PoP and the 'ping_VPN' loopback address of the Provider Edge.

5.3 Infrastructure Security

The services will be offered jointly using a distributed, multi-domain infrastructure. Many kinds of information will be exchanged between domains, which can significantly influence network stability. Therefore, it is important to keep this information exchange as stable and secure as possible.

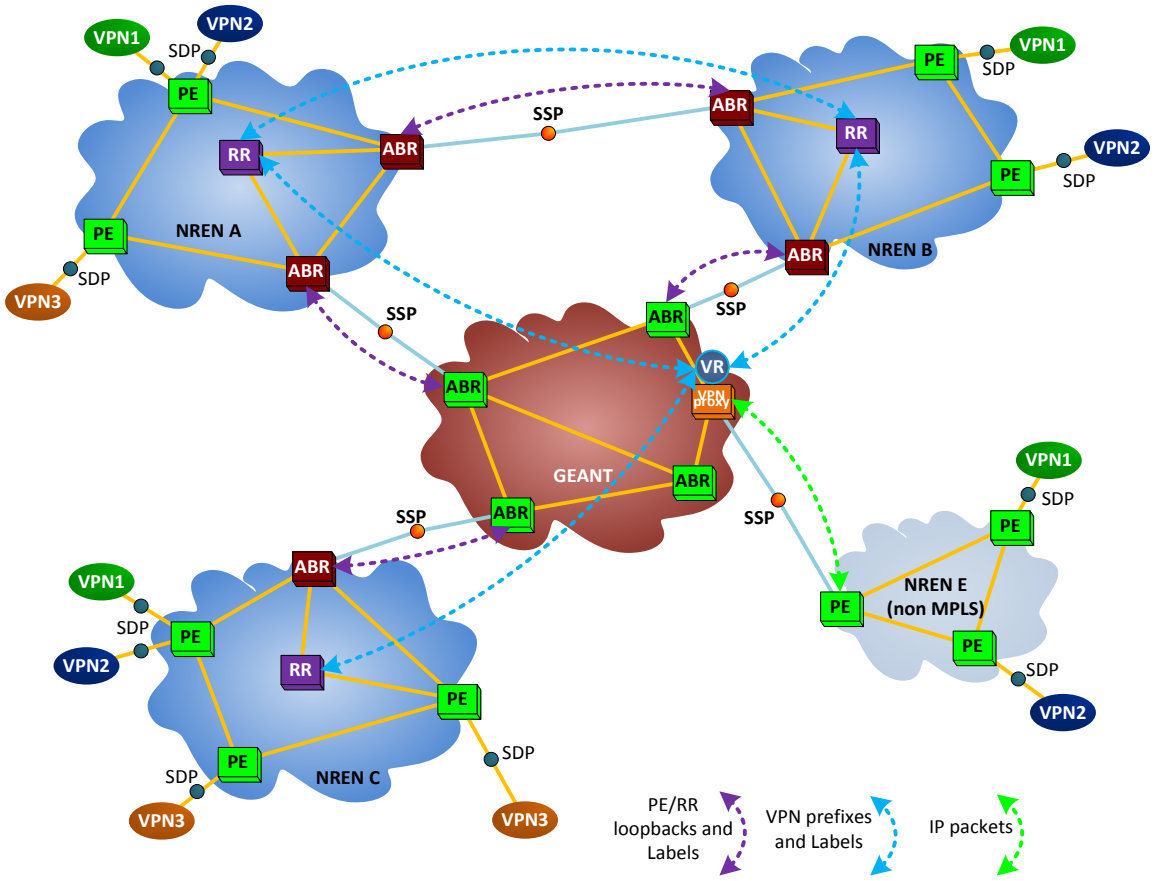

Figure 17 Relations between control plane elements

Security measures are defined for two possible modes of operation: VPN multiplexing and back-to-back. The following major aspects are considered from a security point of view:

- For VPN multiplexing mode:
  - SSP connection – Peers establish eBGP connections to exchange IPv4 routes with labels (violet line). Possible cases:
    - NREN ABR – GÉANT ABR
    - NREN-A ABR – NREN-B ABR
  - Service label exchange – Peers establish connection to exchange labels for particular services, L3VPN or L2VPN (blue line). Possible cases:
    - NREN RR – VR
    - NREN PE – VR
    - VPN Proxy – VR
    - NREN-A RR/PE – NREN-B RR/PE
  - CPE level – recommended security measures for end users.
- For back-to-back mode:
  - Connection between VPN Proxy and non-MPLS NREN PE (green line).

Security measures are listed and described in the following text. Every measure is marked as one of following:

- Required – implementation of a measure is mandatory.
- Recommended – a measure is optional, but strongly recommended.
- Optional – the item is truly optional.

5.3.1 Security Measures for VPN Multiplexing Mode

5.3.1.1 *SSP Connection*

Possible cases:

- NREN ABR – GÉANT ABR
- NREN-A ABR – NREN-B ABR: Two NRENs have BGP connections established in order to exchange only their own prefixes and the prefixes of the PE routers of their regional networks or other NRENs that do not have direct connection to GÉANT.

On the control plane, these peers exchange IPv4 routes with labels via eBGP. The purpose is to exchange the labels that should be used in order to reach PE routers. The control plane can be secured with the following measures:

- **Filtering**
  - Prefix filtering:

- Outbound filter on NREN ABR (**required**) – The peers need only to exchange /32 prefixes for the NREN RR and PE router. The route policy filter should be configured on NREN ABR router to match only /32 prefixes. This route policy filter should be applied to BGP neighbour (on NREN ABR to GÉANT ABR, or on NREN-A ABR to NREN-B ABR) outbound.
- Inbound filter on NREN ABR (**recommended**) – Since NREN ABR router should expect only /32 prefixes from its BGP neighbour, the route policy filter should be configured to match only /32 prefixes and applied on NREN ABR router to its BGP neighbour (on NREN ABR to GÉANT ABR, or on NREN-A ABR to NREN-B ABR) inbound.

○ AS-path based filtering:

- Outbound filter on NREN ABR (**required**) – In the first step of the service deployment, NREN RR and PE prefixes received from other NRENs should not be re-advertised, except in a case when an NREN provides transit to the MDVPN service to other participants (regional networks or other NREN that has not directly subscribed to GÉANT's VPN-transport service).
- The route policy filter should be configured on the NREN ABR router to only match prefixes that are originated from AS of that NREN (The NREN can use the same means as it uses for its IP peering with GÉANT).
- In case an NREN offers the VPN transport service (CoC) for networks behind them, these networks must apply the outbound filter (towards the NREN) that will match only prefixes originated from their AS(s).
- Inbound filter on NREN ABR (optional) – The route policy filter should be configured on an NREN's ABR router to match only the prefixes that are originated from ASs of NRENs that participate in VPN deployed in the inbound NREN, and to filter prefixes originated from ASs of NRENs that do not participate in any VPN deployed in the inbound NREN (for instance, if NREN A doesn't participate in the same VPN as NREN B, NREN B can filter all prefixes announced with AS number of NREN A). If a participating NREN uses more than one AS number or provides transit for other participants, those AS numbers should be registered and included in the route policy filter. For defining AS numbers as-path access list should be used. This route policy filter should be applied on NREN ABR router to its BGP neighbour (on NREN ABR to GÉANT ABR, or on NREN-A ABR to NREN-B ABR) inbound. Note: In the case of a NREN that participates in lot of VPNs it could be difficult to maintain this measure, thus it is marked as optional.

- **Address families** (**required**) – Only the IPv4 labelled-unicast address family should be configured on both peers for the corresponding neighbour (on NREN ABR for GÉANT ABR and vice versa, or on NREN-A ABR for NREN-B ABR and vice versa).

- **Preventing prefix flooding** (**required**) – The maximum number of prefixes for each BGP peer should be configured in order to prevent prefix flooding and memory exhaustion of the devices. Configuration should be done as described in the following:

○ NREN ABR – GÉANT ABR connection – in this case, maximum number of prefixes should be configured on both peers:

- GÉANT ABR – the maximum number of prefixes should be determined according to the number of PE routers for corresponding NREN. The recommendation is 1000 prefixes per NREN.
- NREN ABR – should receive prefixes from all NRENs that participate in the same VPN thus the maximum number of prefixes should be 1000.

- NREN-A ABR – NREN-B ABR connection – the maximum number of prefixes should be configured on both peers:
  - The maximum number of prefixes should be determined according to the number of PE routers for corresponding NREN. The recommendation is 1000 prefixes per NREN.

- **MD5 authentication for BGP** (**required**) – BGP authentication with MD5 should be configured between these peers to validate the peer that sends routing updates, thus protects the BGP connection from being spoofed.
- **Route-flap damping** (**optional**) – Several NRENs used damping for their IP BGP peering with GÉANT, while other NRENs do not use it. As a result, the recommendation is that the NREN is free to use it. The NRENs could, for instance, follow the same rule of their IP BGP peering for their labelled unicast peering.

  Damping reduces the number of update messages sent between BGP peers to reduce CPU load of the peers. If this feature is used, it should be configured on all peers. As a route incurs a penalty of 1000 each time when it flaps it is recommended to configure route flap damping with the following parameters:
  - *Suppress value* – when penalty of the route exceeds this value, the route is suppressed; it should be at least 5000.
  - *Half-life* – penalty of the route decays when this period expires; it should be set to 15 min.
  - *Reuse* – when penalty decreases below this value, the route is unsuppressed; it should be set to 750.
  - *Max-suppressed-time* – the maximum duration for the suppression of the route, after being suppressed for max-suppressed time route becomes unsuppressed; it should be set to 60 min.

  Note: This feature might make troubleshooting more complex.

- **Generalized TTL Security Mechanism, GTSM (RFC 3682) (optional)** – This mechanism compares TTL value of the incoming BGP update with expected value for BGP peer to protect a protocol stack from CPU-utilisation-based attacks. If the received value is lower than expected, it is considered that the packet is bogus and it is discarded. The expected value should be determined for each case separately, based on the topology of the connection between peers (directly connected routers or multi-hop peers).

5.3.1.2 *Service label exchange*

Possible cases:

- NREN RR – VR
- NREN PE – VR
- VPN Proxy – VR
- NREN PE/RR – NREN PE/RR

L3VPN

On the control plane, the peers exchange labels for particular services. The control plane can be secured resorting to the following measures:

- **Filtering**
  - AS-Path-based filtering – routes that will be advertised or accepted should be restricted based on the AS-Path of the route.

- Outbound filter on NREN PE/RR (**required**) – In the first step of the deployment of MDVPN, the NREN should not be re-advertised VPN routes except in a case when NREN provides transit to the MDVPN service to other participants (regional networks or other NREN that doesn't have subscribed directly to VPN-transport service of GÉANT).
- Inbound filter on VR (**required**) – On VR, route policy filter should be configured to accept only routes that in AS-Path have only AS number of the connected NRENs. In case that NREN uses more than one AS number or provide transit for other NREN, those AS numbers should be registered and included in the route policy filter. For defining AS numbers as-path access list should be used. This route policy filter should be applied inbound on VR for all its peers (NREN PE/RR).

  - Filtering based on community (**required**) – There will be a community set definition (assigned by DANTE for MDVPN service) which will be added by NRENs, marking VPNs which should be accepted by VR.
    - Outbound filter on NREN PE/RR – NREN PE/RR will advertise only routes marked with the defined community to VR. This can be done by configuring a route policy filter on NREN PE. This route policy filter should be applied to VR (as BGP neighbour) outbound. This should avoid advertising unwanted (internal) VPNs by NRENs.
    - Inbound filter on VR – VR will accept only routes that are marked with defined community from its peers. Route policy filter should be configured on VR for this purpose and applied inbound to all its peers.
  - Route-target filtering
    - Inbound filter on NREN PE – (**recommended**) this router will receive VPN prefixes with route target(s) that define VPN(s) to which those prefixes belong. If route targets import and export parameter are wrongly configured propagated prefixes, it could lead to wrong prefix importation. To avoid wrongly propagated RTs on NREN PEs, RT filtering should be configured on NREN PE routers to accept only routes with RT that is used by the VPNs configured on this local PE.
    - RT Constrained Route Distribution (RFC 4684) (**recommended**) – VR will send all VPN routes to NREN PE routers. PE routers will import only prefixes for which there is an importing VRF. To avoid waste of processing power on VR and PE devices it is recommended to implement a RTC feature. With this feature VR will send only wanted VPN prefixes to PE routers. It is also recommended to configure RTC for the connection between NREN RR and NREN PE routers.

- **Address families** (**required**) – Since there is no IPv4 routing between these peers, only the VPN address family should be configured on both peers for the corresponding neighbour.
- **Preventing prefix flooding** (**required**)
  - A maximum number of prefixes for each BGP peer should be configured in order to prevent prefix flooding and memory exhaustion of the devices. Configuration should be set up as follows:
    - VR – maximum number of prefixes should be 1000 per peer at the starting of the service. If the number of prefixes exceeds the defined maximum number, the maximum number may be increased according to the end-users' needs.
    - NREN PE/RR and VPN proxy - maximum number of prefixes should be 1000 at the start of the service. If the number of prefixes for VRF exceeds the defined maximum number, the maximum number may be increased according to the end users' needs.
  - A maximum number of prefixes within a VRF should be configured on PE routers for each NREN to avoid memory exhaustion because a single VPN may announce too many routes. NREN should

determine the maximum number of prefixes for each VPN separately depending on the end user's needs. One solution for determining the maximum number of prefixes can be that end user specifies expected number of prefixes for the VPN when requesting for service provisioning

- **MD5 authentication for BGP** (**required**) – BGP authentication with MD5 should be configured between these peers to validate the peer that sends routing updates, thus protecting any BGP connection from being spoofed.
- **Route flap damping** (**optional**) – Several NRENs used damping for their IP BGP peering with GÉANT while other NRENs do not use it. So the recommendation is that the NREN is free to use it, the NRENs could for instance follow the same rule of their IP BGP peering for their multi-hop eBGP VPNv4 peering.

  This mechanism reduces the number of update messages sent between BGP peers to reduce CPU load of the peers. If this feature is used it should be configured on all peers. As a route incurs a penalty of 1000 each time when it flaps, it is recommended to configure route flap damping with the following parameters:

  - *Suppress value* – when penalty of the route exceeds this value, the route is suppressed; it should be at least 5000.
  - *Half-life* – penalty of the route decays when this period expires, it should be set to 15 min.
  - *Reuse* – when penalty decreases below this value, the route is unsuppressed, it should be set to 750.
  - *Max-suppressed-time* – the maximum duration for the suppression of the route, after being suppressed for max-suppressed time route becomes unsuppressed, it should be set to 60 min.

  Note: This feature might make troubleshooting more complex.

- **Generalized TTL Security Mechanism, GTSM (RFC 3682)** (**optional**) – This mechanism compares TTL value of the incoming BGP update with expected value for BGP peer to protect a protocol stack from CPU-utilisation-based attacks. If the received value is lower than expected, the packet is considered bogus and it is discarded. The expected value should be determined separately for each case, based on the topology of the connection between peers (directly connected routers or multi-hop peers).

L2VPN

Only point-to-point L2VPN will be considered, for now. In this case, the two NRENs that established the P2P L2VPN can guarantee that it is the two interfaces of the end-users that is connected to the L2VPN. In this case, end-users are reassured that they are connected to the right user interface.

When BGP is used for service label exchange, the following security measures must be considered:

- Address families – Only the LV2PN address family should be configured on both peers for the corresponding neighbour (NREN PE, NREN PE, GÉANT VR).
- Preventing l2vpn prefix flooding (**required**)
  - Maximum number of l2vpn prefixes for each BGP peer should be configured in order to prevent prefix flooding and memory exhaustion of the devices. Maximum number of prefixes should be 1000 per peer at a beginning. If the number of prefixes exceeds the defined maximum number, the maximum number may be increased according to the needs.

- MD5 authentication for BGP (**required**) – BGP authentication with MD5 should be configured between these peers to validate the peer that sends routing updates, thus protecting any BGP connection from being spoofed.
- Route flap damping (**optional**) – see previous version related to damping.

When LDP is used for service label exchange following configuration can be considered:

- MD5 authentication for LDP (optional) – LDP authentication with MD5 could be configured between these peers to validate the peer in order to protect against label spoofing.

5.3.1.3 *CPE Level*

L3VPN

- The MDVPN service is deployed in a multi-domain context, therefore no entity (including DANTE or NRENs) is able to provide a guarantee that human errors (such as connecting to the wrong VRF) won't happen; no one has a global view of all router configurations. Therefore, it is **strongly recommended** that end users implement filters (based on prefix lists) of the prefixes authorised to connect to their site. Only end users can manage the list of prefixes for a VRF (creation, changes, suppression).

L2VPN – recommendations for layer 2 security

- In case of point-to-point L2VPN end-users' layer, end-users are interconnected at layer 2. Users can implement a MAC-address-based filter to be sure that it is the right machine on the other side of the L2VPN.

5.3.2 Security Measures for Back-to-Back Mode

Connections between VPN Proxy and NREN PE devices are VRF based. Each VPN requires separate connection (interface or subinterface). Those (sub)interfaces connect directly into VRFs of corresponding VPNs (VPN Proxy 'sees' NREN PE as a CE router), thus there is no connection between the global routing tables of the VPN Proxy and NREN PE. VPN Proxy and NREN PE router exchange routes via BGP for configured VPNs.

The following security measures should be taken into account on the control plane:

- Preventing prefix flooding (required) – maximum number of prefixes within a VRF should be configured on VPN proxy router to avoid memory exhaustion because single VPN announces too many routes. Non-MPLS NREN should determine the maximum number of prefixes for each VPN separately depending on the needs of the end user. The end user needs to specify expected number of prefixes for the VPN (among other things), when requesting for service provisioning.
- MD5 authentication for BGP (required) – it is strongly recommended to configure BGP authentication with MD5 between these peers to validate the peer that sends routing updates, thus protect the BGP connection from being spoofed. Use one password per NREN.
- Route flap damping (optional) – it is up to the two partners to decide whether they will implement damping. This mechanism reduces the number of update messages sent between BGP peers to reduce CPU load

of the peers. If this feature is used it should be configured on all peers. As a route incurs a penalty of 1000 each time it flaps, it is recommended to configure route flap damping with the following parameters:

- *Suppress value* – when penalty of the route exceeds this value, the route is suppressed, it should be at least 5000.
- *Half-life* – penalty of the route decays when this period expires, it should be set to 15 min.
- *Reuse* – when penalty decreases below this value, the route is unsuppressed, it should be set to 750.
- *Max-suppressed-time* – the maximum duration for the route suppression. After being suppressed for max-suppressed time route becomes unsuppressed. It should be set to 60 min.

Note: This feature might make troubleshooting more complex.

- Generalised TTL Security Mechanism, GTSM (RFC 3682) (**optional**) – This mechanism compares TTL (IPv4) value of the incoming BGP update with the expected value for BGP peer to protect a protocol stack from CPU-utilisation-based attacks. If the received value is lower than expected, it is considered a bogus packet and discarded. The expected value should be determined for each case separately, based on the topology of the connection between peers (directly connected routers or multi-hop peers).

References

[BoD]	http://www.geant.net/Services/ConnectivityServices/Pages/Bandwidth_on_Demand.aspx
[DS4.3.1]	GN3plus Deliverable DS4.3.1: End-to-end management – catalogue of business processes <link to be added once final uploaded>
[GB921D]	Business Process Framework (eTOM) Addendum D: Process Decompositions and Descriptions - GB921 Addendum D - Version 12.3 – TMForum
[GB921F]	Business Process Framework (eTOM) Addendum F: Process Flow Examples - GB921 Addendum F - Version 12.0 – TMForum
[GN3 D.J2.1.1]	Deliverable D.J2.1.1: Information Schemas and Workflows for Multi-Domain Control and Management Functions - GN3-11-072 https://geant3-intranet.archive.geant.net/sites/Management/SC/Qasper/Documents/GN3-11-072_DJ2-1-1_Information_Schemas_and_Workflows_for_Multi-Domain_Control_and_Management_Functions.doc
[ITIL]	http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx
[RFC3107]	Carrying Label Information in BGP-4. Y. Rekhter, E. Rosen, May 2001
[RFC4364]	BGP/MPLS IP Virtual Private Networks (VPNs), Y. Rekhter, E. Rosen, February 2006
[RFC4684]	Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs). P. Marques, R. Bonica, L. Fang, L. Martini, R. Raszuk, K. Patel, J. Guichard, November 2006
[RFC5601]	Pseudowire (PW) Management Information Base (MIB), T.Nadeau, Ed., D.Zelig, Ed., July 2009
[RFC5603]	Ethernet Pseudowire (PW) Management Information Base (MIB), T.Nadeau, Ed., D.Zelig, Ed., July 2009
[RFC6368]	Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs). P.Marques, R.Raszuk, K.Patel, K.Kumaki, T.Yamagata, September 2001.

Glossary

ABR (or ASBR)	AS Border Router
AMI	Authorised Member Institution
AS	Autonomous System
AUP	Acceptable User Policy
BGP	Border Gateway Protocol
BoD	Bandwidth on Demand
CE	Customer Edge router (within end users domain)
CoC	Carrier of Carriers
DSCP	Differentiated Services Code Point
eBGP	external Border Gateway Protocol
End-users	it is the users of the NRENs (i.e. scientists, researchers) that use VPNs delivered by the MDVPN service. MDVPN is a joint service delivered by the NRENs and DANTE.
FSI	Federated Service Inventory
GN3plus	The 4th GÉANT project year
GSD	General Service Description
HPC	High Performance Computing
iBGP	internal Border Gateway Protocol
L2	Layer 2, with reference to the OSI model
L3	Layer 3, with reference to the OSI model
LDP	Label Distribution Protocol
LHCONE	Large Hadron Collider Open Network Environment
LHCOPN	Large Hadron Collider Optical Private Network
MD5	Message Digest Algorithm 5
MDSD	Multi-domain Service Desk
MDVPN	Multi-domain Virtual Private Network. A service delivered collaboratively by DANTE and the European NRENs in order to provide to end users VPN (L2VPN or L3VPN) to end users.
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NOC	Network Operations Centre
NREN	National Research and Education Network
OLA	Operational Level Agreement
OSPF	Open Shortest Path First
PE	Provider Edge router
PoP	Point of Presence
PW	Pseudowire
QoS	Quality of Service

RFC	Request for Comments (publication of the Internet Engineering Task Force)
RR	Route Reflector
RT	Request Tracker
RSVP	Resource Reservation Protocol
SFD	Service Functionality Description
SA3 T3	Service Activity 3 (Network Service Delivery) Task 3 Multi-Point Virtual Private Network Services (MPVPN)
SDP	Service Demarcation Point
Service Provider	The network operator (NREN or DANTE) providing transmission services for the End-users
SLS	Service Level Specification
SSP	Service Stitching Point
ToS	Type of Service (IPv4 header field)
TSS	Technical Service Specification
TTL	Time to Live
User	The users of VPN transport service provided by DANTE. It is mainly the European NRENs.
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network.
VPN provider	NREN which provide access to the MDVPN service for End Users.
VPN transport provider	DANTE. VPN transport service is delivered across GÉANT network operated by DANTE.
VPN transport Service	Service delivered by DANTE that transports VPN data across GÉANT backbone from one NREN to other NRENs
VR	VPN Route Reflector
VRF	Virtual Routing and Forwarding