GÉANT MD-VPN

Multi-Domain Virtual Private Network service - a seamless infrastructure for NRENs, GÉANT and NORDUnet

MD-VPN Team authors:

Xavier Jeannin (RENATER), Tomasz Szewczyk (PSNC), Bojan Jakovljevic (AMRES), Thomas Schmid (DFN), Dave Wilson (HEAnet), Brian Bach Mortensen (NORDUnet).

Issue Date: 15 June 2015

Abstract:

The GÉANT Multi-domain Virtual Private Network (MD-VPN) is providing an international network service, enabling scientists all over Europe to collaborate via a common private network infrastructure. The XiFi Future Internet project faced exactly this challenge: interconnect 16 sites located in 12 countries, some of which are affiliated with no NREN at all. MD-VPN fulfilled this requirement in an effective manner.

GÉANT MD-VPN is a seamless multi-domain infrastructure that is able to deliver a bundle of services: Layer 3 VPN (IPv4, IPv6), point-to-point Layer 2 VPN and multi-point Layer 2 VPN. MD-VPN demonstrated its reliability during pilot in July 2014 and will enter in production phase at the end of GN3+.

MD-VPN service can be used for connectivity between clusters, grids, clouds and HPC centers, allowing them to form virtual distributed resources for third-party research projects. As MD-VPN is fast to deliver VPNs to end users, there is a wide scope for MD-VPN use, from the long-term infrastructure with a high demand for intensive network usage to quick point-to-point connections for a conference demonstration.

MD-VPN is easy to deploy for a NREN as it uses only standardized protocols and can be implemented on existing hardware (No CAPEX). MD-VPN requires only once to set-up BGP peerings, then all subsequent VPNs only require to be configured at the NREN edge. This makes the implementation of VPN between domains as easy and straightforward as in a single domain. The adoption of MD-VPN in less than two years by 15 NRENs, NORDUnet and GEANT is the proof of that.

MD-VPN can be extended to regional networks. Its proxy technology is used in order to connect non-MD-VPN capable NREN, non-European NREN or commercial sites.

What is Multi Domain Virtual Private network (MD-VPN)?

GÉANT MD-VPN is a new network service designed, piloted and deployed in GEANT, NORDUnet and 15 NRENs during the GN3+ project. MD-VPN is in fact a new seamless multi-domain infrastructure that is able to transport and deliver a bundle of services over several NRENs or Regional Networks (over several domains): Layer 3 VPN (IPv4, IPv6), point-to-point Layer 2 VPN (both Martini and Kompella) and multi-point Layer 2 VPN (VPLS).

A VPN, in commodity internet, is generally used to link together several network sites of a company, that are distant from each other, as if these different networks are physically in the same location, thus enabling the same level of security. While this is also true for customers of the NREN community, the usage of international VPN in the science and education world in general is quite different. It aims to help and foster international collaboration that is often created around a scientitific project. A typical application of the MD-VPN service can be used for connectivity between clusters, research groups, grids, cloud centers and HPC centers, allowing them to form virtual distributed resources or provide services for third-party research projects (A grid can use a multi-domain VPN to manage its production in order to deliver access to scientists computing and storage functions). In fact MD-VPN is a connectivity service and thus, as a low network layer service, can be used for lot of potential applications. For instance, on top of a multipoint Layer 2 VPN delivered by MD-VPN, you can develop and test new networking paradigms (Software Defined Network), new services or new protocols.

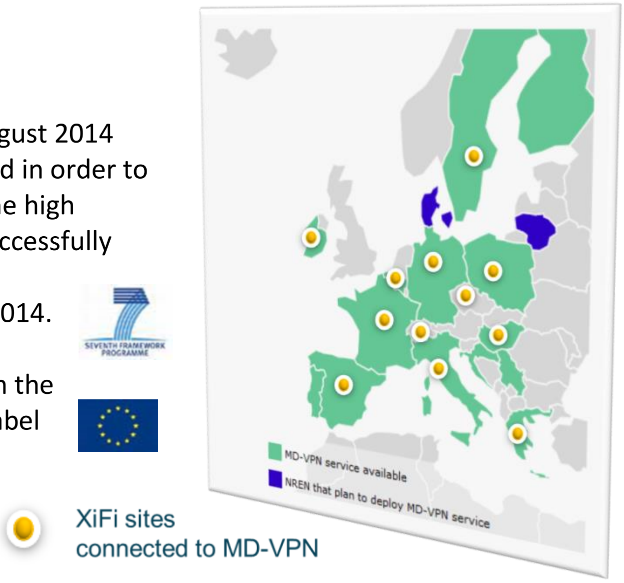
As MD-VPN is very flexible and fast to deliver to end users, there is a wide scope for MD-VPN use cases, from long-term infrastructures with intensive network usage to quick point-to-point connections for a conference demonstration. While MD-VPN provides useful and innovative services, the very good NREN take-up of MD-VPN was also due to the fact that MD-VPN is easy, quick and cheaper to deploy for a NREN than other connectivity services:

MD-VPN is based on standards already deployed on NREN router (BGP/MPLS IP VPNs - RFC 4364, Carrying Label Information in BGP-4 RFC 3701). MD-VPN does not require the installation of additional hardware (CAPEX).

MD-VPN requires only MPLS label exchange between NRENs (not mandatory in the NREN) and 2 BGP peerings.

MD-VPN reduces OPEX as the manual stitching operations between NRENs are not anymore necessary.

As soon as a NREN (or a regional network) sets up these 2 BGP peerings, this NREN can offer to all its users the possibility to create VPNs throughout the whole infrastructure currently 15 European NRENs, GEANT and NORDUnet. Moreover, these new services are delivered to users at a very low cost thanks to NREN collaboration.


🟩 MD-VPN service available
■ NREN that plan to deploy MD-VPN service
● XiFi sites connected to MD-VPN

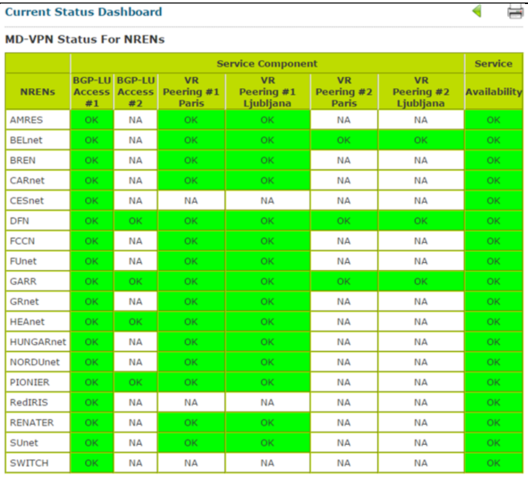
Status of Deployment

MD-VPN was rolled-out in pilot phase in august 2014 among 14 NRENS and was deeply monitored in order to make sure that the reliability is satisfying the high standards for production. After MD-VPN successfully proved its reliability, the service will be launched at the end GN3+ project in April 2014.

The MD-VPN service availability depends on the availability of 2 BGP peerings, one for the label exchange and one for the exchange of VPN routes; the MD-VPN service is up when both the BGP peerings required are up. The service instance availability can be checked on the GEANT monitoring portal and a MD-VPN Monthly Service Report is also available. 17 NRENs (including the 2 pan-European networks GEANT and NODUnet) are now directly connected to MD-VPN, plus 2 NRENS who are working on this subject:

AMRES, BELnet, BREN, CARNet, DeiC (on test), DFN, FUnet, FCCN, GARR, GÉANT, GRNET, HEAnet, LITnet (on going), HUNGARnet, NORDUnet , PSNC, RENATER, RedIRIS, SUnet.

This European infrastructure is currently offering roughly 400 MD-VPN PoPs in Europe where the VPNs can be delivered.



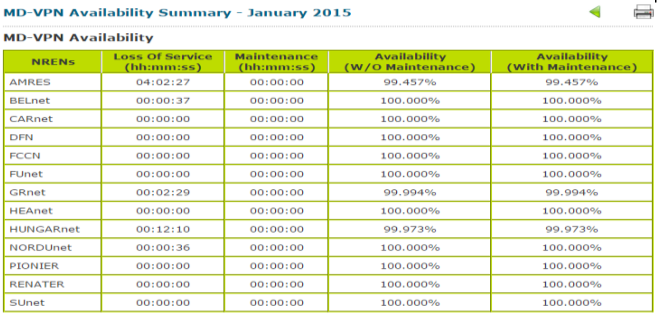
Current Status Dashboard

MD-VPN Status For NRENs

	Service Component						Service
NRENs	BGP-LU Access #1	BGP-LU Access #2	VR Peering #1 Paris	VR Peering #1 Ljubljana	VR Peering #2 Paris	VR Peering #2 Ljubljana	Availability
AMRES	OK	NA	OK	OK	NA	NA	OK
BELnet	OK	NA	OK	OK	OK	OK	OK
BREN	OK	NA	OK	OK	NA	NA	OK
CARnet	OK	NA	OK	OK	NA	NA	OK
CESnet	OK	NA	NA	NA	NA	NA	OK
DFN	OK	OK	OK	OK	OK	OK	OK
FCCN	OK	NA	OK	OK	NA	NA	OK
FUnet	OK	NA	OK	OK	NA	NA	OK
GARR	OK	OK	OK	OK	OK	OK	OK
GRnet	OK	NA	OK	OK	NA	NA	OK
HEAnet	OK	OK	OK	OK	NA	NA	OK
HUNGARnet	OK	NA	OK	OK	NA	NA	OK
NORDUnet	OK	NA	OK	OK	NA	NA	OK
PIONIER	OK	OK	OK	OK	NA	NA	OK
RedIRIS	OK	NA	NA	NA	NA	NA	OK
RENATER	OK	NA	OK	OK	NA	NA	OK
SUnet	OK	NA	OK	OK	NA	NA	OK
SWITCH	OK	NA	NA	NA	NA	NA	OK

Instant MD-VPN service availability

https://tools.geant.net/portal/links/mdvpn/ms_status_dashboard.jsp



MD-VPN Availability Summary - January 2015

MD-VPN Availability

NRENs	Loss Of Service (hh:mm:ss)	Maintenance (hh:mm:ss)	Availability (W/O Maintenance)	Availability (With Maintenance)
AMRES	04:02:27	00:00:00	99.457%	99.457%
BELnet	00:00:37	00:00:00	100.000%	100.000%
CARnet	00:00:00	00:00:00	100.000%	100.000%
DFN	00:00:00	00:00:00	100.000%	100.000%
FCCN	00:00:00	00:00:00	100.000%	100.000%
FUnet	00:00:00	00:00:00	100.000%	100.000%
GRnet	00:02:29	00:00:00	99.994%	99.994%
HEAnet	00:00:00	00:00:00	100.000%	100.000%
HUNGARnet	00:12:10	00:00:00	99.973%	99.973%
NORDUnet	00:00:36	00:00:00	100.000%	100.000%
PIONIER	00:00:00	00:00:00	100.000%	100.000%
RENATER	00:00:00	00:00:00	100.000%	100.000%
SUnet	00:00:00	00:00:00	100.000%	100.000%

MD-VPN Monthly Service Report

https://tools.geant.net/portal/links/mdvpn/ms_avail_summ.jsp.

Table 1: GEANT monitoring portal

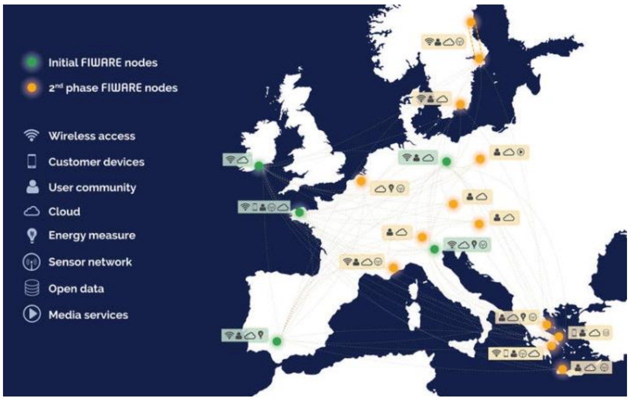
The European scientist project XiFi (https://www.fi-xifi.eu/home.html) uses currently MD-VPN to interconnect its 16 sites located in 12 countries in order to create a distributed research environment. The XiFi L3VPN was fully delivered by MD-VPN in all sites since September 2014. During the deployment of the XiFI L3VPN, MD-VPN demonstrated its extreme flexibility by being able to interconnect to the VPN several sites in countries where MD-VPN was not available. This can be achieved thanks to a VPN-Proxy technology that was developed in the first phase of the project. The reliability of L3VPN delivered was also demonstrated, no incident known so far.
MD-VPN is new service at Europe scale and even as all new services there will be certainly adjustement in operational procedure, MD-VPN demonstrated that this service is now ready for production.

Use cases

MD-VPN is a low layer connectivity service on top of which one can build different services or infrastructures. As MD-VPN is very flexible and can deliver VPN in a very short time, MD-VPN can suit to a lot of use cases:
All scientific projects based on international collaboration
LHCONE is an example of a successful multi-domain L3VPN and even if LHCONE uses another technology, it proves the interest of multi-domain VPNs for science. A first P2P circuit between a Tier2 site located in Poznan and a Tier 1 located in Karlsruhe is now delivered by MD-VPN.
ITER, CONFINE, Visionair and other prestigious international projects could be a good candidate for MD-VPN
XiFi is one of the projects that do research on the future of the Internet that currently use MD-VPN.

XiFi testbed infrastructure provided by MD-VPN
https://www.fi-xifi.eu/home.html

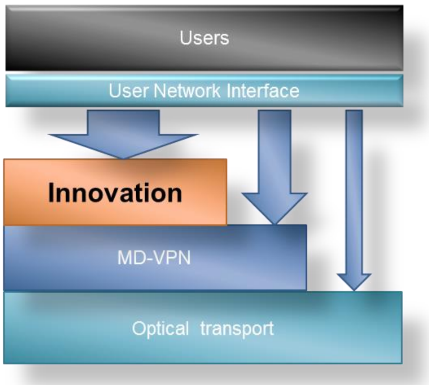
HEAnet
Waterford
Berlin
Fraunhofer FOKUS
Brittany
TELECOM
CREATE-NET
Trento
Trentino Network
IRIS
Sevilla



Distributed infrastructure
Cloud provider, Grid – HPC center, Scientific infrastructure:
Telescope, sensor network
Quick P2P connection
P2P data transport between two sites
Conference demonstrations

A P2P L2VPN was set up for a demonstration of live UHD stream from the camera in Poland (Poznan square) to the UHD TV in Croatia (conference venue) across multiple network domains during CARNet Users Conference CUC 2014.

Live UHD using MD-VPN



http://cuc.carnet.hr/2014?news_hk=5605&news_id=285&mshow=1105#mod_news

- Education
- Remote lecture, E-learning
- Art and education
- Innovation support
- Network, computing and storage research
- New network usage for science and education
- Projects with a high security demands
- Participating sites are not reachable via the public internet

Multi-Domain MPLS VPN Engineering

MD-VPN uses the same principle as conventional MPLS VPNs. The VPN is built by setting up a Label Switch Path between two edge routers. In MPLS VPN, two labels are added to the packets that are exchanged inside the VPN. The first label (top label) is called PE (Provider Edge) label or Egress PE label and the second label is called VPN or service label. In conventional MPLS VPN , the PE label is distributed via LDP or RSVP and the service label is distributed via BGP thanks to a special BGP family (VPNv4, VPNv6, L2VPN, auto-discovery-only).

In multi-domain VPN, the use of LDP or RSVP protocol is not possible for scalability, security and NREN independence reasons. Therefore BGP is used between the different domains (NRENs, Regional Network) to exchange only the PE addresses and labels of the PE routers that take part in MD-VPN. This “inter-AS VPN” technique refers to the “option C” in RFC 4364.

For the service label , the same procedure as for single-domain VPN MPLS is used. The exchange of service labels requires that each domain peers with all other domains, leading to a peering figure of the order of the square of number of domains. In order to reduce this number, a VPN route reflector was put in place in GEANT domain, reducing the number of BGP peerings to only 1 or 2 for redundancy per NREN.

In in this manner, the information exchange between domains is reduced to the bare minimum and the provisioning of new VPNs is as easy as it is in the local network.

The design and the technology used provides a highly scalable service (it will be discussed below). When MD-VPN is deployed in a standard way, MD-VPN will provide the same level of redundancy for end user VPNs as MPLS and IP in a single domain.

Provider Edge and VPN label multi-domain distribution
Signaling is split in 2 parts:
Transmission path between PE routers
BGP (labelled unicast SAFI) is used to exchange the labelled route toward the PE where all the VPNs are delivered to the user.
A NREN needs to establish this peering only once and this point is called Service Stitching Point (SSP); All LSPs and therefore all VPNs are multiplexed over this SSP.
Labels for VPN prefixes exchanged between PE routers
Depending on which VPN (L3VPN, P2P L2VPN martini, P2P L2VPN Kompella, VPLS using LDP or BGP) iust used, BGP or LDP will be used to exchange VPN labels between PEs.

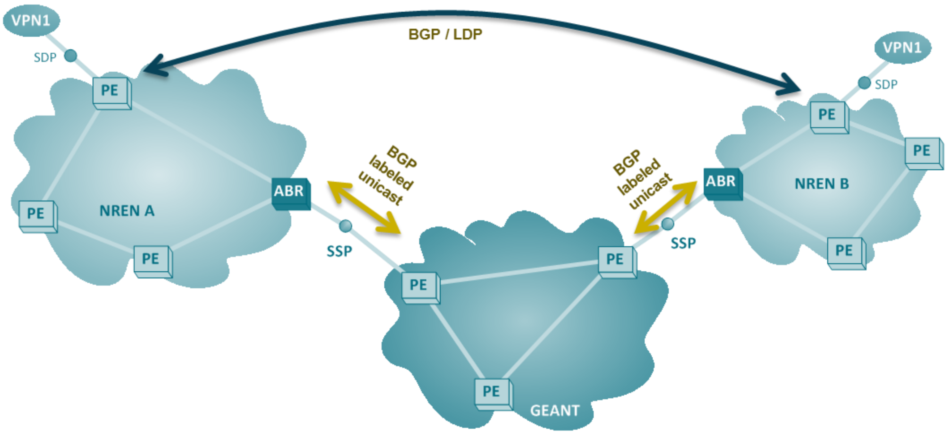


Figure 1: MD-VPN signaling

VPN Route Reflector

Exchanging VPN labels and routes for the customer prefixes between PEs can lead to a huge number of peerings. In order to reduce this number of BGP peerings between PE, a VPN route reflector function was set up in GEANT extending the scalability and flexibility of MD-VPN. Additionally the signaling information exchange between NRENs is significantly simplified by the implementation of VPN Route Reflector (VR). This reduces the number of BGP sessions which must be established between NRENs to zero.

The VPN route reflector exchanges via a multi-hop peering BGP with the NREN route reflector or NREN PE all the SAFI (VPNv4, VPNv6, L2VPN, auto-discovery-only). The VPN route reflector is configured to accept all VPN routes

In order to maximize the availability of this crucial function, 2 VPN route reflectors were deployed with which NRENs can peer. NRENs can also peer from several route reflectors in order to improve reliability.

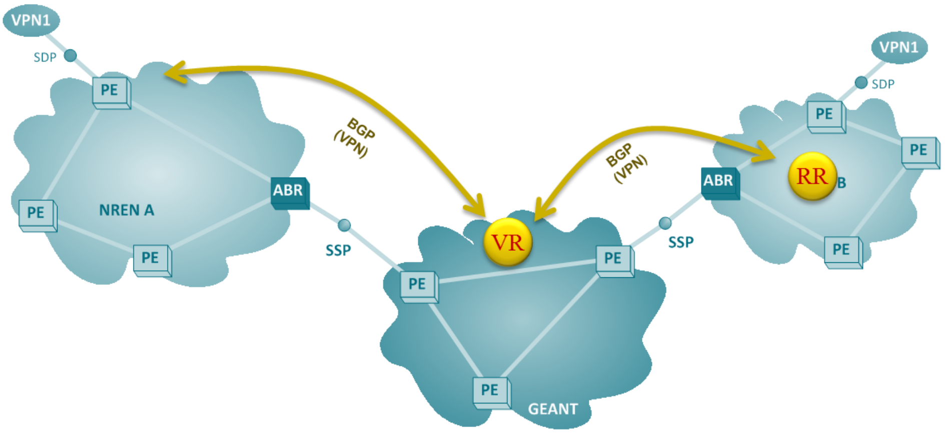


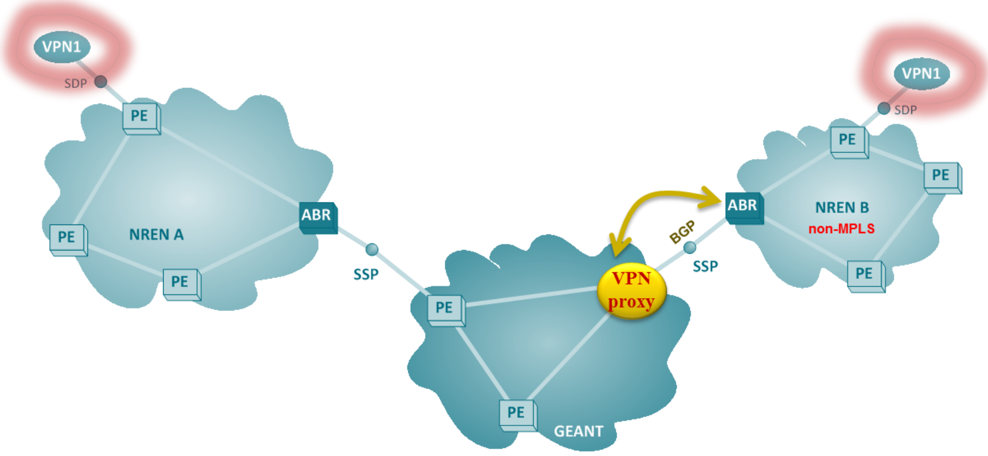
Figure 2: VPN Route Reflector

Carrier of Carrier/Carrier Supporting Carrier (CsC)

The 2 Pan-European networks (GEANT and NODUnet) choose to encapsulate the VPN MPLS of MD-VPN in a internal MPLS L3VPN. This technique is called Carrier of Carrier or Carrier supporting Carrier for hierarchical VPNs and allows a NSP (a carrier) to transport transparently VPNs of another NSP (Carrier). What is original in MD-VPN is that in conventional CsC the VPN is transported between two areas of the same NSP (the same AS), whereas in MD-VPN the CsC used to transport VPN between different ASes and NSPs (Carrier). This choice is motivated by the fact that both Pan-European networks do not deliver VPN to end user but focus on transporting VPN for the NRENs. Isolating the MD-VPN service in VRF could also be an advantage for a network provider allowing him to easily monitor the service. Therefore technically speaking, a third label is used when the packet is going through GEANT or NORDUnet.

How to connect “non MD-VPN site”: VPN-proxy

It is crucial for end-user projects to know if all of their user sites could be connected to the VPN. The solution is simply that MD-VPN is able to connect any type of site. It is recommended for European NREN to support the MD-VPN service but in the situation where this is not possible,, VPN-Proxy Technology provided by GEANT could extend a VPN to NREN who is not MD-VPN capable.



Scalability

The network scalability is a significant advantage of the MD-VPN architecture over other existing service architectures. It is designed to provide thousands (and more) of service instances without any negative impact on GEANT or NREN's core networks. This fact is extremely important when SDN approach or other research activities are taken into account.

That goal can be achieved thanks to the separation between data transport in the core network and services provided at the edge. Basically in the core network only labels and routes related to PE routers are maintained. Currently these are less than one thousand entries for all participating NRENs. When comparing it to current size of global Internet route table size (~500k), it is easy to notice that MD-VPN has strong growth potential. The services are maintained at the network edge, on PE routers. Each PE router maintains only the set of entries (labels or routes) related to services provided by this very PE router.

The number of VPNs that are active between NRENs has zero impact on the GEANT infrastructure since they are completely transparent to the GEANT network. The only state GEANT has to keep is the addresses and labels of the PEs, which is independent of the number of VPNs.

Network services and extensibility

The key concept of MDVPN – which is the transport label for remote PE router allows providing many transmission services at the same time. It is quite easy to implement L3VPN services for IPv4 and IPv6 protocols or L2VPN for point to point or multipoint data exchange in a multi-domain architecture.

L3VPN for IPv4 and IPv6

The signaling protocols currently implemented by leading router vendors allow to build virtual Layer3 networks used to carry IPv4 and IPv6 traffic. This functionality is significant for distributed environments (like research projects) where large broadcast domains are not acceptable. This service is based on IETF RFC 4364 (known as BGP/MPLS VPNs). The BGP protocol is used to distribute VPN routing information across the MD-VPN backbone. MPLS then is used to forward VPN traffic across the NRENs or Regional/Metro network backbone to remote VPN sites. The end users can use either public addresses or overlapping private addresses inside VPNs.

Thanks to the BGP protocol, NRENs can re-use for L3VPNs all available policies or filters used for IPv4 protocol, in order to control prefix exchange with remote networks. This significantly improves network scalability and reduces maintenance overhead.
The MD-VPN route reflector (called VR) implemented in GEANT network supports IPv4 and IPv6 address families.

The MD-VPN infrastructure can be also extended with multicast features. Because of the nature of multicast transmission it may requires some additional components (like point-to-multipoint LSPs) which will be investigated and tested in the future.

P2P L2VPN – BGP signaling and LDP signaling

Point to point transmission for Ethernet frames is one of most popular service delivered for research projects. It allows connecting two remote sites with transparent circuit carrying Ethernet data. It is also good example to explain MD-VPN components and its flexibility.

As mentioned earlier one of the key components of MD-VPN is the transport label for remote PE router. This label is used to build the LSP that can be shared between many types of services. Second MD-VPN component is service label, which is used to differentiate and assign packets to appropriate service instances on PE router. It is important to underline, that this label has no significance for core devices and is used only on edge nodes. Because of that, the label service exchange process is executed only between two PE routers.

Currently this functionality can be provided by two legacy protocols: LDP and BGP. In case of LDP , the service labels are exchanged through targeted LDP session (TCP) between PE routers. In case of BGP , the service labels are exchanged with dedicated NLRI in BGP updates. PE routers may establish direct BGP session (known as BGP multi-hop) or use existing route reflectors.

As a result the PE routers can mark packets with two labels allowing to form pseudowire which is virtual entity used to send and receive Ethernet frames generated by end user sites located in distinct domains.

VPLS

VPLS is emulation of LAN. Basically it allows connecting two or more remote sites as it were connected with an Ethernet switch. Most important difference comparing to point-to-point circuits is that usually for VPLS a full mesh of pseudowires is established between PE routers. Currently such functionality can be provided by two legacy protocols: LDP and BGP. Both are described by IETF RFCs: RFC 4761 and RFC 4762. Another property of VPLS service is MAC learning. This functionality is implemented only on PE routers and is required in order to choose appropriate interface or pseudowire over which Ethernet frame should be sent out.

The complexity introduced by the VPLS service is reflected in signaling protocols. In case of LDP the remote PE addresses must be explicitly given in the service configuration. Thanks to that, the LDP process gets information with which peer the targeted LDP session must be established. In case of BGP, for each service instance the Route Target value must be specified additionally with site ID and range. This allows proper BGP update distribution and label calculation. The advantage of BGP is of course its scalability. However in multi-domain environment the uniqueness of site ID parameter can cause some problems.

So currently MD-VPN allows establishing VPLSes only with LDP protocol. The BGP signaling is subject of further studies.

Geographical extensibility

MD-VPN is very flexible. Some NRENs for example may want to extend the service to their regional network. A NREN can easily do it by the same connection technique used between NRENs and GEANT:

Create a SSP between the NREN and the Regional Network, Option C of RFC 4364

Set-up BGP peering in VPN BGP family between NREN route reflector and regional network route reflector.
The main motivation to extend the service is to provide the service closer to the end-users.

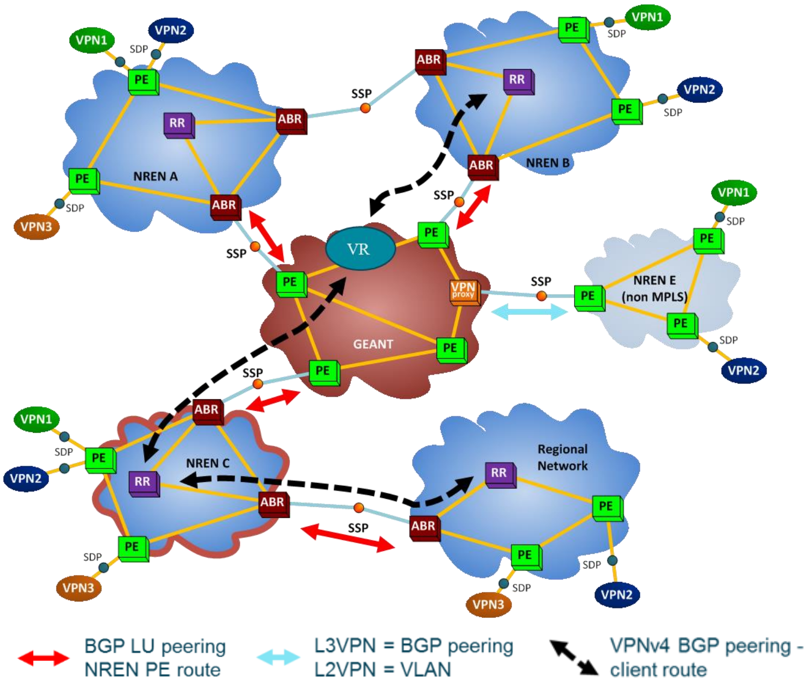


Figure 3: global view MD-VPN service

Service extensibility

Another example of MDVPN extensibility is research activity. NREN's research team can build brand new (not yet existing) transmission services on PE routers. It is quite important in relation to SDN, where new services can be built with external software components. On PE router only transport label will be added to the packet, and delivered to other PE router through the existing MD-VPN infrastructure. It is important to underline that such activity does not require any configuration changes in running network/in current MD-VPN infrastructure. This can speed up collaboration within research projects and allow using network resources much more efficiently.

MD-VPN security

The security level of MD-VPN can be assessed from the security level of MPLS VPN in single domain context which was intensively studied and documented as this service is intensively deployed by network service provider. The book “MPLS VPN Security” [Behringer M. H.] is a good example of the flourishing documentation on this subject. The main difference with mono domain context is that in MD-PVN service that the core network delivered by several NSPs (multi-domain).

So if we consider the user effect on MD-VPN security it is the same as for MPLS VPN, i.e. the user cannot endanger both the infrastructure or the VPN of other users.

If we consider the case of the compromising of network core, in MPLS VPN it impossible to protect the access to a VPN. It means if NREN router is compromised, the confidentiality of all VPN going through this NREN is corrupted. In general if a router is compromised, for any type of service, it is very difficult to protect user data confidentiality. In general, users can protect their data confidentiality against NREN espionage thanks to cryptology. For MD-VPN specifically, the question is what is the status of the VPN located in other NRENs?

So in first conclusion, the security of MD-VPN is the same as for MPLS VPN except for the case when a router is corrupted in one domain (in one NREN).

So the rest of this section is a discussion about how to protect user VPN against a pirate that would have taken a control a router in another domain.

As MD-VPN is delivered by several NREN, the user should trust the NREN that deliver the VPN. If we consider the case of corrupted router in a NREN, we have to consider 3 cases:

- Man in the middle – The risk here is that a NREN spy information of a VPN. It is the same level of security as simply using a NREN. If the users do not trust the NRENs then the users can use cryptography.
- Control plane attack – In this case a NREN would like to introduce into user VPN traffic when this NREN is not on the path. There are several counter measures based on AS filter and password usage for P2P L2VPN LDP that will stop this potential attack.
- Data plane attack – we could imagine that a pirate, first take control of a NREN router and secondly forge packet and inject into the NREN with the purpose to compromise a user VPN that is not located in remote NREN in the MD-VPN infrastructure. This type of attack is a data plane attack and is called label spoofing (like IP spoofing exists for IP service). This case is very rare and our investigation demonstrates that such attack is very difficult to put in place and very long to lead [see Multi Domain VPN label spoofing]. Moreover label spoofing attack requires a specific step called label scan and this step is easy to detect thanks to NetFlow. One can detect the sudden increase of number of VPN labels as the figure below. Then when the scan is detected, it is easy to set-off an alarm. Therefore in this condition, the scan detection feature is capable to be our firewall.

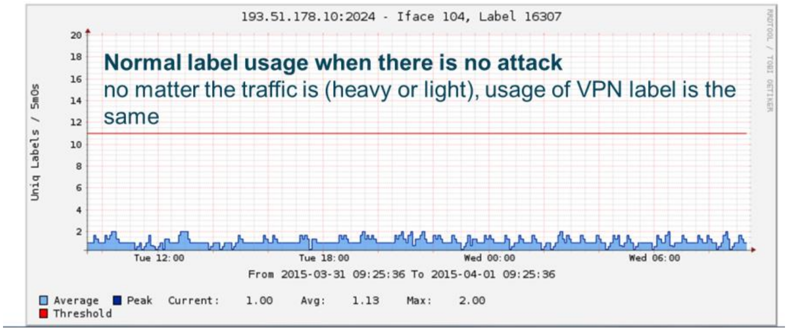


Figure 4: Normal MD-VPN traffic

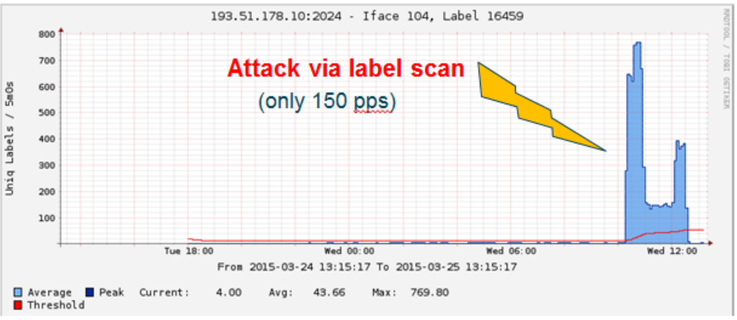


Figure 5: Label spoofing attack detected

The number of VPN label used on a PE is very stable and completely independent of the nature of the traffic (heavy or light) into the different VPNs set-up on this PE. Therefore the number of VPN labels increases only when a new VPN is implemented on a PE by the NREN NOC. When the number of VPN label exceeds a threshold, an alarm sets off and the NOC can shut down the MD-VPN access of the NREN corrupted. It is important that this detection system will be deployed at specific place. The deployment is easy as it consist to enable MPLS NetFlow on the border routers and set-up a NetFlow collector fits with our scan detector program. This system will be deployed on GEANT router so it will be easy to isolate the source of the attack and therefore protect MD-VPN infrastructure.

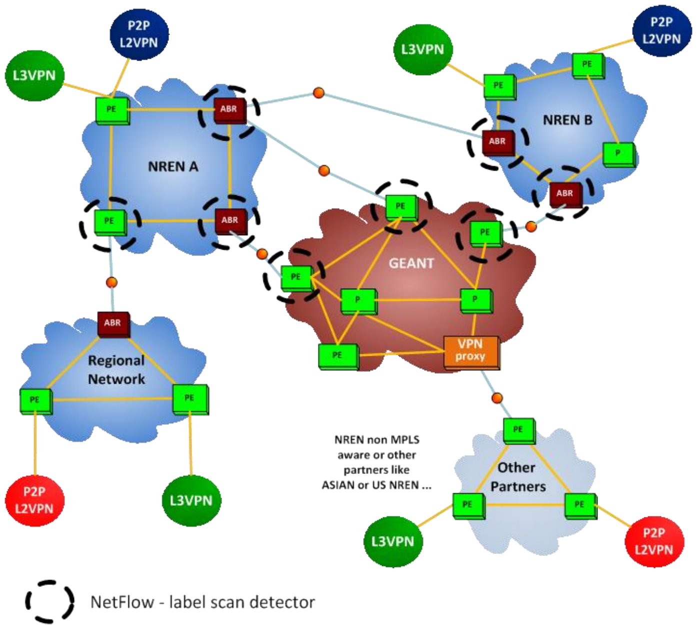


Figure 6: Scan detector deployment

MD-VPN Operation and Quality

Flexible design of MD-VPN service and all advance technical features of MD-VPN technology are not sufficient for MD-VPN service wide adoption, successful deployment and excellent users' experience. To achieve these goals the MD-VPN service providers should also provide excellent service operation and continually improve processes and procedures important for service management. All entities involved in delivery of service should understand and have a clear picture about their role and responsibilities in overall service design and architecture. Seamless collaboration between partners, coordinated communication and well organized MD-VPN service management are crucial for service success. This was a reason why during the design phase of MD-VPN service have been given special attention to development of operational processes needed for MD-VPN provider's coordination. To be able to conduct, control and manage the day-to-day operation of MD-VPN service we have defined some operational procedures which will facilitate introduction of MD-VPN service to support environment and help us to smoothly transit to the production phase of service.

MD-VPN provisioning process

One of the advantages of MD-VPN service is the very short provisioning time of a requested VPN instance across the Pan-European R&E community. This characteristic is not so easy achievable by other available connectivity solutions and differentiates MD-VPN service from them. To achieve reliable and smooth provisioning process, MD-VPN group define provisioning procedure which will be respected by all VPN service providers.

Important principles which lead definition of provision process were:

- The provisioning request should be as easy as possible for the end-users.
- The MD-VPN provisioning is decentralized in each local NREN. Every domain (NREN) will provide support to their user community. User group/project member institution will contact and communicate to the the local NREN service desk for every question or request regarding the MD-VPN service.
- VPN service providers should guarantee that provisioning process will be managed and monitor until the fulfillment of users request.
- Request fulfillment by MD-VPN service providers should be as short as possible.
- High-level overview of the provisioning procedure is:
- The end user group/project authoritative institution/person should submit MD-VPN service request to the local NREN. The NREN that registers the request is called the coordinator NREN and will be responsible to further coordinate VPN provisioning process. In some cases and depending on the project (e.g. several NRENs involved and large user group), GEANT will take the role of the coordinator NREN.
- The coordinator NREN will receive all important technical details regarding service request by the filled MD-VPN request form sent by authoritative persons of the project.

- The coordinator NREN will register all received information in the MD-VPN database and contact other partner NRENs involved in the project to provision the VPN in their own domains. Partner NRENs will further contact their end users sites and organize VPN provisioning with them. Status of VPN provisioning in every domain will be reported to the MD-VPN database and each NREN will update and keep up to date information about their end users sites.

When the implementation is completed in the each NREN, an acknowledgement is communicated to all NRENs and to the authoritative persons of the end-user projects.

MD-VPN problem management

Another very important part of the successful service operation is organization of problem management. Irrespective to the fact that during the testing and pilot phase, the MD-VPN service has demonstrated great stability in the functioning, effective and efficient MD-VPN troubleshooting process is mandatory to achieve user satisfaction. MD-VPN troubleshooting procedure is developed with this aim and to help MD-VPN service providers to identify, communicate and resolve potential issues as easy as possible.

Taking into account the fact that NRENs cooperate on maintenance of their IP networks for many years MD-VPN group has not the intention to develop totally new and independent procedure for the MD-VPN problem management. Our aim was to use already existing models and hierarchies of communication and cooperation between NRENs and to integrate MD-VPN troubleshooting procedure in this matrix.

Important principles which lead definition of troubleshooting process were:

- User group/project member institution will contact and communicate the local NREN service desk for every issue or problem regarding the MDVPN service.
- The troubleshooting procedure will use the same escalation schema as for GEANT IP service (Regional network>NREN>Pan-European network).
- The domain (NRENs, Regional Network etc.) that raises the trouble incident must follow it until the resolution in order to ensure that all incidents are completely treated.

High-level overview of the troubleshooting procedure is:

- The end-users report an issue or a problem to their local MD-VPN provider (e.g. NREN, Regional network etc.). The local NOC is responsible to identify the root cause of an issue (e.g. check if the problem in the MD-VPN service is caused by the improper usage of the MD-VPN service by the user, or if is it caused by a problem linked to the underlying services, or finally if it is due to a problem in MD-VPN service by itself).
- If the problem impacts other domains, the local NOC must inform the Service Desks of other involved entities (participating NRENs, GÉANT etc.) about the existence of problems in the functioning of service.
- If the problem cannot be solved locally, the escalation procedure will follow the model which is applied for IP service (Regional network>NREN>Pan-European network).
- After the successful resolution of the MD-VPN service problem, the local NOC notifies peer NRENs and the local user’s institution about the repairing and restoration activities.

MD-VPN Quality assurance

Many different entities and domains participate in delivery of MD-VPN service to the end users. To achieve users satisfaction all “links in the chain” of these domains must perform on a agreed level. In order that all MD-VPN service providers understand their role, responsibility, level of service that should be provided to the MD-VPN users, MD-VPN group developed Operational level agreement [MD-VPN OLA]. The purpose of MD-VPN OLA document 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). All MD-VPN service providers are obliged to adhere to the level of the service defined in this document.

In order to monitor technical aspects of the service quality GEANT provide a MD-VPN Monthly Service Report portal. This portal provides monthly statistics about availability and reliability of service and presents its current status. Mechanisms which will monitor efficiency and effectivity of adopted processes and procedures will be further developed during the GN4 project.

MD-VPN in GÉANT service portfolio

The purpose of the three network services “GÉANT plus”, “L3VPN” and “MD-VPN GÉANT” are to facilitate a private interconnection amongst common research and education network users (collaborating on a single research project).
These services as all services delivered by GÉANT fall in a scope of Business-to-Business scope, meaning that the service delivered will be not used by NRENs directly but delivered by the NRENs or the Regional Network (RN) to end-users. From the end-users point of view these services delivered are the same but from the NREN point of view these services are different in the way that GÉANT delivered them to the NREN and in the border of service.
L3VPN GÉANT service aims to allow the deployment of L3VPN multi-domain. GÉANT Plus offers point to point layer 2 connectivity (i.e. Point-to-Point L2VPN). GÉANT plus and L3VPN deliver their service at the border of GÉANT whereas MD-VPN aims to provide the service at end user site. MD-VPN delivers jointly with GÉANT and NRENs an End-to-End service, where L3VPN and GÉANT plus service deliver their service to the NREN. These latter two services are then delivered to end-users by stitching manually L3VPN and L2 circuit to the same services in all adjacent domains.
GÉANT plus service delivers the L2VPN service to the end users by stitching P2P circuit multiplying therefore the single point of failure (SPoF) at each stitching point. MD-VPN, when it is deployed in standard way, will provide the same redundancy for end user VPNs as MPLS in a one domain.

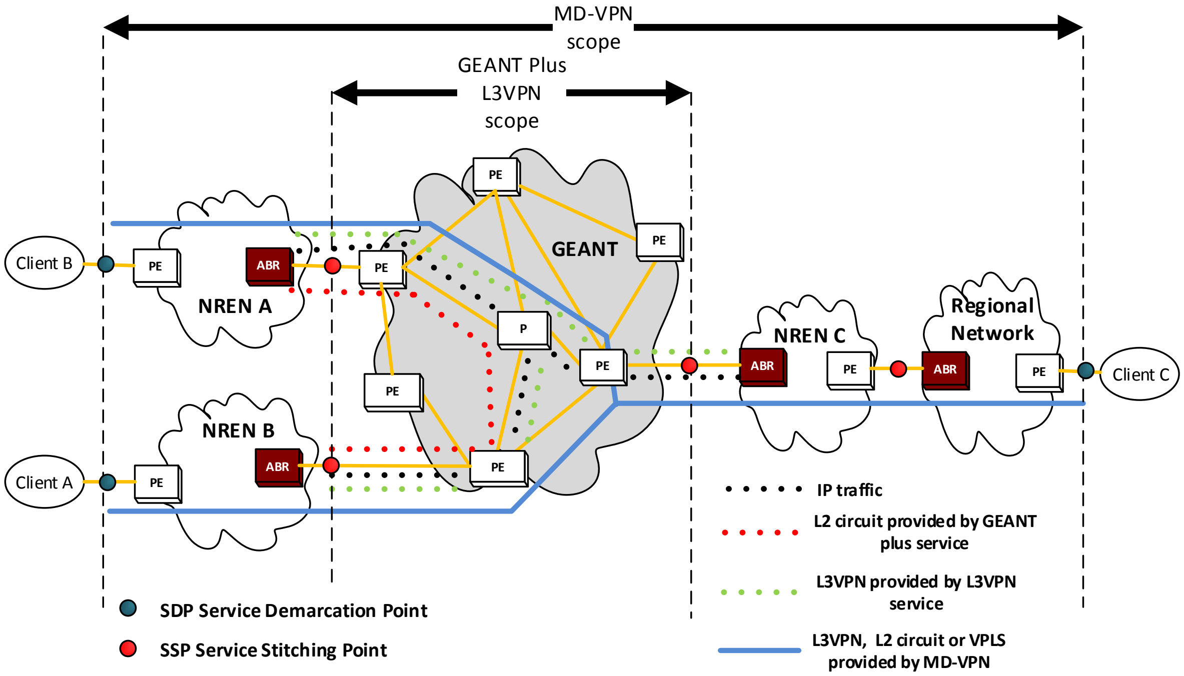

MD-VPN
scope
GEANT Plus
L3VPN
scope
PE
PE
GEANT
PE
Client B
PE
ABR
NREN A
P
PE
PE
NREN C
ABR
PE
Regional
Network
ABR
PE
Client C
NREN B
ABR
PE
Client A
PE
IP traffic
L2 circuit provided by GEANT plus service
L3VPN provided by L3VPN service
L3VPN, L2 circuit or VPLS provided by MD-VPN
SDP Service Demarcation Point
SSP Service Stitching Point

Figure 7: GÉANT VPN services

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

Table 2: feature comparison

MD-VPN is able to provide the same services as GÉANT Plus and L3VPN but without manual configuration between GÉANT, NRENs and Region Network reducing lead time and OPEX for NREN, Regional Network and GEANT.

This MD-VPN collaboration relies on confidence between partners and is technically based on label exchange. MD-VPN is more intrusive than GÉANT Plus and L3VPN service, this can lead NRENs to decide to not use this service due to its own network policy.

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

Conclusion and perspectives

The MD-VPN is a seamless transport infrastructure that thanks to an innovative design achieved to be highly scalable. MD-VPN delivers bundle of services (L3VPN IPv4-IPv6, P2P L2VPN, VPLS) with added value for our users. This infrastructure was designed, tested, deployed in 15 NRENs, NORDUnet and GÉANT in only two years. The SA3T3 task successfully adds to GÉANT portfolio MD-VPN service which is an original and useful service that is unavailable in a commercial NSP portfolio. The infrastructure built allows users avoiding to appeal more expensive commercial offer that requires a public tender which is by itself a burden. This new infrastructure saves OPEX on NREN side and investment on user side while the lead time was dramatically reduced.

In the near future, new services could be deployed over this infrastructure like Ethernet VPN, multicast VPN and will be studied during GN4 phase 1. MD-VPN has already spread over network project as GÉANT Join Research Activity in GN4 is now considering MD-VPN as a potential leverage tool for deployment of new network technology.

Reference

RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 3701, Carrying Label Information in BGP-4
SA3T3 team, 2013, MD-VPN architecture, GN3+ deliverable,
<**http://www.geant.net/Resources/Deliverables/Documents/D7.1_DS%203%203%201-MDVPN-service-architecture.pdf**>
Behringer M. H. (Distinguish Engineer at Cisco), Morrow M. J., 2005, MPLS security, Cisco Press
Jeannin X., Tomasz Szewczyk, Multi Domain VPN label spoofing, STF meeting Berlin March 2015
https://intranet.geant.net/SA1/APM/March2015/_layouts/15/listform.aspx?PageType=4&ListId={03B89020-DE26-41C7-9C1E-533A3A73297D}&ID=4&RootFolder=*
MD-VPN OLA (Open Level Agreement)
https://intranet.geant.net/SA6/mdvpn/_layouts/15/start.aspx#/SitePages/Home.aspx
https://intranet.geant.net/SA6/mdvpn/Shared%20Documents/AUP-OLA/MD-VPN_AUP_V0.07.doc?Web=1

Bibliography

Xavier Jeannin (RENATER) was formerly activity manager of the network activity in the European Grid project EGEE. He was in charge of LHCONE deployment in France, an international L3VPN that currently connect the LHC computing center over the world. He is the task leader of MP-VPN in GN3-plus project (SA3T3) that is in charge of the design, service specification and deployment of Multi-Domain VPN service in Europe.

Tomasz Szewczyk (PSNC) is network engineer and transmission team leader in PSNC. He was responsible for design and deployment of MPLS-based services in polish NREN (PIONIER) and metropolitan area network in Poznan (POZMAN). During GN3 project he was involved in multi-domain services architecture definition and BoD service specification. In GN3plus project (SA3T3) he is involved in technical design and deployment of MDVPN service.

Bojan Jakovljević (AMRES) is lead senior network engineer in department for infrastructure in AMRES. He manages and coordinates activities of the department of infrastructure and the AMRES NOC team. During GN3plus project he was involved in development and deployment of MD-VPN operational model (SA3T3) and in modelling and analysing the main business process flows which should be executed during the operations of the MD-VPN service (SA4T3 E2E Management – Network Management Architecture Approach).

Thomas Schmid (DFN), senior architect network at DFN.

Dave Wilson (HEAnet), senior architect network at HEAnet.

Brian Bach Mortensen (NORDUnet) was born in 1970 and received the M.Sc. EE and Ph.D. from the Technical University of Denmark in 1998 and 2006. He is currently working as head of network service delivery activity (SA3) within the GÉANT3plus project. His main responsibility is coordination of design, piloting and launching new services that will benefit the scientific community both in and out of Europe. Before joining the NREN sector Brian worked at DONG Energy as a network strategist, with his main responsibility of choosing network technologies and architectures for triple play customers and b2b network solutions.