



MPLS connectivity services to the campus edge

Best Practice Document

Produced by the CSC/FUNET-led AccessFunet working group

Authors: Jani Sirpoma (CSC/FUNET)
Antti Ristimäki (CSC/FUNET), Jani Myrsky (CSC/FUNET)

April 2016

© CSC / Funet, 2016

© GÉANT, 2016. All rights reserved.

| | |
|--------------------------|---|
| Document No: | GN4-NA3-T2-FN3.3 |
| Version / date: | 1.0 / 26.04.2016 |
| Original language : | Finnish |
| Original title: | MPLS-yhteyspalvelut kampusverkon reunalle |
| Original version / date: | 1.0 / 07.04.2016 |
| Contact: | jani.sirpoma@csc.fi |

The work has been carried out by a CSC/Funet led working group AccessFunet as part of a joint-venture project within the HE sector in Finland.

Parts of the report may be freely copied, unaltered, provided that the original source is acknowledged and copyright preserved.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).



Table of Contents

| | | |
|-------|--|----|
| 1 | Introduction | 1 |
| 2 | Requirements for the service provisioning | 2 |
| 3 | Implementation within Funet network | 3 |
| 4 | Use Cases | 5 |
| 4.1 | Remote campus interconnection | 5 |
| 4.1.1 | Redundant interconnection to the main campus | 5 |
| 4.1.2 | Interconnection to the main campus via another Funet member's connection | 6 |
| 4.2 | Provision of colocated data center services | 6 |
| 5 | Available connection types | 8 |
| 5.1 | Routed L3VPN | 8 |
| 5.2 | Virtual switch L2VPN / VPLS | 10 |
| 5.3 | International connections | 12 |
| 6 | Comparisons between connectivity service technologies | 14 |
| 7 | Conclusions | 17 |
| | References | 18 |
| | Glossary | 19 |

Table of Figures

| | |
|--|----|
| Figure 3.1: MPLS label switching between core routers | 3 |
| Figure 3.2: Connection between Funet backbone network and CSC's data center network | 4 |
| Figure 4.1: Example of provision of colocation data center services for a campus | 7 |
| Figure 5.1: Illustration of a routed L3VPN service where private addresses are being used at remote campus | 9 |
| Figure 5.2: Illustration of a routed L3VPN service where private addresses are being used at remote campus | 11 |
| Figure 5.3: An MD-VPN infrastructure between several NRENs interconnecting ImaginLabs © GÉANT | 13 |

Table of Tables

| | |
|--|----|
| Table 6.1: Comparison of connectivity service technologies | 16 |
|--|----|

1 Introduction

Within the Funet network, Layer 2 and Layer 3 MPLS (Multi-Protocol Label Switching) connectivity services – generally known as "MPLS VPN" services – can be used to interconnect the campus networks of a member organisation, or to interconnect to another member organisation [RFC 4364]. These can be implemented for all access links connected to Funet IP core network, using the same router ports through which Internet access is provided.

With MPLS connectivity services, spare capacity in existing Funet connections can be used for connections that are either within or between organisations and separated from a public network. Traditionally, the term VPN (Virtual Private Network) is used to refer to the transmission of encrypted traffic through a public network. In the case of an MPLS VPN, traffic is not encrypted; instead, privacy should be understood as logical separation within a trusted network.

Typical use cases include shared virtualisation environments, cloud services, research group collaboration, and connections to centralised data repositories or the creation of backups outside the campus. In some cases, MPLS VPN can be an alternative to a long lightpath connection without a redundant route. The implementation of short-lived connections is also easier than using lightpaths.

If member organisation has a backup connection for its campus, an MPLS connection can be implemented from the Funet location to the campus using the main and backup connection. All MPLS connections are always redundant between backbone network routers.

MPLS connection services use free network capacity in the access links between the Funet backbone network and member organisation. Separate capacity is reserved for these on the network, so that MPLS VPN connections are not hampered by peak traffic on the Internet, and vice versa. The organisation itself can determine how its own Funet connection bandwidth is divided between public and MPLS traffic.

For instance, a separate quality category can be defined for the background transfer of large data quantities (e.g. backup runs), which use only the connections' momentary spare capacity, leaving space for all other traffic as required. In such a case, data transmission does not interfere with other network use.

2 Requirements for the service provisioning

MPLS VPN connections are connected to Funet via the edge device(s) of the member organisation, within their own VLANs [IEEE 802.1Q]. The organisation's own network devices do not need to support MPLS. Because the organisation's Internet traffic is not usually VLAN tagged at the outset, a service break in the Funet connection is needed for the introduction of VLAN tags. No restrictions from the Funet side are set on the available numbering. In addition, when using routed L3VPN connections, a separate, new link network with at least two IP addresses must be defined between the devices.

When the campus is connected to the Funet backbone network, the MPLS VPN connections can be implemented through the same access link to any other campuses connected to the Funet network. When selecting a solution, account must be taken of current and estimated future traffic volumes to ensure sufficient capacity on a case-by-case basis.

When installing an MPLS VPN connection in an office which does not already have a physical interface with the Funet backbone network, a Funet additional connection to the office is needed.

For organisations already using the Funet router service, a VPN connection is configured by Funet specialist all the way to the organisation's Funet edge routers. Alongside Funet, the member organisation has the task of defining the routing between the internal network and the Funet edge routers.

3 Implementation within Funet network

MPLS LSPs (Label-switched Paths) between core routers within the Funet backbone network are signalled using the LDP protocol [RFC 5036]. These paths are always direct between neighbours and follow the best routes advertised by IS-IS, thereby preventing routing loops. In most cases, routers advertise their own loopback addresses and the corresponding labels to the LDP. An LDP-speaking router advertises the route learned (using the LDP) to other LDP neighbours. Once payload frame arrives to the provider edge router, one or more labels are added on top. In each device, MPLS packet switching through the network occurs by changing the outer label. Switching of outer label is illustrated in Figure 3.1.

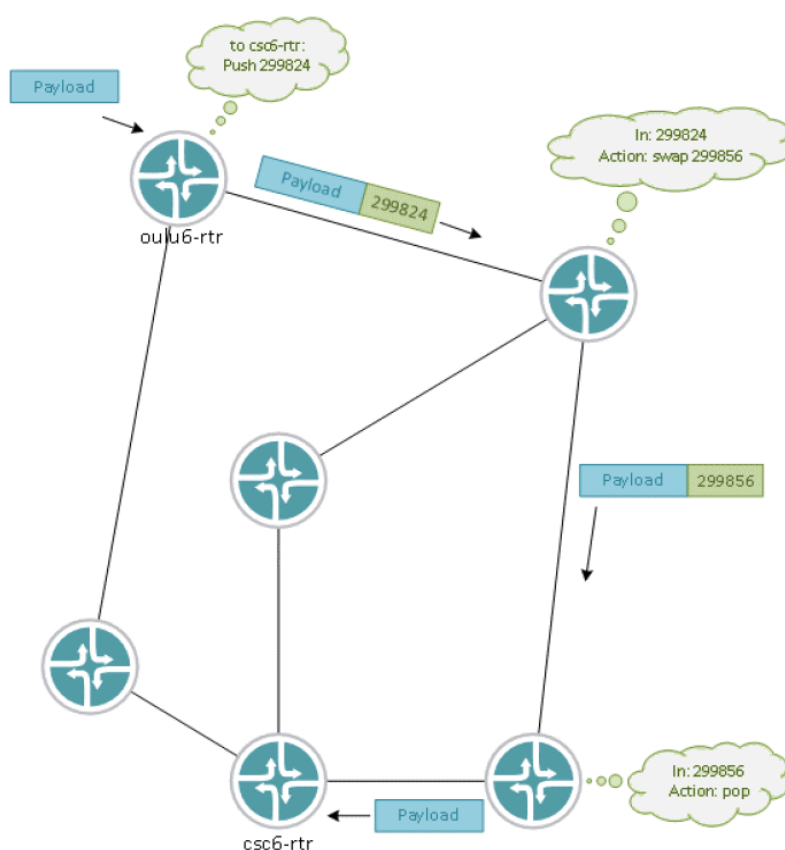


Figure 3.1: MPLS label switching between core routers

Label values are link-local, even if LSP is network-wide. The outer label is omitted at the second last router, reducing the load of the receiving device. This behavior is also called Penultimate Hop Popping. The inner labels can be used to distinguish e.g. different VPN services from each other by the egress router, which maps the payload to a certain VLAN towards campus network based on the label.

VPN routes are signalled in a BGP session that is separate from a BGP session controlling the Internet traffic. A VPN label is advertised in connection with VPN route advertising. The route information includes a unique route-distinguisher, using which the routes of different organisations at the same link are kept in separate VPN routing tables within the routers. MPLS traffic originating from customer networks is not accepted. More in-depth knowledge of Ethernet over MPLS transport technologies can be found e.g. from GÉANT Deliverable DJ1.1.1: Transport Network Technologies Study [DJ1.1.1].

Data center networks providing CSC services are logically connected to the same "MPLS cloud" as the Funet backbone network, enabling easy connectivity with any member organisation. However, these networks have independent internal routing and LSP signalling. There is no MPLS-level connection from Funet's router service devices to the Funet backbone network – the links between them are always purely IP or Ethernet and are handled as customer networks. An MD-VPN platform, used for establishing international connections, functions as a logically separate system using the same backbone network routers. Connection between Funet backbone network and CSC's data center network is illustrated in Figure 3.2.

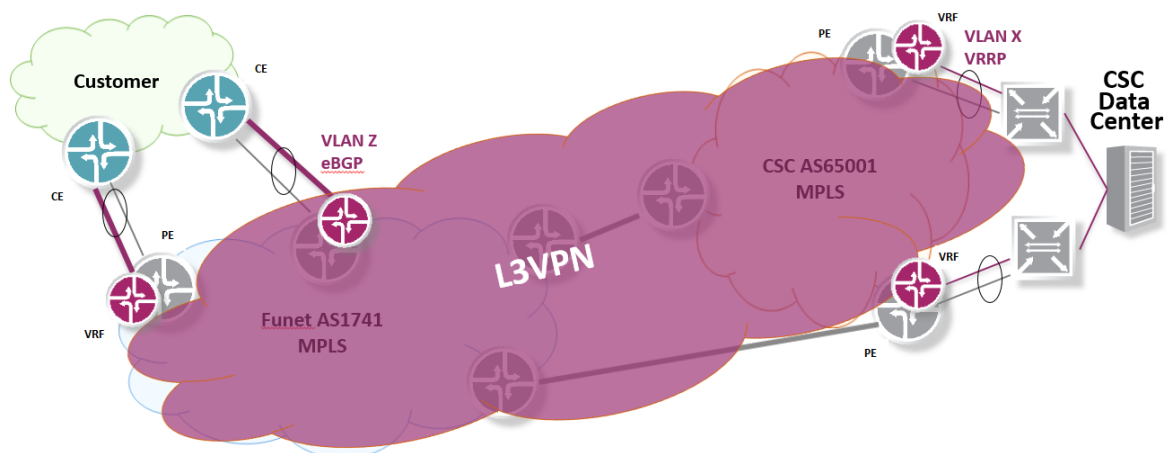


Figure 3.2: Connection between Funet backbone network and CSC's data center network

4 Use Cases

4.1 Remote campus interconnection

4.1.1 Redundant interconnection to the main campus

The organisation's headquarters are in the Helsinki metropolitan area and smaller remote office is in Oulu. The remote office has its own connection to the Oulu Funet router, through which it sends traffic directly to the Internet. Connections to services located in the main office are handled over the public Internet using a software-based VPN solution behind its own firewall. The aim is to achieve a direct connection with the same LAN and handle Internet traffic via a single point from the main office.

This could involve a traditional optical lightpath approach, or an MPLS-based VPN connection within the Funet network. A redundant backbone network-level route between the campuses is considered necessary from the perspective of reliability. Depending on the route, the distance between Helsinki and Oulu is 850–1,000 fibre kilometres, which may expose the connection to a significant amount of downtime each year. This requirement makes a lightpath solution a relatively expensive option in relation to the small number of employees. Construction of a lightpath would require visits to a number of intermediate locations before the route could be made available throughout the transmission network between the two locations, slowing down deployment.

In such a case, an MPLS-based connection would be a considerably more flexible option – configuration changes to customer connections, involving routers within the Funet backbone network in Helsinki and Oulu, would suffice. Gigabyte capacity would be more than sufficient for this location with respect to traffic directed to both the local area network and the Internet. Since the links between backbone routers are always redundant, in the event of a break in the fibre-optic network, the traffic will be automatically rerouted. Geographically, the routes are exactly the same as for the lightpaths but, in the case of the Funet IP backbone network, plenty of (shared) capacity is already available due to the 100 GB/s links between the core routers.

If the remote site did not already have an access link to the backbone router, more parameters and cost factors would have to be taken into account. In this context, no consideration has been given to a short, intra-city connection between the organisation and the Funet device. The most suitable MPLS VPN solution can be chosen for the organisation's environment, which is a routed L3VPN in this case. The different connection types are described in more detail below.

4.1.2 Interconnection to the main campus via another Funet member's connection

The above solution is also applicable to a situation in which one organisation has employees on the campus of another Funet member without their own Funet connection. With the consent and assistance of the owner of the local connection, these employees can be connected to their own organisation's internal network. Using the access links of the local Funet member, a connection can be established between the edge devices of the two organisations.

4.2 Provision of colocated data center services

CSC, which operates the Funet network, provides Funet members with a range of data center services, as well as colocation hosting services for members' own IT equipment. MPLS connection services are an ideal solution for this purpose, particularly if connections are needed to a single site from several offices. For example, virtual servers can be hosted in a remote data center for the provision of a few distinct internal services.

In principle, the aim is to realise connections of this kind as routed L3VPN solutions. Implementation as a routed connection enables features such as IP-level filtering between the campus network and colocations data center networks. This allows L2-level problems to be kept separate from each other. A routed solution is also more optimal with respect to network use – for example, there is no need for the pointless transmission of L2 broadcast traffic over the backbone network.

Traffic between internal campus networks and data center networks is routed via the organisation's internal network router or firewall, depending on how internal routing is handled within the current network topology. The user organisation defines the IP networks to be used on the data center side. If necessary, new addresses can be requested from the Funet Hostmaster. Each of the first three IP addresses is reserved for use by CSC data center routers: two specific router addresses and one virtual gateway address (VRRP). These provide a default route to the virtual servers.

In addition, VLAN identifiers are defined for Internet and data center traffic. The latter requires a new /30 or /31-size link network. If the connection from the campus is redundant, the backup connection needs another new link network for each added VLAN.

In the example in Figure 4.1, the organisation's Funet connection terminates directly at the firewall, which both acts as a router for the internal network and handles external routing to the Internet. In such topologies, the firewall is therefore often the campus network's only routing device and static routing is used. Traffic from a data center to the public Internet is routed via the campus firewall. The black line in the figure represents the Internet VLAN and the red one depicts the MPLS-VPN VLAN connected to the data center.

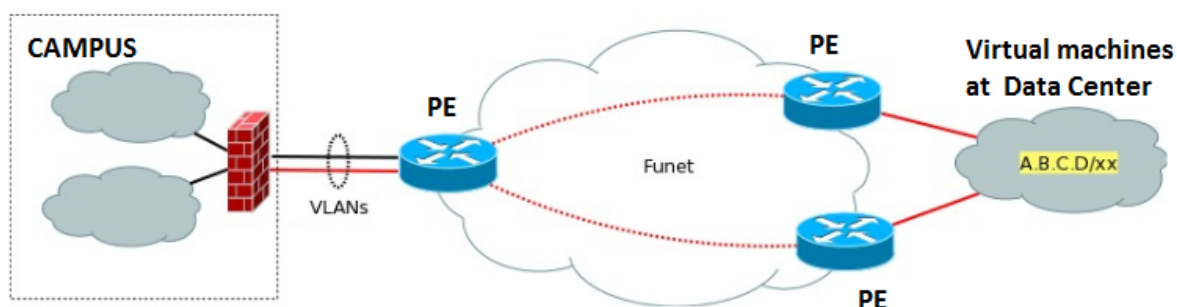


Figure 4.1: Example of provision of colocation data center services for a campus

If separate internal and external network routers are located on the edge of the campus network, the VPN can also be terminated directly at the internal network router, if the VLAN can be connected between the devices. If the routers' roles are separated by virtualisation based on the same physical device, this can be done by configuration. In this model, the Funet backbone router and the organisation's internal network router are connected to each other at L2 level.

If BGP is used for routing between the campus and Funet, different BGP neighbour relationships are formed for the links of different purpose. The Funet core router advertises the networks of the virtual machines to the campus via the VPN BGP neighbour relationship, while the campus advertises a default route to the backbone network. Figure 3.2 in the previous section presents such an implementation over a redundant access link. There are many more possible architectures not covered in this document.

5 Available connection types

Routed L3VPN connections and various L2-level connections, which allow the extension of the desired Ethernet VLAN segments between campuses, can be realised using MPLS connectivity services. A more detailed description of different types of VPN connections is presented in the following sections. It is worth noting that several VPN connections of different types can be realised simultaneously through the same access links to the same or different remote sites. – for example, an L3VPN connection can be created between two campuses via a single VLAN, and several L2VPN connections via parallel VLANs.

5.1 Routed L3VPN

A routed L3VPN connection is a service whereby the entire Funet backbone network is visible to a member organisation in the same manner as a single virtual router. This service enables the interconnection of IP sub-networks within the member organisation's internal network, via a virtual network logically isolated from other traffic. Any networks desired by the member organisation can be routed over an L3VPN connection, including private networks meeting standard RFC1918 [RFC 1918]. The L3VPN service also supports the routing of IPv6 networks.

The L3VPN service is particularly suitable e.g. for connecting remote campus networks to a member organisation's internal network, or the creation of a routed virtual network between the networks of various member organisations. An L3VPN service is a highly scalable and technically sound solution for redundant Funet access links in particular, where route redundancy can be achieved using a routing protocol.

The service is provided within its own VLAN on the access link between the Funet network and the member organisation. MPLS VPN traffic is logically separated from the member organisation's other Internet traffic. If a member organisation's edge device is capable of routing, a point-to-point link network is generally configured within the VLAN of the L3VPN connection. The desired networks are routed via this network either statically or using a dynamic routing protocol (generally BGP, possibly OSPF). In some cases, the member organisation's LAN segment can be directly connected to the Funet backbone router, in which case the network gateway is a Funet router. If necessary, in such situations a failover route can be provided to the gateway using VRRP [RFC 5798].

Depending on the campus network topology and other possible boundary conditions, logic suggests that an L3VPN connection should also be located in its own virtual router on the edge of the campus network. Most modern IP routers support virtual routers in some form or other, whether under the name of VRF, virtual-router or VRF-lite etc. Virtualisation of this kind can be implemented in Funet router service devices.

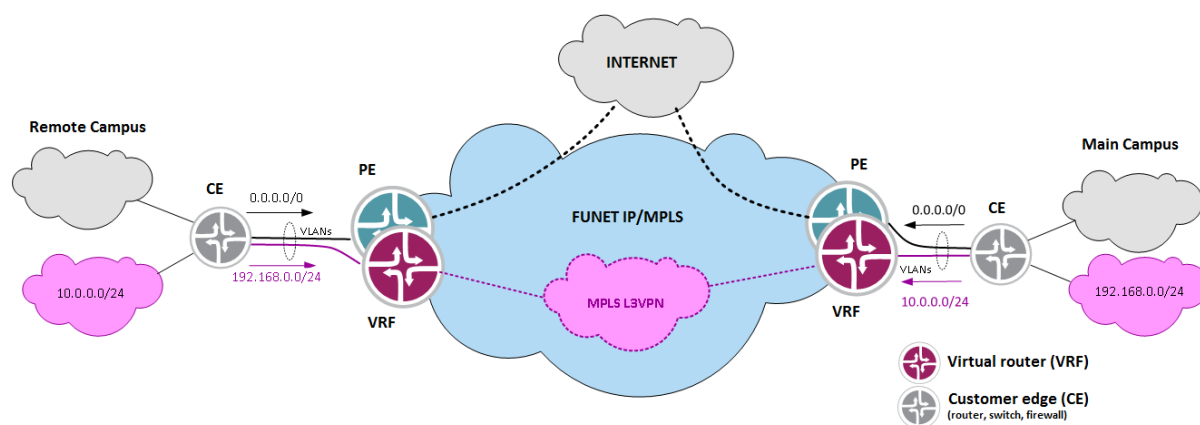


Figure 5.1: Illustration of a routed L3VPN service where private addresses are being used at remote campus

5.2 Virtual switch L2VPN / VPLS

The L2VPN service can be used, for example, to extend VLAN segments between campuses. Depending on what is needed, a connection can be implemented as a point-to-point connection where, from the perspective of the campus network, the Funet network functions like a virtual Ethernet bridge; or as a multipoint-to-multipoint connection where the Funet network functions like a virtual Ethernet switch. The latter case is referred to as a Virtual Private LAN Service (VPLS) [RFC 4761].

If the edge device of a member organisation supports stacked VLAN tags (QinQ tunneling), Ethernet frames on the Funet access link can be tagged with two VLAN tags. This enables the member organisation to use any inner VLANs it wishes via the same VLAN. The maximum allowed frame size (MTU) in the QinQ tunnel is reduced by four bytes for every ~ 4k VLAN stack. The Funet network is then transparent to the member organisation's VLANs. If QinQ is not possible, the L2VPN connection can be implemented to accept predefined VLAN space. In such a case, there is no need to implement a separate VPN in order to extend an individual VLAN to another office. Where necessary, Funet routers can also be used for flexible rewritings of VLAN tags, in which case the tags do not have to be the same at both ends of the connection.

A typical use case would be one in which the intention was to use the L2VPN connection's VLANs to create a connection from the member organisation's edge device all the way to the internal network. If the VPN connection is implemented using a member organisation's existing Funet access link, the member's edge device needs to be able to perform L2 switching in the direction of the desired VLANs. This should be considered, particularly in situations where the Funet access link terminates at a device that only performs L3 routing. If a Funet access link is already physically connected via a switch, the VLANs can be directly connected to the internal network using the edge switch. In either case, VLAN tags should be adopted for the links between Funet and the member organisation.

Unlike DWDM-based optical lightpaths, the L2VPN connections provided on top of a IP/MPLS network are not completely bit-transparent and, as a rule, the transmission of various L2-level control frames (Spanning Tree BPDU, LACP etc.) over an MPLS network is not supported. Furthermore, Funet network routers do not participate in the Spanning Tree topology of the member organisation's L2 network. If the Funet access link is redundant, the L2VPN connection can also be implemented as a redundant connection, in which case active route selection and L2 loop prevention are handled using the features of the Funet backbone network. Ethernet OAM features should be used between the Funet router and member organisation's edge device, particularly in the case of redundant connections, so that redundancy is not solely dependent on link status.

Figure 5.2 illustrates how a VPLS service can be used to interconnect Layer 2 segments in different campuses via the Funet backbone network. In practice, from the viewpoint of the member organisation, the Funet network is rather like one large virtual switch. The L2VPN service is similar in most respects, except that it has only point-to-point connections, while a VPLS network is a multipoint-to-multipoint network. In the figure, the member organisation's Funet connection terminates at the switching device, but it should be noted that, depending on the characteristics of the edge device, the switch functions can often be implemented on the same physical device as L3 routing.

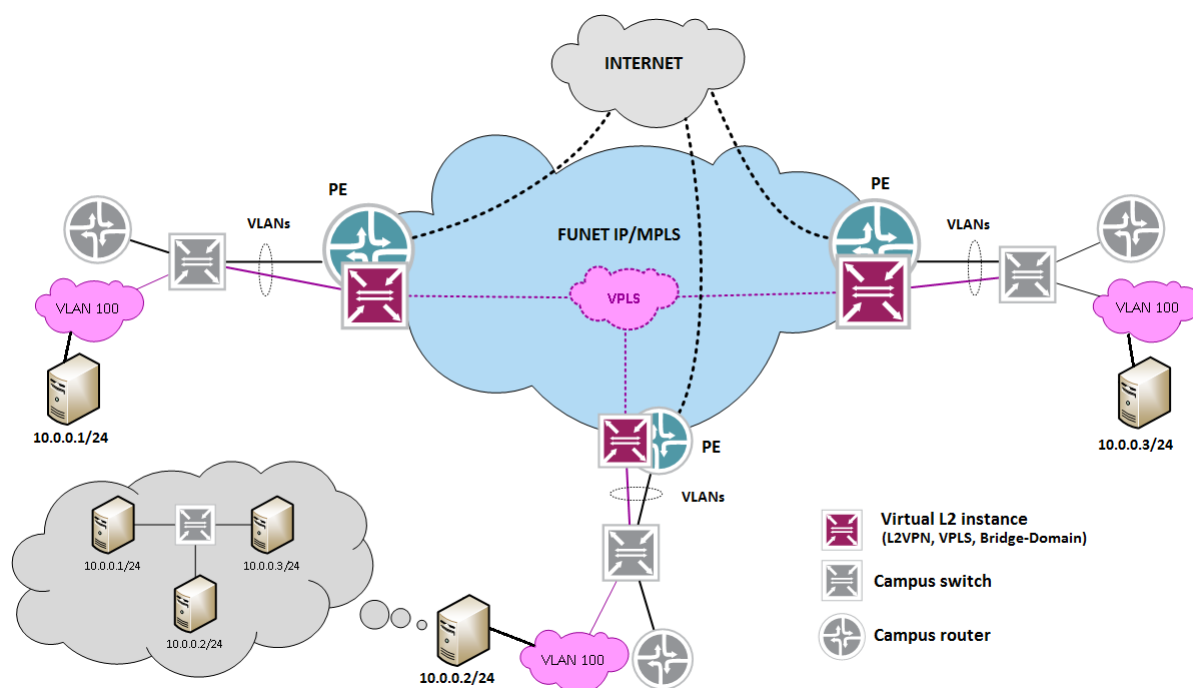


Figure 5.2: Illustration of a routed L3VPN service where private addresses are being used at remote campus

5.3 International connections

MPLS VPN connections to other research networks abroad can also be implemented, in addition to internal connections within the Funet network. Typical applications include multi-national research projects, in which someone wants to create connections from several locations to a data repository or measuring device. This type of connectivity service is typically not available from commercial ISPs.

Most MPLS VPN connections built abroad are realised using the Multi-Domain VPN infrastructure, which is developed and run by GÉANT and brings National Research and Education Networks (NRENs) together. The platform is designed to scale up for large projects. VPN routes are maintained only on network PE devices considered essential to the service concerned. The backbone network can only identify routes between routers. MD-VPN technology is available to around twenty research networks and 400 locations in Europe. Full MD-VPN service architecture description is available from GÉANT [DS3.3.1].

If MD-VPN is unavailable within the research network to which a connection is needed, connections can also be implemented using so-called Bandwidth-on-Demand (BoD) technology. This is available in a number of countries in which MD-VPN is not supported.

MD-VPN technology can be used to implement both L3VPN connections and point-to-point L2VPN connections. Only point-to-point connections can be built within research networks that support BoD technology.

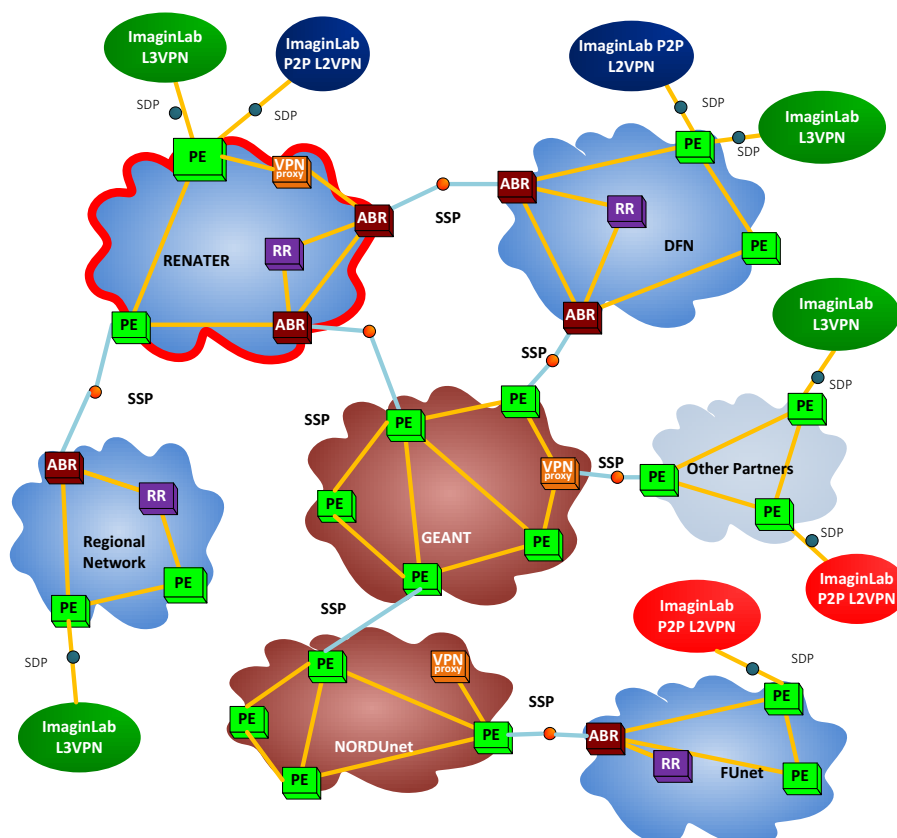


Figure 5.3: An MD-VPN infrastructure between several NRENs interconnecting ImaginLabs © GÉANT

6 Comparisons between connectivity service technologies

In terms of capacity, an optical lightpath is the only solution that guarantees capacity: all of the acquired capacity is available at all times. MPLS-based solutions share IP backbone network capacity on a Best-Effort quality basis. Using service categories, a certain minimum is always reserved for such traffic and no congestion is expected on the 100 GB/s backbone network links for years. The organisation's access network connection with Funet would probably experience congestion first. For connections that regularly need speeds of several gigabytes per second, a lightpath remains the best option.

In any case, the time taken to deploy a lightpath depends on the geographical location and the capacity already installed in the network. Connections within the Funet transmission network are always fixed and point-to-point and can reach around 30 locations. If hardware purchases are needed, the deployment time can last several months. In general, a capacity upgrade is only possible by increasing the former speed ten-fold, by changing components in the 1–10–40/100 GB/s category.

Redundancy for the lightpath usually requires the construction of a second physical path between the end points in the Funet transmission network. This tends to make this a more expensive and time-consuming solution. Optically redundant connections exist between some key locations, which incur no costs for the user. These reserve the same network capacity as two separately implemented connections.

In all cases, Funet's internal MPLS between backbone network routers is redundant. Redundancy between the client organisation's campus and the nearest Funet device depends on the rest of the network implementation at both ends. Redundancy of MD-VPN connections corresponds to the local, IP-level redundancy for each party's network through which traffic is moving.

In the case of applications that are sensitive to variations in the end-to-end delay, a lightpath is the best option. The delay is constant on a given geographical route and the traffic does not end up queuing on its way through transmission network devices. In MPLS VPN connections, a delay occurs in each router device through which the connection passes. When loads are exceptionally high, this may have an impact on variation in the delay. Because there are more processing points and longer distances in the case of international connections, both the absolute delay and variations in it may be greater than within the national network.

The introduction of an MPLS service tends to require only configuration work in the case of existing connections. Since Funet access links are often implemented on backbone routers located further along lightpaths, such solutions always have dependencies related to the structure of the transmission network. An MPLS service always terminates at a Funet backbone router, or a router service device being used by the customer. Within the limits imposed by the access link, capacity can be adjusted using software. This makes deployment lighter and faster than in the case of a traditional lightpath.

A lightpath which physically separates its traffic from all other traffic is the most secure option: traffic can only be intercepted by capturing light from the optical fibres. In addition, Ethernet traffic at the campus ends can be encrypted, for example by using devices that support the MACsec [IEEE 802.1AE] standard.

Apart from in crisis situations, Funet's internal MPLS remains within its own network, which logically separates member organisations from each other. Network devices along the way are under Funet's own control. Only simultaneous failures across the backbone network could lead to a situation in which Finland's internal IP network connections follow the "backup route of the backup route", through NORDUnet in Sweden. Of course, in such a case, lightpaths between the same locations would be broken anyway.

Despite the use of the term, "VPN", traffic is not encrypted within the MPLS network. International MD-VPN connections share infrastructure with other trusted research networks.

Financially and administratively, and in terms of the deployment time, the MD-VPN is by far the best option for international, dedicated connections. It could take months to get a traditional lightpath provisioned and ready for use. Funet MPLS VPN services are available in Finland only.

There is no difference between a lightpath and Funet internal MPLS VPN solution in terms of lifecycle. The capacity categories available can vary between network generations. The lifecycle of MD-VPNs will depend on the decisions taken by international actors. GÉANT, the pan-European data network for the research and education community, is investing heavily in the technology.












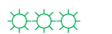


















| | Lightpath | MPLS VPN within Funet | International MD-VPN |
|--|--|---|---|
| Capacity |  guaranteed |  best effort |  best effort |
| Security level |  highest physically separated within own network |  high logically separated within own network |  fairly high logically separated within international network |
| Delay variation |  fixed delay |  slightly variable |  variable |
| International connections |  limited |  not available |  around 20 countries within Europe |
| Redundancy |  for extra fee and installation work |  between core IP routers |  between core IP routers |
| Provisioning |  heavy investments and physical installations |  light configuration |  reasonable configuration and international coordination |
| Provisioning costs |  high hardware investments |  low if existing connections used |  reasonable if existing connections used |
| Technology lifetime |  guaranteed |  guaranteed |  technical: guaranteed administrative: reasonable guaranteed |
| Applicability for production level connections |  good |  good |  good |
| Scale:  = high,  = moderate,  = low | | | |

Table 6.1: Comparison of connectivity service technologies

7 Conclusions

MPLS VPNs are a proven technology to provide connectivity services between locations covered by the Funet network. Typical use cases include remote office interconnection, shared virtualisation environments, cloud services, research group collaboration, and connections to centralised data repositories etc.

MPLS VPN connections can share the same link capacity with campus Internet connectivity on a best-effort basis, resulting in higher link utilisation rates and added value to existing connections. MPLS VPNs are redundant between Funet core routers by default and can be configured to use redundant access links to campuses as well. Compared to traditional VPNs, traffic is not encrypted between sites, but logically separated in a trusted network environment.

MPLS VPN connections can operate at layers 2 or 3 depending on the use case. Network devices on the campus edge just need to support VLAN tagging. The L2VPN service can be used, for example, to extend VLAN segments between campuses. A routed L3VPN service enables the interconnection of IP sub-networks within the member organisation's internal network, via a virtual network instance logically isolated from other network traffic.

Setup is rather straightforward and fast configuration work compared to installing dedicated lightpath connections. Especially provision of short term connections is more flexible and affordable. Lightpaths still have their place in high capacity connections where network transparency, guaranteed bandwidth or possibly fixed delay is needed.

Multi-Domain VPN is an extension of the same idea in an international scale. Such connections can reach locations connected to other national research and educational networks in most countries within Europe. Interconnecting research groups over organisation and/or country borders has never been easier.

References

- [DJ1.1.1] GÉANT Deliverable DJ1.1.1: Transport Network Technologies Study, May 2010.
http://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-09-224-DJ1-1-1v1-0_Transport_Network_Technologies_Study_Read_Only.doc
- [DS3.3.1] GÉANT Deliverable D7.1 (DS3.3.1): MDVPN Service Architecture, Oct 2013
http://geant3plus.archive.geant.net/Resources/Deliverables/Documents/D7.1_DS%203%203%201-MDVPN-service-architecture.pdf
- [IEEE 802.1AE] "IEEE Standard for Local and Metropolitan Area Networks- Media Access Control (MAC) Security", IEEE 802.1AE-2006, June 2006
<http://standards.ieee.org/findstds/standard/802.1AE-2006.html>
- [IEEE 802.1Q] "IEEE Standard for Local and Metropolitan Area Networks- Bridges and Bridged Networks", IEEE 802.1Q-2014, December 2014.
<http://standards.ieee.org/findstds/standard/802.1Q-2014.html>
- [RFC 1918] Y. Rekhter, B. Moskowitz, D. Karrenberg, "Address Allocation for Private Internets", RFC 1918, February 1996.
<https://tools.ietf.org/html/rfc1918>
- [RFC 4364] E. Rosen, Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.
<https://tools.ietf.org/html/rfc4364>
- [RFC 4761] K. Kompella (Ed.), Y. Rekhter (Ed.), "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling", RFC 4761, January 2007.
<https://tools.ietf.org/html/rfc4761>
- [RFC 5036] L. Andersson (Ed.), I. Minei (Ed.), B. Thomas (Ed), "LDP Specification", RFC 5036, October 2007.
<https://tools.ietf.org/html/rfc5036>
- [RFC 5798] S. Nadas (Ed.), "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6.", RFC 5798, March 2010.
<https://tools.ietf.org/html/rfc5798>

Glossary

| | |
|---------------|---|
| BGP | Border Gateway Protocol |
| BoD | Bandwidth on Demand |
| CE | Customer Edge |
| DWDM | Dense Wavelength Division Multiplexing |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| L2 | Layer 2 |
| L3 | Layer 3 |
| LACP | Link Aggregation Control Protocol |
| LBE | Less than Best-Effort |
| LDP | Label Distribution Protocol |
| LSP | Label-switched Path |
| LSR | Label Switching Router |
| MD-VPN | Multi-Domain VPN |
| MPLS | Multiprotocol Label Switching |
| MTU | Maximum Transferrable Unit |
| NREN | National Research and Education Network |
| OAM | Operations, Administration, Management |
| PE | Provider Edge |
| PHP | Penultimate Hop Popping |
| QinQ | Queue-in-Queue |
| QoS | Quality of Service |
| VLAN | Virtual Local Area Network |
| VPLS | Virtual Private LAN Service |
| VPN | Virtual Private Network |
| VRF | Virtual Routing and Forwarding |
| VRRP | Virtual Router Redundancy Protocol |

