Multi-Domain Virtual Private Network service a seamless infrastructure for regional network and NRENS

Sébastien Boggia (OSIRIS)
Benjamin Collet (OSIRIS)
Jean Benoit (OSIRIS)
Christophe PALANCHE (OSIRIS)
Alain Bidaud (SYRHANO – CRIHAN)
Xavier Jeannin (RENATER) - presenter,

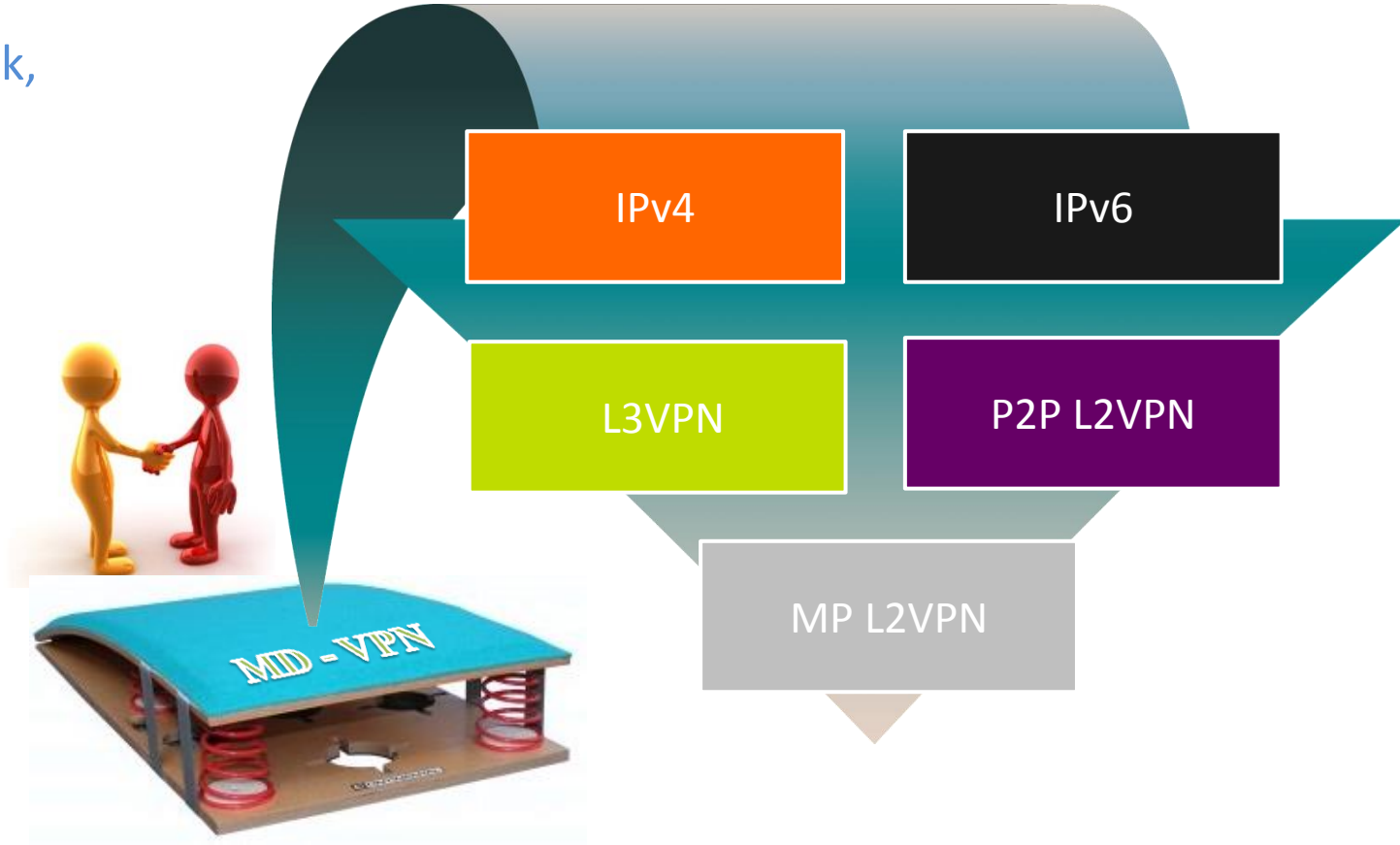
9 Dec 2015

jres Montpellier 2015

What is MD-VPN?

The service provides a seamless, scalable transport infrastructure

- A **joint service** provided by the GÉANT network, NRENs and Regional Network
- **A seamless transport infrastructure** that provides **a connectivity service**:
  - **Layer3 or Layer2 VPNs spanning several domains**
  - **point-to-point or multipoint**
  - Multi-domain networking

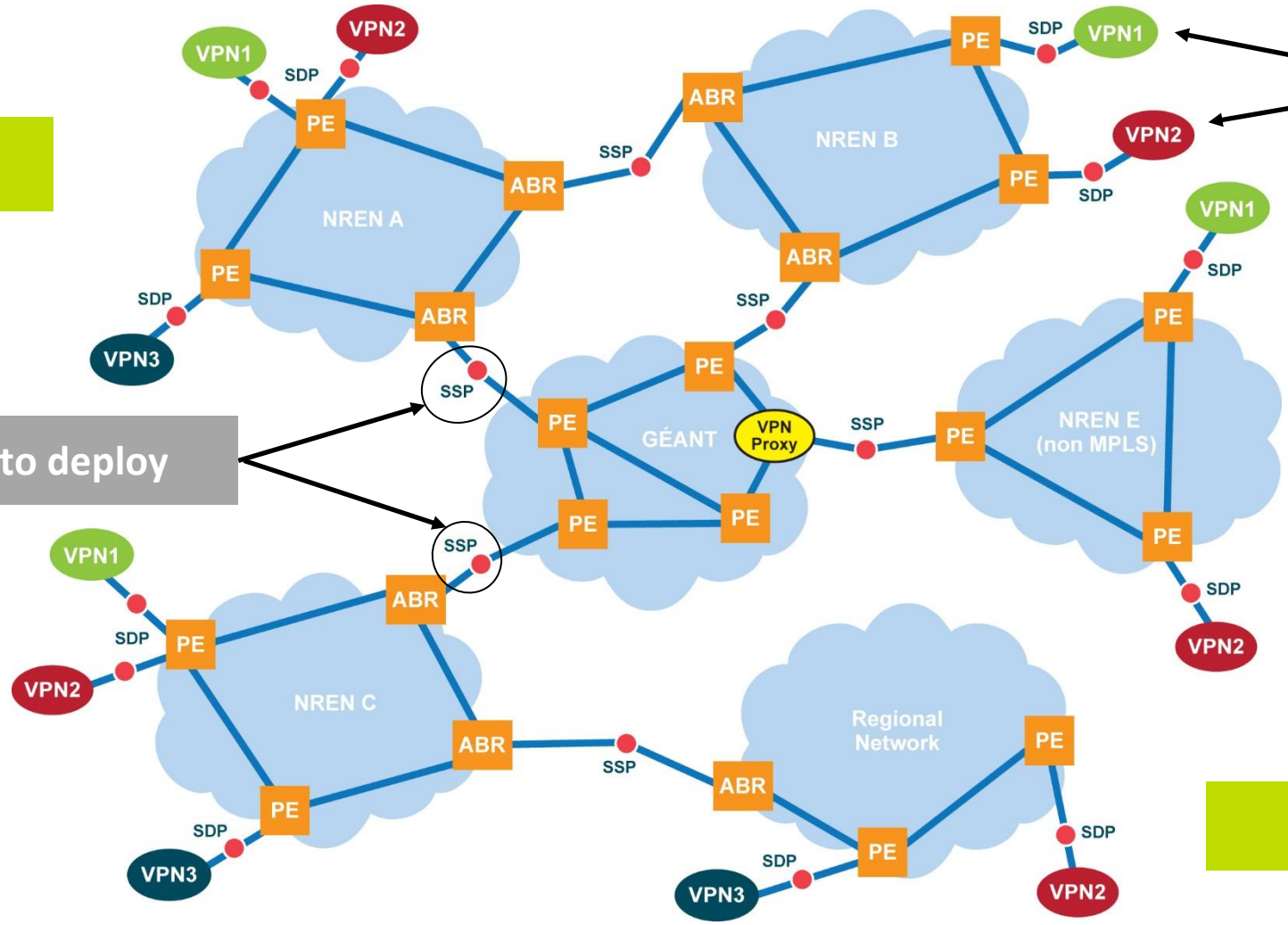


MD-VPN service highly scalable, seamless transport infrastructure

High scalability

Easy to deploy

An end-to-end extensible and flexible service

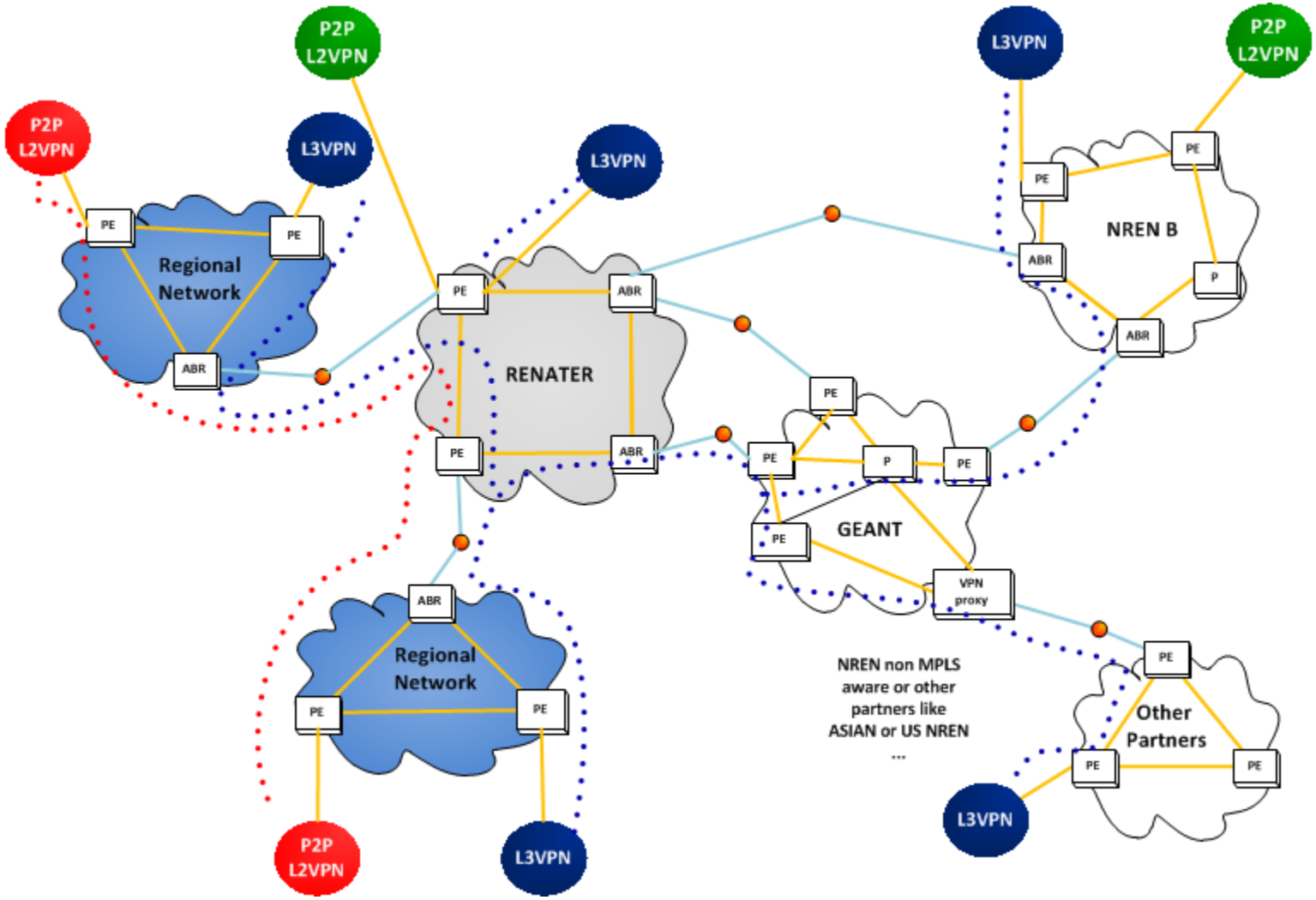


Configure only at the edge

Lead-time reduced

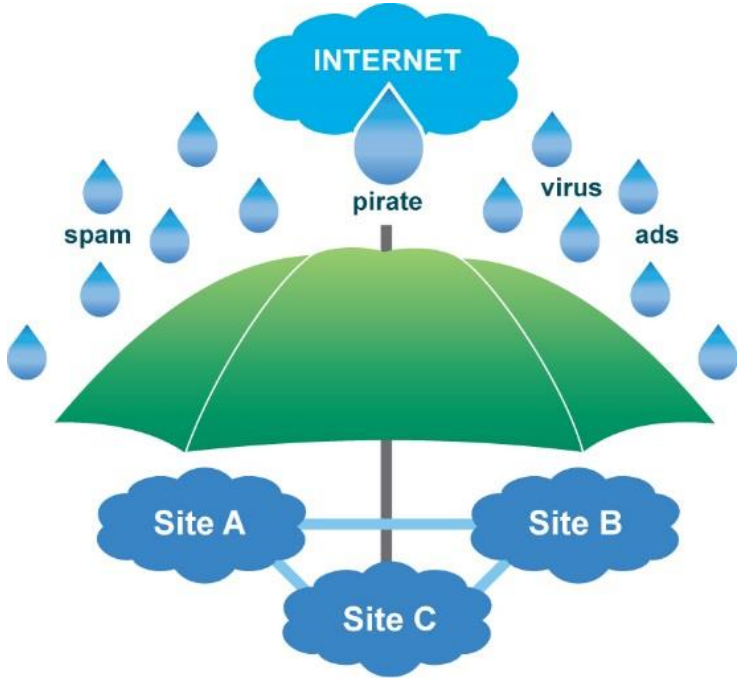
NREN OPEX Reduced

A double benefit for NRENs with regional network



An innovative design with added value for end-users

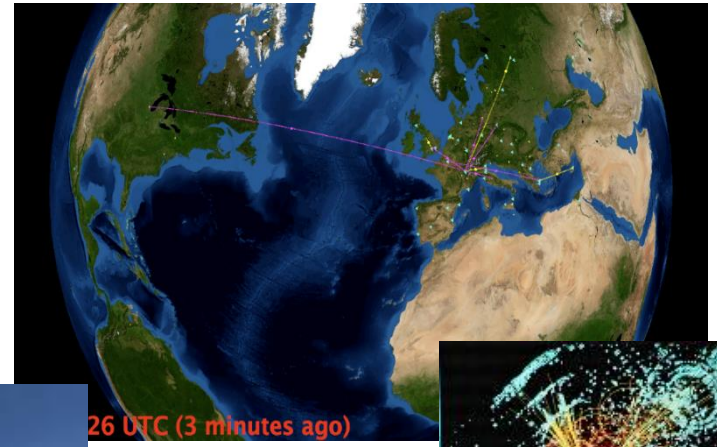
- **An original connectivity network service**
  - Multi-domain networking
- **Facilitate and foster distributed collaboration in Europe**
  - Cover a wide scope of use cases
- **Reduce OPEX and CAPEX for use**
  - Cost saving – VPN cheaper
  - Cost saving – No tender for research project
- **Safe infrastructure**
  - Security opex saved on site
  - Reduce firewall usage



MD-VPN use cases

A wide scope for MD-VPN use

- **All scientific projects based on international collaboration**
  - LHCONE is an example of successful L3VPN multi-domain service
  - ITER, CONFINE

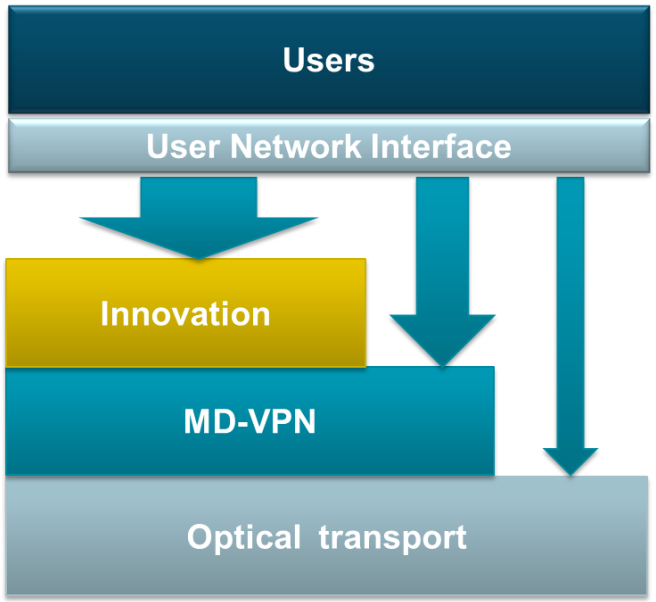


- **Distributed infrastructure**
  - **Cloud provider**
  - **Grid – HPC center**
  - **Scientific infrastructure:** Telescope, sensor network

MD-VPN use cases

A wide scope for MD-VPN use

- **Quick P2P connection**
  - Conference demonstration
  - P2P data transport between to sites
  - http://cuc.carnet.hr/2014?news_hk=5605&news_id=285&mshow=1105#mod_news



- MD-VPN transparent data transport layer for **high level network services like SDN,** … and in general by **future Internet project**

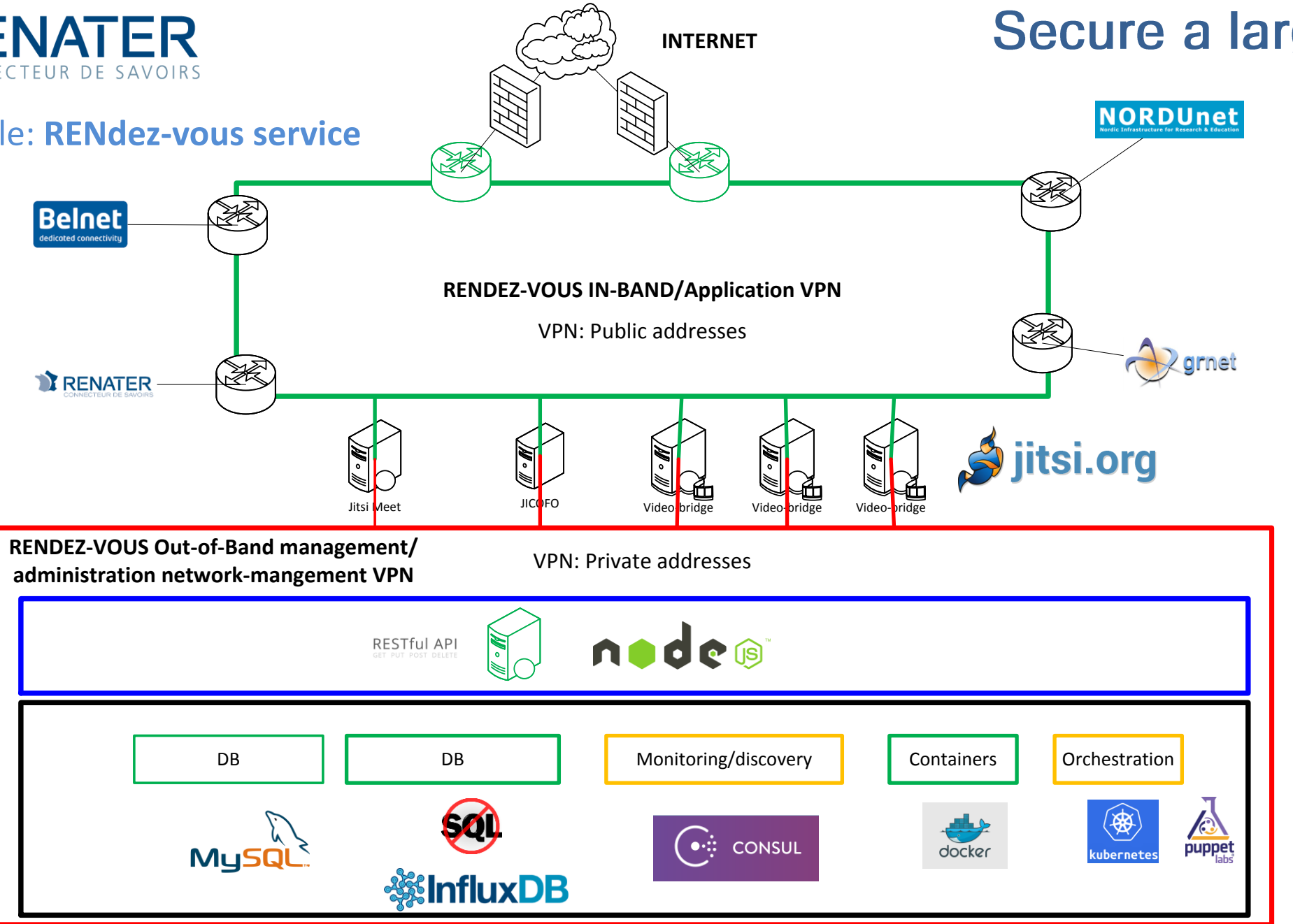
MD-VPN use cases
Regional Network

- **Large institutes spanned over several regions**
  - CNRS, University
- **ADD new services regional network portfolio**
- **Region enlargement …**
- **Data-Centers:**
  - Cloud, Méso-centres
- **Education**
  - Remote lecture : Medecine, …
  - E-learning
  - Exam: ECNI project
- **Virtual infrastructure**
  - Inter-university Backup L3VPN
  - Etc …

MD-VPN use cases

Secure a large service

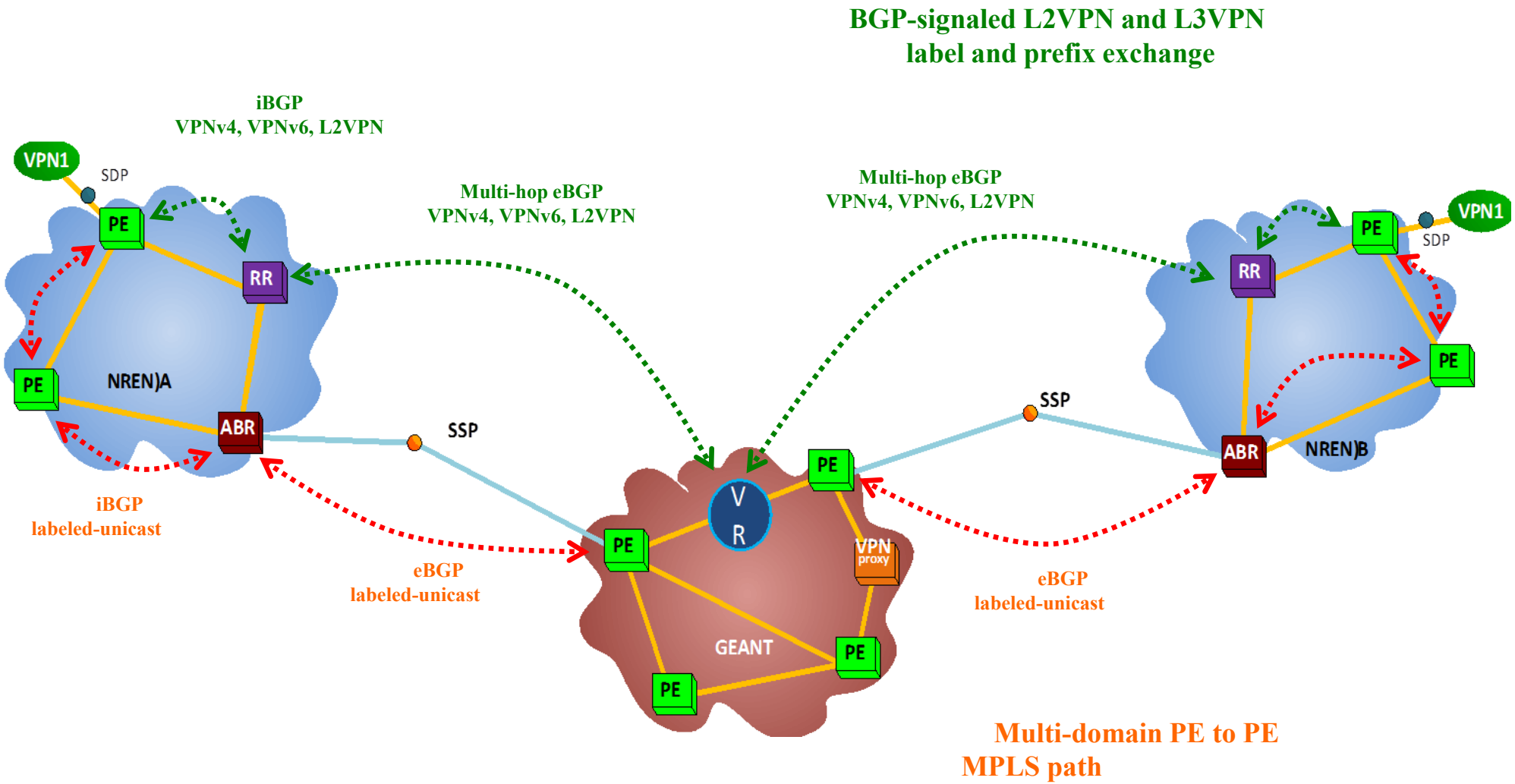
- Exemple: **RENdez-vous service**



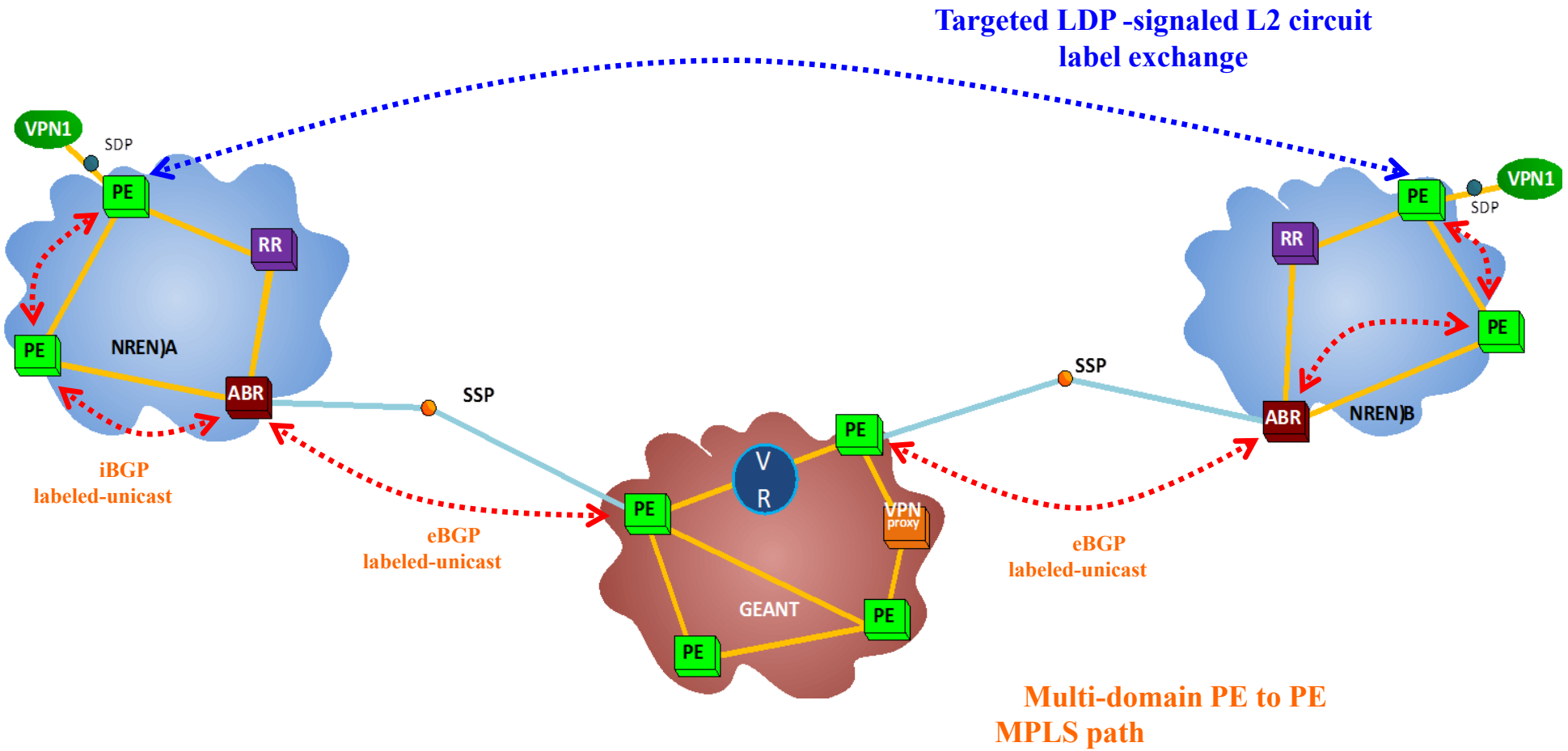
How it works?

- **Underlying principle behind this Multi-Domain VPN technology**
  - The LSP is extended from a PE up to the remote PE in another domain
  - **Signaling is split in 2 parts**
    - *Signalling for multi-domain MPLS path between PE routers* ***thanks to a BGP peering with labelled unicast SAFI (internal route)***
    - *Signalling for VPN labels and prefixes exchange between PE routers* ***(external route) thanks to an external BGP VPNv4 family peering***
  - GEANT and NORDUnet implement Carrier of Carriers (CoC) providing transparent transport of VPN traffic

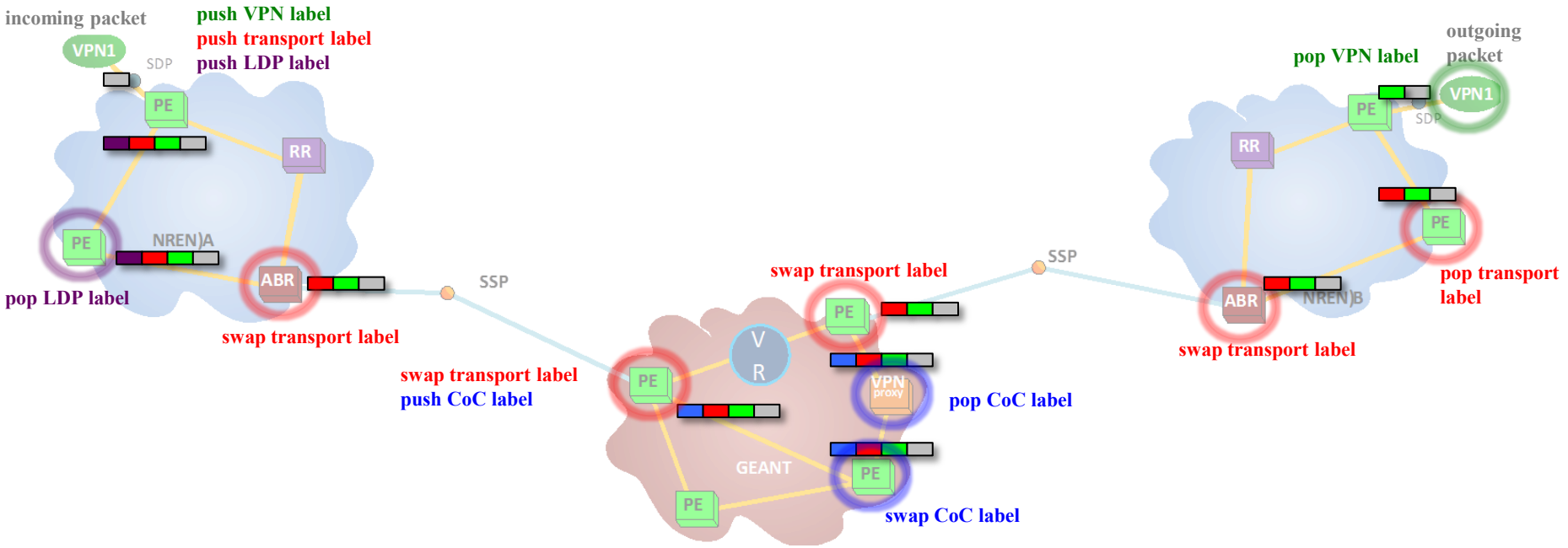
MDVPN: BGP-signalling L2VPN, L3VPN



MDVPN: tLDP-signalling L2 circuit



MDVPN data plane label operations



MDVPN packets labels:

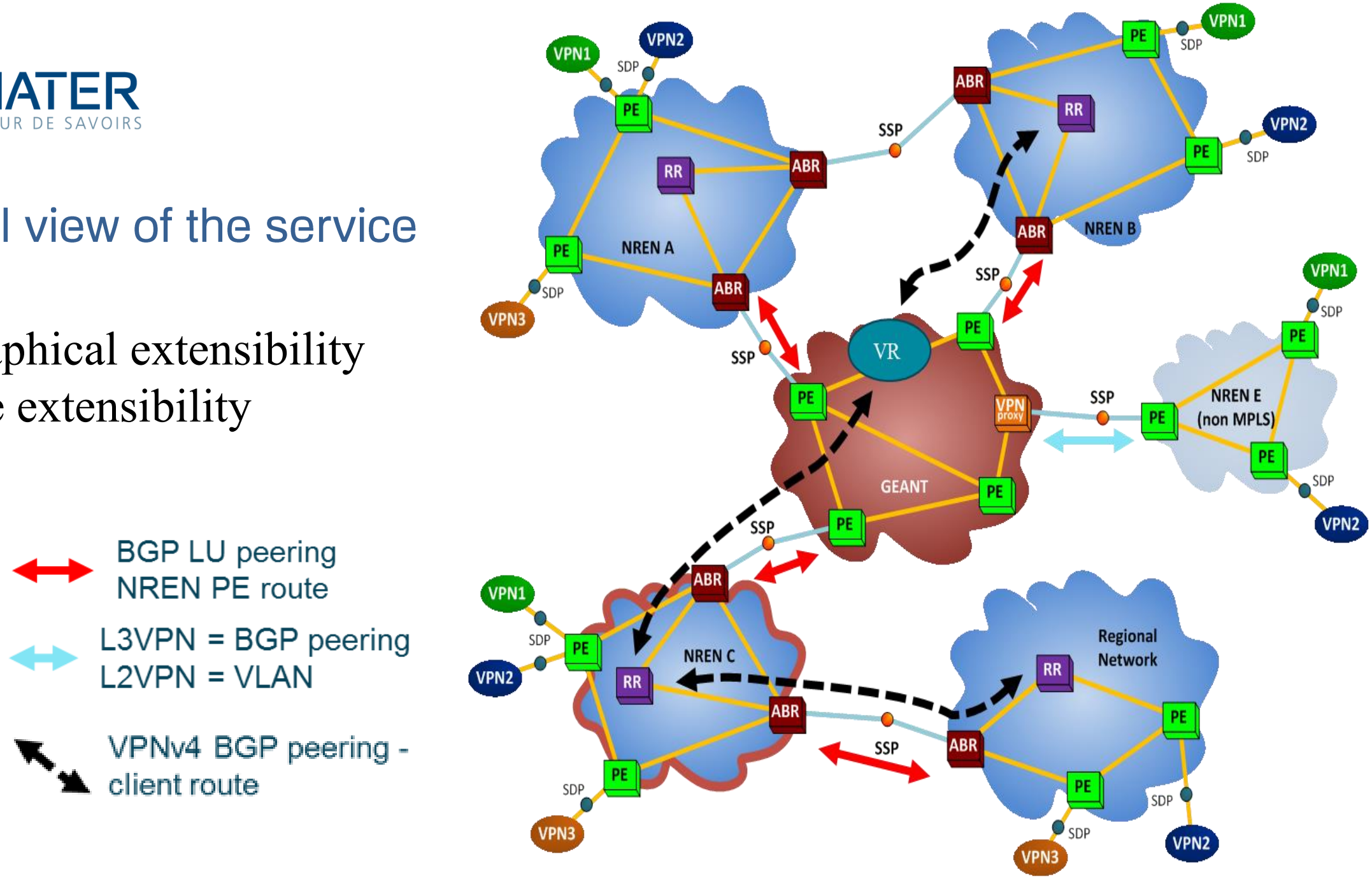
LDP label	Transport label	VPN label	Data
CoC label	Transport label	VPN label	Data

With the courtesy of Jani Myyry **(Funet)**

RENATER
CONNECTEUR DE SAVOIRS

Global view of the service

- Geographical extensibility
- Service extensibility



RENATER
CONNECTEUR DE SAVOIRS

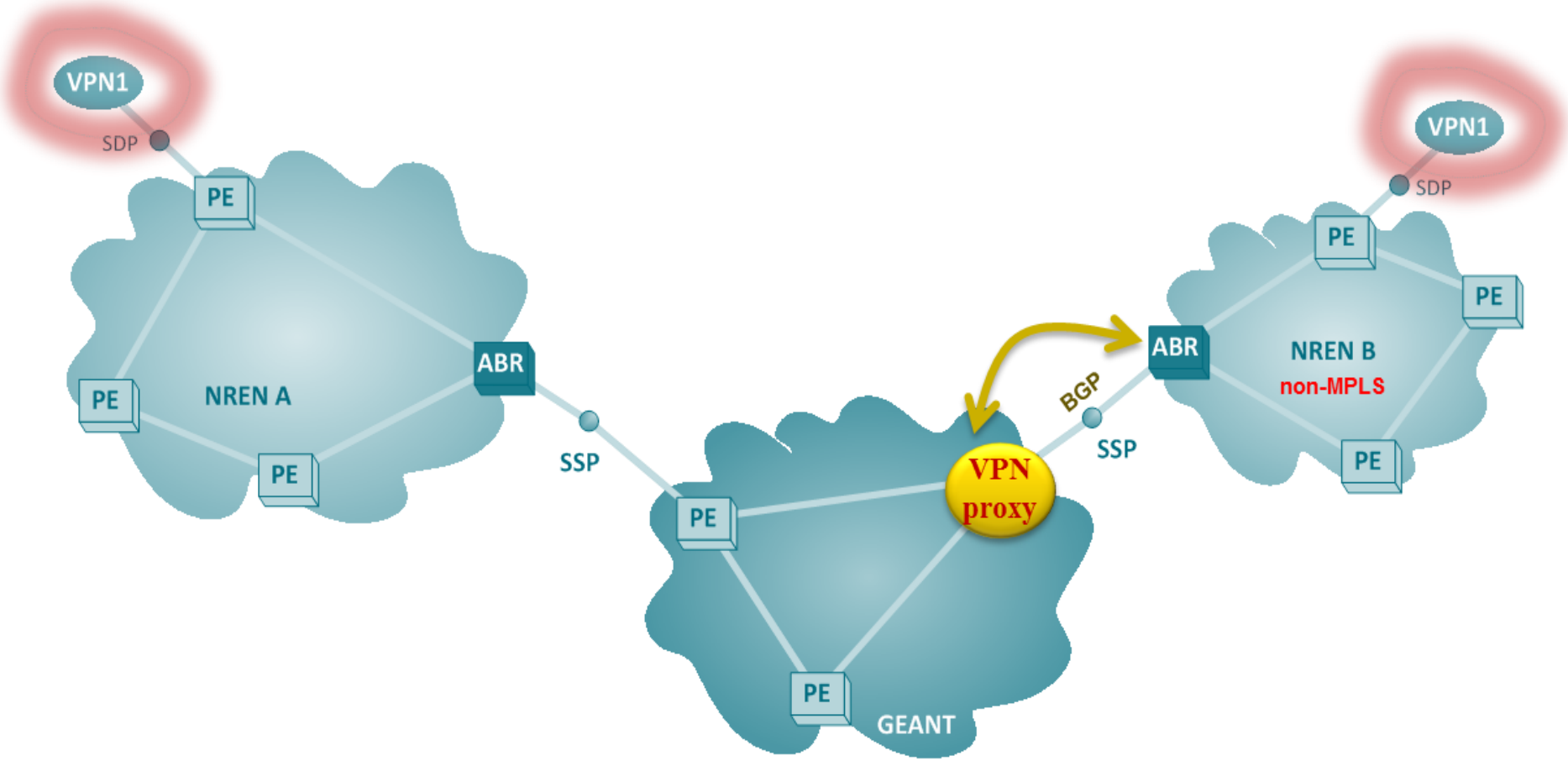
Scalability

- **MD-VPN is designed to provide thousands (and more) of service**

- Thanks to separation between data transport in the core network and services provided at the edge.
  - In the core network only labels and routes related to PE routers are maintained (1000 routes)
  - 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 and NORDUnet infrastructure since they are completely transparent to the GEANT network.

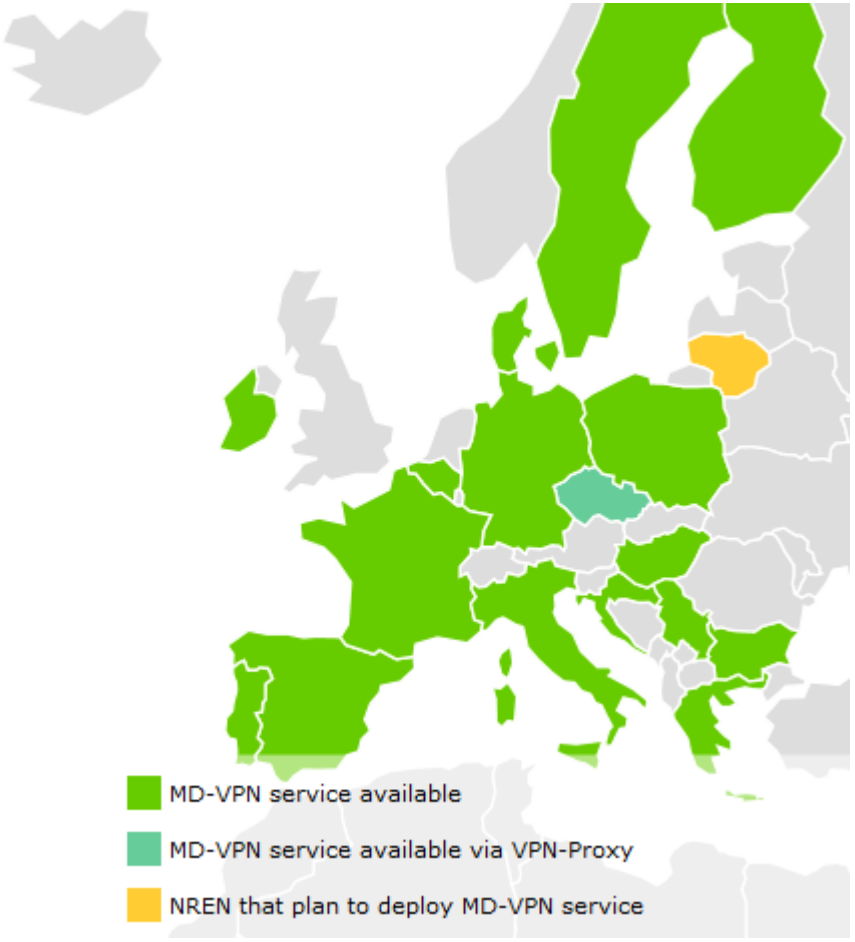
How to connect “non MD-VPN site”? VPN-proxy



Where can you use MD-VPN?

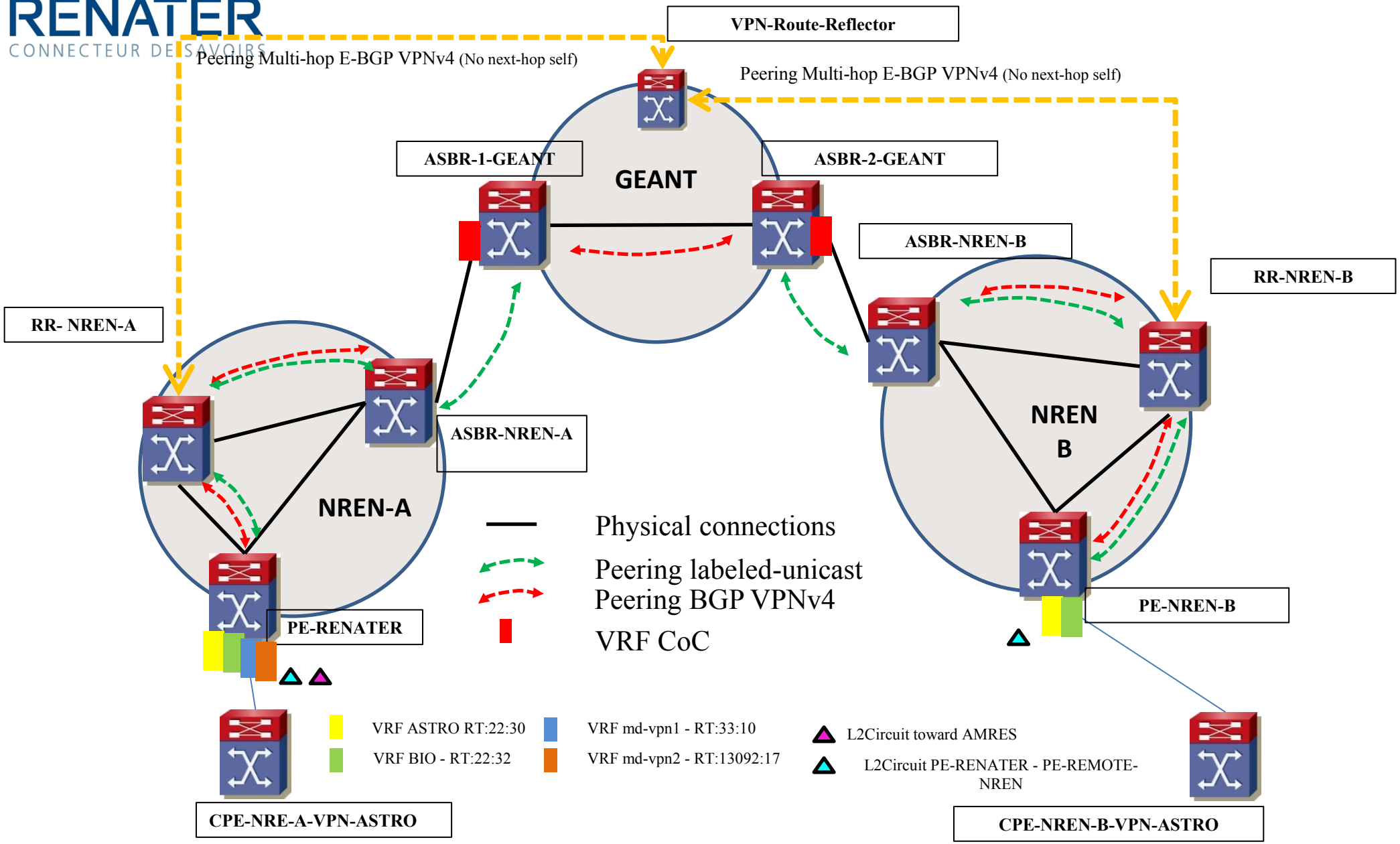
- **Pilot phase**
  - Service reliability long-term assessment ✔
  - Operation implementation ✔

- **MD-VPN service in the GÉANT**
  - **18 NRENs connected**
    (+ 1 NREN using MD-VPN Proxy + 1 NREN still working on)
  - **Roughly 400 PoPs available that European scientist can already use MD-VPN**
  - **In France : OSIRIS, SYNRHANO, RENATER …**

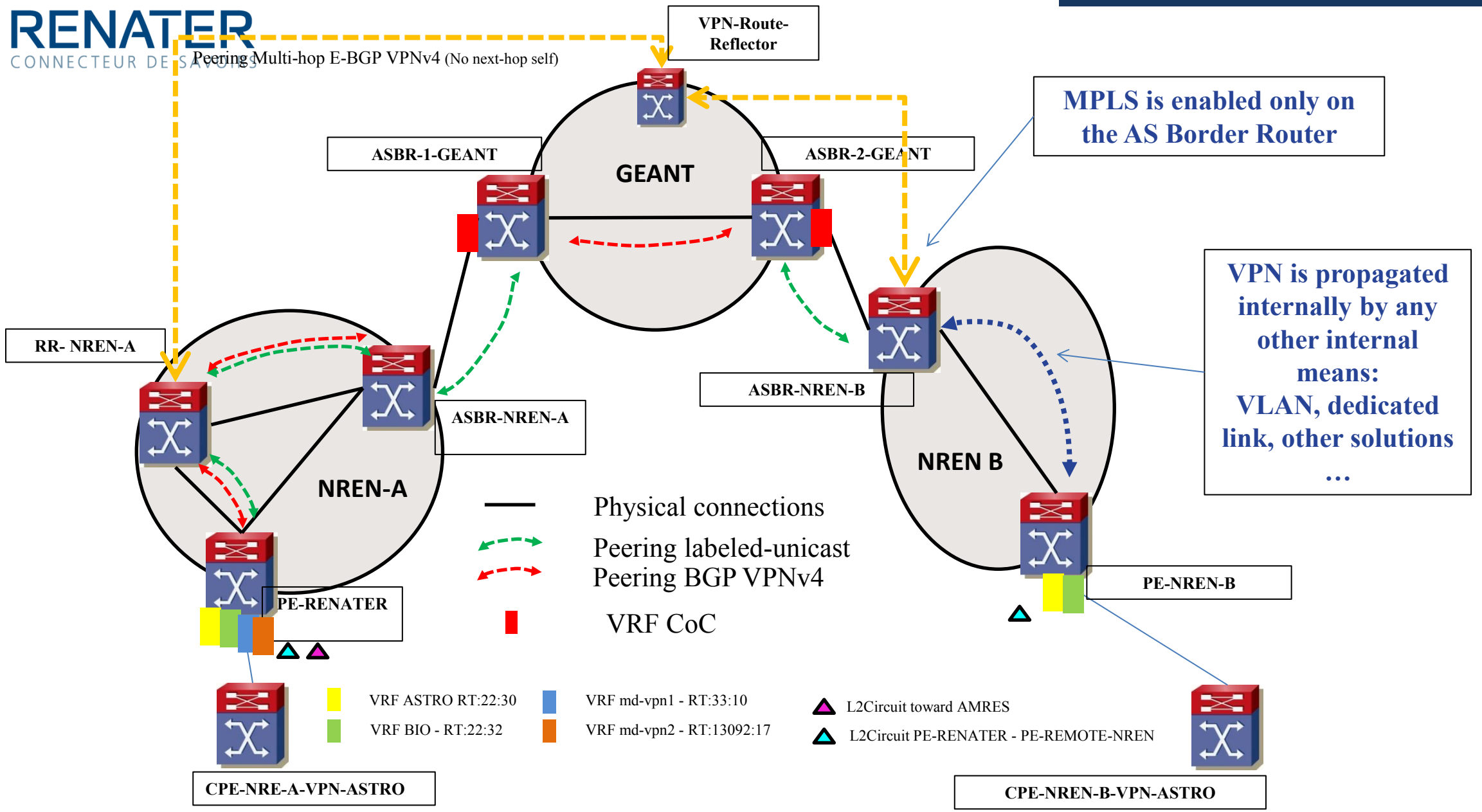


Standard deployment

RENATER
CONNECTEUR DE SAVOIRS



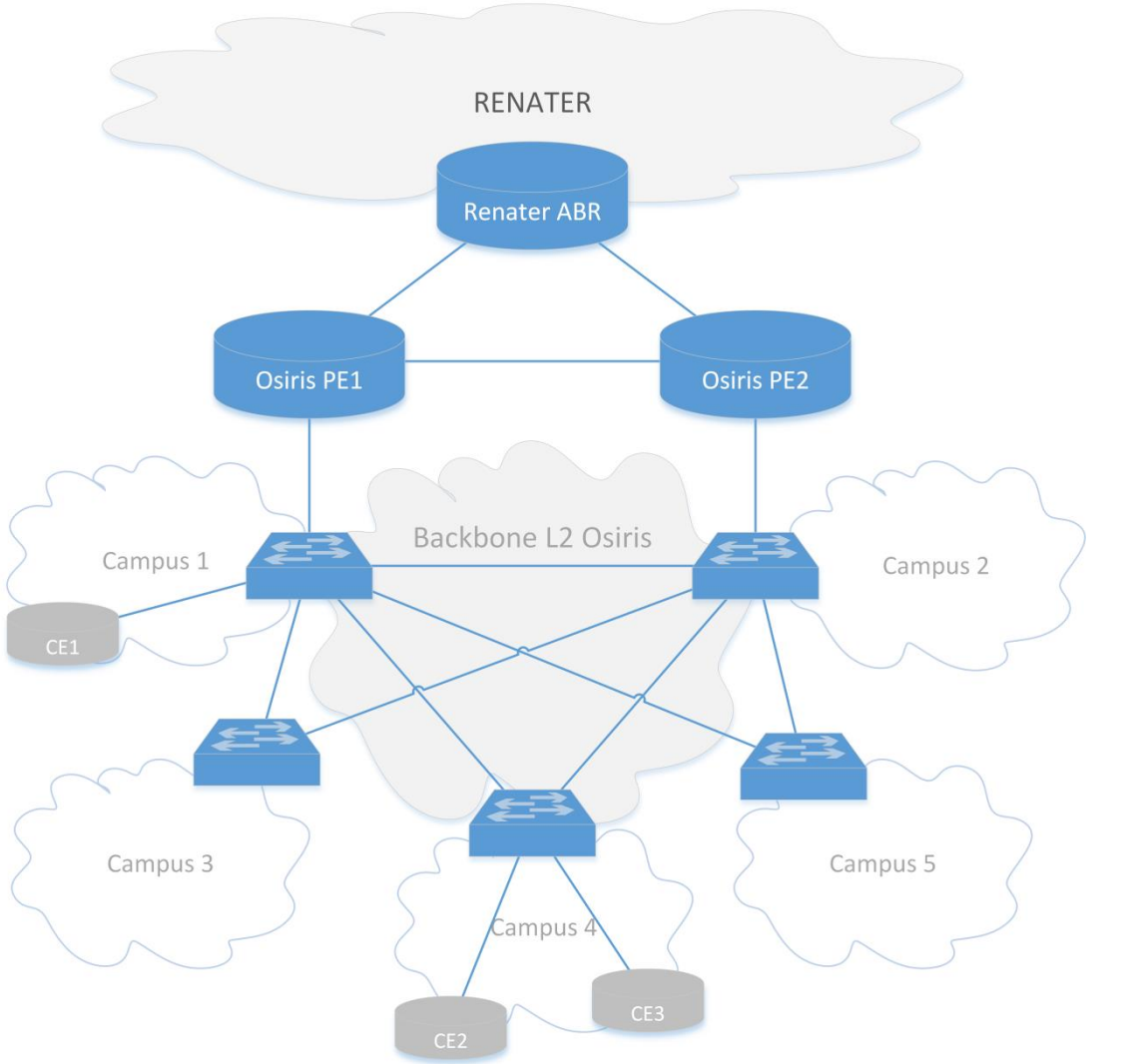
Limited deployment



OSIRIS deployment

- **Osiris network overview**
  - Research and Education network in Strasbourg and region Alsace
  - 10Gbs connectivity on its own optical fibre infrastructure in Strasbourg
  - Up to 400Mbs lease lines in region Alsace
  - 70000 users

- **Osiris network architecture**
  - 2 main routers attached to Renater
  - L2 ethernet backbone for aggregation
  - **MPLS not implemented**



OSIRIS deployment

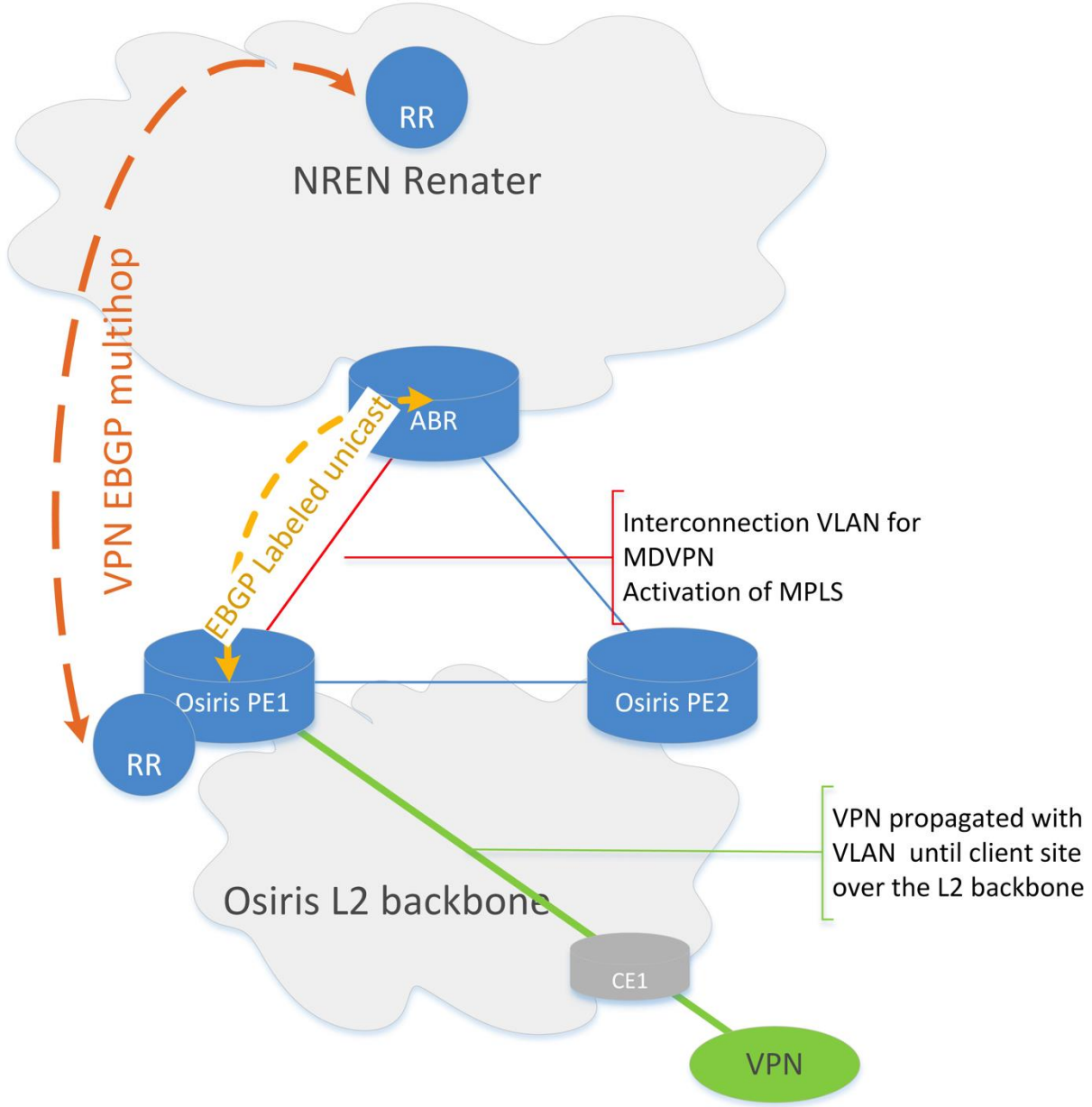
Deployment methodology

First step : Basic configuration.

Only one Osiris PE for delivering VPNs

Simplest way to deploy MDVPN

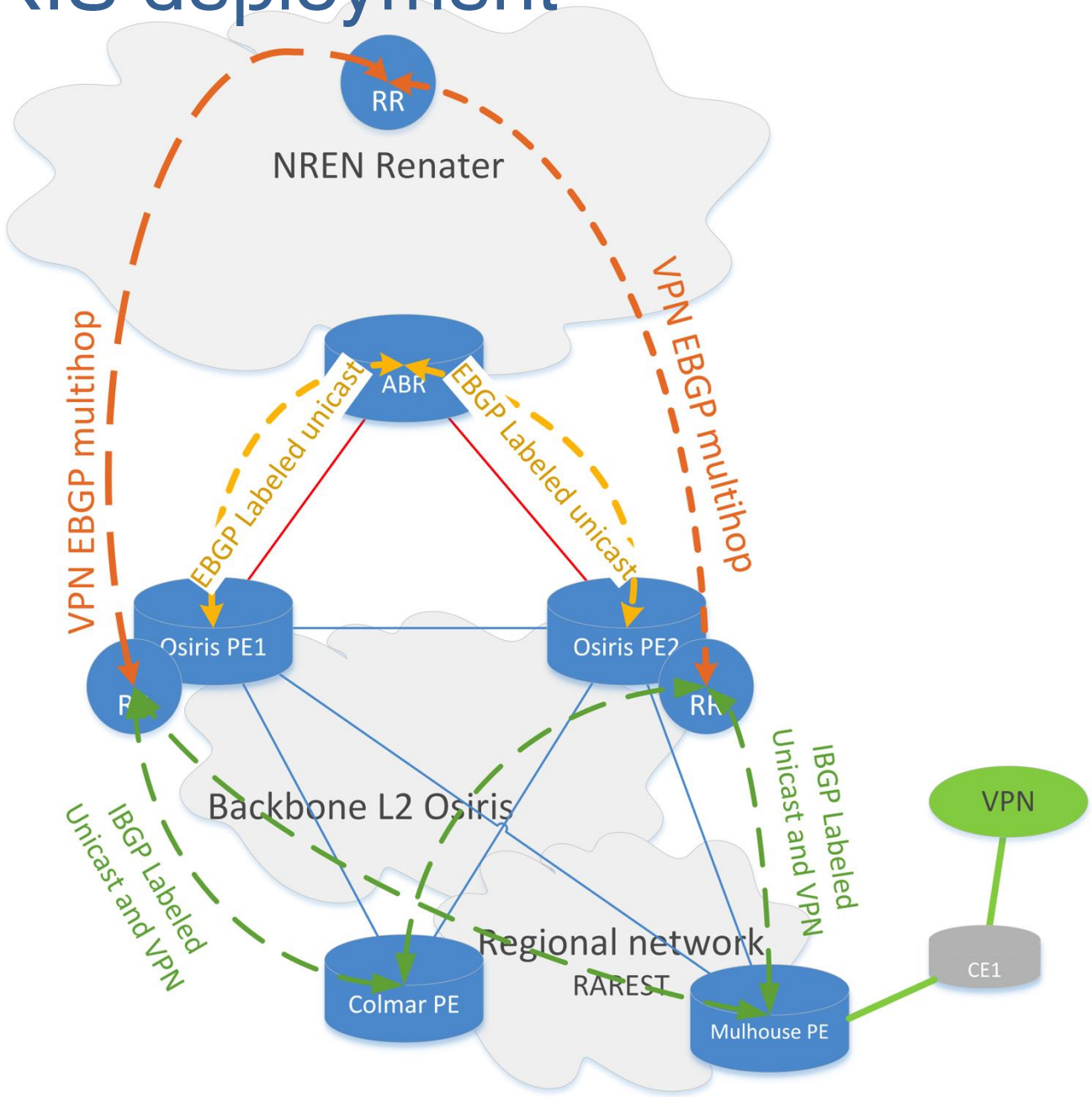
- 1 dedicated P2P MPLS connection between Renater and Osiris (same physical link than default Internet connection)
- Dedicated EBGP Labeled Unicast peering. Only PE router loopback announced (Osiris PE1)
- Dedicated EBGP peering between Oisiris PE1 and Renater Route Reflector for sharing VPN routes



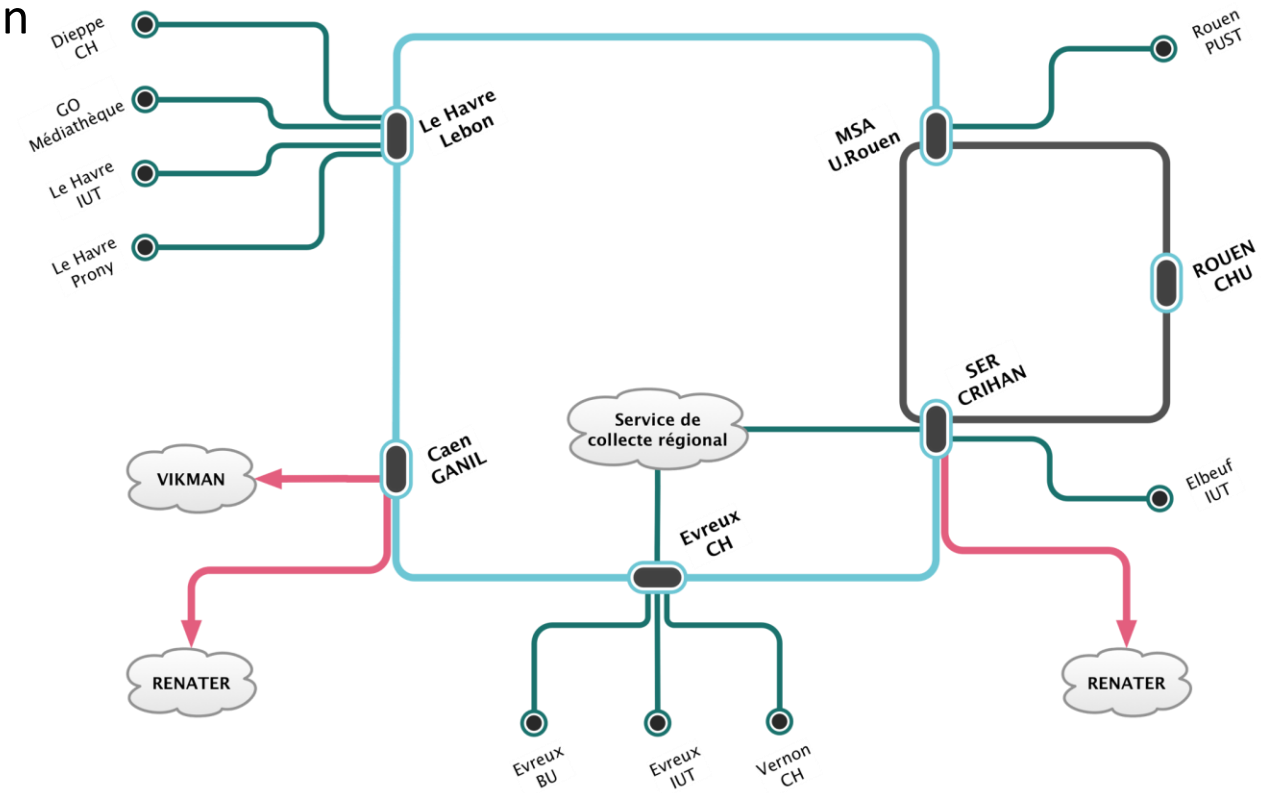
OSIRIS deployment

Second step :
Full redundancy and extension of MDVPN service to regional network

- Second dedicated P2P MPLS connection between Renater and Osiris with EBGP Labeled Unicast peering (Renater – Osiris PE2)
- Activation of MPLS between Osiris PE routeurs
- Second EBGP peering between Oisiris PE2 and Renater RR to share VPN routes
- Activation of MPLS on regional network PE routers
- IBGP Labeled Unicast et VPN peerings between regional network PE routers and Osiris Route Reflectors

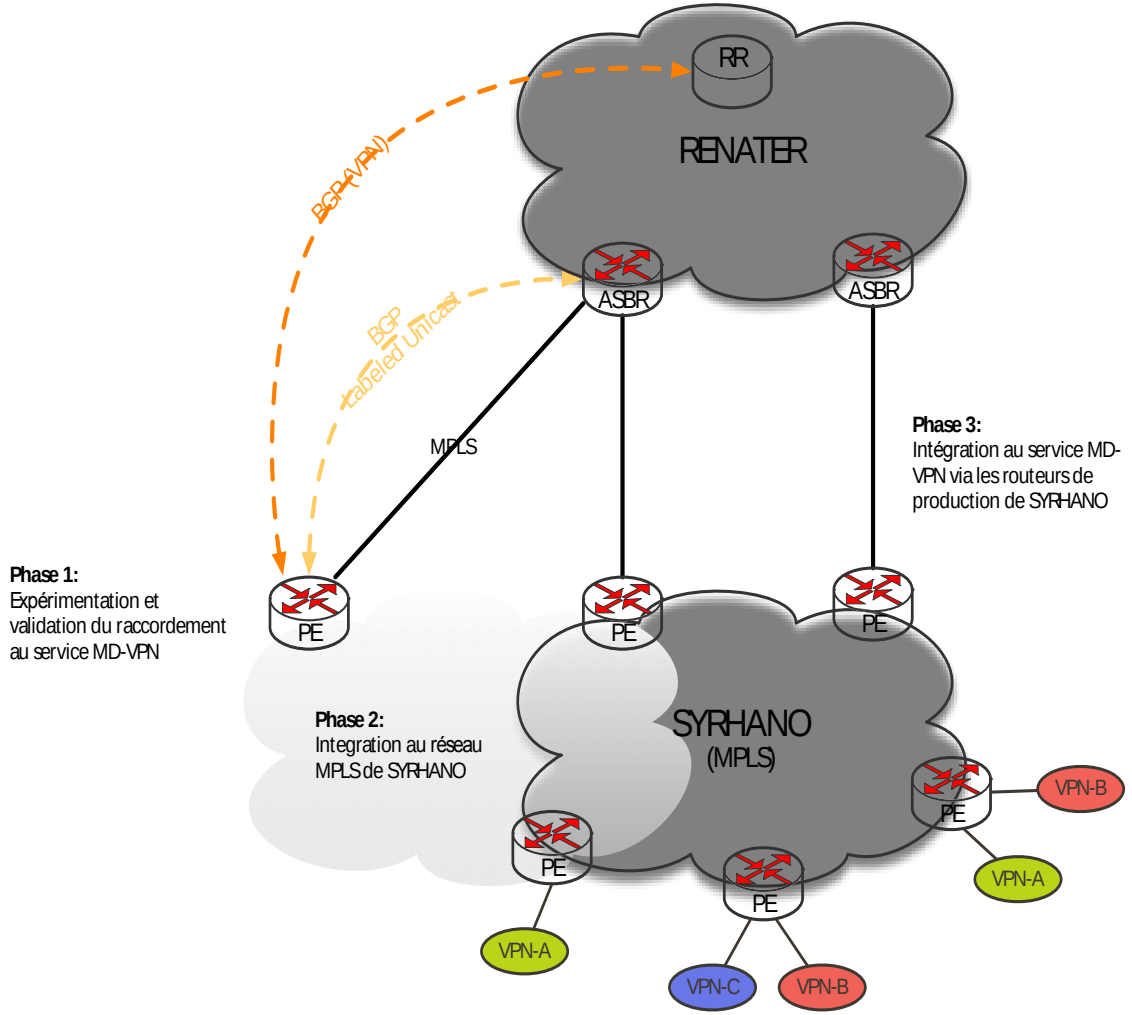


- **SYRHANO**
  - Research and Education network for the region Haute-Normandie
  - 10Gbs backbone infrastructure on dark fiber and operator lease lines
  - 50 organisations representing more than 600 sites connected to the network
- **SYRHANO network architecture**
  - Full MPLS network since 2000
  - L3VPN and L2VPN services over MPLS
    - High usage of L3VPN services (more than 35 VPN) and some of them are extended through RENATER (using back to back only)



MD-VPN deployment for SYRHANO

- **First step :** connecting to the testbed
  - Use of spare router for a local testbed
  - Validation of configuration and service management
- **Second step :** pre-production service
  - Integration of the test router in our production MPLS network
  - Pre-production service for beta users
- **Third step :** production service
  - Implementation of MD-VPN service on production router
  - Full Redundancy with a second LU-BGP connection



Reliability demonstrated since August 2014

- **Pilot phase :**Service reliability checking during 3 months ✔

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%

://tools.ge

Stat http avail v

A monitored service

RENATE
CONNECTEUR DE SAV

Current Status Dashboard

MD-VPN Status For NRENs

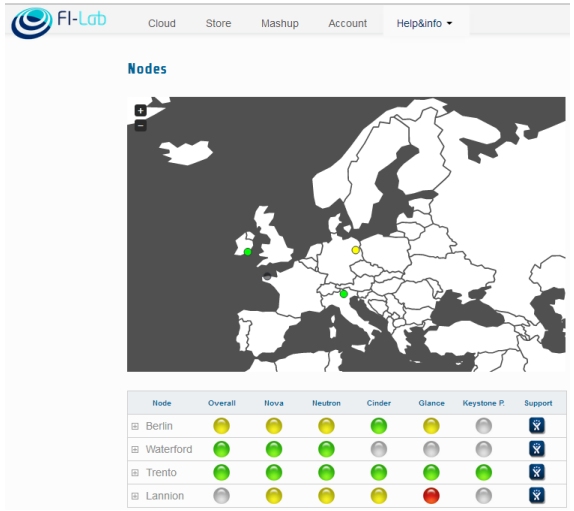
NRENs	Service Component						Service
	BGP-LU Access #1	BGP-LU Access #2	VR Peering #1 Paris	VR Peering #1 Ljubljana	VR Peering #2 Paris	VR Peering #2 Ljubljana	Availability
AMRES	OK	NA	OK	OK	NA	NA	OK
BELnet	OK	NA	OK	OK	OK	OK	OK
BREN	OK	NA	OK	OK	NA	NA	OK
CARnet	OK	NA	OK	OK	NA	NA	OK
CESnet	OK	NA	NA	NA	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
RESTENA	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

://tools.geant.net/portal/links/mdvpn/ms_st

Portal: mdvpn_dashboard.jsp

A scientist project using MD-VPN for production

- **16 sites connected in 12 countries**
- Using all types of connection
  - Direct connection
  - Via VPN-Proxy



http://infographic.lab.fi-ware.org/status

[A first scientist project XiFi]

XIFI is a project of the European Public-Private-Partnership on Future Internet (FI-PPP) programme

OSIRIS deployment
Conclusion

- Implementation of MDVPN quite simple despite of non-MPLS network at the origin
- 30 man-days

- Benefits for Osiris network administrators
  - Study of VPN MPLS technologies
  - Participation to an european innovative project

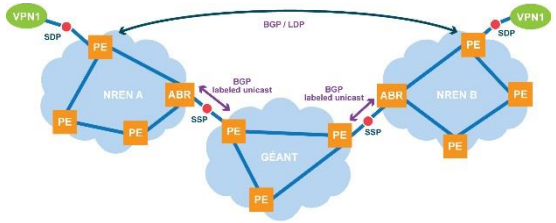
- Benefits for Osiris network
  - No hardware investment : the production equipments make the deal
  - An easier way to implement all sort of VPN with MDVPN
  - A new service for the scientific community in the Osiris catalog of services

SYRHANO deployment Conclusion

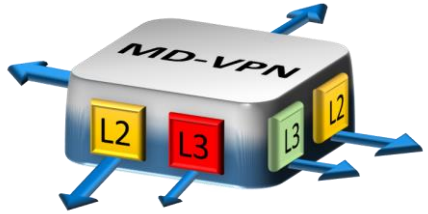
- Deployement was very simple
  - SYRHANO is already using MPLS for his backbone
  - MD-VPN implementation is based on standard protocols
    - no vendor specific implementation needed

- Benefits for SYRHANO users
  - Extension of users VPN over multiple networks
    - what could take weeks or months to extend VPN over multiple networks can be achieved almost instantly

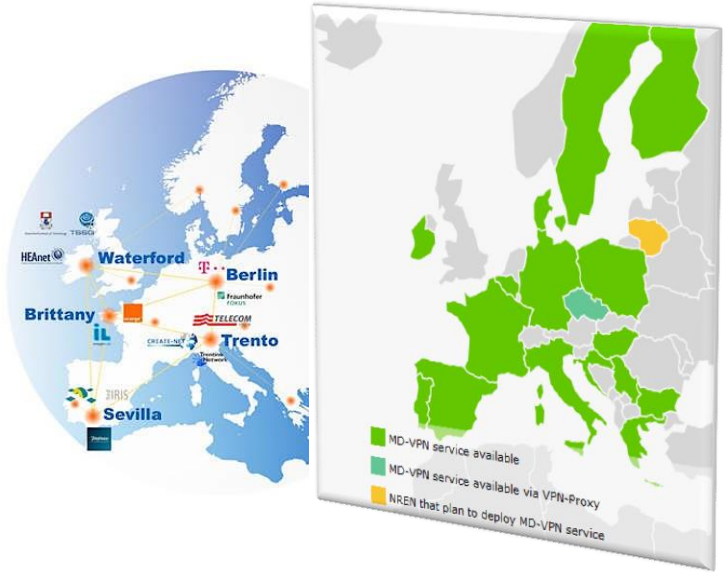
Summary



- **An innovative and highly scalable design**
  - *Seamless transport infrastructure*



- **<u>A bundle of services</u>** (IPv4, IPv6, P2P L2VPN, VPLS, L3VPN) **with added value for our users <u>for regional networks</u>**
- **An original and useful service unavailable in a commercial NSP portfolio**
- **Broad European deployment**
  - **18 connected NRENs**
  - **Roughly 400 PoPs already available**
  - **2 first regional networks in France**



- **Data Center Interconnect: EVPN**