

GN3Plus SA3T3 - Multi Domain VPN - technical architecture

2nd TERENA Network Architects Workshop

(Prague) — 14th Nov. 2013

Xavier Jeannin / RENATER, SA3T3 Task Leader
Tomasz Szewczyk / PSNC, SA3T3 Deputy

- What is Multi-domain VPN (MDVPN)?
- MDVPN architecture components
- Proof of concept
- Reason to deploy MDVPN
- Conclusions

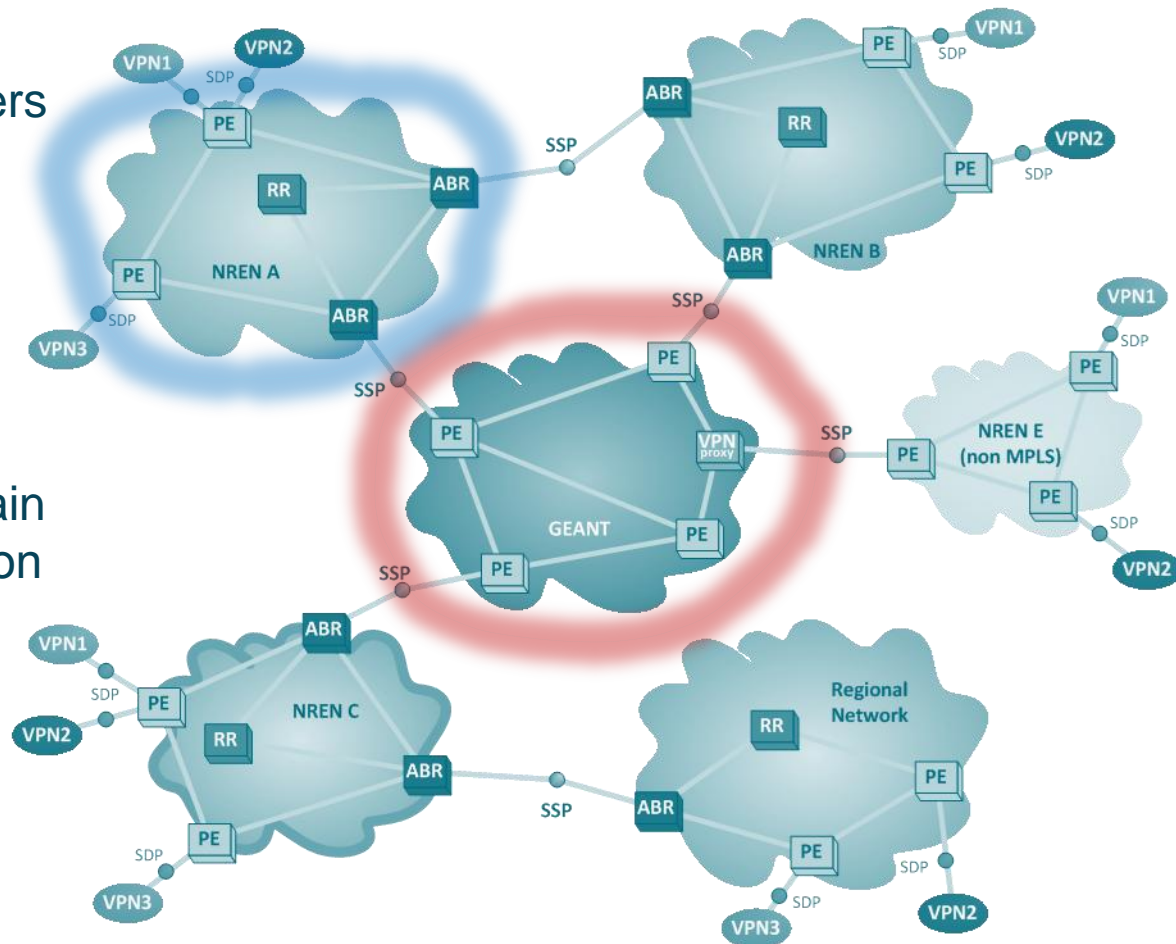


- A **joint service** provided by GEANT and NRENs
- Baseline **transport infrastructure** for many data transmission services
 - “Umbrella” for VPNs
 - L3 or L2 VPNs spanned over several domains only by configuring the edge routers
 - Point-to-point and multipoint topologies
 - High scalability
 - *Total number of provisioned VPNs has no impact on GEANT and NREN core*
- Based on MPLS and BGP protocols
 - RFC 4364 (BGP/MPLS IP VPNs)
 - RFC 3107 (BGP Labeled Unicast)
- Well known and proven technology
 - Available in almost all box and right now
 - No material investment only configuration

MDVPN service overview



- Hierarchical Multi-domain infrastructure
 - GEANT - Carrier of Carriers
 - NRENs – peers
 - Ready to cooperate with non-MPLS domains and regional/metro networks
- Bandwidth management
 - Independent traffic engineering in each domain
 - BGP based “path” selection

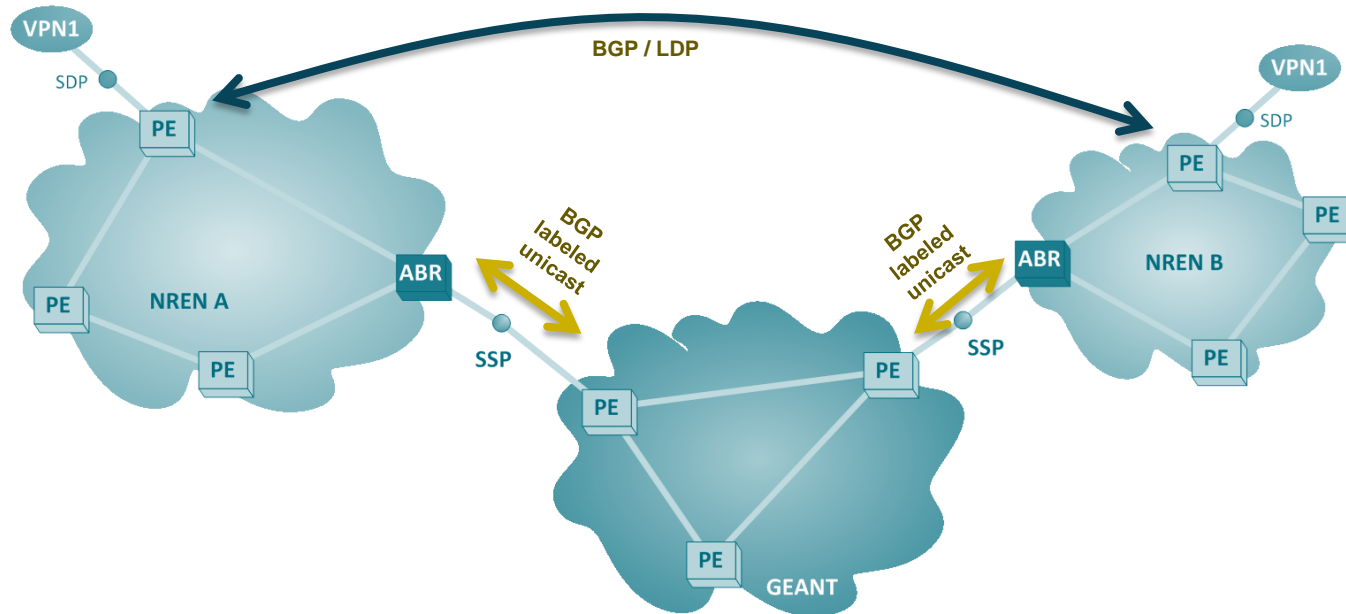


- VPN provider (NRENs)
- VPN transport provider (GEANT)

MDVPN technical principle overview

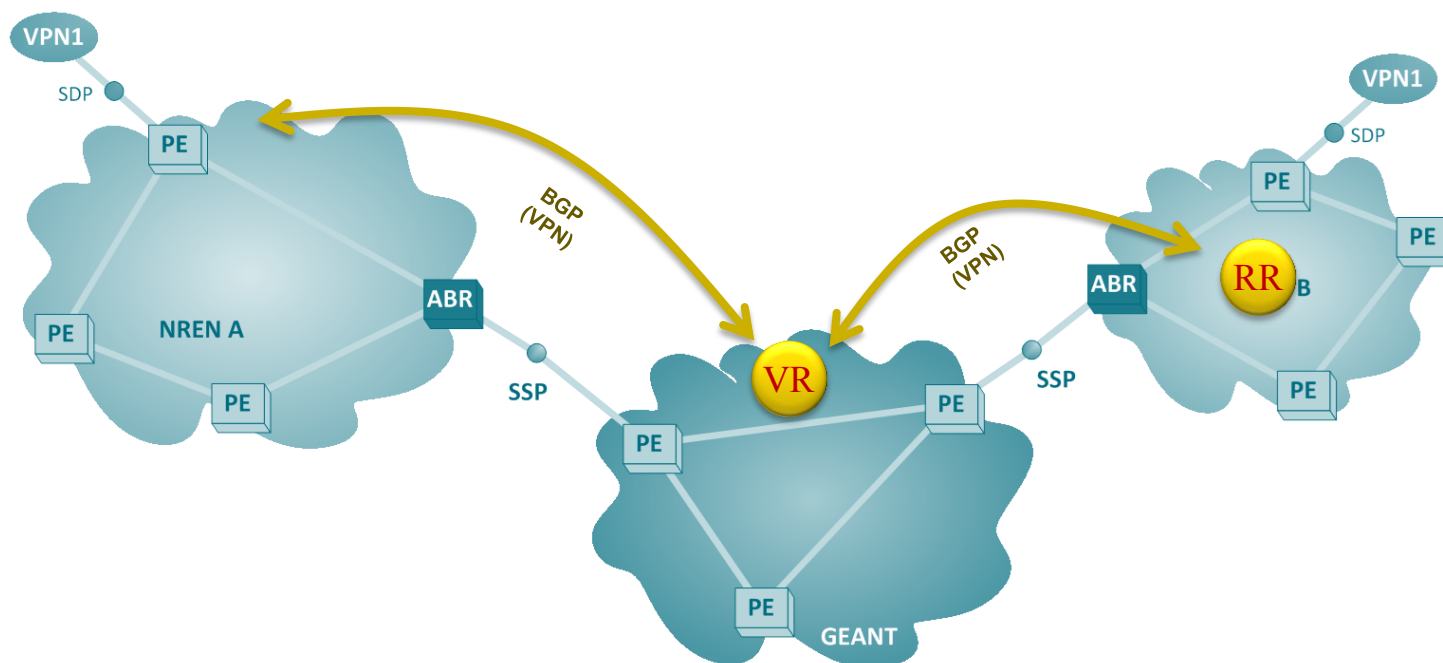


- **Underlying principle behind this Multi-Domain VPN technology**
 - MPLS transmission path from a PE up to the remote PE in another domain
 - *MDVPN design supports non-MPLS domains as well*
 - Signaling is split in 2 parts
 - *Transmission path between PE routers*
 - BGP (labelled unicast SAFI)
 - Loopback prefixes (/32 only)
 - *Labels for VPN prefixes exchange between PE routers*
 - BGP or LDP



MDVPN technical principle overview

- **VPN Route Reflector (VR)**
 - Extended scalability and flexibility
 - Easy implementation

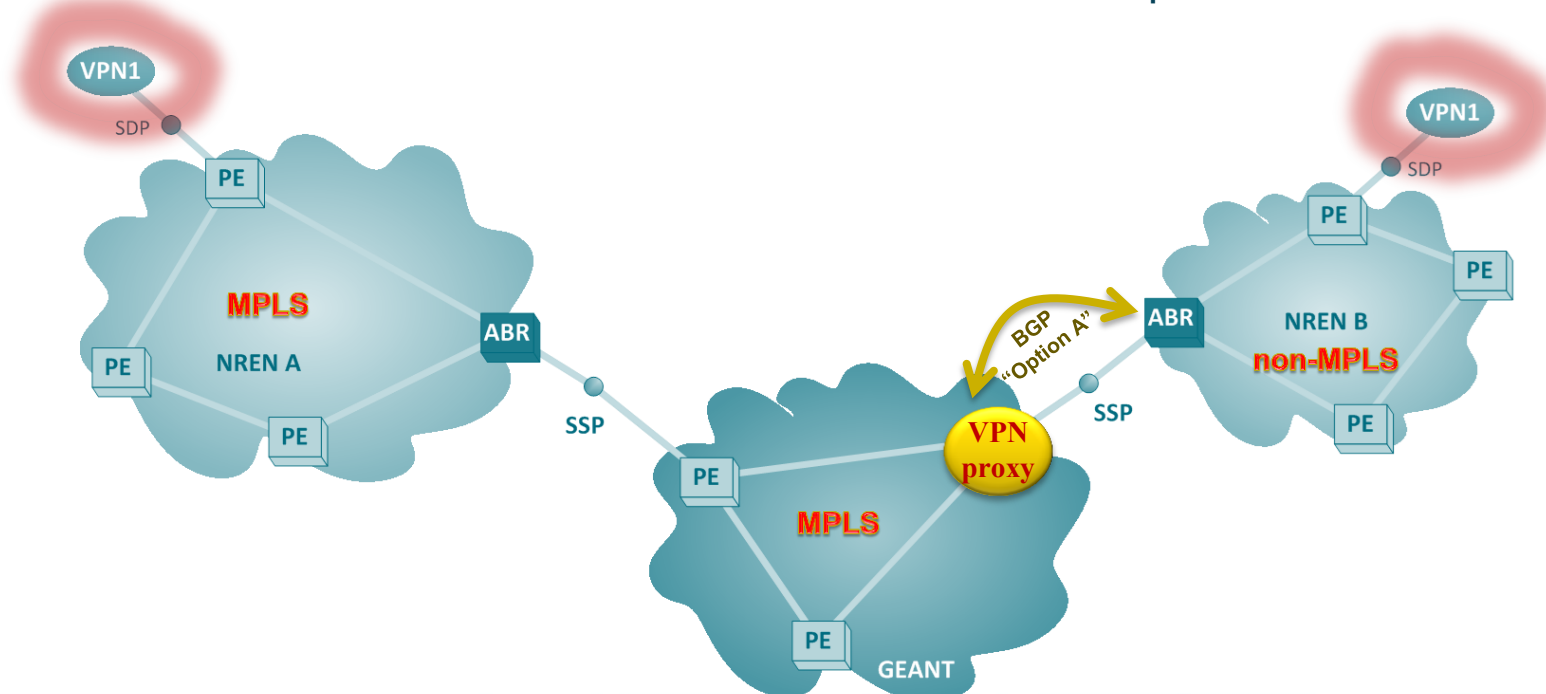


MDVPN technical principle overview



● VPN Proxy

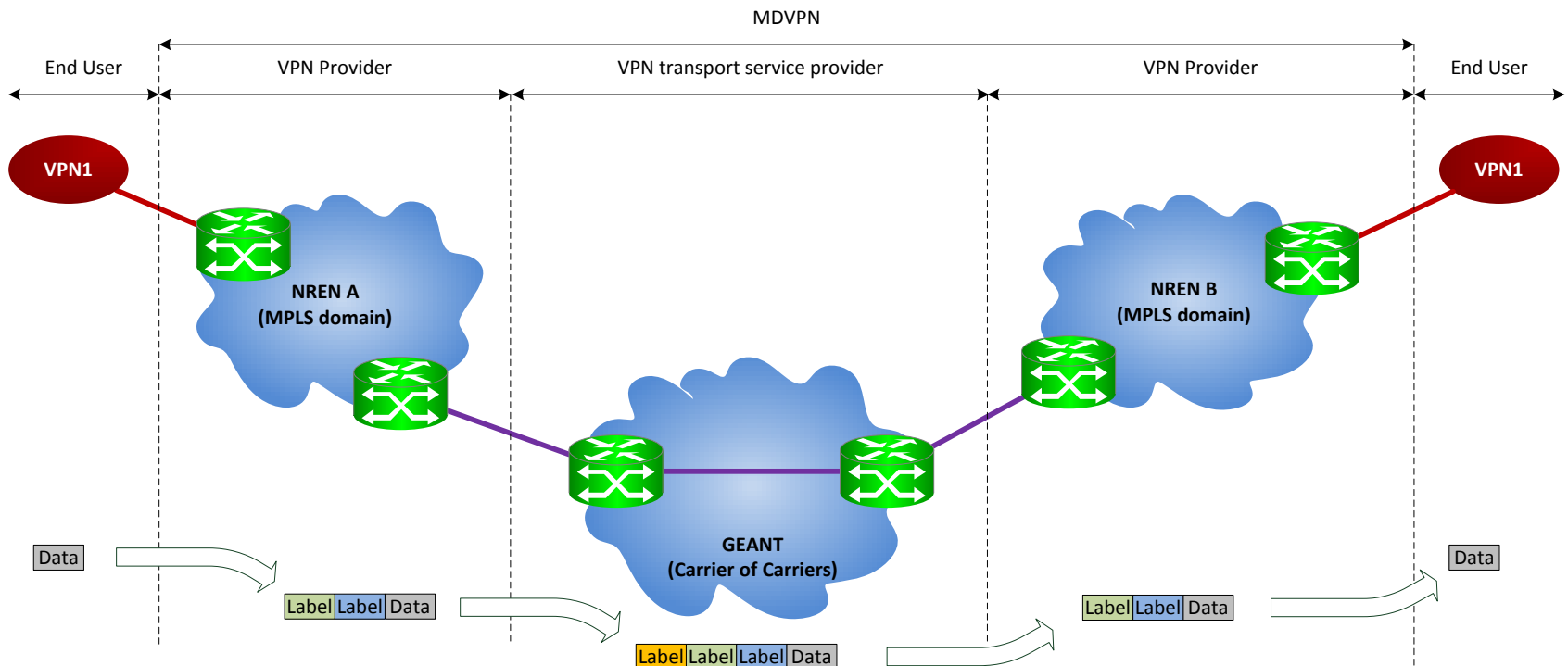
- Interoperability with non-MPLS domains (NRENs)
 - *Route/prefix information exchange through BGP session (Option A)*
 - *Data exchange through physical or logical interface*
- Not “visible” for end user
 - *End users located in non-MPLS domain are getting access to the same set of VPN services which are available for other end users*
- Enables collaboration with networks outside Europe and GEANT service area



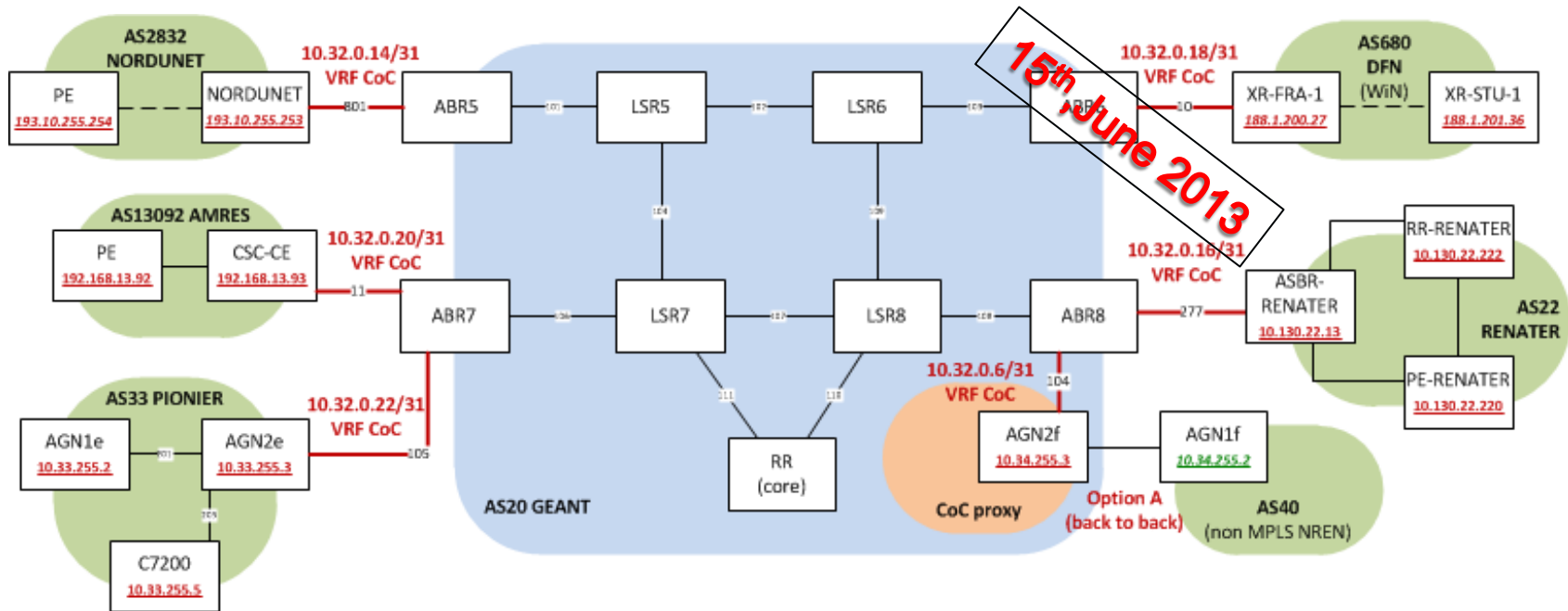
MDVPN traffic flow



- Transparent transport technology
- Scalability in the core
 - Label hierarchy and...
 - No MAC learning and/or prefixes for end user traffic
 - No VLAN ID negotiations between NRENs and GEANT



Proof of concept



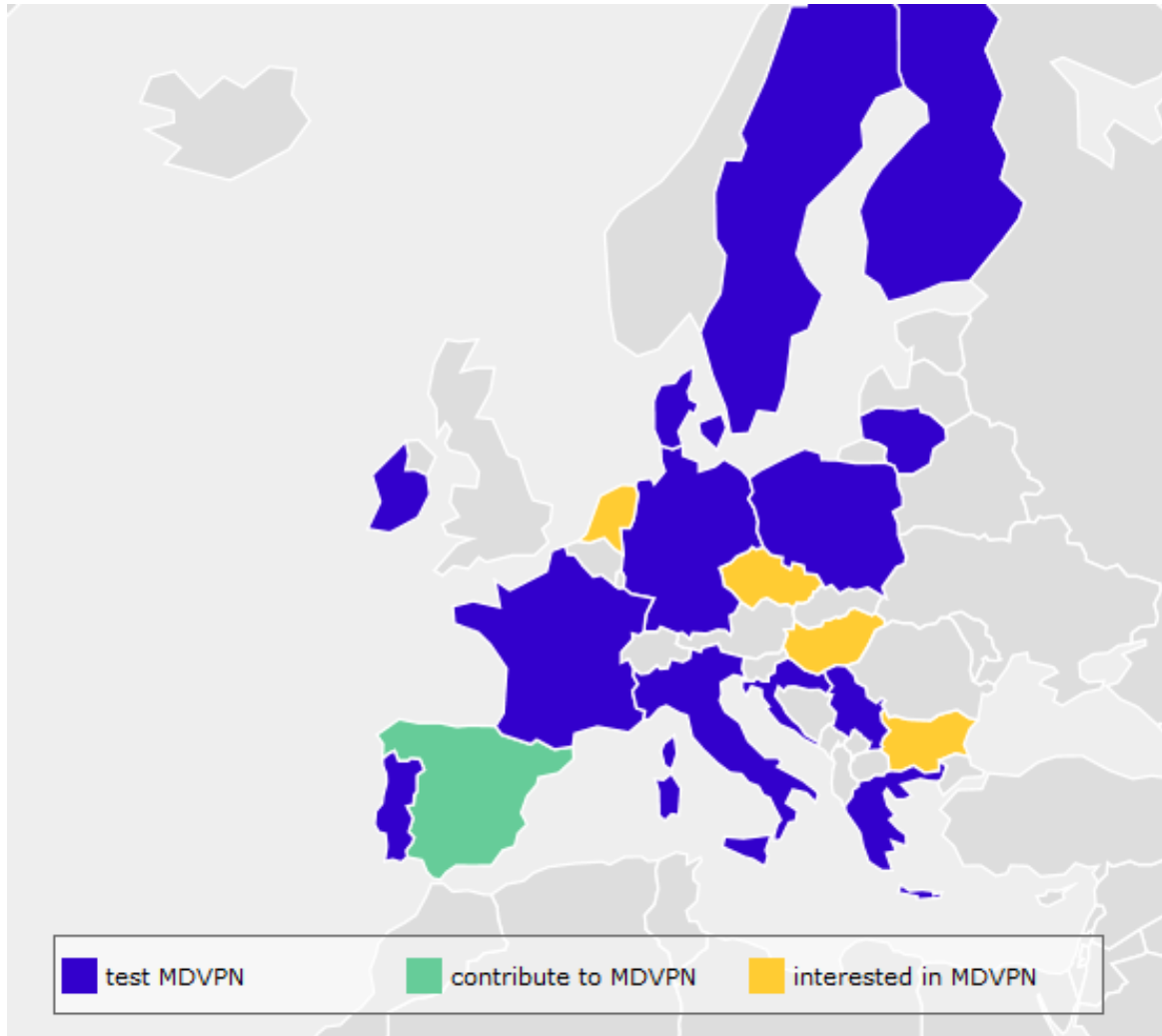
15th June 2013

- Multidomain infrastructure
 - Carrier of Carrier infrastructure emulated in the lab
 - VPN Route Reflector
 - VPN proxy
 - NREN's labs connected
- Multi-domain VPNs
 - MP L3VPN, P2P L2VPN
- Some monitoring functionalities tested/presented

SA3T3 work: MDVPN service



- Very positive feedback from NRENs
- Service specification already published
 - D7.1 (DS3.3.1): MDVPN Service Architecture



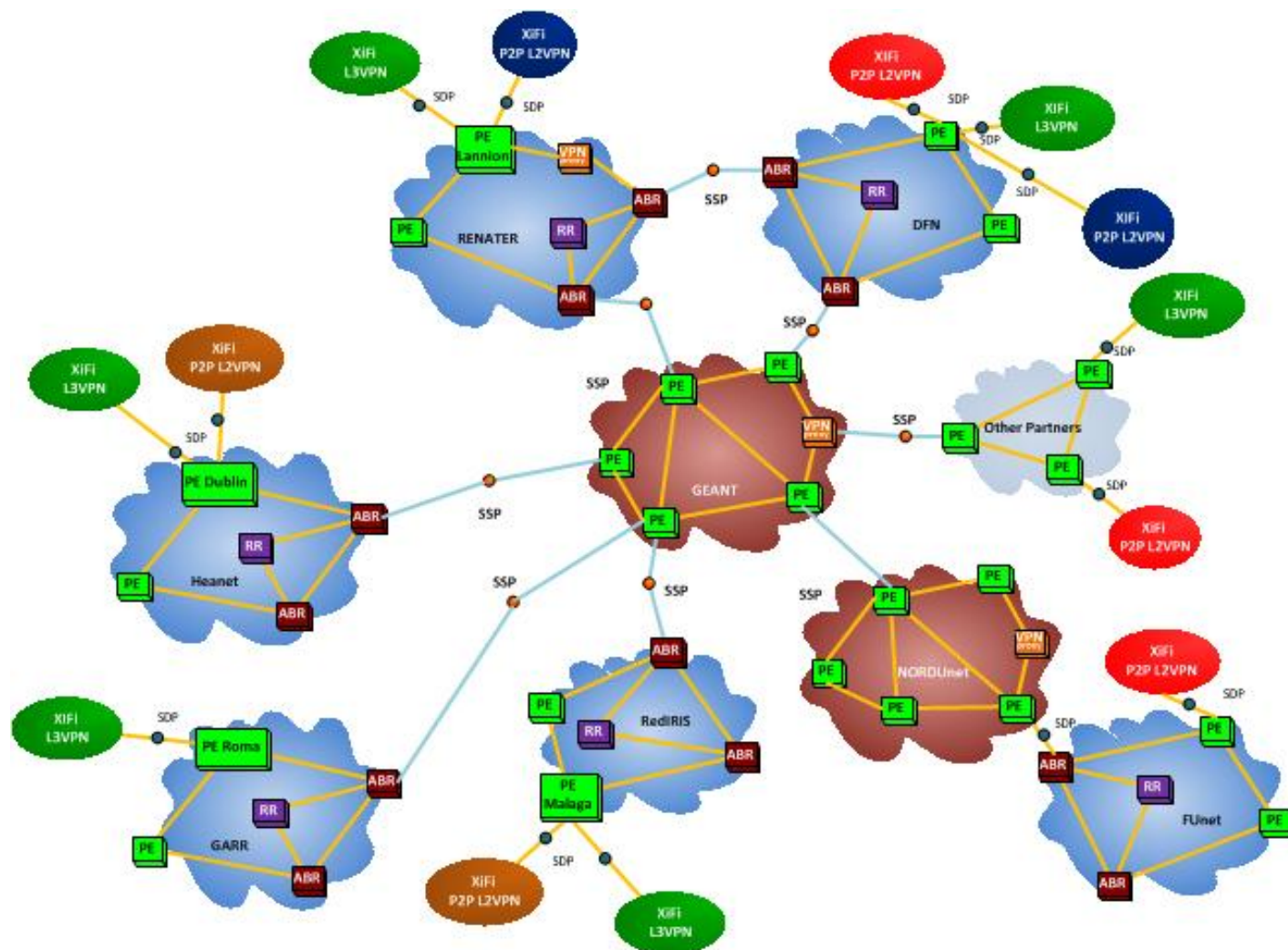
http://www.geant.net/Resources/Deliverables/Documents/D7.1_DS%203%203%201-MDVPN-service-architecture.pdf

Reason to deploy MDVPN



- A set of services useful for end users
 - Cover a wide scope of user needs
 - *Long-term infrastructure with intensive network usage*
 - *Quick point-to-point for a conference demonstration*
 - A End-to-End services
 - *European and Worldwide scope*
 - Rapid to deploy
 - *VPN provisioning only on PE routers*
 - Flexibility
 - *Ready to meet user needs*
- Unique service
 - Offered jointly by GEANT and NRENs
 - *Not provided by commercial telecoms*
 - An innovative service and a scale deployment never seen
 - Interoperable with other services (like BoD or network virtualization)
 - Ability to deliver the service directly to “the desk”
 - *Small CE devices + simple configuration*

Example Use case: XiFi project



- A seamless infrastructure at European level for delivering VPN services to end users
 - *Useful service for science and education*
 - *An original network service*
- Based on stable and scalable technology
 - *MPLS transport*
 - *RFC based BGP/LDP signaling*
- OPEX cost reduction for NREN and DANTE
 - *Easy and fast provisioning (less maintenance overhead)*



Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv

