Multi-Domain Virtual Private Network service
une infrastructure sans couture pour les réseaux régionaux et les NREN

Xavier JEANNIN
RENATER

Sébastien Boggia
OSIRIS
Université de Strasbourg - Direction informatique

Jean Benoit
OSIRIS
Université de Strasbourg - Direction informatique

Benjamin Collet
OSIRIS
Université de Strasbourg - Direction informatique

Christophe PALANCHE
OSIRIS
Université de Strasbourg - Direction informatique

Alain Bidaud
SYRHANO - CRIHAN

Résumé

Les opérateurs réseau de l'enseignement et de la recherche proposent des services de VPN de niveau 2 et 3. Ces derniers sont délicats à mettre en œuvre lorsque le service doit s'étendre au-delà d'un réseau régional ou national (NREN). C'est le type de problème que résout le nouveau service réseau Multi-domain Virtual Private Network (MD-VPN).

MD-VPN est une infrastructure multi-domaine « sans couture » capable de délivrer un bouquet de services réseau : L3VPN (IPv4, IPv6), L2VPN point-à-point et multipoint.

MD-VPN est un service très flexible, il permet de délivrer les VPNs rapidement ; seule une configuration locale aux extrémités est nécessaire (dans le réseau régional), aucune configuration n'étant nécessaire dans les réseaux traversés (RENATER, GEANT, autres NRENs).

Au 1er mars 2015, MD-VPN est déployé dans 16 pays en Europe. Cela représente déjà de formidables possibilités de connexion entre 457 points d'accès en Europe potentiellement pour les projets de nos usagers. De plus, dans le cas où le service n'est pas disponible localement, il est toujours possible de se raccorder via un VPN-Proxy.

MD-VPN est un très bon outil pour le développement des réseaux régionaux français, OSIRIS et SYRHANO étant pionniers en la matière (Instituts disséminés en France, mutualisation de grands équipements, grilles de calcul, cloud ...). Les VPNs internationaux visent à supporter informatiquement des collaborations internationales qui sont maintenant très fréquentes dans le monde scientifique.

Basé sur des standards et des technologies éprouvés (RFC 4364, 3107), MD-VPN est supporté sur beaucoup de routeurs. Son déploiement n'engendre aucun coût d'investissement et les coûts d'exploitation sont pour leur part significativement réduits.

Mots-clefs

Connecter les communautés, MPLS, VPN, Carrier-of-Carriers, Labeled Unicast, BGP

1 Qu'est-ce que le service Multi Domain Virtual Private Network (MD-VPN)?

Le service MD-VPN est un service réseau déployé sur GEANT, NORDUnet, RENATER et 15 autres NREN. MD-VPN est en fait une nouvelle infrastructure sans-couture multi domaines capable de transporter et délivrer un ensemble de services qui fonctionnent entre plusieurs NREN ou réseaux régionaux : VPN de niveau 3 (IPv4, IPv6), VPN point à point de niveau 2 (Martini et Kompella) et VPN multipoint de niveau 2 (VPLS).

On peut distinguer deux usages pour les VPNs multi-domaines :

- Relier plusieurs sites, d'une même compagnie (un institut de recherche, etc.), distants les uns des autres de telle manière que les sites apparaissent pour les utilisateurs comme s'ils étaient interconnectés physiquement. On fournit ainsi le même niveau de sécurité à l'utilisateur que si les sites étaient localement raccordés. Les VPN multi-domaines nationaux (inter-régions) entrent dans cette catégorie ;
- Collaboration entre deux entités différentes autour d'un projet scientifique ou de mise en commun d'une infrastructure : cloud, grille de calcul, HPC, télescope, etc. MD-VPN a pour but d'aider à la mise en place de la collaboration inter-régionale et internationale. Les VPN internationaux et nationaux entrent dans cette catégorie.

MD-VPN est en fait un service de connectivité et donc un service réseau bas niveau qui peut être utile à un grand nombre d'applications. Par exemple, au-dessus d'un VPN multipoint de niveau 2 fourni par MD-VPN, on peut développer de nouveaux paradigmes (Software Defined Network), de nouveaux services ou protocoles.

MD-VPN étant très flexible et délivrant les VPN aux utilisateurs très rapidement, il y a ainsi une grand diversité d'usages possibles : depuis une infrastructure VPN pérenne avec usage intensif du réseau jusqu'à des VPN point à point mis en place pour une démonstration de courte durée. MD-VPN est un service innovant, il a été rapidement adopté par les NREN parce qu'il est plus simple à mettre en œuvre et moins onéreux que les services de connexion équivalents :

- MD-VPN est basé sur des standards éprouvés (BGP/MPLS IP VPNs - RFC 4364, Carrying Label Information in BGP-4 RFC 3701). MD-VPN ne nécessite pas d'installation de matériels supplémentaires (CAPEX) ;
- MD-VPN utilise seulement un échange de label MPLS entre les domaines (entre les opérateurs réseau) (MPLS n'est pas obligatoire à l'intérieur du domaine) et 2 sessions BGP ;
- MD-VPN réduit les couts d'exploitation (OPEX) car MD-VPN ne nécessite aucune opération entre les opérateurs comme les anciennes solutions.

Dès qu'un réseau régional établit ces 2 sessions BGP, le réseau régional peut offrir à tous ses utilisateurs la possibilité de créer des VPNs à travers toute l'infrastructure présente, soit aujourd'hui 16 NREN en Europe, GEANT et NORDUnet. Enfin ce service permet de délivrer aux utilisateurs ses services à un cout réduit.

Etat du déploiement

MD-VPN est désormais en production au niveau de GEANT à l'issue **du projet end GN3+ en avril 2015**. Cela veut dire que le service MD-VPN est supervisé et fait partie du rapport mensuel des services de GEANT (cf. ci-dessous).

18 NREN sont connectés : AMRES, BELnet, BREN, CARNet, DeiC, DFN, FUnet, FCCN, GARR, GÉANT, GRNET, HEAnet, HUNGARnet, NORDUnet , PSNC, RENATER, RedIRIS, SUnet.

L'infrastructure européenne représente 400 points de présence (PoP) MD-VPN en Europe dans lesquels les VPN peuvent être délivrés.

En France, au niveau des réseaux de collecte régionaux, OSIRIS est connecté au service et SYRHANO est en cours de connexion.

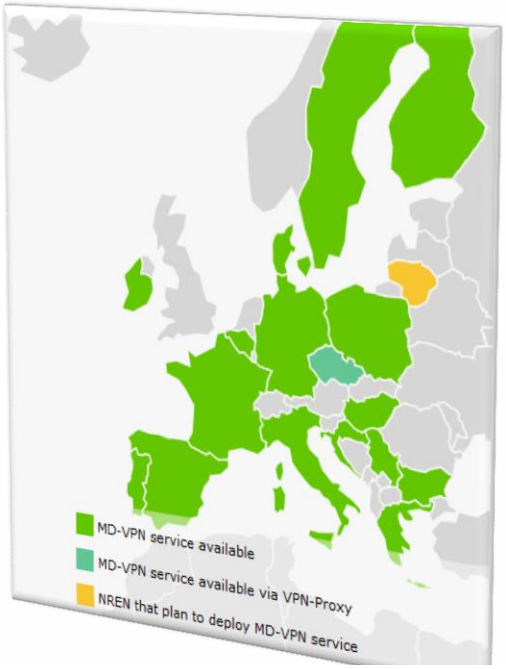

Figure 1: MD-VPN déploiement

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
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

Supervision

Disponibilité instantané du service MD-VPN

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%

Rapport mensuel du service MD-VPN

Monthly Service Report

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

Table 1: GEANT monitoring portal

Le projet européen scientifique XiFi (https://www.fi-xifi.eu/home.html) utilise MD-VPN pour interconnecter 16 sites situés dans 12 pays afin de créer un environnement de recherche distribué. Le L3VPN pour le projet XiFi a été déployé entièrement grâce à MD-VPN dans l'ensemble des sites en septembre 2014. Pendant le déploiement du L3VPN XiFi, MD-VPN a démontré son extrême flexibilité en interconnectant des sites dans des pays où MD-VPN n'était pas déployé. Ceci est possible grâce la technologie VPN-Proxy. Enfin, la fiabilité du L3VPN fourni au travers du service MD-VPN a été démontrée, aucun incident n'ayant été signalé jusqu'à présent.

2 Cas d'utilisation

MD-VPN est un service de connectivité de bas niveau sur lequel il est possible de construire différents services et infrastructures. Comme le service MD-VPN permet de fournir des VPN étendus en un temps très court il peut servir dans de nombreux cas d'usage :

- Tout projet scientifique basé sur des collaborations internationales :
  - LHCONE est un exemple de L3VPN multi-domaines existant. Même si LHCONE utilise une autre technologie, ceci démontre bien l'intérêt des VPN multi-domaines pour la science. Un premier circuit point à point (P2P) entre un Tier2 situé à Poznan et un Tier1 situé à Karlsruhe est maintenant fourni pour le LHCONE au travers du service MD-VPN ;
  - ITER, CONFINE, Visionair et d'autres projets internationaux sont de bons candidats pour MD-VPN. Le projet XiFi est un exemple de travaux scientifiques utilisant MD-VPN.

Figure 2 : XiFi, infrastructure de test fourni par MD-VPN
https://www.fi-xifi.eu/home.html

- Connexion de sites de la même organisation en particulier entre plusieurs régions françaises :
  - Universités, grands instituts scientifiques, …
  - Aide à la fusion des régions
- Infrastructures distribuées :
  - Fournisseur de service de type cloud, grilles et centres de calcul intensif (HPC), infrastructure scientifique : télescope, réseaux de capteurs ;
- Connexion rapide point-à-point :
  - Pour le transport entre 2 sites grâce à un P2P ;
  - Pour une démonstration lors d'une conférence. Par exemple ci-contre : un circuit P2P L2VPN monté en 1 journée entre Poznan (Pologne) et la Croatie pour une démonstration à la conférence Users Conference CUC 2014[1] ;

Figure 3 : UHD démonstration grâce à MD-VPN

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

- Education :
  - Cours à distance, E-learning
- Art et education
    - Support de l'innovation :
- Recherche sur les technologies informatiques, réseaux et de stockage ;
- Nouveaux usages dans le domaine de l'éducation et la recherche ;
- Projets nécessitants un certain niveau de sécurité ;
- Protection d'un service en production :
  - Lorsqu'un service devient populaire, il est sujet à des attaques. Placer ce service dans un VPN permet de contrôler les accès à ce service. Par exemple un service de vidéo de RENATER comme Rendez-Vous peut utiliser un VPN pour la gestion des éléments techniques internes qui rendent le service (Jitsi Meet, Jicof, video-bridges), c'est à dire pour la gestion de son backoffice (ce que l'on nomme l'out-of-band management). Mais il est également possible d'utiliser un VPN pour la partie application (partie in-band) qui délivre le service aux utilisateurs (VPN nommé « application VPN » dans le schéma ci-dessous). Les utilisateurs et leur opérateur n'ont pas besoin de configurations particulières. Les opérateurs accèdent de manière transparente au VPN. On peut ainsi séparer les différents accès au service :
    - 1 accès pour GEANT ;
    - 1 accès pour chacun des NREN (RENATER, Belnet, etc.) ;
    - 1 accès pour les utilisateurs de l'Internet.

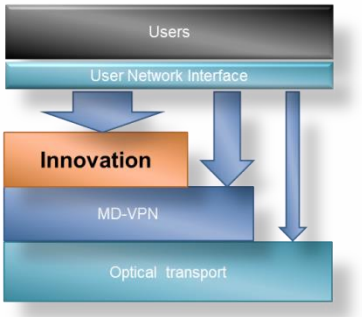

Figure 4 : MD-VPN base pour l'innovation

Grâce à cette architecture, si une attaque survient en provenance de l'internet ou d'un NREN, il est très simple d'isoler le service Rendez-Vous de la source de l'attaque et de protéger ainsi le service, tout en permettant aux utilisateurs de la communauté éducation et recherche de continuer àbénéficier du service.

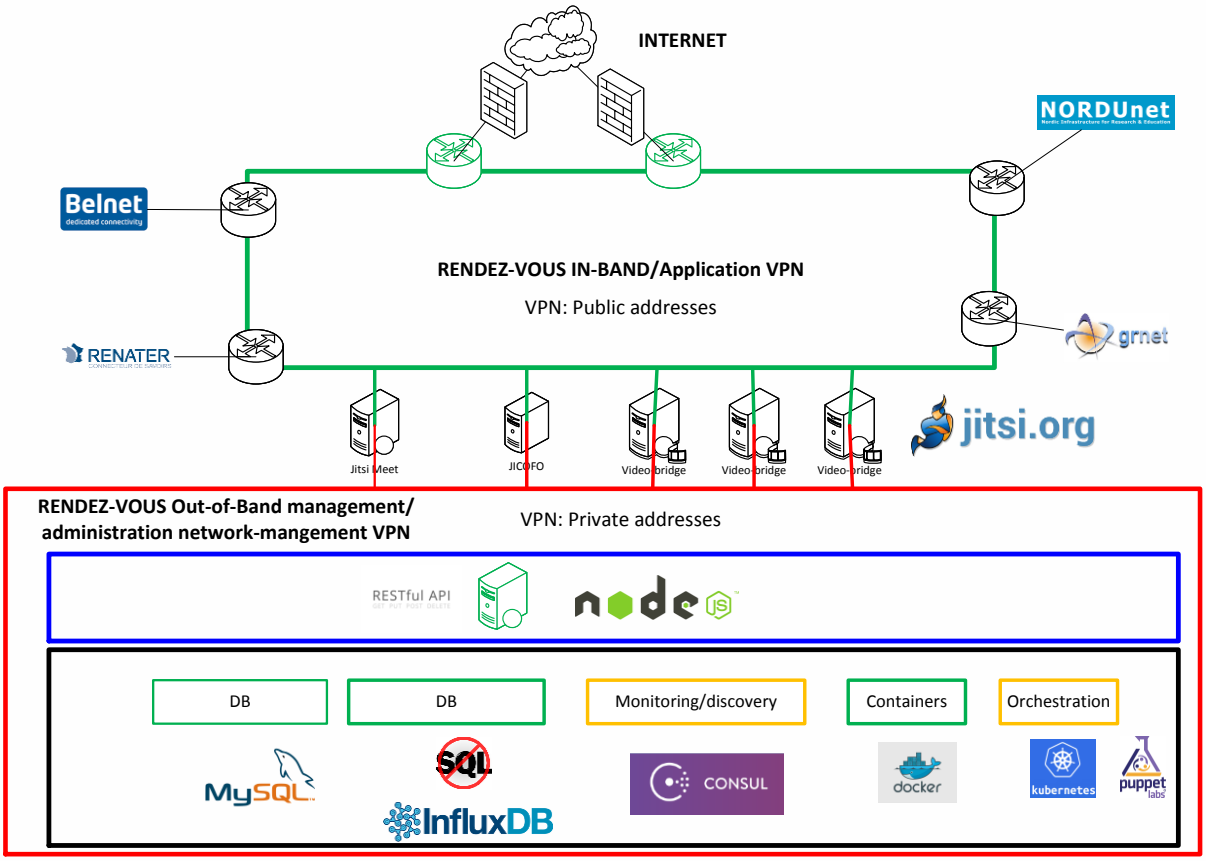

Figure 5 : utilisation de MD-VPN pour sécuriser le service vidéo Rendez-vous

3 Ingénierie des VPN MPLS multi-domaines

MD-VPN utilise les mêmes principes que ceux des VPN MPLS conventionnels. Le VPN est établi grâce à l'établissement d'un Label Switch Path (LSP) entre les deux routeurs qui relient les deux sites utilisateurs. Les paquets d'un VPN MPLS se voient ajouter 2 labels lors de leur entrée dans le backbone. Le premier label (top label) est appelé « PE (Provider Edge) label » ou « Egress PE label » et le second label est nommé « VPN label » ou « Service label ». Dans un VPN MPLS conventionnel, le PE label est distribué via LDP ou RSVP et le Service label est pour sa part distribué via BGP grâce aux familles BGP (VPNv4, VPNv6, L2VPN, auto-discovery-only).

Pour un VPN multi-domaine, l'utilisation des protocoles LDP ou RSVP est impossible pour des raisons de passage à l'échelle, de sécurité et d'indépendance des différents opérateurs. C'est donc grâce à BGP que s'effectue l'échange des adresses des PE ainsi que des PE labels entre les différents domaines (NREN, Réseau Régional). Cette technique "inter-AS VPN" est appelée "option C" dans le RFC 4364.

L'échange des Service label suit la même procédure que dans une configuration mono-domaine à savoir que les Service label sont échangés via BGP.

L'architecture et la technologie utilisée permet un passage à l'échelle européenne (cf ci-dessous). Déployé dans son mode standard, MD-VPN permet le même niveau de redondance qu'en mono-domaine.

3.1 Provider Edge et distribution multi-domaines des labels

La signalisation est séparée en 2 parties :

- Transmission du chemin entre 2 routeurs PE :

- BGP (labelled unicast SAFI) permet l'échange de routes labellisées de PE (PE label) entre PE qui délivreront les VPN aux utilisateurs ;
- Pour cela, les opérateurs (NREN ou un réseau régional) doivent établir entre eux une session BGP et cela une seule fois, on nomme ce point d'échange « Service Stitching Point » (SSP); Dès lors tous les LSPs et tous les VPN sont multiplexés sur ce SSP ;

- Echange des labels de VPN et préfixes utilisateurs entre routeurs PE :
  - Selon le type de VPN (L3VPN, P2P L2VPN martini, P2P L2VPN Kompella, VPLS sur LDP ou sur BGP), BGP ou LDP sont utilisés pour l'échange des VPN labels entre PE.

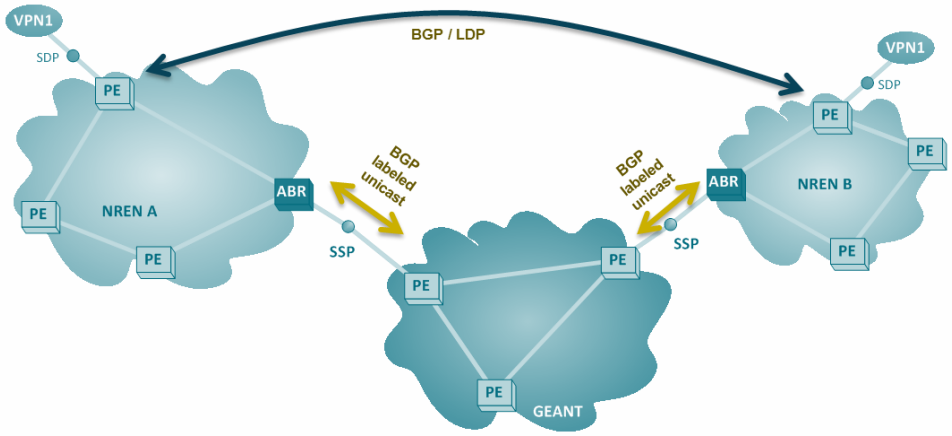

Figure 6 : Signalisation MD-VPN

3.2 VPN Route Reflector

Comme expliqué plus haut, l'échange des Service labels suit la même procédure que dans une configuration mono-domaine, à savoir que les Service labels sont échangés via BGP. Ceci nécessiterait la mise en place d'une session BGP entre chaque domaine. Afin de réduire le nombre de sessions d'échange (de l'ordre du carré du nombre de domaines), 2 « VPN route reflector » ont été installés sur GEANT, réduisant ce nombre de sessions à 2 fois le nombre de NREN. Il n'est donc plus nécessaire d'avoir de sessions BGP directes entre NREN. RENATER fera la même opération à l'échelle nationale pour les réseaux régionaux.

Le VPN route reflector échange via une session BGP multi-hop entre le route reflector du NREN ou le routeur PE du NREN (de même entre les réseaux régionaux et RENATER). Les SAFI (VPNv4, VPNv6, L2VPN, auto-discovery-only) sont échangées et le VPN route reflector est configuré pour accepter toutes les routes VPN.

Pour augmenter la fiabilité de ce point crucial, 2 VPN route reflectors ont été déployés et les NREN peuvent de leur côté déployer plusieurs route reflectors.

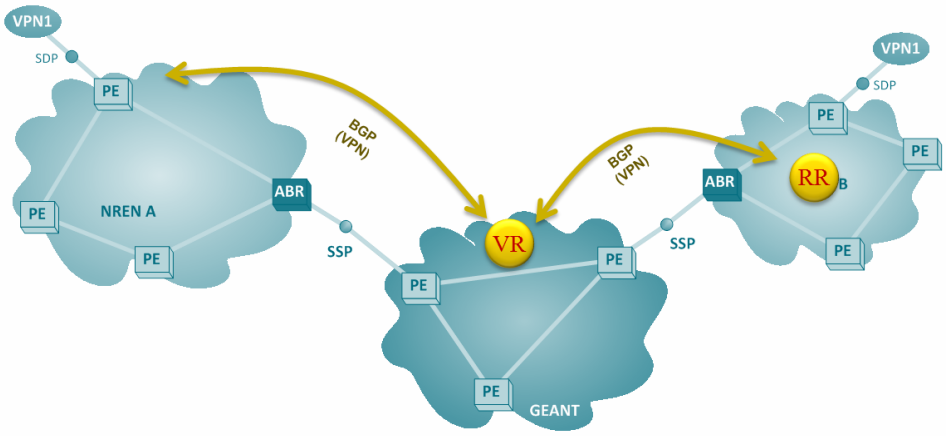

Figure 7 : VPN Route Reflector

3.3 Carrier of Carrier/Carrier Supporting Carrier (CsC)

Les 2 réseaux pan-européens (GEANT and NORDUnet) ont choisi d'encapsuler les VPN MPLS du service MD-VPN dans un L3VPN interne. Cette technologie est appelée « Carrier of Carrier » (CsC) ou « Carrier supporting Carrier for hierarchical VPNs ». Elle permet à un opérateur (un « carrier ») de transporter les VPN d'un autre opérateur de manière transparente. Ce qui est original dans MD-VPN par rapport à un CsC conventionnel, c'est que le VPN est transporté entre 2 opérateurs différents qui n'ont pas le même AS. Ce choix a été motivé par le fait que les 2 réseaux pan-européens (GEANT et NORDUnet) ne délivrent pas les VPN directement à des utilisateurs finaux, mais se consacrent uniquement au transport des VPN pour les NREN. Isoler le service MD-VPN dans une VRF a des avantages pour un opérateur, il peut ainsi facilement superviser globalement le service. D'un point de vue technique, cette technologie entraine l'utilisation d'un troisième label quand les paquets transitent par GEANT ou NORDUnet.

3.4 Comment interconnecter un site "non MD-VPN" : VPN-proxy

Pour un projet utilisateur, il est crucial d'être certain de pouvoir interconnecter l'ensemble de ses sites au sein d'un VPN. MD-VPN est capable de connecter tous types de sites. Il est recommandé aux NREN de supporter MD-VPN, mais si cela n'est pas possible, la technologie VPN-Proxy fourni par GEANT permet d'étendre un VPN jusqu'à un NREN qui n'implémente pas le service MD-VPN.

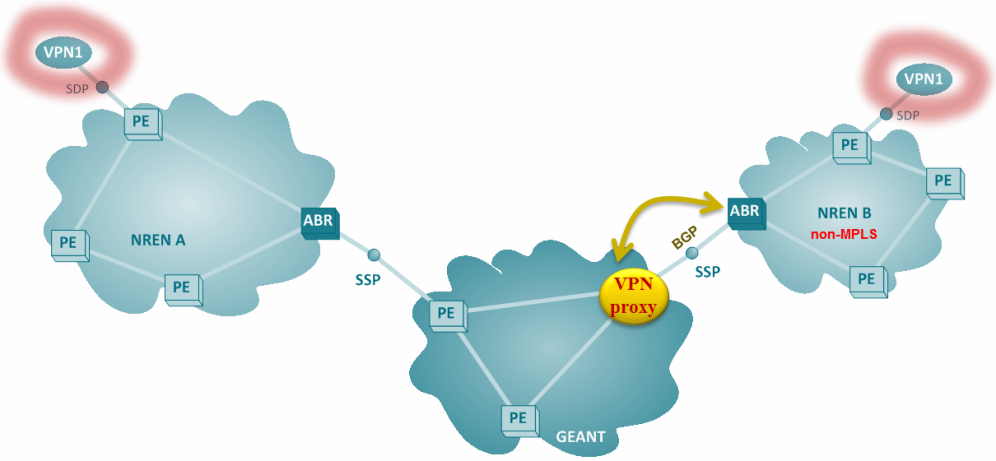

Figure 8 : VPN-Proxy

3.5 Passage à l'échelle

La capacité de passer à l'échelle est un avantage majeur de l'architecture MD-VPN par rapport aux architectures de services existants. MD-VPN a été conçu pour pouvoir fournir des milliers (et plus) d'instances de VPN sans impacter GEANT et le cœur de réseau des NREN.

Ces performances peuvent être atteintes grâce à la séparation entre le transport des données dans le cœur du réseau et les services (de type VPN) fournis en bordure. Dans le cœur, seul les labels ainsi que l'adressage des routeurs PE sont maintenus. A l'heure actuelle pour le service MD-VPN, il y a moins de 1000 entrées de routes pour l'ensemble des NREN. Si on compare avec la taille globale de routes de l'Internet (~500k), il est facile de de noter que MD-VPN a un fort potentiel de croissance. Les services VPN sont maintenus en bordure, sur les routeurs PE. Chaque PE maintient uniquement une liste d'entrées (labels et routes) relatives aux services VPN déployés sur ce PE.

Le nombre de VPN actifs entre les NREN et les réseaux régionaux n'a pas d'impact sur GEANT car les services sont transparents pour GEANT. Il ne doit maintenir que les adresses et labels des routeurs PE

4 Services réseau et extension

Si MD-VPN a été facilement adopté par une très grande majorité des NRENs européens, son succès repose également sur son adoption par les réseaux régionaux organisant la collecte de la majorité des sites clients potentiels.

Cette partie de l'article relate l'expérience d'intégration de MD-VPN des réseaux régionaux SYRHANO et OSIRIS dont les architectures et technologies réseaux sont sensiblement différentes. Dans les deux cas, MD-VPN est intégré sans grandes difficultés et sans investissement matériel.

4.1.1 Réseau Osiris

Le réseau Osiris est le réseau métropolitain de l'enseignement supérieur et de la recherche de l'agglomération strasbourgeoise. Il offre une connectivité 10Gbits en IPv4 et IPv6 pour environ 75000 utilisateurs.

Par l'intermédiaire du réseau régional RAREST, basé sur des liaisons louées, il est prolongé dans les principales villes alsaciennes.

MD-VPN est basé sur la technologie MPLS. L'exemple du réseau Osiris montre qu'il est tout à fait possible de déployer MD-VPN sans disposer à la base de MPLS et sans révolutionner l'architecture réseau, comme nous le verrons ci-dessous.

La figure ci-dessous donne un aperçu de l'architecture actuelle du réseau Osiris.

Deux routeurs de cœur Juniper MX480 redondants l'un de l'autre, disposant chacun d'un peering BGP avec Renater, assurent l'essentiel des fonctionnalités de routage de niveau 3. Un réseau de niveau 2 totalement maillé agrège l'ensemble des sites (110 bâtiments) présents sur les 5 principaux campus Strasbourgeois. Dans chaque bâtiment un CE interconnecte les réseaux des clients au cœur de réseau en niveau 2 ou en niveau 3.

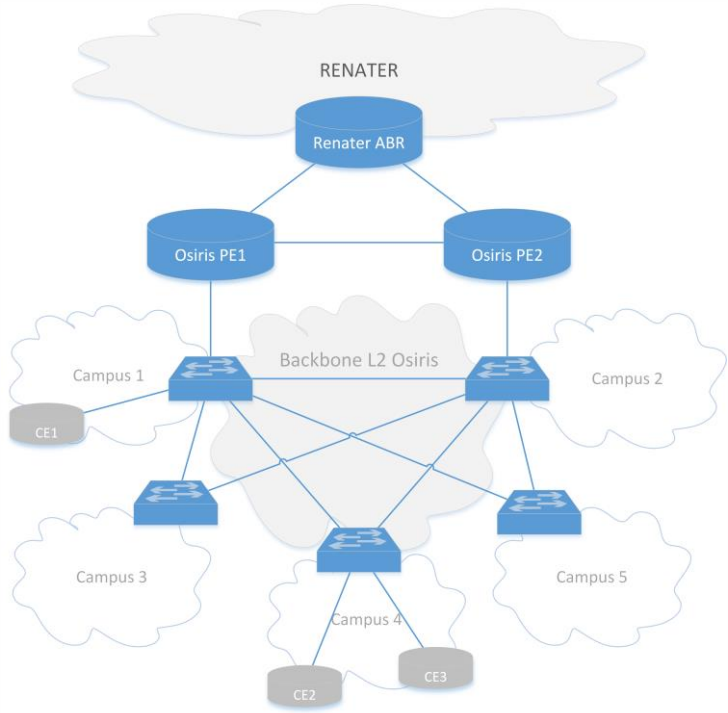

Figure 9 : Architecture réseau Osiris

L'intégration du service MD-VPN à l'architecture existante ne nous semblait pas triviale. Cependant, ce service a suscité un vif intérêt pour plusieurs raisons.

Tout d'abord plusieurs sites Osiris sont utilisateurs de VPNs délivrés par Renater et propagés sur Osiris. C'est le cas, entre autres, de réseaux de recherche comme LHCONE, dont l'un des sites Osiris est Tier 2, de réseaux administratifs comme RENO pour le CROUS ou de réseau de transport de la voix sur IP pour l'INSERM. De plus, de nouveaux VPN seront prochainement créés, notamment pour sécuriser les examens nationaux des facultés de médecine (ECNi) en 2016.

A ce jour, la mise en œuvre de chacun des VPN est fastidieuse. Elle nécessite plusieurs échanges avec le NOC et les chefs de projet Renater. Renater termine le VPN sur son routeur PE. Une sous-interface est créée entre Renater et Osiris puis Osiris crée un bridge sur ses routeurs qui connecte le VPN à un VLAN jusqu'au site client.

Les besoins des clients Osiris en virtualisation de réseaux de niveau 2 et 3 sont en augmentation. Osiris y répond par l'utilisation massive de VLANs étendus ou de VRF Lite, avec les problèmes inhérents à l'exploitation et au provisioning.

MDVPN nous a apporté une réelle opportunité de veille sur une technologie riche et éprouvée, MPLS. Le projet nous permis également de confirmer notre idée que MPLS pourrait améliorer la fiabilité de nos infrastructures et réduire nos coûts d'exploitation.

Enfin, la présentation du service en interne a suscité un réel intérêt auprès des instances politiques. L'inscription du projet au schéma directeur du numérique nous a permis d'étoffer le catalogue des services Osiris avec MD-VPN.

Les coûts matériels et humains de notre participation au projet MD-VPN sont restés modérés. Aucun investissement matériel n'a été nécessaire. Le réseau Osiris fonctionne avec des équipements Juniper MX480 et MX80. Ces équipements, comme la plupart des routeurs de cœur, implémentent les fonctionnalités requises. Les équipements de spare nous ont permis de participer aux différentes étapes du projet. Au niveau humain environ 30 jours/homme ont été nécessaires.

Suite aux bons résultats apportés par les tests, à l'investissement matériel nul et au soutien politique du comité de pilotage du réseau Osiris, il a été décidé de déployer MD-VPN en production en juin 2015.

Le déploiement de MD-VPN sur Osiris est en cours au moment où nous écrivons cet article.

Dans l'architecture OSIRIS actuelle, les équipements d'agrégation sur les campus ne supportent pas l'ensemble des technologies VPN MPLS requises pour MD-VPN. En revanche, les routeurs Juniper MX480 (Osiris PE1 et PE2 : figure 7) sont totalement compatibles.

Une refonte complète du réseau Osiris étant prévue pour 2017, un investissement matériel avant cette date est inenvisageable. Le déploiement en cours consiste donc à délivrer les VPNs depuis les routeurs Juniper MX480 directement connectés à Renater. Les VPNs sont ensuite prolongés sur le cœur de réseau niveau 2.

La figure 8 représente l'intégration la plus simple du service MD-VPN au réseau. L'équipement Osiris PE1 est le point de terminaison de l'ensemble des VPNs. C'est l'état du déploiement au moment de l'écriture de l'article.

L'opération consiste en trois étapes principales :

- Créer une interconnexion IP dédiée au service MD-VPN entre Osiris et Renater et y activer MPLS ;
- créer sur l'interconnexion un peering EBGP Labeled Unicast sur lequel seules les adresses de loopback des PE participant à MD-VPN sont annoncées ;
- créer un peering EBGP vers le Route Reflector Renater pour y annoncer et recevoir les routes des VPNs.

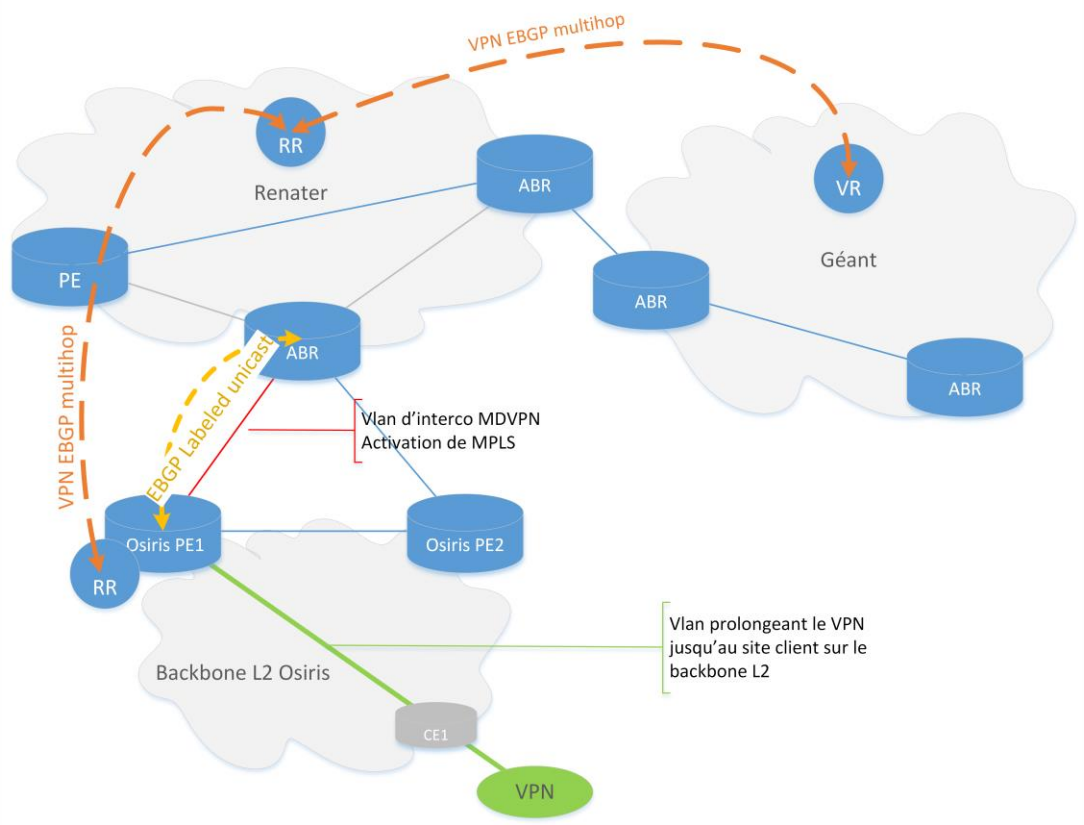

Figure 10 : Activation MDVPN sans redondance

La seconde étape consistera à sécuriser l'infrastructure MD-VPN sur Osiris :

- Une deuxième interconnexion dédiée sera créée entre Osiris et Renater ;
- MPLS sera activé entre Osiris PE1 et Osiris PE2 ;
- Un peering EBGP Labeled Unicast supplémentaire sera créé entre Osiris et Renater ;
- Un peering EBGP supplémentaire vers le Route Reflector Renater sera créé.

Par la suite, les PE du réseau régional alsacien seront intégrés à MD-VPN de la manière suivante :

- MPLS sera activé sur les interconnexions entre tous les PE Osiris et les PE du réseau régional ;
- Un peering IBGP avec les familles Labeled Unicast et VPN sera créé entre chaque PE du réseau régional et des Route Reflector créés sur chacun des PE Osiris.

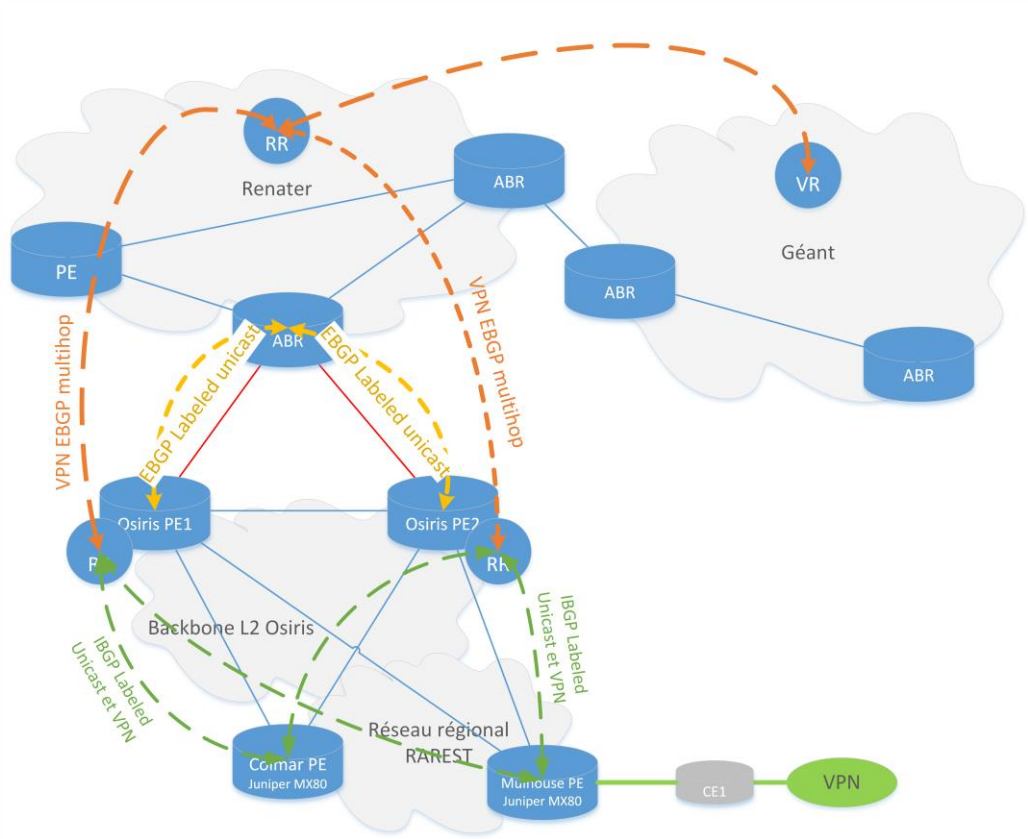

Figure 11: Intégration MD-VPN complète

Dans la future architecture d'Osiris, à l'instar de SYRHANO, le service MD-VPN sera totalement intégré sur une infrastructure MPLS de bout en bout.

4.1.2 Réseau SYRHANO

SYRHANO est le réseau régional pour l'enseignement et la recherche en Haute-Normandie. Il raccorde aujourd'hui environ 650 sites qui représentent 45 établissements de la communauté. SYRHANO fournit un ensemble de services réseaux (connectivité IPv4 / IPv6 généraliste, L3VPN, L2VPN, etc.) et applicatifs (stockage recherche, visioconférence, courrier électronique, etc.) à ses utilisateurs.

Depuis plus de 15 ans, le réseau SYRHANO s'appuie sur les technologies MPLS pour implémenter des services réseaux avancés : L2VPN, L3VPN, Fast Rerouting, Traffic Engineering. Aujourd'hui, SYRHANO compte plus de 40 L3VPN pour différents établissements régionaux dont certains sont également prolongés au travers de RENATER vers d'autres résaux régionaux. C'est dans ce contexte d'usage fort des services réseaux de type L3VPN, que SYRHANO est en cours de test et de raccordement en production sur le service MD-VPN.

Le réseau SYRHANO fonctionne sur une infrastructure totalement MPLS avec des équipememts de type Brocade MLXe et Cisco 12k sous IOS-XR. Les équipements Brocade dans leurs versions logiciels actuelles ne supportent pas les extensions de BGP pour l'échange de label (RFC 3107 : Carrying Label Information in BGP-4). Pour l'expérimentation MD-VPN nous avons donc utilisé un équipement Cisco 12K de spare qui supporte l'ensemble des fonctionnalités nécessaires.

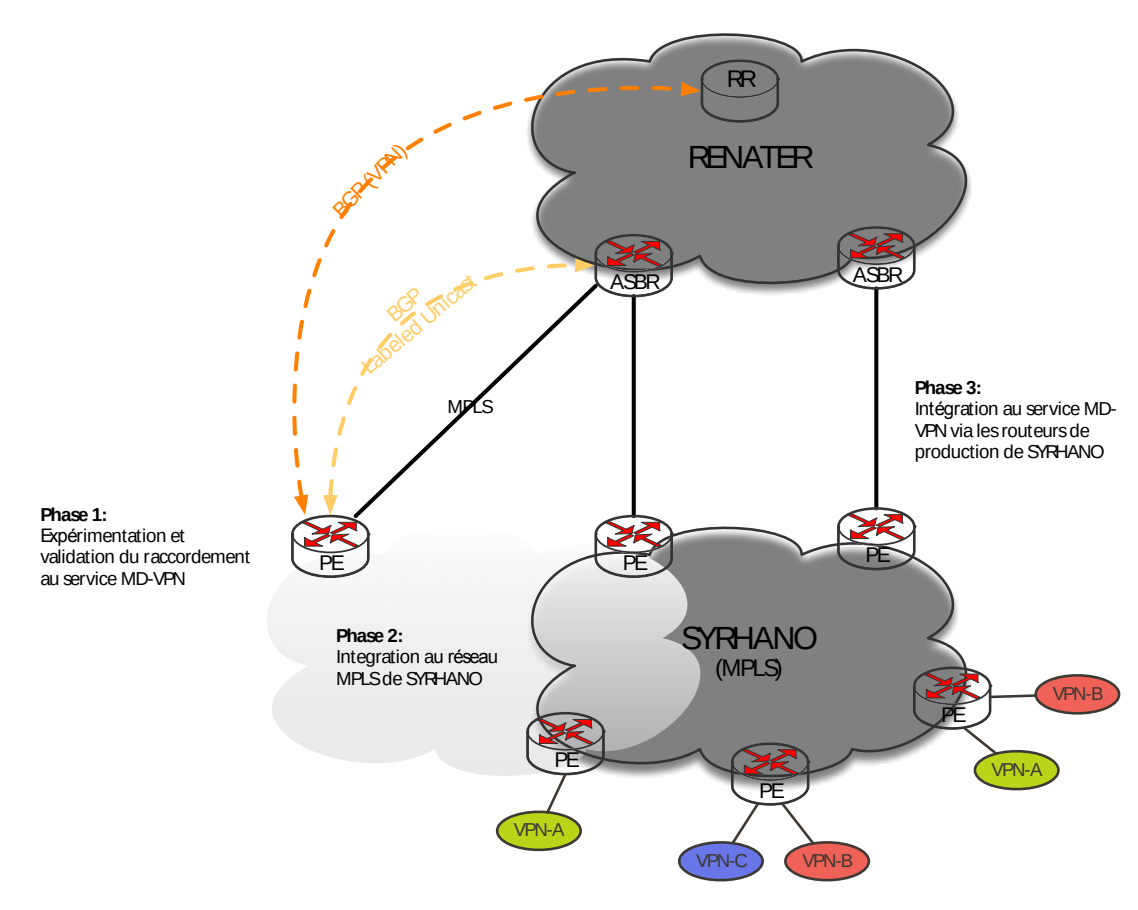

Figure 12 : Phases de déploiement de MD-VPN sur SYRHANO

Afin de valider le fonctionnement de MD-VPN sur SYRHANO nous avons établi un plan de déploiement en trois phases :

- Phase 1 : dans un premier temps nous avons raccordé notre routeur de spare au service MD-VPN dans un environnement de test pour valider les configurations à déployer. Cette phase nous a permis de détecter un comportement particulier sous IOS-XR lorsque celui-ci assure les fonctions ASBR et PE pour le service MD-VPN ;
- Phase 2 : une fois le raccordement au service MD-VPN validé, nous intégrons le routeur de test au sein de l'IGP de SYRHANO. Ceci permet de prolonger les VPN MPLS existants sur notre infrastructure vers le routeur de test afin de faire participer des utilisateurs de notre réseau au service MD-VPN et d'élargir la phase de test à d'autres participants ;

- Phase 3 : la dernière phase consiste a basculer le raccordement au service MD-VPN sur nos routeurs de production qui assurent également le raccordement au service IPv4 et IPv6 généraliste. Cette phase nous permettra notamment de sécuriser l'accès au service au travers de nos deux points d'accès RENATER.

Avec un faible investissement en temps hommes et en matériel, il nous a été possible de déployer très simplement le service MD-VPN. Au-delà du fait que le réseau SYRHANO soit déjà totalement basé sur le protocole MPLS, le principal avantage de MD-VPN est qu'il utilise un ensemble de protocoles déjà standardisés. De plus MD-VPN nous permet de proposer à nos établissements régionaux un service à forte valeur ajoutée dans le cadre de leurs collaborations avec d'autres établissements français ou européens.

5 Conclusions et perspectives

MD-VPN a permis de créer une infrastructure sans couture de transport de service à l'échelle européenne. Le service est un grand succès du projet européen GEANT GN3+, et RENATER ainsi que les réseaux régionaux OSIRIS et SYRHANO ont joué un grand rôle dans la réussite de du déploiement de MD-VPN. Comme MD-VPN est une infrastructure, il lui est possible d'accueillir de nouveaux services. Nous (OSIRIS, SYRHANO et RENATER) travaillons sur le nouveau service Ethernet VPN qui visent à proposer de nouvelles fonctionnalités dans la connexion entre 2 data center, par exemple la mobilité de machine virtuelle, le partage de charge par flux, le multi-homing actif/actif, etc.

Dans un contexte de collaboration et de mutualisation forte au niveau des acteurs de l'éducation et de la recherche (Communautés d'universités et d'établissements, laboratoires et équipes de recherche, etc.), le service MD-VPN apporte à tous les acteurs des réseaux une forte valeur ajoutée. Au niveau des réseaux de collecte régionaux, ce service permet de répondre rapidement à des demandes utilisateurs et de s'intégrer pleinement dans des contextes inter-régionaux, nationaux ou européens. Le service MD-VPN montre bien l'utilité des réseaux spécifiques pour l'enseignement et la recherche qui permet de monter un service de bout en bout homogène.

Bibliographie

1. RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs)
2. RFC 3701, Carrying Label Information in BGP-4
3. 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**>
4. Behringer M. H. (Distinguish Engineer at Cisco), Morrow M. J., 2005, MPLS security, Cisco Press
5. 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=*
6. MD-VPN OLA (Open Level Agreement) https://intranet.geant.net/SA6/mdvpn/_layouts/15/start.aspx#/SitePages/Home.aspx
    a. https://intranet.geant.net/SA6/mdvpn/Shared%20Documents/AUP-OLA/MD-VPN_AUP_V0.07.doc?Web=1

Glossaire

- VPN : Virtual Private Network

- MD-VPN : Multi Domain VPN
- VPLS : Virtual Private Leased Line
- MPLS : Multi-Protocol Label Switching
- LDP : Label Distribution Protocol
- RSVP : Resource Reservation Protocol
- BGP : Border Gateway Protocol
- VRF : Virtual Routing and Forwarding
- ASBR : Autonomous System Boudary Router
- SDN : Software Defined Network
- L3VPN : Layer 3 Virtual Private Network
- L2VPN : Laye 2 Virtual Private Network
- PE : Provider Edge
- SAFI : Subsequent Address Family Identifiers
- PoP :Point of Presence
- P2P : Point to Point
- CsC : Carrier supporting Carrier
- NREN : National Research and Education Network