Multi-Domain VPN service, une infrastructure sans couture pour les réseaux régionaux, NRENs et GEANT

Auteurs : Xavier Jeannin (RENATER), Alain Bidaud (SYRHANO), Sebastien Boggia (OSIRIS), Jean Benoit (OSIRIS), Benjamin Collet (OSIRIS), Christophe Palanche (OSIRIS).

Mot Clefs : MPLS, VPN, Carrier-of-Carriers, BGP Labelled unicast peering, GEANT, GN3+, D7.1 (DS3.3.1) MDVPN Service Architecture

Avertissement :
Compte tenu des circonstances particulières de la présentation du service MDVPN aux JRES 2013, ce document ne constitue pas un article complet JRES mais vise à vous fournir au lecteur une introduction à ce sujet. Le service MDVPN est spécifié plus complètement dans le délivrable GN3+ « D7.1 (DS3.3.1) MDVPN Service Architecture » et peut être téléchargée à http://www.geant.net/Resources/Deliverables/Documents/D7.1_DS%203%203%201-MDVPN-service-architecture.pdf.

Service description

Le service GN3plus Multi-Domain VPN (MDVPN) permet d'interconnecter deux réseaux par un réseau privé virtuel à travers plusieurs réseaux ou domaines (GEANT, NRENS ou Réseau Régionaux). Les utilisateurs de ces réseaux voient ainsi leurs services réseau IPv4/IPv6 ou niveau 2 étendus jusqu'au site distant comme s'ils étaient connectés localement.

Un cas d'utilisation typique est une organisation qui a besoin de connecter des sites éloignés géographiquement avec le même niveau de sécurité que si ces sites étaient localisés au même endroit. Mais il y a de multiples bénéfices à l'usage des VPN. Le premier est une forte réduction des coûts de sécurité pour les sites. Cette amélioration de la sécurité permet de se passer de firewall (deep inspection) comme il est nécessaire pour l'IP généraliste, et d'atteindre ainsi un haut niveau de performance réseau. L'isolation du trafic VPN du trafic Internet permet de se protéger d'attaque DDoS, du spoofing d'adresse et permet aux NRENs de mieux gérer ces flux en utilisant du traffic Engineering (choix des chemins utilisés).

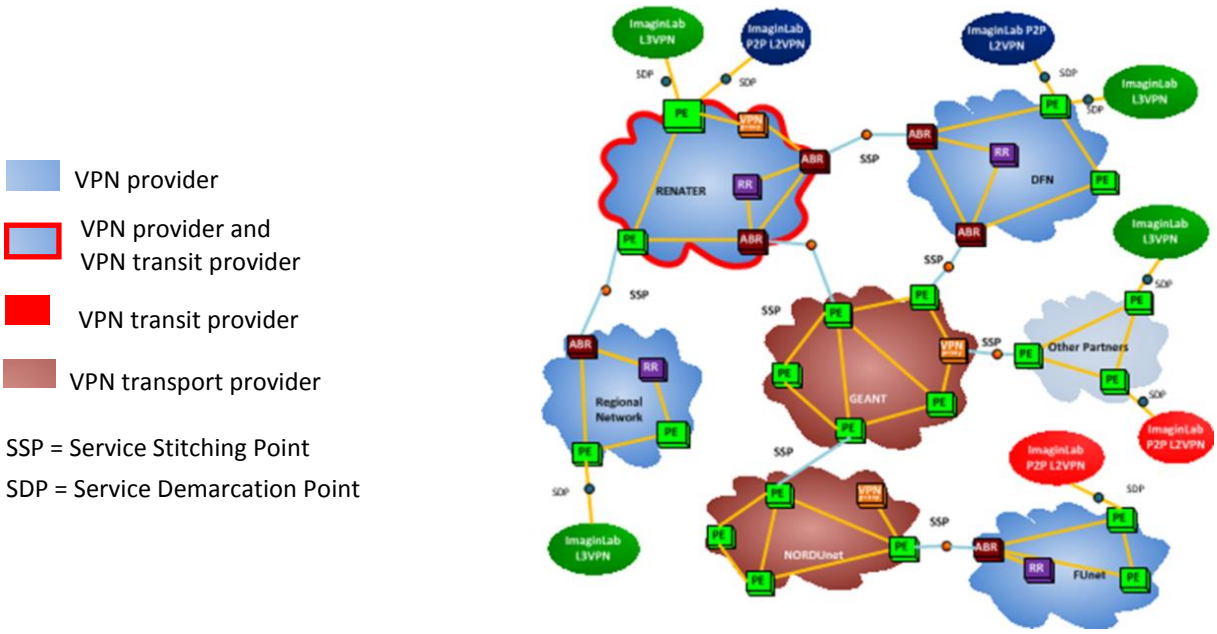

Figure 1 : MDVPN architecture

Un autre exemple d'utilisation du service MDVPN service est la connectivité de clusters, grids, cloud centres et centres HPC, car MDVPN permet à ces activités précitées de créer une ressource distribuée virtuelle qu'elles mettent ainsi à disposition à leurs utilisateurs (projets de recherche). Le LHCONE est un exemple réussi de l'usage de VPN dans la recherche. Le service MDVPN est très utile pour les utilisateurs dans le cadre de collaborations internationales (échanges de données, jobs, transfert de VM « vivante »). Comme MDVPN est très flexible et délivre des VPNs très rapidement, il y a un très large spectre d'utilisation de MVPN, depuis l'infrastructure de long terme avec échange intensif de donnés (LHCONE) jusqu'au VPN P2P monter rapidement pour une démonstration lors d'une conférence.

Le service est offert conjointement par GEANT, les NRENs et les Réseaux Régionaux afin de délivrer un service de bout en bout. **Les NRENs et les Réseaux Régionaux n'ont besoin de souscrire qu'une seule fois au service en un point nommé Service Stitching Point (SSP)**. Puis les NRENs et Réseau Régionaux ouvrent le service MDVPN à leurs utilisateurs. Les utilisateurs souscrivent au service MDVPN autant de fois qu'ils ont besoin de VPNs, le point de livraison du service est nommé Service démarcation point (SDP) localisé sur l'interface du Provider Edge routeur (PE). **Les NRENs et les Réseaux Régionaux n'ont besoin de configurer que les routeurs d'extrémité et les VPNs sont « multiplexés » et transporter à travers les différents domaines au travers des SSPs de manière transparente.** Le SSP peut être le même lien qui interconnecte deux domaines ou cela peut être un lien dédié.

MDPVPN peut être délivré au travers d'une cross-border fiber entre 2 NRENs pour fournir une meilleure redondance et une plus grande flexibilité. Pour fournir le service MDVPN à des sites non directement connectés peut utiliser la technologie qu'il considère la plus adéquate. Les domaines peuvent aussi implémenter eux même le service de transport de VPN (Carrier-of-Carriers) comme GEANT.

Chaque domaine utilisera son propre système de souscription pour les utilisateurs finaux et pour les domaines qui lui sont connectés mais il est nécessaire que les domaines échangent un minimum d'information pour la délivrance et la gestion du service.

Le service MDVPN est plus plutôt un ensemble, un package de services qu'un simple service, il permet de fournir des L3VPN (IPv4, IPv6), P2P L2VPN sans couture (seamlessly). De plus, une analyse du service multi-point Ethernet (VPLS) va être réalisée pour ajouter aussi ce service au portfolio GÉANT.

Design Technique

Un des atouts majeurs de ce service, c'est qu'il est bâtit sur des standards bien connus, BGP et MPLS (RFC 4364, 3107), qui sont disponibles sur les routeurs depuis des années. Le coût en termes de CAPEX est dès lors très limité alors que d'autre part les coûts opérationnels (OPEX) sont fortement réduits.

Les principes de base du service Multi-Domain VPN sont :

- Le LSP est étendu du PE jusqu'au PE distant de l'autre domaine
- La signalisation est séparée en 2 parties :
    - La signalisation MPLS multi-domaine du chemin entre les router PE grâce à un peering BGP labelled unicast SAFI (les routes internes sont annoncées aux points de fin du LSP)
    - La signalisation des labels VPN et des préfixes utilisateurs sont échangés entre PE (routes externes et préfixes utilisateurs dans les cas d'un L3VPN) grâce à un peering E-BGP VPNv4. Afin de permettre le passage à l'échelle, un route-reflector est prévu.

- Le service Carrier-of-Carriers, implémentation d'un service transparent de transport de VPN au niveau de GEANT.

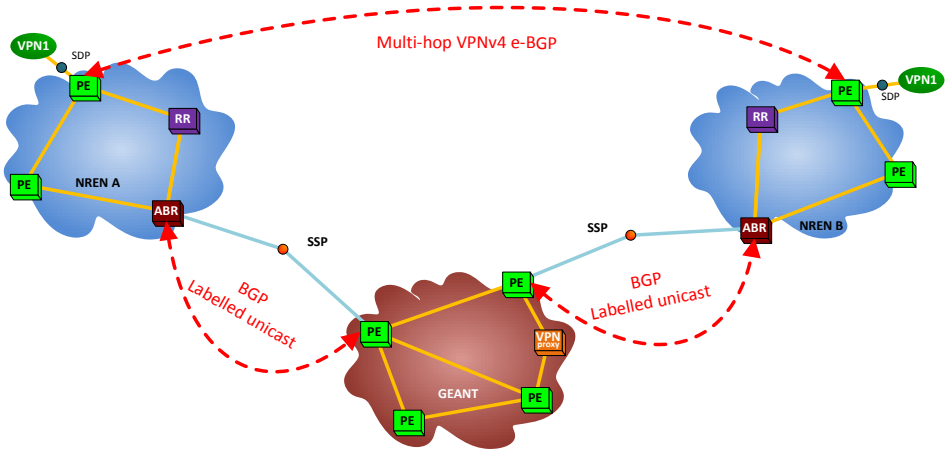

Figure 2 : échange de label pour L3VPN and L2VPN (Kompella)

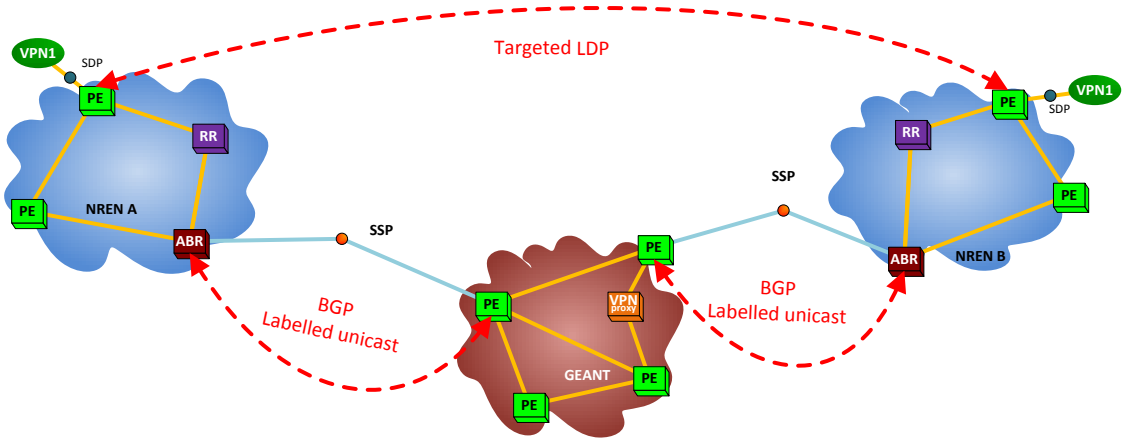

Figure 3 : P2P L2VPN utilisant LDP (Martini)

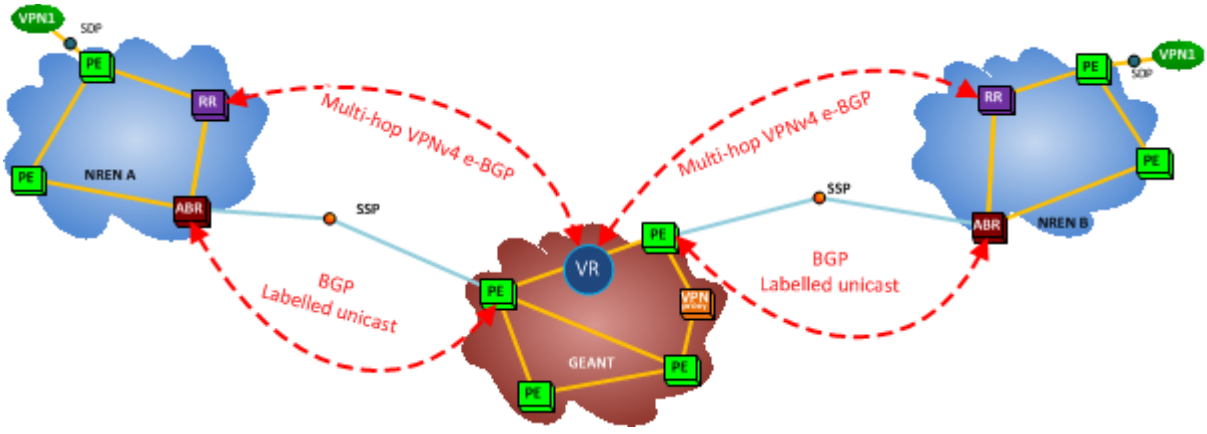

Figure 4 : Réduction du nombre de peering BGP grâce au VPN Route-Reflector

Les NRENs et les Réseaux Régionaux doivent implémenter les fonctionnalités suivantes pour participer aux services MDVPN :

- MPLS based forwarding dans les domains NRENs et les Réseaux Régionaux,

- Labelled unicast BGP + labels annonces sur le SSP pour la construction des LSP de bout-en-bout,
- Session LDP (targeted LDP) pour l'échange des labels du service L2VPN (Martini),
- BGP pour l'annonce des routes utilisateurs L3VPN.

Si un domaine ne peut fournir ces fonctionnalités, une technologie de VPN proxy a été développée et sera implémentée dans GÉANT et les NRENs qui le souhaitent afin connecter ce type de domaine.

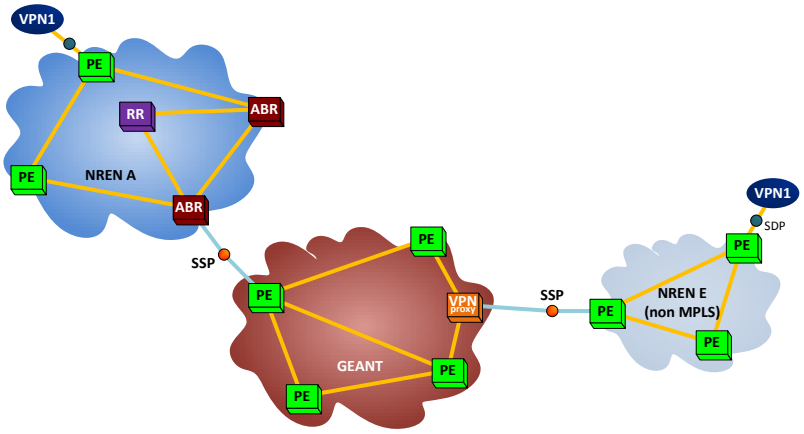

Figure 5 : Connexion d'un domaine non-MPLS via le VPN Proxy

Au-delà des conditions techniques requises, tout le l'aspect opérationnel et sécurité sont des points clé pour le déploiement de MDVPN. Les opérations du service multi-domain VPN est un sujet innovant car DANTE et les NOCs des NRENs doivent collaborer pour la fourniture, le troubleshooting et la gestion des VPNs utilisateurs mais comme MDVPN est un service de bout-en-bout, l'interaction avec les NOCs des réseaux régionaux doit être prise en considération. Enfin, la mise en place de SLA entre ces domaines doit être étudiée afin de permettre garantir un bon niveau de service pour MDVPN.

Reference:

- RFC 3107, Carrying Label Information in BGP-4
- RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs)

Vitae:

Xavier Jeannin - Ingénieur réseau - RENATER - Équipe Études et Projets Réseaux
Xavier Jeannin a travaillé dans un laboratoire de mathématiques, puis sciences cognitives. Il a été administrateur réseau au centre de génétique moléculaire de Gif-sur-Yvette.
Il a travaillé à l'Unité Réseaux du CNRS (UREC) sur IPv6 et sur les grilles de calcul dans le projet européen EGEE.
Il a été notamment l'ancien Activity Manager de l'activité Réseau du projet EGEE. Il travaille maintenant à RENATER dans l'équipe études et projets réseau.
Il travaille dans la Joint Research Activity Open Flow du projet GEANT GN3-plus.
Il est responsable pour le déploiement du LHCONE, VPN international qui relie les centres de calcul de la communauté des hautes énergies et physique. Il est Task leader de la tâche MP-VPN (SAT3) pour le projet GEANT GN3-plus qui vise à déployer des VPNs multi-domaines sans couture sur les NRENs et les Réseaux Régionaux européens.

Alain Bidaud - Responsable Technique du CRIHAN (Centre de Ressources Informatiques de Haute-Normandie)
Alain BIDAUD a travaillé pendant 7 ans en tant qu'ingénieur réseau au sein du CRIHAN. Il a participé aux évolutions techniques du réseau régional Haut-Normand SYRHANO et à la mise en place des services réseaux avancés (IPv6, MPLS VPN).
Il a participé aux groupes de travail TF-NGN en collaboration avec Terena et Geant et a travaillé en particulier sur la mise en place de service basées sur les technologies MPLS (VPN, Traffic Engineering)
Il travaille actuellement en tant que responsable technique du CRIHAN. Il est en charge des évolutions techniques et la mise en place d'infrastructures lourdes (datacentre, réseaux, calcul, stockage, etc.) au niveau régional, en particulier pour les besoins des établissements d'enseignement supérieur et de recherche.

Sebastien Boggia – Ingénieur systèmes et réseaux – Université de Strasbourg – réseau OSIRIS
Après une première expérience chez un opérateur de télécommunications, Sébastien a intégré en 2004 l'université pour participer à l'administration du réseau de l'enseignement supérieur et de la recherche de l'agglomération strasbourgeoise.
A ce jour il prend en charge le développement des services réseau ainsi que les problématiques de supervision et de métrologie.

Jean Benoit – ingénieur de recherche à la Direction Informatique de l'Université de Strasbourg, au Département Infrastructures. Ses sujets de prédilection sont l'architecture réseau, le système, la sécurité, la messagerie et l'automatisation de la gestion des infrastructures complexes.

Benjamin Collet – Ingénieur réseaux – Université de Strasbourg – réseau OSIRIS
De 2010 à 2011 Benjamin a travaillé à l'université de Strasbourg sur les questions de supervision et de métrologie, avant d'y retourner début 2013 en qualité d'ingénieur réseaux sur le réseau régional alsacien d'enseignement supérieur et de recherche OSIRIS. Il prend également part à la conception et à l'administration de services tels que la messagerie ou la supervision.

Christophe Palanché – Ingénieur systèmes et réseaux – Université de Strasbourg – réseau OSIRIS
Ingénieur d'étude à la Direction Informatique de l'université de Strasbourg au sein du Département Infrastructure. Il travaille actuellement sur l'architecture réseau, la messagerie et l'automatisation de la gestion des systèmes.