Service de VPN de niveau 2 sur RENATER

Documentation

Table des matières

1 Introduction

Le but de ce document est de présenter le service de VPN de niveau 2 de RENATER (ou L2VPN – Layer 2 Virtual Private Network). Il décrit les modalités générales d'interconnexion au service ainsi que les principes généraux du fonctionnement du service sur le réseau RENATER.

2 A qui s'adresse ce document

Ce document s'adresse :

- Aux utilisateurs du service L2VPN de RENATER
- Aux réseaux de collecte ayant des utilisateurs du service L2VPN de RENATER
- Aux équipes techniques du GIP RENATER
- Au NOC-RENATER

3 Vue d'ensemble

Le service L2VPN permet d'offrir une interconnexion privée de niveau 2 (Ethernet) entre des sites connectés sur RENATER. On peut distinguer sur RENATER 2 offres différentes, correspondant à des usages distincts :

- Une offre L2VPN point-à-point standard reposant sur la technologie MPLS, et pouvant être déployée en tout point du réseau sans délai. Chaque L2VPN bénéficie naturellement du maillage mis en œuvre sur RENATER. Deux types de L2VPN MPLS qui peuvent être configurés :
  - L2VPN VLAN-à-VLAN où un seul VLAN est transporté entre les 2 sites d'extrémité
  - L2VPN port-à-port où tous les VLANs sur un port Ethernet sont transportés entre les 2 sites d'extrémité.
- Une offre de circuit de niveau 2 à très haut débit (de l'ordre de 10Gb/s) reposant sur une commutation Ethernet sur des longueurs d'onde dédiées. La mise en place de circuits de ce type nécessite des modifications sur la topologie optique (ajout de nouveaux matériels), et implique des délais de mise en service de plusieurs semaines. Les circuits 10Gb/s ne sont par défaut pas secourus et chaque mise en place fait l'objet d'une étude approfondie.

Pour pouvoir bénéficier de ce service, les sites aux 2 extrémités du circuit doivent être raccordés en direct sur RENATER, éventuellement via un service de VPN fourni par un réseau de collecte. Il est possible de redonder la connexion des différents sites.

Les procédures opérationnelles, en particulier les contacts, sont rappelés pour les diverses requêtes qu'un site peut être amené à réaliser.

4 Service L2VPN standard

4.1 Description générale du service

En plus des services de connectivité IPv4/IPv6 unicast/multicast, le réseau RENATER propose des solutions de VPN (L2/L3 VPN) reposant sur le protocole MPLS.

Avec le service de L2VPN MPLS, deux établissements peuvent bénéficier d'une interconnexion Ethernet privée entre eux, sur l'infrastructure RENATER. Ils bénéficient donc de fait de la haute disponibilité offerte nativement sur RENATER : le circuit virtuel emprunte à tout moment le meilleur chemin entre les 2 NR d'extrémités où les clients sont raccordés.

Il n'y a pas dans le réseau RENATER de réservation de débit faite pour les L2VPN MPLS. Cependant les liens sont dimensionnés pour permettre, même en cas de re-routage, un transfert des données sans pertes de paquets. Les indicateurs de qualité du réseau sont publics et peuvent être consultés à tout moment sur le site web de RENATER www.renater.fr.

4.2 Différents types de L2VPN

Deux types de L2VPN MPLS peuvent être configurés :

- L2VPN VLAN-à-VLAN où un seul VLAN est transporté entre les 2 sites d'extrémité
- L2VPN port-à-port où tous les VLANs sur un port Ethernet sons transportés entre les 2 sites d'extrémité.

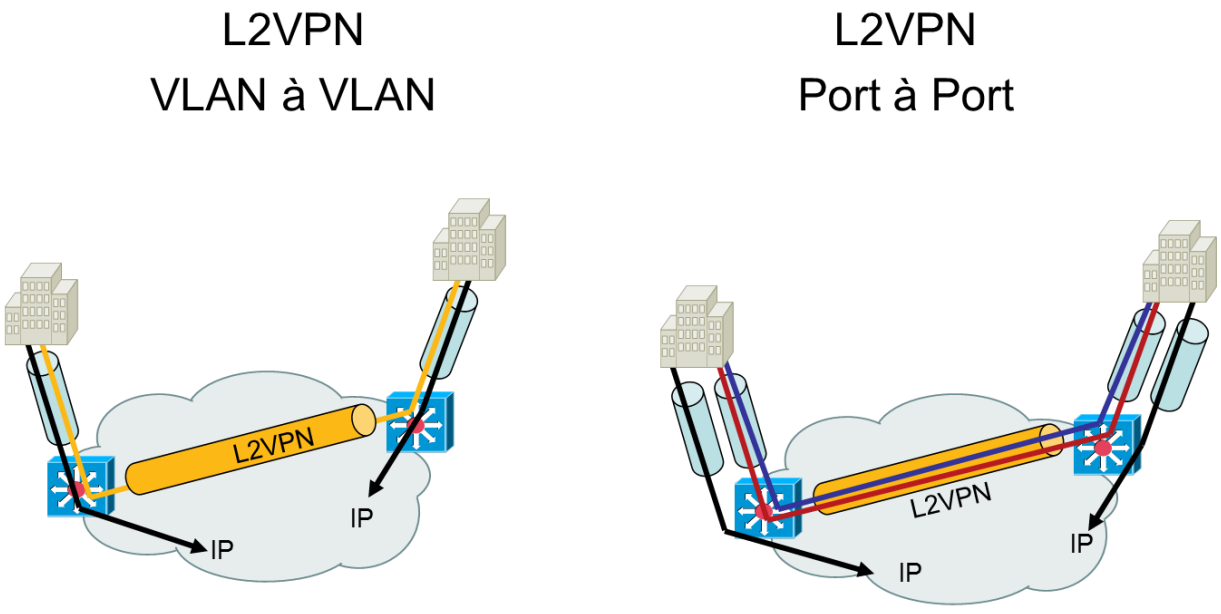

Figure 1 – Les différents types de L2VPN

Les deux solutions ont chacune leurs avantages et inconvénients et leur mise en place dépend généralement du mode de raccordement du site sur le NR :

Port dédié / non-dédié

- Dans le cas d'un L2VPN port-à-port, il est nécessaire aux 2 extrémités qu'une interface physique soit **intégralement** dédiée pour le L2VPN. Si un des 2 sites d'extrémité nécessite un autre service de RENATER (par exemple de la connectivité IP, ou alors un autre L2VPN vers un autre établissement) alors une seconde interface physique est nécessaire. Cela n'est souvent pas possible lorsque le site est « loin » du NR (nécessite de multiplier les raccordements NR)
- Dans le cas d'un L2VPN VLAN-à-VLAN, il est possible à chaque extrémité d'activer tous les services sur une seule interface physique (IP, plusieurs L2VPN, plusieurs L3VPN…)

Numéro de VLANs / transport de plusieurs VLANs

- Dans le cas d'un L2VPN port-à-port, les sites d'extrémité peuvent utiliser tous les VLANs sur le lien virtuel créé. L'ajout d'un nouveau VLAN ne nécessite pas de modification de service sur RENATER. Il y a une dissociation complète entre l'architecture Ethernet des sites et celle de RENATER.
- Dans le cas d'un L2VPN VLAN-à-VLAN, un seul VLAN est transporté. Le numéro de VLAN dépend de disponibilité sur le réseau RENATER. Dans le cas où les 2 sites voudraient s'interconnecter avec plusieurs VLANs, cela nécessiterait la configuration d'autant de L2VPN sur RENATER ce qui n'est pas souhaitable. La solution à base de QinQ (IEEE 802.1ad) est recommandée entre les sites d'extrémité (voir figure ci-dessous). Cette solution permet de dissocier un VLAN de transport (celui transporté par le L2VPN) des VLANs clients (encapsulés dans un unique VLAN de transport).

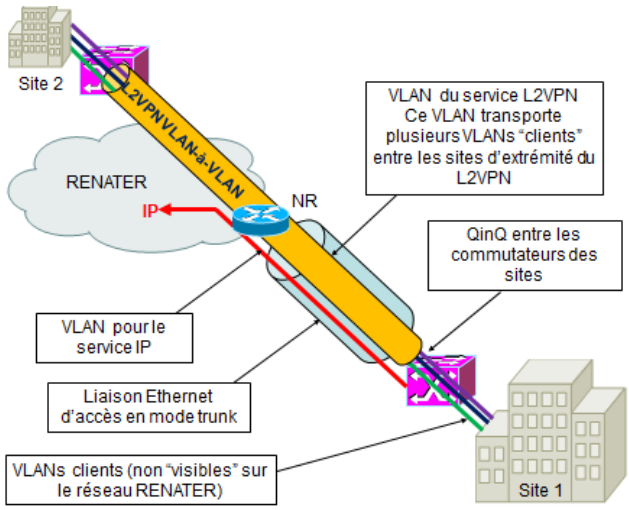

Figure 2 – Transporter plusieurs VLANs dans le cas d'un L2VPN VLAN-à-VLAN avec du QinQ (IEEE 802.1ad) sur les commutateurs de site

4.3 L2VPN entre plus de 2 sites

Sur RENATER, seuls des L2VPN MPLS point-à-point sont mis en place, permettant ainsi le raccordement de 2 sites en Ethernet sur le réseau national. Il n'y a pas de service de L2VPN multipoint-à-multipoint (VPLS). Pour raccorder plusieurs sites entre eux, d'autres solutions peuvent être envisagées :

- L3VPN MPLS (pour une interconnexion IP) www.renater.fr/vpn
- Mise en place de plusieurs L2VPN MPLS point-à-point (maillage complet, topologie en étoile ou double étoile)

4.4 Transport des BPDU clients

Dans le mode standard, les BPDU clients ne sont pas transportés dans le L2VPN, quelque soit le mode retenu (VLAN-à-VLAN ou port-à-port). Des solutions peuvent être étudiées au cas par cas pour permettre de transporter les BPDU (Spanning-Tree protocol) sur les L2VPN créés. Les sites d'extrémité doivent donc s'assurer qu'il n'y a pas de boucles dans l'architecture Ethernet globale.

4.5 Prolongation du L2VPN vers GEANT

Il est possible, sous réserve de validation technique, de prolonger le L2VPN sur l'infrastructure GEANT pour desservir des sites à l'étranger. Selon les débits et services demandés, cette prolongation sera faite soit sur le service L2VPN MPLS de GEANT, soit via le service GEANT+ qui permet la mise en place de circuits de type TDM à débit garanti.

Le support technique du GIP RENATER se chargera de la synchronisation avec GEANT et le réseau de la recherche national du pays concerné. Aussi il est nécessaire que le site distant entame également les démarches nécessaires pour demander le service également à son réseau national.

4.6 Interconnexion des sites au service L2VPN standard de RENATER

Pour se connecter au L2VPN, chaque site d'extrmité doit disposer d'un accès direct à RENATER. Cet accès peut être réalisé à l'aide d'une liaison louée, ou d'une simple fibre (jarretière), mais il peut très bien être fourni à travers des offres de VPN de niveau 2 de réseaux de collecte. Cet accès direct est indispensable pour garantir l'étanchéité des flux du VPN vis-à-vis du reste de l'Internet. L'interface d'accès au service VPN est soit :

- Une interface physique de type Ethernet
- Un VLAN particulier d'une interface Ethernet

Les figures ci-dessous illustrent les différents modes de raccordement des sites au service :

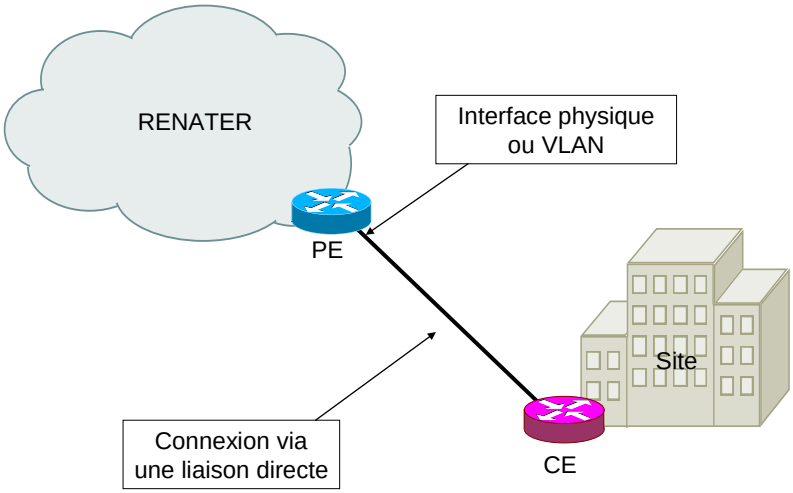

Figure 3 - Connexion via une liaison directe

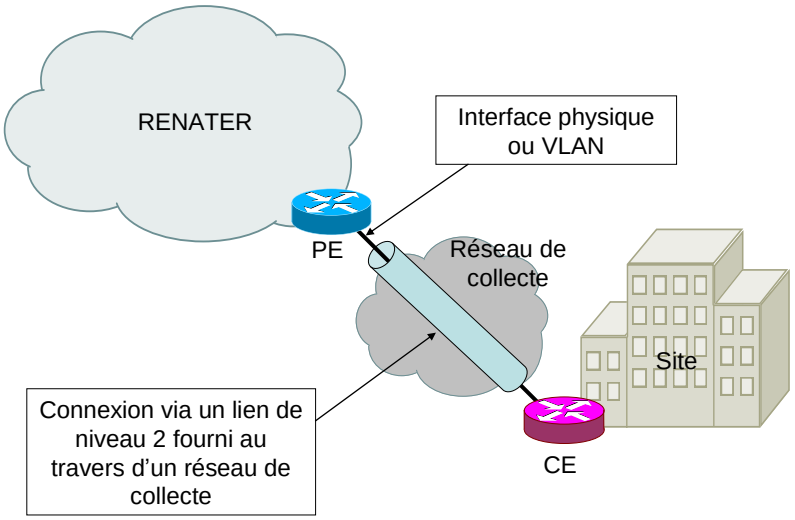

Figure 4 - Connexion via un lien de niveau 2 fourni au travers d'un réseau de collecte (L2VPN MPLS ou VLAN…)

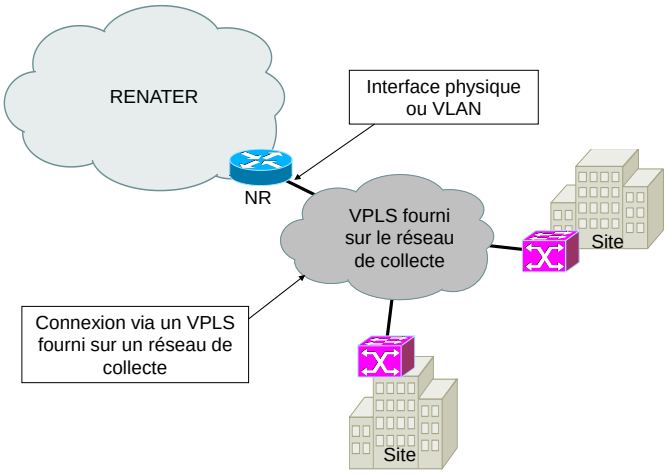

Figure 5 - Connexion via un VPLS fourni au travers d'un réseau de collecte.

4.7 Connexion redondée au service L2VPN

Dans le cas où un (ou les 2) site(s) d'extrémité du L2VPN possède(nt) un double raccordement sur RENATER, se pose la question de la redondance du L2VPN.

La solution préconisée reste la mise en place de deux L2VPN entre les sites d'extrémité, chacun étant routé via l'un des ports d'accès. L'utilisation d'un même VLAN n'est pas possible pour chaque L2VPN, aussi le site doit mettre en place les mécanismes de bascule approprié (routage…) Une étude spécifique doit être faite dans chaque cas.

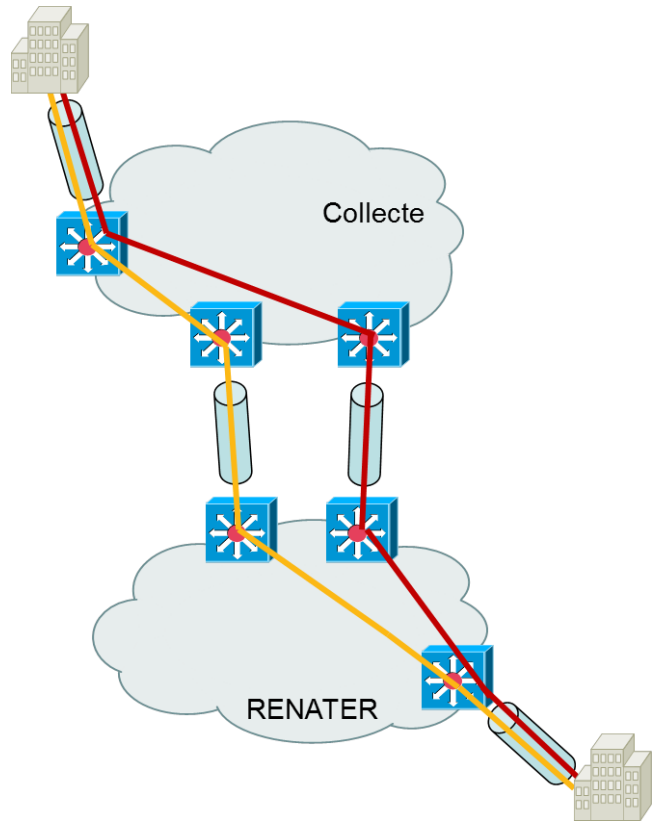

Figure 6 – Sécurisation du L2VPN dans le cas où un site est raccordé sur 2 NR via un unique réseau de collecte dans la figure ci-dessus.

Les mécanismes mis en jeux pour garantir un accès redondé au L2VPN sont plus complexes que ceux mis en place pour le L3VPN (www.renater.fr/vpn) et nécessite une étude au cas par cas.

5 Le service de circuits 10Gb/s dédiés

5.1 Description générale du service

L'infrastructure DWDM sur fibres optiques noires de RENATER rend possible la création de longueurs d'ondes à 10Gb/s qui peuvent être dédiées pour des usages particuliers (projets de calculs, transferts de données importants…)

Les accès des sites d'extrémité continuent de se faire sur les équipements de commutation de RENATER (et non directement sur les équipements optiques). Cela permet à la fois un meilleur contrôle sur le service rendu, ainsi qu'une plus grande souplesse dans la configuration des services.

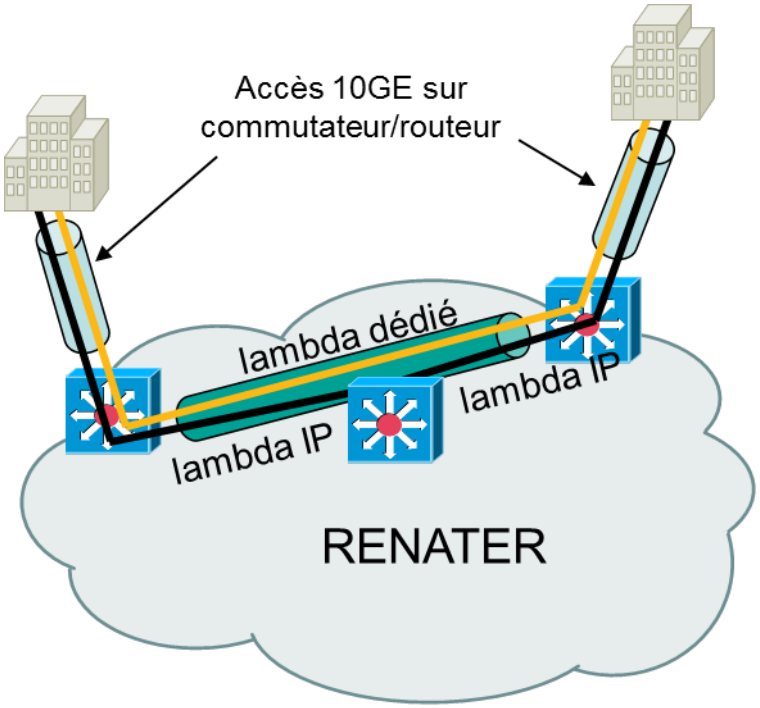

Figure 7 – Lambda dédié 10Gb/s

Chaque circuit 10Gb/s est physiquement construit sur un chemin défini et ne bénéficie donc pas d'une sécurisation en cas de perte d'un des liens optiques sous-jacents (ie. Il n'y a pas de retoutage).

Chaque demande de circuit 10Gb/s sur RENATER fait l'objet d'une étude technique et scientifique. La création du circuit, après validation, prend généralement une dizaine de semaines (temps de livraison et d'installation des équipements optiques permettant d'activer la nouvelle longueur d'onde)

5.2 Prolongation du circuit 10Gb/s vers GEANT

Il est possible, sous réserve de validation technique, de prolonger le circuit sur l'infrastructure GEANT pour desservir des sites à l'étranger. Cela nécessite l'activation d'un circuit 10Gb/s sur GEANT (délai de plusieurs semaines nécessaires après commande)

Le support technique du GIP RENATER se chargera de la synchronisation avec GEANT et le réseau de la recherche national du pays concerné. Aussi il est nécessaire que le site distant entame également les démarches nécessaires pour demander le service également à son réseau national.

6 Procédures opérationnelles

6.1 Rappel des contacts divers

- **NOC-RENATER**

noc-renater@noc.renater.fr
0800 77 47 95
+33 1 78 41 05 51

- **Support technique de RENATER**

support-reseau@renater.fr
+33 1 53 94 20 40

- **Direction des relations extérieures (DRE)**

agrements@renater.fr
Mme Hoinville : +33 4 67 16 38 25
Mme Gomes : +33 4 67 16 38 23

6.2 Qui contacter ?

- **Incident sur le service ou question sur l'état du service**
  ➔ Contacter le NOC-RENATER

S'assurer de l'ouverture d'un ticket d'incident. Le temps garanti pour le rétablissement du service est 4 heures.

- **Demande de report d'une maintenance ou en cas de question sur l'impact d'une maintenance sur le service**
  ➔ Contacter le NOC-RENATER

- **Demander un changement du service (interface, nouveau L2VPN…)**
  ➔ Contacter le support technique de RENATER. Le temps de réponse est inférieur à 72 heures.

- **Demander des ressources (Adresses IP, numéros d'AS, délégation DNS inverse…)**
  ➔ Contacter le support technique de RENATER. Le temps de réponse est inférieur à 72 heures.

- **En cas d'insatisfaction sur le traitement d'un incident**
  ➔ Contacter le support technique de RENATER

- **Modifier les contacts ou l'adresse des sites**
  ➔ Faire une modification d'agrément via SAGA

- **Demande de renseignement administratif (contrat, agrément)**
  ➔ Contacter la direction des relations extérieures (DRE)

7 Appendice

7.1 Références

- RFC2547 : BGP/MPLS VPNs
- Cours MPLS en ligne de Christophe Fillot : http://www.frameip.com/mpls-cisco/

7.2 Glossaire

- AS : Autonomous System
- ASN : Autonomous System Number
- BGP : Border Gateway Protocol
- DRE : Direction des Relations Extérieures
- FIB : Forwarding Information Base
- IGP : Interior Gateway Protocol
- L2VPN : Layer 2 Virtual Private Network
- L3VPN : Layer 3 Virtual Private Network
- LDP : Label Distribution Protocol
- LFIB : Label Forwarding Information Base
- LIB : Lable Information Base
- LSP : Label Switched Path (pour MPLS) ou Link State Packets dans le cas d'ISIS
- LSR :Label Switched Router
- LER : Label Edge Router
- LIR : Local Internet Registry
- MD5 : Message-Digest Algorithm (IETF - RFC 1321)
- MPLS : Multi-Protocol Label Switching
- NR : Nœud RENATER
- NRI : Nœud RENATER International
- PA : Provider Aggregate
- PI : Provider Independant
- RC : Réseau de collecte
- RIB : Routing Information Base
- RID : Router Identifier
- RIR : Regional Internet Registry
- SAFI : Sub-Address Family Identifier
- SAGA : Système d'Aide à la Gestion des Agréments
- VPN : Virtual Private Network