Service de VPN de niveau 3 sur RENATER (L3VPN MPLS)

Documentation

Table des matières

1 Introduction

Le but de ce document est de présenter le service de VPN de niveau 3 de RENATER. Il décrit les modalités générales d'interconnexion au service ainsi que les principes généraux du fonctionnement du service sur le réseau RENATER. Pour chaque L3VPN, ce document est remis aux contacts techniques des sites utilisateurs. Il est accompagné d'un second document donnant les détails de l'implémentation du L3VPN.

2 A qui s'adresse ce document

Ce document s'adresse :

- Aux utilisateurs du service L3VPN de RENATER
- Aux réseaux de collecte ayant des utilisateurs du service L3VPN de RENATER
- Aux équipes techniques du GIP RENATER
- Au NOC-RENATER

3 Vue d'ensemble

Le service de L3VPN permet d'offrir une interconnexion privée de niveau 3 entre des sites connectés sur RENATER. Pour pouvoir bénéficier de ce service, les sites 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. Le routage entre les sites et RENATER est fait uniquement à l'aide du protocole BGP, afin de simplifier l'administration du VPN.

La communication entre le VPN (Intranet) et l'Internet nécessite la configuration de un ou plusieurs sites « passerelles », qui devront annoncer les routes reçues du VPN dans l'Internet et vice-versa. Cette redistribution peut poser des problèmes et des moyens de les contourner sont proposés dans ce document.

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

4 Descriptions du service L3VPN MPLS

4.1 Principes généraux 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 ce service de VPN, les établissements bénéficient d'un Intranet qui assure une communication inter-site dans un mode totalement maillé. Ils bénéficient de la haute disponibilité offerte nativement sur RENATER-5.

Les avantages de cette solution sont :

- Proposer un service de VPN sur l'ensemble du territoire national. Les communications inter-sites se feront par le biais d'une table de routage isolée du reste de l'Internet.
- Cette solution est souple et à l'épreuve de la mise à l'échelle. L'ajout/le déménagement/la suppression d'un site ne nécessite que très peu de migration opérationnelle du point de vue du réseau RENATER.
- Les sites connectés au VPN restent « maîtres » de leur politique de routage qui reste dynamique. Aucun appel au NOC-RENATER n'est nécessaire dans le cas où un site désire modifier sa politique de routage sous réserve de ne pas dépasser le nombre de routes maximum autorisées.
- Les établissements ont la possibilité d'utiliser des adresses privées entre leurs sites (RFC1918).
- Les établissements ont la possibilité d'utiliser un seul ou plusieurs AS privés entre leurs sites.
- Les sites ont la possibilité d'utiliser les classes de services proposées par RENATER.

Les désavantages sont :

- L'impossibilité de bénéficier du service IPv4 multicast à travers le VPN.
- L'impossibilité de bénéficier du service IPv6 multicast à travers le VPN.

> ***Remarque :***
> *Les limitations pour IPv4 multicast et IPv6 mulicast devraient disparaître dans le cadre de l'évolution du réseau RENATER.*

4.2 Service L3VPN en mode « any-any »

Les L3VPN configurés sur RENATER sont par défaut en mode « any-any ». Cela signifie qu'un site connecté à ce VPN peut communiquer directement avec tous les autres sites du même VPN, sans passer par un site central.

Les VPN en mode hub&spoke, c'est-à-dire en étoile centrée sur un ou plusieurs sites ne sont pas supportés sur RENATER.

> ***Remarque :***
> *Cette restriction est davantage liée à une absence de demande plutôt qu'à une limitation technique. Les équipes techniques du GIP RENATER étudieront la faisabilité en cas de demande motivée.*

Détails du service L3VPN de RENATER

De nombreux services ont été créés reposant sur un domaine MPLS commuté. Le principe repose sur l'exploitation de l'en-tête MPLS. Il est ainsi possible de définir des VPNs discriminés par un label supplémentaire (en plus du label de commutation). Chaque VPN possède sa propre table de routage dans le concept de VRF impliquant une notion de RD et de RT (« *Route Distinguisher* » et « *Route target* »). Pour plus de détail sur MPLS-VPN consulter la RFC IETF 2547.

Au sein de RENATER, la mise en place d'un L3VPN est régie par les règles suivantes :

Le RT à la forme suivante : 2200:<ID_VPN_SITE>.

- Le RD est unique par PE, il permet de différencier 2 préfixes identiques émis sur le même VPN depuis 2 sites différents.
- La notion de VRF est locale au PE. Cependant pour des raisons de cohérence, les VRFs associées à chaque client sur tous les PEs ont le même nom sur tous les routeurs RENATER, selon les règles de nommage existant sur RENATER.
- Une VRF de type « *any-any* » est définie sur chaque PE ayant une interface connectée à un site du VPN. La VRF n'utilise qu'un seul « *Route-Target* » (RT). La politique d'import et d'export de RT est statique.

5 Interconnexion des sites au service L3VPN de RENATER

5.1 Interconnexion physique

Pour se connecter au VPN, le site 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 ou 3 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 :

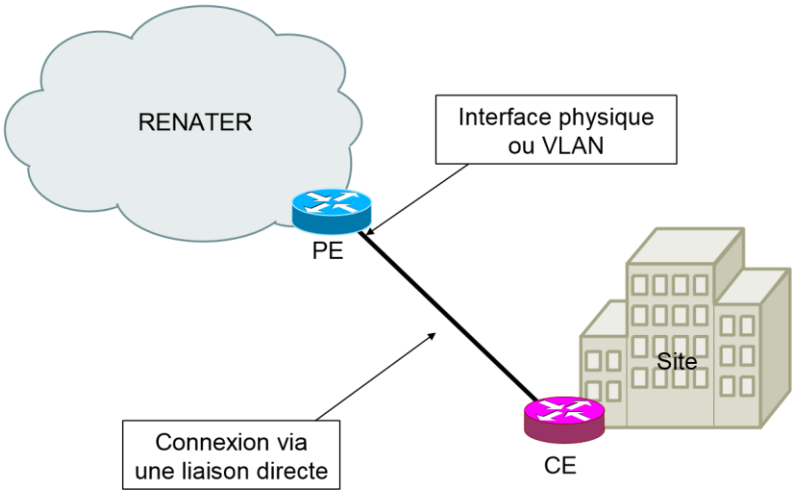

Figure 1 - Connexion via une liaison directe

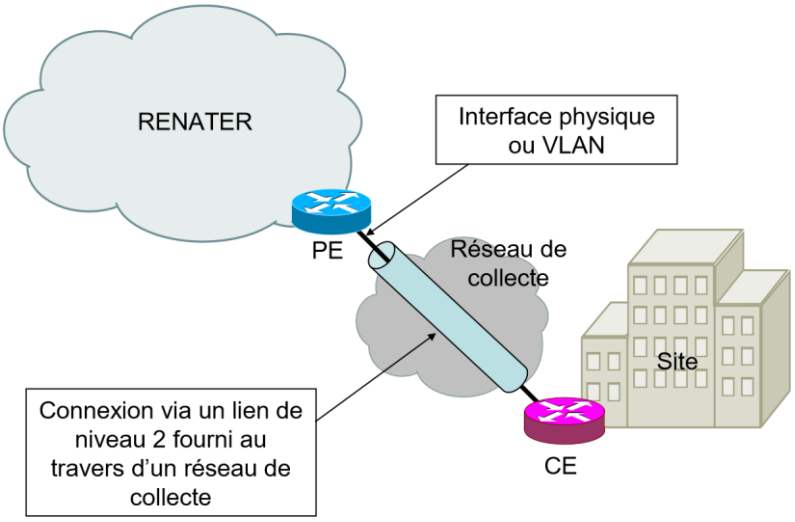

Figure 2 - Connexion via un lien de niveau 2 fourni au travers d'un réseau de collecte (L2VPN MPLS ou VLAN…)

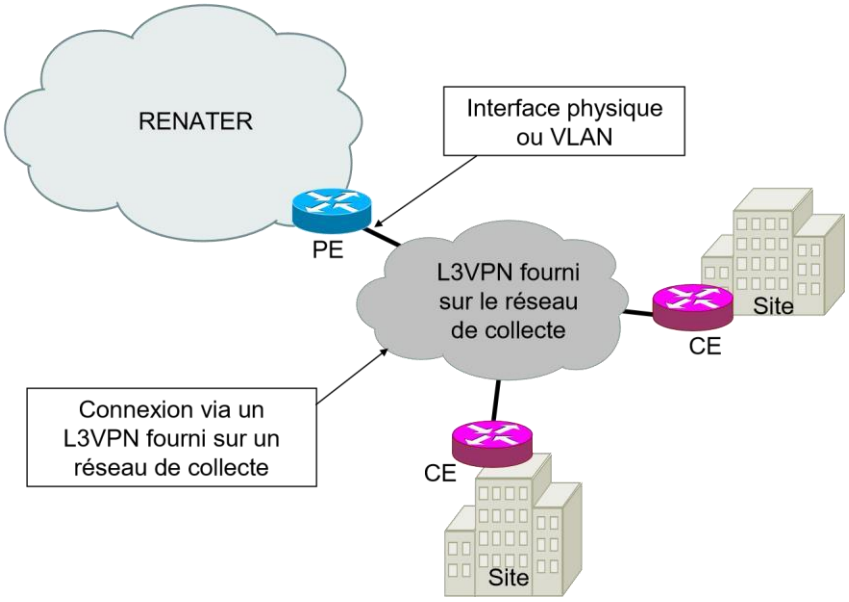

Figure 3 - Connexion via un VPN de niveau 3 fourni sur un réseau de collecte (VRF-to-VRF - RFC 4364 - 10.a)

5.2 Interconnexion IPv4

Sur l'interconnexion entre le site et le VPN (ou alors entre le réseau de collecte), un préfixe IPv4 d'interconnexion est attribuée par le NOC-RENATER lors de la connexion. Par défaut ce préfixe est un /30 (2 adresses). Dans certains scénarios, un préfixe /29 pourra être attribué. Ces scénarios devront faire l'objet au préalable d'une validation du support technique du GIP RENATER.

5.3 Routage

Le protocole de routage entre le routeur de chaque site (CE) et le routeur RENATER (PE) est BGP. Le routage statique ou d'autres protocoles de routage dynamiques ne peuvent pas être utilisés. Pour un site disposant déjà d'un peering BGP avec RENATER pour le service IPv4 standard, il sera nécessaire de configurer un nouveau peering pour le service L3VPN. Le site peut utiliser au choix un numéro d'AS BGP publique ou privé.

Dans le cas où le site utilise déjà un service de VPN de niveau 3 du réseau de collecte pour s'interconnecter à celui fourni sur RENATER, alors le peering BGP s'établit entre le routeur du réseau de collecte et le routeur RENATER.

A travers ce peering, RENATER n'applique aucune restriction quant aux préfixes acceptés et envoyés. La seule restriction est le nombre de préfixes acceptés en total dans le VPN, comme cela est décrit dans la section suivante 5.5. Les préfixes acceptés sur chaque peering BGP d'un L3VPN seront envoyés à travers tous les autres peerings du même VPN.

Les sites veilleront donc à appliquer les bonnes configurations de routage puisque la moindre erreur ne sera pas corrigée par des filtres placés sur RENATER. De la même manière, en cas d'incident dû à des annonces erronées, RENATER n'appliquera pas de corrections. Les sites du VPN devront corriger eux-mêmes leurs annonces.

BFD (Bidirectional Forwarding Detection) peut être configuré sur les peerings BGP afin d'optimiser la convergence.

5.4 Connexion redondée au service L3VPN

Un site peut avoir plusieurs accès à un même L3VPN, que ce soit sur un seul NR ou sur des NR différents. Le site établira alors plusieurs peerings BGP avec RENATER sur chacun des accès et il utilisera les communautés BGP de service RENATER pour gérer la précédence des accès les uns par rapport aux autres (voir la documentation disponible sur site web RENATER). Les schémas suivants montrent des exemples possibles connexions redondées sur RENATER.

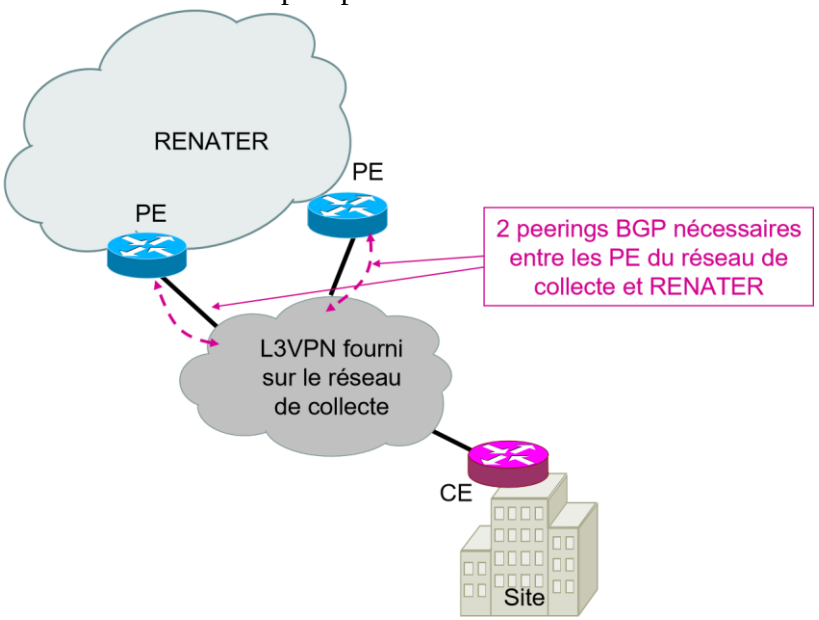

Figure 4 - Connexion redondée via un service L3VPN fourni par un réseau de collecte (VRF-to-VRF - RFC 4364 - 10.a)

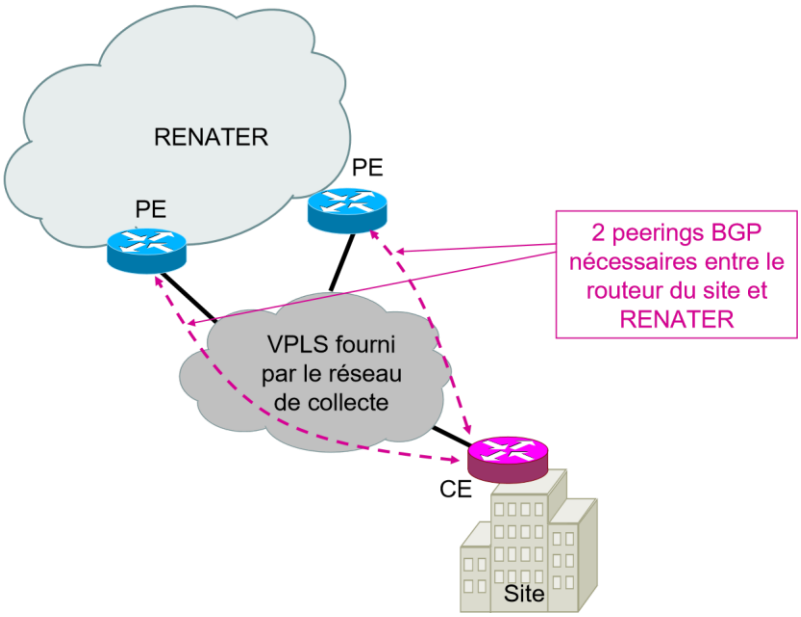

Figure 5 - Connexion redondée via un service VPLS fourni par un réseau de collecte

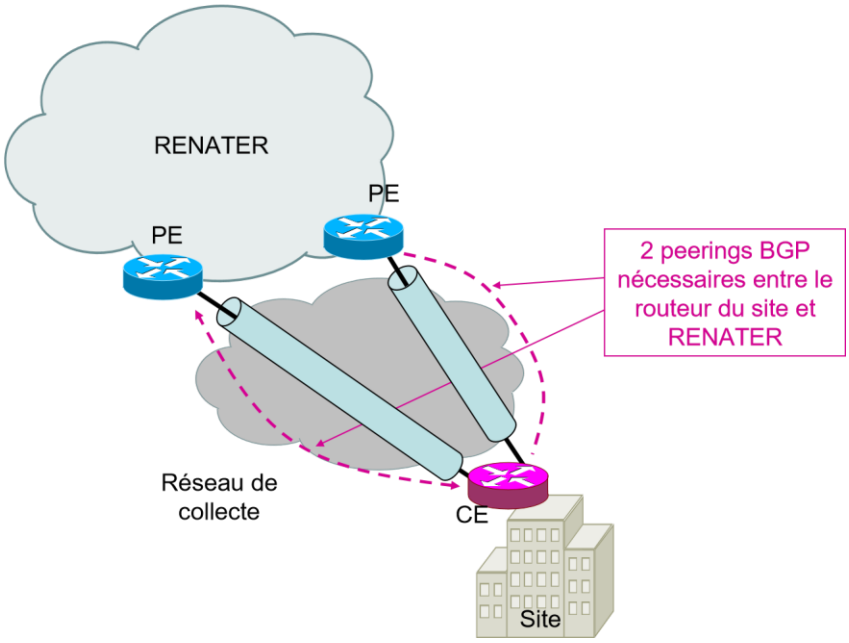

Figure 6 - Connexion redondée via la création de 2 tunnels points-à-point sur le réseau de collecte (VLANs, L2VPN MPLS…)

5.5 Limitation sur le nombre de routes acceptées dans le L3VPN

Pour des raisons de stabilité de routage, et pour protéger le réseau RENATER en cas d'annonces mal contrôlées de routes dans le L3VPN, un nombre de routes maximum est configuré pour chaque L3VPN.

Par défaut cette limite est fixée à 300, et des erreurs sont remontées au NOC-RENATER dès que plus de 200 routes sont présentes dans le VPN.

Pour toute demande de changement quant à la valeur maximale autorisée, le contact technique de l'établissement demandeur du VPN contactera l'équipe de support technique du GIP RENATER et indiquera les nouvelles limites qu'il souhaite mettre en œuvre (le contact technique doit être celui qui est mentionné sur l'agrément RENATER)

5.6 Interconnexion avec l'Internet

5.6.1 Principe de l'interconnexion VPN ⇔ Internet

L'accès à Internet n'est pas directement possible depuis le L3VPN. Dans chaque VPN, un ou plusieurs sites devront être configurés pour être les passerelles entre le L3VPN et l'Internet, en utilisant les accès au service IPv4 unicast standard de RENATER.

Cette solution a pour avantage de fournir un meilleur contrôle de l'accès Internet en termes de métrologie et sécurité vis-à-vis du VPN. Cela évite de multiplier les « pare-feu » qui sont nécessaires sur les sites « passerelle ».

Une double connexion logique est donc nécessaire sur les sites passerelles (une connexion vers le VPN et l'autre vers l'Internet). Le trafic Internet des sites du VPN doit obligatoirement transiter vers celui-ci.

Sur la connexion Internet, les spécifications de raccordement au service IP Internet s'appliquent. Les modifications de routage sur ces accès se font via le biais de modifications sur l'agrément à travers l'interface SAGA. Dans le cas où plusieurs passerelles sont configurées entre le VPN et l'Internet, les communautés BGP de service pourront être utilisées pour gérer la priorité entre les divers accès (voir documentation disponible sur le web
RENATER)

⚠ ***Attention :*** ** Les sites passerelles veilleront à bien agréger les préfixes sur les annonces vers l'Internet, ou vérifiera l'agrégation des routes faites sur RENATER. En effet, seuls les préfixes de longueur inférieure ou égales à /24 sont d'ordinaire acceptés dans l'Internet. RENATER agrège aussi les préfixes alloués.*

** Les bases de données Internet doivent être à jour afin d'avoir les préfixes correctement annoncés par les fournisseurs de transit IP de RENATER. Le GIP RENATER se charge de mettre à jour les objets « routes » pour les routes faisant partie intégrante des blocs RENATER, mais pas pour les autres préfixes.*

** Un « remove-private-as » sera automatiquement positionné lors de l'établissement des sessions BGP.*

** Les adresses référencées dans la RFC1918 seront annoncées dans le VPN mais pas à l'Internet.*

Remarque :
Afin de garantir un service quasi permanent, le réseau RENATER est doté d'un accès Internet IPv4/IPv6/MULTICASTv4/MULTICASTv6 commercial pouvant atteindre un débit de 10 Gbps. En outre, ce service repose sur plusieurs fournisseurs d'accès différents en mode partage de charge.

5.6.2 Difficultés potentielles liées à l'interconnexion VPN ⇔ Internet

5.6.2.1 Description du problème

Le site passerelle reçoit les routes des autres sites du VPN via BGP. Ces routes sont installées dans la table BGP du site avec le chemin d'AS suivant : AS RENATER (2200) - AS site distant

Si rien n'est mis en œuvre au niveau du site passerelle, celui-ci annonce sur son accès Internet avec RENATER le préfixe du site distant avec le chemin d'AS suivant : AS site passerelle - AS RENATER (2200) - AS site distant

Le préfixe du site distant est alors refusé par RENATER sur l'accès Internet puisque le numéro d'AS RENATER est dans son AS-path. Ce principe de base BGP permet d'éviter les boucles de routage dans l'Internet

5.6.2.2 Solutions pour contourner le problème

Plusieurs solutions permettent de contourner le problème et doivent être implémentées par le site, aucun mécanisme spécifique n'étant mis en œuvre sur RENATER :

- **Agrégation des préfixes des sites distants au niveau du site passerelle**. L'agrégat est annoncé sur RENATER avec comme AS d'origine l'AS du site passerelle, et un AS-path vide. L'agrégat est accepté sur RENATER. Cette solution ne peut être mise en œuvre que si tous les sites ont des adresses proches (ce qui est la cas généralement dans le cas où tous les sites appartiennent à un unique organisme à qui RENATER a alloué des adresses.

- **Utilisation de « l'AS-override »**. Cette option, lorsqu'elle est implémentée sur les routeurs, permet d'ignorer le mécanisme anti-boucle BGP, et remplacer le chemin d'AS initial par un autre chemin d'AS. Le site passerelle peut avec ce mécanisme supprimer l'AS-RENATER de l'AS-path initial et ne laisser que le numéro d'AS du site passerelle. Cette solution peut nécessiter l'application de VRF-lite sur le routeur CE.

Remarque :
D'une manière générale ce point peut faire l'objet d'une étude détaillée au cas par cas.

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, nombre de routes…)**
  - 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

- **Ajouter un site dans le VPN**
  - Faire une modification d'agrément du site qui doit être ajouté via SAGA, en spécifiant la demande et les détails dans la section « observations ».

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

7 Appendice

7.1 Références

- RFC1195 : Use of IS-IS for Routing in TCP/IP and Dual Environments
- RFC1771 : A Border Gateway Protocol 4
- RFC1966 : BGP Route Reflection An alternative to full mesh IBGP
- RFC1997 : BGP Communities Attribute
- RFC2385 : Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC2439 : BGP Route Flap Damping
- RFC2545 : Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC3031 : Multiprotocol Label Switching Architecture
- RFC2547 : BGP/MPLS VPNs
- ripe-399 : RIPE routing working group recommendations on route aggregation
- Cours MPLS en ligne de Christophe Fillot : http://www.frameip.com/mpls-cisco/
- Communauté de service BGP RENATER : http://www.renater.fr/bgp

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

7.3 Liste des figures