

Évolution de l'infrastructure de RENATER : RENATER-5

Jérôme Durand
GIP RENATER
151 Bd de l'Hôpital
75013 PARIS

Franck Simon
GIP RENATER
151 Bd de l'Hôpital
75013 PARIS

Résumé

Depuis fin 2008, le réseau RENATER est entré dans sa cinquième génération, conçue pour répondre aux besoins toujours plus exigeants de la communauté Education et Recherche française, en termes de débit, de services et de fiabilité.

Le réseau RENATER-5 est basé sur une infrastructure optique (fibres optiques noires) sur laquelle sont activées des longueurs d'ondes utilisées pour le transport du trafic IP ou dédiées à de grands projets de recherche. Divers équipements de routage ont été mis en œuvre sur cette infrastructure. Alors que des tera-routeurs ont été déployés sur les nœuds de cœur du réseau, des commutateurs/routeurs ont été installés sur la plupart des points d'accès.

Ce déploiement massif de liaisons, d'équipements DWDM, de routeurs et de commutateurs, a dû intégrer des contraintes fortes de réutilisation du matériel existant et la résolution de challenges techniques, notamment pour la partie optique.

Mots clefs

RENATER-5, fibres optiques noires, DWDM, longueur d'onde, IPv6, multicast, MPLS, VPN, BGP, haute-disponibilité

1 Introduction

Déployé depuis fin 2008, le réseau RENATER-5 est un formidable outil de communication pour la communauté Recherche et Education en France. Basé sur une infrastructure de fibres optiques noires, activées par des équipements optiques DWDM, l'architecture RENATER-5 mise en place est capable de répondre pour les années à venir aux besoins croissants des usagers en termes de débit : de nouvelles longueurs d'ondes peuvent être ajoutées tant pour le transport du trafic IP que pour des besoins spécifiques en rapport avec de grands projets de recherche.

Après avoir présenté le réseau (liaisons, équipements et topologie), l'article reviendra sur la phase de déploiement. Avec l'enchaînement des phases de construction de l'infrastructure de fibres optiques, d'installations d'équipements DWDM puis de mise en place des routeurs et/ou commutateurs, ce déploiement s'est étalé au total sur près de 6 mois. En dernier lieu les services réseau et leur ingénierie seront présentés.

2 Le réseau RENATER-5

2.1 Un réseau de fibres optiques noires

RENATER-4 a permis d'acquérir une expérience sur l'opération d'un réseau DWDM¹ sur fibres noires, dans la mesure où près de 3 000 km de fibres noires ont été activées. En service entre 2005 et 2008, ce réseau hybride utilisait des services de liaisons louées SDH 2,5 Gbit/s pour le trafic IP, et reposait sur une infrastructure DWDM sur fibres noires pour des projets nécessitant des débits importants (de l'ordre de 10 Gbit/s). Dans un but de diminution des coûts mais aussi afin de permettre une évolution des débits sur les différents axes, RENATER-5 est maintenant majoritairement basé sur une seule infrastructure optique avec des longueurs d'ondes à 10 Gbit/s pour le transport trafic IP dit de « production » et des longueurs d'ondes spécifiques pour les grands projets de recherche.

¹Dense Wavelength Division Multiplexing

S'il a été possible de disposer de fibres optiques noires sur la plupart des axes, il a été nécessaire de conserver certaines liaisons STM-16 (2,5 Gbit/s) faute d'offre acceptable pour les NR² de Limoges, Pau et Corte. Pour ce dernier NR, la contrainte est surtout liée aux technologies des transmissions sous-marines qui imposent une gestion couplée des infrastructures FON³ et des équipements actifs (DWDM, SDH...) : l'opérateur du câble devant assurer lui-même l'amplification des signaux, il éclaire lui-même les fibres afin de s'affranchir de toute incompatibilité qui pourrait exister entre les divers équipements actifs de la liaison.

Les liaisons FON ont été acquises soit sous forme d'IRU⁴ de 10 ans (droit inaliénable d'usage), soit sous forme de location. Un nouveau déploiement majeur a été mené pour le renouvellement de ces dernières (phase RENATER-5bis). Cette nouvelle étape permet une optimisation complémentaire (en termes de coûts notamment) et consolide davantage des options de type IRU par rapport aux locations annuelles récurrentes.

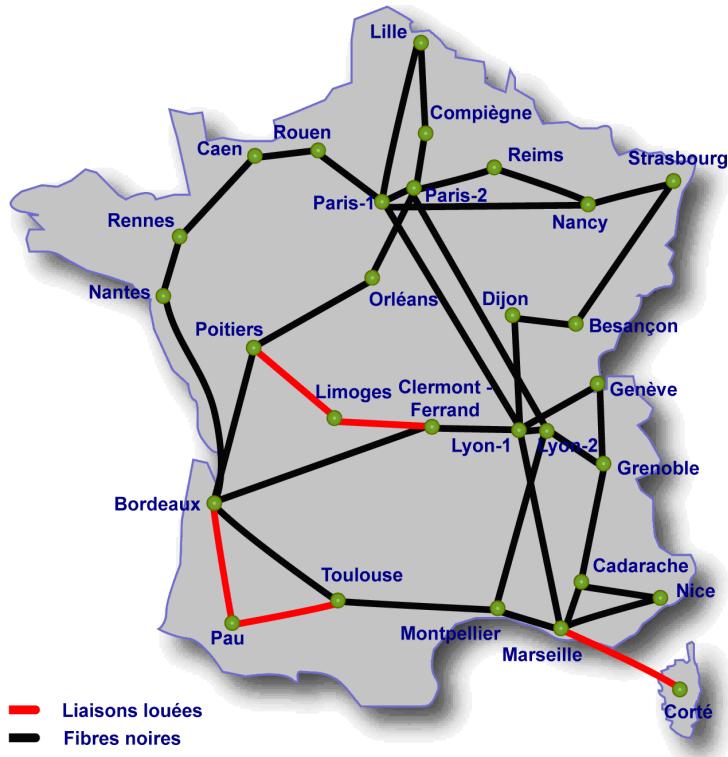


Figure 1 - *Les fibres noires sur RENATER-5*

Des études techniques ont aussi été menées pour redondrer certains NR. Il est apparu que les solutions techniques à mettre en place et surtout les coûts associés (fibres et équipements) étaient disproportionnés au regard du gain de disponibilité apporté pour les NR concernés. A cet effet un historique complet des incidents et coupures avait confirmé cette analyse de risque. En revanche l'axe principal Paris-Lyon a été redondé avec 2 nouveaux points de présence interconnectés. Le deuxième point de présence de Paris est également connecté au SFINX, à GEANT et à l'infrastructure d'Ile-de-France.

2.2 L'infrastructure DWDM

Le constructeur retenu pour les équipements DWDM de RENATER-5 est CIENA. Des châssis CN4200, équipements de type « métropolitain », ont été déployés sur la majeure partie des NR. Ils ont parfois nécessité l'installation d'amplificateurs Raman (au lieu d'amplificateurs EDFA⁵ plus communément utilisés) sur les liaisons les plus longues pour éviter de devoir régénérer le signal entre deux NR. La régénération, qui consiste à reconvertis chaque longueur d'onde en signal électrique « propre » pour ensuite le ré-émettre est non seulement très coûteuse, mais en plus son coût est évidemment proportionnel au nombre de longueurs d'ondes activées. Au final la régénération du signal n'est nécessaire que sur deux liaisons uniquement.

²Nœud RENATER

³Fibre Optique Noire

⁴Indefeasible Right of Use

⁵Erbium Doped Fiber Amplifier

Les équipements DWDM ALCATEL-LUCENT de RENATER-4 ont été conservés et redéployés sur les boucles Est et Nord du réseau afin d'avoir un sous-ensemble DWDM cohérent et éviter ainsi autant que possible le chaînage d'équipements optiques de plusieurs constructeurs différents. Les contraintes inhérentes à ce redéploiement sont détaillées dans la section 5 de cet article .

Deux types de longueurs d'ondes ont été déployées : des longueurs d'ondes entre NR adjacents pour le trafic IP/MPLS (trafic de NR à NR, c'est-à-dire de routeur à routeur) et des « lambdas express » reliant directement 2 NR pour les besoins spécifiques d'un projet.

2.3 Le routage et la commutation

2.3.1 Routage ou commutation ?

Les services réseau sont fournis par les équipements de commutation et de routage. Sur l'ensemble des NR, le trafic est routé, c'est-à-dire que les paquets sont acheminés selon leur adresse IP de destination. S'il avait été envisagé à un moment de diminuer le nombre de points de routage pour diminuer les coûts, force a été de constater que cela aurait été un net recul technologique :

- Si les algorithmes de routage au niveau IP sont évolués, Ethernet ne se base que sur le protocole spanning-tree (STP⁶) et ses dérivés (RSTP⁷, PVST⁸...). Ce protocole se contente de bloquer un port en cas de présence d'une boucle. Avec des temps de convergence limités, STP ne permet pas d'optimiser l'usage des liaisons puisque seule une désactivation d'un lien est faite en cas de boucle (il n'y a pas de répartition de charge entre les diverses liaisons).
- La gestion du multicast IP est complexe au niveau Ethernet. Cette contrainte concerne sans doute davantage les opérateurs de contenus sur Internet, mais doit être prise en compte pour un réseau qui se veut être à la pointe de l'innovation en termes de services.
- Si la gestion d'un réseau IP est possible, le management d'un réseau Ethernet étendu à l'échelle d'un territoire reste un véritable challenge technique. Divers protocoles et mécanismes commencent à faire leur apparition sous l'appellation globale « Ethernet OAM⁹ », mais leur implémentation n'en est qu'à ses débuts et il n'y a pas réellement de bonnes pratiques dans ce domaine.
- La fourniture de services de circuits basés sur Ethernet peut se faire simplement via des tunnels Ethernet en mode Q-in-Q (802.1ad). Cette pratique est surtout mise en œuvre sur des infrastructures métropolitaines mais supporte mal le passage à l'échelle (limitation en nombre de VLANs, problématiques liées au STP...). Divers mécanismes émergent pour contourner ces difficultés comme le MAC-in-MAC (tunnels réels d'une trame Ethernet cliente dans une trame Ethernet d'opérateur) ou encore TRILL¹⁰ (adaptation d'IS-IS pour réaliser un IGP¹¹ performant au niveau d'un domaine Ethernet) mais ils ne sont pas encore largement adoptés ni même implémentés.

La nette diminution des coûts des plateformes de routage performantes chez la plupart des constructeurs a permis de conserver une infrastructure IP sur l'ensemble du réseau et de s'affranchir de ces contraintes. Pour pouvoir offrir des circuits (des VPN), MPLS a été déployé sur tous les NR. Largement adopté par les opérateurs, MPLS reste le protocole le plus fiable et le plus évolutif pour offrir des VPN.

Seuls les circuits à 10Gbit/s sur des lambdas dédiés pour des projets restent commutés à l'échelle de RENATER.

2.3.2 Les équipements

Plusieurs gammes d'équipements de routage ont été retenues pour RENATER-5 :

- Mise en place de commutateurs/routeurs CISCO 7600 pour la majorité des NR, sur lesquels des connexions d'usagers (sites ou réseaux de collecte) en 10 Gigabit-Ethernet sont prévues à court ou moyen terme. Ce type d'équipement s'est avéré être un excellent compromis entre les besoins en densité d'interfaces (notamment pour les projets de recherche à 10 Gbit/s) et les services disponibles. Principalement adapté aux infrastructures MPLS, ce commutateur/routeur offre également des fonctionnalités de métrologie avancées adaptées aux nombreux services déployés sur RENATER.
- Utilisation d'un routeur CISCO 12000-XR et d'un commutateur CISCO Catalyst 6500 sur les NR où il n'est pas prévu de raccordements d'usagers en 10 Gigabit-Ethernet. Il a été décidé de réutiliser les matériels RENATER-4 et de les mettre à jour pour supporter les nouvelles versions du système d'exploitation (système modulaire) et les débits RENATER-5. La densité de ports est assurée par le commutateur.

⁶Spanning Tree Protocol

⁷Rapid Spanning Tree Protocol

⁸Per VLAN Spanning Tree

⁹Operations, Administration, and Management

¹⁰Transparent Interconnection of Lots of Links

¹¹Interior Gateway Protocol

- Mise en place de tera-routeurs CISCO CRS-1 dans les NR de cœur de réseau (Paris et Lyon), ces tera-routeurs assurant également l'interconnexion avec les éléments extérieurs tels que GEANT, le SFINX et les fournisseurs de transit IP vers l'Internet. Sur chaque NR de cœur, un commutateur/routeur est également configuré pour l'accueil des connexions des usagers. Cette dissociation entre les routeurs de cœur et de bordure présente des avantages certains en termes d'exploitation et permet de mieux limiter les risques opérationnels.

2.3.3 L'architecture RENATER-5

La carte ci-dessous résume l'architecture physique de RENATER-5.

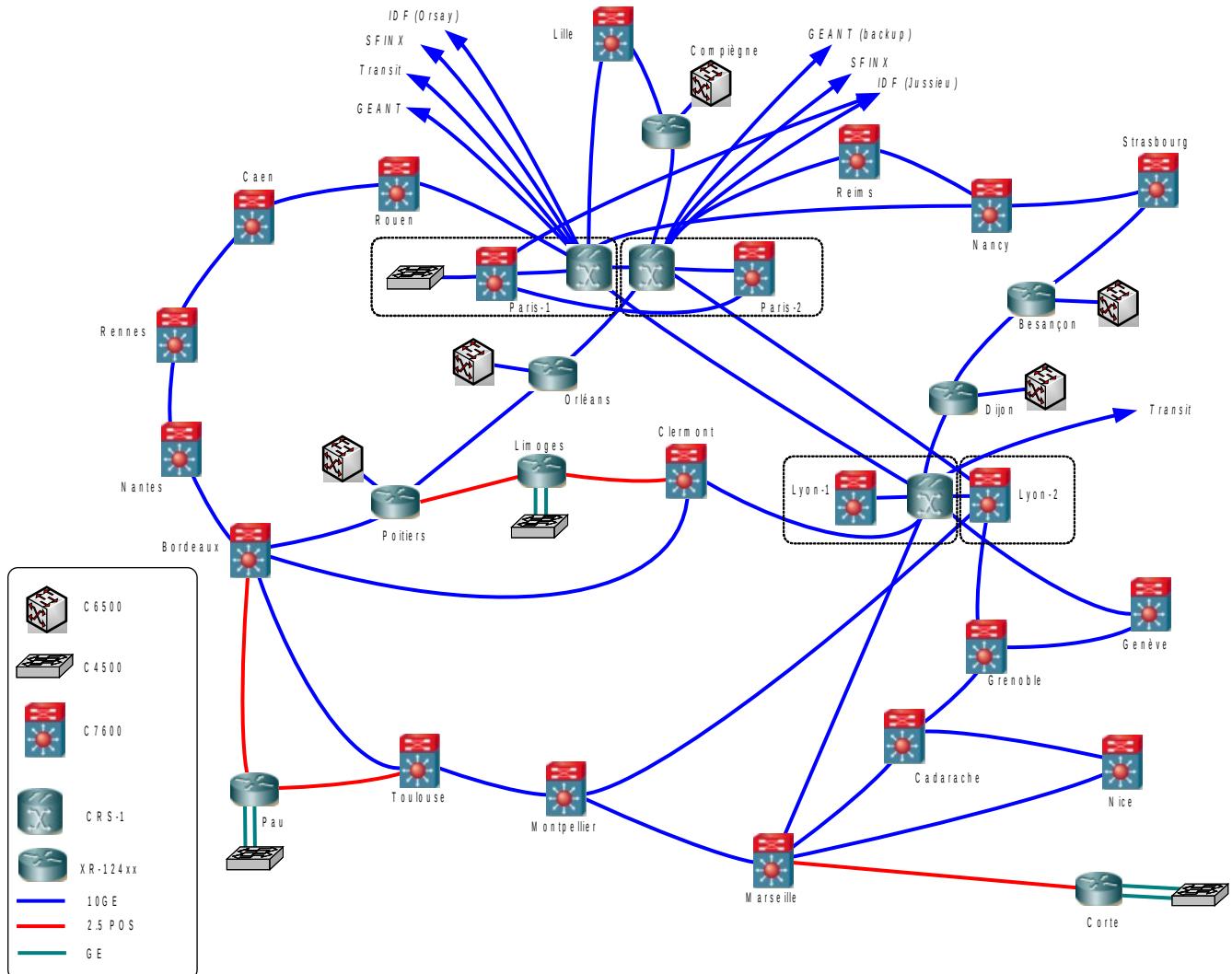


Figure 2 - L'architecture IP/Ethernet

2.3.4 Le routage sur RENATER-5

Cette section décrira succinctement les différents protocoles déployés avec leurs caractéristiques principales.

- IS-IS¹² reste l'IGP de RENATER. Configuré depuis RENATER-5 en mode « multi-topologie » il est maintenant possible d'avoir une non congruence pour les topologies IPv4 et IPv6. Si l'objectif reste de garder des topologies identiques pour les 2 versions du protocole de l'Internet, ce mode permettra de gérer plus facilement des exceptions s'il devait y en avoir à l'avenir.
- BGP-4¹³ est déployé sur l'ensemble du réseau pour les familles d'adresses IPv4 unicast, IPv4 multicast, IPv6 unicast, IPv6 multicast et IPv4 VPN :

¹²Intermediate System to Intermediate System (RFC 1142)

¹³Border Gateway Protocol (RFC 4271)

- Sur l'ensemble des NR, la totalité des routes de l'Internet (300 000 environ à la date de rédaction de l'article) est présente dans la table BGP.
 - BGP reste l'unique protocole de routage accepté pour l'interconnexion des sites¹⁴ usagers. Si les sites peuvent demander à recevoir seulement une route par défaut ou les préfixes des établissements RENATER, ils peuvent aussi demander la table complète si leurs matériels disposent de suffisamment de mémoire. Des communautés dites « de service » ont été généralisées¹⁵ et permettent à chaque site d'influer sur le routage effectué par RENATER en apposant simplement une ou plusieurs communauté(s) BGP prédefinie(s). Ces communautés sont d'autant plus intéressantes que de plus en plus les sites ou réseaux de collecte raccordés sur les NR le sont en double attachement. Il est alors possible de façon simple d'opter pour un mode de type primaire/secours ou encore partage de charge sur les différentes interfaces d'interconnexion.
- Au niveau iBGP, afin d'éviter un *full-mesh* entre tous les NR, 2 *route-reflectors* ont été configurés sur les CRS-1 de Paris1 et de Lyon1.
- Depuis RENATER-5, tous les NR sont configurés en *next-hop-self*. Ainsi le *next-hop* pour une route apprise d'un site n'est plus l'adresse IP du site sur son lien d'interconnexion avec RENATER, mais l'adresse IP de *loopback* du NR où le site est raccordé. Les avantages sont une simplicité de management et un temps de convergence optimisé dans le cœur de réseau.
- BFD¹⁶ permet avant tout d'améliorer les temps de convergence pour les sites raccordés sur RENATER à travers une infrastructure Ethernet. S'il est déployé par le site et RENATER, BFD permet de faire « tomber » rapidement le peering BGP du site en cas de problème IP indécelable au niveau des liaisons Ethernet (sans BFD, il faut attendre que le *holdtime* BGP soit expiré et plus d'une minute peut s'écouler avant que le peering ne « tombe »). BFD est également déployé sur les liens de cœur afin de se prémunir d'un problème au niveau IP qui ne serait pas vu au niveau physique.
- LDP¹⁷ est déployé en parallèle de l'IGP pour l'échange des informations sur les labels MPLS.
- PIM-SMv2¹⁸ est également déployé en parallèle de l'IGP pour permettre la construction des arbres de diffusion multicast (pour IPv4 et IPv6)
- MSDP¹⁹ permet l'échange des sources actives multicast IPv4 entre domaines PIM. Sur RENATER-5, MSDP n'est plus activé sur les routeurs de cœur mais sur 2 routeurs dédiés qui ne sont pas impliqués dans le routage des paquets. Ces 2 routeurs sont uniquement en charge de l'échange des sources actives avec les sites mais aussi avec le reste de l'Internet. Cette dissociation a stabilisé ce service sur RENATER et a surtout permis d'éviter que des routeurs de cœur soient impactés en cas de problèmes sur ce protocole qui reste délicat à administrer.

3 De RENATER-4 à RENATER-5

La migration complète vers RENATER-5 s'est étalée sur une période de 6 mois (de juillet à décembre 2008), avec déploiements consécutifs des liaisons, des équipements DWDM et enfin des routeurs avec les migrations des sites usagers. A chaque étape, une coordination avec les divers contacts des NR fut indispensable.

3.1 L'hébergement, là où tout commence...

Le réseau RENATER s'est considérablement transformé depuis sa création : multiplicité des opérateurs, présence d'équipements DWDM, routeurs, commutateurs... avec un impact direct sur les NR. Là où auparavant il suffisait d'une baie pour l'opérateur des liaisons et d'une baie pour les routeurs RENATER, il faut maintenant composer avec les baies DWDM, les arrivées de fibres optiques de chaque opérateur et les baies pour héberger les routeurs/commutateurs RENATER. Pour permettre les migrations dans les meilleures conditions, il est nécessaire de pouvoir installer les nouveaux équipements avant de démonter les anciens. Pour la migration RENATER-5, il a fallu composer avec autant de cas particuliers en élaborant à chaque fois les scénarios les moins impactant pour les usagers.

¹⁴RENATER connecte soit des sites ou des réseaux de collecte, fédérant les connexions des sites. Pour simplifier la lecture de l'article, l'auteur utilisera « site » indifféremment.

¹⁵<http://www.renater.fr/bgp>

¹⁶Bi-directional Forwarding Detection (draft-ietf-bfd-base-09)

¹⁷Label Discovery Protocol (RFC 3036)

¹⁸Protocol Independent Multicast – Sparse Mode (RFC 4601)

¹⁹Multicast Source Discovery Protocol (RFC 3618)

L'élément probablement le plus complexe à gérer lors d'une migration est l'arrivée des différentes fibres optiques. Chaque arrivée se trouve généralement dans une baie contenant des équipements optiques, le plus souvent installée par l'opérateur. Ces arrivées ne peuvent pas être déplacées aisément et représentent autant d'obstacles par la suite lorsqu'il est nécessaire de changer les équipements actifs. Pour lever ce verrou, il est fortement recommandé au sein de chaque NR de mettre en place une ou plusieurs baies « passives » pour les arrivées des câbles des opérateurs, avec une gestion interne des positions et de l'usage de chaque fibre. Ces points de démarcation, passages obligés des opérateurs, permettent aisément de modifier l'infrastructure par simple brassage de fibres.

Une nouveauté de RENATER-5 est aussi la construction de *shelters* sur deux liaisons dans le sud-est de la France. Les *shelters* sont des locaux techniques autonomes et isolés destinés à héberger des équipements permettant le plus souvent d'amplifier le signal optique. Sur une liaison terrestre classique le signal doit être réamplifié tous les 100 km environ même si l'architecture optique doit s'adapter le plus souvent aux contraintes du terrain. Si les opérateurs fournissent le plus souvent ces locaux techniques, les détenteurs de réseaux d'infrastructure tels les autoroutiers par exemple fournissent eux le terrain nu sur lequel doit être bâti le *shelter*. RENATER a donc dû se plier à cet exercice et faire réaliser puis installer deux locaux techniques climatisés avec les contraintes réglementaires et coûts associés.

3.2 Le déploiement DWDM

Le déploiement des équipements DWDM a été long et complexe. Tout d'abord les équipements DWDM ALCATEL-LUCENT déployés dans RENATER-4 ont dû être désinstallés, puis retournés au constructeur pour vérification, inventaire complet et calibrage, avant d'être redéployés sur les boucles Nord et Est du réseau RENATER-5. Entre le début des opérations de démontage et la remise en service complète des liaisons avec les nouveaux équipements CIENA, plusieurs semaines se sont écoulées. La coopération avec les projets utilisant les longueurs d'ondes à 10 Gbit/s a donc été nécessaire. Des circuits basés sur MPLS ont été configurés dans l'intérim pour remplacer les longueurs d'ondes « projets » mais avec un débit limité à 1 Gbit/s. Pour certains circuits critiques, pour lesquels il n'était pas envisageable d'avoir une telle coupure, les opérations ont été planifiées pour que l'impact ne soit pas supérieur à une journée. Compte tenu du nombre d'équipes d'installation disponibles et des contraintes de calendrier, ce type de migration a dû rester exceptionnel.

D'autres contraintes sont apparues liées aux amplificateurs Raman quand ils sont placés en entrée de ligne (*booster*). Avec ce type d'amplificateurs au gain très élevé, il ne doit pas y avoir plus de 2 ou 3 connecteurs sur les premiers kilomètres de la fibre (après l'amplificateur). Chaque connecteur réfléchit en effet une partie du signal optique et quand il y en a trop, l'amplificateur reçoit un signal réfléchi beaucoup trop important et cesse alors de fonctionner. Les amplificateurs Raman sont équipés de ce type de sécurité pour éviter les dommages corporels en cas de manipulation de la fibre (la puissance du laser en sortie de l'amplificateur est telle qu'une exposition aux rayons est dangereuse). Ce comportement inattendu a nécessité de revoir les fibres optiques en place et de limiter le nombre de connecteurs présents (remplacement par des soudures notamment).

3.3 Le déploiement des routeurs, des commutateurs et la migration des usagers

Si les déploiements des liaisons et des équipements DWDM ont été complexes, ils n'ont pas eu de conséquences pour les usagers connectés sur des routeurs et commutateurs. La migration de ces derniers équipements a nécessité plus de souplesse en termes de planning. La migration IP/Ethernet intervient en dernier lieu et subit les aléas des modifications de planning des phases précédentes. Aussi pour ces migrations, les étapes ont été les suivantes lorsqu'il a été possible d'installer le nouvel équipement sur le NR sans avoir à démonter l'ancien :

- Installation du nouvel équipement et interconnexion avec l'ancien en 10 Gigabit-Ethernet. Le nombre de cartes d'interfaces 10 Gigabit-Ethernet sur les équipements RENATER-4 étant limité, il a fallu pour la migration procéder à un véritable jeu de taquin et réutiliser les mêmes matériels sur plusieurs NR.
- Branchement des liaisons 10 Gigabit-Ethernet RENATER-5 sur le nouveau routeur et tests de connectivité sur 24 heures de chaque liaison au niveau IP.
- Mise en service des liaisons RENATER-5 puis résiliation et démontage des liaisons RENATER-4.

- Migration des usagers. Chaque réseau raccordé à RENATER est physiquement déconnecté de l'ancien équipement puis reconnecté sur le nouveau. Normalement cette opération ne doit engendrer une coupure que de l'ordre de la minute pour l'usager. Cependant après la migration il arrive régulièrement que la connexion ne soit pas fonctionnelle pour de multiples raisons (problème de négociation protocolaire, nécessité de vider le cache ARP sur le site distant, *peering* BGP à relancer sur le réseau client...). L'expérience montre que le comportement n'est pas déterministe en raison de la diversité des équipements et liaisons opérateurs. Plusieurs maintenances ont dû être replanifiées car des connexions de sites ne remontaient pas, avec impossibilité de joindre un contact technique sur le site distant. Une plus grande rigueur dans la prise de rendez-vous avec les usagers pour ces maintenances sera nécessaire pour garantir le succès des migrations de ce type à l'avenir.

4 Les services sur RENATER-5

Comme la plupart des réseaux de recherche, RENATER met à la disposition de ses usagers une infrastructure à la pointe de la technologie mais également un portefeuille de services.

4.1 La connectivité, la base pour bâtir des services

4.1.1 Services IP

RENATER fournit en natif tous les services IP : IPv4 et IPv6, à la fois pour l'unicast et le multicast. Le service qui reste très majoritairement utilisé sur RENATER est l'accès Internet classique, qui repose sur le protocole IPv4. IPv6, la nouvelle version du protocole de l'internet, est indispensable à la croissance des usages (le nombre d'adresses IPv4 étant limité). Le service IPv6 est offert en natif sur RENATER depuis 2003. Certains réseaux de collecte en région le transportent également et un nombre croissant de sites l'utilisent. En Europe, les réseaux de la recherche supportent tous le protocole IPv6 en mode natif.

Sur RENATER le service multicast IP (IPv4 et IPv6) permet une diffusion optimale d'une source vers un ensemble de destinataires avec réplication au sein du réseau. Le multicast est adopté très largement par les opérateurs pour la diffusion de contenus multimédias.

4.1.2 Circuits de bout en bout (VPN²⁰ MPLS²¹, longueurs d'ondes...)

Une offre de circuits dédiés est également disponible. Cette offre repose sur des technologies diverses (MPLS, Ethernet sur DWDM...).

Il faut distinguer les circuits point-à-point qui consistent à offrir un service d'interconnexion privée entre 2 établissements, des circuits multi-point à multi-point qui permettent d'interconnecter au sein d'un même réseau privé plusieurs sites RENATER. Pour chaque demande, le GIP RENATER propose la solution technique la plus à même de construire le circuit en fonction des services qui doivent être véhiculés dans le circuit (IPv4, IPv6, multicast...), du débit demandé...

Dans tous les cas, l'interface de raccordement reste sur le commutateur ou le routeur du NR (même pour un circuit dédié à 10 Gbit/s). S'il peut être objecté que la présence d'un équipement de commutation/routage de RENATER vient en opposition avec le besoin d'un circuit dédié, ce choix comporte de nombreux avantages pour les usagers :

- Diminution du nombre de ports nécessaires pour le raccordement d'un usager aux divers services (un site peut à travers une seule interface de type 10 Gigabit-Ethernet bénéficier à la fois d'un « lambda » dédié mais aussi d'un service IP). Chaque service est disponible via un VLAN dédié.
- Flexibilité dans les modifications d'architecture. En cas de demande de modification de la part de l'usager, il n'est pas nécessaire de revoir le câblage ou de provisionner de nouvelles interfaces : la construction d'un nouveau VLAN suffit la plupart du temps. Dans le cas où un circuit à 10 Gbit/s serait indisponible (en raison d'une coupure de fibre par exemple), il est alors possible de bâtir temporairement un L2VPN²² basé sur MPLS via la création d'un nouveau VLAN de service.
- Les équipements configurés sur RENATER-5 sont dimensionnés pour pouvoir absorber la charge de trafic susceptible d'être véhiculée sur les circuits sans risquer de diminution de performance.
- La résolution de problèmes de performance est grandement simplifiée. Les équipements optiques ne fournissant généralement pas d'indicateurs sur le trafic transporté, des statistiques sont ainsi disponibles au niveau Ethernet sur les équipements RENATER.

D'ici juin 2010, une évolution est à prévoir sur les VPN de niveau 3 pour le support du protocole IPv6 et du multicast IPv4. Aujourd'hui, pour ces VPN, seul le transport de l'unicast IPv4 est possible. Des VPN de niveau 2 sont en attente configurés pour les sites nécessitant le transport de ces protocoles.

²⁰Virtual Private Network

²¹Multiprotocol Label Switching

²²Layer 2 VPN

VPLS²³, service de VPN multi-point à multi-point (MPtMP) de niveau 2, n'est pas disponible sur RENATER-5. Le coût nécessaire pour son déploiement est considérable pour des besoins quasiment nuls, qui de surcroit peuvent presque toujours être satisfaits via d'autres technologies.

4.1.3 Classes de service

Depuis plusieurs années, diverses classes de service sont définies sur RENATER pour l'ensemble des établissements. En marquant les paquets un établissement peut influer sur la prioritisation des flux acheminés au sein de RENATER. Des classes de service sont par exemple définies pour la téléphonie ou la visioconférence. Les flux voix, plus sensibles à la gigue, doivent par exemple être traités en priorité.

Avec RENATER-5, l'implémentation des classes de service sur le réseau a dû être intégralement revue. Tout d'abord l'augmentation de la capacité des liens de cœur rend improbable toute congestion, même en cas de re-routage. Dans ce contexte la prioritisation est surtout nécessaire à l'accès mais là encore les interfaces sont le plus souvent largement dimensionnées en termes de débit. Les équipements RENATER-5 étant variés, la configuration de la QoS²⁴, très dépendante du matériel, a dû être repensée. Le faible usage des différentes classes de service de RENATER-4 a aussi montré qu'un ajustement de la politique de QoS devait être réalisé.

Dans ce contexte, des études ont été entreprises et devraient permettre d'ici la mi-2010 les améliorations suivantes :

- ouverture, pour la téléphonie, de la classe Premium (classe EF²⁵) à l'ensemble des établissements connectés à RENATER. Cette classe pourra être utilisée à hauteur de 10% du débit du site ;
- prioritisation en sortie de RENATER vers les sites ;
- gestion de la QoS pour les services de L2VPN, L3VPN et pour les longueurs d'ondes 10 Gbit/s dédiés.

4.2 Les services aux usagers

Avec un réseau à très haut débit, plus fiable, et extensible en termes de services, il est possible de s'intéresser davantage aux usages. Dans cette optique, le GIP RENATER a évolué et revoit son offre en termes de services aux usagers au-delà de la problématique de connectivité. Cette évolution, qui a débuté en douceur il y a 3 ans environ, s'est grandement accélérée et la gamme de services a augmenté.

Le GIP RENATER offre dorénavant, seul ou en coopération avec le CRU et l'UREC, un service de nomadisme avec eduroam, un service d'authentification unifié avec la fédération Education-Recherche, des certificats serveurs, un service anti-spam mutualisé, des services de visioconférence (H323 et EVO²⁶) ainsi qu'un service pilote de téléphonie sur IP. Tous ces services sont fournis dans le but de fédérer les efforts réalisés individuellement par chaque établissement de la communauté.

- Une solution ouverte de *web-conferencing* appelée EVO est disponible pour tous les usagers de RENATER. Les réflecteurs installés sur le cœur du réseau RENATER permettent une mise en relation performante des participants.
- RENATER propose un service national d'interconnexion de « Gatekeepers H323 » pour l'interconnexion de systèmes de visioconférence. Ce service permet non seulement la mise en relation des établissements via leur préfixe téléphonique mais également l'accès aux terminaux des autres réseaux de la recherche via GDS²⁷.
- Depuis le 1^{er} octobre, un service anti-spam 9 est proposé par RENATER à l'ensemble des établissements connectés au réseau (et donc titulaires d'un agrément RENATER). Ce service se présente sous la forme d'un relais de messagerie mutualisé intervenant en amont des serveurs de messagerie des sites, effectuant un premier niveau de filtrage anti-spam et, en option, d'analyse anti-virus pour les messages à destination des utilisateurs des sites raccordés.
- RENATER, en coopération avec le CRU²⁸ et l'UREC²⁹, met à la disposition de sa communauté des certificats serveurs (service basé sur une offre de TERENA appelée TCS³⁰)
- La fédération Education-Recherche 9, gérée en partenariat avec le CRU, offre un cadre technique et de confiance permettant à ses participants de sécuriser l'accès à des ressources Web via les mécanismes de fédération d'identités. Elle met en relation des organismes proposant des ressources web (applications, portails, documents...) avec d'autres organismes gérant les identités d'utilisateurs accédant à ces ressources : les fournisseurs d'identités. Elle permet aux utilisateurs finaux de réduire le nombre de

²³Virtual Private LAN Service

²⁴Quality of Service

²⁵Expedited Forwarding

²⁶Enabling Virtual Organizations - <http://evo.caltech.edu>

²⁷Global Dialing Scheme

²⁸Comité Réseau des Universités

²⁹Unité Réseaux du CNRS

³⁰TERENA Certificate Service

mots de passe à retenir, étend les bénéfices de *Single Sign On* jusqu'à des applications hébergées en dehors de leurs institutions et offre à ces dernières une meilleure maîtrise de la diffusion de données à caractère personnelle.

- Un service pilote d'interconnexion d'IPBX³¹ 9 permet depuis peu aux établissements RENATER de réaliser leurs communications téléphoniques sur IP en s'affranchissant ainsi des coûts associés. Basé sur le protocole SIP, ce service ne permet pour le moment que la communication entre les sites raccordés. Chaque établissement conserve un accès RTC³² pour les autres appels.

- Eduroam, qui signifie "Education Roaming" est une infrastructure basée sur la norme 802.1X et sur le protocole client/serveur RADIUS³³ pour permettre un nomadisme international au sein de la communauté Recherche et Enseignement. Ce service est opéré par le CRU.

Les informations complètes pour tous ces services sont disponibles depuis sur la page web suivante : <http://www.renater.fr/services>

5 Conclusion

Avec RENATER-5, la communauté Recherche et Education en France dispose non seulement d'un réseau performant et évolutif, mais aussi d'une base solide permettant d'offrir davantage de services. C'est surtout sur ces derniers que des avancées majeures sont à prévoir pour les années à venir.

Bibliographie

- [1] F. Simon, S. Aumon, JL Munier, Le service antispam de RENATER est arrivé. Dans Actes du congrès JRES2009, Nantes, Décembre 2009.
- [2] M. Hached, O. Salaün, Shibboleth et la haute disponibilité. Dans Actes du congrès JRES2009, Nantes, Décembre 2009.
- [3] S. Muyal, B. Tuy, Service pilote de téléphonie sur IP (ToIP) dans RENATER. Dans Actes du congrès JRES2009, Nantes, Décembre 2009.

³¹Internet Private Branch Exchange

³²Réseau Téléphonique Communauté

³³Remote Access Dial-In User Service