

Rapport de Stage de fin d'études

Aristote - Renater



Renater

Naël HAMAMEH

5^{ème} année INSA de Lyon - Département Télécommunications

« Plus on sait, et plus on est capable d'apprendre. »

Alain (1868-1951), philosophe français

Stage : n. m.

« Période d'études pratiques dont les aspirants à certaines professions doivent justifier pour être admis à les exercer. »

Dictionnaire Universel Francophone

TABLE DES MATIERES

Remerciements

1/ Introduction

- A/Le contexte
- B/Le sujet du stage
- C/Les acteurs d'IPv6

2/JRES 2003

- A/Présentation JRES
- B/Le tutoriel IPv6
- C/La plate-forme
- D/Autoconfiguration
- E/DNS
- F/Serveur Web
- G/Videoconference
- H/Planification de l'évènement
- BILAN

3/Multicast

- A/Les protocoles
 - A-1)Adresses Multicast
 - A-2)MLD
 - A-3)PIM
 - A-4)MBGP
- B/M6Bone
 - B-1)Présentation du M6Bone
 - B-2)Les différents déploiements
 - B-3)Mes actions au sein de l'équipe M6bone :

Conclusion

Bibliographie

Annexes

Rapport des humanités

Remerciements

Je tiens à remercier mes tuteurs de stage : Bernard Tuy (GIP RENATER, président du G6) et Jacques Prévost (GIP RENATER, Trésorier de l'Association Aristote) qui, m'ont accompagné tout au long de mon stage. Je tiens également à remercier Jérôme Durand (GIP RENATER) avec qui j'ai eu plaisir à travailler.

Je remercie toutes les personnes qui ont contribué à la réalisation de la plate-forme de démonstration des JRES 2003 et plus particulièrement Yves LegrandGerard (DESS ART Paris-7), Thomas Carlu (CRIHAN) et Elba Burity (INRETS).

Je remercie Farid Naït, grâce à qui j'ai eu connaissance du stage, ainsi que Omar Gaouar, mon tuteur de stage à l'INSA de Lyon.

Enfin, je remercie l'ensemble de l'équipe du GIP RENATER, qui m'a permis d'effectuer mon stage dans un cadre particulièrement agréable et enrichissant.

1/INTRODUCTION

A. Le contexte

Je suis étudiant en dernière année au département Télécommunications de l'INSA de Lyon. Le cycle ingénieur au sein du département « *Télécommunications, Services et Usages* » comprend une période de stage de 6 mois au cours de la dernière année. Ce stage a pour vocation de préparer l'élève ingénieur au monde du travail et favoriser un environnement de première expérience professionnelle.

C'est donc dans ce cadre que j'ai effectué un stage de 6 mois au sein du GIP RENATER à Paris. Je vais, à présent, vous expliquer le travail que j'y ai effectué dans le rapport qui suit.

B. Le sujet de stage

Mon stage s'est déroulé dans le cadre d'un partenariat entre l'association Aristote, et le GIP RENATER. Administrativement, j'étais rattaché à l'association Aristote, mais le stage a été effectué dans les locaux du GIP RENATER, à Paris, ENSAM. Mes tuteurs étaient Jacques Prévost (Association Aristote) chargé des applications avancées comme la visioconférence, et Bernard Tuy, responsable de l'équipe SIPA (Services IP Avancés). J'ai également travaillé sous l'encadrement de Jérôme Durand pour les actions relatives au Multicast.

Voici le sujet de stage initial tel qu'il a été défini dans la convention de stage :

« Développement et mise en œuvre de la plate-forme de démonstration IPv6 incluant des logiciels d'applications IPv6. »

Lorsque j'ai commencé mon stage, plusieurs mois après la signature de la convention, nous avons « affiné » le sujet de stage qui comportait désormais 2 axes principaux :

- Mise en place de la plate-forme de démonstration IPv6 de RENATER lors de la semaine des JRES 2003 de Lille.

La mise en place d'un réseau de démonstration pour les JRES 2003 consistait à préparer une plate-forme en IPv6 qui servirait de support à un tutoriel à destination des administrateurs réseaux venus au JRES 2003 afin de leur montrer des exemples de configurations des routeurs, des machines et des services en IPv6.

- Participer à la supervision et développement du M6Bone, réseau de test Multicast IPv6

La partie sur le Multicast IPv6 s'inscrit dans la continuité de ce qui a été fait par Jérôme Durand, Pierre-Emmanuel Goiffon et Ahmed Sahnoun qui ont effectué leur stage de fin d'étude dans le même cadre que moi. Le but était de contribuer au développement du réseau : connexion de nouveaux sites, configuration de routeurs, développement de scripts de supervision, communication avec les usagers...

C. Les acteurs d'IPv6

1.G6

Le G6 est une association Loi de 1901 qui s'est fixé pour objectifs de favoriser le développement et le déploiement de la nouvelle version du protocole de l'Internet : IPv6. En décembre 1995, les premières spécifications de IPv6 étaient tout juste publiées. Quelques - encore rares- personnes en France s'intéressaient alors à cette nouvelle version du protocole IP. C'est de la rencontre aux JRES de Chambéry (Novembre 1995) et de la volonté commune de B. Tuy (UREC) et de A. Durand (IMAG) que naît le G6, groupe français d'expérimentation IPv6. Il cherche à regrouper les expérimentateurs de IPv6 en France pour les aider à partager leurs expériences et commencer à coordonner des actions communes.

Les partenaires de la première heure appartenaient aussi bien au monde académique qu'industriel : la première réunion du groupe a lieu au mois de Janvier 1996. Elle regroupait des personnes de l'IMAG, de l'INRIA, de l'UREC, et de BULL et DASSAULT Electronique. L'association G6 est née de ce groupe informel en Janvier 2000.

Aujourd'hui, La diversité de ses membres s'est accentuée puisque des associations peuvent adhérer au G6. Ses acteurs se sont donnés pour charte :

- l'échange d'expériences avec IPv6
- l'établissement de plates-formes d'expérimentations
- la construction et l'administration d'une infrastructure IPv6 en France
- la diffusion d'information sur IPv6
- les relations avec les différents groupes de travail (RIPE, IETF, IOL ...)
- la conduite d'expérimentations dans le cadre de projets nationaux ou internationaux
- la mise en oeuvre d'un réseau national IPv6 natif (RENATER 3)

Pour en savoir plus : <http://www.g6.asso.fr>

2. GIP RENATER

Le GIP RENATER réunit de grands organismes de recherche et d'enseignement, ainsi que le ministère en charge de l'Education Nationale, de la recherche et de la technologie, pour développer et faire fonctionner le réseau RENATER.

Un GIP (groupement d'Intérêt public) est un organisme à but non lucratif, réunissant des administrations de l'Etat et des organismes publics pour une activité définie : dans le cas du GIP RENATER il s'agit du réseau RENATER.

Le GIP RENATER est le maître d'ouvrage de la partie commune de RENATER, constituée de son épine dorsale RENATER 3, des liaisons internationales, de ses actions pilotes, et du service SFINX, qui est un GIX (Global Internet eXchange), point d'échange de trafic Internet entre prestataires de services Internet, ou opérateurs de télécommunications qui veulent échanger du trafic, sans transit et sans passer par des infrastructures internationales

Le GIP RENATER est également le coordinateur technique et opérationnel global de l'ensemble du réseau RENATER y compris ses éléments régionaux. Il représente le réseau RENATER auprès des institutions françaises et étrangères, et notamment auprès des autres réseaux de la Recherche.

Le directeur du GIP RENATER est M. Dany Vandromme, professeur à l'INSA de Rouen ; L'équipe du GIP RENATER comprend aujourd'hui un peu moins de 30 de personnes : ingénieurs, techniciens et personnel administratif répartis entre Paris et Montpellier.

3. RENATER

RENATER (Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche) a été créé dans les années 1990 dans le but de fédérer et d'organiser les infrastructures de télécommunications pour l'Education, la Recherche et l'Enseignement.

Aujourd'hui, plus de 600 sites sont raccordés au réseau RENATER. Ceci leur permet de communiquer entre eux, d'accéder aux centres de recherche publique et privés, aux établissements d'enseignement du monde entier via l'Internet.

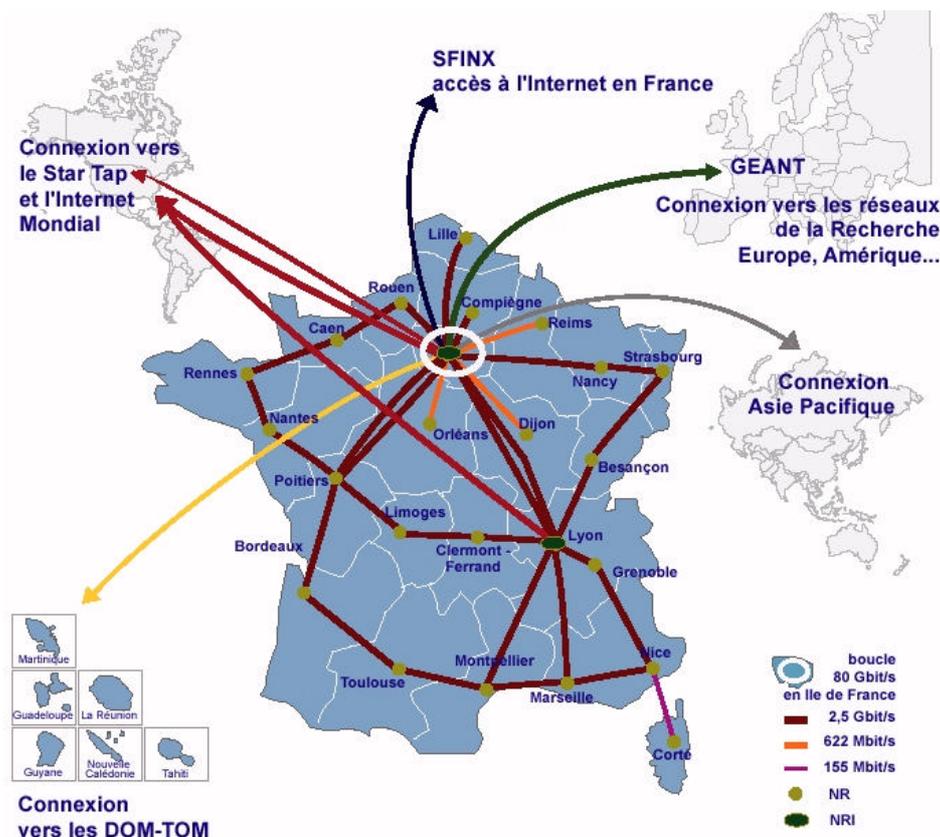
Le réseau RENATER est composé d'une infrastructure métropolitaine et de liaisons internationales à haut débit. Des points de présence de RENATER sont également implantés dans les départements d'Outre Mer. RENATER est basé sur une architecture distribuée : il comprend une épine dorsale nationale à haut débit multi-Gbit/s - RENATER 3 - qui fédère des réseaux de collecte régionaux développés avec le soutien des collectivités territoriales dans le cadre de l'aménagement du territoire.

RENATER est interconnecté à 2.5 Gbit/s aux autres réseaux de recherche européens et américains via le réseau pan-européen GEANT. Une liaison directe de 155 Mbit/s avec les Etats-Unis est exclusivement dédiée à certains projets de recherche prioritaires qui peuvent ainsi communiquer efficacement avec leurs partenaires nord-américains via les réseaux des grands organismes scientifiques des Etats Unis (vBNS, ESNET) à travers le nœud de communication scientifique STAR TAP à Chicago. Une liaison de 40 Mbit/s aboutissant en Corée assure la communication avec les réseaux de la recherche de la zone Asie-Pacifique.

La communication avec l'Internet, en France, est réalisée par le SFINX, un point d'échange entre les opérateurs, auquel RENATER est relié à 1 Gbit/s. La communication avec l'Internet dans le reste du monde est assurée par le raccordement de RENATER à 2.5 Gbit/s à l'épine dorsale Internet mondiale OpenTransit de France Télécom.

Avec la version 3 de RENATER, les débits des liaisons de l'épine dorsale sont presque partout de 2,5 Gbit/s. Ces liaisons sont – presque partout – organisées en boucle : ceci augmente la disponibilité en cas d'incident – il y a toujours un chemin de secours disponible – et facilite la mise en place de liaisons de voisinage entre régions. Ces débits atteignent même 80 Gbit/s en Ile de France.

Voici la carte de RENATER 3 :



Au niveau des points d'accès régionaux de son épine dorsale, RENATER 3 propose de nombreux services :

- **un service IPv4** permettant d'accéder aux communautés de la recherche et de l'enseignement, nationales et internationales ainsi qu'à l'Internet
- **un service de diffusion IPv4 (IP Multicast)**, utilisée pour la visioconférence et le téléenseignement interactif
- **un service IPv6**, utilisé par les universités pour préparer la migration de IPv4 vers IPv6, ainsi que par de nombreux projets de recherche et développement.

IPv6 est la nouvelle version du protocole IP de l'Internet. En Europe, les réseaux de la recherche sont très actifs pour préparer et commencer cette migration, et proposer un service IPv6 pour les expérimentations des premiers utilisateurs. RENATER est au premier plan de cette évolution : dans RENATER 3, il y a un service IPv6 natif, c'est à dire placé sur le même plan que le service IPv4.

IPv6 est conçu pour s'affranchir des limitations d'IPv4 (pénurie d'adresse IPv4, explosion des tables de routage...), mais aussi pour prendre en compte les avancées issues des recherches sur les réseaux, comme l'auto configuration, la mobilité, le Multicast ou encore la sécurité.

Pour en savoir plus : <http://www.RENATER.fr>

4. Association Aristote

Créée de manière informelle en 1984 par l'INRIA, le CEA, EDF et le CNES, formalisée en 1988, l'Association Aristote regroupe de grands organismes ou entreprises français intéressés comme acteurs ou comme utilisateurs à l'évolution des télécommunications de transmissions de données.

L'objectif d'Aristote se situe dans le domaine des technique, moyens, outils et services de communication informatique, notamment :

- mettre en commun des efforts de prospective, d'étude et d'information faits par ses membres.
- promouvoir l'élaboration et la mise en service de nouveaux produits, systèmes et services d'intérêt général au bénéfice de ses partenaires. Cette activité se déroule dans le cadre des groupes de travail techniques d'Aristote.
- organiser ou encourager des actions avancées d'information ou de formation: séminaires d'intérêt général, séminaires de formation technique, journées d'étude thématiques.

L'association Aristote est un acteur important dans le développement et dans la diffusion de connaissances concernant les nouvelles technologies de l'information et de la communication.

Pour en savoir plus : <http://www.aristote.asso.fr>

5. GN6

De nombreux organismes de la communauté des utilisateurs de RENATER désirent actuellement démarrer de petits réseaux IPv6 dans leurs organismes : cela leur permettra d'acquérir l'expertise nécessaire, et d'étudier concrètement divers aspects techniques et opérationnels de l'introduction de IPv6. Ainsi, ils pourront ensuite planifier dans de bonnes conditions le passage de IPv4 vers IPv6.

Pour les aider et les accompagner tout au long de cette démarche, le GIP RENATER a mis en place avec eux le Groupe des Néophytes IPv6 : le GN6.

Le GN6 est un groupe de travail qui met ensemble des acteurs « réseau » des organismes de la communauté RENATER : organismes utilisateurs de RENATER, réseaux de collecte de RENATER, réseaux ou organismes étrangers qui ont une convention de coopération avec le GIP RENATER.

Ses objectifs sont notamment :

- permettre de s'initier à la mise en œuvre de IPv6 et de ses applications de base,
- faciliter, par des échanges d'information et des retours d'expérience systématiques, le démarrage de réseaux pilotes IPv6 – qui pourront être connectés au service IPv6 de RENATER - dans les organismes,
- faciliter, dans les mêmes conditions, la participation aux actions pilotes menées par le GIP RENATER et/ou le G6, par exemple IPv6 Multicast ou DNSsec.
- faciliter l'accès aux connaissances des experts, notamment ceux du GIP RENATER et de l'Association G6.

Démarré mi-2002, le GN6 comporte déjà une vingtaine de personnes, et se réunit tous les deux mois. Certains de ses membres, éloignés de quelques milliers de kilomètres, participent régulièrement aux réunions en visioconférence sur IPv6.

Pour en savoir plus : <http://www.RENATER.fr/Evenements/200210GN6/index.htm>

2/JRES 2003

A /Présentation des JRES

Depuis 1995 et tous les 2 ans, le CRU, RENATER et l'UREC organisent les journées réseaux JRES. Ces journées francophones s'adressent à tous ceux qui, dans les établissements d'enseignement supérieur et de recherche, contribuent au déploiement et à l'essor des nouvelles technologies pour l'information et la communication : les architectes réseaux, les administrateurs systèmes et réseaux, les responsables de projets, les développeurs et les utilisateurs. Ces journées permettent aux participants de parfaire leurs connaissances, d'en acquérir de nouvelles, de dialoguer et de partager leurs expériences.



Pour les JRES 2003, le CRU, RENATER et l'UREC ont confié l'organisation à l'Université des Sciences et Technologies de Lille, à l'Université de Valenciennes et du Hainaut-Cambrésis et au Pôle Universitaire de Lille.

Dans un contexte de perpétuelle évolution des technologies, de déploiement en masse des accès et des applications pour l'enseignement supérieur et la recherche, les JRES ont pour ambition de présenter un panorama très complet des technologies, des services, des usages et des stratégies dans le monde des réseaux.

Les précédentes journées se sont tenues à Chambéry en 1995, à la Rochelle en 1997, à Montpellier en 1999 et à Lyon en 2001. Cette année, cet événement s'est déroulé du 17 au 21 Novembre 2003 au Grand Palais de Lille.

Pour en savoir plus : <http://www.jres.org>

B/ Le tutoriel IPv6

Le programme des JRES comprenait des tutoriaux le lundi puis des présentations en amphithéâtre du mardi au vendredi. En outre, entre 2 présentations, on pouvait visiter des sessions posters et des expositions. Quatre tutoriaux étaient proposés aux participants : VPN, Web Services, Sécurisation de la messagerie électronique et IPv6. J'étais chargé de la préparation de la plate-forme qui a servi de support à ce dernier tutoriel.

Le tutoriel IPv6 avait pour objectif de fournir aux participants des informations pratiques pour installer un réseau IPv6 dans leur environnement de travail (laboratoire, campus, ...). Pour ce faire, le tutoriel s'est appuyé sur les expériences acquises depuis plus d'un an.

Il a principalement reposé sur un ensemble de démonstrations présentées pas à pas, dont les configurations étaient détaillées en fonction du niveau de connaissances des participants.

Le tutoriel s'adressait à des personnes déjà familières d'une façon ou d'une autre avec IPv6. Soit parce qu'elles l'enseignent, soit parce qu'elles ont déjà l'occasion de mettre en oeuvre certaines de ses fonctionnalités. Nous avons donc fait en sorte que les rappels sur le protocole soient très succincts, pour privilégier l'aspect pratique des mises en oeuvre démontrées. En effet, l'auditoire visé est celui des administrateurs réseaux des laboratoires, campus et réseaux de collecte désireux de mettre IPv6 en oeuvre au profit de leurs usagers.

Les démonstrations portaient notamment sur :

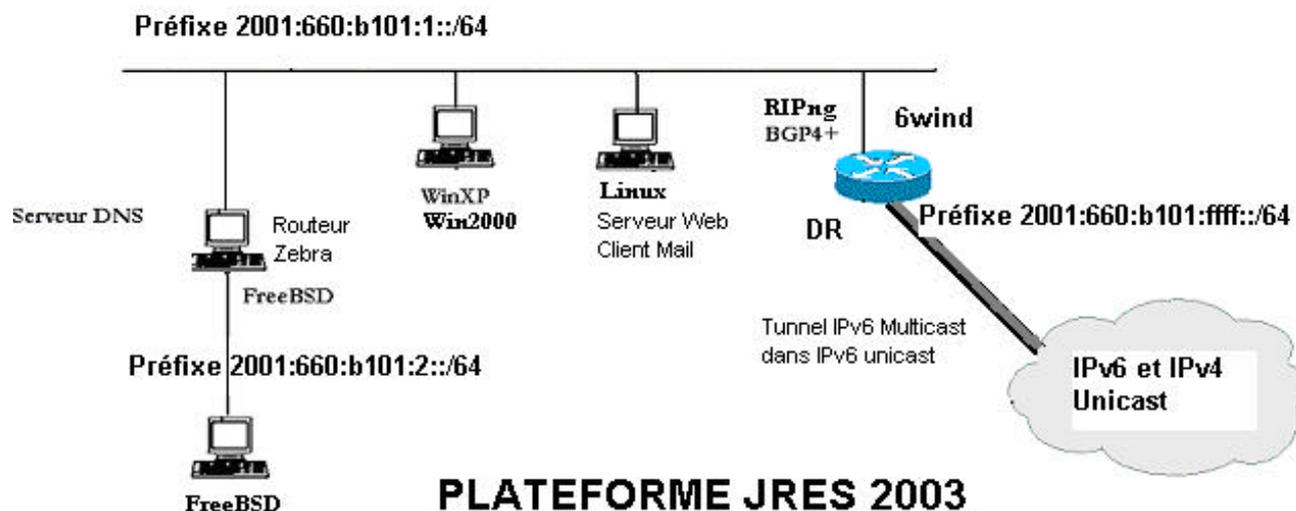
- auto configuration des équipements terminaux : Neighbor Discovery (RFC 2461)
- configuration des équipements intermédiaires
- routage : RIPng (RFC 2080), MBGP (RFC 2283), *OSPFv3 (RFC 2740)*
- Mise en oeuvre des services de base :
 - + DNS (statique et mise à jour dynamique sécurisée)
 - + Web (serveur et client)
 - + *Mail (client)*
- Mise en oeuvre de services avancés
 - + *configuration du Multicast*
 - + *vidéoconférence*

Pour réaliser la plate-forme IPv6, support de ce tutoriel, j'ai été encadré par Monsieur Yves Legrandgérard, enseignant au DESS ART de l'université de Paris 7. C'est également lui qui a animé le tutoriel et qui s'est chargé de la partie sur le DNS.

En Italique, est indiqué ce qui est été initialement prévu mais qui n'a pas pu être montré lors du tutoriel. La configuration du Multicast et la vidéoconférence ont été montrés sur le stand de RENATER les jours suivants le tutoriel.

C/ La plate-forme.

Ci-dessous le plan de la plate-forme IPv6 à mettre en place tel qu'il m'a été présenté au départ:



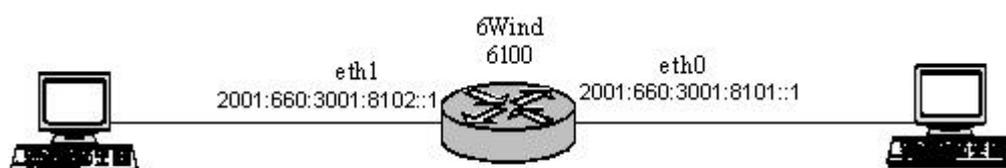
J'avais donc six semaines pour faire en sorte que cette plate-forme soit opérationnelle pour les JRES 2003 à Lille.

Dans un premier temps, j'ai décidé de me familiariser avec les différents équipements et logiciels et d'apprendre à tout faire fonctionner de façon isolée avant de tout assembler. Afin de permettre un confort de lecture optimal, j'ai volontairement évité de rentrer dans le détail des configurations dans les pages qui suivent. Néanmoins, les lecteurs intéressés pourront retrouver les configurations commentées en annexe, dans les dernières pages de ce rapport.

C-1/ Le routeur 6WIND 6100

6WIND est un constructeur de routeurs IPv6. Pour me familiariser avec les configurations et les commandes du 6WIND, j'ai repris des TP qu'avaient fait des anciens stagiaires. En effet, j'ai commencé par une topologie très simple : un routeur et 2 PC, un sur chaque branche.

L'objectif était simplement de faire communiquer les 2 stations. Mais pour cela, il fallait connaître les commandes du 6WIND qui sont différentes de celles des routeurs CISCO. Dans l'annexe, j'ai référencé les principales commandes à connaître pour configurer un routeur 6WIND.



C-2) L'OS FreeBSD

En cours, j'avais déjà eu l'occasion de travailler avec des machines Linux (Red Hat et Mandrake notamment) mais jamais avec une machine BSD. Or, il se trouve que la pile IPv6 Kame a été développée pour BSD. J'ai dû donc apprendre à installer FreeBSD sur un PC et commencer à me familiariser avec les commandes FreeBSD, parfois différentes de Linux. En effet, le fichier dans lequel on configure une machine BSD est **/etc/rc.conf**. Soit on édite le fichier avec « **vi** » soit on utilise l'interface de post-installation de l'OS en tapant : **sysinstall** . J'ai mis en annexe les commandes utiles.

C-3)Le routeur Zebra

Zebra est un routeur logiciel GPL donc gratuit qui présente notamment l'avantage d'offrir une interface similaire à celle d'un routeur Cisco. Je l'ai donc installé sur la machine FreeBSD et la prise en main a été très rapide puisque j'avais l'impression de travailler sur un routeur Cisco.

Zebra fonctionne de la manière suivante : un démon est lancé pour chaque protocole de routage. Il y a donc un démon **ripng**, un démon **bgp** etc... et un démon **zebra** supervise les autres démons.

Donc pour configurer le routeur on lance « **telnet** » en local sur le port correspondant (2601 pour **zebra**, 2603 pour **ripng** etc...) :

telnet localhost 2601

Une autre solution est de modifier directement le fichier de configuration avec un éditeur comme **vi** :

vi /usr/local/ripngd.conf

Ensuite, pour lancer le démon :

ripngd -d

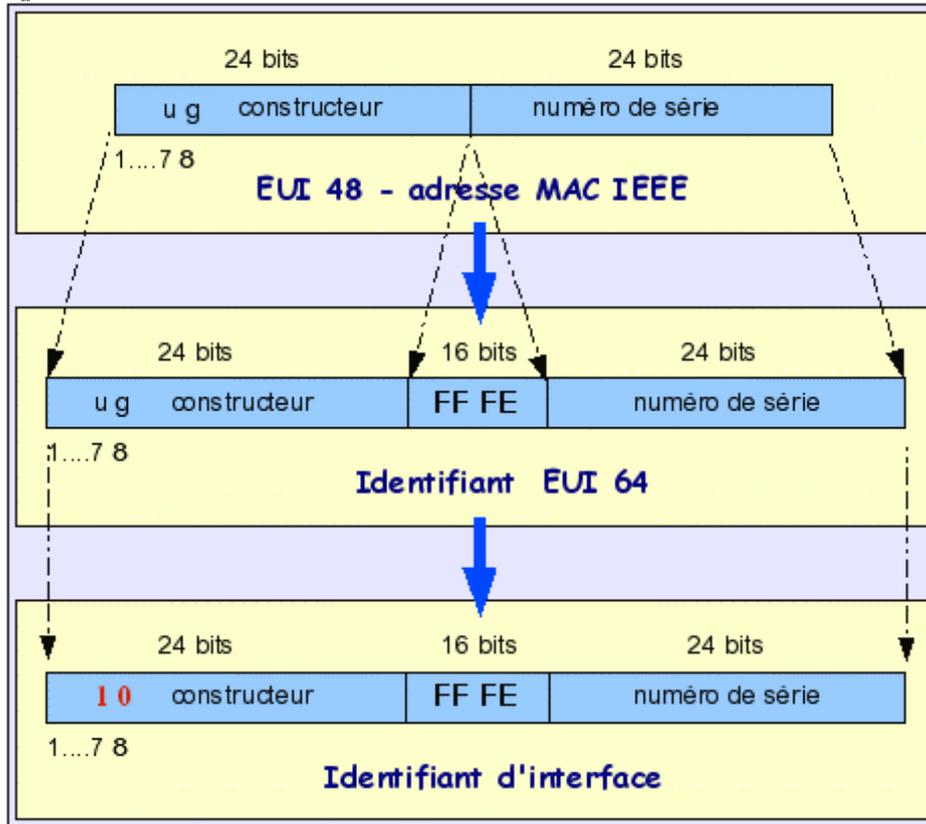
D) Autoconfiguration

L'autoconfiguration a été un point central à montrer lors du tutoriel. Ci-dessous, j'en explique la théorie. L'autoconfiguration est réalisée par le protocole de découverte des voisins « neighbor discovery (RFC 2461) » qui permet à un équipement de s'intégrer dans l'environnement du lien local et qui met en œuvre plusieurs fonctionnalités pour permettre la configuration automatique d'un équipement. L'algorithme de la procédure d'autoconfiguration d'adresse se décompose de la manière suivante :

- La toute première étape consiste à créer l'adresse lien local, qui est de la forme FE80 ::XXXX :XXXX :XXXX :XXXX
- Une fois l'unicité de cette adresse vérifiée grâce à l'algorithme DAD (détection d'adresses dupliquées), la machine est en mesure de communiquer avec les autres machines du lien.
- La machine doit chercher à acquérir un message d'annonce du routeur pour déterminer la méthode d'obtention de l'adresse Unicast globale et de connaître la route par défaut (dans le cas d'une autoconfiguration sans état). Cette étape permet à la machine de connaître le ou les préfixes du réseau qui sont annoncés par les routeurs. Ce préfixe a une longueur de 64 bits. La machine ajoute son identifiant d'interface (dédié à partir de son adresse IEEE 802.3) pour construire son adresse IPv6.
- S'il y a un routeur sur le lien local, la machine doit appliquer la méthode indiquée par le message d'annonce du routeur, à savoir : l'autoconfiguration sans état ou l'autoconfiguration avec état.
- En l'absence de routeur sur le lien local, la machine doit essayer d'acquérir l'adresse Unicast globale par la méthode d'autoconfiguration avec état. Si la tentative échoue, c'est terminé. Les communications se feront uniquement au niveau du lien local.

ID interface et Format EUI-64 de l'EEE :

L'identifiant d'interface IPv6 va donc être conçu à partir de l'adresse Mac. On va donc recourir à une petite astuce qui consiste à rajouter les 16 bits manquants entre les 24 premiers bits (qui identifient par un numéro le constructeur de la carte réseau) et les 24 derniers bits (qui identifient le numéro de série de cette carte fabriquée par ce constructeur). Les 16 bits rajoutés ont pour valeur: FFFE. Les 24 premiers bits identifient toujours par un numéro le constructeur de la carte réseau et les 24 derniers bits identifient par un numéro de série la carte fabriquée par ce constructeur.



Si le bit **u=0**, il s'agit d'un identifiant universel,

Si le bit **u=1**, il s'agit d'un identifiant local,

Si le bit **g=0**, il s'agit d'une adresse individuelle (Unicast), dans ce cas le 1er octet est toujours pair,

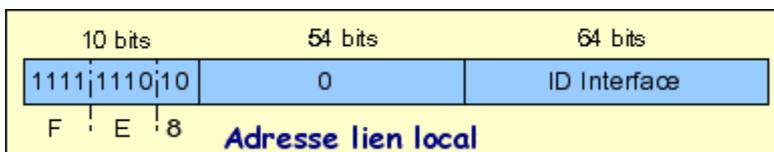
Si le bit **g=1**, il s'agit d'une adresse de groupe (Multicast), dans ce cas l'octet est impair.

La construction de l'identifiant de l'adresse IPv6 est alors simple, il suffit de reprendre entièrement ces 64 bits et d'inverser le bit "**u**" en lui attribuant la valeur "**1**".

Adresse lien local :

Cette adresse de lien local est valide uniquement sur un même espace de lien sans routeur intermédiaire. Un routeur ne route pas ce type d'adresse. L'interconnexion par hub ou switch de niveau Mac représente cet espace de lien.

Le préfixe d'une adresse de lien local est **fe80::/10**



Une adresse lien local est donc constituée de la concaténation du préfixe fe80 et de l'ID interface.

Constitution d'une adresse Unicast Global :

| | |
|---|--------------|
| Adresse IPv6 (128 bits) | |
| Préfixe du sous-réseau annoncé par le routeur | Interface ID |
| 64 bits | 64 bits |

Exemple d'autoconfiguration d'une machine :

Ma machine a pour adresse MAC : 00-C0-4F-4E-3F-EB. Le routeur du site sur lequel je suis connecté annonce le préfixe : 2001:660:3001:4014/64. En effet, comme expliqué plus haut, le routeur peut être configuré pour envoyé régulièrement un message «Router Advertisement » sur le lien local, pour annoncer aux stations le préfixe du réseau.

On obtient l'adresse globale en concaténant les deux: 2001:660:3001:4014:2c0:4ff:fe4e:3feb

On remarque qu'on a inséré « **ffe** » pour obtenir les 64 bits de l'interface ID. En outre, le bit « u » est égal à 1, ce qui donne un « 2 » (voir explication ci-dessus).

Intérêt de l'autoconfiguration :

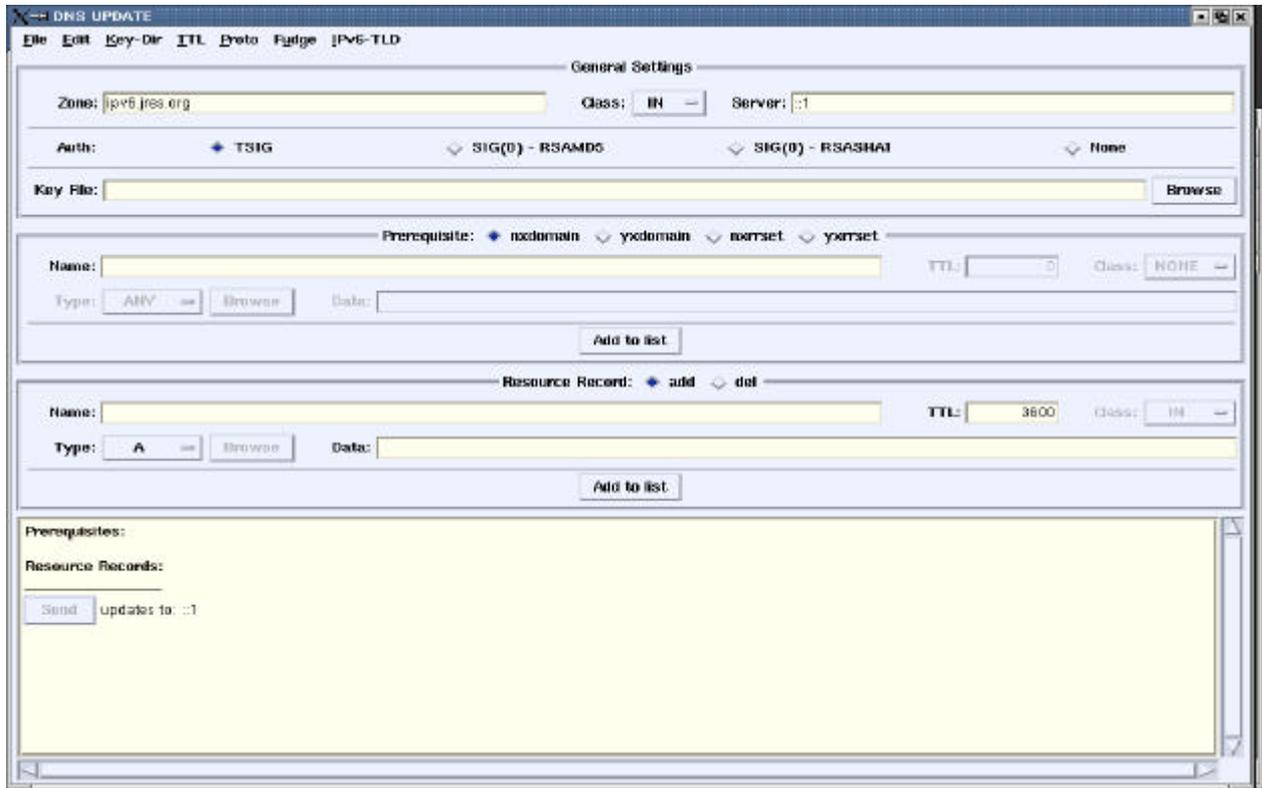
Traditionnellement, la configuration d'une interface réseau d'une machine demande une configuration manuelle. C'est un travail souvent fastidieux. Avec IPv6, cette configuration est automatisée donnant par là-même des caractéristiques de fonctionnement immédiat («plug and play») à l'interface réseau. La configuration automatique signifie qu'une machine obtient toutes les informations nécessaires à sa connexion à un réseau local IP sans aucune intervention humaine. En particulier, l'autoconfiguration d'adresses IPv6 se trouve au cœur de la configuration automatique des interfaces IPv6. Dans le cas idéal, un utilisateur quelconque déballe son nouvel ordinateur, le connecte au réseau local et le voit fonctionner sans devoir y introduire des informations de «spécialiste».

L'autoconfiguration d'adresses IPv6 a pour objectifs :

- l'acquisition d'une adresse quand une machine est attachée à un réseau pour la première fois.
- l'obtention de la nouvelle adresse suite à la renumérotation des machines du site (après un changement de fournisseur d'accès par exemple). L'opération de renumérotation revient concrètement à changer la partie haute de l'adresse. L'autoconfiguration d'adresses va servir de vecteur dans l'attribution du nouveau préfixe.
- De contribuer à la mobilité. En effet, lorsque l'on change le Mobile Node, l'obtention d'adresse dans le nouvel environnement se fait de manière automatique.

E) DNS :

Afin de présenter le service de DNS, M. Yves LegrandGerard a développé un logiciel de gestion du DNS IPv6, avec mise à jour dynamique et sécurisée des informations sur le serveur, c'est à dire en utilisant des algorithmes de chiffrement, et aussi une interface graphique dont on voit un aperçu ci-dessous.



Bien que je n'ai pas participé au développement du DNS, cette partie a constitué une part importante du tutoriel. Afin de le faire fonctionner, j'ai simplement décompresser et installer le fichier **nsupdate.tgz**. Ensuite, pour le lancer, on lance le serveur DNS puis l'interface :

`./usr/local/nsupdate/server/test/named`

`./usr/local/src/nsupdate/xnsupdate.py`

L'interface graphique est relativement instinctive. Il suffit de préciser l'adresse IPv6, le nom de la machine et de prendre comme type «AAAA» et non pas «A» comme en IPv4. Les types d'enregistrement «PTR», «SOA» et «NS» sont également disponibles.

F) Serveur Web

Le serveur que j'ai utilisé est le serveur http Apache version 2.0.48. Je l'ai installé sur un PC avec Linux RedHat. Seule la version 2.0 d'Apache est capable de gérer IPv6 et il n'y a aucune action spécifique à faire par rapport à IPv4. Après avoir préparé quelques pages en html, il m'a suffit de lancer un client WEB, compatible avec IPv6 : Internet Explorer 6 par exemple. Pour entrer une URL en IPv6, il suffit alors de mettre des crochets.

En annexe, se trouve l'installation et la configuration du serveur Web.

G) Vidéoconférence :

A la fin du tutoriel qui s'est déroulé le lundi, j'ai désinstallé la plate-forme pour en réinstaller une partie, quelques étages plus bas, sur le stand de RENATER. Cette fois-ci, l'objectif a été d'établir une connexion en Multicast IPv6 entre notre stand des JRES de Lille et celui d'INTEROP à Paris, ces 2 événements ayant eu lieu la même semaine et de faire des démonstrations de vidéoconférences jusqu'à la fin de la semaine.

Nous avons testé des applications comme les Mtools (vic, rat, sdr..) et Videolan.

Comme on peut le voir sur les fichiers de configuration en annexes, nous avons du mettre des routes statiques pour atteindre les RP (Rendez-vous Point).

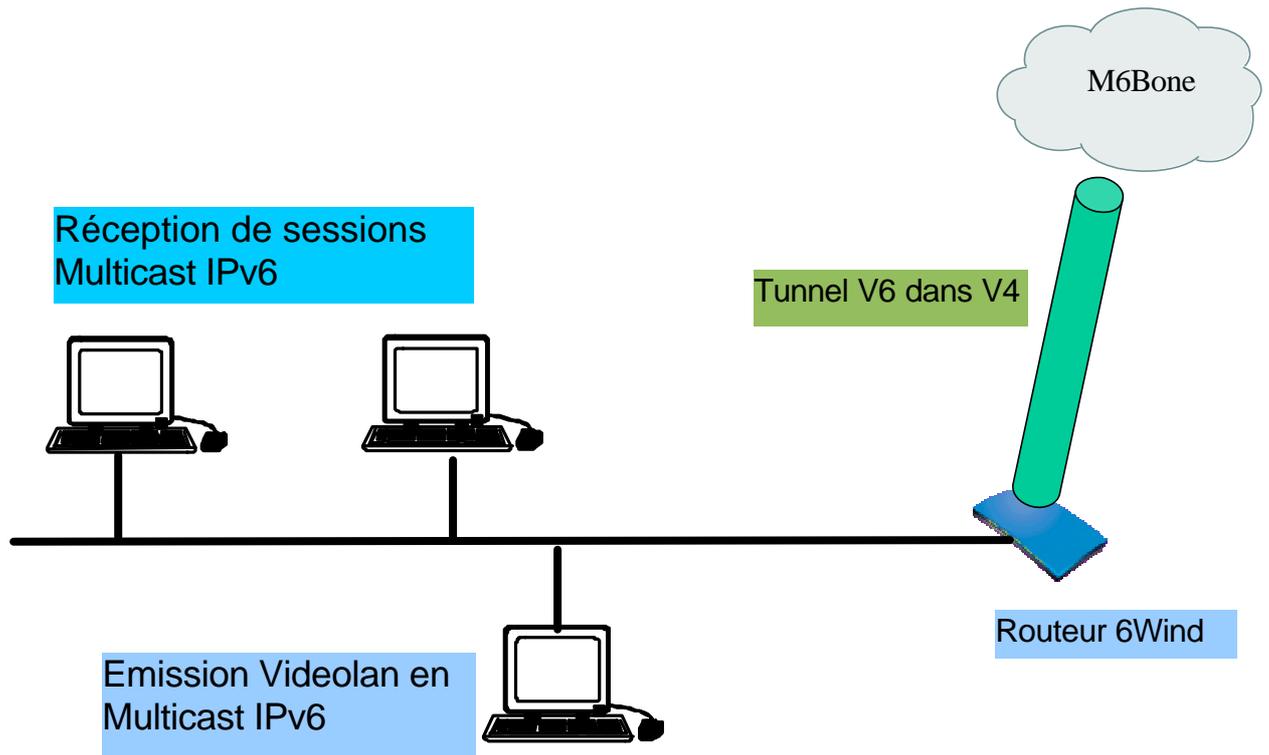
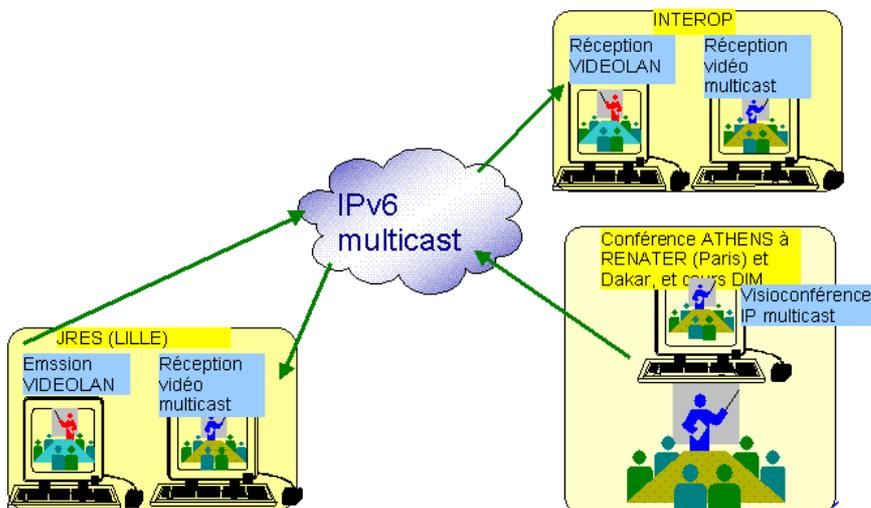


Schéma de la démonstration aux JRES 2003



H) Planification de l'évènement

| Tache à réaliser | S41 | S42 | S43 | S44 | S45 | S46 | S47 | S48 | S49 | S50 | S51 |
|--|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| T1 : Formation générale à IPv6 | ■ | | | | | | | | | | |
| T2 : Rassembler le matériel nécessaire à la réalisation de la plate-forme. | | ■ | | | | | | | | | |
| T3 : Prise en main du 6wind. | | | ■ | | | | | | | | |
| T4 : Prise en main de FreeBSD. | | | | ■ | | | | | | | |
| T5 : Prise en main de Zebra. | | | | ■ | | | | | | | |
| T6 : Configuration des stations de travail. | | | | | ■ | | | | | | |
| T7 : Installation et configuration des services sur les stations de travail. | | | | | | ■ | | | | | |
| T8 : Intégration de l'ensemble et test au GIP RENATER. | | | | | | ■ | | | | | |
| T9 : Préparation de l'expédition de la plate-forme aux JRES (Lille). | | | | | | | ■ | | | | |
| T10 : Réception de la plate-forme à Lille et tests finaux dans les locaux du tutorial. | | | | | | | ■ | | | | |
| T11 : Présentation de la plate-forme aux JRES 2003. | | | | | | | ● | | | | |
| T12 : Renvoi de la plate-forme au GIP RENATER. | | | | | | | | ■ | | | |
| T13 : Réception de la plate-forme. | | | | | | | | ■ | | | |
| T14 : Documentation et remontage de la plate-forme. | | | | | | | | | ■ | | |

BILAN :

La préparation de la plate-forme a été intéressante du point de vue technique et organisationnel. J'ai appris énormément d'aspects et de nouveautés concernant le protocole IPv6. En effet, j'ai pu très rapidement passer de la théorie récemment apprise à la mise en pratique jusqu'à la transmission de connaissances par l'intermédiaire du tutoriel. Je suis content que le travail que j'ai réalisé aie pu servir de support au tutoriel IPv6 à destination de nombreux professionnels des réseaux.

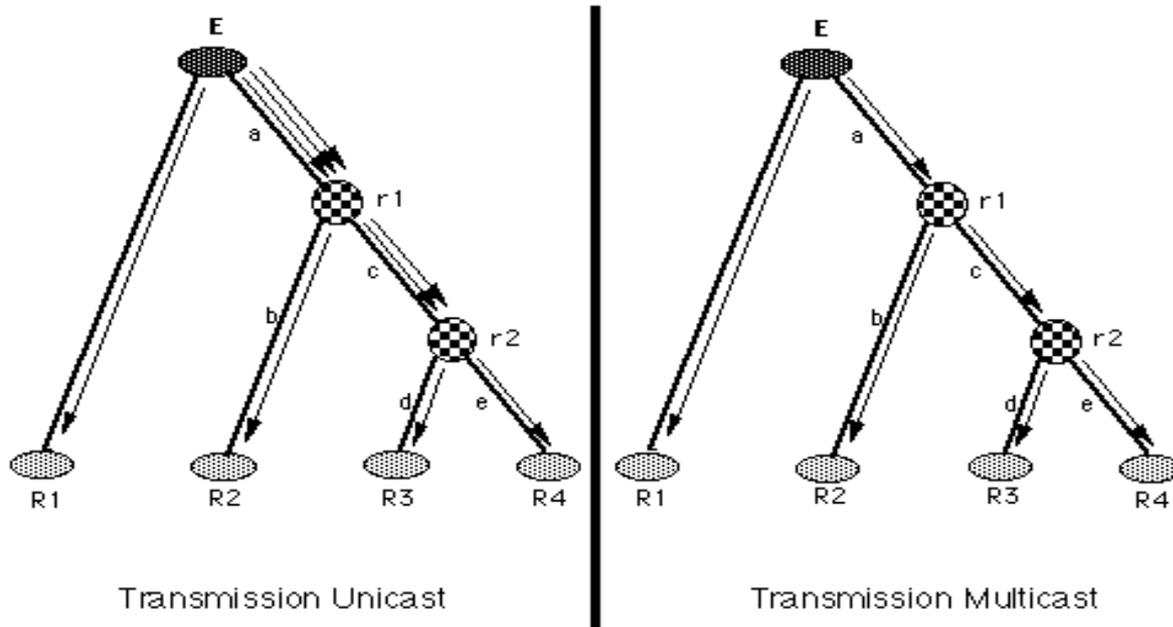
Du point de vue organisationnel, ce travail a été enrichissant. J'ai dû m'organiser pour effectuer toutes les tâches avant le jour de l'évènement. En outre, j'ai eu à collaborer avec plusieurs personnes sur des points divers. Il s'agissait pour moi de dialoguer à la fois avec les organisateurs des JRES, avec mes tuteurs, avec le transporteur de la plate-forme, avec mes collaborateurs du tutoriel etc..

En somme, j'ai réussi à mettre en place un réseau IPv6 opérationnel et j'y ai installé des services. Bien que dans l'ensemble mon travail a semble-t-il été satisfaisant, je pense que la plate-forme aurait pu inclure encore plus de services et qu'il reste des choses à améliorer. Je pense que mon principal souci a été le temps puisque j'ai mis trop de temps à démarrer la réalisation même de la plate-forme. En effet, le plus long a été rassembler l'ensemble du matériel et intégrer l'ensemble des connaissances techniques nécessaires. J'aurais pu gagner énormément de temps si dès le début, j'avais bénéficié d'une aide qui me dise exactement quoi apprendre, où chercher telle information etc... C'est la raison pour laquelle, j'ai proposé à mes tuteurs de rédiger un livret d'accueil à l'attention des nouveaux stagiaires au GIP RENATER dont l'objectif serait qu'ils profitent de mon expérience pour être opérationnel le plus rapidement possible. Il s'agira de leur apporter aussi bien des informations pratiques (où manger rapidement, à qui s'adresser pour telle ou telle requête etc...) que des informations techniques (comment remonter la plate-forme, quels sites Internet ou quels RFC consulter pour tel protocole).

3/ Multicast IPv6:

A) Les Protocoles

Le Multicast consiste en l'envoi d'un seul flux de données, tel qu'une émission vidéo, à un grand nombre de récepteurs, au lieu d'un flux par récepteur. Les participants à une application Multicast constituent un groupe de diffusion qui possède une adresse de groupe.



L'intérêt du Multicast est d'une part d'économiser les ressources du réseau (bande passante, ressources des routeurs, ressources de la source ...) et d'autoriser un nouveau type d'applications comme les vidéoconférences ou les télé-séminaires ...

Le service Multicast est susceptible d'être fourni par l'opérateur de services de tout réseau IP en complément de son service Unicast IPv4 ou IPv6. Par exemple, RENATER-3 et certains réseaux de la recherche dans le monde offrent le service Multicast sur IPv4 et ces services sont interconnectés entre eux au niveau des points d'échange comme SFINX. Pour RENATER : le service est disponible sur l'épine dorsale nationale et sur les réseaux de collecte modernes. Certains réseaux de collecte plus anciens ne l'offrent pas encore.

RENATER et certains réseaux de la recherche ont mis en oeuvre le M6bone, un service Multicast sur IPv6 à titre expérimental – ce qui n'empêche pas certains utilisateurs d'en faire un usage proche de l'opérationnel pour la visioconférence, les applications habituelles (VIC, RAT, Videolan) étant disponibles sur IPv6 ! Il sera question du M6bone un peu plus loin.

Pour le Multicast, il y a 3 niveaux protocolaires :

- MLD (Multicast Listener Discovery) pour l'abonnement à des groupes de diffusion auprès du routeur Multicast du lien local.
- PIM SM (Protocol Independent Multicast - Sparse Mode) pour la création d'arbres de diffusion.
- MBGP (Multiprotocol Border Gateway Protocol) pour s'échanger les routes, de manière à construire l'arbre de diffusion.

A-1/Adresses Multicast

Une adresse IPv6 Multicast identifie un groupe de diffusion qui peut être éventuellement jointe par plusieurs hôtes

- Un hôte peut appartenir à autant de groupes qu'il le souhaite
- Les adresses Multicast ont le format suivant :



- 1111 1111 (FF) : identifie l'adresse comme étant de type Multicast
- scope : valeur qui définit l'étendue d'un groupe Multicast (ci-dessous le tableau des scopes)

| | | | |
|-----------------|-----------------|-----------------------|-----------------|
| 0: reserved | 4: (unassigned) | 8: organization-local | C: (unassigned) |
| 1: node-local | 5: site-local | 9: (unassigned) | D: (unassigned) |
| 2: link-local | 6: (unassigned) | A: (unassigned) | E: global |
| 3: (unassigned) | 7: (unassigned) | B: (unassigned) | F: reserved |

- group ID: identifie un groupe Multicast.
- Adresses Multicast prédéfinies :

| Adresse | Descriptif |
|-----------|---|
| FF02::1 | groupe de tous les hôtes au niveau link-local |
| FF02::2 | groupe de tous les routeurs au niveau link-local |
| FF02::1:0 | groupe de tous les serveurs DHCP au niveau link-local |

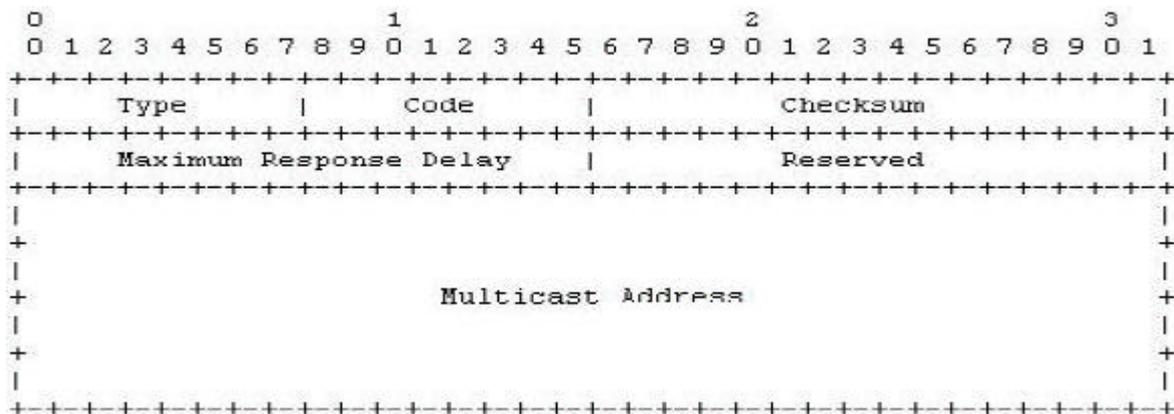
A-2/Le protocole MLD (RFC 2710)

MLD est un sous-ensemble de ICMPv6.

MLDv1 est un protocole d'interaction entre le MLD Querier, c'est à dire le routeur Multicast du LAN et les hôtes Multicast du LAN. MLDv1 permet donc à un hôte de s'abonner (et se désabonner) à un groupe. MLD présente les mêmes fonctionnalités que le protocole IGMPv2 en IPv4.

Il existe deux versions : MLDv2 est en cours de normalisation et permet de sélectionner les sources que les hôtes veulent recevoir parmi le groupe Multicast.

Format d'un message MLD



- **Type :** Types de messages

General Query et Multicast-Address-Specific Query (type=130)

Multicast Listener Report (type=131)

Multicast Listener Done (type=132)

- **Code :** initialisé à 0 par l'émetteur et ignoré par la suite
- **Checksum :** porte sur tout le message MLD et sur l'en-tête IPv6
- **Maximum Response Delay :** Permet de définir un temps maximum de réponse pour les messages de type query
- **Reserved :** pas utilisé : initialisé à 0 puis ignoré par la suite
- **Multicast Address :** adresse IPv6 Multicast ou initialisé à 0 suivant le type de messages

Fonctionnement :

1/ « Qui veut s'abonner à quel groupe ? »

Le routeur envoie périodiquement un message **General Query** sur le réseau auquel il est directement connecté. L'adresse de destination est ff02::1 (équivalent à toutes les stations Multicast du lien). Ici le champ Multicast Address est à 0.

Il peut aussi envoyer des messages **Multicast-Address Specific Query**. Cette fois-ci, on demande qui est abonné à un groupe spécifique donné en paramètre. On met alors le champ Multicast Address égal à l'adresse Multicast spécifique.

2/ « Quand un hôte reçoit le query message. »

Il fixe un délai aléatoire compris entre 0 et « **Maximum Response Delay** » avant de répondre. Lorsque le compte à rebours arrive à 0 et si aucun **Multicast Listener Report** n'a été envoyé par une station, il envoie un **Multicast Listener Report** à l'adresse du routeur et à l'adresse du groupe Multicast. Le champ Multicast Address contient l'adresse Multicast du groupe auquel la station s'abonne. Avec cette technique, un hôte donne une réponse au nom de tous les hôtes du groupe Multicast et de cette manière il n'y a pas de messages redondants.

3/ « Lorsque le routeur reçoit un Multicast Listener Report. »

Avant tout, le routeur met à jour sa table MLD et réinitialise un compte à rebours à la valeur « **Multicast Listener Interval** ». Le routeur arme un compte à rebours sur les abonnements aux groupes Multicast avant de solliciter à nouveau tous les hôtes. Enfin, si le routeur ne reçoit aucune réponse pour un groupe donné, il arrête alors la rémission des paquets Multicast de ce groupe et le groupe est donc réputé sans abonné local.

A-3/ Le protocole PIM SM (RFC 2362)

PIM signifie **Protocol Independent Multicast**. Il s'agit du protocole de création d'arbres de diffusion, utilisé dans un routeur Multicast pour propager l'information concernant les groupes. Pour adresser les messages, le protocole PIM propose deux modes différents : PIM-DM (PIM - Dense Mode) et PIM-SM (PIM - Sparse Mode).

Nous nous intéresserons surtout à PIM-SM, qui est beaucoup plus adapté pour le Multicast IPv6 car contrairement à PIM-DM, le protocole PIM-SM émet du trafic seulement là où c'est nécessaire, c'est à dire là où il y a des demandes explicites pour recevoir le flux alors que PIM-DM « inonde » tout le réseau.

PIM-SM construit pour chaque groupe un arbre de diffusion partagé et unidirectionnelle, chaque arbre prenant racine en un point spécifique appelé RP (Rendez-vous Point). Lorsqu'il y a plusieurs sources alimentant le même groupe, les paquets en provenance des différentes sources convergent vers le RP associé au groupe, puis à partir de celui-ci, les paquets empruntent (et donc partagent) l'arbre associé au groupe, ce qui leur permet d'atteindre tous les destinataires membres du groupe.

Le routeur RP est désigné soit statiquement soit par une élection entre les différents routeurs Multicast du domaine PIM. La découverte par les routeurs du RP se fait grâce au mécanisme du Bootstrap Router (BSR). Un routeur d'un domaine PIM est élu comme Bootstrap Router, et son rôle est d'émettre régulièrement à tous les routeurs qui ont été candidats au titre de Bootstrap Router des messages BSR qui contiennent l'ensemble des RP du domaine.

Le routeur désigné ou DR (routeur Multicast qui gère le protocole PIM lorsque plusieurs routeurs d'un même LAN peuvent gérer le PIM) est lui aussi élu, et les messages utilisés pour son élection sont les messages PIM Hello.

Les messages Hello servent aussi pour connaître les routeurs PIM voisins sur chaque interface. Ces messages sont nécessaires car si un routeur n'a pas envoyé de PIM Hello, il est ignoré par les autres routeurs PIM, ce qui rendra difficile la construction de l'arbre de diffusion.

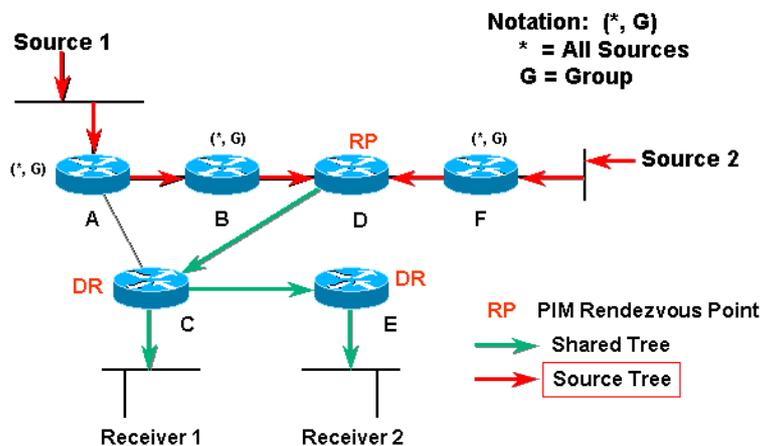
Enfin, notons l'existence du protocole PIM-SSM (PIM- Source Specific Multicast, Draft-ietf-ssm-arch-xx.txt) qui est actuellement en cours de standardisation à l'IETF. Ce protocole permet de simplifier les mécanismes mis en œuvre dans PIM-SM pour optimiser la création d'arbre de diffusion dans le cas d'une source unique. En effet, PIM-SSM permet de préciser la source et donc il devient possible d'établir des canaux directement entre les récepteurs et la source, sans passer par un RP.

Le fonctionnement du protocole PIM-SM suit trois phases principales :

Phase 1 : L'arbre partagé ou RPT (Rendez-vous Point Tree)

Un client souhaite recevoir du trafic Multicast d'un groupe défini. Cette demande se fait en utilisant un protocole de gestion des groupes Multicast, MLD pour IPv6. Le routeur Multicast (DR), chargé du sous-réseau IP du client, envoie un message PIM d'abonnement vers le RP du groupe Multicast. On note $PIM (*,G) join$ ce type de message car il permet la réception de paquets Multicast pour le groupe G en provenance de n'importe quelle source. Le message va voyager de routeur en routeur jusqu'au RP du groupe, et dans chaque routeur traversé, un état associé à l'arbre Multicast du groupe G est créé. Finalement, le $PIM (*,G) join$ atteint soit le RP, soit un routeur possédant déjà un état $(*,G)$ associé au groupe. Il y a alors création entre le DR et le RP d'un arbre partagé par toutes les sources. Quand plusieurs récepteurs adhèrent à un groupe, leur message Join convergent vers le RP de ce groupe, ce qui forme l'arbre Multicast pour ce groupe, arbre ayant pour racine ce RP. Cet arbre est appelé RPT (Rendez-vous Point Tree) et il est qualifié d'arbre partagé puisqu'il sera utilisé pour atteindre tous les destinataires du groupe quelque soit l'émetteur du paquet Multicast. Des messages PIM d'adhésion sont envoyés périodiquement tant qu'au moins un destinataire est membre du groupe. Quand tous les destinataires situés sur un sous-réseau IP quittent un groupe, le DR peut envoyer un message PIM d'élagage (PIM Prune). Une durée limite de validité étant associée à chaque adhésion, si aucun message PIM ne parvient, l'adhésion sera résiliée.

Rendez-vous Point Tree



Dès qu'une station émet des données vers un groupe Multicast, le DR envoie des paquets encapsulés dans un datagramme Unicast ayant pour adresse de destination le RP associé au groupe. Le RP désencapsule alors les données et les propage suivant l'arbre RPT associé au groupe. Les paquets Multicast suivent alors les informations $(*,G)$ placées dans les routeurs formant l'arbre RPT. Ces paquets sont dupliqués aux nœuds qui forment de nouvelles branches, et donc parviennent à l'ensemble des destinataires membres du groupe. L'encapsulation des paquets vers le RP est appelé enregistrement et les paquets encapsulés sont des PIM register.

Lorsque la phase 1 est terminée, le trafic est envoyé encapsulé par le DR vers le RP, et le RP le renvoie alors nativement sur l'arbre RP, et vers les récepteurs.

Phase 2 : L'acheminement spécifique

La phase 1 reste assez inefficace, puisqu'il est nécessaire d'encapsuler les données entre le DR et le RP, ce qui est une opération coûteuse pour un routeur.

Bien que la technique proposée lors de la phase 1 puisse perdurer indéfiniment puisque c'est le mode de fonctionnement par défaut, le RP va chercher à basculer vers une technique d'acheminement native, sans encapsulation. Dans ce cas, lorsque le RP reçoit un message PIM Register, contenant un paquet Multicast provenant d'un émetteur S pour un groupe G, il peut entreprendre de construire un chemin d'acheminement spécifique pour l'émetteur noté (S,G). Pour ce faire, le RP envoie un message PIM (S,G) Join vers l'émetteur. Ce message provoque dans tous les routeurs traversés la création d'un état Multicast spécifique (S,G). Ces états ne seront utilisés que pour transmettre les paquets Multicast émis par S vers le groupe G. A la fin, ce message PIM (S,G) Join arrivera au DR du sous-réseau IP hébergeant l'émetteur S. La source S peut alors émettre des paquets Multicast natifs.

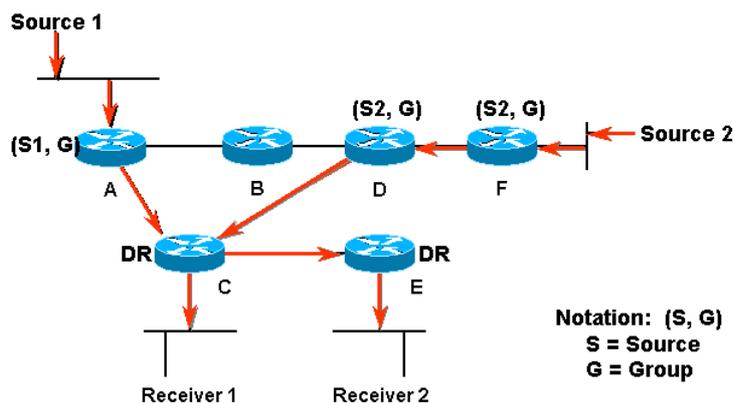
Quand les paquets Multicast arrivent nativement vers le RP, celui-ci reçoit les messages en doubles puisqu'il reçoit à la fois le trafic encapsulé et le trafic natif. Le RP détruit alors la copie des messages encapsulés et il envoie un message PIM Register-Stop vers le DR de l'émetteur afin de lui demander de stopper l'encapsulation devenue inutile. A la fin de cette phase, le trafic émis par la source S pour le groupe G suit le chemin d'acheminement spécifique jusqu'au RP, puis utilise l'arbre RPT (associé au groupe G) pour atteindre tous les destinataires du groupe G. Là où les deux arbres (l'arbre RPT entre le RP et les DR des récepteurs et l'arbre entre le RP et le DR de l'émetteur) se croisent, et pour certains destinataires proches de la source, le trafic peut passer du chemin d'acheminement spécifique à une branche de l'arbre RPT, en évitant ainsi un détour via le RP.

Phase 3 : L'arbre des plus courts chemins ou SPT (Shortest Path Tree)

La phase 2 supprime le surcoût introduit par l'encapsulation entre l'émetteur et le RP, cependant, cela n'optimise pas complètement le chemin suivi par les paquets Multicast : pour de nombreux destinataires, le transit par le RP provoque un détour important si on compare ce chemin avec le chemin le plus court entre l'émetteur et chaque destinataire. Pour obtenir des délais plus courts, le DR associé au destinataire peut lancer la construction d'un arbre des plus courts chemins spécifiques à l'émetteur S pour un groupe G. On désigne cet arbre par SPT (Shortest Path Tree). Dans ce cas, le DR émet un message PIM (S,G) Join vers l'émetteur. Cela crée des états spécifiques (S,G) dans les routeurs concernés sur le chemin de l'émetteur.

Un fois le message arrivé à l'émetteur ou à un routeur possédant déjà l'état (S,G), les paquets Multicast émis par l'émetteur S n'ont plus qu'à suivre les états (S,G) présents dans les nœuds des routeurs formant l'arbre Multicast (S,G).

Shortest Path Tree



De la même manière que précédemment, le DR du destinataire peut recevoir deux copies des paquets Multicast, une provenant du RP et ayant suivi l'arbre RPT associé et une autre provenant de l'arbre des plus courts chemins. Le DR détruit alors les paquets provenant du RPT, et envoie un message PIM (S,G) Prune vers le RP.

Conclusion

A l'issue de ces trois phases, on peut avoir des destinataires qui reçoivent leur trafic Multicast des trois manières différents, certains par le RPT (encapsulé ou non) et d'autres par le SPT. Le protocole PIM est donc un protocole qui s'adapte aux divers environnements, en utilisant les trois modes proposés non exclusifs.

A-4/ Le protocole MBGP (RFC 2858)

MBGP est la nouvelle version de BGP. La version actuelle BGP4 est le protocole de routage externe, c'est à dire routage entre les AS ou « systèmes autonomes », utilisé pour le routage global de l'Internet IPv4. Compte tenu de sa criticité, ce protocole est l'objet d'évolutions constantes. La version qui nous intéresse ici est donc le [RFC 2858] qui rend BGP4 multi-extensions en introduisant la notion de famille d'adresse (ex. IPv4, IPv6, MPLS,...) et de sous-famille d'adresse (ex. Unicast, Multicast). Le [RFC 2545] précise l'usage des extensions multi-protocoles pour le cas d'IPv6.

Les implémentations du [RFC2858] sont souvent appelées MBGP ou BGP4+ (pour faire référence à leur capacité de traitement des routes Multicast IPv6). Il est à noter que les mêmes numéros d'AS sont utilisés pour IPv4 et IPv6.

L'adaptation multi-protocole de BGP4 est assez simple car elle ne concerne que les trois attributs dont le format dépend de l'adresse soit :

- NLRI : *Network Layer Reachability Informations* (suite de préfixes)
- NEXT_HOP : Adresse IP où il faut router les NLRI.
- AGGREGATOR : Adresse IP d'un routeur qui a fait une agrégation de préfixes.

En outre, BGP4+ introduit deux nouveaux attributs :

- MP_REACH_NLRI : *Multiprotocol Reachable NLRI*
- MP_UNREACH_NLRI: *Multiprotocol Unreachable NLRI*

B/ Le M6bone

B-1/Présentation

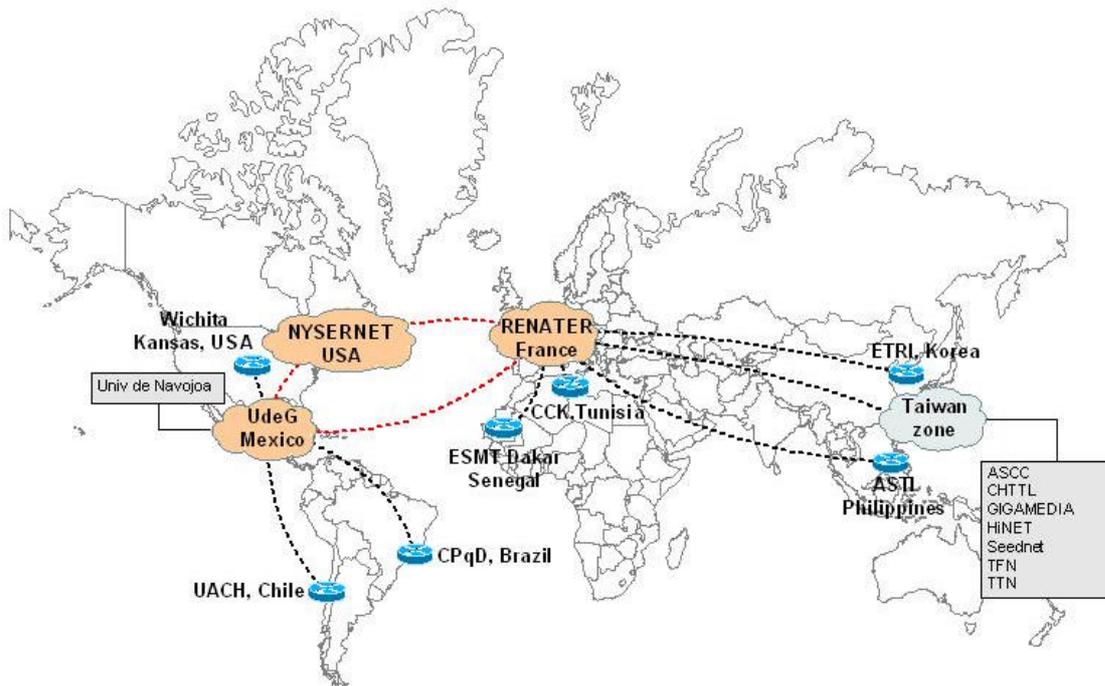
Le projet M6bone a pour objet de mettre en œuvre un service Multicast IPv6 au niveau mondial. L'objectif est de fournir une connectivité IPv6 Multicast aux sites qui sont intéressés par le projet, d'ouvrir de plus en plus de monde à cette technologie et de participer à la promotion du protocole IPv6.

Le M6Bone représente la plate-forme idéale pour valider les protocoles Multicast IPv6 et tester des équipements ou des applications liés au Multicast IPv6 ce qui permet de mieux comprendre cette technologie, la développer et d'aboutir ainsi à un service avancé dans le future proche. De plus, la connexion au M6Bone est une bonne occasion pour se former au protocole IPv6 et au Multicast. Les administrateurs des sites sont amenés eux-mêmes à configurer les routeurs nécessaires à leur connexion, ainsi que les stations de travail clientes qui permettent de faire de la visioconférence. Cette phase de formation sur un réseau de test s'avère très importante en vue de l'utilisation future de la technologie Multicast IPv6 dans un contexte de production.

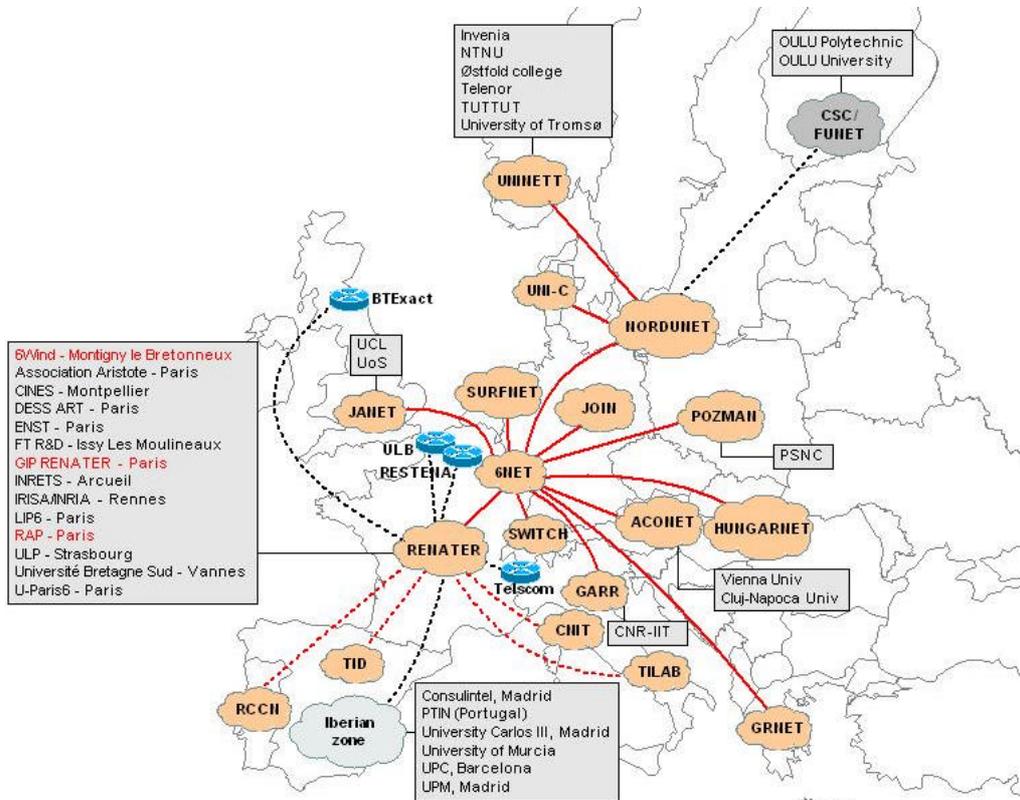
Enfin, le M6Bone permet de regrouper différents projets travaillant autour du Multicast IPv6 en Europe comme 6Net qui joue un rôle important dans le développement de la nouvelle génération des technologies Internet. Ce réseau favorise aussi un environnement de test pour des équipementiers et développeurs comme CISCO, JUNIPER et 6WIND.

Plusieurs événements ont été transmis à travers le M6Bone dans le cadre des causeries RENATER, ou des plates-formes de démonstration des JRES et de INTEROP qui permettent de promouvoir le protocole IPv6 en France et à travers le monde.

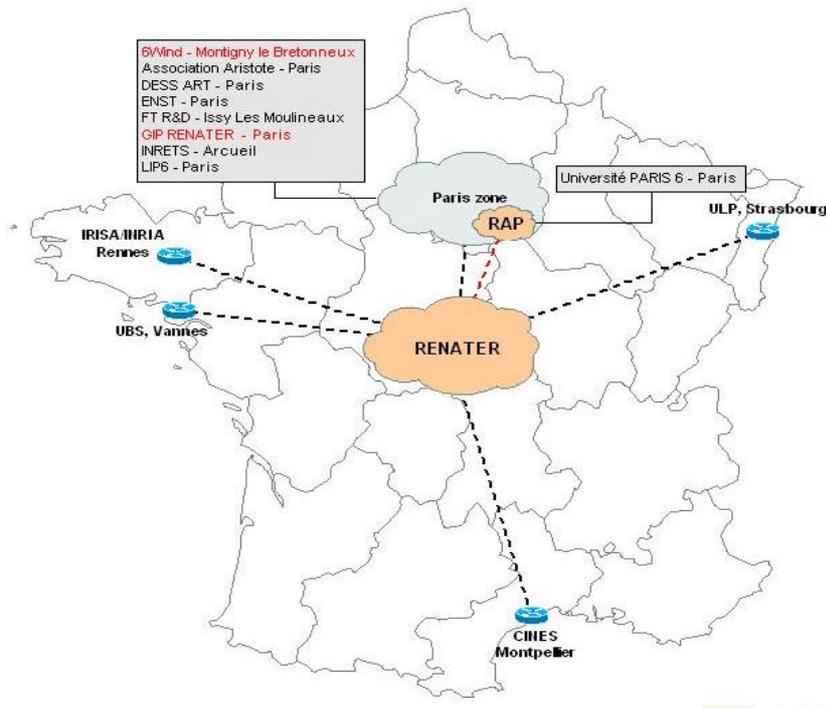
Aujourd'hui, le M6Bone compte 45 sites et 25 réseaux interconnectés répartis dans plus de 20 pays. Ci-dessous les cartes qui montrent l'architecture logique du réseau :



Sites en Asie, Afrique et en Amérique



Sites en Europe



Sites en France

Le M6Bone est un réseau composé en partie de tunnels entre les différents routeurs Multicast IPv6. La mise en place de tunnels pour la connexion des sites permet de faire passer les paquets Multicast IPv6 à travers des réseaux qui sont IPv4 ou IPv6 Unicast. Ceci permet de pallier l'absence de routeurs commerciaux qui implantent les protocoles de Multicast IPv6 dans des réseaux de production.

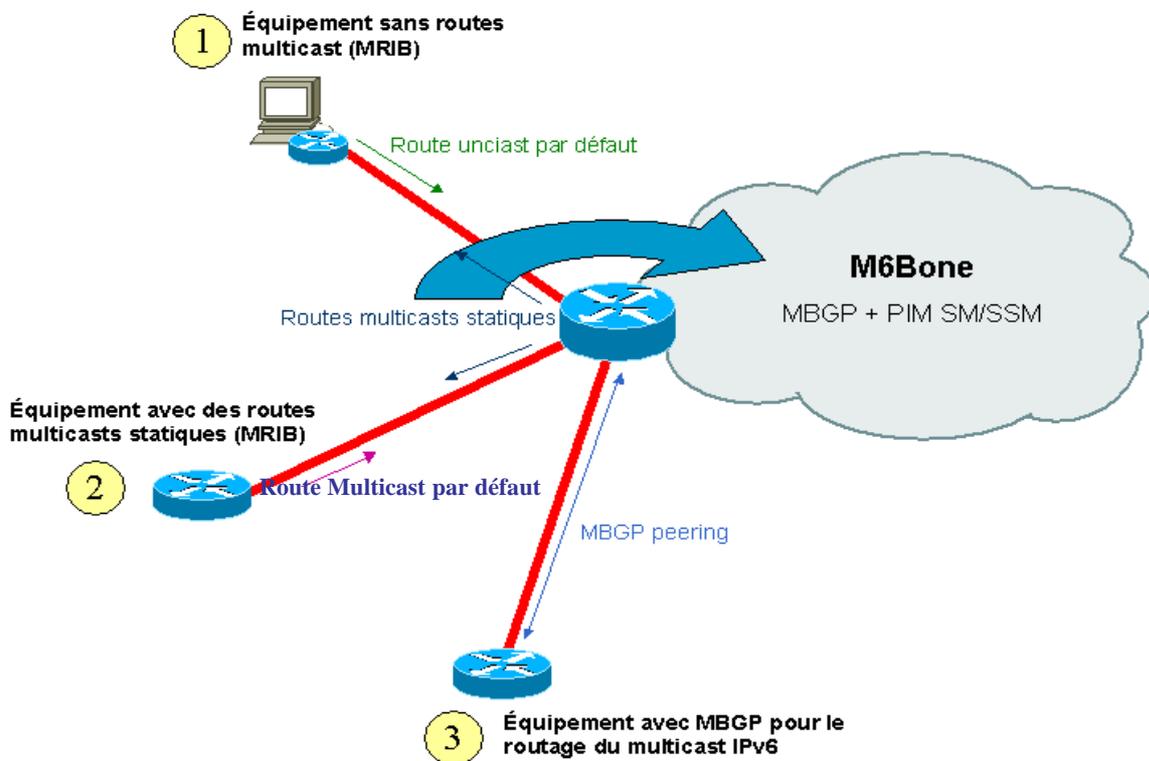
Le réseau M6Bone utilise le protocole PIM SM (Protocol Independent Multicast, Sparse Mode). Le RP (Rendez-vous Point) se trouve au GIP RENATER même. Certaines implantations incluent déjà ce protocole, comme FreeBSD à partir de la version 4.6, la pile Kame qui est développée dans le cadre du projet Wide et aussi certains équipementiers avec des images de test (Cisco, 6Wind, Hitachi, Juniper...)

Dans un premier temps, le M6Bone présentait une architecture simple avec une topologie en étoile. Ensuite, le M6Bone a logiquement évolué vers une topologie plus complexe.

B-2/ Les différents déploiements

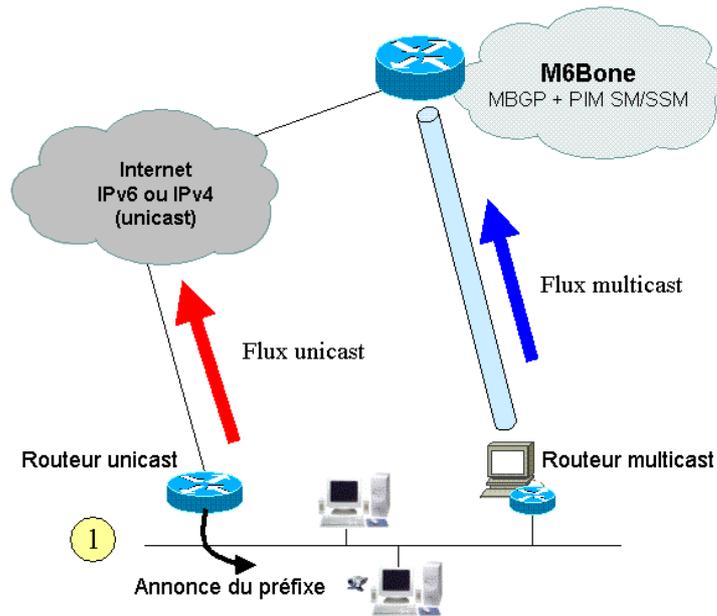
Le GIP RENATER est le point d'interconnexion principale du M6Bone. Son rôle est donc de fournir et maintenir le service IPv6 Multicast aux sites qui en feraient la demande, en France, en Europe et même au-delà comme on peut le voir sur les cartes ci-dessus.

La personne qui est chargée du M6bone au GIP RENATER est Jérôme Durand, ancien élève du département télécommunications de l'INSA de Lyon. Pendant mon stage, j'ai été amené à travailler souvent avec lui sur ce projet. Ci-dessous, en collaboration avec Jérôme Durand, j'ai recensé et expliqué trois cas de déploiement du service IPv6 Multicast à un site demandeur. Dans les 3 cas, le routeur central se trouve au GIP RENATER et est gérée par Jérôme et moi.



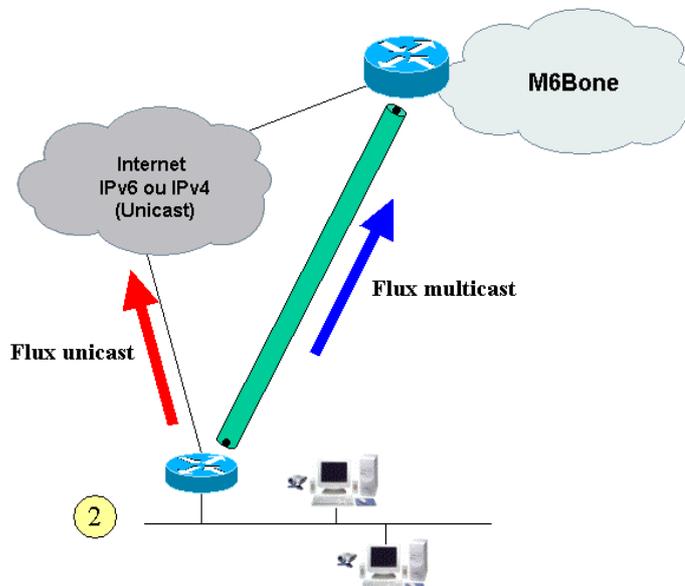
Cas n°1 : Le routeur ne gère pas les routes Multicast :

Il s'agit souvent d'un PC avec l'OS FreeBSD ou tout autre routeur qui n'implémente pas de table de routage Multicast (autrement appelée MRIB pour Multicast Routing Information Base). On a alors 2 routeurs sur le réseau local : d'une part, le routeur de production Unicast IPv6 et d'autre part le PC qui sert de routeur Multicast IPv6. Contenu du fait que tous les routeurs n'implémentent pas le Multicast IPv6, on établit des tunnels entre les routeurs Multicast et les paquets Multicast IPv6 sont donc encapsulés dans des paquets IPv6 Unicast ou IPv4 Unicast. Sur le routeur Multicast, on configure une route par défaut qui envoie les paquets à l'autre bout du tunnel.



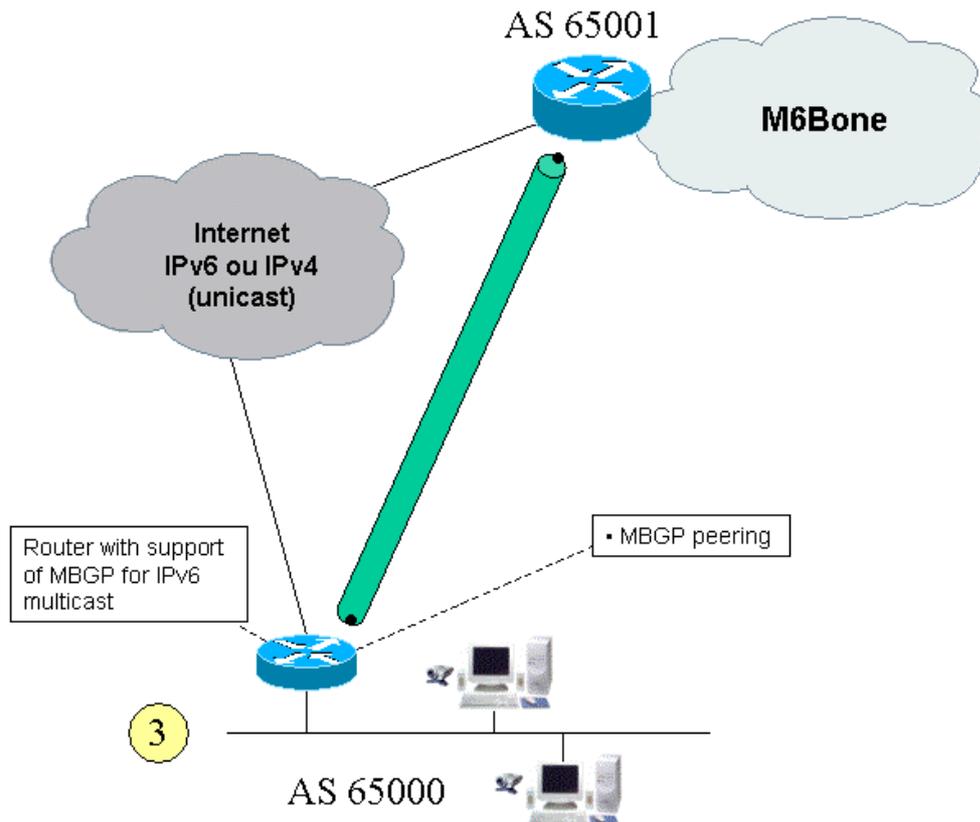
Cas n°2 : L'équipement implémente une MRIB

Autrement dit, on est dans le cas où on a un routeur qui implémente effectivement des routes Multicast. C'est le cas des routeurs 6100 ou 6200 du constructeur français 6WIND ainsi que de quelques IOS de cisco. Dans ce cas, nul besoin d'avoir 2 routeurs puisque le même routeur gère l'Unicast et le Multicast.



Cas n°3 : L'équipement implémente MBGP

Certains routeurs implémentent le protocole de routage MBGP qui gère le Multicast IPv6. On peut alors établir un peering MBGP avec le routeur du site demandeur. De même que dans le cas n°2, un seul routeur est nécessaire.



Méthodologie :

Quand je suis arrivé au GIP RENATER, les demandes de connexion au M6bone étaient traitées au cas par cas et prenaient beaucoup de temps. Une réflexion de fond avec Jérôme Durand nous a permis de distinguer les 3 cas cités ci-dessus et de produire des documents et des procédures pour chacun d'eux permettant de rendre plus efficaces et plus simples les connexions des sites au M6Bone.

B-3/ Mes actions au sein de l'équipe M6bone :

Après un long travail pour comprendre l'existant et les problématiques relatives à la gestion du réseau mondial Multicast IPv6, à savoir le M6Bone, j'ai travaillé en collaboration avec Jérôme Durand sur diverses tâches visant à développer le réseau.

Organisation :

Chaque semaine, nous avons une réunion pour faire le point sur l'avancement des tâches, les nouvelles tâches à effectuer, les nouveaux objectifs, les délais, les problèmes rencontrés. Très vite, nous avons éprouvé le besoin de mettre en place une fiche de suivi des tâches. Ci-dessous un extrait :

| ACTION | CREATION | ETAT | DEADLINE | FIN | PRIORITE | REMARQUES |
|---|----------|----------|------------|--------|-------------|---|
| Créer fiche de suivi de mes tâches sur le M6one | 21-oct | FINI | | 21-oct | | |
| Donner ses remarques sur l'article de France telecom | 21-oct | FINI | 30/10/2003 | 30-oct | TRES URGENT | |
| Faire un script qui envoie un mail aux peers qui ont leur connexion down. | 21-oct | EN COURS | | | | |
| Rendre automatique la relance du demon zebra et ripngd sur xcast | 21-oct | FINI | 07/11/2003 | 30-oct | | |
| Ecrire un script qui permet simplement de configurer les tunnels en modifiant tous les fichiers concernés | 21-oct | Annulé | | | | Intérêt limité par rapport au temps que ça prend. |
| Configurer le tunnel de Luc Beurton (Université Bretagne sud) | 22-oct | FINI | 23-oct | 23-oct | URGENT | |
| Page pour expliquer la connexion au M6bone | 22-oct | EN COURS | | | | |

Pour l'anecdote, cette fiche a été reprise par Bernard Tuy, responsable du groupe SIPA (Services IP avancées) de RENATER pour planifier les tâches des différents membres du groupe.

Nature des tâches :

A/ Site web www.m6bone.net : Remettre à jour certaines pages du site web, ajout de nouvelles rubriques, en anglais...

Exemple: j'ai notamment rajouté une section FAQ (Frequently Asked Questions) concernant l'utilisation du Multicast IPv6 et développer une procédure à destination des utilisateurs pour résoudre les problèmes rencontrés. Globalement, l'idée est de procéder comme suit :

- 1/ Je cherche la réponse à ma question dans la liste du FAQ.
- 2/ Si je ne la trouve pas, j'envoie un mail à toute la communauté des utilisateurs.
- 3/ Une fois mon problème résolu, j'envoie un mail au Webmaster afin qu'il rajoute la solution dans la section FAQ afin de faire partager mon expérience avec tout le monde.

B/ Assistance technique: Répondre aux nombreux mails des utilisateurs de la communauté M6bone. Il s'agit notamment de leur apporter des informations techniques ou pas d'ailleurs, le plus souvent en anglais.

Exemple: voici l'extrait d'un mail comme on en reçoit plusieurs par jour.

```
>>Hi,  
>>How are you?  
>>I have upgraded our m6bone router to FreeBSD 4.8  
>>Now, I can see with the sdr the m6bone sessions but I can't see  
>>two local sessions between them. Each one in a different interface,  
>>fxp1 and gif3.  
>>Any idea?
```

C/ Documentation : Il s'agit de produire des documents techniques à destinations de lecteurs divers : utilisateurs du M6bone, 6WIND, autres personnes du GIP RENATER etc... Il m'est arrivé aussi d'avoir à relire un document de France Telecom concernant une démonstration qu'ils ont réalisé en IPv6 Multicast.

Exemple : J'ai travaillé sur un document présentant les différents cas de déploiement d'une connexion Multicast IPv6, afin d'expliquer simplement aux utilisateurs le fonctionnement des connexions au M6Bone.

D/ Supervision du réseau : Il s'agit de mettre en place un ensemble d'outils pour améliorer la supervision du réseau.

Exemple : J'ai programmé un script en shell qui vérifie l'état des connexions des sites au M6Bone. Lorsque une connexion « tombe », le script envoie automatiquement un mail à l'administrateur du site pour l'informer.

E/ Mise en place de connexions vers les sites demandeurs : pour avoir une connexion, les sites remplissent un formulaire sur le site Web du M6Bone, géré par Jérôme Durand et moi-même. A réception de ce formulaire, nous configurons notre routeur central afin de créer un tunnel avec le site afin de lui fournir la connectivité IPv6 Multicast.

Exemple : Au départ, j'ai mis beaucoup de temps à me familiariser avec toutes les subtilités des configurations. En effet, il y a de nombreux fichiers à configurer (Access list, adressage, routage, backup, etc...) et des commandes à connaître pour tester le bon fonctionnement. Au fur et à mesure, je me suis familiarisé à l'ensemble et à la fin du stage, j'étais capable de traiter une demande dans son intégralité. J'ai par exemple mis en place une connexion avec l'Arabie Saoudite.

Conclusion :

Cette expérience était riche sur tous les aspects (technique, travail en groupe, organisation et communication). En effet, j'ai beaucoup appris à propos du protocole IPv6 et des réseaux en général à travers la mise en place de la plate-forme que j'ai évoquée dans mon rapport. Ces connaissances concernent les spécifications du protocole IPv6, de son fonctionnement (autoconfiguration, adressage, routage...) et de son déploiement. J'ai pu aussi renforcer, les bases théoriques acquises à l'INSA de Lyon concernant les réseaux et leurs architectures en travaillant sur divers aspects.

Les différentes tâches réalisées sur le réseau M6Bone m'ont permis de beaucoup apprendre à propos du Multicast IPv6, des différents protocoles mis en œuvre pour faire fonctionner ce service (PIM, MLD...) et des applications de visioconférence (SDR, VIC, RAT...). Je me suis considérablement amélioré au niveau de la recherche d'informations et des spécifications techniques à propos des technologies réseaux. Je me suis aussi habitué à la documentation technique réalisée par l'IETF (drafts et RFC)

J'ai eu la chance de travailler en groupe à plusieurs reprises : Collaboration avec des sites connectés au M6Bone répartis sur des dizaines de pays dans le cadre du développement du réseau et avec des équipementiers comme CISCO et 6WIND dans le cadre de la mise en place de la plate-forme. En outre, pendant ce stage, j'étais contraint de réaliser plusieurs tâches en parallèle et travailler sur différents aspects, ce qui m'a appris à m'organiser et à bien gérer mon temps.

En conclusion, ce stage s'est révélé très formateur sur tous les aspects. Pour être sincère, mon objectif, en parallèle de ma formation en 3 ans du cycle ingénieur à l'INSA, était de trouver quel type de carrière me plairait le plus parmi les 2 que j'avais identifié :

- Une carrière d'expert technique, dans le domaine de la recherche sur une technologie donné, en commençant donc par un stage long très pointu dans un laboratoire (RENATER).
- Une carrière de manager dans les nouvelles technologies, en me formant donc à des domaines aussi divers que la finance, le marketing ou le droit.

J'ai donc entrepris de tester les deux extrêmes dans le but de trouver la réponse à la question que je me pose : « qu'est-ce que je vais faire après l'obtention de mon diplôme ». Au second semestre, j'ai choisi de suivre exclusivement des cours de management lors de mon échange universitaire aux Etats-Unis. Au-delà de tout ce que j'ai pu apprendre lors de ce stage, j'aurais surtout pu vivre au moins une fois l'une des deux possibilités de mon orientation professionnelle. Quant à savoir quel choix définitif je ferais, j'attendrais d'expérimenter la formation en management pour me décider : réponse dans 6 mois.

Bibliographie

Livres :

Deploying IP Multicast Networks (Volume 1)
Beau Williamson, Cisco Press

IPv6, Théorie et Pratique
Gizelle Cizeault (Ouvrage du G6), O'Reilly

Sites web :

Site de RENATER
<http://www.RENATER.fr>

Site du M6bone
<http://www.m6bone.net>

Site de l'association Aristote
<http://www.aristote.asso.fr>

Site du G6
<http://www.g6.asso.fr>

Site de FreeBSD
<http://www.freebsd.org>

Site de 6wind
<http://www.6wind.com>

Site de Zebra
<http://www.zebra.org>

Site des JRES
<http://www.jres.org>

Site de Kame
<http://www.kame.net>

Site des RFC de l'IETF
<http://www.ietf.org/rfc.html>

Site personnel de Konstantin Kabassanov du Lip6 pour sa rubrique « Mtools ».
http://www-rp.lip6.fr/~kabassan/index_fr.html

Site de l'UCL (University College of London) pour télécharger les Mtools (VIC, RAT, SDR)
<http://www-mice.cs.ucl.ac.uk/multimedia/software/>

Annexes

1) Configuration du 6WIND aux JRES 2003 :

Fichier pim6sd.conf:

```
static_rp ff0E::/16 2001:660:3007:300:1:: priority 1;
static_rp ff1E::/16 2001:660:3007:300:1:: priority 1;
static_rp ff3E:30:2001:700::/64 2001:700:e000:501::2 priority 0;
```

Fichier clingpp.sh :

```
kill -15 `cat /var/run/pim6sd.pid` >/dev/null 2>&1
/usr/admin/advanced/pim6sd -c /usr/admin/advanced/pim6sd.conf -V 1
ifconfig6 -mld setdaemon
```

Fichier de routage :

```
#####
# GENERAL #
#####
```

```
# GEN STATEMENT
  hostname kriska
  domainname IPv6.jres.org
  enable ipv4forwarding
  enable IPv6forwarding
  disable telnet
  enable ssh
  disable http_config
```

```
#####
# INTERFACES #
#####
```

#configuration de l'interface eth0_0

```
eth0_0
  # IPV4 ADDRESS
  ipaddress 193.50.84.49/24
  # IPV6 ADDRESS
  ipaddress 2001:660:b101:ffff::2/64
  # IPV6 PREFIX
  # INTERFACE STATEMENT
  intf up
  disable autoconfv6
  mtu default
```

```
tcp4mss disable
tcp6mss disable
disable ipsec
disable qos in
disable qos out
enable arp
enable ndp
router_advert smart 30000 1800 none 0 yes
```

#configuration de l'interface eth1_0

```
eth1_0
# IPV4 ADDRESS
ipaddress 193.50.84.41/29
# IPV6 ADDRESS
ipaddress 2001:660:b101:1::1/64
# IPV6 PREFIX
prefix 2001:660:b101:1::/64
# INTERFACE STATEMENT
intf up
disable autoconfv6
mtu default
tcp4mss disable
tcp6mss disable
disable ipsec
disable qos in
disable qos out
enable arp
enable ndp
router_advert smart 30000 1800 none 0 yes
```

```
#####
# MIGRATION #
#####
```

#configuration du tunnel IPv6 dans IPv4

```
# 6IN4 TUNNELS
6in4 1 193.50.84.49 194.254.101.6 2001:660:3007:603:2:: 2001:660:3007:603:1::

# 4IN6-6IN6 TUNNELS

# 6TO4 TUNNELS

# AUTOMATIC TUNNELS

# ISATAP_ROUTER

# ISATAP_PREFIX
```

```
#####  
# ROUTE #  
#####
```

#configuration du routage**# DYNAMIC ROUTING PROTOCOLS**

```
dynamic  
#  
router rip  
redistribute connected  
network 193.50.84.0/24  
network 193.50.84.40/29  
#  
router ripng  
default-information originate  
network 2001:660:b101:1::/64  
redistribute connected  
#  
router bgp 65094  
neighbor 2001:660:3007:603:1:: remote-as 1717  
neighbor 2001:660:3007:603:1:: soft-reconfiguration inbound  
#  
address-family IPv6 Multicast  
network 2001:660:b101::/48  
neighbor 2001:660:3007:603:1:: activate  
neighbor 2001:660:3007:603:1:: soft-reconfiguration inbound  
exit-address-family  
#  
router ospf  
#  
router ospf6  
ospf6 router-id 0.0.0.0  
#  
exit-dynamic
```

DEFAULT ROUTE

```
ipv4_defaultroute 193.50.84.1  
IPv6_defaultroute 2001:660:b101:ffff::1
```

DEFAULT MULTICAST ROUTE

```
IPv6_defaultmroute none
```

IPV4 ROUTE**# IPV6 ROUTE****# IPV6 MULTICAST ROUTE****# LOG**

2) Commandes spécifiques aux routeurs 6WIND

Créer une nouvelle configuration nommée « test » :

```
hurricane}{new conf test
```

Visualiser la configuration la configuration test:

```
hurricane}{display conf test
```

Editer la configuration test :

```
hurricane}{edit conf test
```

Pour rentrer dans le menu général:

```
hurricane{test}gen
```

Et afficher son contenu :

```
hurricane{test-gen}display
```

Pour obtenir la configuration des interfaces :

```
hurricane}{show interface
```

Pour configurer l'interface eth0 :

```
hurricane{test}eth0_0  
hurricane{test-eth0_0}display
```

Pour rentrer une adresse IPv6:

```
hurricane{test-eth0_0}ipaddress 2001:660:3001:8102::1/64  
hurricane{test-eth0_0}prefix 2001:660:3001:8102::/64
```

Pour rentrer dans le menu routage:

```
hurricane{test}rtg
```

Pour rentrer dans le menu routage dynamique :

```
hurricane {test-rtg}dynamic
```

Pour sauvegarder une configuration :

```
hurricane}{copy running start
```

Plus généralement :

- il suffit de taper « ? » pour connaître les commandes disponibles.
- On tape « exit » pour revenir dans le menu supérieur
- On tape « delete » + la commande à effacer.

3) Configuration du routeur PC sous FreeBSD aux JRES 2003 :Fichier zebra.conf:

```
! Zebra configuration saved from vty
! 2004/01/08 15:40:04
!
hostname affligem-zebra
password 8 bJFoEOB0obLL6
enable password 8 4DwwIFdKLWvU.
service password-encryption
!
interface xl0
IPv6 address 2001:660:b101:1::53/64
ip address 193.49.159.169/29
IPv6 nd suppress-ra
!
interface xl1
IPv6 address 2001:660:b101:2::53/64
no Multicast
no IPv6 nd suppress-ra
IPv6 nd prefix-advertisement 2001:660:b101:2::/64 86400 86400 onlink autoconfig
!
interface x10
IPv6 nd suppress-ra
!
ip route 0.0.0.0/0 193.50.84.41/29
!
```

Fichier ripngd.conf :

```
! Zebra configuration saved from vty
! 2003/11/13 12:02:40
!
hostname affligem-ripngd
password zebra
log stdout
!
router ripng
network xl0
passive-interface xl1
redistribute connected
!
```

4) Commandes spécifiques à l'OS FreeBSD

Dans le fichier /etc/rc.conf, on rajoute les lignes suivantes :

Pour pouvoir utiliser IPv6 :

```
IPv6_enable= « YES »
```

Pour pouvoir utiliser la machine comme routeur IPv6 :

```
IPv6_gateway_enable= « YES »
```

Pour configurer les interfaces réseau :

```
IPv6_ifconfig_xl1="2001:660:3001:8102:204:76ff:fe0:ac1 prefixlen 64"  
IPv6_ifconfig_xl2="2001:660:3001:8101::1 prefixlen 64"
```

Pour configurer une route par défaut :

```
IPv6_defaultroute="2001:660:3001:8102:201:3ff:fe83:7d09"
```

Pour configurer une route statique :

```
IPv6_route_mynet="2001:660:3001:8101:: prefixlen 64 ::1"
```

5) Installation et configuration d'Apache 2.0.48

Apache 2.0.48 peut être téléchargé sur le site <http://www.apache.org>

Installer le package `httpd-2.0.48.tar.gz` dans le répertoire `/usr/local/src/`

Décompresser le package :

```
gunzip -c > httpd-2.0.48.tar httpd-2.0.48.tar.gz  
tar -xvf httpd-2.0.48.tar httpd-2.0.48
```

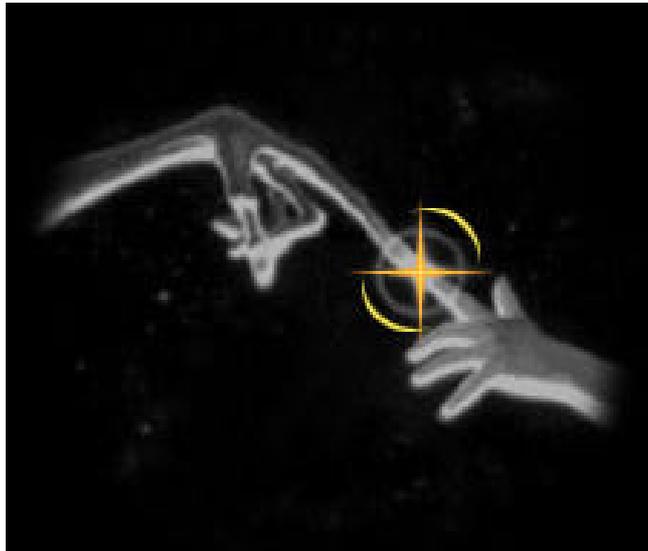
Aller dans le répertoire extrait `httpd-2.0.48`, et lancer les commandes suivantes qui permettent d'installer Apache :

```
./configure --prefix=/usr/local  
make  
make install
```

Enfin pour lancer Apache, on exécute la commande suivante :

```
/usr/local/bin/apachectl start
```

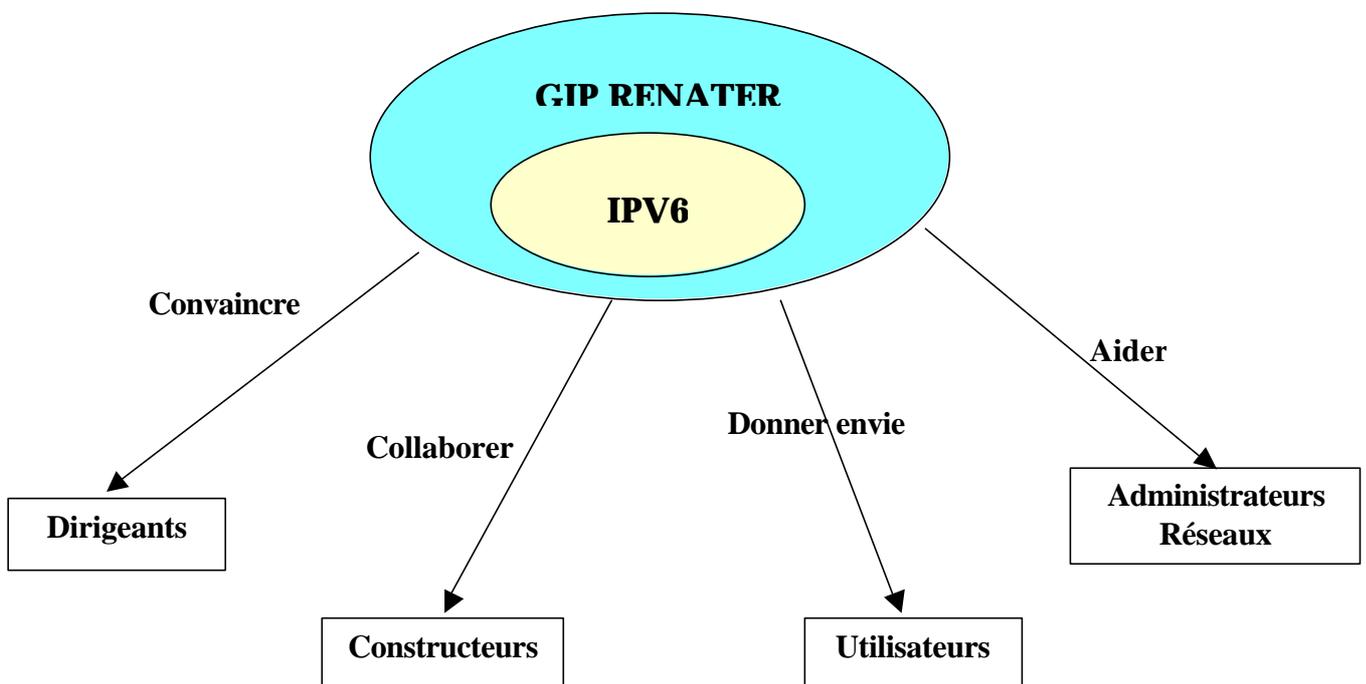
Stratégie de communication sur une nouvelle technologie



Intro:

Mon stage au GIP RENATER était axé principalement autour de IPv6 (Internet Protocol version 6), la nouvelle version du protocole Internet. RENATER agit activement pour le développement d'IPv6 en France et partout dans le monde. Un outil fondamental lorsque une nouvelle technologie est déployée est la communication. C'est la raison pour laquelle j'ai choisi comme thème d'étude pour mon rapport des humanités « la stratégie de communication » et plus précisément la communication sur une nouvelle technologie, en me basant sur ce que j'ai pu observer lors de mon stage.

En communication, ce qui importe n'est pas tant ce qu'on dit mais ce que comprend l'interlocuteur. Pour bien comprendre le sens de la stratégie de communication, on pourrait faire une analogie avec la stratégie de vente d'un nouveau produit où il convient de segmenter l'ensemble des clients en plusieurs groupes homogènes afin d'adapter l'emballage et le message à chaque groupe. De même, dans la stratégie de communication sur une nouvelle technologie, l'objectif, la forme, le degré de technicité du message sont différents selon l'interlocuteur. RENATER l'a bien compris et suit une stratégie de communication pour promouvoir IPv6.



Communiquer avec les administrateurs réseaux.

L'objectif est de les rassurer. Le jour où un réseau donné migre de IPv4 à IPv6, une chose est sûr, c'est l'administrateur réseau qui aura la tâche de réaliser cette entreprise alors que la décision ne vient pas de lui. En effet, deux cas sont envisageables : soit la demande vient de dessous, c'est à dire que c'est les utilisateurs qui demandent à avoir telle ou telle nouvelle technologie sur leur poste de travail, soit ça vient de dessus, c'est à dire que c'est un ordre de la direction qui a pris la décision d'investir dans telle technologie.

Pour l'instant, les administrateurs réseaux ne reçoivent pas de pression importante ni d'en haut ni d'en bas pour intégrer IPv6 et sont donc tenter de mettre le projet de coté. Cela s'explique d'une part par le fait que la migration d'IPv4 à IPv6 ne leur semble pas indispensable pour l'heure et d'autre part qu'ils ont une charge de travail très conséquente, dans le milieu académique surtout.

Le message que RENATER envoie aux administrateurs réseaux est qu'il faut commencer à migrer le plus tôt possible à IPv6 pour s'y familiariser progressivement sachant qu'il y aura une période de cohabitation entre IPv4 et IPv6. Pour les encourager dans cette optique, la communication est tournée vers la pratique : « comment faire ? ». C'était notamment l'objectif du tutoriel auquel j'ai participé aux JRES 2003 à Lille et où on leur a présenté une plate-forme de tests IPv6 en donnant des informations techniques comme par exemple des exemples de configurations de routeurs IPv6.

Communiquer avec les dirigeants.

L'objectif est de leur montrer les enjeux stratégiques et économiques du protocole IPv6. Comme expliqué ci-dessus, la décision d'intégrer IPv6 dans son réseau viendra forcément des décideurs : politiciens, directeur informatique ou directeur général. C'est donc un publique fortement stratégique et où la communication est un enjeu capital.

Ce qui intéresse principalement un décideur, c'est ce qu'une nouvelle technologie pourrait apporter à son entreprise en terme de rentabilité économique. RENATER adopte donc un message techniquement simple et accessible et qui est orienté vers les avantages pour l'entreprise : avance technologique par rapport aux concurrents ou au contraire risque d'être en retard au niveau de la veille technologique. Pour les politiques, il convient de les impliquer dans une stratégie à l'échelle nationale et internationale. En effet, RENATER fournit le service IPv6 sur son épine dorsale mais c'est ensuite le rôle des autorités régionales d'offrir la connexion aux sites. De même, il existe des enjeux internationales comme les collaboration entre les pays européens ou entre la France et les pays d'Asiatiques dans le déploiement d'une nouvelle technologie. Pour l'anecdote, les Etats-Unis tardent à s'intéresser à IPv6 pour des raisons historiques et c'est peut-être là l'occasion de marquer une avance technologique.

Le salon INTEROP, qui a eu lieu à Paris en novembre 2003 est une bonne illustration de cette communication. C'était l'occasion pour RENATER de communiquer avec Claudie Haigneré, ministre délégué à la recherche et aux nouvelles technologies, et avec des responsables de divers entreprises, présentes sur le salon. On peut aussi évoquer la présence de représentants de RENATER lors de certains sommets européens, à Bruxelles.

Communiquer avec les constructeurs.

Parallèlement à la stratégie d'augmenter la demande en IPv6, il est nécessaire de s'assurer que l'offre suive ou même anticipe cette demande. Plus concrètement, il s'agit d'accompagner les constructeurs de matériel réseau et plus globalement toutes les entreprises dont les produits peuvent avoir un lien avec IPv6.

Il s'agit donc de collaborer avec des entreprises comme Alcatel, France Telecom, CISCO, CS, JUNIPER ou 6WIND dans le développement de matériels, de routeurs et d'implémentations de protocoles relatifs à IPv6. Durant mon stage, j'ai pu assister à une réunion du G6 (cf. partie « acteur d'IPv6 ») où le monde de la recherche travaillait conjointement avec des industriels et où des chercheurs du LIP6 ou de l'INRIA pouvaient confronter leurs points de vue avec des industriels. Evidemment, le but d'une entreprise est de réaliser du chiffre alors que celui d'une équipe de recherche est de réaliser des prouesses technologiques. Cependant, les deux trouvent un intérêt commun dans le sens où les industriels tirent profit des travaux des chercheurs et ces derniers trouvent un intérêt à ce que la croissance économique des premiers financent indirectement leurs recherches. Pour RENATER, il s'agit notamment de communiquer avec les constructeurs sur les résultats des tests qu'on réalise sur leurs produits, de donner un retour des expériences diverses des utilisateurs d'IPv6 et de les conseiller pour ne pas dire tenter de les convaincre de développer telle ou telle fonction technique.

Communiquer avec les utilisateurs.

IPv6 est une technologie qui intervient au niveau du transport de l'information. Autrement dit, elle est transparente pour les utilisateurs d'Internet au sens où elle n'apporte aucun changement remarquable dans l'usage même de l'Internet : l'internaute ne verrait pas de gros changement sur l'écran de son ordinateur et ne remarquerait pas la nouveauté. Pour prendre une image relative au transport du courrier, si la Poste changeait tous ses vélos pour un nouveau modèle, les employés de la Poste travailleront autrement, mais la personne qui reçoit son courrier ne remarquerait pas forcément de grande différence, du moins dans l'immédiat. En somme, il n'y a pas encore de « killer application » IPv6, c'est à dire une application qui rencontrerait un grand succès mais qui ne pourrait fonctionner sans la technologie IPv6 et qui pousserait de facto les usagers à réclamer des connexions en IPv6.

Ceci ayant été dit, vous aurez compris que RENATER ne concentre pas sa communication auprès du grand public, et peu d'internautes connaissent aujourd'hui la signification du mot IPv6. Par contre, on trouve quand même des utilisateurs de IPv6 en France et dans le monde. Il s'agit la plupart du temps de personnes du milieu universitaire et de la recherche qui désirent apprendre et tester IPv6. C'est la raison pour laquelle, sans avoir forcément une communication offensive envers ce public, RENATER met à disposition des utilisateurs potentiels les informations nécessaires à travers le site WEB www.RENATER.fr où l'on trouve des documents et de nombreuses vidéos, rendus publiques et très accessibles pour commencer à se former à IPv6.

Nous avons vu que dans le cas des administrateurs réseaux, la migration à IPv6 s'apparentait à une tâche tandis que dans le cas des dirigeants, il s'agissait d'une stratégie et d'un investissement. Dans le cas des utilisateurs, la raison est plus subjective et donc la communication n'a plus pour objectif de rassurer, de former ou de convaincre mais plutôt de séduire. C'est pourquoi la communication envers les utilisateurs se doit d'être convaincante sur la forme. Il s'agit par exemple de faire une démonstration d'une vidéoconférence

fonctionnant en IPv6 lors d'évènements comme le salon INTEROP, les JRES (Journées Réseaux), ou les causeries RENATER qui ont lieu régulièrement et qui sont retransmis sur Internet avec la technologie IPv6.

Des outils nombreux et adaptés :

Souvent, l'image populaire d'un laboratoire de recherche est celui d'un groupe d'individus enfermés dans un monde compris d'eux seuls et totalement indifférents vis à vis de l'environnement extérieur. De ce que j'ai vu à RENATER, il n'en est rien. RENATER a su développer tout un ensemble d'outils de communication.

D'abord, il y a énormément de documents, imprimés sur du papier de qualité et en couleur, avec des informations claires et des images pour expliquer rapidement et simplement qui est RENATER et qu'est-ce qu'IPv6. Ces documents sont massivement distribués lors des salons, expositions et autres événements, envoyés sur demande par courrier, et sont également disponible sur le site WEB www.RENATER.fr. D'ailleurs lors des évènements, un ensemble de cadeaux à l'effigie de RENATER sont offerts : stylos, tasses, poster

Le site WEB est d'ailleurs très complet et propose des vidéos de bonne qualité, qui ont été filmées lors de conférences ou de causeries RENATER. Les causeries RENATER sont des conférences virtuelles, qui ont lieu plusieurs fois par mois et qui sont retransmis sur RENATER en IPv6.

Des réunions diverses, à l'initiative des membres de RENATER, ont lieu régulièrement : des réunions du G6 pour les « spécialistes » rassemblent chercheurs et industriels et des réunions du GN6, le groupe français des néophytes en IPv6, rassemblent des chercheurs et des universitaires intéressés dans l'expérimentation et les tests d'IPv6. Dans le cadre du M6Bone, le service Multicast d'IPv6, il y a également des meetings virtuelles, par vidéoconférence, qui rassemblent des initiés du monde entier.

Enfin des mailing listes permettent de fédérer les connaissances et les expériences de leurs membres afin que chacun participe au développement d'IPv6.

Bilan :

Il existe plusieurs philosophies quant au succès d'un nouveau produit ou d'une nouvelle technologie. La pensée idéaliste voudrait que les meilleures technologies supplantent naturellement les moins intéressantes. Dans la réalité, ce n'est évidemment pas toujours le cas. A l'inverse, la philosophie sceptique explique que seules les technologies qui ont le support des leaders du marché ont une chance. Même si c'est malheureusement parfois vrai, on assiste quelque fois à l'émergence d'un produit développé par un outsider, un nouveau groupe méconnu. La réalité est entre ces deux extrêmes.

Mon analyse me permet de dire que la communication est un élément insuffisant mais nécessaire. En effet, même si la communication sur une nouvelle technologie est irréprochable, il faut que cette nouvelle technologie apporte réellement un nouvel intérêt. C'est sans doute pour cela qu'il arrive de constater des échecs, y compris chez les grands constructeurs et ce malgré une communication massive et puissante.

A l'inverse, beaucoup de projets ne verront jamais le jour, bien que fondamentalement très intéressant et ce, parfois à cause d'une communication insuffisante ou mal ciblée.

En tout cas, l'avenir d'IPv6 est très prometteur à la fois parce qu'il apporte une nouveauté incontestablement nécessaire et aussi parce que RENATER continue de fournir des efforts importants au niveau de sa communication.