Un exemple de généralisation opérationnelle à grande échelle d'IPv6 sur un réseau métropolitain

Philippe Pegon
Centre Réseau Communication, Université Louis Pasteur
Philippe.Pegon@crc.u-strasbg.fr

Résumé

En 2001, le CRC (Centre Réseau Communication), opérateur du réseau métropolitain Osiris, a initié un déploiement à grande échelle du protocole IPv6. Le mot d'ordre pour ce projet était « IPv6 = IPv4 », signifiant que les performances de l'infrastructure réseau, la facilité d'exploitation et les services associés doivent être au même niveau pour IPv6 que pour IPv4.

Après avoir conçu un plan d'adressage pratique et extensible, ainsi qu'une architecture de routage, nous avons v6-ifié les services d'infrastructure, jusqu'au réseau sans fil en passant par l'accès VPN, procurant ainsi à nos utilisateurs une riche palette de services. Nous sommes à présent engagés dans une démarche de formation de nos correspondants pour aller jusqu'aux postes clients.

Nous retraçons dans cette contribution notre démarche, les problèmes rencontrés et les solutions que nous avons apportées. Nous avons trouvé que les implémentations d'IPv6 ont suffisamment mûri pour qu'il soit raisonnable de mettre en place ce protocole dans les conditions réelles d'un réseau métropolitain.

Mots clefs

IPv6, déploiement, réseau métropolitain, VPN, réseau sans fil, messagerie, routage, formations, plan d'adressage.

1 Introduction

Le réseau métropolitain universitaire Osiris rassemble 17 établissements situés sur le territoire de la Communauté Urbaine de Strasbourg. Il connecte 110 bâtiments à 1 Gb/s (ou 100 Mb/s) directement à la dorsale multi-gigabits, pour un total de 50 000 utilisateurs potentiels, et environ 25 000 machines aujourd'hui déclarées dans le DNS.

Le Centre Réseau Communication (CRC), service de l'Université Louis Pasteur en charge de l'exploitation d'Osiris, s'est engagé très tôt dans une démarche volontariste de déploiement du protocole IPv6 à grande échelle.

Si mettre en place IPv6 à titre expérimental sur un petit réseau de quelques machines est raisonnablement facile, il en va tout autrement de la mise à disposition de la mise à disposition de la connectivité vers plus de 200 sous-réseaux et un grand nombre de machines, avec toute la palette de services associés (DNS, messagerie, mais également réseau sans-fil, VPN, etc.). Les problématiques deviennent alors la performance, la facilité d'exploitation au quotidien, ainsi que la couverture fonctionnelle des services. Le mot d'ordre est alors « IPv6 = IPv4 », signifiant que tout ce qui est disponible en IPv4 doit l'être dans les mêmes conditions en IPv6. La conception générale de l'architecture doit dès lors être pensée pour répondre à l'ensemble des problématiques citées.

Nous avons pû profiter de conditions favorables comme une volonté politique du directeur, la proximité d'un laboratoire de recherche travaillant sur ce protocole, la maturité grandissante des implémentations et l'opportunité de renouveler les équipements actifs de cœur de réseau. Nous avons pu travailler dès 2001 sur la mise en place d'IPv6 sur Osiris. Avec la mobilisation de l'ensemble de l'équipe, dont chaque membre a intégré IPv6 dans les projets dont il était responsable, nous disposons aujourd'hui d'une couverture de services quasiment complète.

Cet article résume tout le travail accompli pour ce déploiement à grande échelle, en espérant que notre expérience, les problèmes rencontrés et les solutions apportées, puissent bénéficier à d'autres. Nous avons fait un effort constant de documentation de notre progression, accessible à l'adresse www-crc.u-strasbg.fr/osiris/ipv6/

2 Historique

Le protocole IPv6 a été mis en place sur Osiris à la fin des années 1990. Comme sur beaucoup de sites, cette mise en œuvre se limitait au transport d'un tunnel de manière opaque par le CRC pour le compte du LSIIT (Laboratoire des Sciences de l'Image, de l'Informatique et de la Télédétection) qui disposait d'un routeur IPv6 sur un système BSD. En 2001, cette situation a évolué vers un ELAN ATM de backbone et nous avons mis en place nos premiers routeurs IPv6 sous FreeBSD. Nous avons alors entamé une réflexion pour sortir du stade expérimental et déployer ce protocole à grande échelle sur Osiris. L'objectif de pouvoir disposer d'IPv6 dans tous les sous-réseaux nous a amenés à diviser les actions en 3 grandes catégories :

- l'infrastructure réseau (adressage, routage)
- les services associés (DNS, messagerie, applications spécifiques)
- les formations nécessaires pour promouvoir le déploiement d'IPv6 dans les établissements.

3 L'infrastructure réseau

Malgré la littérature abondante sur les mécanismes de transition d'IPv6, il nous a semblé évident qu'Osiris devait être un réseau à double pile IPv4 et IPv6 (*dual stack*), car Osiris n'est pas encore concerné par la pénurie d'adresses IPv4, et les systèmes capables de fonctionner uniquement en IPv6 ne sont pas encore légion.

Cette section présente les différents éléments de v6-ification de l'infrastructure réseau : les équipements de la dorsale, le plan d'adressage, les protocoles de routage et les

services de connectivité réseau associés que sont le VPN et le réseau sans-fil.

3.1 La dorsale

En 2003, nous avons publié un appel d'offres pour renouveler l'ensemble des équipements actifs de cœur du réseau Osiris. Le support du protocole IPv6, à un niveau comparable à ce que nous connaissons sous IPv4, était un prérequis indispensable explicitement fixé dans le CCTP. Après les tests de l'ensemble des solutions proposées par les fournisseurs, nous avons retenu des routeurs Juniper (M20) et des commutateurs Cisco (Catalyst 4500).

Parallèlement, nous avons mené un travail important de réflexion sur la mise en œuvre concrète d'IPv6 sur Osiris, en particulier sur le plan d'adressage et sur les protocoles de routage.

3.2 Le plan d'adressage

Nous avons tout d'abord demandé à Renater l'allocation d'un préfixe pour chaque établissement, ainsi que pour la dorsale. Les retours d'expérience sur les questions d'adressage étant rares [1], nous avons imaginé un plan d'adressage simple, structuré et ouvert sur l'avenir, applicable à tous les établissements Osiris, résumé sur la figure 1.

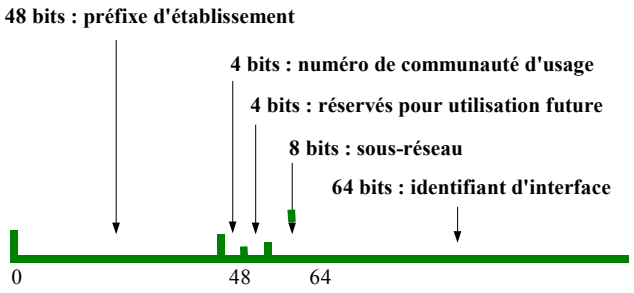

Figure 1 – *plan d'adressage en vigueur sur Osiris*

Les 48 premiers bits représentent le préfixe d'établissement, tel qu'alloué par Renater.

Les 4 bits suivants représentent le numéro de « communauté d'usage » et peuvent prendre les valeurs suivantes :

0x0	dorsale
0x1	recherche
0x2	enseignement
0x3	administration
0x4	gestion technique (supervision, téléphone, etc)
0x5-0xE	réservé
0xF	expérimentation

Les 4 bits suivants sont réservés, laissant ainsi la place pour étendre ultérieurement le plan d'adressage.

Les 8 bits suivants représentent le numéro de sous-réseau attribué séquentiellement par le CRC.

Quelques exemples de préfixes pris parmi des sous-réseaux d'Osiris permettent d'illustrer notre plan d'adressage :

– Un laboratoire de l'ULP : 2001:660:4701:100A::/64

  Les 48 premiers bits (2001:660:4701) représentent le préfixe alloué par Renater pour l'ULP. Dans 100A, la valeur 1 pour la communauté d'usage indique un réseau utilisé pour la recherche, les 4 bits réservés pour une utilisation future sont à 0, et la valeur hexadécimale A pour le numéro de sous-réseau signifie qu'il est le 10e dans cette catégorie.

– Un réseau pédagogique d'une UFR de l'ULP : 2001:660:4701:2002::/64

  Dans 2002, la première valeur 2 signifie que c'est un réseau à vocation pédagogique, les 4 bits réservés pour une utilisation future sont à 0, et la dernière valeur 2, pour le numéro de sous-réseau, signifie que c'est le 2e réseau de l'ULP a avoir été alloué dans cette catégorie.

Conformément au format des adresses IPv6, les 64 derniers bits identifient la machine dans le réseau (identifiant d'interface EUI 64). Nous avons réservé la plage 00FF:0000:0000:0000 à 00FF:FFFF:FFFF:FFFF pour les équipements réseau. En particulier, l'adresse :FF:: est dédiée à la passerelle par défaut, ce qui est très facile à mémoriser et à taper. Pour illustrer ce propos, la passerelle par défaut du dernier exemple est 2001:660:4701:2002:FF::

La version initiale du plan d'adressage réservait une adresse de passerelle résultant en un bit U (7e bit de l'identifiant d'interface) à 1, caractéristique d'une adresse autoconfigurée. Nous avons rapidement rencontré des problèmes avec Windows sur les postes clients qui refusait alors d'adresser directement la passerelle (le routage fonctionnait bien, mais il était impossible d'adresser directement à la passerelle, avec ping par exemple). La nouvelle adresse que nous avons choisi (:FF::) ne présente plus ce problème.

Les réseaux d'interconnexion entre les routeurs ainsi que les adresses de loopback utilisent le préfixe de dorsale alloué par Renater et suivent la règle générale à l'exception des 64 derniers bits : ils sont égaux à 1 ou à 2, sauf pour les adresses de loopback (::FF), comme représenté sur la figure 2, où les adresses de loopback sont en italiques, et les adresses pour les réseaux d'interconnexion sont en caractères droits.

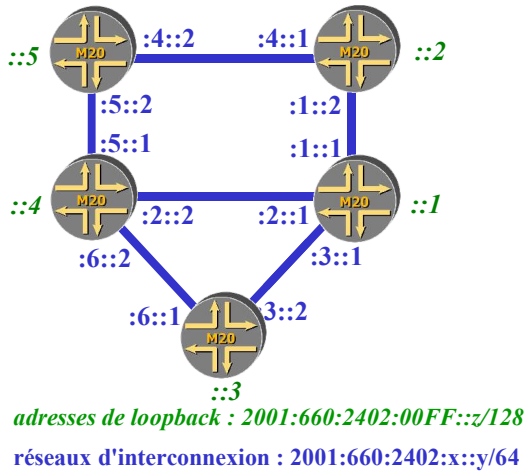

Figure 2 – *adressage de la dorsale Osiris*

Pour ce qui concerne la partie « identifiant d'interface », nous recommandons aux utilisateurs d'Osiris de fixer les adresses des serveurs connus (serveurs Web, NFS, etc.) pour éviter qu'elles soient dépendantes de la carte réseau, et de laisser l'autoconfiguration agir pour les autres, et en particulier pour les postes clients. Par ailleurs, nous leur demandons également de désactiver l'anonymisation des adresses [2] (qui est activée par défaut sous Windows XP), car ce mécanisme n'est pas gérable dans un environnement professionnel tel qu'Osiris : par exemple, il est impossible pour le gestionnaire d'un parc informatique de localiser géographiquement une machine incriminée dans un incident sécurité à l'aide de son adresse IPv6, et de la filtrer sur son pare-feu.

3.3 Activation d'IPv6

L'activation d'IPv6 dans un sous-réseau suit un schéma simple : une fois le préfixe alloué suivant le plan d'adressage, la connectivité IPv6 est activée sur le routeur en ajoutant une configuration de ce type dans l'interface concernée (sur Juniper) :

```
family inet6 {
        address 2001:660:4701:100a:ff::/64;
    }
```

puis les « Router Advertisement » (RA) sont activés pour ce réseau sur le routeur :

```
router-advertisement {
    interface ge-1/2/0.124 {
        prefix 2001:660:4701:100A::/64;
    }
```

Cette activation est très simple sur le plan technique. Elle doit cependant être accompagnée d'une formation des correspondants réseau concernés, comme nous le verrons dans la section 5.

3.4 Protocoles de routage

Routage externe

Le protocole de routage externe pour l'interconnexion avec Renater est bien entendu BGP4+. IPv6 bénéficie de son propre peering BGP et, par conséquent, n'est donc pas dépendant d'IPv4.

Alors qu'IPv4 bénéficie d'une double connexion BGP vers Renater, le temps nous a manqué pour répliquer cette fonctionnalité en IPv6. Il n'y a pas de problème technique particulier, aussi ce point sera réalisé rapidement.

Routage interne

Osiris utilisait précédemment le protocole de routage interne OSPFv2. La facilité aurait pu nous pousser à ajouter OSPFv3 pour IPv6, mais nous avons préféré utiliser IS-IS pour IPv6 et IPv4. Même si cela demandait un effort initial plus important, le bénéfice est aujourd'hui clair : un seul protocole de routage pour les deux protocoles, et une bien plus grande simplicité de fonctionnement.

Le LSIIT, pour ses besoins d'expérimentation, a reçu 64 préfixes distincts. Du fait d'une topologie dynamique avec un nombre conséquent de préfixes, et compte tenu de la capacité limité de leur routeur, nous avons choisi d'utiliser RIPng et de redistribuer les routes apprises, après filtrage, dans IS-IS.

3.5 Réseau sans fil

L'Université Louis Paster a initié dès 2001 une grande réflexion autour du réseau sans fil. Le projet a été découpé en trois phases :

- phase 0 : test dans l'UFR de math-info en 2001- 2002 ;
- phase 1 : dix sites pilotes 2002 – 2003 ;
- phase 2 : généralisation à partir de 2004.

Le support d'IPv6 a été bien évidemment dès le départ placé au cœur de la réflexion, notamment grâce au rôle moteur du LSIIT. En effet, le déploiement initial des bornes et le portage de certaines applications, ainsi que des tests de mobilité IPv6 faisaient partie de projets de DESS et de travaux de recherche du LSIIT.

Le CRC a été très tôt impliqué pour mettre en œuvre l'architecture réseau, mais n'est devenu un acteur majeur qu'à partir de la phase 1 correspondant réellement au début du stade opérationnel. IPv6, tout au long de ces phases, est resté une fonctionnalité essentielle et a été placé au même niveau qu'IPv4.

Aujourd'hui, le projet s'est élargi à tous les établissements strasbourgeois connectés à Osiris et intéressés par le réseau sans-fil. Le CRC opère directement les bornes des établissements concernés. Cela représente actuellement environ 200 bornes pour 35 bâtiments, chiffres en constante progression.

Le CRC offre deux modes de connexion au réseau sans-fil :

- mode sécurisé
- mode non sécurisé

Le mode sécurisé se base pour l'authentification sur des mécanismes de niveau 2 (IEEE 802.1X). Dans ce mode, la mise en œuvre d'IPv6 a été simple car elle est uniquement dépendante des routeurs, comme le reste de l'infrastructure réseau.

Le mode non sécurisé a été mis en place dans le but de ne pas freiner l'adoption du réseau sans-fil, afin de faciliter la connexion des personnes utilisant un système non encore compatible avec le protocole IEEE 802.1X, ainsi que pour d'autres besoins plus ponctuels comme les conférences. Dans ce but une solution de type « portail captif » a été mise en place. Un certain nombre de produits existent déjà, mais aucun ne supportait IPv6. Une solution a donc été développée localement puis déployée.

Afin de supporter le protocole IPv6 aussi bien qu'IPv4, notamment au niveau du filtrage des paquets, nous avons choisi une solution basée sur FreeBSD et PF [3]. PF est pour le moment le seul logiciel de filtrage, en version stable, capable de supporter le filtrage IPv6 avec une table de connexions.

Le principe de fonctionnement d'IPv6 dans le portail captif est décrit plus en détail en annexe.

3.6 VPN

Le CRC a ouvert en 2004 un service de VPN pour remplacer un serveur RTC obsolète. Ce service devait permettre aux utilisateurs d'avoir une adresse IP bien identifiée sur Osiris pour accéder à certaines ressources privées.

Nous nous étions fixés les contraintes suivantes : facilité de déploiement, client gratuit multi-plateformes, facilité

d'installation et support natif d'IPv6. Malheureusement, cette dernière contrainte semble être exclusive des trois premières. Nous avons donc dû nous résigner et choisir une solution, basée sur un routeur Cisco 3725 avec une carte de cryptographie, qui ne supporte pas IPv6 de manière native.

Cependant nous n'avons pas baissé les bras, et nous avons implémenté une solution actuellement au stade de préproduction, illustrée par la figure 3. Elle consiste à monter un deuxième tunnel de type ISATAP [4] dans le premier tunnel IPSEC. Un client VPN Cisco a été packagé par nos soins pour les plateformes Windows afin de détecter la présence d'IPv6 sur le poste client. Si IPv6 est activé, un tunnel ISATAP est automatiquement monté après authentification et permet donc d'offrir une connectivité IPv6. Nous avons rédigé des scripts pour Linux et FreeBSD pour bénéficier également de cette connectivité.

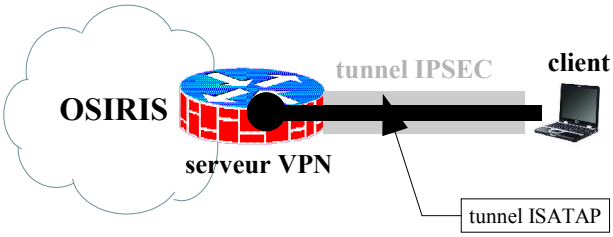

Figure 3 – *intégration d'IPv6 dans le service VPN*

3.7 Filtrage

Le filtrage est un élément indissociable de la mise en place de la connectivité IPv6 sur un réseau. On distingue trois catégories de systèmes de filtrage :

- le filtrage par machine, où chaque machine doit posséder un pare-feu intégré ;
- les garde-barrières, disposant généralement d'un filtrage à états ;
- le filtrage de base en cœur de réseau, sur les routeurs, sans état : une interface Web de gestion des ACL est en cours de développement ; cependant il manque encore le filtrage sur les flags TCP en IPv6 sur les routeurs Juniper.

En ce qui concerne les services liés à l'infrastructure, chaque serveur du CRC utilise PF, disponible sur FreeBSD, et les garde-barrières hébergés au CRC utilisent également PF, sur FreeBSD et OpenBSD.

3.8 Métrologie

Une fois l'infrastructure mise en place, il importe d'en mesurer l'usage. La métrologie est malheureusement, pour le moment encore, le parent pauvre d'IPv6. En particulier, il faut bien avouer que que les MIB IPv6 sont rarement implémentées.

En l'absence de solution satisfaisante, nous avons réalisé une métrologie simplifiée grâce aux capacités de comptage des paquets des routeurs Juniper.

En insérant une directive « firewall filter », nos routeurs d'entrée comptent les paquets IPv6 et placent cette information dans une MIB privée. Les lignes ajoutées dans la configuration des routeurs sont :

```
filter osirisv6-out {
    term compter-paquets {
        then count ipv6-out;
    }
    term accepter {
        then accept;
    }
}
```

Ces compteurs sont ensuite interrogés et représentés sous forme de graphique à l'aide de MRTG. Cela nous donne une vision rudimentaire, qu'il faudra améliorer dans le futur par un outil de métrologie plus évolué.

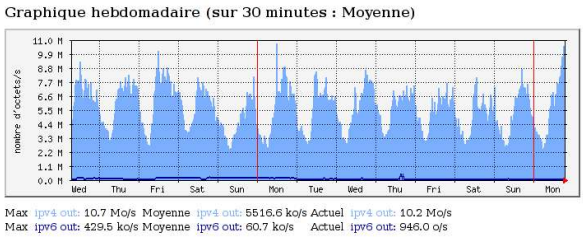

Figure 4 – *courbes de trafic IPv4 et IPv6*

La figure 4 montre un exemple. La courbe bleue foncée, bien qu'encore basse, est maintenant bien distincte. Le trafic IPv6 représente actuellement en moyenne environ 1% du trafic IPv4 sur Osiris, ce qui est considérable par rapport au début du déploiement.

4 Services

On ne le dira jamais assez : pour publier l'adresse IPv6 d'une machine dans le DNS, il faut que tous les services accessibles par des clients IPv6 soient v6-ifiés.

Autrement dit, si un serveur est presque complètement v6-fié et qu'il reste un service n'acceptant pas de connexion IPv6, alors les clients supportant IPv6 n'arriveront pas à utiliser ce service. Pour illustrer avec un exemple vécu sur Osiris : lorsque nous avons publié l'adresse IPv6 du serveur principal du CRC, le directeur n'a pu lire ses courriers car le serveur IMAP n'avait pas encore été v6-fié. D'autres exemples sont arrivés sur des sites externes, dont certains fréquentés par notre communauté, le protocole HTTP était très souvent en cause...

Il importe donc que tous les services soient v6-ifiés avant que l'adresse IPv6 soit publiée dans le DNS. Une solution transitoire consiste à publier l'adresse IPv6 sous un autre nom (par exemple crc.u-strasbg.fr et crc6.u-strasbg.fr) pour tester les services IPv6 un par un, avant de supprimer définitivement le nom transitoire (crc6) et d'ajouter l'adresse IPv6 au nom officiel.

4.1 DNS

Nous avons rénové en profondeur l'architecture DNS sur Osiris en 2003. Cette architecture a donné lieu à une présentation aux JRES [5]. Auparavant, le service de nommage était réparti géographiquement, un serveur DNS se-

condaire sur chacun des 5 campus principaux d'Osiris. Du fait de l'augmentation des débits et de la fiabilité du nouveau réseau, nous avons mis en place une solution qui consiste à n'avoir plus qu'une seule adresse IP pour le service DNS. En réalité, deux machines partagent une même adresse grâce au protocole VRRP [6]. Cependant, VRRP ne supporte que le protocole IPv4. C'est pourquoi nous avons remplacé en juin 2005 VRRP par CARP [7] qui permet d'offrir la même redondance en IPv6 et en IPv4.

Pour des raisons de maintenance, la version de BIND utilisée était celle fournie avec le système standard. Cette version permettait d'abriter des zones IPv6 (avec des RR de type AAAA), mais pas de répondre en IPv6 aux requêtes des clients et des autres serveurs DNS dans le monde. Ceci interdisait donc de publier une adresse IPv6 pour nos serveurs DNS. Nous avons donc migré vers BIND 9. La seule modification dans le fichier **named.conf** a été l'ajout de la ligne :

```
listen-on-v6 { any; } ;
```

L'application de gestion du DNS (WebDNS [8]), qui permet à nos correspondants réseau de déclarer eux-mêmes des machines, a été modifiée pour intégrer les adresses IPv6. La modification a été grandement facilitée par l'intégration complète des adresses IPv6 dans les types INET/CIDR du moteur SGBD PostgreSQL (à partir de la version 7.4).

Lors de l'annonce initiale de la disponibilité de l'application WebDNS, effectuée en avril 2004, celle-ci incorporait déjà les modifications requises pour IPv6.

4.2 Le relayage de messagerie

Le relayage de messagerie pour l'ensemble d'Osiris s'effectue sur huit serveurs regroupés sous un seul nom (mailhost.u-strasbg.fr) avec 16 adresses, 8 pour IPv4 et 8 pour IPv6. La configuration de Sendmail, basée sur le Kit Jussieu [9], n'a été modifiée que pour inclure les deux lignes (dans un fichier d'inclusion du kit) :

```
O DaemonPortOptions=Family=inet
O DaemonPortOptions=Family=inet6
```

Attention : les deux lignes sont indispensables sous FreeBSD (et sans doute les autres Unix). Sous Linux, il faut seulement la deuxième ligne, car un attachement à la famille « inet6 » entraîne également un attachement à la famille « inet », contrairement à ce qui est dit dans la documentation de Sendmail.

Les deux lignes ont été incluses dans le Kit Jussieu, ainsi que le support des adresses IPv6 dans les listes noires. Ces modifications seront intégrées dans la prochaine version distribuée du Kit.

Depuis le passage en IPv6 de tous les relais de messagerie Osiris, un problème est apparu à quelques reprises. Le symptôme en est que certains clients SMTP externes ne peuvent plus nous joindre :

```
test@xxx.u-strasbg.fr.. Connecting to mrX.u-strasbg.fr. via esmtp.
test@xxx.u-strasbg.fr... Deferred: No route to host
```

C'est le cas typique d'un îlot IPv6 non connecté au reste de l'Internet IPv6. Concrètement, le client SMTP mal programmé dispose d'une adresse IPv6 par défaut, et il essaie de se connecter en IPv6 sur nos relais de messagerie. N'ayant pas une adresse routée sur l'Internet, le client ne peut donc pas joindre nos relayeurs en IPv6 et le dialogue SMTP s'arrête là. Il faut alors contacter directement l'administrateur du site concerné, lui expliquer le problème et parfois l'aider à le résoudre...

La politique de relayage en vigueur sur Osiris spécifie que toute machine Osiris ayant une adresse IPv4 non enregistrée dans le DNS ne peut envoyer de courrier aux relais. Cette politique n'est évidemment pas applicable en IPv6 car, du fait de l'autoconfiguration, il est impossible de déclarer toutes les machines sur des réseaux à population très dynamique comme le réseau sans fil. De plus, pré-déclarer toutes les adresses potentielles d'un réseau est difficilement réalisable (2^{64} combinaisons) et nous n'avons pas mis en place la déclaration dynamique dans le DNS, qui ne nous semblait pas une solution mature et déployable à grande échelle.

4.3 L'hébergement des boîtes aux lettres

Le service d'hébergement des boîtes aux lettres a été v6-ifié en mai 2004. Le logiciel utilisé (courier-imap), étant compatible IPv6 depuis longtemps, l'opération s'est déroulée sans problème (ajout d'une adresse IPv6, des filtres adéquats et publication dans le DNS).

Le service de « Webmail » a été v6-fié en juillet 2004 grâce à l'installation du serveur Apache 2.

4.4 Le serveur ftp

Le serveur FTP d'Osiris (ftp.u-strasbg.fr) a été migré en octobre 2004. Il a fallu attendre une version compatible IPv6 du logiciel proftpd.

L'adaptation de la configuration de ce logiciel pour IPv6 n'a pas été très simple, il a fallu ajouter les lignes :

```
SocketBindTight On
DefaultAddress 127.0.0.1
```

puis créer un « VirtualHost » pour chaque adresse IPv4 et IPv6 en incluant pour chacun le même fichier de configuration pour éviter de dupliquer des lignes :

```
<VirtualHost 130.79.200.5>
    ServerName     "Réseau Osiris - Strasbourg"
    Include "/local/etc/proftpd/proftpd-crc.conf"
</VirtualHost>
<VirtualHost 2001:660:2402::6>
    ServerName     "Réseau Osiris - Strasbourg (IPv6)"
    Include "/local/etc/proftpd/proftpd-crc.conf"
</VirtualHost>
```

Enfin, l'accès à ce serveur en utilisant le protocole HTTP a nécessité la migration vers le serveur Apache 2.

4.5 Le serveur de bases de données

Le CRC, pour un grand nombre de ses applications utilise des bases de données reposant sur PostgreSQL. La v6-fication du serveur de bases de données n'a posé aucun problème. PostgreSQL supporte IPv6 depuis au moins 5 ans.

5 Formations

Sur le plan technique, moyennant un effort raisonnable, il est relativement aisé de mettre en œuvre IPv6 sur la dorsale d'un réseau universitaire ainsi que les services d'infrastructure. Il reste cependant le cœur du problème : l'adoption de ce protocole par les utilisateurs, c'est à dire pour nous l'adhésion de nos 100 correspondants réseaux et à travers eux de nos 50 000 utilisateurs. Nous rencontrons ici

une toute autre problématique, celle du poste client qui est complètement différente de celle d'un opérateur réseau.

Pour accompagner nos utilisateurs et les convaincre des bienfaits d'IPv6, nous avons conçu une formation d'une journée accompagnée de travaux pratiques que nous dispensons tous les mois. La partie théorique se décompose de la manière suivante :

- pourquoi IPv6 ?
- historique d'IPv6
- adressage sur l'Internet IPv6
- format des datagrammes
- mécanismes (autoconfiguration, voisinnage, etc...)
- IPv6 sur Osiris

La partie pratique est orientée vers la prise en main d'IPv6 sous Linux et Windows.

Malgré notre impatience à déployer IPv6, cette formation est un pré-requis à l'activation d'un préfixe IPv6. Aujourd'hui, 53 correspondants réseaux ont été formés et 27 préfixes sont routés sur Osiris.

Une deuxième formation est en cours d'élaboration pour accompagner les administrateurs systèmes et les aider à migrer leurs services réseaux en IPv6.

6 Conclusion

L'objectif fixé (IPv6 = IPv4) est en passe d'être atteint pour ce qui concerne l'infrastructure (réseau et services) d'Osiris. Du fait de l'intégration de cet objectif depuis 2001 dans l'ensemble des projets du CRC, nous disposons à présent d'un ensemble très complet et nous pouvons mesurer le chemin accompli.

La métrologie nous indique qu'IPv6 est réellement utilisé au quotidien. Avec 27 préfixes routés aujourd'hui, ce sont plus de 700 machines distinctes qui génèrent du trafic IPv6. L'adoption est encore loin d'être générale, mais le nombre de machines croît régulièrement. Notre réseau est d'ores et déjà prêt pour la sortie des prochaines versions de systèmes d'exploitation de postes clients proposant IPv6 en standard.

Il reste cependant quelques points à terminer :

- double connexion BGP vers Renater, ne demandant essentiellement qu'un peu de temps ;
- connectivité multicast IPv6, pour laquelle nous attendons la disponibilité du service natif de Renater ;
- redondance du routage IPv6 pour chaque réseau, comparable à celle dont nous disposons en IPv4, basée sur VRRP. Nous sommes actuellement en attente d'une solution équivalente pour nos routeurs.

Le protocole IPv6 est utilisé sur le réseau interne du CRC, et notamment par tous les membres de l'équipe. Par ailleurs, les services critiques (Web, routage de messagerie, etc.) reposent également sur ce protocole. Ces deux facteurs contribuent à renforcer la rapidité de détection des problèmes pouvant survenir sur l'infrastructure IPv6, que ce soit celle d'Osiris ou d'autres réseaux traversés.

La v6-ification d'Osiris étant le fruit du travail de toute l'équipe d'ingénierie du CRC, je tiens à citer Jean Benoit, Sébastien Boggia, Pascal Gris, Laurence Moindrot, Christophe Saillard et Alain Zamboni. De plus, sans la volonté politique de notre directeur, Pierre David, nous n'en serions pas là.

Annexe

Cette annexe décrit en détail les mécanismes mis en œuvre pour l'accès IPv6 sur le réseau sans fil (cf 3.4).

Lorsqu'un client veut accéder au réseau sans fil, il s'associe sur un point d'accès (SSID osiris) et arrive dans le Vlan « ouvert » du réseau sans fil. Le portail captif envoie des « Router Advertisement » (programme **rtadvd**) permettant aux postes clients supportant IPv6 de s'autoconfigurer, comme l'illustre la figure 5.

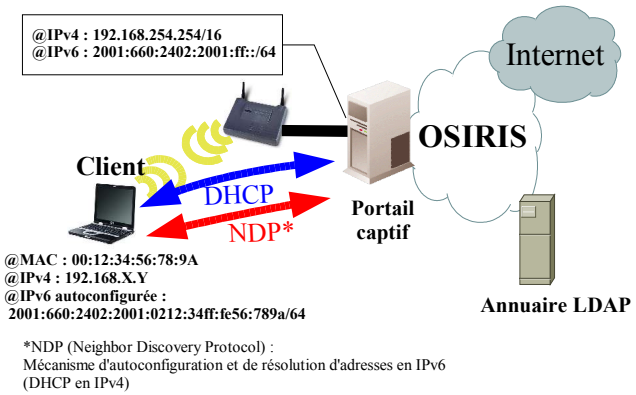

Figure 5 – *connexion d'un client IPv6 au réseau sans fil*

La connexion donne accès à une page Web (CGI) qui permet à l'utilisateur du poste client de s'authentifier de manière sécurisée via le protocole HTTPS. La figure 6 illustre les mécanismes mis en œuvre lors de l'authentification.

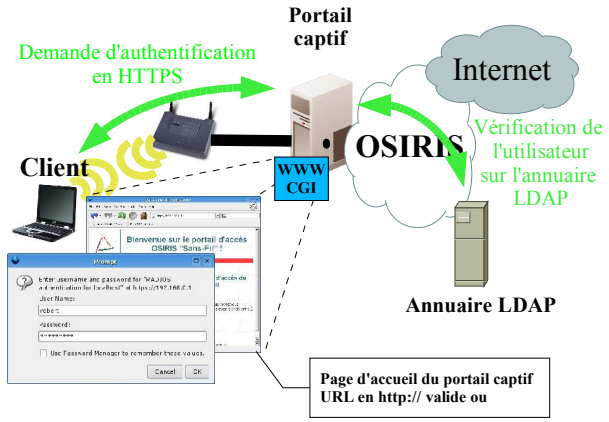

Figure 6 – *authentification sur le portail captif*

Une fois l'utilisateur authentifié le script CGI récupère l'adresse IPv4 du poste. En interrogeant les baux DHCP actifs, le portail captif récupère l'adresse Ethernet, puis en déduit l'adresse IPv6 autoconfigurée. Il vérifie ensuite que le

poste client supporte IPv6, en envoyant un paquet ICMP6 à destination de cette adresse pour remplir le cache de voisinage (équivalent au cache ARP en IPv4) sans attendre la réponse, afin de déclencher un « Neighbor Sollicitation ». À la suite de cette action, si l'adresse Ethernet du poste client se trouve dans le cache de voisinage du portail captif, cela signifie que le poste client supporte IPv6. Des règles PF sont alors automatiquement ajoutées pour ouvrir l'accès au poste client en IPv6. La figure 7 schématise les échanges d'informations et les traitements réalisés sur le portail captif pour la reconnaissance d'un client IPv6.

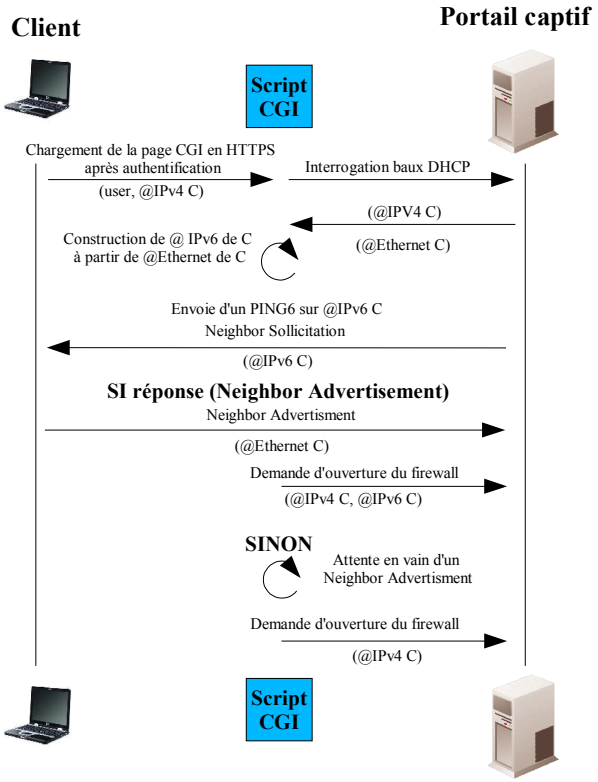

Figure 7 – *reconnaissance d'un client IPv6 par le portail captif*

Bien évidemment, cette solution ne permet pas aux postes clients qui utilisent l'anonymisation d'accéder à l'Internet IPv6, c'est pourquoi nous demandons aux utilisateurs et aux administrateurs de la désactiver.

Cette solution repose sur des mécanismes initiaux IPv4. Le support de clients non compatibles IPv4 (« IPv6 only ») n'est pas encore implémenté, mais ça ne nous a pas paru être un objectif prioritaire.

Références

[1] H. Prigent, T. Carl, Exemples de mise en œuvre du protocole IPv6 et de services associés sur le réseau régional SYRHANO (Haute-Normandie), JRES2003, Lille.

[2] RFC 3041, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, janvier 2001.

[3] Packet Filter, http://www.openbsd.org/faq/pf

[4] Internet Draft, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 27 janvier 2005.

[5] P. Pegon, Fiabilisation d'une architecture DNS, JRES2003, Lille.

[6] R. Hinden, Virtual Router Redundancy Protocol (VRRP), avril 2004.

[7] http://www.openbsd.org

[8] J. Benoit, P. David, WebDNS

[9] Kit Jussieu,http://www.kit-jussieu.org