Déploiement d'IPv6 à l'université Paris 1 – Panthéon-Sorbonne

Benoît Branciard, David Chopard-Lallier, Yvonne Girard
Université Paris 1 – Panthéon-Sorbonne, Service informatique pour la recherche et l'enseignement

Date : 12 octobre 2005.

Résumé

Cet article présente un retour d'expérience sur le déploiement d'IPv6 à l'université Paris 1 – Panthéon-Sorbonne. La méthodologie, les différentes étapes, les difficultés rencontrées et leurs solutions y sont décrites.

Mots-clés

IPv6, déploiement, retour d'expérience.

1 Raisons et objectifs

Le déploiement d'IPv6 à l'université Paris 1 a été initié par le Centre de Ressources Informatiques et du Réseau (CRIR), essentiellement motivé par la pénurie d'adresses IPv4 (l'université ne disposant que d'une vingtaine de « /24 »), ainsi que la volonté de segmenter le plus finement possible les communautés d'utilisateurs (passage du triplet classique « enseignement / recherche / administration » à *au moins* un sous-réseau par entité et par site) dans un contexte de dispersion géographique (vingt-quatre implantations). L'intégration d'IPv6 dans la stratégie réseau de l'établissement a débuté en octobre 2001, notamment en mentionnant le support d'IPv6 dans les appels d'offres pour le renouvellement du matériel actif. L'objectif étant dans un futur proche de déployer des VLANs purement IPv6 en remplacement des allocations massives d'adresses IPv4 privées (RFC 1918) en usage actuellement.

2 Contraintes

Le déploiement d'IPv6 a été soumis principalement aux contraintes suivantes :

- faire coexister[1] IPv4 et IPv6 sur la même architecture réseau,
- ne pas introduire de perturbations sur les services réseau en usage, particulièrement pendant les heures ouvrables,
- ne pas introduire de dégradation de la sécurité par rapport à l'existant,
- s'accommoder des faibles ressources disponibles, autant humaines : deux personnes « réseau » et une personne « système » à temps partiel, que financières, le surcoût lié à IPv6 devant rester dans les limites des enveloppes prévues pour la mise à niveau et le renouvellement planifiés des matériels (équipements actifs, serveurs) et logiciels.

3 Prérequis

Disposer d'équipements actifs et de plateformes logicielles supportant IPv6 a été un préalable mais se former à cette nouvelle version du protocole IP a également été nécessaire afin de le mettre en oeuvre. La dernière étape a été d'obtenir un préfixe de site auprès de Renater.

3.1 Support d'IPv6 par les équipements actifs

Le raccordement des principaux bâtiments au réseau académique parisien[2] (RAP) en 2002 [1] et le renouvellement du coeur du réseau local des principales implantations de l'université, échelonné de 2003 au premier semestre 2005, ont été l'occasion de disposer d'équipements actifs supportant IPv6, pour lesquels cette caractéristique a été déterminante dans le choix des titulaires du marché. Pour les routeurs Cisco, l'installation de la version de l'IOS 12.3(3) supportant IPv6 a été faite en septembre 2003. Des commutateurs-routeurs Extreme Summit 48si sont utilisés pour les petits sites ; pour ceux-ci, l'image système supportant IPv6 « Version 7.0.0 (Build 61) IPv6 1.3.4 » n'a été disponible qu'en janvier 2004.

3.2 Support d'IPv6 par les systèmes d'exploitation et les logiciels

Les machines fournissant les services réseau de base (DNS, messagerie, web et FTP) fonctionnaient sous Solaris 2.6 et Red Hat Linux 7.x. A l'occasion de leur renouvellement, Solaris 8 ou 9 et Debian Gnu/Linux « Sarge » ont été installés sur ces serveurs, ainsi que des versions mises à jour des services réseau, basés sur des logiciels libres : Bind 9.2.4, sendmail 8.12.10, UW-Imap 2004g, Apache 2 et Pure-FTPD 1.0.19. Cet ensemble,

[1] Les routeurs, les principaux serveurs et les postes de travail sont en « double pile ».

[2] http://www.rap.prd.fr

affiné progressivement, a constitué une base solide pour la mise en exploitation d'IPv6.

3.3 Formation de l'équipe à IPv6

Parallèlement à la mise en oeuvre des opérations précédentes, l'équipe système et réseau a suivi des conférences (JRES 2001, 2003, Caen – juin 2003), des formations CiRen (2002 et 2004) et/ou a lu la littérature sur le sujet, notamment l'ouvrage de Gisèle Cizault [2].

3.4 Obtention d'un préfixe de site auprès de Renater

Cette opération a été réalisée en mars 2003, en utilisant le « Formulaire de requête NLA IPv6 » disponible en envoyant un message à `AdressesIP@renater.fr`. Après avoir vérifié que l'agrément Renater était à jour, le formulaire complété a été renvoyé à l'adresse électronique précédente. A cette date, la livraison imminente des nouveaux commutateurs/routeurs, supportant IPv6, laissait entrevoir la possibilité des premières expérimentations.

4 Préparatifs

Un plan d'adressage a d'abord été défini. Il a fallu ensuite élaborer la politique de sécurité IPv6, point essentiel afin de ne pas compromettre la sécurité de l'existant (réseau IPv4). Après avoir affecté des adresses IPv6 explicites aux principaux serveurs, les services réseaux de base (DNS, web, FTP, SMTP, POP et IMAP) ont été activés en IPv6.

4.1 Plan d'adressage

Le réseau de l'université comporte dix sites RAP haut débit, ainsi que des « petits » sites en cascade, pour un total de vingt-quatre implantations, susceptible d'évoluer. L'adressage devait prendre en compte cet attribut géographique ainsi que la segmentation en communautés d'usagers. La lisibilité humaine de l'adresse a été privilégiée, en affectant à chaque attribut un nombre entier de chiffres hexadécimaux. Les quatre chiffres $X_1X_2X_3X_4$ faisant suite au préfixe de site attribué par Renater (2001:660:3305/48) ont ainsi été utilisés pour définir des préfixes de sous-réseaux en « /64 » de la façon suivante :

- X_1X_2 : attribut « géographique » (numéro de site).
- X_3X_4 : attribut « communauté ». Il correspond au numéro de VLAN sur le site, dont sont retenus les deux derniers chiffres du « tag » 802.1q. La valeur « FF » est attribuée aux VLANs d'administration réseau, non « tagués » (nommés « default » pour les commutateurs Extreme). X_3 caractérise l'activité : « 0 » enseignement, « 1 » recherche, « 2 » documentation, « 3 » administration, « 4 » imprimantes et copieurs connectés, « 5 » réseaux sans-fil. X_4 est un numéro de catégorie ou d'entité au sein de l'activité (bureaux, postes publics, laboratoire, etc.) attribué séquentiellement.

Quelques exemples de préfixes de sous-réseaux sont donnés ci-dessous pour les sites Pierre Mendès-France (PMF), Arago et Saint-Charles :

Site	X_1	X_2	*tag*	X_3X_4	*préfixe IPv6 (/64)*
PMF	0	0		FF	2001:0660:3305:00FF
PMF	0	0	201	01	2001:0660:3305:0001
PMF	0	0	230	30	2001:0660:3305:0030
Arago	0	2	301	01	2001:0660:3305:0201
Arago	0	2	330	30	2001:0660:3305:0230
Saint-Charles	8	0		FF	2001:0660:3305:80FF
Saint-Charles	8	0	801	01	2001:0660:3305:8001

4.2 Politique de sécurité

Le niveau de sécurité doit être au moins égal à celui du réseau IPv4. La solution adoptée fournit un niveau équivalent dans les deux versions du protocole.

Au niveau du poste de travail

A l'exception des salles informatiques et des nouveaux postes pour lesquels le CRIR établit une « matrice » système préréglée, la sécurité au niveau du poste est laissée à l'initiative de l'utilisateur. A cet effet, des recommandations sur les principaux points de sécurité sont mises à sa disposition sur le site web du CRIR ; celles-ci couvrent désormais IPv6. Pour les postes Windows XP, le service pack 2 (SP2) apporte notamment un pare-feu supportant IPv6.

Réseau

Un réseau d'établissement a été reconstitué au-dessus du réseau de collecte RAP, sur lequel les principaux sites de Paris 1 sont connectés, par des VPN de niveau 3 [1] (tunnels GRE dans lesquels est routé le trafic IP unicast IPv4 et IPv6, ainsi que le trafic multicast IPv4). Le centre PMF est le point central du réseau d'établissement. Les équipements de raccordement des sites de l'université au RAP sont des routeurs Cisco 7200 VXR ou 7301.

Le site PMF est raccordé au RAP en IPv4 et en IPv6, un VLAN est affecté à chacune des versions du protocole IP.

La sécurité est effectuée par des *access-lists* sur les routeurs Cisco ; on distingue :

- des règles générales peu restrictives implémentées en IN et en OUT sur l'interface RAP du réseau d'établissement (interdictions générales),
- des règles plus strictes, implémentées sur les routeurs de chaque site, en OUT sur les sous-interfaces de chaque VLAN, de la forme « tout ce qui n'est pas permis est interdit ».

Les *access-lists* IPv6 ont été calquées sur leurs équivalentes IPv4, en remplaçant les ACLs de type « established » par des types « reflexive » (à mémoire d'état). Des extraits de configuration du routeur principal de PMF (Cisco 7200) sont donnés en annexe.

4.3 Activation d'IPv6 avec déclaration d'adresse explicite sur les serveurs

L'adresse explicite permet de s'affranchir de la dépendance au matériel des adresses EUI-64, ce qui évite les perturbations liées à un changement d'adresse en cas de remplacement du matériel (temps de propagation DNS, modification des déclarations administratives, etc.). Comme pour le plan d'adressage, la lisibilité humaine a été privilégiée : la représentation décimale du dernier octet de l'adresse IPv4 est stockée dans les trois derniers chiffres hexadécimaux de l'adresse IPv6 (en DCB[3]), tous les autres chiffres étant à zéro jusqu'au préfixe de sous-réseau.

Des directives de configuration d'IPv6 avec adresse explicite sur plusieurs variantes de systèmes sont données en annexe.

4.4 Activation d'IPv6 pour les services réseau de base

L'activation du protocole IPv6 a été réalisée sur les services préexistants en IPv4 (HTTP, FTP, DNS, SMTP, POP, IMAP, NTP et SSH) de façon progressive, en testant la connectivité IPv6 avec un nombre restreint de clients avant la généralisation. Dans la majorité des cas, le logiciel utilisé en IPv4 a été conservé, après une éventuelle mise à jour ou l'ajout de directives de configuration. Quelques logiciels incompatibles (protocoles FTP, NTP, ou méta-serveur inetd) ont dû être remplacés par des équivalents.

Des exemples de configuration IPv6 des principaux services sont donnés en annexe.

4.5 Automatisation de la gestion du DNS

Un programme a été développé en interne pour répondre à la problématique suivante :

- utilisation de Bind 9.2,
- choix d'une gestion « autoritaire » des entrées DNS (pas de *DDNS update* à l'initiative des clients),
- la gestion manuelle des tables DNS, déjà très lourde et source d'erreurs en IPv4, devient impraticable en IPv6 (conversion MAC/EUI-64, AAAA/PTR, longueur des adresses),
- espace d'adressage IPv4 morcelé en de multiples « /24 », d'où un grand nombre de fichiers de zones à maintenir,
- souhait de conserver une bonne lisibilité aux fichiers de zones (tri des entrées),
- bijection tables DHCP (baux réservés sur adresses MAC) et tables DNS (adresse EUI-64 dépendant de l'adresse MAC).

Ce programme nommé « `majdns` », réalisé en Perl, prend en charge la gestion des fichiers de zones DNS spécifiques à Bind. Il offre une interface de saisie interactive de type terminal, et un mode *batch* pour l'importation d'une liste de noms d'hôtes associés à leurs paramètres IP (adresse IPv4, IPv6 ou adresse MAC). Un filtre permettant d'importer des déclarations d'hôtes extraites de *dhcpd.conf* (fichier de configuration du démon ISC DHCPD[4]) a également été créé.

Aperçu des fonctionnalités de majdns

- Gestion des tables au niveau du sous-réseau. Le fichier « subnets » contient la liste des sous-réseaux gérés avec pour chacun le nom, la plage IPv4 (en notation CIDR « */xx* ») et/ou la plage IPv6. Pour chaque sous-réseau *subnet* disposant d'une plage IPv4, les fichiers zd.*subnet* et zi.*subnet* contiennent respectivement les enregistrements A et PTR v4 des hôtes membres, tandis que zd6.*subnet* et zi6.*subnet* (ce dernier décliné en -int et -arpa, ce qui n'est désormais plus nécessaire depuis l'abandon du domaine ip6.int par la RFC 4159) contiennent les AAAA et PTR v6 le cas échéant. Les fichiers de zones db.*zone* déclarés dans *named.conf* sont réduits aux enregistrements SOA et NS et à une série de $INCLUDE des fichiers zd*xx* et zi*xx*.

[3] Décimal Codé Binaire

[4] http://www.isc.org/index.pl?/sw/dhcp/

```
pmf-adm         194.214.25.0/24
2001:660:3305:30::/64
srb-rech        194.214.32.0/24         -
ulm-pers        194.214.30.32/27
2001:660:3305:1230::/64
```

Exemple de fichier « subnets »

- Automatisation de toutes les tâches « mécaniques » : mise à jour des SOA, tri des entrées, contrôle des collisions, conversions MAC/EUI-64 et AAAA/PTR, recherche d'adresses IPv4 libres, etc.
- Gestion des entrées au niveau hôte ou CNAME, un hôte étant caractérisé par son nom, son sous-réseau, son adresse IPv4 et/ou son adresse IPv6 et/ou son adresse MAC. Pour IPv6, la saisie d'une adresse MAC ou IPv6 détermine le choix entre une adresse EUI-64 ou explicite.
- gestion de deux « vues » DNS, interne et externe, cette dernière excluant les adresses IPv4 privées.

La structuration en hôtes et sous-réseaux et les automatismes du programme « `majdns` » permettent à un opérateur d'effectuer de façon simple les opérations courantes (ajout, suppression et modification d'hôtes, ajout et suppression de CNAMEs) en s'affranchissant de la « cuisine » nécessaire à la maintenance des fichiers de zones, mais en gardant le contrôle de tous les paramètres pertinents.

4.6 Raccordement en IPv6 au réseau de collecte

Le raccordement en IPv6 du coeur de réseau (site PMF) au réseau de collecte RAP a été effectué en juin 2004, en mode « double pile » simplifié (cf. http://www.rap.prd.fr/pdf/ipv6Raccord.pdf), avec un VLAN 802.1q pour chaque version du protocole. Un extrait de la configuration correspondante du routeur Cisco de PMF est donné en annexe. Afin d'assurer une redondance, il est prévu de mettre en place BGP sur ce routeur, selon les directives du mode « préconisé » de connexion au RAP.

4.7 Raccordement en IPv6 des différents sites du réseau d'établissement

Dans un premier temps, l'annonce de préfixe par le routeur a été activée sur un VLAN unique du site PMF à titre d'essai ; puis elle a été validée pour tous les VLANs de ce site. Ensuite, cette manipulation a été progressivement étendue aux autres implantations de Paris 1, avec deux cas de figure :

- les « gros » sites raccordés au RAP haut débit : le trafic IPv4 et le trafic IPv6 (unicast uniquement à ce jour) transitent par des tunnels GRE IPv4. A cette fin, des adresses IPv6 ont été ajoutées aux tunnels.
- les « petits » sites en cascade d'un site RAP via des liaisons louées : le routage IPv6 est effectué (comme le routage IPv4) avec des commutateurs-routeurs Summit48si d'Extreme Networks.

Le routage IPv4 et IPv6 s'effectue par des routes statiques. Quelques exemples de configurations de routage sont donnés en annexe.

4.8 Délégation de la zone inverse IPv6

Cette procédure constitue l'étape finale de la mise en place d'une connectivité IPv6 de bout en bout. La demande en a été faite fin juin 2004 par un courriel à `dnsv6@renater.fr`, après avoir validé le fonctionnement en IPv6 des serveurs DNS de l'université (gestion des enregistrements AAAA et écoute en IPv6). Un des deux serveurs secondaires ne reste cependant accessible qu'en IPv4, car il est situé sur le réseau inter-établissements de la Sorbonne dont le routeur ne gère pas IPv6 à l'heure actuelle.

5 Opérations à effectuer après la mise en place de la connectivité IPv6

5.1 Activation d'IPv6 avec autoconfiguration d'adresse sur les postes de travail

L'autoconfiguration d'adresse de type EUI-64, basée sur les annonces de préfixe des routeurs et l'adresse physique (MAC) de l'interface réseau du poste, a été retenue en raison de sa simplicité de mise en oeuvre et de sa disponibilité en standard sur les plateformes usuelles. D'une façon générale, les plateformes les plus anciennes (Windows XP, noyau Linux < 2.6, Mac OS X < 10.2) nécessitent une activation explicite, tandis que sur les plus récentes, l'autoconfiguration IPv6 est activée par défaut, rendant la connectivité IPv6 totalement « *plug and play* ». Des directives de configuration IPv6 des postes sont données en annexe pour les principales plateformes. Quelques bogues dans les implémentations ont été constatés ; voir à ce sujet le §6.

La plupart des postes neufs étant installés par matriçage (clonage d'une image système préréglée, que ce soit en

interne pour les parcs homogènes, ou par un accord avec le vendeur pour les postes individuels livrés « au fil de l'eau »), l'activation d'IPv6 a été incluse dans les matrices, facilitant grandement son déploiement. Pour les autres cas, une procédure d'activation a été mise à disposition des utilisateurs sur le site du CRIR (cf. §5.4).

5.2 Stratégie d'entrée des adresses IPv6 dans le DNS

La difficulté d'exercer un contrôle strict de tous les postes de travail, en particulier les portables « invités », ainsi que la volonté de maintenir un espace de nommage « propre », ont amené à renoncer à toute forme de DNS dynamique (DDNS) initié par les clients eux-mêmes. D'un autre côté, les règles anti-relais du serveur de messagerie[5], ainsi que d'autres règles de contrôle d'accès basées sur l'appartenance au domaine, rendent la déclaration DNS des postes de travail indispensable. Le choix s'est porté sur une saisie manuelle des adresses IPv6, grandement facilitée par l'utilisation du programme « majdns » (cf. §4.5) et l'utilisation des adresses EUI-64. Trois cas de figure peuvent se présenter :

- les parcs de postes homogènes (salles d'enseignement ou de travail, libre-service, postes de consultation en bibliothèque) : ceux-ci utilisent DHCP pour l'obtention d'adresses IPv4 fixes, configurées sur le serveur DHCP sur la base de leurs adresses MAC. La déclaration de leurs adresses IPv6 dans le DNS se résume à l'importation de la table DHCP les concernant *via* le mode « *batch* » de majdns. Pour l'achat de nouvelles machines, il a été convenu avec le vendeur que celui-ci fournisse au CRIR, préalablement à toute livraison, la liste (papier ou de préférence électronique) des adresses MAC, et colle sur chaque machine une étiquette comportant son adresse MAC ;
- les nouveaux postes de travail individuels achetés « au fil de l'eau » : le marché établi avec les fournisseurs prévoit la livraison « clés en main » de la machine, et comprend une procédure de transmission/validation des paramètres réseau entre le CRIR et le vendeur. Le retour de l'adresse MAC par le vendeur a été ajouté à cette procédure. Ces adresses MAC sont saisies *via* le mode interactif de majdns à leur réception ;
- les postes de travail individuels existants ou achetés par d'autres canaux que le marché Paris 1 (marchés CNRS, ...) : le passage à IPv6 est laissé à l'initiative de l'utilisateur. A cet effet la rubrique « IPv6 » du site du CRIR (cf. §5.4) contient les instructions nécessaires, lesquelles incluent la transmission de l'adresse MAC du poste pour saisie interactive *via* majdns par le CRIR.

[5] basées sur le kit de configuration de sendmail de Jussieu, http://www.kit-jussieu.org

5.3 Automatisation de la recherche du *proxy*

Initialement, de nombreux postes (disposant d'adresses IPv4 privées de type RFC 1918 ou volontairement filtrées) accédaient au Web via un relais (*proxy*) Squid[6], dont les paramètres étaient obtenus par un script d'autoconfiguration de type Netscape[7]. En absence de support IPv6 finalisé dans Squid, Apache 2 a été choisi comme relais pour les postes double pile ; cependant il était souhaitable de conserver Squid pour certains postes pour ses fonctionnalités de filtrage et sa finesse de configuration. Un script PHP a donc été développé, lequel renvoie un script d'autoconfiguration différent selon l'adresse IP du client, ce qui permet de rediriger vers l'un ou l'autre des serveurs (Squid ou Apache 2) tout en conservant une URL d'autoconfiguration unique.

5.4 Communication auprès des utilisateurs

Celle-ci n'a pas été négligée : une rubrique dédiée est ainsi disponible sur le site du CRIR (http://crir.univ-paris1.fr/ipv6) depuis juin 2004 et régulièrement actualisée et complétée (procédure d'activation de l'auto-configuration, test de la connectivité, procédure en cas de problèmes, logiciels compatibles, etc.). Des présentations d'IPv6 seront également intégrées dans les différentes formations organisées par le CRIR. Le site du centre de ressources informatiques indique aux utilisateurs s'ils sont connectés en IPv4 ou en IPv6 et si leur poste est déclaré dans le DNS.

5.5 Métrologie et supervision

Une bonne maîtrise de son réseau passe par la mise en place d'une métrologie et d'une supervision. L'outil utilisé (netMET[8]) pour la métrologie IPv4 ne supportant pas actuellement IPv6, de nouveaux logiciels sont actuellement étudiés. L'objectif étant de ne plus dépendre d'un protocole propriétaire. A ce jour, les MIBs disponibles dans la version de l'IOS utilisée (12.4(1a) et 12.3(13)) ne permettent pas de mesurer le trafic IPv6. Il est néanmoins possible d'obtenir le nombre de paquets IPv6 entrants et sortants avec la commande « `show interfaces accounting` ». Un programme interrogeant chaque heure les routeurs avec cette commande et utilisant

[6] http://www.squid-cache.org

[7] http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html

[8] http://www.netmet-solutions.org.

RRDtool[9] est en cours d'écriture. La supervision s'effectue dans les deux versions du protocole IP avec Nagios[10].

6 Difficultés

Quelques bogues ont été constatés dans les implémentations d'IPv6 lors du déploiement de celui-ci sur les postes de travail :

- Windows XP pré-SP2 : le système ne se rabat pas sur une connexion IPv4 lorsque la connectivité IPv6 est indisponible, interdisant toute connexion aux serveurs double pile dans cette situation. Des problèmes liés à la résolution des CNAMEs ont aussi été constatés. Le SP2 corrige ces problèmes.
- Mandriva Linux 10.0 : un bogue au niveau de la glibc provoque un fort ralentissement des résolutions de noms en IPv6, gênant en usage courant, ainsi qu'un rabattage injustifié sur les adresses IPv4. La version 10.1 corrige ces problèmes.

Quelques comportements déficients ou inattendus ont aussi été observés. Sur un client double pile, le comportement habituel à l'établissement d'une connexion est de résoudre l'adresse IPv6 en priorité, et de se rabattre sur l'IPv4 en cas d'absence ou d'échec de connexion. Les applications suivantes dérogent cependant à cette règle : Firefox sous Mac OS X, qui se connecte prioritairement en IPv4, ou NTP 4.2 sous Unix, qui ne se rabat pas d'IPv6 vers IPv4 en cas d'échec de connexion. A noter également : l'inaptitude de Windows XP à l'IPv6 pur, en raison de l'impossibilité de saisir des adresses IPv6 pour les serveurs DNS, et l'absence de support IPv6 pour le protocole SMB. Enfin, les applications Windows compatibles IPv6 restent encore rares.

Les difficultés actuelles sont notamment :

- les applications de gestion Apogée et Harpège basées sur Oracle SQL/Net ne sont pas « IPv6 ready ». Il en va de même pour d'autres basées sur des partages de disque Windows. Actuellement, le déploiement des réseaux IPv6 purs ne peut être envisagé que pour l'enseignement et la recherche. Il faudra cependant que les protocoles SMB, ICA et RDP, utilisés dans les applications « enseignement » supportent IPv6.
- les applications nouvelles (TICe, bibliothèques, ...) pour lesquelles l'intérêt d'IPv6 ne fait pas toujours partie des préoccupations et est considérée comme exotique par les éditeurs ou intégrateurs. Une implication du centre de ressources informatiques est nécessaire lors de la rédaction du cahier des charges de toute nouvelle application. Ainsi, lorsque le service commun de documentation a renouvelé ses applications (système intégré de gestion de bibliothèques - SIGB et système d'information documentaire – SID), le CRIR a demandé que ces deux systèmes soient accessibles dans les deux versions du protocole, au moins pour leurs interfaces web.

7 Etat actuel

La connectivité IPv6 est actuellement en production sur l'ensemble des implantations de l'université Paris 1 où cela est techniquement possible, soit dix-huit sites sur vingt-quatre ; la plupart des sites non-IPv6 ne dépendent pas de Paris 1 pour l'administration de leur réseau, notamment celui de la Sorbonne. La majorité des services réseau de base sont disponibles dans les deux versions du protocole ; il y a aujourd'hui vingt-et-un serveurs double pile. Environ 550 postes de travail ont été configurés en double pile, principalement sous forme de parcs de machines homogènes, en raison de la facilité d'installation liée au matriçage et à l'import direct des tables DHCP dans le DNS.

7.1 Qui utilise IPv6 à Paris 1 ?

Ce sont principalement les étudiants, dans les salles de travail ou de libre-service, où les machines ont été configurées à cet effet, ainsi que certains membres du personnel disposant de postes récemment installés. La plupart utilisent IPv6 sans le savoir, et ne connaissent pas plus l'existence d'adresses IPv6 qu'ils n'avaient connaissance des adresses IPv4 !

8 Prochaines étapes

Quelques éléments du déploiement d'IPv6 restent à effectuer ou sont en cours de réalisation. Les mécanismes de communication entre les deux versions du protocole en vue de la mise en place de VLANs purement IPv6 restent à mettre en place :

- serveurs d'impression double pile : lpd fonctionne correctement sous Solaris 9, au contraire de la version actuelle de CUPS qui est seulement IPv4. La version 1.2 devrait intégrer IPv6,
- Dual Stack Transition Mechanism (DSTM) : permet à des machines IPv6 de communiquer avec des machines IPv4 et à des applications IPv4 de fonctionner sur des réseaux IPv6.

[9] http://people.ee.ethz.ch/~oetiker/webtools/rrdtool

[10] http://www.nagios.org.

Une première étape a été franchie avec l'utilisation d'Apache 2 comme relais. Le multicast IPv6 sera déployé dès que possible. La gestion DNS IPv6 des « nomades » (portables, invités...) reste à définir : la mise à jour dynamique du DNS par le démon *dhcpd* est une piste possible. Une autre, plus expérimentale, est constituée par la mise en oeuvre de la mobilité IPv6. L'université participe en effet dans le cadre de l'opération lancée par la direction de la recherche du MENESR au projet ADIRE sur la mobilité, dont l'aboutissement constitue aussi un des objectifs actuels.

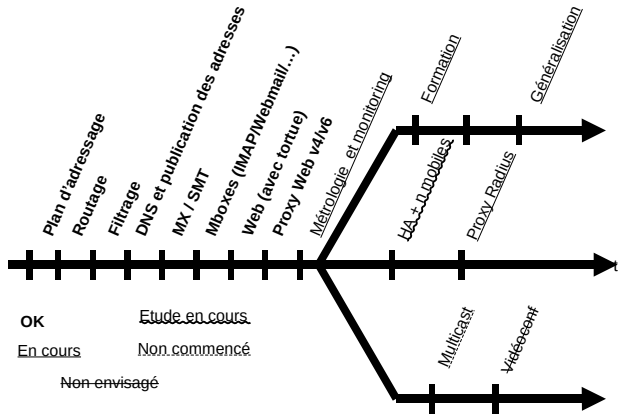

Figure 1- *Etat d'avancement de Paris 1 dans ADIRE*

9 Durée du déploiement

Un an et demi, effectué dans le cadre du renouvellement des équipements actifs. Les prestataires n'ont été d'aucune aide en raison de leurs connaissances extrêmement réduites sur IPv6.

Conclusion

Bien que disposant de ressources humaines et financières (le principal poste de dépense relevant de la mise à niveau matériel et logiciel et du renouvellement des équipements actifs) limitées, le déploiement d'IPv6 à Paris 1 est déjà bien engagé. Il a commencé en septembre 2003 au gré du renouvellement des équipements actifs.

Il reste à mettre en place un certain nombre de services afin de parfaire son déploiement, mais les services essentiels sont déjà disponibles et sont de plus en plus utilisés. La mise en place d'IPv6 à Paris 1 s'est finalement effectuée progressivement et sans problème majeur.

Bibliographie

[1] David Chopard-Lallier, Yvonne Girard, *Utilisation de VPN de niveau 3 à l'université Paris 1 - Panthéon-Sorbonne*. Journées RSSI 2003, Ensam, Paris. En ligne : https://www.cru.fr/rssi/Journees/mars.2003/vpn-paris1.

[2] Gisèle Cizault, *IPv6, théorie et pratique*, O'Reilly, 3e édition, 2002.

Annexe

Configuration des routeurs

Activation d'IPv6 et connexion au RAP du routeur Cisco de coeur de réseau (PMF)

Sous-interfaces d'interconnexion avec le RAP

VLAN pour IPv4

```
interface FastEthernet2/0.953
 encapsulation dot1Q 953
 ip address 195.221.126.58 255.255.255.252
 ip accessgroup in-pmf-rap in
 ip accessgroup out-pmf-rap out
```

VLAN pour IPv6

```
interface FastEthernet2/0.927
 encapsulation dot1Q 927
 ipv6 address 2001:660:2401:2006::2/64
 ipv6 enable
 ipv6 traffic-filter in-ipv6-pmf-rap in
```

Sous-interface du réseau local

VLAN interne du site PMF, avec des postes et des serveurs

```
interface GigabitEthernet0/2.200
 encapsulation dot1Q 200
 ip address 193.55.96.72 255.255.255.0
 ip access-group out-vlan-pmf-scipre out
 ip access-group in-vlan-pmf-scipre in
 ipv6 address 2001:660:3305:0000::/64 eui64
 ipv6 enable
 ipv6 nd prefix-advertisement
2001:660:3305:0000::/64 604800 604800
 onlink autoconfig
 ipv6 traffic-filter in-ipv6-pmf-scipre in
 ipv6 traffic-filter out-ipv6-pmf-scipre out
!*** route par défaut vers le RAP
ip route 0.0.0.0 0.0.0.0 195.221.126.57
ipv6 route ::/0 2001:660:2401:2006::1
```

Exemples d'access-lists sur le routeur Cisco de coeur de réseau (PMF)

Sur l'interface du RAP : « permit » de tout ce qui n'est pas explicitement interdit

```
ipv6 access-list in-ipv6-pmf-rap
 deny ipv6 ::1/128 any
 deny ipv6 fec0::/48 any
 deny ipv6 2001:660:3305::/48 any
```

```
! entrée unique de la messagerie
 permit tcp any host 2001:660:3305:0:203::71 eq smtp
 deny tcp any any eq smtp
...
 permit ipv6 any any
```

Sur les interfaces du réseau local : *access-lists* réflexives correspondant aux sessions initialisées depuis les postes internes et « permits » spécifiques pour les serveurs.

```
ipv6 access-list in-ipv6-pmf-scipre
 permit icmp any any
 permit tcp any any reflect pmf-scipre-ipv6-tcpconnections
 permit udp any any reflect pmf-scipre-ipv6-udpsessions
 deny ipv6 any any log
ipv6 accesslist out-ipv6-pmf-scipre
# politique par défaut pour tout poste
 permit icmp any any
 evaluate pmf-scipre-ipv6-tcpconnections
 evaluate pmf-scipre-ipv6-udpsessions
# permit particuliers pour les serveurs du VLAN
! dns primaire, mailhub de campus (smtp), ssh en interne
 permit udp any host 2001:660:3305:0:203::71 eq domain
 permit tcp any host 2001:660:3305:0:203::71 eq smtp
 permit tcp 2001:660:3305::/48 host 2001:660:3305:0:203::71 eq 22
...
deny ipv6 any any log
```

Exemples de routage au sein du réseau d'établissement

Site Saint-Charles (raccordé au RAP haut débit)

Extrait de la configuration du Cisco 7301 du site Saint-Charles :

```
interface Loopback0
 ip address 194.214.30.9 255.255.255.255
!
interface Tunnel1
 description *** Tunnel vers PMF ***
 ip address 10.1.12.91 255.255.255.0
 ipv6 address 2001:660:3305:FF08::B/64
 ip mtu 1476
 tunnel source Loopback0
 tunnel destination 194.214.30.1
! route vers l'autre extrémité du tunnel via RAP
ip route 194.214.30.1 255.255.255.255 195.221.125.197
ip route 0.0.0.0 0.0.0.0 Tunnel1
ipv6 route ::/0 Tunnel1
```

Extrait correspondant de la configuration du Cisco 7200 du site PMF :

```
interface Loopback0
 ip address 194.214.30.1 255.255.255.255
!
interface Tunnel12
 description *** Tunnel vers Saint-Charles ***
 ip address 10.1.12.1 255.255.255.0
 ipv6 address 2001:660:3305:FF08::A/64
 ip mtu 1476
 tunnel source Loopback0
 tunnel destination 194.214.30.9
!
! routes vers les réseaux de Saint Charles
ipv6 route 2001:660:3305:80ff::/64     Tunnel12
ipv6 route 2001:660:3305:8001::/64     Tunnel12
ipv6 route 2001:660:3305:8030::/64     Tunnel12
ip route ...
```

Site Arago en cascade du site PMF via une LS 2 Mbit/s zone locale

le réseau d'interconnexion est le 2001:660:3305:ff /64.

commutateur Summit 48si d'Arago :

```
# adresse IPv6 des interfaces et activation du routage IPv6
configure vlan arago-pers ipaddress ipv6 eui64 2001:660:3305:230::/64
enable ipforwarding ipv6 vlan arago-pers
# route par défaut vers PMF
configure iproute add ipv6 default 2001:660:3305:ff:20b:60ff:feb0:b006 1
# pour l'auto-configuration des postes de réseaux locaux
enable router-discovery ipv6 arago-pers
configure vlan arago-pers router-discovery ipv6 add prefix 2001:660:3305:230::/64
```

routes vers les VLANs de ce site sur le Cisco de PMF :

```
ipv6 route 2001:660:3305:0230::/64 2001:660:3305:ff:201:30ff:fe12:a5e0
```

Configuration IPv6 des systèmes d'exploitation

Activation d'IPv6 avec adresse explicite sur les serveurs

Debian GNU/Linux Sarge

Dans le fichier */etc/network/interfaces*, ajouter à la suite de la section « `iface` *`eth0`* `inet static` » (*eth0* étant le nom de l'interface à configurer) :

```
iface eth0 inet6 static
    pre-up modprobe ipv6
    # desactive l'autoconfig d'adresse IP
    up sysctl -q -w net.ipv6.conf.eth0.autoconf=0
    address xx:xx:xx:xx:xx:xx
    netmask nn
```

Note : la ligne « `pre-up modprobe ipv6` » n'est nécessaire qu'avec un noyau de version antérieure à 2.6.

Solaris >= 8

Dans cet exemple, l'interface à configurer est « *hme0* », et l'adresse explicite à affecter est « *2001:660:3305::73/64* ».

- Modifier ou créer l'entrée « ipnodes » dans */etc/nsswitch.conf* à l'identique de l'entrée « hosts » :
```
hosts:      files dns
ipnodes:    files dns
```
- Créer un fichier */etc/hostname6.hme0* contenant la ligne :
```
addif 2001:660:3305::73/64 up
```
- Ajouter dans le fichier */etc/inet/ndpd.conf* (le créer si nécessaire) :
```
if-hme0 StatelessAddrConf false
```
- redémarrer la machine par « init 6 ».

Red Hat Enterprise Linux 3

- dans le fichier */etc/sysconfig/network* :
```
NETWORKING_IPV6=yes
IPV6_AUTOCONF=yes
```
- dans */etc/sysconfig/network-scripts/ifcfg-eth0* (*eth0* étant le nom de l'interface à configurer) :
```
IPV6INIT=yes
IPV6ADDR=xx:xx:xx:xx:xx:xx/nn
# desactive l'autoconfig d'adresse IP
/sbin/sysctl -n -w
net.ipv6.conf.eth0.autoconf=0
```

Note : la commande « *sysctl* » peut être remplacée par un réglage équivalent dans le */etc/sysctl.conf*.

Activation d'IPv6 avec autoconfiguration d'adresse sur les postes de travail

Aucune configuration n'est nécessaire sur les systèmes suivants : RedHat Linux 9, Fedora Linux, Mandriva Linux 10.x, Mac OS X (depuis la version 10.2), Debian GNU/Linux Sarge (avec noyau 2.6).

RedHat Linux 7.1 – 8

- dans le fichier */etc/sysconfig/network*
```
NETWORKING_IPV6=yes
IPV6_AUTOCONF=yes
```
- dans */etc/sysconfig/network-scripts/ifcfg-eth0*
```
IPV6INIT=yes
```

Debian GNU/Linux Sarge (noyau 2.4)

Ajouter dans */etc/network/interfaces*, juste après « `iface eth0 inet static` » :

```
pre-up modprobe ipv6
```

Windows XP

Exécuter à partir d'une session « administrateur » les lignes de commande suivantes :

```
ipv6 install
ipv6 -p gpu UseTemporaryAddresses no
```

puis redémarrer le poste.

Configuration IPv6 des services réseau

Apache 2[11]

Les directives suivantes doivent être ajoutées :

http[12]

```
Listen [adresse IPv6]:80
```

Pour l'utilisation des hôtes virtuels :

```
NameVirtualHost [adresse IPv6]:80
<VirtualHost adresse IPv4:80 [adresse IPv6]:80>
```

https[12]

```
Listen [adresse IPv6]:443
```

Pour l'utilisation des hôtes virtuels :

```
NameVirtualHost [adresse IPv6]:443
<VirtualHost adresse IPv4:443 [adresse IPv6]:443>
```

proxy

Les modules suivants doivent être chargés :

- mod_proxy
- mod_proxy_connect
- mod_proxy_ftp
- mod_proxy_http

Les directives à ajouter :

```
ProxyRequests On
<Proxy *>
 Order deny,allow
 Deny from all
 Allow from 2001:660:3305::/48
 Allow from univ-paris1.fr
</Proxy>
```

Pure-FTPD[13] *1.0.19 et 1.0.20*

Le support d'IPv6 est activé par défaut.

---

[11] http://httpd.apache.org

[12] Configuration recommandée pour éviter tout problème lié au DNS au démarrage d'Apache ; cf. http://httpd.apache.org/docs/2.0/dns-caveats.html

[13] http://pureftpd.org

Bind[14] 9.2.4

Ajouter la ligne suivante dans la section « options » du *named.conf* :

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

Sendmail[15] 8.12.10 sous Solaris 9

Ajouter les options suivantes au *sendmail.cf* :

```
# SMTP daemon options
O DaemonPortOptions=Family=inet
O DaemonPortOptions=Family=inet6
```

Sendmail 8.13.4 Debian

Activer les directives suivantes du *sendmail.mc* :

```
FEATURE(`no_default_msa')dnl
DAEMON_OPTIONS(`Family=inet6, Name=MTA-v6,
Port=smtp, Addr=::')dnl
DAEMON_OPTIONS(`Family=inet, Name=MSP-v4,
Port=submission, Addr=127.0.0.1')dnl
```

Ce qui se traduit par l'extrait *sendmail.cf* suivant après exécution de *sendmailconfig* :

```
O DaemonPortOptions=Family=inet6, Name=MTA-v6,
Port=smtp, Addr=::
O DaemonPortOptions=Family=inet4, Name=MSP-v4,
Port=submission, Addr=127.0.0.1
```

Notes

- Cet exemple s'applique à un serveur SMTP « public » (écoute sur toutes les adresses par « *Addr=::* »).
- Contrairement à Solaris, seule l'instance IPv6 du MTA doit être déclarée, les connexions IPv4 étant automatiquement redirigées en IPv6 par le noyau (adresses v4-dans-v6).
- Le port MSP local (« *submission* ») reste ici en IPv4.

Pop3 et Imap avec UW-Imap[16]

Ces services sont lancés « à la demande » à partir d'un méta-serveur de type *inetd*. Les conditions suivantes sont requises :

- Utiliser un *inetd* compatible IPv6 :
    - Solaris 9 12/03 : l'*inetd* standard de la distribution convient.
    - Debian Sarge : le *netkit-inetd* de base ne supporte pas IPv6. Le remplacer par *openbsd-inetd*, disponible en tant qu'alternative parmi les paquetages Debian.
- Modifier le *inetd.conf*. Sur les deux plates-formes précédentes, il est nécessaire de dupliquer les entrées, une ligne par version du protocole :
    - Solaris 9 12/03 :

```
pop3    stream  tcp     nowait  root    /
usr/local/sbin/ipop3d   ipop3d
pop3    stream  tcp6     nowait  root    /
usr/local/sbin/ipop3d   ipop3d
imap    stream  tcp     nowait  root    /
usr/local/sbin/imapd    imapd
imap    stream  tcp6     nowait  root    /
usr/local/sbin/imapd    imapd
```

    - Debian Sarge :

```
pop3    stream  tcp6    nowait  root    /
usr/sbin/tcpd /usr/local/sbin/ipop3d
pop3    stream  tcp4    nowait  root    /
usr/sbin/tcpd /usr/local/sbin/ipop3d
imap2   stream  tcp6    nowait  root    /
usr/sbin/tcpd /usr/local/sbin/imapd
imap2   stream  tcp4    nowait  root    /
usr/sbin/tcpd /usr/local/sbin/imapd
```

- Utiliser une version des démons *imapd* et *ipop3d* compatible IPv6, pour que les adresses et noms des clients soient correctement rendus dans les journaux systèmes. UW-Imap 2004g répond à ce critère.

Postfix[17]

Directive à ajouter dans */etc/postfix/main.cf* :

```
inet_protocols = all
```

NTP

NTP 4.2[18] écoute par défaut en IPv4 et v6. Sous Solaris 8 et 9, le démon *xntpd* fourni n'est pas compatible IPv6 et doit être remplacé par NTP 4.2.

[14] http://www.isc.org/sw/bind

[15] http://sendmail.org/

[16] http://www.washington.edu/imap

[17] http://www.postfix.org

[18] http://www.ntp.org (paquetage Debian : ntp-server)