Résilience de l'Internet français

2013

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

Document réalisé par l'ANSSI avec la participation de l'AFNIC.

Recherche et rédaction par : François Contat, Mathieu Feuillet, Pierre Lorinquer, Samia M'timet, Guillaume Valadon, Rémi Varloot, et Nicolas Vivet.

Relecteurs principaux : Florian Maury et Mohsen Souissi.

L'équipe de rédaction remercie les membres de l'observatoire ainsi que les relecteurs pour leurs commentaires et remarques qui ont enrichi ce rapport.

Document mis en page à l'aide de LaTeX. Figures réalisées avec les outils TikZ et PGFPlots.

Vous pouvez adresser vos commentaires et remarques à l'adresse suivante :

rapport.observatoire@ssi.gouv.fr

Table des matières

Synthèse

Mis en place sous l'égide de l'ANSSI [1] en 2011, l'observatoire de la résilience de l'Internet français vise à améliorer la connaissance de celui-ci en étudiant les technologies critiques à son bon fonctionnement. Un de ses objectifs est donc d'augmenter la compréhension collective de l'Internet afin d'en avoir une vision la plus complète possible.

De par sa nature, l'Internet ne possède pas de frontière. L'Internet en France peut toutefois se définir comme l'ensemble des acteurs exerçant une activité sur le territoire national. L'observatoire se focalise sur l'Internet français, un sous-ensemble de l'Internet en France ne prenant pas en compte les acteurs étrangers, afin d'appréhender les dépendances des activités économiques et sociales françaises vis-à-vis de l'étranger.

La résilience est définie comme la capacité à fonctionner pendant un incident et à revenir à l'état nominal. Une extension naturelle en est la robustesse, c'est-à-dire la capacité à limiter au maximum les impacts d'un incident. La résilience et la robustesse de l'Internet peuvent être caractérisées par des indicateurs techniques mesurables.

Rédigé par l'ANSSI avec la participation de l'Afnic [2], ce rapport fournit une analyse de la résilience en étudiant deux protocoles essentiels au fonctionnement de l'Internet. Le premier, BGP [3], permet d'acheminer des données à l'aide d'annonces de routage. Le second, DNS [4], fournit la correspondance entre un nom de domaine et une adresse IP.

Au regard de ses analyses, l'observatoire considère que la situation de l'Internet français est satisfaisante. Cependant, les bonnes pratiques d'ingénierie admises ne sont pas pleinement suivies par les acteurs de l'Internet français. Par conséquent, l'observatoire les encourage à se les approprier et émet les recommandations suivantes :

- **déployer IPv6** afin de développer rapidement les compétences, et d'anticiper les problèmes opérationnels futurs ;
- **bien répartir les serveurs DNS faisant autorité** afin d'améliorer la robustesse de l'infrastructure ;
- **tester DNSSEC** et le déployer pour lutter contre les attaques par pollution de cache ;
- **déclarer systématiquement les objets route**, et les **maintenir à jour**, afin de faciliter la détection et le filtrage d'annonces BGP illégitimes ;
- **utiliser la RPKI** et déclarer des ROA ;
- **appliquer les bonnes pratiques BGP** au niveau des interconnexions entre opérateurs.

1. Agence nationale de la sécurité des systèmes d'information.
2. Association Française pour le Nommage Internet en Coopération.
3. Border Gateway Protocol.
4. Domain Name System.

Présentation de l'observatoire

L'Internet est une infrastructure essentielle pour les activités économiques et sociales aux échelles mondiale, nationale, et locale. Une panne majeure affecterait considérablement la bonne marche de la France et de son économie. De plus, le fonctionnement de l'Internet dans son ensemble est souvent méconnu et peut être perçu comme un système opaque, géré par des acteurs dont les rôles sont mal identifiés. Jusqu'à récemment, malgré l'importance de cette problématique, il n'existait pas d'organisme chargé d'étudier les risques de dysfonctionnement de l'Internet au niveau national.

Mis en place sous l'égide de l'ANSSI en 2011, l'observatoire de la résilience de l'Internet français vise ainsi à améliorer la connaissance de celui-ci en étudiant les technologies critiques à son bon fonctionnement. Un de ses objectifs est d'augmenter la compréhension collective de l'Internet français afin d'en avoir une vision cohérente et la plus complète possible. Cela permet notamment d'identifier les interactions entre les différents acteurs concernés.

De par sa nature, l'Internet est international et ne possède pas de frontière. Il est cependant possible de définir l'Internet en France comme l'ensemble des acteurs français et internationaux exerçant une activité en lien avec les technologies de l'Internet. Dans le cadre de ses études, l'observatoire se focalise sur l'Internet français, un sous-ensemble de l'Internet en France qui n'inclut pas les acteurs étrangers. L'étude de l'Internet français permet de mieux comprendre les interdépendances des activités économiques et sociales françaises vis-à-vis de sociétés ou d'organismes étrangers.

La résilience est, quant à elle, définie comme la capacité à fonctionner pendant un incident et à revenir à l'état nominal. Une extension naturelle en est la robustesse, c'est-à-dire la capacité, en amont, à limiter au maximum les impacts d'un incident sur l'état du système. Sur le plan technique, la résilience et la robustesse de l'Internet peuvent être caractérisées par un ensemble d'indicateurs techniques mesurables. Certains sont directement issus de règles d'ingénierie, appelées bonnes pratiques, définies par la communauté technique et scientifique.

La mission de l'observatoire de la résilience de l'Internet français est également de définir et de mesurer des indicateurs représentatifs de la résilience, et de rendre leurs résultats publics. Il associe à cette démarche les acteurs de l'Internet français afin d'augmenter l'efficacité du dispositif et de favoriser une adoption la plus large possible des bonnes pratiques.

Introduction

Depuis la publication du premier rapport portant sur l'année 2011, les membres de l'observatoire ont eu l'opportunité de présenter leurs travaux lors de plusieurs conférences en France et en Europe, et d'échanger sur le sujet de la résilience. En marge des recommandations émises dans son rapport, l'observatoire et les opérateurs de communication partenaires ont également rédigé un guide de bonnes pratiques de configuration de BGP [1]. La communauté technique et scientifique a très bien accueilli l'initiative ainsi que les documents publiés.

Des échanges ont par ailleurs été initiés avec des membres de projets européens [2] complémentaires cherchant à mieux comprendre les dépendances d'un pays vis-à-vis de l'Internet. Les approches utilisées pour étudier la résilience sont cependant différentes. Ainsi en Allemagne, le BSI[5] a publié un article [3] analysant le graphe de connectivité des opérateurs allemands. Aux Pays-Bas, après avoir identifié les noms de domaine des sociétés liées aux secteurs d'activités à risque, des chercheurs de NLnet Labs [4] ont pu identifier les opérateurs cruciaux pour leur pays, et les services critiques hébergés à l'étranger.

Fort de ces constats, l'observatoire s'est attaché à consolider les indicateurs techniques existants et à affiner ses analyses. Par exemple, en ce qui concerne le protocole BGP, les analyses utilisent désormais plus de données que dans les rapports précédents sans pour autant augmenter les temps de calcul. La plupart des méthodologies ont été modifiées, notamment à l'aide des différents commentaires que nous avons reçus.

Tout comme dans les rapports précédents, le premier chapitre s'ouvre par une présentation succincte du protocole BGP. Il décrit ensuite le fonctionnement de la RPKI[6], une première étape vers la sécurisation du routage de l'Internet à l'aide de signatures cryptographiques. Dans la suite du chapitre, l'ensemble des indicateurs suivants sont analysés :

- la connectivité entre opérateurs, qui permet notamment de caractériser ceux qui sont critiques pour l'Internet français ;
- le phénomène d'usurpation, survenant lorsqu'un opérateur annonce des informations de routage illégitimes ;
- l'utilisation des objets `route` qui vise à s'assurer qu'ils sont correctement déclarés et mis à jour ;
- l'utilisation de la RPKI qui cherche à mesurer l'adoption de cette infrastructure

5. Bundesamt für Sicherheit in der Informationstechnik, en français Office fédéral de la sécurité des technologies de l'information.
6. Resource Public Key Infrastructure.

de gestion de clés.

Rédigé en collaboration avec l'Afnic, le second chapitre offre une vision synthétique du protocole DNS, et s'accompagne d'une description plus approfondie des extensions de sécurité DNSSEC [7]. Enfin, la résilience de l'Internet vue sous l'angle du DNS est évaluée à l'aune des indicateurs suivants :

- la dispersion topologique des serveurs DNS faisant autorité selon les pays et les opérateurs ;
- le taux de pénétration de DNSSEC ;
- l'état du déploiement du protocole IPv6 ;
- les résolveurs interrogeant la zone `.fr`.

Les opérateurs désireux d'obtenir des informations détaillées concernant les indicateurs BGP peuvent solliciter des rapports individualisés.

7. DNS SECurity extensions.

Chapitre 1

Résilience sous l'angle du protocole BGP

1.1 Introduction

Chacun des opérateurs de l'Internet gère des ensembles d'adresses IP [1] contiguës, appelés blocs ou préfixes, qu'il peut diviser en sous-réseaux pour ses propres besoins ou ceux de ses clients. Afin de constituer l'infrastructure de l'Internet, les opérateurs se connectent entre eux à l'aide du protocole BGP défini dans la RFC 4271 [5]. L'objectif de ce protocole est d'échanger des préfixes entre ces réseaux qui sont alors appelés AS [2] et qui sont identifiés par un numéro unique.

Une interconnexion BGP est bilatérale (c'est-à-dire entre deux AS). Chacun des AS échange des préfixes IP et informe son interlocuteur (appelé pair en français et *peer* en anglais) qu'il a la possibilité d'acheminer le trafic à destination de ces préfixes. Les interconnexions se divisent en deux catégories :

- **le peering :** accord où chaque pair annonce les préfixes qu'il gère. Par exemple, si un fournisseur d'accès à Internet et un diffuseur de contenu passent un accord de *peering*, tout le trafic entre ces deux interlocuteurs sera alors échangé directement. Les interconnexions de *peering* se réalisent souvent via des points d'échange, qui sont des infrastructures d'interconnexion distribuées sur plusieurs centres d'hébergement de données. Ces interconnexions peuvent aussi être réalisées au travers d'un lien direct entre deux opérateurs ;
- **le transit :** accord commercial entre un client (une société qui peut, elle aussi, être un fournisseur d'accès à Internet ou un fournisseur de contenu) et son opérateur (appelé transitaire) qui lui permet de joindre le reste de l'Internet. Le client annonce ainsi à son opérateur de transit les préfixes qu'il gère. L'opérateur de transit se charge de propager l'annonce de son client et lui annonce en retour le reste des préfixes constituant l'Internet.

Dans une interconnexion BGP, chacun des routeurs annonce pour chaque préfixe un `AS_PATH`, ou chemin d'AS. Ainsi, comme représenté dans la figure 1.1, si un routeur de l'AS65550 a uniquement appris l'`AS_PATH 65540 64510 64500` pour le préfixe 192.0.2.0/24, cela indique que pour joindre l'adresse IP 192.0.2.1, un paquet au départ d'une des IP de l'AS65550 traversera successivement les réseaux AS65540 et AS64510 avant d'arriver à l'AS64500. Il convient de noter que l'AS gérant le préfixe

1. Internet Protocol.
2. Autonomous System.

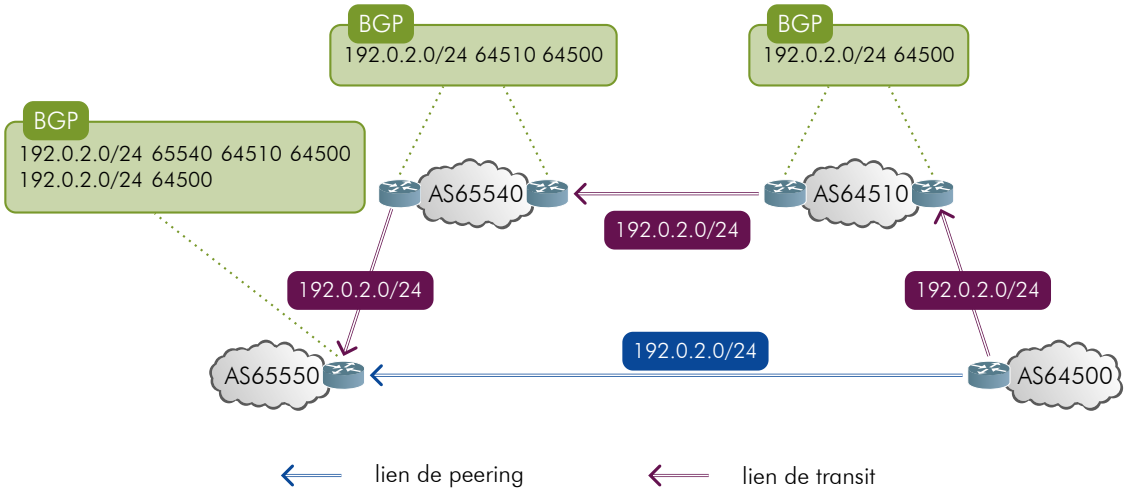

Figure 1.1 – Exemple de chemins d'AS sur des liens de transit et peering

se situe à droite dans la liste que constitue un chemin d'AS.

Lorsque plusieurs routes pour atteindre un même préfixe sont à la disposition d'un routeur, ce dernier choisit celle dont le chemin d'AS est le plus court. Dans la figure 1.1, le routeur de l'AS65550 possède deux routes différentes pour joindre le préfixe 192.0.2.0/24. L'une a été apprise *via* son interconnexion avec l'AS64500 (en bleu), et l'autre *via* son interconnexion avec l'AS65540 (en violet). Dans cet exemple, le lien de peering est préféré, le chemin d'AS étant le plus court.

1.2 La sécurisation du routage à l'échelle d'Internet

Le protocole BGP n'inclut aucun mécanisme permettant de vérifier qu'un AS est en droit d'annoncer un préfixe donné. Ce défaut entraîne régulièrement des incidents de routage dus à des annonces illégitimes de préfixes [6] :

- Le 24 février 2008, le fournisseur Pakistan Telecom a annoncé à PCCW, son transitaire, des préfixes plus spécifiques que ceux habituellement annoncés par YouTube [7]. En l'absence de filtre, les préfixes plus spécifiques ont été annoncés à l'ensemble de l'Internet, entraînant une redirection d'une partie du trafic de YouTube à destination de Pakistan Telecom ;
- Le 8 avril 2010, China Telecom a annoncé plusieurs dizaines de milliers de préfixes ne lui appartenant pas, entraînant également une redirection d'une partie du trafic à destination de ces préfixes [8].

De tels incidents montrent qu'il est nécessaire de disposer d'un moyen sûr pour vérifier la légitimité de l'annonce d'un préfixe par un AS.

Cependant, la validation des annonces de préfixes par un AS n'est pas suffisante. En effet, il est possible de modifier le chemin d'AS en remplaçant un numéro d'AS par un autre, ou encore en rajoutant des numéros d'AS, ce qui pourrait par exemple influencer le choix d'une route par un AS voisin.

Un moyen de sécuriser le routage à l'échelle d'Internet serait d'utiliser le mécanisme de signature électronique pour vérifier cryptographiquement les messages BGP que s'échangent les routeurs. Il s'agit du modèle employé par BGPSEC [9], une version sécurisée de BGP en cours de conception à l'IETF [3]. Dans BGPSEC, chaque AS possède un certificat associant une clé publique à un numéro d'AS. Elle est utilisée pour signer les annonces de préfixes effectuées par l'AS. Lors de l'annonce d'un préfixe, le routeur inclut une signature comprenant le préfixe, son propre numéro d'AS et le numéro de l'AS voisin dans le message BGP. Par la suite, chacun des AS souhaitant propager l'annonce ajoute une nouvelle signature au message BGP. Celle-ci couvre les données protégées par la signature de l'AS lui ayant transmis l'annonce, ainsi que le numéro d'AS du voisin auquel le message est envoyé. Chaque AS peut ainsi valider l'intégralité du chemin d'AS, depuis l'origine jusqu'au voisin lui ayant transmis l'annonce.

Par exemple, sur la figure 1.1, le routeur de l'AS64500 inclut une signature couvrant le préfixe `192.0.2.0/24`, le numéro d'AS 64500, et le numéro d'AS 64510. Le routeur de l'AS64510, lorsqu'il reçoit le message, vérifie la signature à l'aide de la clé publique de l'AS64500. Avant de propager l'annonce à l'AS65540, le routeur de l'AS64510 inclut une nouvelle signature couvrant `192.0.2.0/24`, les numéros d'AS 64500 et 64510, ainsi que le numéro d'AS de son voisin : 65540. L'AS65540 répète le même processus de vérification, et inclut une nouvelle signature lorsqu'il propage l'annonce à l'AS65550. Enfin, lorsque l'annonce parvient au routeur de l'AS65550, celui-ci peut constater que le chemin d'AS n'a pas été modifié en vérifiant les signatures effectuées par chacun des AS grâce à leurs certificats.

Aujourd'hui, la conception de BGPSEC est toujours en cours. Une étape préliminaire à sa mise en œuvre, qui introduit notamment un mécanisme permettant de vérifier l'origine d'une annonce, est maintenant normalisé à l'IETF : il s'agit de la *Resource Public Key Infrastructure* (RPKI).

1.2.1 Description de la RPKI

La RPKI est une infrastructure de gestion de clés (IGC) dédiée à la certification des ressources IP (préfixes IP ou numéro d'AS). Elle est issue de travaux de l'IETF, et décrite dans la RFC 6480 [10].

Dans cette IGC, les organismes certificateurs sont enregistrés auprès de l'IANA [4]. Chaque RIR [5] est ancre de confiance et autorité de certification pour les ressources dont il a la

3. Internet Engineering Task Force.
4. Internet Assigned Numbers Authority.
5. Regional Internet Registry.

gestion. Par exemple, le RIPE-NCC[6] est à la racine de la chaîne de confiance dont dépendent les LIR[7] européens, et peut délivrer un certificat à chacun de ses membres qui le demande.

La RPKI est une infrastructure répartie : chaque RIR maintient un dépôt dans lequel sont publiés les objets de la RPKI pour les ressources dont il a la gestion. Un dépôt contient plusieurs types d'objets signés cryptographiquement :

- des **resource certificate** (certificats de ressources) : ces objets attestent qu'un membre détient des préfixes IP et des numéros d'AS. Il s'agit de certificats X.509 [11], dont le profil est défini dans la RFC 6487 [12]. Ils utilisent les extensions de la RFC 3779 [13], notamment `sbgp-autonomousSysNum` et `sbgp-ipAddrBlock`, pour inclure respectivement des numéros d'AS et des préfixes IP ;
- des **Route Origin Authorization** (ROA) : ils sont assimilables à des objets `route` signés comportant des informations supplémentaires. Les `ROA` permettent en effet d'indiquer la longueur maximale des préfixes annoncés par un AS. Par exemple, un `ROA` peut spécifier que l'AS64500 est en droit d'annoncer le préfixe `198.18.0.0/15` et des préfixes plus spécifiques jusqu'à une longueur maximale de 17. De plus, une période de validité est associée au préfixe au travers des certificats. Les `ROA` sont utilisés indirectement par les routeurs pour valider les annonces qu'ils reçoivent. Ces objets sont décrits dans la RFC 6482 [14] ;
- des **Manifest** : un objet contenant une liste des noms de tous les autres objets du même répertoire, aussi appelé point de publication, ainsi qu'un condensat cryptographique du contenu de chaque objet. Un *Manifest* permet de s'assurer que la totalité des objets du point de publication a été récupérée, et de protéger le point de publication contre des altérations. Les détails d'implémentation de cet objet sont donnés dans la RFC 6486 [15]. Chaque point de publication doit contenir un *Manifest* ;
- des **Ghostbusters Record** : cet objet contient des informations permettant de contacter un administrateur de l'autorité de certification l'ayant délivrée. L'implémentation des *Ghostbuster Record* est décrite dans la RFC 6493 [16]. La présence de *Ghostbuster Record* dans un point de publication est optionnelle ;
- des **Certificate Revocation List** (CRL) : les CRL permettent de révoquer les certificats de ressources qui ne sont plus valides, ou les objets incluant un certificat *End-Entity* (EE). Les certificats EE sont uniques : il en existe un par objet de la RPKI (en dehors des certificats de ressources). En d'autres termes, un objet est signé par un unique certificat EE, et un certificat EE ne signe qu'un seul objet. Ceci permet de révoquer aisément un objet en révoquant le certificat EE qui lui est associé. D'autre part, les clés privées des certificats EE n'ont pas besoin d'être conservées.

6. RIPE Network Coordination Centre.
7. Local Internet Registry.

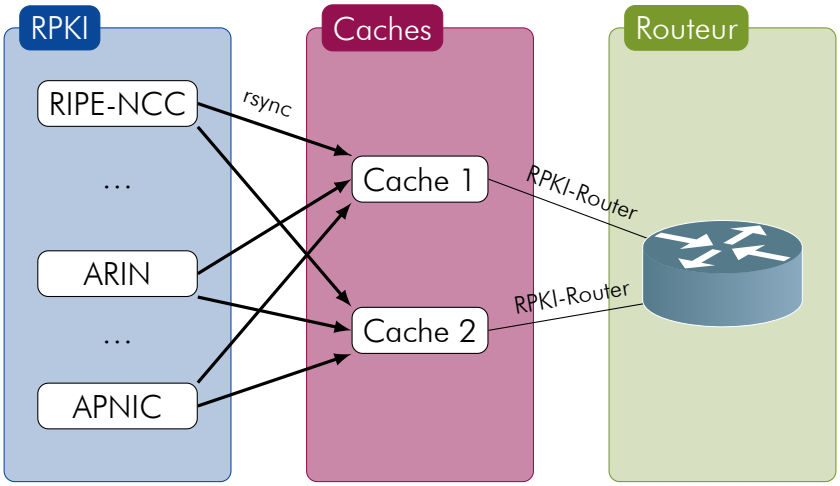

Figure 1.2 – Mise en œuvre de la RPKI

1.2.2 Exploitation de la RPKI

Participer à la RPKI

Un détenteur de ressources IP peut participer à la RPKI de deux manières différentes :

- en autorisant le RIR à gérer l'autorité de certification et le point de publication. Ce modèle de gestion est couramment désigné par l'expression *hosted model*. Cela permet au détenteur des ressources IP de s'affranchir de la gestion de l'infrastructure associée à l'autorité de certification et au point de publication. En adoptant ce modèle de gestion, l'organisation accepte que le RIR conserve sa clé privée. Le RIPE-NCC décrit la gestion de l'autorité de certification dans leur *Certification Practice Statement* [17]. Le RIR a notamment recours à un HSM[8] pour protéger les éléments secrets en confidentialité et en intégrité, en particulier les clés privées des membres ;
- en gérant sa propre autorité de certification et son propre point de publication. Cela permet notamment au détenteur des ressources de gérer lui-même sa clé privée et sa politique de signature. Il s'agit du *delegated model*.

À l'heure de l'écriture de ce document, le RIPE-NCC indique que le *delegated model* n'est pas en production [18]. Il met à disposition de ses membres une interface web [19] simplifiant la création et la gestion des `ROA`. L'administrateur décrit les annonces qu'il souhaite autoriser en indiquant l'AS origine, le préfixe devant être annoncé, ainsi que la longueur maximale des annonces. Une fois cette étape effectuée, il peut utiliser cette même interface pour publier les modifications dans la RPKI.

L'utilisation de la RPKI

8. Hardware Security Module.

Les routeurs n'interrogent pas directement les dépôts de la RPKI pour valider les annonces de préfixes. Ils dialoguent avec des serveurs caches, dont le rôle est de se synchroniser avec les dépôts de la RPKI, et d'effectuer les opérations cryptographiques liées à la validation des objets du dépôt.

Les serveurs caches récupèrent les objets des différents dépôts de la RPKI à l'aide du protocole rsync [20]. Ils valident ensuite l'intégralité des objets récupérés en utilisant la chaîne de certification de la RPKI.

Les serveurs caches transmettent les informations contenues dans les `ROA` validés aux routeurs : il s'agit des *Validated `ROA` Payload* (VRP). Les routeurs utilisent les VRP afin de déterminer la légitimité des annonces de préfixes reçues. La figure 1.2 illustre les interactions existant entre la RPKI, les serveurs caches et un routeur.

Au sens de la RPKI, une annonce peut être :

- **valide** : il existe un `ROA` couvrant l'annonce du préfixe ;
- **invalide** : il existe bien un `ROA` qui couvre le préfixe annoncé, mais l'annonce est faite par un AS non autorisé, ou la longueur du préfixe est supérieure à la longueur maximale autorisée ;
- **non couverte** : aucun `ROA` n'existe.

Dans la pratique, il est possible de configurer les routeurs afin qu'ils ne prennent pas en compte les VRP et qu'ils acceptent des annonces invalides selon la RPKI. La RPKI peut en effet être utilisée pour discriminer les routes selon leur validité, en leur associant, par exemple, une communauté [9] spécifique.

1.2.3 Données utilisées

L'ensemble des analyses effectuées sur le protocole BGP utilise des données disponibles publiquement sur le site du RIPE-NCC, notamment via la base `whois` et le projet RIS [10] [21]. En 2013, celui-ci gère douze collecteurs BGP répartis à travers la planète. Ils stockent et mettent à disposition toutes les annonces de préfixes qu'ils reçoivent.

Dans les rapports précédents, seules les données du collecteur situé à Londres (au LINX, *London Internet Exchange*) étaient utilisées. Afin d'obtenir une vision exhaustive de l'Internet français, il est nécessaire d'utiliser l'ensemble des collecteurs car certains AS français ne sont pas visibles depuis tous les collecteurs. Dans cette nouvelle édition, afin d'améliorer la qualité des analyses tout en limitant la quantité de données générée, deux collecteurs supplémentaires sont utilisés : celui d'Amsterdam (à l'AMS-IX, *Amsterdam Internet Exchange*) et celui de Genève (au CIXP, *CERN Internet eXchange Point*). Ils ont été sélectionnés car ils permettent de voir tous les pairs français du projet RIS, et offrent une vision presque exhaustive des AS français et des préfixes qu'ils annoncent.

9. Dans BGP, une communauté permet de marquer une route en lui associant une valeur.
10. Routing Information Service.

1.3 Identification automatique des AS français

1.3.1 Description

La précédente étude de l'observatoire portait sur 1270 AS identifiés à l'aide d'une méthode automatique. Cette identification nous a permis d'élargir notre analyse, qui ne concernait à l'origine que 4 AS français.

Cependant, la méthodologie employée en 2012 reposait sur une seule extraction de données, effectuée durant le mois de juillet. Cela ne permettait pas de prendre en compte les AS apparus ultérieurement lors du second semestre de l'année.

Afin d'y remédier, quatre extractions de données ont été réalisées au cours des mois de mars, juin, septembre et décembre 2013. Cette évolution a pour objectif d'obtenir la vision de l'Internet français la plus représentative possible.

1.3.2 Méthodologie de mesure

Pour chacune des extractions, nous avons conservé les huit critères indépendants choisis en 2012, et permettant de donner une indication sur le fait que l'AS puisse être français ou non :

1. la description dans la base `whois` du RIPE-NCC [22] contient des mots-clés français ;
2. plus de 75 % des adresses IP sont localisées en France par la bibliothèque `GeoIP` [23] ;
3. la description dans la base du RIPE-NCC contient des mots-clés issus de la liste des opérateurs déclarés auprès de l'ARCEP [24] ;
4. l'organisation gérant l'AS a une adresse postale en France dans la base du RIPE-NCC ;
5. les administrateurs de l'AS ont une adresse postale en France dans la base du RIPE-NCC ;
6. il s'agit de l'un des trente-quatre AS français identifiés manuellement par les membres de l'observatoire ;
7. c'est un AS directement connecté à l'un de ces trente-quatre AS ;
8. son numéro d'AS a été attribué par le RIPE-NCC.

Une première liste d'AS français a été constituée en faisant l'union des listes obtenues à l'issue de ces quatre extractions, ainsi qu'avec la liste des AS français identifiés manuellement. Nous ajoutons volontairement cette dernière liste prédéfinie afin de garantir leur présence dans la liste définitive. Il est en effet possible d'obtenir des faux négatifs avec l'algorithme de partitionnement utilisé.

Limitations

À chaque extraction de données, la méthode de classification que nous employons actuellement entraîne l'apparition de faux positifs et de faux négatifs. Des traitements plus fins ont permis de réduire significativement les erreurs de classification. Cependant, la spécificité de ces traitements rend notre méthode moins généralisable à d'autres pays.

Pour la prochaine édition, nous souhaitons évaluer d'autres algorithmes afin d'essayer d'améliorer la classification automatique des AS, en particulier en limitant le recours à des prétraitements spécifiques à la France.

1.3.3 Résultats et analyse

Au cours de l'année 2013, le nombre d'AS français obtenu après chaque extraction a varié entre 1245 et 1353. L'union des listes obtenues grâce aux quatre extractions a permis de définir une première liste de 1404 AS. En incluant les 765 AS visibles en 2012 [11], nous avons obtenu une nouvelle liste de 1422 AS français. Au cours de nos travaux sur les différents indicateurs, nous avons pu remarquer la présence de quelques faux positifs, qui ont par la suite été retirés. La liste définitive utilisée pour l'étude décrite dans ce rapport comporte 1412 AS français.

À retenir

En 2013, l'observatoire a identifié 1412 AS français. Parmi ceux-ci, le nombre d'AS actifs est de l'ordre de 850, et peut varier en fonction de l'indicateur concerné.

Évolution des AS français en 2013

À l'instar de l'étude portant sur l'année 2012, nous avons étudié l'évolution du nombre d'AS français visibles dans les archives BGP. Pour ce faire, nous avons eu recours aux données des trois collecteurs retenus pour l'étude portant sur le protocole BGP (au LINX, à l'AMS-IX, et au CIXP).

Cette année, 885 AS distincts ont effectué au moins une annonce visible depuis un des trois collecteurs. Le nombre d'AS français visibles quotidiennement a varié entre 767,

11. Dans le rapport portant sur l'année 2012 [25], le nombre d'AS visibles avait été déterminé sur un seul collecteur. Pour définir la nouvelle liste d'AS, nous avons à nouveau effectué la mesure sur les trois collecteurs. Cela explique la différence entre la valeur de 765 indiquée dans ce rapport et celle de 752 indiquée dans le rapport précédent.

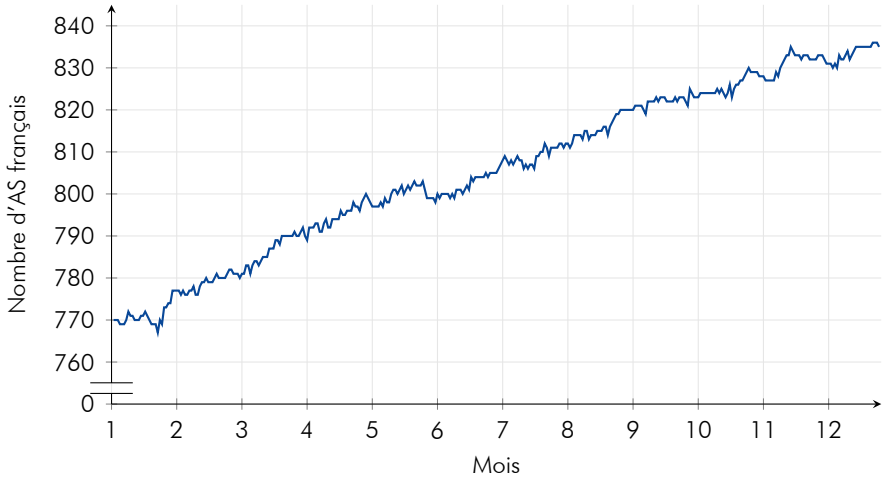

Figure 1.3 – Nombre d'AS français vus dans les archives BGP en 2013

valeur observée en janvier 2013, et 835 à la fin du mois de décembre. La figure 1.3, donnant l'évolution du nombre d'AS visibles quotidiennement tout au long de l'année 2013, illustre l'augmentation.

Un noyau dur de 706 AS annonce au moins un préfixe par jour tout au long de l'année 2013, ce qui représente près de 80 % du nombre total d'AS distincts visibles au cours de l'année. Parmi les 20 % d'AS visibles restant, quelques-uns n'ont été vus qu'un seul jour dans l'année, mais un peu plus de la moitié d'entre eux ont été visibles plus de la moitié de l'année.

1.4 Connectivité des AS français

1.4.1 Description

L'objectif de cet indicateur est d'obtenir une vision globale de la connectivité des AS français. Nous cherchons en particulier à évaluer la robustesse de la connectivité d'un AS. Ceci permet de mettre en lumière quelques AS dont la disparition pourrait entraîner la perte de connectivité à l'Internet pour des AS français. Ces AS seront appelés « AS pivots » dans la suite de ce chapitre.

Pour évaluer cette connectivité, nous représentons les relations entre AS sous la forme d'un graphe à partir des données extraites d'archives BGP. Ainsi, il existe une arête entre deux AS s'ils sont consécutifs dans un `AS_PATH`. Cette arête est orientée en fonction du type de relation commerciale qui existe entre les deux AS. Comme expliqué dans l'introduction, les liens peuvent être de deux types : de *transit* ou de *peering*.

La connaissance de ces types de relation est indispensable pour comprendre correctement la connectivité entre différents AS. Dans une relation de *peering*, deux AS ne vont échanger que leur trafic et celui de leurs clients alors que dans le cadre d'une relation de transit, le fournisseur va accepter de transporter tout le trafic depuis et à destination de son client. Inversement, toujours dans une relation de transit, le client va refuser le trafic en provenance de son transitaire et qui n'est pas destiné à lui ou à l'un de ses clients. La conséquence de ces règles est que tous les chemins dans le graphe entre deux AS ne sont pas acceptables. Seuls ceux qui commencent par des liens de client vers transitaire, suivis d'un éventuel lien de *peering* et de liens de transitaire vers client sont acceptables. Dans la littérature scientifique, on parle de propriété *Valley-free* [26].

Tout ceci a une influence sur la connectivité. Ainsi, sur la figure 1.4, se trouve un exemple minimal de relations entre AS. On peut voir que la disparition de l'AS2 entraîne une perte de connectivité entre les AS6 et AS5. En effet, il existe toujours un chemin dans le graphe mais celui-ci passe par l'AS3, l'AS4, puis par l'AS7. Ce dernier étant client des AS4 et AS5, il refuse de transmettre du trafic de l'un à l'autre.

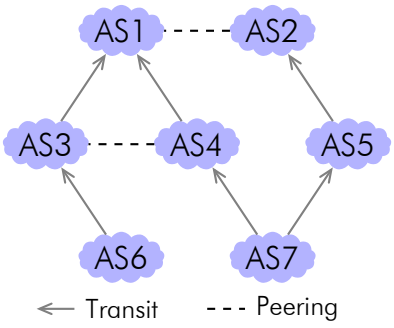

Figure 1.4 – Exemple de graphe d'AS avec les types de relations

Dans les bases `whois` mises à disposition et maintenues par les RIR, les mainteneurs

des objets `aut-num` peuvent renseigner des informations de routage au travers des attributs `import` et `export`. Ces informations sont initialement destinées à la configuration de routeurs, notamment pour le filtrage. Néanmoins, comme ces informations sont renseignées sur la base du volontariat et ne sont pas vérifiées, leur pertinence n'est pas assurée. À la fin de cet indicateur, nous allons évaluer cette dernière en utilisant le graphe de connectivité.

1.4.2 Méthodologie de mesure

Afin de construire le graphe des relations entre AS, nous allons utiliser l'ensemble des archives BGP produites par les collecteurs des projets RIS [21] et Route Views [27] lors des cinq premiers jours de chaque mois. Ensuite, le graphe est produit en utilisant l'algorithme d'inférence de relation de CAIDA [26, 28]. À partir de ce graphe, nous cherchons à obtenir la liste des métriques suivantes :

- **l'enveloppe convexe des AS français** qui est le graphe contenant l'ensemble des AS français et tous les AS qui se trouvent entre deux AS français sur un `AS_PATH` ;
- **les AS pivots** qui sont des AS dont la panne entraînerait la perte de connectivité à l'Internet d'un ou plusieurs AS français. On considère qu'un AS français perd la connectivité à l'Internet s'il ne peut plus contacter un AS Tier 1 [12] ;
- **l'exactitude des bases whois** en comparant les liens déclarés à ceux qui sont observés au travers des archives BGP.

Afin d'obtenir le graphe à partir des bases de donnée `whois`, nous utilisons les attributs `import` et `export` des objets `aut-num`. Ceux-ci permettent à un opérateur de décrire l'ensemble de sa politique de routage. Les différentes relations possibles sont rappelées dans l'introduction.

```
aut-num:        AS64496
as-name:        AS-D-EXEMPLE
descr:          AS d'exemple
[...]
import:         from AS-TRANSIT action pref=430; accept ANY
export:         to AS-TRANSIT announce AS-SET-D-EXEMPLE
import:         from AS-CLIENT action pref=200; accept AS-SET-CLIENT
export:         to AS-CLIENT announce ANY
import:         from AS-PEER action pref=200; accept AS-SET-PEER
export:         to AS-PEER announce AS-SET-D-EXEMPLE
```

Figure 1.5 – Exemple d'un objet `aut-num` avec des attributs `import` et `export`

Un exemple d'objet `aut-num` est donné dans la figure 1.5. L'objet *AS-SET-D-EXEMPLE* est de type `as-set` et contient *AS-D-EXEMPLE* ainsi que ses clients comme représenté

12. Par définition, un AS Tier 1 n'a pas de fournisseur de transit, il n'a que des relations de *peering*.

sur la figure 1.6. Les objets *AS-SET-PEER* et *AS-SET-CLIENT* sont construits de la même façon. On peut en déduire que les AS *AS-TRANSIT*, *AS-CLIENT* et *AS-PEER* sont respectivement un transitaire, un client et un peer de l'AS 64496.

```
as-set: AS-SET-D-EXEMPLE
[...]
members: AS64496
members: AS-CLIENT
```

Figure 1.6 – Exemple d'un objet `as-set`

Améliorations vis-à-vis de du rapport 2012

Dans le rapport 2012, le graphe qui était construit n'avait pas d'orientation des arêtes. Les résultats obtenus étaient donc beaucoup moins précis car certains AS pivots pouvaient ne pas avoir été détectés. De plus, Le graphe était construit à partir d'un seul collecteur du RIS, et était basé sur une unique archive BGP.

Cette année, l'ensemble des collecteurs du RIS et du projet Route Views ont été utilisés. Enfin, pour générer une vue complète à partir des données issues des bases `whois`, l'analyse des attributs `import` et `export` des objets `aut-num` et l'analyse des objets `as-sets` a été automatisée.

Limitations

L'approche qui a été utilisée pour étudier la connectivité dans ce rapport souffre de plusieurs limites. Tout d'abord, la vision des tables de routage est partielle car limitée aux différents collecteurs utilisés. En particulier, nous ne voyons ni les accords de *peering* des AS qui ne sont pas directement connectés aux collecteurs, ni ceux des AS qui ne les propagent pas, ni les routes de secours. Ceci implique que le graphe réel de connectivité est plus riche que celui que nous étudions.

Par ailleurs, l'inférence des relations entre AS est une approximation. Il existe de nombreuses situations qui peuvent différer d'une relation entre un opérateur de transit et son client ou une relation de *peering*. Néanmoins, cette approximation donne des résultats très précis comme le montre la littérature sur le sujet [28].

1.4.3 Résultats et analyse

Comme on peut le voir sur la figure 1.7, au cours de l'année 2013, le nombre d'AS présents sur des chemins d'AS a crû de manière linéaire aussi bien en IPv4 qu'en IPv6. En IPv4, le nombre d'AS présents en décembre 2013 était de 844 contre 787 en janvier soit une croissance d'environ 7 %. Ces valeurs sont légèrement supérieures à celles présentées dans la figure 1.3 car, dans ce cas-là, les AS considérés sont ceux

qui annoncent des préfixes ; certains opérateurs de transit peuvent être présents sur des chemins d'AS sans annoncer de préfixes eux-mêmes. De manière similaire, au mois de décembre 2013, le nombre d'AS français présents sur des chemins d'AS en IPv6 était de 265 contre 183 en janvier, soit une croissance très significative de 44 %.

L'Internet français ne se suffit pas et des AS étrangers peuventpeuvent êtree nécessaires pour faire transiter le trafic entre deux AS français. C'est pour cette raison qu'il est nécessaire de calculer l'enveloppe convexe de l'Internet français. Le nombre d'AS étrangers contenus dans celle-ci est représenté sur la figure 1.7. On peut voir qu'en IPv4, le nombre d'AS étrangers dans l'enveloppe a décru de manière régulière tout au long de l'année 2013, passant de 356 en janvier à 270 en décembre, soit une diminution de 24 %. En IPv6, le nombre d'AS étrangers dans l'enveloppe est resté relativement stable, d'un maximum à 67 en février, il est passé à un minimum de 50 en août et ce malgré la forte augmentation du nombre d'AS présents sur les chemins d'AS en IPv6. Enfin, on peut remarquer que la proportion d'AS étrangers dans l'enveloppe convexe de l'Internet français en décembre 2013 est de 24 % en IPv4 contre 17 % en IPv6.

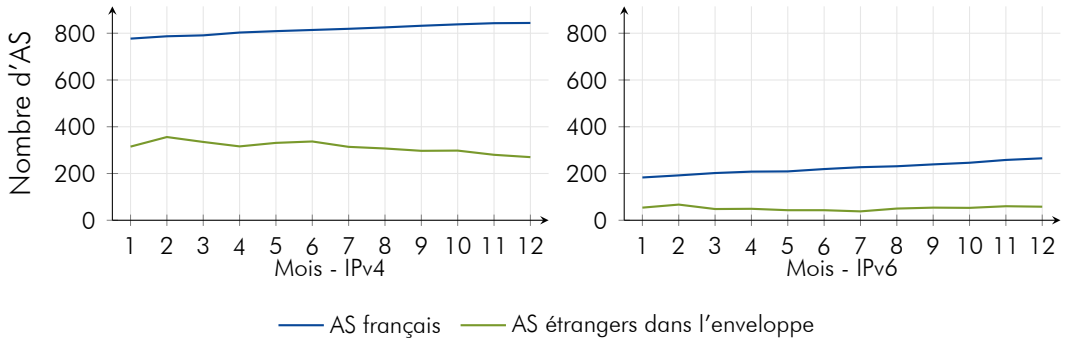

Figure 1.7 – Évolution du nombre d'AS français et de l'enveloppe en 2013

Au cours de l'année 2013, les AS pivots en IPv4 ont peu évolué comme on peut le voir sur la figure 1.8. Le nombre d'AS pivots français a légèrement augmenté sur l'année, évoluant entre 59 en janvier et 63 en décembre. En revanche, le nombre d'AS pivots étrangers a diminué en passant de 28 en janvier à 21 en décembre. Ces deux tendances se compensent et le nombre d'AS pivots est resté stable sur l'année 2013. En revanche, la situation est différente pour IPv6 où le nombre d'AS pivots a sensiblement augmenté au cours de l'année. Ainsi, il y avait 13 AS pivots français en janvier contre 21 en décembre et 5 AS pivots étrangers contre 12 en décembre avec un maximum de 15 en septembre. Au total, le nombre d'AS pivots a crû de 83 % sur l'année. Cette augmentation s'explique certainement par la croissance forte des AS actifs en IPv6. En effet, les nouveaux entrants n'ont pas forcément tous encore consolidé leur connectivité en prenant plusieurs fournisseurs pour IPv6. La connectivité IPv4 paraît d'ailleurs légèrement plus robuste que celle en IPv6 avec environ un AS pivot pour dix AS français en IPv4 contre un pour huit en IPv6.

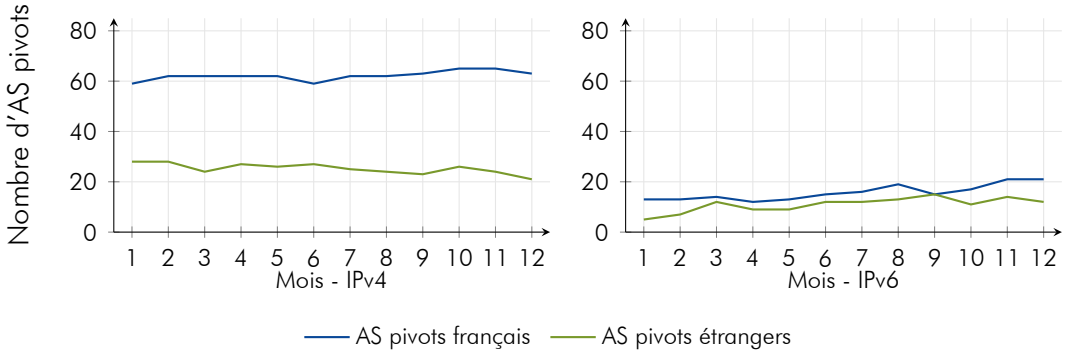

Figure 1.8 – Évolution du nombre d'AS pivots français et étrangers en 2013

Le nombre d'AS pivots ne suffit pas pour évaluer la robustesse de la connectivité, il faut également évaluer l'impact de la disparition d'un AS pivot. Il existe relativement peu d'AS dont la disparition aurait un impact significatif. Ainsi, comme on peut le voir sur la figure 1.9, pour le cas d'IPv4, seuls 8 AS pivots affecteraient au moins dix AS en cas de défaillance et seuls 22 auraient un impact sur au moins trois AS. En revanche, les 8 AS les plus critiques peuvent avoir un impact significatif. Ainsi, l'AS pivot le plus critique aura un impact sur 34 AS, soit 4 % des AS français actifs au même moment.

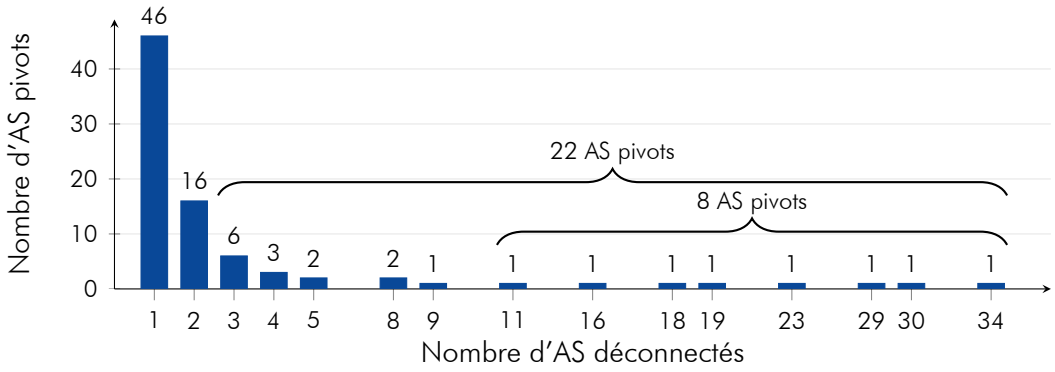

Figure 1.9 – AS pivots en fonction du nombre d'AS déconnectés (IPv4, déc 2013)

Pour IPv6, la figure 1.10 montre qu'il existe seulement 2 AS pivots pouvant déconnecter au moins dix AS mais chacun d'entre eux peut affecter 15 ou 16 AS soit plus de 5 % des AS français actifs en IPv6. De même, 12 AS pivots peuvent avoir un impact sur plus de trois AS français. En proportion, c'est 33 % des AS pivots contre 26 % pour IPv4.

Enfin, il est bon de noter que l'utilisation de deux transitaires est suffisante pour avoir un bon niveau de protection contre la défaillance d'un AS dans l'Internet. Aucun des AS français qui ont plus d'un fournisseur de transit ne serait déconnecté de l'Internet par la défaillance de l'un des AS pivots. Ceci n'est pas vrai dans l'Internet globalement et on pourra se reporter à un rapport technique [26] pour plus de détails à ce sujet.

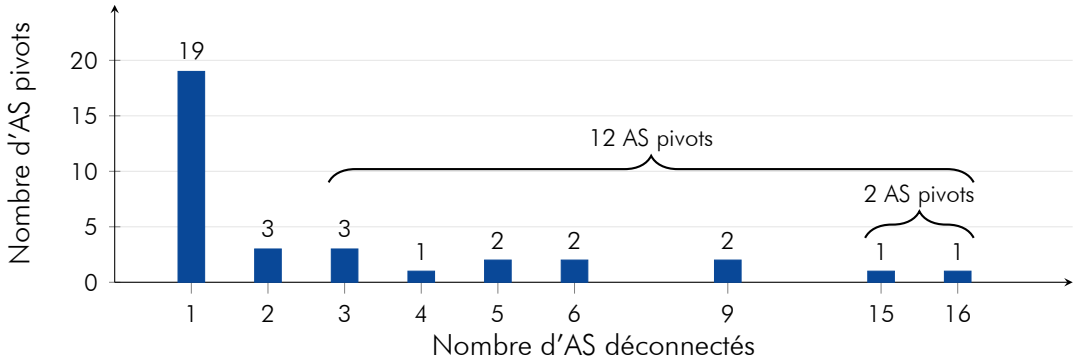

Figure 1.10 – AS pivots en fonction du nombre d'AS déconnectés (IPv6, déc 2013)

Une représentation graphique de la connectivité en IPv4 et en IPv6 est donnée sur les figures 1.11 et 1.12. Afin de permettre à ces figures de rester lisibles, nous avons représenté uniquement les AS français, les AS pivots et quelques AS nécessaires pour que l'ensemble soit connecté. Ces graphes permettent néanmoins d'appréhender la structure de l'Internet français et de constater visuellement la différence significative entre IPv4 et IPv6. Sur cette représentation, les AS ayant un rang élevé selon les relations de transit, se retrouvent naturellement au centre du dessin. On peut remarquer en particulier que les relations de *peering* visibles sont fortement concentrées au centre. Cela vient du fait qu'une relation de *peering* n'est visible que si un des collecteurs est connecté à un des membres de la relation de *peering* ou l'un de ses clients (directs ou indirects).

À retenir

Afin d'assurer la résilience de sa connectivité à l'Internet, il est recommandé d'avoir plusieurs fournisseurs de transit.

Qualité des informations dans les bases `whois`

Afin d'évaluer la qualité des informations `import/export` saisies par les acteurs de l'Internet français dans les bases `whois`, une analyse automatique a été effectuée sur celle-ci et les résultats principaux sont donnés dans le tableau 1.1. Ces résultats sont ceux du de décembre 2013 mais les variations au cours de l'année sont faibles. Dans la colonne de gauche, se trouve le pourcentage des relations annoncées par BGP présentes dans les bases `whois` et, dans la colonne de droite, est donné le pourcentage de relations présentes dans les bases `whois` et visibles dans des annonces BGP.

Comme on peut le voir, les informations sur les relations de transit sont relativement correctes. Ainsi 76 % des relations de transit observées dans les archives BGP sont dé-

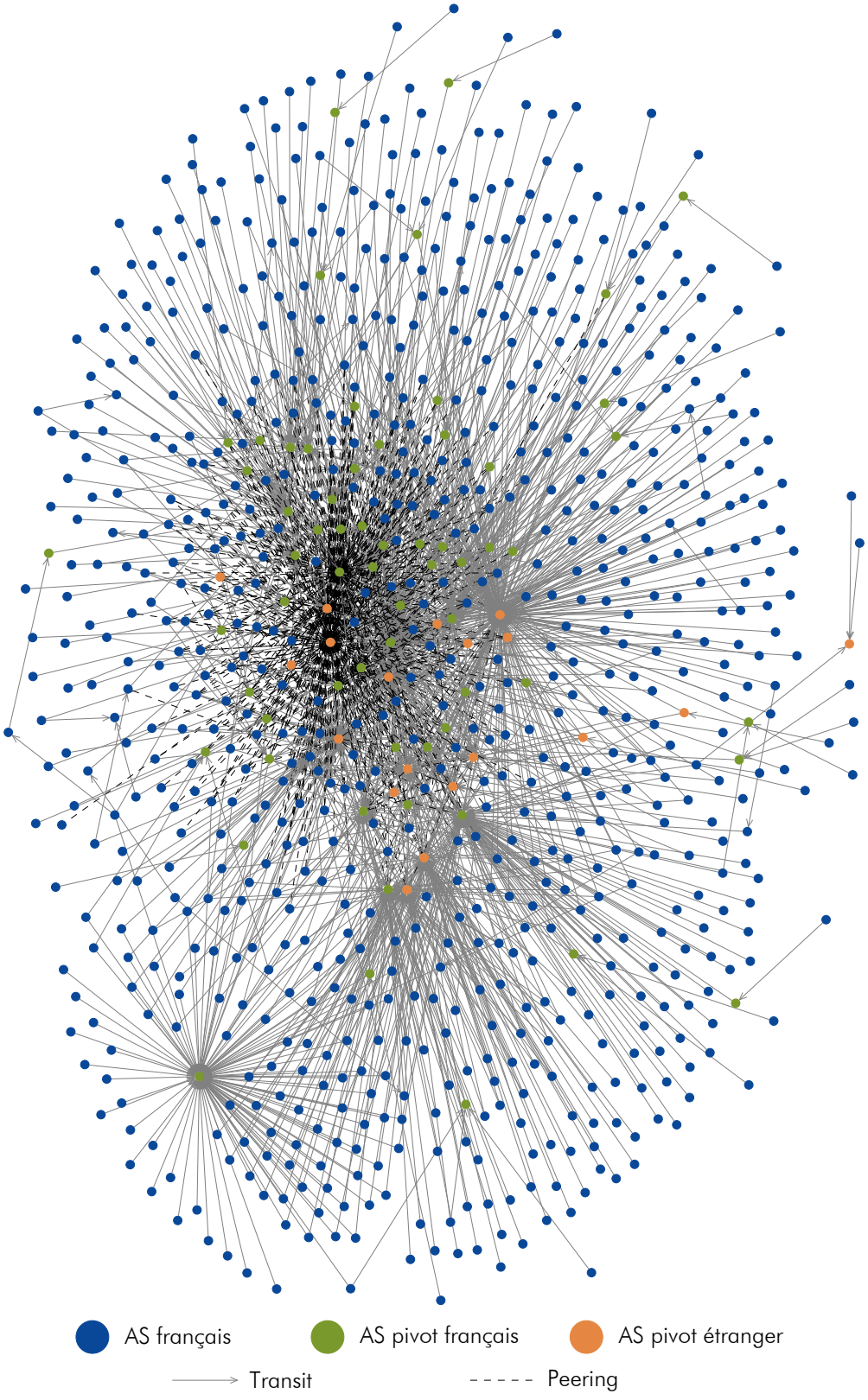

Figure 1.11 – Graphe de connectivité en IPv4 (décembre 2013)

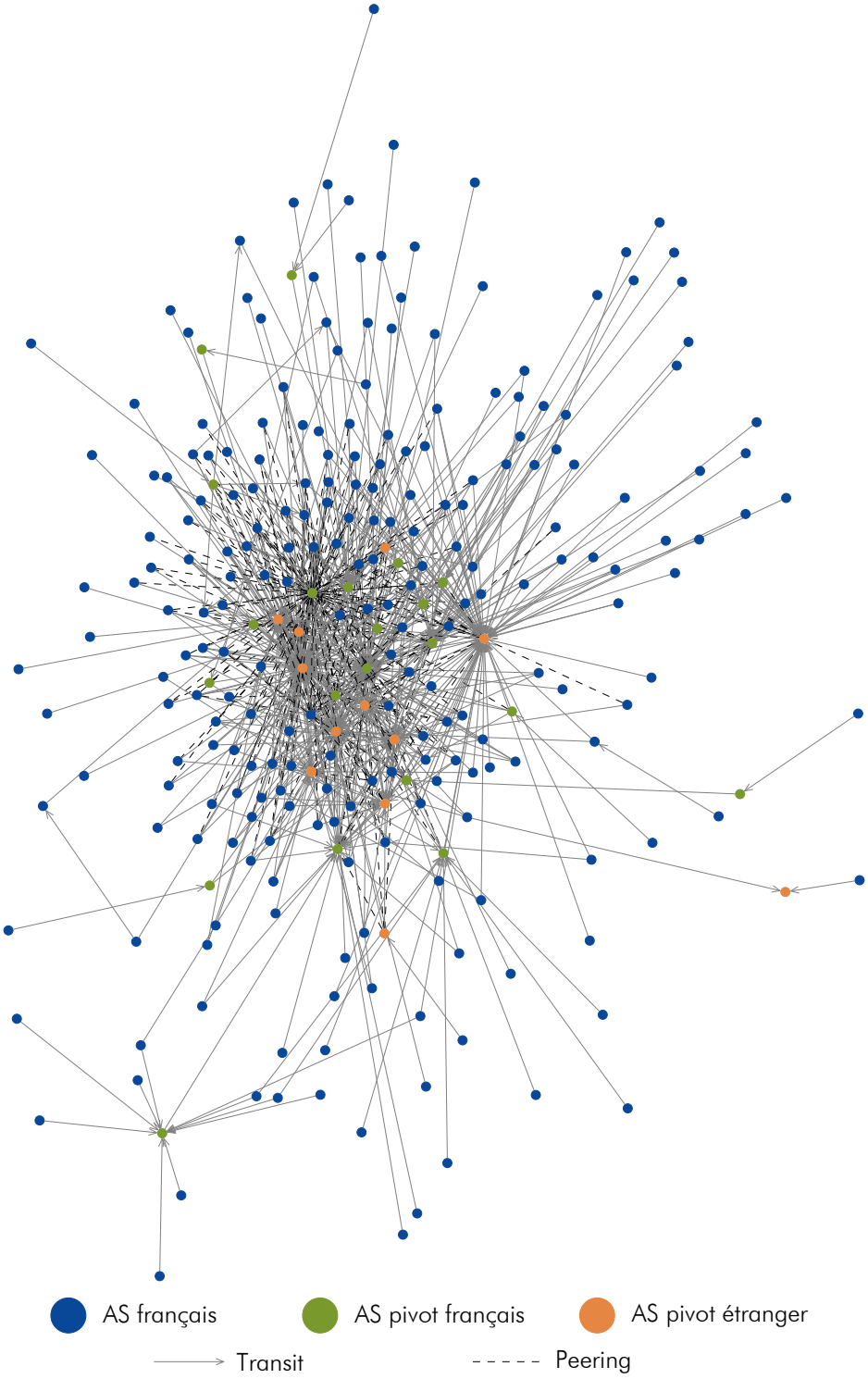

Figure 1.12 – Graphe de connectivité en IPv6 (décembre 2013)

clarées dans les bases `whois`. Ce résultat peut sans doute s'expliquer par le fait que de nombreux fournisseurs de transit demandent à leurs clients de renseigner les informations dans les bases de données avant d'autoriser leur trafic. Par ailleurs, les fournisseurs changent relativement peu. Inversement, 65 % des relations de transit déclarées sont vues dans les archives BGP. Les 35 % qui ne sont pas vues peuvent s'expliquer en partie par les liens de secours qui ne sont annoncés que lorsque c'est nécessaire.

Relation	BGP/`whois`	`whois`/BGP
Transitaires	76 %	65 %
Clients	41 %	52 %
Peering	10 %	6 %

Table 1.1 – Adéquation des informations dans les archives BGP et dans les bases `whois`

Les résultats sur les relations de clients sont plus mitigées. Ainsi, seules 52 % des relations annoncées dans les bases `whois` sont visibles dans les archives BGP. Inversement, 41 % des relations visibles dans les archives BGP sont déclarées dans les bases `whois`. Deux phénomènes principaux sont sans doute à l'origine de ce constat. Premièrement, les changements parmi les clients d'un AS sont beaucoup plus fréquents que ceux parmi les fournisseurs. En second lieu, nous avons pu observer que beaucoup de mises-à-jour sont incomplètes. Pour certaines connexions, des AS ont les attributs `import` sans avoir les attributs `export` associés ou réciproquement. Ceci est en particulier dû à la mauvaise maintenance des objets `as-set` associés. Ces résultats sont problématiques car une mauvaise déclaration dans les bases `whois` peut entraîner des problèmes de connectivité, du fait de la politique de filtrage de certains fournisseurs de transit.

Enfin, seulement 10 % des relations de peering vues dans les archives BGP sont déclarées dans les bases `whois`, et seulement 6 % des relations déclarées sont visibles. Les remarques précédentes sur le maintien des objets s'appliquent également pour les relations de *peering*. Par ailleurs, certains AS ne sont pas en capacité de lister l'ensemble de leurs relations de *peering*, notamment lorsqu'ils utilisent les *peerings* publics dans les points d'échange. Enfin, il n'est pas surprenant qu'une faible proportion des relations déclarées soient visibles car, comme expliqué plus haut, pour qu'une relation soit visible dans les archives BGP, il faut qu'un des collecteurs utilisés soit connecté à l'un des AS dans la relation de *peering* ou l'un de ses clients.

À retenir

Certains fournisseurs de transit utilisent les attributs `import` et `export` des objets `aut-num` pour filtrer les annonces de leurs clients. Il est donc important de maintenir à jour ces objets ainsi que les objets `as-set` associés.

1.5 Usurpations de préfixes

1.5.1 Description

Il n'existe pas de lien fort entre l'AS qui a la délégation d'un préfixe et les annonces de préfixes qui sont effectivement réalisées sur Internet. En conséquence, n'importe quel AS peut annoncer n'importe quel préfixe. On parle d'usurpation de préfixes lorsqu'un AS, appelé « AS usurpateur », annonce de façon illégitime un préfixe égal ou plus spécifique à un préfixe délégué à un autre AS, appelé « AS usurpé ».
Sur Internet, il est toutefois fréquent de voir des annonces de préfixes faites par des AS qui n'en ont pas la délégation. Un fournisseur d'accès peut, en effet, autoriser un de ses fournisseurs de service à annoncer ses préfixes de façon légitime.

Afin d'identifier les usurpations de préfixes, nous recherchons les annonces de préfixes plus spécifiques ou égales aux annonces légitimes effectuées par les AS français. Ces annonces en conflits sont alors classées afin d'identifier si elles sont légitimes ou non.

Pour chacune des annonces détectées, nous regardons tout d'abord si un objet `route` ou un `ROA` existe. Si c'est le cas, l'annonce est considérée comme valide. Les objets `aut-num` des AS en conflit sont alors utilisés afin de déterminer, par exemple, s'ils appartiennent à la même organisation, ou s'ils sont administrés par les mêmes gestionnaires. Cette validation faible est cependant pertinente en pratique, car elle permet de mettre en évidence des relations techniques ou commerciales entre deux AS.

L'`AS_PATH` est par ailleurs utilisé afin de déterminer la distance, en nombre d'AS, entre l'AS usurpé et l'AS usurpateur. La distance est un facteur pertinent pour l'analyse des usurpations. En effet, lorsque l'AS usurpateur est directement connecté à l'AS usurpé, l'expérience et le rapport 2012 montrent que les annonces associées sont pour la majorité des défauts de déclaration d'objets `route` ou de `ROA`.

Afin de faciliter l'identification des usurpations de préfixes, les annonces en conflit sont regroupées afin d'en déterminer la durée. Ces regroupements d'annonces, appelées « événement » dans la suite du document, permettent à la fois de réduire les données à analyser, et d'identifier plus finement les usurpations de préfixes. En effet, elles ont habituellement des durées plus courtes que les événements légitimes.

En marge des usurpations de préfixes, les analyses menées dans le cadre de cet indicateur permettent également de mettre en évidence des réannonces de table de routage. Suite à des erreurs de configuration, il arrive parfois qu'un AS réannonce l'intégralité des routes de l'Internet à ses fournisseurs en prétendant être à l'origine de ces préfixes. Par conséquent, il semble usurper un nombre important de préfixes au même instant.

Les analyses concernant les réannonces récentes [8, 29, 30] mettent en évidence que les fournisseurs des AS, à l'origine de ces réannonces, n'appliquent pas de filtre sur le nombre maximal de préfixes annoncés par leurs clients [1].

Par ailleurs, dans le cadre d'accords entre deux opérateurs, il est fréquent que des services de *peering* [13] soient annoncés localement au sein de leurs réseaux, afin de faire transiter les paquets via des liens de *peering* plutôt que sur Internet. Il arrive parfois que des annonces de services réannoncées par erreur soient visibles sur Internet.

1.5.2 Méthodologie de mesure

La méthodologie décrite dans le rapport 2012 a été améliorée afin d'identifier les usurpations de manière plus efficace. Ainsi à partir des archives publiques BGP, nous établissons la liste de toutes les annonces survenues durant l'année 2013 qui sont en conflit avec des annonces effectuées par des AS français. Ces annonces sont des messages `UPDATE` reçus par les trois collecteurs du projet RIS que l'observatoire utilise. Elles comportent chacune un *timestamp* correspondant à l'instant où le message BGP a été reçu. Elles contiennent également le préfixe annoncé par l'AS français usurpé, un préfixe, égal au précédent ou plus spécifique, annoncé par l'AS usurpateur, l'`AS_PATH` correspondant, ainsi que le pair BGP l'ayant vu. Pour cet indicateur, nous étudions à la fois les préfixes IPv4 et IPv6, sans distinction.

Dans un premier temps, l'ensemble de ces annonces est comparé aux archives quotidiennes des objets `route`, des `ROA` et des objets `aut-num`. Cela permet de classer les annonces dans les quatre catégories suivantes :

- **valide :** un objet `route` ou un `ROA` correspond au préfixe à l'origine de l'annonce ;
- **relation :** les attributs [14] des objets `aut-num` en conflit indiquent qu'ils appartiennent aux même gestionnaires, ou à la même organisation ;
- **direct :** l'AS usurpé est présent dans l'`AS_PATH` entre l'AS usurpateur et le collecteur ;
- **anormal :** aucune autre catégorie ne s'applique.

Des annonces aux événements

Afin de faciliter les analyses, les annonces sont alors transformées en événements possédant un début et une fin. Pour cela, les annonces sont regroupées selon : les numéros d'AS, les préfixes en conflits ainsi que le pair et le collecteur ayant reçu l'annonce de l'AS usurpateur. L'algorithme suivant est alors appliqué à toutes les annonces regroupées et triées selon leurs *timestamps* :

1. les deux premiers *timestamps* correspondent respectivement au début et à la fin d'un nouvel événement ;
2. tant que les annonces suivantes sont séparées de moins de 8 heures [15] de la

13. Il s'agit de préfixes /25, /32, ou /128 qui correspondent, par exemple, à des adresses de serveurs d'authentification.
14. Les attributs `org`, `mnt-by`, `mnt-lower`, `mnt-routes`, `tech-c` et `admin-c` sont utilisés.
15. Les collecteurs du RIS enregistrent toutes les routes au moins une fois toutes les 8 heures.

fin de l'événement, ces annonces sont assimilées à l'événement courant, et l'annonce la plus récente devient la fin de l'événement ;

3. sinon, on retourne en 1.

Des annonces en conflits peuvent être reçues par plusieurs collecteurs. Toutefois, en raison d'une mauvaise synchronisation temporelle des collecteurs, ou des temps de propagation des messages `UPDATE` dans l'Internet, il est possible que ces annonces ne soient pas reçues au même moment par les collecteurs. Il convient donc de synchroniser les événements. Tous les événements commençant ou se terminant au même instant sont considérés comme un seul événement vu par plusieurs pairs.

Identification des réannonces de route

Afin d'identifier les réannonces de table de routage, il faut rechercher les AS qui sont à l'origine d'un nombre d'événements importants, dont les durées sont d'environ une heure, et les préfixes en conflits strictement identiques aux annonces légitimes.

De plus, les réannonces de services de *peering* peuvent également être retrouvées en recherchant les événements concernant des préfixes très spécifiques [16] reçus directement par un pair de l'un des trois collecteurs utilisés (i.e. dont la longueur de l'`AS_PATH` est comprise entre 1 et 2).

Identification des usurpations

Afin de simplifier l'identification, une nouvelle étape d'agrégation est effectuée. Pour chaque couple de préfixes et d'AS en conflits, nous identifions les dates d'apparition et de disparition des événements associés, la durée réelle, ainsi que le nombre de collecteurs et de pairs l'ayant reçu. La durée réelle est une information intéressante car elle permet d'identifier des événements ponctuels vus pendant une grande période de l'année. Ces regroupements d'événements sont par la suite appelés « conflits ».

Tout d'abord, les conflits correspondants aux réannonces identifiées sont supprimés. Ensuite, si un conflit est dû à une annonce effectuée par un numéro d'AS réservé [17], il l'est également.

Le regroupement des événements en conflits permet d'adopter une approche plus fine que celle du rapport précédent afin d'éliminer ceux qui ne sont probablement pas des usurpations. Ainsi, lorsqu'un conflit change de catégorie au cours de l'année, cela indique qu'il existe probablement une relation entre les deux AS. Ce type de conflits n'est alors pas pris en compte dans l'identification des usurpations. Par exemple, s'il existe des conflits entre deux AS identifiés comme valides et en relation, l'ensemble des conflits entre ces deux AS n'est pas considéré.

16. La taille du masque est supérieure à 24 bits en IPv4 ou 64 bits en IPv6.
17. Il s'agit des AS privés, de documentations, et de l'AS_TRANS.

Finalement, on s'intéresse aux conflits très longs ; qui durent plus de 6 mois, et qui ont commencé avant le mois de juin 2013. S'il existe un tel conflit entre deux AS, alors on peut supposer qu'il existe une relation entre eux. Il est alors acceptable d'écarter de nos analyses les autres conflits entre ces deux AS.

Limitations

Tout comme dans les rapports précédents, nous ne prenons pas en compte les conflits portant sur des préfixes appartenant à un AS mais qui n'auraient pas été annoncés par cet AS. De plus, les conflits d'annonces ne concernant que les AS français, nos analyses peuvent donc manquer des réannonces de tables de routage si un `max-prefix` est mis en place avant qu'un grand nombre d'acteurs français ne soit touché.

Les identifications de conflits sont effectuées indépendamment, pour chacun des trois collecteurs utilisés. Il est donc possible que nous manquions des conflits, dans le cas où une annonce légitime est uniquement reçue par un collecteur, et l'annonce conflictuelle par un autre. Par ailleurs, l'algorithme décrit ne prend pas en compte les messages `WITHDRAW`. En conséquence, les durées calculées peuvent être supérieures aux durées réelles. Dans la prochaine édition du rapport, nous souhaitons le calculer de manière plus précise à l'aide des messages `WITHDRAW`.

Il est difficile de déterminer de façon automatisée et fiable si un événement anormal est effectivement une usurpation de préfixes. Les outils utilisés dans cette section permettent d'accompagner l'analyse manuelle et de réduire considérablement le nombre de conflits à analyser manuellement. Afin d'identifier les usurpations de façon plus efficace, nous souhaitons étudier la possibilité d'effectuer des mesures actives, pour identifier si les événements détectés s'accompagnent de changements dans les politiques de routage.

1.5.3 Résultats et analyse

Résultats globaux

Sur les 1412 AS français étudiés, seuls 215 sont la cible d'événements au cours de l'année 2013. Par ailleurs, 257 AS sont à l'origine des événements non valides, dont 124 AS français. L'analyse des chemins d'AS correspondant aux événements indique que 242 AS, dont 78 français, ne filtrent pas les annonces faites par leurs clients à l'aide des objets `route` ou des `ROA`, car ils redistribuent des annonces non valides.

La figure 1.13 présente la répartition des 181 957 événements [18] identifiés suivant les quatre types définis. On peut constater que près de la moitié des événements détectés sont validés par des objets `route` ou des `ROA`.

18. Ils correspondent à 28 827 142 annonces BGP en conflit.

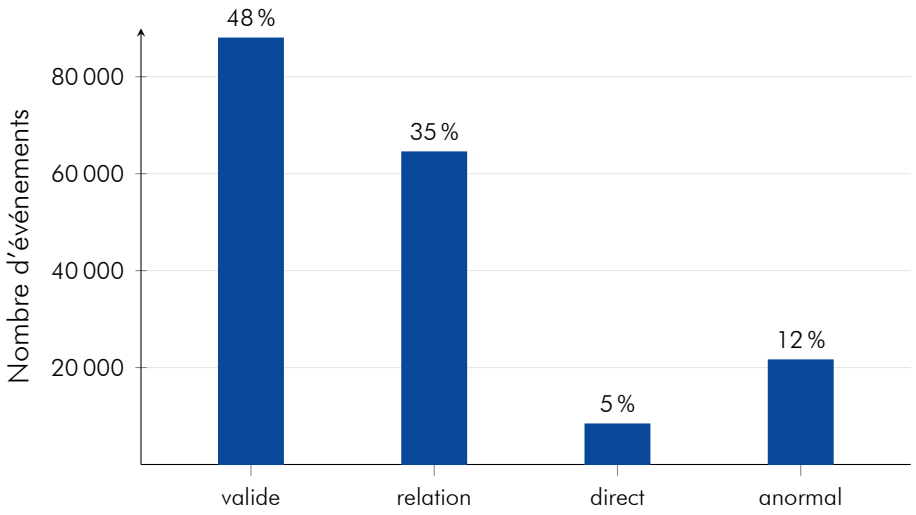

Figure 1.13 – Types des événements détectés en 2013

Par ailleurs, la catégorie relation représente 35 % des événements. Il s'agit d'un résultat très important qui confirme les intuitions formulées dans le rapport 2012 : un grand nombre d'événements non valides correspond à des défauts de déclarations d'objets. Il est intéressant de signaler que l'utilisation des `ROA`, quoique anecdotique, permet de valider quelques événements pour lesquels aucun objet `route` n'est déclaré.

L'étude de la catégorie relation montre que 84 couples d'AS sont à l'origine de ces événements. La plupart de ces couples correspondent à des réseaux universitaires, des délégations de services à des clients d'opérateurs, des filiales ou des AS avec numéros sur 16 et 32 bits. Les événements de la catégorie relation proviennent, pour la plupart, d'annonces anormales ou directes.

Près de 65 % des 64 379 événements en relation rentrent dans cette catégorie car les numéros d'AS en conflits ont au moins deux attributs en commun [19]. Une analyse manuelle uniquement basée sur la connaissance des AS et de leurs noms a permis de valider que les trois quarts des relations concordent, et correspondent bien à des défauts de déclaration.

À retenir

35 % des événements en conflit correspondent à des défauts de déclaration d'objets `route` ou de `ROA`. Les annonces associées sont principalement effectués par des AS appartenant aux mêmes organisations.

19. Les attributs les plus significatifs sont `mnt-*` et `admin-c/tech-c`, `mnt-*` et `org`.

Identification des réannonces de route

La méthodologie utilisée identifie 13 réannonces de table de routage touchant entre 2 et 15 préfixes français chacune. Cinq d'entre elles sont effectuées par des AS français. Par ailleurs, un AS jordanien est à l'origine de cinq d'entre elles, entre mi-avril et et mi-mai 2013. Après analyse, il s'avère que cet AS a annoncé ponctuellement plus de 700 préfixes. En temps normal, il en annonce une vingtaine. Il s'agit d'un résultat particulièrement intéressant car ces réannonces n'avaient pas été discutées publiquement. Ces réannonces sont probablement dues à des erreurs de configuration de routeurs chez cet AS jordanien.

Environ 250 réannonces de service de *peering* ont pu être identifiées. Elles concernent principalement des préfixes IPv4 /32 inclus dans des préfixes annoncés par des AS français. Un transitaire international est à l'origine de la plupart de ces réannonces.

Une analyse manuelle complémentaire a permis de mettre en évidence d'autres phénomènes de réannonces. La première concerne une série d'annonces effectuées par un AS américain entre janvier et mars 2013, et rapportées publiquement [31, 32]. À ce jour, il n'existe pas d'explication claire à ces réannonces, car l'AS américain n'aurait jamais annoncé ces préfixes. De plus, ces préfixes sont appris via des `AS_PATH` qui ne sont pas habituellement ceux de cet AS américain [20].
La seconde a été effectuée par un AS français pendant 10 minutes environ. Trois autres AS français ont été touchés. Les préfixes en cause étaient annoncés de façon légitime par cet AS avant 2013. Il pourrait s'agir de la mise en route d'un vieil équipement, ou de l'utilisation d'une ancienne configuration.
Pour ce qui est des autres réannonces, nos outils ne les ont pas détecté car il s'agit de préfixes plus spécifiques que ceux habituellement annoncés. Nos algorithmes n'avaient pas identifié ces réannonces car elles ont duré plus d'une heure et concernaient parfois des préfixes plus spécifiques que ceux annoncés par les AS légitimes.

Finalement, nos outils ont manqué 2 réannonces de services de *peering* concernant des préfixes IPv4 /32 et IPv6 /128. Elles n'ont pas été identifiées car les `AS_PATH` correspondants sont composés de plus de 2 AS. Ces deux réannonces sont très courtes, et ne sont vues que par un seul pair.

Identification des usurpations

Au cours de l'année 2013, nous avons identifié 3739 conflits d'annonces. Notre méthodologie nous permet de focaliser nos analyses sur 242 d'entre eux qui ne font pas partie de réannonces de route identifiées automatiquement, et pour lesquels aucun événement valide ou en relation n'existe.

20. Le transitaire apparaissant dans les AS_PATH incriminé a indiqué qu'il ne fournissait pas de service de transit à l'AS incriminé

Afin d'identifier les conflits qui sont des usurpations, il est nécessaire de procéder à une analyse manuelle.
Un ensemble de 48 conflits d'annonces correspondent en fait à une erreur de configuration, car les deux numéros d'AS sont très proches. En mai 2013, pendant près de 15 heures, un AS étranger a annoncé ses préfixes avec le numéro d'un AS français qui n'annonce jamais de préfixe. Un conflit d'annonce a ainsi été détecté par nos outils.

De février à juillet 2013, des conflits très courts correspondant à des annonces d'un AS français contre des préfixes d'un transitaire français sont apparus. Il s'agit probablement d'une erreur, car les `AS_PATH` correspondants indiquent que ces annonces passent toutes par un troisième AS, qui est la maison mère du transitaire usurpé.

En mars 2013, des conflits ponctuels contre un transitaire français ont été détectés. Ils semblent également provenir d'une erreur de configuration. En effet, le numéro d'AS à l'origine des conflits n'est pas attribué. Il est cependant très proche du numéro d'un AS français pour lequel le transitaire a déclaré des objets `route` : seul le dernier chiffre diffère entre ses deux numéros d'AS.

Quatre conflits correspondent au préfixe 2002 ::/16 utilisé par le mécanisme de transition 6to4. Il est normal que ce préfixe soit annoncé par plusieurs AS en même temps afin d'assurer une bonne qualité du service. Un AS français fournissant un relais 6to4, des conflits sont détectés.

À ce stade, il reste une centaine de conflits qui pourraient être des usurpations. Afin de simplifier les dernières analyses, nous ne conservons que les 34 derniers conflits effectués par des AS étrangers et dont la durée réelle est comprise entre 1 jour et 6 mois. Cela permet de mettre en évidence les conflits qui auraient pu provoquer des détournements de trafic sans que les AS français ciblés ne puissent réagir rapidement.

Une dernière analyse manuelle a permis d'identifier que 10 de ces conflits semblent être des usurpations contre 7 AS français. Elles ont des durées variables, de 15 à 166 jours, et ont été vues par les trois collecteurs. Cela laisse à supposer qu'elles ont pu être suivies par des détournements de trafic. L'une des ces usurpations correspond d'ailleurs aux usurpations rapportées par la société Renesys [33] et pour lesquelles du trafic a été détourné.

À retenir

En 2013, 10 conflits d'annonces semblent être des usurpations envers 7 AS français.

1.6 Utilisation des objets route

1.6.1 Description

Les objets `route`[21] sont des informations importantes pour la mise en place d'interconnexions BGP. Ils permettent de s'assurer de la légitimité d'un AS à annoncer un préfixe donné. C'est par leur intermédiaire qu'un opérateur de transit peut mettre en place des filtres sur les préfixes IP annoncés par ses clients.

Un opérateur, titulaire du bloc d'adresses IP 198.18.0.0/15, peut déclarer l'objet `route` correspondant et annoncer le préfixe 198.18.15.0/24 avec BGP. Dans ce cas, l'objet `route` est couvrant car il englobe le préfixe. Il est aussi possible de déclarer des objets `route` plus spécifiques, comme 198.18.0.0/23.

Les opérateurs de transit peuvent avoir trois politiques différentes sur le filtrage par objets `route` :

- **aucun filtrage** ;
- **filtrage couvrant** : le préfixe a un objet `route` contenant le préfixe annoncé ;
- **filtrage précis** : les préfixes annoncés correspondent exactement à des objets `route` déclarés.

La figure 1.14 permet d'illustrer les deux sous-parties de l'indicateur. Deux ensembles, violet et orange, représentent respectivement les objets `route` déclarés auprès du RIPE et les préfixes annoncés en BGP par les 1412 AS. La première analyse nommée « cohérence des objets `route` » porte sur l'ensemble des objets `route`. Tout d'abord, l'intersection entre les deux ensembles permet de mettre en évidence les objets `route` qui ont un préfixe, ce sont les objets `route` utilisés. La différence entre l'ensemble des objets `route` et celui des préfixes annoncés représente les objets `route` pour lesquels aucun préfixe n'est annoncé, et correspond donc aux inutilisés. La seconde analyse, « filtrage via les objets `route` » concerne l'ensemble des préfixes annoncés. Ici, l'intersection des deux ensembles permet d'extraire les préfixes pour lesquels un objet `route` existe, donnant les préfixes couverts. Enfin, la différence entre l'ensemble des préfixes et les objets `route` donne les préfixes pour lesquels aucun objet `route` n'existe, il s'agit donc des préfixes non couverts.

À retenir

Il est conseillé de déclarer systématiquement un objet `route` pour chaque `inetnum` attribué par le RIR, et de déclarer un objet `route` par préfixe annoncé.

21. objet `route` pour IPv4 et objet `route6` pour IPv6

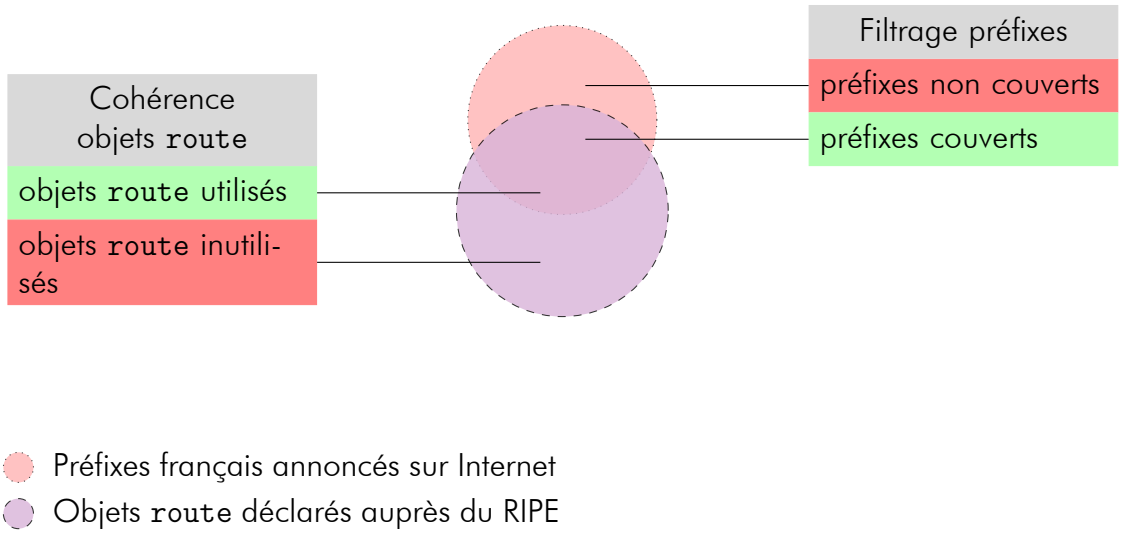

Figure 1.14 – Représentation des analyses sur les objets `route`

1.6.2 Cohérence des objets route

Méthodologie de mesure

Cette sous-partie de l'indicateur vise à mesurer les objets `route` et leur utilisateur au cours de l'année par les opérateurs les ayant déclaré.

Une base de données a été alimentée quotidiennement avec les dépôts du serveur `whois` du RIPE-NCC, et contient exclusivement les objets route déclarés par les 1412 AS français.

Les objets `route` extraits sont comparés avec les préfixes reçus pas les collecteurs du RIS choisis, à savoir Londres, Genève et Amsterdam.

L'analyse porte sur l'ensemble des objets `route` déclarés par les AS français, qui sont alors classés dans deux catégories :

- **utilisé** : l'objet `route` a un préfixe plus spécifique ou égal annoncé au cours de l'année ;
- **inutilisé** : l'objet `route` n'a aucun préfixe plus spécifique ou égal annoncé au cours de l'année.

Par ailleurs, concernant les objets `route`, les AS ont été classés en quatre catégories :

- **aucun objet route déclaré** : il n'existe aucun enregistrement de type objet `route` dans la base de données du RIPE-NCC ;
- **aucun objet route utilisé** : l'AS a réalisé au moins une déclaration d'objet `route`, mais aucun préfixe annoncé n'est inclus dans cet objet `route` ;

- **quelques objets route utilisés** : au moins un objet `route` n'a pas de préfixe annoncé qui lui corresponde ;
- **objets route totalement utilisés** : tous les objets `route` déclarés par l'AS au RIPE-NCC sont utilisés par un ou plusieurs préfixes sur Internet.

Ces classements sont réalisés pour l'ensemble des 1412 AS français recensés, et sur les AS français annonçant des préfixes sur Internet qui seront appelés « AS français actifs » dans l'analyse et l'interprétation des résultats.

Améliorations vis-à-vis du rapport 2012

Les calculs de l'indicateur utilisent désormais les annonces BGP extraites de 3 collecteurs du projet RIS.

Il était prévu ,dans le précédent rapport, de prendre en compte l'importance des objets route en fonction de la taille du sous-réseau associé. Après une série de tests, il s'avère que les résultats ne sont pas pertinents. Par conséquent, ils n'ont pas été intégrés à ce rapport.

Résultats et analyse

Les résultats varient de manière linéaire au cours de l'année 2013. Pour cette raison, seules les valeurs du 1er janvier 2013 et du 31 décembre 2013 sont représentées.

Pour IPv4, deux graphiques illustrent les catégories pour les AS français. La figure 1.15 représente l'utilisation des objets `route` pour l'ensemble des AS français. La figure 1.16, quant à elle, représente les mêmes résultats pour les AS français actifs au cours de l'année 2013.

Nous pouvons constater que deux tendances se dégagent à l'analyse des graphiques représentés. La première tendance, encourageante, montre que le nombre d'AS n'ayant aucun objet `route` déclaré diminue de 2 points pour l'ensemble des AS français. De plus, même si le nombre d'AS n'utilisant aucun objet `route` augmente d'un point pour l'ensemble des AS français, ce chiffre diminue pour les AS français actifs et ramène le pourcentage d'AS sans objet `route` à 5,4 %. Enfin, le pourcentage d'AS français actifs utilisant au moins un objet `route` croît de 2,9 points.

La seconde tendance, en revanche, montre que le nombre d'objets `route` inutilisés dans la base de données du RIPE augmente, pouvant expliquer la diminution de 2,1 points des AS français actifs utilisant tous leurs objets `route`.

L'évolution des déclarations d'objets `route` représentée dans le tableau 1.2 montre que le nombre de déclarations d'objets `route` croît significativement, augmentant de 324 objets `route`. De plus, 113 objets `route` inutilisés s'ajoutent au cours de l'année,

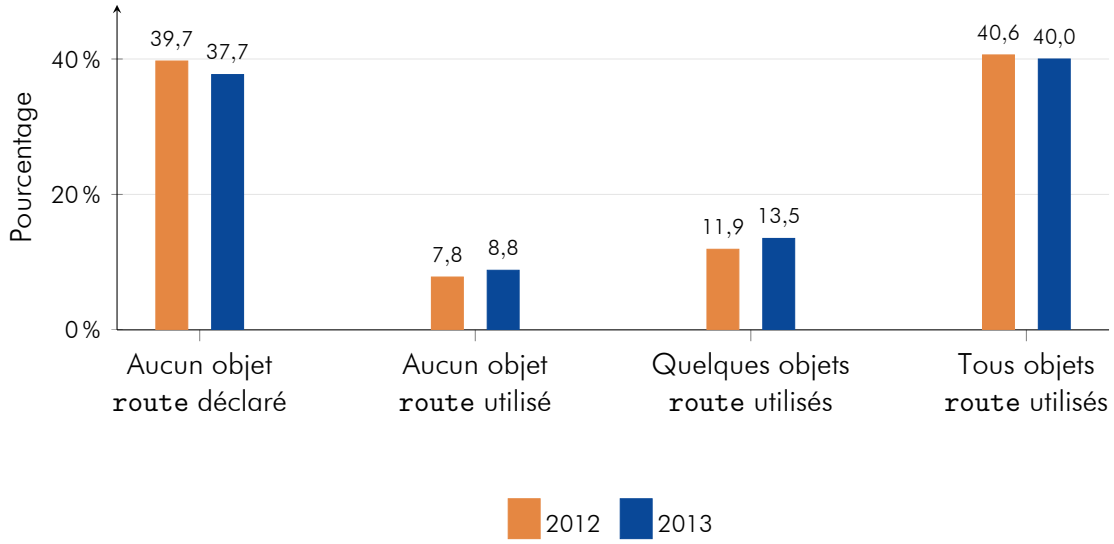

Figure 1.15 – Utilisation des objets `route` des AS français

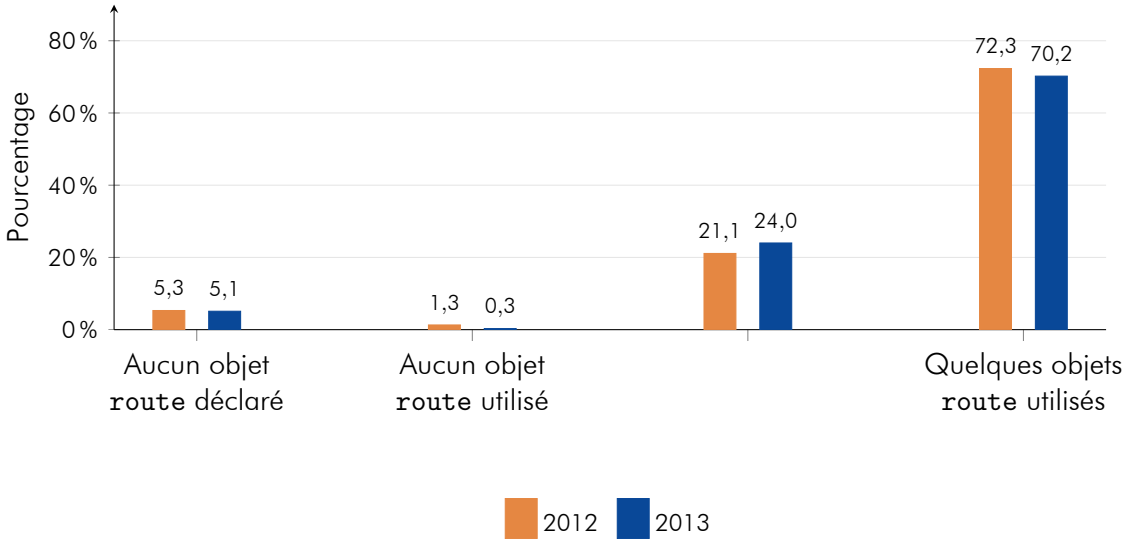

Figure 1.16 – Utilisation des objets `route` des 795 AS français actifs

augmentant de manière significative le reliquat d'objets `route` inutilisés. Néanmoins, le nombre de nouveaux objets `route` utilisés reste plus important que le nombre d'objets `route` inutilisés.

Pour IPv6, la figure 1.17 pourrait laisser penser que les AS français respectent mieux les bonnes pratiques de déclaration d'objet `route6`. En effet, une baisse de 3,8 points des AS français n'ayant aucun objet `route6` déclaré, ainsi qu'une augmentation de 2,1 points du nombre d'AS français utilisant l'ensemble des objets `route6` déclarés tendent à conforter cette intuition.

Objets route	Inutilisés	Utilisés
1er janvier 2013	1177	2914
31 décembre 2013	1290	3240

Table 1.2 – Évolution des déclarations d'objets route en 2013

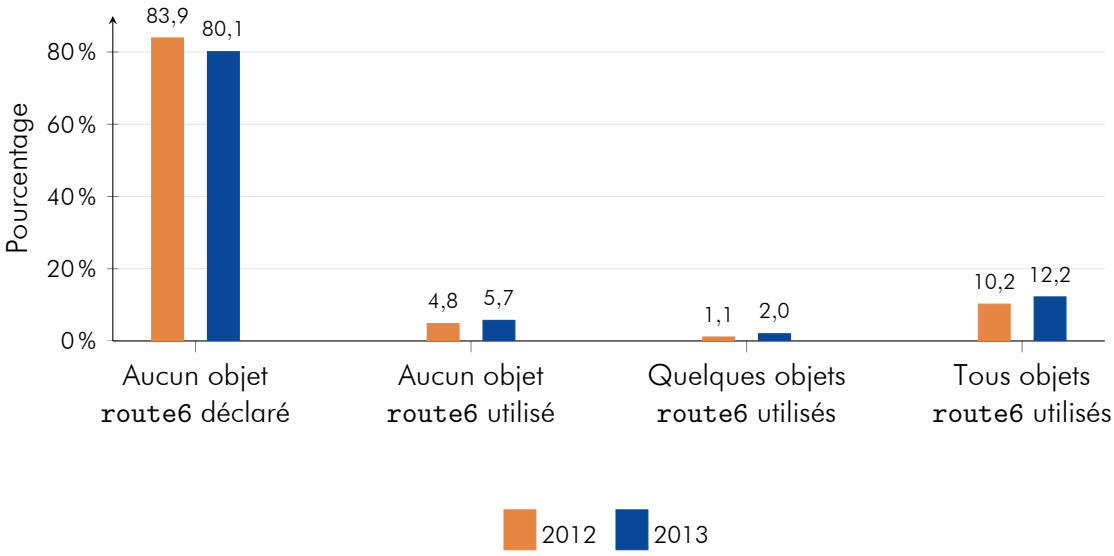

Figure 1.17 – Utilisation des objets route6 des AS français

Objets route6	Inutilisés	Utilisés
1er janvier 2013	96	216
31 décembre 2013	143	285

Table 1.3 – Évolution des déclarations d'objets route6 en 2013

L'analyse des AS français actifs en IPv6 présentés dans la figure 1.18, montre cependant que la réalité est toute autre. Entre 2012 et 2013, le nombre d'AS français actifs en IPv6 est passé de 178 à 240. Cette croissance d'AS français utilisant le protocole IPv6 n'a pas été accompagnée d'une déclaration systématique d'objets route6. La quantité d'AS français actifs n'ayant aucun objet route6 a augmenté de 3,2 points.

Dans le tableau 1.3, il apparaît que le nombre d'objets route6 inutilisés passe de 96 à 143. Cette importante augmentation montre que IPv6 ne bénéficie pas du même traitement que IPv4, car même si les objets route6 utilisés augmentent, près de la moitié des objets route6 créés au cours de l'année demeurent inutilisés. Néanmoins,

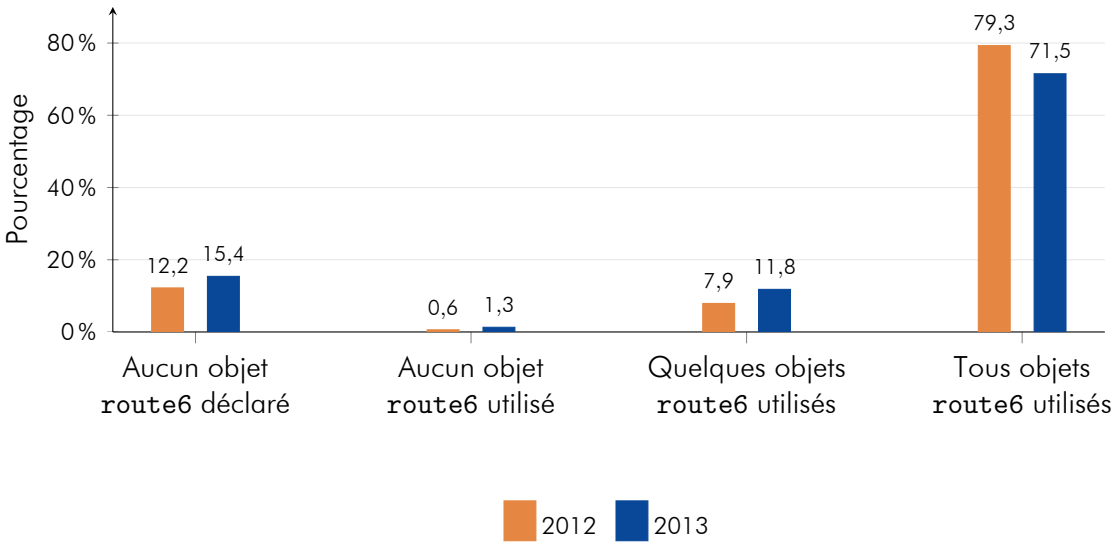

Figure 1.18 – Utilisation des objets `route6` des 240 AS français actifs

il est probable qu'une grande partie des objets `route6` ont été créés pour des annonces futures. L'analyse de l'année 2014 permettra de confirmer cette supposition.

À retenir

Les objets `route` et objets `route6` doivent faire l'objet d'une suppression systématique dès qu'un `inetnum` est rendu à son RIR et plus utilisé, ou que l'AS stoppe son activité. Dans le cas d'un rachat d'entreprise, les changements de politique de routage, peuvent impliquer des modifications d'objets `route`

1.6.3 Filtrage via les objets route

Méthodologie de mesure

Le but de cette sous-partie de l'indicateur est d'observer les préfixes annoncés et leur couverture par des objets `route`, afin de mieux appréhender le routage de l'Internet en France dans le cas d'un filtrage important de la part des opérateurs de transit. Pour cette partie, la base de données contenant les objets `route` déclarés au cours de l'année 2013 est utilisée. Chaque jour, chaque préfixe reçu par les collecteurs du RIS, ainsi que le numéro d'AS à l'origine de cette dernière sont stockés et comparés avec la base de données des objets `route` afin de rechercher une correspondance. Les 1412 AS entrent alors dans l'une des deux catégories suivantes :

- **correspondance :** tous les préfixes annoncés par l'AS sont couverts par un objet `route` ;
- **objet route manquant :** l'AS annonce au moins un préfixe pour lequel aucun objet `route` n'existe.

De plus, une recherche de conflit d'annonce est faite : si un AS annonce un préfixe pour lequel l'AS n'a pas d'objet `route` mais qu'un objet `route` existe pour un autre AS, il est marqué comme AS en conflit.

Améliorations vis-à-vis du rapport 2012

Comme pour les autres indicateurs, les calculs utilisent les annonces BGP extraites des serveurs RIS de Genève, Londres et Amsterdam, donnant une meilleure précision sur les correspondances avec les préfixes.

Afin de donner une meilleure perception sur le nombre d'hôtes concernés par une absence de filtrage, les calculs ont été réalisés sur le nombre de préfixes et d'adresses IP couvertes par des objets `route`.

Résultats et analyse

Le nombre de préfixes annoncés au cours de l'année n'a cessé de croître. Les nouveaux préfixes proviennent en grande majorité des 66 nouveaux AS apparus au cours de l'année. Quelques désagrégations [22] ponctuelles ont eu lieu, mais une grande partie de ces dernières ayant duré moins d'une journée, elles ne sont pas traitées dans cette analyse. L'évolution des résultats est linéaire au cours de l'année. Les résultats présentés se concentrent donc sur les valeurs au 1er janvier 2013 et 31 décembre 2013.

Pour l'évolution des AS en IPv4, le tableau 1.4 montre une diminution de 7 AS dans les AS actifs pour lesquels au moins un préfixe annoncé n'a pas d'objet `route` le couvrant. Cette diminution se fait au profit du nombre d'AS ayant l'ensemble de leurs préfixes couverts, passant de 611 à 684 en fin d'année. Ce chiffre est particulièrement encourageant car il confirme le fait que des opérateurs ont appliqué les bonnes pratiques concernant les déclarations auprès de l'IRR.

Pour IPv6, les résultats présentés dans le tableau 1.5 montrent un plus faible respect des bonnes pratiques. En effet, 62 nouveaux AS annoncent des préfixes en IPv6, mais seulement 45 de ces AS s'ajoutent à la catégorie des AS ayant une parfaite correspondance. Quant aux 17 autres AS, ils s'unissent aux AS dont au moins un préfixe n'a pas d'objet `route6`. La différence de comportement des AS entre IPv4 et IPv6 pourrait provenir du fait que certains opérateurs de transit ne filtrent que les objets `route` et pas les objets `route6`. De ce fait, les opérateurs clients n'ont pas d'incident de production les enjoignant à faire les déclarations associées.

22. Division d'un préfixe en plusieurs préfixes de plus petite taille

Type	1er janvier 2013	31 décembre 2013
Nombre d'AS actifs	769	835
Correspondance	611	684
Objet `route` manquant	158	151

Table 1.4 – Évolution des AS en IPv4

Type	1er janvier 2013	31 décembre 2013
Nombre d'AS actifs	178	240
Correspondance	145	190
Objet `route6` manquant	33	50

Table 1.5 – Évolution des AS en IPv6

Type	1er janvier 2013	31 décembre 2013
Préfixes couverts	4837	5113
Préfixes non couverts	1145	1050

Table 1.6 – Évolution des préfixes en IPv4

En début d'année, 109 AS avaient au moins un préfixe annoncé pour lequel un objet `route` ou un objet `route6` existait sous l'égide d'un autre AS. Il s'agit, majoritairement, de clients dudit AS. Une partie des opérateurs concernés ont corrigé ces défauts de déclaration. Au 31 décembre 2013, 90 AS étaient marqués avec des préfixes en conflit avec des objet `route` ou objets `route6`.

L'évolution des préfixes IPv4 annoncés par les AS observés a crû au même rythme que l'apparition des nouveaux AS au cours de l'année 2013. L'analyse s'est focalisée ici sur chaque préfixe sans tenir compte de l'AS d'origine, afin de mesurer les préfixes en tant qu'ensemble. Le tableau 1.6 montre les résultats au 1er janvier et au 31 décembre 2013 ; 95 préfixes non couverts au début de l'année ont rejoint la catégorie des préfixes couverts, participant à l'augmentation de 276 préfixes pour cette catégorie.

Pour IPv6, même si 105 nouveaux préfixes ont été ajoutés à la catégorie des préfixes couverts, 29 sont apparus dans les préfixes non couverts. Ces chiffres semblent appuyer le fait que l'application des bonnes pratiques est moins systématique qu'en IPv4.

Les préfixes en conflit étaient au nombre de 1189 en début d'année ; 45 de ces préfixes

Type	1er janvier 2013	31 décembre 2013
Préfixes couverts	304	409
Préfixes non couverts	79	108

Table 1.7 – Évolution des préfixes en IPv6

Type	1er janvier 2013	31 décembre 2013
IP couvertes	96,4 %	97,4 %
IP non couvertes	3,6 %	2,6 %

Table 1.8 – Évolution des IP en IPv4

ont fait l'objet de déclarations auprès de l'IRR. Les opérateurs continuent d'améliorer la situation concernant les déclarations d'objets `route`.

L'analyse de l'évolution de la couverture des adresses IP porte sur les adresses IP traitées de manière unique. Représentés dans le tableau 1.8, les résultats changent radicalement et tendent à confirmer que la couverture des adresses IP par des objets `route` pour IPv4 a un impact bien plus important. En effet, au 1er janvier 2013, 96,4 % des adresses IP annoncées par les 1412 AS sont couvertes par des objets route. De plus, le pourcentage du nombre d'adresses IP couvertes au 31 décembre augmente de 1 point, atteignant 97,4 % de l'ensemble des adresses IP. Un filtrage strict sur la base des objets `route` rendrait indisponible seulement 2,6 % des adresses IP annoncées par les 1412 AS. Dans le cas d'un filtrage systématique par les opérateurs de transit, une faible quantité d'hôtes serait injoignable.
Les résultats ne sont pas représentés pour IPv6 car ils ne sont pas pertinents. En effet, le taux d'occupation des préfices IPv6 est, par nature, extrêmement faible.

À retenir

Les bonnes pratiques de déclaration auprès de l'IRR doivent être mises en œuvre pour IPv4 comme pour IPv6.

1.7 Déclarations dans la RPKI

1.7.1 Description

En introduisant un moyen de vérifier la légitimité d'une annonce de préfixe, la RPKI, présentée en section 1.2, constitue une première étape vers la sécurisation du routage à l'échelle de l'Internet. L'objectif de cet indicateur est de mesurer l'adoption de la RPKI par les AS français.

1.7.2 Méthodologie de mesure

Afin de mesurer l'évolution des déclarations dans la RPKI par les AS français, les données du dépôt maintenu par le RIPE-NCC [34] sont récupérées quotidiennement. Pour chaque mois depuis janvier 2013, nous considérons les métriques suivantes :

- **le nombre d'AS français participant à la RPKI**, c'est-à-dire le nombre d'AS ayant publié au moins un `ROA` ;
- **le nombre de préfixes IPv4 et IPv6 déclarés par ces AS**, c'est-à-dire le nombre de préfixes déclarés dans les `ROA` publiés ;
- **les pourcentages d'annonces valides, invalides ou non couvertes au regard de la RPKI**. Ces métriques permettent notamment d'estimer l'adéquation des déclarations des AS français dans la RPKI, ainsi que la couverture des annonces.

Limitations

Les mesures effectuées sur le dépôt du RIPE-NCC ne permettent pas de mesurer l'utilisation de la RPKI à des fins de filtrage, ou, plus généralement, d'analyse des annonces de préfixes effectuées. En effet, la publication de `ROA` par un AS n'implique pas nécessairement que celui-ci utilise la RPKI pour le filtrage des annonces de préfixes. Les métriques présentées précédemment ne reflètent donc pas l'utilisation réelle de la RPKI par les AS français.

Dans la prochaine édition du rapport, nous souhaitons faire évoluer cet indicateur afin de réaliser une étude comparable à celle sur les objets `route`, avec les indicateurs « cohérence » et « filtrage ».

1.7.3 Résultats et analyse

Le nombre d'AS français participant à la RPKI a quasiment triplé au cours de l'année 2013 : au 31 décembre 2013, 110 AS avaient publié un `ROA` dans la RPKI, tandis qu'ils n'étaient que 41 au 1er janvier 2013.

La figure 1.19 montre l'évolution du nombre de préfixes IPv4 et IPv6 déclarés par les AS français dans la RPKI. On peut constater que le nombre de préfixes IPv4 a augmenté significativement au cours de l'année, tandis que l'augmentation du nombre de préfixes

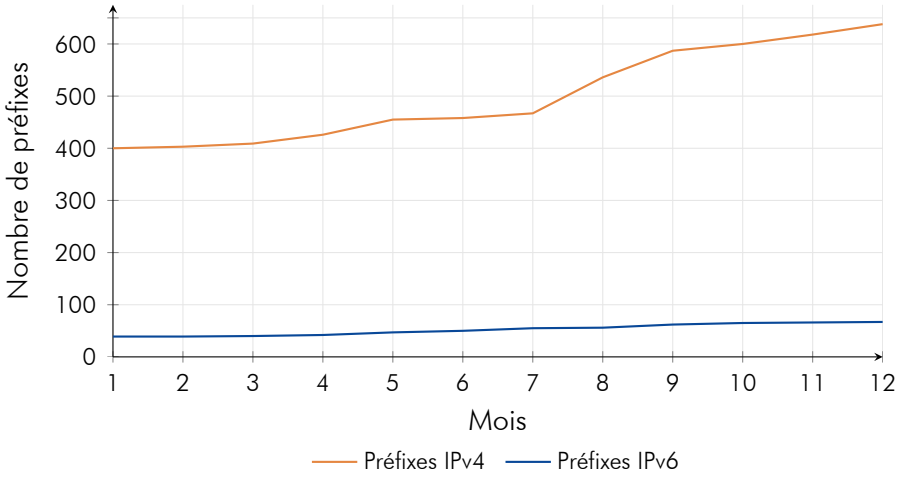

Figure 1.19 – Évolution du nombre de préfixes déclarés par les AS français

IPv6 a été plus faible. L'augmentation observée en IPv4 et en IPv6 n'est pas uniquement due à l'arrivée progressive de nouveaux AS : la mise à jour de ROA par les AS déjà présents dans la RPKI participe à cette augmentation.

La figure 1.20 illustre l'évolution de la validité des annonces des AS français par rapport à la RPKI. On peut constater que le pourcentage d'annonces non couvertes a diminué sensiblement : d'environ 90 % au début de l'année 2013, il est passé à moins de 80 % à la fin de l'année. Cette baisse ne s'est pas directement traduite par une augmentation du même ordre de grandeur du pourcentage d'annonces valides : celui-ci est passé de 8 % au début de l'année à 12 % au 31 décembre 2013. Le pourcentage d'annonces invalides a, quant à lui, augmenté significativement au cours de l'année : de 2 % au 1er janvier 2013, il est passé à presque 9 % à la fin de l'année.

On observe notamment une brusque augmentation de ce pourcentage d'avril à mai 2013. En parallèle, le pourcentage d'annonces non couvertes a diminué significativement sur la même période. Cette évolution provient de l'arrivée d'un nouvel AS dans la RPKI. Cet événement a eu principalement deux conséquences. Tout d'abord, un grand nombre d'annonces effectuées par d'autres AS dépendant administrativement de ce nouvel arrivant sont devenues invalides. Par ailleurs, certaines annonces effectuées par cet AS sont elles aussi devenues invalides, étant trop spécifiques par rapport à la longueur maximale autorisée par le ROA. Au 31 décembre 2013, ces observations étaient toujours d'actualité.

Notre analyse nous a permis de constater que les données publiées dans la RPKI ne correspondent pas toujours aux annonces effectuées. Pour commencer, près de la moitié des AS participant à la RPKI ne déclarent pas la totalité de leurs préfixes IP dans la RPKI. Au 31 décembre 2013, le pourcentage d'AS participant à la RPKI pour lesquels chaque annonce était couverte par un ROA était de 55 %. Par ailleurs, à la même date,

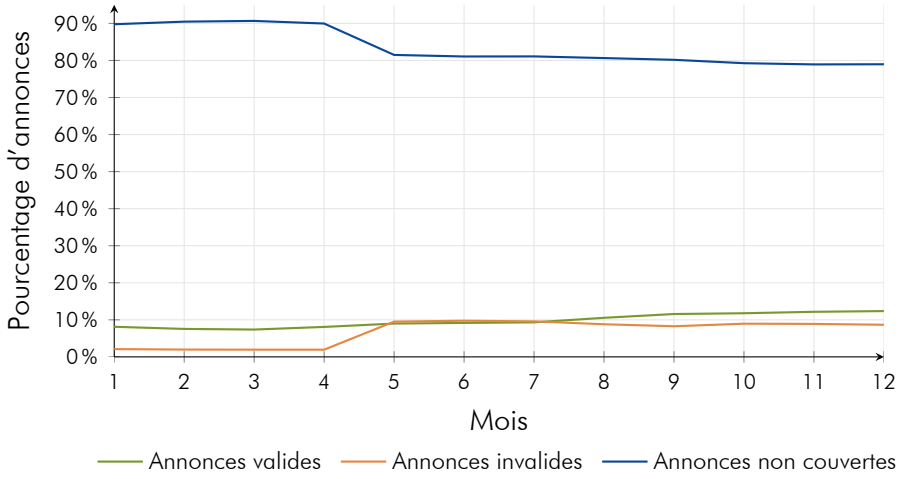

Figure 1.20 – Évolution de la validité des annonces des AS français selon la RPKI

6 AS français participant à la RPKI effectuaient au moins une annonce invalide, car trop spécifique.

Nos observations montrent qu'un filtrage strict, c'est-à-dire n'acceptant que les annonces considérées comme valides, entraînerait le rejet de près de 90 % des annonces. En revanche, on peut remarquer qu'un filtrage consistant à rejeter uniquement les annonces invalides aurait un impact bien moindre, et entraînerait le rejet de 9 % des annonces à la fin de l'année. Par ailleurs, bien que les données fournies par la RPKI soient incomplètes, nos observations montrent également une nette augmentation de son utilisation. Enfin, l'étude menée sur les usurpations (voir section 1.5) montre que la RPKI permet de statuer sur des annonces non couvertes par des objets `route`, indiquant une certaine complémentarité avec les informations fournies par les objets `route`. Ce constat peut inciter certaines structures à combiner les deux sources d'information afin d'effectuer du filtrage sur les annonces de préfixes [35].

À retenir

Afin de faciliter le filtrage, il est nécessaire de déclarer les préfixes annoncés en BGP au sein de la RPKI.

1.8 Conclusion et perspectives

Cette nouvelle édition du rapport exploite plus de sources de données que les années précédentes. Les collecteurs BGP situés à Amsterdam et Genève sont utilisés en plus de celui de Londres. Cela permet d'obtenir une meilleure vision de l'Internet en France et d'obtenir des résultats plus précis pour chacun des indicateurs présentés. Un travail important a été effectué afin d'optimiser les outils de l'observatoire pour qu'ils puissent traiter un volume de données conséquent sans perte de performance. Par ailleurs, dans un souci d'amélioration constante des indicateurs techniques, les méthodologies associées ont été reprises pour prendre en compte les limitations décrites dans les rapports précédents.

En ce qui concerne la connectivité des AS français, la méthodologie utilisée permet désormais d'identifier les liens de *peering* et de mieux caractériser les effets de la disparition d'un AS. Fin 2013, nous avons identifié 84 pivots dont 21 étrangers. Il existe relativement peu d'AS dont la disparition aurait un impact significatif. Aucun des AS français ayant plus d'un seul fournisseur ne serait déconnecté de l'Internet par la défaillance d'un des AS pivots que nous avons identifié.

Nous avons constaté des tendances intéressantes lors de l'étude des objets `route`. Le nombre d'AS sans objets `route` déclarés a baissé en 2013. Cependant, les objets `route` inutilisés ont augmenté s'ajoutant aux objets `route` obsolètes. Il convient donc de rappeler qu'il faut vérifier régulièrement que les informations déclarées auprès du RIPE sont encore valables. En ce qui concerne IPv6, les objets `route` sont moins bien déclarés qu'en IPv4. Cela semble donc indiquer qu'un moindre soin est apporté à la gestion des ressources IPv6. Finalement, les AS créés au cours de l'année 2013 ont tendance à bien appliquer les bonnes pratiques de déclaration. Il s'agit d'un résultat très encourageant pour les travaux de l'observatoire.

Concernant les usurpations de préfixes, une nouvelle catégorie a permis de valider les suppositions émises lors du dernier rapport. Il est ainsi possible de corréler des annonces en conflits en se basant sur les informations des AS incriminés. Ainsi, près de 35 % des événements détectés en 2013 correspondent à des AS appartenant à la même organisation ou aux mêmes gestionnaires et pour lesquels des objets `route` ne sont pas correctement déclarés. La nouvelle méthodologie a par ailleurs mis en évidence des phénomènes de réannonces de routes suite à des erreurs de configuration chez certains opérateurs. L'analyse manuelle des 34 événements anormaux identifiés a révélé que 10 d'entre eux sont très probablement des usurpations de préfixes. L'une d'elles correspond d'ailleurs aux détournements de trafic discutés publiquement fin 2013 [33].

Pour ce qui est de la RPKI, nous avons constaté une nette augmentation du nombre de déclarations au cours de l'année 2013 : de 40 au début de l'année, le nombre d'AS participants est passé à 110 au 31 décembre 2013. Bien que nos mesures ne nous permettent pas d'étudier l'utilisation réelle de la RPKI, nous observons que 90 %

des annonces de préfixes seraient rejetées en cas de filtrage strict. Ce constat semble donc indiquer que la RPKI est plus utilisée à des fins de détection plutôt que de filtrage. Cependant, pour ce qui est du filtrage, la RPKI pourrait, dans certains cas, être utilisée pour rejeter les annonces invalides. Un point d'échange français a d'ailleurs commencé à utiliser la RPKI pour filtrer les préfixes annoncés par ses clients.

Ce rapport a vu disparaitre l'indicateur cherchant à mesurer l'adoption d'IPv6 et des bonnes pratiques d'utilisation de BGP. En effet, les résultats étaient peu pertinents. Un travail de refonte de cet indicateur est actuellement en cours pour en améliorer la qualité. Nous pensons pouvoir identifier des comportements intéressants en séparant les AS transitaires des AS clients. Il semble ainsi possible d'identifier quels transitaires mettent en place du filtrage via les objets `route` en étudiant finement le nombre de préfixes qui sont mal déclarés.

L'amélioration des outils va également se poursuivre afin de pouvoir utiliser les données issues de tous les colleteurs du RIS. À court terme, l'observatoire souhaite pouvoir appliquer les indicateurs concernant le protocole BGP à l'échelle de l'Europe.

Chapitre 2

Résilience sous l'angle du protocole DNS

2.1 Introduction

Le système de noms de domaine, géré par le protocole DNS [36, 37], est un système de nommage réparti et hiérarchique dont les deux objectifs essentiels sont d'associer à une adresse IP un nom lisible par les utilisateurs et de fournir de la stabilité aux identificateurs. Ainsi, l'adresse IP `2001:67c:2218:2::4:20` correspond au nom de domaine `www.afnic.fr` . Dans le cas d'un changement d'hébergeur, seul le responsable du domaine doit modifier l'adresse IP pointée par le nom. Grâce au DNS, ce changement est transparent pour les utilisateurs.

La structure du DNS est illustrée dans la figure 2.1. Au sommet de la hiérarchie se trouve la racine représentée par un point « . ». Il s'agit du point final que l'on retrouve au niveau des noms de domaines comme `www.afnic.fr.` .

À chaque niveau de la hiérarchie se trouve un ou plusieurs nœuds de l'arbre DNS. L'arborescence issue d'un nœud donné est appelée domaine. Elle peut avoir à son tour des sous-domaines, et ainsi de suite. Ce rapport ne tient pas compte de la différence subtile entre domaine et zone. Par conséquent, ces deux termes seront désormais employés comme synonymes.

Une zone est dite déléguée lorsque sa gestion est assurée par un organisme différent

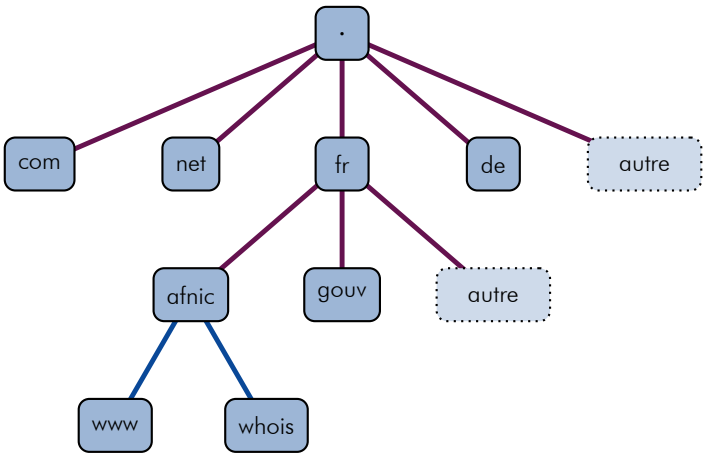

Figure 2.1 – Structure du DNS

de celui qui administre la zone parente. Le responsable d'une zone dont il reçoit la délégation peut alors gérer ses ressources indépendamment de sa zone parente. À titre d'exemple, la zone `.fr` a été déléguée à l'Afnic qui fixe les règles d'attribution des noms de domaines sous `.fr` indépendamment de sa zone parente, la racine gérée par l'ICANN [1]. Les délégations sont illustrées en violet dans la figure 2.1.

Pour chaque zone DNS, un ensemble de serveurs DNS décrit les ressources qu'elle contient, ainsi que les éventuelles délégations vers certains sous-domaines. De tels serveurs sont appelés serveurs DNS faisant autorité sur une zone. Les ressources attachées à une zone sont décrites par des enregistrements DNS. Chaque enregistrement DNS est défini par un nom de domaine, un type, la durée souhaitée de mise en cache, et des données qui dépendent du type de l'enregistrement. L'ensemble des enregistrements de même classe, même type et se rapportant au même nom de domaine s'appelle un `RRSet`. Par exemple, toutes les adresses IPv4 associées à un même nom de domaine font parties du même `RRSet`.

La résolution DNS est le mécanisme qui permet de récupérer un enregistrement, généralement une adresse IP, associée à un nom de domaine. Elle fait intervenir deux types de serveurs DNS, comme l'illustre la figure 2.2, qui met en évidence des interactions numérotées :

- **un serveur récursif** (également appelé serveur cache ou résolveur). C'est un serveur que la machine de l'utilisateur connaît et à qui elle soumet sa requête DNS [2] (interaction 1). Ce serveur va alors interroger le DNS en partant de la racine (interaction 2) et en suivant de proche en proche les points de délégation [3] jusqu'aux serveurs faisant autorité pour le nom de domaine objet de la requête (interactions 3-4). Enfin, le serveur récursif répond à la machine de l'utilisateur (interaction 5) et garde en même temps en mémoire (fonction de cache) les informations reçues, afin de les distribuer plus vite la fois suivante ;
- **des serveurs faisant autorité** pour des zones données, qui répondent au serveur récursif. Soit ils font effectivement autorité pour le nom de domaine demandé par la machine utilisateur, et ils lui retournent la réponse ; soit ils l'aiguillent vers d'autres serveurs à interroger qui seraient plus susceptibles de faire autorité sur le nom de de domaine recherché.

2.1.1 Les vulnérabilités du DNS

Le protocole DNS a été conçu il y a maintenant plus de 30 ans, dans un environnement complètement différent de ce qu'est l'Internet aujourd'hui et sans tenir compte de problèmes de sécurité qui pourraient survenir. Le niveau de la menace était alors moindre, et les moyens techniques étaient plus limités.

1. Internet Corporation for Assigned Names and Numbers.
2. Dans cet exemple de requête DNS, `IN A` signifie qu'on cherche le type d'adresse IPv4 dans la classe `IN` (Internet).
3. La réponse `NS` indique une liste de serveurs de noms (*Name Server*).

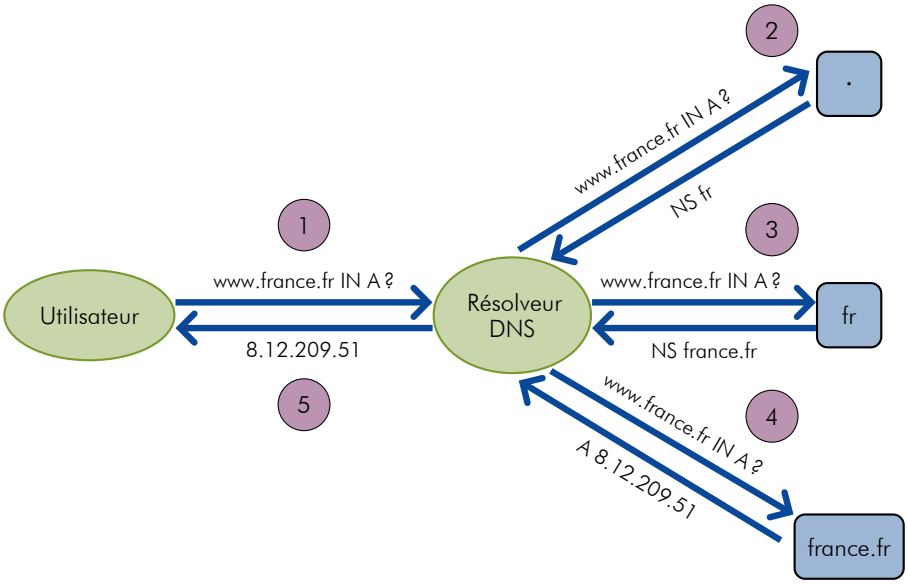

Figure 2.2 – Résolution DNS

Depuis déjà deux décennies, les serveurs cache font l'objet d'attaques par pollution de cache visant à y introduire des données erronées. Lorsqu'elles réussissent, ces attaques touchent tous les utilisateurs du serveur DNS cache ciblé. Les attaquants peuvent alors les diriger, par exemple, vers des sites web de filoutage [4].

Ces attaques sont possibles car un résolveur DNS ne dispose que de très peu d'éléments pour vérifier que la réponse reçue correspond bien à la requête qu'il a envoyée. En pratique, le quadruplet suivant est utilisé :

- l'adresse IP source de la réponse ;
- l'adresse IP de destination de la réponse ;
- un identifiant de 16 bits, le *Query ID*, envoyé dans la requête et recopié dans la réponse ;
- le contenu de la section *Question* du message DNS, lui aussi recopié dans la réponse.

Malheureusement ces données sont insuffisantes pour se protéger contre un empoisonnement de cache. En effet, il suffit que l'attaquant envoie une réponse comportant le bon quadruplet avant celle du serveur DNS légitime pour qu'elle soit prise en compte par le résolveur.

Lorsque l'attaquant se trouve entre le résolveur et le serveur faisant autorité dont il usurpe l'adresse IP, l'attaque est triviale. Il lui suffit de recopier le quadruplet dans la réponse. À l'inverse, si l'attaquant ne peut pas capturer le quadruplet, il va chercher à répondre plus vite que le serveur légitime en bombardant le résolveur DNS de pa-

4. En anglais, *phishing*. C'est une technique utilisée pour obtenir les données confidentielles (comme des mots de passe ou des numéros de carte de crédit) de victimes puis s'en servir contre eux.

quets pour deviner le bon quadruplet. S'il réussit à répondre avant le serveur légitime interrogé, la réponse illégitime est alors injectée dans le cache du résolveur DNS.

Il est généralement difficile de deviner le quadruplet. Au cours de l'été 2008, Dan Kaminsky [38] a rendu cette attaque beaucoup plus efficace. Les serveurs vulnérables peuvent ainsi être empoisonnés en quelques minutes, à l'aide de programmes disponibles sur Internet. Une solution à court terme appelée SPR[5] a été proposée. Elle vise à prendre en compte le port source utilisé dans la requête en plus du quadruplet. Elle est aujourd'hui mise en œuvre dans la plupart des résolveurs DNS. Certains, comme `Unbound` ou `PowerDNS`, l'utilisaient déjà avant la découverte de Dan Kaminsky.

D'autres techniques [39, 40] de pollution de cache ont récemment été découvertes. Elles montrent le besoin d'une solution durable à la falsification des enregistrements DNS. Pour y répondre, le protocole DNSSEC fournit des signatures cryptographiques permettant une vérification forte de l'intégrité des données stockées dans le DNS.

Le protocole DNSSEC

DNSSEC a été conçu pour empêcher la modification des enregistrements DNS par un tiers. Pour cela, de nouveaux types d'enregistrement DNS ont été introduits et des extensions ont été faites au protocole. Les principaux RFC [41, 42, 43] définissant le protocole DNSSEC ont été publiés en 2005. Avec DNSSEC, chaque jeu d'enregistrements DNS possède une signature cryptographique afin d'assurer les deux propriétés suivantes :

- **l'authenticité de l'origine des données**, c'est-à-dire la possibilité de vérifier que les données proviennent bien des zones légitimes ;
- **l'intégrité des données**, c'est-à-dire la possibilité de vérifier que les données n'ont pas été modifiées entre le serveur faisant autorité et la machine effectuant la vérification de la signature.

Il est important de souligner que les serveurs DNS récursifs sont généralement les seuls éléments qui vérifient les signatures. Ils sont alors appelés serveurs DNS validants. Par conséquent, la sécurité des communications entre un tel serveur et ses clients n'est pas traitée par DNSSEC. De plus, il est important de noter que les signatures ne couvrent que les données et non pas l'ensemble du message DNS reçu avec son en-tête.

La racine du DNS utilise DNSSEC depuis juillet 2010. La zone `.fr` a, quant à elle, été signée dès septembre 2010. En avril 2011, elle a ensuite permis à ses zones déléguées d'utiliser DNSSEC.

Signatures électroniques : les enregistrements RRSIG

Les signatures électroniques reposent sur la cryptographie asymétrique. Une personne

5. Source Port Randomization.

souhaitant protéger des données en intégrité va générer une clé comportant une partie publique et une partie privée. La partie privée lui permet de signer les données, et ne doit pas être connue par d'autres personnes. La partie publique permet quant à elle de vérifier ces signatures. Elle est distribuée à toutes les personnes susceptibles d'effectuer des vérifications.

Dans le cadre de DNSSEC, le responsable d'une zone génère une clé afin d'émettre des signatures. Tous les `RRSet` sont signés un à un avec la clé privée de la zone. Les signatures sont directement publiées dans la zone dans des nouveaux enregistrements appelés `RRSIG`[6]. Le résolveur validant peut vérifier ces signatures à l'aide de la partie publique de la clé. La figure 2.3 en donne un exemple. Les champs remarquables sont :

- **le type de l'enregistrement signé** ;
- **les algorithmes** utilisés pour la signature, ici RSA-SHA256 ;
- **la date d'expiration de la signature** : instant UTC[7] où la signature ne peut plus être prise en compte pour la validation ;
- **le début de prise en compte de la signature** : instant UTC avant lequel la signature ne peut être prise en compte pour la validation.
- **la signature**.

```
host1.example.com.     AAAA 2001:db8:1000:3::9:12

host1.example.com.     RRSIG  AAAA 10 4 3600 20130616101137 (
                                    20130517060654 49703 example.com.
                                    mXS6b [..] xOg==)
```

Figure 2.3 – Exemple d'un enregistrement `AAAA` et sa signature `RRSIG`

Dans la plupart des implémentations de DNSSEC, le choix a été fait de signer les zones en avance de phase, puis de les charger dans les serveurs DNS faisant autorité. Deux raisons viennent justifier ce choix. D'une part, à l'époque où le protocole a commencé à être développé, peu de matériel était capable de signer à la volée le trafic DNS de serveurs importants dont le débit moyen variait entre 2000 et 6000 requêtes/seconde avec des pics pouvant atteindre 20 000 requêtes/seconde. D'autre part, signer les réponses à la volée signifie avoir accès à la partie privée de la clé en permanence ; ce qui implique une plus grande exposition de la clé à des risques de compromission.

Les signatures cryptographiques étant volumineuses, les enregistrements `RRSIG` ont un impact important sur la taille des messages DNS. Par conséquent, elle risque fort de dépasser la taille conventionnellement admise de 512 octets en transport UDP. L'extension `EDNS0` [44] permet de négocier l'échange de messages UDP de plus grande taille (généralement 4096 octets). Sa prise en charge est donc nécessaire au niveau de tous les serveurs DNS.

6. Resource Record digital SIGnature.
7. Temps Universel Coordonné.

Un résolveur compatible DNSSEC le signale avec le drapeau *DNSSEC Ok* (DO) [45]. Dès qu'un serveur faisant autorité reçoit une requête avec le drapeau DO levé, il doit inclure dans la réponse des enregistrements qui permettront d'authentifier les RRSet renvoyés si la zone correspondante est signée.

La machine d'un utilisateur interrogeant un serveur validant peut être informée que la réponse ait été validée ou non. Pour cela, il place le drapeau DO dans sa requête. Si les données de la réponse sont signées et vérifiées, le résolveur lèvera le drapeau *Authenticated Data* (AD) dans sa réponse. En plaçant le drapeau *Checking Disabled* (CD) dans sa requête, l'utilisateur peut également demander à recevoir une réponse quand bien même la signature est invalide.

L'infrastructure de clés : les enregistrements DNSKEY et DS

Chaque zone possède sa propre clé. La partie privée de la clé doit évidemment être particulièrement bien protégée et idéalement stockée hors-ligne. La partie publique est directement stockée et distribuée au sein de l'infrastructure DNS dans un nouvel enregistrement appelé DNSKEY dont un exemple est donné dans la figure 2.4. Cet enregistrement est publié au niveau de la zone, au même titre que ses autres ressources.

```
example.com.    DNSKEY  256 3 10 ( AwEAA [..] MtB9= ) ; key id = 57483
```

Figure 2.4 – Exemple d'un enregistrement DNSKEY

Afin de valider les signatures, un résolveur validant a besoin d'obtenir les clés publiques associées. Les concepteurs de DNSSEC ont ainsi tiré parti de la nature hiérarchique du DNS. Un résolveur validant peut ainsi établir une chaîne de confiance avec toutes les zones protégées par DNSSEC à l'aide de la clé publique signant la zone racine et en vérifiant les signatures de proche en proche.

L'enregistrement DNSKEY comporte plusieurs champs, parmi lesquels on peut citer :

- **Le drapeau** qui permet de différencier les deux types de clés possibles de DNSSEC. Dans le modèle de gestion de clés le plus communément utilisé, lorsque ce champ vaut 256, il s'agit d'une clé servant à signer la zone appelée ZSK [8]. Lorsqu'il vaut 257, cela désigne généralement une clé KSK [9] qui ne signe que les enregistrements DNSKEY. La distinction entre ces deux types de clés est délicate et n'est pas abordée dans cette introduction à DNSSEC ;
- **L'algorithme** qui spécifie l'algorithme utilisé pour générer la clé ;
- **La clé** est le dernier champ de l'enregistrement.

8. Zone Signing Key.
9. Key Signing Key.

La liste des algorithmes utilisables avec DNSSEC est maintenue par l'IANA dans le registre `DNSSEC algorithm numbers` [46]. Étant donné les algorithmes actuellement pris en charge par les différentes implémentations, il est recommandé d'utiliser RSA et SHA-256. Une grande partie des déploiements actuels utilise des clés RSA de 1024 bits pour les `ZSK`, et 2048 bits pour les `KSK`. Étant donné les attaques connues et les risques associés, le RGS [10] [47] préconise une taille de 2048 bits au minimum.

Un nouvel enregistrement a été introduit pour établir des délégations de zone sécurisées. Il s'agit de `DS` [11], dont un exemple est fourni dans la figure 2.5. Lorsqu'une zone, comme `example.com`, active DNSSEC et que sa zone parente, ici `.com`, est signée, ses administrateurs communiquent l'empreinte de la partie publique de sa clé `DNSKEY` à ceux de la zone parente via son bureau d'enregistrement. À partir de ces éléments, l'administrateur de la zone parente publie un enregistrement `DS` et le signe avec sa propre clé. Cet enregistrement `DS` signé permet d'indiquer que la `DNSKEY` peut être utilisée pour signer les enregistrements de la zone, ici `example.com`.

```
example.com.     NS  ns1.example.com.
example.com.     NS  ns2.example.com.
example.com.     DS 31589 8 1 3490A6806D47F17A34C29E2CE80E8A999FFBE4BE
```

Figure 2.5 – Enregistrement `DS` apparaissant dans la zone `.com`

Il est important de signaler ici que lorsqu'il y a délégation, les enregistrements `NS` qui établissent cette délégation ne sont pas signés au niveau de la zone parente, car ce n'est pas elle qui fait autorité pour ces enregistrements.

Lorsque la zone parente n'est pas signée, le système DLV [12] de l'ISC [13], mis en place en 2006, peut servir de registre pour la validation des clés publiques des zones signées. La clé publique de DLV est alors une ancre de confiance pour la validation DNSSEC. Le système DLV est un mécanisme transitoire qui ne doit pas être utilisé si la zone parente supporte DNSSEC.

Preuve de non-existence : les enregistrements NSEC et NSEC3

Dans le protocole DNS standard, lorsqu'une requête est reçue et qu'elle ne correspond à aucun nom de domaine existant, le serveur récursif à l'origine de cette requête reçoit un message DNS dont le statut `NXDOMAIN` indique que le domaine n'existe pas et le message ne contient pas de section `ANSWER`. De même, si le nom existe mais qu'aucune ressource du type demandé ne lui est associée, la réponse aura comme statut `NOERROR`

10. Référentiel général de sécurité.
11. Delegation Signer.
12. DNSSEC Look-aside Validation.
13. Internet Systems Consortium.

et là encore, il n'y aura pas de section ANSWER.

Pour prouver la non-existence d'un enregistrement, les concepteurs du protocole DNSSEC ont introduit l'enregistrement NXT [48], qui a ensuite été modifié puis renommé en enregistrement NSEC [14] [49]. Il repose sur un principe simple : prouver qu'aucun nom ne se trouve entre deux autres noms de domaine.

L'inconvénient majeur de l'enregistrement NSEC est qu'il permet de parcourir une zone entière et de découvrir l'ensemble des noms de la zone. Par ailleurs, il engendre une contrainte importante pour les zones contenant de nombreuses délégations. En effet, le coût engendré par l'insertion d'un enregistrement NSEC et sa signature pour chaque nom de la zone est prohibitif.

Du fait de ces inconvénients, l'enregistrement NSEC3 [15] a été proposé [50]. Un exemple est donné dans la figure 2.6. Il permet de résoudre le second inconvénient de NSEC à l'aide de l'option Opt-out. Si elle est activée au niveau d'une zone, elle conduira à l'insertion d'enregistrements NSEC3 et RRSIG associés uniquement aux zones déléguées signées par leur gestionnaire. Les délégations non sécurisées seront alors considérées comme inexistantes vis-à-vis de la validation DNSSEC.

```
15bg9l6359f5ch23e34ddua6n1rihl9h.example.com. (
      NSEC3 1 0 2 ANSSI A6EDKB6V8VL5OL8JNQQLT74QMJ7HEB84
                    NS SOA MX RRSIG DNSKEY NSEC3PARAM )
```

Figure 2.6 – Enregistrement NSEC3 pour le nom example.com.

De plus, afin de rendre plus difficile le parcours d'une zone signée, NSEC3 remplace les deux noms de domaine apparaissant dans un enregistrement NSEC par leurs empreintes cryptographiques obtenues en appliquant, une ou plusieurs fois, une fonction de hachage sur ces noms en combinaison avec un sel.

Considérations opérationnelles

La mise en œuvre de DNSSEC implique des mesures nouvelles pour les administrateurs DNS et nécessite de le faire de manière soignée afin de ne pas invalider des données par des erreurs de manipulation. Ainsi, le processus de base pour gérer une zone suit les étapes suivantes :

1. édition de la zone et insertion des clés DNSKEY ;
2. signature des RRSet de la zone ;
3. publication de la zone.

14. Next SECure.
15. Next SECure version 3.

Par rapport à l'administration classique d'un serveur DNS, des nouvelles étapes ont été introduites, notamment :

- la génération des clés et la sauvegarde de leur partie privée ;
- la signature des zones qui doit se faire périodiquement, même si son contenu n'a pas changé, du fait de l'expiration des signatures ;
- le remplacement programmé de clés (appelé roulement de clés) ou en cas d'urgence lorsqu'une clé a été compromise.

Les bonnes pratiques associées au déploiement de DNSSEC sont disponibles en ligne dans de nombreux documents [51, 52].

2.1.2 Plateforme, outils et données utilisés

Afin d'appréhender la résilience sous l'angle du DNS, nous utilisons `DNSwitness` [53], plateforme générique développée par l'Afnic permettant de réaliser des mesures via le DNS. Cette plateforme est multi-usage et capable de prendre en compte divers types de métriques. Les données brutes sont stockées dans une base de données afin d'étudier leur évolution dans le temps. Elle est conçue pour être distribuée librement et pour un usage flexible et adaptable au besoin.

DNSdelve

`DNSdelve` permet d'effectuer des mesures actives. Il prend en entrée une liste de zones (toutes les zones déléguées sous `.fr` par exemple), effectue des requêtes DNS sur les zones en question, puis stocke les résultats extraits des réponses à ces requêtes dans une base de données.

`DNSdelve` comporte plusieurs modules spécialisés utilisables de manière indépendante. Pour les besoins de l'observatoire, deux modules ont été utilisés.
Le module `IP` effectue des requêtes DNS portant sur les adresses (IPv4 et IPv6) de certains types d'enregistrement des zones déléguées sous `.fr` tels que les serveurs de noms, les relais de messagerie et les serveurs web. Outre les adresses IP, il peut également stocker des informations concernant le numéro d'AS ainsi que le pays. Ce module fournit les données utilisées pour les indicateurs de dispersion des serveurs DNS faisant autorité et de taux de pénétration du protocole IPv6.
Le deuxième module est employé pour mesurer le taux de pénétration du protocole DNSSEC des zones déléguées sous `.fr`.

DNSmezzo

`DNSmezzo` se présente sous la forme d'une sonde placée sur le réseau local du serveur de noms cible, et permet d'effectuer des mesures passives. `DNSmezzo` capture et analyse les requêtes reçues par le serveur et permet la sauvegarde des résultats dans une base de données.

Actuellement, les serveurs de noms de la zone `.fr` se répartissent en serveurs directement administrés par l'Afnic et en serveurs administrés par quatre partenaires dont trois sont des fournisseurs de solutions *anycast*.

Déployé par l'Afnic, `DNSmezzo` nous permet d'alimenter les indicateurs relatifs à la progression d'IPv6 et aux résolveurs les plus demandeurs.

Données utilisées

Toutes les mesures actives ont été faites en utilisant la zone `.fr` qui varie au gré des créations, suppressions et modifications de zones déléguées. De 2012 à 2013, le nombre de ces zones déléguées a augmenté de 7,6 % (contre 14 % entre 2011 à 2012) pour atteindre le nombre de 2 716 055 au 31 décembre 2013. Ce nombre était de 2 509 913 au 31 décembre 2012.

Les mesures actives sont effectuées de manière hebdomadaire pour chacun des modules de `DNSdelve`. Ce dernier calcule, à chaque lancement, un échantillon aléatoire représentant 10 % de la copie du jour de la zone `.fr`, soit plus de 250 000 zones déléguées. Nous avons choisi ce taux d'échantillonnage afin de rester dans des temps de calcul raisonnables : de l'ordre de cinq heures pour les modules les plus lourds sur la plateforme matérielle en exploitation en 2013.

Les chiffres présentés dans ce rapport pour la partie active de la plateforme proviennent des mesures faites tout au long de 2012 et 2013 ainsi que de campagnes ponctuelles en 2011. Les données de 2010 ont été exploitées lorsqu'elles étaient disponibles.

Les données de `DNSmezzo` proviennent, quant à elles, de sondes installées au niveau de certaines instances de `d.nic.fr` qui est anycasté. Les sondes en service, fin 2013, sont au nombre de cinq (pour huit instances de serveurs DNS) et se situent en région parisienne, à Lyon, Londres, Francfort et Bruxelles.

Il faut noter qu'en basant nos mesures sur les serveurs de la zone `.fr` uniquement administrés par l'Afnic, et en ne tenant pas compte des autres serveurs, nous introduisons un biais dans ces mesures en faveur des requêtes DNS en provenance du territoire français. En effet, les instances de `d.nic.fr` présentes en France reçoivent plus de requêtes en provenance d'opérateurs français que celles qui se trouvent à l'étranger.

En pratique, une dizaine de mesures sont effectuées par semaine. Les requêtes DNS sont capturées en utilisant un échantillonnage aléatoire de 5 % des requêtes reçues durant 24 heures. Cela représente un volume important car les huit instances de serveurs DNS administrés par l'Afnic reçoivent environ 3400 requêtes par seconde (moyenne en journée et en pleine semaine). Le nombre de requêtes DNS, toutes sondes confondues, analysées par semaine par `DNSmezzo` est de l'ordre de 45 millions de requêtes pour octobre 2013. Ce taux d'échantillonnage a été choisi en fonction des ressources matérielles disponibles en termes de stockage et de calcul.

2.2 Dispersion topologique des serveurs DNS faisant autorité

2.2.1 Description

Cet indicateur sert à apprécier la qualité de la répartition topologique et géographique des serveurs de noms pour l'ensemble des zones DNS déléguées sous la zone de référence (ici, `.fr`).

L'idée principale est de minimiser le risque qu'une panne arrête tous les serveurs de noms d'une zone. Ainsi, si une zone est servie par deux serveurs connectés au même bandeau électrique, une panne de la distribution électrique entrainera l'arrêt des deux serveurs. Ils ne sont donc pas réellement indépendants. De même, une panne à un endroit du réseau affecterait la totalité des serveurs de noms d'une zone et, par conséquent, l'ensemble des ressources attachées à cette zone.

La dispersion physique est importante mais n'est pas la seule à considérer. La dispersion au sens du routage IP en est une autre. Les serveurs DNS sont en effet interrogés en utilisant le protocole IP standard et leur accessibilité à l'échelle mondiale dépend du routage BGP. Si tous les serveurs sont situés dans un réseau géré par un même opérateur et que ce réseau est rendu inaccessible depuis un point donné (à cause d'une panne de routage par exemple), la zone sera probablement inaccessible, même si elle est servie par un grand nombre de serveurs faisant autorité.

Selon le type de panne envisagé, ce sera l'une ou l'autre dispersion qui sera plus importante pour la résilience. Ainsi, pour les pannes physiques, le facteur important est, en général, la dispersion géographique, et notamment le nombre de pays différents. De même, dans une zone inondable, le facteur important n'est pas la distance mais l'altitude. Pour certaines pannes logiques (erreur de configuration d'un routeur BGP), c'est la dispersion sur plusieurs AS qui doit être prise en compte. La dispersion topologique est un indicateur de résilience des plus significatifs comme l'ont montré des pannes de domaines importants, notamment lors de l'incident chez `Go Daddy` en septembre 2012 [54].

Avoir au moins deux serveurs faisant autorité est recommandé par la RFC 1035 [37]. L'idée derrière cette exigence est que les deux serveurs ne tomberont pas en panne en même temps. Avec un seul serveur, toute panne est fatale. Leur dispersion topologique est cependant une exigence plus récente (RFC 2182 [55] et 2870 [56]), issue de l'ingénierie de la résilience. Il s'agit d'éviter les SPOF [16], que ceux-ci soient un AS ou un pays. Notons toutefois que la mesure externe ne suffit pas à détecter tous les SPOF. Pour reprendre l'exemple précédent, on ne peut pas détecter à distance si deux serveurs partagent la même alimentation électrique.

16. Single Point Of Failure.

2.2.2 Méthodologie de mesure

L'ensemble des mesures est obtenu grâce au module actif `DNSdelve` qui prend un échantillon de 10 % de la zone `.fr` pour en analyser les zones déléguées. Les mesures sont faites à une fréquence hebdomadaire.

La dispersion des serveurs de noms par pays ou par AS, présentée dans cette section, tient compte du nombre de zones gérées par ces serveurs. En d'autres termes, si un serveur gère dix zones, il sera comptabilisé dix fois.

Pour mesurer la dispersion topologique des serveurs DNS faisant autorité, nous avons introduit les métriques suivantes :

- **nombre de serveurs de noms par zone déléguée** : il est directement déduit de la zone `.fr` ;
- **nombre d'AS par zone déléguée** : il est obtenu à l'aide du service de Team Cymru [57] qui permet de faire la relation entre les adresses IP des serveurs DNS faisant autorité et leurs numéros d'AS ;
- **dispersion des serveurs de noms sur les AS** : pour cette métrique, nous mettons l'accent sur les quatre AS les plus importants en termes de nombre de serveurs de noms ;
- **nombre de pays par zone déléguée** : il est obtenu à l'aide de la base `GeoIP` de Maxmind [23] qui associe un pays à une adresse IP [17] ;
- **dispersion des serveurs de noms sur les pays les plus couvrants** : pour cette métrique, nous nous focalisons sur les cinq pays les plus importants en termes de nombre de serveurs de noms.

Limitations

Notons que la méthodologie actuelle ne permet pas de détecter les serveurs DNS utilisant l'*anycast* parmi les zones mono AS. Si cette technique permet une plus grande redondance des serveurs et une réduction des temps de latence des réponses DNS, elle n'en reste pas moins inadaptée pour ce qui est de la tolérance aux pannes qui peuvent affecter l'ensemble du réseau d'un opérateur.

2.2.3 Résultats et analyse

Nombre de serveurs par zone déléguée

Si l'on observe la moyenne du nombre de serveurs par zone, on note qu'elle progresse peu d'année en année. En décembre 2011, elle était de 3,2 ; en décembre 2012 de 3,6 et en décembre 2013 de 3,8 serveurs par zone.

17. Ces bases `GeoIP` sont typiquement constituées à partir des données que les RIR publient via le protocole `whois`.

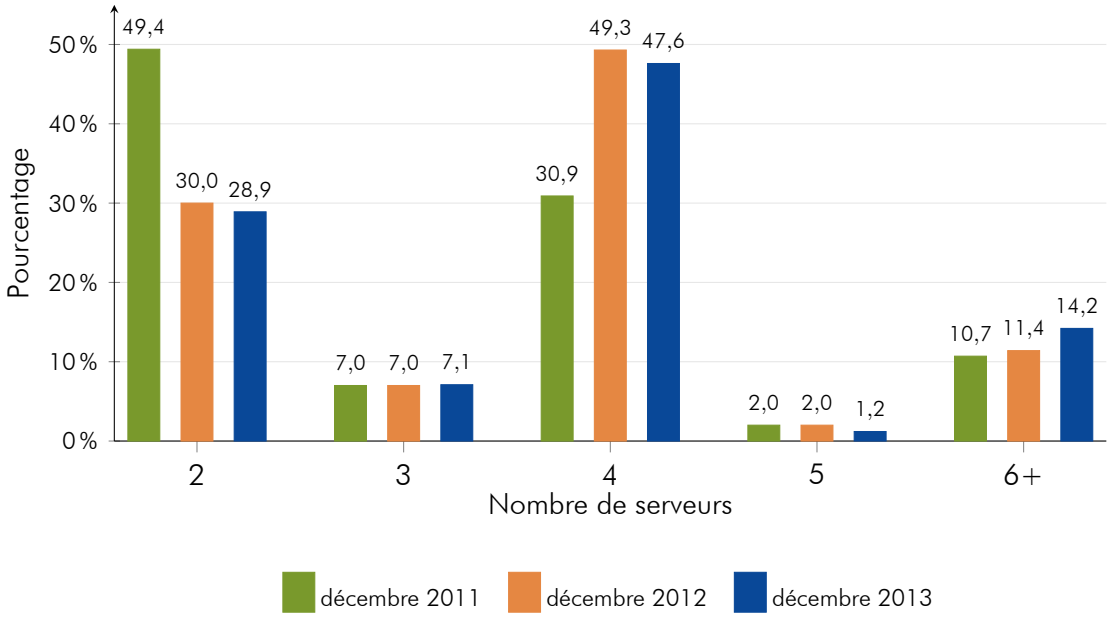

Figure 2.7 – Nombre de serveurs par zone déléguée

Dans la figure 2.7, nous comparons les résultats de 2011, 2012 et 2013 en regardant la dispersion des zones par nombre de serveurs, ce qui permet de faire ressortir des faits plus marquants que ne peut le faire la moyenne du nombre de serveurs par zone. Les zones ne disposant que d'un seul serveur DNS faisant autorité ne sont pas représentées sur cette figure. En effet, leur nombre reste négligeable d'année en année et représente depuis 2011 moins de 1 % des zones.

L'année 2012 avait été marquée par un accroissement sensible du nombre de serveurs par zone. En effet, en 2011, pratiquement la moitié des zones déléguées sous le `.fr` ne possédaient que 2 serveurs ; alors qu'en 2012 plus de la moitié des zones possédaient 4 serveurs et plus.

En 2013, nous observons toujours la même tendance : le nombre de serveurs par zone est très souvent un nombre pair. La répartition du nombre de serveurs reste sensiblement la même que l'année précédente, avec un léger infléchissement pour les zones ayant respectivement 2 et 4 serveurs. Mais cette baisse est compensée par la hausse des zones ayant plus de 6 serveurs (gain de près de 3 points). On retrouve notamment 500 zones ayant 12 serveurs DNS, et et 200 zones ayant 20 serveurs.

Nombre d'AS par zone déléguée

Le nombre moyen d'AS par zone a très légèrement augmenté en 2013. Il était de 1,26 en 2011 et 2012 et atteint 1,30 en 2013.

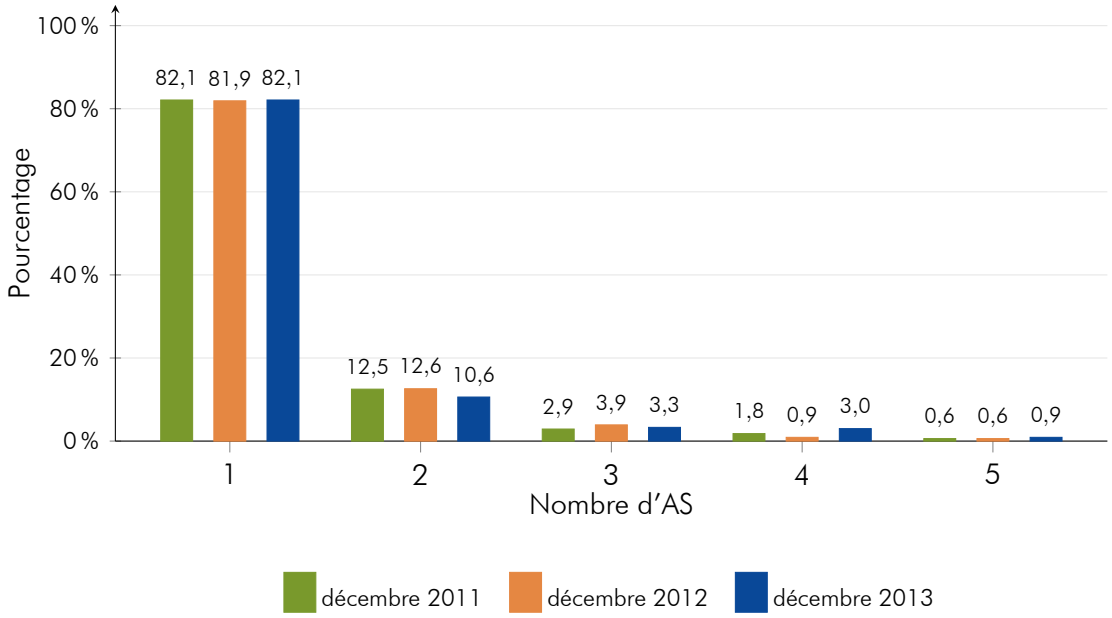

Figure 2.8 – Nombre d'AS par zone déléguée

Quant aux zones dont tous les serveurs sont déployés dans un unique AS, leur taux reste inchangé d'année en année pour se stabiliser à 82 % de l'ensemble des zones, comme le montre la figure 2.8. Le seul fait notable en 2013, est la diminution du nombre de zones dont les serveurs sont déployés sur deux AS au profit des zones déployées sur quatre.

La dispersion des serveurs DNS par AS reste donc toujours faible avec la majeure partie des zones ayant tous leurs serveurs au sein d'un unique AS. Facteur aggravant, 70 % de ces serveurs sont tributaires des AS de quatre hébergeurs DNS.

À retenir

La plupart des zones ont plus de 2 serveurs DNS, cependant ceux-ci sont généralement localisés dans un seul AS.

Dispersion des serveurs sur les AS les plus importants

La figure 2.9 montre la dispersion des serveurs de noms par AS afin d'observer la concentration des serveurs chez les hébergeurs DNS.

Nous nous focalisons ici sur les quatre AS les plus importants en termes de nombre de serveurs DNS hébergés. Il s'agit des mêmes AS d'année en année. La figure 2.9 permet

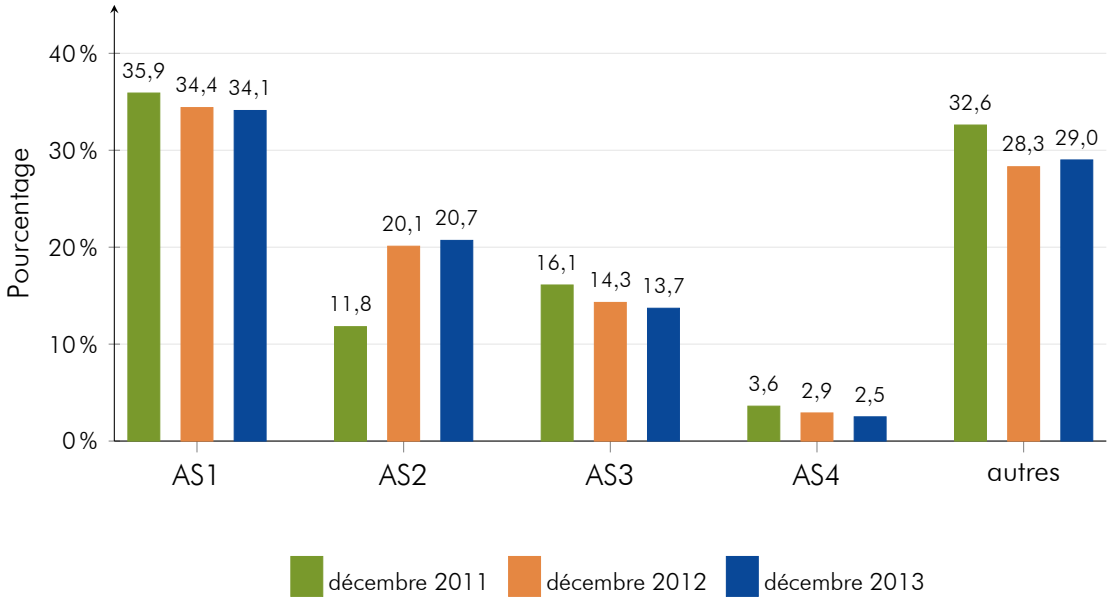

Figure 2.9 – Dispersion des serveurs sur les AS

également d'observer la variation des parts de marché de chacun de ces hébergeurs au cours de la période d'étude.

On constate que ces quatre acteurs concentrent près de 70 % des serveurs DNS faisant autorité pour les zones déléguées sous `.fr` depuis 2012. Le premier acteur reste relativement stable sur les trois années d'études avec plus de 34 % des serveurs DNS hébergés. L'AS2 passé de la troisième à la seconde place en 2012, conserve sa position en 2013 avec une part importante des serveurs hébergés : plus de 20 %.

Il est donc probable qu'une panne de routage chez l'un ou l'autre des deux premiers AS affecte un nombre important de zones sous le `.fr`.

Nombre de pays par zone déléguée

La dispersion des serveurs de noms par pays n'a pas évolué durant la période 2011-2013 : plus de 80 % des zones déléguées ont leurs serveurs de noms dans un seul pays. La moyenne également n'a pas changé au cours de ces trois années ; elle s'établit à 1,2 pays par zone déléguée.

Toutefois, ce manque de variété est moins problématique que la dispersion par AS : une panne affectant un pays entier est moins probable qu'une panne au niveau d'un AS. En ce qui concerne la France, les analyses effectuées dans le chapitre 1 montrent qu'il existe peu d'AS dont la panne affecterait une fraction significative de l'Internet français. D'après les observations de l'Afnic, cette conclusion pourrait également s'ap-

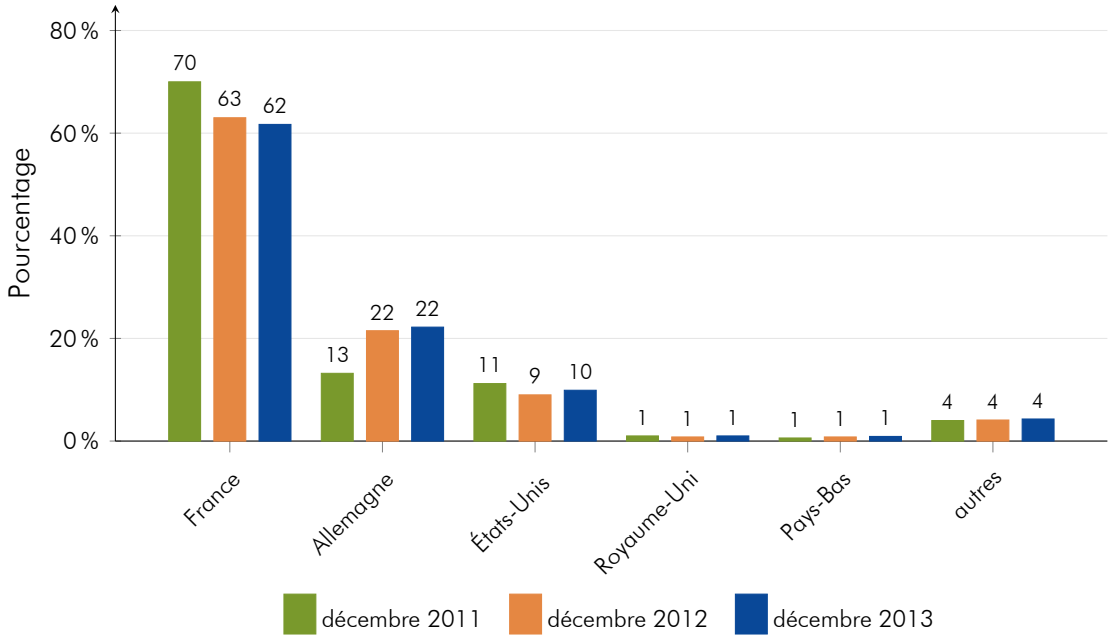

Figure 2.10 – Dispersion des serveurs sur les pays les plus couvrants

pliquer aux autres pays (Allemagne, États-Unis, Royaume-Uni) dans lesquels se trouvent majoritairement les serveurs de noms qui font autorité pour la zone `fr`.

Dispersion des serveurs par pays

La figure 2.10 pointe les cinq pays où se trouve le plus grand nombre de serveurs de noms faisant autorité pour la zone `fr`. Si la France est toujours prééminente avec plus de 60 % des serveurs, sa part diminue néanmoins depuis 2012 au profit de l'Allemagne avant tout.

2.3 Taux de pénétration de DNSSEC

2.3.1 Description

DNSSEC est une technique d'authentification des enregistrements DNS reposant sur la cryptographie. Le principe est de signer les enregistrements. Les extensions de sécurité introduites par cette technique au niveau du protocole et des enregistrements DNS sont décrites dans les RFC 4033 [41], 4034 [42] et 4035 [43].

Un résolveur qui gère DNSSEC pourra ainsi valider ces enregistrements DNS en authentifiant l'origine de ces données (c'est-à-dire en vérifiant que ces données proviennent bien de la zone qui est supposée les contenir), d'une part ; et d'autre part en vérifiant l'intégrité des données reçues. Ledit résolveur doit connaître et faire confiance à une clé de départ (typiquement celle de la racine) ; il trouve les clés suivantes dans le DNS, en parcourant une série de délégations signées (appelée chaîne de confiance) et en s'appuyant sur une série d'enregistrements nommés DS.

Pour cet indicateur, nous utilisons deux métriques : le taux de zones signées avec DNSSEC, et le taux de zones ayant un enregistrement DS dans la zone `.fr`.

Un enregistrement DS présent dans la zone `.fr` témoigne de la signature de la clé de la zone en question par celle de sa zone parente. C'est également un engagement de la part de l'administrateur de cette zone de déployer DNSSEC. Cette signature permet d'établir une chaîne de confiance : il suffit qu'un résolveur fasse confiance à la clé de la zone parente et qu'un enregistrement DS soit présent au niveau de celle-ci pour que les données de la zone fille puissent être vérifiées par le résolveur.

DNSSEC n'est pas un facteur de résilience en soi. Aujourd'hui, il n'y a guère plus de débat sur son intérêt mais plutôt sur le moment de le déployer pour chaque acteur concerné. Par conséquent, il est nécessaire de respecter les bonnes pratiques afin de ne pas diminuer la résilience du service de résolution DNS avec validation DNSSEC. En effet, une erreur de mise en œuvre, de configuration, ou une négligence provoquant l'expiration des signatures DNSSEC, peut entraîner un échec de résolution sur les résolveurs validants, et, par conséquent, une inaccessibilité du service visé après résolution DNS.

2.3.2 Méthodologie de mesure

Les données sur le nombre d'enregistrements DS sont simplement tirées de la base de données de `.fr`. Celles sur le nombre de zones signées proviennent du module DNSSEC de `DNSdelve`. Celui-ci est lancé une fois par semaine et prend un échantillon de 10 % d'une copie du jour de la zone `.fr` puis parcourt les zones déléguées de l'échantillon en envoyant des requêtes DNS particulières.

Une zone est considérée signée dès lors qu'elle possède un enregistrement `DNSKEY` et

un enregistrement NSEC ou NSEC3. Ces deux derniers enregistrements permettent de présenter une signature valide pour des enregistrements n'existant pas dans la zone. Une zone considérée signée n'a pas forcément un enregistrement DS dans la zone .fr.

Limitations

La différence entre le pourcentage de zones signées et le pourcentage de zones possédant un enregistrement DS dans .fr vient des zones signées à titre expérimental, pas encore stabilisées, et surtout des zones dont le bureau d'enregistrement n'offre pas la possibilité de soumettre un DS au niveau de .fr. C'est le cas aujourd'hui pour la majorité des bureaux d'enregistrement en France.

Il est à noter que les indicateurs présentés ici ne s'intéressent qu'aux signatures de zones. Un autre indicateur permettrait également de mesurer la pénétration de DNSSEC en regardant le taux de résolveurs DNS validant ces signatures. Nous prévoyons d'introduire cet indicateur dans une version future du rapport.

Par ailleurs, les signatures cryptographiques ne sont pas vérifiées. Il est donc possible que des zones identifiées comme signées par DNSSEC soient en pratique rejetées par des résolveurs validants.

2.3.3 Résultats

Zones signées avec DNSSEC

En décembre 2011, un nombre infime de zones étaient signées : 170. En décembre 2012, on en décomptait 36 960 et en décembre 2013, ce nombre a augmenté de 250 % pour atteindre 92 500 zones signées.

Même si d'année en année, l'augmentation du nombre de zones signées est substantielle, proportionnellement à la taille de la zone .fr, ce chiffre reste faible : en 2013 cela ne représente que 3,4 % des zones déléguées.

La figure 2.11 indique le taux de zones signées à la fin de chaque trimestre pour les années 2012 et 2013. Pour l'échantillon de fin décembre 2013, on observe que les 92 500 zones signées se répartissent entre 39 bureaux d'enregistrement. Cependant, un bureau d'enregistrement détient à lui seul plus de 97 % de ces zones, le bureau d'enregistrement qui suit, en nombre de zones signées, n'en détient que 0,7 %.

Zones ayant un enregistrement DS dans la zone .fr

Le nombre de zones déléguées possédant un enregistrement DS a augmenté de 263 % entre décembre 2012 et décembre 2013. Cette augmentation est comparable à celle des zones signées. En décembre 2011, la zone .fr comptait 33 enregistrements DS.

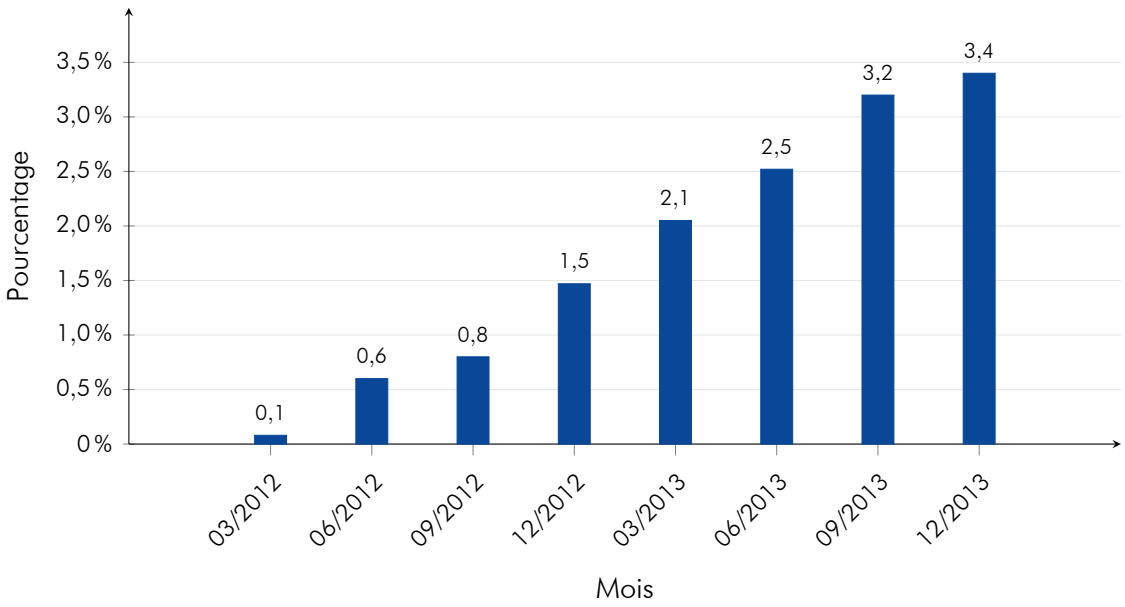

Figure 2.11 – Taux de zones signées de mars 2012 à décembre 2013 (par trimestre)

En décembre 2012, il y en avait 34 496 et en décembre 2013 ce nombre a progressé de 163 % pour atteindre 90 954 zones.

Là encore, proportionnellement à la taille de la zone `.fr`, le taux de zones possédant un DS dans la zone parente reste faible : il représentait 1,4 % des zones en 2012 et 3,3 % en 2013.

À partir de 2012, l'écart entre le taux de zones signées et le taux de zones possédant un DS reste faible.

Il est à noter qu'en décembre 2013, 29 zones déléguées sous `.fr` avaient des enregistrements DLV dans la zone `dlv.isc.org`. Parmi ces zones seules 12 possédaient un DS dans la zone `.fr` ; en revanche elles étaient encore toutes signées. On peut penser que les administrateurs de ces zones, qui ont dû être signées avant que la zone `.fr` ne permette la prise en compte des DS en avril 2011, vont progressivement transmettre ces données au registre du `.fr`.

À retenir

Le protocole DNSSEC est très peu utilisé par les zones déléguées sous `.fr`. Fin 2013, il y avait 92 500 zones signées. Un seul bureau d'enregistrement détient plus de 97 % de celles-ci.

2.4 Taux de pénétration d'IPv6

2.4.1 Description

Sous l'angle du DNS, on peut caractériser l'évolution de la pénétration d'IPv6 en exploitant les données qui sont à disposition du registre du `.fr`. Ces données sont en premier lieu le fichier de zone, où sont déclarées toutes les zones déléguées, et, en second lieu, les requêtes reçues par les serveurs faisant autorité pour `.fr`. On peut alors estimer le taux de pénétration d'IPv6 à l'aide des métriques suivantes :

- le taux de zones qui publient une adresse IPv6 pour un ou plusieurs services (comme le DNS, le web ou le mail) ;
- la proportion de requêtes DNS transportées par IPv6 ;
- la proportion de requêtes DNS demandant une adresse IPv6.

Avec l'épuisement des adresses IPv4 et les politiques en matière d'allocation de blocs d'adresses menées par les RIR, la proportion d'équipements connectés uniquement en IPv6 va croître par rapport à celles des équipements purement IPv4 ou à double pile IPv4-IPv6 (appelée *dual-stack*).

Le RIPE-NCC a ainsi annoncé en septembre 2012 [58] qu'il commençait à allouer des adresses IPv4 à partir de son dernier bloc d'adresses /8 et que toute nouvelle allocation d'adresses IPv4 était, dès lors, subordonnée à une allocation d'adresses IPv6. Début 2014, l'ARIN [18], le RIR nord-américain, a également commencé à puiser dans son dernier bloc /8 d'adresses IPv4 [59]. La nécessité de déploiement d'IPv6 au niveau des infrastructures existantes se fait donc plus pressante.

À retenir

Compte-tenu de la diversité des technologies dans lesquelles on peut observer l'évolution du déploiement d'IPv6, le taux de pénétration de ce dernier est difficile à appréhender. Le protocole DNS fournit cependant une vision pertinente de cette évolution.

2.4.2 Méthodologie de mesure

Zones déléguées ayant des services IPv6

Le taux de zones déléguées sous `.fr` ayant des serveurs répondant en IPv6 est mesuré par le composant actif de la plateforme : `DNSdelve`. Pour cette partie, nous avons fait le choix d'examiner les types de serveurs qui paraissaient les plus pertinents en termes de fréquence d'utilisation : les serveurs DNS, les relais de messagerie et les serveurs

18. American Registry for Internet Numbers.

web.

DNSdelve examine les adresses IPv6 déclarées au niveau du DNS en faisant des requêtes de type AAAA sur des noms particuliers, détaillées ci-dessous, appartenant aux zones analysées. Nous avons donc défini à ce stade trois premières métriques pour mesurer le taux de pénétration d'IPv6 :

- le taux de serveurs DNS faisant autorité compatibles IPv6 ;
- le taux de serveurs de messagerie compatibles IPv6 ;
- le taux de serveurs web compatibles IPv6.

Pour la première métrique, nous avons examiné les serveurs de noms déclarés dans la zone parente : la zone .fr. Pour les serveurs de messagerie, nous nous sommes appuyés sur les enregistrements de type MX déclarés au niveau des zones analysées. Pour les serveurs web, nous avons tenu compte des noms :

- www.<nom-du-domaine>.fr ;
- www.ipv6.<nom-du-domaine>.fr ;
- <nom-du-domaine>.fr.

Il est à noter que pour chacune des métriques présentées dans ce chapitre, le taux de pénétration d'IPv6 est calculé comme étant le rapport entre le nombre de zones ayant activé IPv6 pour un service particulier et le nombre de zones ayant activé ce service. Ainsi, si une zone déléguée n'a pas de serveur web tel que nous les identifions, elle ne sera pas comptabilisée.

À partir des trois métriques précédentes, nous avons synthétisé deux nouvelles métriques afin d'obtenir un éclairage par zone :

- le taux de zones dites « IPv6 activé » qui disposent d'au moins un serveur IPv6 parmi ceux examinés ;
- le taux de zones dites « IPv6 complet » dont tous les serveurs examinés sont compatibles IPv6.

Les mesures pour l'observation de la pénétration d'IPv6 à partir des données déclarées au niveau du DNS se font de manière régulière à raison d'une mesure hebdomadaire sur un échantillon de 10 % des zones déléguées sous .fr. L'échantillonnage est aléatoire et est lancé avant chaque mesure sur une copie du jour de la zone .fr. Les échantillons observés sont donc différents d'une mesure à l'autre.

Requêtes DNS liées à IPv6

DNSmezzo, la partie passive de la plateforme DNSwitness, est utilisé pour examiner les requêtes reçues par les serveurs DNS faisant autorité pour la zone .fr. Cela permet d'observer deux métriques indépendantes :

- le transport : le protocole utilisé pour envoyer la requête DNS ;
- le type d'enregistrement demandé. Le type A représente une adresse IPv4 et

le type `AAAA` une adresse IPv6.

Ces métriques permettent, pour la première, d'estimer le déploiement d'IPv6 au niveau des résolveurs DNS interrogeant les serveurs de la zone `.fr` ; alors que la seconde est un indicateur du déploiement d'IPv6 au niveau des clients faisant appel à ces résolveurs.

Limitations

Les mesures actives effectuées pour cet indicateur ne concernent que trois services. Même s'il s'agit des services les plus courants, une zone pourrait héberger d'autres types de services en IPv6 sans activer ce protocole sur les trois premiers. Par ailleurs, les noms de domaines que nous utilisons pour déterminer les serveurs web associés à une zone introduisent également une limitation : une zone peut très bien héberger son service web sous un nom de domaine autre que `www.<nom-du-domaine>.fr`, `www.ipv6.<nom-du-domaine>.fr`, ou `<nom-du-domaine>.fr`.

2.4.3 Résultats et analyse

Les zones déléguées sous `.fr`

Les résultats suivants nous permettent d'observer la progression du taux de pénétration d'IPv6 sur les quatre dernières années. La figure 2.12 indique la progression d'IPv6 par type de services.

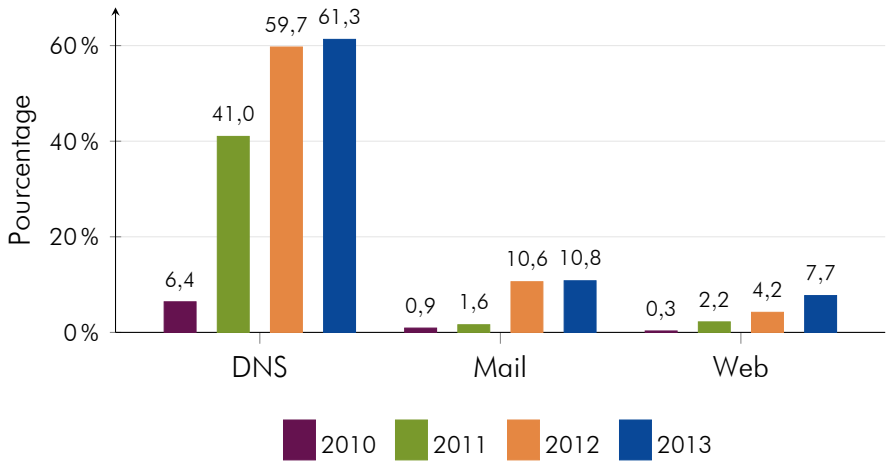

Figure 2.12 – Progression des serveurs compatibles IPv6 entre 2010 et 2013

En 2013, on constate que le taux de déploiement d'IPv6 s'est stabilisé pour les serveurs DNS et les serveurs de messagerie, après une très forte hausse en 2012. Les deux tiers

des serveurs DNS sont actifs en IPv6.

Le taux de serveurs web ayant activé IPv6 a progressé de manière significative en 2013 (progression supérieure à 80 %) pour atteindre 7,7 %. Cependant c'est toujours au niveau des serveurs web que le protocole IPv6 est le moins déployé des trois services étudiés.

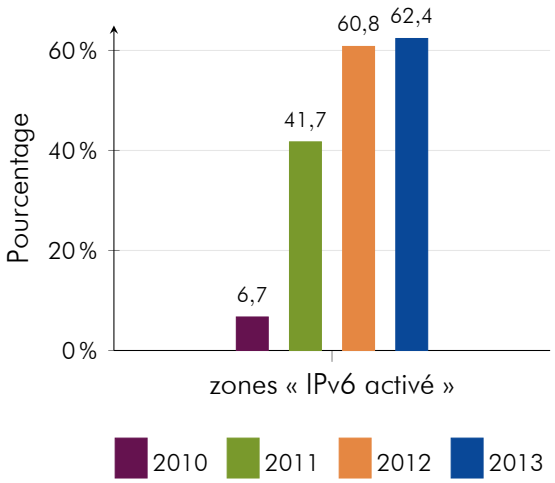

Figure 2.13 – Progression des zones compatibles IPv6 entre 2010 et 2013

Si l'on regarde maintenant la progression d'IPv6 par zone et non plus par service, on constate qu'après deux fortes hausses en 2011 et 2012, le nombre de zones ayant au moins un serveur compatible IPv6 (zones de type « IPv6 activé ») s'est stabilisé en 2013 autour de 2 zones sur 3 (voir figure 2.13).

Comme pour les années précédentes, ce chiffre reflète avant tout le déploiement d'IPv6 sur les serveurs DNS. Cependant, si le taux de zones ayant au moins un service IPv6 est légèrement supérieur au taux de serveurs IPv6, cela provient du fait qu'une faible proportion de zones n'a pas de serveur DNS IPv6, mais que leur serveur de messagerie ou leur serveur web est lui activé en IPv6.

En revanche, pour les zones dites « IPv6 complet », celles ayant tous leurs serveurs (DNS, mail et web) compatibles IPv6, leur taux reste faible comme les années précédentes : il était de 0,2 % en 2011, 0,5 % en 2012 et il est de 0,7 % en 2013.

Les requêtes DNS reçues

Pour les serveurs faisant autorité pour `.fr` et étant directement administrés par l'Afnic, environ 16 % des requêtes sont transportées en IPv6 (voir figure 2.14) en décembre 2013. On remarque donc une progression constante, bien que limitée, du transport IPv6 au cours des deux dernières années.

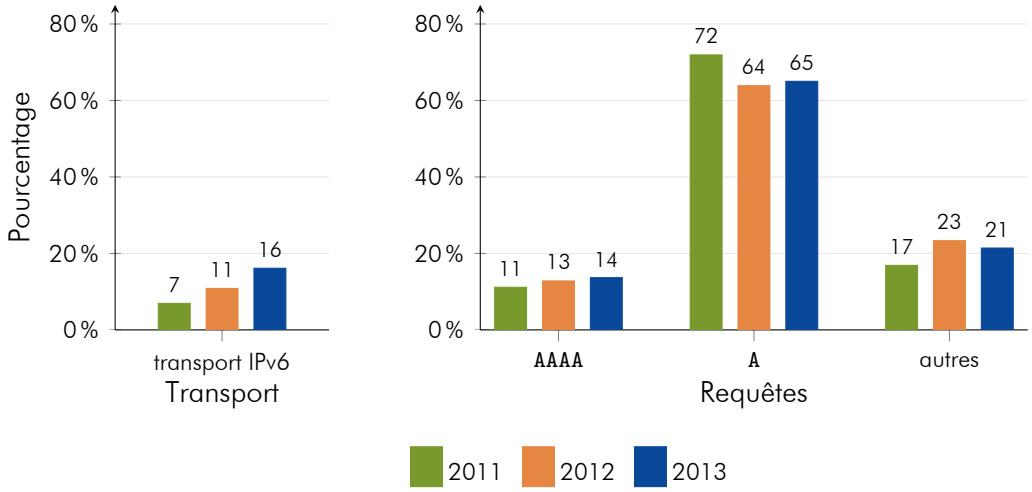

Figure 2.14 – Progression du transport et des requêtes IPv6 entre 2011 et 2013

Quant aux types de données demandées, on remarquera la faible progression des adresses IPv6 au niveau des requêtes (voir figure 2.14). Il faut se rappeler que les clients des serveurs faisant autorité pour le `.fr` ne sont généralement pas des machines d'utilisateurs finaux mais plutôt des résolveurs DNS, souvent gérés par des FAI[19] et hébergeurs. Le type de transport observé par les serveurs de l'Afnic dépend de ses clients directs, soient les gros résolveurs, alors que le type de données demandées reflète le choix des machines des utilisateurs finaux.

Par ailleurs, la figure 2.14, présente entre l'année 2011 et 2012, une forte décroissance des requêtes de demande d'adresses IPv4 (requêtes `A`) qui sont les requêtes observées les plus fréquentes. En 2013, le taux de ce type de requêtes est resté sensiblement le même que l'année précédente. Cette différence de 8 points entre 2011 et 2012 pour les requêtes `A`, s'est faite au profit des requêtes `MX`[20] qui ont gagné 3 points. Par ailleurs, les requêtes `DS`[21] ont également gagné 2 points.

Les requêtes de type `ANY` (demande de tous les types d'enregistrement associés à un nom de domaine) ont gagné 1 point entre ces deux années de référence, au détriment des requêtes de type `A`. Entre 2012 et 2013, le nombre de requêtes `ANY` est resté stable pour représenter 1,9 % du trafic sur les serveurs faisant autorité pour la zone `.fr` et étant administrés par l'Afnic. Les requêtes `ANY` sont souvent utilisées dans les attaques par amplification. Devant la recrudescence de ce type d'attaques, l'Afnic a mis en place des limitations du débit des réponses.

19. Fournisseur d'Accès à Internet.
20. Un enregistrement DNS désignant les relais de messagerie
21. Un enregistrement permettant d'établir une chaîne de confiance entre une zone mère et une zone fille dans le cadre de DNSSEC

2.5 Résolveurs DNS les plus demandeurs

2.5.1 Description

Historiquement, les FAI mettaient à la disposition de leurs utilisateurs un résolveur DNS. Ce résolveur était le seul à interroger les serveurs faisant autorité. Aujourd'hui, des résolveurs publics sont à la disposition du grand public, mais nous ne savons pas dans quelle mesure ils sont utilisés.

Dans un premier temps, cet indicateur vise à identifier les résolveurs les plus demandeurs, c'est-à-dire ceux qui interrogent le plus les serveurs faisant autorité pour la zone `.fr` , et à en étudier les caractéristiques. Dans un second temps, il cherche à les classer selon des catégories reconnaissables, telles que résolveur de FAI, résolveur public ou résolveur individuel. À terme, cet indicateur permettra d'étudier sur la durée l'évolution de ces catégories.

2.5.2 Méthodologie de mesure

Contrairement à la précédente édition du rapport, nous analysons les requêtes reçues par les cinq sondes `DNSmezzo` en activité en faisant une quinzaine de mesures pendant le mois de décembre, chaque mesure durant 24 heures. Alors que l'an dernier nous n'avions pris en compte que l'activité des sondes sur une seule période de 24 heures. Multiplier les mesures permet d'avoir une meilleure vision de l'activité et de l'origine des serveurs récursifs interrogeant les serveurs de la zone `.fr`, et permet de ne pas fausser les résultats globaux par des phénomènes marginaux. Une campagne de spam serait ainsi détectée par un fort taux de requêtes de type `MX`.

Pour rappel, chacune des sondes capture le trafic DNS sur une période de 24 heures en l'échantillonnant à 5 % et ce, deux à trois fois par semaine. Comme l'année dernière, nous ne prenons en compte que les adresses IP des résolveurs ayant généré au moins dix requêtes par période d'observation de 24 heures dans l'objectif d'éliminer les résolveurs dont le nombre de requêtes est peu significatif.

Pour identifier les résolveurs les plus demandeurs, nous avons mis en place deux méthodologies distinctes. Nous nous intéressons tout d'abord aux adresses IP brutes de ces résolveurs. Puis nous les regroupons suivant les préfixes déclarés dans les bases `whois` des RIR dans un premier temps ; et dans un second temps, nous les regroupons suivant les numéros d'AS déclarés. Pour ces regroupements, nous avons utilisé les archives maintenues par le service Team Cymru [57]. En effet, il est fréquent que les opérateurs de résolveurs DNS utilisent plusieurs serveurs. Le regroupement en préfixes permet de comparer le trafic généré par ces opérateurs. Ces derniers peuvent opter pour des choix différents : plusieurs petits résolveurs ou bien un nombre restreint de résolveurs importants.

Rappelons également, que les adresses IP des résolveurs vues par les serveurs faisant

autorité pour la zone `.fr`, ne sont pas forcément celles qui sont employées par les utilisateurs faisant appel à ces résolveurs. Un service public de résolution DNS utilise généralement la technologie anycast et une adresse IP unique offerte aux utilisateurs masque en réalité plusieurs résolveurs dispersés sur le réseau qui interrogeront les serveurs faisant autorité avec une adresse IP propre à chaque instance.

Pour cet indicateur, nous avons donc défini les métriques suivantes :

- **nombre de requêtes par adresse IP** : il est calculé à partir des données des sondes `DNSmezzo`. Pour cette métrique ainsi que pour les suivantes, nous distinguons le trafic IPv6 du trafic IPv4 car les résultats sont assez différents ;
- **nombre de requêtes par pays** : il est calculé à partir de la géolocalisation des adresses IP des résolveurs, en utilisant la base GeoIP de Maxmind [23] ;
- **nombre de requêtes par préfixe** : nous regroupons ici les résultats obtenus par préfixe BGP déclaré dans les bases `whois` des différents IRR [22] ;
- **nombre de requêtes par AS** : en utilisant les numéros d'AS déclarés dans les bases `whois`, nous isolons les acteurs les plus actifs ;
- **nombre de requêtes par AS français** : cette dernière métrique permet d'observer la dispersion des requêtes sur les acteurs français les plus représentatifs.

Limitations

Si un organisme utilise ses propres résolveurs mais ne possède pas d'AS, les requêtes envoyées par ses serveurs seront comptabilisées dans les résultats de son FAI aussi bien pour l'analyse par AS, que pour l'analyse par préfixe BGP.

En utilisant un seuil de dix requêtes journalier et non un seuil couvrant la période d'étude entière, nous introduisons un biais : les résolveurs peu actifs sont ignorés. Dans la prochaine édition, nous utiliserons un seuil pour toute la période et nous verrons si cela a des répercussions sur l'identité des résolveurs les plus actifs. Cependant cette méthode, nous donnera une vision plus fine sur les résolveurs les moins actifs.

Par ailleurs, nous avons vérifié que `d.nic.fr` n'avait pas été utilisé dans le cadre d'attaques DNS par réflexion, notamment avec le type `ANY`. Ces attaques peuvent en effet complètement fausser les mesures.

2.5.3 Résultats et analyse

Nombre de requêtes par adresse IP

Dans l'échantillon de requêtes capturées sur un transport IPv4, en décembre 2013 sur les cinq sondes `DNSmezzo` on compte 1 213 087 adresses différentes, dont 150 589 (soit un peu plus de 12 %) ont envoyé plus de dix requêtes. Ces résolveurs ont envoyé,

22. Internet Routing Registry.

au total, un peu plus de 99 millions de requêtes en IPv4 et la dispersion de ces dernières par résolveur donne les résultats suivants :

- 87 % des requêtes sont effectuées par 10 % des résolveurs ;
- 63 % des requêtes sont effectuées par 1 % des résolveurs.

En IPv6, nous avons 56 724 adresses distinctes, dont 9132, soit 16 %, sont retenues pour l'étude. Un peu plus de 17 000 000 requêtes IPv6 ont été envoyées ; leur dispersion par résolveur donne les résultats suivants :

- 91 % des requêtes sont effectuées par 10 % des résolveurs ;
- 67 % des requêtes sont effectuées par 1 % des résolveurs.

Cette analyse permet de retenir près de 160 000 résolveurs qui interrogent le serveur `d.nic.fr` ; 6 % d'entre eux effectuent leurs requêtes en IPv6 et génèrent 15 % du trafic.

Nombre de requêtes par pays

Si l'on s'intéresse maintenant à l'origine géographique des adresses IP des résolveurs, le tableau 2.1 indique le pourcentage de requêtes reçues par pays et pour chacun des protocoles de transport. Pour le trafic IPv6, le taux particulièrement élevé des requêtes en provenance d'Irlande, provient d'un moteur de recherche américain qui semble avoir localisé une grande part de ses résolveurs européens dans ce pays.

Pays	Requêtes IPv4
France	41 %
États-Unis	15 %
Allemagne	8 %
Royaume-Uni	2 %
Russie	2 %

Pays	Requêtes IPv6
France	45 %
Irlande	31 %
Allemagne	6 %
États-Unis	6 %
Royaume-Uni	2 %

Table 2.1 – Trafic IPv4 et IPv6 par pays

Nombre de requêtes par préfixe

Les préfixes ont été ici constitués sur la base des préfixes BGP déclarés au niveau des différents IRR en décembre 2013, au moment de la capture des requêtes `DNSmezzo`. L'étude qui suit tient compte du nombre de requêtes générées et du nombre de résolveurs contenus dans ces préfixes. L'analyse du trafic IPv4 montre que les 150 589 résolveurs ayant envoyé plus de dix requêtes se répartissent 47 856 préfixes différents. La figure 2.15 indique comment se répartit ce trafic entre les préfixes les plus demandeurs. Quant à la taille des préfixes, sur les dix premiers préfixes les plus demandeurs,

neuf sont des /24. Le nombre de résolveurs par préfixe est de 1 pour le premier préfixe et pour les neuf autres, il varie entre 3 et 24.

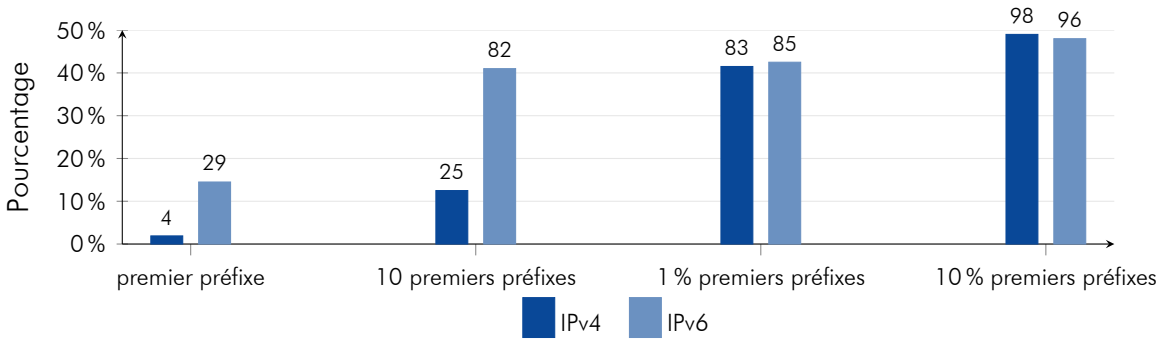

Figure 2.15 – Répartition du trafic par préfixe

Le trafic IPv6, lui, montre que les 9132 résolveurs de l'étude se répartissent en 1569 préfixes différents. La figure 2.15 indique comment se répartit ce trafic entre les préfixes les plus demandeurs. En termes de nombre de résolveurs par préfixe, on remarque que les opérateurs ont des politiques très différentes : le premier, deuxième et troisième préfixe les plus demandeurs ont respectivement 12, 90 et 2210 résolveurs. Quant à la taille de ces trois préfixes IPv6, il s'agit respectivement d'un /29 et de deux /32.

Cette analyse par préfixes met en évidence une forte différence entre IPv4 et IPv6. En IPv6, le nombre moins élevé d'acteurs implique une plus grande concentration en termes de requêtes (les trois premiers préfixes générant à eux seuls 66 % du trafic) ; et la taille des préfixes permet de regrouper un plus grand nombre de résolveurs.

Nombre de requêtes par AS

Le tableau 2.2 indique les cinq AS les plus demandeurs pour les requêtes IPv4 et IPv6. Ces résultats mettent en évidence le phénomène des résolveurs publics : un moteur de recherche mettant un résolveur DNS à la disposition des internautes est en deuxième position aussi bien en IPv4 qu'en IPv6 ; et un second opérateur de résolveur public apparaît dans les résultats IPv6.

Nombre de requêtes par AS français

Un focus sur les AS français permet d'obtenir les résultats présentés dans le tableau 2.3. Nous avons compté au total 422 AS français pour le transport IPv4 et 59 AS pour le transport IPv6. On remarquera, pour les deux types de transport, le rôle prépondérant des deux premiers acteurs qui sont des organismes différents pour chacune des catégories.

Requêtes IPv4	Nombre de résolveurs	Nature de l'AS
21,2 %	7093	Opérateur français
6,5 %	2086	Moteur de recherche
3,5 %	1217	Opérateur français
2,0 %	341	Opérateur belge
1,9 %	4422	Opérateur américain

Requêtes IPv6	Nombre de résolveurs	Nature de l'AS
29,3 %	12	Opérateur français
29,1 %	298	Moteur de recherche
11,0 %	2248	Hébergeur français
4,8 %	303	Réseau social
4,0 %	167	Opérateur allemand

Table 2.2 – Les cinq AS les plus demandeurs en IPv4 et en IPv6

Requêtes IPv4 par rapport aux AS français	Requêtes IPv4 par rapport au trafic global	Nombre de résolveurs	Nature de l'AS
59,9 %	21,2 %	7093	Opérateur
10 %	3,5 %	1217	Opérateur
4 %	1,4 %	803	Opérateur
2,8 %	1 %	1663	Hébergeur
2,8 %	1 %	9	Opérateur

Requêtes IPv6 par rapport aux AS français	Requêtes IPv6 par rapport au trafic global	Nombre de résolveurs	Nature de l'AS
64 %	29,3 %	12	Opérateur
23,9 %	10,9 %	2248	Hébergeur
2,8 %	1,3 %	19	Opérateur
1,4 %	0,6 %	110	Réseau univ.
1,3 %	0,6 %	54	Opérateur

Table 2.3 – Les cinq AS français les plus demandeurs en IPv4 et en IPv6

2.6 Conclusion et perspectives

Dans cette nouvelle édition du rapport, nous avons examiné la résilience de l'Internet français sous l'angle du protocole DNS en poursuivant l'étude des indicateurs que nous avions définis dès la première édition en 2012.

Cette année, nous avons supprimé l'indicateur qui concernait les serveurs DNS vulnérables à la faille Kaminsky [60]. Du fait des mises à jour appliquées aux serveurs concernés, cet indicateur devenait de moins en moins significatif. En effet, les résolveurs DNS qui n'avaient toujours pas corrigé ce problème ne représentaient plus que 6 % du trafic observé par les serveurs de l'Afnic.

Comme dans les rapports précédents, nos analyses se sont basées sur les domaines délégués sous la zone `.fr` et les données publiées au niveau de leurs zones respectives, ainsi que sur les requêtes DNS reçues par les serveurs faisant autorité pour la zone `.fr` et administrés par l'Afnic.

L'Internet français, du point de vue du DNS, se caractérise par de fortes concentrations au niveau des hébergeurs DNS mais également au niveau des opérateurs et autres FAI auxquels les utilisateurs finaux s'adressent pour la résolution DNS. Ce dernier point s'explique dans une certaine mesure par la concentration du marché de l'accès à l'Internet en France.

En effet, si l'on regarde la dispersion topologique des serveurs DNS faisant autorité, on remarque que depuis la mise en place de cet indicateur, quatre acteurs, les mêmes d'année en année, se partagent près de 70 % du marché de l'hébergement DNS. En ce qui concerne la dispersion du trafic IPv4 par AS, un seul opérateur français est à l'origine de plus de 22 % du trafic total. Cette forte concentration du marché soulève la question des impacts d'une panne majeure chez un opérateur de taille importante.

Au-delà de cette concentration, les faits marquants de l'édition 2013 sont :

- un nombre de serveurs DNS faisant autorité par zone déléguée qui se stabilise autour de 3,8 en moyenne, après une forte croissance en 2012 ;
- un déploiement d'IPv6 qui se stabilise également pour les serveurs DNS faisant autorité aux alentours de 60 % et qui évolue peu pour les serveurs de messagerie. Il reste toutefois peu visible pour les serveurs web malgré la croissante observée en 2012 ;
- un déploiement de DNSSEC qui est inférieur aux attentes. En décembre 2013, seuls 3,4 % des zones sous `.fr` étaient signées en dépit du plan d'accompagnement élaboré par l'Afnic. Lancé en octobre 2013 pour une durée de cinq ans, il s'adresse avant tout aux bureaux d'enregistrement du `.fr`, en actionnant deux leviers importants : le renforcement de capacités et l'incitation financière ;
- une diversité des acteurs les plus importants, en particulier des acteurs français, pour la résolution DNS entre ceux à l'origine du trafic IPv4 et IPv6.

Dans les prochaines éditions du rapport, tout en continuant de suivre les indicateurs actuels, il nous semble pertinent d'avoir une meilleure connaissance du déploiement de DNSSEC au niveau des zones signées en ce qui concerne les algorithmes cryptographiques et les tailles de clés utilisées, mais également de connaître la proportion des résolveurs validants. Parmi les autres pistes de réflexion, nous pouvons citer la qualité technique des zones sous `.fr` et l'étude du phénomène des résolveurs individuels.

Conclusion générale

Les améliorations apportées aux méthodologies de l'observatoire permettent d'obtenir une compréhension fine de l'Internet en France. Fin 2013, il était constitué d'environ 850 AS français actifs quotidiennement. L'étude de sa structure a mis en évidence une hétérogénéité des acteurs qui a une influence positive sur la résilience. Ainsi, un AS français possédant deux fournisseurs sera toujours en mesure de joindre le reste de l'Internet en cas de panne de n'importe quel autre AS. En revanche, la concentration des acteurs est très forte en ce qui concerne le DNS. Dès lors, les choix techniques effectués par les hébergeurs français se reflètent directement dans les résultats, notamment concernant le nombre de serveurs par zone.

En marge des observations générales, un certain nombre de résultats est à souligner. Tout d'abord, la proportion d'objets `route` inutilisés augmente, et s'ajoute petit à petit à la liste des objets obsolètes. Sur ce point, la RPKI constitue une solution particulièrement intéressante car ses objets expirent automatiquement. Par ailleurs, la plupart des AS créés pendant l'année 2013 semblent suivre les bonnes pratiques de déclarations. Près d'un tiers des conflits d'annonces de préfixes correspondent à des défauts de déclaration d'objets `route`, et sont principalement effectués par des AS appartenant à la même organisation. L'analyse exhaustive des conflits a montré que sept d'entre eux sont vraisemblablement des usurpations de préfixes qui ont pu être suivies d'un détournement de trafic.
Concernant le DNS, la majeure partie des zones sous `.fr` a un nombre de serveurs satisfaisant, mais la plupart ne sont présents que dans un seul AS. Dans la majorité des cas, ceci est le symptôme d'une résilience amoindrie.
En 2013, il n'y a pas eu de changements notables concernant la RPKI, et les protocoles DNSSEC et IPv6. Leurs utilisations restent marginales, mais continuent de croître lentement.

En guise de conclusion et au regard des résultats, les membres de l'observatoire considèrent que la situation de l'Internet français demeure satisfaisante. Cependant, les bonnes pratiques admises pour BGP et DNS ne sont pas pleinement suivies par les acteurs de l'Internet français. Par conséquent, l'observatoire les encourage à s'approprier ces bonnes pratiques et émet les recommandations suivantes :

- **déployer IPv6** afin de développer rapidement les compétences, et d'anticiper les problèmes opérationnels futurs ;
- **bien répartir les serveurs DNS faisant autorité** afin d'améliorer la robustesse de l'infrastructure ;
- **tester DNSSEC** et le déployer pour lutter contre les attaques par pollution

de cache ;

- **déclarer systématiquement les objets route**, et les **maintenir à jour**, afin de faciliter la détection et le filtrage d'annonces BGP illégitimes ;
- **utiliser la RPKI** et déclarer des ROA ;
- **appliquer les bonnes pratiques BGP** au niveau des interconnexions entre opérateurs.

Bibliographie

[1] ANSSI, "Bonnes pratiques de configuration de BGP," tech. rep., 2013.

[2] ENISA, "Understanding the importance of the Internet Infrastructure in Europe," tech. rep., 2013.

[3] M. Wählisch, T. C. Schmidt, S. Meiling, M. de Brün, and T. Häberlen, "Towards a Nation-Centric Understanding of the Internet," in *Proc. of the 6th ACM SIGCOMM International Conference on emerging Networking EXperiments and Technologies (CoNEXT'10). Student Workshop*, (New York), ACM, Nov 2010.

[4] F. Alizadeh and R. C. Oprea, "Discovery and Mapping of the Dutch National Critical IP Infrastructure," tech. rep., 2013.

[5] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)." RFC 4271 (Draft Standard), Jan. 2006. Updated by RFCs 6286, 6608, 6793.

[6] F. Contat, S. Nataf, and G. Valadon, "Influence des bonnes pratiques sur les incidents BGP." `<https://www.sstic.org/2012/presentation/influence_des_bonnes_pratiques_sur_les_incidents_bgp/>`, June 2012.

[7] RIPE NCC, "YouTube Hijacking : A RIPE NCC RIS case study." `<http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>`, 2008.

[8] J. Cowie, "China's 18-Minute Mystery." `<http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml>`, Nov. 2010.

[9] M. Lepinski, Ed., "BGPSEC Protocol Specification." `<http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-08>`, Nov. 2013.

[10] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing." RFC 6480 (Informational), Feb. 2012.

[11] ITU-T, "X.509 : Information technology - Open Systems Interconnection - The Directory : Public-key and attribute certificate frameworks." `<http://www.itu.int/rec/T-REC-X.509/en>`, 2012.

[12] G. Huston, G. Michaelson, and R. Loomans, "A Profile for X.509 PKIX Resource Certificates." RFC 6487 (Proposed Standard), Feb. 2012.

[13] C. Lynn, S. Kent, and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers." RFC 3779 (Proposed Standard), June 2004.

[14] M. Lepinski, S. Kent, and D. Kong, "A Profile for Route Origin Authorizations (ROAs)." RFC 6482 (Proposed Standard), Feb. 2012.

[15] R. Austein, G. Huston, S. Kent, and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)." RFC 6486 (Proposed Standard), Feb. 2012.

[16] R. Bush, "The Resource Public Key Infrastructure (RPKI) Ghostbusters Record." RFC 6493 (Proposed Standard), Feb. 2012.

[17] RIPE-NCC, "RIPE NCC RPKI (Resource Public Key Infrastructure) Certification Practice Statement (CPS)." <http://www.ripe.net/ripe/docs/ripe-549>, 2012.

[18] RIPE-NCC, "Resource Certification (RPKI) Roadmap." <http://roadmap.ripe.net/rpki/>, 2013.

[19] RIPE-NCC, "Welcome to the RIPE NCC LIR Portal." <https://lirportal.ripe.net/>.

[20] Andrew Tridgell and Paul Mackerras, "rsync." <http://rsync.samba.org/>.

[21] RIPE-NCC, "Routing Information Service (RIS)." <http://www.ripe.net/data-tools/stats/ris/>.

[22] RIPE-NCC, "The RIPE Database." <ftp://ftp.ripe.net/ripe/dbase/ripe.db.gz>.

[23] MaxMind, "GeoIP | IP Address Location Technology." <http://www.maxmind.com/app/ip-location>.

[24] ARCEP, "Opérateurs déclarés (liste)." <http://www.arcep.fr/index.php?id=2102>, 2012.

[25] ANSSI, "Observatoire de la résilience de l'Internet français." <http://www.ssi.gouv.fr/observatoire/>.

[26] R. Varloot, "BGP-level topology of the internet : Inference, connectivity and resiliency," tech. rep., 2013.

[27] University of Oregon, "University of Oregon Route Views Project." <http://www.routeviews.org/>.

[28] M. Luckie, B. Huffaker, k. claffy, A. Dhamdhere, and V. Giotsas, "AS Relationships, Customer Cones, and Validation," in *Internet Measurement Conference (IMC)*, October 2013.

[29] Andree Toonk, "How the Internet in Australia went down under." <https://bgpmon.net/blog/?p=554>, Feb. 2012.

[30] Andree Toonk, "Hijack event today by Indosat." <http://www.bgpmon.net/hijack-event-today-by-indosat/>, Apr. 2014.

[31] NANOG mailing list, "Dreamhost hijacking my prefix...." <http://mailman.nanog.org/pipermail/nanog/2013-January/054846.html>, Jan. 2013.

[32] NANOG mailing list, "Dreamhost/AS26347 unauthorized bgp announcement." <http://mailman.nanog.org/pipermail/nanog/2013-March/056625.html>, Jan. 2013.

[33] J. Cowie, "The New Threat : Targeted Internet Traffic Misdirection." <http://www.renesys.com/2013/11/mitm-internet-hijacking/>, Nov. 2013.

[34] RIPE-NCC, "Dépôt RPKI." <rsync://rpki.ripe.net/>.

[35] LyonIX, "Nouvelle méthode de filtrage sur les Route Serveurs : RPKI + ROA." <http://www.lyonix.net/fr/news-lyonix/item/nouvelle-methode-de-filtrage-sur-les-route-serveurs-rpki-roa>.

[36] P. Mockapetris, "Domain names - concepts and facilities." RFC 1034 (INTERNET STANDARD), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.

[37] P. Mockapetris, "Domain names - implementation and specification." RFC 1035 (INTERNET STANDARD), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604.

[38] CERT-VU-800113, "Multiple DNS implementations vulnerable to cache poisoning." <http://www.kb.cert.org/vuls/id/800113>, July 2008.

[39] Amir Herzberg and Haya Shulman, "Fragmentation Considered Poisonous." <http://arxiv.org/pdf/1205.4011v1.pdf>, May 2012.

[40] Florian Maury and Mathieu Feuillet, "Démonstration d'un détournement possible de technologies anti-déni de service distribué (DDoS)." <http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/articles-de-conferences/demonstration-d-un-detournement-possible-de-technologies-anti-deni-de-service.html>, 2013.

[41] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements." RFC 4033 (Proposed Standard), Mar. 2005. Updated by RFCs 6014, 6840.

[42] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Resource Records for the DNS Security Extensions." RFC 4034 (Proposed Standard), Mar. 2005. Updated by RFCs 4470, 6014, 6840, 6944.

[43] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Protocol Modifications for the DNS Security Extensions." RFC 4035 (Proposed Standard), Mar. 2005. Updated by RFCs 4470, 6014, 6840.

[44] J. Damas, M. Graff, and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))." RFC 6891 (INTERNET STANDARD), Apr. 2013.

[45] D. Conrad, "Indicating Resolver Support of DNSSEC." RFC 3225 (Proposed Standard), Dec. 2001. Updated by RFCs 4033, 4034, 4035.

[46] IANA, "Domain Name System Security (DNSSEC) Algorithm Numbers," tech. rep., Nov. 2003.

[47] ANSSI, "Référentiel général de sécurité." <http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/>, July 2014.

[48] D. E. 3rd, "Domain Name System Security Extensions." RFC 2535 (Proposed Standard), Mar. 1999. Obsoleted by RFCs 4033, 4034, 4035, updated by RFCs 2931, 3007, 3008, 3090, 3226, 3445, 3597, 3655, 3658, 3755, 3757, 3845.

[49] S. Weiler, "Legacy Resolver Compatibility for Delegation Signer (DS)." RFC 3755 (Proposed Standard), May 2004. Obsoleted by RFCs 4033, 4034, 4035, updated by RFCs 3757, 3845.

[50] B. Laurie, G. Sisson, R. Arends, and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence." RFC 5155 (Proposed Standard), Mar. 2008. Updated by RFCs 6840, 6944.

[51] Afnic, "Déployer DNSSEC. Comment, quoi, où ?." <http://www.afnic.fr/medias/documents/DNSSEC/afnic-dnssec-howto-fr-v2.pdf>>, Jan. 2014.

[52] O. Kolkman, W. Mekking, and R. Gieben, "DNSSEC Operational Practices, Version 2." RFC 6781 (Informational), Dec. 2012.

[53] Afnic, "DNSwitness." <http://www.dnswitness.net/>.

[54] Go Daddy, "The INSIDE STORY about what happened at GoDaddy.com Sept. 10, 2012." <http://inside.godaddy.com/inside-story-happened-godaddy-com-sept-10-2012/>, Sept. 2012.

[55] R. Elz, R. Bush, S. Bradner, and M. Patton, "Selection and Operation of Secondary DNS Servers." RFC 2182 (Best Current Practice), July 1997.

[56] R. Bush, D. Karrenberg, M. Kosters, and R. Plzak, "Root Name Server Operational Requirements." RFC 2870 (Best Current Practice), June 2000.

[57] Team CYMRU Community Services, "IP TO ASN MAPPING." <http://www.team-cymru.org/Services/ip-to-asn.html>.

[58] RIPE-NCC, "RIPE-NCC begins to allocate IPv4 address from the last /8." <http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8/>, Sept. 2012.

[59] ARIN, "ARIN enters phase four of the IPv4 countdown plan." <https://www.arin.net/announcements/2014/20140423.html>, Apr. 2014.

[60] Dan Kaminsky, "details." <http://dankaminsky.com/2008/07/24/details/>, July 2008.

Acronymes

Afnic	Association Française pour le Nommage Internet en Coopération
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARIN	American Registry for Internet Numbers
AS	Autonomous System
BGP	Border Gateway Protocol
DLV	DNSSEC Look-aside Validation
DNS	Domain Name System
DNSSEC	DNS SECurity extensions
DS	Delegation Signer
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IRR	Internet Routing Registry
KSK	Key Signing Key
LIR	Local Internet Registry
NSEC	Next SECure
NSEC3	Next SECure version 3
RGS	Référentiel général de sécurité
RIPE-NCC	RIPE Network Coordination Centre
RIR	Regional Internet Registry
RIS	Routing Information Service
RPKI	Resource Public Key Infrastructure
RRSIG	Resource Record digital SIGnature
SPOF	Single Point Of Failure
ZSK	Zone Signing Key

À propos de l'Afnic

L'Afnic est le registre des noms de domaine `.fr` (France), `.re` (Île de la la Réunion), `.yt` (Mayotte), `.wf` (Wallis et Futuna), `.tf` (Terres Australes et Antarctiques), `.pm` (Saint-Pierre et Miquelon).
L'Afnic se positionne également comme fournisseur de solutions techniques et de services de registre. L'Afnic - Association Française pour le Nommage Internet en Coopération - est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). Elle est à but non lucratif.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.
En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.
Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Septembre 2014

Agence nationale de la sécurité des systèmes d'information
ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : `www.ssi.gouv.fr` et `www.securite-informatique.gouv.fr`
Messagerie : communication [at] ssi.gouv.fr