Résilience de l'Internet français

2012

Document réalisé par l'ANSSI et l'AFNIC. Recherche et rédaction par : François Contat, Mathieu Feuillet, Pierre Lorinquer, Guillaume Valadon, Stéphane Bortzmeyer, Samia M'timet, Mohsen Souissi, et Xavier Beaudouin.

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

La résilience de l'Internet est définie comme sa capacité à fonctionner pendant un incident et à revenir ensuite à un état nominal. L'Internet étant une infrastructure importante pour la société française, sa résilience est devenue une nécessité. 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, notamment définies par la communauté.

Dans ce contexte, l'observatoire de la résilience de l'Internet français, placé sous l'égide de l'ANSSI [1], cherche en premier lieu à définir puis à mesurer des indicateurs représentatifs de la résilience. Dans un second temps, ces travaux ont pour objectif de fournir des analyses détaillées et anonymes dans un rapport publié annuellement.

Cette nouvelle édition, rédigée conjointement avec l'Afnic [2], livre ainsi une analyse de la résilience en étudiant deux protocoles indispensables au bon fonctionnement de l'Internet. Le premier, BGP [3], permet aux acteurs de l'Internet 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. Parmi toutes les analyses fournies, soulignons tout d'abord qu'il existe peu d'opérateurs dont la panne affecterait une part significative de l'Internet français. Cependant, certaines bonnes pratiques concernant le déploiement des serveurs DNS et le filtrage des annonces BGP sont peu suivies.

Au regard de tous ces résultats, l'observatoire estime que la situation actuelle de l'Internet français est acceptable. Par ailleurs, l'observatoire adresse les recommandations suivantes aux acteurs de l'Internet français :

- **déployer IPv6** afin de développer les compétences et d'anticiper des problèmes de déploiements futurs ;
- **répartir les serveurs DNS faisant autorité au sein de différents opérateurs** afin de limiter les effets d'une panne locale ;
- **déclarer systématiquement les objets route**, et les **maintenir à jour**, afin de faciliter la détection et le filtrage d'annonces BGP illégitimes ;
- **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.

Introduction

L'Internet est devenu 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 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 donc 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 et les dépendances entre les différents acteurs concernés.

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, 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, notamment définies par la communauté.

La mission de l'observatoire de la résilience de l'Internet français est également d'identifier et de mesurer des indicateurs représentatifs de la résilience, et de rendre leurs résultats publics. En outre, il associe à sa démarche les acteurs de l'Internet français afin d'augmenter son efficacité et de favoriser une adoption franche des bonnes pratiques.

Le premier rapport de l'observatoire a été publié en juin 2012. Rédigé conjointement par l'ANSSI et l'Afnic, il a posé les bases de l'étude de la résilience durant l'année 2011. Le concept et les résultats ont fait l'objet de nombreuses présentations, qui ont reçu un bon accueil de la part des acteurs de l'Internet. Fort de ces réactions, l'observatoire a rédigé, dans la continuité du précédent, un nouveau rapport qui porte toujours sur l'étude des protocoles BGP et DNS à travers différents indicateurs techniques mesurables.

La liste de ces indicateurs et leurs définitions ont cependant évolué afin de prendre en compte les commentaires émis par la communauté. Par exemple, concernant le protocole BGP, les travaux effectués portent désormais sur l'ensemble des acteurs de l'Internet français. Pour chaque indicateur, le rapport propose une définition aussi rigoureuse que possible, décrit la méthodologie de mesure associée et présente les résultats ainsi que leur analyse. Une attention particulière a par ailleurs été portée à la présentation synthétique des protocoles BGP et DNS.

Ainsi, le premier chapitre s'ouvre par une description du fonctionnement du protocole BGP. Afin de sensibiliser la communauté à certains mécanismes utiles pour la résilience, les objets `route` font l'objet d'explications plus détaillées. 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, dans lequel un opérateur annonce des informations de routage illégitimes ;
- la cohérence des objets `route`, qui vise à s'assurer qu'ils sont correctement déclarés et mis à jour ;
- l'influence des filtrages des annonces via les objets `route` sur le nombre de préfixes joignables ;
- l'utilisation de la RPKI [5], par laquelle l'adoption de cette nouvelle technologie est mesurée ;
- l'évolution du déploiement d'IPv6 et le respect des bonnes pratiques BGP depuis 2009.

Dans le second chapitre, une vision synthétique du protocole DNS est donnée avec une description plus approfondie du mécanisme *anycast*, toujours dans un but pédagogique. Enfin, la résilience 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 nombre de résolveurs encore vulnérables à la faille dite « Kaminsky » ;
- le taux de pénétration de DNSSEC [6] ;
- l'état du déploiement du protocole IPv6 ;
- les résolveurs qui interrogent la zone `.fr`.

5. Resource Public Key Infrastructure.
6. DNS SECurity extensions.

Chapitre 1

Résilience sous l'angle du protocole BGP

1.1 Introduction

Après un rappel succinct du fonctionnement du protocole BGP, ce nouveau rapport se focalise sur la définition des objets `route`, leur déclaration ainsi que leur utilisation. Les objets `route` identifient clairement quels préfixes sont susceptibles d'être annoncés par un AS. Ils permettent ainsi de mettre en place des filtres sur les annonces de préfixes.

1.1.1 Rappels sur BGP

Chacun des opérateurs de l'Internet gère des blocs d'adresses IP [1] contiguës, qu'il peut diviser en plus petites plages appelées préfixes pour ses propres besoins ou pour 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 [1]. 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 :** c'est un 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 les infrastructures propres aux deux opérateurs ;

1. Internet Protocol.
2. Autonomous System.

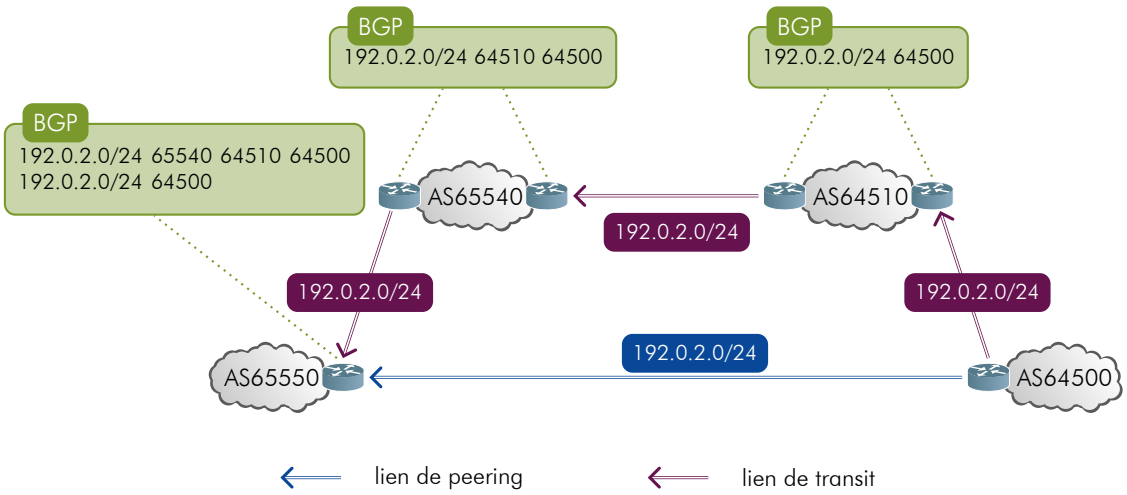

Figure 1.1 – Exemple de chemins d'AS sur des liens de transit et peering

- **le transit :** il s'agit là d'un accord commercial entre un client (c'est-à-dire, 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 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 se situe à droite dans la liste que constitue un chemin d'AS.

En pratique, un message BGP de type `UPDATE` est utilisé pour indiquer le chemin d'AS associé à un préfixe. Ce message BGP est ainsi responsable de l'apprentissage et de l'annonce des routes. 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 une interconnexion de peering avec l'AS64500 (en bleu), et l'autre via une interconnexion de transit avec l'AS65540 (en violet). En l'absence d'autre information, le chemin d'AS le plus court détermine la route utilisée. Dans cet exemple, il s'agit du lien de peering.

1.1.2 Les objets routes

De la création d'un AS aux objets route

Lorsqu'une organisation souhaite utiliser le protocole BGP pour communiquer sur Internet, il lui faut un numéro d'AS et des adresses IP. En Europe, ce nouvel acteur de l'Internet doit en faire la demande [2] auprès du RIPE-NCC ou d'un intermédiaire appelé LIR [3]. En pratique, un LIR est un opérateur capable d'attribuer des adresses IP à ses clients.

Lorsqu'un numéro d'AS est attribué à un organisme, un objet de type `aut-num`, similaire à l'exemple de la figure 1.2, est créé dans la base `whois` [3] du RIPE-NCC. Les attributs `admin-c` et `tech-c` fournissent respectivement les contacts administratif et technique pour l'AS décrit ici, 64496. L'attribut `mnt-by` fait référence à un objet de type `mntner` qui définit le gestionnaire et la méthode d'authentification requise (par mot de passe ou clé PGP [4]) pour modifier l'objet `aut-num`.

```
aut-num:        AS64496
as-name:        AS-D-EXEMPLE
descr:          AS d'exemple
admin-c:        GV-EXEMPLE
tech-c:         FC-EXEMPLE
mnt-by:         MNTNER-EXEMPLE
```

Figure 1.2 – Exemple d'un objet `aut-num`

De la même façon, lorsqu'un bloc d'adresses IP est alloué à une organisation, un objet de type `inetnum` est créé, comme celui de la figure 1.3. Ce nouvel objet indique le responsable d'un bloc d'adresses IP. Il faut souligner que cet objet `inetnum` peut être modifié par *MNTNER-LIR*, le LIR de l'organisation, et ne contient aucune référence au numéro d'AS susceptible d'annoncer des préfixes contenus dans ce bloc.
Dans cet exemple, l'attribut `status` indique que le bloc d'adresses IP alloué par le LIR de l'organisation est de type PA [5]. Cela signifie que l'objet `inetnum` de l'organisation fait partie d'un objet `inetnum` plus grand appartenant à son LIR, par exemple `198.18.0.0-198.18.255.255`. L'attribut `mnt-routes` indique, quant à lui, qui peut créer et modifier des objets `route` sur cet objet `inetnum`.

3. Local Internet Registry.
4. Pretty Good Privacy.
5. Provider Aggregate.

```
inetnum:        198.18.0.0-198.18.7.255
netname:        FR-EXEMPLE-RESEAU
descr:          Reseau d'exemple
country:        FR
admin-c:        GV-EXEMPLE
tech-c:         FC-EXEMPLE
status:         ASSIGNED PA
mnt-by:         MNTNER-LIR
mnt-lower:      MNTNER-EXEMPLE
mnt-routes:     MNTNER-RO-EXEMPLE
```

Figure 1.3 – Exemple d'un objet `inetnum`

```
route:          198.18.7.0/24
descr:          Prefixe d'exemple
origin:         AS64496
mnt-by:         MNTNER-RO-EXEMPLE
```

Figure 1.4 – Exemple d'un objet `route`

Une fois le bloc d'adresses IP alloué, l'organisme peut décider de le découper en objets `inetnum` de plus petites tailles. Ce découpage peut être utilisé pour affiner ses politiques de routage, ou pour permettre à ses clients d'annoncer de plus petits préfixes. Dans la figure 1.3, de plus petits objets `inetnum` peuvent être créés par *MNTNER-LIR* et *MNTNER-EXEMPLE*. Une fois ce découpage réalisé, l'opérateur peut annoncer sur Internet ses préfixes via le protocole BGP.

Sans plus de précision, il n'est pas possible de savoir si une annonce de préfixes effectuée via le protocole BGP est légitime ou non, car un AS a la possibilité d'annoncer n'importe quel préfixe. Pour cette raison, les bonnes pratiques veulent qu'un organisme déclare, dans la base `whois`, les préfixes qu'il annonce en BGP. Ces déclarations doivent être effectuées par l'intermédiaire d'objets `route` et sont stockées dans les serveurs d'un IRR [6]. Ce service est opéré par chaque RIR [7], dont le RIPE-NCC pour l'Europe. Un objet `route` permet d'identifier clairement les AS susceptibles d'annoncer les préfixes de l'organisation.

L'objet `route` de la figure 1.4 indique que le préfixe 198.18.7.0/24 est annoncé par

6. Internet Routing Registry.
7. Regional Internet Registry.

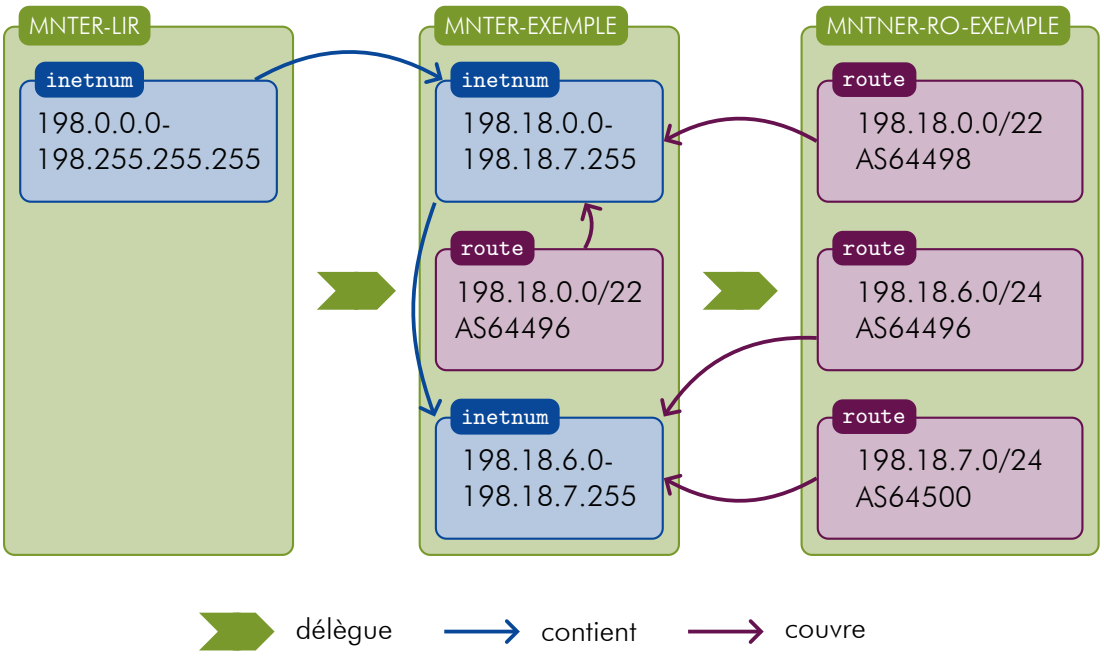

Figure 1.5 – Relations entre objets `mntner`, `route` et `inetnum`

l'AS 64496. L'organisation pourrait déléguer l'utilisation de ce préfixe à un client ou à un partenaire. Dans ce cas, l'attribut `origin` porterait donc sur un numéro d'AS différent de 64496. Afin d'autoriser certains types de déploiements, dont le routage *anycast* (décrit page 62), il est légitime de déclarer différents objets `route` avec des attributs `route` identiques mais des attributs `origin` différents. L'attribut `mnt-by` indique quant à lui les personnes en charge de la déclaration et de la maintenance de cet objet `route`.

La figure 1.5 résume les relations entre les objets `inetum`, les objets `route` et les gestionnaires ayant l'autorisation de modifier ces objets. Les gestionnaires *MNTNER-LIR*, *MNTER-EXEMPLE*, et *MNTNER-RO-EXEMPLE* ont les permissions pour modifier les objets contenus dans les boites correspondantes.

Dans cet exemple, le LIR possède l'objet `inetnum 198.0.0.0-198.255.255.255` et en délègue une partie, équivalente à un préfixe de 21 bits, à l'organisation. L'organisation déclare quant à elle un objet `inetnum` plus petit pour ses clients, ainsi qu'un objet *route* reflétant ses propres besoins opérationnels.

Le gestionnaire *MNTNER-RO-EXEMPLE* est en charge de la création des objets `route` pour les clients. On constate que les objets `déclarés` autorisent plusieurs AS à annon-

cer les mêmes préfixes. Ce type de déclaration est par exemple utilisé pour protéger l'AS 64496 d'un DDoS [8]. En cas d'attaque, l'AS 64498 pourrait légitimement annoncer les routes à la place de l'AS 64496 pour attirer le trafic à destination du préfixe 198.18.0.0/22 afin de le nettoyer. Le trafic légitime serait alors redirigé vers l'AS 64496.

Exploitation des objets route

Nous prenons maintenant le cas de deux interconnexions de transit établies entre un client A, et ses opérateurs de transit B et C. Afin de mettre en place les bonnes pratiques d'interconnexion et de filtrage d'annonces BGP, un fournisseur de transit doit connaître à l'avance les préfixes utilisés par ses clients. Ces informations lui sont nécessaires afin de configurer des filtres sur les annonces BGP effectuées par les clients. Ces filtres lui permettent, par exemple, de se prémunir d'erreurs de configuration entraînant des annonces de préfixes n'appartenant pas à l'un de ses clients.

L'opérateur de transit dispose de différentes méthodes pour récupérer la liste des préfixes annoncés par ses clients. La figure 1.6 présente les deux principales :

1. au moment de la mise en place de l'interconnexion entre le client A et l'opérateur B, A envoie la liste de ses préfixes par voie électronique (action 1), le fournisseur met alors en place ses filtres (action 2) ;
2. le client A déclare auprès de son RIR les objets `route` correspondant aux préfixes qu'il va annoncer (action 1'). L'opérateur C contacte le RIR de son client (action 2') et configure les filtres sur les routeurs d'interconnexion en utilisant les objets `route` déclarés (action 3').

La méthode 1 comporte ses limites. Par exemple, lorsque le client A se voit attribuer de nouveaux objets `inetnum`, il doit contacter son fournisseur pour l'informer des nouveaux préfixes qu'il souhaite annoncer en BGP. Tant que cette action n'est pas réalisée, les nouveaux préfixes sont systématiquement refusés par l'opérateur B. De plus, la mise à jour des filtres peut prendre un certain temps selon les besoins opérationnels. Notons également que toute erreur commise lors de la communication des préfixes aura un impact significatif sur le temps nécessaire à l'équipe d'exploitation pour la mise en place des filtres.

La méthode 2, quant à elle, permet de se dédouaner des échanges entre le client A et son fournisseur C. Lorsque le client se voit attribuer de nouveaux objets `inetnum`, la déclaration des objets `route` correspondants permet de s'assurer que son homologue pourra mettre à jour ses filtres de manière automatique. Il est toutefois important de noter que cette méthode implique le développement d'un outil interne permettant

8. Distributed Denial of Service.

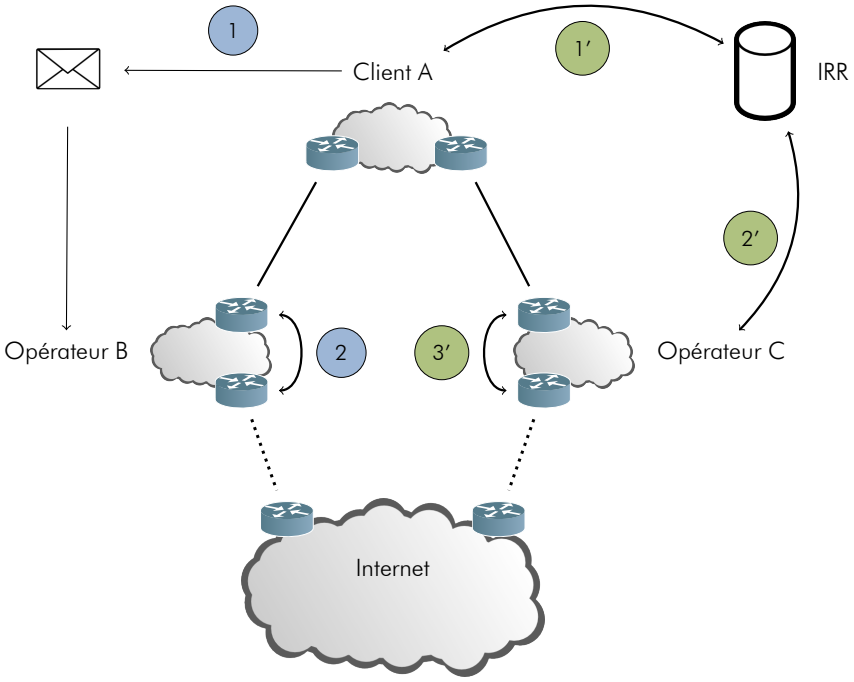

Figure 1.6 – Relations IRR et opérateurs

de générer automatiquement les filtres et de les mettre en place sur les équipements concernés.

L'utilisation des filtres d'annonces BGP basés sur des objets `route` n'est pas systématique chez tous les acteurs de l'Internet. L'un des objectifs de ce rapport est de faire le point sur la déclaration, l'obsolescence éventuelle et l'utilisation des objets `route` dans le cadre de la détection des usurpations de préfixes.

1.1.3 Objectifs de ce chapitre

Dans la suite de ce chapitre, nous présentons six indicateurs concernant le protocole BGP. Certains de ces indicateurs sont issus du rapport 2011, et d'autres sont nouveaux. Il s'agit :

1. de la connectivité des AS français ;
2. des usurpations de préfixes ;
3. de la cohérence des objets `route` ;
4. du filtrage d'annonces via les objets `route` ;
5. de l'utilisation de la `RPKI` ;
6. du déploiement d'IPv6 et le respect des bonnes pratiques BGP.

Nous avons également défini une méthodologie permettant d'identifier automatiquement les AS français. Elle ne permet pas d'appréhender la résilience, mais ses résultats sont réutilisés par les six indicateurs.

1.1.4 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[9] [4]. Celui-ci gère seize collecteurs BGP répartis à travers la planète. Ils stockent et mettent à disposition toutes les annonces de préfixes qu'ils reçoivent. Dans ce rapport, nous utilisons les données du collecteur situé à Londres, qui donne une bonne vision de l'Internet français.

L'étude effectuée dans le rapport 2011 portait sur quatre AS français. Dans cette nouvelle édition, nous avons choisi d'analyser globalement l'ensemble des AS français (voir la section 1.2 pour leur définition) et d'effectuer une analyse fine sur dix AS français lorsque cela est nécessaire. Ces dix AS français ont été sélectionnés par les membres de l'observatoire car l'analyse de leurs résultats apporte des éléments de réflexion intéressants. De plus, ils représentent différents métiers de l'Internet français : fournisseurs d'accès, fournisseurs de services, ou transitaires. Ils seront appelés AS-fr1 à AS-fr10 afin de préserver leur anonymat. Il n'y a volontairement pas de correspondance entre les numéros d'AS d'un indicateur à l'autre.

9. Routing Information Service.

1.2 Identification automatique des AS français

1.2.1 Description

Le rapport de l'observatoire portant sur l'année 2011 se focalisait sur quatre AS français sélectionnés pour être représentatifs dans le cadre de l'étude. Ce choix restrictif a permis de mettre en place le concept de l'observation de la résilience de l'Internet sous l'angle du protocole BGP. Ces quatre AS ne représentant cependant pas l'ensemble de l'Internet français, nous avons décidé de définir une méthodologie permettant d'identifier automatiquement l'Internet français et les AS qui le composent.

Lors des différentes présentations des résultats de l'observatoire, de nombreuses questions ont porté sur la définition de l'Internet français. En ce qui concerne l'étude du protocole BGP, nous considérons qu'il est constitué par l'ensemble des AS français. Il est cependant difficile d'apporter une définition unique et fiable d'un AS français. En effet, différentes définitions peuvent être envisagées, quelques-unes d'entre elles pouvant être opposées. Par exemple, certains estiment qu'un AS est français si son activité commerciale est située en France, et d'autres qu'un AS est français si les administrateurs sont en France. Nous avons donc choisi de sélectionner un ensemble de critères utilisables pour réaliser une classification automatique.

Cette première définition automatique de l'Internet français est perfectible. Elle permet toutefois de comparer nos résultats avec les jeux de données d'AS français existants et d'étudier la structure de l'Internet français de façon plus fine et exhaustive que dans le rapport sur l'année 2011. Ainsi, la définition de l'Internet français est utile afin de déterminer les AS à étudier pour mieux appréhender sa résilience.

1.2.2 Méthodologie de mesure

Nous avons tout d'abord défini huit critères indépendants 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 [3] contient des mots-clés français ;
2. plus de 75 % des adresses IP sont localisées en France par la bibliothèque `GeoIP` [5] ;
3. la description dans la base du RIPE-NCC contient des mots-clés issus de la liste des opérateurs déclarés auprès de l'ARCEP [6] ;
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-deux AS français identifiés manuellement par les membres de l'observatoire ;
7. c'est un AS directement connecté à l'un de ces trente-deux AS ;
8. son numéro d'AS a été attribué par le RIPE-NCC.

Ces différents critères ont été appliqués successivement aux 24 962 AS présents en juillet 2012 dans la base `whois` du RIPE-NCC. Pour un critère donné, cela permet de déterminer si un AS semble être français, étranger ou s'il n'est pas possible de faire un choix. Par exemple, pour le quatrième critère, un AS n'est probablement pas français si l'adresse de l'organisation qui le gère est à l'étranger.

Ces résultats sont utilisés comme données d'entrée d'un algorithme d'apprentissage. Nous avons utilisé l'algorithme des k-moyennes afin de classifier automatiquement les AS du RIPE-NCC. Cet algorithme regroupe les AS les plus similaires étant donné les huit critères définis dans une liste d'AS français, et une liste d'AS étrangers.

Limitations

La liste des AS français a été établie au cours du mois de juillet 2012. Étant donnée la nature dynamique de l'Internet, cette liste n'est pas figée, et évolue naturellement au cours du temps. Afin d'obtenir une liste actualisée et fiable, nous souhaitons à l'avenir identifier automatiquement les AS français plusieurs fois dans l'année.

Par ailleurs, nous souhaitons utiliser plus de critères permettant de déterminer si un AS est français. Un axe de réflexion envisageable serait de déterminer les AS dont les clients accèdent le plus à des sites francophones.

1.2.3 Résultats et analyse

En juillet 2012, notre méthode a permis de mettre en évidence de façon automatique 1270 AS français sur les 24 962 présents dans la base du RIPE-NCC. Sur ces 1270 AS détectés, d'après les archives BGP, seuls 709 français annonçaient des préfixes le 31 juillet 2012. Parmi les AS qui ne sont pas utilisés pour effectuer des annonces de préfixes, on trouve notamment :

- des numéros d'AS 32 bits attribués à des opérateurs qui n'utilisent que les AS 16 bits correspondants ;
- des organismes disposant de nombreux numéros d'AS inutilisés ;
- des sociétés qui n'existent plus.

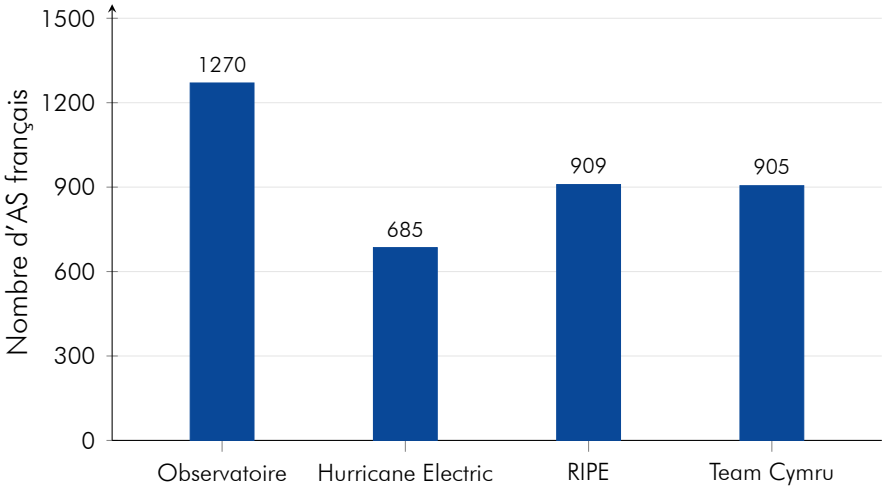

Figure 1.7 – Comparaison du nombre d'AS français

Comparaison avec d'autres jeux de données d'AS français

Nous avons également cherché à comparer notre liste avec trois jeux de données fournissant une correspondance entre numéro d'AS et pays. Ces trois bases sont par la suite appelées : Team Cymru [7], Hurricane Electric [8] et RIPE [9]. Les figures 1.7, 1.8, et 1.9 permettent de comparer ces jeux de données afin d'étudier la qualité des résultats obtenus par notre méthode.

La figure 1.7 indique que le nombre d'AS français identifiés n'est pas le même pour les quatre jeux de données. Le nombre d'AS français dans la base de Hurricane Electric est presque deux fois plus faible que le nombre calculé par notre méthode.

Afin d'identifier plus finement la qualité des résultats, la figure 1.8 présente la différence entre les trois jeux de données récupérées sur Internet et les résultats obtenus. Elle souligne que certains AS français ne sont pas détectés par notre méthode. Si l'on s'intéresse uniquement aux AS français réellement visibles dans les annonces BGP, 9 AS sont mal identifiés par notre méthode. Une étude manuelle de ces AS montre qu'ils sont bel et bien français mais que les critères que nous utilisons ne permettent pas de les détecter automatiquement. Ces 9 AS sont les mêmes pour les trois jeux de données avec lesquels nous comparons notre méthode.

La figure 1.9 présente, quant à elle, les AS français identifiés par notre méthode mais qui n'apparaissent pas dans les autres jeux de données. L'analyse manuelle des AS français supplémentaires par rapport à la base de Team Cymru montre que tous ces

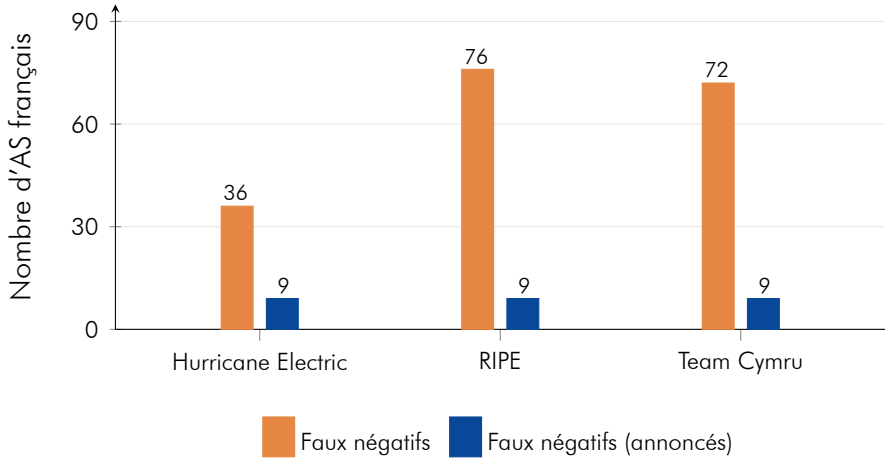

Figure 1.8 – Nombre d'AS français non trouvés par notre méthode

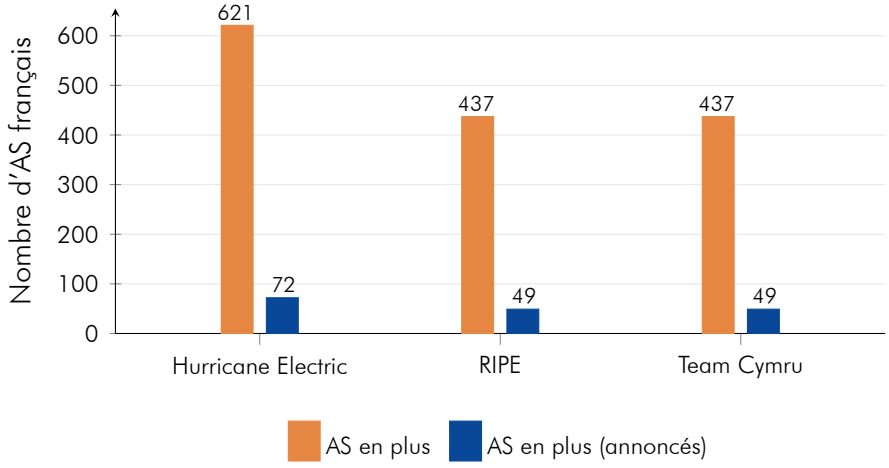

Figure 1.9 – Nombre d'AS français absents des autres jeux de données

AS appartiennent à des sociétés ou à des organismes de recherche français.

Les premiers résultats concernant l'analyse automatique des AS français sont très encourageants. En effet, ils montrent que notre méthodologie est efficace et identifie plus d'AS français que les jeux de données existants. Dans la suite de nos travaux, nous souhaitons ajouter des nouveaux critères d'identification des AS français et ainsi obtenir une liste encore plus proche de la réalité.

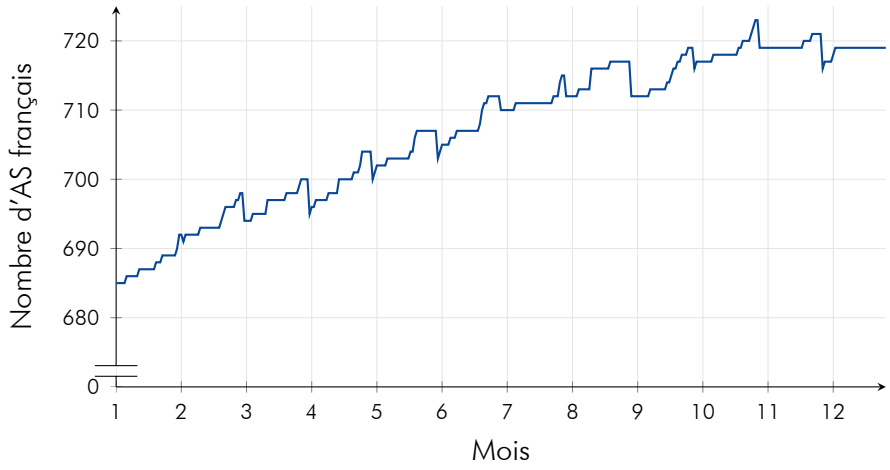

Figure 1.10 – Nombre d'AS français vus dans les archives BGP en 2012

Évolution des AS français en 2012

La liste des AS français ayant été établie en juillet 2012, nous avons cherché à étudier l'évolution des AS français vus dans les archives BGP. À partir de la liste des 1270 AS français, nous avons étudié quels AS annoncent réellement des préfixes durant l'année 2012.

Au cours de l'année 2012, 752 AS français distincts ont ainsi annoncé des préfixes. Le nombre d'AS français vu chaque jour passe quant à lui de 685 AS en janvier à 719 AS en décembre. Comme le montre la figure 1.10, ce nombre est en augmentation régulière sur l'année en dépit de quelques variations peu significatives.

Un noyau dur de 661 AS français annonce des préfixes quotidiennement durant toute l'année 2012. Parmi les 91 AS français restants, certains ne sont visibles qu'une journée, et d'autres plus de trois cents jours dans l'année.

1.3 Connectivité des AS français

1.3.1 Description

L'objectif de cet indicateur est d'obtenir une vision globale de la connectivité des AS français. Pour cela, nous utilisons les données du collecteur londonien du RIS et nous représentons les relations entre AS sous la forme d'un graphe. Les AS constituent les nœuds du graphe. Il existe une arête entre deux AS s'ils sont consécutifs dans un `AS_PATH`.

Il est alors possible d'étudier la structure du graphe obtenu pour évaluer la robustesse de la connectivité entre AS français. En particulier, il est possible de mettre en lumière quelques AS potentiellement critiques pour l'Internet français.

1.3.2 Méthodologie de mesure

Les `AS_PATH` sont extraits des archives de routage BGP fournies par le collecteur londonien du RIS, le 31 juillet 2012, donnant une vision instantanée des tables de routage à cette date. À partir du graphe obtenu, nous cherchons à obtenir la liste des sous-indicateurs suivants :

- **l'enveloppe connexe des AS français**, qui est le graphe contenant tous les AS français ainsi que tous les AS présents sur une route minimale entre deux AS français ;
- **les AS pivots**, qui sont les systèmes autonomes dont l'absence entraînerait la perte de connectivité entre des AS français ;
- **la distribution du degré des AS français** qui consiste en la répartition des AS français en fonction de leur nombre de connexions directes.

Pour l'étude spécifique sur les 10 AS (appelée focus dans la suite), nous avons étudié les relations entre AS à l'aide des objets `aut-num` déclarés par les opérateurs dans la base `whois` et plus particulièrement les attributs `import` et `export`. Ceux-ci permettent à un opérateur de décrire l'ensemble de sa politique de routage. Les différentes relations possibles sont rappelées dans la section 1.1.1.

Si l'on considère une interconnexion entre deux AS X et Y, déclarée dans l'objet `aut-num` de X, elle sera considérée comme :

- **de transit :** si les attributs `import` et `export` associés sont respectivement `accept ANY` et `announce AS-SET-XX` ;
- **cliente :** si les attributs `import` et `export` associés sont respectivement `accept AS-SET-YY` et `announce ANY` ;
- **de peering :** si les attributs `import` et `export` associés sont respectivement `accept AS-SET-YY` et `announce AS-SET-XX`.

Dans les définitions précédentes, *AS-SET-XX* est un objet de type `as-set` contenant l'AS *AS-X* et ses clients. L'objet *AS-SET-YY* est défini de manière similaire pour l'AS *AS-Y*.

L'exemple d'objet `aut-num` de la figure 1.2, page 11, est repris dans la figure 1.11 et complété avec des attributs `import` et `export`. L'objet *AS-SET-D-EXEMPLE* est de type `as-set` et contient *AS-D-EXEMPLE* ainsi que ses clients. 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.

```
aut-num:        AS64496
as-name:        AS-D-EXEMPLE
descr:          AS d'exemple
admin-c:        GV-EXEMPLE
tech-c:         FC-EXEMPLE
mnt-by:         MNTNER-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 1.11 – Exemple d'un objet `aut-num` avec des attributs `import` et `export`

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 au collecteur londonien du RIS. En particulier, nous ne voyons ni les accords de peering des AS qui ne sont pas directement connectés au collecteur 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. Inversement, une autre limite importante de la méthode utilisée vient du fait que les informations de routage de chaque lien ne sont pas prises en compte. De ce fait, il peut exister un chemin dans le graphe de connectivité entre deux AS sans que les paquets ne puissent être routés en pratique. Ces deux limitations font qu'il n'est pas possible de déterminer précisément si la situation réelle est pire ou meilleure que celle décrite dans notre étude. Cette dernière doit être considérée comme une première approche du problème.

En ce qui concerne la base de données `whois` utilisée pour le focus des dix AS, l'ensemble des informations qui y sont contenues sont purement déclaratives et rien ne leur exactitude. De plus, il n'est pas obligatoire de renseigner cette base et les informations peuvent être absentes.

1.3.3 Résultats et analyse

Avec cette approche, 81 AS pivots, dont 34 étrangers, ont été trouvés. Sur la figure 1.12, les AS pivots sont ordonnés en fonction du nombre d'AS qui seraient déconnectés de l'Internet français s'ils venaient à disparaitre. Par exemple, il y a 39 AS dont la disparition entraînerait la déconnexion de deux AS. En lisant cette figure, on peut remarquer qu'il y a seulement 19 AS pivots dont la disparition entraînerait la perte de connectivité pour plus de deux AS. Il se trouve que parmi ceux-ci, il y a quatre transitaires non français. Par ailleurs, il apparaît qu'il y a seulement 8 AS dont la disparition entraînerait la perte de connectivité pour plus de 8 AS dont un opérateur de transit non français. Il y a donc peu d'AS dont une panne affecterait beaucoup d'autres AS.

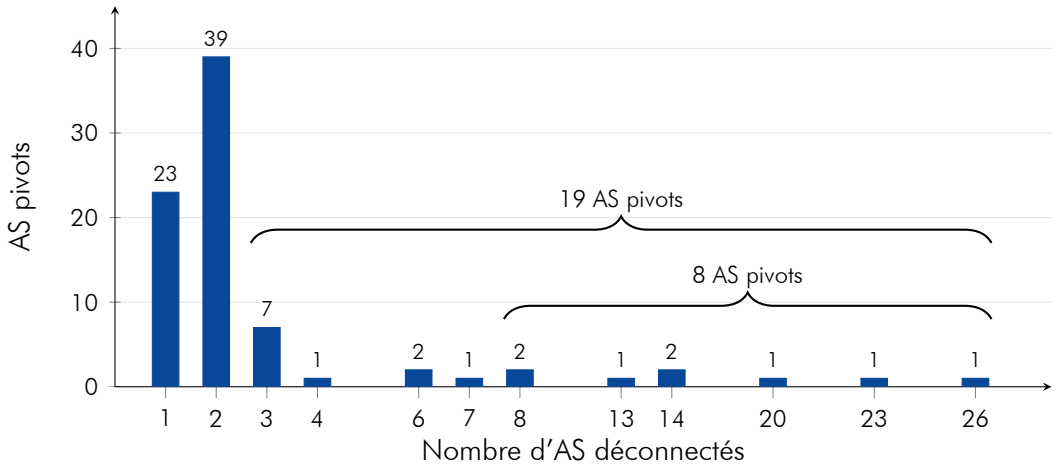

Figure 1.12 – AS pivots en fonction du nombre d'AS déconnectés

Le 31 juillet 2012, il y a 739 AS français présents dans les `AS_PATH` annoncés. Dans la section 1.2.3, page 18, il est expliqué que, ce jour-là, seuls 709 AS français annoncent des préfixes. Les 30 AS supplémentaires correspondent à des AS d'opérateurs de transit qui n'annoncent pas de préfixe mais sont présents dans les `AS_PATH` des préfixes de leurs clients. Parmi ces 739 AS français annoncés sur Internet, 161 annoncent des chemins d'AS IPv4 et IPv6, 575 annoncent exclusivement des chemins

d'AS IPv4 et 3 que des chemins d'AS IPv6. Il faut noter pour ces trois derniers que leurs propriétaires ont d'autres AS annonçant des préfixes IPv4.

En ce qui concerne la distribution des degrés, nous l'avons modélisée à l'aide d'une loi de puissance telle que la probabilité pour un AS d'avoir un degré de n est proportionnelle à $n^{-\alpha}$ avec $\alpha > 0$. À l'aide d'une régression linéaire, nous obtenons que le coefficient α est de l'ordre de 2 pour l'ensemble du monde et 1,3 pour la France. En gardant les limites de cette étude à l'esprit, ceci permet de conclure que la proportion d'AS avec un fort degré de connectivité est plus importante en France que dans le monde pris dans son ensemble. Du point de vue de la résilience, il est difficile de conclure si ceci est positif ou non. La présence d'un plus grand nombre d'AS avec un fort degré augmente la robustesse du graphe. En revanche, il est probable que la propagation d'annonces BGP erronées soit plus aisée. Il est donc primordial d'appliquer une politique de filtrage sur les annonces pour éviter cette propagation.

Une représentation graphique de la connectivité en IPv4 et en IPv6 est donnée sur les figures 1.13 et 1.14. 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.

Focus sur dix AS français

Parmi les dix AS français, présentés au 1.1.3, sur lesquels nous effectuons une étude détaillée, sept sont des AS pivots. Certains sont des opérateurs de transit mais d'autres appartiennent à une organisation possédant plusieurs AS dont tout le trafic passe par l'AS étudié.

Parmi les dix AS étudiés, neuf d'entre eux fournissent leurs informations de routage dans les objets `aut-num` de la base `whois`. Les résultats sont synthétisés dans le tableau 1.1. Chaque colonne contient les interconnexions visibles dans les archives BGP par rapport à celles qui sont déclarées. La dernière colonne contient les interconnexions qui sont visibles mais qui n'ont pas été déclarées dans la base de données `whois`. Par exemple, AS-fr1 a déclaré dans la base `whois` 3 interconnexions de transit, 1 interconnexion cliente et 404 interconnexions de peering parmi lesquelles, respectivement 2, 1 et 10 sont visibles dans les archives BGP. De plus, 3 interconnexions visibles dans les archives BGP ne sont pas déclarées dans la base `whois`.

On peut remarquer que tous les AS à l'exception d'un utilisent plusieurs transitaires, ce qui est un point positif pour la résilience. Comme annoncé plus haut, on peut également remarquer que le nombre d'accords de peering est extrêmement élevé,

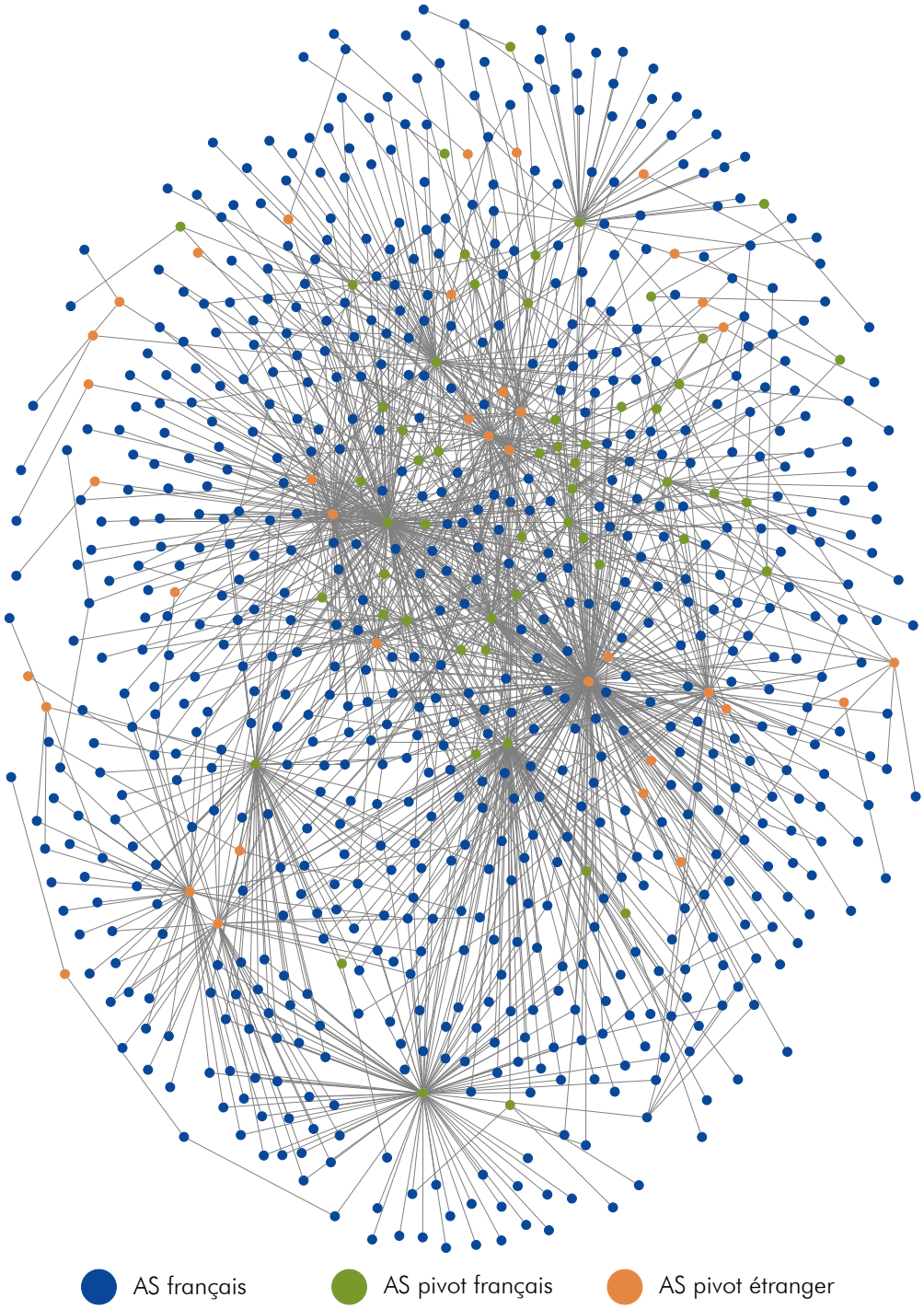

Figure 1.13 – Graphe de connectivité en IPv4

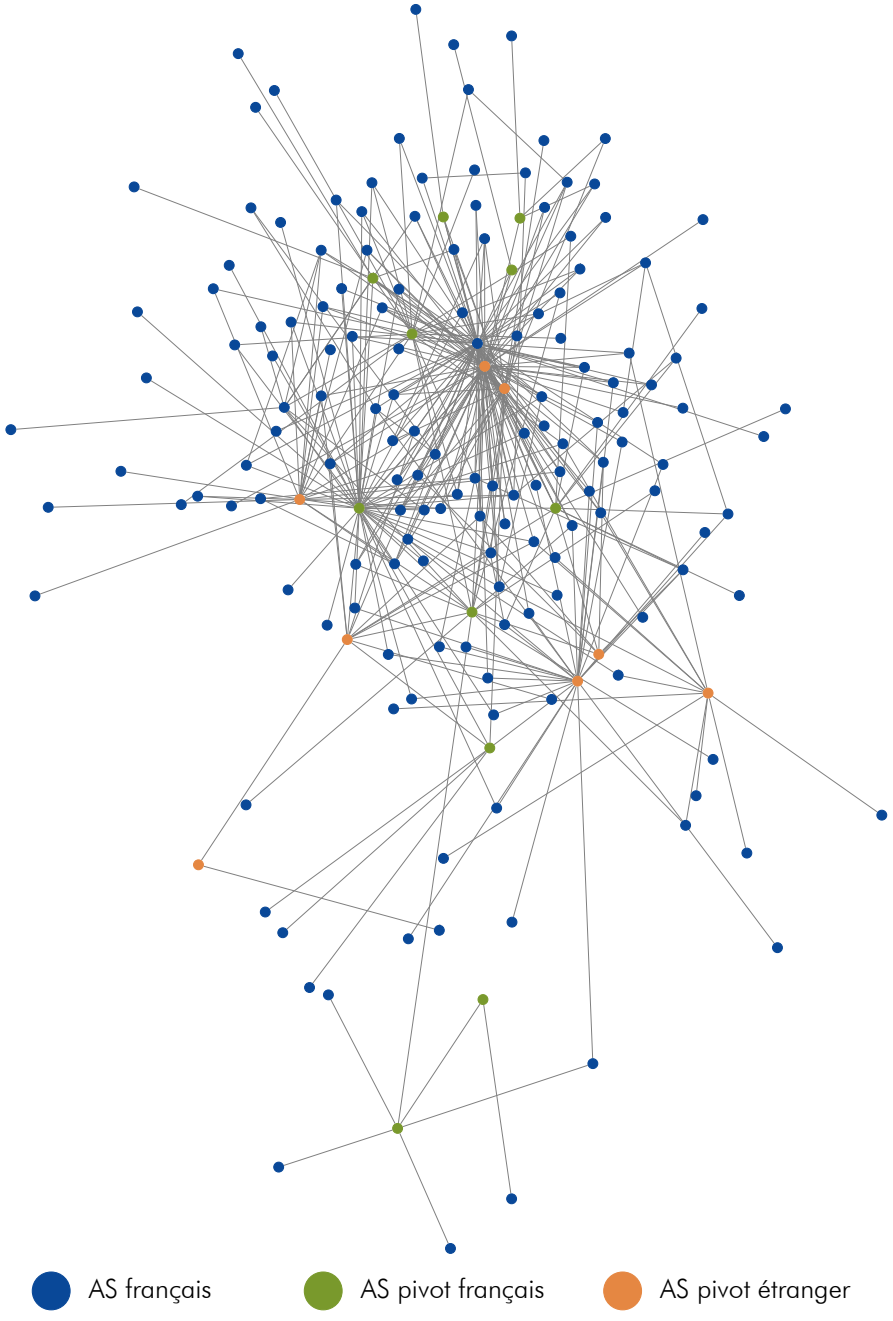

Figure 1.14 – Graphe de connectivité en IPv6

AS	Transit	Client	Peering	Non déclaré
AS-fr1	2/3	1/1	10/404	3
AS-fr2	4/5	0/0	3/214	7
AS-fr3	2/3	1/1	4/94	19
AS-fr4	0/3	0/3	3/217	9
AS-fr5	1/1	59/107	0/13	41
AS-fr6	4/7	71/130	6/27	14
AS-fr7	0/4	20/38	14/152	12
AS-fr8	3/3	55/68	11/322	13
AS-fr9	2/2	0/0	5/165	1

Table 1.1 – Connectivité des dix AS français au 31 juillet 2012 (visible/déclaré)

ce qui est au moins partiellement dû aux différents points d'échange présents sur le territoire français. Par ailleurs, on peut voir également que le nombre d'interconnexions de peering visibles dans les archives BGP du collecteur du RIS est beaucoup plus faible que ce qui est annoncé dans la base de données `whois` ; cela est dû au fait que la plupart de ces accords ne sont pas visibles car annoncés uniquement entre les AS concernés. Enfin, on peut voir que certaines interconnexions de transit ou vers des clients ne sont pas visibles et, inversement, certaines interconnexions sont visibles sans être présentes dans la base de données ; ceci met en exergue le fait que les informations présentes dans les bases `whois` sont purement déclaratives, pas forcément correctes et souvent obsolètes.

1.4 Usurpations de préfixes

1.4.1 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 de lutter contre les usurpations, deux grands mécanismes sont à la disposition des acteurs de l'Internet : le filtrage et la détection.
Les bonnes pratiques d'interconnexion définissent des mécanismes de filtrage dont l'objectif est d'interdire les annonces illégitimes au plus près de la source, en se basant sur des déclarations préalables, notamment des objets `route` définis dans la section 1.1.2 et dont il est question dans les sections 1.5 et 1.6.
La détection consiste quant à elle à surveiller toutes les annonces de préfixes afin de mettre en évidence les usurpations. Si la surveillance est effectuée en temps réel, elle permet aux acteurs de l'Internet de prendre connaissance des usurpations le plus rapidement possible puis de prendre des mesures [10] pour rétablir rapidement la situation.

Dans le cadre de nos travaux, nous nous intéressons à la détection des usurpations effectuées contre les AS français. Dans cette section, nous considérons qu'un préfixe est délégué à un AS français si cet AS l'annonce en BGP. Afin de récupérer toutes les annonces qui sont en conflit les unes avec les autres, nous appelons *événement*, une annonce de préfixe plus spécifique ou égale à une annonce de préfixe effectuée par un autre AS, à un instant donné. Chacun des événements est alors classé afin d'identifier s'ils sont légitimes ou non.

Pour chacun des événements détectés, nous regardons tout d'abord si un objet `route` existe. L'événement est alors considéré comme valide. S'il n'existe pas d'objets `route` correspondant à l'annonce, l'`AS_PATH` est alors utilisé pour 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 montre que les événements associés sont pour la majorité des défauts de déclaration d'objets `route`.

10. Par exemple, en contactant les administrateurs du transitaire de l'AS usurpateur, ou en annonçant des préfixes plus spécifiques.

Les analyses effectuées dans le rapport 2011 avaient conclu que la plupart des événements anormaux ne sont pas des usurpations. Avec ce nouveau rapport, nous cherchons avant tout à compter de façon fiable tous les événements qui ne sont pas valides. Cela permet également de montrer de manière efficace les efforts nécessaires pour déclarer les objets `route`.

1.4.2 Méthodologie de mesure

À partir des archives publiques BGP, nous établissons la liste de tous les événements survenus durant l'année 2012 et qui ont touché des AS français. Les événements sont liés aux messages `UPDATE` de BGP reçus par le collecteur londonien du projet RIS. Par conséquent, ils comportent chacun un *timestamp* correspondant à l'instant où le message BGP a été reçu. Tous les événements collectés contiennent le préfixe annoncé par l'AS français usurpé, un préfixe, égal au précédent ou plus spécifique, annoncé par l'AS usurpateur, et le chemin d'AS correspondant. Pour cet indicateur, nous étudions à la fois les préfixes IPv4 et IPv6.

L'étape suivante consiste à comparer l'ensemble de ces événements avec les archives quotidiennes des objets `route`. Cela permet de classer les événements dans les quatre catégories suivantes :

- **valide :** un objet `route` correspond au préfixe à l'origine de l'événement ;
- **direct :** l'AS usurpateur est connecté à l'AS usurpé ;
- **indirect :** l'AS usurpé est présent dans l'`AS_PATH` entre l'AS usurpateur et le collecteur ;
- **anormal :** l'AS usurpé n'est pas l'`AS_PATH`.

Durées des événements

Il est possible d'agréger les événements à l'aide de leurs *timestamps* afin d'obtenir leurs durées totales. Pour cela, il convient de :

1. regrouper tous les événements selon : (a) le numéro de l'AS français surveillé, (b) le préfixe qu'il annonce, (c) le numéro de l'AS usurpateur, et (d) le préfixe, égal ou plus spécifique, que ce dernier annonce ;
2. pour tous les événements regroupés, trier les *timestamps* ;
3. conserver un *timestamp* trié, si et seulement si, il est séparé de moins de 8 heures [11] du *timestamp* qui le précède.

Identification des usurpations

Dans le cadre des travaux de l'observatoire, nous n'avons pas encore mis en place

11. Le collecteur du RIS enregistre toutes les routes au moins une fois toutes les 8 heures.

de mécanisme automatique permettant de trouver les usurpations parmi les événements anormaux. Le volume de ces événements, même après agrégation, est bien trop important pour envisager une analyse manuelle des données. Nous avons défini les heuristiques suivantes afin de réduire le nombre d'événements à analyser manuellement :

1. **événements anormaux seulement**. En effet, les événements directs et indirects semblent être le fait de déclarations d'objets `route` incorrectes ;
2. **pas d'AS privés** à l'origine de l'événement ;
3. **annonces plus spécifiques uniquement**. Ce sont les annonces avec les effets, à priori, les plus néfastes ;
4. **AS étrangers seulement** ;
5. **moins d'une semaine**. Étant donné que 61 % des événements durent moins d'une semaine, il est plus probable de trouver des usurpations dans les événements courts ;
6. **durée non nulle**.

Limitations

Tout comme dans le rapport 2011, nous ne prenons pas en compte les usurpations portant sur des préfixes appartenant à un AS mais qui n'auraient pas été annoncés par cet AS.

Les événements agrégés peuvent avoir une durée nulle. En pratique, cela n'est pas possible car il n'est pas possible recevoir un message `UPDATE` et un message `WITHDRAW` [12] simultanément. Dans la prochaine édition du rapport, nous souhaitons calculer les durées d'événements de manière plus précise à l'aide des messages `WITHDRAW`.

La méthodologie présentée dans ce rapport ne permet pas de déterminer si un événement anormal est réellement une usurpation. Un traitement manuel est ainsi nécessaire pour déterminer la nature d'un événement anormal. Dans la suite des travaux de l'observatoire, nous souhaitons implémenter des algorithmes de détection d'usurpations définis dans la littérature scientifique [10, 11].

1.4.3 Résultats et analyse

Résultats globaux

Sur les 1270 AS français, seuls 104 sont la cible d'événements au cours de l'année 2012. Pour 27 d'entre eux, il y a une correspondance parfaite entre les objets `route`

12. Ce message BGP indique qu'un préfixe n'est plus annoncé sur Internet.

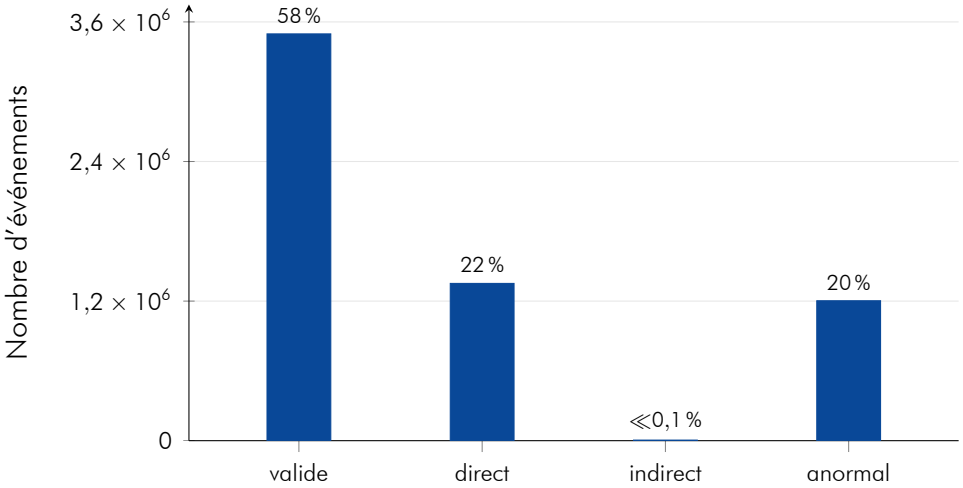

Figure 1.15 – Types des événements détectés en 2012

déclarés et les événements [13]. Il faut noter que 32 AS ont plus de 99 % d'événements de type valide. Une étude plus approfondie des données indique que 129 AS sont à l'origine des événements non valides, dont 84 AS français. Par ailleurs, l'analyse des chemins d'AS correspondant aux événements indique que 122 AS, dont 43 français, ne filtrent pas les annonces faites par leurs clients à l'aide des objets `route` car ils laissent passer des annonces non valides.

La figure 1.15 présente, quant à elle, le nombre d'événements associés à chacun des types qui ont été définis. Le résultat concernant les événements direct et indirect est particulièrement intéressant à détailler. En effet, une analyse manuelle de ces événements semble indiquer qu'ils sont principalement dûs à des défauts de déclarations d'objets `route`. Par exemple, si un opérateur délègue un préfixe à un client sans en faire de déclaration, l'annonce faite par le client sera considérée comme un événement de type direct. Il s'agit d'un résultat encourageant qui montre qu'il serait possible d'atteindre près de 80 % d'événements de type valide en déclarant les objets `route`.

Au cours de l'année 2012, 271 préfixes appartenant à des AS français sont la cible d'événements non valides. Aucun objet `route` n'est déclaré pour 65 de ces préfixes. Par ailleurs, les événements non valides correspondent à 891 préfixes, contenus dans les 271 préfixes ciblés, qui deviendraient inaccessibles si des filtres stricts utilisant des objets `route` étaient systématiquement déployés.

13. On ne voit que des événements de type valide pour ces 27 AS.

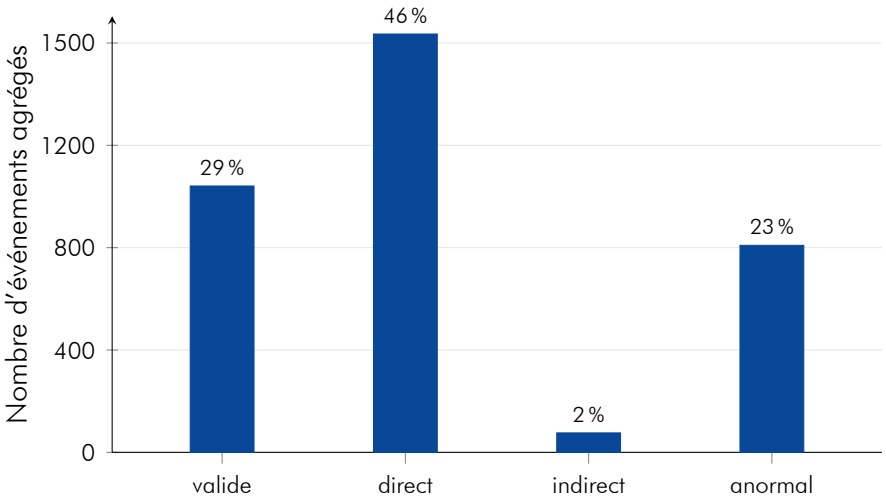

Figure 1.16 – Types des événements agrégés détectés en 2012

Durées des événements

Après agrégation, on passe de 6 057 288 événements uniques à 3561 événements agrégés, dont la figure 1.16 représente les types. Par rapport à la figure 1.15, il y a plus d'événements directs que d'événements valides. Ceci est dû au fait que les événements valides sont plus longs que les événements directs. Ainsi, 83 % des événements directs durent moins d'un mois, contre 43 % pour les événements valides. Un événement long agrégeant plus d'événements, le pourcentage des événements valides agrégés est inférieur à celui des événements uniques.

Les durées des événements s'étendent de quelques secondes à une année entière ; 61 % des événements durent cependant moins d'une semaine. Sur les 77 AS français cibles d'événements non valides, seuls 19 sont usurpés quotidiennement. Cela laisse croire que ces 19 AS n'ont pas correctement déclaré leurs objets `route`. Les 58 autres AS subissent des événements dont le nombre et la durée sont variables au cours de l'année 2012.

Identification des usurpations

Après agrégation, il reste 2520 événements non valides. Le tableau 1.2 présente le nombre d'événements agrégés obtenu en appliquant successivement, et de manière cumulative, les heuristiques précédemment définies page 31.

Filtre	Nombre d'AS ciblés	Nombre agrégé
1	67	809
2	67	788
3	40	579
4	16	179
5	12	63
6	8	48

Table 1.2 – Nombre d'événements agrégés après filtrage

Ces filtrages successifs permettent ainsi de limiter à 48 le nombre d'événements à analyser manuellement. Une première étude des événements après l'application des cinq premiers filtres met en évidence des annonces d'adresses IP d'interconnexions entre AS, qui ne devraient pas être visibles sur Internet. Le mercredi 5 septembre, durant une seule annonce BGP, un transitaire étranger important a ainsi annoncé des préfixes IPv6 /128 gérés par trois AS français. Le lundi 30 mai, pendant quelques heures, un autre transitaire étranger a annoncé des préfixes IPv4 /32 appartenant à un autre AS français.

Afin d'analyser le reste des événements, il semble nécessaire de bien connaître le marché de l'Internet français afin d'identifier correctement les usurpations. Certains événements anormaux peuvent en fait être légitimes. C'est ainsi le cas lorsqu'un AS délègue des préfixes à un autre AS de la même entité, lorsqu'une société en rachète une autre, et donc ses AS et ses préfixes, ou lorsqu'un AS demande à son transitaire ou à un prestataire d'annoncer ses préfixes pour limiter les effets d'un DDoS et pour le nettoyer.

Les objets `route` sont toutefois une bonne manière d'appréhender le marché. Ainsi, même si aucun objet `route` n'est déclaré pour une annonce particulière, le fait que d'autres objets `route` existent indique qu'il y a une relation entre les deux AS. Si une telle relation existe, on peut alors supposer que les événements anormaux sont en fait des défauts de déclaration. Parmi les événements étudiés, ces relations commerciales permettent d'éliminer un événement de 48 heures portant sur un préfixe IPv4 /24.

L'étude minutieuse des derniers événements semble indiquer que seuls sept événements anormaux sont en fait des usurpations de préfixes. Ces sept usurpations ont toutes comme caractéristiques de porter sur des préfixes IPv4 /24, d'être effectuées par des AS étrangers qui n'ont aucune activité commerciale en France, et de du-

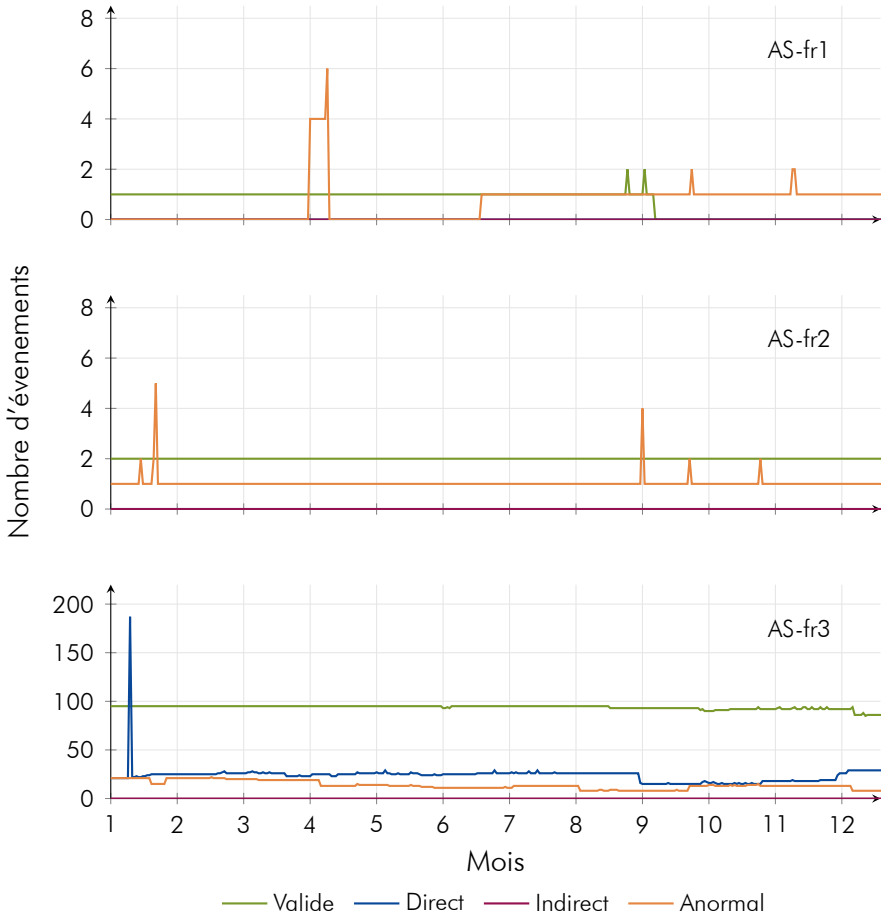

Figure 1.17 – Catégories d'événements pour les AS-fr1, AS-fr2 et AS-fr3

rer moins d'une journée. Certaines d'entre elles ont d'ailleurs été confirmées par les membres de l'observatoire.

Focus sur dix AS français

Sur les dix AS français que nous avons sélectionnés pour effectuer des analyses plus fines, huit sont cibles d'événements au cours de l'année 2012. Les figures 1.17, 1.18, et 1.19 représentent l'évolution des différentes catégories d'événements pour chacun de ces AS.

Pour l'AS-fr1, les événements valides s'arrêtent après le 11 septembre. La plupart sont effectués par le même AS. À l'inverse, des événements anormaux sont effectués quotidiennement à partir du 24 juin par un autre AS. Étant donné leurs durées, ces

événements sont probablement dus à des défauts de déclaration d'objet `route`. Du 3 au 11 avril, un autre AS annonce des préfixes plus spécifiques que ceux annoncés par l'AS-fr1.

Les événements concernant l'AS-fr2 évoluent peu au cours de l'année 2012. Les deux événements valides quotidiens correspondent à des préfixes délégués à un client. L'événement anormal quotidien correspond à un préfixe délégué à un fournisseur de service. La figure ne le représente pas, mais le 30 octobre, ce préfixe est attribué à un autre fournisseur de service. Les pics d'événements anormaux du mois de janvier correspondent à des annonces de préfixes IPv4 /32 et ceux du mois de septembre à l'annonce de préfixes IPv6 /128. Il s'agit vraisemblablement de la réannonce de préfixes d'interconnexion par l'un de ses transitaires étrangers. Le pic à la fin du mois de septembre correspond probablement à un test préparant le changement de fournisseur de service. Le pic du 29 octobre correspond quant à lui à l'annonce simultanée d'un préfixe par les deux fournisseurs de service avant d'être transféré de l'un vers l'autre.

L'AS-fr3 est la cible de beaucoup plus d'événements que les deux premiers car il gère beaucoup plus de préfixes. Étant donné le nombre d'événements, il est difficile d'en fournir une analyse détaillée. Certaines tendances se dégagent cependant. Ainsi, on observe une décroissance du nombre d'événements anormaux au cours de l'année 2012 [14]. De la même manière, on observe une décroissance des événements directs fin août et une augmentation début décembre. Nous n'avons pas d'explications pour ces deux phénomènes. Le pic survenu le 9 janvier 2012 correspond à des préfixes IPv4 /24 annoncés par un AS appartenant à la même société que l'AS-fr3. Il s'agit probablement d'une réannonce malencontreuse des routes internes.

Pour l'AS-fr4, une inversion du nombre d'événements valides et anormaux apparait en août 2012. Il s'agit en fait d'un changement de l'AS à l'origine des événements anormaux. À partir du 14 août, des annonces identiques sont faites par un autre AS. Il est intéressant de noter que les objets `route` existaient dès le début de l'année. Le 1er novembre 2012, on note un pic de 17 événements directs et de 12 événements indirects. Il s'agit d'annonces de plusieurs préfixes plus spécifiques par deux AS de la même entité que l'AS-fr4. Il n'existe pas d'objet `route` pour ces préfixes. Les cinq pics d'événements valides de la fin de l'année 2012 correspondent à des annonces de plusieurs préfixes effectuées par un AS appartenant à la même entité.

L'AS-fr5 est la cible d'événements anormaux jusqu'au 20 juin 2012. Jusqu'au 2 février, il y a deux événements anormaux. Il s'agit en fait d'une seule annonce d'un préfixe IPv6 /48. Deux préfixes IPv6, un /32 et un /40, étant annoncés par l'AS-fr5, deux événements anormaux sont comptabilisés. Après le 2 février, le préfixe /40 n'est

14. On passe de 21 événements en janvier à 8 en décembre.

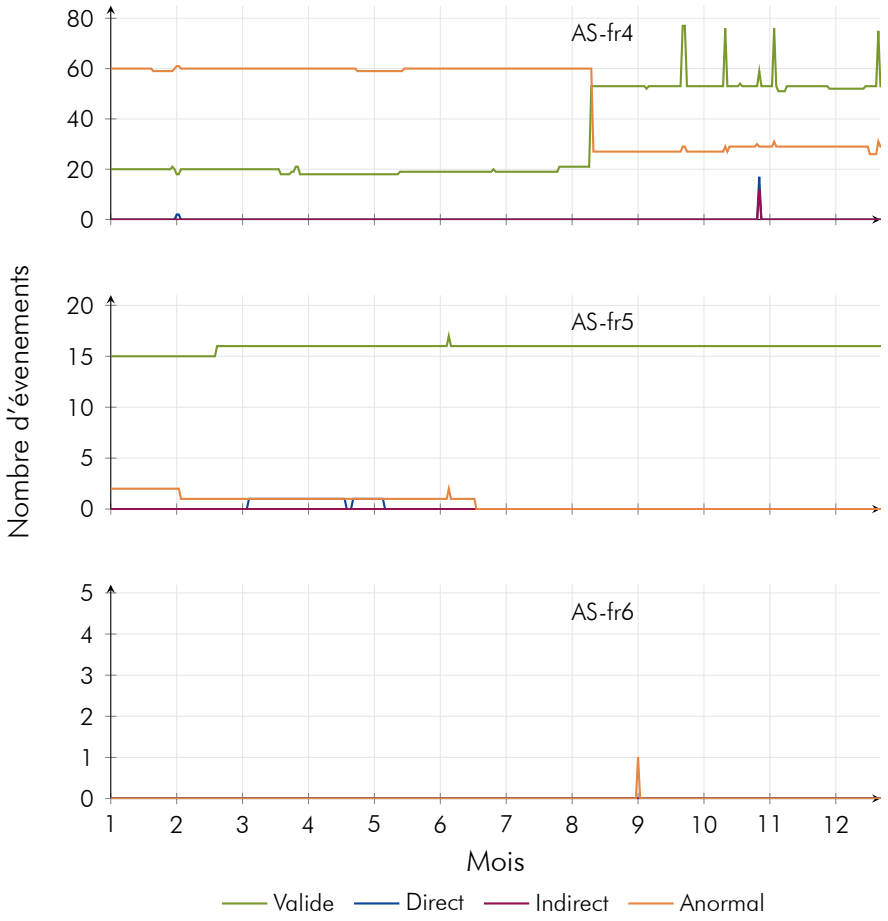

Figure 1.18 – Catégories d'événements pour les AS-fr4, AS-fr5 et AS-fr6

plus annoncé. Il est intéressant de noter que de mars à mai, l'annonce du préfixe IPv6 /48 est vue à la fois comme un événement normal et un événement direct, ce qui laisse à penser qu'il s'agit d'un défaut de déclaration. Le 7 juin, on voit un événement valide et un événement anormal de plus que le reste de l'année. Ces deux événements correspondent à l'annonce d'un préfixe IPv4 et d'un préfixe IPv6 par un autre AS. Un objet `route` portant sur un préfixe IPv4 est bien déclaré. Cependant, l'objet `route6` correspondant au préfixe IPv6 n'existe pas.

Un seul événement ponctuel a touché l'AS-fr6. Le 5 septembre, l'un de ses transitaires a annoncé des préfixes IPv6 /128 probablement utilisés dans le cadre d'une interconnexion BGP.

Peu de changements interviennent au cours de l'année 2012 pour l'AS-fr7. Le 25 juin, pendant quelques heures, plusieurs préfixes IPv4 /24 sont annoncés par un AS

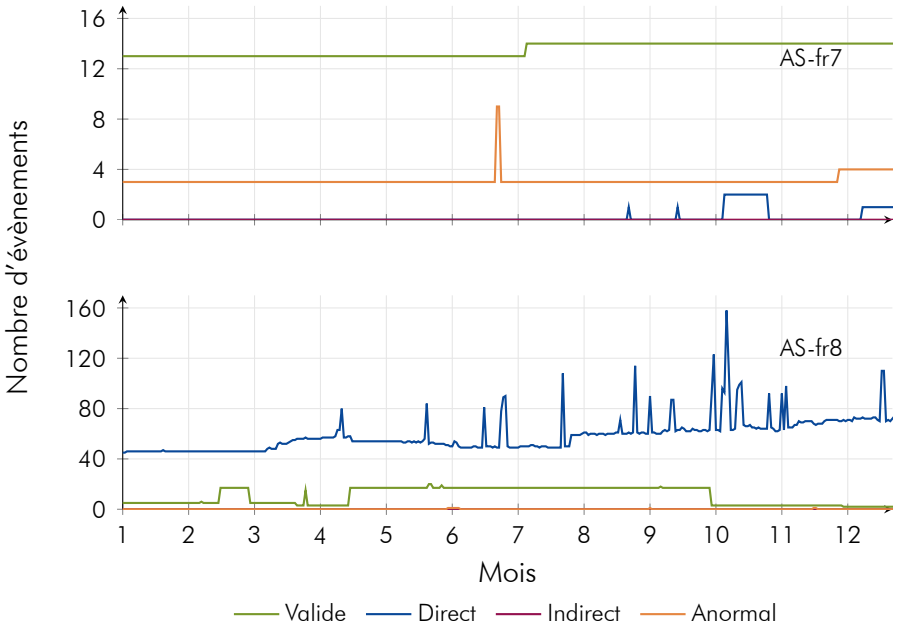

Figure 1.19 – Catégories d'événements pour les AS-fr7, et AS-fr8

étranger. Cet incident court pourrait être une usurpation de préfixes. Le 8 juillet, une nouvelle annonce de préfixes IPv4 /24 est effectuée par un AS partenaire, pour lequel des objets `route` existent déjà pour d'autres préfixes. Les événements directs du mois d'octobre correspondent à des événements anormaux perçus différemment par les collecteurs. Cela laisse donc à penser que les événements anormaux correspondant sont en fait des défauts de déclaration d'objets `route`.

L'AS-fr8 subit beaucoup plus d'événements directs que les sept autres AS étudiés. La plupart de ces événements sont des défauts de déclaration d'objets `route`. Trois événements anormaux ont eu lieu en 2012[15]. Ils concernent des AS sans relation avec l'AS-fr8 et portent sur des annonces ponctuelles de préfixes IPv4 /22 et /24. Il pourrait s'agir d'usurpations de préfixes. Un AS de la même entité que l'AS-fr8 est à l'origine des variations du nombre d'événements valides. Le 15 février, puis pendant quinze jours, le 27 mars, et à partir du 26 mai, il a annoncé 12 préfixes supplémentaires. Le 3 octobre, ce même AS a arrêté d'annoncer 14 préfixes.

15. Ils ne sont pas visibles sur la figure.

1.5 Cohérence des objets route

1.5.1 Description

Les objets `route` sont des informations essentielles permettant de s'assurer de la légitimité d'un AS à annoncer un préfixe donné sur Internet. Grâce à eux, des filtres peuvent être mis en place au niveau des interconnexions BGP, afin de bloquer les annonces illégitimes. Les déclarations d'objets `route` n'ont pas à être aussi précises que les préfixes qui sont annoncés. Par exemple, un opérateur qui obtient l'objet `inetnum` 198.18.0.0/15 peut déclarer l'objet `route` correspondant et annoncer sur Internet des préfixes plus spécifiques, par exemple 198.18.10.0/24.

La pénurie d'adresses IPv4, l'attribution de nouveaux blocs ou la réutilisation de blocs alloués historiquement à d'autres AS peuvent conduire à des incohérences dans les filtres mis en place sur les interconnexions BGP à partir des objets `route`. Si un AS restitue un bloc mais ne détruit pas l'objet `route` associé, alors d'un point de vue extérieur, cet opérateur peut toujours légitimement annoncer le préfixe. La suppression de reliquats dans les bases de données des IRR doit être systématique afin d'assurer une cohérence entre les déclarations et les préfixes annoncés sur Internet. De cette manière, les filtres basés sur les objets `route` peuvent rester cohérents avec les attributions des objets `inetnum`.

En pratique, une organisation peut retourner un objet `inetnum` inutilisé à son LIR, ou au RIR, afin qu'il soit délégué à un autre AS. Dans ce cas, les objets `route` correspondants ne sont plus corrects et doivent être supprimés. Si ce nettoyage n'est pas effectué, l'organisation ayant rendu l'objet `inetnum` pourrait réaliser une usurpation de préfixe qui ne serait pas bloquée par les filtres mis en place.

1.5.2 Méthodologie de mesure

Afin de mettre en évidence les objets `route` incorrects, une base de données a été créée pour nos besoins. Cette dernière a été alimentée quotidiennement avec les dépôts du serveur `whois` du RIPE-NCC. Les informations qui ont été extraites sont exclusivement les objets `route` déclarés par les AS français.

Chaque jour, après avoir alimenté cette base de données, les correspondances entre les objets `route` extraits sont comparées avec les préfixes annoncés, issus du collecteur londonien du RIS. À chaque itération, les objets `route` pour lesquels un préfixe exact ou plus spécifique est annoncé sont marqués comme utilisés. Lorsque toute l'année a été analysée, il suffit d'extraire les objets `route` pour lesquels aucun préfixe n'a été rencontré sur l'Internet pour les caractériser comme inutilisés, ce qui représente plus de 10 % des objets `route` sous des numéros d'AS français.

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`.
- **tous objets route utilisés** : tous les objets `route` déclarés par l'AS au RIPE-NCC sont utilisés par un ou plusieurs préfixes sur Internet ;
- **quelques objets route utilisés** : seule une partie des objets `route` déclarés a des préfixes en regard.

L'indicateur équivalent, dans le rapport précédent, intitulé « Comparaison des objets `route` avec la table de routage » comportait un biais dans le recoupement. En effet, les objets `route` étaient issus d'une archive du `whois` du RIPE-NCC datée du mois de novembre 2011 et amenaient une quantité négligeable de faux positifs dans les catégories retenues. Ce biais a été retiré en archivant quotidiennement les données et en confrontant les données de routage avec ces archives.

Limitations

Cette étude ne prend pas en compte l'importance d'un objet `route`, c'est-à-dire la taille du masque de sous-réseau. Dans le cas d'un filtrage basé sur les objets `route`, l'oubli d'un objet `route` avec une taille de masque de 16 bits rendra indisponible un plus grand nombre d'adresses IP que s'il est de taille 24 bits. Nous modifierons cet indicateur dans la prochaine version de ce rapport pour que la taille du masque de sous-réseau entre en compte dans les analyses.

1.5.3 Résultats et analyse

Résultats globaux

L'analyse des objets `route` sur l'ensemble de l'année montre qu'il y a peu de variation à l'échelle nationale sur l'ensemble des AS observés. C'est pour cette raison que nous ne présentons que les résultats agrégés au 31 décembre 2012 dans la figure 1.20.

Afin de refléter la réalité de l'Internet français, un filtre a été appliqué aux résultats bruts. Dans la partie gauche de la figure, la répartition des AS a été réalisée sur les 1270 AS français identifiés, tandis qu'à droite, seuls ont été pris en compte les AS français annonçant des préfixes au moment de la mesure. Grâce à ce filtre, la proportion d'AS français n'ayant aucun objet `route` déclaré passe de 39,7 % à 5,7 %, ce qui montre que le nombre d'opérateurs actifs n'ayant fait aucune déclaration est relativement faible.

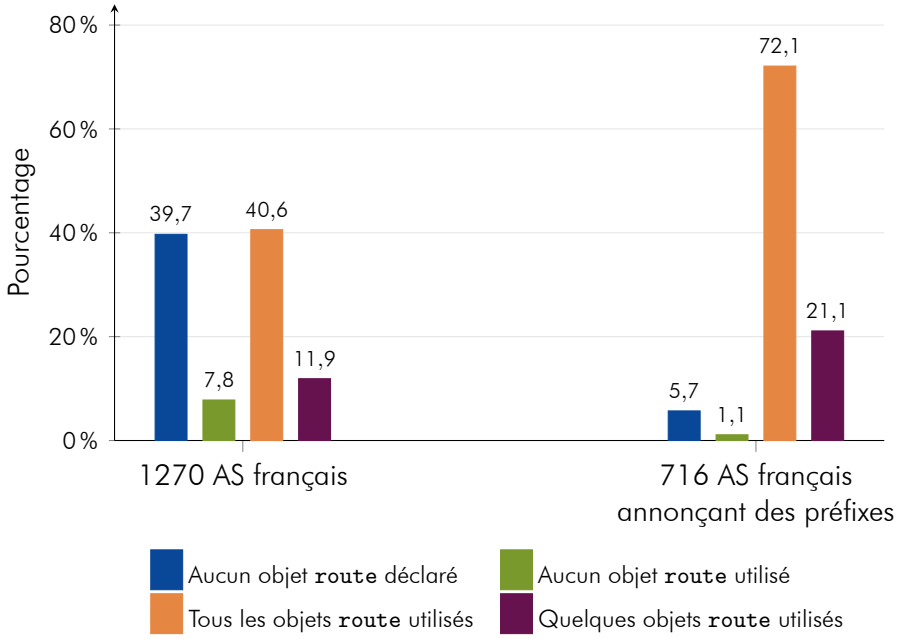

Figure 1.20 – Cohérence des objets `route` IPv4 au 31 décembre 2012

La quantité d'AS n'ayant aucun objet `route` utilisé varie peu au cours de l'année et représente 1,1 % des opérateurs recensés. Cette catégorie pourrait être aisément ramenée à 0 par des déclarations d'objets `route` systématiques.

Le pourcentage d'AS dont l'ensemble des objets `route` couvre des préfixes annoncés, passe de 40,6 % à 72,1 % après l'application du filtre. Ce résultat est particulièrement encourageant car près de trois opérateurs sur quatre ont une exploitation complète de leurs objets `route`.

Enfin, près de 21,1 % des AS ont une utilisation partielle des objets `route`, c'est-à-dire qu'un ou plusieurs objets `route` ne couvre jamais de préfixe. De plus, ce chiffre croît de manière linéaire au cours de l'année et pourrait donc continuer à augmenter pendant l'année 2013. Les résultats de l'année prochaine permettront de savoir si cette tendance se maintient.

La même analyse a été réalisée sur les objets `route6` portant sur les préfixes IPv6 et montre, après application du filtre, des résultats aux tendances similaires à IPv4, représentés par la figure 1.21.

L'intérêt du filtre consistant à ne représenter que les AS annonçant des préfixes IPv6 est ici bien plus important, car ce dernier ramène le nombre d'AS n'ayant aucun

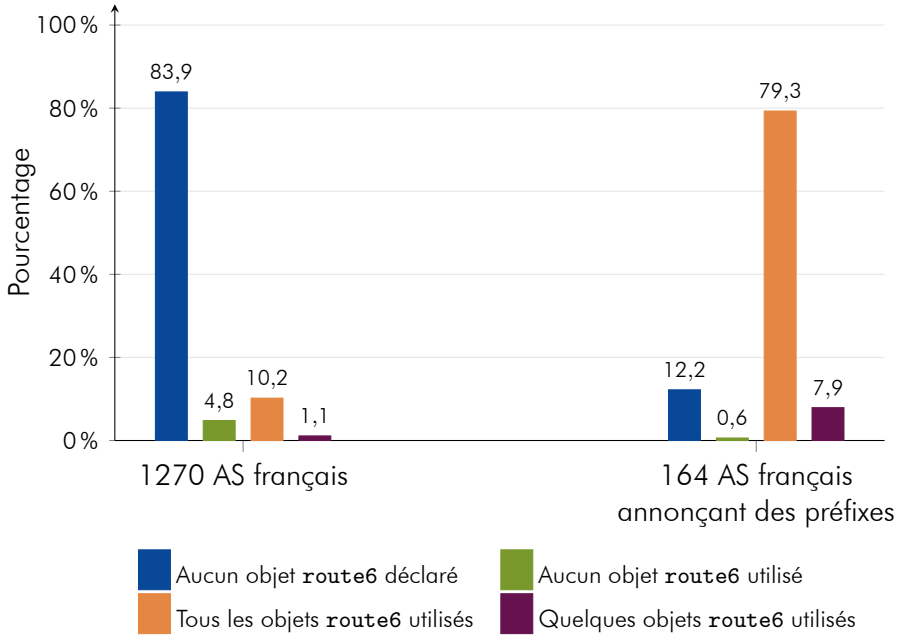

Figure 1.21 – Cohérence des objets `route6` IPv6 au 31 décembre 2012

objet `route6` de 83,9 % à 12,2 %. Cette catégorie, une fois filtrée, a une valeur bien inférieure qui met en évidence un non-respect des bonnes pratiques de déclarations qui est plus important sur IPv6 que sur IPv4.

Le nombre d'AS n'ayant aucun objet `route6` utilisé est très faible : 0,6 % des AS annonçant des préfixes IPv6. À l'inverse, près de 79,3 % des AS ont une utilisation totale des objets `route6`. L'effort de déclaration en IPv6, lorsqu'il est réalisé, est plus systématique qu'en IPv4.

Enfin, les opérateurs ayant une partie d'objets `route6` utilisés est de 7,9 %, ce qui peut être perçu comme un élément encourageant, mais aussi comme un point sur lequel il faut rester vigilant. En effet, IPv6 étant un protocole encore peu adopté, les reliquats de déclarations devraient être faibles. Cependant, ce chiffre est assez élevé en comparaison de la proportion des AS annonçant des préfixes IPv6.

Focus sur dix AS français

Par souci de simplicité, les résultats de l'analyse se résument en deux catégories au lieu des quatre du rapport portant sur l'année 2011 :

- **objet route utilisé** : au moins un préfixe inclus dans l'objet `route` existe

dans la table de routage globale ;

- **objet route inutilisé** : aucun préfixe inclus dans l'objet `route` n'est annoncé.

Seulement trois AS français voient leurs objets `route` évoluer durant l'année 2012. Pour deux d'entre eux, l'AS-fr1 et l'AS-fr6, le changement a été exclusivement une croissance du nombre d'objets `route` déclarés.

L'AS-fr1 a réalisé de nouvelles déclarations chaque trimestre, partant de 67 % d'objets `route` utilisés en début d'année, à 86 % au 31 décembre 2012. L'AS-fr6 a fait une modification des objets `route` déclarés une unique fois dans l'année, passant de 78 % d'objets `route` utilisés à 91 %. Cet AS a nettement amélioré ses déclarations d'objets `route` au cours de l'année.

Enfin, l'AS-fr9 a vu le nombre d'objets `route` évoluer tout au long de l'année de manière linéaire. Il s'est vu attribuer un certain nombre de nouveaux `inetnum` pour lesquels il a parfois réalisé les déclarations d'objets `route`. L'AS-fr9 avait 82 % de ses objets `route` utilisés par des préfixes au 1er janvier. Malgré une croissance de près de 50 % en nombre de préfixes annoncés, le pourcentage d'objets `route` utilisés est resté inchangé au 31 décembre, ce qui met en évidence que les déclarations ne sont pas faites de manière systématique.

Sur les dix AS français observés, neuf annoncent des routes en IPv6. Parmi les neuf AS, seuls trois ont vu leurs objets `route6` varier durant l'année 2012. En IPv6, les résultats montrent que, contrairement à IPv4, les déclarations ne s'améliorent pas au cours de l'année pour ces AS.

Tous les objets `route6` des six AS pour lesquels aucun changement n'intervient au cours de la mesure sont utilisés. En revanche, pour les trois AS subissant des modifications, le taux d'objets `route6` inutilisés augmente entre le 1er janvier et le 31 décembre 2012 :

- l'AS-fr6 passe de 0 % à 33 % ;
- l'AS-fr7 de 12 % à 24 % ;
- l'AS-fr9 de 0 % à 33 %.

Le focus sur l'IPv6 de cet indicateur montre que la suppression d'objet `route6` n'a pas plus lieu en IPv6 qu'en IPv4. En effet, seul l'ajout d'objet `route6` est considéré par les administrateurs des AS, comme étant nécessaire. Il est probable que les filtres qui sont ou seront mis en place entre les interconnexions BGP tendront à croître. De plus, ils pourraient contenir des informations erronées si la suppression d'objets `route` n'est jamais faite, d'où l'importance de tenir à jour ces déclarations.

1.6 Filtrage via les objets route

1.6.1 Description

Les objets `route` peuvent servir de base d'information dynamique pour la génération des filtres sur les interconnexions BGP. La correspondance entre les préfixes annoncés et les objets `route` déclarés est donc très importante. Il ne peut y avoir de filtrage efficace que si les déclarations englobent l'ensemble des préfixes qui seront annoncés par l'AS.

Nous nous sommes intéressés à l'étude de la précision des filtres qui seraient générés à partir des objets `route` déclarés par les 1270 AS français. Cet indicateur, dans le rapport 2011, s'intitulait « Comparaison des objets `route` avec la table de routage ».

1.6.2 Méthodologie de mesure

Une base de données a été mise en place et alimentée par les données issues du collecteur RIS de Londres. Chaque jour, l'ensemble des préfixes annoncés, ainsi que le numéro d'AS à l'origine de ces derniers sont stockés. Une fois la base de données renseignée, une comparaison est réalisée avec les informations contenues dans les archives quotidiennes du dépôt `whois` du RIPE-NCC. Chaque préfixe annoncé est alors comparé avec les objets `route` afin de rechercher une correspondance. Chacun des 1270 AS est placé dans l'une des catégories suivantes :

- **correspondance :** chaque annonce de l'AS est couverte par un objet `route` ;
- **conflit :** l'AS annonce au moins un préfixe qui a un objet `route` déclaré par un autre AS ;
- **objet route manquant :** l'AS annonce au moins un préfixe pour lequel aucun objet `route` n'existe.

Le focus sur les dix AS français utilise les mêmes catégories pour détailler le filtrage des préfixes IPv4 et IPv6 annoncés par chacun de ces dix AS.

1.6.3 Résultats et analyse

Résultats globaux

À la lecture du tableau 1.3, les résultats changent peu au cours de l'année. Le pourcentage d'AS pour lesquels il y a des correspondances totales entre l'ensemble des préfixes annoncés et les objets `route` déclarés est passé de 78 % à 82 % avec une augmentation du nombre d'AS présents.

Type	1er janvier 2012	31 décembre 2012
nombre d'AS actifs	681	716
correspondance	78 %	82 %
conflit	11 %	9 %
objet `route` manquant	11 %	9 %

Table 1.3 – Filtrage des préfixes IPv4 via les objets `route`

Type	1er janvier 2012	31 décembre 2012
nombre d'AS actifs	128	164
correspondance	82 %	82 %
conflit	14 %	12 %
objet `route6` manquant	4 %	6 %

Table 1.4 – Filtrage des préfixes IPv6 via les objets `route6`

Le taux d'AS en conflit diminue et passe de 11 % à 9 %. Il en va de même pour les AS dont au moins un objet `route` fait défaut. Des administrateurs ont opéré des déclarations d'objets `route`, améliorant la situation.

Ces résultats montrent que les AS français mettent à jour plus régulièrement leurs filtres et ont tendance à corriger les défauts de déclarations. Il subsiste encore une marge de progression importante, notamment en ce qui concerne les annonces de préfixes conflictuelles. Elles sont souvent réalisées par des AS clients d'un LIR qui délègue des préfixes sans faire les déclarations d'objets `route` auprès de son IRR.

Les résultats présentés dans le tableau 1.4 montrent que les comportements diffèrent légèrement en IPv6. Le taux d'AS pour lesquels il y a une correspondance totale des préfixes annoncés avec des objets `route6` reste à 82 % tout au long de l'année.

Comme c'est le cas pour IPv4, les AS en conflit en IPv6 diminuent au cours de l'année et passent de 14 % à 12 %. Un effort notable de déclarations par les nouveaux opérateurs explique que cette proportion diminue.

Enfin, pour les objets `route6` faisant défaut pour certains AS en IPv6, les résultats sont bien moins encourageants et montrent que même si une proportion importante des nouveaux acteurs semble faire une déclaration systématique des objets `route6`,

des AS qui opéraient de l'IPv6 en début d'année ont omis des déclarations d'objets `route6`.

Nous constatons que les bonnes pratiques de déclaration d'objets `route6` sont souvent respectées au moment de la mise en œuvre, mais que l'effort semble ne pas se maintenir dans le temps.

Focus sur dix AS français

En IPv4, l'indicateur montre des variations pour 5 AS sur 10 au cours de l'année. Trois d'entre eux ont régularisé leurs annonces assez rapidement, de l'ordre d'une dizaine de jours. Les variations observées pour les deux autres AS sont plus importantes.

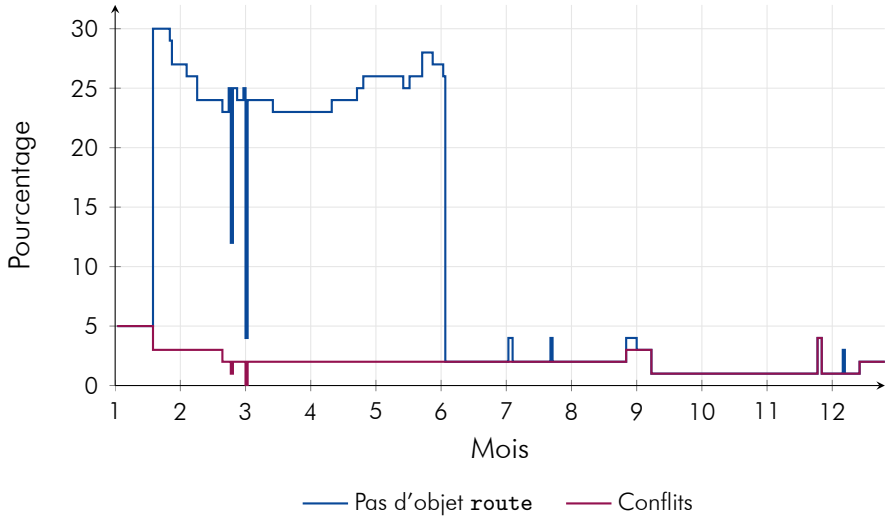

Figure 1.22 – Filtrage des préfixes IPv4 via les objets `route` pour AS-fr1

Comme le présente la figure 1.22, la correspondance entre annonces de préfixes par l'AS-fr1 et les objets `route` déclarés a subi de nombreuses variations au cours de l'année. L'AS-fr1 a reçu de nouveaux `inetnum` le 18 janvier 2012 et, une fois le découpage de préfixes réalisé, les a annoncés. Cependant, aucune déclaration d'objets `route` correspondant à ces annonces n'a été effectuée. Le 2 mars 2012, une forte désagrégation des préfixes a amené une chute du pourcentage de préfixes non couverts par des objets `route`. Une très grande partie des préfixes désagrégés étaient couverts par un même objet `route`. L'amélioration du pourcentage n'est donc pas due à des déclarations d'objets `route`, mais à une augmentation du nombre de préfixes couverts annoncés sur la journée. La plupart des objets `route` manquants sont déclarés à partir du 5 juin.

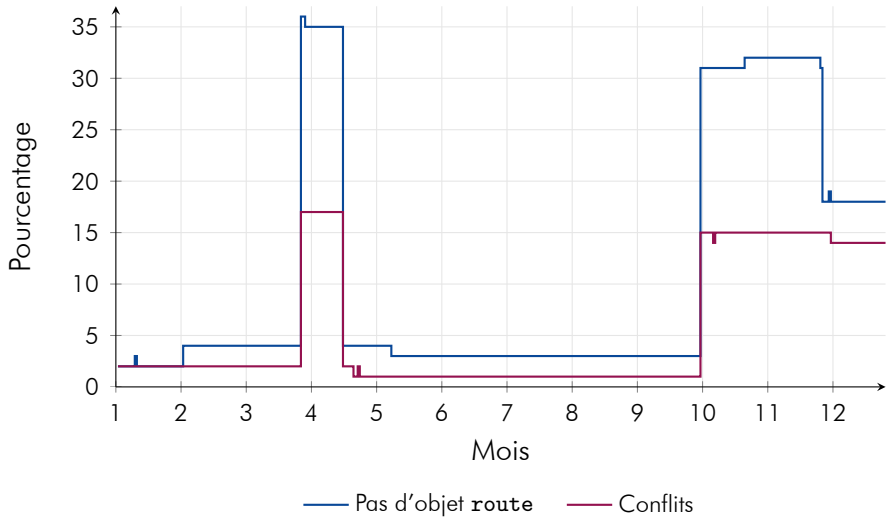

Figure 1.23 – Filtrage des préfixes IPv4 via les objets `route` pour AS-fr2

L'AS-fr2, dont l'évolution de l'indicateur est présentée sur la figure 1.23, a vu son nombre de préfixes non couverts par des objets `route` augmenter de manière significative à partir du 28 mars 2012. Cette augmentation provient d'une agrégation importante de ses préfixes. Les objets `route` déclarés étant plus spécifiques que les annonces effectuées après agrégation, il en résulte un nombre important de préfixes sans objets `route` dans nos résultats. Le 17 avril 2012, une désagrégation des préfixes ramène les pourcentages à des valeurs proches de celles du début de l'année. Cette désagrégation dure jusqu'au 4 septembre 2012 puis laisse place à une nouvelle agrégation des préfixes observée jusqu'à la fin de l'année.

En ce qui concerne l'IPv6, 9 AS sur 10 sont concernés par cet indicateur. Sept d'entre eux ont une correspondance quasi-parfaite entre les annonces et les déclarations d'objets `route`. En revanche, les deux autres AS se sont vu attribuer de nouveaux `inetnum` pour lesquels aucune déclaration n'a été effectuée.

1.7 Utilisation de la RPKI

1.7.1 Description

Aujourd'hui, aucun mécanisme interne à BGP ne permet de savoir si un AS a le droit d'annoncer un préfixe. Des travaux récents de l'IETF [16] ont conduit à la normalisation et à l'implémentation de deux technologies complémentaires permettant de filtrer automatiquement les annonces de préfixes :

- une infrastructure de gestion de clés permettant de vérifier qu'un AS est en droit d'annoncer un préfixe à l'aide d'une signature numérique : la RPKI [12] ;
- le protocole *RPKI to Router* [13], permettant d'exploiter la RPKI au niveau des routeurs.

Au sein de cette infrastructure, des objets permettent d'attester qu'un AS est en droit d'annoncer un préfixe : ce sont les `ROA` [17]. Les `ROA` sont des objets signés cryptographiquement listant les ressources détenues par un AS : le numéro d'AS et la liste des préfixes IP. Les `ROA` constituent donc, en quelque sorte, des objets `route` signés.

En comparaison des objets `route`, les `ROA` apportent une information supplémentaire : pour chaque préfixe déclaré, il est possible de préciser la longueur maximale que peut prendre son masque. Par exemple, si le préfixe est `198.18.0.0/15`, et que la longueur maximale du masque imposée est 20, l'AS ayant délivré le `ROA` ne peut annoncer que des préfixes du bloc `198.18.0.0/15` avec un masque compris entre 15 et 20 afin que ses annonces soient considérées comme valides.

Dans la RPKI, l'IANA constitue l'ancre de confiance, c'est-à-dire la racine de la chaîne de confiance. Dans la pratique, le RIPE-NCC dispose d'un certificat auto-signé, et constitue donc la racine de la chaîne de validation d'un `ROA`. Les RIR, comme le RIPE-NCC, délivrent à leurs membres, les LIR, des certificats attestant des ressources IP dont ils disposent. Les LIR sont des autorités de certification capables de générer les certificats nécessaires à la création des `ROA` [18].

Les `ROA` sont publiés dans des dépôts accessibles en ligne [15]. Les routeurs ne sont pas chargés de récupérer l'ensemble des `ROA` et de les valider : c'est le rôle des serveurs cache. La présence de ce nouvel élément de l'infrastructure permet de ne pas avoir besoin de ressources additionnelles pour les routeurs. Les serveurs cache communiquent les données des `ROA` validés (préfixes, longueurs maximales, AS origine) aux routeurs au moyen du protocole *RPKI to Router* [13].

16. Internet Engineering Task Force.
17. Route Origin Authorization.
18. Au sein de la RPKI, l'ensemble des certificats suit la norme X.509 [14].

Disposant de ces informations, un routeur peut examiner les annonces pour déterminer si elles sont valides. Ce processus peut avoir plusieurs issues :

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

Afin de donner un exemple d'exécution de ce processus, prenons le cas d'une organisation ayant créé un ROA pour l'AS 64496 et le préfixe 198.18.0.0/15, avec une longueur maximale de 17. L'AS 64496 annonce trois préfixes en BGP : 198.18.0.0/17, 198.18.128.0/24 et 203.0.113.0/24. Le ROA couvre la première annonce, qui est donc considérée comme valide. L'annonce du second préfixe est en revanche considérée comme invalide, la longueur maximale du masque du préfixe ayant été dépassée. Enfin, l'annonce du préfixe 203.0.113.0/24 n'est ni valide ni invalide : le ROA ne couvre pas le préfixe annoncé.

Après avoir examiné les annonces de préfixes, le routeur prend la décision de routage : il est possible de le configurer afin qu'il ne tienne pas compte des assertions fournies par les ROA. Ainsi, si on considère à nouveau l'exemple précédent, le routeur pourrait accepter les trois préfixes annoncés, bien qu'une seule annonce soit valide.

Enfin, il convient de préciser que les ROA n'apportent aucune garantie sur l'intégrité d'un chemin d'AS. En effet, les ROA permettent seulement de vérifier qu'un AS est autorisé à annoncer un préfixe. Malgré son périmètre d'action restreint, l'introduction de la RPKI constitue néanmoins une première étape vers la sécurisation des annonces BGP. L'étape suivante consiste à protéger la totalité du chemin d'AS, ce qui fait l'objet de travaux en cours à l'IETF [16], en particulier avec la définition du protocole BGPSEC [17].

1.7.2 Méthodologie de mesure

Afin de mesurer l'évolution de l'utilisation de la RPKI par les AS français, les données du dépôt maintenu par le RIPE-NCC ont été récupérées quotidiennement depuis le mois de septembre. Pour chaque mois depuis septembre 2012, 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 ;

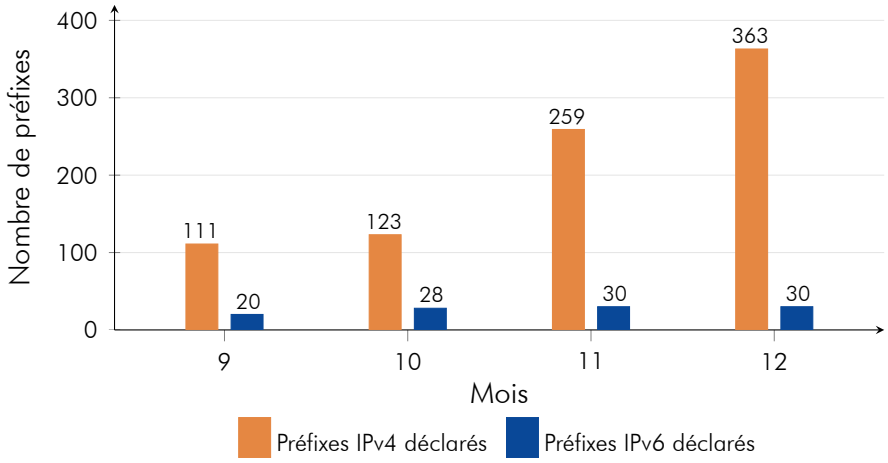

Figure 1.24 – Évolution du nombre de préfixes déclarés

- **le nombre de préfixes IPv4 et IPv6 déclarés par ces AS**, c'est-à-dire le nombre de préfixes déclarés dans les ROA publiés ;
- **le pourcentage d'annonces de préfixes par les 1270 AS français qui sont considérées comme valides au regard de la RPKI**.

Limitations

Les relevés effectués 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 dans le filtrage des annonces de préfixes. Les indicateurs présentés précédemment ne reflètent donc pas l'utilisation réelle de la RPKI par les AS français.

1.7.3 Résultats et analyse

Parmi les 1270 AS français, nous observons que seule une trentaine d'entre eux a publié des ROA durant l'année 2012. Depuis le début des mesures, en septembre 2012, ce nombre augmente jusqu'à atteindre 36 AS fin décembre 2012. Une analyse manuelle a permis de déterminer que la plupart de ces AS sont des opérateurs ou des hébergeurs.

La figure 1.24 donne l'évolution du nombre de préfixes IPv4 et IPv6 déclarés dans les ROA depuis septembre 2012. Ce nombre augmente en IPv4 comme en IPv6, l'augmentation la plus remarquable concernant les préfixes IPv4. En outre, il faut noter que la répartition du nombre de préfixes déclarés parmi les AS participants à

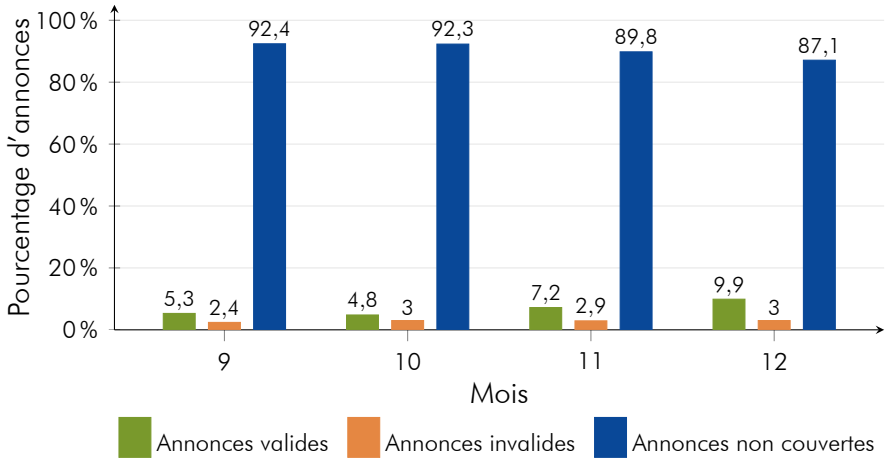

Figure 1.25 – Évolution de la validité des annonces des AS français

la RPKI n'est pas homogène : en décembre 2012, un AS concentre à lui seul un peu moins de trois-quarts des préfixes déclarés.

La figure 1.25 montre l'évolution de la validité des annonces faites par les 1270 AS français depuis septembre 2012 au regard de la RPKI [19]. Malgré une augmentation du nombre d'annonces valides au cours du temps, on constate que celui-ci reste faible : un peu moins de 10 % des préfixes annoncés fin décembre 2012. En conséquence, un filtrage strict [20] effectué sur la base des `ROA` entraînerait le rejet d'un peu plus de 90 % des annonces pour la même période. On peut également constater que le pourcentage d'annonces invalides est presque constant sur la période d'observation : il atteint les 3 % en décembre 2012. Ce pourcentage, bien que faible, représente tout de même un tiers des annonces valides. Parmi les annonces invalides observées, un fort pourcentage est constitué d'annonces provenant d'AS non autorisés. Une analyse manuelle, possible en raison du faible nombre d'annonces à traiter, permet de déterminer que seul un nombre très faible d'entre elles peuvent être considérées comme des usurpations. Les autres annonces sont valides au regard des objets `route`, ou constituent des événements directs, d'après la classification établie précédemment dans ce rapport (section 1.4).

Focus sur 10 AS français

L'utilisation de la RPKI reste aujourd'hui marginale : à la fin du mois de décembre

19. En raisons des arrondis, la somme des valeurs données pour chaque mois peut ne pas être 100.
20. Nous considérons qu'un filtrage « strict » ne conserve que les annonces considérées comme valides par le processus de validation à l'aide des `ROA`.

2012, seuls 36 AS sur les 1270 AS français y participent. Parmi les dix AS étudiés plus en détails, seuls 4 AS participent à la RPKI, et un AS concentre à lui seul la grande majorité des préfixes déclarés dans les ROA.

1.8 Déploiement d'IPv6 et respect des bonnes pratiques BGP

1.8.1 Description

Sous l'angle du protocole BGP, il est très facile de caractériser les comportements des AS français en utilisant directement les archives de tables de routage du projet RIS. Avec cet indicateur, nous cherchons à étudier, sur la durée, l'adoption du protocole IPv6 ainsi que les bonnes pratiques d'interconnexion BGP. Ces dernières consistent à respecter les limites de longueur des masques des préfixes fixées par le RIPE-NCC à 24 bits pour IPv4 [18], et à 48 bits pour IPv6 [19], ainsi qu'à supprimer les numéros d'AS privés dans les `AS_PATH`.

Il ne s'agit pas d'un nouvel indicateur de résilience, cependant il permet d'appréhender, sur plusieurs années, la maturité des déploiements du protocole IPv6, et l'utilisation des bonnes pratiques d'ingénierie du protocole BGP.

1.8.2 Méthodologie de mesure

Afin de comptabiliser le nombre d'AS français annonçant des préfixes IPv6, nous utilisons les archives BGP du 31 décembre à 16h00 pour les années de 2009, 2010, 2011 et 2012. Pour chacun des 1270 AS français, nous extrayons à la fois les préfixes IPv4 et IPv6 qu'ils annoncent. Cela nous permet d'étudier l'évolution de l'utilisation du protocole IPv6 à travers le nombre d'AS français effectuant des annonces en IPv6.

En ce qui concerne le respect des bonnes pratiques BGP, les annonces de préfixes IPv4 et IPv6 et les `AS_PATH` sont de plus observées sur l'ensemble de l'année 2012. De plus, pour les analyses de préfixes, seules les annonces dont l'`AS_PATH` est supérieur ou égal à 2 sont prises en compte. Ceci permet de ne pas comptabiliser les préfixes échangés au travers d'interconnexion de peering.

Limitations

La liste des AS français ayant été établie en juillet 2012, son utilisation pour analyser des données anciennes comporte des limites. Par exemple, un AS créé en juillet 2010 est présent dans la liste mais ne sera pas visible dans les annonces de préfixes avant cette date.

Des événements survenant au cours d'une année ne sont pas tous nécessairement visibles au 31 décembre de chaque année. Cependant, cette étude sur le long terme permet de faire ressortir des tendances générales.

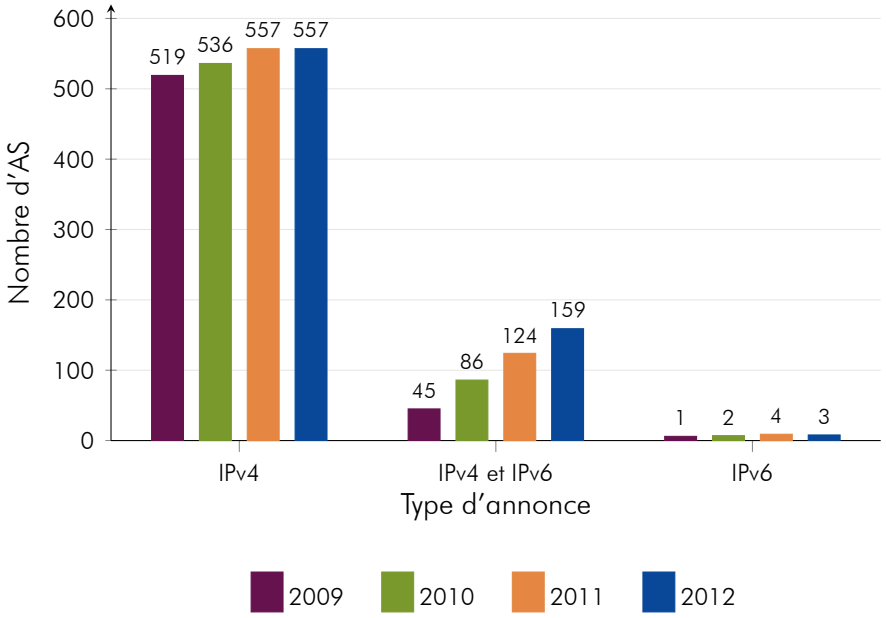

Figure 1.26 – AS français effectuant des annonces en IPv6

1.8.3 Résultats et analyse

Déploiement d'IPv6

La figure 1.26 représente l'évolution du nombre d'AS français effectuant des annonces en IPv6, et à titre de comparaison en IPv4, entre 2009 et 2012. Ce nombre augmente à un rythme régulier : près de 40 nouveaux AS par an font des annonces en IPv6. Il n'y a quasiment pas d'AS ne faisant que de l'IPv6 et cela n'a pas évolué depuis 2009.

Malgré la croissance du nombre d'AS effectuant des annonces en IPv6, les résultats montrent qu'IPv6 n'a pas encore été massivement adopté par les AS français. Cette tendance se retrouve également dans les offres des fournisseurs d'accès : aujourd'hui, il existe très peu d'offres permettant d'obtenir une connectivité IPv6.

Respect des bonnes pratiques

L'analyse des annonces de préfixes effectuées au cours de l'année 2012 montre que 43 préfixes IPv6 d'une longueur supérieure à 48 bits sont annoncés par des AS français. D'autre part, 5 préfixes IPv4 d'une longueur supérieure à la longueur maximale recommandée sont également annoncés sur Internet.

Le nombre de préfixes IPv6 dans la table de routage globale étant bien plus faible que le nombre de préfixes IPv4, cela laisse à penser que les bonnes pratiques de filtrage sont beaucoup moins suivies en IPv6 qu'en IPv4 par les AS français.

L'adoption lente de l'IPv6 par les AS français et l'observation de la qualité des annonces effectuées soulèvent des questions quant à la maitrise de ce protocole par l'ensemble des acteurs de l'Internet français. De plus, bien qu'IPv6 ait été défini en décembre 1995 [20], les nombreux avis de sécurité relatifs à IPv6 et à son usage appellent à la vigilance quant à la qualité de son implémentation dans les équipements et logiciels.

Enfin, nous observons que certains AS français ne retirent pas les numéros d'AS privés de leurs clients, ce qui conduit à la propagation d'annonces de préfixes avec un `AS_PATH` incorrect.

Focus sur dix AS français

L'étude minutieuse des dix AS français ne fait pas ressortir de faits majeurs. En 2009, 7 AS faisaient déjà de l'IPv6. Dès 2010, 9 des dix AS étudiés utilisent IPv6. Ce nombre n'a pas évolué en 2011 et 2012. Enfin, entre 2009 et 2012, aucun des dix AS français étudiés dans ce rapport n'effectue que des annonces de préfixes IPv6.

En ce qui concerne l'application des bonnes pratiques, le constat est le même : aucun fait remarquable ne se dégage de l'étude menée sur les dix AS français retenus. Ces dix AS semblent donc bien respecter les bonnes pratiques.

1.9 Conclusion et perspectives

En comparaison avec le rapport 2011, cette nouvelle édition décrit de nouveaux indicateurs concernant le protocole BGP, et élargit la portée de l'étude de 4 à 1270 AS français. Ces deux améliorations correspondent aux objectifs fixés lors du dernier rapport, et fournissent une meilleure compréhension de l'Internet français.

Les nouveaux indicateurs portant sur la RPKI et le protocole IPv6 permettent de poser les bases de l'étude de ces technologies. À l'avenir, ils pourront notamment nous aider à comprendre si elles sont adoptées, ou à l'inverse si elles ne sont pas utilisées. Concernant le protocole IPv6, tous les indicateurs montrent qu'il est peu déployé, et que les bonnes pratiques le concernant sont peu suivies. Tout comme dans le rapport 2011, cette constatation soulève la question de la maturité des déploiements et des implémentations du protocole.

Nous avons également étudié la structure de l'Internet afin d'évaluer la connectivité des AS français. Cette vision ne prend pas en compte les relations de peering mais permet toutefois d'appréhender la dépendance de l'Internet français vis-à-vis d'AS étrangers. Ainsi, nous avons identifié 81 AS pivots, parmi lesquels 34 étrangers, dont l'absence perturberait l'Internet français. Cependant, seule l'indisponibilité de 8 d'entre eux aurait un impact lourd.

Les objets `route` décrits en détail dans l'introduction ont été le centre de l'étude de deux indicateurs. Ils visent à étudier la qualité des déclarations sous deux angles différents.
Nos résultats ont tout d'abord montré que la base `whois` du RIPE-NCC contient un nombre important d'objets `route` obsolètes qui ne correspondent pas aux annonces de préfixes effectuées en BGP. Une campagne de nettoyage est donc nécessaire afin de remédier à ce problème et ainsi utiliser des filtres de bonne qualité.
Dans un second temps, nous avons mis en évidence que près de 10 % des annonces de préfixes effectuées par les AS français seraient rejetées si des filtres stricts étaient utilisés. Ce phénomène est fortement accentué par les politiques d'agrégation et de désagrégation de préfixes mises en place par les opérateurs. Il s'agit d'un résultat fort qui montre que les bonnes pratiques de filtrage ne sont pas largement appliquées.

Concernant l'observation des usurpations de préfixes, la méthodologie a été entièrement revue pour ce rapport afin d'affiner les résultats. Nous utilisons désormais la notion d'*événements* pour qualifier les annonces de préfixes faites par plusieurs AS simultanément. Nos analyses montrent tout d'abord que 58 % de ces événements sont valides au sens des objets `route`, et que 22 % sont probablement dus à des défauts de déclarations d'objets `route`. Les 20 % d'événements anormaux mettent en évidence des erreurs ponctuelles de configuration d'équipements, des réannonces

de préfixes d'interconnexions, et quelques usurpations dont les durées varient. Cela confirme l'importance de la déclaration des objets `route` pour faciliter la détection des usurpations.

Finalement, nous avons cherché à étudier si les bonnes pratiques d'ingénierie BGP étaient respectées par les 1270 AS français. Les résultats sont mitigés car ils mettent en évidence que ces bonnes pratiques ne sont pas systématiquement mises en place. En effet, des annonces contenant des préfixes de mauvaises tailles et des numéros d'AS privés ont été vues au cours de l'année 2012.
Tout comme la déclaration et la mise à jour des objets `route`, l'application des bonnes pratiques BGP doit être systématisée.

Les résultats présentés dans ce rapport constituent une extension importante du rapport 2011. En effet, nous avons défini des nouveaux indicateurs, tout en augmentant très nettement le nombre d'AS français étudiés. Différents axes d'amélioration existent et seront développés par l'observatoire dans la prochaine édition du rapport.

En ce qui concerne la connectivité, il paraît indispensable de prendre en compte la nature des liens entre AS (transit ou peering). Il serait notamment intéressant d'utiliser les informations présentes dans les bases `whois` pour améliorer notre compréhension des relations de peering, et des méthodes d'inférence de liens décrites dans la littérature scientifique [21, 22].

Les travaux concernant les objets `route` et la RPKI pourraient être menés conjointement, notamment en ce qui concerne la cohérence de ces bases vis-à-vis des préfixes annoncés en BGP. Par ailleurs, il conviendrait de prendre en compte le nombre d'adresses IP affectées par des filtrages, et non le nombre de préfixes, afin d'obtenir des analyses plus précises.

En dernier lieu, l'étude des usurpations effectuées contre des AS français se doit d'être automatisée afin de s'affranchir des analyses manuelles. Différentes méthodes complémentaires peuvent ainsi être mises en place comme l'étude des changements d'`AS_PATH` et des relations inter-AS telles que définies par l'état de l'art [10, 11].

Chapitre 2

Résilience sous l'angle de l'infrastructure DNS

2.1 Introduction

Le système de noms de domaine, géré par le protocole DNS [23] [24], est un système de nommage distribué et hiérarchique dont les deux objectifs essentiels sont d'associer à une adresse IP un nom lisible par les utilisateurs et, surtout, 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` .

En effet, l'adresse IP, dans la majorité des cas, dépend du FAI [1]. Si on n'utilisait que les adresses IP, un changement d'hébergeur impliquerait de prévenir tous les utilisateurs, pour les informer de la nouvelle adresse. Le DNS permet au contraire de garder un identificateur stable. Dans le cas d'un changement d'hébergeur, seul le responsable du domaine devra modifier l'adresse IP pointée par le nom. Avec le DNS, ce changement sera 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 « . ». Elle se situe à droite du nom `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. Si l'on considère les caractéristiques d'un nœud DNS uniquement à son niveau hiérarchique, c'est-à-dire, sans se préoccuper des éventuels sous-domaines qui en dérivent, on parle dans ce cas de zone DNS. Ce rapport ne tient pas compte de la différence subtile entre domaine (toute une arborescence à partir d'un nœud) et zone (seule la portion administrative autour de ce nœud). Par conséquent, ces deux termes seront désormais employés ici comme synonymes.

Une zone est dite *déléguée* lorsque sa gestion a été donnée à un autre organisme que celui gère sa zone parente. Une zone déléguée peut alors gérer ses ressources

1. Fournisseur d'Accès à Internet.

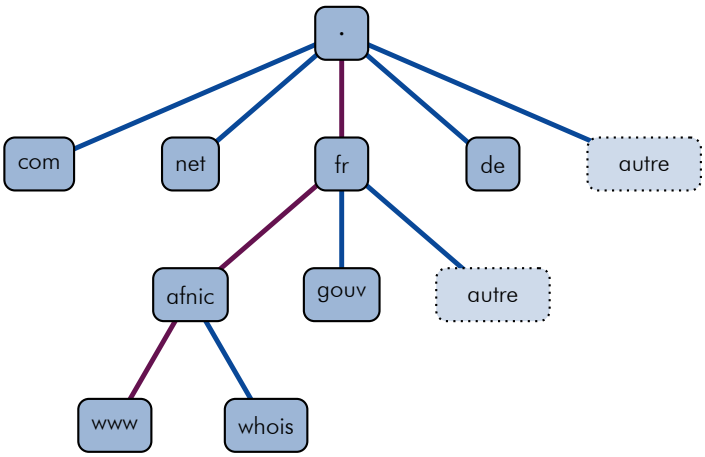

Figure 2.1 – Structure du DNS

indépendamment de sa zone parente. Ainsi, 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 [2].

Pour chaque zone DNS, un ensemble de serveurs DNS permet de décrire les ressources qui lui sont directement attachées, ainsi que les éventuelles délégations directement au niveau en-dessous (zones déléguées). De tels serveurs sont appelés serveurs DNS faisant autorité sur une zone. Les ressources attachées à une zone sont décrites au niveau des serveurs DNS faisant autorité par ce qu'on appelle des « enregistrements DNS » qui permettent de définir le type des ressources et leurs caractéristiques propres. Dans le cas d'une zone déléguée, la zone parente indique les serveurs DNS de la zone déléguée permettant ainsi aux administrateurs de celle-ci de gérer leurs ressources sans intervention de la part des administrateurs de la zone parente.

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

- **un serveur récursif** (encore appelé serveur cache ou résolveur). C'est un serveur que la machine de l'utilisateur connaît et à qui elle soumet sa requête DNS [3] (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 déléga-

2. Internet Corporation for Assigned Names and Numbers.

3. Dans cet exemple de requête DNS, `IN A` signifie qu'on cherche le type d'adresse IPv4 dans la classe `IN` (Internet).

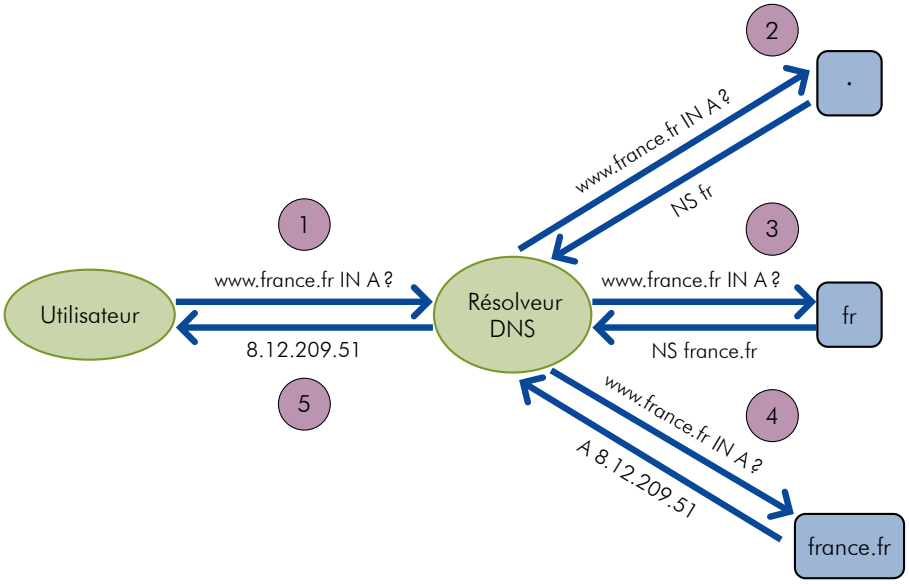

Figure 2.2 – Résolution DNS

tion [4] 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 utilisateur (interaction 5) et garde en même temps en mémoire (fonction « 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 s'ils font effectivement autorité pour le nom de domaine demandé par la machine utilisateur, en lui retournant la réponse, soit en l'aiguillant vers d'autres serveurs à interroger faisant autorité et qui pourraient alors lui donner une meilleure réponse. Les serveurs faisant autorité sont généralement configurés volontairement sans la fonction cache : ils ne répondent qu'avec des données provenant de leur propre base de données.

Il est à noter que de la même manière que l'on associe une adresse IP à une ressource désignée par un nom de domaine, on peut retrouver le nom de domaine associé à une adresse IP donnée. Cela est possible si l'adresse IP, et les délégations asscociées, ont été déclarées au niveau de l'arborescence `in-addr.arpa.` qui est la racine sous laquelle les adresses IPv4 sont déclarées. La résolution DNS qui permet de retrouver le nom de domaine associé à une adresse IP, le fait en demandant les enregistrements DNS de type `PTR` rattachés à l'adresse IP. Cette résolution s'appelle « résolution inverse ».

4. La réponse `NS` indique une liste de serveurs de noms (« Name Server »).

Le DNS et l'anycast

Au début des années 2000, certains opérateurs de serveurs DNS de la racine ont employé l'*anycast*, qui avait été testée initialement sur les serveurs de l'AS 112. Cet AS a été mis en place afin de rediriger vers des trous noirs le trafic important généré par des requêtes DNS illégitimes concernant des adresses IP privées, et soulager ainsi les serveurs DNS faisant autorité pour `in-addr.arpa.` [25]. L'*anycast* a ainsi permis de rapprocher les serveurs de la racine d'emplacements mal desservis jusque-là par les treize serveurs originels [5] et cela sans augmenter la taille des paquets DNS.

Notons que l'*anycast* n'est pas réservée au seul service DNS. Elle est également utilisée pour d'autres services pour lesquels redondance et proximité sont souhaitées. C'est le cas par exemple pour les CDN [6] [26] qui permettent de rapprocher de l'utilisateur le contenu d'un fournisseur au travers d'un service web.

Depuis, cette technique s'est largement démocratisée dans le secteur du DNS : elle est pratiquement déployée sur l'ensemble des serveurs de la racine : sur les 13 serveurs, 11 sont anycastés [27]. Elle est également largement utilisée par des opérateurs DNS de premier niveau, tels que l'Afnic, qui voient en elle un moyen d'améliorer simultanément plusieurs paramètres de performances du service DNS. En effet, cela permet à la fois de diminuer la latence du réseau lors de la résolution DNS et d'augmenter la résilience de ce service en offrant - grâce à une meilleure redondance - une meilleure répartition de charge, limitant ainsi les effets d'éventuelles attaques par déni de service. L'adoption de cette technique a été facilitée par l'émergence de nouveaux acteurs économiques : les fournisseurs de service *anycast*.

La technique en elle-même est simple, mais elle requiert beaucoup d'attention dans sa gestion quotidienne [28]. L'*anycast* repose sur une technique d'adressage et de routage qui permet d'envoyer les paquets vers la machine la plus proche au sens de la politique et de la topologie du réseau.

Un serveur DNS anycasté est en réalité un ensemble de machines appelées nœuds ou instances formant un réseau ou nuage *anycast*. Elles sont réparties physiquement et topologiquement à différents endroits de l'Internet. La particularité de ces instances est qu'elles partagent toutes la même adresse IP. De plus, cette adresse est généralement annoncée à partir du même AS [7] grâce au protocole BGP (voir chapitre 1). Les routeurs BGP auxquels les instances du serveur sont attachées vont alors propager cette annonce dans l'Internet. L'annonce aura donc pour origine différents points du réseau. À partir de là, l'algorithme de sélection de route de BGP décidera de

5. Ils sont identifiés par les 13 noms de `a.root-servers.net` à `m.root-servers.net`.
6. Content Delivery Network.
7. Le RFC 6382 décrit l'utilisation d'un numéro d'AS par instance.

l'acheminement des paquets.

L'*anycast* distingue deux types de nœuds : des *nœuds globaux* dont l'adresse a été diffusée de manière globale sans restriction et qui sont capables de répondre à un trafic élevé et des *nœuds locaux* dont l'adresse n'a été diffusée qu'aux systèmes autonomes pairs adjacents aux nœuds en question [8] et qui sont mis en place afin d'offrir le service à une population locale restreinte. Par exemple, l'instance située à la Réunion du serveur DNS `d.nic.fr`, serveur faisant autorité pour la zone `.fr`, est un nœud local. À l'inverse, les instances situés à Lyon et Paris sont des nœuds globaux.

Prenons maintenant le point de vue d'un résolveur DNS marseillais, comme illustré dans la figure 2.3. Celui-ci envoie une requête à l'adresse IP du serveur DNS `2001:678:c::1`. La requête est alors routée, grâce à BGP, vers le nœud lyonnais qui est le plus proche au sens de la métrique du routage. De fait, l'*anycast* apporte de la résilience. En cas de défaillance de ce nœud, le trafic est redirigé, après mise à jour des tables de routage, vers d'autres nœuds du nuage *anycast*. Dans la figure, il s'agit du nœud parisien.

Les nœuds *anycast* possèdent généralement deux interfaces réseau, l'une, dite « interface de service », est réservée à l'adresse IP anycastée, tandis que l'autre, dite « interface d'administration », est associée à une adresse IP unicast standard et permet à l'administrateur DNS d'accéder à la machine pour gérer le service. C'est d'ailleurs à travers cette adresse IP unicast que se fait la synchronisation des données, notamment les transferts de zone entre les serveurs faisant autorité.

Les attaques par déni de service ont peu d'impact lorsqu'elles sont lancées à partir d'une seule origine puisque le trafic est alors dirigé vers le nœud le plus proche de l'attaquant, les autres nœuds restant accessibles normalement. Lorsque l'attaque est distribuée, le trafic généré par celle-ci est réparti sur plusieurs nœuds *anycast* et la charge supplémentaire induite sur chacune des instances touchées est de fait inférieure à celle que recevrait un nœud si le service n'était pas anycasté [29].

2.1.1 Objectifs de ce chapitre

Nous avons défini cinq indicateurs de résilience en lien avec le protocole DNS : quatre indicateurs du rapport 2011 de l'observatoire et un nouvel indicateur. Il s'agit de :

1. la dispersion des serveurs de noms au niveau réseau ;
2. le nombre de serveurs DNS vulnérables à la faille dite « Kaminsky » ;
3. l'état du déploiement du protocole IPv6 ;
4. l'état du déploiement de DNSSEC ;

8. On peut utiliser la communauté `NO_EXPORT` de BGP par exemple.

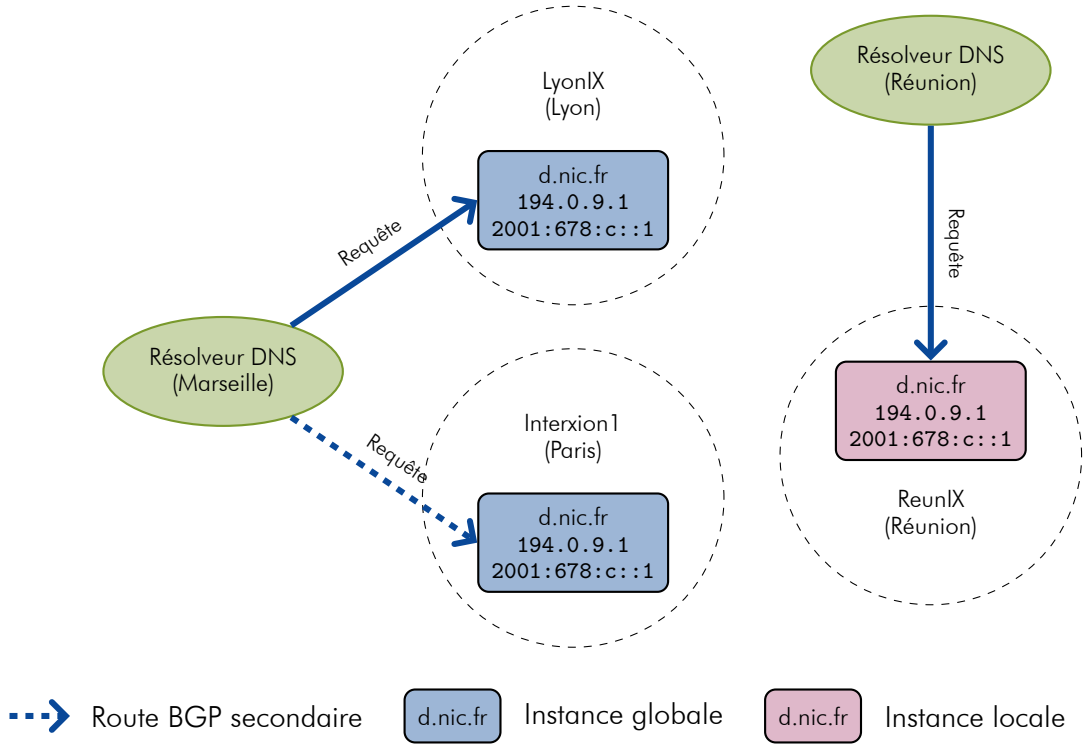

Figure 2.3 – Exemple de résolution DNS avec de l'*anycast*

5. les résolveurs DNS les plus demandeurs.

2.1.2 Plateforme, outils et données utilisés

Pour mesurer ces différents indicateurs, nous utilisons `DNSwitness` [30], plateforme générique développée par l'Afnic permettant de réaliser des mesures via le DNS. Cette plateforme est multiusage 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.

`DNSwitness` a deux composantes :

- `DNSdelve`, pour les mesures actives ;
- `DNSmezzo`, pour les mesures passives.

DNSdelve

`DNSdelve` 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 lui-même plusieurs modules spécialisés que l'on peut utiliser de manière indépendante. Pour les besoins de l'observatoire, nous en utilisons deux.

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. `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*.

`DNSmezzo` nous permet d'alimenter les indicateurs relatifs à la progression d'IPv6, aux serveurs DNS non corrigés vis-à-vis de la faille « Kaminsky » et aux résolveurs les plus demandeurs.

Données utilisées

Toutes les mesures actives ont été faites en utilisant la zone `.fr`. Il faut se rappeler que `.fr` n'est pas toute la France. D'une part, des titulaires de noms de domaine établis en France peuvent utiliser des domaines de premier niveau autres que `.fr` (par exemple, `.com`, `.net`, ou `.org`), et de l'autre, des acteurs établis en dehors de la France peuvent choisir des noms de domaine en `.fr`[9].

La zone `.fr` varie au gré des créations, suppressions et modifications de zones dé-

9. Peuvent enregistrer des noms de domaine sous `.fr` (et aussi sous les autres domaines de premier niveau gérés par l'Afnic comme `.pm`), les personnes physiques ou morales établies sur le territoire de l'un des états membres de l'Union Européenne ou de celui de l'un des pays suivants : Islande, Liechtenstein, Norvège, et Suisse.

léguées. De 2011 à 2012, le nombre de ces zones déléguées a augmenté de 14 % (contre 15 % entre 2010 à 2011) pour atteindre le nombre de 2 537 000 au 31 décembre 2012. Ce nombre était de 2 226 000 au 31 décembre 2011.

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 200 000 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 notre plateforme matérielle en exploitation en 2012.

Les chiffres présentés dans ce rapport pour la partie active de la plateforme proviennent des mesures faites tout au long de 2012 ainsi que des campagnes plus ponctuelles en 2011. Lorsque cela était possible, nous sommes remontés jusqu'à l'année 2010.

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 2012, sont au nombre de cinq (pour neuf instances de serveurs DNS) et se situent en région parisienne, à Lyon, Londres, Francfort et Bruxelles. Il est à noter que l'ensemble des serveurs observés n'est pas fixe et peut varier durant l'année lors de la suppression ou l'ajout d'instances.

Il faut noter que le nombre de sondes a évolué au cours de l'année 2012 et a suivi les évolutions qui ont eu lieu au niveau des serveurs faisant autorité pour la zone `.fr`.

Il faut également 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 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 un intervalle de 24 heures. Pour avoir une idée du volume que cela représente, il faut savoir que les neuf instances de serveurs DNS administrés par l'Afnic reçoivent environ 3000 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 2012. Ce taux d'échantillonnage, là aussi, 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 arrêtera les 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 dépendent donc de 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 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 le facteur important pour la résilience. Ainsi, pour les pannes « physiques », le facteur important est, en général, la dispersion géographique, et notamment le nombre de pays différents. Dans une région sismique comme la Californie, le facteur important n'est pas la distance mais la position relative aux failles géologiques. 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. La plus importante qu'on ait connue dans l'histoire du DNS est sans doute celle qui a touché `Go Daddy`, le plus gros bureau d'enregistrement du `.com` en septembre 2012 [31]. Celui-ci hébergeait alors les serveurs DNS de 40 millions de zones, situés tous au sein du même AS mais répartis sur différents sites grâce à l'*anycast*. Une panne de routage interne a rendu cet AS inaccessible pendant quatre heures, rendant à leur tour inaccessibles les serveurs DNS des clients ainsi que toutes les ressources attachées à ces zones (serveurs web, relais de messagerie ...) pendant ce laps de temps.

Avoir au moins deux serveurs faisant autorité est recommandé par la RFC 1035 [24]. 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 [32] et 2870 [33]), issue de l'ingénierie de la résilience. Il s'agit d'éviter les SPOF [10], que ceux-ci soient un AS ou un pays. Certaines pannes peuvent paralyser tout un AS, par exemple une faute de frappe dans une *route-map* BGP [11]. 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, ni s'ils sont contrôlés par un même logiciel susceptible de changer leur configuration lorsqu'un évènement particulier survient.

2.2.2 Méthodologie de mesure

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

Les pourcentages de serveurs de noms par pays ou par AS, présentés dans cette section sont en fait des « pourcentages de couples serveur et zone ». Un serveur gérant mille zones est ainsi comptabilisé mille fois, sa localisation topologique étant plus importante que celle d'un serveur qui ne sert qu'une zone.

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 [34] 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 faisons un focus sur les cinq 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 [5] qui associe un pays à une adresse IP [12] ;
- **Dispersion des serveurs de noms sur les pays les plus couvrants** : pour cette métrique, nous faisons un focus sur les cinq pays les plus importants en

10. Single Point Of Failure.
11. Un mécanisme de configuration des routeurs permettant, entre autres, de filtrer les annonces d'un AS donné.
12. Ces bases `GeoIP` sont typiquement constituées à partir des données que les RIR publient via le protocole `whois`.

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, comme l'a démontré la panne subie par `Go Daddy` [31].

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 notera qu'elle a très légèrement augmenté entre décembre 2011 et décembre 2012 pour passer de 3,2 à 3,6 serveurs par zone.

Dans la figure 2.4, nous comparons les mois de décembre 2011 et décembre 2012 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. Le fait remarquable de l'année 2012 a été l'accroissement sensible du nombre de serveurs DNS par zone : en 2011, à peine plus de 40 % des zones déléguées sous le `.fr` possédaient 4 serveurs de noms ; en 2012 elles étaient plus de 60 %.

Nombre d'AS par zone déléguée

Le nombre d'AS par zone n'a pas évolué durant l'année 2012 comme le montre la figure 2.5 : il est de 1,25 AS par zone. Par ailleurs, 82 % de zones ont tous leurs serveurs de noms dans le même AS en 2012, comme en 2011.

La dispersion des serveurs DNS par AS reste toujours faible avec la majeure partie des zones ayant tous leurs serveurs au sein d'un unique AS. Facteur aggravant, 75 % de ces serveurs sont tributaires des AS de seulement 5 hébergeurs DNS.

Dispersion des serveurs sur les AS

La figure 2.6 montre la dispersion des serveurs de noms par AS afin d'observer la concentration des serveurs chez les hébergeurs DNS. Afin de ne pas dévoiler les

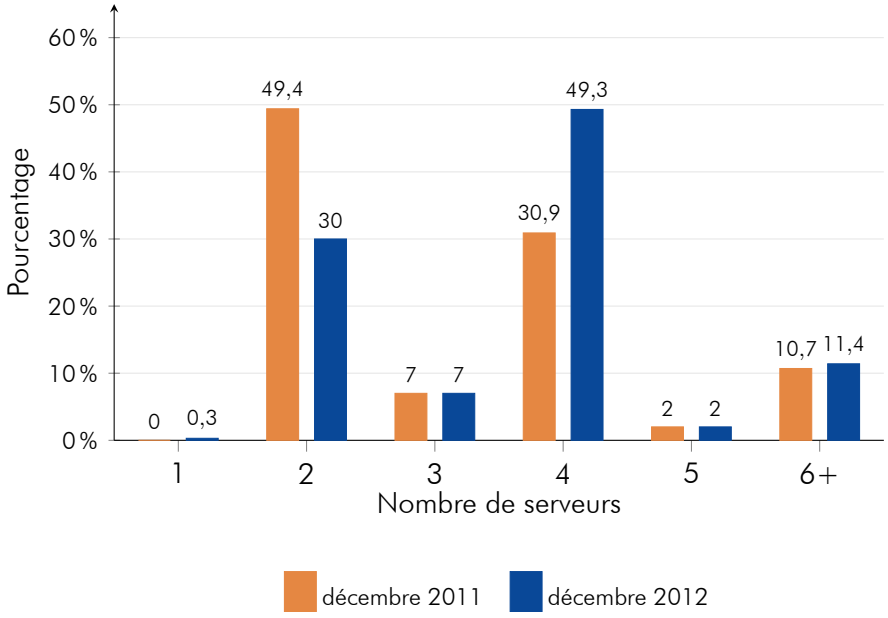

Figure 2.4 – Nombre de serveurs par zone déléguée

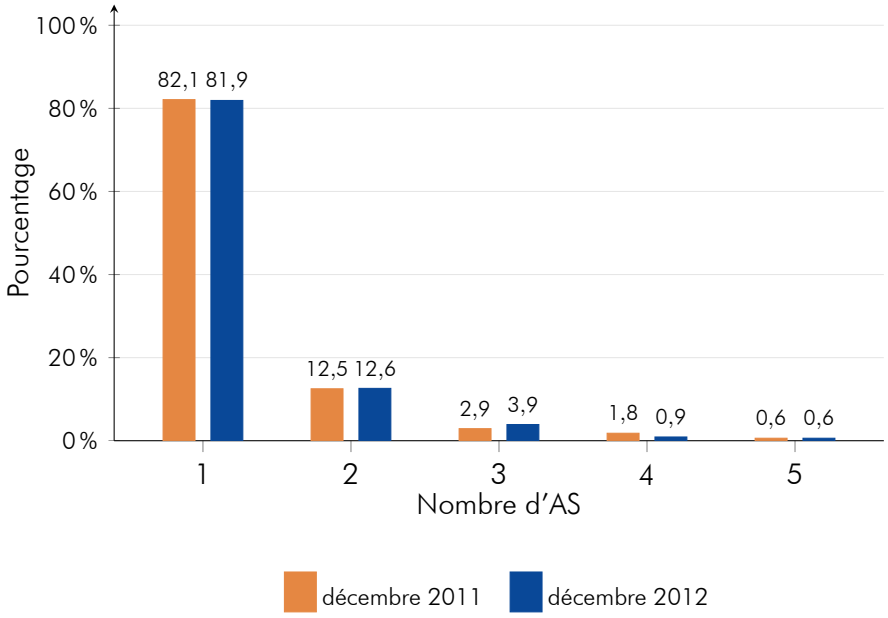

Figure 2.5 – Nombre d'AS par zone déléguée

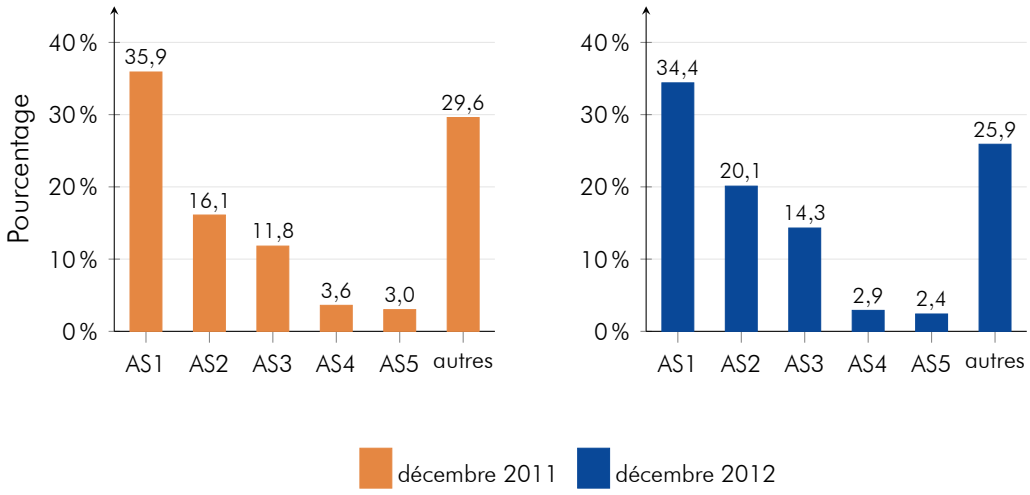

Figure 2.6 – Dispersion des serveurs sur les AS

données relatives aux hébergeurs, l'AS noté « AS n » sur le premier diagramme ne correspond pas forcément au même AS sur le second.

La comparaison des cinq premiers AS en termes de serveurs de noms entre l'année 2011 et 2012 montre que la concentration s'est accentuée au cours de l'année 2012 où cinq fournisseurs hébergent près de 75 % des serveurs de noms, contre 70 % en 2011. Une panne au niveau d'un de ces hébergeurs serait assez problématique.

Nombre de pays par zone déléguée

La dispersion des serveurs de noms par pays a également peu évolué durant l'année 2012 où plus de 80 % des zones déléguées ont leurs serveurs de noms dans un seul pays. La moyenne est, comme en 2011, de 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'appliquer aux autres pays (Allemagne, États-Unis, Royaume-Uni) dans lesquels se trouvent majoritairement les serveurs de noms qui font autorité pour la zone `fr`.

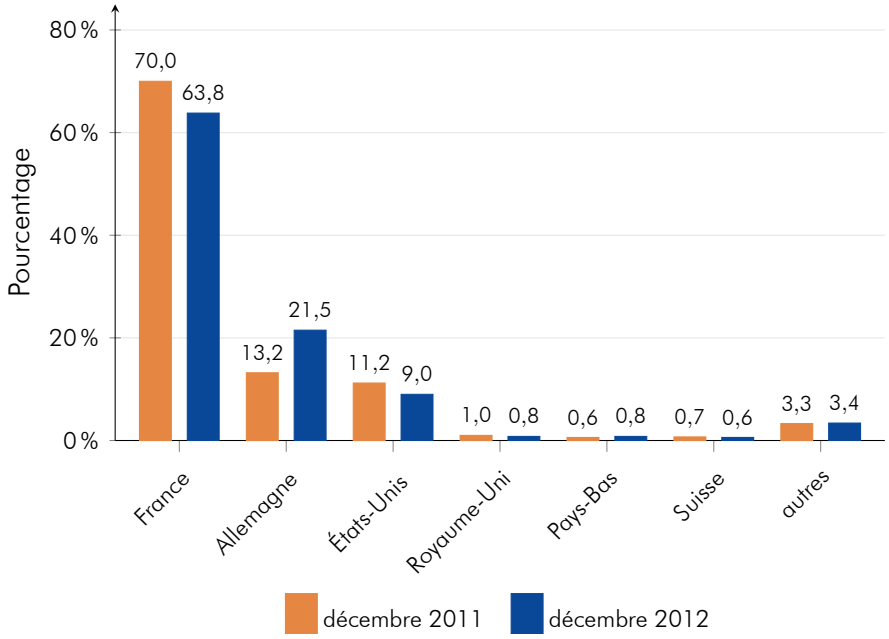

Figure 2.7 – Dispersion des serveurs sur les pays les plus couvrants

Dispersion des serveurs sur les pays les plus couvrants

La figure 2.7 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 a néanmoins diminué entre 2011 et 2012 au profit de l'Allemagne et des États-Unis.

Cas de la zone `.fr`

Nous appliquons ici les indicateurs définis plus haut à la zone `.fr`. Celle-ci est actuellement desservie par cinq serveurs de noms. Parmi ceux-ci, quatre sont anycastés pour un total de plus de soixante instances.

Les serveurs de noms sont répartis sur cinq AS différents (un AS par nuage *anycast*, à une exception) et dans plus de vingt-cinq pays. Le serveur `d.nic.fr`, opéré par l'Afnic, dispose de neuf instances dont quatre en France métropolitaine et une à la Réunion. La figure 2.8 cartographie les instances des serveurs qui font autorité pour la zone `.fr`.

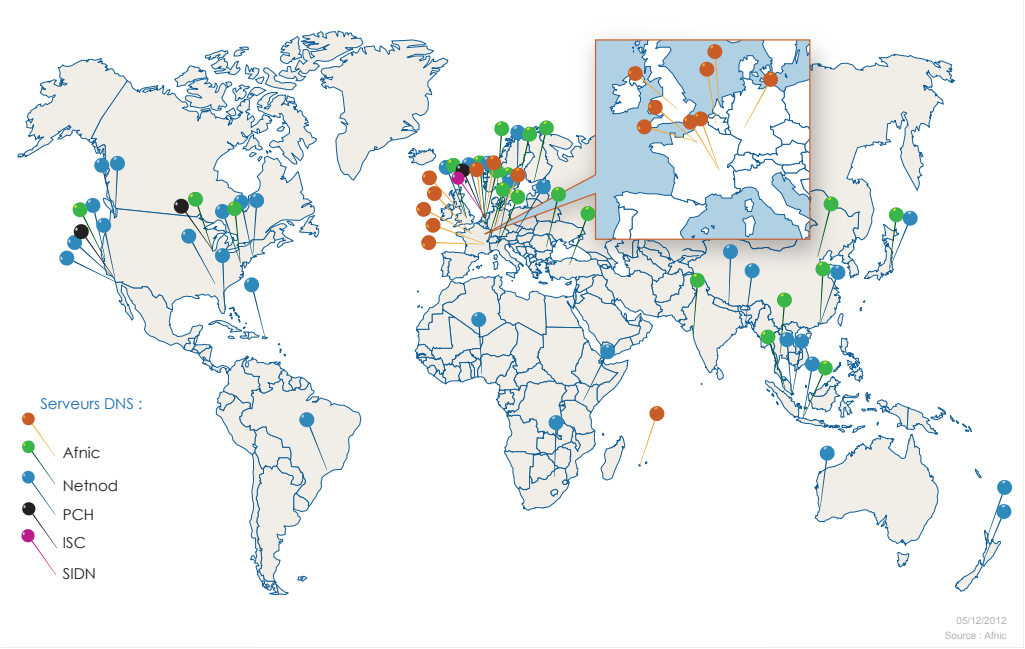

Figure 2.8 – Les serveurs DNS de la zone `.fr` [35]

2.3 Taux de résolveurs vulnérables à la faille Kaminsky

2.3.1 Description

La faille Kaminsky, annoncée en 2008s [36], exploite une faiblesse du protocole DNS qui permet un empoisonnement du cache DNS, c'est-à-dire l'injection de fausses informations dans un serveur cache. Elle peut donc être exploitée pour détourner les utilisateurs, par exemple vers un site Web de hameçonnage. Ils pourront, par exemple, être incités à fournir des données de connexion. Celles-ci seront utilisées par la suite par les fraudeurs pour usurper l'identité des utilisateurs ainsi piégés.

La vulnérabilité était connue depuis longtemps, mais l'idée de Dan Kaminsky a rendu l'utilisation de cette faille beaucoup plus efficace. Les serveurs vulnérables peuvent ainsi être empoisonnés en quelques minutes, à l'aide de programmes disponibles sur l'Internet.

Deux solutions à cette faille étaient proposées en 2008 : une à court terme appelée SPR [13], qui ajoute de l'entropie à la requête en rendant aléatoire la sélection du port source ; et l'autre à long terme, DNSSEC, qui permet de signer cryptographiquement les enregistrements DNS. La première solution a été mise en œuvre dans la plupart des résolveurs DNS ; certains, comme `Unbound` ou `PowerDNS`, l'utilisaient déjà.

2.3.2 Méthodologie de mesure

À partir des données fournies par `DNSmezzo`, nous cherchons à mesurer le nombre de ports source différents utilisés par les résolveurs qui interrogent les serveurs faisant autorité pour `.fr`. Nous avons pris de manière arbitraire un seuil de dix ports différents [14] pour classer un résolveur comme faisant varier suffisamment le port source pour ses requêtes ; seules les données pour les serveurs envoyant au moins dix requêtes sont donc analysées.

Limitations

Les données provenant de `DNSmezzo` représentent un échantillonnage de 5 % des requêtes DNS reçues par les serveurs faisant autorité pour la zone `.fr` administrés par l'Afnic. Les mesures sont faites une dizaine de fois par semaine et durent 24 heures chaque fois (deux mesures par semaine et par sonde `DNSmezzo` installée). Les

13. Source Port Randomization.

14. À l'usage, ce seuil arbitraire est estimé satisfaisant pour la qualification des résolveurs vulnérables.

résolveurs ayant une faible activité pourront, cependant, ne pas être détectés par les sondes DNSmezzo.

2.3.3 Résultats et analyse

L'étude montre que, en fonction de l'instance de d.nic.fr observée, 7 à 9 % des résolveurs utilisent trop peu de ports source différents : souvent, un seul port est utilisé.

Par rapport à l'année 2011, où ce taux variait entre 9 à 10 % des résolveurs selon l'instance de d.nic.fr, une baisse est donc observée. De plus, les résolveurs vulnérables à cette faille font beaucoup moins de requêtes en 2012 qu'en 2011, puisqu'en décembre 2011 les trois premiers résolveurs vulnérables émettaient chacun plus de 40 000 requêtes alors qu'en décembre 2012 les trois premiers résolveurs émettent seulement entre 8000 et 15 000 requêtes.

Pour l'année 2012, la moyenne des serveurs DNS encore vulnérables à la faille de Kaminsky représente un peu plus de 7 % de l'ensemble des serveurs interrogeant d.nic.fr et ces serveurs génèrent en moyenne 6 % du nombre total de requêtes reçues.

D'une manière générale, les résolveurs vulnérables à ce type d'attaques commencent à représenter un trafic de plus en plus marginal. Cela s'explique sans doute par le remplacement de machines obsolètes ou hors service.

2.4 Taux de pénétration de DNSSEC

2.4.1 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 [37], 4034 [38] et 4035 [39].

Un résolveur qui gère DNSSEC pourra ainsi valider ces enregistrements DNS et s'assurer de leur authenticité, quel que soit le chemin par lequel il les a reçus. Le-dit résolveur doit connaître 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 [15].

Pour cet indicateur, nous utilisons deux métriques :

- pourcentage de zones signées avec DNSSEC ;
- pourcentage 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 la zone parente 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 faire 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 de clés DNSSEC, peut entraîner un échec de résolution sur les résolveurs validants, et, par conséquent, une inaccessibilité du service visé après résolution DNS.

2.4.2 Méthodologie de mesure

Les données sur le nombre de `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 %

15. Delegation Signer.

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 [16] ou NSEC3. Ces enregistrements permettent de présenter une signature valide pour des enregistrements n'existant pas dans la zone. Comme indiqué plus bas, une zone considérée comme 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 de 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 pourrait 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.

2.4.3 Résultats

En examinant la zone `.fr`, on constate qu'il y avait en décembre 2012 33 790 enregistrements DS, sur un total de 2 537 000 zones déléguées.

D'autre part, le module DNSSEC de `DNSdelve` permet de voir qu'il y avait, en décembre 2012, 36 960 zones signées (soit près de 1,5 % de la zone), ce qui est compatible avec la valeur précédente. La différence entre ces deux chiffres indique que les administrateurs signant leurs zones avec DNSSEC ne fournissent pas toujours d'enregistrements DS à la zone `.fr`.

La figure 2.9, montre l'évolution des résultats `DNSdelve` sur l'année 2012. On constate que le nombre de zones signées a augmenté régulièrement au cours de l'année 2012. En analysant plus finement les résultats, nous nous apercevons que cette progression est due avant tout à un bureau d'enregistrement particulier. En 2011, nous avions estimé que seules 140 zones étaient signées avec DNSSEC.

16. Next SECure.

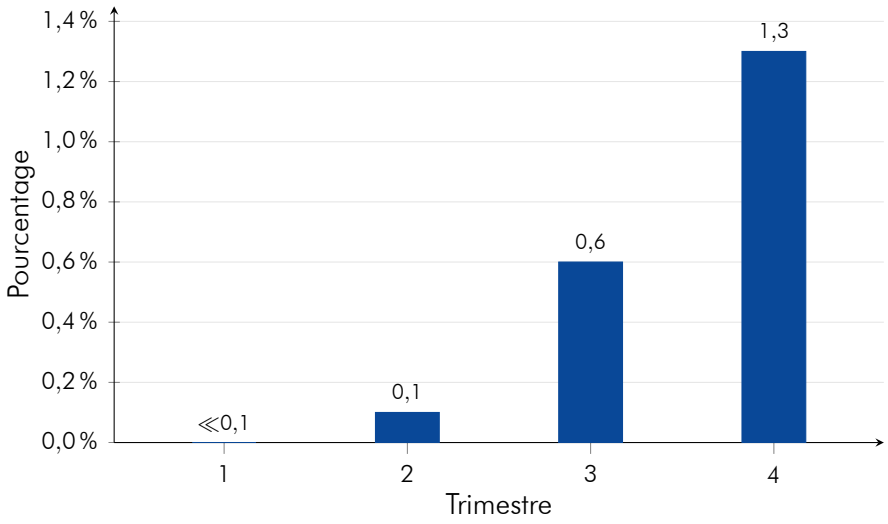

Figure 2.9 – Evolution du taux de zones signées en 2012

2.5 Taux de pénétration d'IPv6

2.5.1 Description

Compte-tenu de la diversité des domaines dans lesquels on peut observer l'évolution du déploiement d'IPv6, le taux de pénétration de ce dernier est difficile à appréhender.

Cependant, 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 son 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.

Précisons tout d'abord que le taux de pénétration d'IPv6 ne peut être considéré comme un facteur de résilience en soi. Cependant, la technique de déploiement en double pile IPv4-IPv6 (appelée *dual-stack*) apparait comme une condition nécessaire dans plusieurs environnements pour assurer une transition fluide. Par exemple, publier dans le DNS un enregistrement de type IPv6 `AAAA` pour un service, au côté d'un enregistrement `A`, sans s'assurer au préalable que le service est bien opérationnel en IPv6, rend le service au mieux dégradé et au pire inaccessible. À l'inverse, un déploiement d'IPv6 dans les règles de l'art peut représenter un facteur supplémentaire de résilience pour un service existant en IPv4. Le service est alors disponible dans les deux protocoles, il restera accessible pour les clients compatibles IPv6 en cas de panne IPv4.

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. Le RIPE-NCC a ainsi annoncé en septembre 2012 [40] qu'il commençait à allouer des adresses IPv4 à partir de son dernier bloc d'adresses et que toute nouvelle allocation d'adresses IPv4 était, dès lors, subordonnée à une allocation d'adresses IPv6.

La nécessité de déploiement d'IPv6 au niveau des infrastructures existantes se fait donc plus pressante. C'est pourquoi nous avons choisi d'inclure un indicateur de mesure de la pénétration d'IPv6.

2.5.2 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 nous paraissaient les plus pertinents en termes de fréquence d'utilisation : les serveurs DNS, les relais de messagerie et les serveurs web.

`DNSdelve` examine les adresses IPv6 déclarées au niveau du DNS en faisant des requêtes de type `AAAA` sur des noms particuliers, détaillés 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`.

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 nous 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.

Les cinq sondes `DNSmezzo` en service fin 2012 capturent 5 % des requêtes DNS reçues par les instances de serveurs de noms près desquelles elles sont placées. Les mesures sont lancées plusieurs fois par semaine et chaque mesure est faite pendant 24 heures d'affilée. Cela représente un volume de l'ordre de 45 000 000 de requêtes DNS analysées par semaine.

Limitations

Rappelons que la zone `.fr` varie au cours du temps et que des zones déléguées sont créées et d'autres supprimées d'une version à l'autre de la zone. Ainsi, le nombre de zones déléguées a augmenté de 15 % en 2011 et de 14 % en 2012 pour atteindre le nombre de 2 537 000 zones déléguées au 31 décembre 2012.

2.5.3 Résultats et analyse

Les zones déléguées sous `.fr`

Les figures suivantes nous permettent d'observer la progression du taux de pénétration d'IPv6 sur les trois dernières années. La figure 2.10 montre la progression des zones compatibles IPv6 (zones « IPv6 activé » ou « IPv6 complet »). La figure 2.11 détaille cette progression par type de service.

Après une très forte hausse en 2011, le nombre de zones ayant au moins un serveur compatible IPv6 (zones de type « IPv6 activé ») a continué sa progression en 2012 pour atteindre près de 2 zones sur 3. En revanche, le taux de zones ayant tous leurs serveurs (DNS, mail et web) compatibles IPv6 reste faible, même si la progression a été sensible.

En 2012, la progression d'IPv6 par type de service nous permet d'observer que l'accroissement du taux de zones de type « IPv6 activé » est avant tout dû aux serveurs DNS (voir figure 2.11).

La proportion de serveurs de messagerie et de serveurs web compatibles IPv6 a progressé entre 2011 et 2012. Ces services restent cepdendant peu connectés en IPv6, et c'est ce qui explique la faible proportion des zones de type « IPv6 complet ».

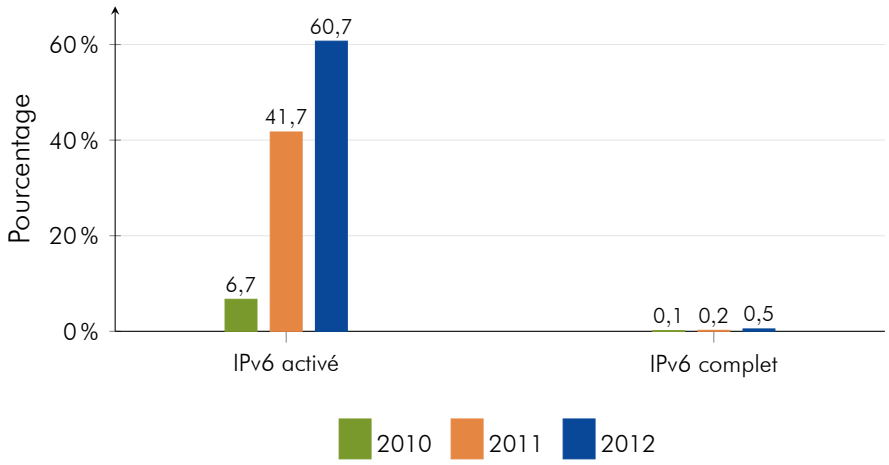

Figure 2.10 – Progression des zones compatibles IPv6 entre 2010 et 2012

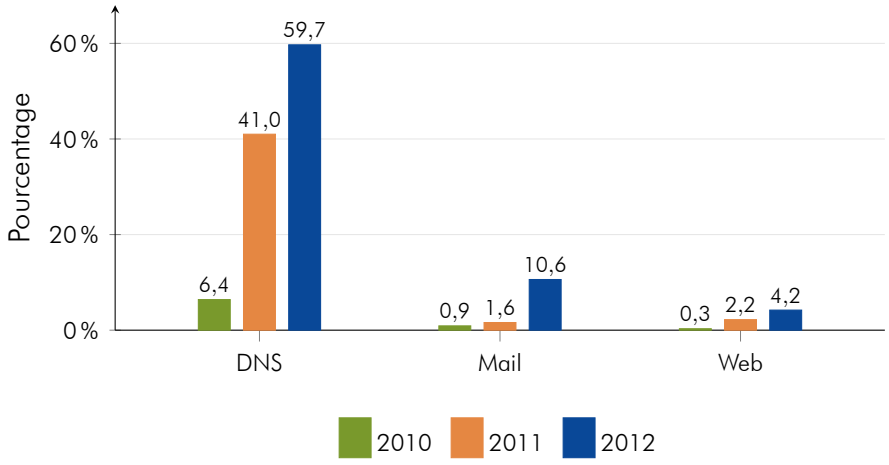

Figure 2.11 – Progression des serveurs compatibles IPv6 entre 2010 et 2012

Les requêtes DNS reçues

Pour les serveurs faisant autorité pour `.fr` et étant directement administrés par l'Afnic, environ 11 % des requêtes sont transportées en IPv6 (voir figure 2.12).

Quant aux types de données demandées, on remarquera la faible progression des adresses IPv6 (voir figure 2.12).

Il faut se rappeler que les clients des serveurs faisant autorité pour le `.fr` ne sont

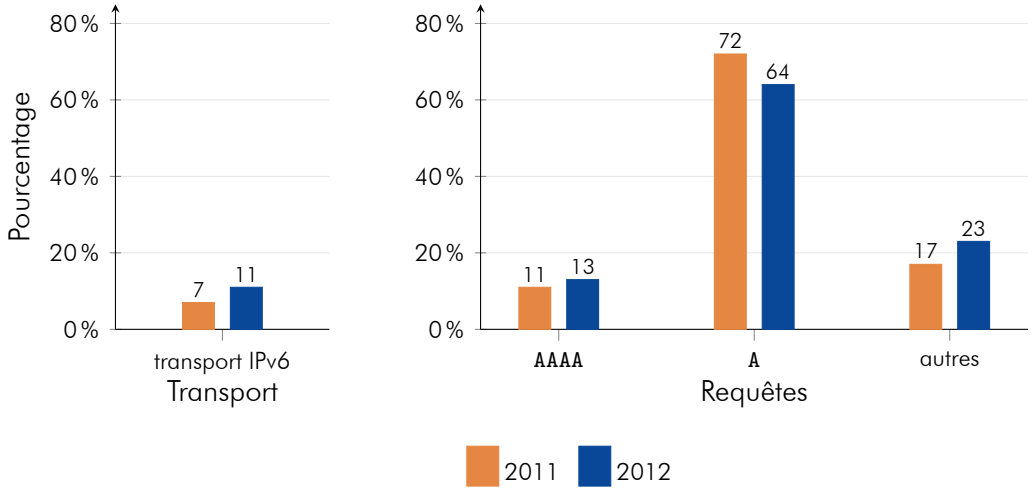

Figure 2.12 – Progression du transport et des requêtes IPv6 entre 2011 et 2012

généralement pas des machines d'utilisateurs finaux mais plutôt des résolveurs DNS, souvent gérés par des FAI et hébergeurs réseau. 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.

Le fait que le nombre de requêtes DNS transportées sur IPv6 ait enregistré une hausse significative, alors que la proportion de requêtes demandant une adresse IPv6 par rapport aux demandes d'adresses IPv4 a très peu augmenté, permet de déduire que c'est le nombre de résolveurs DNS compatibles IPv6 qui a augmenté et non celui des machines clientes qui les interrogent.

2.6 Résolveurs les plus demandeurs

2.6.1 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 on ne sait pas s'ils sont beaucoup 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 ou résolveur public. À terme, cet indicateur permettra d'étudier sur la durée l'évolution de ces catégories.

2.6.2 Méthodologie de mesure

On observe les clients DNS de `d.nic.fr` pendant 24 heures et on ne prend en compte que les adresses IP des résolveurs ayant généré au moins dix requêtes. Cela permet d'éliminer ceux qui ne seraient pas de « vrais résolveurs » comme des tests manuels. En raison de l'échantillonnage (5 % des requêtes DNS reçues), un client très peu actif peut donc ne pas être enregistré du tout. Par ailleurs, nous avons vérifié que ce serveur 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.

Afin d'identifier les résolveurs les plus demandeurs, nous avons mis en place deux méthodologies distinctes. On s'intéresse tout d'abord aux adresses IP, puis on les regroupe suivant les préfixes annoncés sur Internet et visibles dans les archives BGP. 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.

Limitations

Si une entreprise utilise un résolveur pour ses clients mais ne possède pas d'AS, le préfixe correspondant dans les archives BGP appartient en fait à son FAI. Le résolveur de l'entreprise fera donc partie des résultats de son FAI. Dans la suite de nos travaux, nous envisageons d'étudier l'influence de regroupements différents dans les

prochaines éditions du rapport.

Une alternative envisageable est de regrouper les adresses IP en préfixes de taille fixe, par exemple /24 en IPv4 et /48 en IPv6. La méthodologie associée au choix de cette taille reste toutefois à définir.

2.6.3 Résultats et analyse

Nombre de requêtes par adresse IP

Dans l'échantillon de requêtes capturées sur un transport IPv6, on compte 6200 adresses différentes, dont seulement 1300 ont envoyé plus de dix requêtes. Elles sont donc retenues dans la suite de l'étude. L'analyse de la dispersion de ces résolveurs donne les résultats suivants pour les requêtes effectuées en IPv6 :

- 62 % des requêtes sont effectuées par 10 % des résolveurs ;
- 25 % des requêtes sont effectuées par 1 % des résolveurs.

En IPv4, on a 103 000 adresses distinctes, dont 12 000 sont retenues pour l'étude. Les résultats obtenus pour les requêtes IPv4 sont assez semblables à l'analyse du trafic IPv6, ainsi :

- 66 % des requêtes sont effectuées par 10 % des résolveurs ;
- 31 % des requêtes sont effectuées par 1 % des résolveurs.

Cette première analyse permet donc d'identifier que 13 300 résolveurs interrogent le serveur `d.nic.fr` ; 10 % d'entre eux effectuent leurs requêtes en IPv6.

Nombre de requêtes par pays

Si on s'intéresse maintenant à l'origine des adresses IP, les requêtes envoyées par les résolveurs se répartissent comme suit :

- États-Unis : 37 % des requêtes ;
- France : 11 % des requêtes ;
- Allemagne : 9 % des requêtes ;
- Royaume-Uni : 4,5 % des requêtes ;
- Pays-Bas : 2,5 % des requêtes.

Rappelons ici que les requêtes observées proviennent de résolveurs et qu'il ne s'agit pas de requêtes envoyées par les utilisateurs finaux. La proportion importante de requêtes en provenance des États-Unis s'explique en partie par la prééminence de trois acteurs américains qui génèrent à eux seuls près de 13 % du trafic (voir section suivante « Nombre de requêtes par AS »).

Nombre de requêtes par préfixe

Les préfixes ont été ici constitués sur la base des annonces BGP observées en décembre 2012, au même moment que la capture des requêtes `DNSmezzo`. L'analyse qui suit tient compte du nombre de requêtes générées et du nombre de résolveurs contenus dans ces préfixes.

Le trafic IPv6 est assez hétérogène. En effet, le premier préfixe le plus demandeur génère 25 % des requêtes, alors que les vingt premiers cumulent plus de 75 % des requêtes. L'inégalité est moins forte en nombre de résolveurs : le premier préfixe regroupe 9 % des résolveurs et les vingt premiers 40 %.

En IPv4, le premier préfixe le plus demandeur génère moins de 5 % des requêtes, les vingt premiers préfixes cumulent quant à eux 30 % des requêtes. La dispersion des résolveurs est encore plus faible : les vingt premiers préfixes ne cumulent que 12 % du nombre total des résolveurs. Il est nécessaire de souligner que ce ne sont pas les mêmes préfixes qui sont en tête dans le classement par nombre de requêtes et dans celui par nombre de résolveurs.

Cette analyse par préfixes met en évidence une forte différence entre IPv4 et IPv6. En effet, le premier préfixe IPv6 génère plus de requêtes que le premier préfixe IPv4. Ce phénomène peut s'expliquer par la taille des préfixes annoncés sur Internet en IPv4 et en IPv6. Les adresses IPv6 étant plus grandes que les adresses IPv4, les préfixes IPv6 regroupent plus de résolveurs que les préfixes IPv4. Une analyse plus fine est nécessaire afin de mieux caractériser ce phénomène.

Nombre de requêtes par AS

Nous ne nous intéressons qu'au trafic IPv4, qui représente 90 % des requêtes reçues par le serveur `d.nic.fr`. Les cinq AS les plus demandeurs, classés par pourcentage de requêtes décroissant, sont présentés dans le tableau 2.1. Ces résultats sont particulièrement importants pour notre étude car ils mettent en évidence le phénomène des résolveurs publics : le troisième AS met un serveur DNS cache à disposition de tous les internautes. Il est à noter que les pays donnés dans le tableau le sont à titre indicatif. En effet, un FAI peut être présent dans plusieurs pays.

Nombre de requêtes par AS français

Un focus sur les AS français, définis dans le chapitre 1, permet d'obtenir les résultats présentés dans le tableau 2.2. Les pourcentages représentent le trafic généré par ces AS par rapport au trafic global. Si nous ne considérons que le trafic généré par les AS

Pourcentage de requêtes	Nombre de résolveurs	Nature de l'AS
4,5 %	1314	FAI américain
4,2 %	1	FAI américain
3,6 %	1626	Moteur de recherche
3,6 %	36 744	FAI et hébergeur français
3,5 %	908	FAI français

Table 2.1 – Les cinq AS les plus demandeurs

Pourcentage de requêtes	Nombre de résolveurs	Nature de l'AS
3,6 %	36 744	FAI et hébergeur français
3,5 %	908	FAI français
1,3 %	1801	Réseau universitaire
0,5 %	24	FAI français
0,4 %	1	FAI français

Table 2.2 – Les cinq AS français les plus demandeurs

français, les requêtes envoyées par les trois premiers AS du tableau 2.2 représentent alors respectivement 33,4 %, 32,7 % et 12,6 %.

Nous observons ainsi que si le trafic global est relativement équilibré au niveau de la dispersion par AS, le trafic généré par les AS français seuls fait ressortir des concentrations fortes et des disparités importantes.

2.7 Conclusion et perspectives

Dans cette nouvelle édition du rapport, nous avons examiné la résilience de l'Internet français à travers le prisme du protocole DNS en poursuivant l'étude des quatre indicateurs du rapport 2011 et en introduisant un nouvel indicateur.

Comme l'année précédente, nos analyses ont porté sur les domaines délégués sous la zone `.fr` ainsi que sur les requêtes DNS vues par un des serveurs faisant autorité pour la zone `.fr` et administrés par l'Afnic.

Vu sous l'angle du DNS, on remarque que l'Internet français se caractérise par de fortes concentrations : 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 avant d'accéder à toute autre ressource sur le réseau.

Dans ces conditions, on comprend que nos indicateurs sont très sensibles aux politiques des opérateurs majeurs. Ainsi, si l'un d'eux modifie ses pratiques en matière de déploiement d'un protocole ou d'une technologie, cela influe sur nos résultats. Par ailleurs, cette forte concentration du marché implique une résilience moindre en cas de panne majeure chez un opérateur. En septembre 2012, un évènement [31] chez un opérateur américain a montré que plusieurs millions d'utilisateurs pouvaient être affectés simultanément pendant quelques heures du fait d'une seule panne.

Cette concentration est illustrée avant tout par deux indicateurs. Le premier concerne la dispersion topologique des serveurs DNS faisant autorité, qui nous indique qu'en 2012, 75 % des zones déléguées sous la zone `.fr` sont hébergées au sein de 5 AS distincts (ce taux était de 70 % des zones déléguées en 2011). Par ailleurs, 80 % des zones déléguées ont tous leurs serveurs DNS au sein d'un AS unique.

Le second indicateur qui nous permet de mesurer ce manque de diversité des opérateurs est celui concernant les résolveurs les plus demandeurs. En effet, on observe que les deux tiers du trafic DNS IPv4 [17] généré par les AS français est en provenance de deux acteurs.

Au-delà de ce phénomène de concentration, les faits marquants de l'édition 2012 sont :

- un nombre de serveurs DNS faisant autorité par zone déléguée en forte progression ;
- un déploiement d'IPv6 croissant aussi bien sur les serveurs DNS faisant autorité que sur les résolveurs DNS ;
- un début de déploiement de DNSSEC sur les serveurs DNS faisant autorité.

17. Il s'agit du trafic enregistré par les serveurs faisant autorité pour la zone `.fr` et administrés par l'Afnic. Le transport IPv4 représente près de 90 % du trafic observé.

En 2012, 60 % des zones déléguées possèdent au moins quatre serveurs DNS alors que ce taux était de 40 % en 2011. De même, en 2012, 60 % des serveurs DNS faisant autorité utilisent le protocole IPv6 ; alors que ce protocole est peu déployé sur les serveurs de messagerie (11 % l'utilisent) et encore moins sur les serveurs web (4 %).

La progression d'IPv6 pour l'année 2012 a donc été essentiellement le fait des opérateurs DNS, qu'ils soient hébergeurs de zones déléguées ou opérateurs de résolveurs DNS tels que les FAI.

Le déploiement de DNSSEC est sensible en 2012, du fait d'un hébergeur DNS en particulier. En 2011, 140 zones déléguées étaient signées. En 2012, ce chiffre est estimé à 36 000 zones, dont 90 % ont communiqué la partie publique de leur clé de chiffrement [18] à la zone parente, permettant ainsi la mise en place d'une chaîne de confiance depuis la racine jusqu'aux zones signées.

Pour ce qui est de l'adoption des bonnes pratiques au niveau DNS, notons que les serveurs cache vulnérables à la faille dite de « Kaminsky » disparaissent petit à petit : ils ne génèrent plus que 6 % du trafic DNS observé.

Pour conclure, cette édition 2012 nous a permis de consolider les résultats obtenus en 2011 et de voir s'amorcer des tendances, notamment pour IPv6 et DNSSEC, et de mieux saisir ce qui caractérise l'Internet français. Dans les prochaines éditions, nous poursuivrons l'étude de la plupart des indicateurs et nous en développerons de nouveaux afin d'étendre le champ de nos observations. Ainsi, deux indicateurs que nous pourrions adjoindre sont la progression de DNSSEC sur les résolveurs, ainsi que la qualité technique des zones sous `.fr`.

18. L'enregistrement DS pour être plus précis.

Conclusion générale

À travers l'étude des protocoles BGP et DNS, ce rapport présente une vision fidèle de l'Internet français en 2012. Concernant BGP, l'étude des 1270 acteurs français identifiés a mis en évidence une forte diversité. Par conséquent, il existe peu d'opérateurs dont la panne affecterait une part significative de l'Internet français. Les analyses concernant DNS révèlent en revanche une concentration importante au niveau des hébergeurs et des résolveurs des FAI. Cette double concentration laisse à penser qu'une défaillance d'un acteur important de la communauté DNS pourrait avoir un impact significatif sur le fonctionnement de l'Internet français. Il est donc très important que tous les acteurs apportent un soin tout particulier à la résilience de leur infrastructure, qui commence par l'application des bonnes pratiques.

En effet, il est avéré que l'usage de ces dernières contribue à la sécurité et à la robustesse de l'Internet. En ce qui concerne BGP, les observations contenues dans ce rapport montrent que la plupart des acteurs français déclarent des objets `route`. Cependant, la qualité de ces déclarations doit être améliorée. À titre d'exemple, 10 % des préfixes annoncés par des acteurs français seraient rejetés par des filtres stricts utilisant les objets `route`. Pour ce qui est du DNS, tandis que la plupart des zones sous `.fr` a un nombre suffisant de serveurs, la majorité de ces serveurs n'est présente que dans un seul opérateur. De manière générale, les bonnes pratiques admises pour BGP et DNS ne sont pas pleinement adoptées par les acteurs de l'Internet français et il y a une marge de progression significative.

En ce qui concerne le protocole IPv6, en 2012, les déploiements chez les acteurs français sont croissants sans toutefois être francs. En effet, sous l'angle de BGP, moins de 30 % des opérateurs annoncent des préfixes en IPv6. De même, sous l'angle de DNS, moins de 5 % des sites web possèdent un enregistrement IPv6. Pour comprendre le caractère mitigé de ces observations, il faut rappeler que les clients finaux ne peuvent utiliser IPv6 que si leurs FAI leur fournissent une connectivité IPv6. De plus, les opérateurs gérant leurs services doivent utiliser IPv6 aussi bien en BGP qu'en DNS. Ceci explique en partie la faible utilisation d'IPv6 pour accéder à des services comme les sites web ou le courrier électronique. De manière plus préoccupante, il apparait que les bonnes pratiques pour BGP sont moins bien suivies en IPv6 qu'en IPv4.

Deux technologies émergentes, DNSSEC et RPKI, ont également été étudiées dans ce rapport. Elles visent, respectivement, à authentifier tout ou partie des informations

échangées avec DNS et BGP à l'aide de signatures cryptographiques. DNSSEC offre ainsi une protection très complète contre les empoisonnements de cache DNS. En revanche, la RPKI ne répond que partiellement aux problèmes d'usurpation BGP en proposant seulement des objets `route` signés. Bien que ces deux protocoles soient critiques pour la sécurité de l'Internet, leur utilisation est très minoritaire. Ainsi, en 2012, le déploiement de DNSSEC reste marginal avec 2 % des zones sous `.fr` signées mais une forte croissance a été observée, pouvant laisser espérer un début d'adoption de ce protocole. En ce qui concerne RPKI, son utilisation reste anecdotique car le standard n'est pas encore implémenté par l'ensemble des équipementiers.

En guise de conclusion et au regard de tous ces résultats, l'observatoire estime que la situation actuelle de l'Internet français est acceptable. Par ailleurs, l'observatoire souhaite adresser les quatre recommandations suivantes aux acteurs de l'Internet français :

- **déployer IPv6** afin de développer les compétences et d'anticiper des problèmes de déploiements futurs ;
- **répartir les serveurs DNS faisant autorité au sein de différents opérateurs** afin de limiter les effets d'une panne locale ;
- **déclarer systématiquement les objets route**, et les **maintenir à jour**, afin de faciliter la détection et le filtrage d'annonces BGP illégitimes ;
- **appliquer les bonnes pratiques BGP** au niveau des interconnexions entre opérateurs.

Bibliographie

[1] 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.

[2] RIPE-NCC, "Resource management." <http://www.ripe.net/lir-services/resource-management>.

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

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

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

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

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

[8] Hurricane Electric, "World Report : France." <http://bgp.he.net/country/FR>.

[9] RIPE-NCC, "RIR Statistics." <ftp://ftp.ripe.net/ripe/stats/delegated-ripencc-latest>.

[10] G. Siganos and M. Faloutsos, "Analyzing BGP Policies : Methodology and Tool," in *IEEE INFOCOM*, vol. 3, 2004.

[11] P.-A. Vervier and O. Thonnard, "Spamtracer : How stealthy are spammers ?," in *TMA 2013, 5th IEEE International Traffic Monitoring and Analysis Workshop, April 19th, 2013, Turin, Italy*, (Turin, ITALY), Feb. 2013.

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

[13] R. Bush and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol." RFC 6810 (Proposed Standard), Jan. 2013.

[14] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280 (Proposed Standard), May 2008. Updated by RFC 6818.

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

[16] Secure Inter-Domain Routing Working Group, "Sidr Status Pages." <http://tools.ietf.org/wg/sidr/>.

[17] M. Lepinski, Ed., "BGPSEC Protocol Specification - draft-ietf-sidr-bgpsec-protocol-07." <http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-07>, Feb. 2013.

[18] RIPE-NCC, "RIPE Routing Working Group Recommendations on Route Aggregation." <http://www.ripe.net/ripe/docs/ripe-399>, Dec. 2006.

[19] RIPE-NCC, "RIPE Routing Working Group Recommendations on IPv6 Route Aggregation." <http://www.ripe.net/ripe/docs/ripe-532>, Nov. 2011.

[20] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification." RFC 1883 (Proposed Standard), Dec. 1995. Obsoleted by RFC 2460.

[21] L. Gao, "On inferring autonomous system relationships in the internet," *IEEE/ACM Transactions on Networking*, Dec. 2001.

[22] CAIDA, "AS Ranking." <http://as-rank.caida.org>.

[23] 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.

[24] 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, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604.

[25] J. Abley and W. Maton, "AS112 Nameserver Operations." RFC 6304 (Informational), July 2011.

[26] Wikipedia, "Content Delivery Network." <http://fr.wikipedia.org/wiki/Content_delivery_network/>.

[27] Root servers operators, "Root Server Technical Operations Assn." <http://www.root-servers.org/>.

[28] J. Abley and K. Lindqvist, "Operation of Anycast Services." RFC 4786 (Best Current Practice), Dec. 2006.

[29] T. Hardie, "Distributing Authoritative Name Servers via Shared Unicast Addresses." RFC 3258 (Informational), Apr. 2002.

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

[31] 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.

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

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

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

[35] Afnic, "Rapport d'activité 2011." <http://www.afnic.fr/medias/documents/afnic-rapport-activite-2011.pdf>, 2011.

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

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

[38] 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.

[39] 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.

[40] 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.

Acronymes

Afnic	Association Française pour le Nommage Internet en Coopération
ANSSI	Agence nationale de la sécurité des systèmes d'information
AS	Autonomous System
BGP	Border Gateway Protocol
CDN	Content Delivery Network
DNS	Domain Name System
DNSSEC	DNS SECurity extensions
DDoS	Distributed Denial of Service
DS	Delegation Signer
FAI	Fournisseur d'Accès à Internet
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRR	Internet Routing Registry
LIR	Local Internet Registry
NSEC	Next SECure
PA	Provider Aggregate
PGP	Pretty Good Privacy
RIR	Regional Internet Registry
RIS	Routing Information Service
ROA	Route Origin Authorization
RPKI	Resource Public Key Infrastructure
SPOF	Single Point Of Failure
SPR	Source Port Randomization

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.

Juin 2013

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