

L'observatoire de la résilience de l'Internet français : l'essentiel du rapport sur l'année 2012

Stéphane Bortzmeyer, François Contat, Mathieu Feuillet,
Pierre Lorinquer, Samia M'timet, Mohsen Souissi,
Guillaume Valadon

rapport.observatoire@ssi.gouv.fr

20 septembre 2013



afnic



L'Agence Nationale de la Sécurité des Systèmes d'Information

- Créée le 7 juillet 2009, l'ANSSI est l'autorité nationale en matière de défense et de sécurité des systèmes d'information ;
- Ses missions principales sont :
 - la [prévention](#) ;
 - la [défense des systèmes d'information](#).
- L'une de ses priorités d'action est la [résilience de l'Internet](#).

<http://www.ssi.gouv.fr/>



Quelques mots sur l'observatoire

Les motivations à l'origine de l'observatoire

- L'Internet reste méconnu.
- Les analyses d'incidents sont rarement orientées sur la France.
- L'étude de l'utilisation des bonnes pratiques.

Objectifs de l'observatoire

- Étudier en détail la résilience de l'Internet français.
- Favoriser les échanges techniques entre acteurs de l'Internet.
- Publier ses résultats anonymisés.
- Publier des recommandations et diffuser des bonnes pratiques.

L'Afnic est moteur de l'initiative depuis ses débuts.



La résilience ?

« La capacité de fonctionner pendant un incident et de revenir à l'état nominal. »

Livre blanc sur la défense et la sécurité nationale, 2008

On peut notamment observer :

- la structure de l'Internet (routage & nommage) ;
- le trafic et les services (HTTPS, SPAM, botnets...).

L'observatoire se focalise pour l'instant sur **la structure de l'Internet**.



Sous l'angle du protocole BGP

Définition de l'Internet français

Qu'est-ce que l'Internet français ?

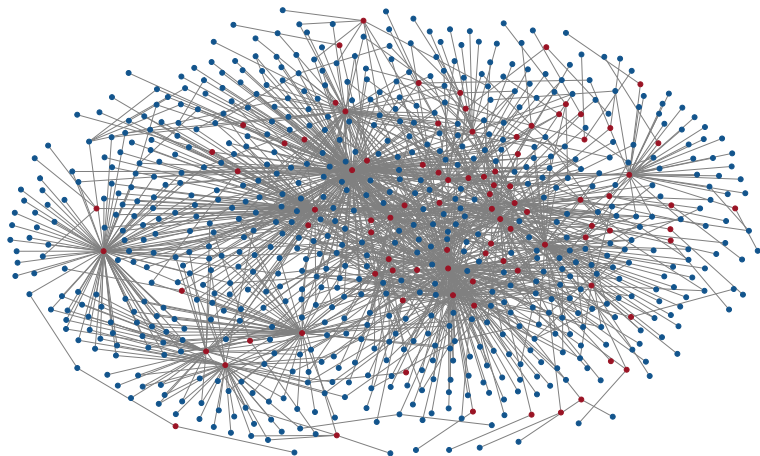
- Identification des AS constituant l'Internet français au moyen d'un algorithme d'apprentissage.

Résultats

- 1270 AS français (entre 700 et 800 sont visibles) ;
- comparaison avec des bases publiques existantes :
 - notre base en comporte entre 40 et 70 en plus ;
 - 9 AS manquants dans notre base.



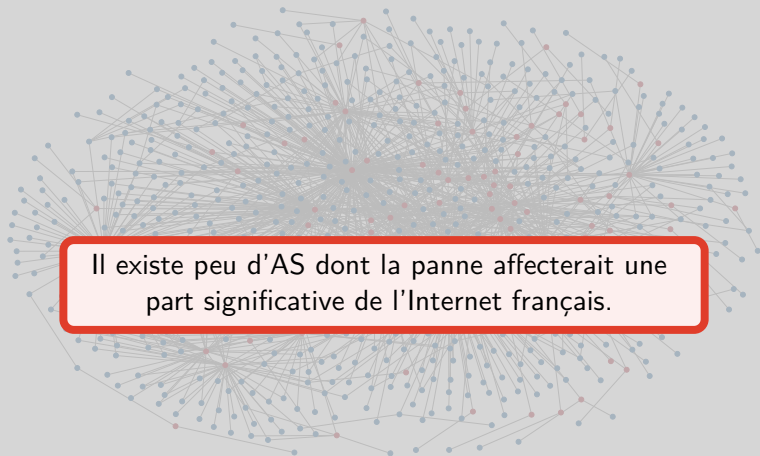
Connectivité des AS : BGP



- En **bleu**, les AS français.
- En **rouge**, les AS dont la disparition pourrait en isoler d'autres.



Connectivité des AS : BGP



Il existe peu d'AS dont la panne affecterait une part significative de l'Internet français.

- En **bleu**, les AS français.
- En **rouge**, les AS dont la disparition pourrait en isoler d'autres.



Connectivité des AS : base whois

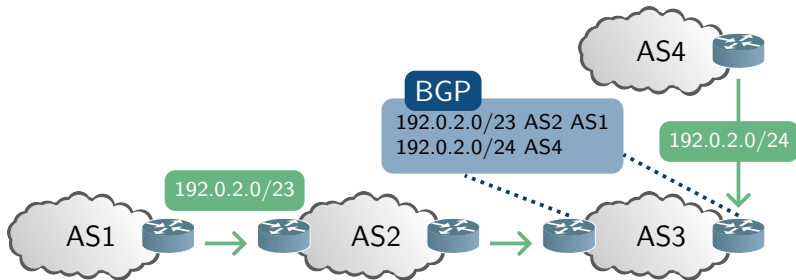
Utilisation des attributs import et export.

AS	Transit	Client	Peering	Non déclaré
AS-fr1	2/3	1/1	10/404	3
AS-fr6	4/7	71/130	6/27	14
AS-fr9	2/2	0/0	5/165	1

Connectivité de trois AS français au 31 juillet 2012 :
Nombre de liens vus/Nombre de liens déclarés.



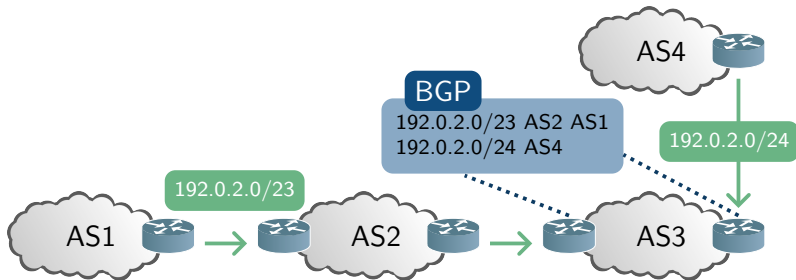
Qu'est-ce qu'une usurpation de préfixe ?



- Annonce d'un préfixe appartenant à un autre AS : est-ce légitime ?

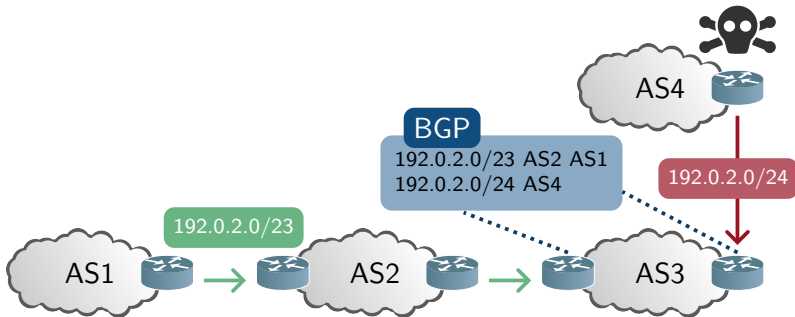


Qu'est-ce qu'une usurpation de préfixe ?



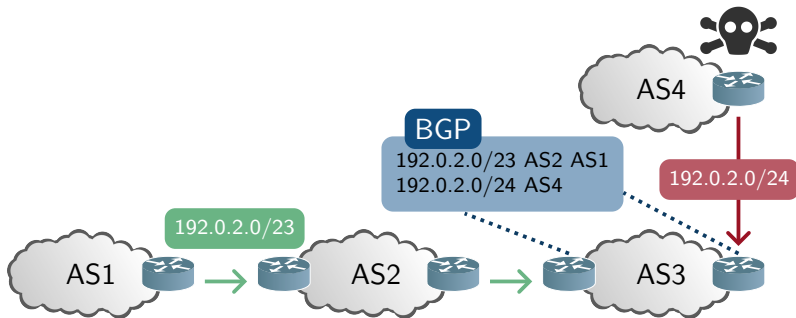
- Annonce d'un préfixe appartenant à un autre AS : est-ce légitime ?
 - **Oui** : par exemple, délégation d'un préfixe à un AS client ;

Qu'est-ce qu'une usurpation de préfixe ?



- Annonce d'un préfixe appartenant à un autre AS : est-ce légitime ?
 - **Oui** : par exemple, délégation d'un préfixe à un AS client ;
 - **Non** : il s'agit dans ce cas d'une usurpation.

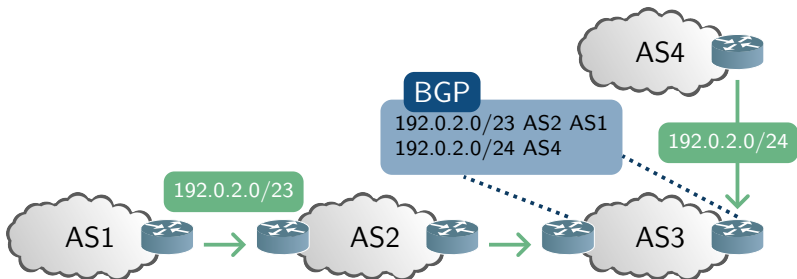
Qu'est-ce qu'une usurpation de préfixe ?



- Annonce d'un préfixe appartenant à un autre AS : est-ce légitime ?
 - **Oui** : par exemple, délégation d'un préfixe à un AS client ;
 - **Non** : il s'agit dans ce cas d'une usurpation.
- **Comment déterminer la légitimité d'une annonce ?**



Légitimité des annonces : les objets route



Déclaré par l'AS1, l'objet route suivant indique que l'AS4 a le droit d'annoncer le préfixe 192.0.2.0/24.

```
$ whois -T route 192.0.2.42
descr:          Objet route d'exemple
route:         192.0.2.0/24
origin:        AS-4
mnt-by:        FRNOG-MNT
```



Utilisation des objets route

	janvier 2012	décembre 2012
Correspondance	78%	82%
Problème	22%	18%

- **Augmentation** du pourcentage de correspondance.
- **Diminution** du pourcentage d'AS ayant des déclarations conflictuelles ou manquantes.



Utilisation des objets route

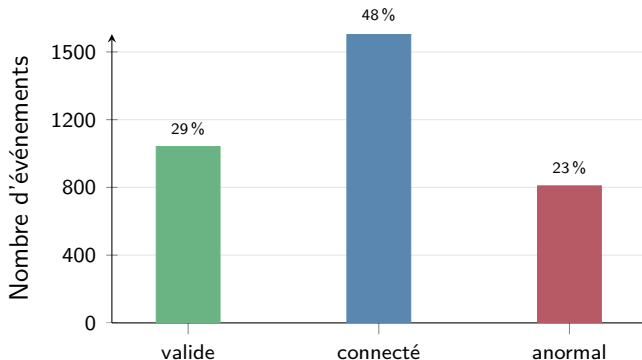
	janvier 2012	décembre 2012
Correspondance	78%	82%
AS ayant des déclarations conflictuelles ou manquantes	22%	18%

Les préfixes annoncés en BGP doivent être couverts par un objet route. Les objets route doivent être maintenus à jour.

- Augmentation du pourcentage de correspondance.
- Diminution du pourcentage d'AS ayant des déclarations conflictuelles ou manquantes.



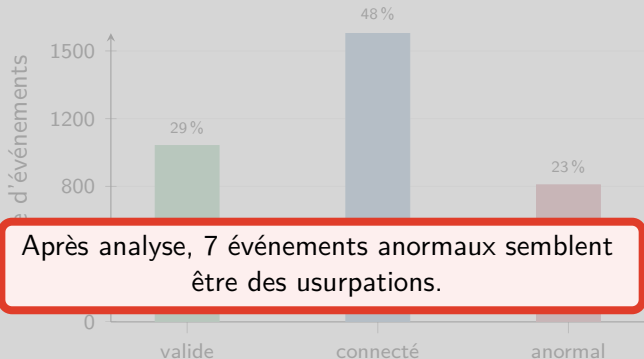
Usurpations de préfixes



- **Valide** : événement validé par un objet route.
- **Connecté** : l'AS usurpateur est connecté à l'AS usurpé.
- **Anormal** : c'est peut-être une usurpation.



Usurpations de préfixes



- **Valide** : événement validé par un objet route.
- **Connecté** : l'AS usurpateur est connecté à l'AS usurpé.
- **Anormal** : c'est peut-être une usurpation.



Observations générales

Déploiement d'IPv6

	2009	2010	2011	2012
Seulement IPv4	519	536	557	557
IPv4 et IPv6	45	86	124	159
Seulement IPv6	1	2	4	3

Nombre d'AS ayant déployé IPv6

Respect des bonnes pratiques

- Annonces de préfixes trop spécifiques :
 - 5 annonces de préfixes IPv4 (> /24, RIPE-399) ;
 - 43 annonces de préfixes IPv6 (> /48, RIPE-532) ;
- AS_PATH avec des numéros d'AS privés.



Observations générales

Déploiement d'IPv6

	2009	2010	2011	2012
Seulement IPv4	519	536	557	557
IPv4 et IPv6	45	86	124	159
Seulement IPv6	1	2	4	2

Les bonnes pratiques ne sont pas respectées par tous les acteurs, notamment pour l'IPv6.

Respect des bonnes pratiques

- Annonces de préfixes trop spécifiques :
 - 5 annonces de préfixes IPv4 (> /24, RIPE-399) ;
 - 43 annonces de préfixes IPv6 (> /48, RIPE-532) ;
- AS_PATH avec des numéros d'AS privés.



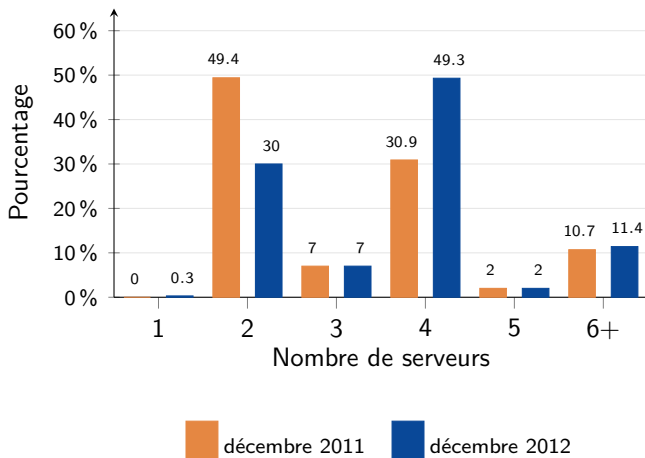
Sous l'angle de l'infrastructure DNS

Sources de données et mesures

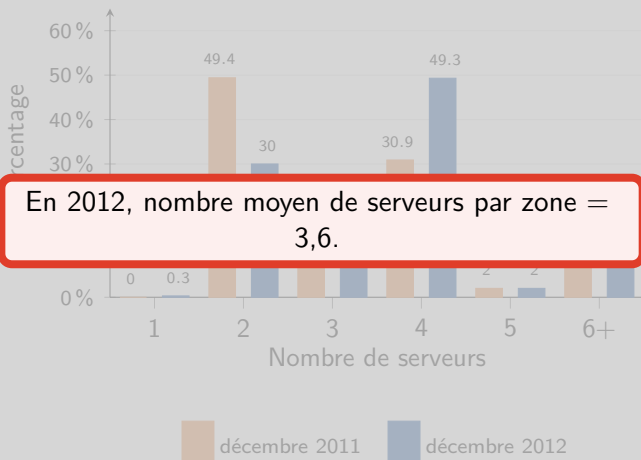
- Plateforme *DNSWitness*.
- Domaines de la zone *.fr*.
- Publications DNS des zones déléguées.
- Trafic DNS reçu par des serveurs de la zone *.fr*.



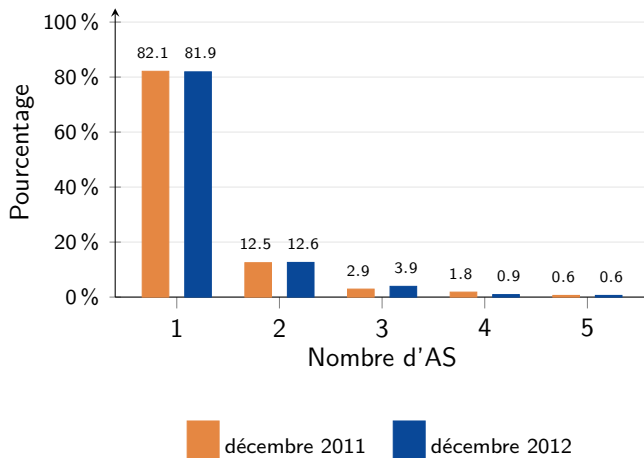
Distribution topologique des serveurs DNS faisant autorité



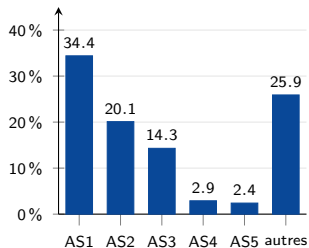
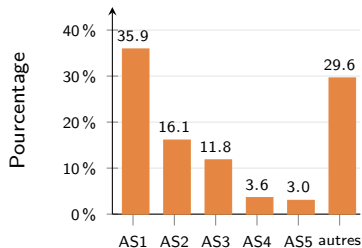
Distribution topologique des serveurs DNS faisant autorité



Distribution topologique des serveurs DNS faisant autorité



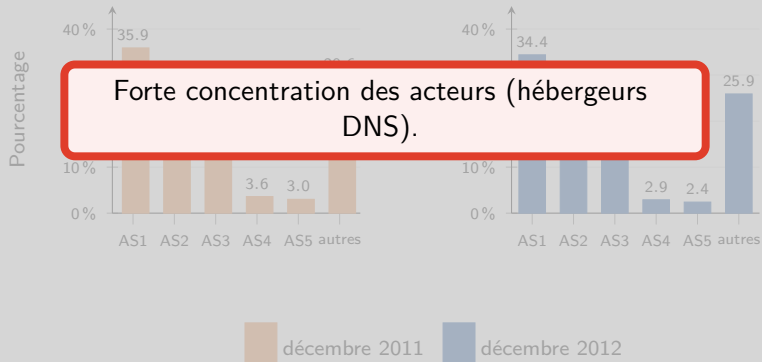
Distribution topologique des serveurs DNS faisant autorité



■ décembre 2011 ■ décembre 2012



Distribution topologique des serveurs DNS faisant autorité



Déploiement de DNSSEC

DNSSEC :

- n'est pas un facteur de résilience en soi ;
- authentifie l'origine des données (évite l'empoisonnement de cache).

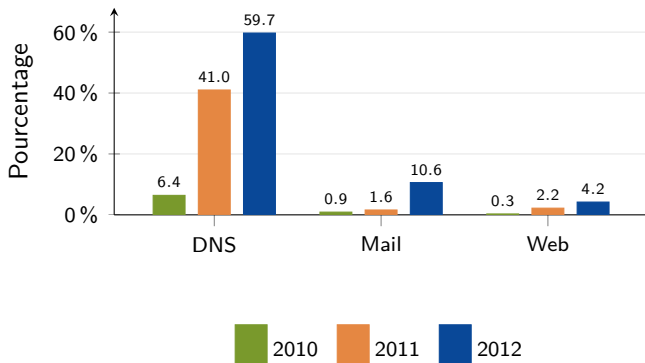
Déploiement de DNSSEC :

- signature de la racine : juillet 2010 ;
- signature de la zone .fr : septembre 2010 ;
- prise en compte des zones signées dans la zone .fr : avril 2011.

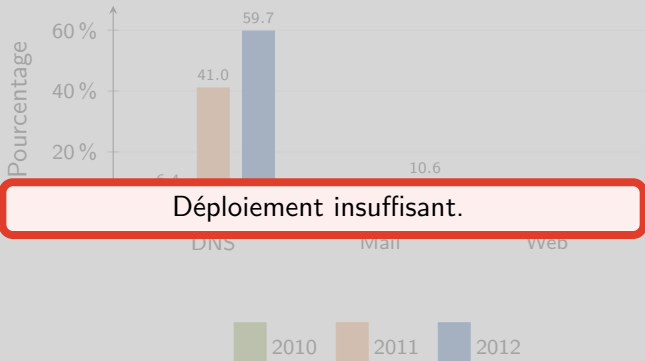
	Zones ayant un enregistrement DS
2011	33
2012	33790 (1,5%)



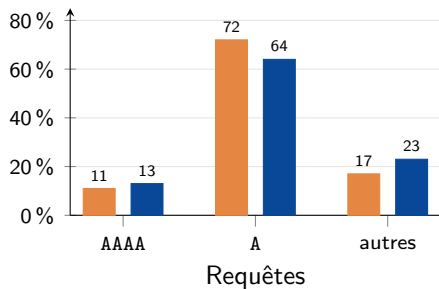
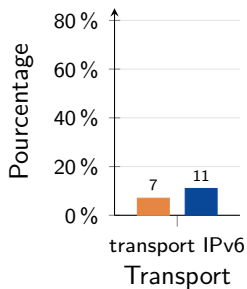
Déploiement d'IPv6



Déploiement d'IPv6



Déploiement d'IPv6



Résolveurs les plus demandeurs

Opérateur	Requêtes générées	Nombre de résolveurs
FAI américain	4,5%	1314
FAI américain	4,2%	1
Moteur de recherche	3,6%	1626
<i>Registrar</i> français	3,6%	36744
FAI français	3,5%	908

Nombre de requêtes par AS



Résolveurs les plus demandeurs

Opérateur	Requêtes générées (% Total)	Requêtes générées (% AS français)	Nombre de résolveurs
<i>Registrar</i>	3,6%	33,4%	36744
FAI	3,5%	32,7%	908
Réseau universitaire	1,3%	12,6%	1801
FAI	0,5%	4,6%	24
FAI	0,4%	3,9%	1

Nombre de requêtes par AS français



Conclusion & recommandations

Conclusion & recommandations

« Concernant les protocoles BGP et DNS, la situation de l'Internet français est aujourd'hui acceptable, mais rien ne garantit que cela suffise à l'avenir. »

Rapport 2012 de l'observatoire de la résilience

Recommandations

- Déclarer les objets route, et les maintenir à jour, afin de faciliter le filtrage d'annonces BGP illégitimes et la détection.
- Déployer IPv6 pour anticiper des problèmes.
- Appliquer les bonnes pratiques BGP au niveau des interconnexions entre opérateurs.
- Répartir les serveurs DNS faisant autorité au sein de différents opérateurs pour limiter les effets d'une panne.



Comment pouvons-nous vous aider ?

Rapports « individualisés »

- communication des résultats des indicateurs du rapport :
 - usurpations ;
 - filtrage à l'aide des objets route ;
 - cohérence des objets route ;
 - RPKI.

Comment obtenir le rapport ?

- un des `mnt-x` de l'aut-num a un objet `key-cert` dans la base `whois` du RIPE avec une clé permettant de chiffrer ;
- vous avez jusqu'au 30 septembre prochain pour vous manifester ;
- contact : `rapport.observatoire@ssi.gouv.fr`.



Comment pouvez-vous nous aider ?

Collecteur BGP de l'observatoire

- collecteur BGP au France-IX ;
- données collectées à des fins de recherche uniquement ;
- fait l'objet d'une convention :
 - vous pouvez vous retirer quand vous le souhaitez ;
 - vous pouvez demander la destruction de l'intégralité des données collectées.

Comment s'interconnecter ?

- faire une demande à : rapport.observatoire@ssi.gouv.fr.



Questions

Rapports et guides

- Rapport 2011 disponible.
- Rapport 2012 disponible.
- Guide de bonnes pratiques de configuration de BGP disponible à la fin du mois.

