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

9 juillet 2013

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 :

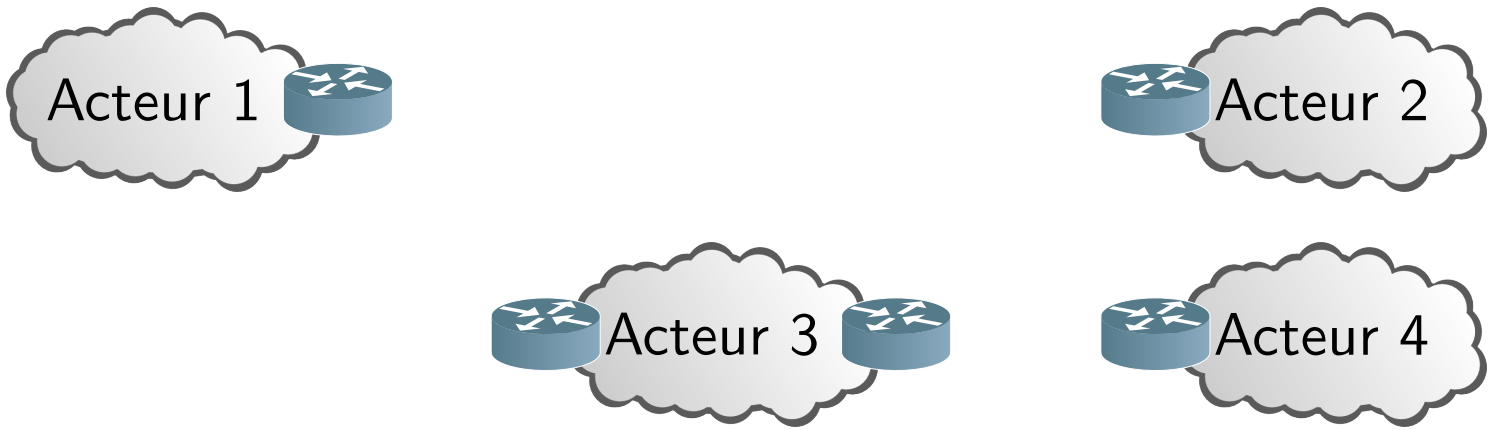
- la structure de l'Internet (routage & nommage) ;
- le trafic et les services (HTTPS, SPAM, botnets...).

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

Sous l'angle du protocole BGP

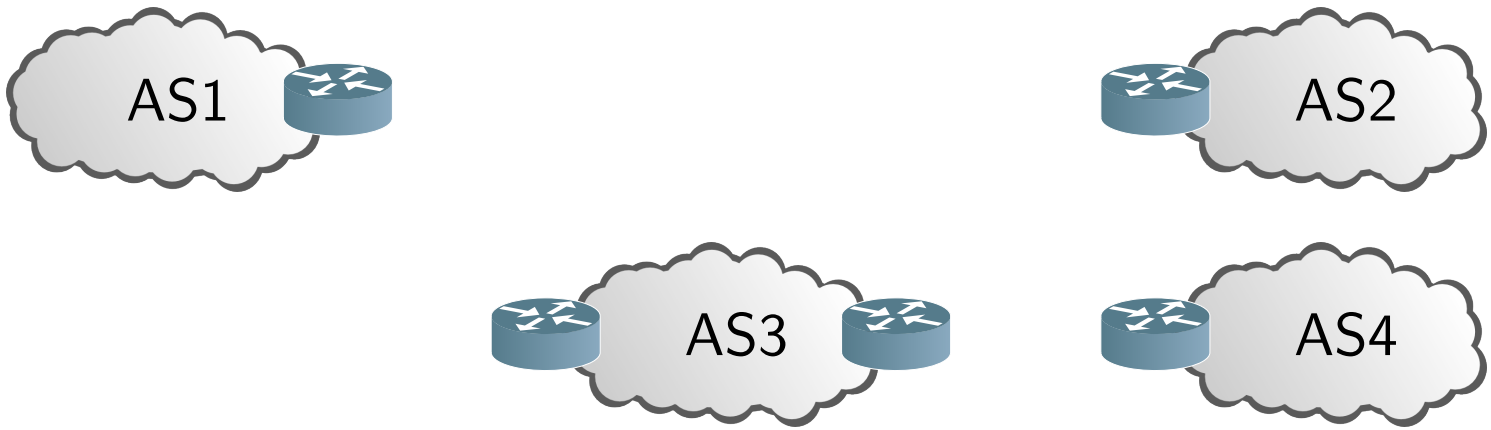
Border Gateway Protocol (BGP)

BGP est le protocole de routage utilisé par tous les acteurs/opérateurs de l'Internet.



Border Gateway Protocol (BGP)

BGP est le protocole de routage utilisé par tous les acteurs/opérateurs de l'Internet.

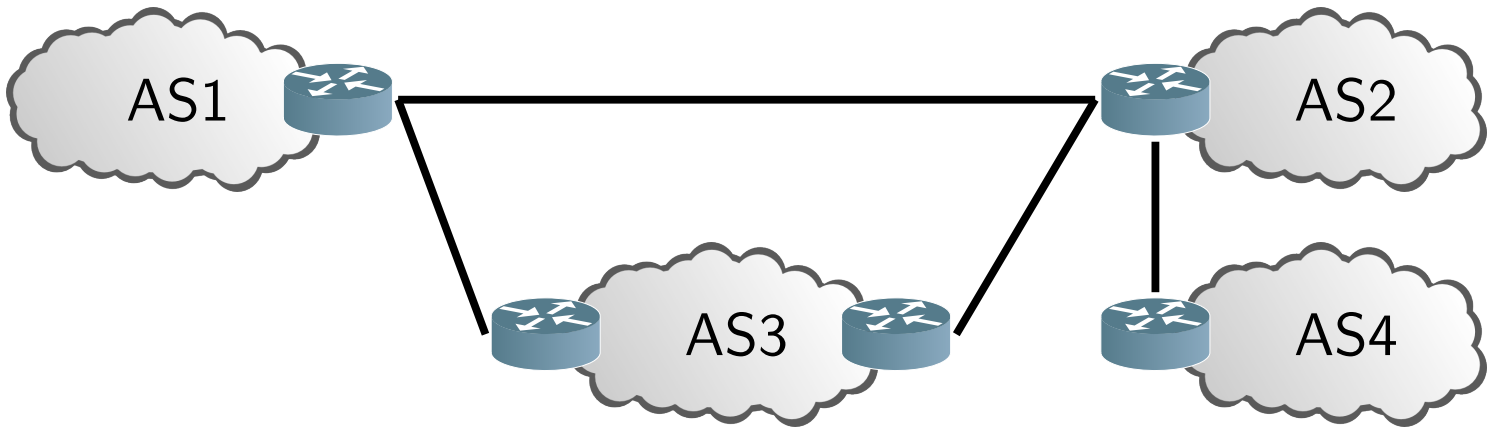


Le protocole BGP :

- associe un numéro d'*AS* (*Autonomous System*) à un acteur ;

Border Gateway Protocol (BGP)

BGP est le protocole de routage utilisé par tous les acteurs/opérateurs de l'Internet.

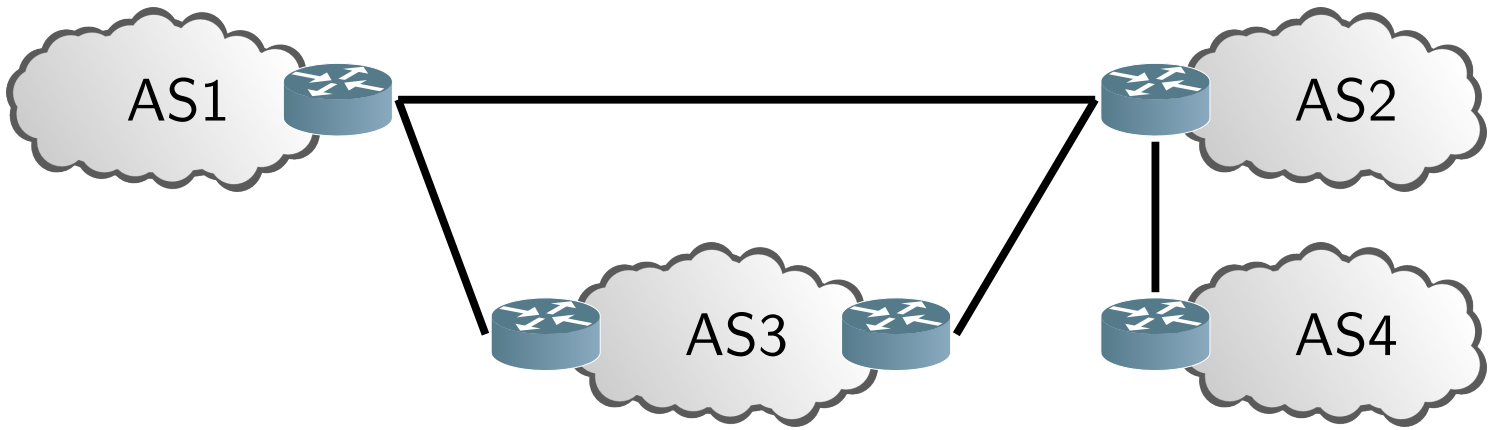


Le protocole BGP :

- associe un numéro d'*AS* (*Autonomous System*) à un acteur ;
- interconnecte directement ces acteurs :
  - propagation d'informations de routage de proche en proche ;

Border Gateway Protocol (BGP)

BGP est le protocole de routage utilisé par tous les acteurs/opérateurs de l'Internet.



Le protocole BGP :

- associe un numéro d'*AS* (*Autonomous System*) à un acteur ;
- interconnecte directement ces acteurs :
  - propagation d'informations de routage de proche en proche ;
- assure une visibilité mondiale à ces acteurs.

Définition de l'Internet français

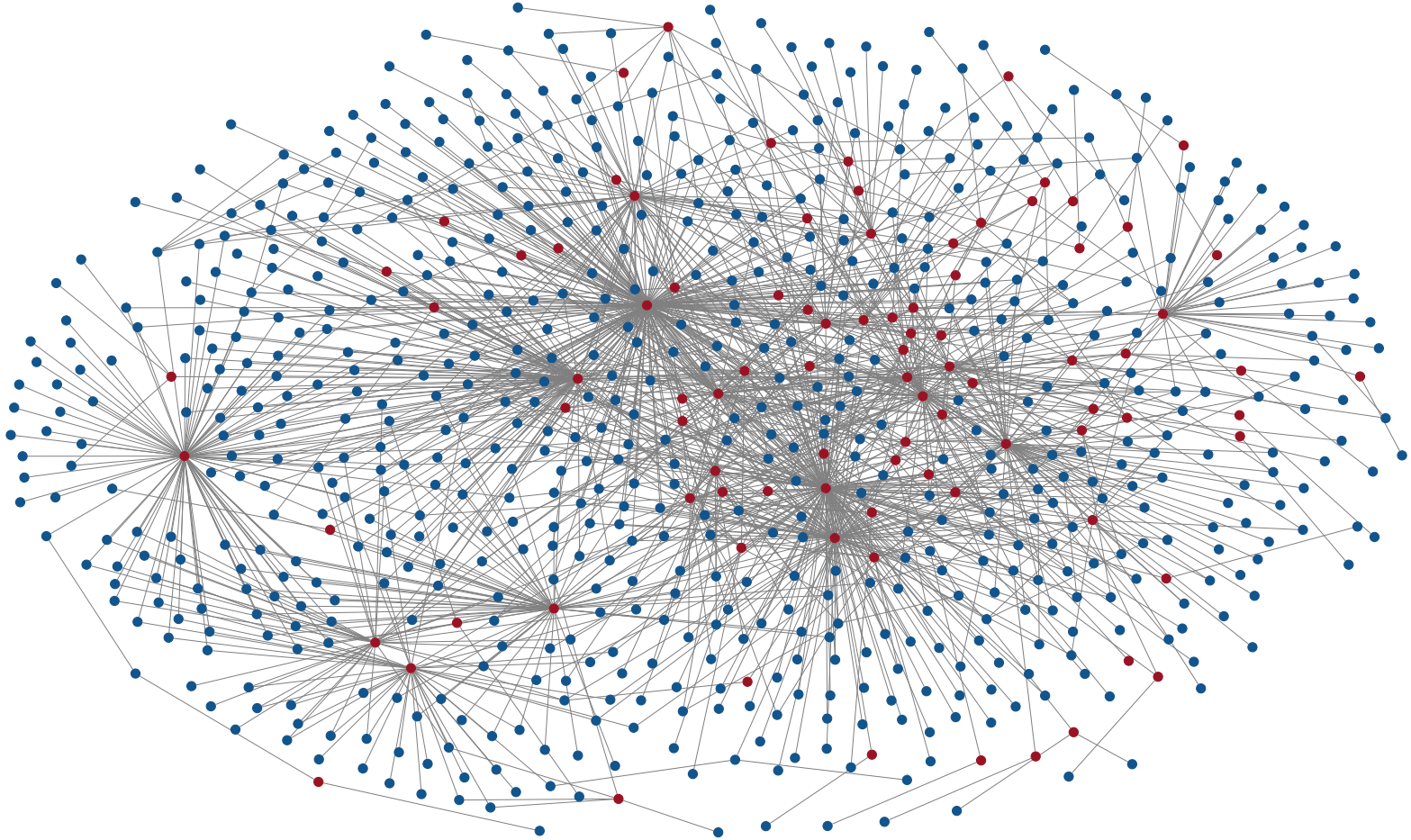
Qu'est-ce que l'Internet français ?

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

Résultats

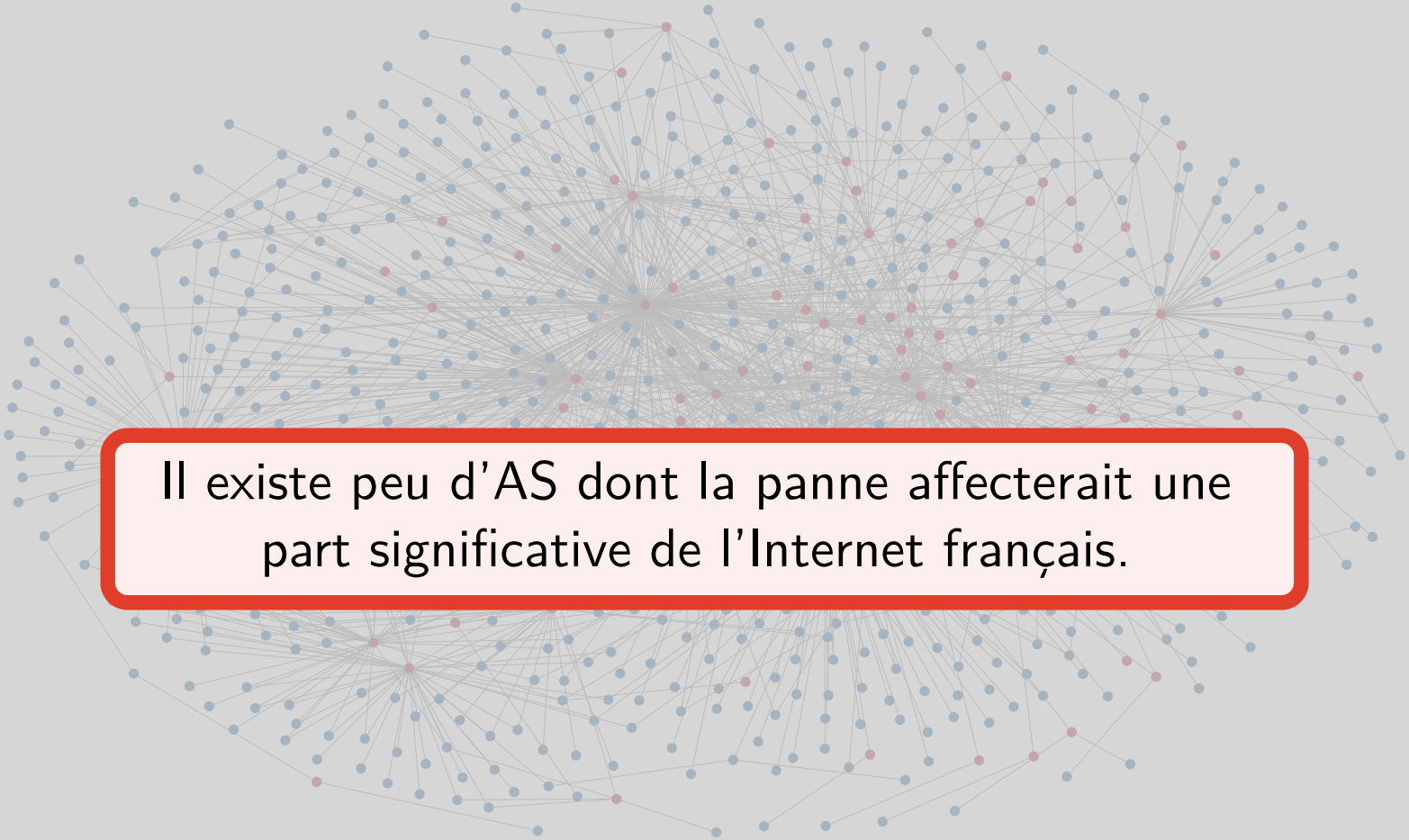
- 1270 AS français (entre 700 et 800 sont visibles) ;
- comparaison avec des bases publiques existantes :
  - notre base comporte entre 40 et 70 en plus ;
  - 9 AS manquants dans notre base.

Connectivité des AS



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

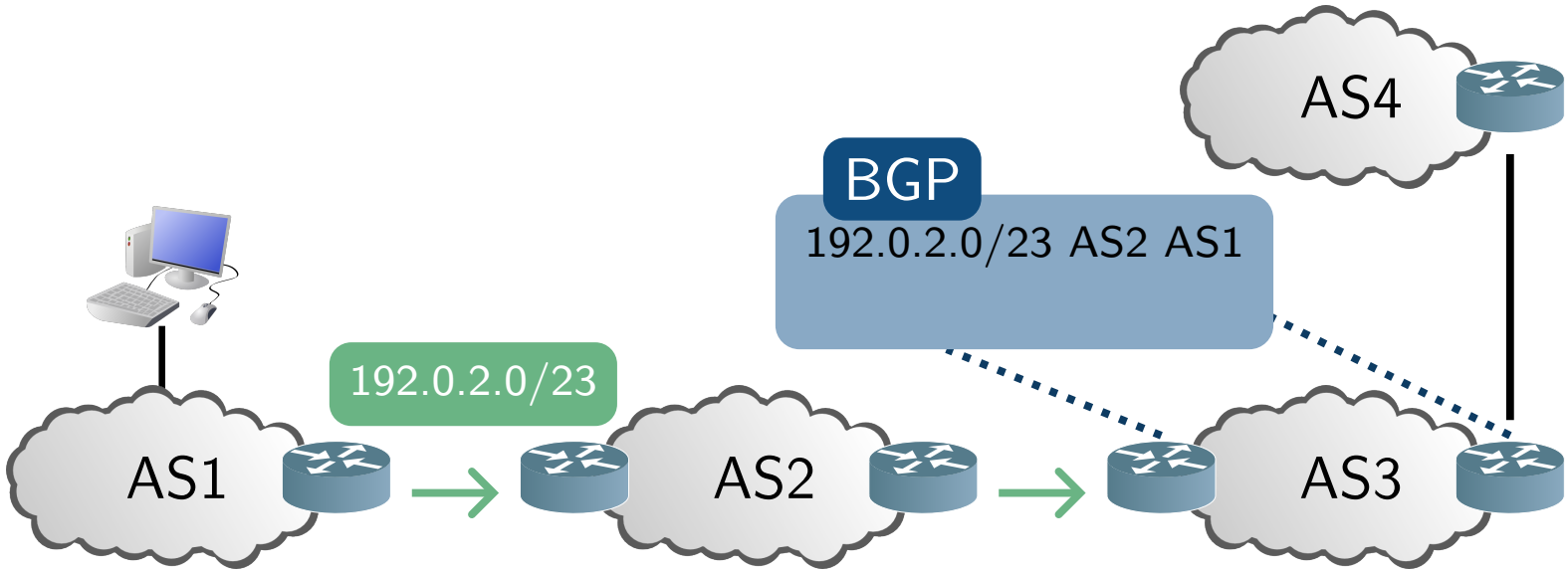
Connectivité des AS



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

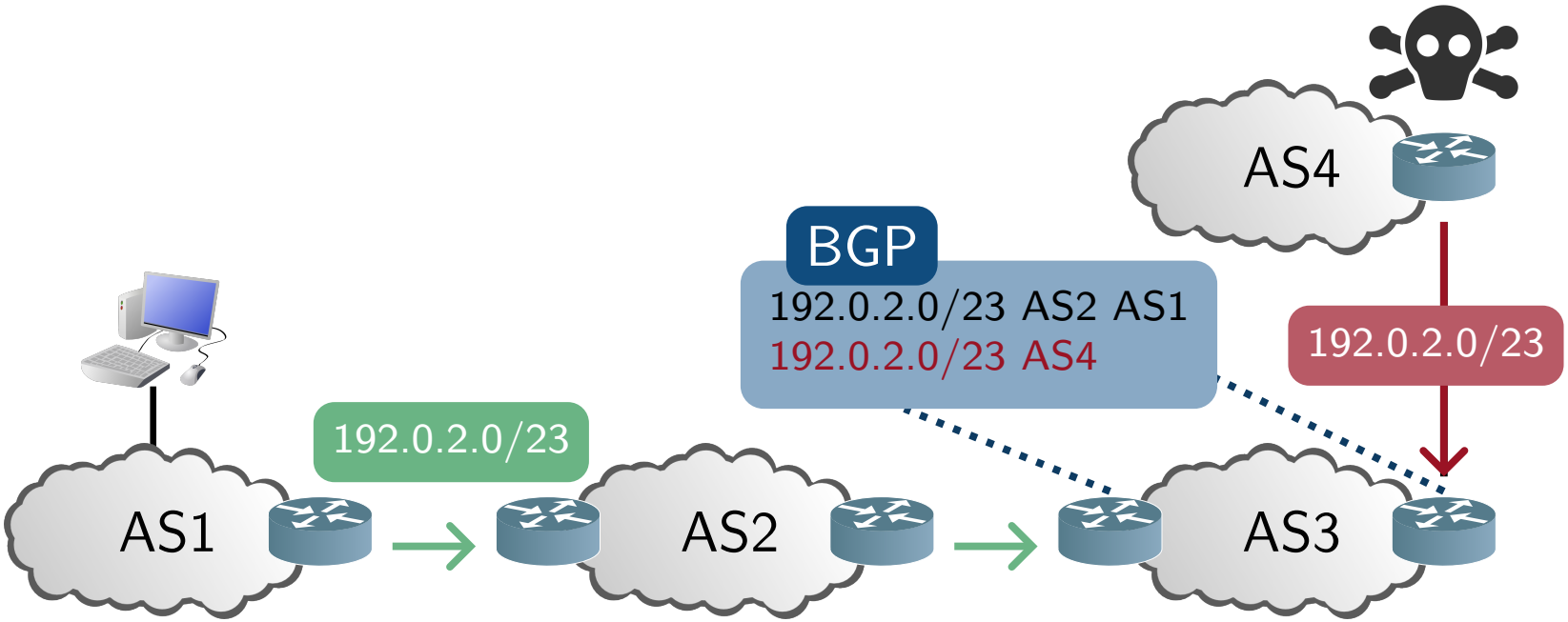
- En bleu, les AS français.
- En rouge, les AS dont la disparition pourrait en isoler d'autres.

Principe de fonctionnement de BGP



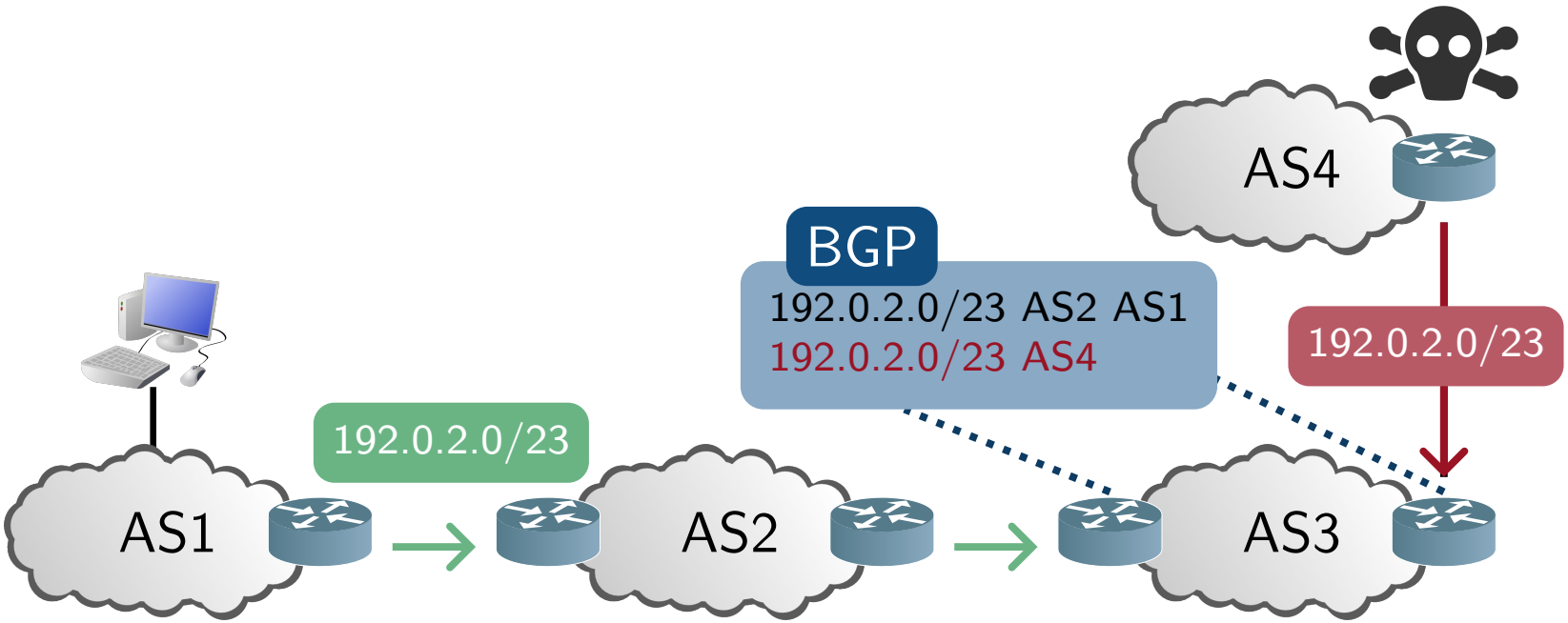
- Annonces de préfixes (blocs d'adresses IP) entre AS : échange de routes.

Principe de fonctionnement de BGP



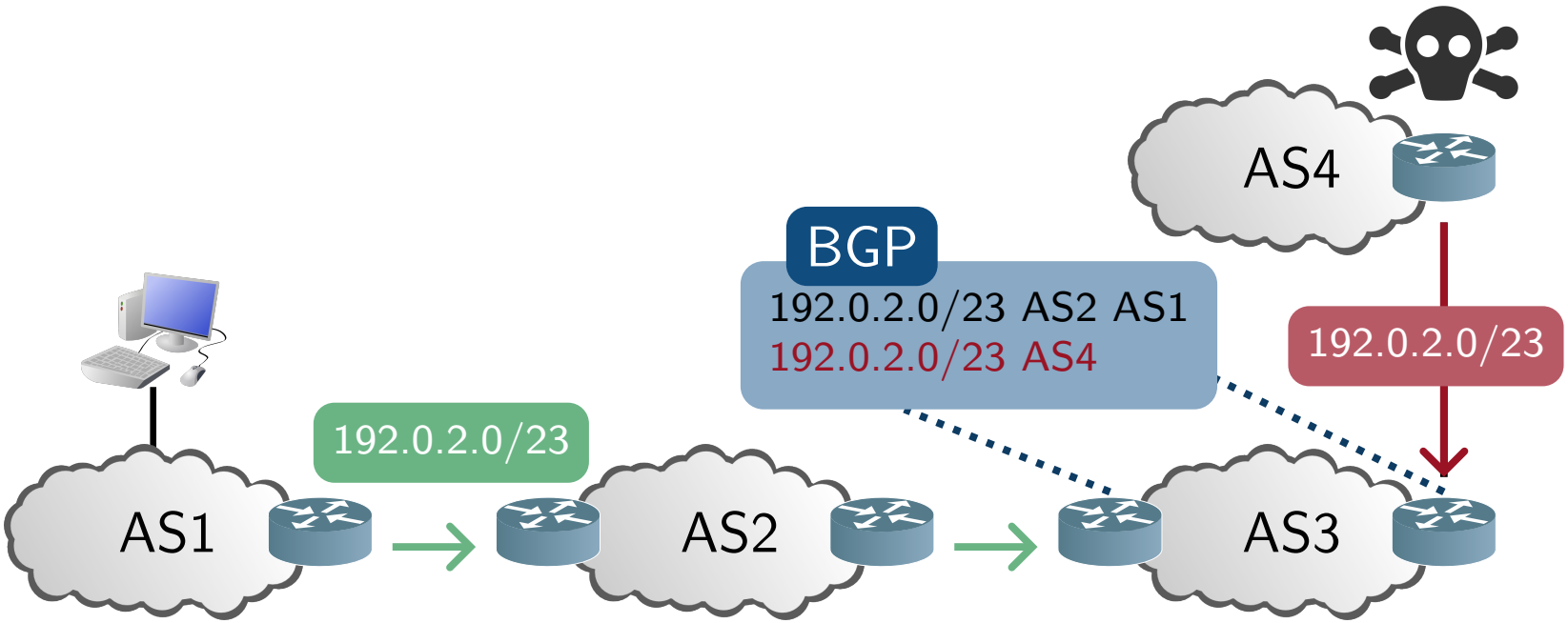
- Annonces de préfixes (blocs d'adresses IP) entre AS : échange de routes.
- Annonce d'un préfixe appartenant à un autre AS, sans en avoir la délégation : usurpation.

Les usurpations de préfixes



- Règle du chemin le plus court : peut entraîner un détournement de trafic.

Les usurpations de préfixes



- Règle du chemin le plus court : peut entraîner un détournement de trafic.
- Deux AS peuvent-ils annoncer le même préfixe ?
  - Oui : délégation d'un préfixe à un AS client par exemple.

Légitimité des annonces : les objets `route`

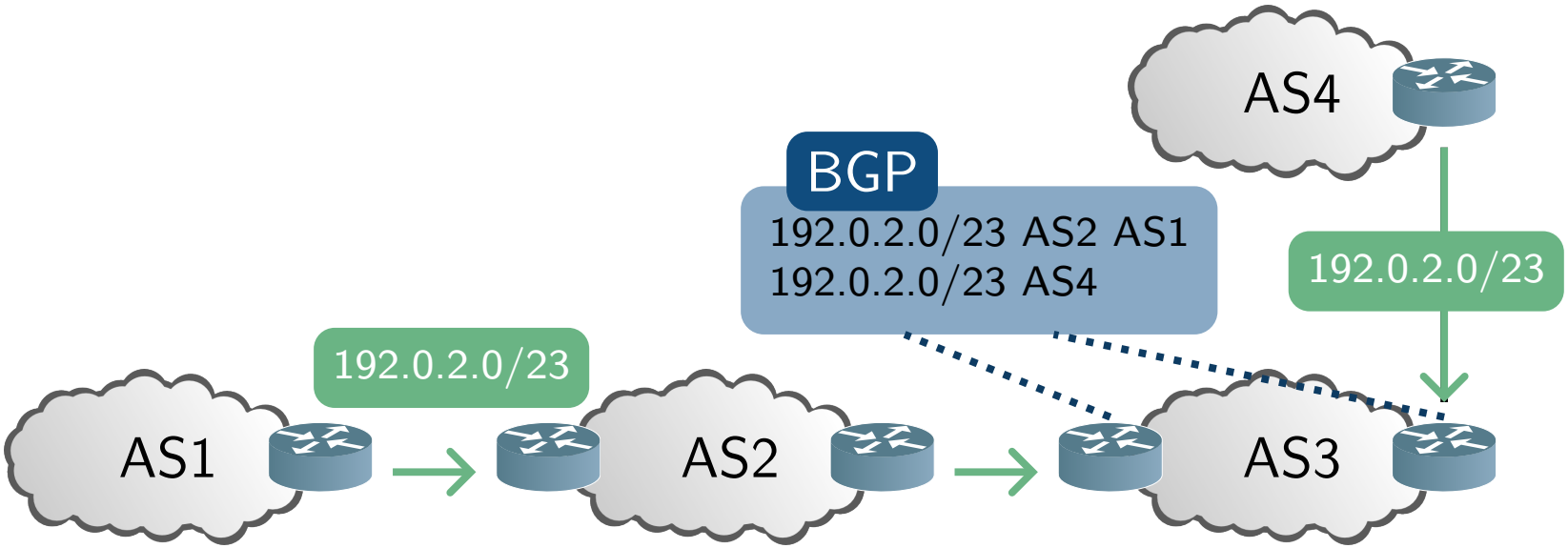
Comment déterminer la légitimité d'une annonce de préfixe ?

- Comparer les annonces avec une base de données d'objets `route` (RIPE-NCC pour l'Europe).
- Objet `route` : déclaration d'un préfixe annoncé en BGP.

Les objets `route` peuvent être utilisés pour :

- créer des filtres d'annonces sur les routeurs BGP ;
- détecter des usurpations ;
- obtenir des informations sur un AS ou un préfixe.

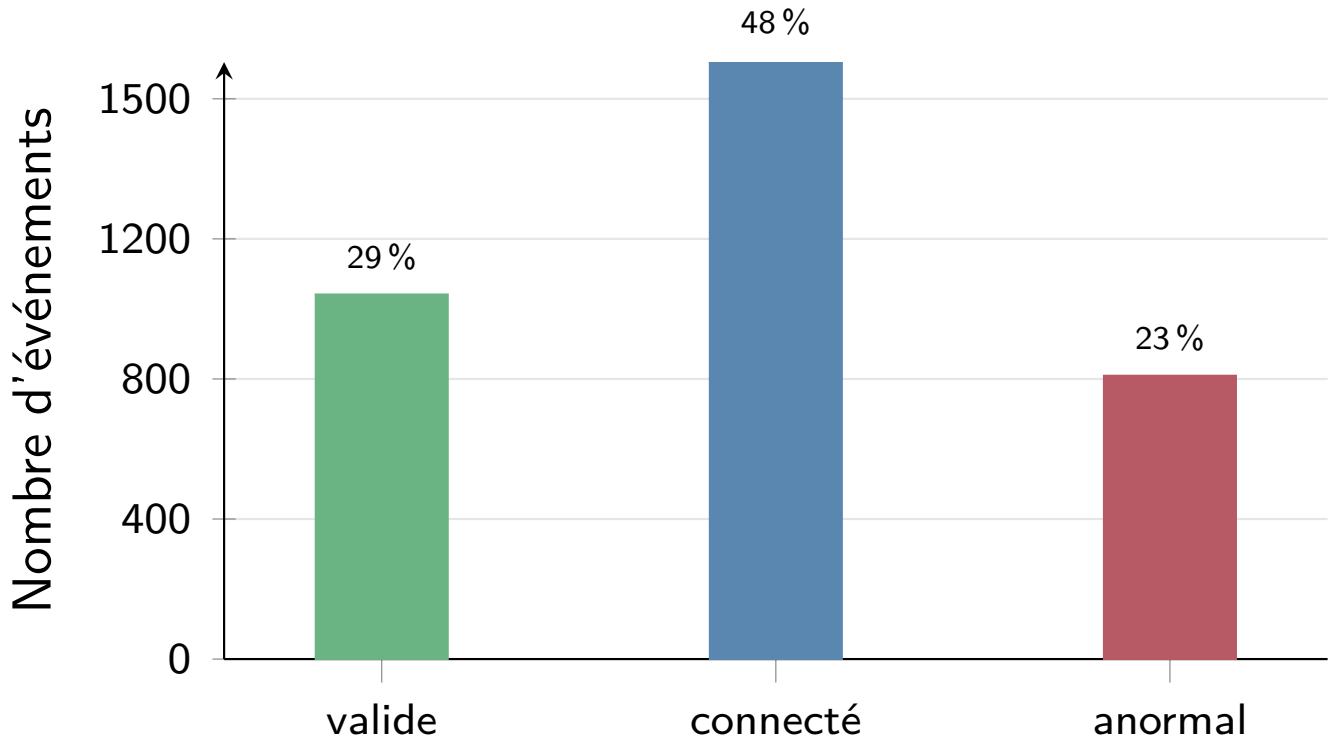
Les objets `route` en pratique



Déclaré par l'AS1, l'objet `route` indique que l'AS4 a le droit d'annoncer le préfixe 192.0.2.0/23.

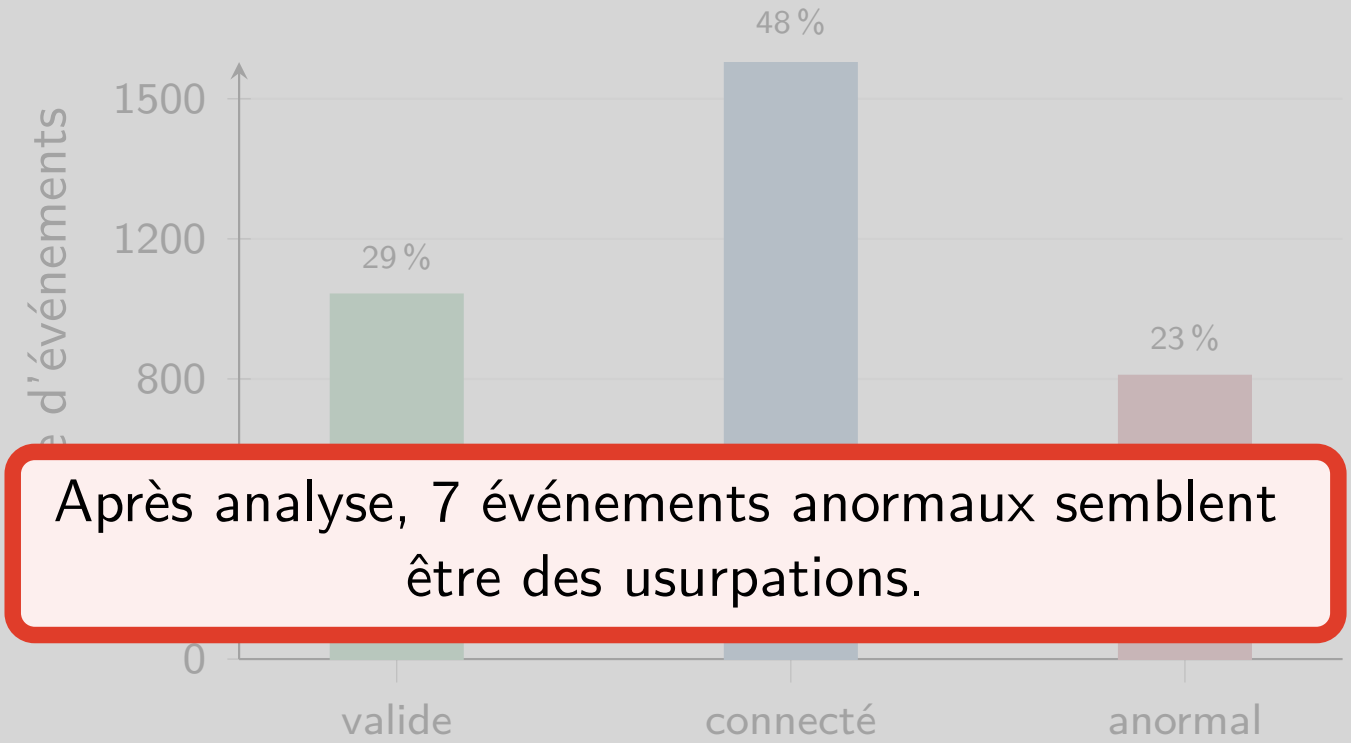
```
$ whois -T route 192.0.2.42
descr:          Objet route d'exemple
route:          192.0.2.0/23
origin:         AS-4
mnt-by:         JCSA-MNT
```

Détecter les 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.

Détecter les usurpations de préfixes



Après analyse, 7 événements anormaux semblent être des usurpations.

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

Filtrage via les 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.

Filtrage via les objets `route`

	janvier 2012	décembre 2012
Correspondance	78%	82%

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.

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	3

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

Respect des bonnes pratiques

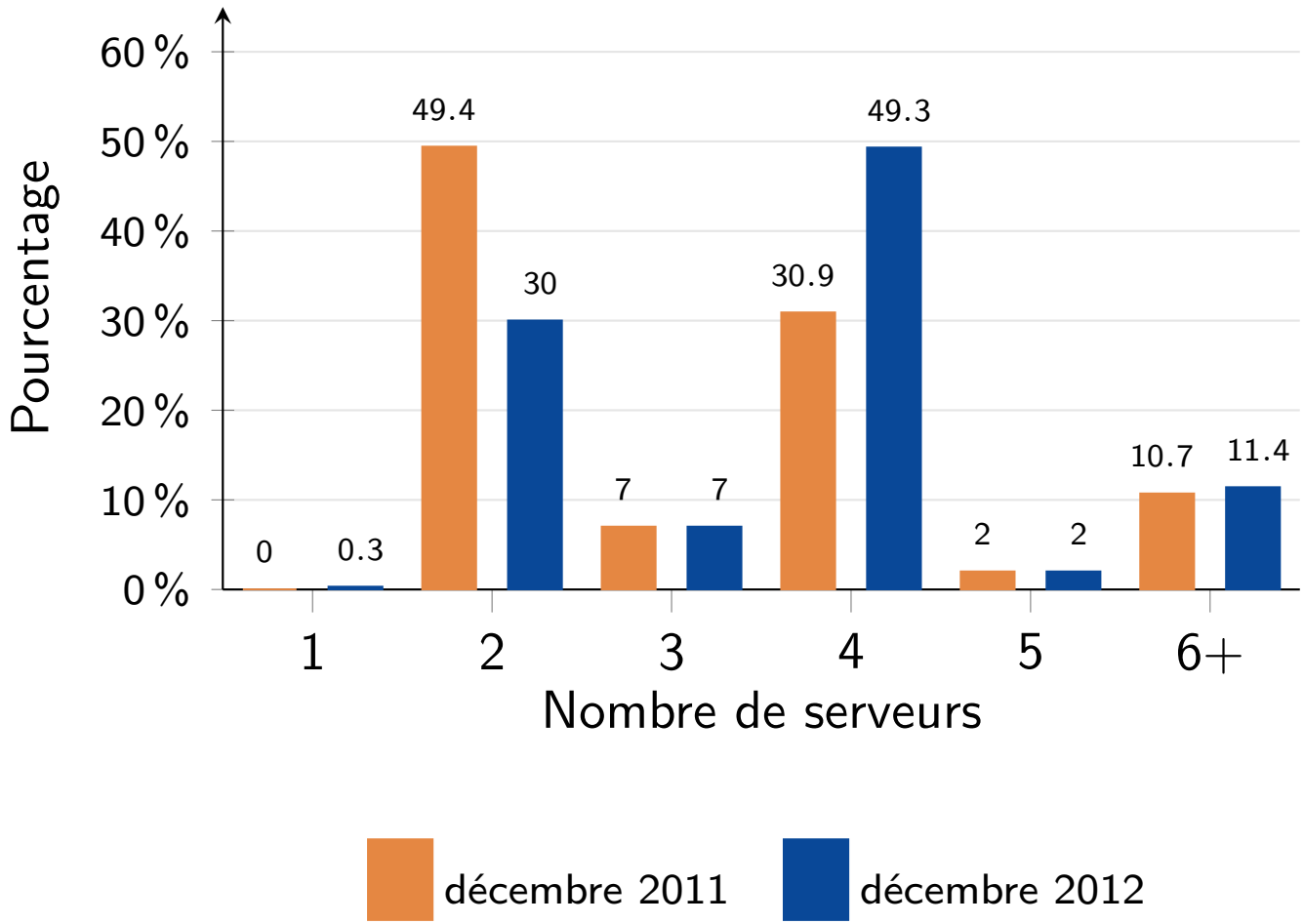
- Annonces de préfixes trop spécifiques :
  - 5 annonces de préfixes IPv4 (> /24, RIPE-399) ;
  - 43 annonces de préfixes IPv6 (> /48, RIPE-532) ;
- `AS_PATH` avec des numéros d'AS privés.

Sous l'angle de l'infrastructure DNS

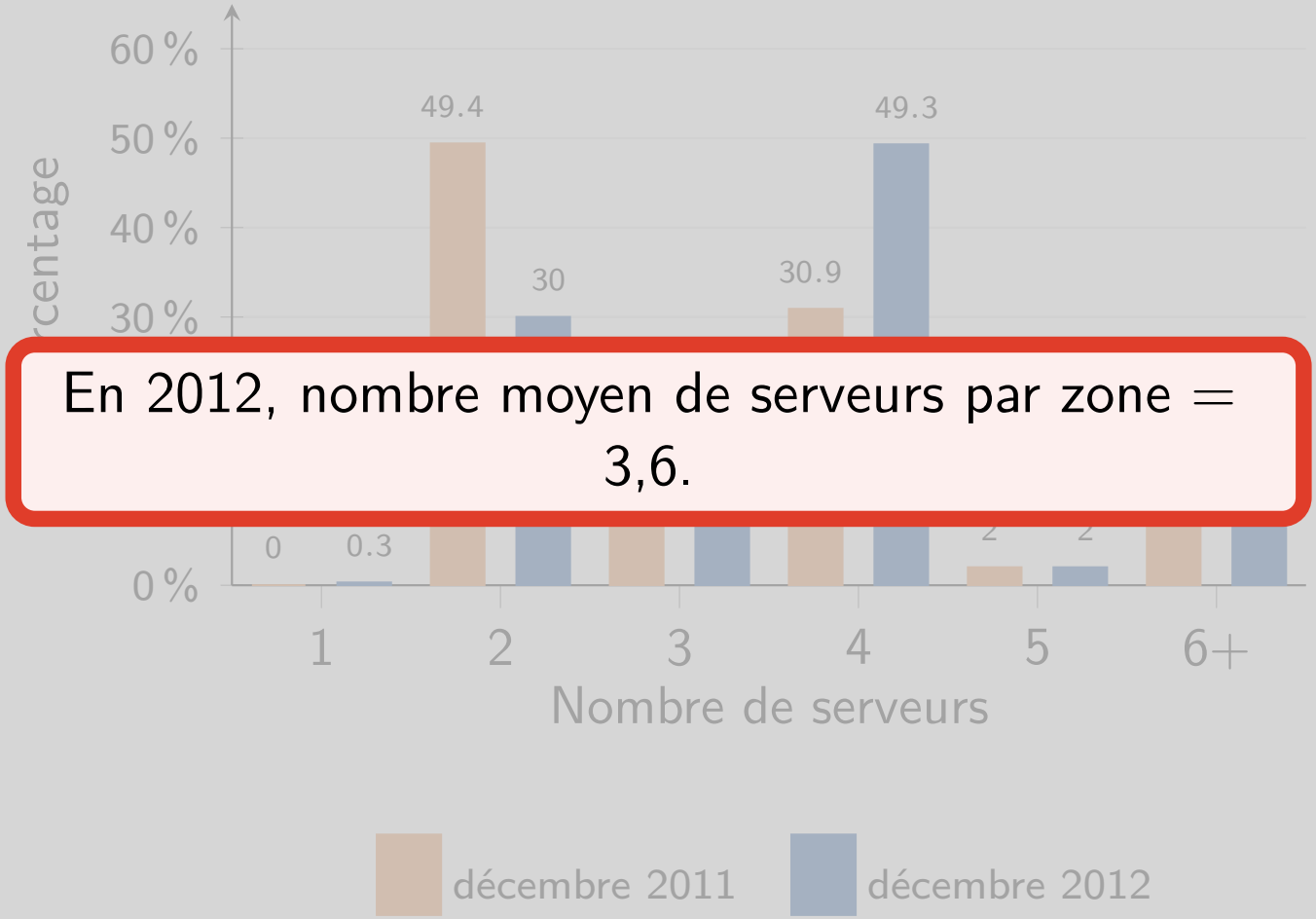
Sources de données et mesures

- 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

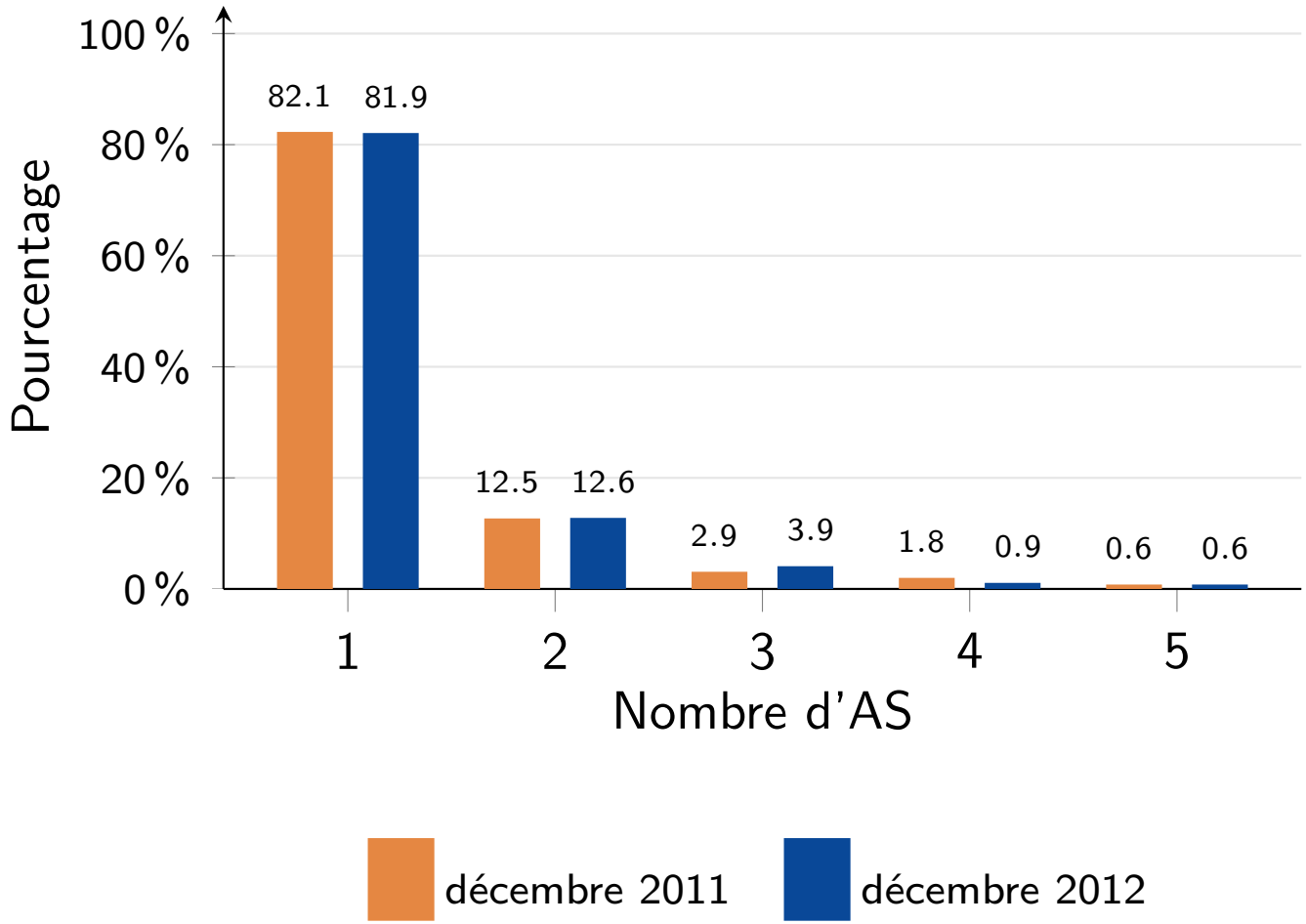


Distribution topologique des serveurs DNS faisant autorité

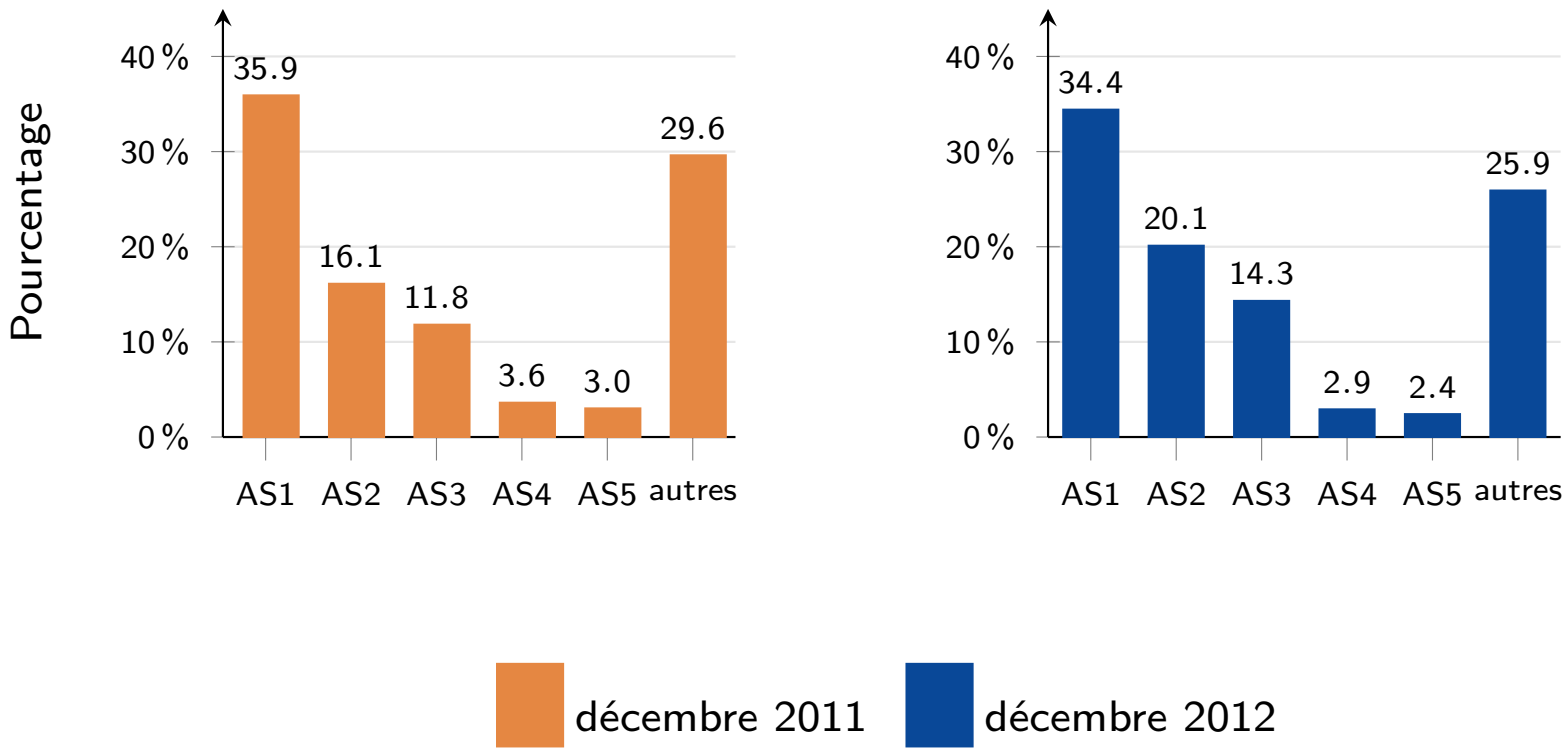


En 2012, nombre moyen de serveurs par zone = 3,6.

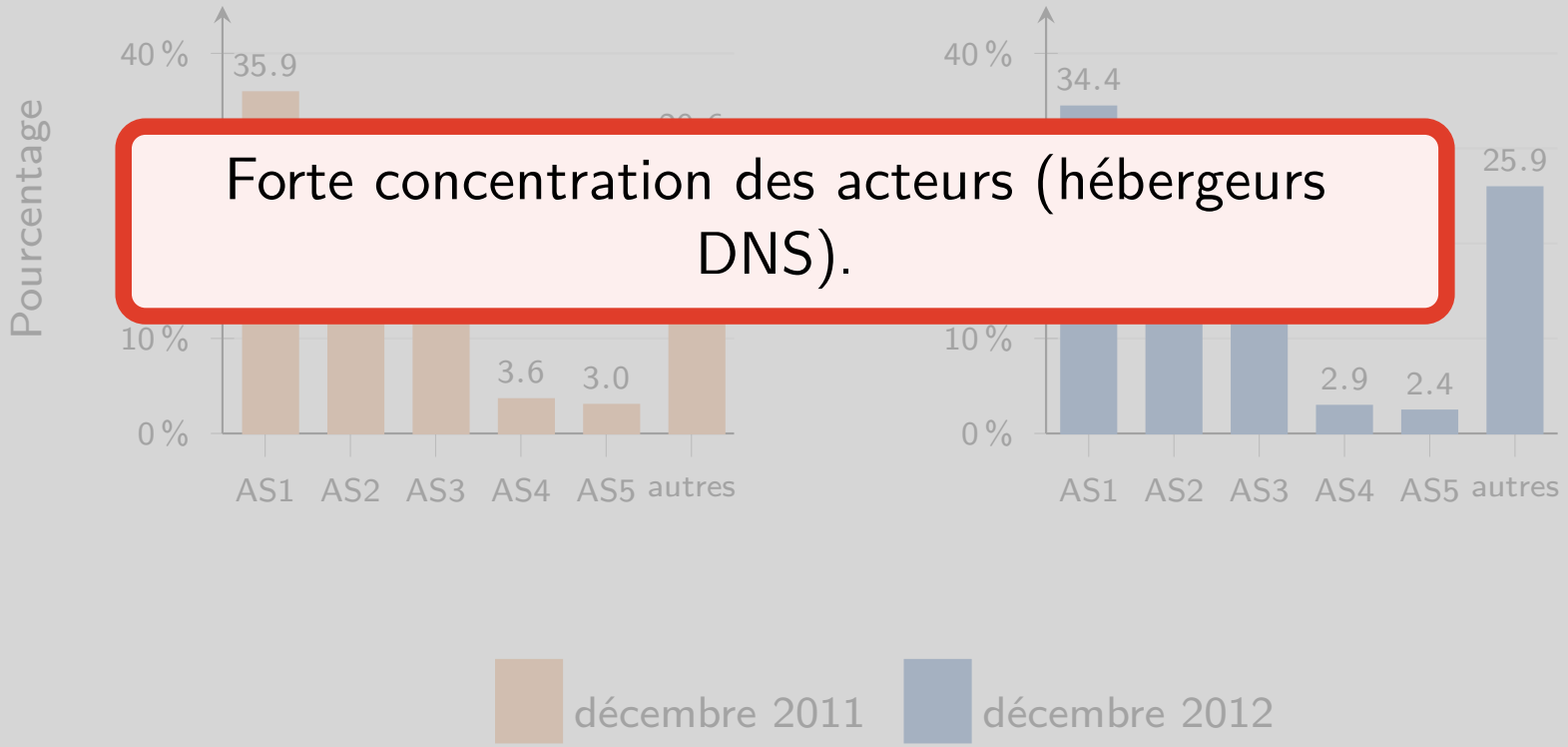
Distribution topologique des serveurs DNS faisant autorité



Distribution topologique des serveurs DNS faisant autorité



Distribution topologique des serveurs DNS faisant autorité



Forte concentration des acteurs (hébergeurs DNS).

Déploiement de DNSSEC

DNSSEC :

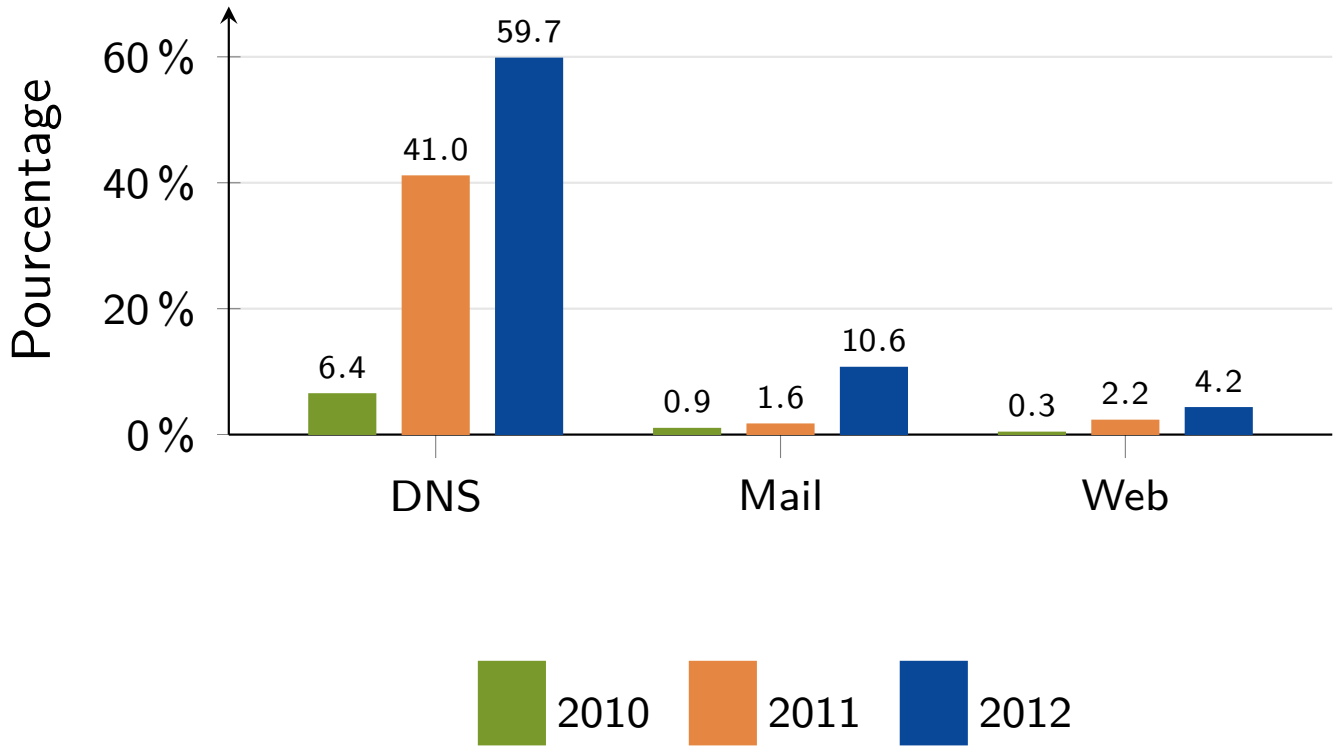
- n'est pas un facteur de résilience en soi ;
- authentifie l'origine des données (évite l'empoisonnement de cache).

Déploiement de DNSSEC :

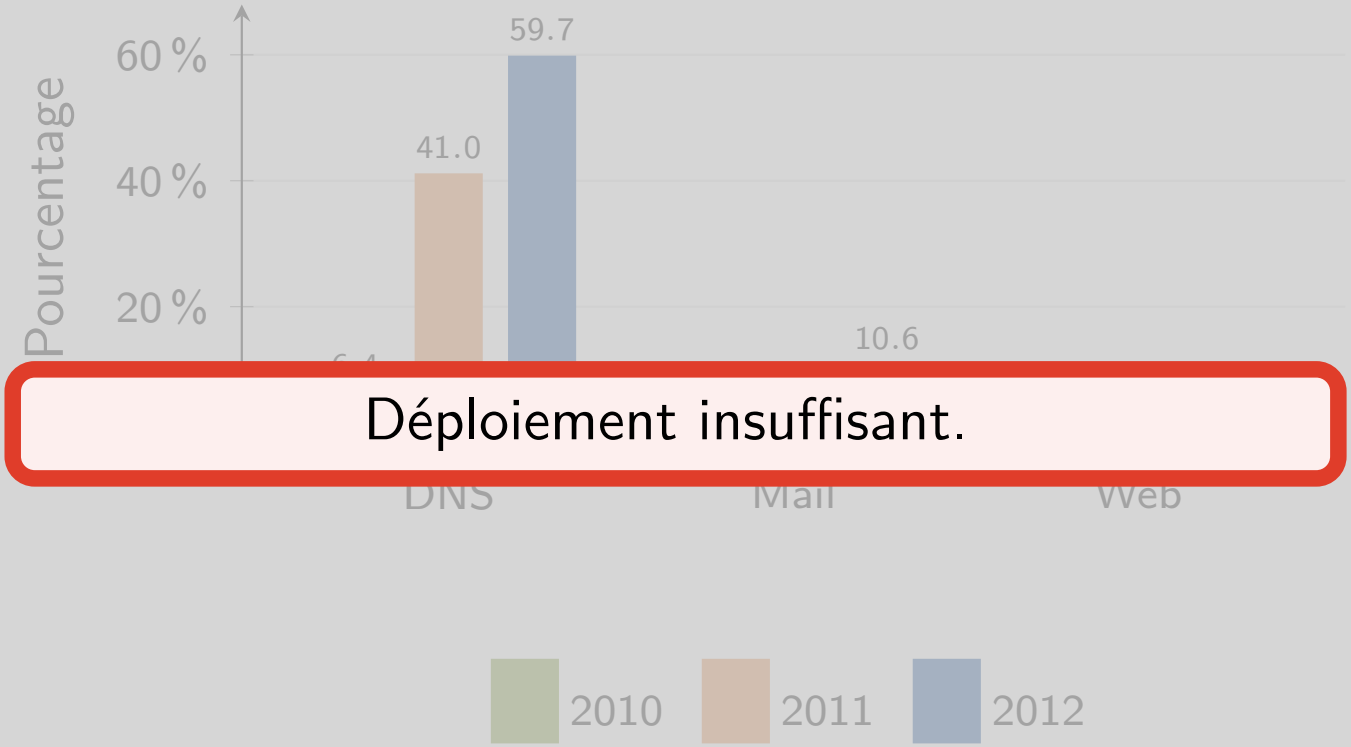
- signature de la racine : juillet 2010 ;
- signature de la zone `.fr` : septembre 2010 ;
- prise en compte des zones signées dans la zone `.fr` : avril 2011.

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

Déploiement d'IPv6

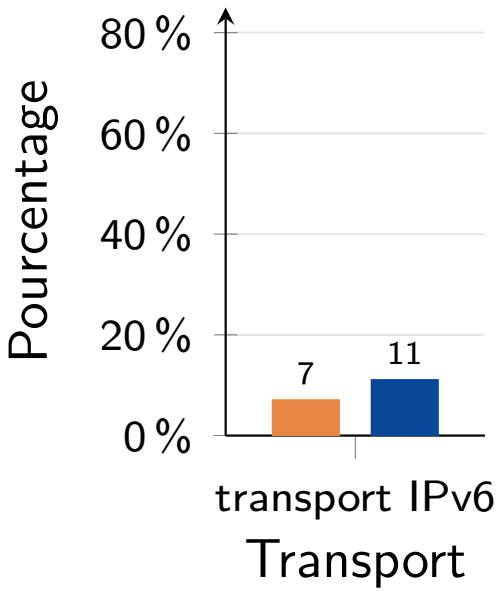


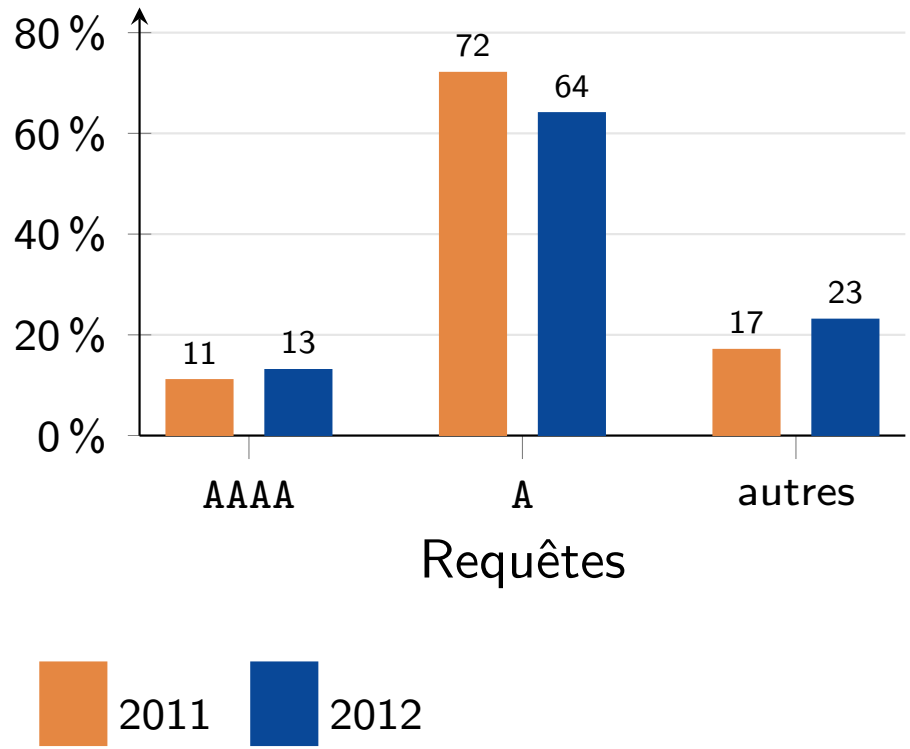
Déploiement d'IPv6



Déploiement insuffisant.

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
Registrar 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
Registrar	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

« 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.

Questions

Rapports et guides

- Rapport 2011 disponible.
- Rapport 2012 disponible.
- Guide de bonnes pratiques de configuration de BGP disponible à la rentrée prochaine.