Observatoire de la résilience de l'Internet français

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

rapport.observatoire@ssi.gouv.fr

7 juin 2013

Contexte

L'Observatoire

- qui ?
  - ANSSI, Afnic, et des acteurs de l'Internet français
- quoi ?
  - mesures et analyses techniques
- quand ?
  - depuis plus de deux ans

Nos motivations

- Internet est méconnu
- pas d'analyses d'incident sur la France
- comprendre si les bonnes pratiques sont bien appliquées
- fournir un rapport annuel anonymisé à la communauté

Tester 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 ne peut pas tester si l'Internet est robuste
  - trop grand, trop gros, trop fragile ?
- il faut se contenter d'observer

Quel est le lien entre l'Observatoire & la securité ?

1. étudier le déploiement de nouvelles technologies
   - quels sont leurs impacts ?
   - est-ce que les implémentations sont robustes ?

2. comprendre la situation actuelle
   - est-ce suffisant ?
   - peut-on faire mieux ?

3. parler *réseau* à un public technique passionné
   - pour faire avancer les choses
   - parler des bonnes pratiques *réseau*

Que peut-on observer ?

- la structure : BGP & DNS
- les services : TLS, P2P, ...
- les abus : DDoS, SPAM, botnets, ...
- les applications : google, twitter, le site du SSTIC, ...
- les logs : openssh, apache, ...

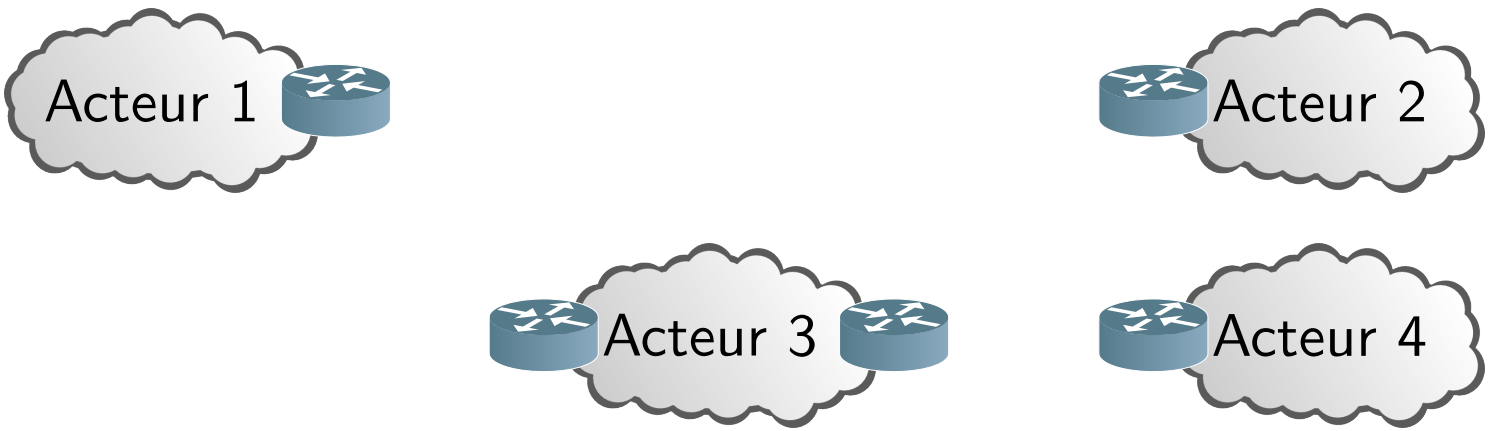
Les données

- archives BGP, et données publiques du RIPE-NCC
- les analyses DNS effectuées par l'Afnic utilisent leur connaissance de la zone `.fr`

Sous l'angle de BGP

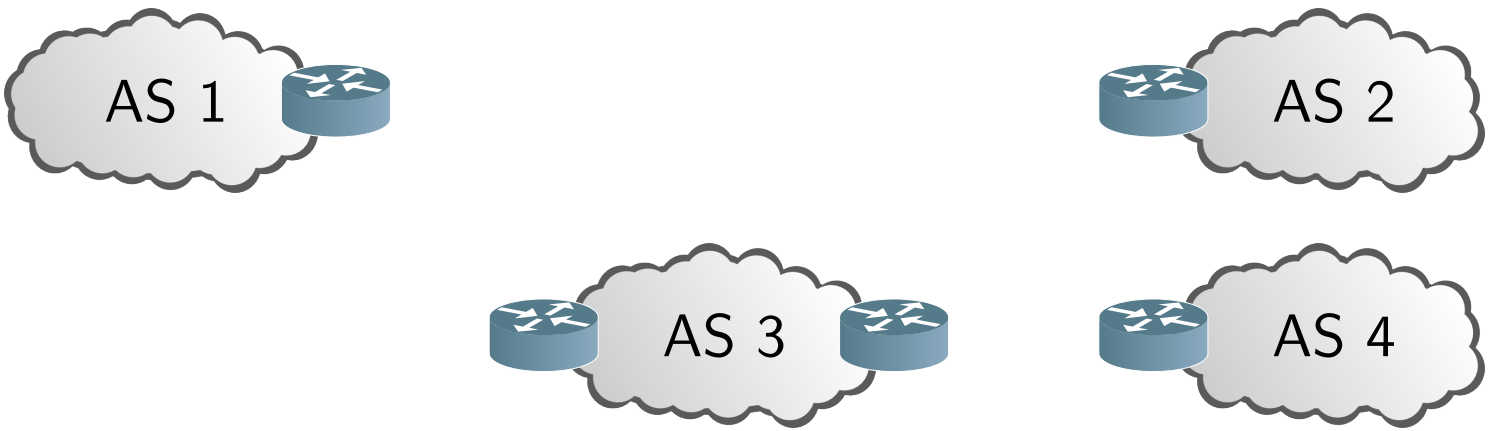
Border Gateway Protocol (BGP)

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.

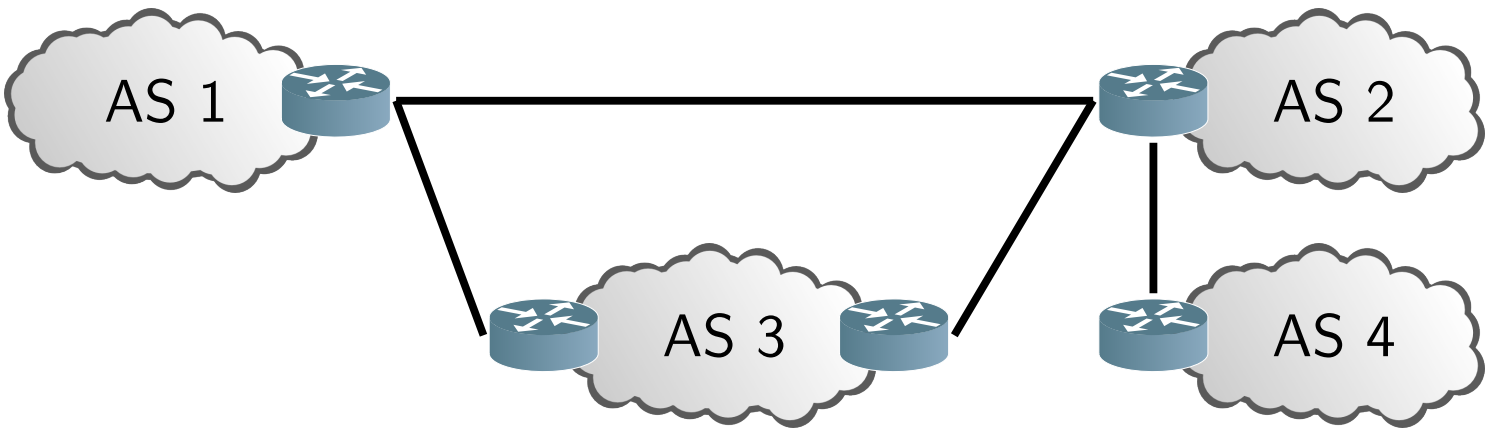


BGP :

- associe un *numéro d'AS* à un acteur

Border Gateway Protocol (BGP)

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

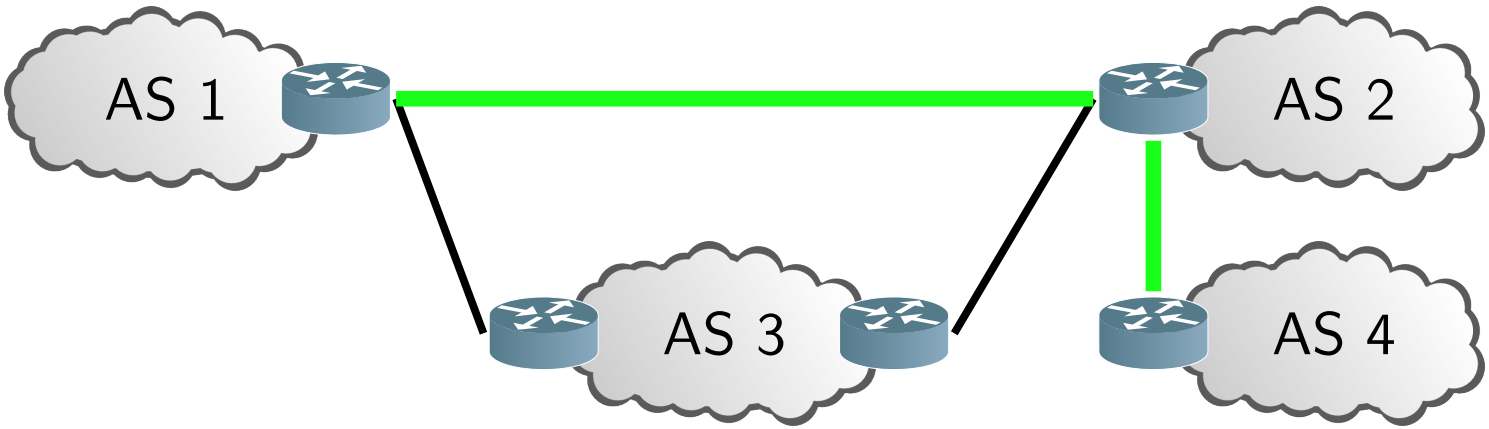


BGP :

- associe un *numéro d'AS* à un acteur
- interconnecte directement ces acteurs

Border Gateway Protocol (BGP)

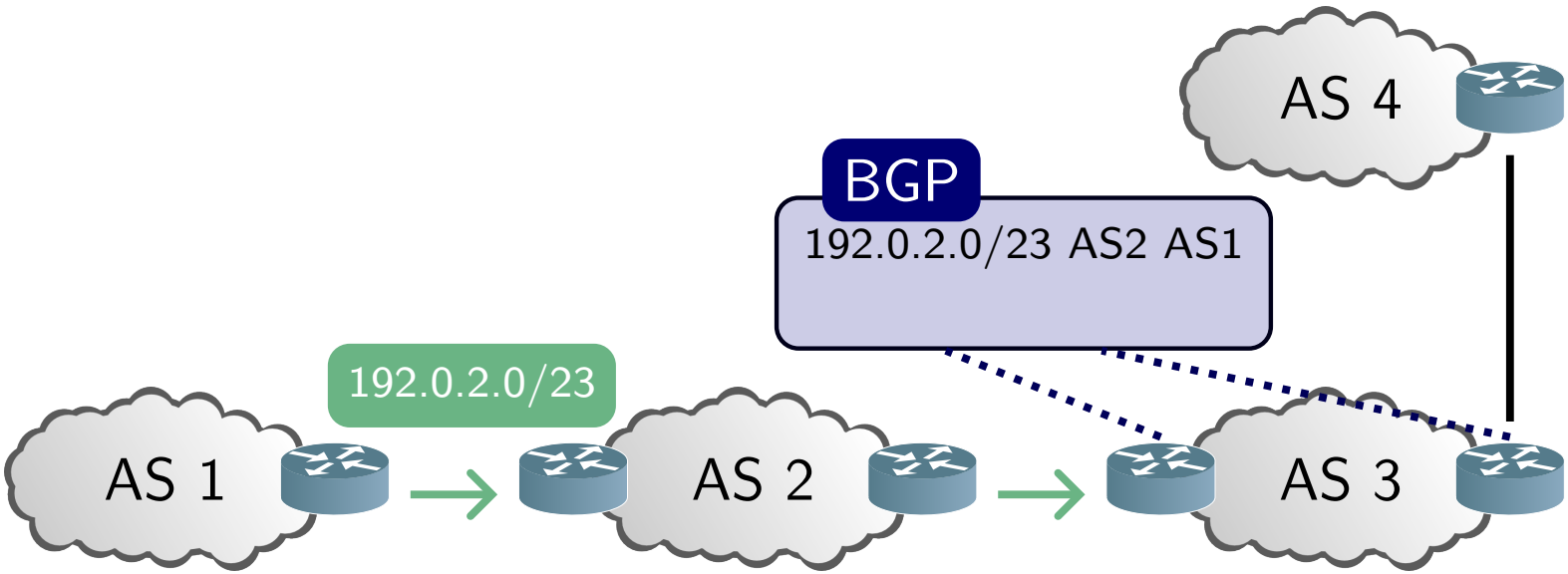
BGP est le protocole de routage utilisé par tous les acteurs/opérateurs de l'Internet.



BGP :

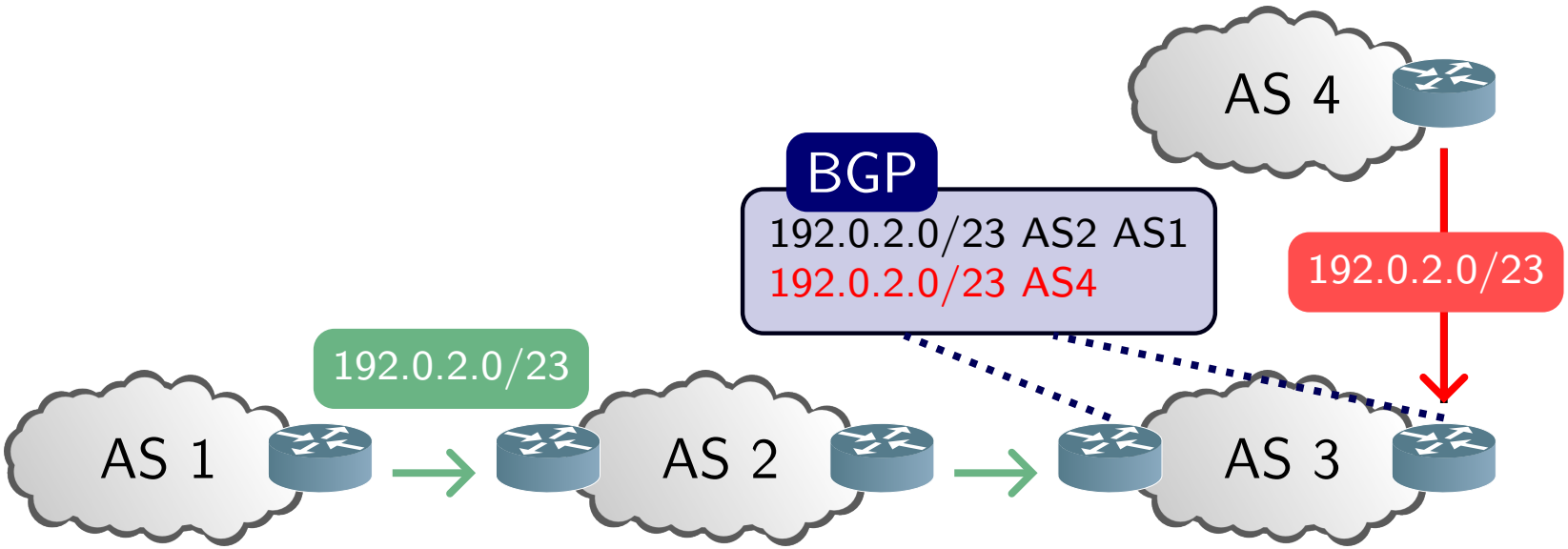
- associe un *numéro d'AS* à un acteur
- interconnecte directement ces acteurs
- assure une présence mondiale à ces acteurs

Usurpation de préfixes



Usurpation : annonce d'un préfixe par un AS ne le gérant pas

Usurpation de préfixes



Usurpation : annonce d'un préfixe par un AS ne le gérant pas

Par défaut, un routeur choisit les chemins les plus courts. L'AS 4 reçoit ainsi du trafic pour le préfixe 192.0.2.0/23.

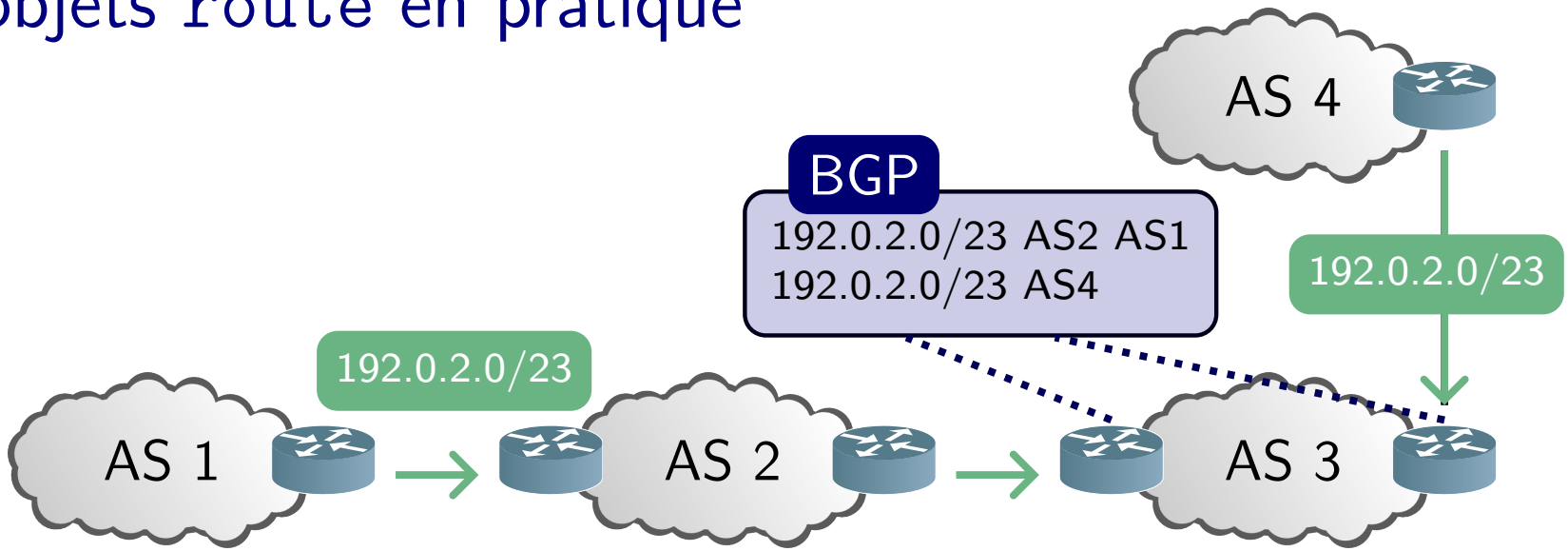
Protection contre les usurpations : les objets `route`

- un AS peut légitiment annoncer un préfixe attribué à un autre AS
  - délégation d'un préfixe à un client, dépollution de DDoS, ...
- en Europe, il suffit simplement de déclarer un objet `route` auprès du RIPE-NCC

Les objets `route` sont utilisés pour :

- créer des filtres d'annonces sur les routeurs BGP
- détecter des usurpations

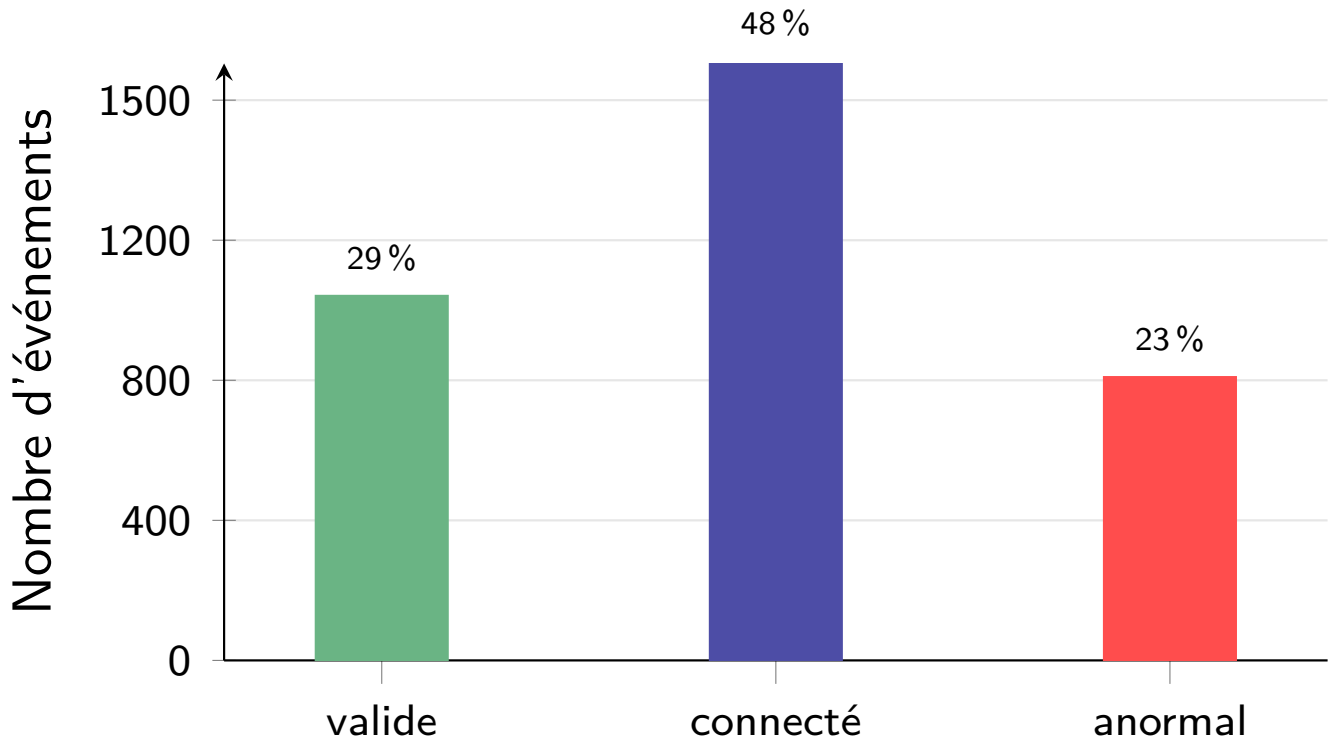
Les objets route en pratique



Déclaré par l'AS 1, l'objet route indique que l'AS 4 a le droit d'annoncer le préfixe 192.0.2.0/23.

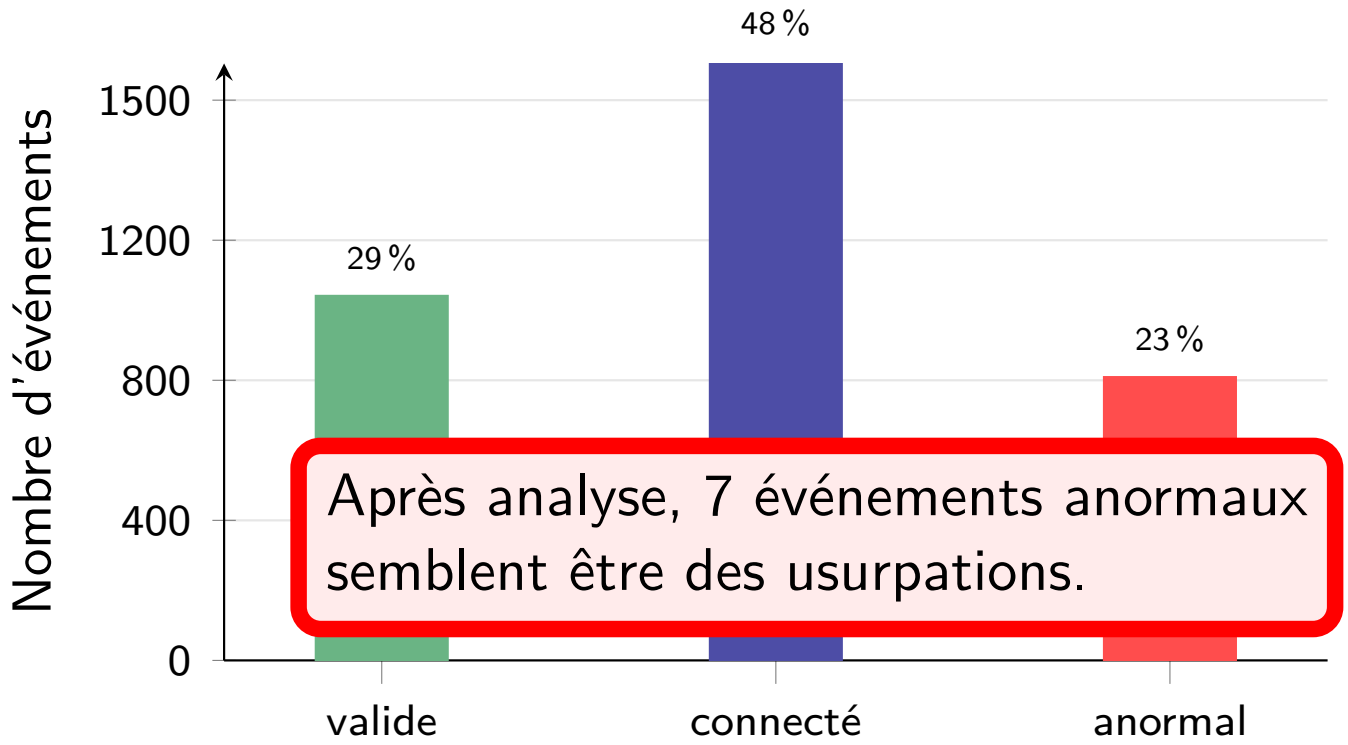
```
$ whois -T route 192.0.2.42
descr:          Objet route d'exemple
route:          192.0.2.0/23
origin:         AS-4
mnt-by:         STIC-MNT
```

Détecter les usurpations de préfixes



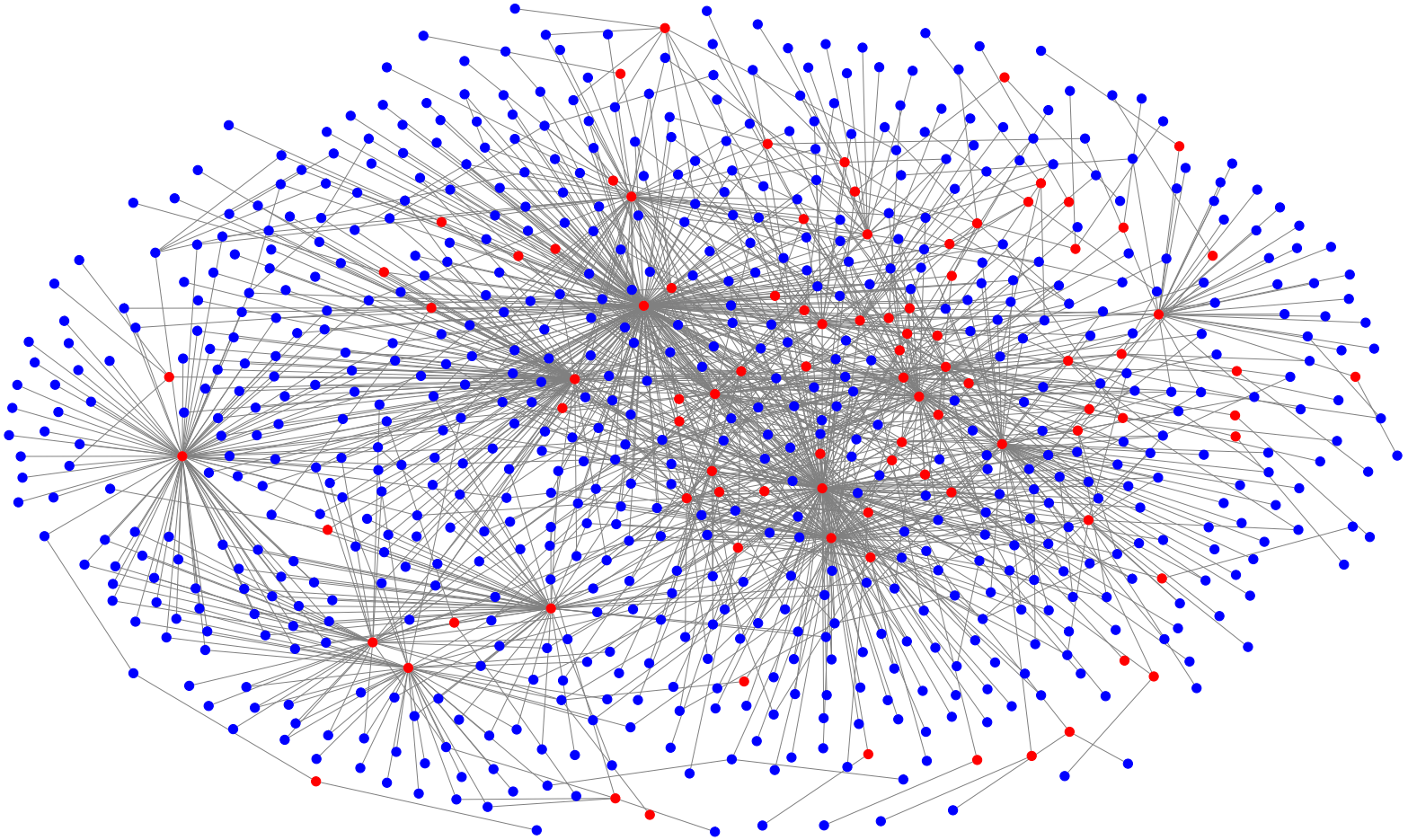
- valide : événement validé par un objet `route`
- connecté : l'AS usurpateur est connecté à l'AS usurpé
- anormal : c'est peut-être une usurpation

Détecter les usurpations de préfixes



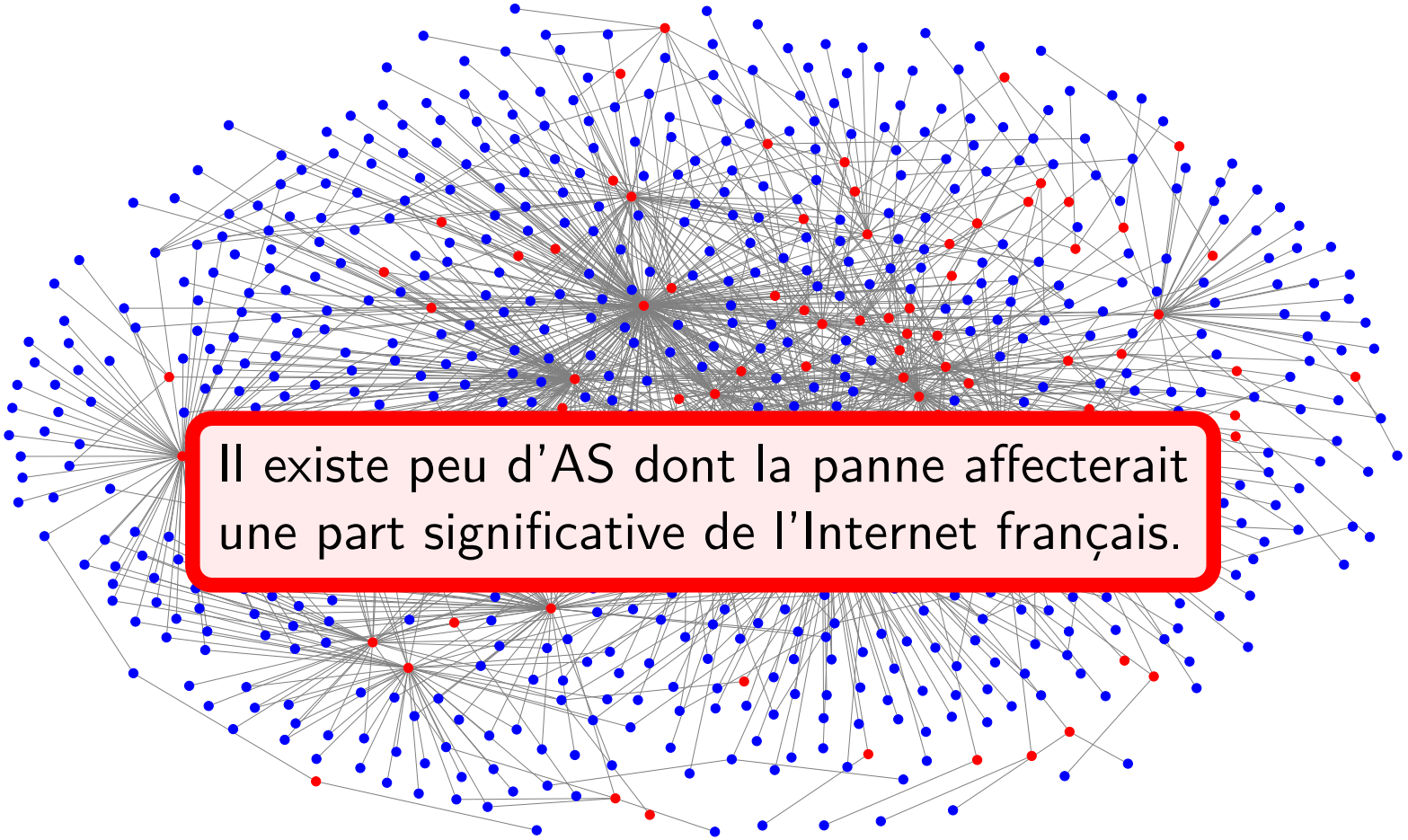
- valide : événement validé par un objet `route`
- connecté : l'AS usurpateur est connecté à l'AS usurpé
- anormal : c'est peut-être une usurpation

Connectivité des AS



- en bleu, les AS français
- en rouge, les AS dont la disparition peut être problématique

Connectivité des AS

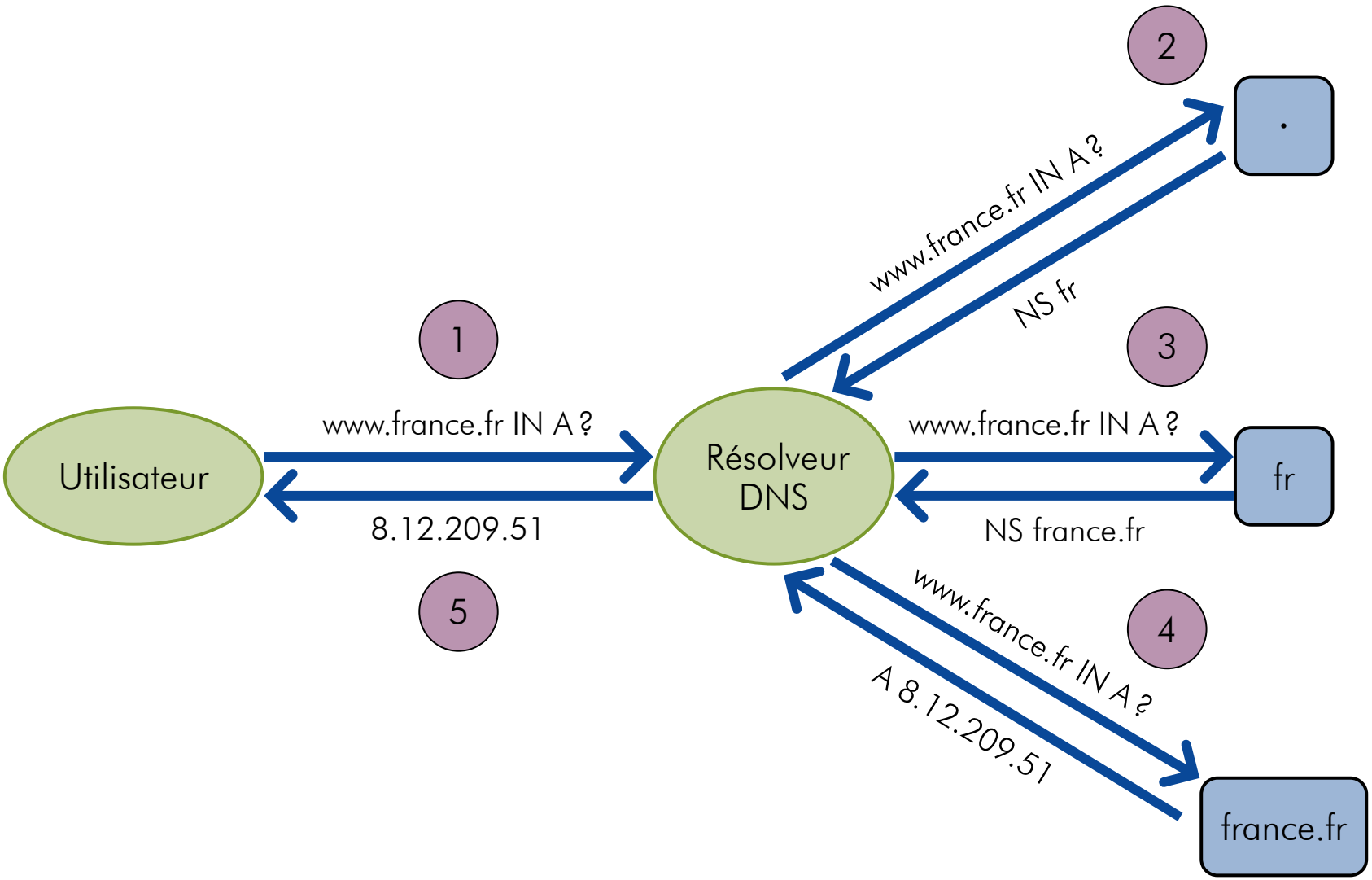


- en bleu, les AS français
- en rouge, les AS dont la disparition peut être problématique

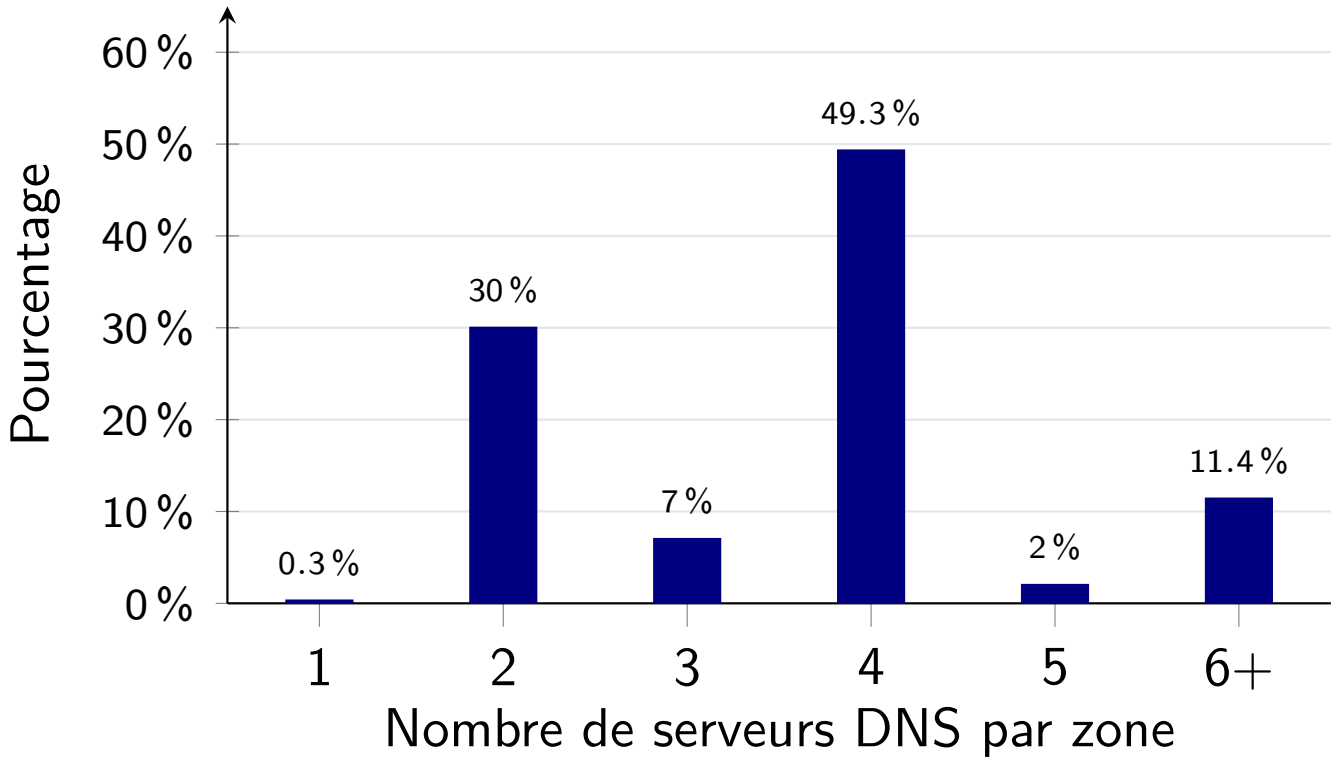
Sous l'angle de DNS

Domain Name System (DNS)

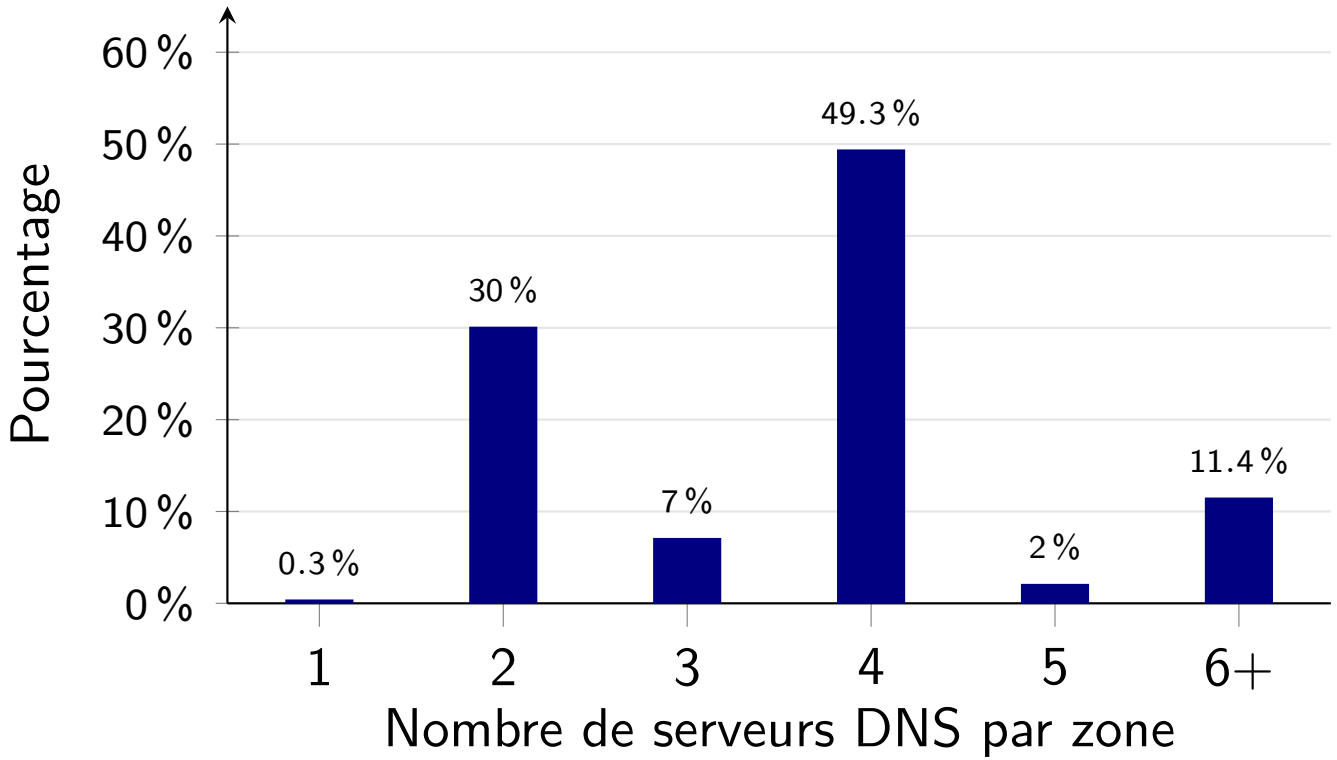
Le DNS permet de trouver l'adresse IP associée à un nom.



Nombre de serveurs par zone sous .fr

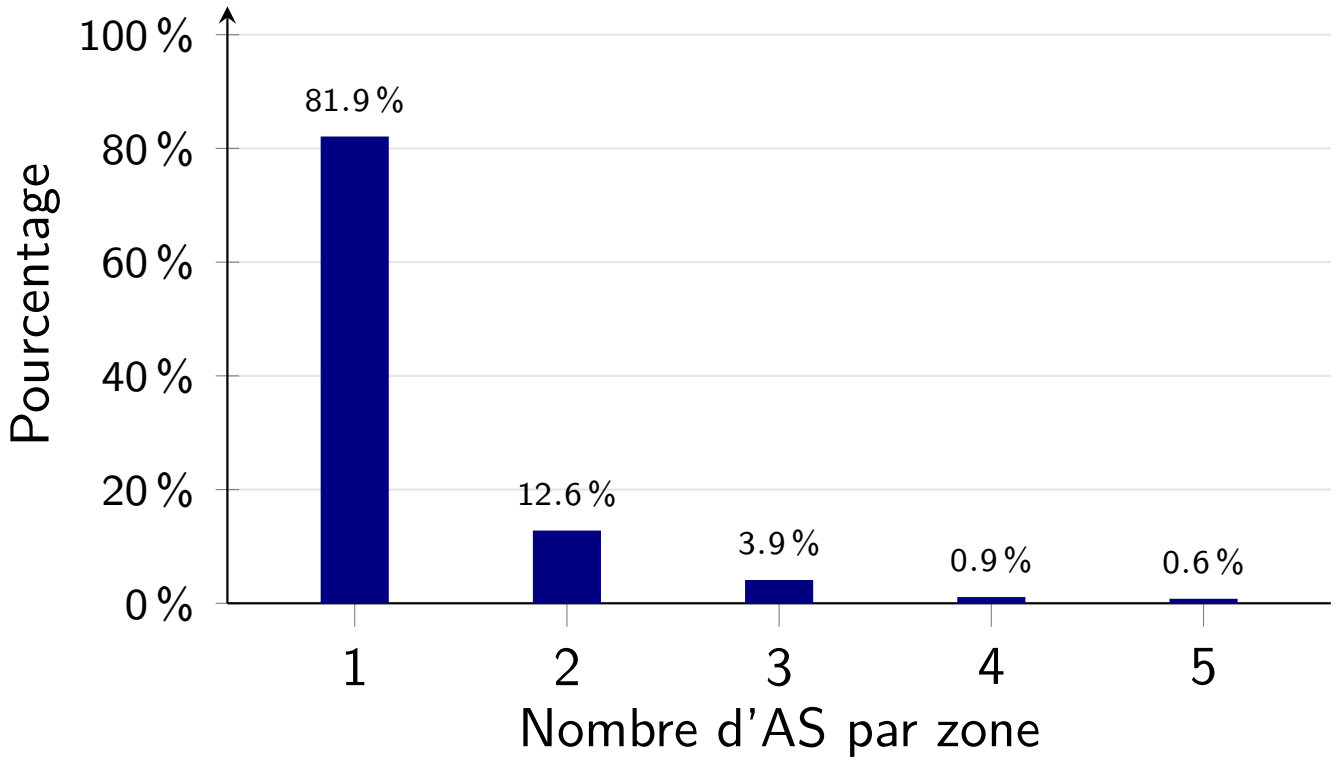


Nombre de serveurs par zone sous .fr

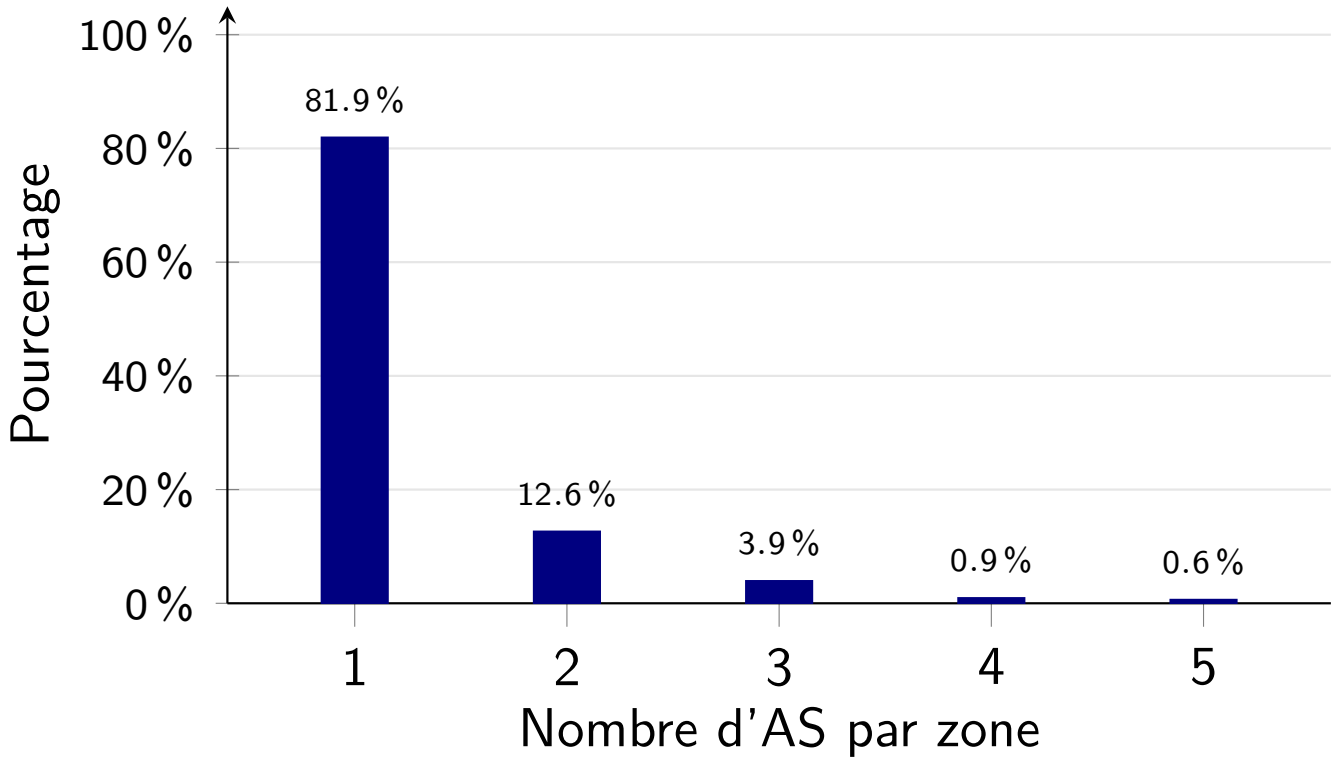


Il y a un nombre suffisant de serveurs DNS par zone
MAIS ...

Nombre d'AS par zone sous .fr

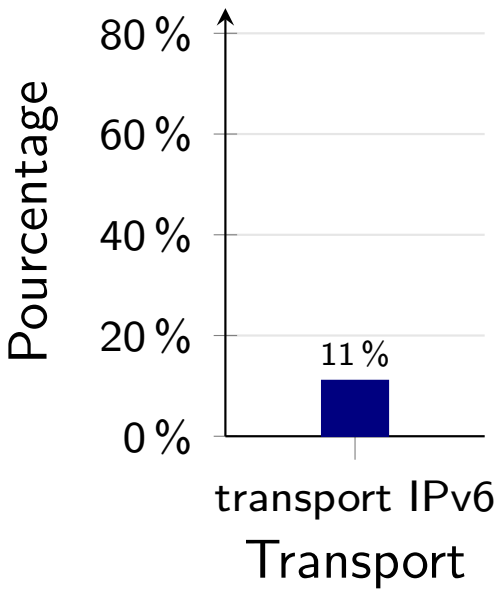


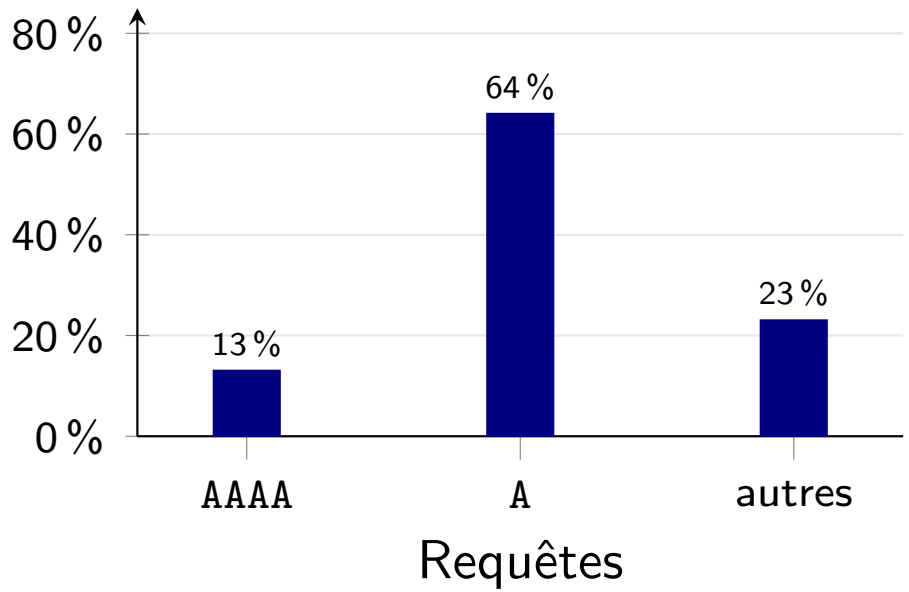
Nombre d'AS par zone sous .fr



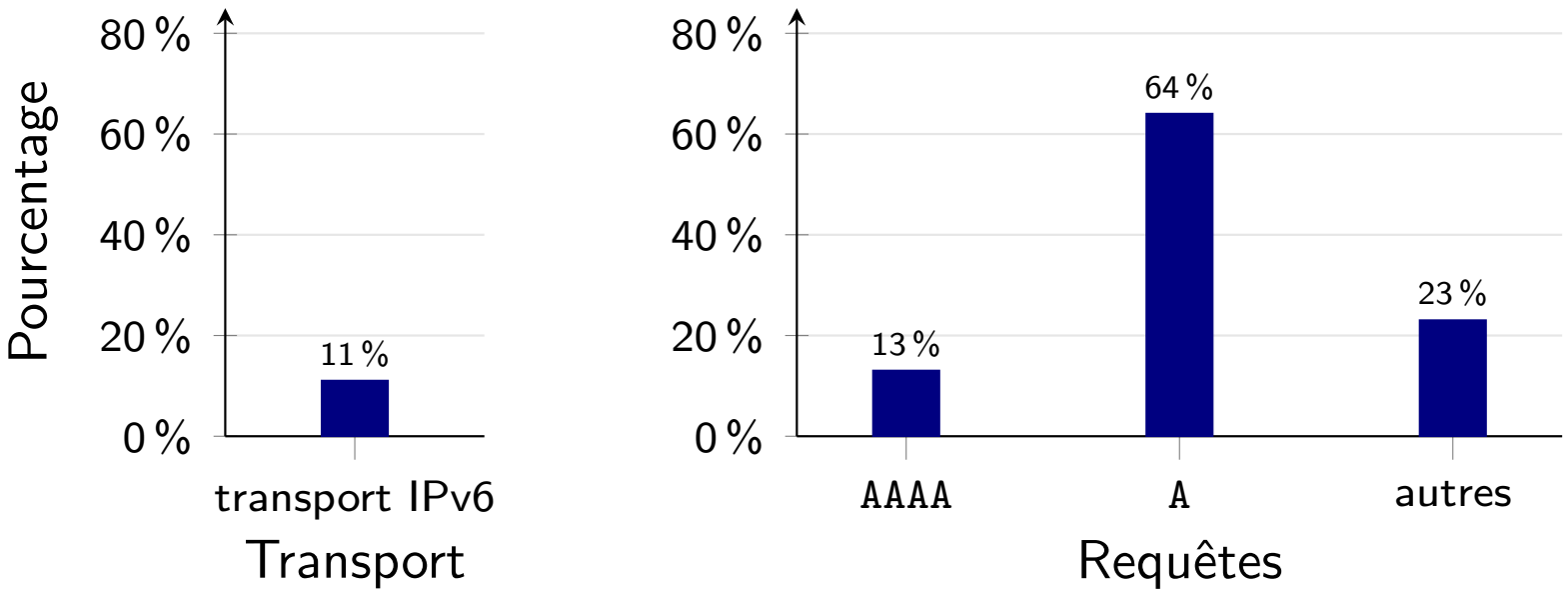
Les serveurs DNS faisant autorité ne sont pas suffisamment bien répartis.

Taux de pénétration d'IPv6





Taux de pénétration d'IPv6



L'utilisation d'IPv6 reste marginale.

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 de l'Observatoire de la résilience

- **déployer IPv6** pour anticiper des problèmes
- **répartir les serveurs DNS faisant autorité au sein de différents opérateurs** pour limiter les effets d'une panne
- **déclarer 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

Questions ?

Rapports & guides

- rapport 2011 disponible
- rapport 2012 disponible fin juin 2013
- guide de bonnes pratiques BGP disponible en septembre 2013