Détection d'usurpations de préfixes en temps réel

Nicolas Vivet

Agence nationale de la sécurité des systèmes d'information

http://www.ssi.gouv.fr

JCSA - 9 juillet 2015

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.

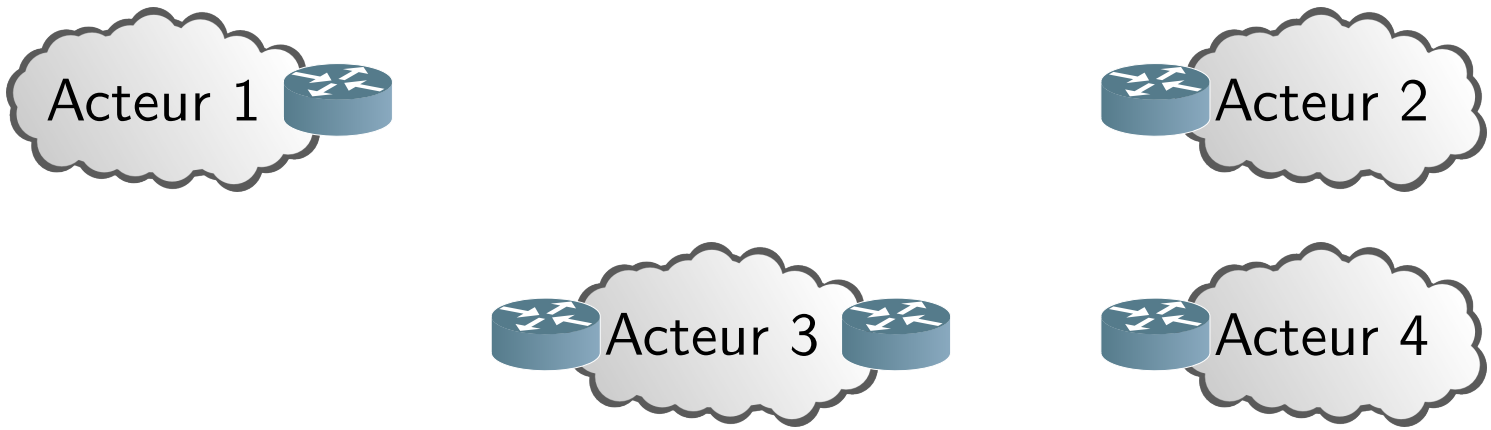
Objectifs de l'observatoire

- 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.

Introduction

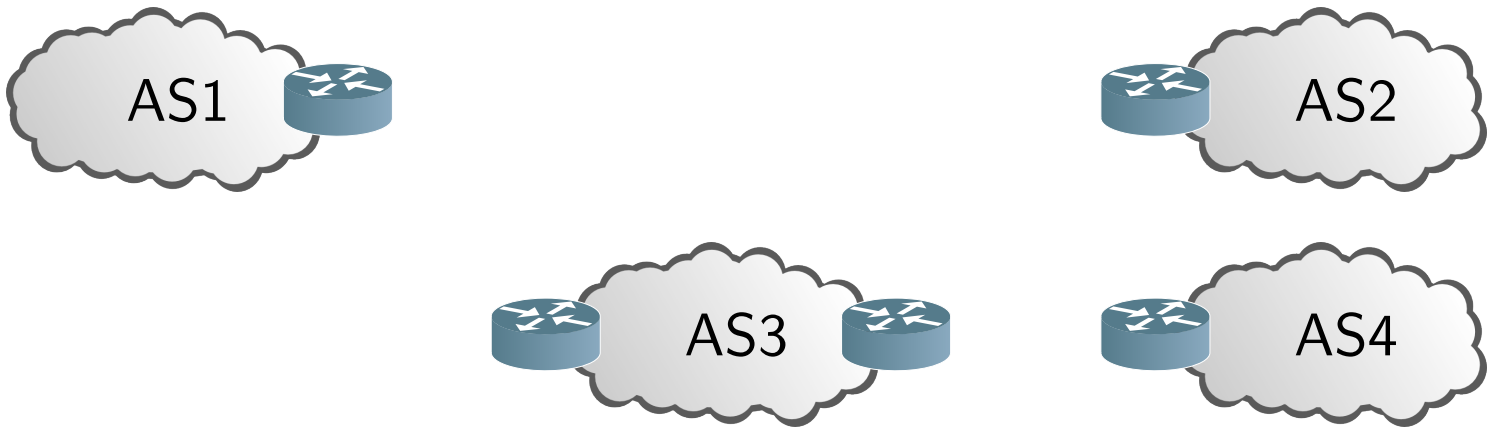
Border Gateway Protocol (BGP)

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.

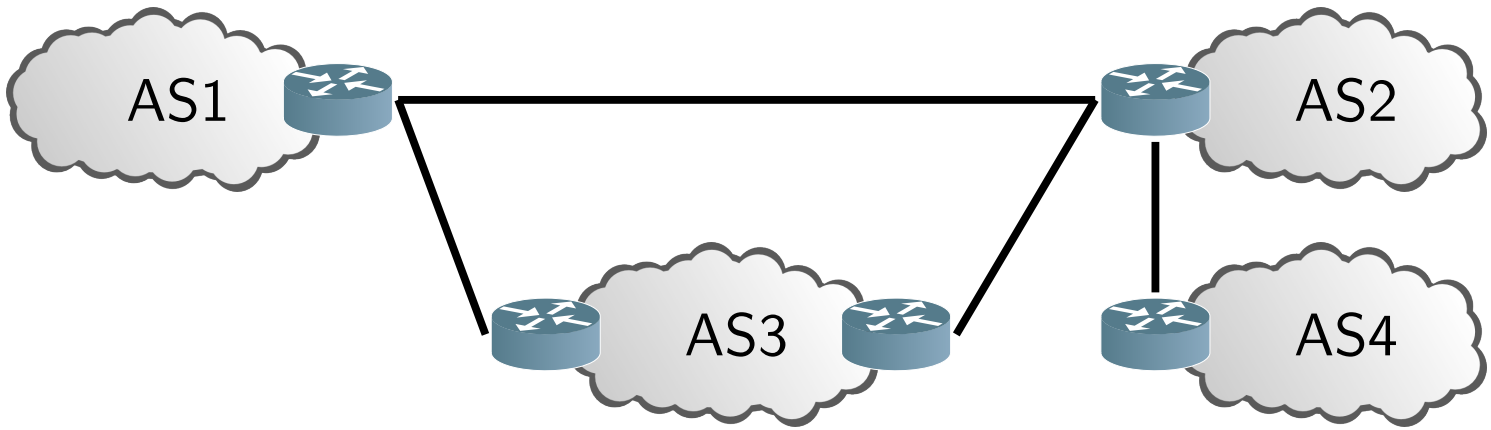


Le protocole BGP

- 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.

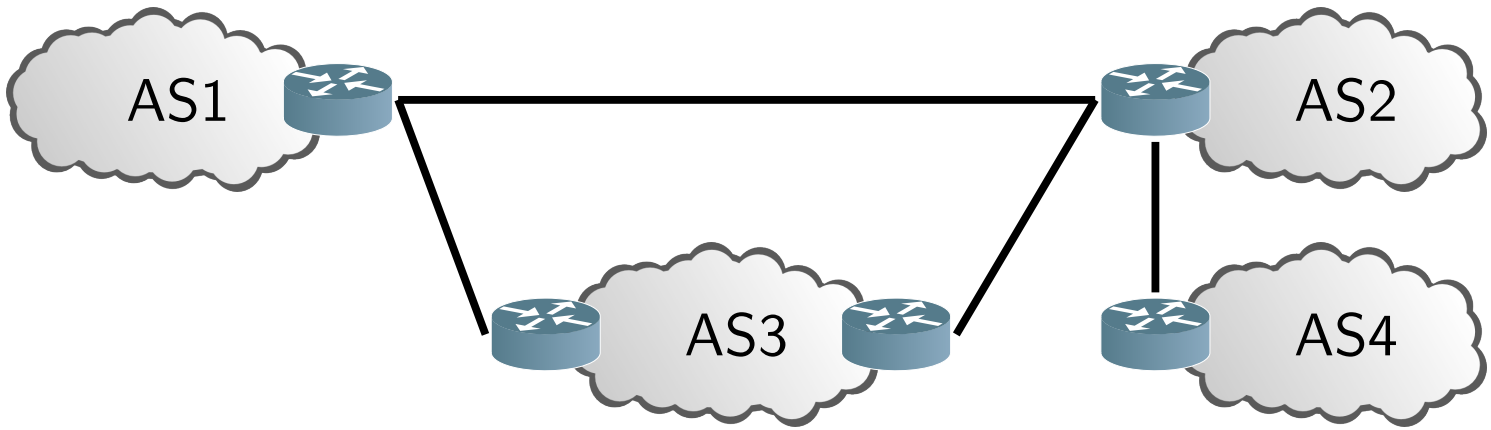


Le protocole BGP

- 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.

Conflits d'annonces de préfixes

Plusieurs AS peuvent annoncer le même préfixe avec BGP

- à cause d'une mauvaise configuration
- légitimement en cas d'accord

Conflits d'annonces de préfixes

Plusieurs AS peuvent annoncer le même préfixe avec BGP

- à cause d'une mauvaise configuration
- légitimement en cas d'accord

Des usurpations se produisent régulièrement

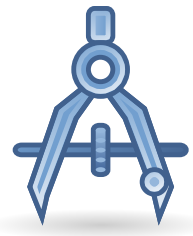
- détournement de trafic par des spammeurs sur plusieurs mois
- campagne de vol de monnaie virtuelle (*bitcoins*)

Détection

Mécanisme de détection des conflits

Routeurs BGP

Détection



Mesures actives

Données BGP

https://ris.ripe.net

Routing Information Service (RIS)

- 13 collecteurs BGP répartis dans le monde
  - bientôt un collecteur en France
  - actuellement 263 pairs BGP
- messages BGP enregistrés dans un format binaire
  - 550 Go compressés par an

Données BGP

https://ris.ripe.net

Routing Information Service (RIS)

- 13 collecteurs BGP répartis dans le monde
  - bientôt un collecteur en France
  - actuellement 263 pairs BGP
- messages BGP enregistrés dans un format binaire
  - 550 Go compressés par an

Nécessite un *parser* dédié

- *parser* BGP fiable et rapide
  - écrit en OCaml
- transforme les messages BGP en JSON
  - format facilement interprétable

Émulation BGP et détection

Reconstruction des tables de routage

- mise à jour des tables à chaque message BGP
  - plusieurs dizaines de messages/s par collecteur en moyenne
- recherche de conflits de préfixes IP
  - utilisation d'une structure de données spécialisée
  - opération coûteuse en temps de calcul et en mémoire vive

Émulation BGP et détection

Reconstruction des tables de routage

- mise à jour des tables à chaque message BGP
  - plusieurs dizaines de messages/s par collecteur en moyenne
- recherche de conflits de préfixes IP
  - utilisation d'une structure de données spécialisée
  - opération coûteuse en temps de calcul et en mémoire vive

Implémentation en Python

- principaux chemins d'exécution en code natif
  - py-radix (`https://github.com/mjschultz/py-radix`)

Émulation BGP et détection

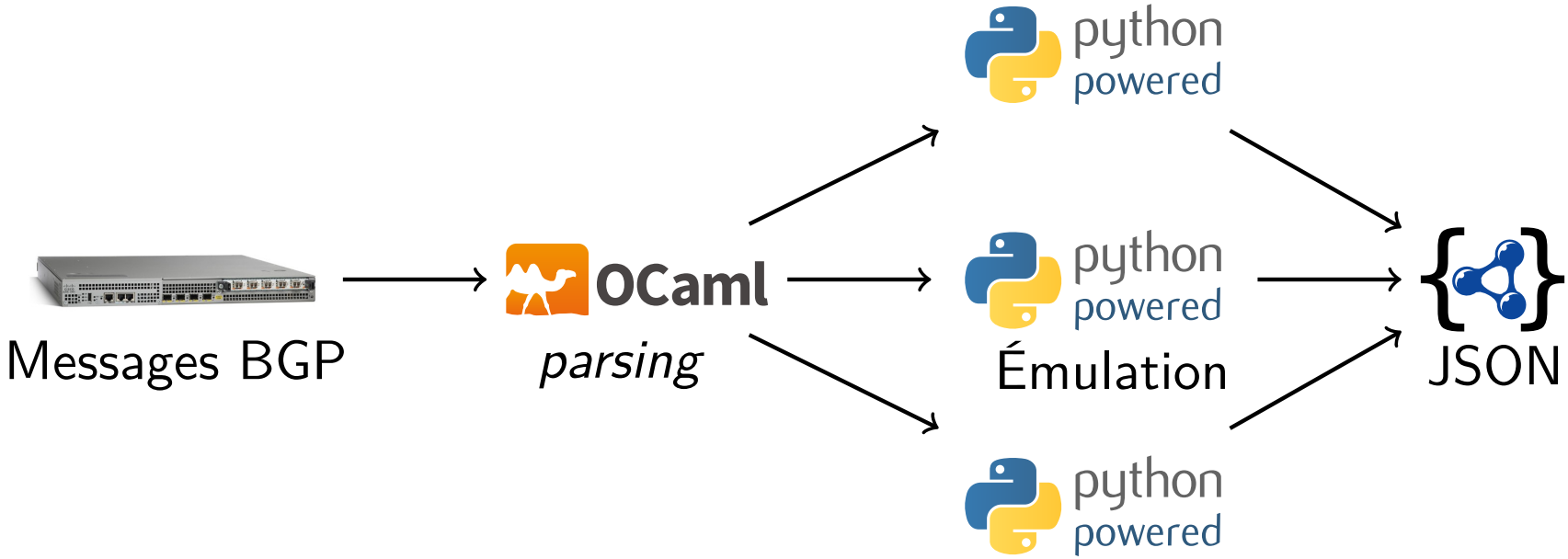
Reconstruction des tables de routage

- mise à jour des tables à chaque message BGP
  - plusieurs dizaines de messages/s par collecteur en moyenne
- recherche de conflits de préfixes IP
  - utilisation d'une structure de données spécialisée
  - opération coûteuse en temps de calcul et en mémoire vive

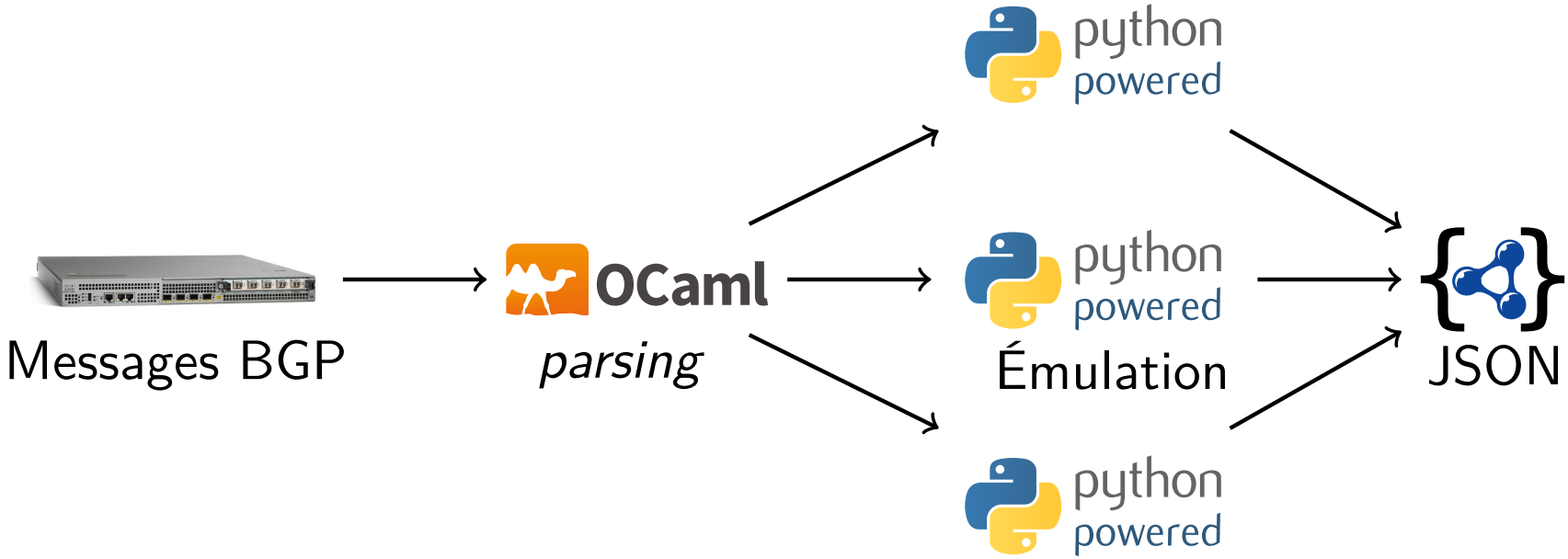
Implémentation en Python

- principaux chemins d'exécution en code natif
  - py-radix (`https://github.com/mjschultz/py-radix`)
- parallélisation (multi-processus)
  - plusieurs milliers d'AS sur chaque coeur

Processus de détection



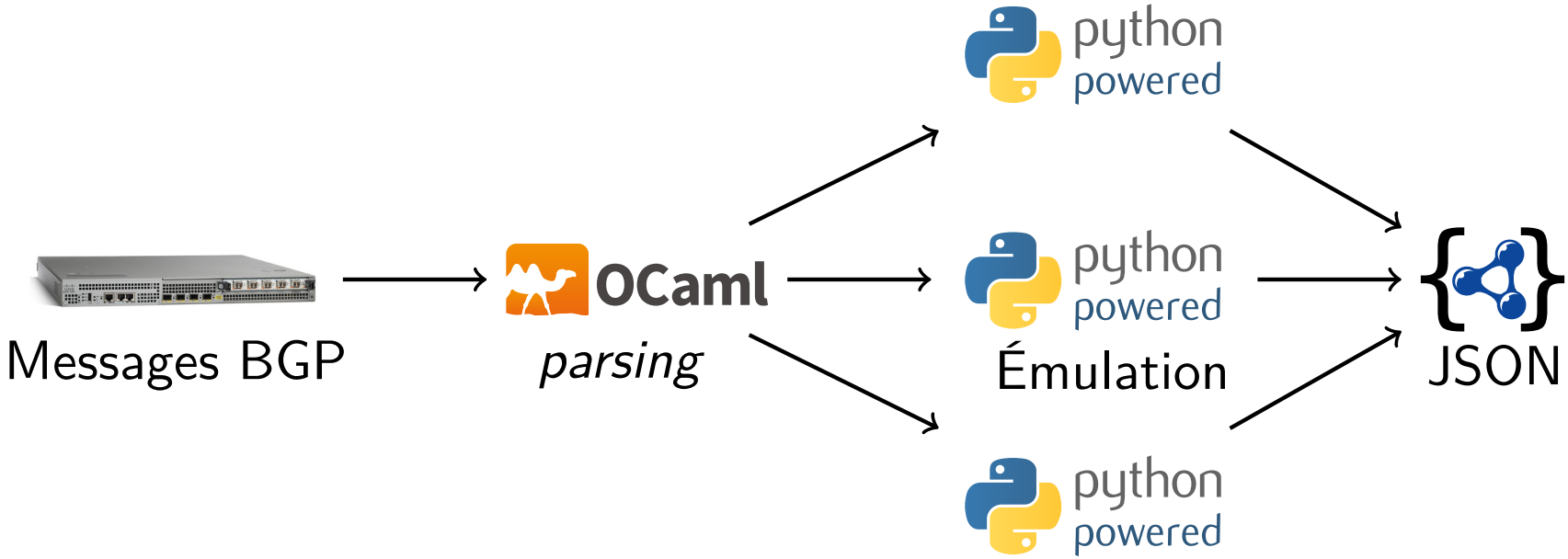
Processus de détection



Tâches automatisées

- récupération des données (`https://github.com/spotify/luigi`)

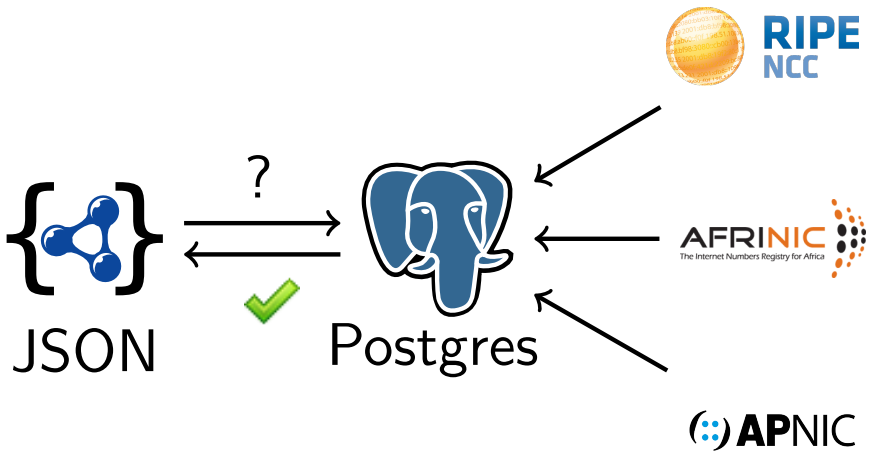
Processus de détection



Tâches automatisées

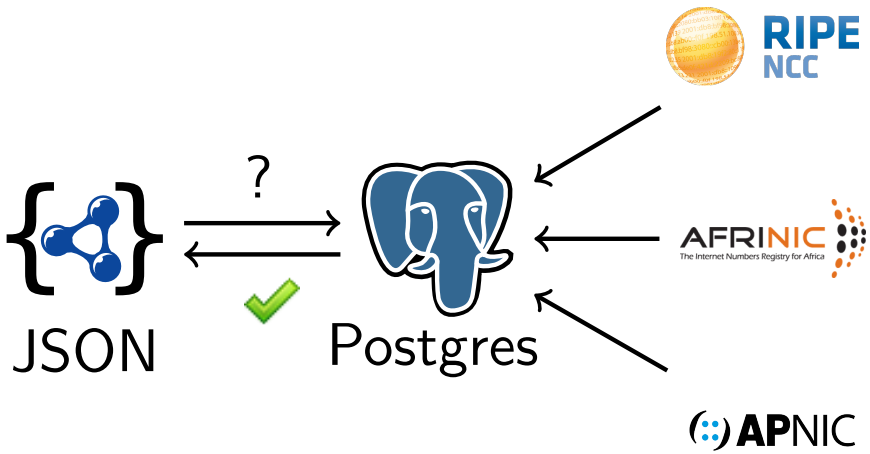
- récupération des données (`https://github.com/spotify/luigi`)
- exécution distribuée (`http://discoproject.org`)

Filtrage des messages en conflit



- Vérification de tous les messages avec les bases `WHOIS`

Filtrage des messages en conflit



- Vérification de tous les messages avec les bases `WHOIS`
- Requêtes spécifiques
  - import quotidien des bases `WHOIS`
  - module `rpsl` développé spécifiquement pour le format
  - module `ip4r` utilisé pour la recherche par préfixe

Quelques résultats pour 2014

Pour 1500 AS français

- 70 millions de messages BGP en conflits

Quelques résultats pour 2014

Pour 1500 AS français

- 70 millions de messages BGP en conflits
- 5136 conflits uniques
  - après aggrégation

Quelques résultats pour 2014

Pour 1500 AS français

- 70 millions de messages BGP en conflits
- 5136 conflits uniques
  - après aggrégation
- 1096 conflits non validés

Quelques résultats pour 2014

Pour 1500 AS français

- 70 millions de messages BGP en conflits
- 5136 conflits uniques
  - après aggrégation
- 1096 conflits non validés
- environ 300 conflits anormaux
  - potentiellement des usurpations
  - traitement manuel (environ une journée de travail)

Mesures avec RIPE Atlas

`https://atlas.ripe.net/`

Traceroute vers les préfixes usurpés

- depuis des sondes correctement placées
- demande automatique via l'API
- executé dans les minutes qui suivent la détection

Mesures avec RIPE Atlas

`https://atlas.ripe.net/`

Traceroute vers les préfixes usurpés

- depuis des sondes correctement placées
- demande automatique via l'API
- executé dans les minutes qui suivent la détection

Sur 187 conflits identifiés en temps réel en 2014, 29 conflits ont pu être mesurés à temps par environ 300 traceroutes.

Conclusion

Détection en temps réel

- grâce aux données BGP publiées par le RIPE
- surveille les annonces de plus de 550 000 préfixes
- rendu possible en distribuant les traitements
- les sondes Atlas aident à l'analyse des usurpations

Détection en temps réel

- grâce aux données BGP publiées par le RIPE
- surveille les annonces de plus de 550 000 préfixes
- rendu possible en distribuant les traitements
- les sondes Atlas aident à l'analyse des usurpations

Des usurpations touchent régulièrement des opérateurs français:
l'observatoire encourage les opérateurs à surveiller leurs préfixes.