Mais qui est vraiment responsable de ce préfixe d'adresses IP ?

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Mais qui est vraiment responsable de ce préfixe d'adresses IP ?

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

afnic

Les cas

Les cas

- Un préfixe d'adresses IP d'une compagnie morte depuis longtemps reprend vie,

Les cas

- Un préfixe d'adresses IP d'une compagnie morte depuis longtemps reprend vie,
- Des préfixes d'adresses IP inutilisés sont annoncés dans l'Internet par quelqu'un qui n'est pas le titulaire.

Les cas

- Un préfixe d'adresses IP d'une compagnie morte depuis longtemps reprend vie,
- Des préfixes d'adresses IP inutilisés sont annoncés dans l'Internet par quelqu'un qui n'est pas le titulaire.
- « *Ghosts of long dead companies are real, and they do walk among us. And they have their own IPs.* » (Ronald Guilmette)

afnic

Les cas

- Un préfixe d'adresses IP d'une compagnie morte depuis longtemps reprend vie,
- Des préfixes d'adresses IP inutilisés sont annoncés dans l'Internet par quelqu'un qui n'est pas le titulaire.
- « *Ghosts of long dead companies are real, and they do walk among us. And they have their own IPs.* » (Ronald Guilmette)
- À propos de Guilmette : investigateur, à remercier pour les travaux exposés ici, mais personnage difficile.

afnic

Le contexte

Le contexte

- Pénurie d'adresses IPv4 depuis de nombreuses années,

Le contexte

- Pénurie d'adresses IPv4 depuis de nombreuses années,
- Par étapes successives, les adresses IPv4 deviennent de plus en plus difficiles à avoir,

afnic

Le contexte

- Pénurie d'adresses IPv4 depuis de nombreuses années,
- Par étapes successives, les adresses IPv4 deviennent de plus en plus difficiles à avoir,
- Paresse et incompétence retardent la migration nécessaire vers IPv6,

afnic

Le contexte

- Pénurie d'adresses IPv4 depuis de nombreuses années,
- Par étapes successives, les adresses IPv4 deviennent de plus en plus difficiles à avoir,
- Paresse et incompétence retardent la migration nécessaire vers IPv6,
- Une cible tentante : les préfixes du marais (alloués avant l'existence des RIR, *Regional Internet Registry*).

afnic

Rappel rapide

Rappel rapide

- Les adresses IP sont allouées par les RIR,

Rappel rapide

- Les adresses IP sont allouées par les RIR,
- L'information est publiée via whois ou RDAP,

Rappel rapide

- Les adresses IP sont allouées par les RIR,
- L'information est publiée via whois ou RDAP,
- Les vérifications sont de qualité variables,

Rappel rapide

- Les adresses IP sont allouées par les RIR,
- L'information est publiée via whois ou RDAP,
- Les vérifications sont de qualité variables,
- Les routes sont annoncées par les opérateurs Internet (AS = *Autonomous System*),

Rappel rapide

- Les adresses IP sont allouées par les RIR,
- L'information est publiée via whois ou RDAP,
- Les vérifications sont de qualité variables,
- Les routes sont annoncées par les opérateurs Internet,
- En théorie après avoir vérifié les bases des RIR,

Rappel rapide

- Les adresses IP sont allouées par les RIR,
- L'information est publiée via whois ou RDAP,
- Les vérifications sont de qualité variables,
- Les routes sont annoncées par les opérateurs Internet,
- En théorie après avoir vérifié les bases des RIR,
- En pratique, les vérifications sont de qualité variable,

afnic

Rappel rapide

- Les adresses IP sont allouées par les RIR,
- L'information est publiée via whois ou RDAP,
- Les vérifications sont de qualité variables,
- Les routes sont annoncées par les opérateurs Internet,
- En théorie après avoir vérifié les bases des RIR,
- En pratique, les vérifications sont de qualité variable,
- Outre les RIR, il existe des registres de route (IRR, *Internet Routing Registry*), maintenus par divers acteurs,

afnic

Rappel rapide

- Les adresses IP sont allouées par les RIR,
- L'information est publiée via whois ou RDAP,
- Les vérifications sont de qualité variables,
- Les routes sont annoncées par les opérateurs Internet,
- En théorie après avoir vérifié les bases des RIR,
- En pratique, les vérifications sont de qualité variable,
- Outre les RIR, il existe des registres de route, maintenus par divers acteurs,
- Et en fait, c'est plus compliqué que cela.

afnic

Un exemple, 143.95.0.0/16

Un exemple, 143.95.0.0/16

- Affecté en 1990 à la société Athenix, Californie, en faillite depuis,

Un exemple, 143.95.0.0/16

- Affecté en 1990 à la société Athenix, Californie, en faillite depuis,
- En 2008, une autre société Athenix est créée dans le Massachussets,

afnic

Un exemple, 143.95.0.0/16

- Affecté en 1990 à la société Athenix, Californie, en faillite depuis,
- En 2008, une autre société Athenix est créée dans le Massachussets,
- Et récupère le préfixe IP !

Un exemple, 143.95.0.0/16

- Affecté en 1990 à la société Athenix, Californie, en faillite depuis,
- En 2008, une autre société Athenix est créée dans le Massachussets,
- Et récupère le préfixe IP !
- Le vrai responsable semble être la société EIGI.

Outils d'investigation

Outils d'investigation

- whois ou RDAP pour voir le titulaire,

Outils d'investigation

- whois ou RDAP pour voir le titulaire,
- Pas toujours de détail public sur l'historique (RIPE-NCC, APNIC et Afrinic),

Outils d'investigation

- whois ou RDAP pour voir le titulaire,
- Pas toujours de détail public sur l'historique (RIPE-NCC, APNIC et Afrinic),
- RIPE stat ou un autre *looking glass* pour le routage,

Outils d'investigation

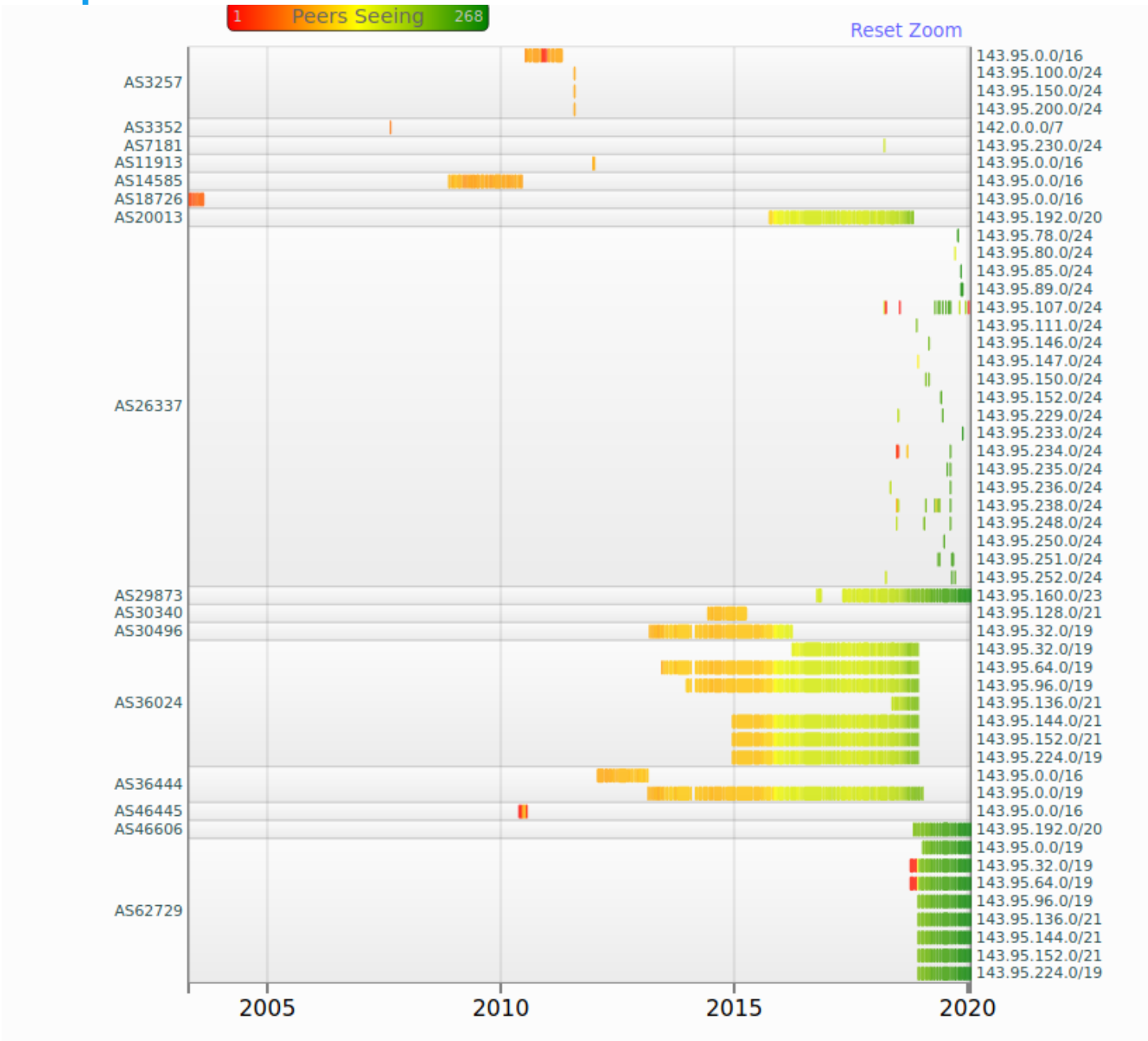
- whois ou RDAP pour voir le titulaire,
- Pas toujours de détail public sur l'historique (RIPE-NCC, APNIC et Afrinic),
- RIPE stat ou un autre *looking glass* pour le routage,
- Divers services officiels étatsuniens comme la SEC, ou des sources ouvertes comme LinkedIn.

Exemple RDAP

```
%  curl -s https://rdap.arin.net/registry/ip/143.95.0.0/16
[Analyse du JSON]

% nicinfo 143.95.0.0/16
...
                   Handle:  ATHENI
              Common Name:  Athenix Inc.
                    Roles:  Registrant
            Last Changed:  Thu, 09 Jan 2020 12:54:30 -0500
            Registration:  Fri, 07 Sep 1990 00:00:00 -0400
...
```

Exemple RIPEstat



Autre exemple, le détournement en Afrique du Sud

Autre exemple, le détournement en Afrique du Sud

- Beaucoup de préfixes enregistrés en Afrique du Sud (mais aussi ailleurs) détournés,

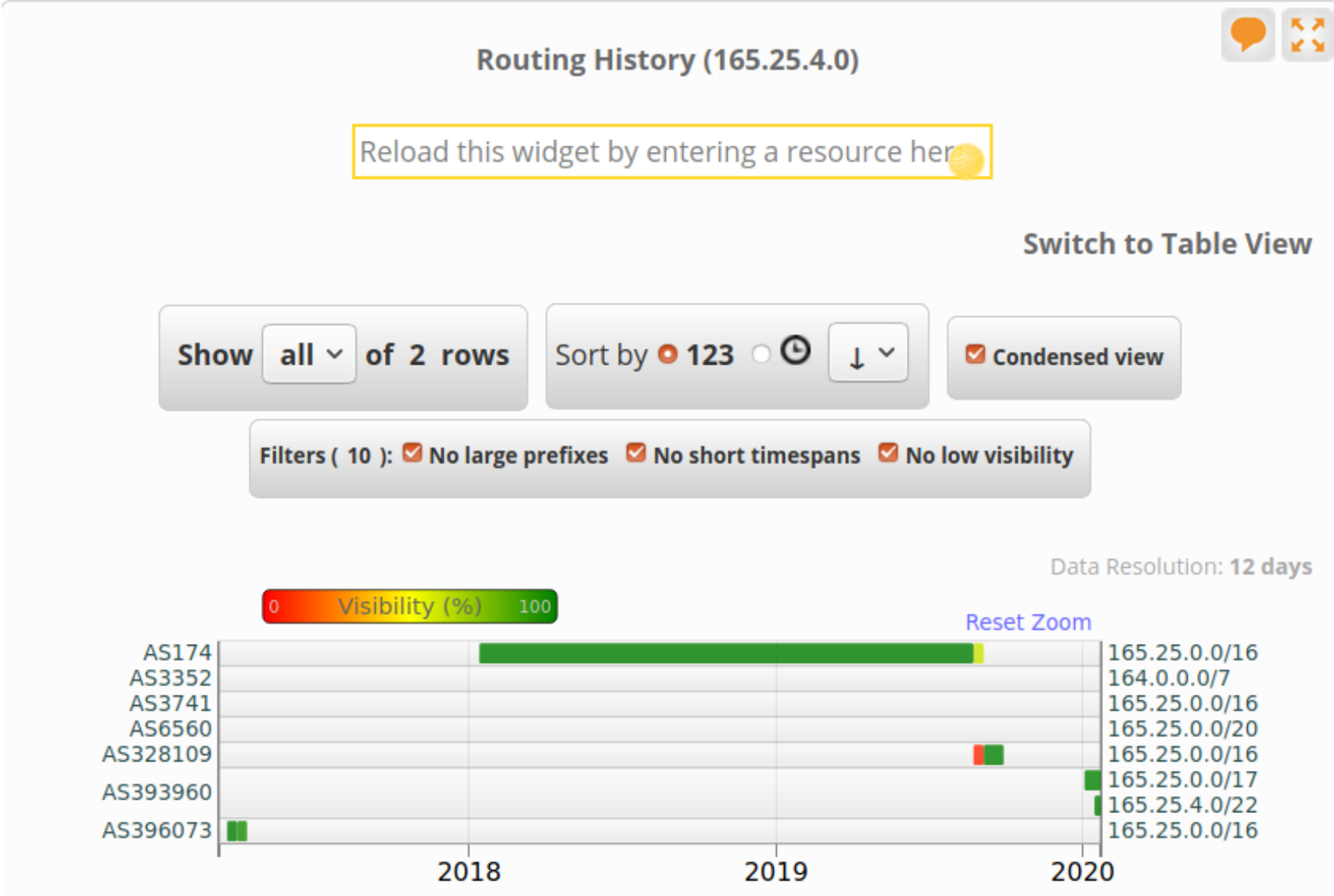
Autre exemple, le détournement en Afrique du Sud

- Beaucoup de préfixes détournés,
- Pas une simple annonce BGP, de vrais/faux objets créés dans un registre de routes, RADB (par le fameux Elad Cohen),

Autre exemple, le détournement en Afrique du Sud

- Beaucoup de préfixes détournés,
- Pas une simple annonce BGP, de vrais/faux objets créés dans un registre de routes,
- Opérateur de transit (Cogent) trop indulgent ?

La ville du Cap



Sécurité du routage, RPKI, ROA

Sécurité du routage, RPKI, ROA

- RPKI : *Resource Public Key Infrastructure*, chaîne de certificats prouvant la titularité d'une ressource (préfixe IP, par exemple),

Sécurité du routage, RPKI, ROA

- RPKI : *Resource Public Key Infrastructure*, chaîne de certificats prouvant la titularité d'une ressource,
- ROA : *Route Origin Authorization*, document structuré et signé autorisant un AS à annoncer un préfixe,

Sécurité du routage, RPKI, ROA

- RPKI : *Resource Public Key Infrastructure*, chaîne de certificats prouvant la titularité d'une ressource,
- ROA : *Route Origin Authorization*, document structuré et signé autorisant un AS à annoncer un préfixe,
- Preuve à présenter : pas évident, surtout pour le marais,

Sécurité du routage, RPKI, ROA

- RPKI : *Resource Public Key Infrastructure*, chaîne de certificats prouvant la titularité d'une ressource,
- ROA : *Route Origin Authorization*, document structuré et signé autorisant un AS à annoncer un préfixe,
- Preuve à présenter : pas évident, surtout pour le marais,
- En dehors de l'Europe, peu de ROA publiés.

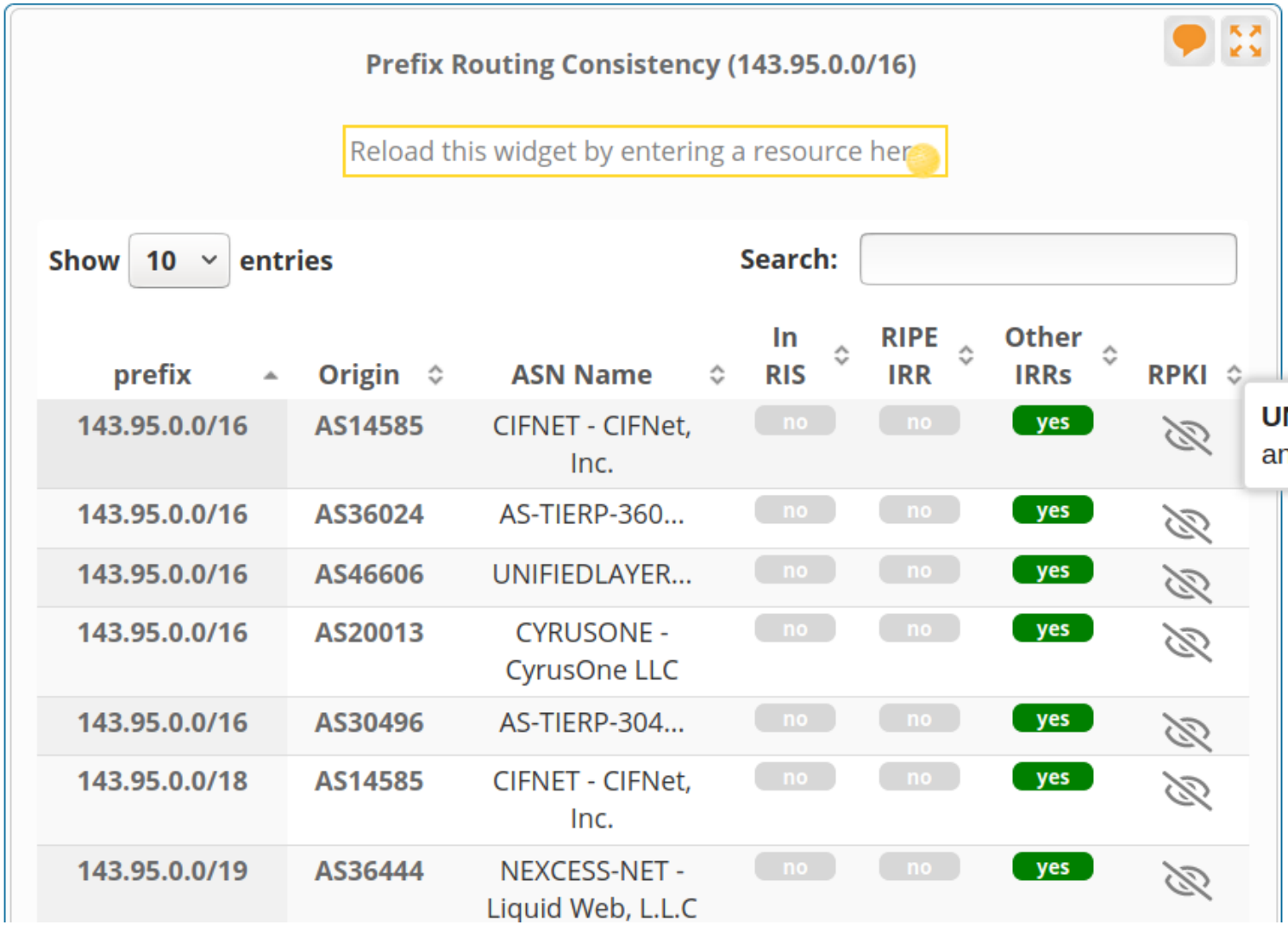
afnic

ROA via BGPmon

```
% whois -h whois.bgpmon.net  2001:678:c::1
...
Prefix:                 2001:678:c::/48
Prefix description:     NIC-FR-DNS-ANYCAST-AFNIC-V6
Country code:           FR
Origin AS:              2484
Origin AS Name:         NIC-FR-DNS-ANYCAST-AFNIC AFNIC (Association Franca
RPKI status:            ROA validation successful
```

afnic

Cohérence, IRR et ROA



Prefix Routing Consistency (143.95.0.0/16)

Reload this widget by entering a resource her

Show 10 entries Search:

prefix	Origin	ASN Name	In RIS	RIPE IRR	Other IRRs	RPKI
143.95.0.0/16	AS14585	CIFNET - CIFNet, Inc.	no	no	yes	
143.95.0.0/16	AS36024	AS-TIERP-360...	no	no	yes	
143.95.0.0/16	AS46606	UNIFIEDLAYER...	no	no	yes	
143.95.0.0/16	AS20013	CYRUSONE - CyrusOne LLC	no	no	yes	
143.95.0.0/16	AS30496	AS-TIERP-304...	no	no	yes	
143.95.0.0/18	AS14585	CIFNET - CIFNet, Inc.	no	no	yes	
143.95.0.0/19	AS36444	NEXCESS-NET - Liquid Web, L.L.C	no	no	yes	

UNKNOWN - no ROA fou
announcement

Dernier exemple, l'AS 8100

Dernier exemple, l'AS 8100

- Samedi dernier...

Dernier exemple, l'AS 8100

- Samedi dernier...
- Plein d'objets créés dans des IRR, RADB et NTT,

Dernier exemple, l'AS 8100

- Samedi dernier...
- Plein d'objets créés dans des IRR, RADB et NTT,
- Par l'AS 8100.

afnic

Dans l'IRR de NTT

La base du RIPE montre que 193.30.32.0/23 est bien à Nova53, AS 42198.

```
% whois  -h rr.ntt.net 193.30.32.0/23
route:          193.30.32.0/23
descr:          CMI IP Transit
origin:         AS8100
changed:        qas_support@cmi.chinamobile.com 20200118
source:         NTTCOM

route:          193.30.32.0/23
origin:         AS42198
last-modified:  2018-05-22T01:53:12Z
source:         RIPE
```

Merci !

www.afnic.fr
contact@afnic.fr