



Together, your Internet, even better



**FRNOG 34**

**Sécurisation du routage sur les serveurs  
de routes et adoption de RPKI**

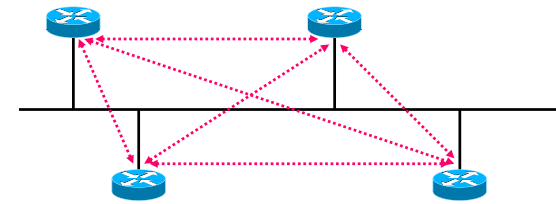
- Rappel sur les serveurs de routes (RS)
- La sécurité sur les RS
  - Rappel sur les filtrages de « base »
  - Filtrage IRR
  - Filtrage RPKI/ROA
    - RPKI/ROA et RTBH
- Quelques BCP et travaux en cours



- Rappel sur les serveurs de routes (RS)
- La sécurité sur les RS
  - Rappel sur les filtrages de « base »
  - Filtrage IRR
  - Filtrage RPKI/ROA
    - RPKI/ROA et RTBH
- Quelques BCP et travaux en cours

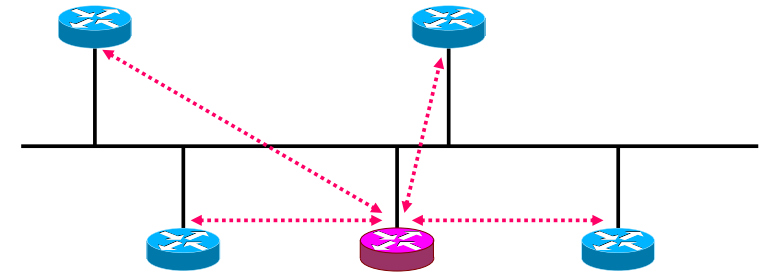
# Rappel sur les serveurs de routes (RS)




- **100** membres présents sur un IXP → **99** sessions BGP si on veut discuter avec tout le monde
  - Fastidieux initialement et très dur à maintenir
    - Des nouvelles sessions à établir/supprimer tous les jours
- La solution: **les serveurs de routes**

# Les serveurs de routes: Fonctionnement



 Routeur ISP  
 Peering eBGP

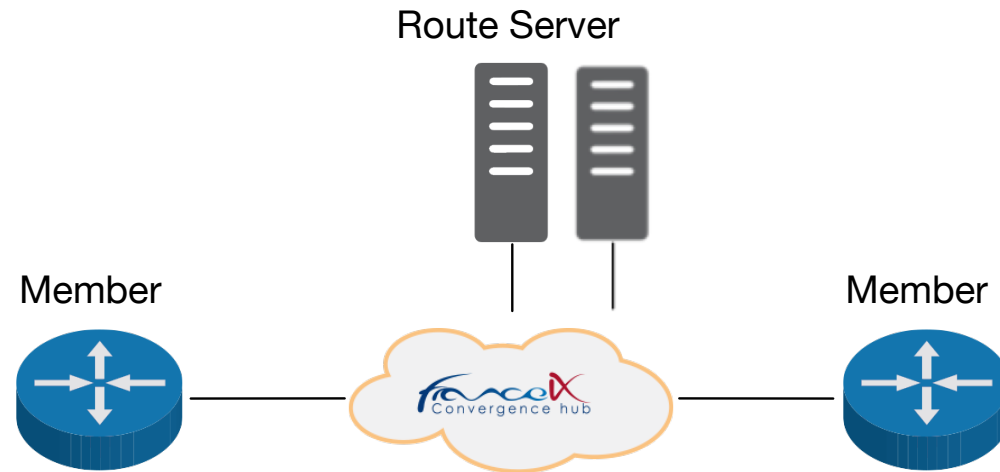


 BGP route server  
 Routeur ISP  
 Peering eBGP

- **Le Next-Hop (NH) BGP n'est pas modifié par le RS**
- **Le trafic ne transite pas par le RS**
- **Communautés BGP disponibles pour affiner la politique de routage par membre**
- **2 RS pour la redondance**

# Les serveurs de routes

- Attention, un RS n'est pas un routeur
- Data plane != Control Plane



- Rappel sur les serveurs de routes (RS)
- La sécurité sur les RS
  - Rappel sur les filtrages de « base »
  - Filtrage IRR
  - Filtrage RPKI/ROA
    - RPKI/ROA et RTBH
- Quelques BCP et travaux en cours

# L'évolution des RS au sein des IXP de + en + de sécurité et de fonctions

- **Initialement**, les RS ont été introduits pour faciliter l'échange des routes
  - Pas "d'intelligence"
  - Le RS agit comme un miroir
  - Ce sont les acteurs qui filtrent les routes non souhaitées
- **Introduction progressive de filtrage pour éliminer les routes non souhaitées**



# L'évolution du rôle des RS au sein des IXP

- Application dans la mesure du possible les BCP sur BGP (RFC7454, etc)
- Quelques sécurités “basiques” mises en place
  - Max-prefix
  - Routes Martians/BOGON filtrées (CYMRU)
  - Vérification que le premier AS de l'AS-PATH est l'AS du peer BGP
  - Les AS privés dans l'AS\_PATH sont filtrés
  - ...

# Les RS et le filtrage des routes

- **Doit-on laisser le peer se protéger et filtrer lui même?**
- **Doit-on filtrer ce qui ne semble pas cohérent? OUI**
- Sur France-IX, par défaut on applique du filtrage IRR + RPKI/ROA depuis **4 ans sur Paris et Marseille et depuis 8 ans sur Lyon**
- Possibilité pour le peer de tout recevoir sans filtrage. En 4 ans, **0 demande reçue**
- Initiatives pour sécuriser l'Internet, les IXP ont un rôle important à jouer

# Les RS et le filtrage des routes : MANRS

## Mutually Agreed Norms for Routing Security

- Programme pour les IXP

### **Action 2. Promote MANRS to the IXP membership. (One or more must be checked)**

The IXP provides encouragement or assistance for members to implement MANRS actions. (There are 4 separate check-boxes for different levels of incentives; one or more must be checked.)

The IXP actively promotes MANRS by encouraging its members to implement the MANRS actions in part or in full.  
The encouragement can take different forms:

#### **Action 2-1: Offer assistance to its members to maintain accurate routing information in an appropriate repository (IRR and/or RPKI)**

This may take a form of trainings or tutorials, for example, as part of the on-boarding process

# Filtrage des routes IRR

- Les préfixes Internet sont déclarés dans différentes bases Internet, les bases des RIR et d'autres bases comme RADB

- Objet « route »

```
% Information related to '37.49.234.0/24AS57734'
```

```
route:          37.49.234.0/24
descr:          FranceIX Services
origin:         AS57734
```

- Utilisation d'un ensemble de bases pour construire une base « FranceIX »
  - Utilisation d'outils tels que BGPQ3/4, la base NTT et des scripts
  - A partir d'un objet AS-SET ou un AUT-NUM, on récupère l'ensemble des objets ROUTE pouvant être annoncés par un membre
  - Import de cette base dans les RS et filtrage des préfixes. Tag des préfixes avant filtrage pour debug

```
51706:65011 = Prefix is present in an AS's announced AS/AS-SET
```

```
51706:65021 = Prefix is not present in an AS's announced AS/AS-SET
```



# RPKI/ROA

- RPKI : Resource Public Key Infrastructure
- Permet de garantir l'appartenance des ressources (IPs, ASN)
- ROA : Route Origin Authorization
  - Permet de valider que l'AS d'origine est autorisé à annoncer le préfixe
- 3 états possibles pour chaque annonce BGP
  - VALID: au moins un Roa existe qui valide cette route
  - **INVALID : Il existe un ROA pour ce préfixe mais cet AS n'est pas autorisé à annoncer ce préfixe. Hijacking?? Ou bien le préfixe annoncé est plus spécifique**
  - UNKNOWN : Il n'y a pas de ROA existant pour ce préfixe
- Délégation possible sur **le portail du RIPE** pour "signer" les ROA
  - <https://my.ripe.net/#/rpki>
- **Très simple, faites le!!!**

Origin AS	Prefix	Current Status
AS57734	2a00:a4c0::/32	VALID
AS57734	37.49.234.0/24	VALID

AS number	Prefix	Most specific length allowed	Affects
AS57734	37.49.234.0/24	24	1

# Adoption de RPKI/ROA

- Prenez 5mins pour déclarer vos ROA

https://my.ripe.net/#/rpk

RPKI

You are editing France IX Services SASU fr.ix

RPKI Dashboard 17 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDR

12 BGP Announcements 11 Valid 0 Invalid 1 Unknown

18 ROAs 18 OK 0 Causing problems

BGP Announcements Route Origin Authorisations (ROAs) History Search...

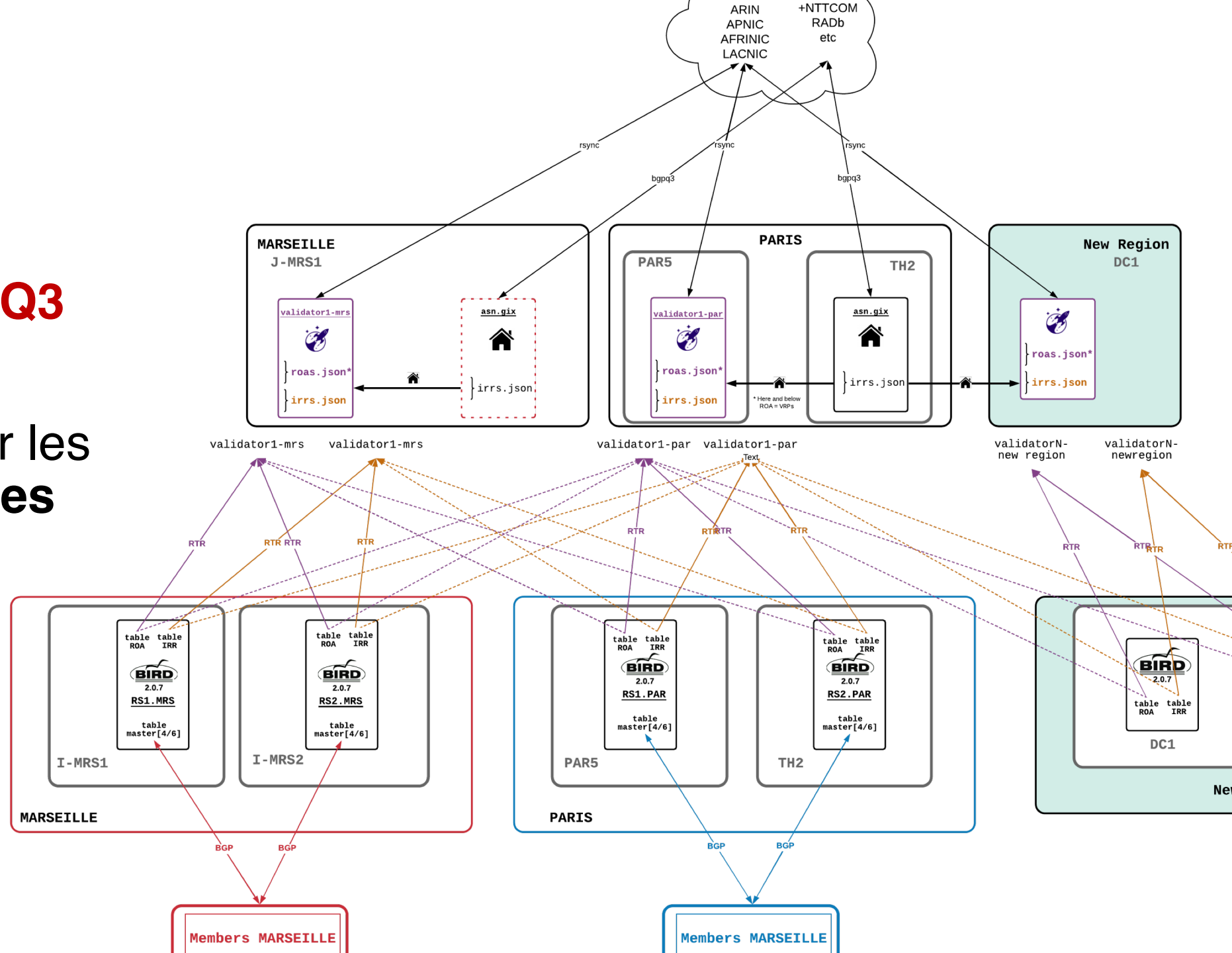
Discard Changes Delete ROAs Causing Problems Not Causing Problems + New ROA

AS number	Prefix	Most specific length allowed	Affected announcements
AS57734	37.49.234.0/24	24	
AS199813	2a03:9180:2::/47	47	1

Tour

# Architecture de filtrage IRR/RPKI

- **PeeringDB+BGPQ3**
- ROUTINATOR
- RTR pour pousser les ROA mais **aussi les entrées IRR**
- **Bird 2.0.7**



# Adoption de RPKI/ROA : Quelques stats

Bonne visibilité coté France-IX de ce qui se passe en France

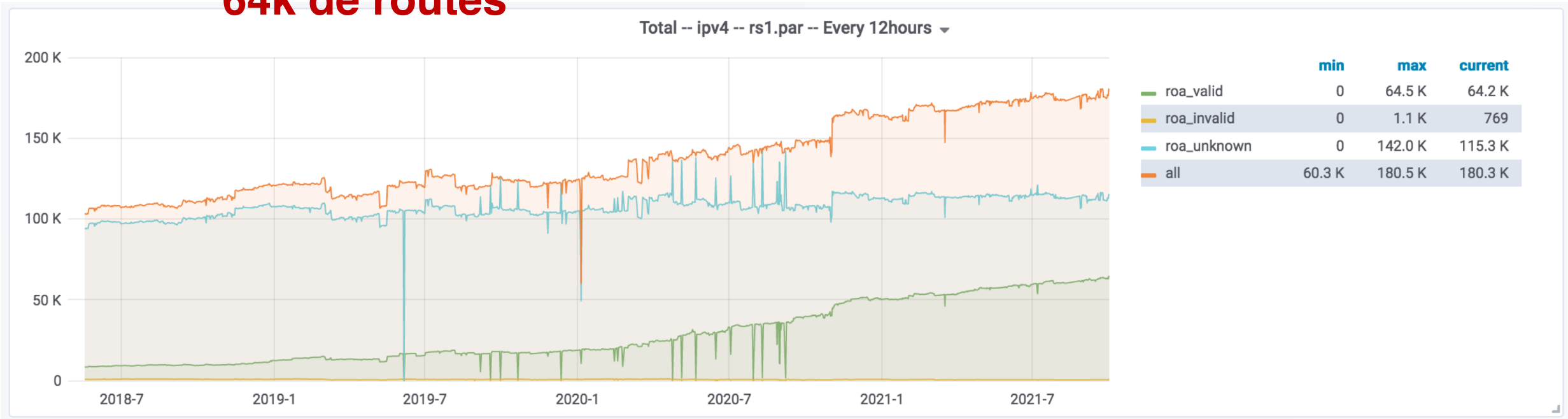
- 500 ASNs distribués sur 3 villes, Paris, Lyon, Marseille
- Taux de raccordement aux RS de **90%**, **450 ASN** connectés sur des RS



# Adoption de RPKI/ROA

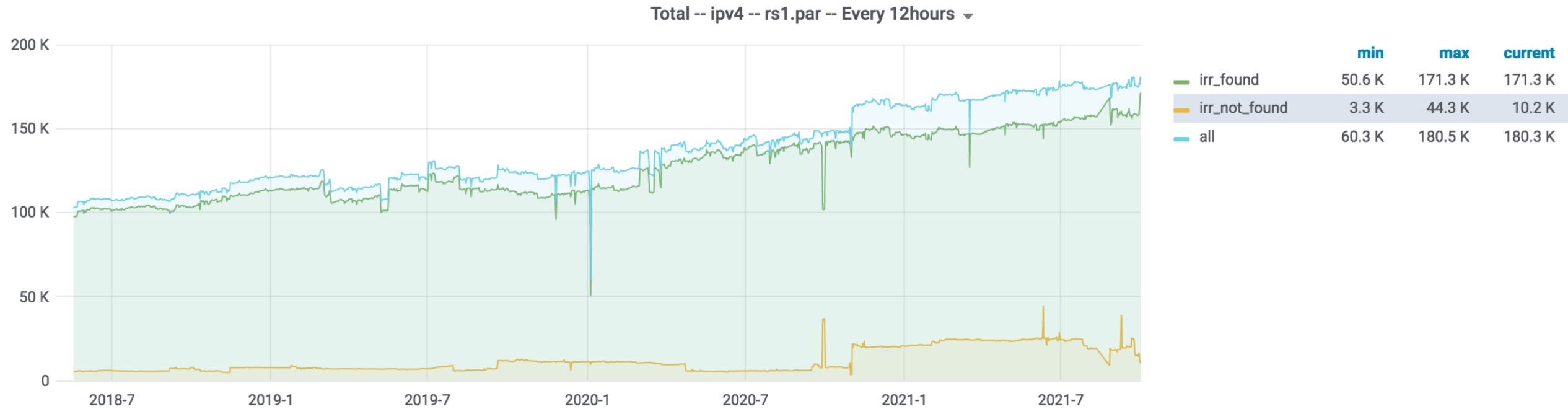
## Quelques stats

- Taux d'adoption en nette progression
  - Début 2018 : <10 % des routes avec un état « valid''
  - **Aujourd'hui > 35% des routes ont un état « valid », + de 64k de routes**



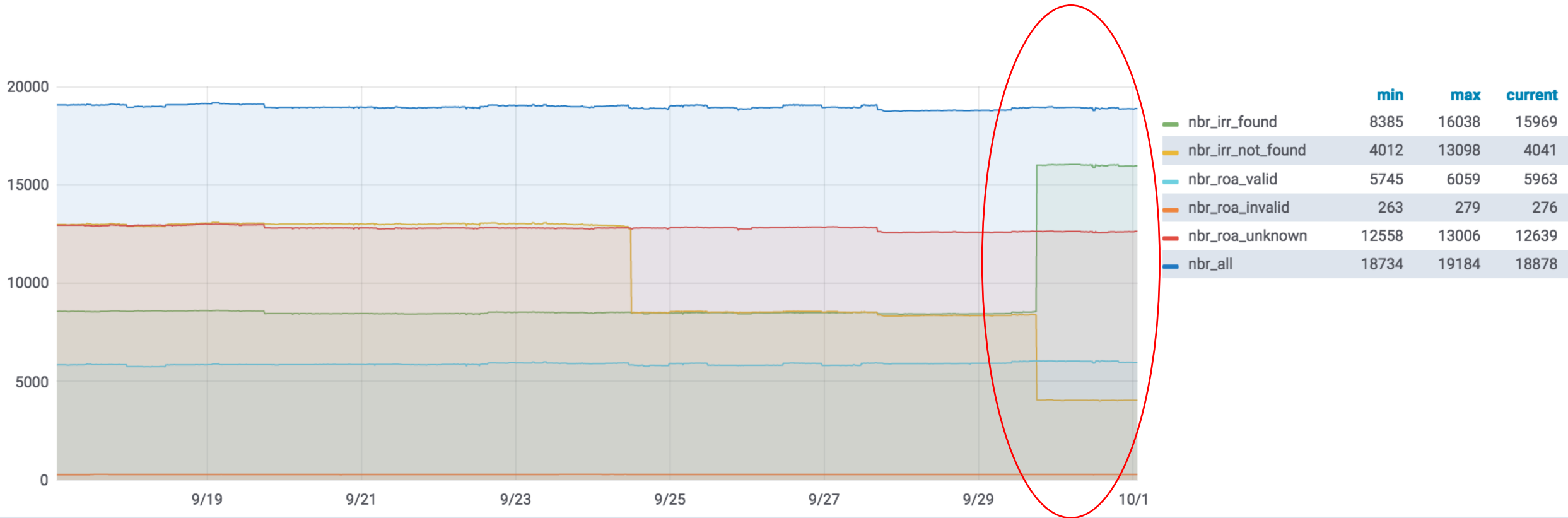
# Filtrage IRR

- Quelques difficultés pour tendre vers 0
  - Certains ressources dans certains RIR...



# Adoption de RPKI

## Filtrage IRR – Effet FRNOG?



# Adoption de RPKI

## Impact potentiel sur le trafic



Résolu avec mise à jour de peeringdb



Bits/s	Last	Avg	Max	95th
In	95.34M	81.92M	815.95M	141.09M
Out	2.57G	1.59G	3.82G	3.05G
Highest				3.05G
Total	559.04T (In 27.43T Out 531.61T)			

# IRR+RPKI/ROA : Les 2 choses à retenir

- Problème “IRR not found” :
  - Maintenir les objets ROUTE @RIR DBs
  - Maintenir PeeringDB à jour

Organisation	<u>France-IX</u>
Alias	FranceIX
Site Internet	<u><a href="http://www.franceix.net">http://www.franceix.net</a></u>
Numéro d'AS principal	57734
IRR as-set/route-set	AS57734







- ROA/RPKI :
  - déclarer les ROA (Ca prend quelques minutes et ca permettra d'avoir un internet plus sur)
  - filtrer les routes “INVALID” ... plus compliqué

# RS - Monitoring

- lg.franceix.net

```
37.49.234.0/24    via 37.49.236.242 on eth1 [RS2_PAR 2017-05-17 from 37.49.236.251] * (100) [AS57734i]
Type: BGP unicast univ
BGP.origin: IGP
BGP.as_path: 57734
BGP.next_hop: 37.49.236.242
BGP.local_pref: 123
BGP.community: (51706,51706) (51706,64602) (51706,64650) (51706,65011) (51706,65012)
```

# RS - Monitoring

Peer	tatus	ASN	AS Set	IP	Since	Routes received	Routes advertised
 1&1	<span style="color: green;">●</span>	8560	AS-IONOS	37.49.236.42	2021-05-12 12:37:12	299	153429
 31173 Services AB	<span style="color: green;">●</span>	39351	AS-ESAB	37.49.237.171	2021-05-12 12:39:04	74	153611
 ABICOM	<span style="color: green;">●</span>	203349	AS-ABICOM	37.49.238.22	2021-09-26 00:10:15	1	153680
 Acorus Networks	<span style="color: green;">●</span>	35280	AS-ACORUS	37.49.237.108	2021-05-12 12:43:22	730	152699
 Acropolis Telecom	<span style="color: green;">●</span>	29513	AS-INITIALS	37.49.236.13	2021-06-13 04:10:31	9	153368
 Adeli	<span style="color: green;">●</span>	43142	AS-adelinovius	37.49.236.111	2021-08-04 19:04:08	36	153643
 Adenis	<span style="color: green;">●</span>	51985		37.49.236.142	2021-05-12 12:46:24	3	153672

IRR-RS1

730

FOUND



0

NOT FOUND



ROA-RS1

521

VALID



0

INVALID



209

UNKNOWN



# ROA et RTBH

- Le service RTBH est souvent proposé par les IXP
- En cas d'attaque DDOS, on veut souvent ajouter une annonce spécifique (IPv4 /32) pour blackholer ce trafic : utilisation de la communauté BGP (RFC7999) (ex : 65535:666)
- Les bonnes pratiques sont :
  - **NE PAS créer temporairement d'entrée ROA pour autoriser cette annonce**
  - **NE PAS créer d'entrée définitive permettant d'autoriser cette annonce**
  - **→ NE PAS JOUER SUR RPKIMAXLEN**



# ROA et RTBH

- **Drafts en cours de discussion : The Use of Maxlength in the RPKI (draft-ietf-sidrops-rpkimaxlen-07)**
  - Décrit les risques d'utiliser un maxlen trop « large »
- **Une autre approche : draft-spaghetti-sidrops-rpki-doa : RPKI Discard Origin Authorization (DOA)**
  - Objet et mécanisme spécifique pour confirmer si un type d'annonce est autorisé à des fins de filtrage de trafic
  - Utilisation de l'infra RPKI déjà en place

# références

- <https://www.franceix.net/fr/infrastructures/serveurs-de-routes>
- <https://www.team-cymru.org/bogon-reference-http.html>
- <https://datatracker.ietf.org/doc/html/rfc7454>
- <https://datatracker.ietf.org/doc/html/rfc7999>
  
- draft-ietf-sidrops-rpkimaxlen-07
- draft-spaghetti-sidrops-rpki-doa



Together, your Internet, even better



**ON RECRUTE!**  
**smuyal@franceix.net**



Together, your Internet, even better



Questions??