Route Servers,
features
and security

Arnaud FENIOUX - FranceIX
@afenioux #RIPE72
2016-05-25

Route Servers Definition

- Multi-Lateral Peering Exchange
- Available at all locations of an IXP
- Members automatically exchange routes with other members through a single BGP session
- Provided as an extra service on many IXs, usually with no extra charge

Route Servers Benefits

- Routes servers are a popular service at IXPs
  - **95%** of France-IX's community use them in **Paris**
  - **68%** of France-IX's community use them in **Marseille**

- Main benefits for the peers:
  - Less BGP sessions to configure
  - Quick and easy way to get lot of routes
  - Easily tunable using BGP communities
  - No need to make multiple peering arrangements with other members

<blink> **SAVE TIME!** </blink>

Route Servers Exceptions

- Can be considered as a SPOF

- Some of the routing intelligence is out of the NetOps control
  -> Need trust into the IXP

- Selective announcement may need some tweaking to keep symmetrical paths

- Peers ASN will vary and increase with time
  -> Adds some new destinations though the IXP
  -> Might not be wanted if you have strict peering policy or fine traffic tuning

-> Some CDN prefer to establish directly bilateral BGP peering

Route Servers RFC-ization

[I-D.ietf-idr-ix-bgp-route-server]
outlines a specification for multilateral interconnections at Internet exchange points.

[I-D.ietf-grow-ix-bgp-route-server-operations]
describes operational considerations for multilateral interconnections at IXPs.

[I-D.kklf-sidr-route-server-rpki-light]
defines the usage of the BGP Prefix Origin Validation State Extended Community to signal prefix origin validation results from a route-server to its peers.

Route Servers Implementation

Various options on the market:

- BIRD (most used, actively developed)
- GoBGP (new, multicore)
- OpenBGPD
- quagga
- Cisco (proprietary, discontinued)

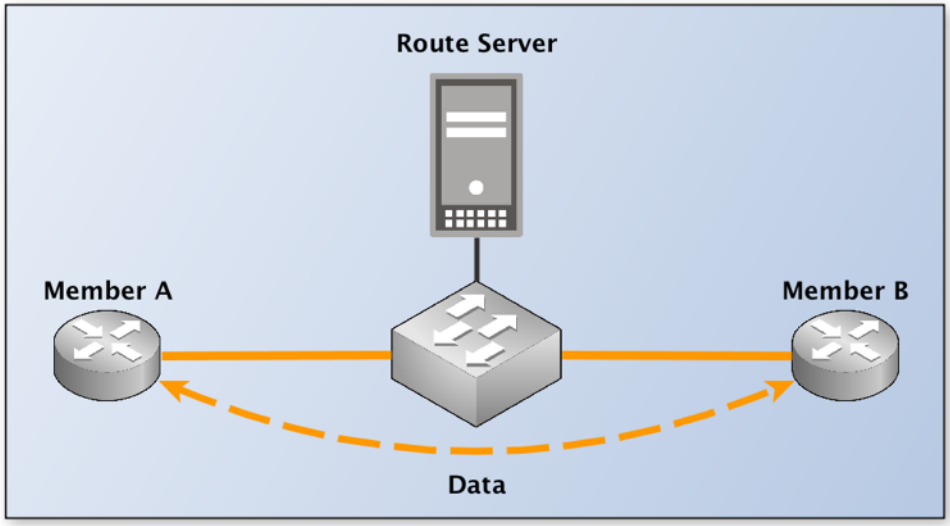
Route Server

Features

Data plane vs Control plane

Data plane :

- Path used by the packets of data to reach the destination
  - e.g. : web browsing… and everything transferred between the client and the server.

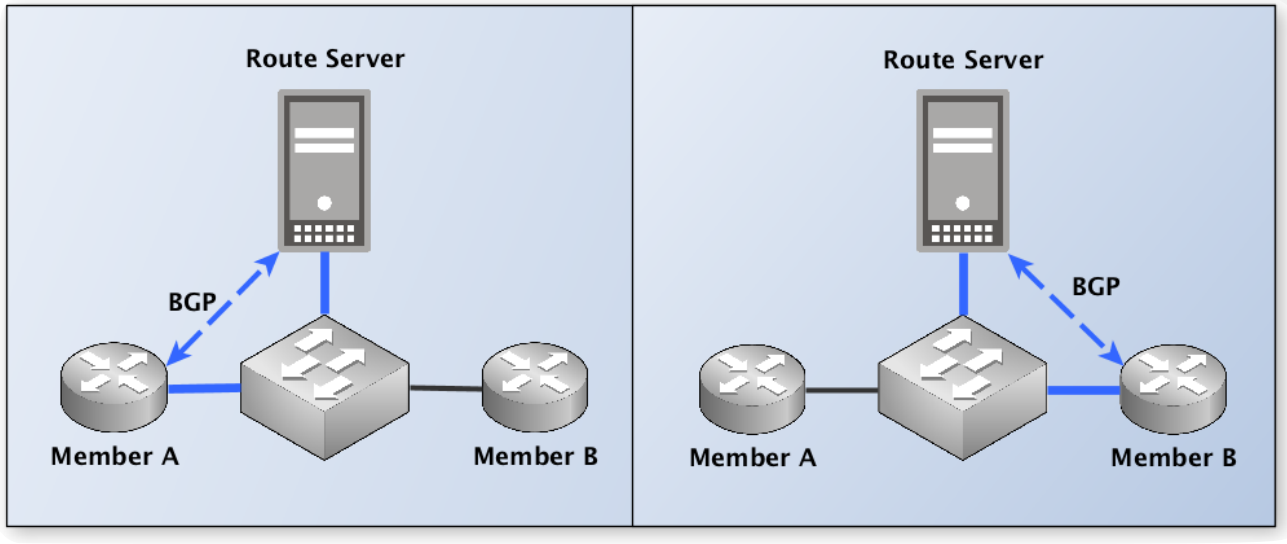


Data plane and Control plane, can be the <u>same</u>

Data plane vs Control plane

Control plane :

- Path used for signaling between routers
  - e.g. : packets of the routing protocol.

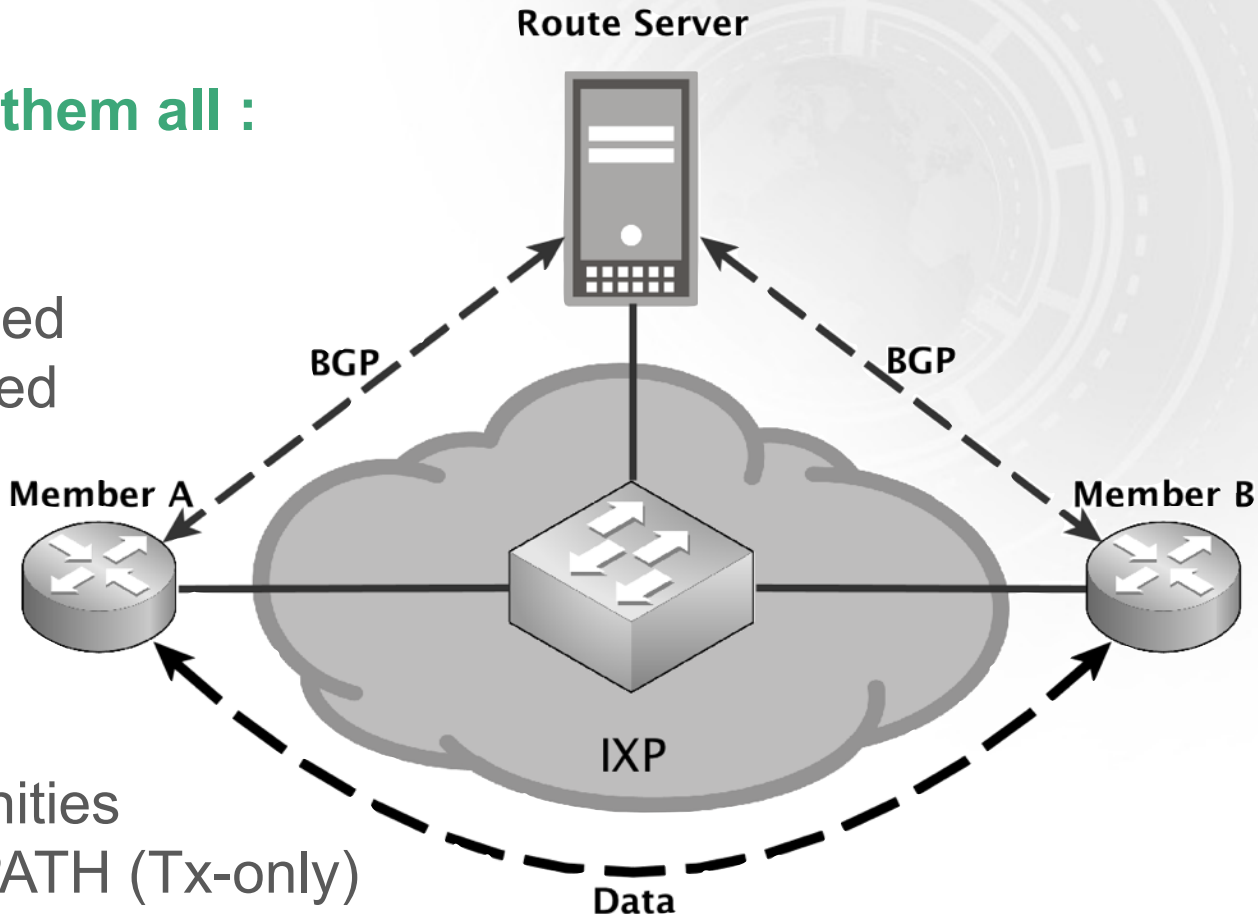


Data plane and Control plane, can be <u>different</u>

Route Server

One session to rule them all :

- Select Best Path
- AS-PATH not modified
- Next-hop not modified
- Trafic in direct



- Should not interpret well-known communities
- May support ADD-PATH (Tx-only)

/!\ Blackholing if Data-Plane broken

Selective announcement

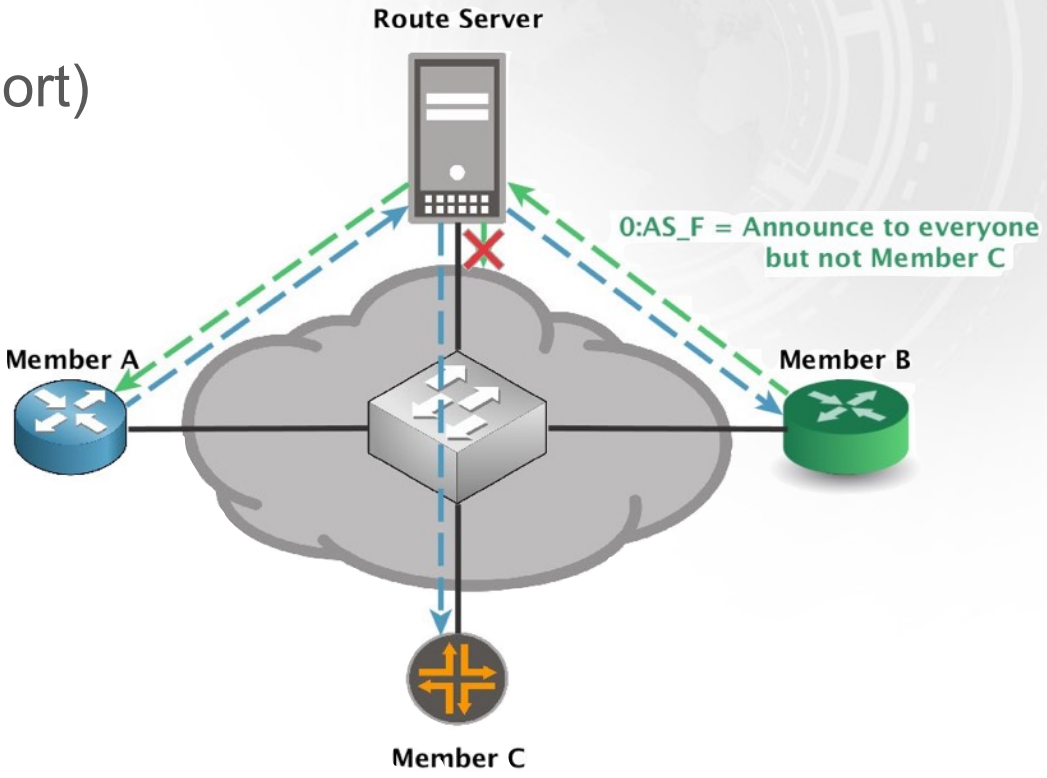
using :

- BGP communities
- IRR (aut-num import / export)

actions :

- Filtering
- AS-PATH prepending
- MED override

0:peer-as = Don't send route to this peer AS



/!\ Can lead to asymmetrical traffic and Path Hiding

Route Server

Security

Fat finger errors

Martians (IPv4 and v6)

- Filtering martian's prefixes
  https://www.team-cymru.org/bogon-dotted-decimal.html

Max prefix limit

- Limits the number of prefixes learned per peer on RS
  Shutdown the BGP session if the threshold is exceeded

Prefix length

- IPv4 : /8 to /24 are allowed
- IPv6 : /19 to /48 are allowed

Protects from :

- leaks of full table / leaks of internal routes

“Thin” finger errors

Next-hop

- Verification that the next-hop IP in the BGP update is also the source of the IP packet.

First AS in AS-PATH

- Verification that the leftmost AS of the AS-PATH is the peer AS.

Protects from :

- Faked BGP announcements
- Traffic redirection to a victime
- Shadowing of the attacker’s AS

IRR Lock Down AS-SET or ASN

- Allows only registered prefixes by some AS-SET or ASN

AS-SET -> AUT-NUM -> ROUTE(6) -> INETNUM(6)

- IRR Explorer + BGPQ3 + rr.ntt.net = <3

```
./bgpq3  -h rr.ntt.net  -S RIPE,APNIC,AFRINIC,ARIN,NTTCOM,\
ALTDB,BBOI,BELL,GT,JPIRR,LEVEL3,RADB,RGNET,SAVVIS,TC \
-A -b -6 -l pfx_table_as57734 AS57734

pfx_table_as57734 = [
   2001:7f8:54::/48,
   2a00:a4c0::/32
];
```

Protects from:

- Prefixes Hijacking

/!\ depends on the quality of data in the IRR

RPKI / ROA

RPKI / ROA

- Validate that the origin AS of the announce is authorised to announce this prefix.

Registration through LIR Portal :
https://www.ripe.net/manage-ips-and-asns/resource-management/certification/resource-certification-roa-management

Protects from :

- Some hijacking of prefixes

/!\ Does not validate transitivity

Conclusion

Filtering prefixes on Route Servers :

- is “good for the internet”
- forces users to update their IRR records
- can lead to reject valid prefixes
  (because some big ISP have to many LIR and records and they don't even know how to manage them)

IXP are working toward an effective filtering solution, enabling secure BGP announcements between members.

References

RIPE 70 : IRR Lockdown
https://ripe70.ripe.net/wp-content/uploads/presentations/52-RIPE70_jobsnijders_irrlockdown.pdf

IRR Explorer
http://irrexplorer.nlnog.net/

Euro-IX 27 : Route Server Policies @ IXPs
https://euro-ix.net/m/uploads/2015/10/27/e-BH-20150921-Euro-IX-Route-Server-Filtering-at-IXPs.pdf

AMS-IX Falcon class Route Servers
https://ams-ix.net/technical/specifications-descriptions/ams-ix-route-servers/falcon-class-route-servers

NANOG 51 : Route Servers, Mergers, Features and More
https://www.nanog.org/meetings/nanog51/presentations/Tuesday/Malayter-Router%20Server%20Presentation%204.pdf

Merci !

Arnaud FENIOUX
@afenioux

For more information about France-IX in Paris and Marseille : **info@franceix.net**