The RPKI Wayback Machine

(or: Ziggy says there's a 50% chance we'll end up in 2011)

Roland van Rijswijk-Deij

NLNETLABS

What we wanted to do

- At NLnet Labs, **we make RPKI Relying Party software** called Routinator
- **Routinator** has seen a **lot of uptake in production** (**thank you!**)
- We want to **test our software** to ensure it is robust
- **Enter:**
  8 years of RPKI ROA data for all the RIRs provided by RIPE NCC!

How we processed the data

- **RIPE NCC archived all RPKI repositories** pretty much **since RPKI day zero**
- We got **dumps in .tar.gz files** with all RPKI objects, but no historic TALs
- So **we wrote a tool we called "Ziggy"** to transport us **back in RPKI time**

Interlude: Ziggy!

- Remember Quantum Leap? I do :-)

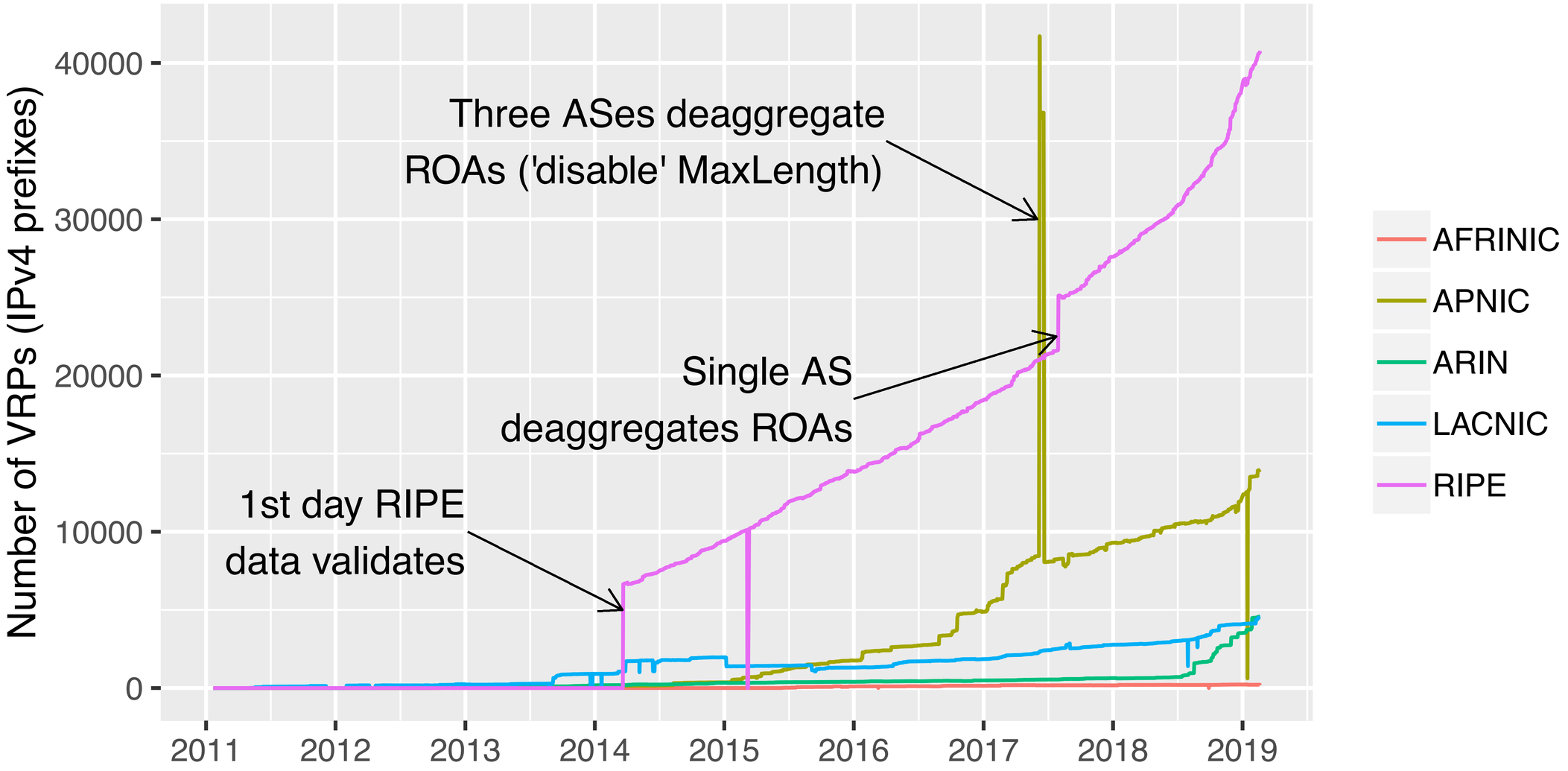
What does Ziggy do?

- You can **give Ziggy** (our Python script) **a date**, and it will then:
  - **Find and unpack all .tar.gz files** for that date, in a Routinator-friendly structure
  - **Recreate TALs** based on the trust anchors from the archives
  - **Run Routinator using "faketime"** for the specified date
- We did this from **January 2011 to February 2019**

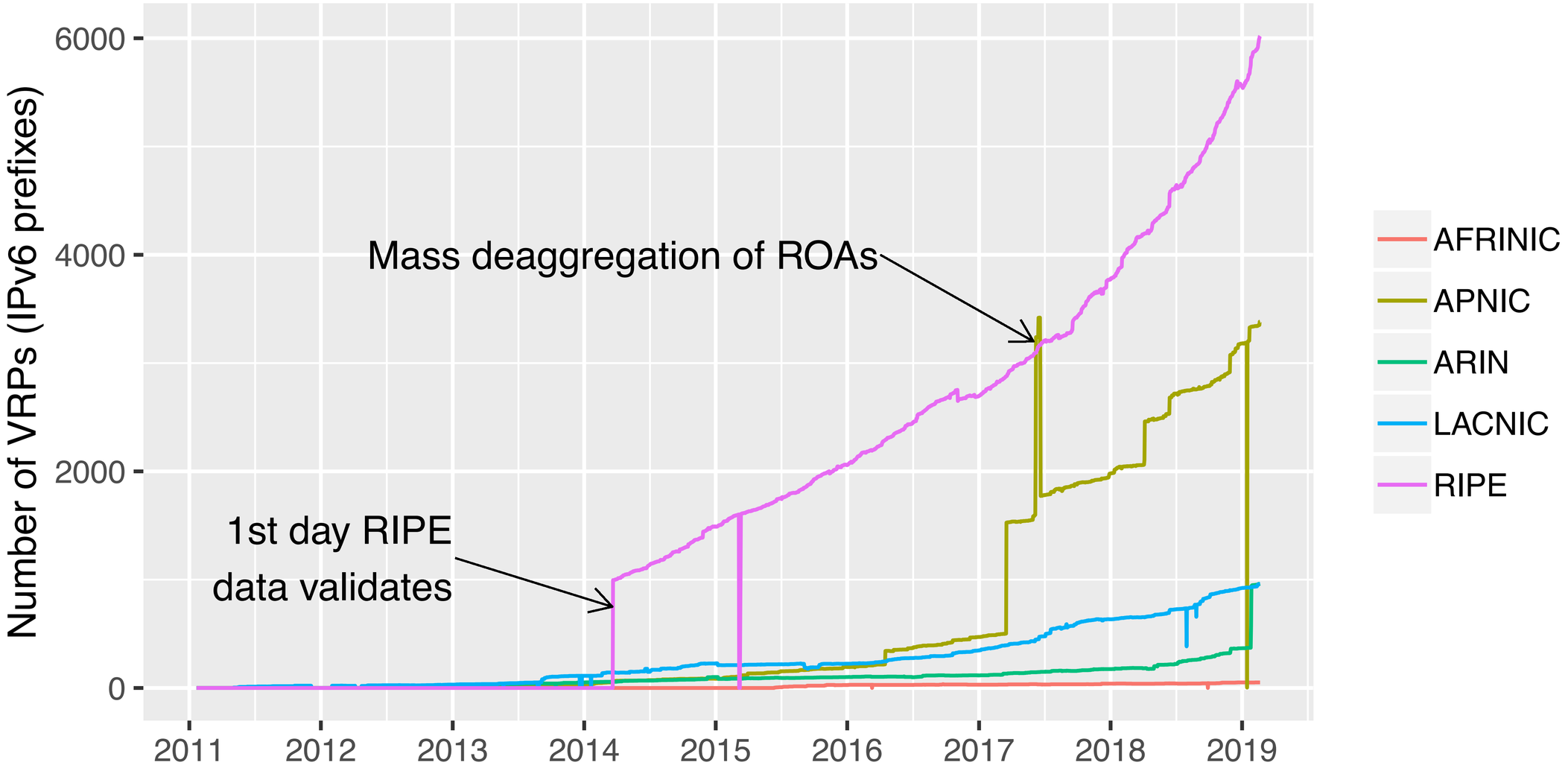
Quick recap: jargon

- Reminder (also if you read the slides later):
- **RPKI** **R**esource **P**ublic **K**ey **I**nfrastructure
- **ROA** **R**oute **O**rigin **A**uthorisation
  (authorises a certain AS to announce certain prefixes)
- **VRP** **V**erified **R**OA **P**ayload (yes, acronym in acronym...)
  (a cryptographically valid statement about a prefix from a ROA)

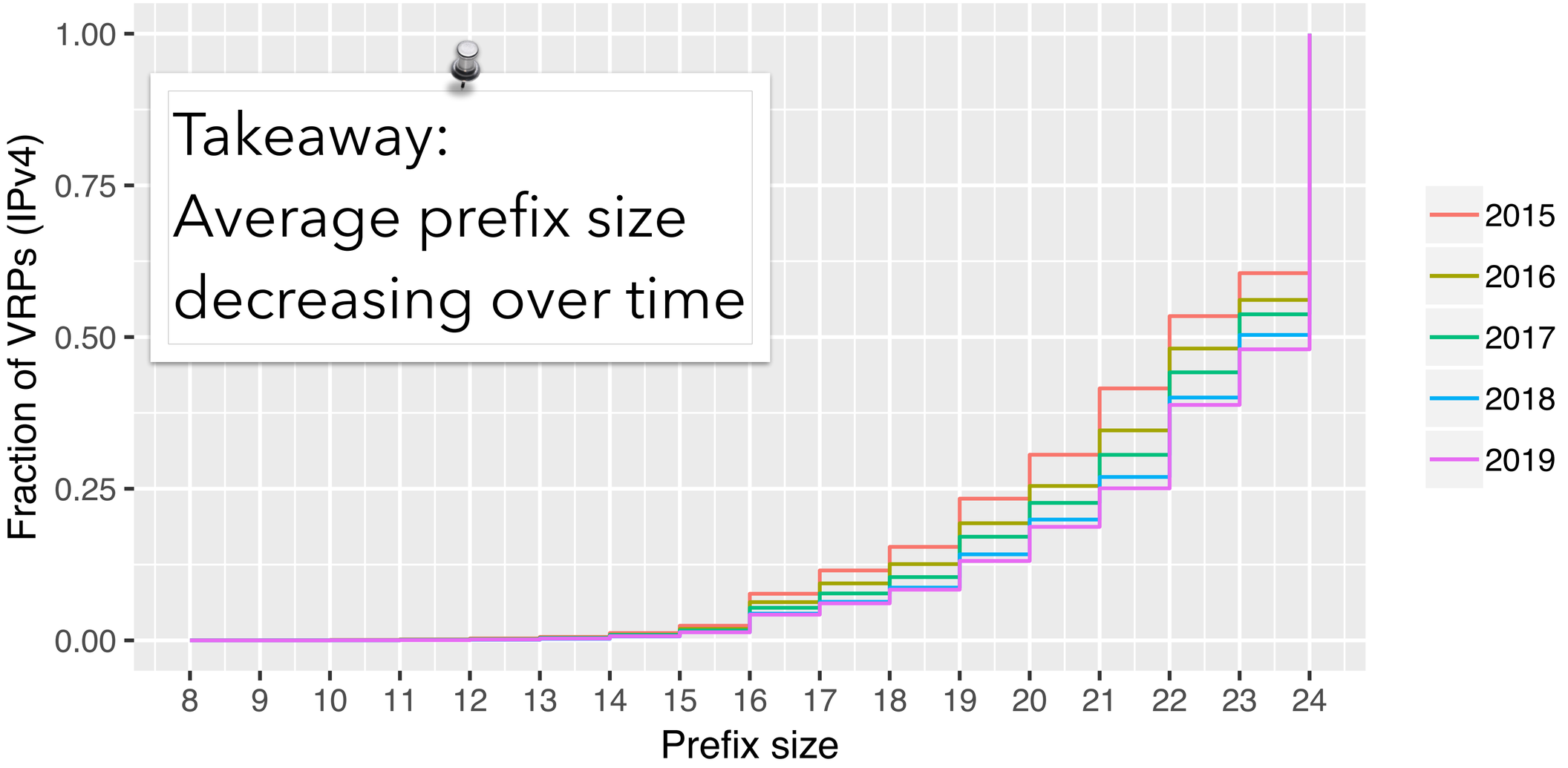
Growth of VRPs over time



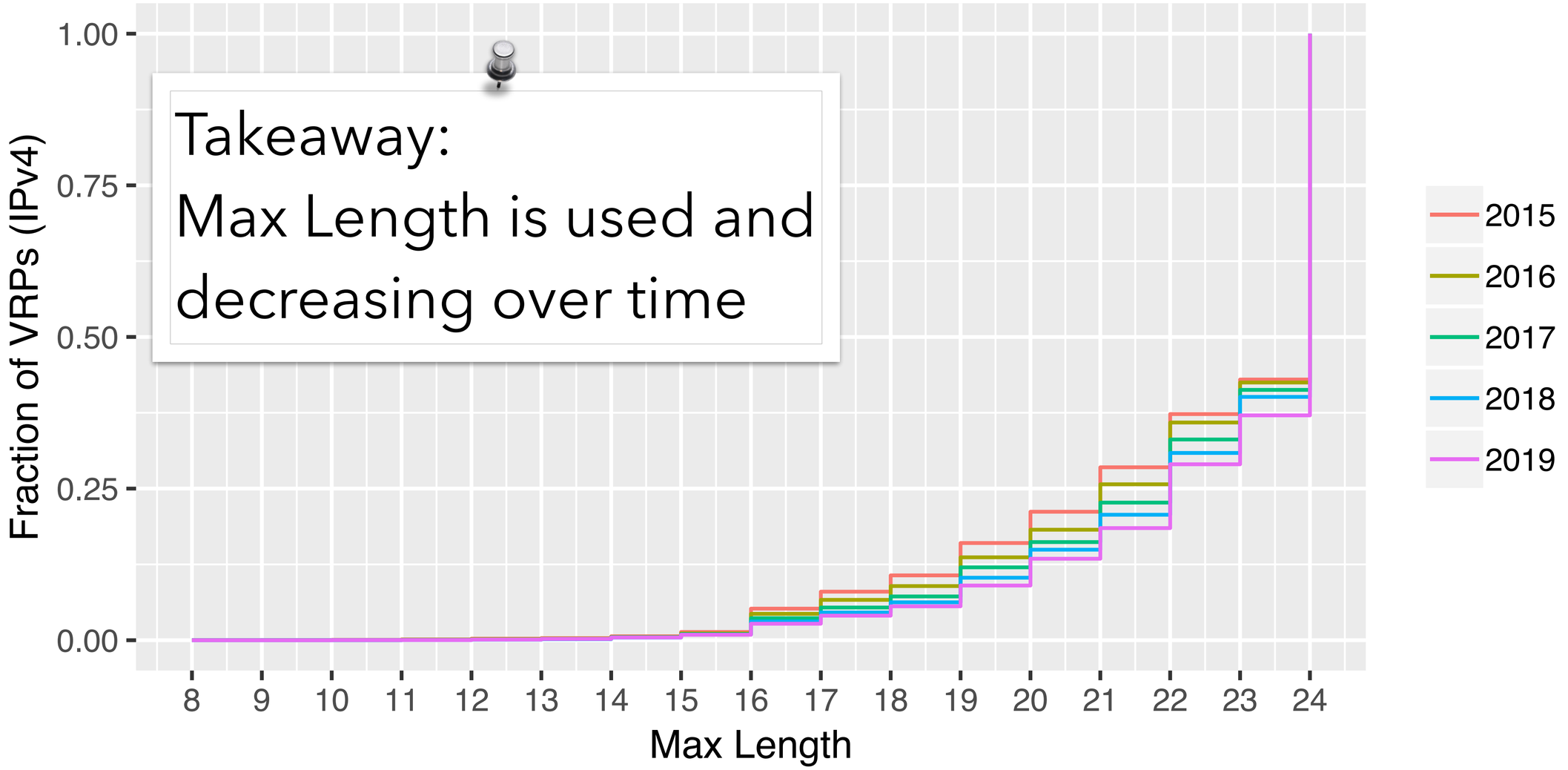
Of course *also* for IPv6 ;-)



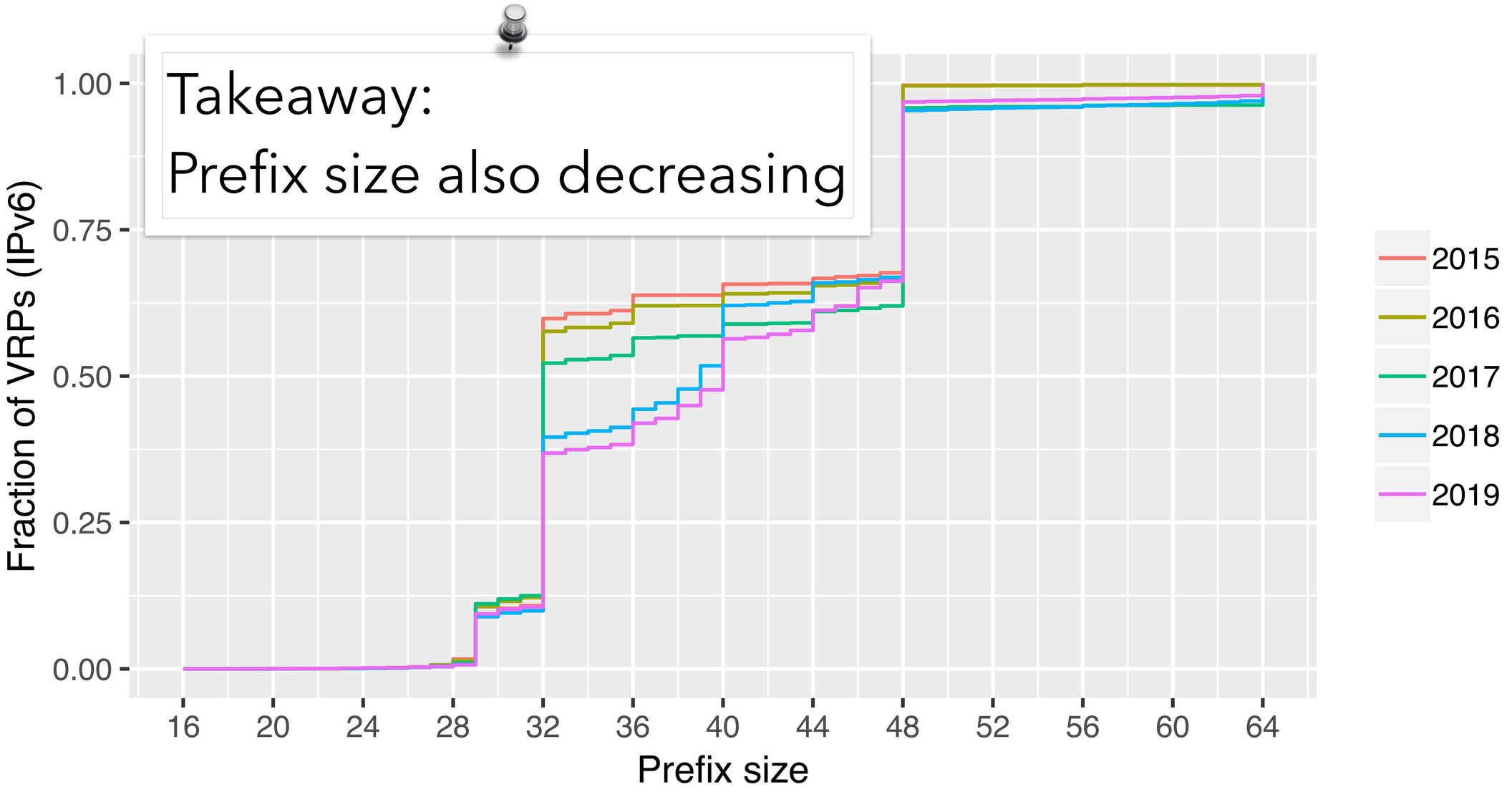
Prefix size in VRPs over time (IPv4)



Max Length in VRPs over time (IPv4)

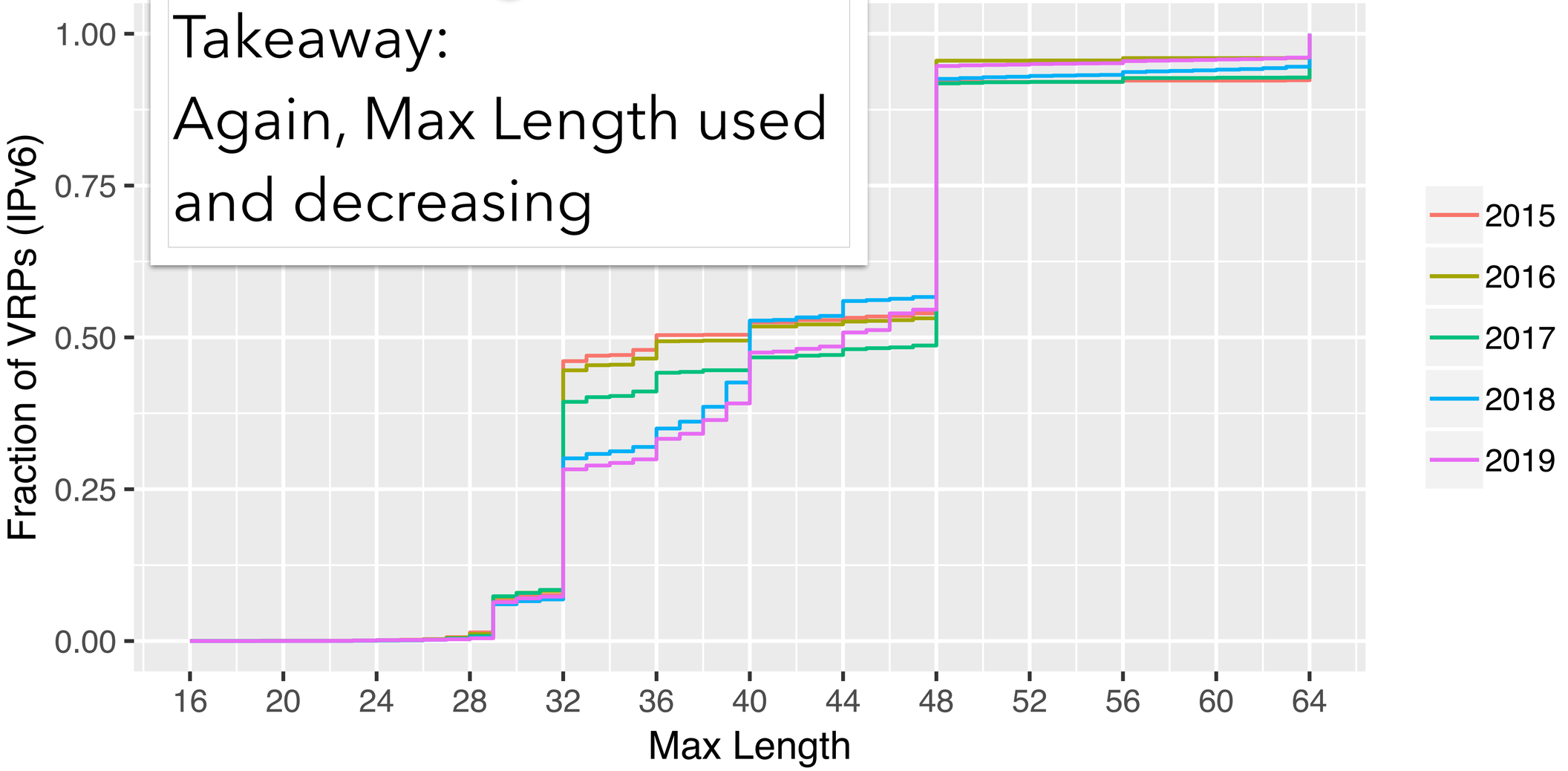


Prefix size in VRPs over time (IPv6)

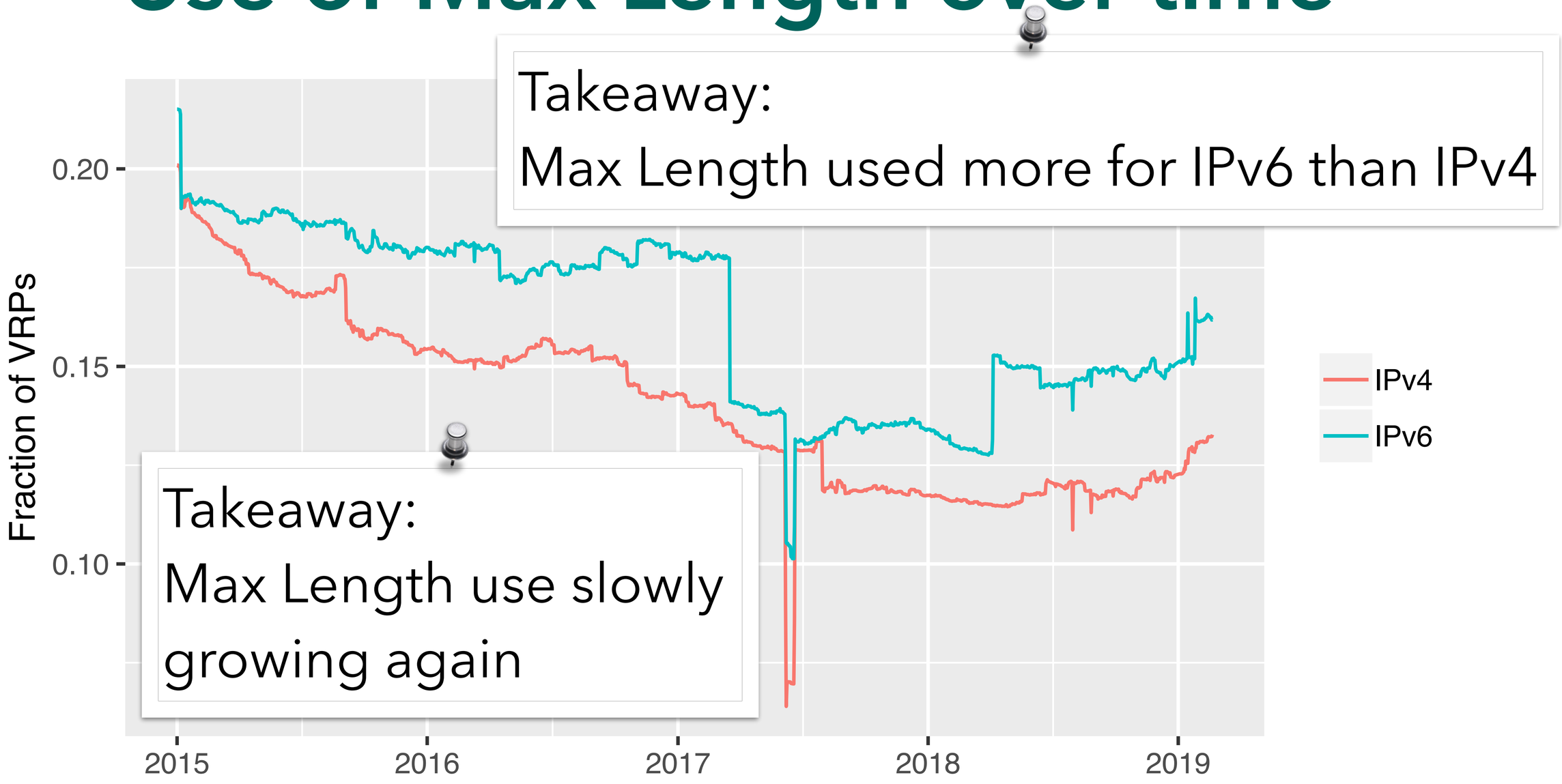


Max Length in VRPs over time (IPv6)

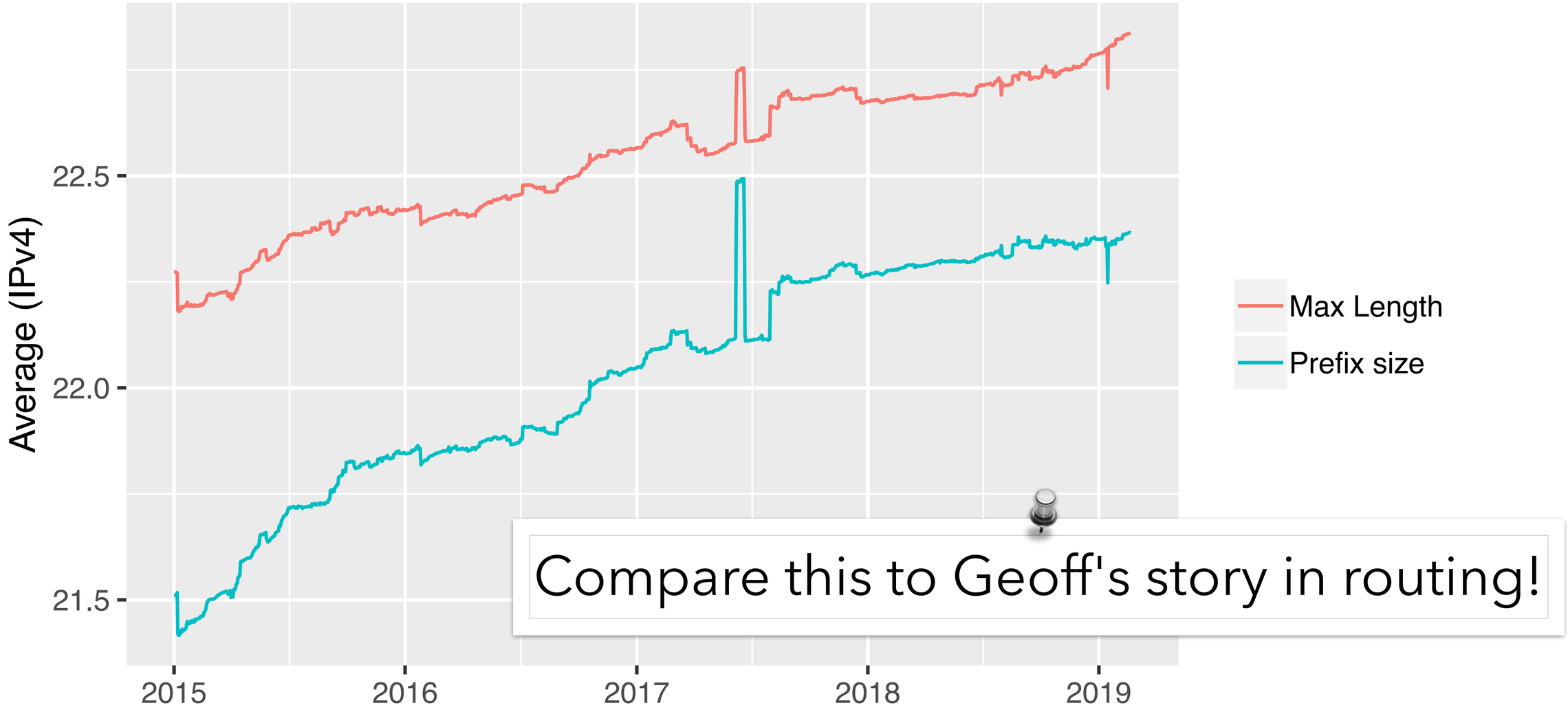
Takeaway:
Again, Max Length used and decreasing



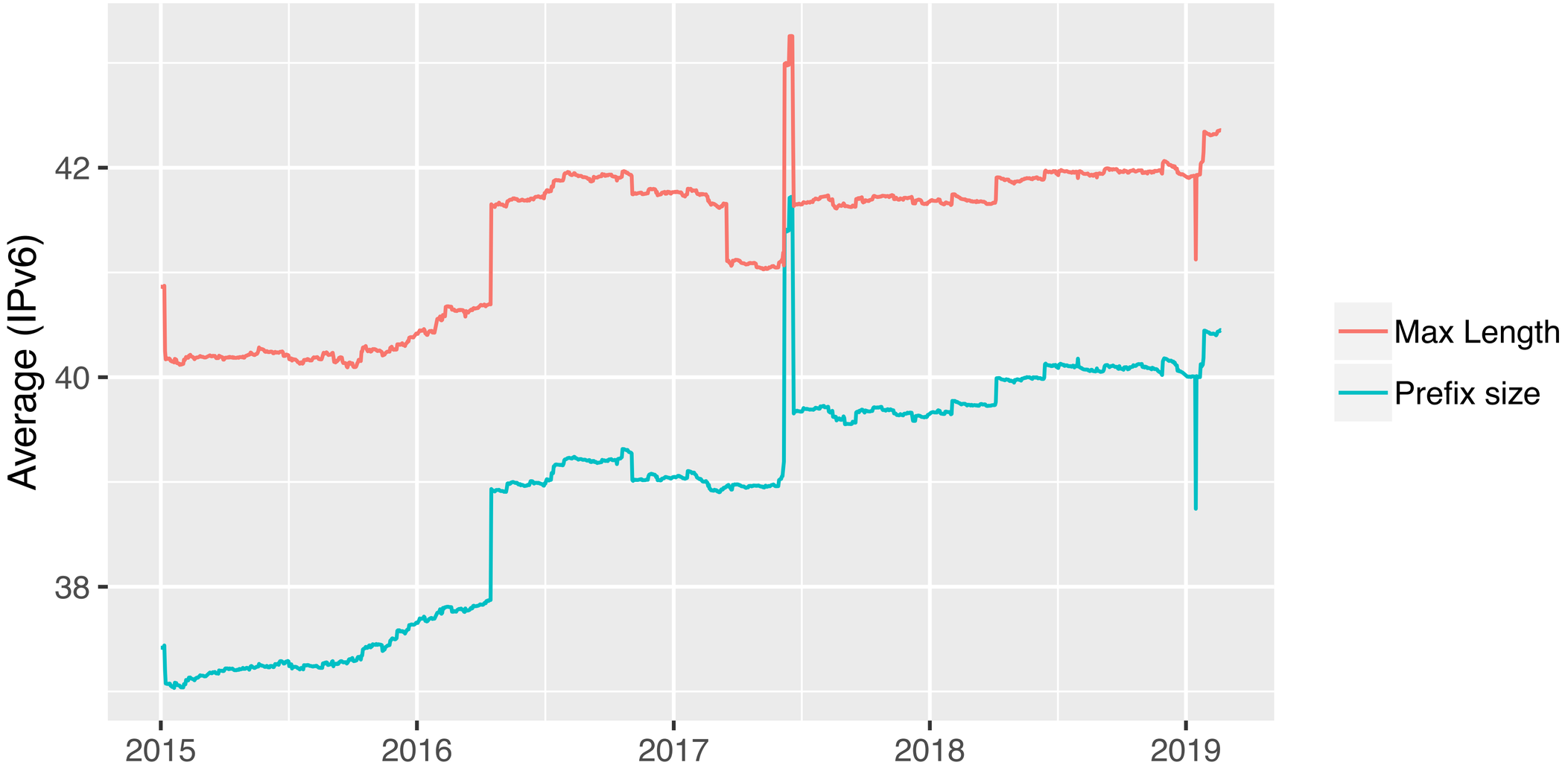
Use of Max Length over time



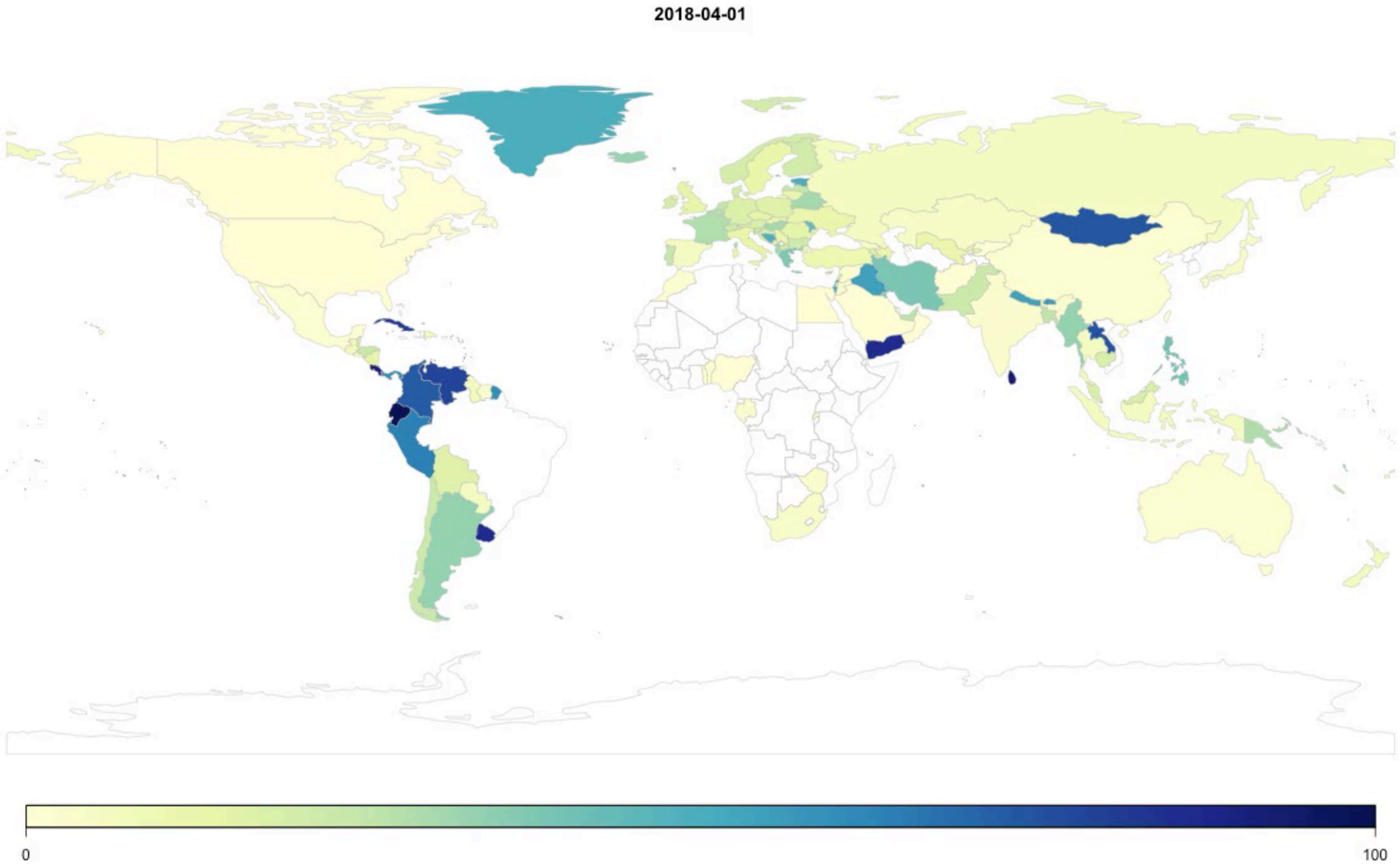
One more thing: average prefix size



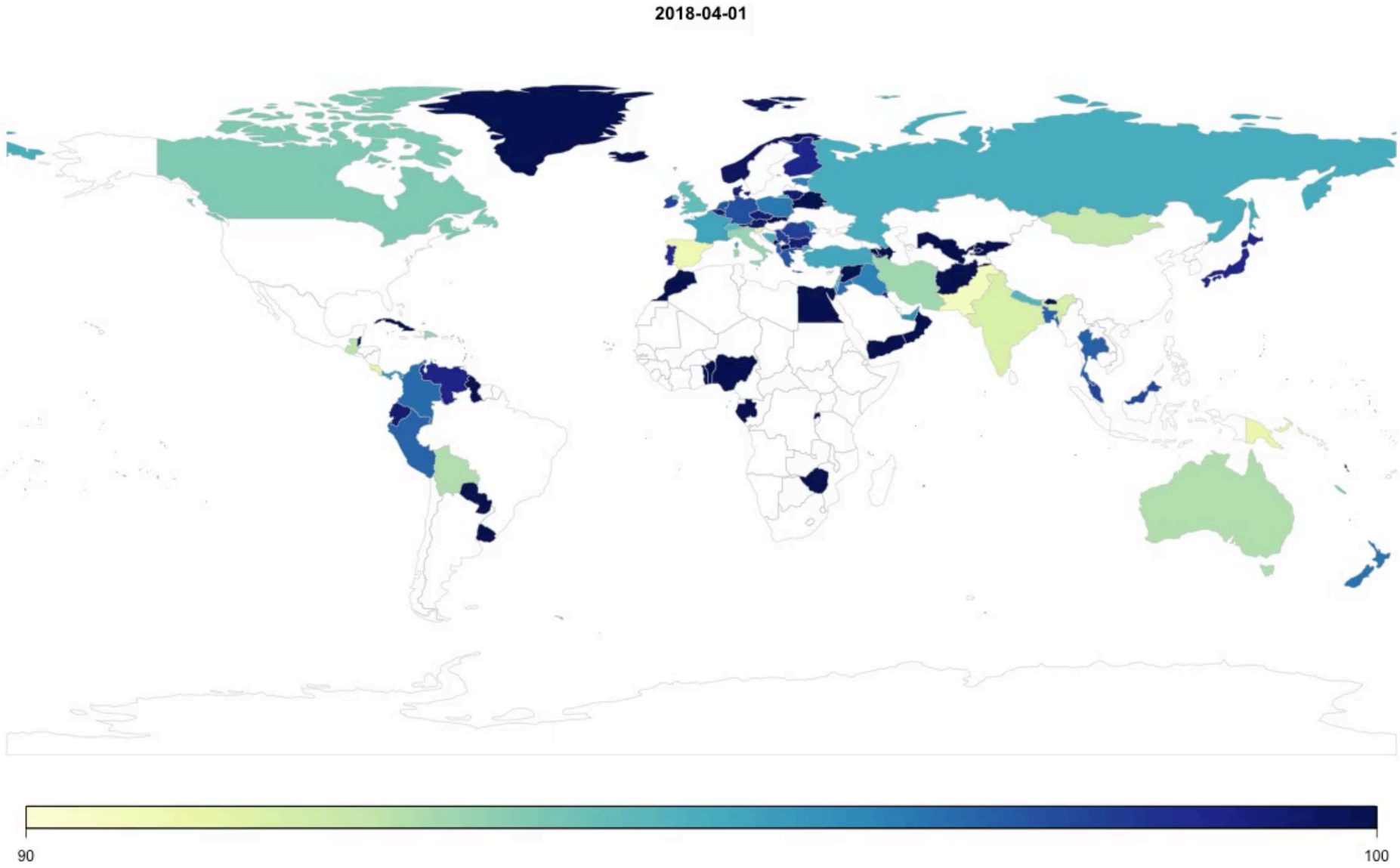
For IPv6 same(-ish) thing



Coverage over time



Accuracy over time



Conclusions

- We wanted to **test Routinator**; turns out **RPKI** use **took** some **time to stabilise to a** well-defined **standard**
  → *Action item: support older standards in Routinator*

- Very **interesting data**, **raises** lots of **questions** and can help **study** how **RPKI** is deployed **in practice**

- **Next step: compare** this **against routing information** over the same period (from RIS, RouteViews, ...)
  → *Paper to be presented at ACM IMC 2019 in Amsterdam, Oct. 21-23*

Open data

- A big **thank you to** the **RIPE NCC and** to **Emile Aben** in particular for providing us with the RPKI dataset!

- The data is now also available as open data: https://ftp.ripe.net/rpki

RIPE NCC

RIPE NETWORK COORDINATION CENTRE

Grab our free OSS tools!

- Routinator:
  https://github.com/NLnetLabs/routinator

- Secure Routing Stats (experimental):
  https://github.com/NLnetLabs/secure-routing-stats
  (produces the graphs with world maps)

- Ziggy:
  https://github.com/NLnetLabs/ziggy

Thank you! Questions?

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

roland@nlnetlabs.nl

and for "Team RPKI": rpki-team@nlnetlabs.nl

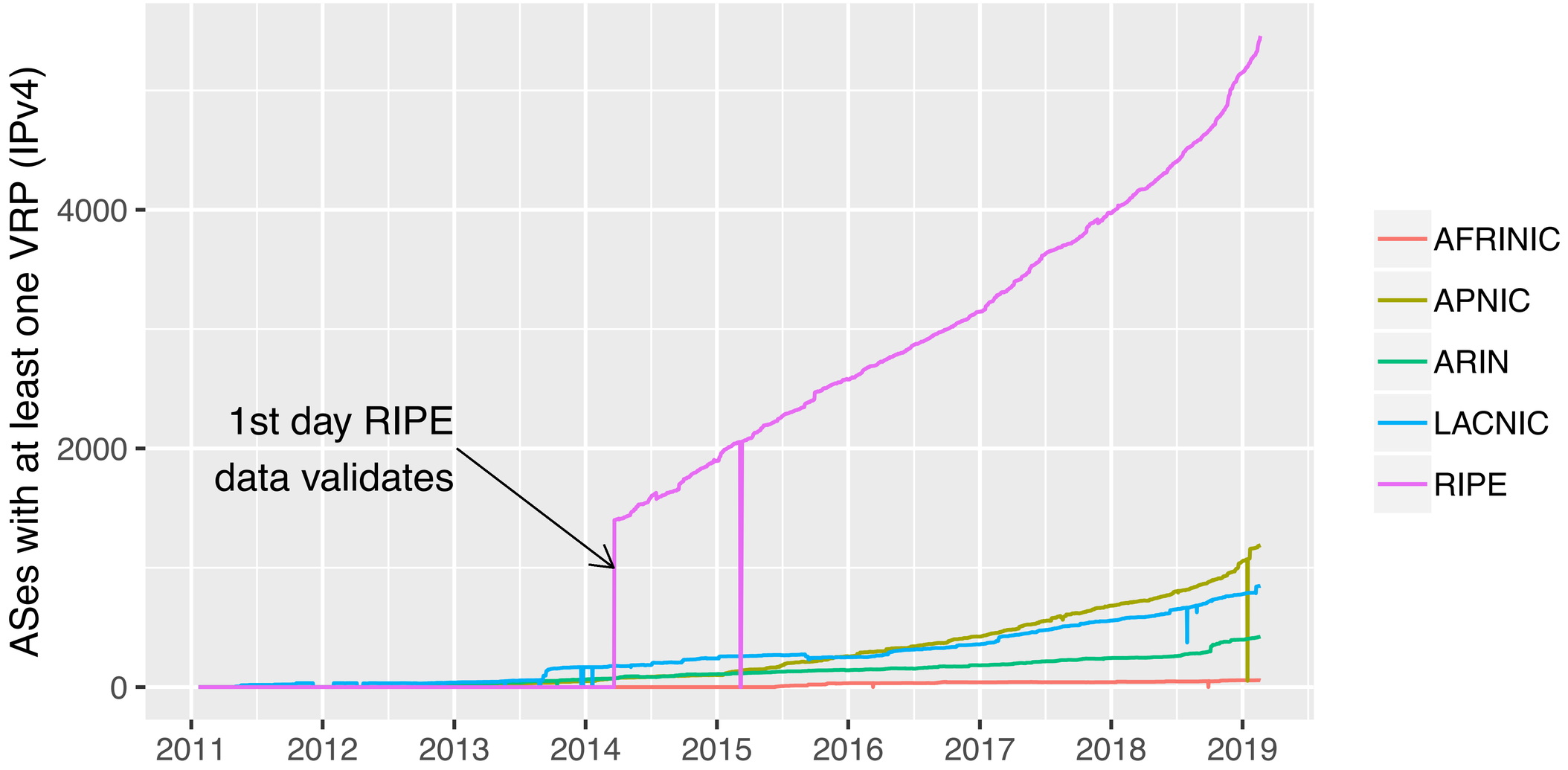
NLNETLABS

BONUS SLIDES

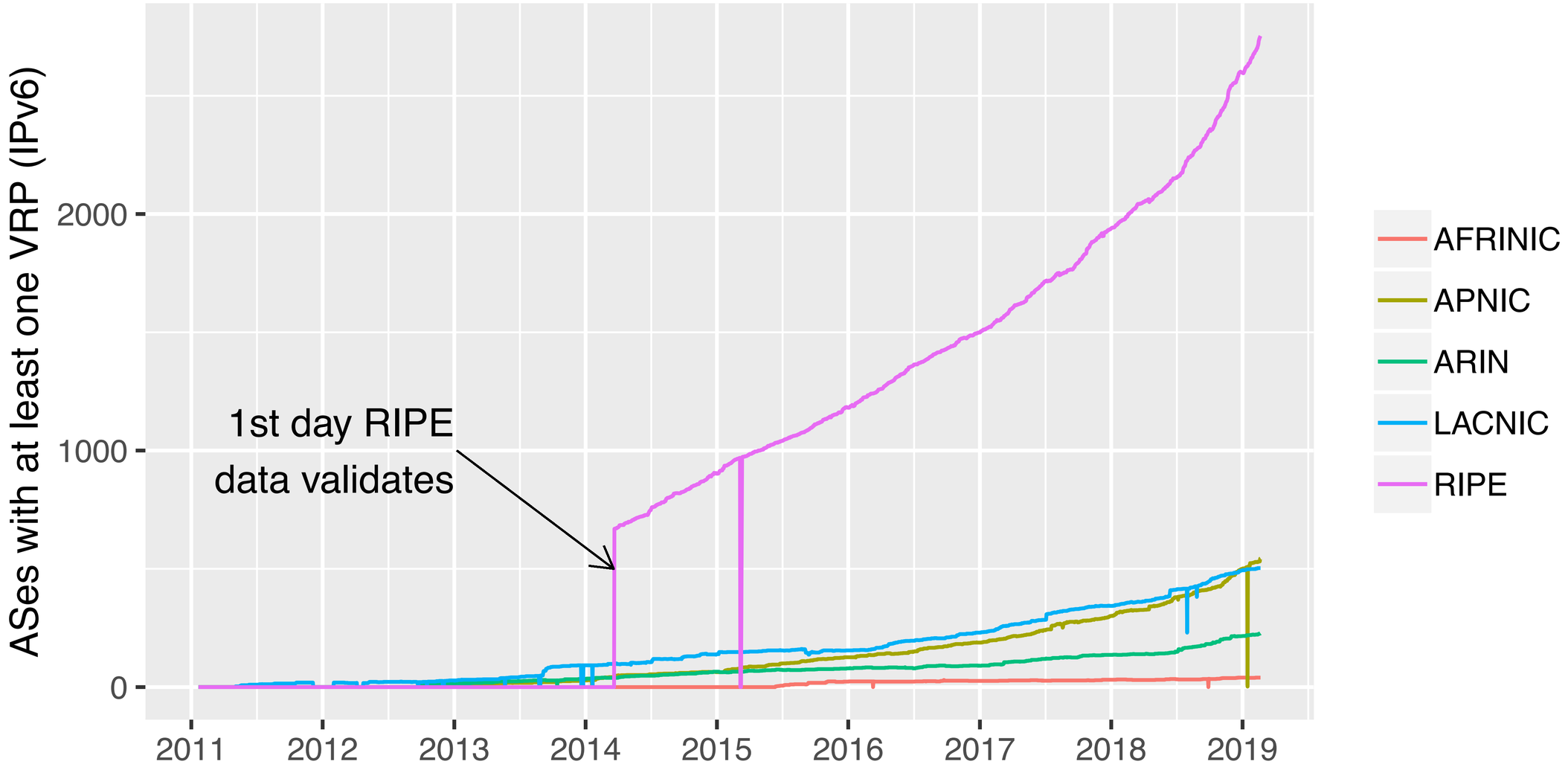
Some more graphs we got from Ziggy
that didn't make it to the talk,
because "time" ;-)

NLNETLABS

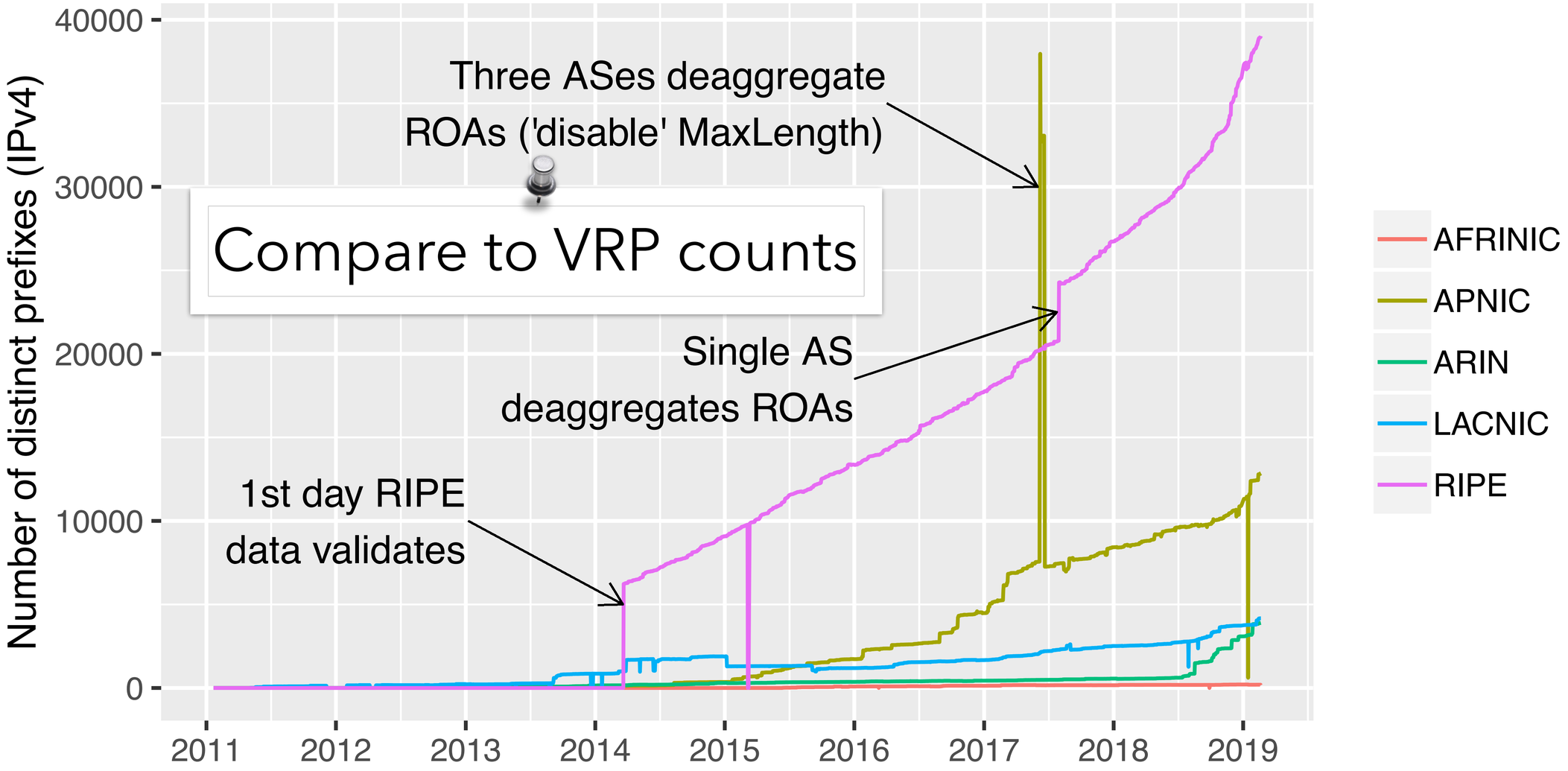
Number of ASes with a VRP (IPv4)



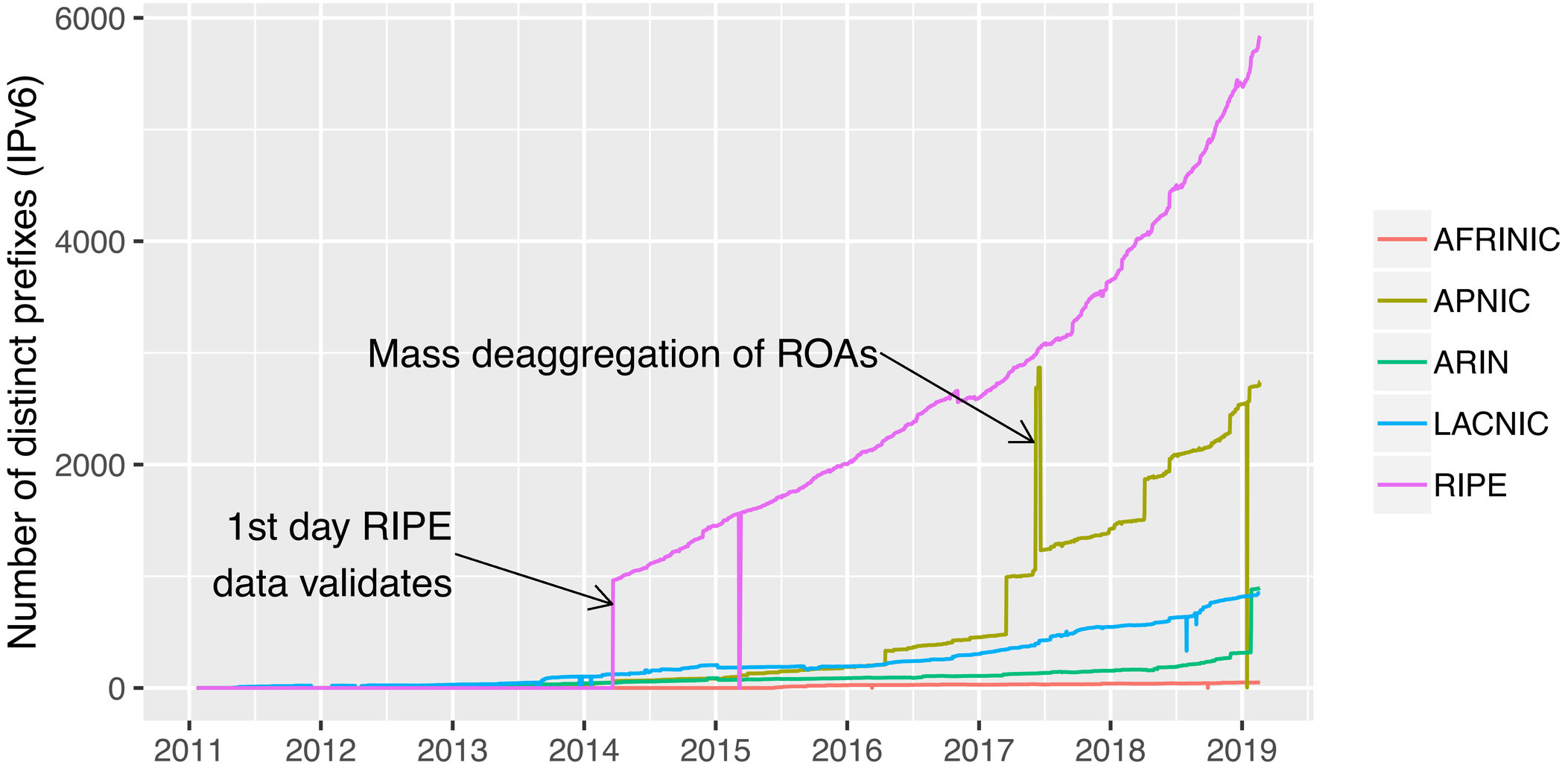
Number of ASes with a VRP (IPv6)



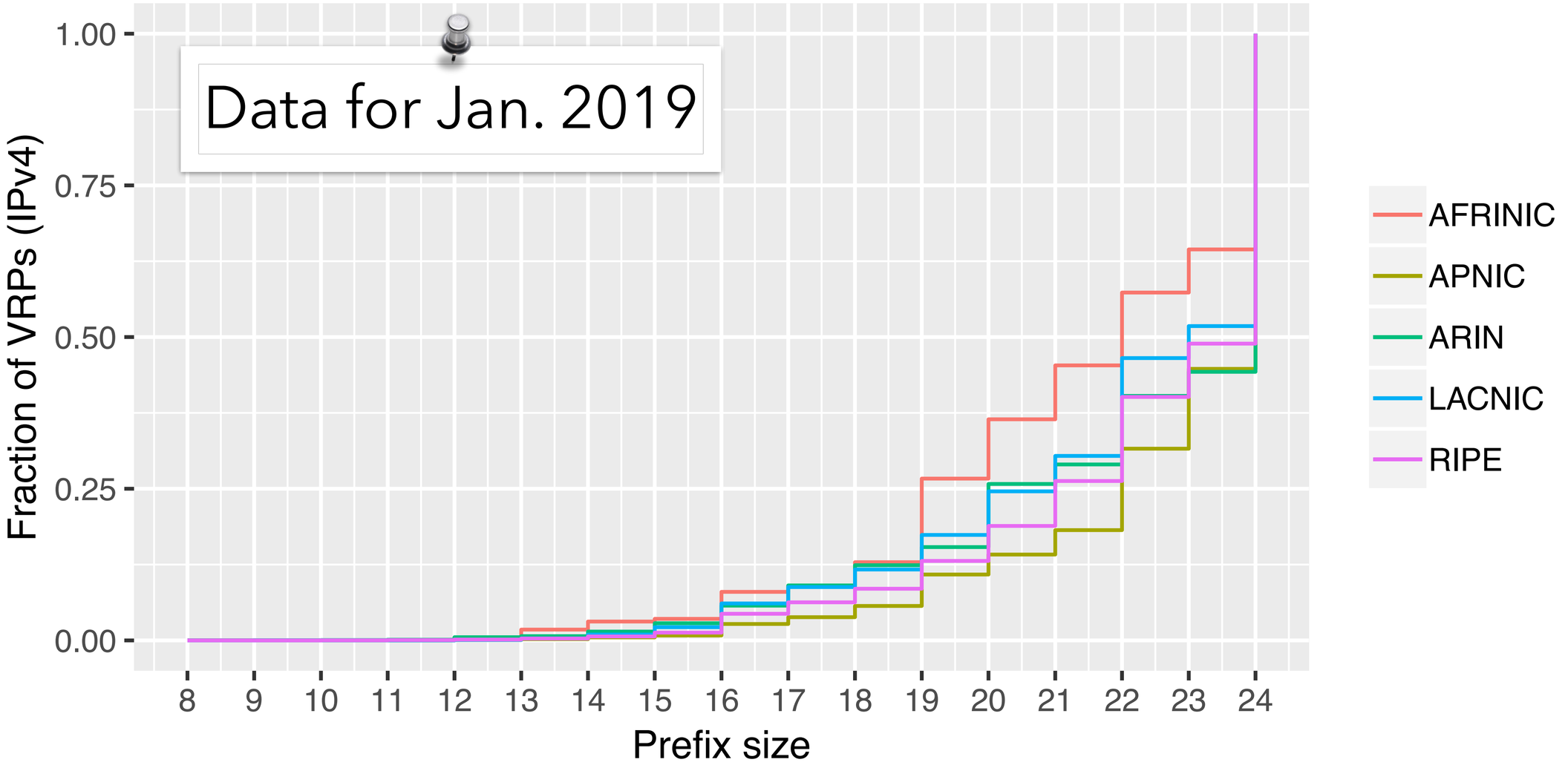
Number of distinct prefixes (IPv4)



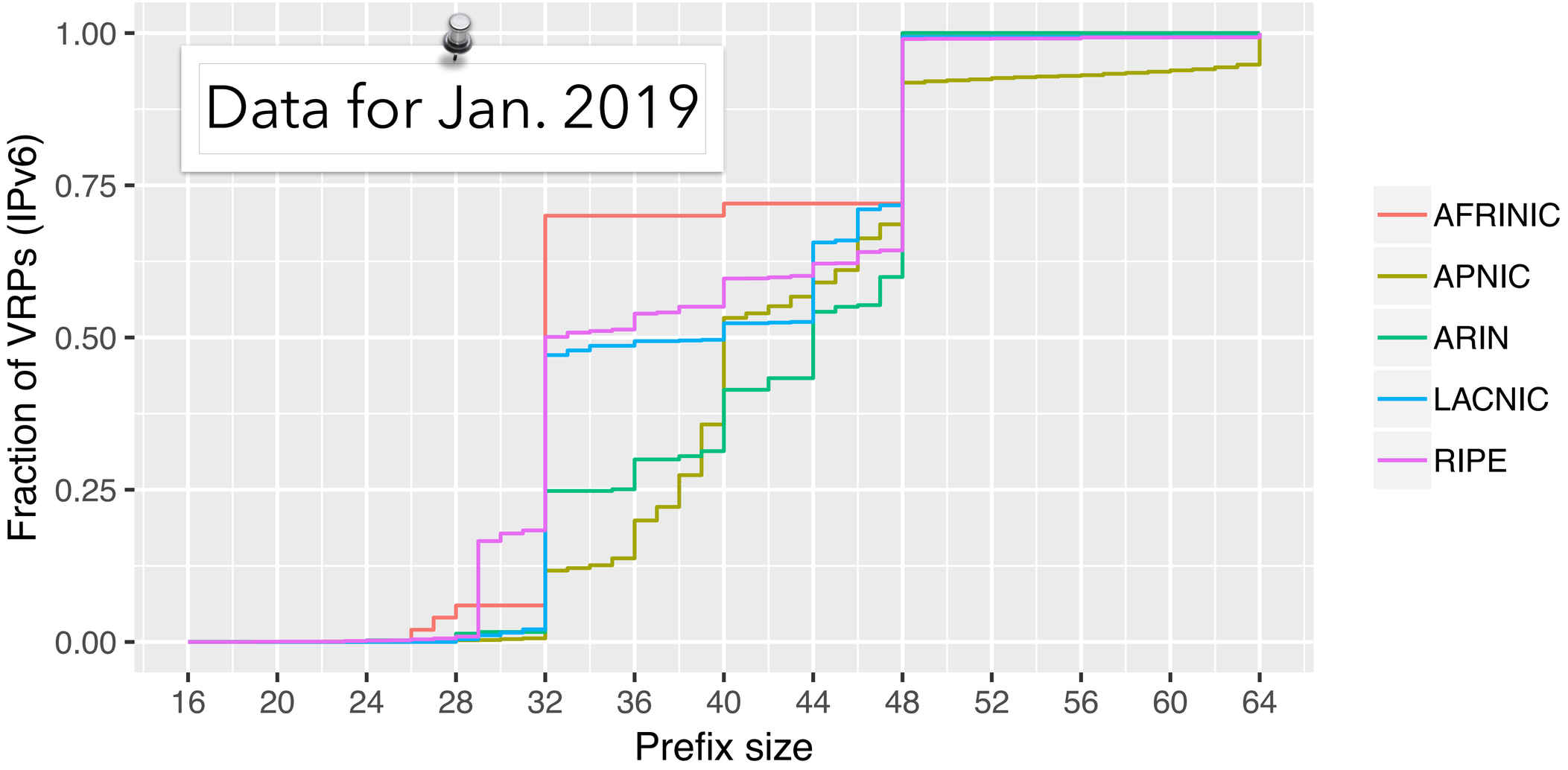
Number of distinct prefixes (IPv6)



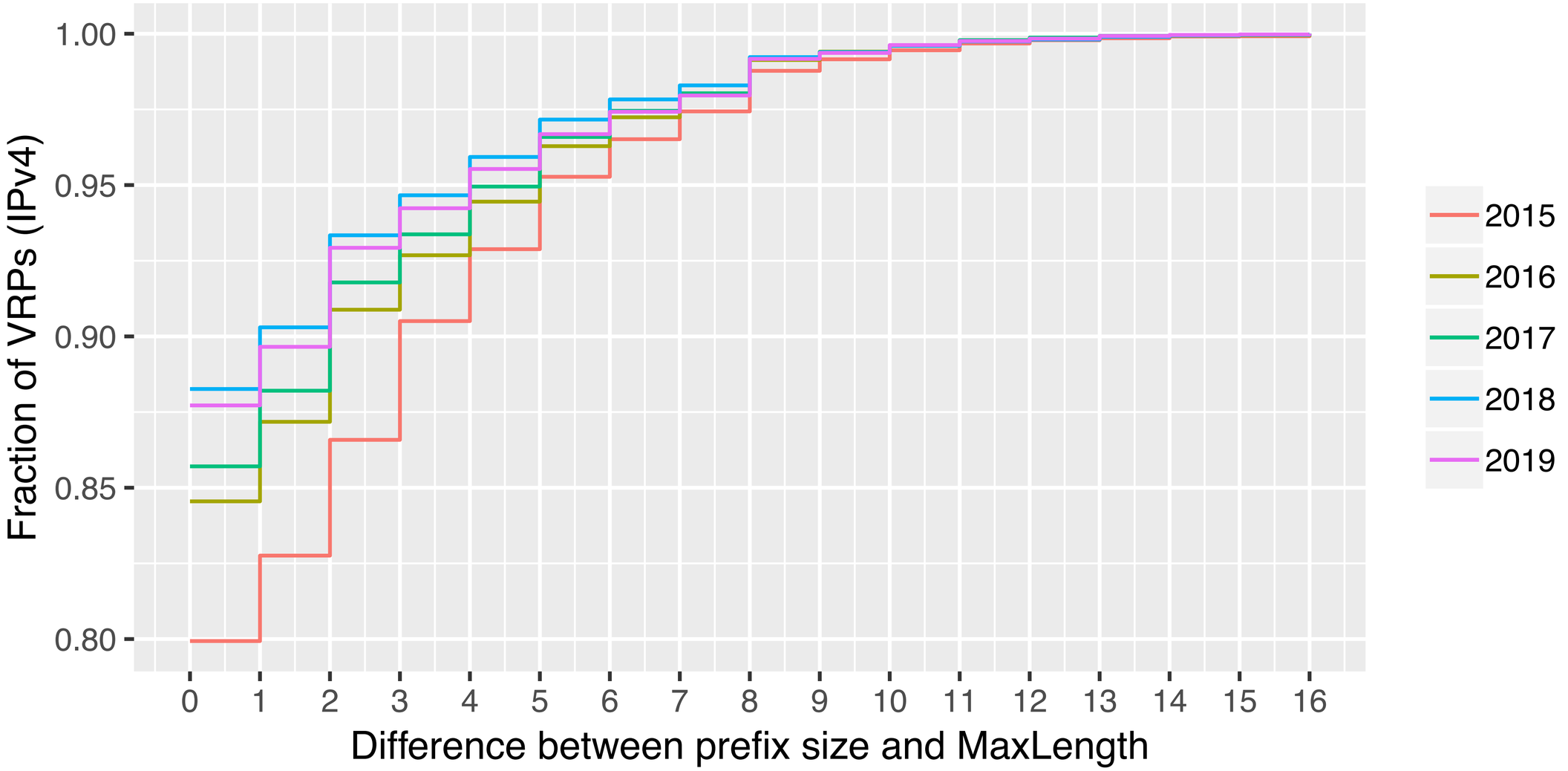
Prefix size distribution RIRs (IPv4)



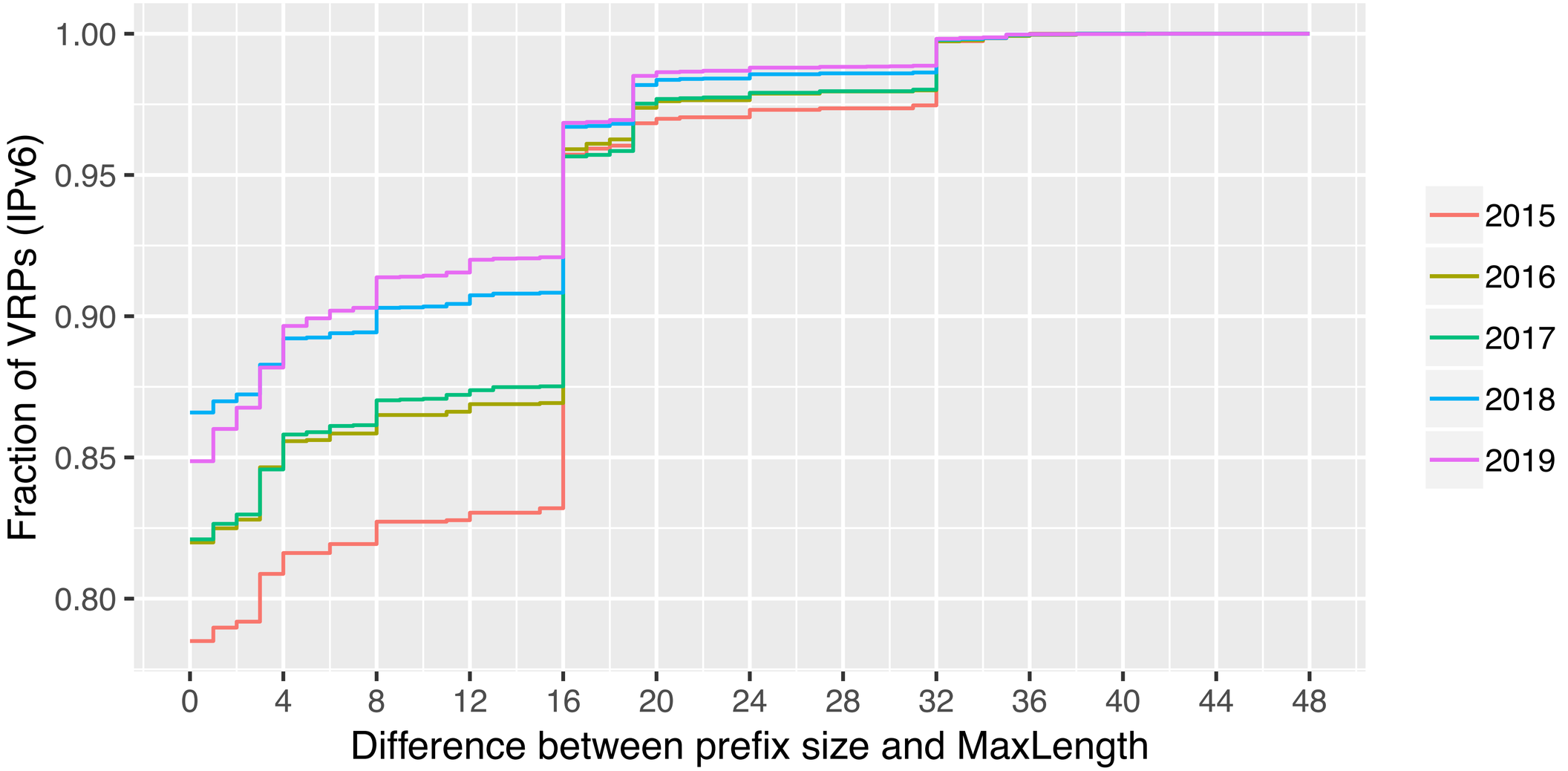
Prefix size distribution RIRs (IPv6)



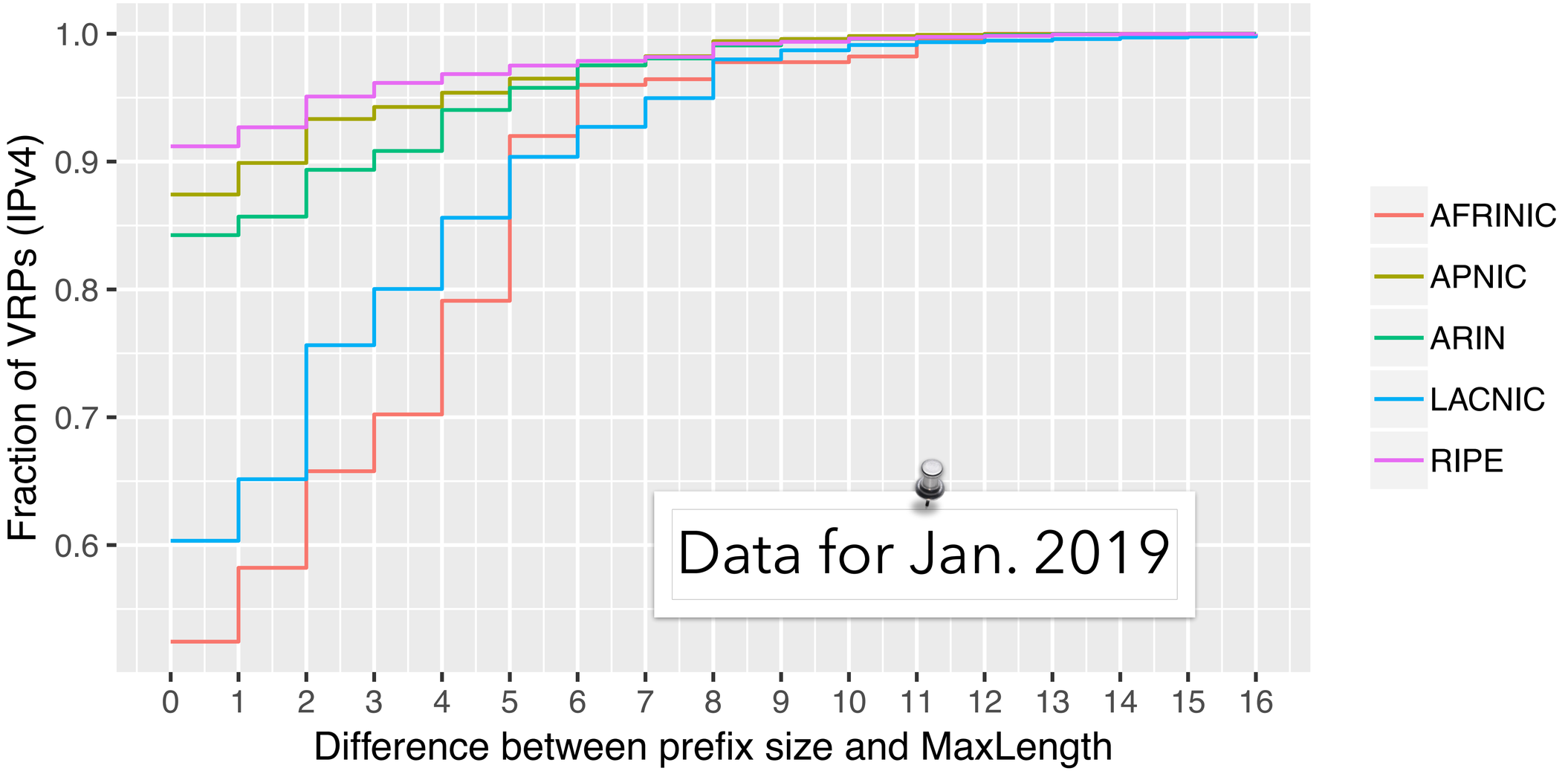
Prefix vs. Max Length (IPv4)



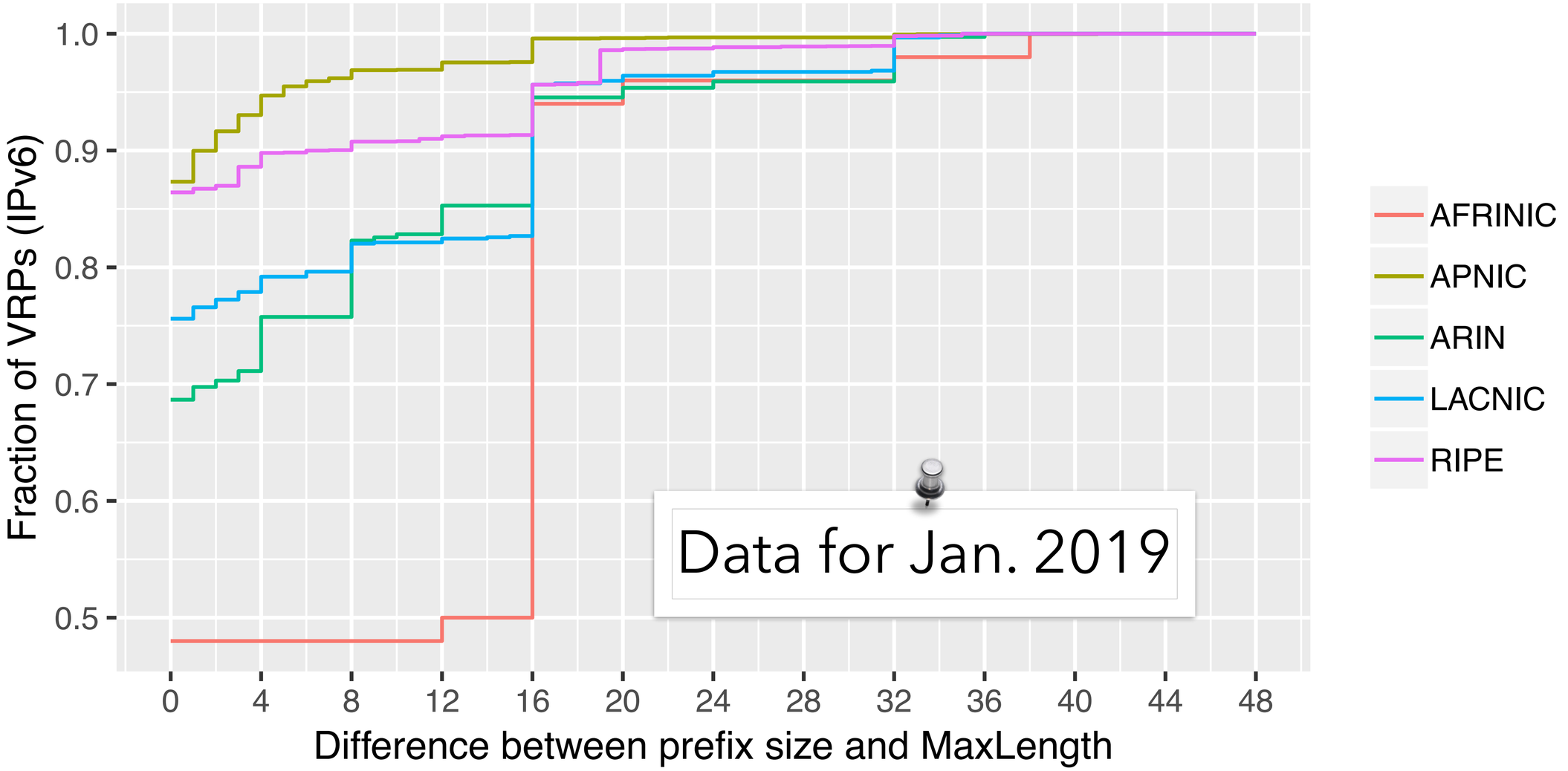
Prefix vs. Max Length (IPv6)



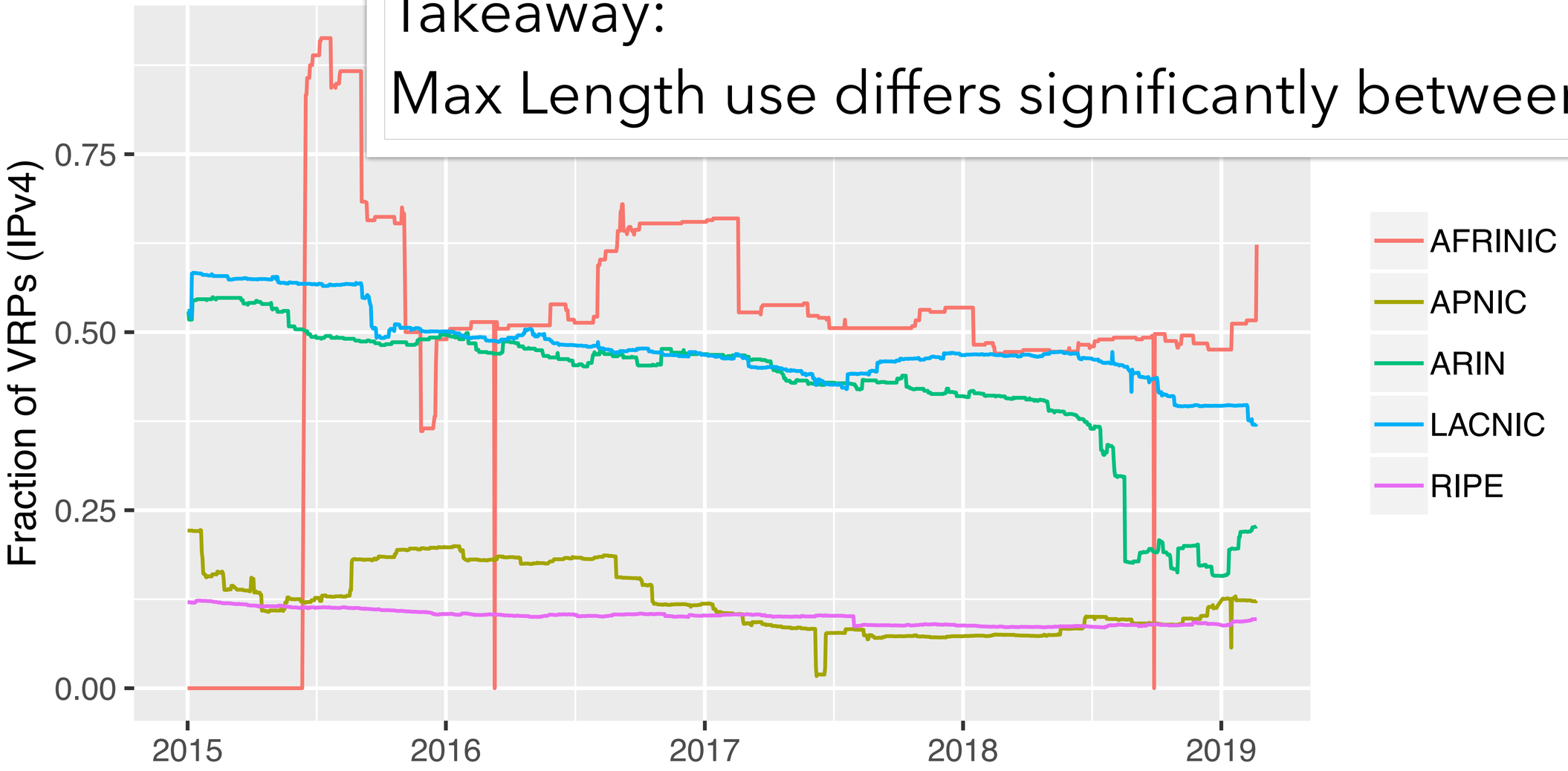
Prefix vs. Max Length RIRs (IPv4)



Prefix vs. Max Length RIRs (IPv6)



Differences between RIRs

Takeaway:

Max Length use differs significantly between RIRs