ORACLE

Excessive BGP AS Path Prepending is a Self-Inflicted Vulnerability

Doug Madory

NANOG 79
June 2020

What is AS_PATH Prepending?

- A technique used to de-prioritize a route by artificially increasing AS_PATH length.
- “Prepending” is repeating an ASN in AS_PATH – typically to a subset of adjacent ASes.

… 3356 4192 4192 7160 208.72.91.0/24

- Assuming all other criterion are equal, BGP route selection prefers the shorter AS path length (i.e. non-prepended route).

But prepending can also be problematic

Rarely the direct cause of problems, with one notable exception:

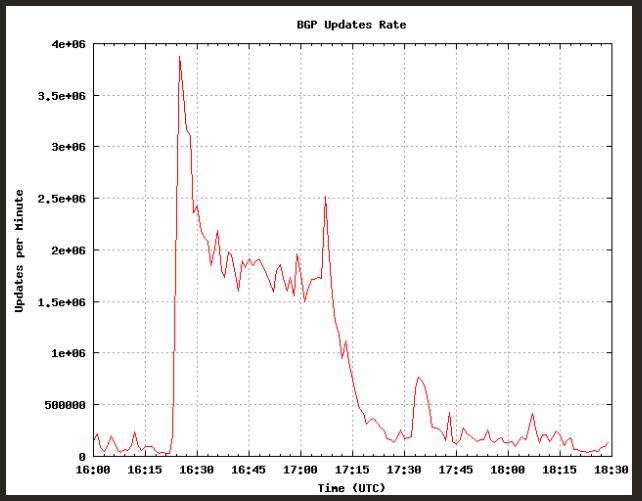
- Feb 2009: Internet-wide outages caused by a single errant routing announcement. In this incident, AS47868 announced its one prefix with an extremely long AS path. [1,2]

- Big difference in MikroTik vs Cisco config
  - Admin entered ASN instead of prepend count
  - *47868 modulo 256 = 252 prepends*

- As AS path lengths exceeded 255, Cisco routers crashed

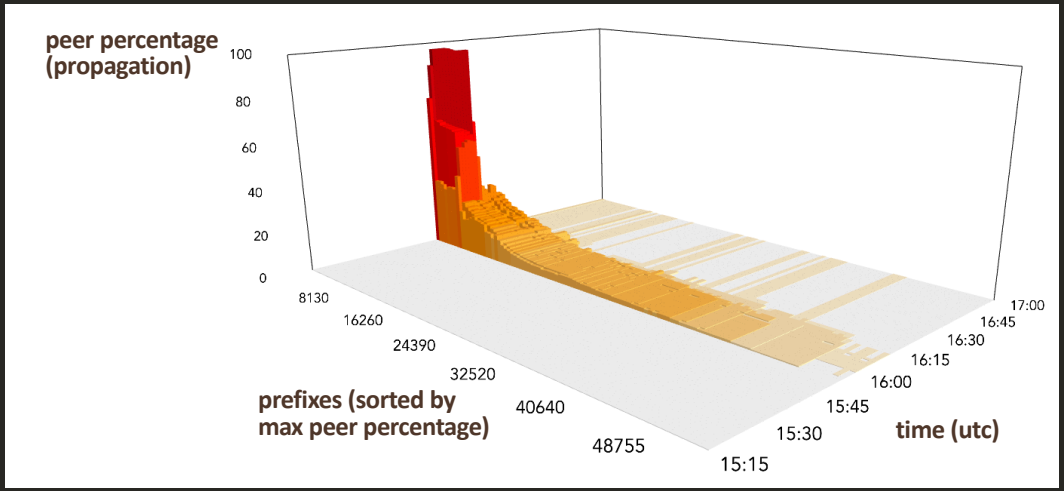
  https://dyn.com/blog/the-flap-heard-around-the-world/

  https://dyn.com/blog/longer-is-not-better/



China **did not** hijack 15% of all internet traffic

- Most impact was constrained to Chinese routes.
- However, two of the top five most-propagated leaked routes were US routes!



China **did not** hijack 15% of all internet traffic

- Why were two of the most-propagated leaked routes from the US?

  12.5.48.0/21 and 12.4.196.0/22 were announced to the internet along following excessively prepended AS path:

  … 3257 7795 12163 12163 12163 12163 12163 12163

Prefix	Country	Origin	Max Peer Percentage
218.30.222.0/24	CN	4134	95.58
59.42.0.0/16	CN	4134	87.91
12.4.196.0/22	US	12163	87.61
12.5.48.0/21	US	12163	87.61
59.52.0.0/14	CN	4134	87.61

- We termed this:

  ~~hijack me please~~
  ~~I hate myself~~
  prepended-to-all

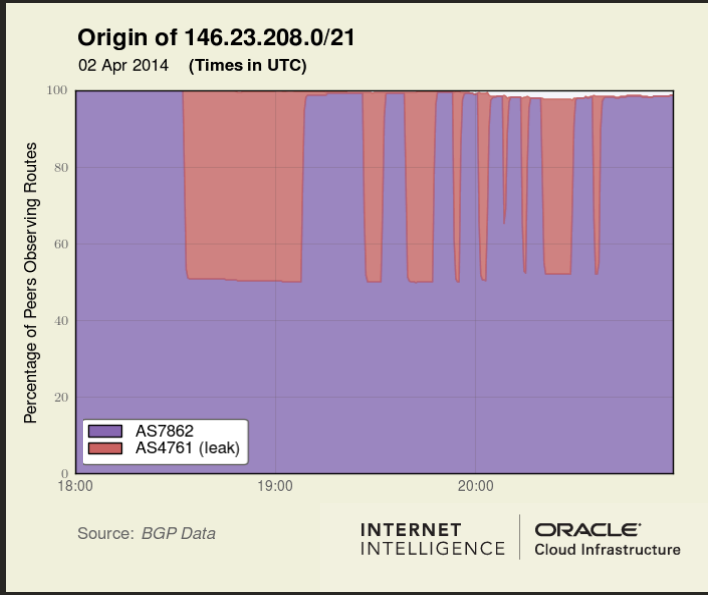
Impacts of Excessive Prepending During Leaks

- Much of the worst propagation of leaked routes during big leak events were due to routes being **prepended-to-all**.

- AS4671 leak of April 2014 (>320,000 prefixes)

  … 2856 7862 7862 7862 7862 7862 146.23.208.0/21

  ^ Prepended-to-all



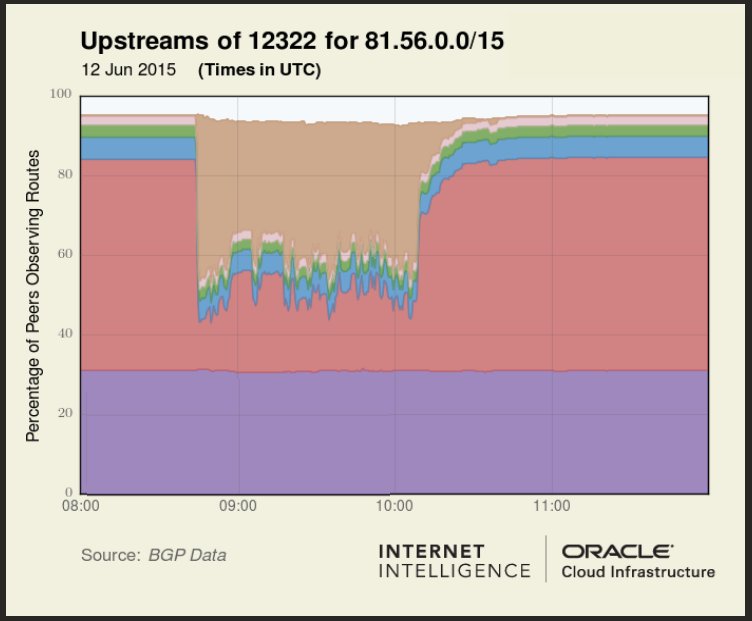
https://dyn.com/blog/indonesia-hijacks-world/

Impacts of Excessive Prepending During Leaks

- Much of the worst propagation of leaked routes during big leak events were due to routes being **prepended-to-all**.
- AS4788 leak of June 2015 (>260,000 prefixes)

  … 174 12322 12322 12322 12322 82.224.0.0/12

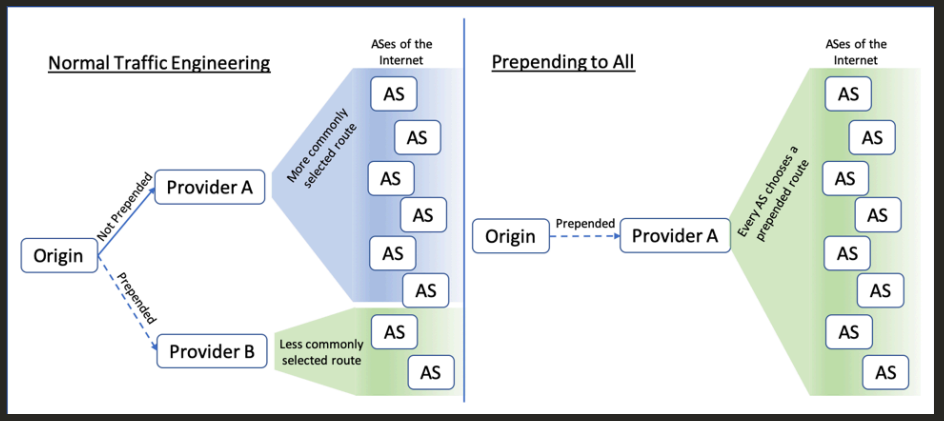
  ^ Prepended-to-all



https://dyn.com/blog/global-collateral-damage-of-tmnet-leak/

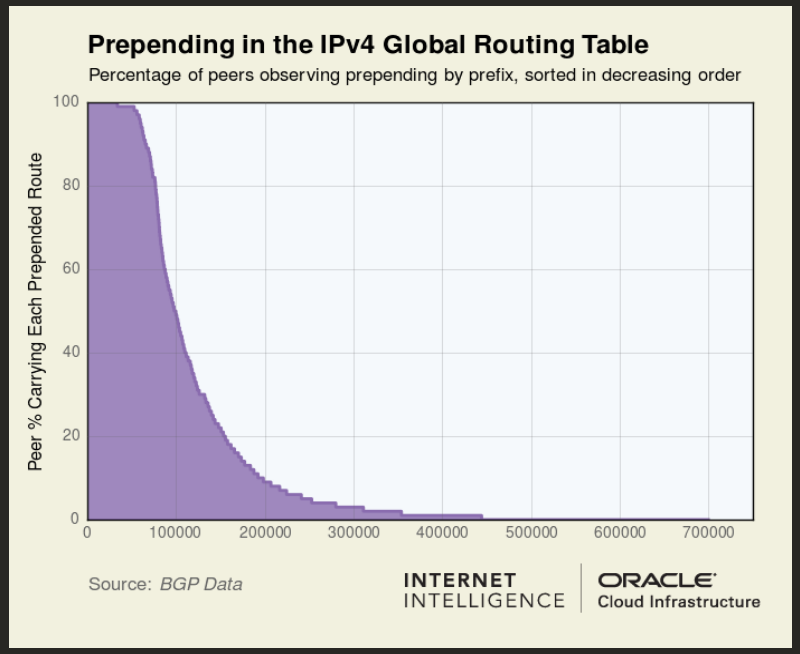
Prepending to Everyone!

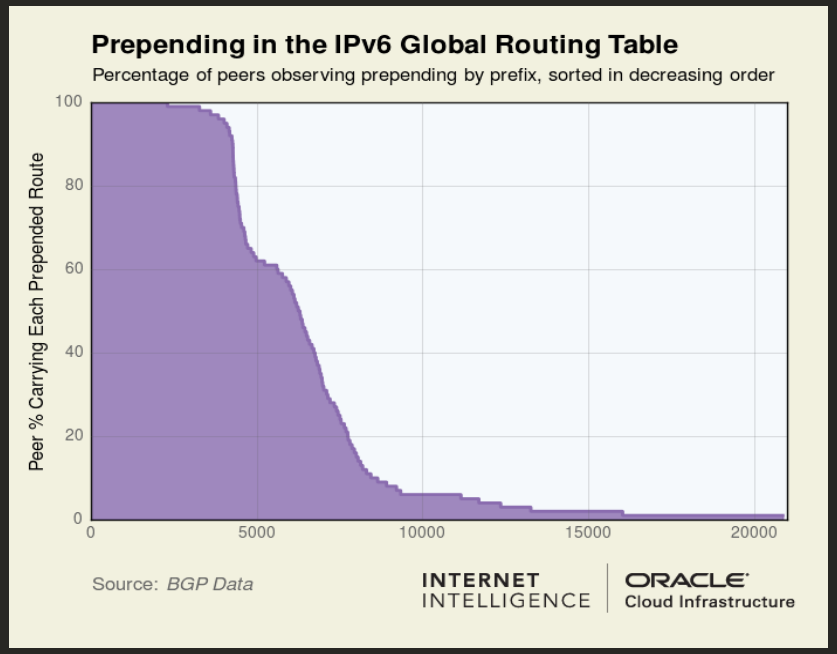
- Prepended-to-all prefixes are those seen as prepended by all (or nearly all) of the ASes of the internet.
- In this configuration, prepending is no longer shaping route propagation.
- It is simply incentivizing ASes to choose *another origin* if one were to suddenly appear whether by mistake or otherwise.



- How many prefixes are **prepended-to-all**? …a lot!

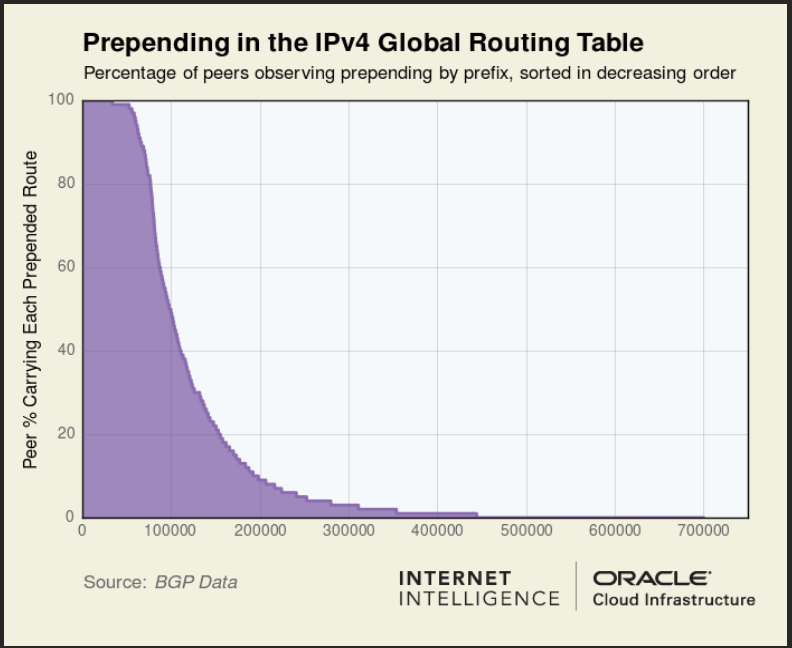
Prepending in the Global Routing Tables





Prepending in the IPv4 Global Routing Table

- Prefixes prepended to 95%+ of ASes: >60k
  - 8% of IPv4 Global Routing Table (1/12)
  - Includes entities of every stripe: govts, banks, internet infrastructure, etc.
- Prefixes prepended to 50%+ of ASes: >100k
  - 13.3% of IPv4 Global Routing Table.



Prepending in the IPv4 Global Routing Table

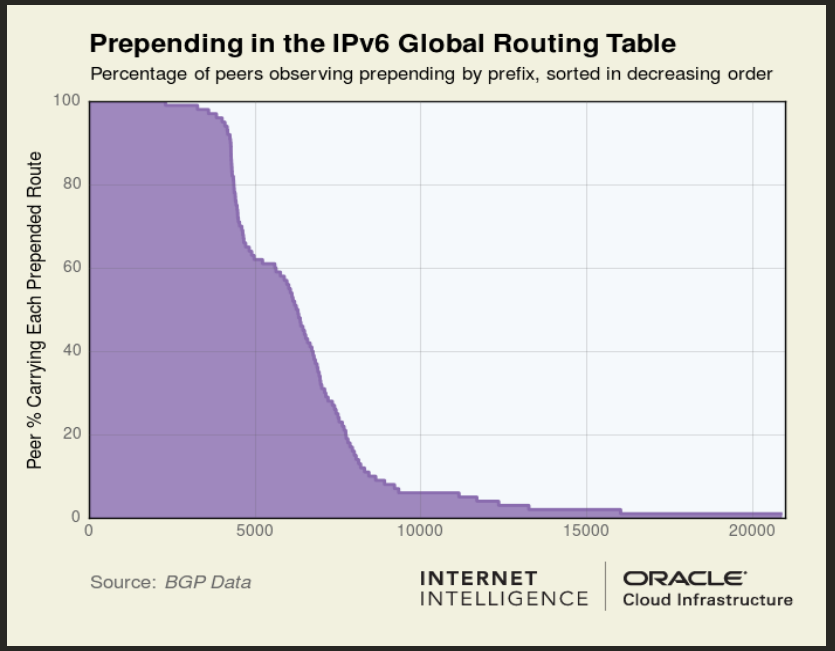
- Prefixes prepended to 95%+ of ASes: >60k
  - 8% of IPv4 Global Routing Table (1/12)
  - Includes entities of every stripe: govts, banks, internet infrastructure, etc.
- Prefixes prepended to 50%+ of ASes: >100k
  - 13.3% of IPv4 Global Routing Table.

Top Ten Sources of IPv4 Prepends

ASN	prefix count	average pp. length	total prepends	example prefix
7545	5756	3.880907	22338	203.206.24.0/22
22394	958	5.020877	4810	174.213.144.0/20
14080	1498	2.992657	4483	201.221.168.0/22
35913	731	6.016416	4398	45.83.140.0/24
6713	1047	3.137536	3285	160.160.0.0/16
20773	788	4	3152	95.142.155.0/24
9121	2742	1.025529	2812	195.175.222.0/23
10201	379	6.868074	2603	58.68.99.0/24
18403	893	2.667413	2382	59.153.255.0/24
20940	2107	1	2107	96.7.40.0/24

Prepending in the IPv6 Global Routing Table

- Prefixes prepended to 95%+ ASes: >3k
  - 5.6% of IPv6 Global Routing Table
- Prefixes prepended to 50%+ ASes: >6k
  - 8.6% of IPv6 Global Routing Table



Prepending in the IPv6 Global Routing Table

- Prefixes prepended to 95%+ ASes: >3k
  - 5.6% of IPv6 Global Routing Table
- Prefixes prepended to 50%+ ASes: >6k
  - 8.6% of IPv6 Global Routing Table

Top Ten Sources of IPv6 Prepends

ASN	prefix count	average pp. length	total prepends	example prefix
22394	671	5.1	3449	2600:1014:d150::/44
12222	207	2.8	575	2001:4878:c037::/48
17072	122	4.0	482	2806:2f0:5060::/48
7545	301	1.0	301	2a02:26f0:700::/48
20940	296	1.0	296	2a02:26f0:fd::/48
18004	24	12.0	288	2407:a600:a800::/38
133798	24	12.0	288	2402:5680:a800::/38
27738	64	3.5	224	2800:440:8041::/48
45609	148	1.4	204	2401:4900:3b7f::/48
38266	65	2.6	168	2402:3a80:c053::/48

Prepending is frequently employed in an excessive manner such that it renders routes vulnerable to disruption or misdirection – accidental or otherwise

What’s the Risk?

On a recent day, 174.213.160.0/20 was “prepended-to-all” like so:

… 701 22394 6167 22394 22394 22394 22394 22394 22394 22394 22394
22394 22394 22394 22394 22394 22394 22394 22394 22394 22394 22394 22394
22394 22394 22394 22394 22394 22394 22394 22394 22394 22394 22394 22394
22394 22394 22394 22394

An attacker might announce the same prefix with a fabricated AS path like the following:

… **ASXXX** 701 22394 6167 22394

Would redirect a portion of traffic to this prefix via ASXXX

What's the Risk?

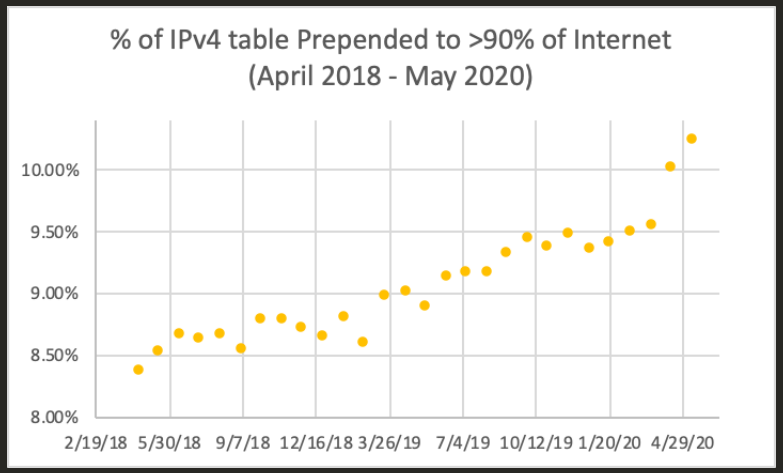
- The length of prepending gives the attacker room to craft an AS path that would appear plausible, comply with origin validation, and not be detected by off-the-shelf route monitoring.

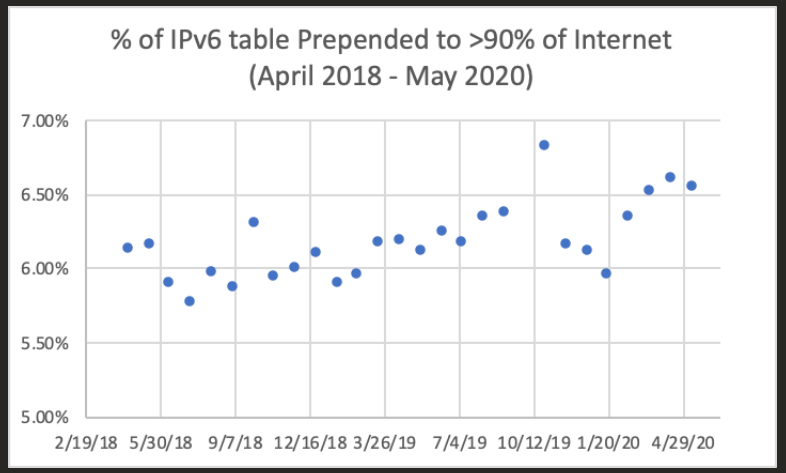
… 701 22394 6167 22394

… ASXXX 701 22394 6167 22394

Is Prepending-To-All a growing problem?

What happens when we run these stats over time? Is there a trend?





Yes! % of IPv4 table that is prepended-to-all is growing at 0.5%/year

- IPv6 table is growing slower: 0.2%/year

An inadvertent origin leak could also disrupt traffic to these routes. Accidents happen, so why deliberately put your routes at risk?

Why does prepending-to-all happen?

We wanted to know, so we asked some folks doing this. Is it intentional?

... 3356 19256 7955 30321 30321 30321 162.212.148.0/23

We asked Burning Man NetOps about their excessive prepending.

They immediately fixed it. 👍

Why does prepending-to-all happen?

We wanted to know, so we asked some folks doing this.

- CloudFlare, Google also removed the excessive prepending when we reported it to them. 👍
- Most either didn't respond or claimed it was an "operational issue" and it remains.

Why does prepending-to-all happen?

Theory 1: Poor Housekeeping - The AS forgets to remove the prepending for one of its transit providers when it is no longer needed.

Theory 2: Return Path Influence – AS attempting to de-prioritize traffic from transit providers over settlement-free peers.

Why does this happen?

Theory 3: Mistakes Abound - There are simply a lot of errors in BGP routing. Consider the prepended AS path of 181.191.170.0/24 below:

… 52981 267429 267429 267492 267492 267429 267429 267492 267492 267429 267429 267492 267492 267429

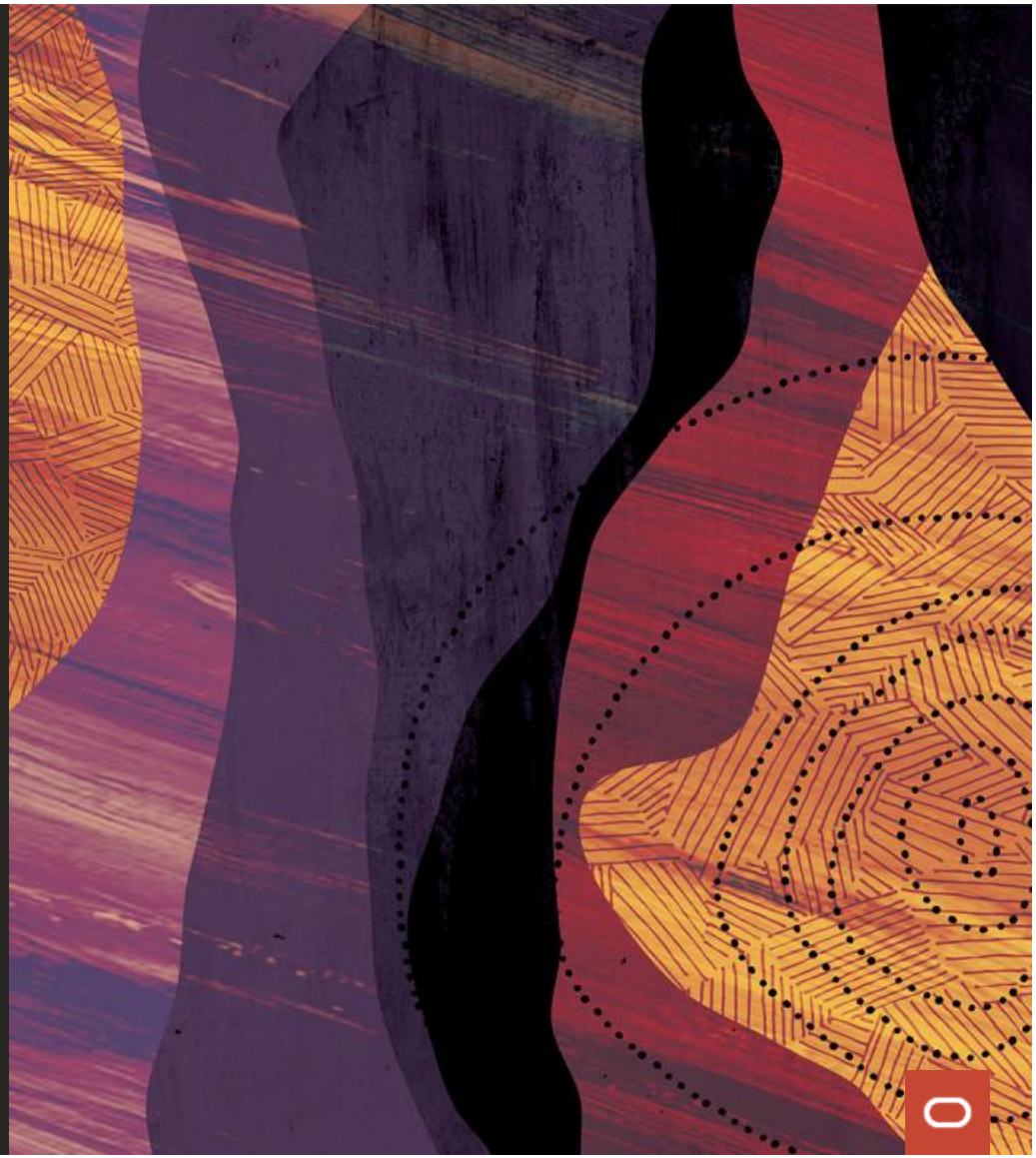
*In case your eyes didn't catch it, the prepending here involves a mix of two distinct ASNs (2674**29** and 2674**92**) with the last two digits transposed.*

Conclusions

- Long AS paths (whether due to prepending or not) incur risk of disruption
  - In the event another AS originates the same prefix with a shorter AS path
- Network operators should ensure prepending is absolutely necessary
  - *Many of your networks have excessive prepending (ask me for examples)*
- With 8% of IPv4 and 5.6% of IPv6 global routing tables presently prepended to *everyone*, this traffic engineering technique is significantly overused.

Thank you

Doug Madory
@InternetIntel
Oracle Internet Intel



Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.