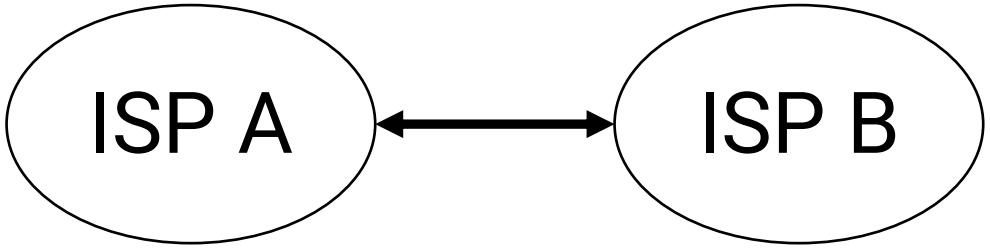
BGP hijacking

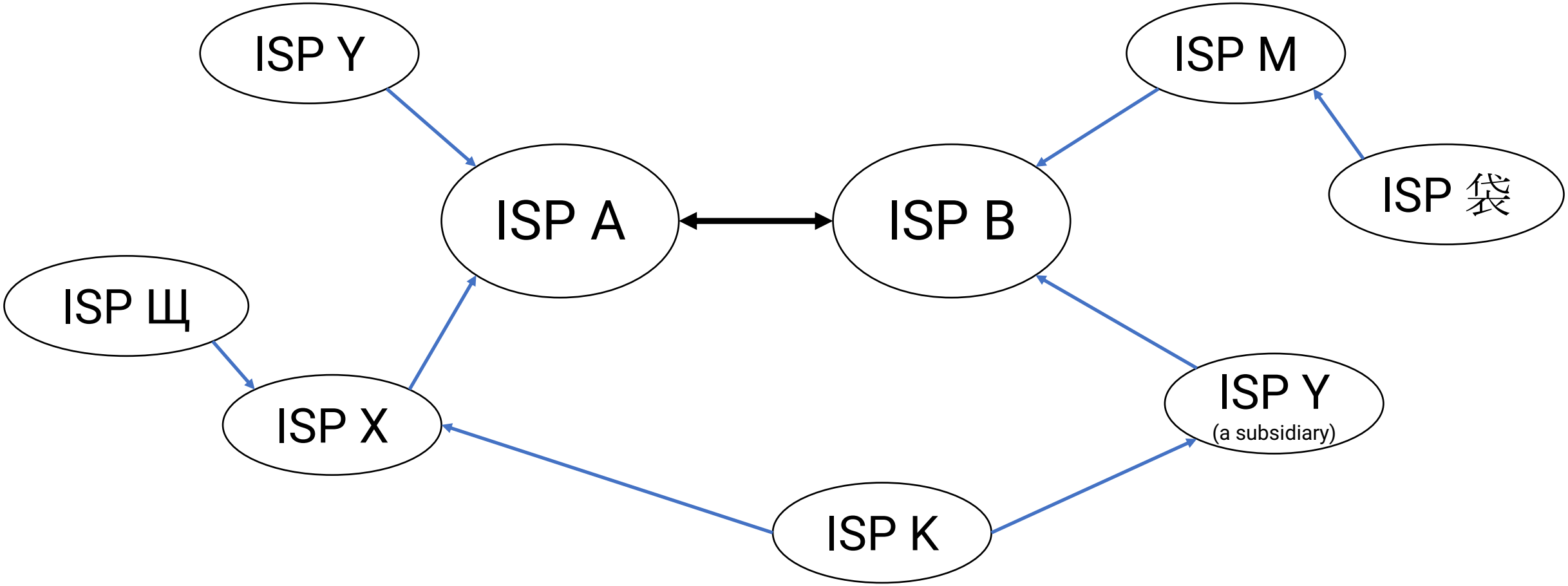
Töma Gavrichenkov <ag@qrator.net>

GPG: 2deb 97b1 0a3c 151d b67f
1ee5 00e7 94bc 4d08 9191

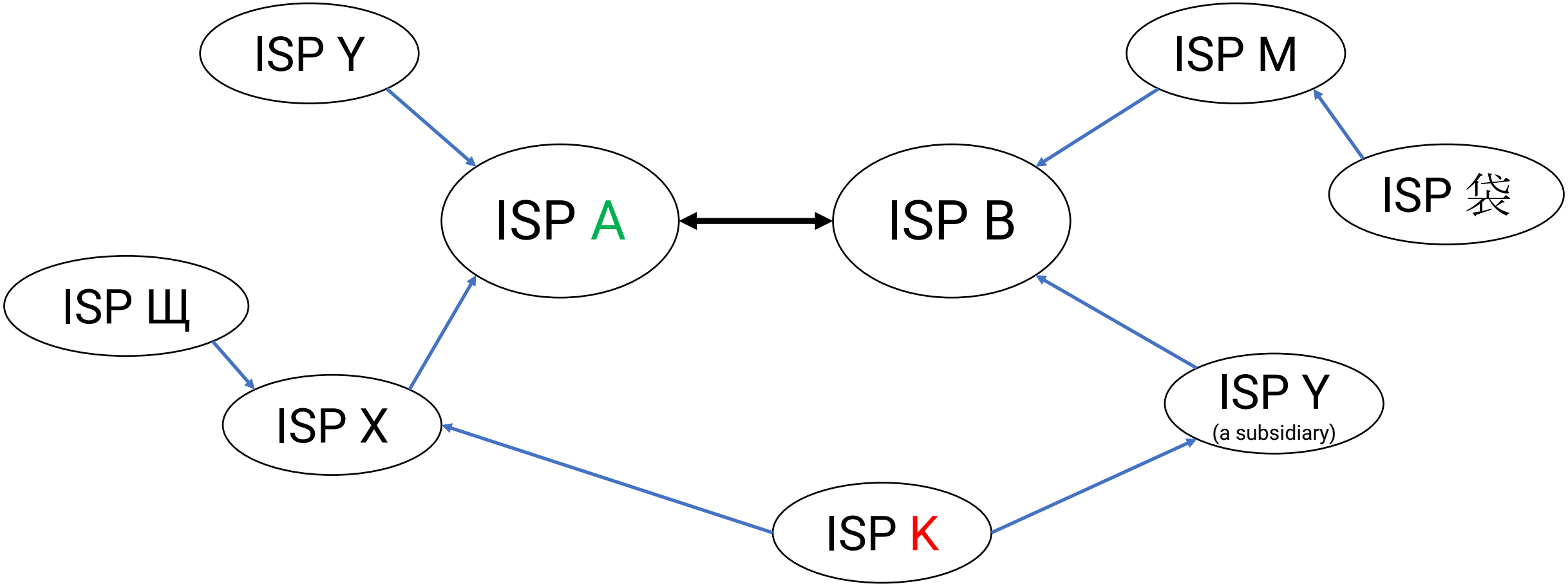
How routing works:



How routing works:



How does A know where to find K?



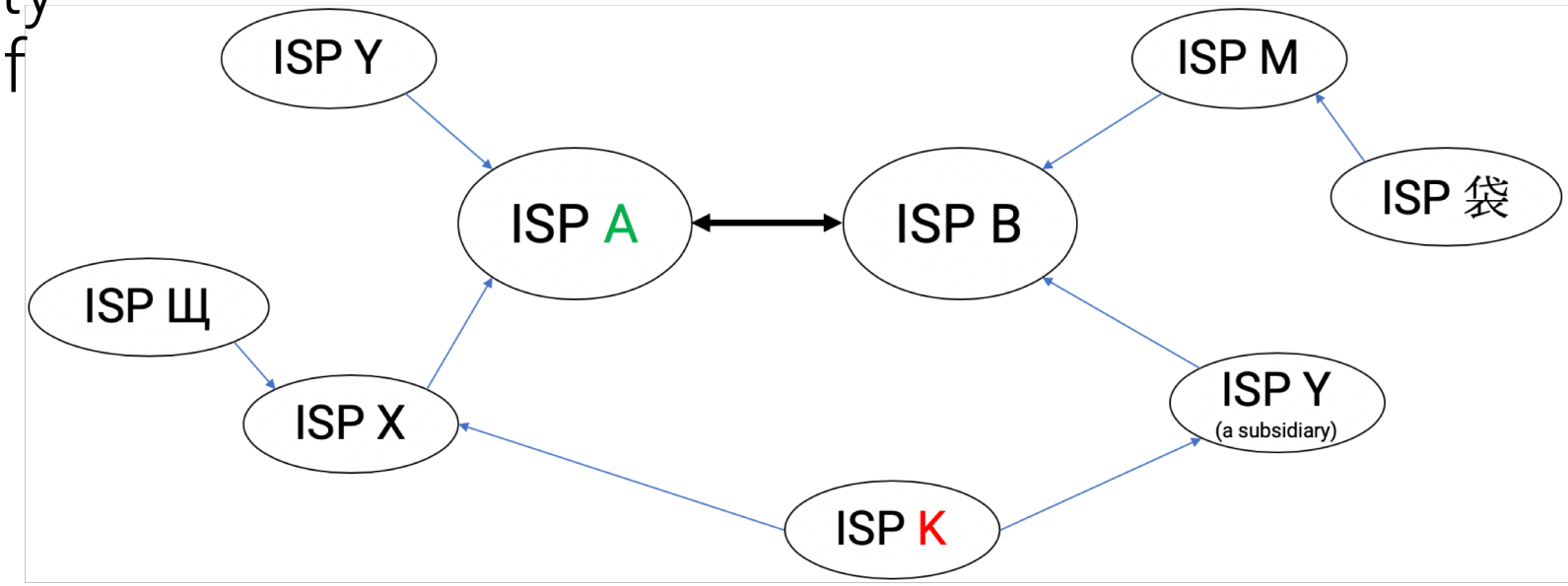
Border Gateway Protocol

- RFC 4271
- Also, 82 other RFCs and 27 I-Ds: https://datatracker.ietf.org/group/idr/documents/
- 2 more RFCs (and 8 I-Ds) here:
- https://datatracker.ietf.org/group/sidrops/documents/

- *"BGP: awarding PhDs since 1995"*

Border Gateway Protocol

- Provides interoperability between the borders of *autonomous systems* (AS) — ISPs and other companies
- “Autonomous system” is an abstraction
- Internal architecture of a network isn’t reflected in BGP

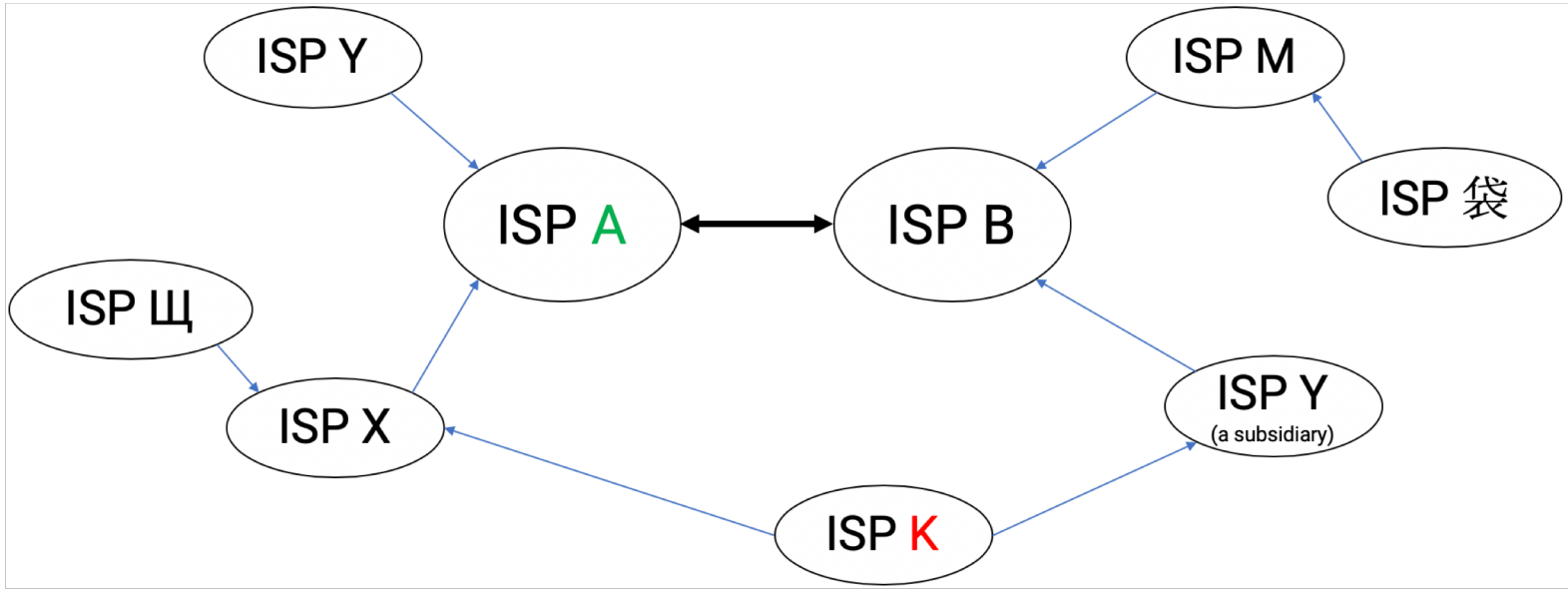


Border Gateway Protocol

- ISP K announces their networks to their two upstreams
- ISP A sees two paths:

```
1. Origin: K
   AS Path: B, Y, K
2. Origin: K
   AS Path: X, K, K
```

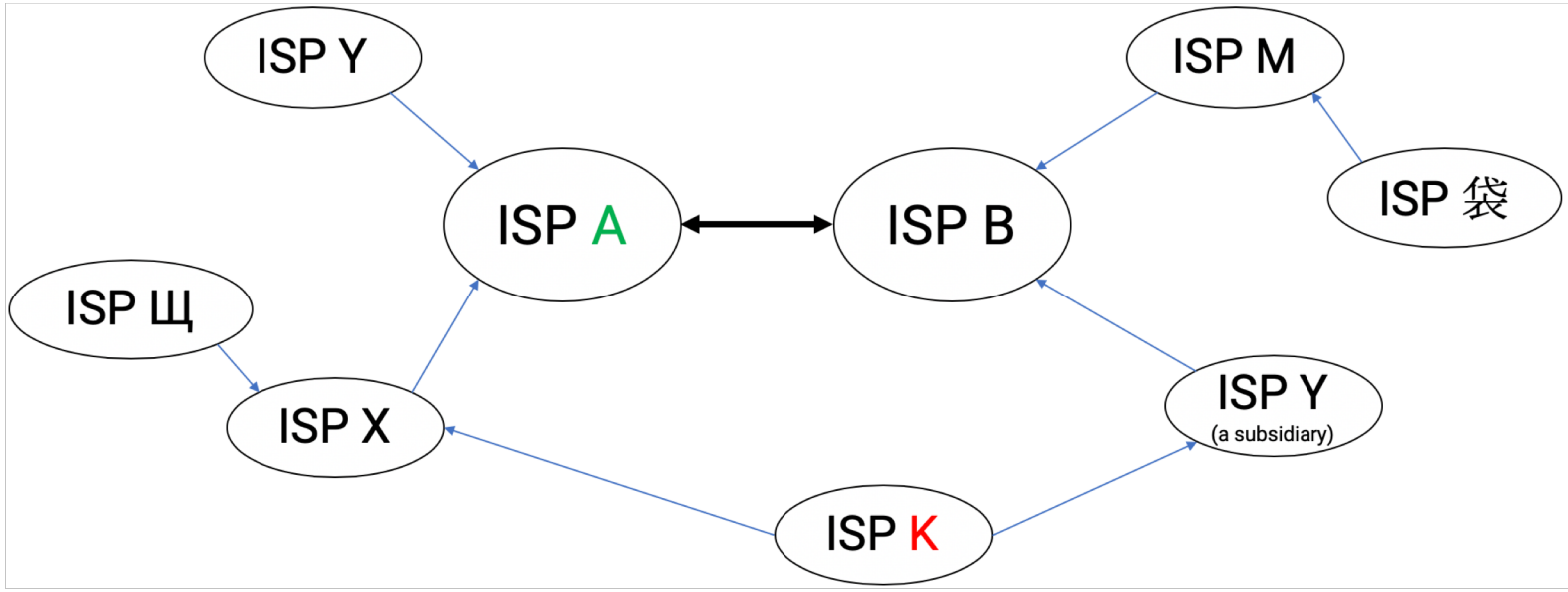
- ISP A chooses the shortest



Border Gateway Protocol

```
Origin: K
AS Path: X, K, K
```

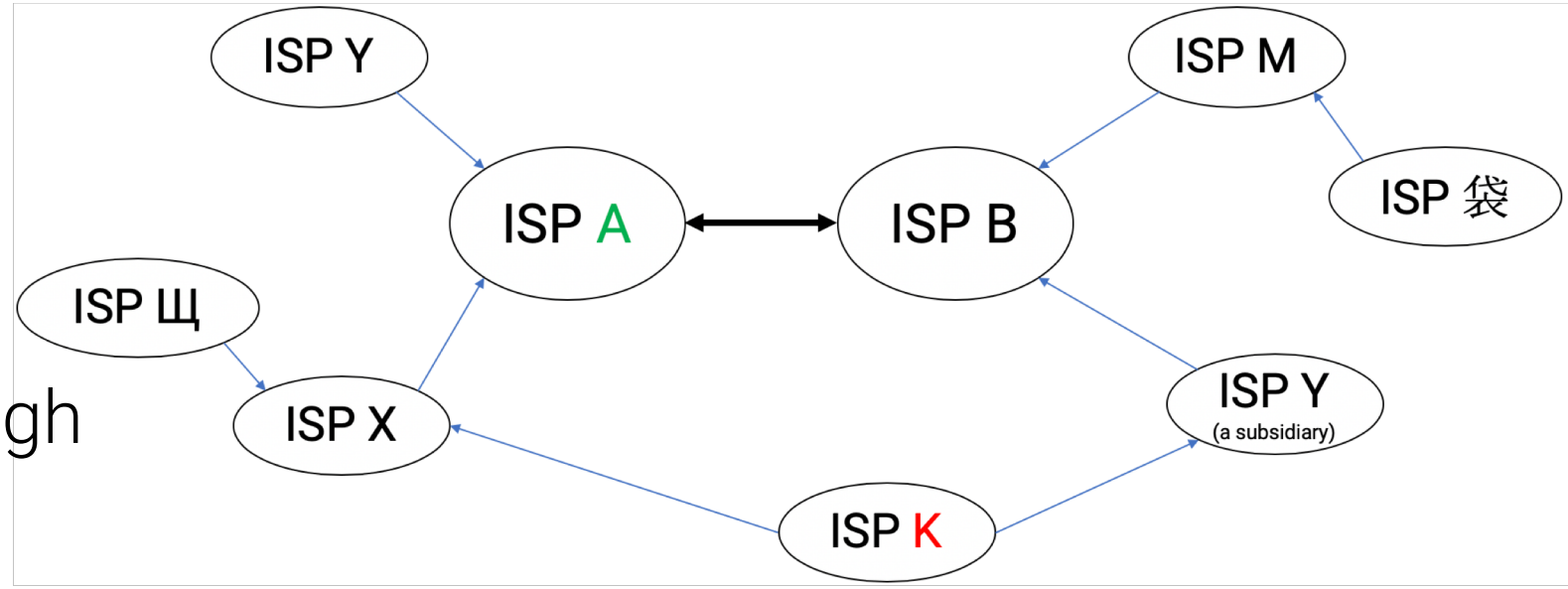
- Hey, this is weird!
- Why is “K” prepended twice?



Border Gateway Protocol

```
Origin: K
AS Path: X, K, K
```

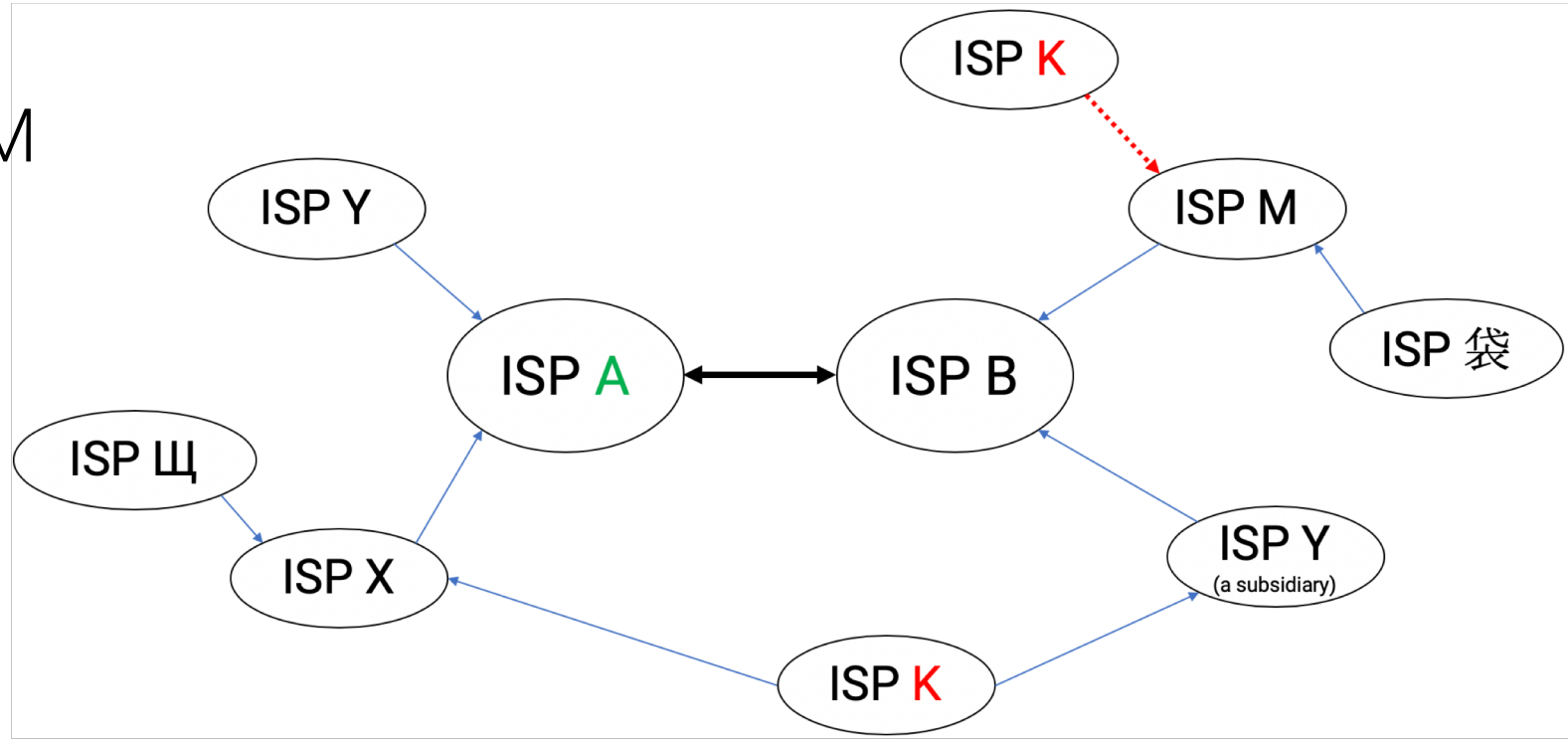
- BGP is a *money vector protocol*
- ISP K doesn't prefer to see lots of traffic through the expensive link to X



BGP hijacking

Now what if an evil ISP M starts announcing K's networks without a permission, for:

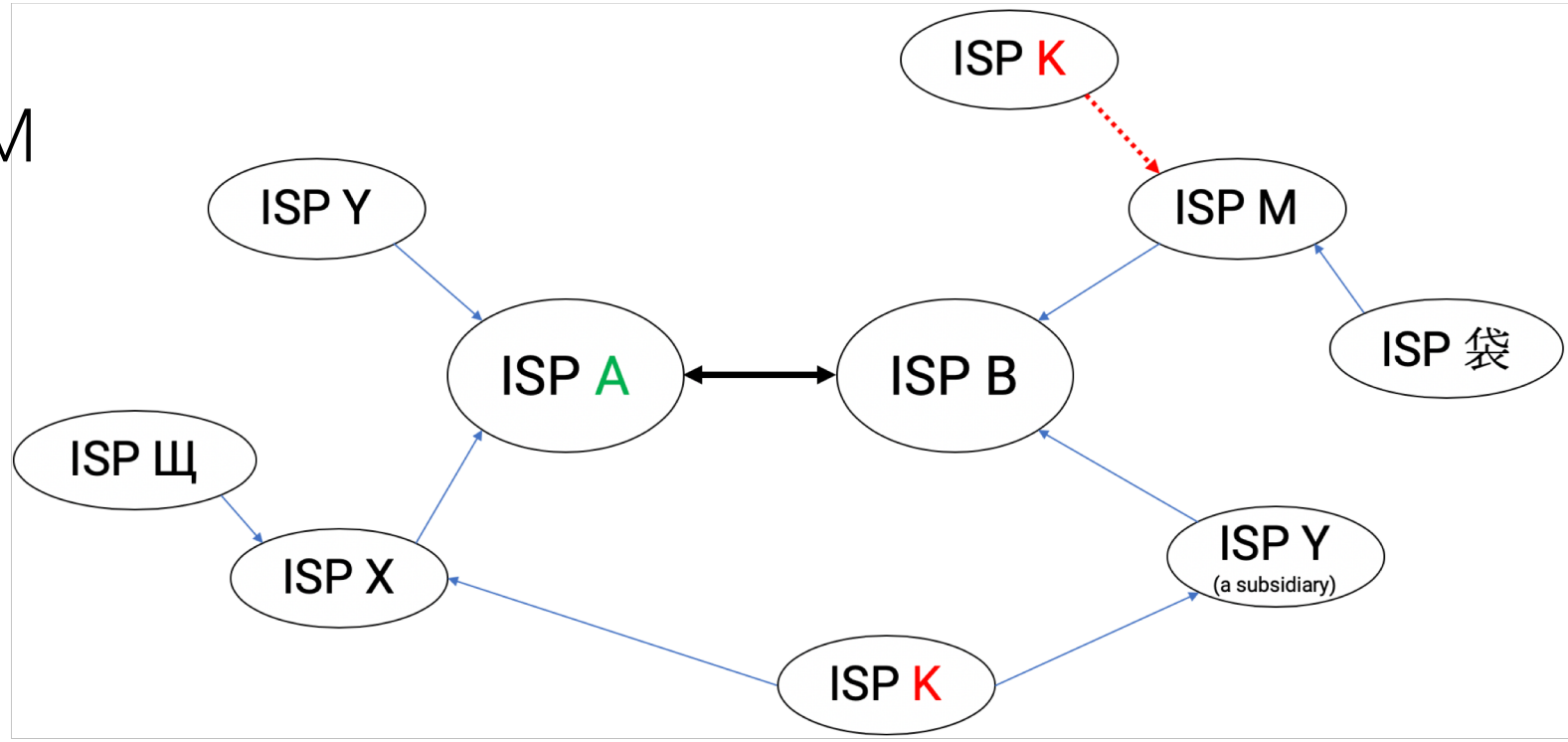
- DoS?
- wiretapping?
- impersonation?
- other evil means?



BGP hijacking

Now what if an evil ISP M starts announcing K's networks without a permission?

1. Origin: K
   AS Path: B, M, K
2. Origin: K
   AS Path: B, Y, K
3. Origin: K
   AS Path: X, K, K



BGP hijacking

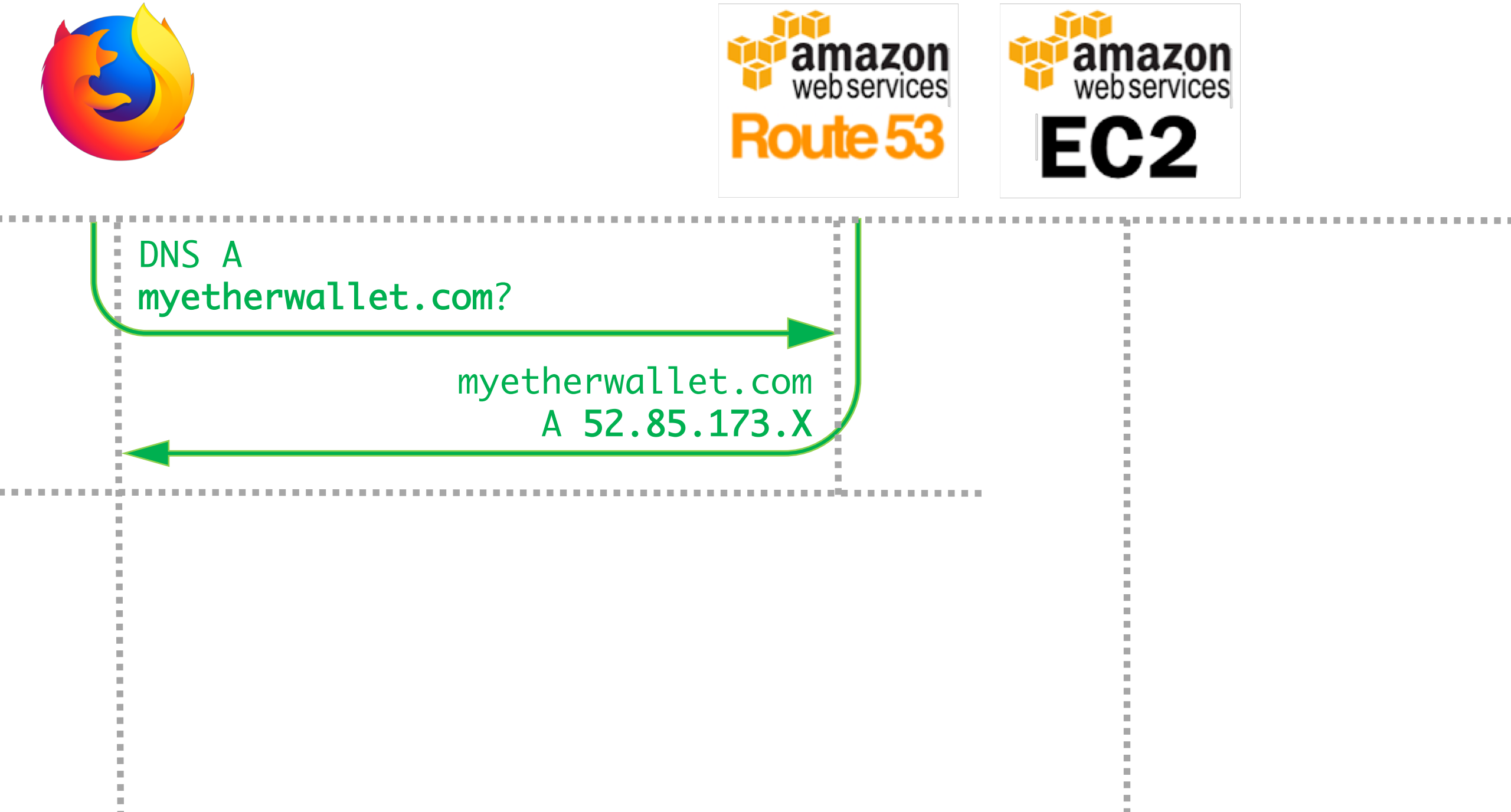
- Can also happen occasionally (in which case it's deemed a ***"route leak"***)
- Caused multiple incidents where complete Internet regions were inaccessible for hours
- Frequently causes increased latency and jitter
- Breaks the Web PKI!
  A certificate authority relies on TOFU when allowing an entity to obtain a TLS certificate for `ietf.org`

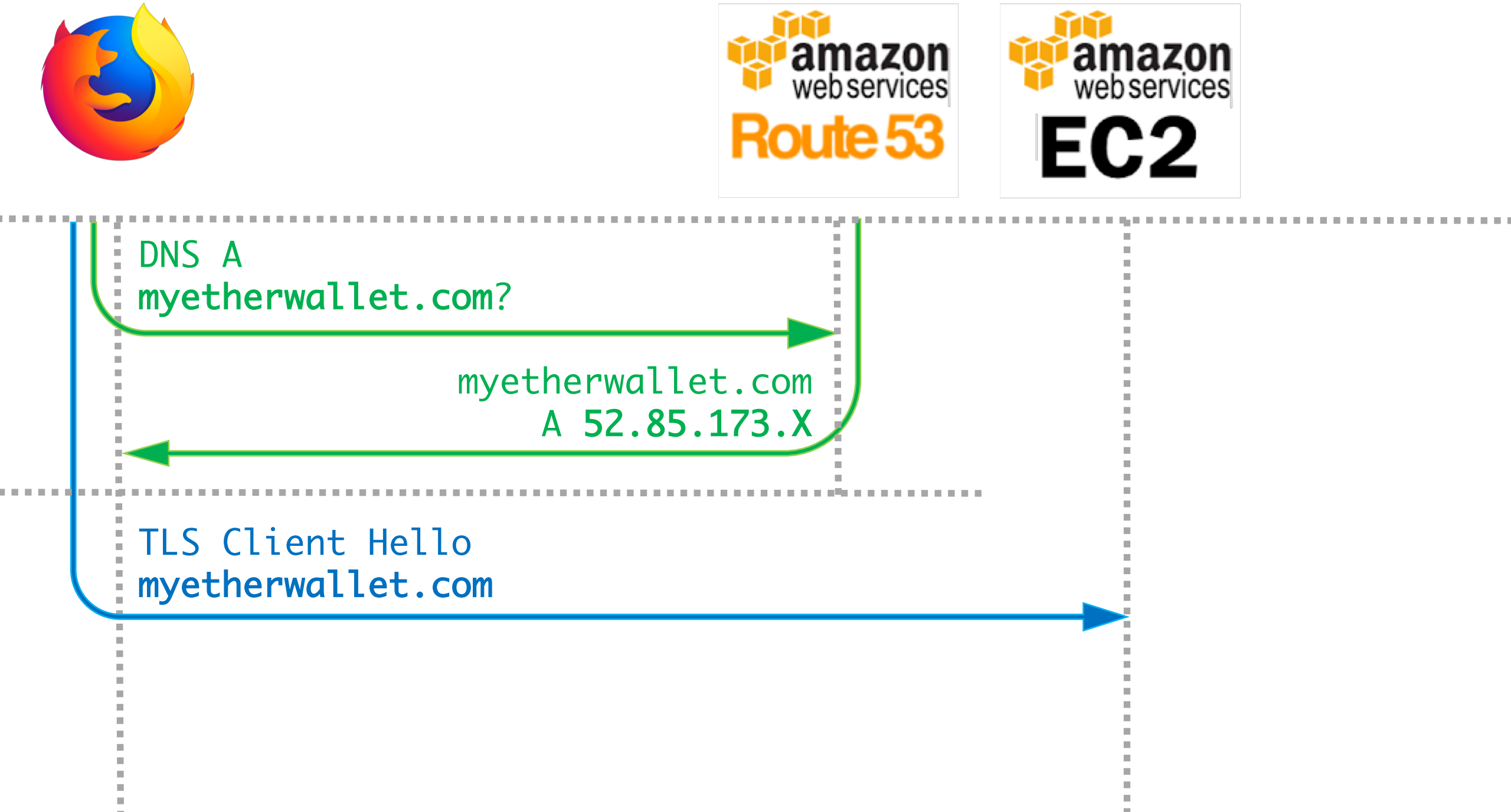
MyEtherWallet

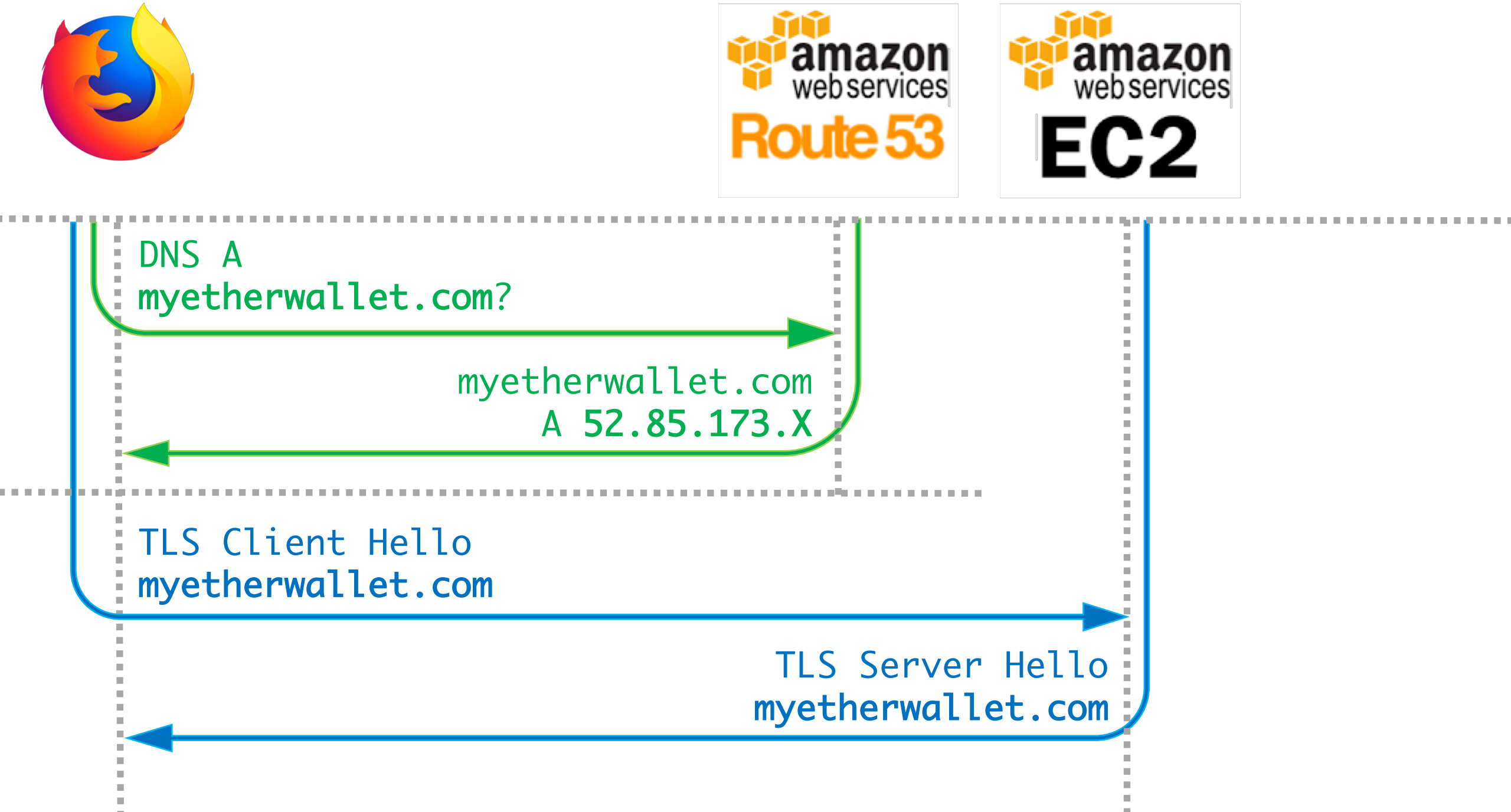
April 24, 2018: myetherwallet.com gets BGP hijacked

- Went for 2 hours unnoticed
- Was using arogue HTTPS certificate
  so users clicked through certificate errors
- https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

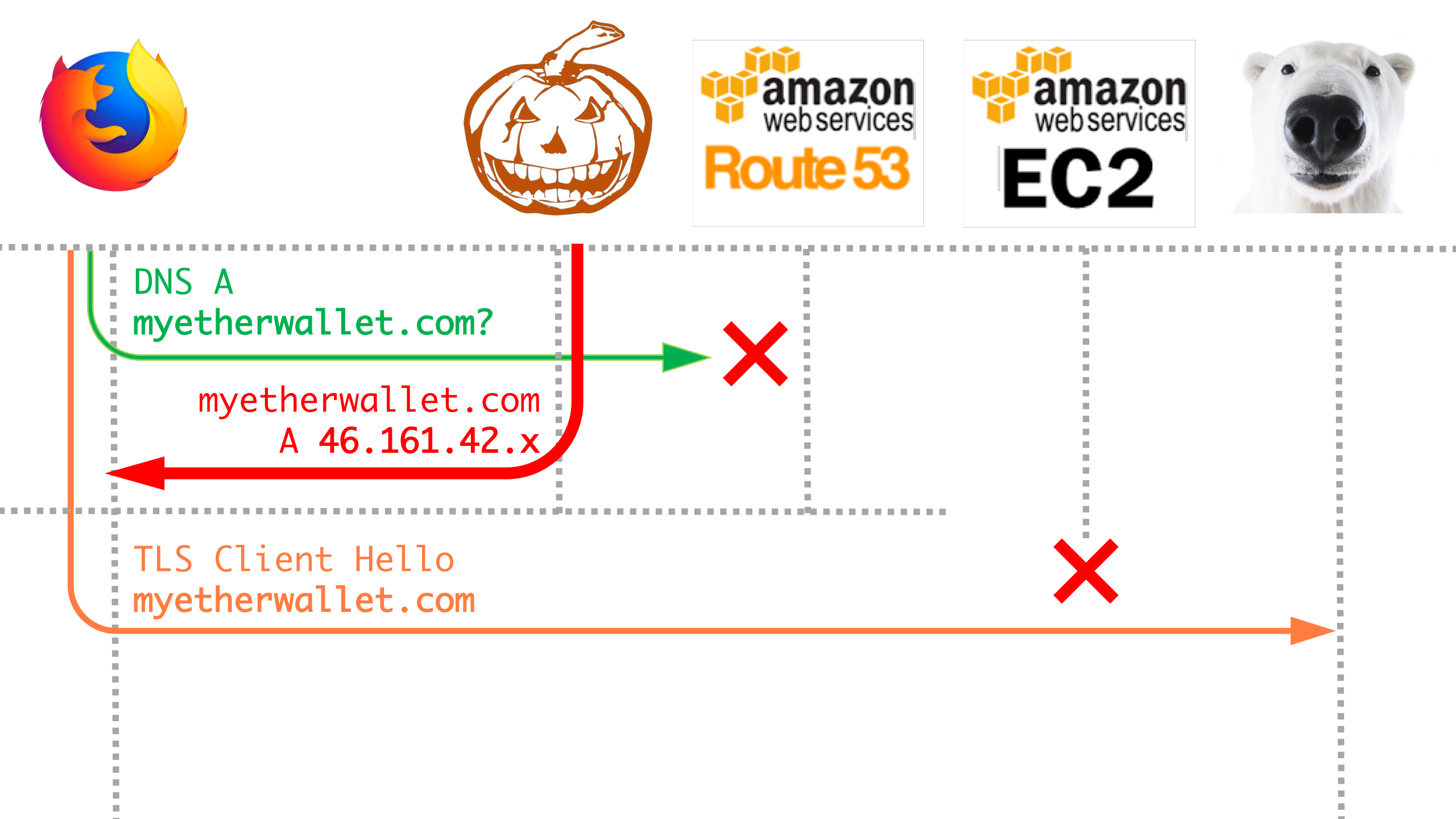
DNS A
myetherwallet.com?

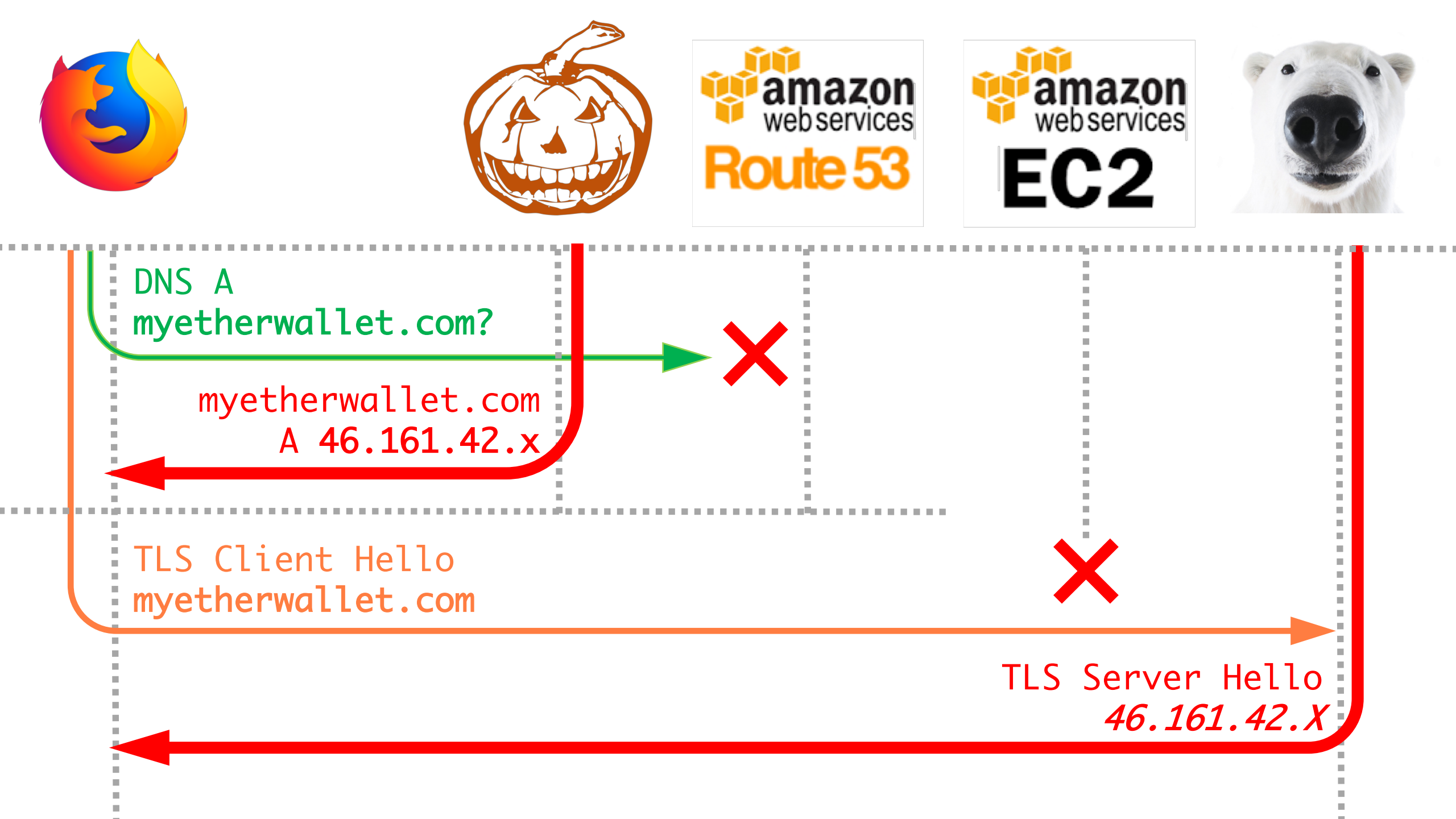

amazon web services
Route 53
amazon web services
EC2
DNS A
myetherwallet.com?
myetherwallet.com
A 52.85.173.X


amazon web services
Route 53
amazon web services
EC2
DNS A
myetherwallet.com?
myetherwallet.com
A 52.85.173.X
TLS Client Hello
myetherwallet.com


amazon web services
Route 53
amazon web services
EC2
DNS A
myetherwallet.com?
myetherwallet.com
A 52.85.173.X
TLS Client Hello
myetherwallet.com
TLS Server Hello
myetherwallet.com


amazon web services
Route 53
amazon web services
EC2
DNS A
myetherwallet.com?
myetherwallet.com
A 46.161.42.x


amazon web services
Route 53
amazon web services
EC2
DNS A
myetherwallet.com?
myetherwallet.com
A 46.161.42.x
TLS Client Hello
myetherwallet.com


amazon web services
Route 53
amazon web services
EC2
DNS A
myetherwallet.com?
myetherwallet.com
A 46.161.42.x
TLS Client Hello
myetherwallet.com
TLS Server Hello
46.161.42.X

Obtaining fraudulent TLS certificates

- http://www.blackhat.com/us-15/briefings.html#breaking-https-with-bgp-hijacking
- https://www.petsymposium.org/2017/papers/hotpets/bgp-bogus-tls.pdf
- http://www.cs.princeton.edu/~jrex/papers/bamboozle18.pdf

- What other parts of today's Web infrastructure could be at risk?

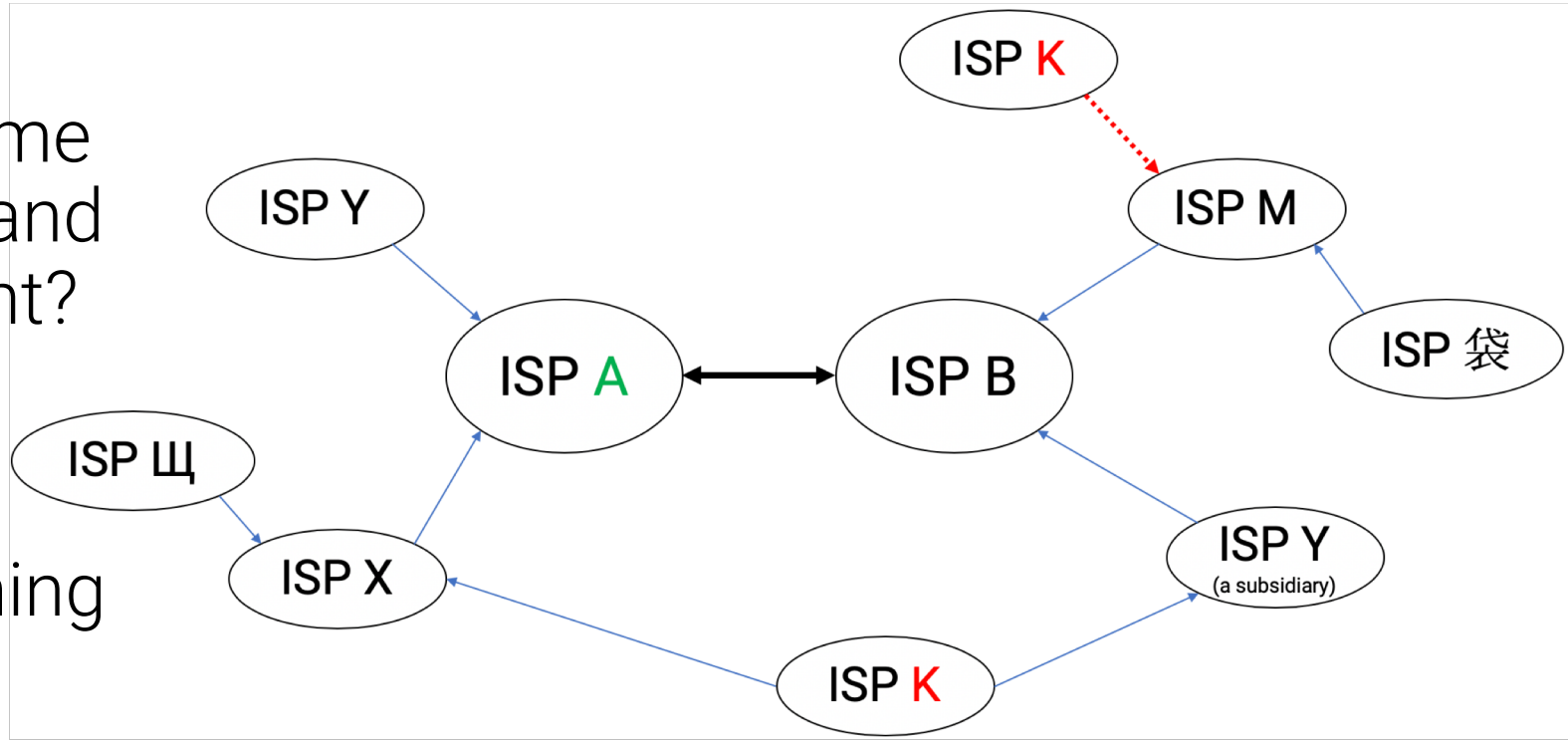
Consequences for other protocols?

E.g. QUIC spin bit:
https://datatracker.ietf.org/doc/draft-ietf-quic-spin-exp/

- Could it be used together with BGP hijacking to triangulate a location of a user behind a VPN?
- Other caveats?

BGP hijacking

- But there should be some kind of authentication and PKI to prevent that, right?
- NOPE.
- Back in 80s and 90s it wasn't seen as something necessary
- It's there now (RPKI and BGPSec), but the adoption rate is low *so far*



Routing policy

- https://www.apnic.net/get-ip/faqs/route-management/
- Regional Internet registries allow (or even encourage) to reflect one's routing policy in the RIR databases: RIPE DB etc.
- That could be next used to set up prefix filters

- Though, both route objects and prefix filtering are voluntary to implement

Changes for the BGP protocol

- DISCO: https://mailman.nanog.org/pipermail/nanog/2018-December/098458.html
- An experiment to evaluate alternatives for speeding up adoption of BGP route origin validation
- Conducted in January
- disco-experiment@googlegroups.com

Changes for the BGP protocol

DISCO: https://mailman.nanog.org/pipermail/nanog/2018-December/098458.html

Testing new approaches in the wild is hard!

- Broken BGP software
- Obsolete BGP s/w
- Months or years between s/w updates

A testbed is necessary!

- At least: bird, quagga, FRR; Cisco, Juniper, Huawei, …

BGP Experiment

Ben Cooper ben at packet.gg
Wed Jan 23 17:00:27 UTC 2019

- Previous message (by thread): BGP Experiment
- Next message (by thread): BGP Experiment
- **Messages sorted by:** [date] [thread] [subject] [author]

Can you stop this?

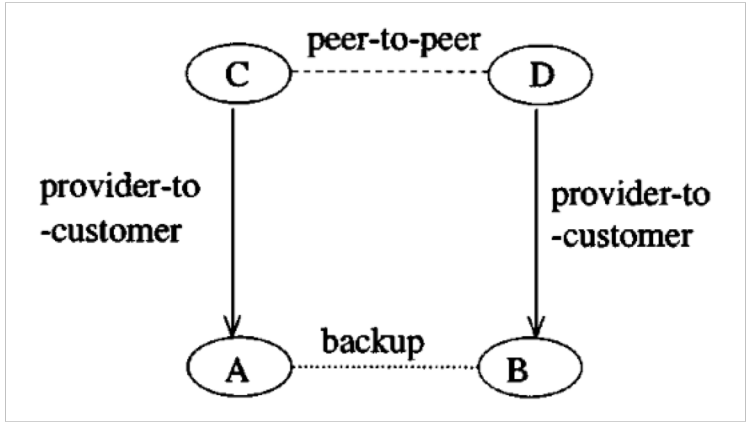
You caused again a massive prefix spike/flap, and as the internet is not centered around NA (shock horror!) a number of operators in Asia and Australia go effected by your “expirment” and had no idea what was happening or why.

Get a sandbox like every other researcher, as of now we have black holed and filtered your whole ASN, and have reccomended others do the same.

Gao-Rexford model

- BGP is a *money-vector protocol!*
- 3 types of ISP relations:

1. Customer (paying)
2. Provider (being paid)
3. Peer (free traffic exchange)



If e.g. a customer announces their provider's prefixes through another customer link, that's *weird*, economically.

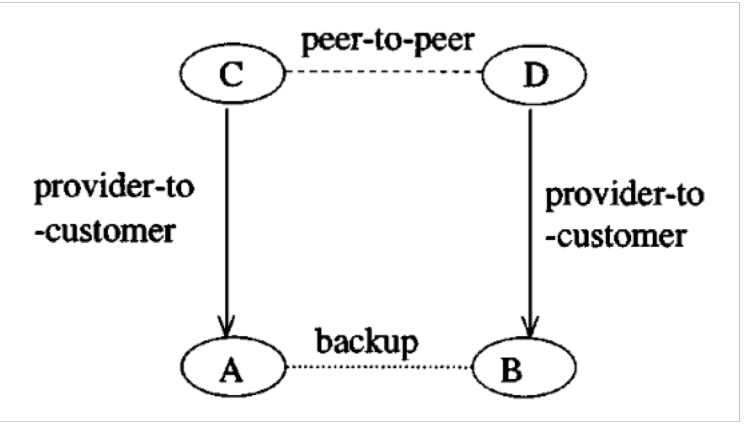
https://people.eecs.berkeley.edu/~sylvia/cs268-2019/papers/gao-rexford.pdf

ASPA

That could also be used to

- detect
- mitigate

the hijacking.



https://datatracker.ietf.org/doc/draft-ietf-idr-**bgp-open-policy**/

https://datatracker.ietf.org/doc/draft-ietf-idr-**route-leak-detection-mitigation**/

https://datatracker.ietf.org/doc/draft-sriram-idr-**route-leak-solution-discussion**/

https://datatracker.ietf.org/doc/draft-azimov-sidrops-**aspa-verification**/

https://datatracker.ietf.org/doc/draft-azimov-sidrops-**aspa-profile**/