Risks & Dangers in BGP

What can we do about it?

Job Snijders

NTT Ltd

Global IP Network (AS 2914)

job@ntt.net

Agenda

- Traffic Engineering challenges in BGP
- "*bGp OtImIsEr*" Misery Deconstructed
  - Post-leak data-plane wasteland
- Mitigating risks
  - NO_EXPORT
  - Direct Peering/interconnection & Origin Validation
  - RPKI ROA MaxLength Considerations
- Outlook on industry trends & projects

Traffic engineering options – “in” vs ”out”

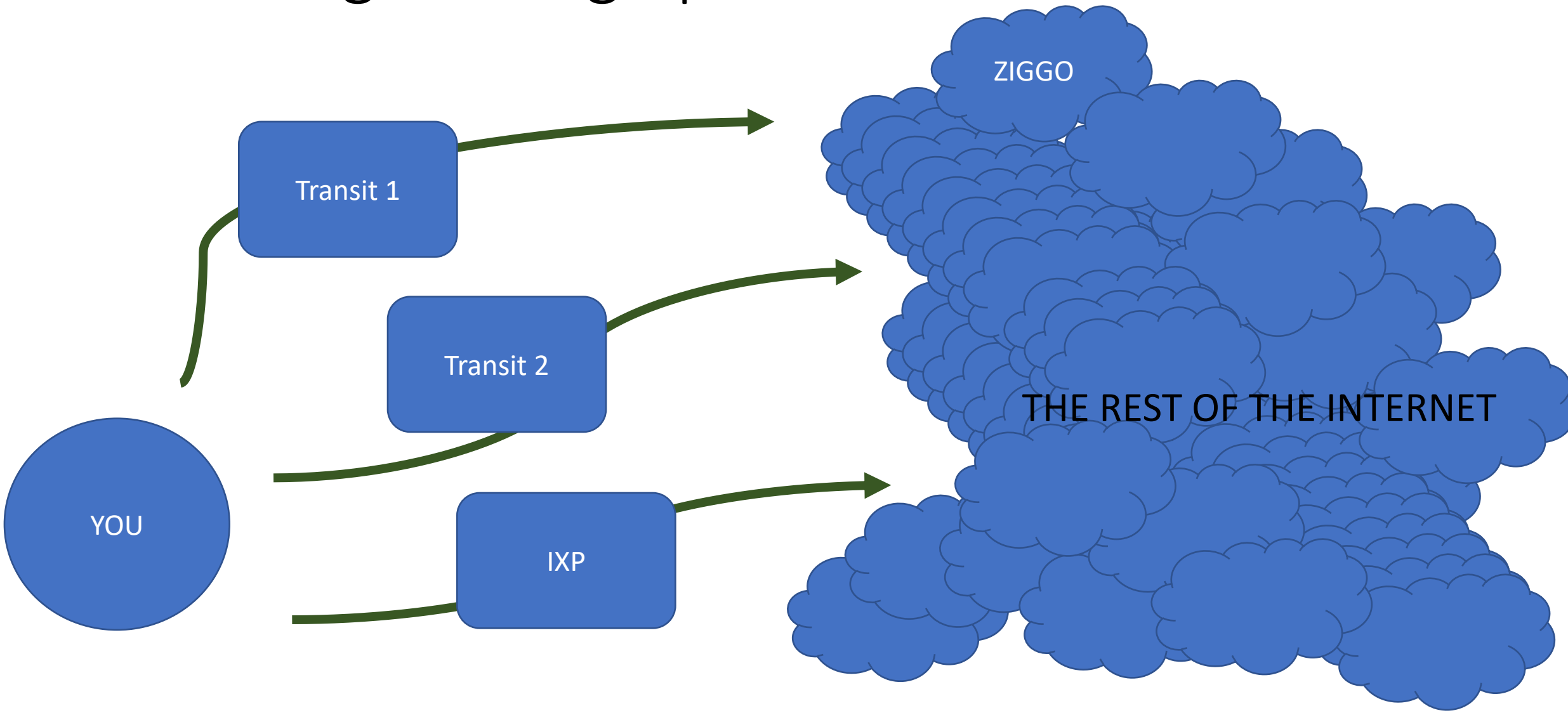
“**in**” means “**from the Internet, to you**”

“**out**” means “**from you, to the Internet**”

In general you can’t really mandate where traffic comes in, but you do have a lot of control over where you send traffic out.

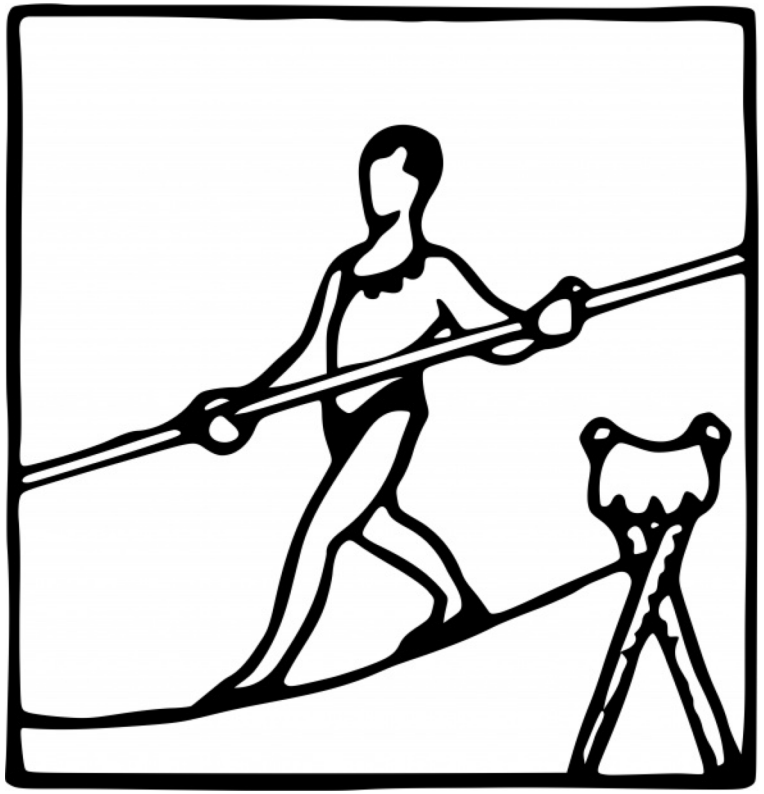
Some carriers use the words “push” and “pull” instead of “in” and “out”, always confirm the direction!

Traffic engineering options – ”**out**”



Challenges (… in some places)

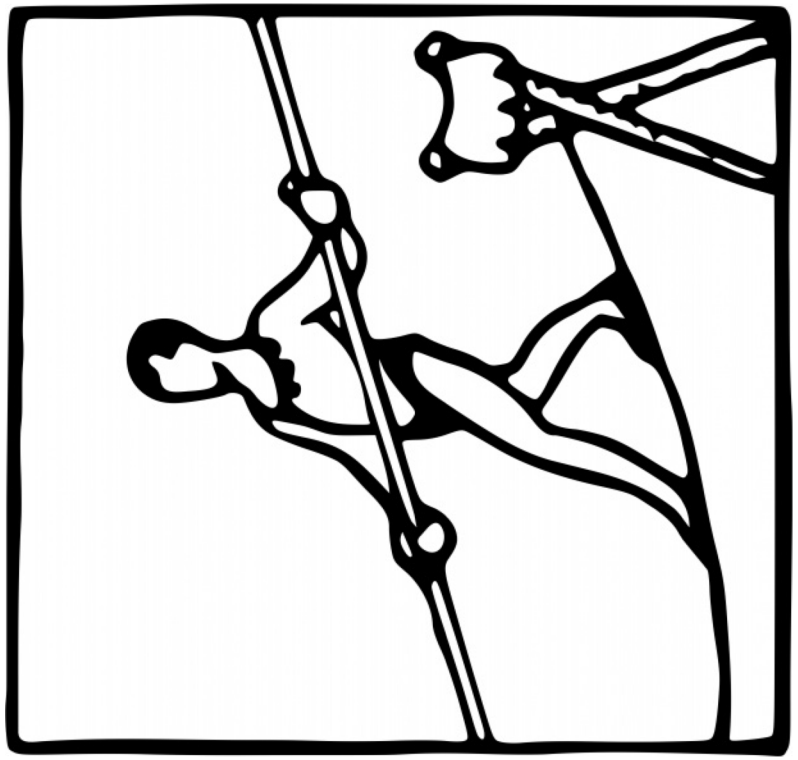
- Your company may not have a lot of choice of upstream providers
- Your company may have to navigate a fine line between multi-year traffic level commitments on circuits
- The organization doesn’t have full time network engineers



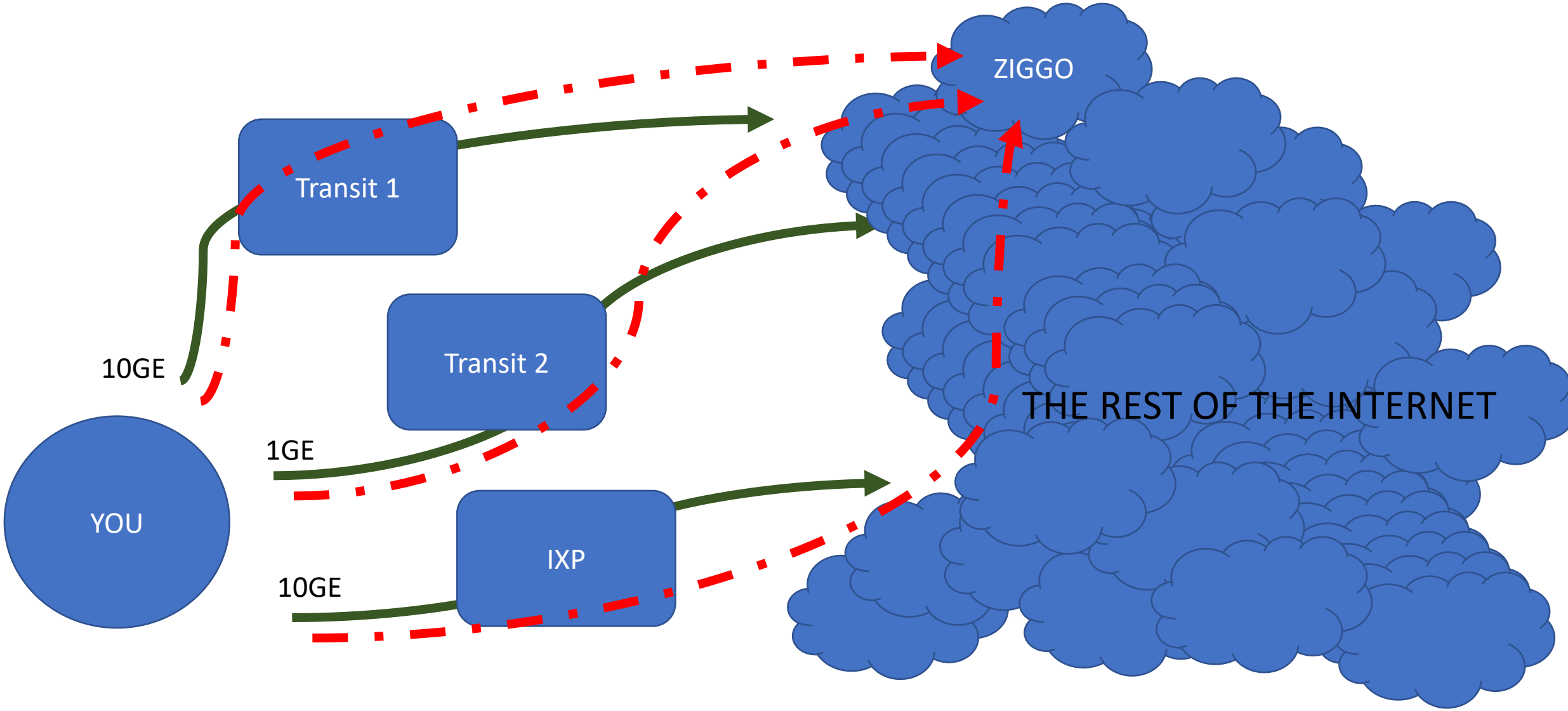
Challenges (… sometimes)

Results in …. software was sold to the company that:

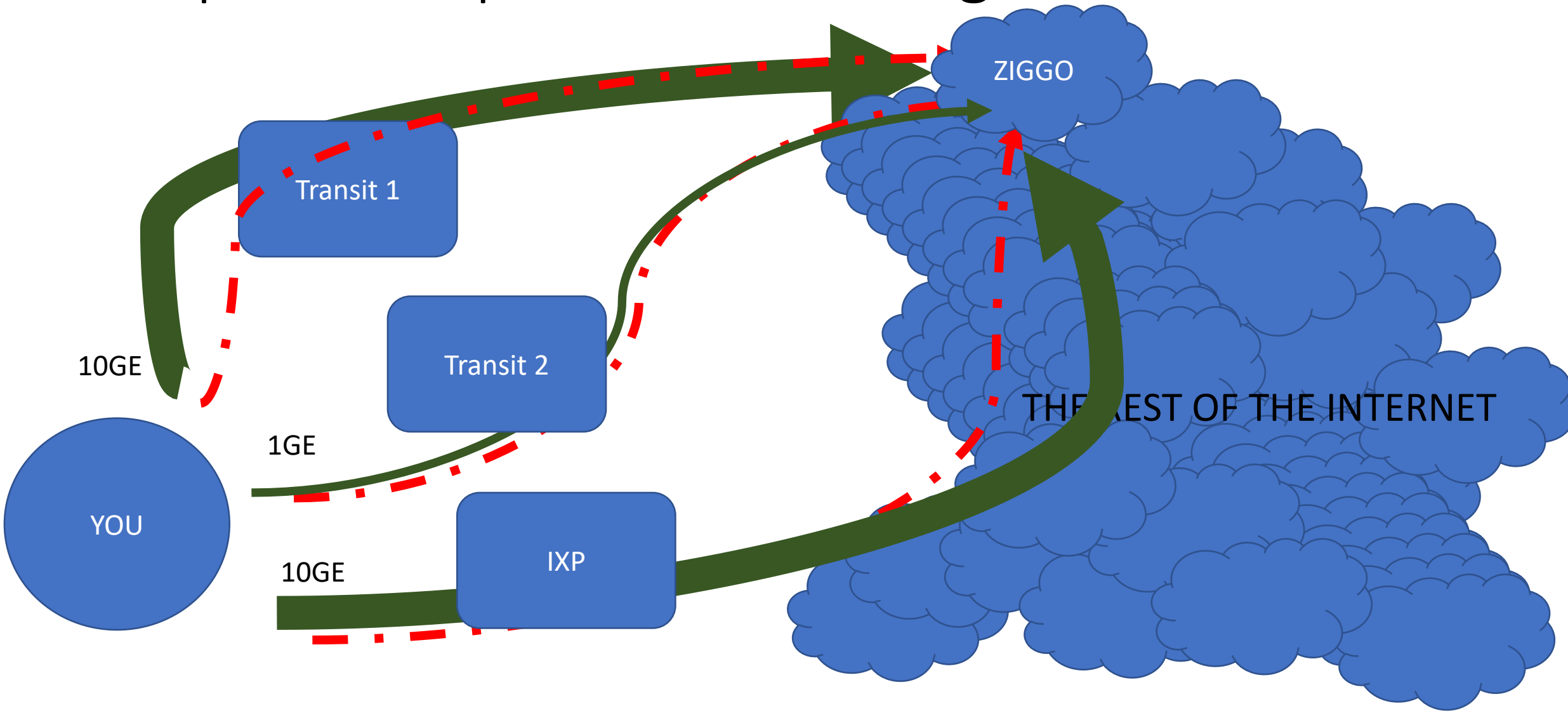
- *Improves performance !111eleven11!!*
- *Reduces* operational *cost*
- Adds *intelligence*
- *Leverages* existing connectivity
- Monitor 24/7



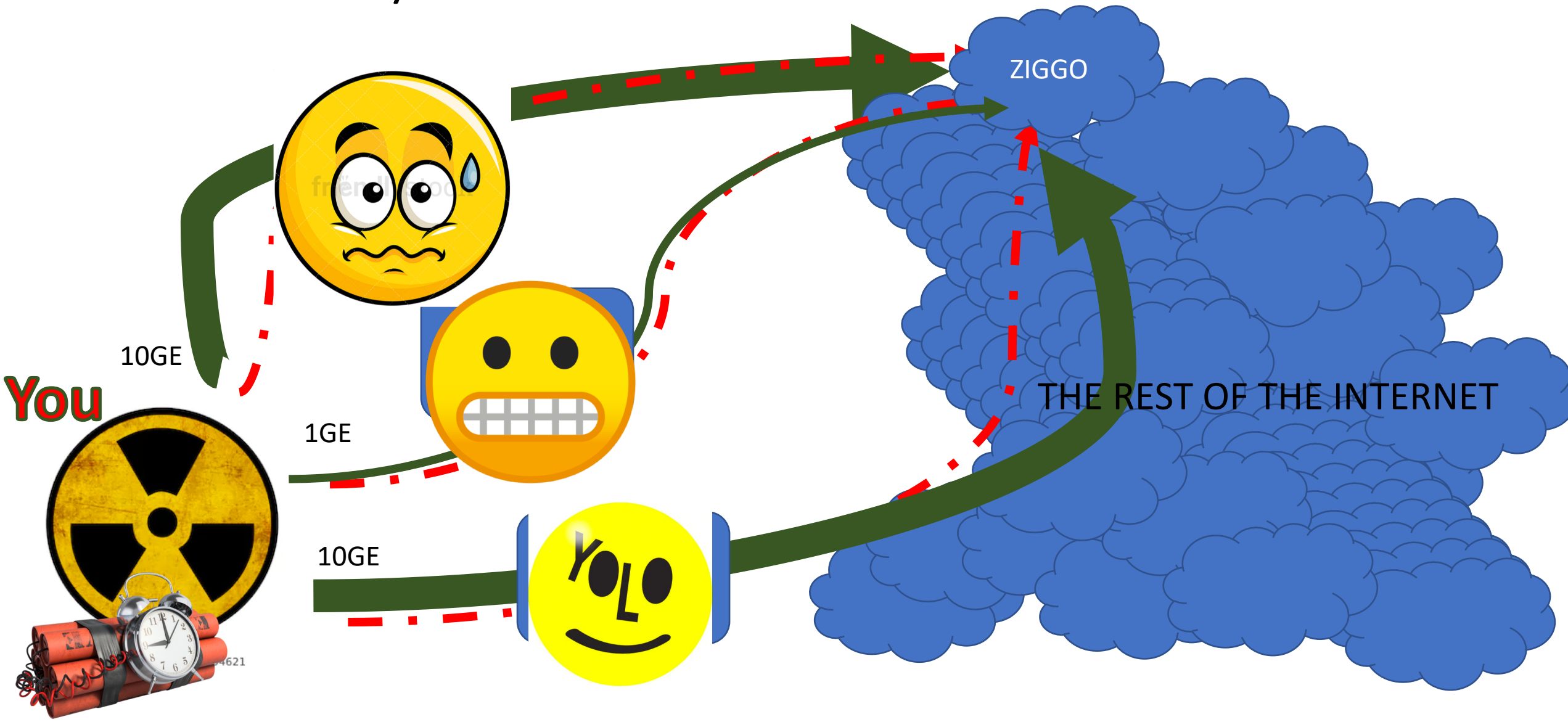
Steering traffic “**Out**” -> “performance probing”



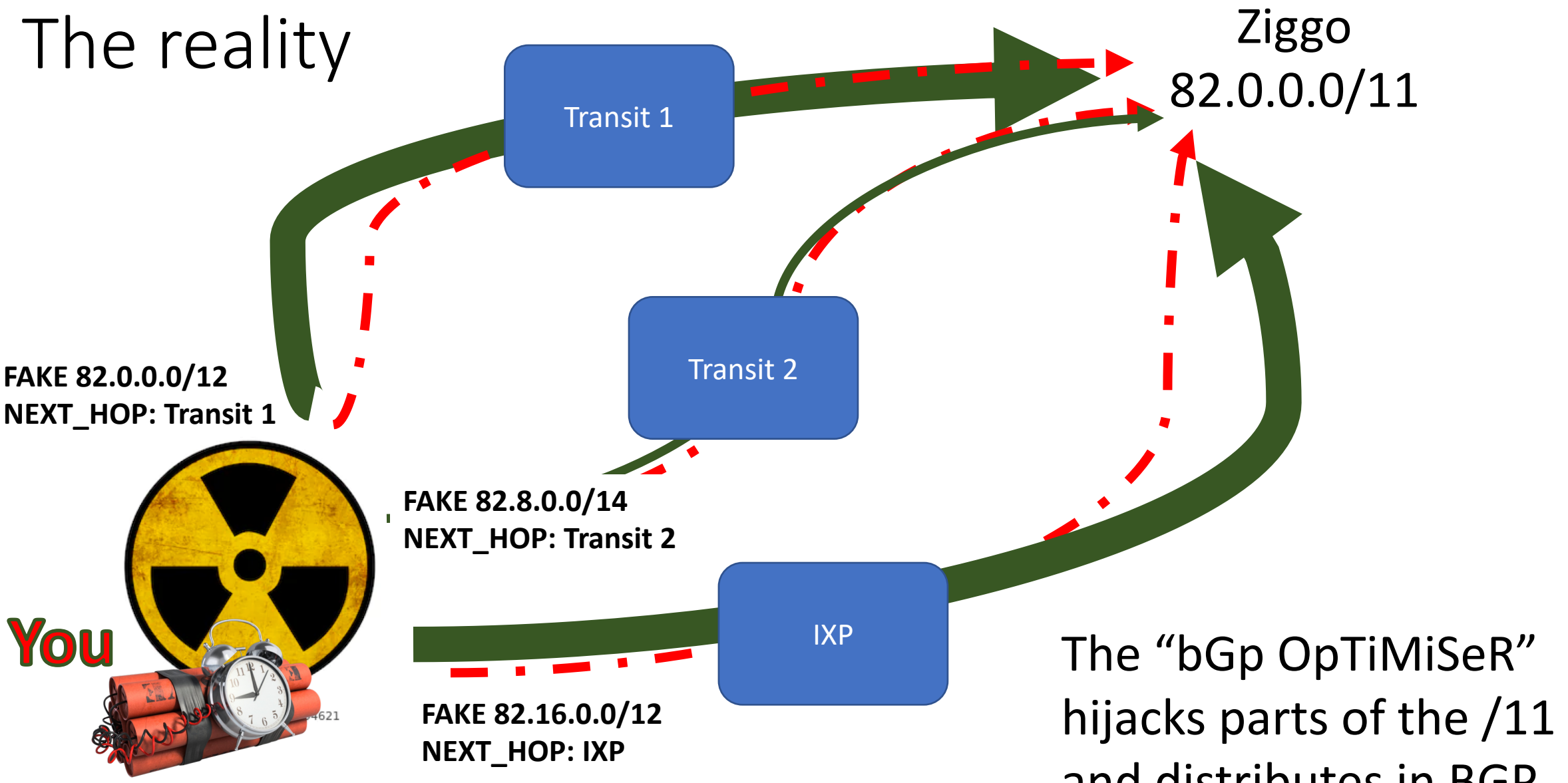
The promise: perfect balancing



The reality



The reality



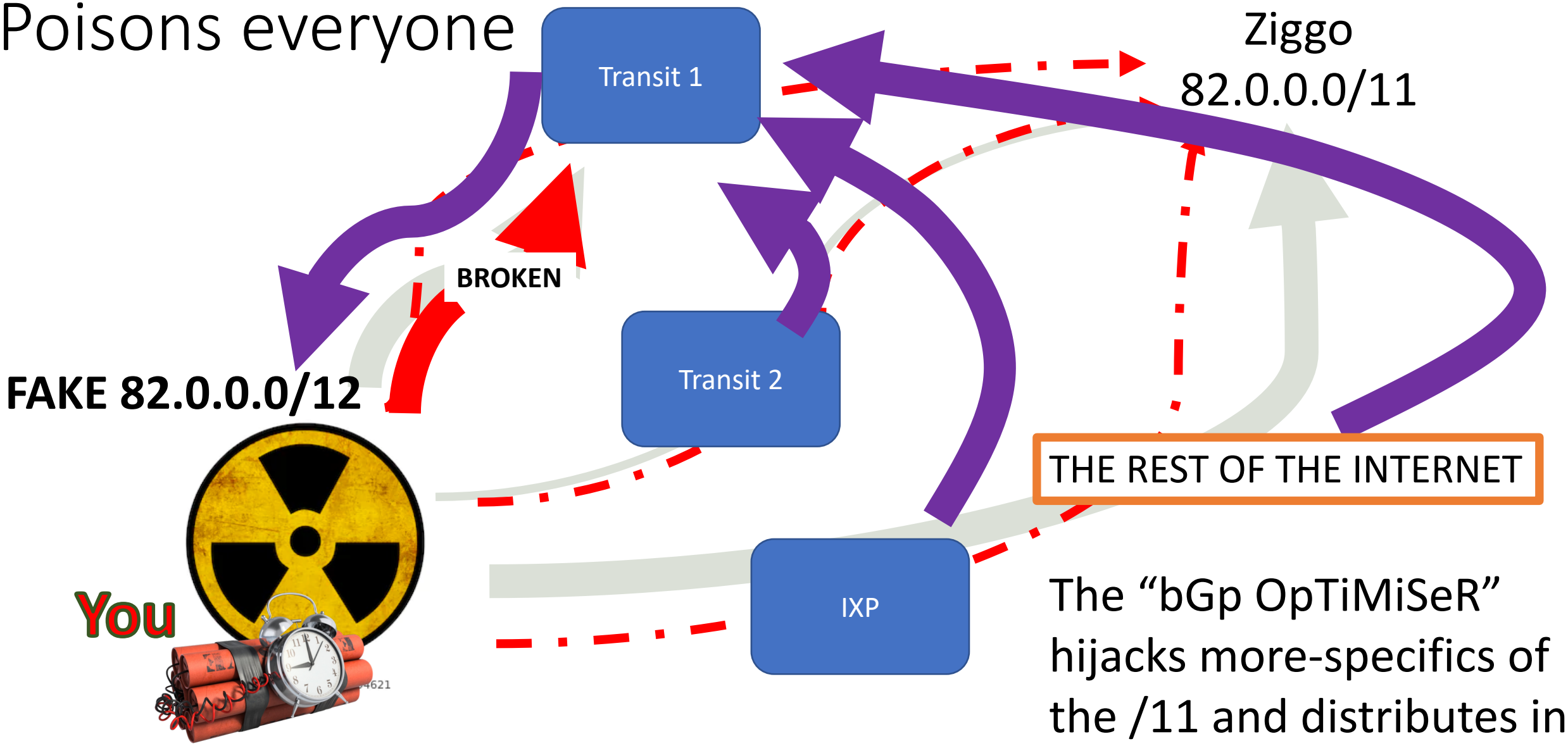
The “bGp OpTiMiSeR” hijacks parts of the /11 and distributes in BGP

When those lies leak out….

10GE

You

Poisons everyone

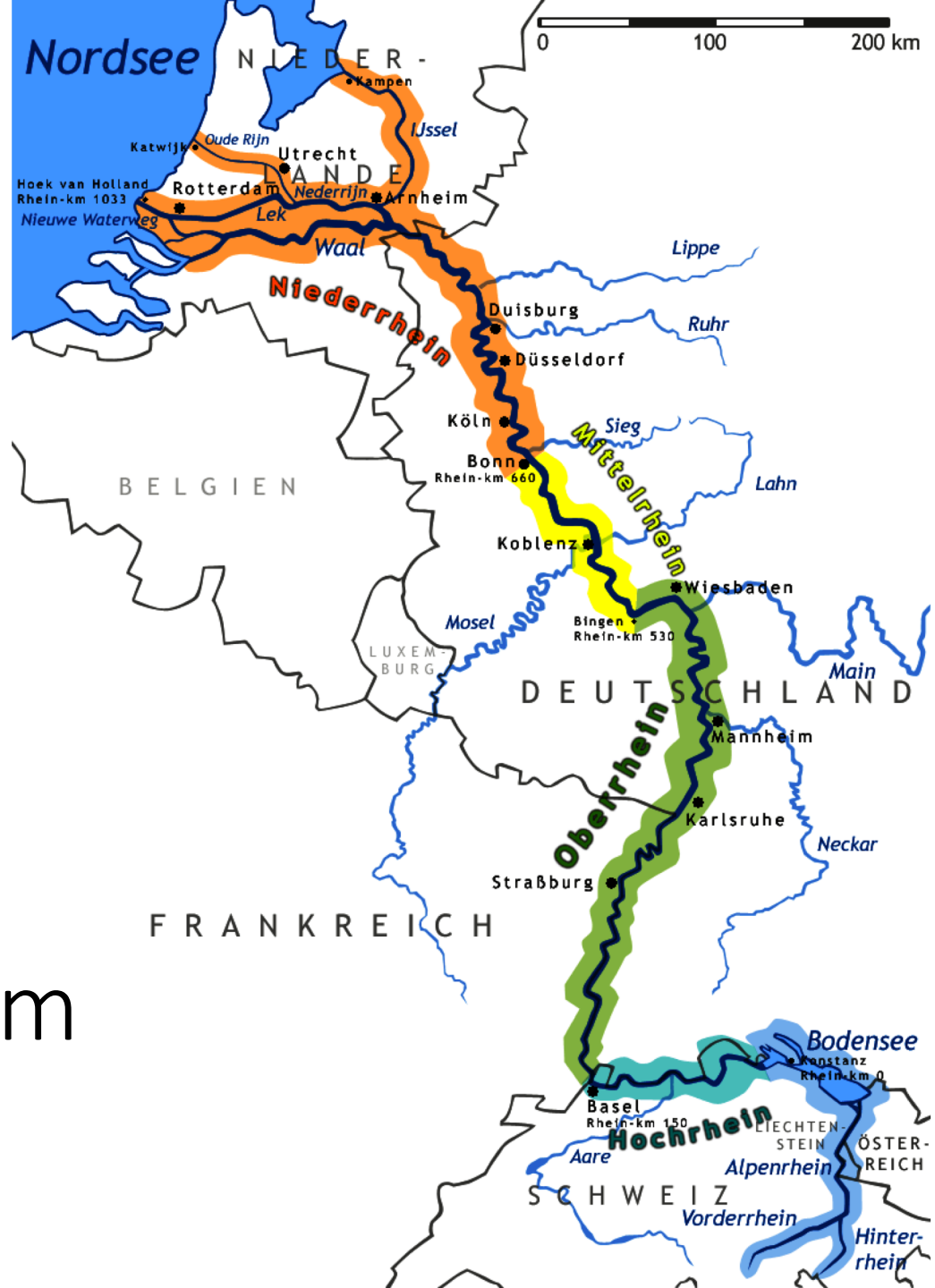


The “bGp OpTiMiSeR” hijacks more-specifics of the /11 and distributes in BGP

If the Default-Free Zone is a shared resource…

bGp OtiMiSeRs are cause for “water conflicts”

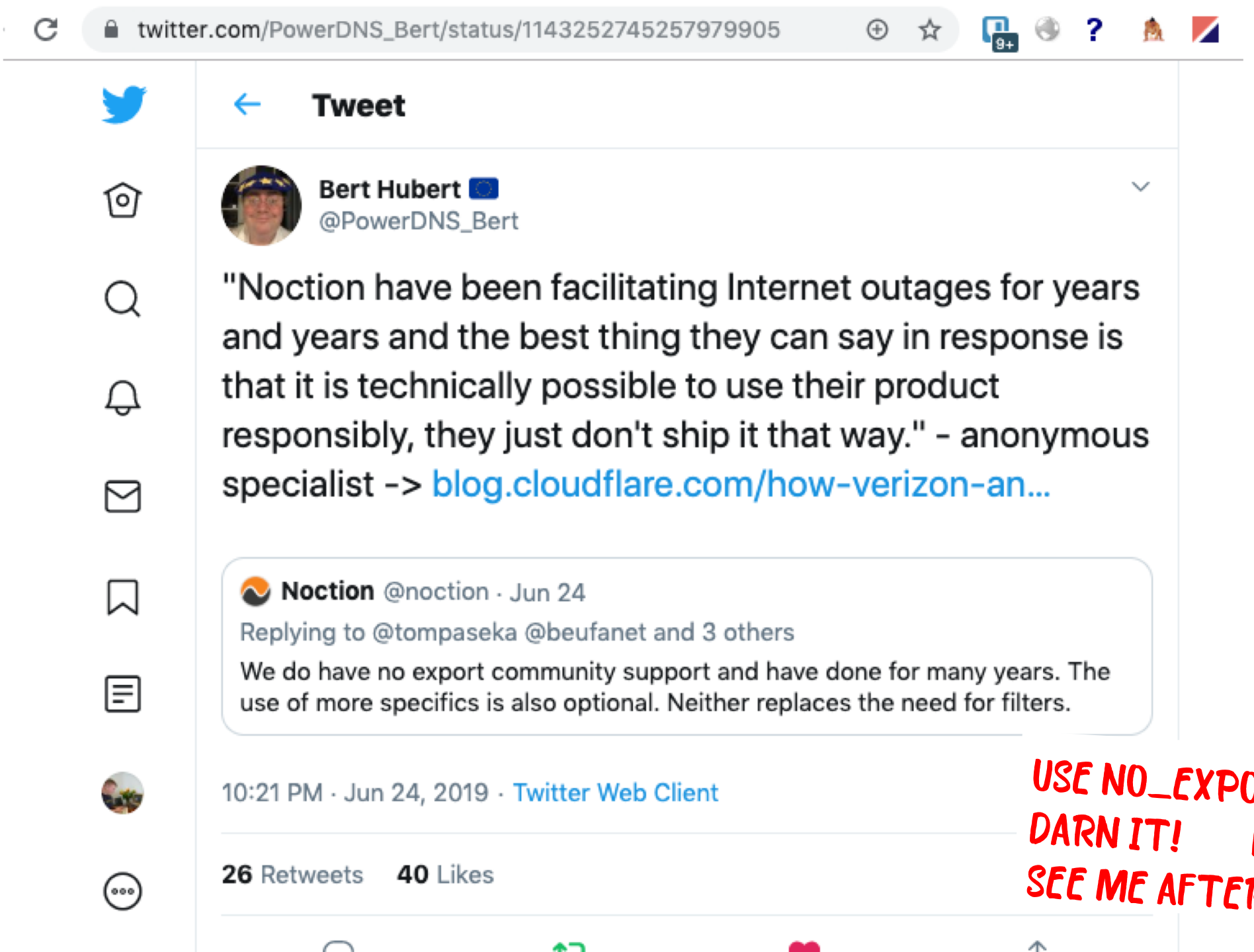
Problems upstream cause problems downstream



Why do these things happen?

- Not all bGp OtImIsErs use NO_EXPORT
- Not all BGP implementations are bug free
- There is no “traffic-engineering” AFI in BGP. All routes are conflated in same IPv4/IPv6 unicast family
- In anticompetitive markets, the cost of Internet access may force people to be creative
- False sense of security ”*If we don’t monitor and optimize, who will?!*”

Why does this happen?



USE NO_EXPORT
DARN IT! F !!!!!
SEE ME AFTER CLASS

What can you do against this? R * P * K * I

1. Help others protect you:

   -> **create RPKI ROAs for your space**

2. Protect yourself and others:

   -> **Deploy RPKI based BGP Origin Validation**

(make sure you set the MaxLength attribute correctly!)

Pro-tip: Peer directly with each other, because…

When an attacker spoofs the origin & same prefix length …

…. their AS_PATH is longer

When an attacker originates more-specifics...

….. you reject the route based on ROA

(Direct peering is sort of "AS_PATH Validation ", for just 1 AS Hop)

Outlook on industry trends

- ARIN TAL
- Pmacct / Kentik business intelligence
- IRRd 4 project
- RIPE 2018-06 Policy Proposal
- BGPalerter
- IXP Manager / Arouteserver

ARIN TAL Politics

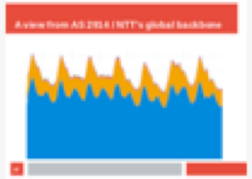
- No real news
- Relaying party agreement is still the same

pmacct

CENTR_Amsterdam_2019_Snijders_ccTLDs_routing.pdf (page 14 of 24) — Edited

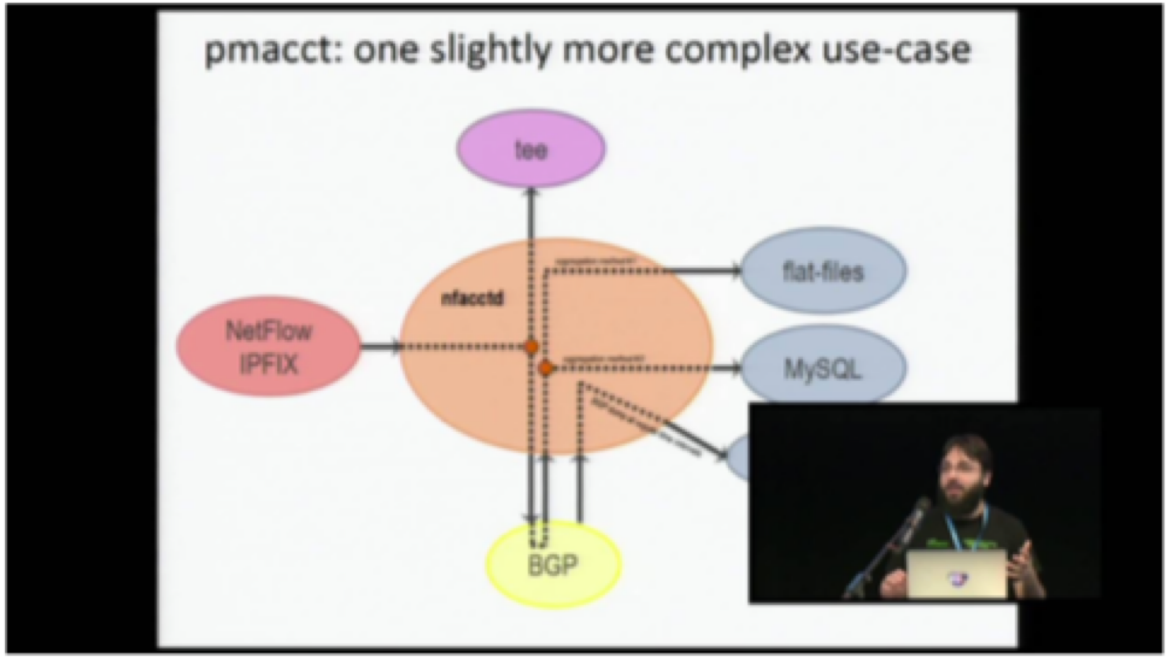
Search

14



15

RPKI based traffic analysis with pmacct



14

A view from AS 2914 / NTT's global backbone

https://mailman.nanog.org/pipermail/nanog/2019-February/099522.html

Free!

http://pmacct.net/

Free!

http://pmacct.net/

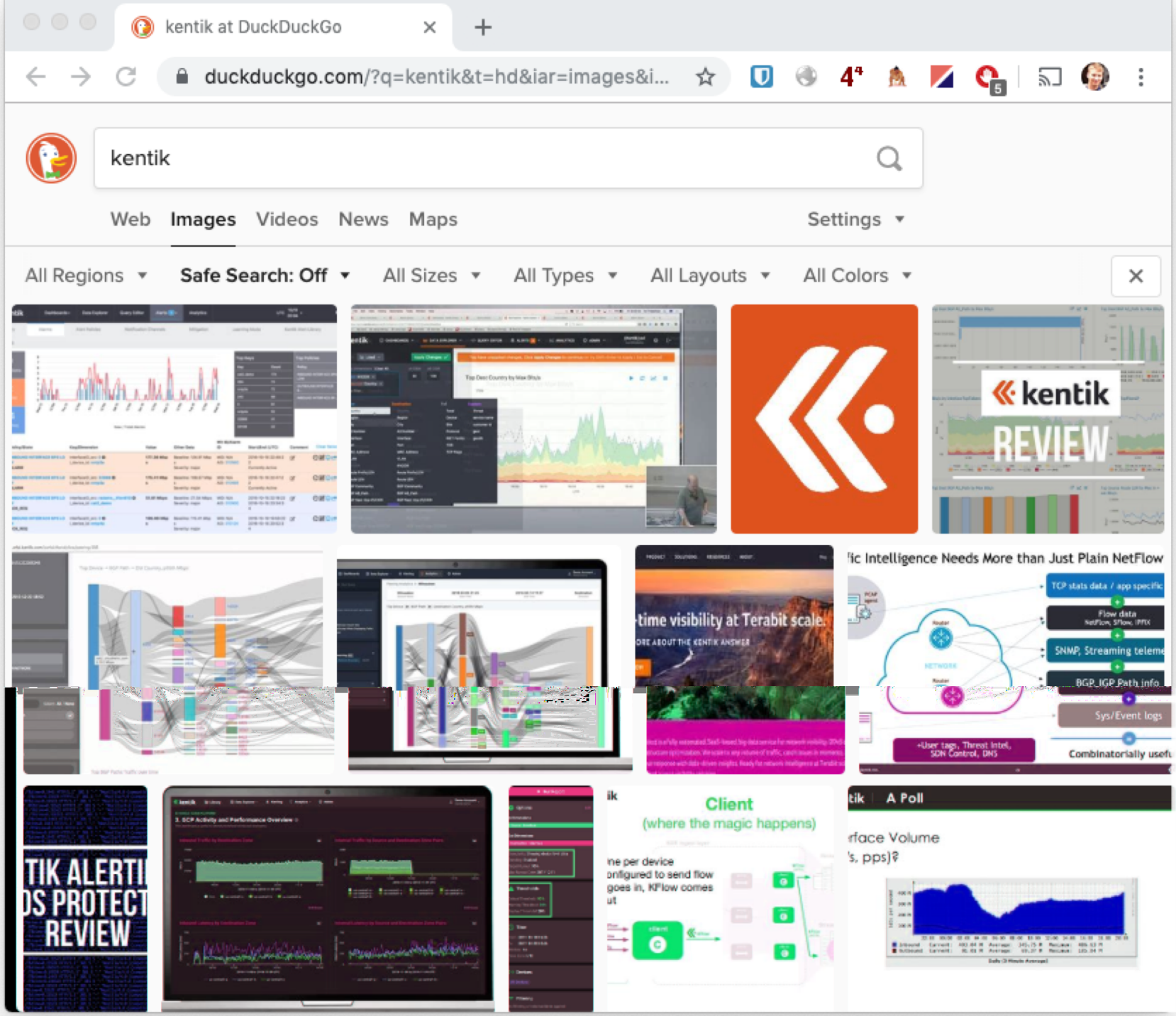
Free!

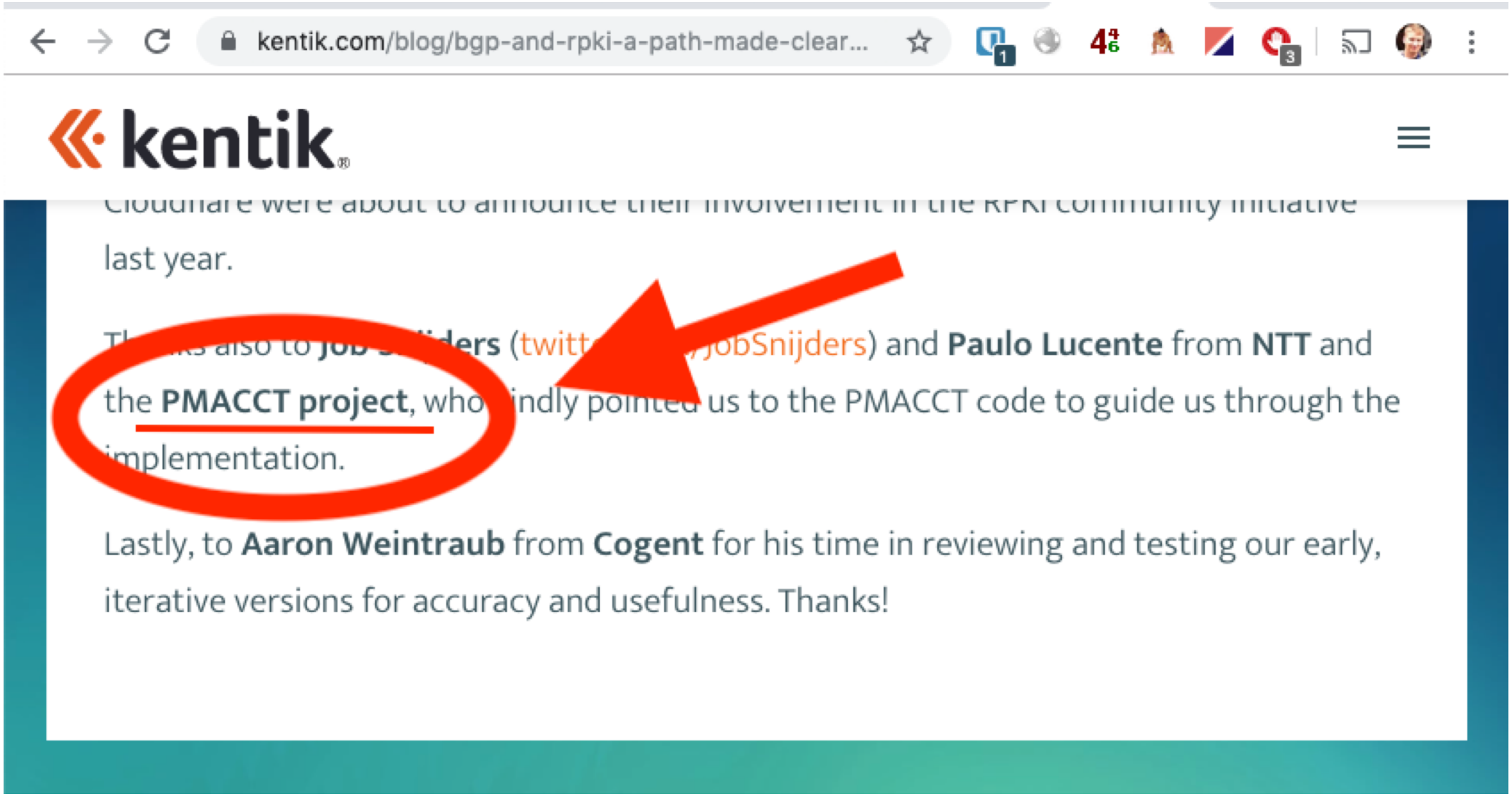
http://pmacct.net/

Free!

http://pmacct.net/

Free!


kentik at DuckDuckGo
duckduckgo.com/?q=kentik&t=hd&iar=images&i...
kentik
Web
Images
Videos
News
Maps
Settings
All Regions
Safe Search: Off
All Sizes
All Types
All Layouts
All Colors
kentik
REVIEW
time visibility at Terabit scale.
ic Intelligence Needs More than Just Plain NetFlow
TCP stats data / app specific
Flow data
NetFlow, SFlow, IPFIX
SNMP, Streaming teleme
BGP, IGP Path info
Sys/Event logs
Combinatorially usefu
TIK ALERTI
S PROTECT
REVIEW
Client
(where the magic happens)
A Poll



https://www.kentik.com/blog/bgp-and-rpki-a-path-made-clear-with-kentik/

IRRd version 4 released!

NTT funded initiative

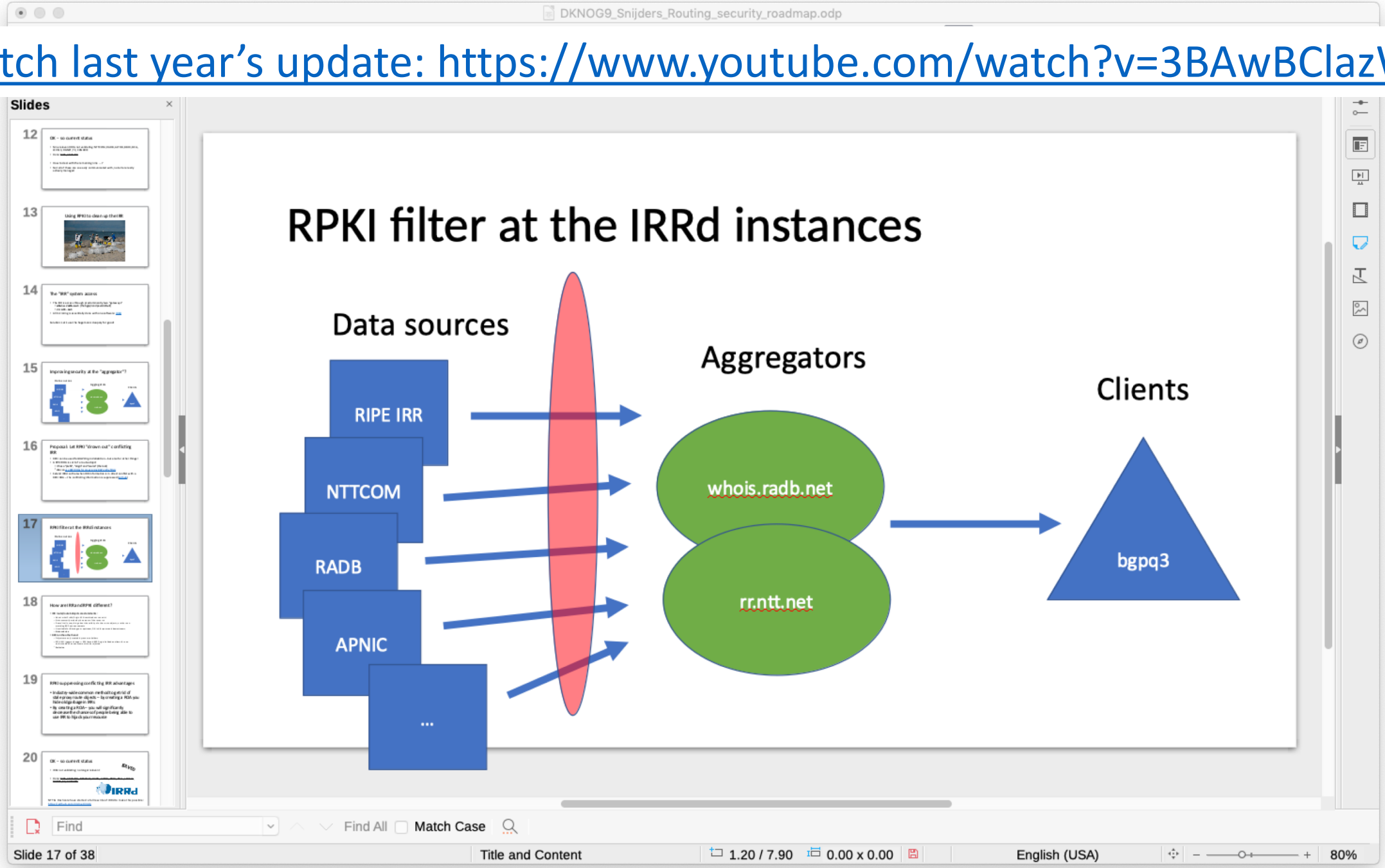
developed by Dashcare

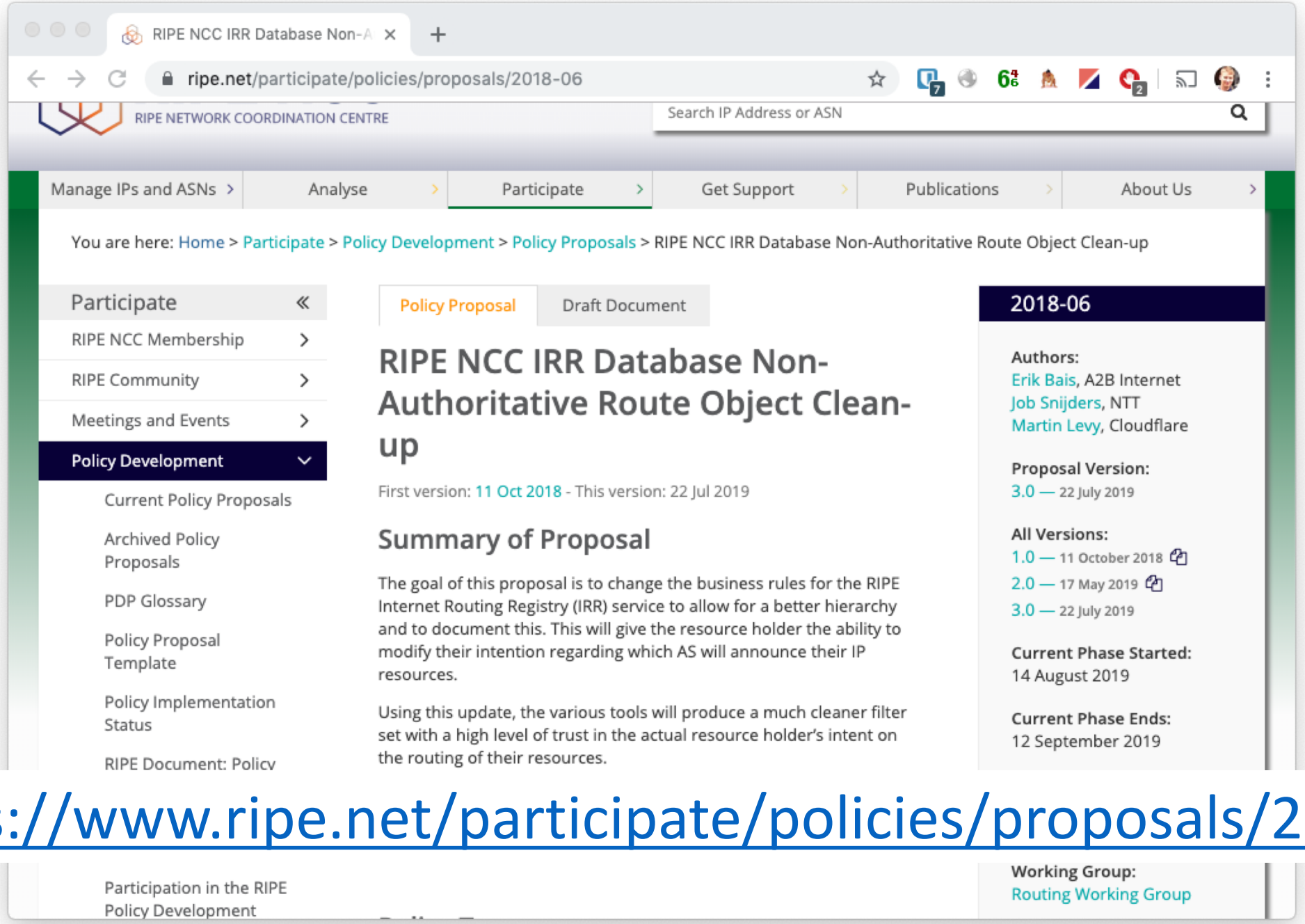
https://github.com/irrdnet/irrd4

https://irrd4.readthedocs.io

`Now in production at rr.ntt.net !!`

Watch last year's update: https://www.youtube.com/watch?v=3BAwBClazWc





https://www.ripe.net/participate/policies/proposals/2018-06

When your favorite startup is a

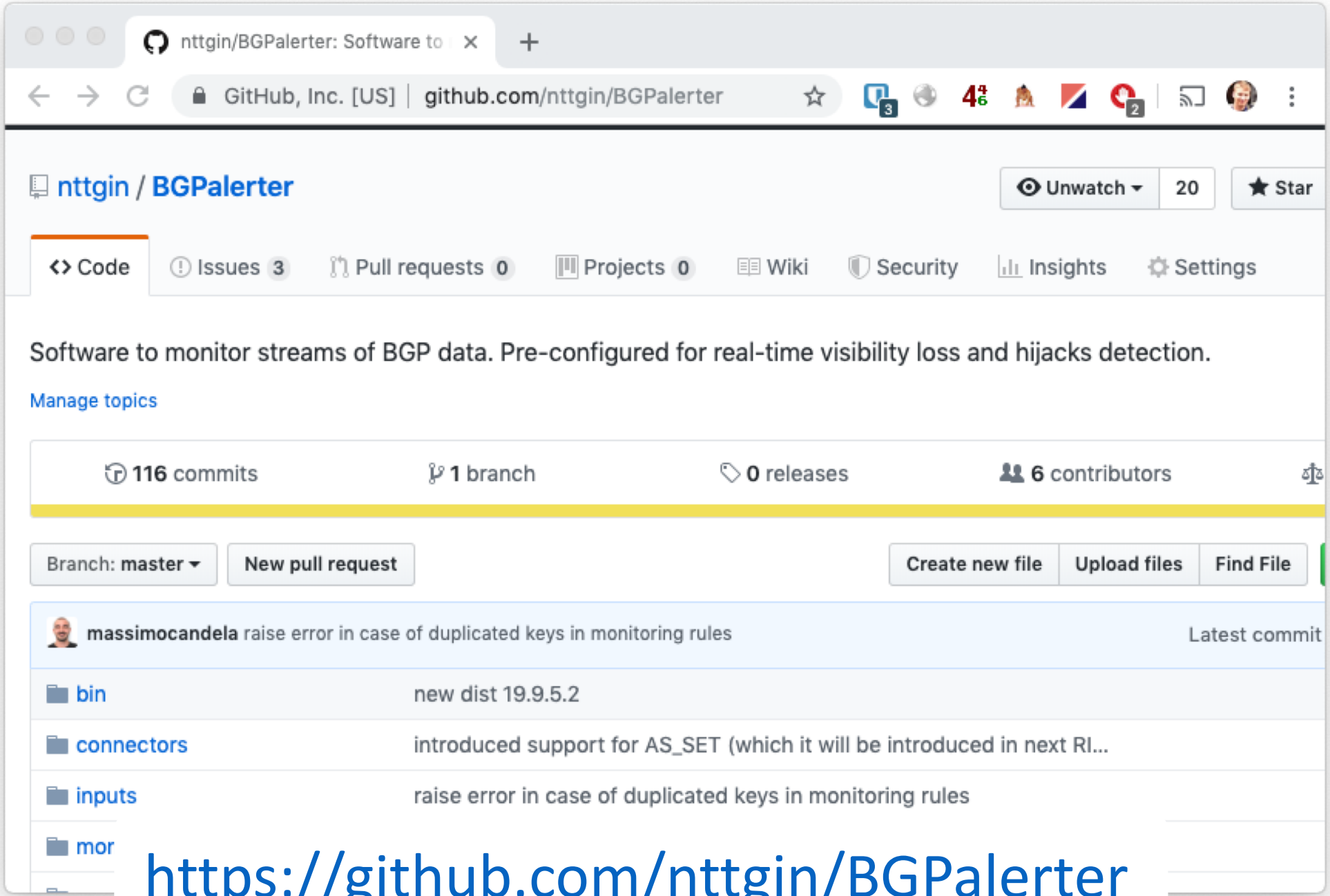
honestnetworker.net/2015/06/28/when-your-favorite-s...

Incognito

Jun
28

When your favorite startup is acquired by Cisco

Posted by ohseuch4aeji4xar



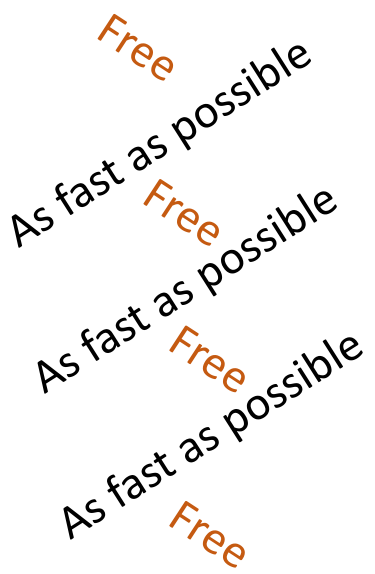
https://github.com/nttgin/BGPalerter

BGPalerter in a nutshell

- Uses data from RIPE RIS collectors (data inputs are “connectors”)
- Then push data through “monitors” for evaluation and alert event detection
- Finally Spit it out via “reports” (slack, email, IRC, etc..)

Use BGPalerter to monitor for hijacks & outages

https://github.com/nttgin/BGPalerter



Start bgpalerter

```
BGPalerter, version: 19.8.30.2 environment: production
Loaded config: /home/rinse/bgpalerter/config.yml
Subscribing to: 2001:9e0::/32
Subscribing to: 91.212.184.0/24
Subscribing to: 185.117.108.0/22
Subscribing to: 185.83.32.0/22
Subscribing to: 217.26.96.0/20
Subscribing to: 5.199.144.0/20
Subscribing to: 81.24.96.0/20
Subscribing to: 212.84.128.0/19
Subscribing to: 213.134.224.0/19
Subscribing to: 212.45.32.0/19
Subscribing to: 213.233.192.0/18
Subscribing to: 83.247.0.0/17
Subscribing to: 87.195.0.0/16
```

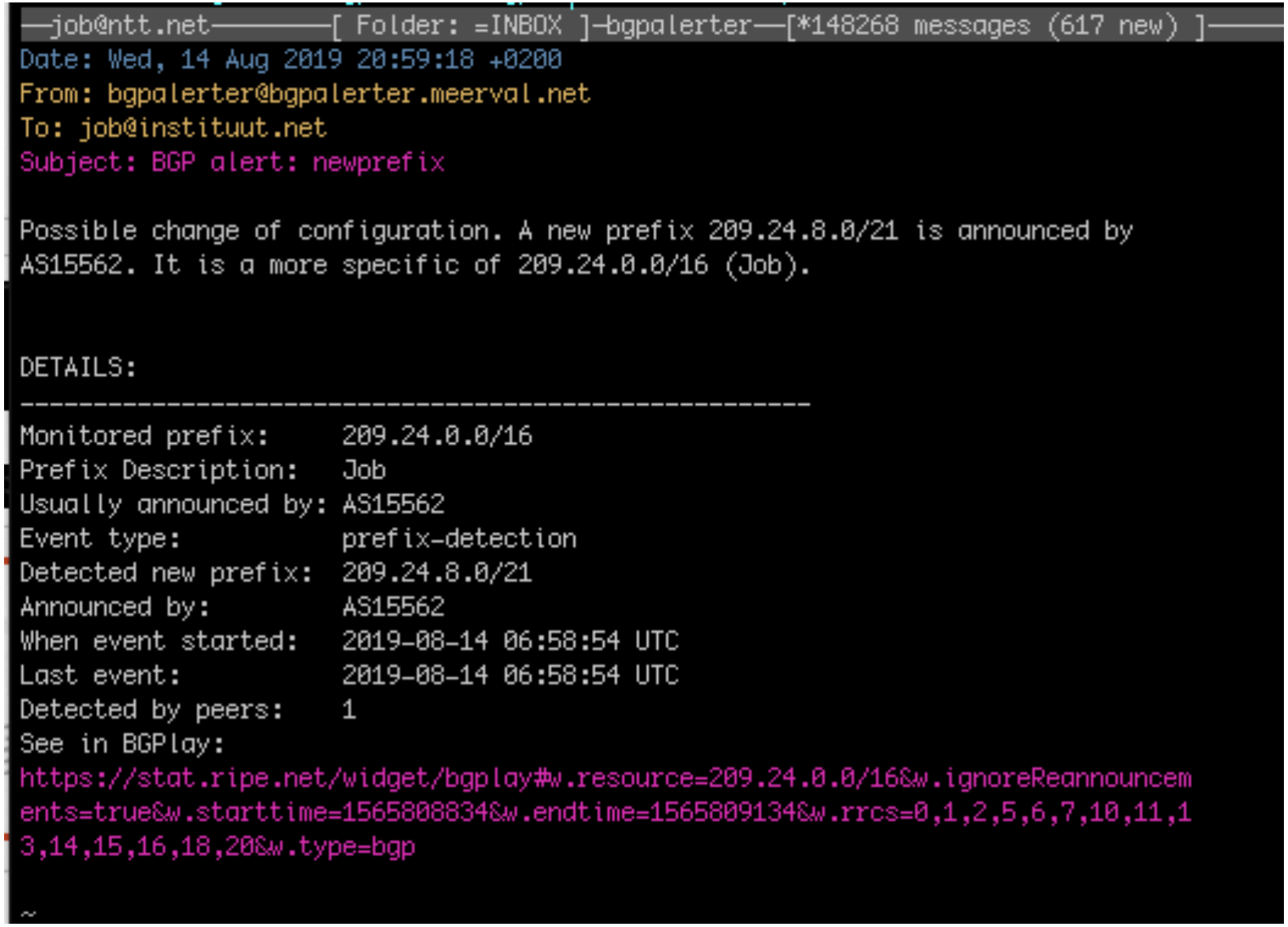
RIPE RIS LIVE MAGIC

Observe DDOS mitigation in progress

```
rinse@mml:~/bgpalerter$ tail -f logs/reports-2019-09-02.log
2019-09-02T14:15:16.534Z [production] verbose: Possible change of configuration. A new prefix 213.134.227.0/24 is announced by
AS12414. It is a more specific of 213.134.224.0/19 (Solcon Internetdiensten B.V).
2019-09-02T14:46:12.292Z [production] verbose: Possible change of configuration. A new prefix 213.134.227.0/24 is announced by
AS12414. It is a more specific of 213.134.224.0/19 (Solcon Internetdiensten B.V).
```

Example contributed by Rinse Kloek

BGPalerter can email (of course)



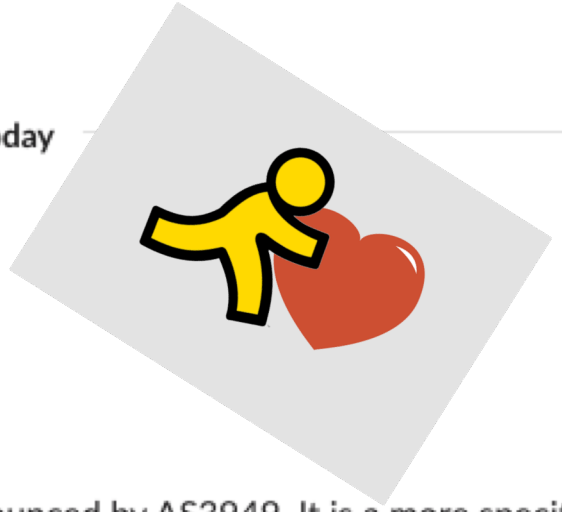
BGPalerter can send to Slack too… (AOL or MSN?)

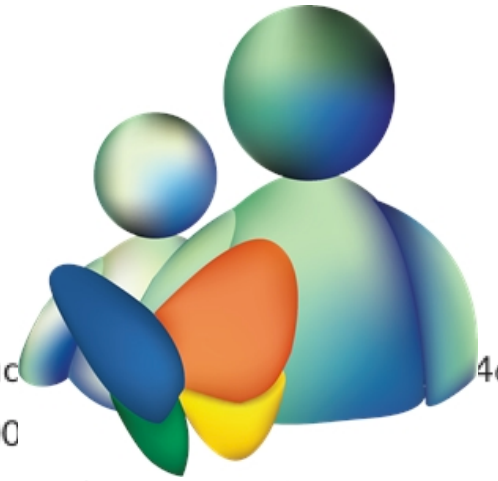
o.slack.com/client/T03CKAZCU/CFW2RF9MJ/details/members

#bgpalerts

☆ | 6 | 0 | Add a topic

Today





Massimo Candela 2:51 PM
(I added coverage in the tests also)

arjen 2:55 PM
I disconnected my AS yesterday

I'll hook it up again tonight and see what happens, thanks! 🙂 (edited)

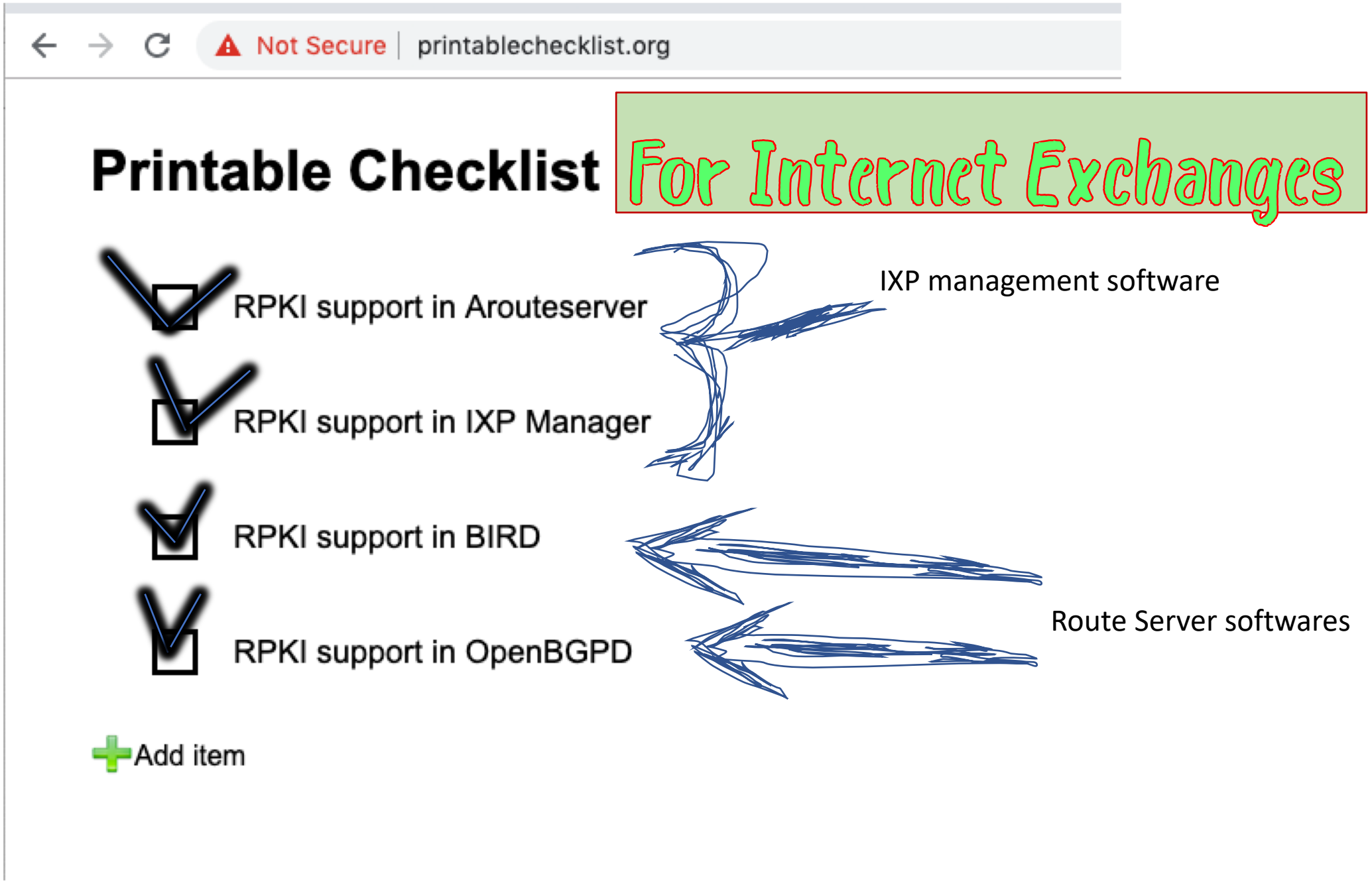
incoming-webhook APP 4:19 PM
Possible change of configuration. A new prefix 203.105.76.0/23 is announced by AS3949. It is a more specific 4600).

A new prefix 120.29.148.0/24 is announced by AS30103. It should be instead 120.29.144.0/21 (subas 64600

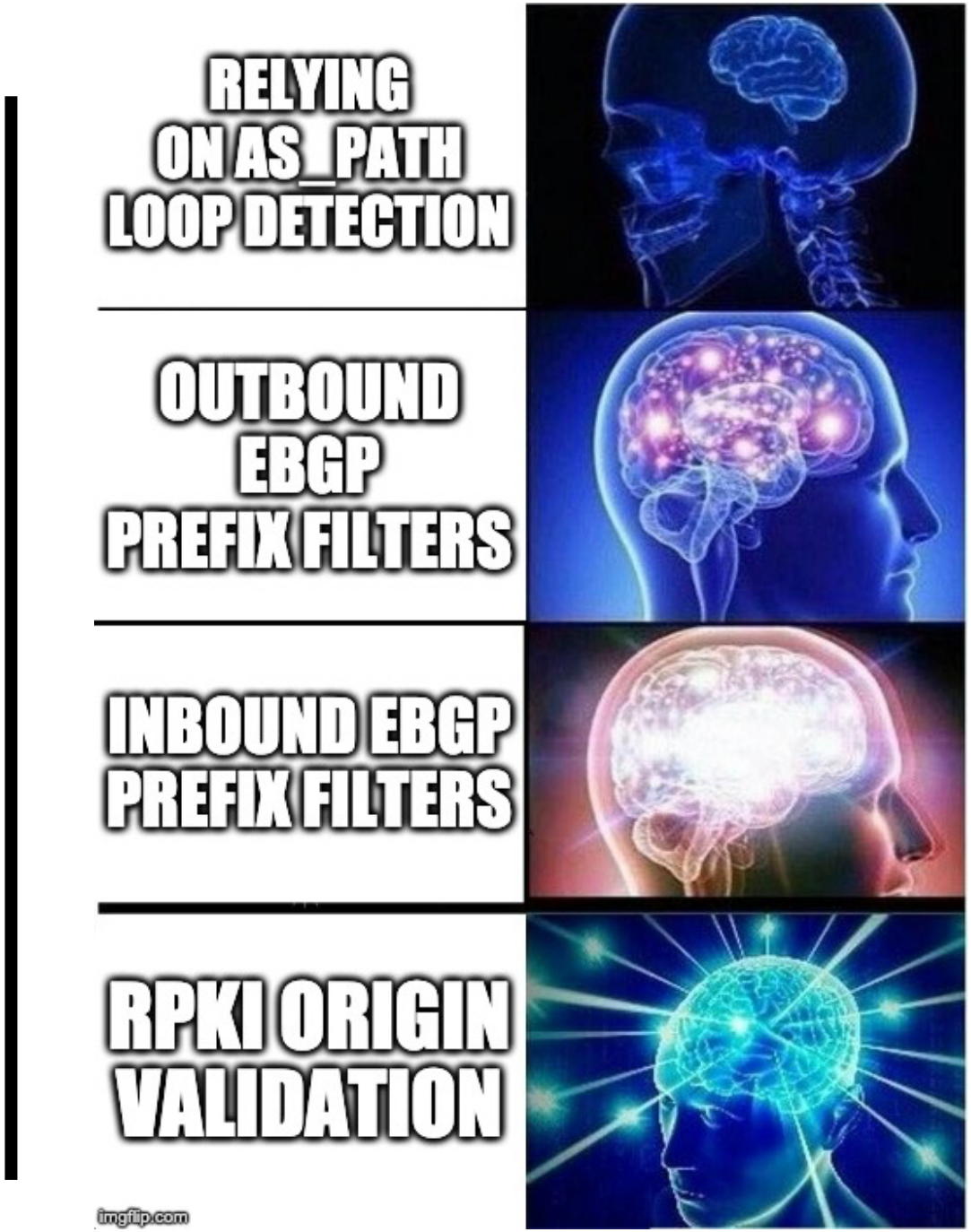
A new prefix 117.104.145.0/24 is announced by AS394265. It should be instead 117.104.128.0/19 (subas 64600) announced by AS2914

Possible change of configuration. A new prefix 180.12.186.0/24 is announced by AS4713. It is a more specific of 180.0.0.0/10 (OCN).

Possible change of configuration. A new prefix 180.12.181.0/24 is announced by AS4713. It is a more specific of 180.0.0.0/10 (OCN).


Not Secure
printablechecklist.org
Printable Checklist
For Internet Exchanges
RPKI support in Arouteserver
RPKI support in IXP Manager
RPKI support in BIRD
RPKI support in OpenBGPD
Add item
IXP management software
Route Server softwares

<<< time for questions! >>>

Also feel free to ask questions later today, or via cyber

job@ntt.net
https://twitter.com/jobsnijders