https://faelix.link/uknof43

SCANNING IPv6 ADDRESS SPACE…

MAREK ISALSKI — FAELIX — UKNOF 43

https://faelix.link/uknof43

SCANNING IPv6 ADDRESS SPACE...

AND THE REMOTE VULNERABILITIES IT UNCOVERS

About Marek

- Stuff I do:
  - CTO @FAELIX – https://faelix.net/
  - PC @uknof – https://uknof.uk/
  - PC @net_mcr – https://www.netmcr.uk/
- Trail of SSIDs in my wake: "AS41495 Faelix Limited"
- Me — @maznu – @NetworkMoose – @IPv6HULK

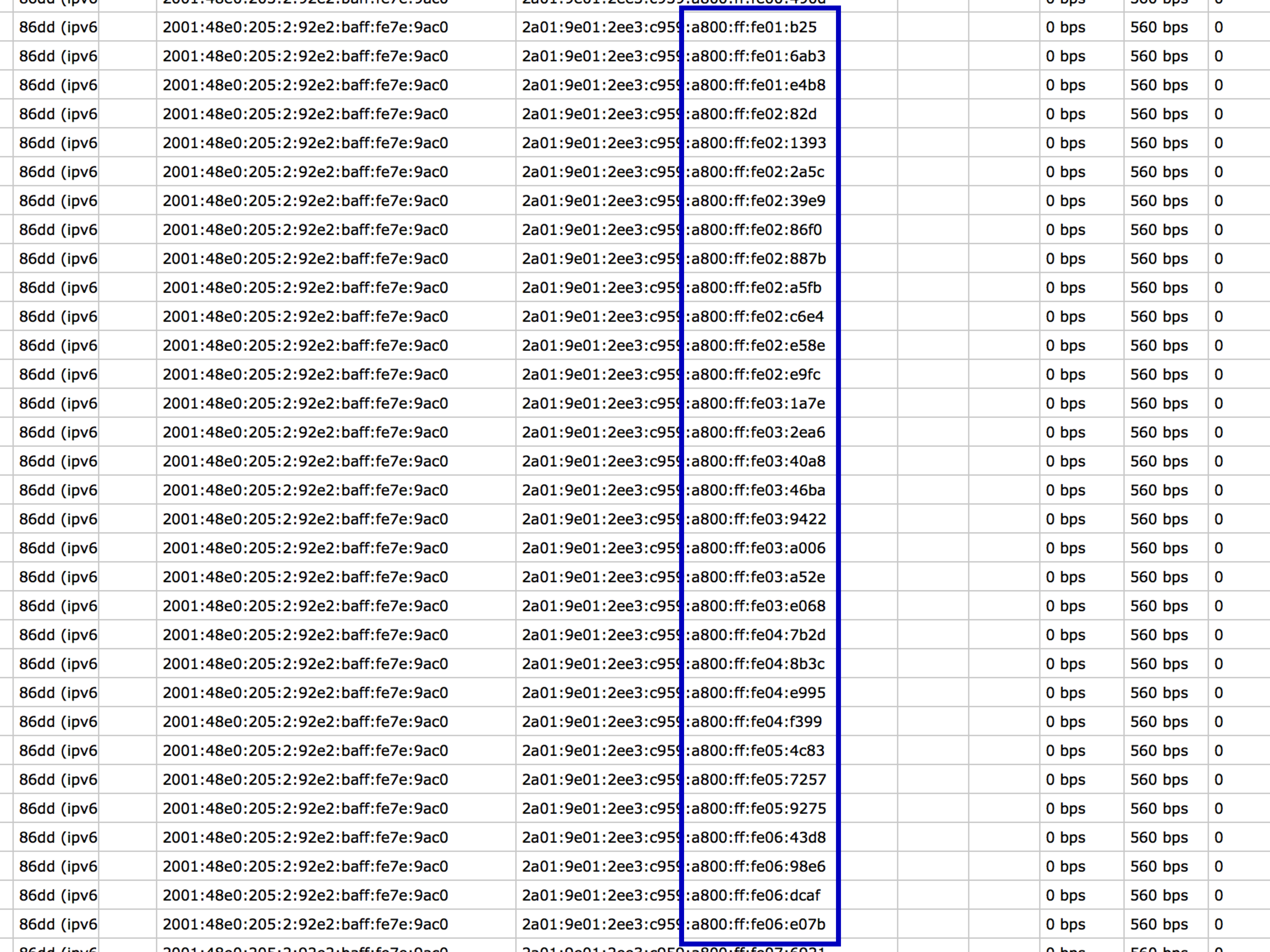
This Talk

- IPv6 Scanning I Have Observed
- IPv6 Scanning Papers
- IPv6 Vulnerabilities

2017-09-17: UNM.EDU

“I never thought I would be writing an email to say that someone is trying to scan our IPv6 address space…”

– email to abuse@unm.edu, 2017-09-17



86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe00:490d			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe01:b25			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe01:6ab3			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe01:e4b8			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:82d			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:1393			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:2a5c			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:39e9			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:86f0			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:887b			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:a5fb			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:c6e4			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:e58e			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe02:e9fc			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:1a7e			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:2ea6			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:40a8			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:46ba			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:9422			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:a006			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:a52e			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe03:e068			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe04:7b2d			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe04:8b3c			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe04:e995			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe04:f399			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe05:4c83			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe05:7257			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe05:9275			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe06:43d8			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe06:98e6			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe06:dcaf			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe06:e07b			0 bps	560 bps	0
86dd (ipv6		2001:48e0:205:2:92e2:baff:fe7e:9ac0	2a01:9e01:2ee3:c959:a800:ff:fe07:6921			0 bps	560 bps	0

Actions

- Emailed abuse
- Blocked their scanner
- Went back to sleep

2018-03-31: BERKELEY

"We've blocked your /48 from our network because the IPv6 scanning you are performing against 2a01:9e00::/32 is aggressive."

– email to cesr-scanning@eecs.berkeley.edu, 2018-03-31

Actions

- Emailed abuse and project contact in WHOIS
- Blocked their scanner
- Went back to sleep
- …got an email back from them!

Discussed with Berkeley

- AM: "smart scanning techniques [...] measurement research [...] probe a large set of hosts on the Internet "
- MI: "slipshod IPv6 implementations"
- AM: "based on RFC7707 and RFC6583 we have decided to add a module to our scanner that will rate control probes sent to each /64 in addition to each routed prefix"

IPv6 SCANNING EXISTS!

Scanning Projects/Papers

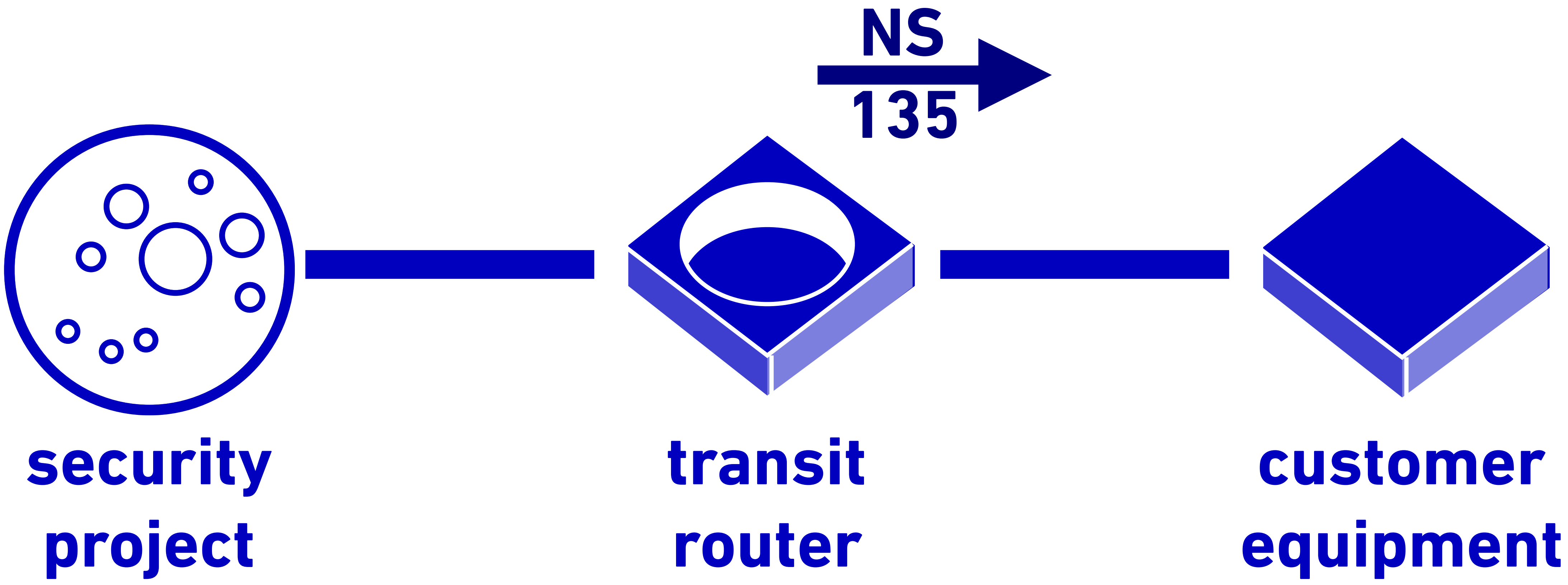
- E Vyncke, UK IPv6 Council, 2014: https://www.ipv6.org.uk/wp-content/uploads/2018/10/evyncke-UK-council-IPv6-security.pdf
- Chris Grundemann, 2015: https://www.internetsociety.org/blog/2015/02/ipv6-security-myth-4-ipv6-networks-are-too-big-to-scan/
- RIPE74, 2017: http://www.entropy-ip.com/
- 6Gen, Berkeley: https://conferences.sigcomm.org/imc/2017/papers/imc17-final245.pdf
- ZMapv6: https://ipv6hitlist.github.io/

Berkeley = UNM

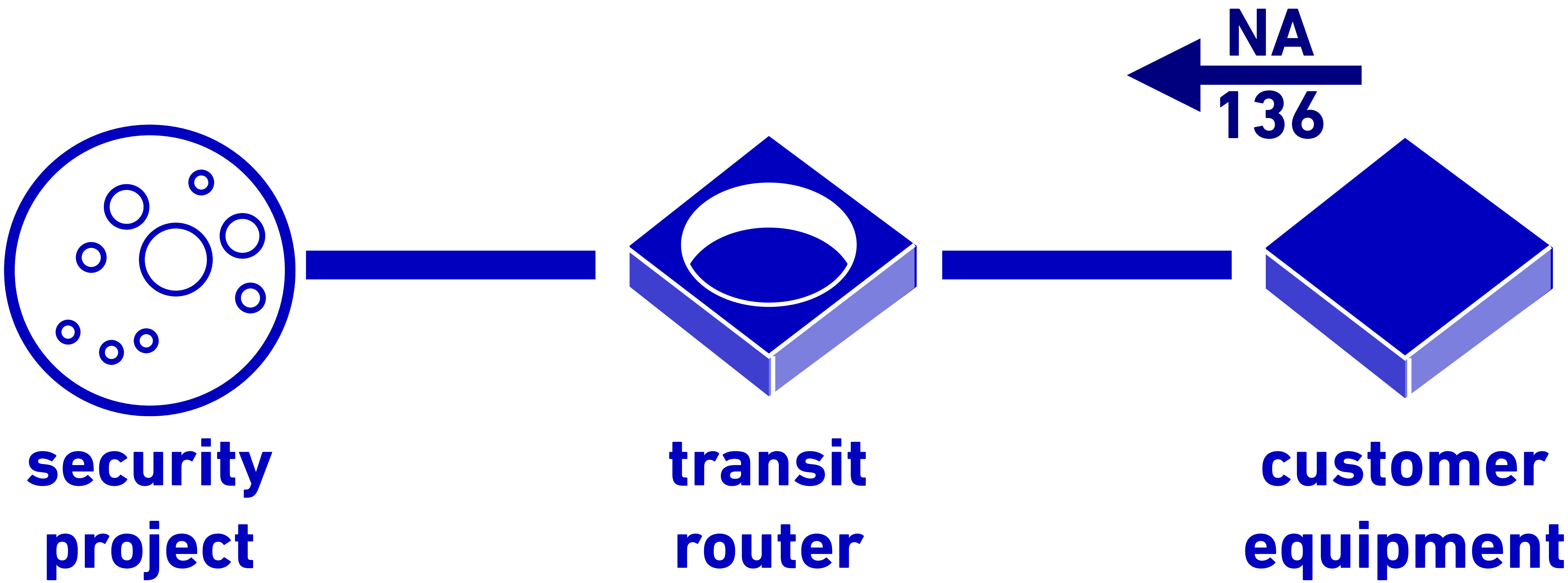
- Subsequent emails with Austin Murdock, PhD student "working on IPv6 measurement as part of [his] dissertation".
  - "Currently we spread our probes across ~19K routed prefixes and probe them in parallel [...] maximum pps rate sent to your route was 179 pps [...] we have now added the subnet rate limiter as discussed to try and avoid disrupting devices."
  - "Note, we used UNM's network to perform scans with 6Gen before the IPv6 scanning infrastructure was set up at Berkeley"

CVE-2018-19298

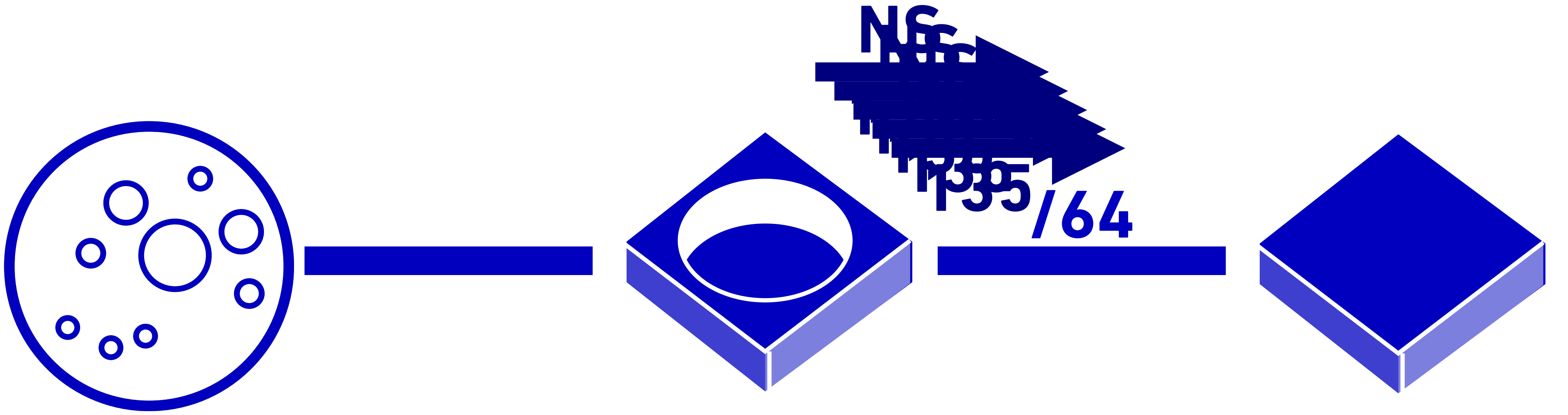
Neighbour Solicitation



Neighbour Advertisement



Neighbour Solicitations



NS

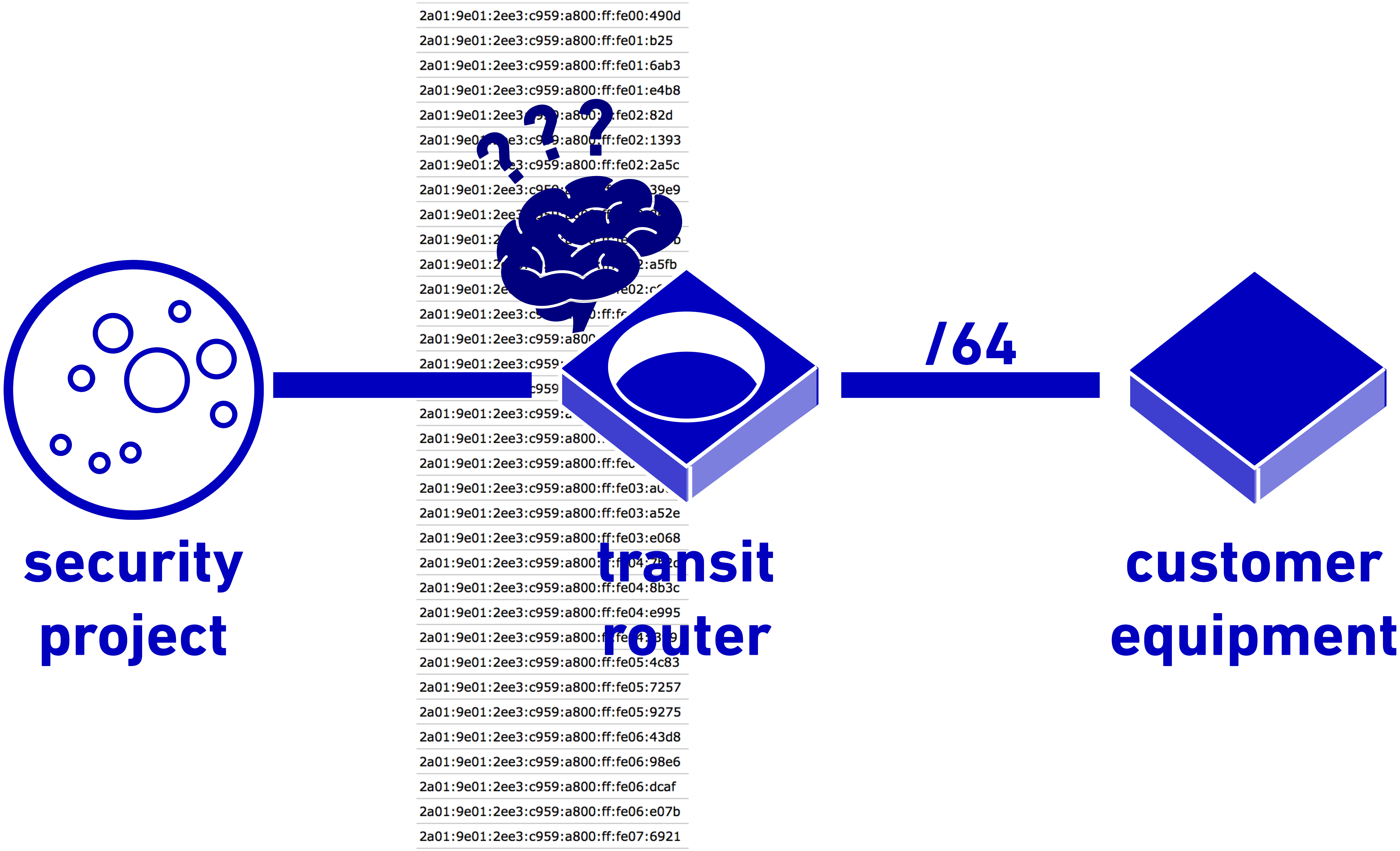
135/64

security project

transit router

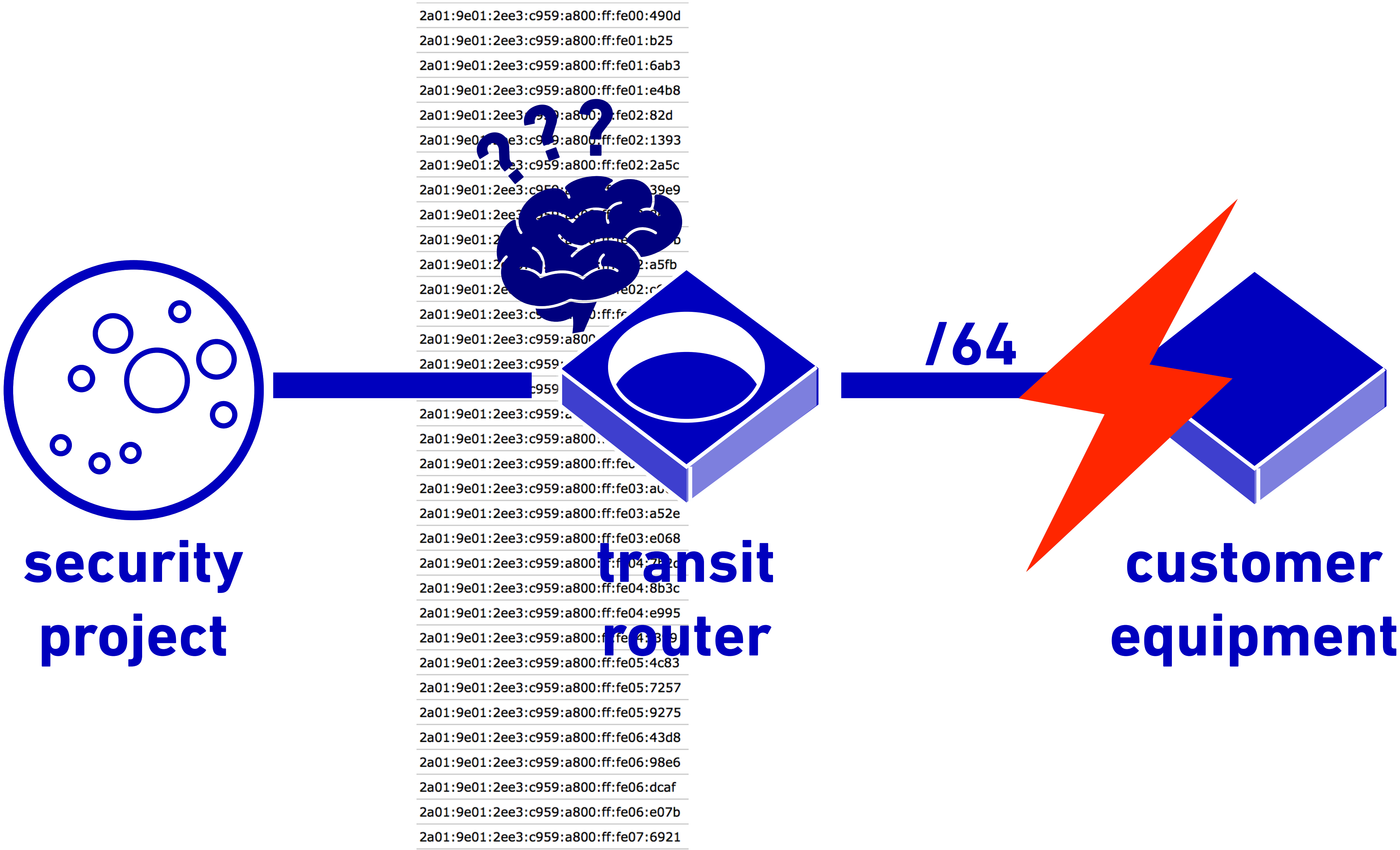
customer equipment

Oldest Entry is Dropped



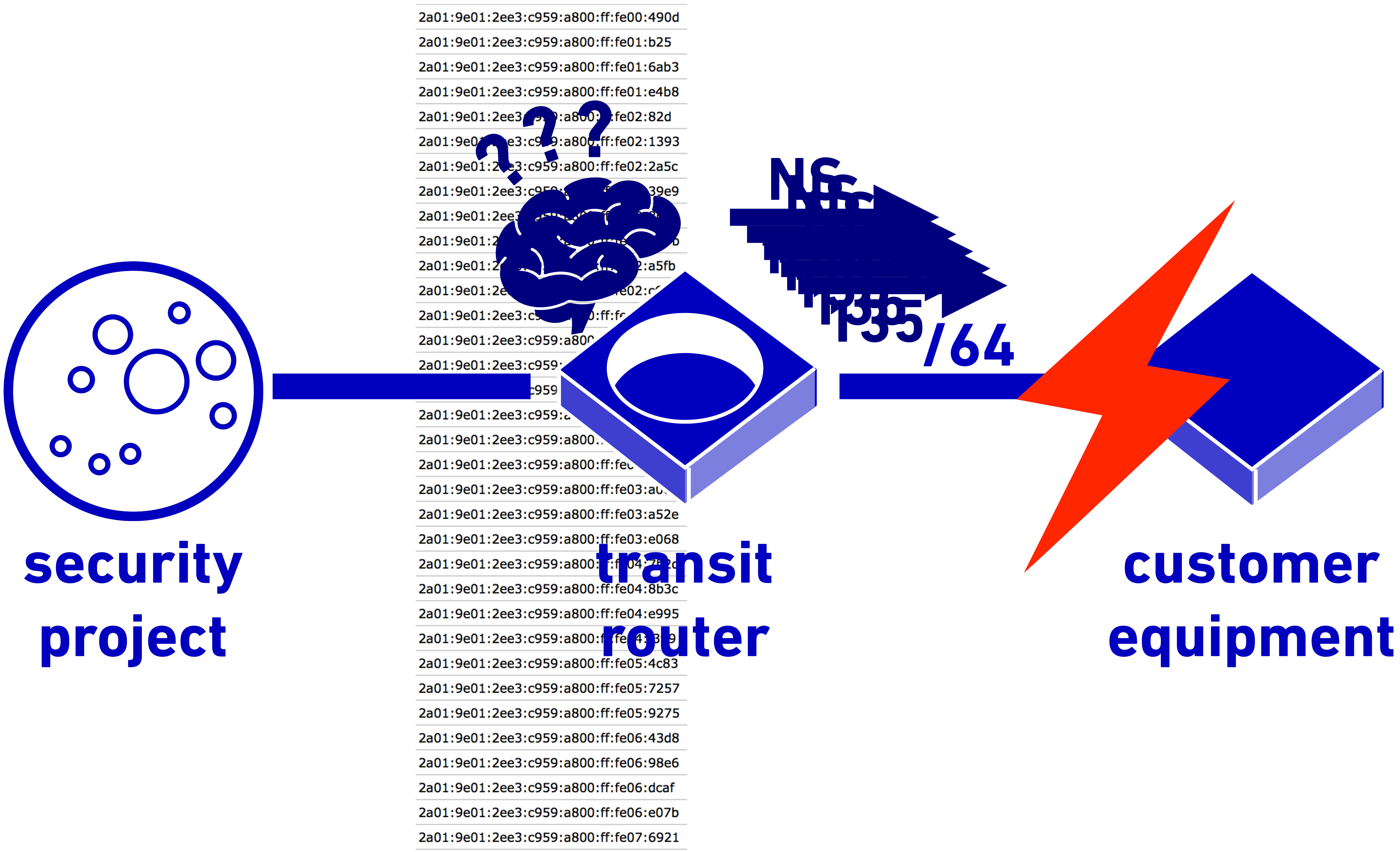
```
2a01:9e01:2ee3:c959:a800:ff:fe00:490d
2a01:9e01:2ee3:c959:a800:ff:fe01:b25
2a01:9e01:2ee3:c959:a800:ff:fe01:6ab3
2a01:9e01:2ee3:c959:a800:ff:fe01:e4b8
2a01:9e01:2ee3  9:a800: :fe02:82d
2a01:9e0  e3:c9 9:a800 ff:fe02:1393
2a01:9e01:2 e3:c959:a800:ff:fe02:2a5c
2a01:9e01:2ee3:c                  39e9
2a01:9e01:2ee3
2a01:9e01:2                          b
2a01:9e01:2                      2:a5fb
2a01:9e01:2e               e02:c
2a01:9e01:2ee3:c          0:ff:fc
2a01:9e01:2ee3:c959:a800
2a01:9e01:2ee3:c959:
              c959
2a01:9e01:2ee3:c959:a
2a01:9e01:2ee3:c959:a800:
2a01:9e01:2ee3:c959:a800:ff:fe
2a01:9e01:2ee3:c959:a800:ff:fe03:a
2a01:9e01:2ee3:c959:a800:ff:fe03:a52e
2a01:9e01:2ee3:c959:a800:ff:fe03:e068
2a01:9e01:2ee3:c959:a800: f:f 04:7  2c
2a01:9e01:2ee3:c959:a800:ff:fe04:8b3c
2a01:9e01:2ee3:c959:a800:ff:fe04:e995
2a01:9e01:2ee3:c959:a800:f fe 4: 3 9
2a01:9e01:2ee3:c959:a800:ff:fe05:4c83
2a01:9e01:2ee3:c959:a800:ff:fe05:7257
2a01:9e01:2ee3:c959:a800:ff:fe05:9275
2a01:9e01:2ee3:c959:a800:ff:fe06:43d8
2a01:9e01:2ee3:c959:a800:ff:fe06:98e6
2a01:9e01:2ee3:c959:a800:ff:fe06:dcaf
2a01:9e01:2ee3:c959:a800:ff:fe06:e07b
2a01:9e01:2ee3:c959:a800:ff:fe07:6921
```

Loss of Connectivity...



```
2a01:9e01:2ee3:c959:a800:ff:fe00:490d
2a01:9e01:2ee3:c959:a800:ff:fe01:b25
2a01:9e01:2ee3:c959:a800:ff:fe01:6ab3
2a01:9e01:2ee3:c959:a800:ff:fe01:e4b8
2a01:9e01:2ee3[illegible]9:a800:[illegible]:fe02:82d
2a01:9e0[illegible]e3:c9[illegible]9:a800:ff:fe02:1393
2a01:9e01:2[illegible]3:c959:a800:ff:fe02:2a5c
2a01:9e01:2ee3:c[illegible]39e9
2a01:9e01:2ee3[illegible]
2a01:9e01:2[illegible]b
2a01:9e01:2[illegible]2:a5fb
2a01:9e01:2e[illegible]e02:c[illegible]
2a01:9e01:2ee3:c[illegible]0:ff:f[illegible]
2a01:9e01:2ee3:c959:a80[illegible]
2a01:9e01:2ee3:c959:[illegible]
[illegible]c959[illegible]
2a01:9e01:2ee3:c959:a[illegible]
2a01:9e01:2ee3:c959:a800:[illegible]
2a01:9e01:2ee3:c959:a800:ff:fe[illegible]
2a01:9e01:2ee3:c959:a800:ff:fe03:a[illegible]
2a01:9e01:2ee3:c959:a800:ff:fe03:a52e
2a01:9e01:2ee3:c959:a800:ff:fe03:e068
2a01:9e01:2ee3:c959:a800:[illegible]f:f[illegible]04:7[illegible]2c
2a01:9e01:2ee3:c959:a800:ff:fe04:8b3c
2a01:9e01:2ee3:c959:a800:ff:fe04:e995
2a01:9e01:2ee3:c959:a800:f[illegible]fe[illegible]4[illegible]3[illegible]9
2a01:9e01:2ee3:c959:a800:ff:fe05:4c83
2a01:9e01:2ee3:c959:a800:ff:fe05:7257
2a01:9e01:2ee3:c959:a800:ff:fe05:9275
2a01:9e01:2ee3:c959:a800:ff:fe06:43d8
2a01:9e01:2ee3:c959:a800:ff:fe06:98e6
2a01:9e01:2ee3:c959:a800:ff:fe06:dcaf
2a01:9e01:2ee3:c959:a800:ff:fe06:e07b
2a01:9e01:2ee3:c959:a800:ff:fe07:6921
```

...until next time!



```
2a01:9e01:2ee3:c959:a800:ff:fe00:490d
2a01:9e01:2ee3:c959:a800:ff:fe01:b25
2a01:9e01:2ee3:c959:a800:ff:fe01:6ab3
2a01:9e01:2ee3:c959:a800:ff:fe01:e4b8
2a01:9e01:2ee3:c959:a800:ff:fe02:82d
2a01:9e01:2ee3:c959:a800:ff:fe02:1393
2a01:9e01:2ee3:c959:a800:ff:fe02:2a5c
2a01:9e01:2ee3:c9                39e9
2a01:9e01:2ee3
2a01:9e01:2                         b
2a01:9e01:2                     2:a5fb
2a01:9e01:2e                  e02:c
2a01:9e01:2ee3:c         0:ff:f
2a01:9e01:2ee3:c959:a800
2a01:9e01:2ee3:c959:
              c959
2a01:9e01:2ee3:c959:a
2a01:9e01:2ee3:c959:a800:
2a01:9e01:2ee3:c959:a800:ff:fe
2a01:9e01:2ee3:c959:a800:ff:fe03:a
2a01:9e01:2ee3:c959:a800:ff:fe03:a52e
2a01:9e01:2ee3:c959:a800:ff:fe03:e068
2a01:9e01:2ee3:c959:a800:
2a01:9e01:2ee3:c959:a800:ff:fe04:8b3c
2a01:9e01:2ee3:c959:a800:ff:fe04:e995
2a01:9e01:2ee3:c959:a800:f
2a01:9e01:2ee3:c959:a800:ff:fe05:4c83
2a01:9e01:2ee3:c959:a800:ff:fe05:7257
2a01:9e01:2ee3:c959:a800:ff:fe05:9275
2a01:9e01:2ee3:c959:a800:ff:fe06:43d8
2a01:9e01:2ee3:c959:a800:ff:fe06:98e6
2a01:9e01:2ee3:c959:a800:ff:fe06:dcaf
2a01:9e01:2ee3:c959:a800:ff:fe06:e07b
2a01:9e01:2ee3:c959:a800:ff:fe07:6921
```

CVE-2018-19298: IPv6 NEIGHBOUR EXHAUSTION (MIKROTIK ROUTEROS v6)

CVE-2018-19298 Timeline

- 2018-04-08 — reported to vendor
- 2018-06-29 — "not yet fixed"
- 2018-11-15 — CVE assigned
- 2019-01-15 — "can not give you any ETA for the fix"
- 2019-02-14 — discussion at NetMcr
- 2019-03-31 — lots of stuff happens
- 2019-04-09 — wider disclosure

Nothing to See Here

- CVE-2018-19298 is not that new, fundamentally
- Most vendors have fixes for NDP exhaustion
- Could just not use /64 subnets
  - ...except for Android not having DHCPv6
  - ...so you rely on IPv6 RA
  - ...and so you probably have /64 subnets (RFC7421)
- But at least not having /64 linknets would save core routers from short-lived loss of adjacency (RFC6164)

“simplistic implementations of [ND] can be vulnerable to deliberate or accidental [DoS], whereby they attempt to perform address resolution for large numbers of unassigned [...]”

– *RFC6583, Operational Neighbor Discovery Problems, 2012*

Conclusion

- IPv6 support in RouterOS needs some love:
  - >6 year old ops-experience RFCs unaddressed
  - MikroTik RouterOS v6 is (very patched) Linux 3.3.5

THE END!

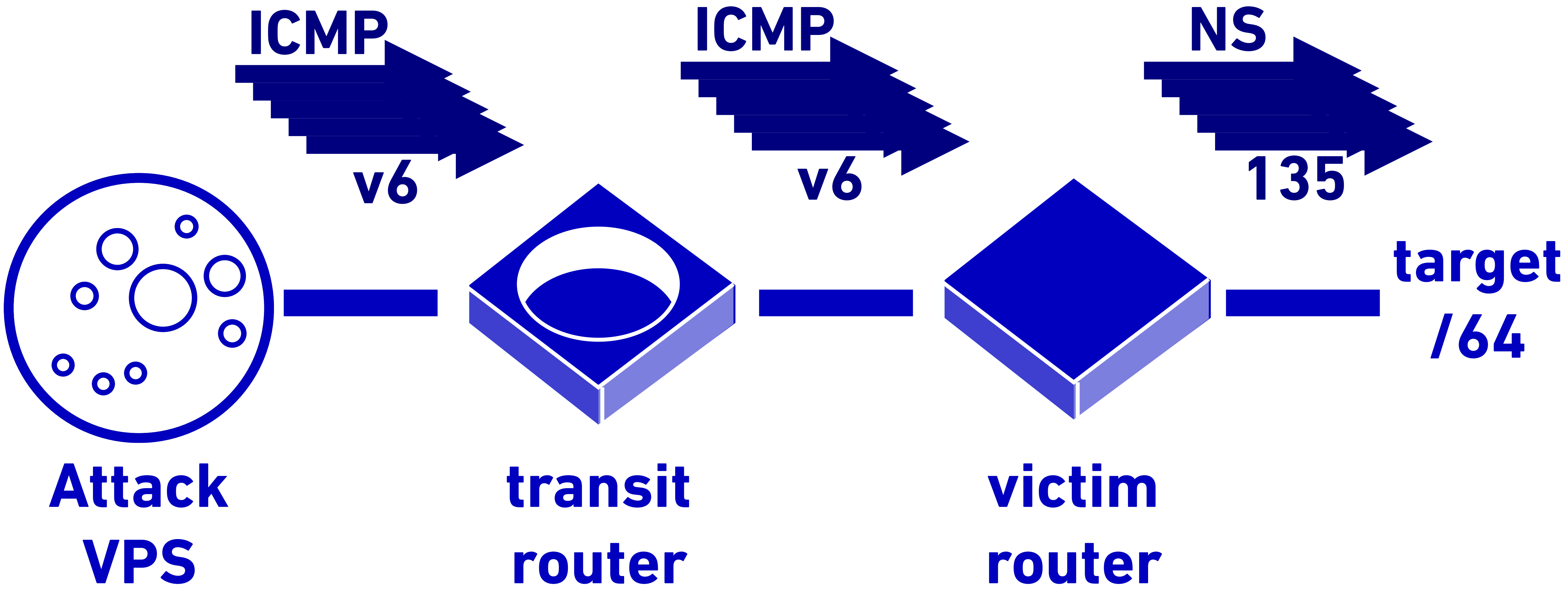
“...only it wasn't the end...”

– Narrator

Voyage of Discovery

- While trying to test IPv6 ND exhaustion...
- Using a VPS and some "l33t t00lz"...
- Aimed at a /64 subnet behind a MikroTik hAP...

IPv6 Neighbour Discovery



Once is an anecdote...

- Built a little lab at home with some spares
- Used a Raspberry Pi to attack RouterOS boxes
- Crash and reboot every time
- Bad times are just one "apt-get install" away

CVE-2018-19299

CVE-2018-19299 Timeline

- 2018-04-16 — reported to vendor
- 2018-04-17 — [this is ND exhaustion]
- 2018-04-17 — no, it isn't
- 2018-04-17 — [yes it is]
- 2018-04-17 — no, it isn't
- 2018-04-17 — [it is! you used an NDP exhaust tool!]
- 2018-04-17 — ...no! I'm begging you! It isn't NDP!

CVE-2018-19299 Timeline

- 2018-04-17 — "Sorry for confusion, dst is two hops away. We will test this scenario."

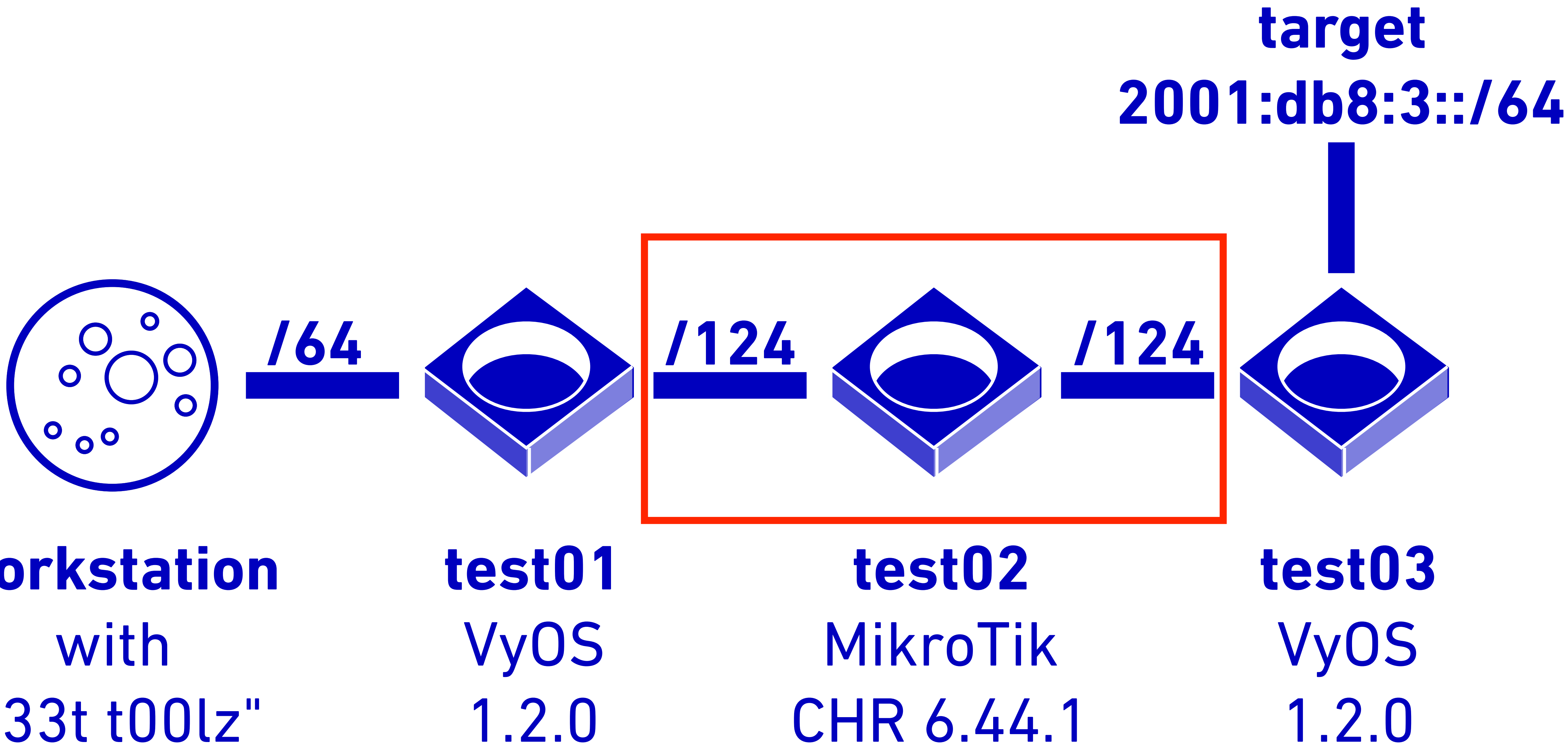
...

CVE-2018-19299 Timeline

- 2018-04-19 — "forwarding of ipv6 traffic eats all the memory"

YES, REALLY.

Simple 4-VPS Lab



Settings on CHR

- /ipv6 settings set accept-redirects=no accept-router-advertisements=no

for safety

- /ipv6 route
  add distance=1 type=unreachable

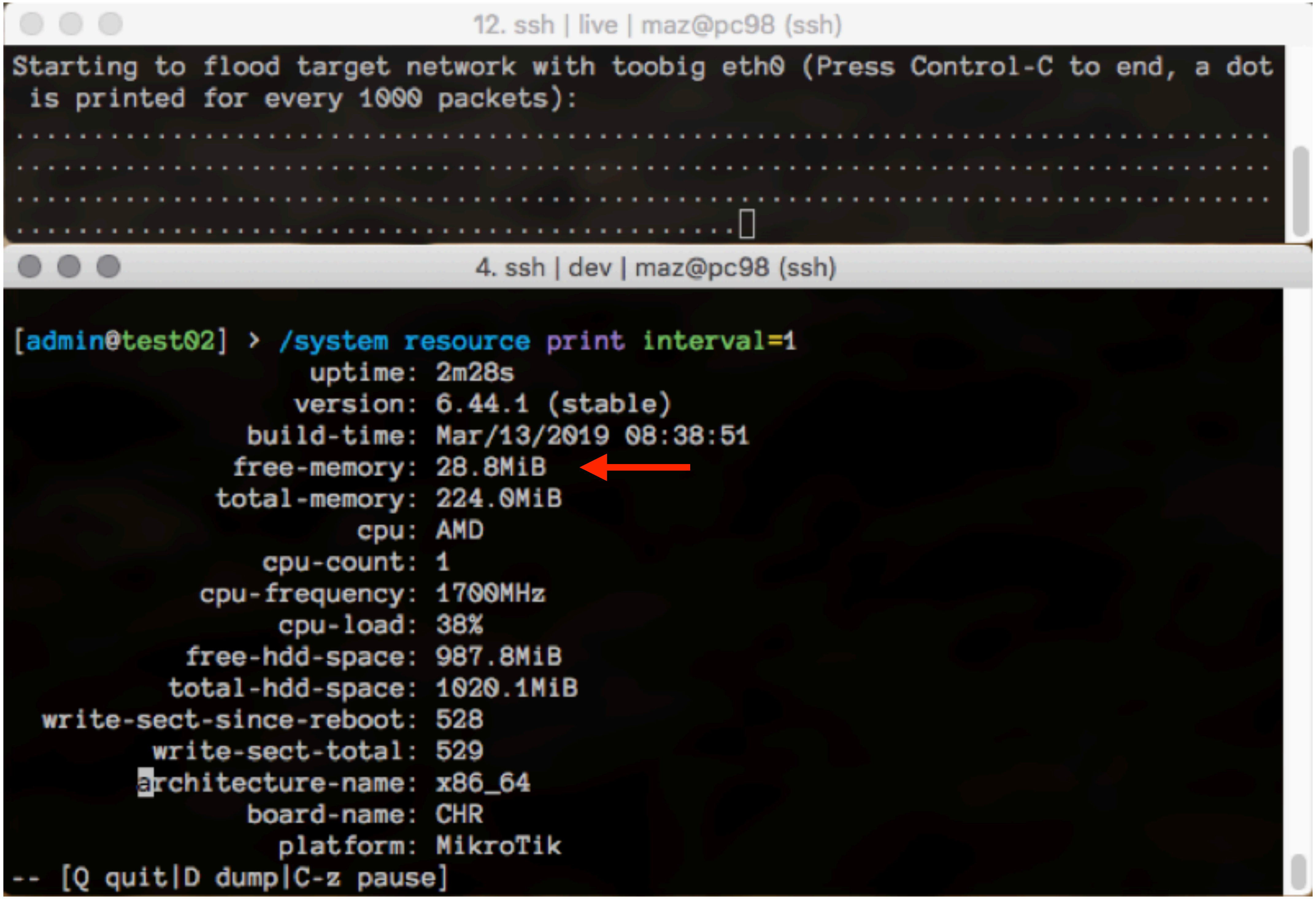
containment

- /ipv6 firewall raw
  add action=notrack chain=prerouting

not conntrack

- /ipv6 route
  add distance=1 dst-address=2001:db8:3::/64
  gateway=2001:db8:2::3

static routes

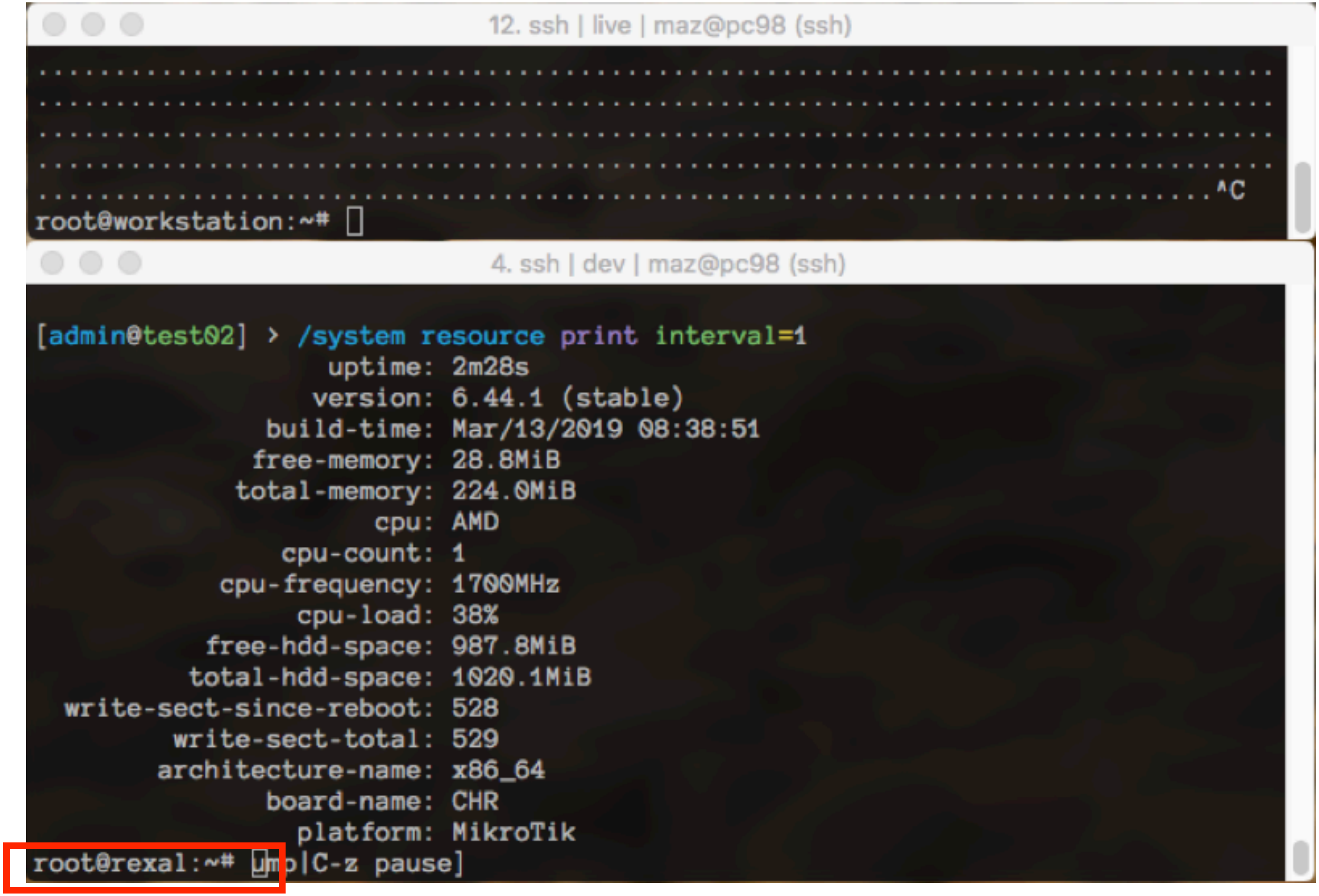


12. ssh | live | maz@pc98 (ssh)

```
Starting to flood target network with toobig eth0 (Press Control-C to end, a dot
 is printed for every 1000 packets):
................................................................................
................................................................................
................................................................................
..............................................
```

4. ssh | dev | maz@pc98 (ssh)

```
[admin@test02] > /system resource print interval=1
                   uptime: 2m28s
                  version: 6.44.1 (stable)
               build-time: Mar/13/2019 08:38:51
              free-memory: 28.8MiB
             total-memory: 224.0MiB
                      cpu: AMD
                cpu-count: 1
            cpu-frequency: 1700MHz
                 cpu-load: 38%
           free-hdd-space: 987.8MiB
          total-hdd-space: 1020.1MiB
  write-sect-since-reboot: 528
         write-sect-total: 529
        architecture-name: x86_64
               board-name: CHR
                 platform: MikroTik
-- [Q quit|D dump|C-z pause]
```


12. ssh | live | maz@pc98 (ssh)

```
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...........................................................................^C
root@workstation:~# 
```

4. ssh | dev | maz@pc98 (ssh)

```
[admin@test02] > /system resource print interval=1
                   uptime: 2m28s
                  version: 6.44.1 (stable)
               build-time: Mar/13/2019 08:38:51
              free-memory: 28.8MiB
             total-memory: 224.0MiB
                      cpu: AMD
                cpu-count: 1
            cpu-frequency: 1700MHz
                 cpu-load: 38%
           free-hdd-space: 987.8MiB
          total-hdd-space: 1020.1MiB
  write-sect-since-reboot: 528
         write-sect-total: 529
        architecture-name: x86_64
               board-name: CHR
                 platform: MikroTik
root@rexal:~# ump|C-z pause]
```

CHR VPS crashed

```
mar/17/2019 20:12:42
system,error,critical router was
rebooted without proper shutdown
```

"/log print" from test02

MITIGATIONS

What about firewalling?

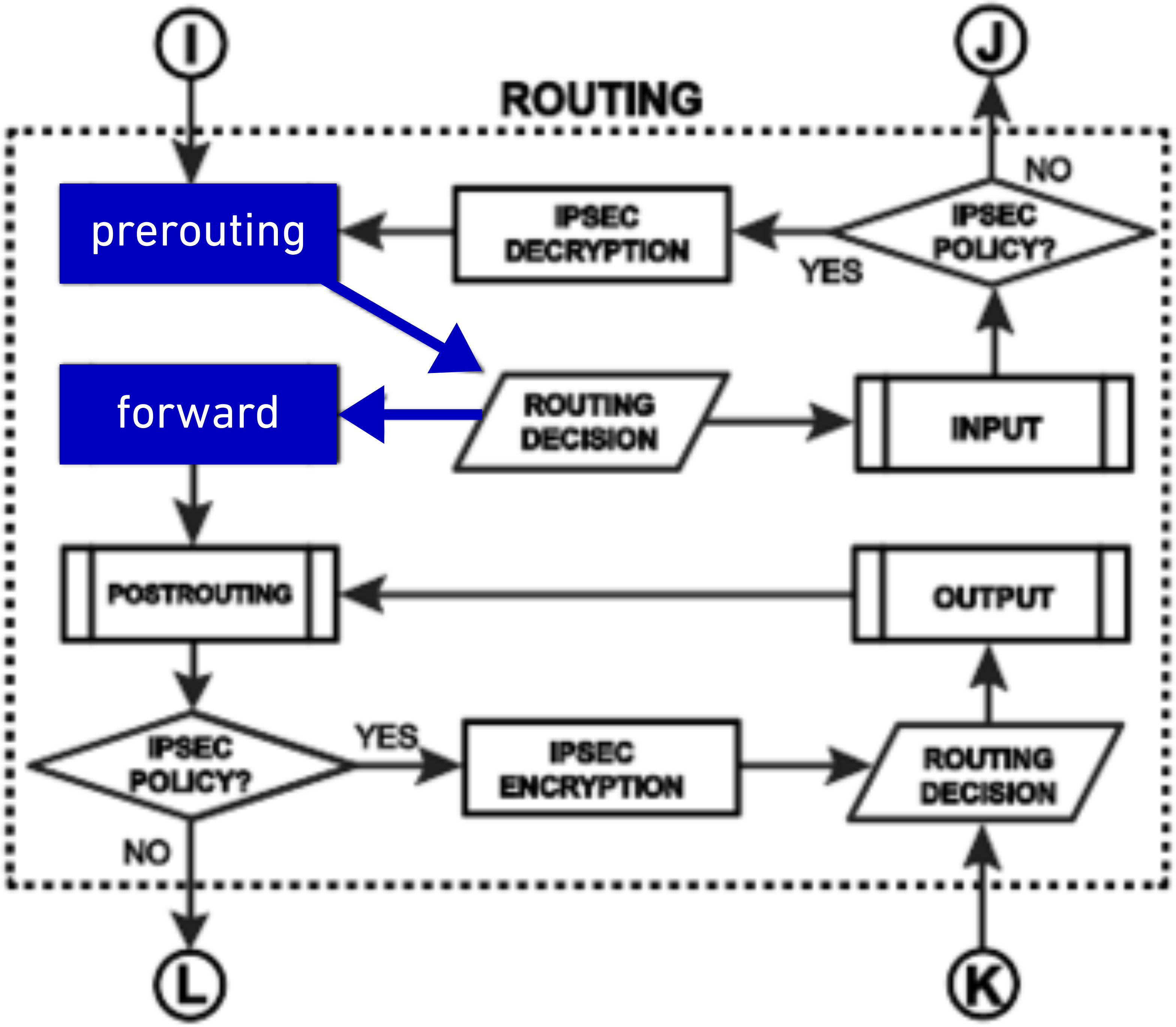
- /ipv6 firewall filter add chain=forward action=drop
  - even "drop all" in forward chain is **vulnerable**
- /ipv6 firewall raw add chain=prerouting action=drop
  - must "drop" in raw table **before routing** to be **safe**
- What about connection-state=established...?
  - stateful is in "filter chain=forward" — vulnerable
  - **default "MikroTik as CPE" config vulnerable**

What about firewalling?

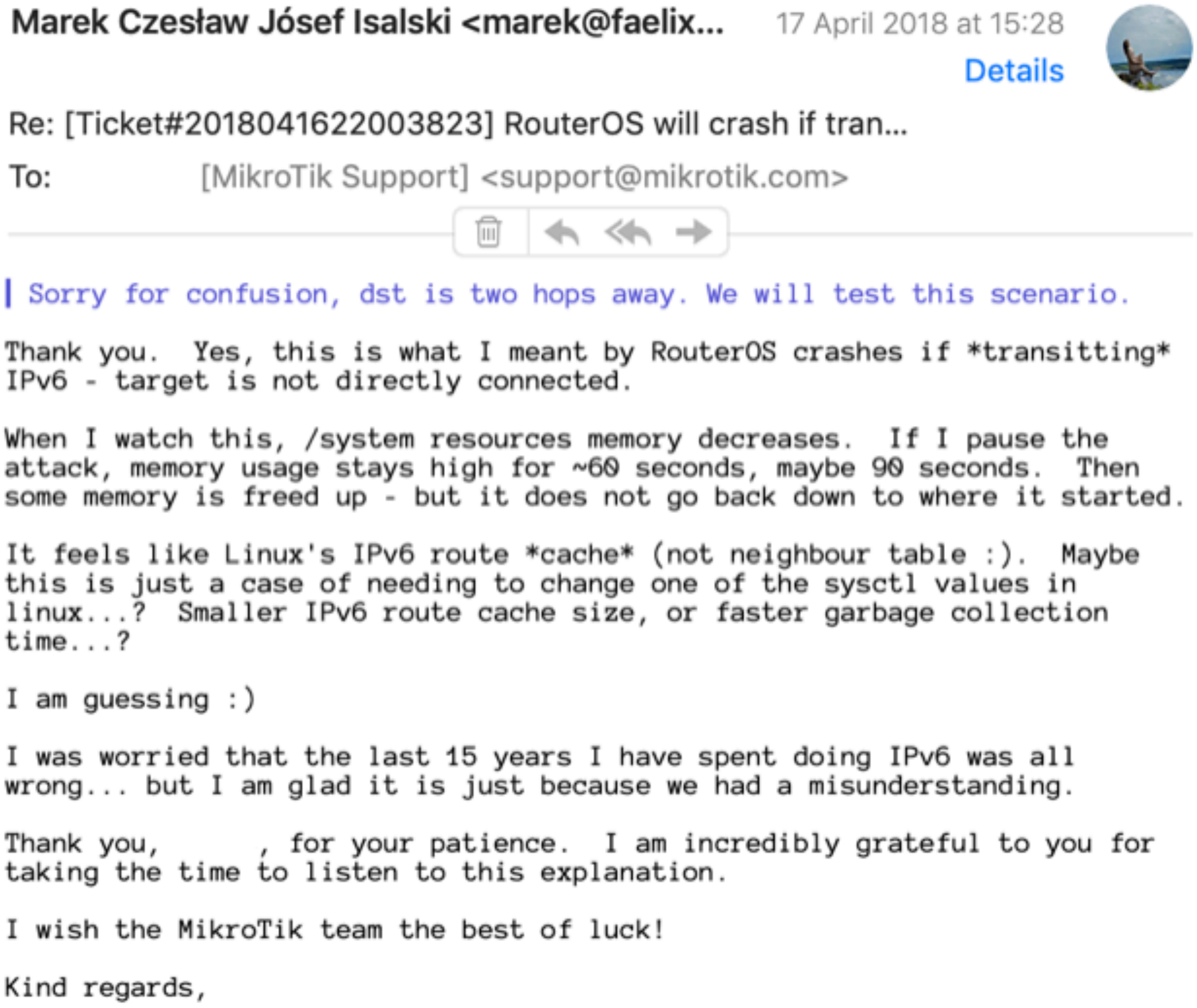
- /ipv6 firewall filter add chain=forward action=drop
  - even "d ll" i f **erable**
- /ipv6 n=drop
  - **safe**
- Wha
  - stateful is in "filte ward" — vulnerable
  - **default "MikroTik as CPE" config vulnerable**

Given someone's IPv6 address,
an attacker can crash MikroTiks
between the attacker and the victim...
including victim's firewalling CPE!

Where does it go wrong?



The hunch...



Marek Czesław Jósef Isalski <marek@faelix... 17 April 2018 at 15:28

Re: [Ticket#2018041622003823] RouterOS will crash if tran...

To: [MikroTik Support] <support@mikrotik.com>

> Sorry for confusion, dst is two hops away. We will test this scenario.

Thank you. Yes, this is what I meant by RouterOS crashes if *transitting*
IPv6 - target is not directly connected.

When I watch this, /system resources memory decreases. If I pause the
attack, memory usage stays high for ~60 seconds, maybe 90 seconds. Then
some memory is freed up - but it does not go back down to where it started.

It feels like Linux's IPv6 route *cache* (not neighbour table :). Maybe
this is just a case of needing to change one of the sysctl values in
linux...? Smaller IPv6 route cache size, or faster garbage collection
time...?

I am guessing :)

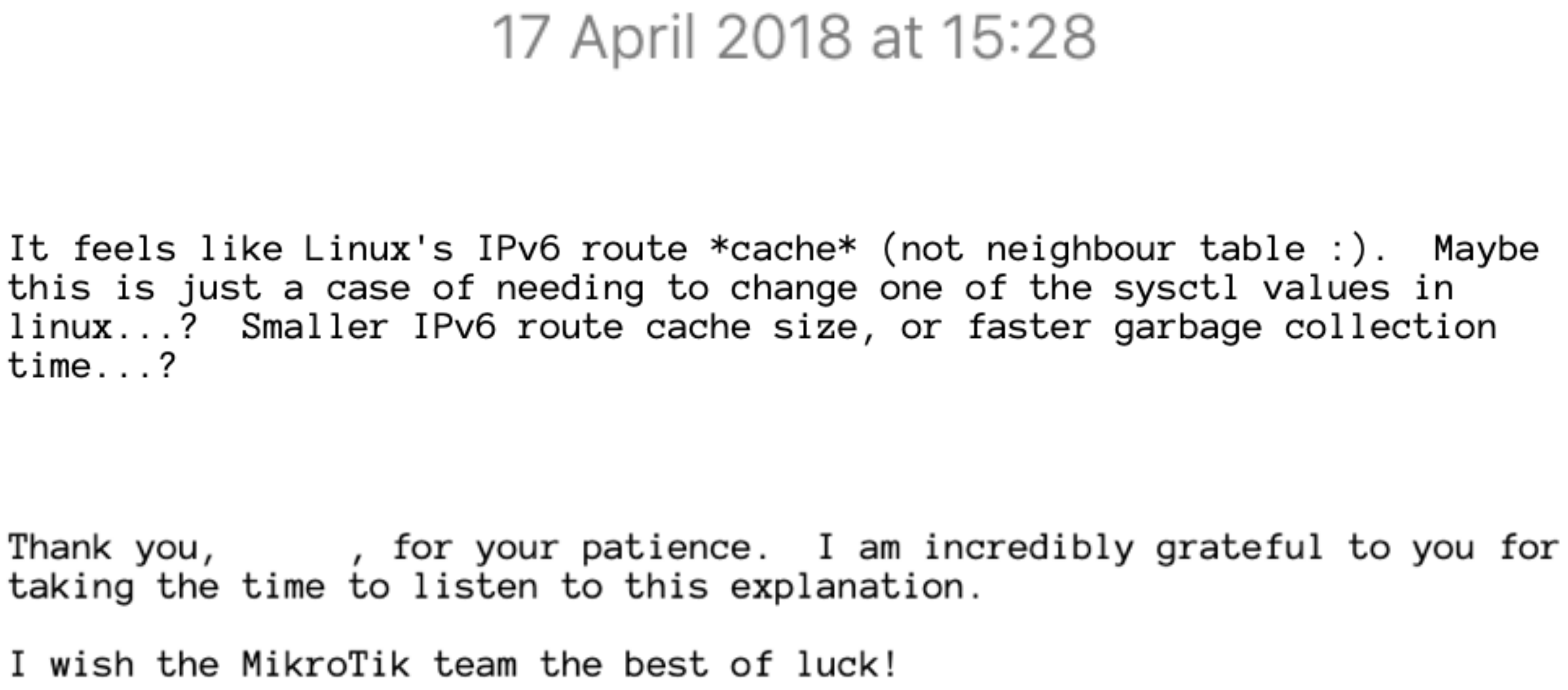
I was worried that the last 15 years I have spent doing IPv6 was all
wrong... but I am glad it is just because we had a misunderstanding.

Thank you,   , for your patience. I am incredibly grateful to you for
taking the time to listen to this explanation.

I wish the MikroTik team the best of luck!

Kind regards,

The hunch...



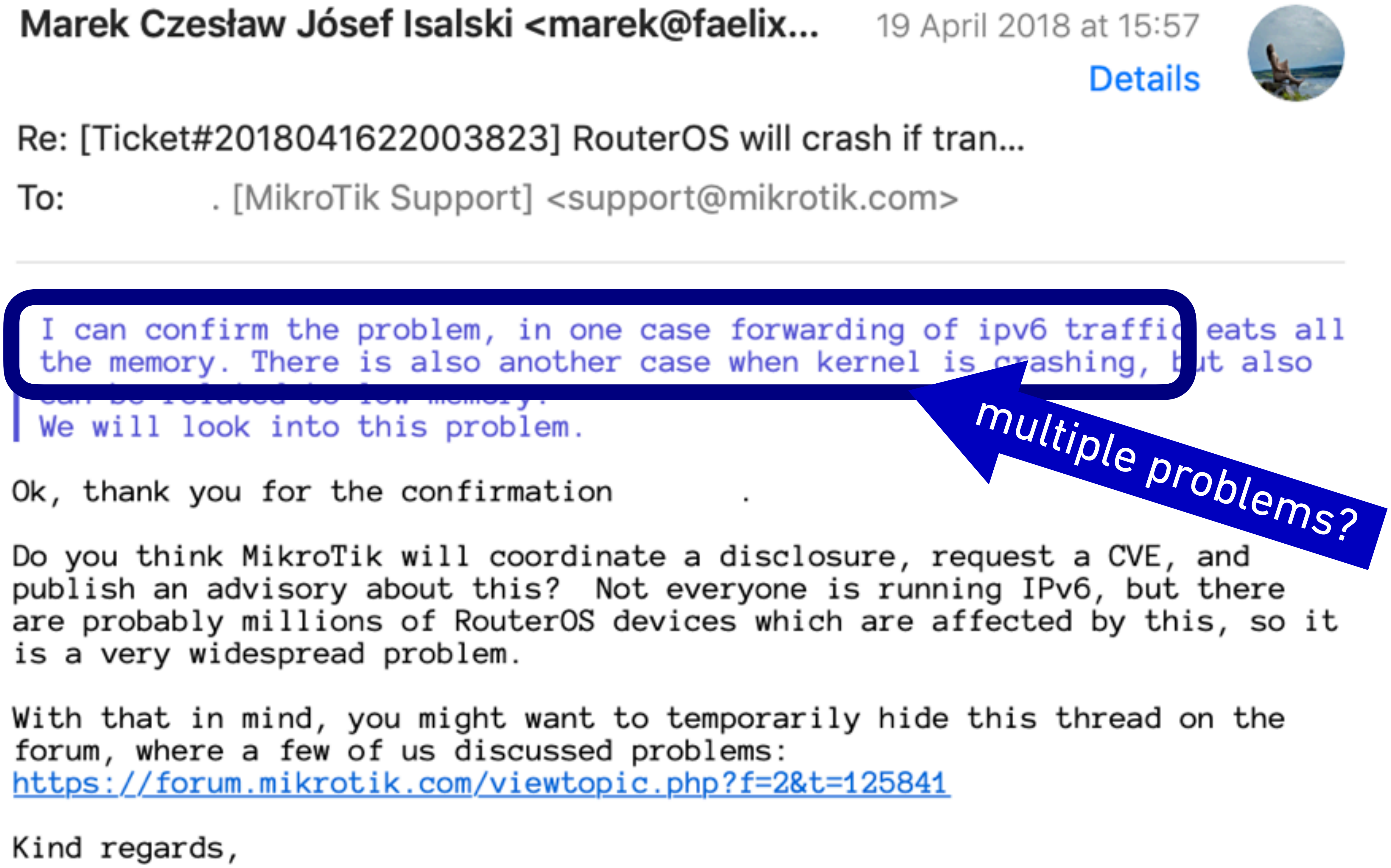
17 April 2018 at 15:28

It feels like Linux's IPv6 route *cache* (not neighbour table :). Maybe this is just a case of needing to change one of the sysctl values in linux...? Smaller IPv6 route cache size, or faster garbage collection time...?

Thank you, , for your patience. I am incredibly grateful to you for taking the time to listen to this explanation.

I wish the MikroTik team the best of luck!

The worries...



Marek Czesław Jósef Isalski <marek@faelix... 19 April 2018 at 15:57

Details

Re: [Ticket#2018041622003823] RouterOS will crash if tran...

To: . [MikroTik Support] <support@mikrotik.com>

> I can confirm the problem, in one case forwarding of ipv6 traffic eats all the memory. There is also another case when kernel is crashing, but also can be related to low memory.
> We will look into this problem.

Ok, thank you for the confirmation .

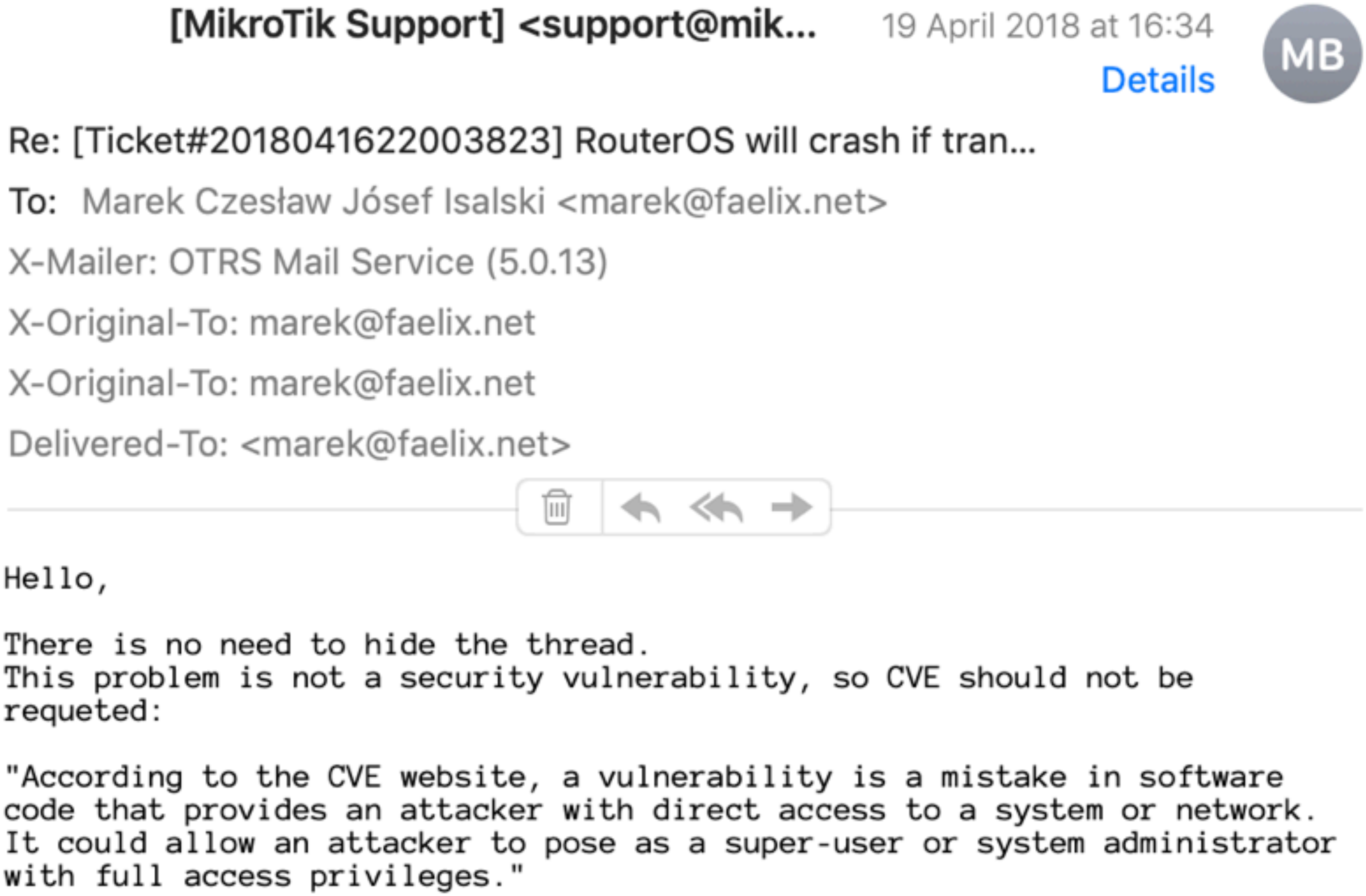
Do you think MikroTik will coordinate a disclosure, request a CVE, and publish an advisory about this? Not everyone is running IPv6, but there are probably millions of RouterOS devices which are affected by this, so it is a very widespread problem.

With that in mind, you might want to temporarily hide this thread on the forum, where a few of us discussed problems:
https://forum.mikrotik.com/viewtopic.php?f=2&t=125841

Kind regards,

multiple problems?

The response…



[MikroTik Support] <support@mik… 19 April 2018 at 16:34

Re: [Ticket#2018041622003823] RouterOS will crash if tran…

To: Marek Czesław Jósef Isalski <marek@faelix.net>

X-Mailer: OTRS Mail Service (5.0.13)

X-Original-To: marek@faelix.net

X-Original-To: marek@faelix.net

Delivered-To: <marek@faelix.net>

Hello,

There is no need to hide the thread.
This problem is not a security vulnerability, so CVE should not be requeted:

"According to the CVE website, a vulnerability is a mistake in software code that provides an attacker with direct access to a system or network. It could allow an attacker to pose as a super-user or system administrator with full access privileges."

CVE-2018-19299 Timeline

- 2018-04-19 — "ipv6 traffic eats all the memory"
- 2018-04-19 — "not a security vulnerability"
- 2018-06-29 — "not yet fixed"
- 2018-10-10 — "we accept this as a bug, but we would not call it a vulnerability"

NetMcr opinion

NetMcr 2018-11-08

- Asked industry peers who attended:
  - If you had a remote unauthenticated crash
  - ...and firewall/etc doesn't appear to help
  - ...and vendor says "not a vulnerability"
  - ...then what would you do?

NetMcr 2018-11-08

- Resulting plan:
  - Get CVEs anyway
  - Talk to NCSC
  - Announce on CISP, etc
  - Keep trying responsible disclosure with vendor
  - Start to inform CERTs
  - Prepare for move towards full disclosure

CVE-2018-19299 Timeline

- 2018-04-19 — "ipv6 traffic eats all the memory"
- 2018-04-19 — "not a security vulnerability"
- 2018-06-29 — "not yet fixed"
- 2018-10-10 — "we accept this as a bug, but we would not call it a vulnerability"
- 2018-11-15 — "with our development team"
- 2019-01-15 — "can not give you any ETA for the fix"

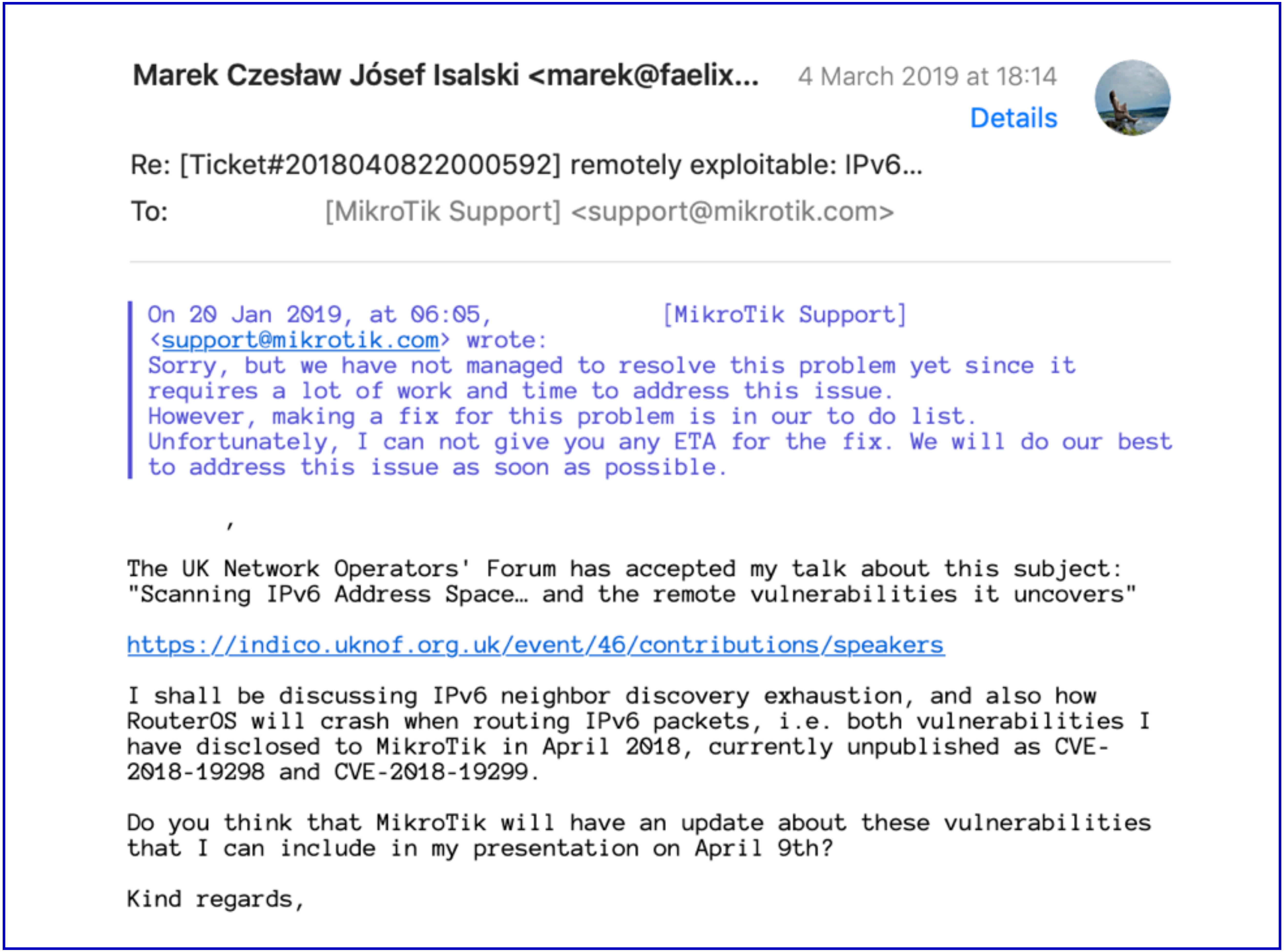
NetMcr discuss

NetMcr 2019-02-14

- Explained IPv6 NDP exhaustion
    - Spoke about how this is CVE-2018-19298
- Presented initial version of first half of this talk
    - Did not give details of exploit of CVE-2018-19299
- Asked the audience, "What next?"
    - Continue to aggro the vendor?
    - Publish full details in MITRE?
    - Make noise in the technology press?

NetMcr 2019-02-14

- Decided plan for way forward:
  - Notify vendor of publication date (2019-04-09)
  - Get word out (notify NCSC, CISP, CERTs, etc)
  - Prepare for move to full disclosure



Marek Czesław Jósef Isalski <marek@faelix... 4 March 2019 at 18:14

Re: [Ticket#2018040822000592] remotely exploitable: IPv6...

To: [MikroTik Support] <support@mikrotik.com>

> On 20 Jan 2019, at 06:05, [MikroTik Support]
> <support@mikrotik.com> wrote:
> Sorry, but we have not managed to resolve this problem yet since it requires a lot of work and time to address this issue.
> However, making a fix for this problem is in our to do list.
> Unfortunately, I can not give you any ETA for the fix. We will do our best to address this issue as soon as possible.

,

The UK Network Operators' Forum has accepted my talk about this subject: "Scanning IPv6 Address Space… and the remote vulnerabilities it uncovers"

https://indico.uknof.org.uk/event/46/contributions/speakers

I shall be discussing IPv6 neighbor discovery exhaustion, and also how RouterOS will crash when routing IPv6 packets, i.e. both vulnerabilities I have disclosed to MikroTik in April 2018, currently unpublished as CVE-2018-19298 and CVE-2018-19299.

Do you think that MikroTik will have an update about these vulnerabilities that I can include in my presentation on April 9th?

Kind regards,

"At the moment there is no news, but I will definitely let you know as soon as there will be an update regarding this matter."

– email from MikroTik support, 2019-03-11

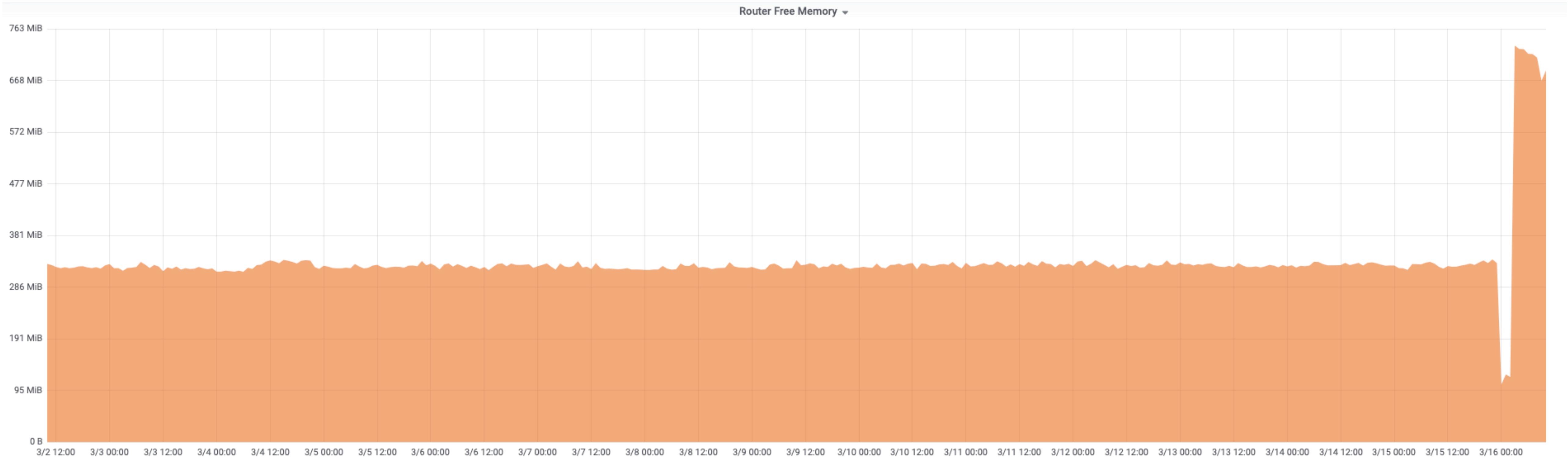
CVE-2018-19299 Timeline

- 2018-04-19 — "ipv6 traffic eats all the memory"
- 2018-04-19 — "not a security vulnerability"
- 2018-06-29 — "not yet fixed"
- 2018-10-10 — "we accept this as a bug, but we would not call it a vulnerability"
- 2018-11-15 — "with our development team"
- 2019-01-15 — "can not give you any ETA for the fix"
- 2019-03-11 — "there is no news"

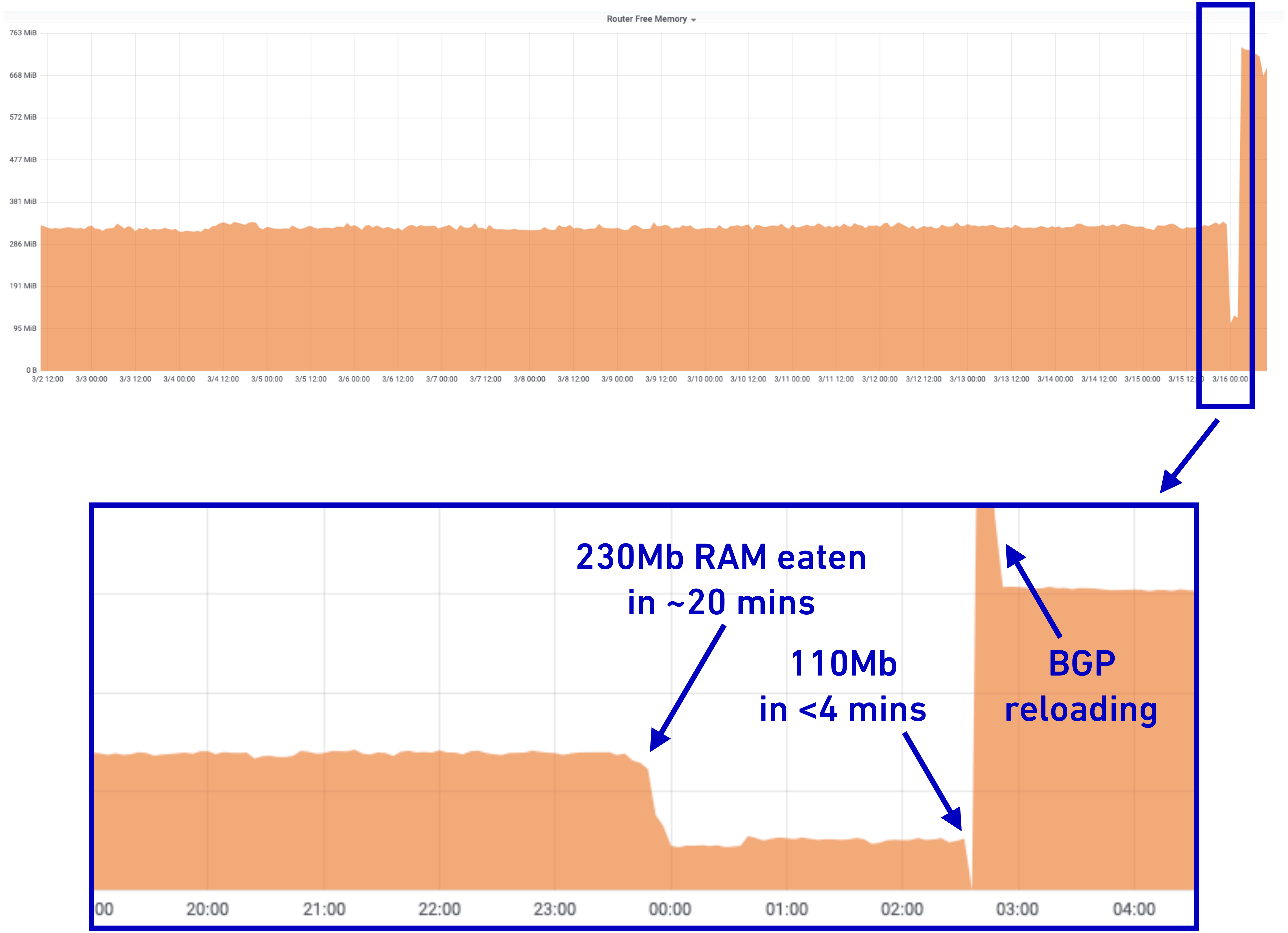
MEANWHILE...

CVE-2018-19299 in Wild?

- mar/09/2019 06:58:04 system,error,critical **router was rebooted** without proper shutdown, probably kernel failure
- mar/09/2019 06:58:04 system,error,critical **kernel failure** in previous boot
- mar/09/2019 06:58:04 system,error,critical **out of memory** condition was detected
- mar/10/2019 16:56:18 system,error,critical **router was rebooted** without proper shutdown, probably kernel failure
- mar/10/2019 16:56:18 system,error,critical **kernel failure** in previous boot
- mar/10/2019 16:56:18 system,error,critical **out of memory** condition was detected



- **production** MikroTik router at **AS41495 edge**
- graph of **free memory** vs **time**
- first two weeks of March 2019
- scraped every 30 seconds by API into Prometheus

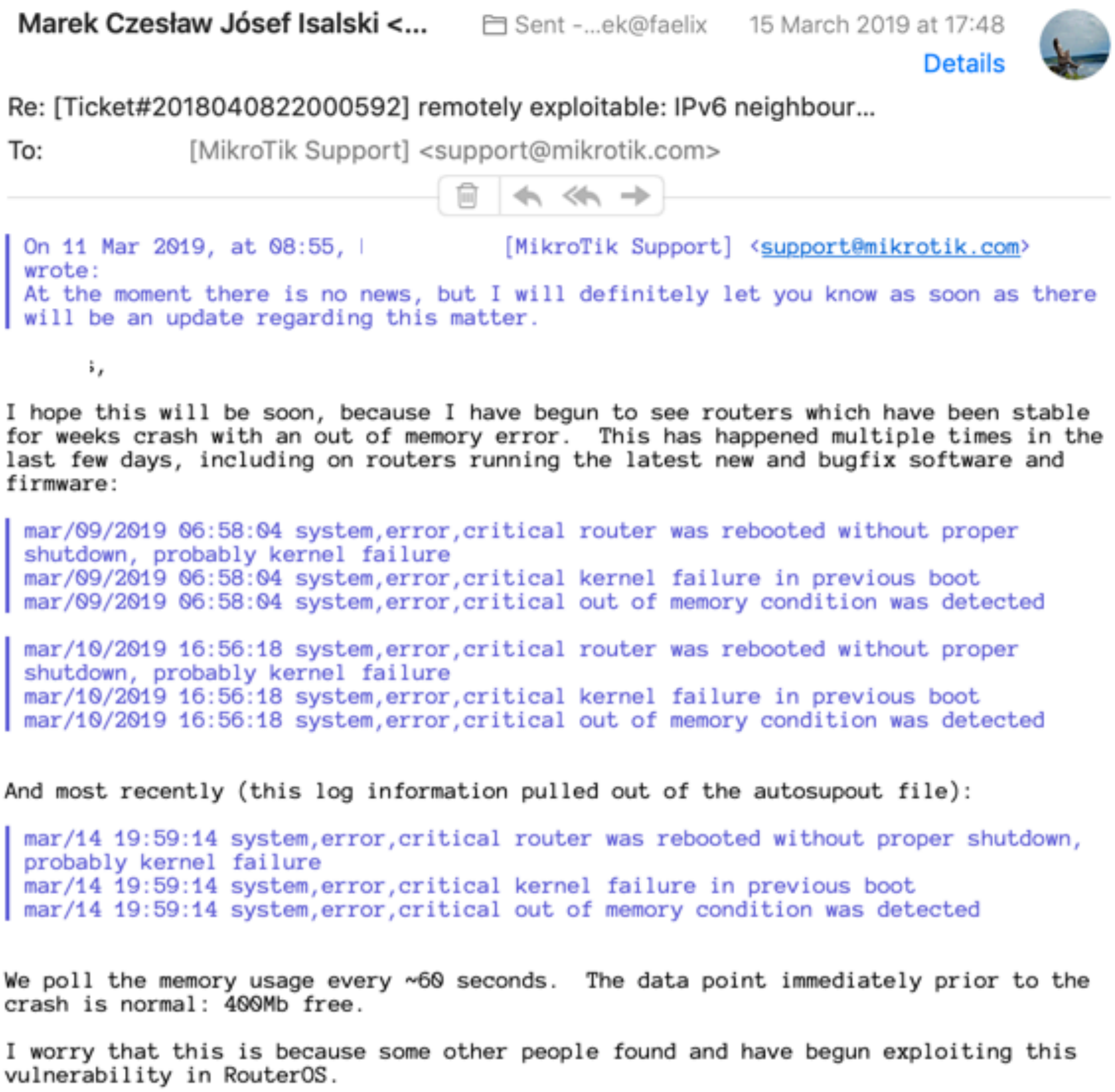


230Mb RAM eaten
in ~20 mins

110Mb
in <4 mins

BGP
reloading

Notify vendor of exploits?



Re: [Ticket#2018040822000592] remotely exploitable: IPv6 neighbour...

To: [MikroTik Support] <support@mikrotik.com>

> On 11 Mar 2019, at 08:55, [MikroTik Support] <support@mikrotik.com> wrote:
> At the moment there is no news, but I will definitely let you know as soon as there will be an update regarding this matter.

s,

I hope this will be soon, because I have begun to see routers which have been stable for weeks crash with an out of memory error. This has happened multiple times in the last few days, including on routers running the latest new and bugfix software and firmware:

```
mar/09/2019 06:58:04 system,error,critical router was rebooted without proper
shutdown, probably kernel failure
mar/09/2019 06:58:04 system,error,critical kernel failure in previous boot
mar/09/2019 06:58:04 system,error,critical out of memory condition was detected
```

```
mar/10/2019 16:56:18 system,error,critical router was rebooted without proper
shutdown, probably kernel failure
mar/10/2019 16:56:18 system,error,critical kernel failure in previous boot
mar/10/2019 16:56:18 system,error,critical out of memory condition was detected
```

And most recently (this log information pulled out of the autosupout file):

```
mar/14 19:59:14 system,error,critical router was rebooted without proper shutdown,
probably kernel failure
mar/14 19:59:14 system,error,critical kernel failure in previous boot
mar/14 19:59:14 system,error,critical out of memory condition was detected
```

We poll the memory usage every ~60 seconds. The data point immediately prior to the crash is normal: 400Mb free.

I worry that this is because some other people found and have begun exploiting this vulnerability in RouterOS.

“Yes, it is highly possible, however, we would prefer to not jump to conclusions without seeing an actual file.”

– email from MikroTik support, 2019-03-21

“Sadly, I will not be able to provide any supouts showing IPv6 crashes - we are removing MikroTik from our IPv6 transit network entirely, because you have not taken this bug seriously.”

– email to MikroTik support, 2019-03-21

SOUNDING THE ALARM

2019-03-14: CERTs?

- No commitment from or progress with vendor
- Posted to UKNOF asking for CERT contacts
  - Next two weeks began involving NCSC UK, NCSC NL, ops-t, FIRST, CERT.BR...
  - Too many people to list — but thank you all for advice and contacts you provided.

WHAT DO CERTS SAY?

[this is with] Incident Management team 😎

– NCSC UK, 2019-04-01

**NEW!
vulnerability
disclosure
co-ordination
process**

“NCSC [NL] may be able to assist in accordance with our Coordinated Vulnerability Disclosure policy”

– NCSC NL, 2019-03-18

CVE-2018-19299: IPv6 CACHE CRASH (MIKROTIK ROUTEROS v6)

CVE-2018-19299 Timeline

- 2018-04-16 — reported to vendor
- 2018-04-19 — **acknowledged** by vendor as "not a security vulnerability"
- 2018-06-29 — "**not yet fixed**"
- 2018-10-10 — "**not [...] a vulnerability**"
- 2018-11-15 — CVE assigned; "**with our development team**"
- 2019-01-15 — "**can not give you any ETA for the fix**"
- 2019-02-14 — V-Day 0-day discussion @net_mcr
- 2019-03-11 — "**there is no news**"
- 2019-03-14 — last ditch scrabble around for CERTs/etc
- 2019-04-09 — full disclosure @uknof

then things got busy

CVE-2018-19299 Timeline

- 2019-03-27 14:08 — "UKNOF 43 CVE" topic starts to MikroTik forum
- 2019-03-28 11:37 — TechRepublic starts coverage
- 2019-03-28 11:57 — another thread starts on forum; multiple Reddits
- 2019-03-28 11:50 — MikroTik: "we are aware [...] working on it"
- 2019-03-29 07:56 — MikroTik: "we aim to fix before [UKNOF]"
- 2019-03-29 08:02 — MI: "contact me privately" (via forum)
- 2019-03-29 11:00 — @mikrotik_build: "version 6.45beta22" claims fix
- 2019-03-29 11:23 — @maznu: "not fixed"
- 2019-03-29 11:35 — MI: "not fixed" (via forum)
- 2019-03-29 12:17 — MikroTik: "please clarify" (via forum)

then things got weird

“For everyone here, I wanted to clarify, that to my best knowledge, the author of the CVE has not contacted MikroTik and we are in the dark as to what he plans to publish.”

– forum post by MikroTik, 2019-03-29 13:00

CVE-2018-19299 Timeline

- At 11:00 on 2019-03-29 MikroTik publicly releases a beta claiming to fix CVE-2018-19299...
  - ...but hadn't contacted the reporter to check it.

not fixed!

- At 13:00 MikroTik publicly accuses the reporter of never telling them about the CVE they just fixed...?

CVE-2018-19299 Timeline

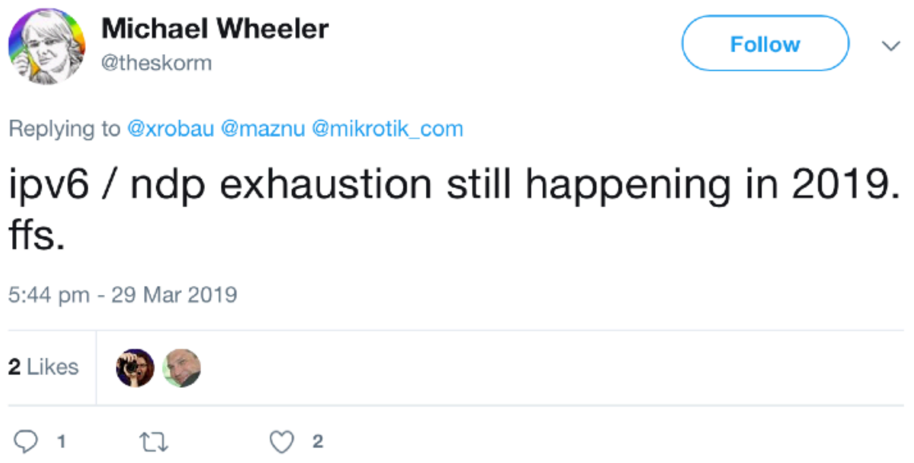
- 2019-03-29 13:00 — public statement: "we are in the dark"
- 2019-03-29 13:03 — MI rebuttal #0, "happy to send you my slides"
- 2019-03-29 13:06 — "I don't know what you will publish in the CVE."
- 2019-03-29 13:09 — MI rebuttal #1
- 2019-03-29 13:19 — email everything again (Ticket#2019032922005182)
- 2019-03-29 14:09 — "[our] settings for ipv6 route cache is too big"
- 2019-03-29 14:43 — public statement: "did not send [PoC]"
- 2019-03-29 14:46 — "firewall config should stop any attack"
- 2019-03-29 15:12 — MI rebuttal #2

THE "WORKAROUND"

"Workaround" Firewall

- /ipv6 firewall filter
  - add action=drop chain=forward connection-mark=drop connection-state=new
- /ipv6 firewall mangle
  - add **action=accept** chain=prerouting connection-state=new dst-address=2001:db8:3::/64 **limit=2,5**:packet
  - add action=mark-connection chain=prerouting connection-state=new dst-address=2001:db8:3::/64 new-connection-mark=drop passthrough=yes

"Workaround" Reaction



Michael Wheeler
@theskorm

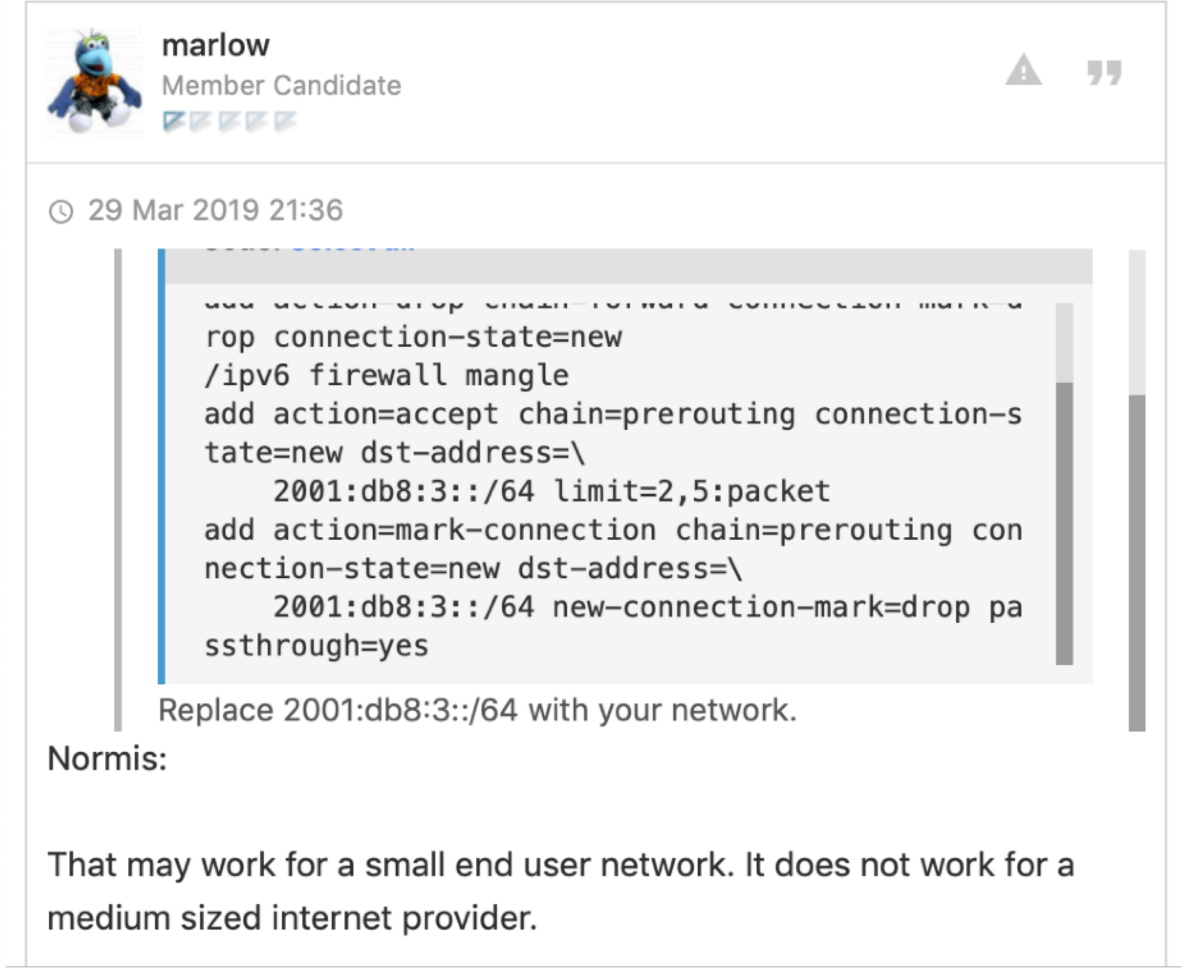
Replying to @xrobau @maznu @mikrotik_com

ipv6 / ndp exhaustion still happening in 2019. ffs.

5:44 pm - 29 Mar 2019

2 Likes

1 2



marlow
Member Candidate

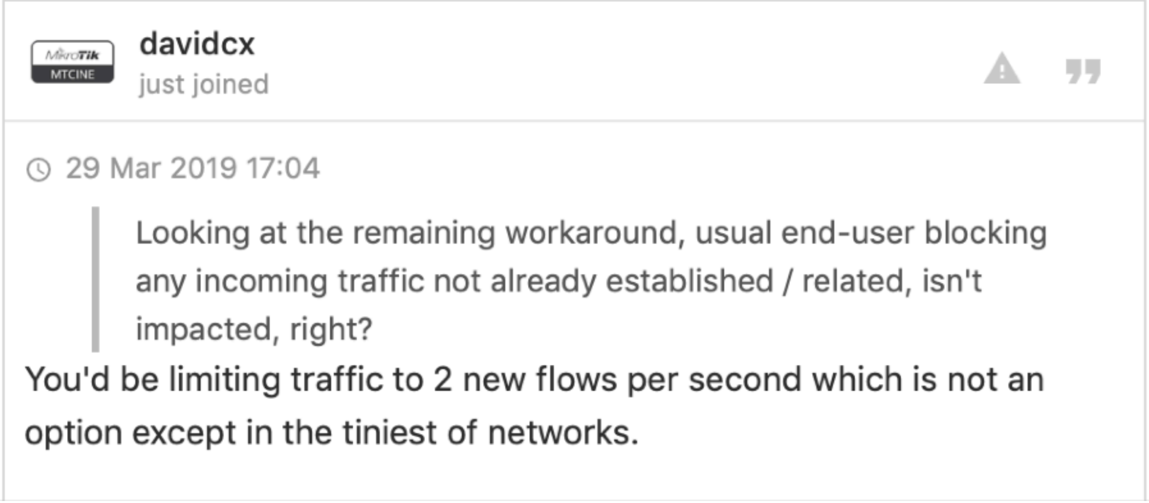
29 Mar 2019 21:36

```
add action=drop chain=forward connection-mark=d
rop connection-state=new
/ipv6 firewall mangle
add action=accept chain=prerouting connection-s
tate=new dst-address=\
    2001:db8:3::/64 limit=2,5:packet
add action=mark-connection chain=prerouting con
nection-state=new dst-address=\
    2001:db8:3::/64 new-connection-mark=drop pa
ssthrough=yes
```

> Replace 2001:db8:3::/64 with your network.

Normis:

That may work for a small end user network. It does not work for a medium sized internet provider.

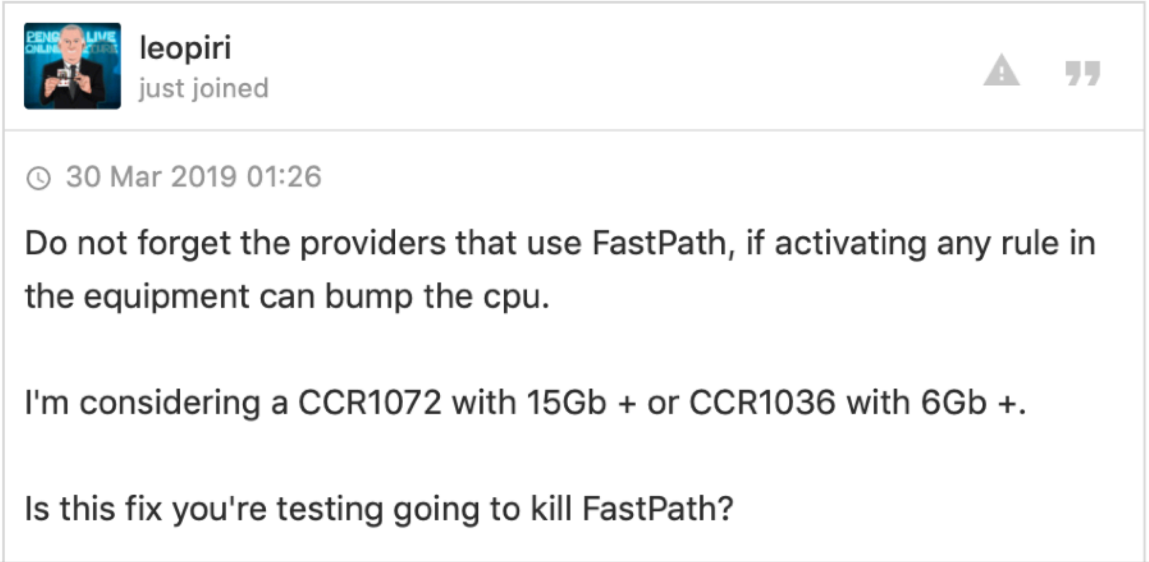


davidcx
just joined

29 Mar 2019 17:04

> Looking at the remaining workaround, usual end-user blocking any incoming traffic not already established / related, isn't impacted, right?

You'd be limiting traffic to 2 new flows per second which is not an option except in the tiniest of networks.



leopiri
just joined

30 Mar 2019 01:26

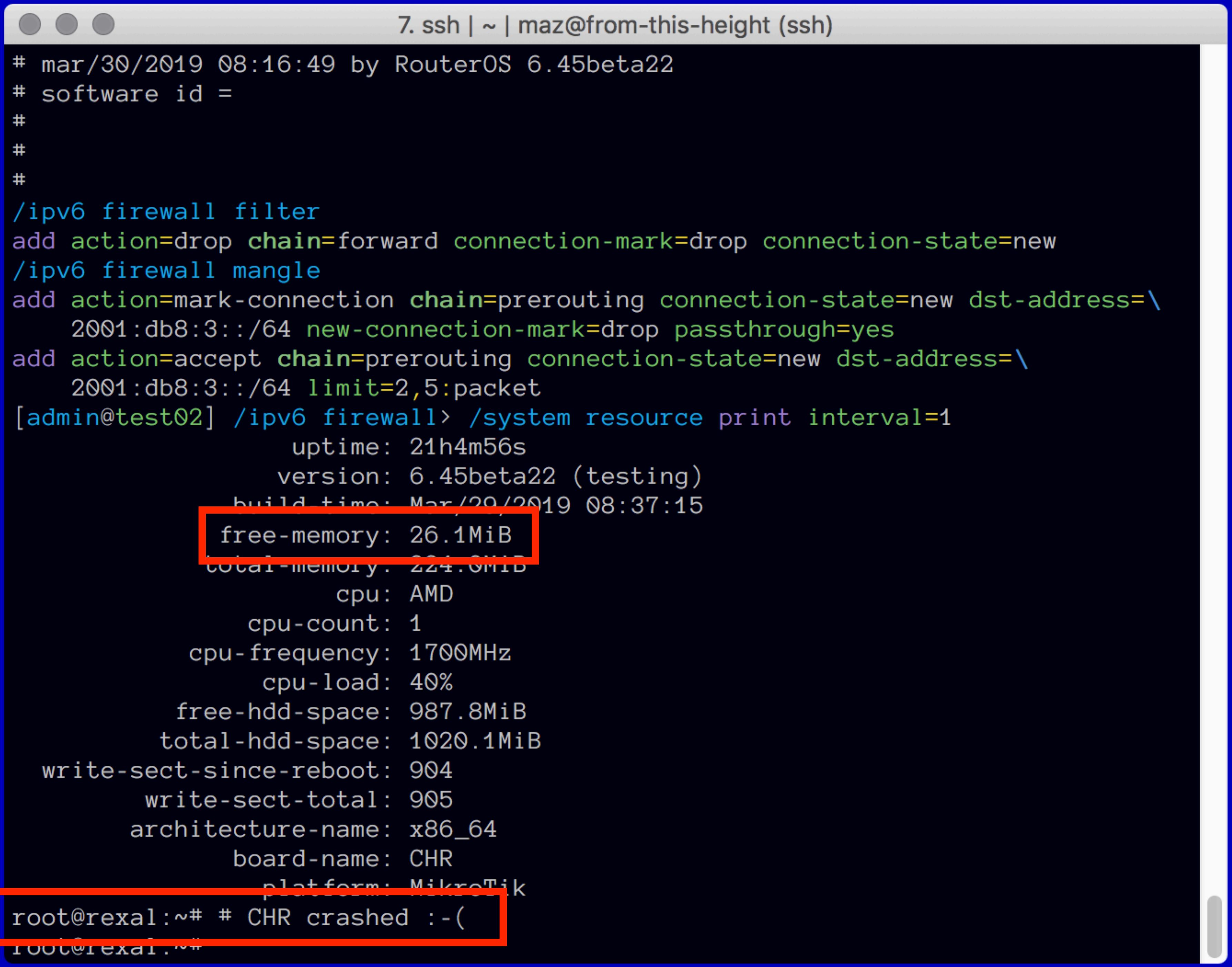
Do not forget the providers that use FastPath, if activating any rule in the equipment can bump the cpu.

I'm considering a CCR1072 with 15Gb + or CCR1036 with 6Gb +.

Is this fix you're testing going to kill FastPath?

"Workaround" or... not?

- /ipv6 firewall **filter**
  - add action=drop **chain=forward** connection-mark=drop **connection-state=new**
- /ipv6 firewall mangle
  - add action=accept chain=prerouting **connection-state=new** dst-address=2001:db8:3::/64 limit=2,5:packet
  - add action=mark-connection chain=prerouting **connection-state=new** dst-address=2001:db8:3::/64 new-connection-mark=drop passthrough=yes



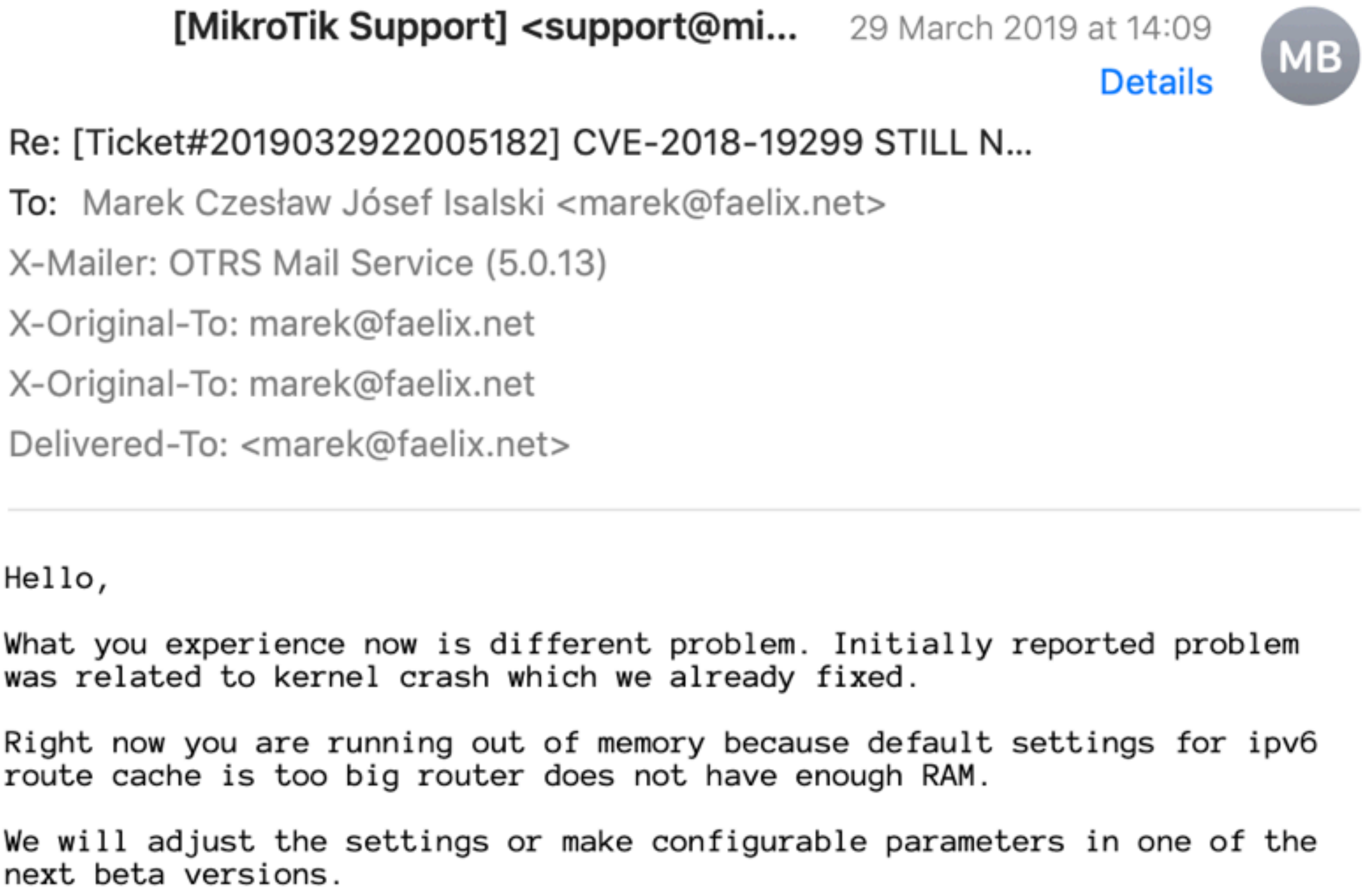
```
# mar/30/2019 08:16:49 by RouterOS 6.45beta22
# software id =
#
#
#
/ipv6 firewall filter
add action=drop chain=forward connection-mark=drop connection-state=new
/ipv6 firewall mangle
add action=mark-connection chain=prerouting connection-state=new dst-address=\
    2001:db8:3::/64 new-connection-mark=drop passthrough=yes
add action=accept chain=prerouting connection-state=new dst-address=\
    2001:db8:3::/64 limit=2,5:packet
[admin@test02] /ipv6 firewall> /system resource print interval=1
                   uptime: 21h4m56s
                  version: 6.45beta22 (testing)
               build-time: Mar/29/2019 08:37:15
              free-memory: 26.1MiB
             total-memory: 224.0MiB
                      cpu: AMD
                cpu-count: 1
            cpu-frequency: 1700MHz
                 cpu-load: 40%
           free-hdd-space: 987.8MiB
          total-hdd-space: 1020.1MiB
  write-sect-since-reboot: 904
         write-sect-total: 905
        architecture-name: x86_64
               board-name: CHR
                 platform: MikroTik
root@rexal:~# # CHR crashed :-(
root@rexal:~#
```

A BREAKTHROUGH!

CVE-2018-19299 Timeline

- 2019-03-29 13:00 — public statement: "we are in the dark"
- 2019-03-29 13:03 — MI rebuttal #0, "happy to send you my slides"
- 2019-03-29 13:06 — "I don't know what you will publish in the CVE."
- 2019-03-29 13:09 — MI rebuttal #1
- 2019-03-29 13:19 — email everything again (Ticket#2019032922005182)
- 2019-03-29 14:09 — **"[our] settings for ipv6 route cache is too big"**
- 2019-03-29 14:43 — public statement: "did not send [PoC]"
- 2019-03-29 14:46 — "firewall config should stop any attack"
- 2019-03-29 15:12 — MI rebuttal #2

The Underlying Problem!



[MikroTik Support] <support@mi... 29 March 2019 at 14:09

Re: [Ticket#2019032922005182] CVE-2018-19299 STILL N...

To: Marek Czesław Jósef Isalski <marek@faelix.net>

X-Mailer: OTRS Mail Service (5.0.13)

X-Original-To: marek@faelix.net

X-Original-To: marek@faelix.net

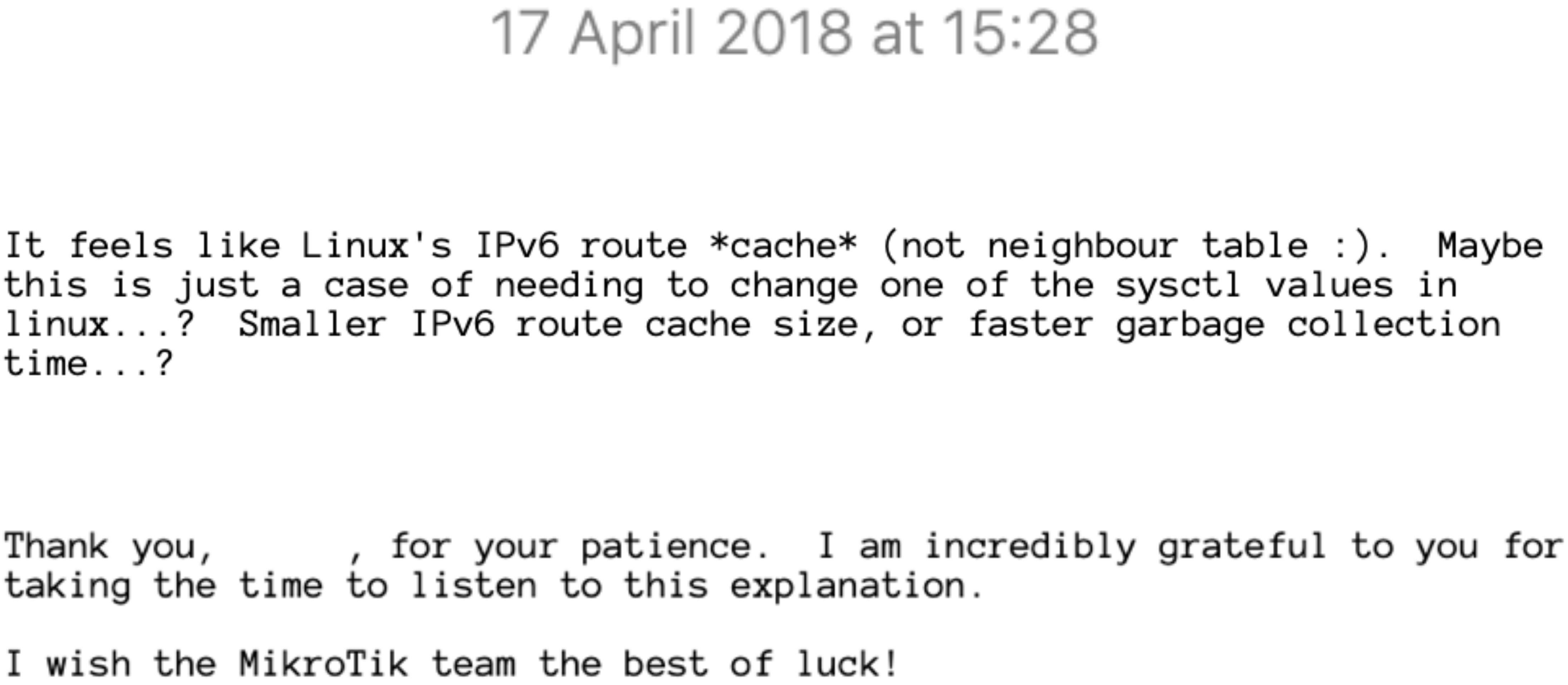
Delivered-To: <marek@faelix.net>

```
Hello,

What you experience now is different problem. Initially reported problem
was related to kernel crash which we already fixed.

Right now you are running out of memory because default settings for ipv6
route cache is too big router does not have enough RAM.

We will adjust the settings or make configurable parameters in one of the
next beta versions.
```

“It’s MikroTik’s fault that this was filed as yet another ipv6 bug [...] The issue is now fixed, the memory exhaustion is also fixed, build is coming Monday.”

– @normis on Twitter, 2019-03-30 12:36

Flashback: the hunch...



17 April 2018 at 15:28

It feels like Linux's IPv6 route *cache* (not neighbour table :). Maybe this is just a case of needing to change one of the sysctl values in linux...? Smaller IPv6 route cache size, or faster garbage collection time...?

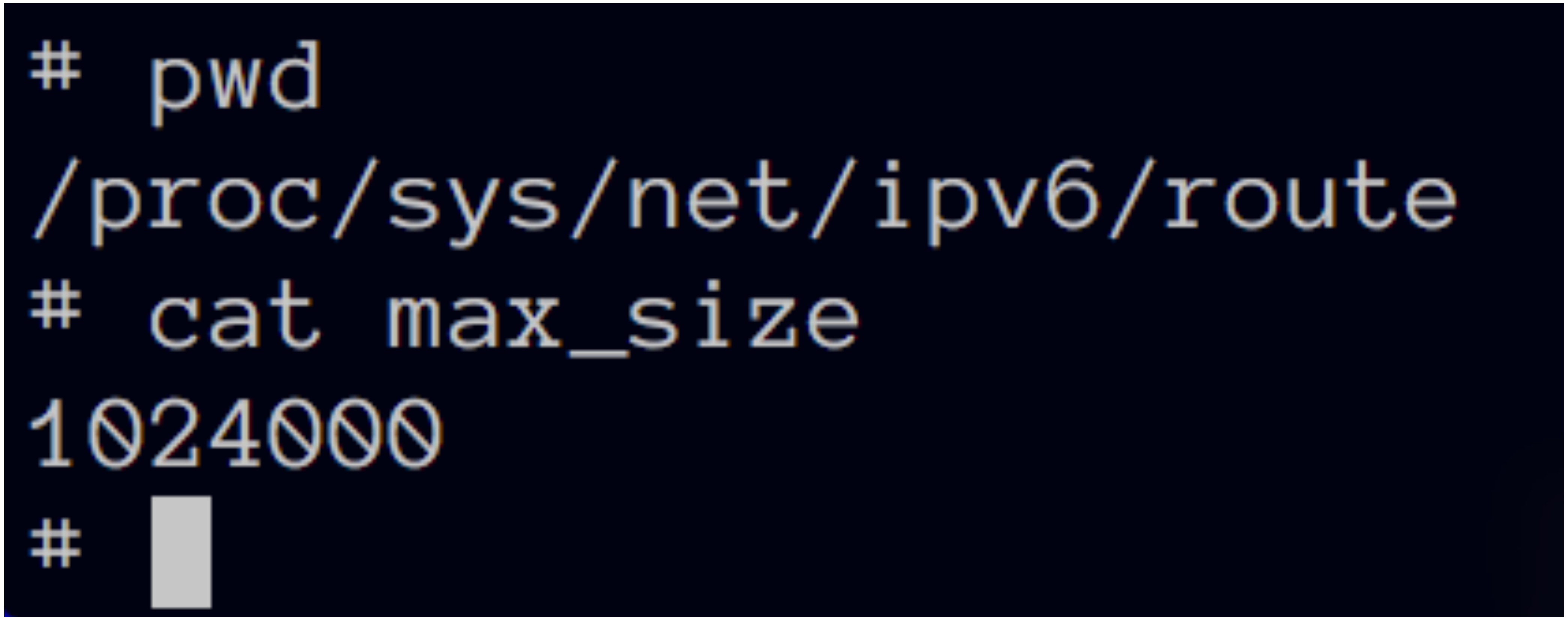
Thank you, , for your patience. I am incredibly grateful to you for taking the time to listen to this explanation.

I wish the MikroTik team the best of luck!

Linux IPv6 Route Cache

- "IPv6 still has a caching mechanism [...] entries are directly put in the radix tree instead of a distinct structure."
    - Excellent deep dive explanation by Vincent Bernat
- Can we confirm RouterOS' sysctl settings?
    - v6.40, touch two files (thanks, @KirilsSolovjovs)
    - Telnet in and get a limited busybox shell!

Linux IPv6 Route Cache



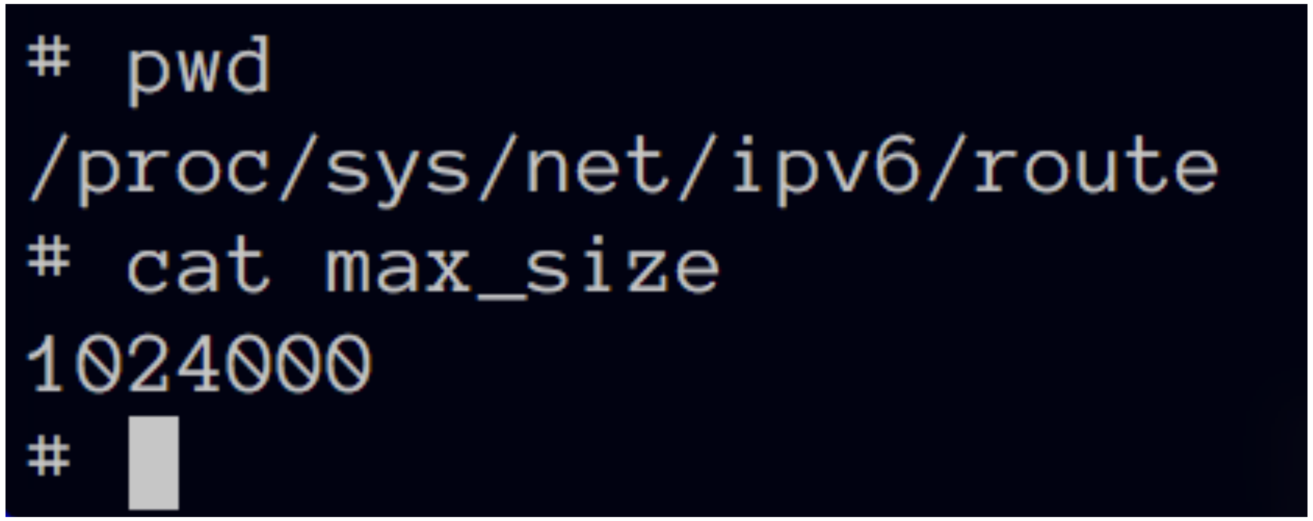
```
# pwd
/proc/sys/net/ipv6/route
# cat max_size
1024000
# 
```

Back to you, M. Bernat…

- The LPC-trie used for IPv4 is more efficient: when 512 MiB of memory is needed for IPv6 to store 1 million routes, only 128 MiB are needed for IPv4. The difference is mainly due to the size of struct rt6_info (336 bytes)

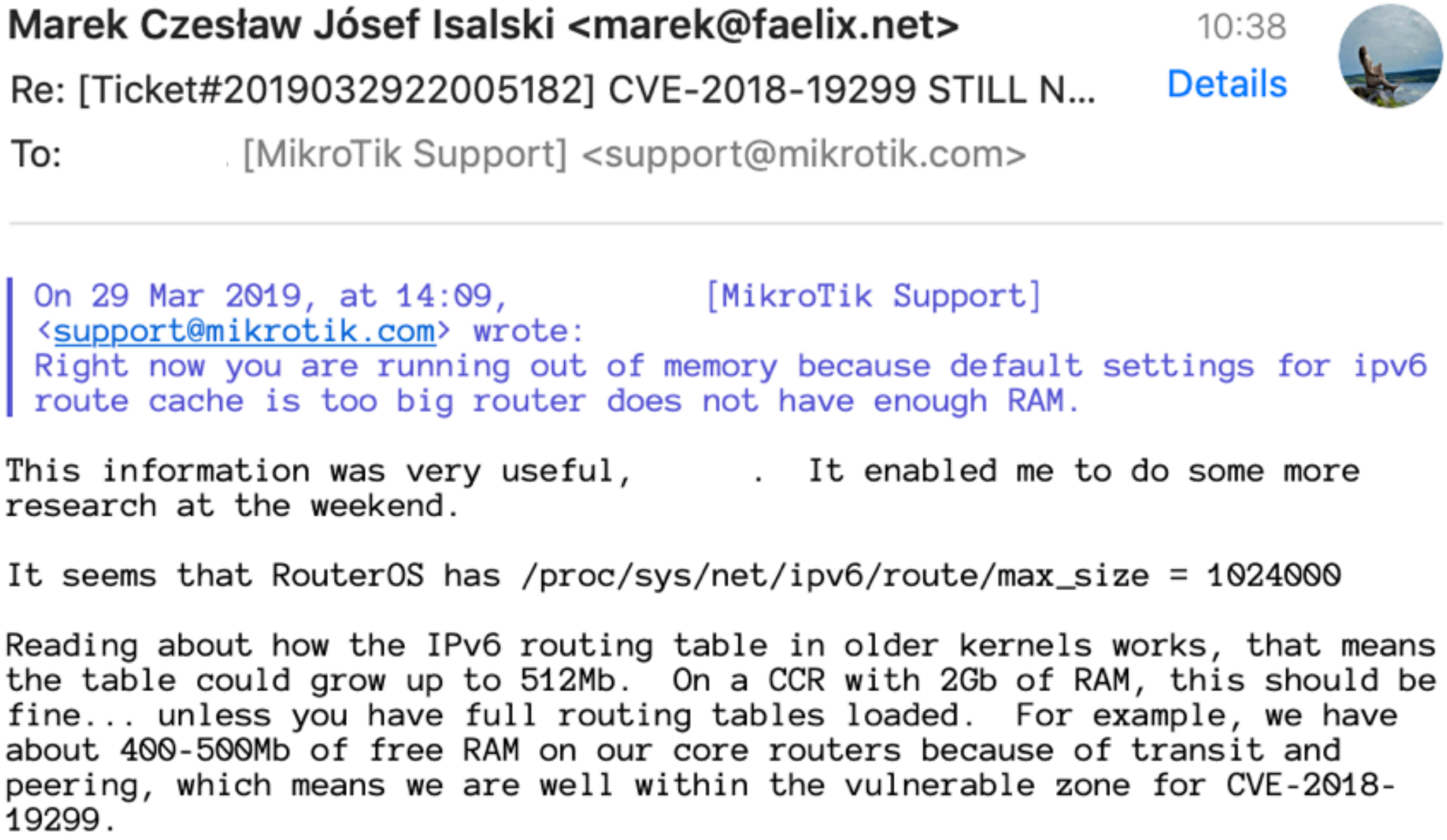
Back to you, M. Bernat...

- The LPC-trie used for IPv4 is more efficient: when **512 MiB** of memory is needed for IPv6 to store **1 million routes**, only 128 MiB are needed for IPv4. The difference is mainly due to the size of struct rt6_info (336 bytes)



```
# pwd
/proc/sys/net/ipv6/route
# cat max_size
1024000
# 
```

Light at end of tunnel…



Marek Czesław Jósef Isalski <marek@faelix.net> 10:38

Re: [Ticket#2019032922005182] CVE-2018-19299 STILL N… Details

To: . [MikroTik Support] <support@mikrotik.com>

> On 29 Mar 2019, at 14:09, [MikroTik Support] <support@mikrotik.com> wrote:
> Right now you are running out of memory because default settings for ipv6 route cache is too big router does not have enough RAM.

This information was very useful, . It enabled me to do some more research at the weekend.

It seems that RouterOS has /proc/sys/net/ipv6/route/max_size = 1024000

Reading about how the IPv6 routing table in older kernels works, that means the table could grow up to 512Mb. On a CCR with 2Gb of RAM, this should be fine... unless you have full routing tables loaded. For example, we have about 400-500Mb of free RAM on our core routers because of transit and peering, which means we are well within the vulnerable zone for CVE-2018-19299.

IT AIN'T OVER
TILL IT'S OVER...

Condensed Timeline

- 2019-03-29 11:00 — 6.45beta22 (not a fix)
- 2019-03-29 14:46 — workaround for other issues
- 2019-03-29 14:09 — "next beta version"
- 2019-03-30 12:36 — "build is coming Monday"

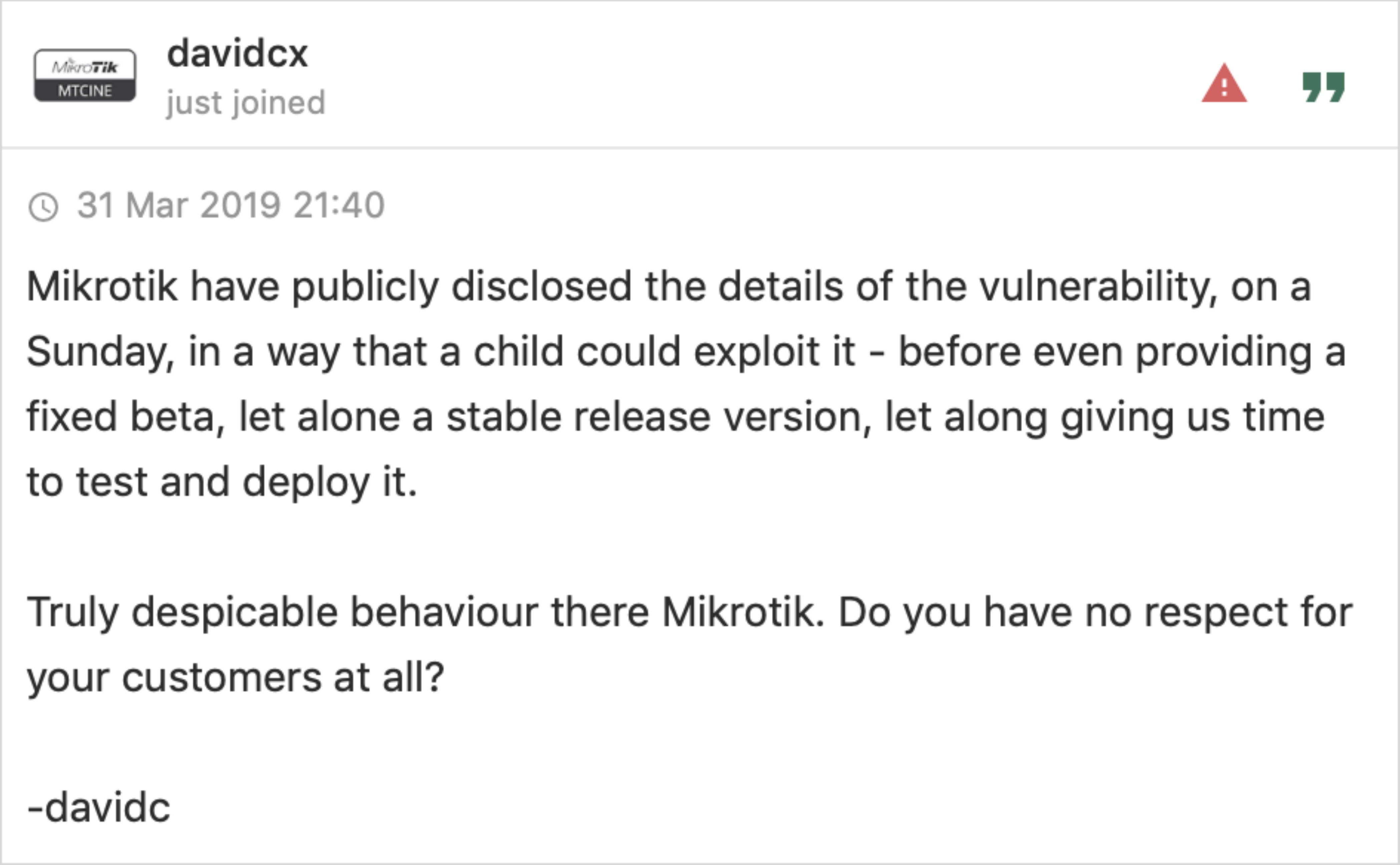
what goes here?

- 2019-04-01 ??:?? — release fix for CVE-2018-19299

“RouterOS IPv6 route cache max size by default is 1 million. [...] If you have device that does not have such resources, it will reboot itself.”

– forum post by MikroTik, 2019-03-31 13:28

A Customer's Reaction



davidcx
just joined

31 Mar 2019 21:40

Mikrotik have publicly disclosed the details of the vulnerability, on a Sunday, in a way that a child could exploit it - before even providing a fixed beta, let alone a stable release version, let along giving us time to test and deploy it.

Truly despicable behaviour there Mikrotik. Do you have no respect for your customers at all?

-davidc

**“However, it can not be considered as a bug or vulnerability. [...]
This is not a bug.”**

– forum post by MikroTik, 2019-03-31 13:28

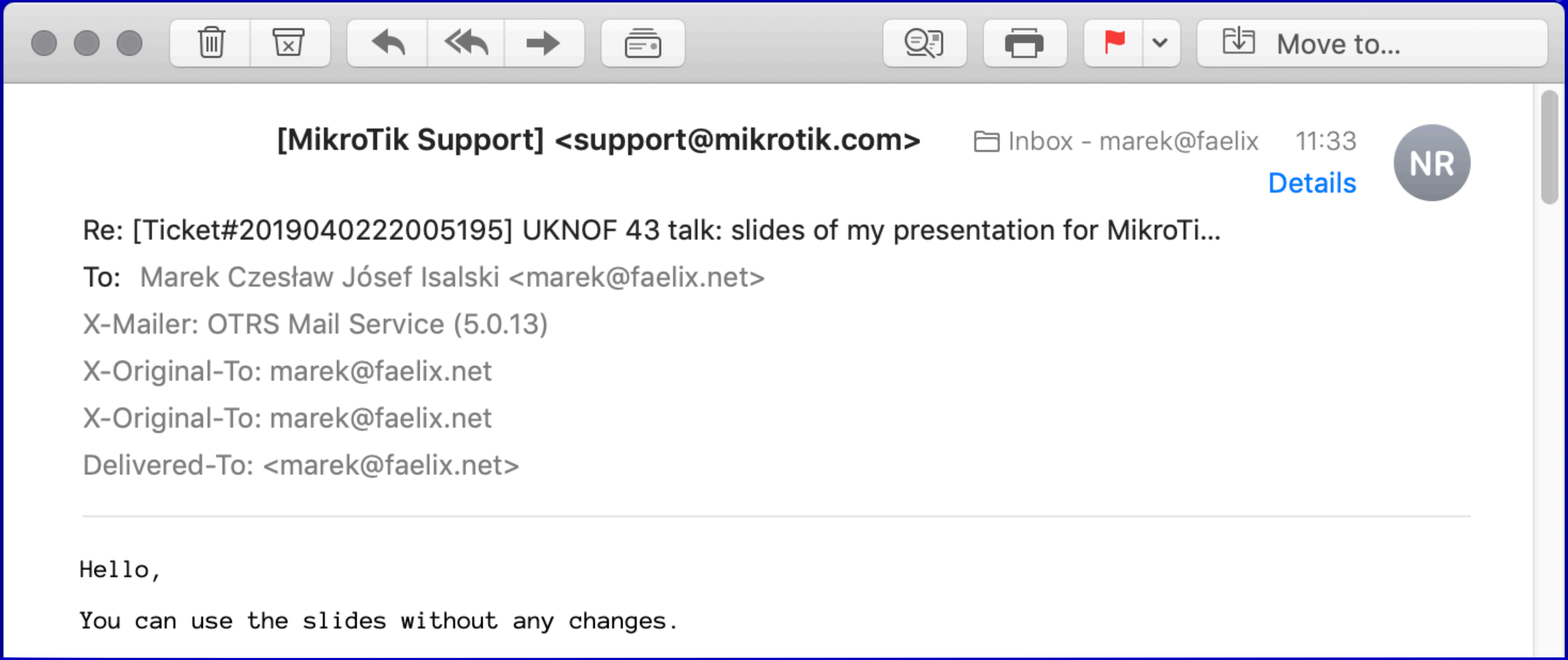
WRAPPING UP...
(I PROMISE!)

6.45beta23

- 2019-04-01 07:00 — @mikrotik_build: "6.45beta23"
- 2019-04-01 07:31 — confirmed fix!
- 2019-04-01 08:00 — "still tweaking [...] Next beta"

- 2019-04-01 09:15 — rewrite talk, now up to v4
- 2019-04-01 13:00 — peer review #1
- 2019-04-01 14:30 — edit talk, bump to v4.1
- 2019-04-01 15:00 — peer review #2
- 2019-04-01 23:45 — edit talk, bump to v4.2

- 2019-04-02 12:00 — sent to MikroTik for "right of reply"



[MikroTik Support] <support@mikrotik.com>

11:33

Re: [Ticket#2019040222005195] UKNOF 43 talk: slides of my presentation for MikroTi...

To: Marek Czesław Jósef Isalski <marek@faelix.net>

X-Mailer: OTRS Mail Service (5.0.13)

X-Original-To: marek@faelix.net

X-Original-To: marek@faelix.net

Delivered-To: <marek@faelix.net>

Hello,

You can use the slides without any changes.

Thanks to...

- MikroTik — it's fixed! 🍺 🍺 🍺
- Austin Murdock and the UNM/Berkeley projects
- Tom, Lou, @net_mcr crew, audience for debates
- Keith, Hal, Tim, Chris, @uknof PC members for input
- Members of UKNOF mailing list (and many others) who helped reach SOCs and NOCs and CERTs

HOW ABOUT A NICE CUP OF TEA?

E: marek @ faelix . net
T: @maznu
T: @faelix
W: https://faelix.net/

SLIDES: https://faelix.link/uknof43