nominet

Rollover and Die?

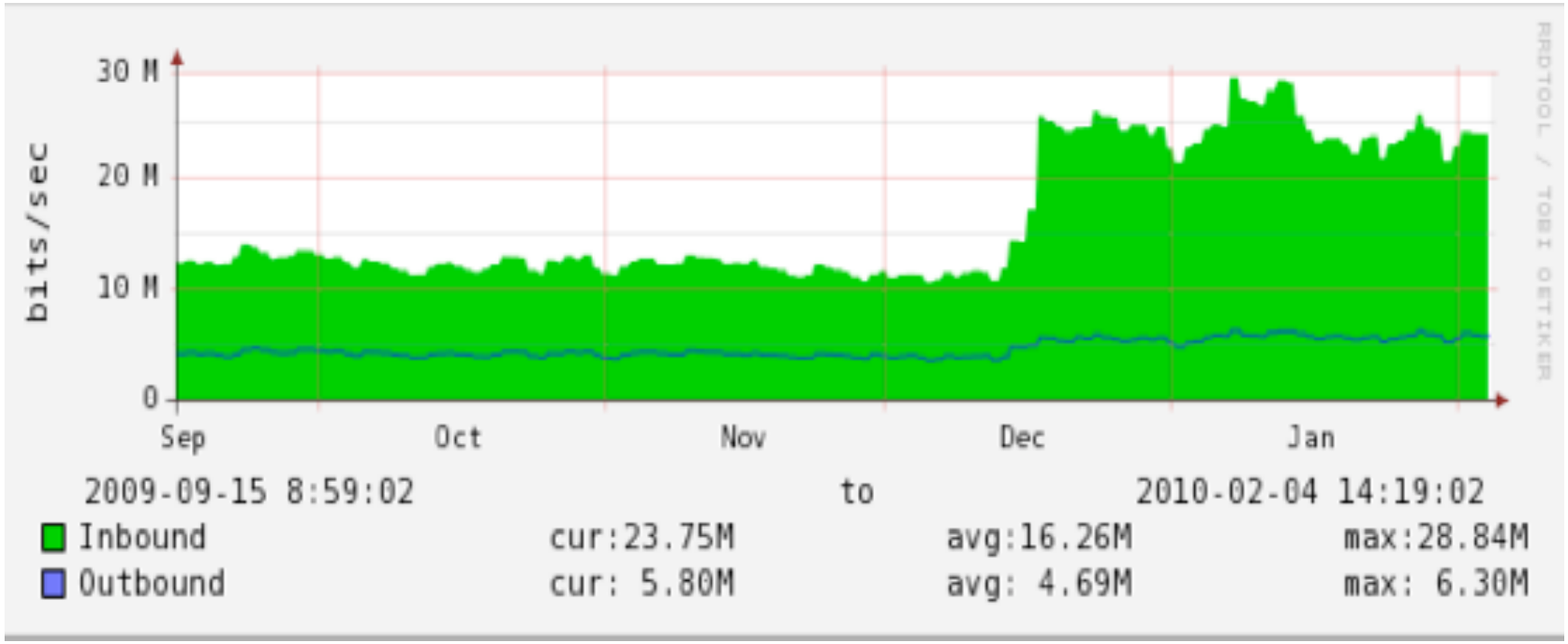
George Michaelson, APNIC

Geoff Huston, APNIC

Patrik Wallström, IIS

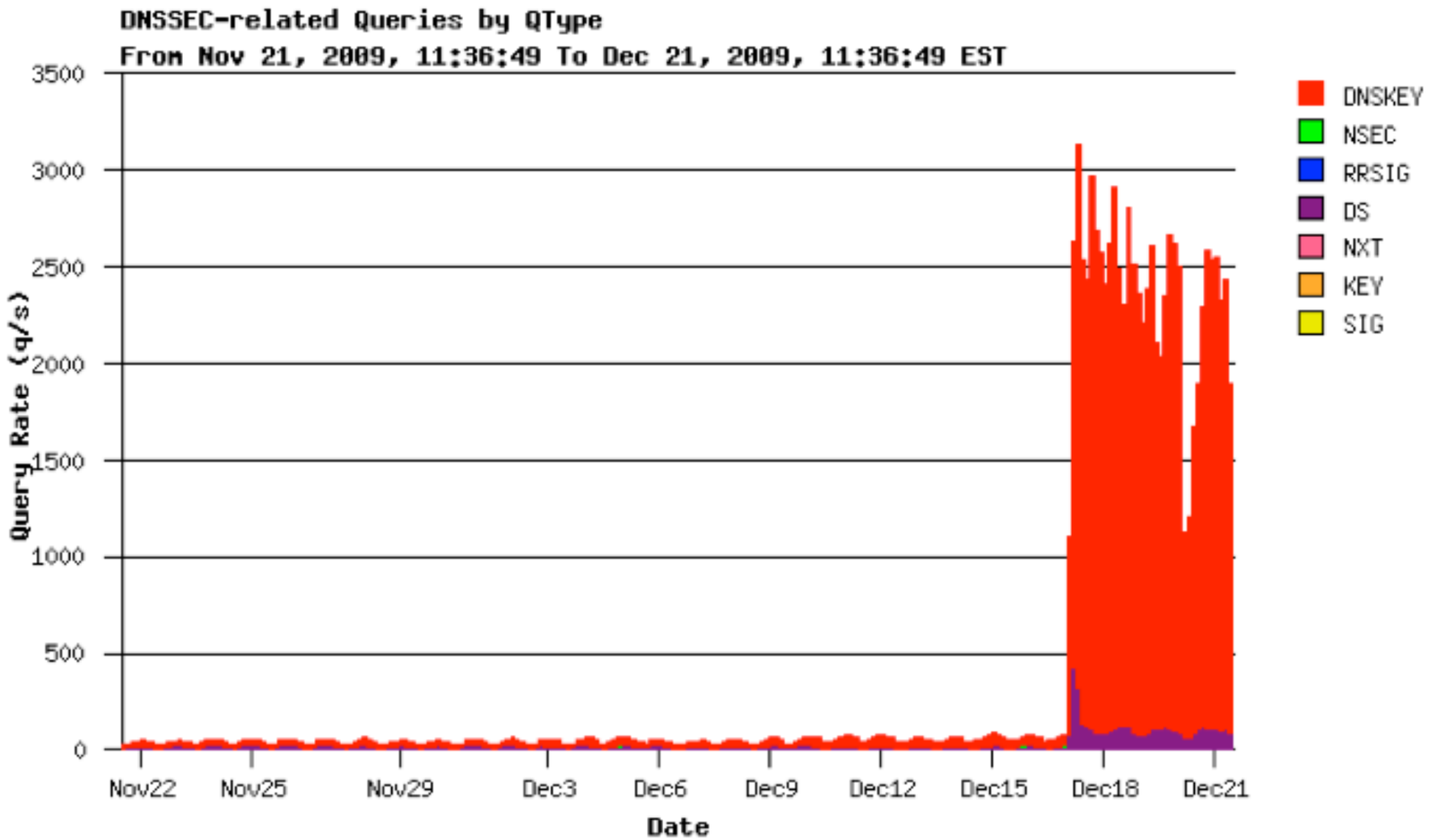
Roy Arends, Nominet UK

We’re under attack!!!



On the 16th of december, traffic more than doubled

DNSKEY amplification attack



DNSKEY response size

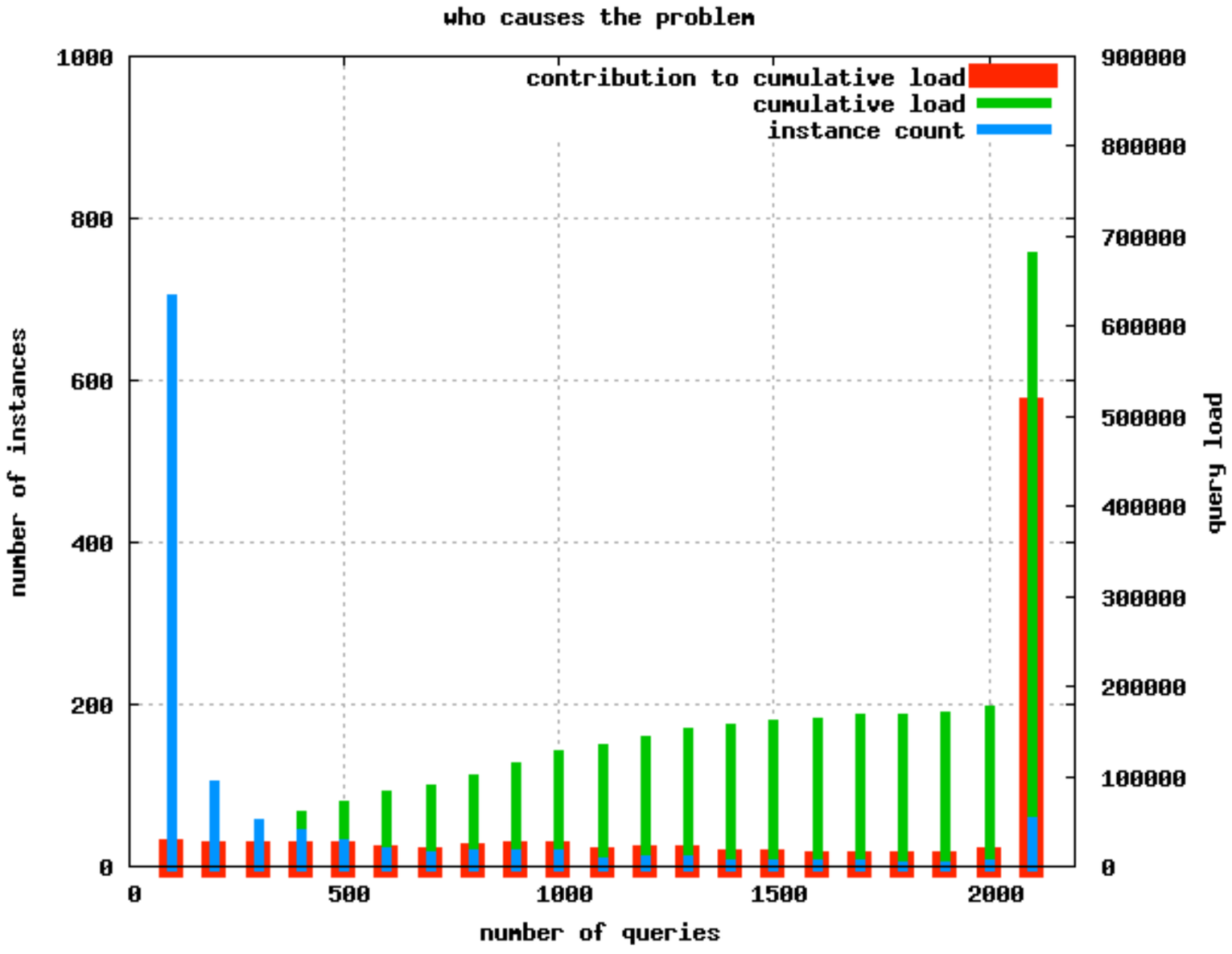
Response size: 990 Bytes

Query rate: 2000 qps

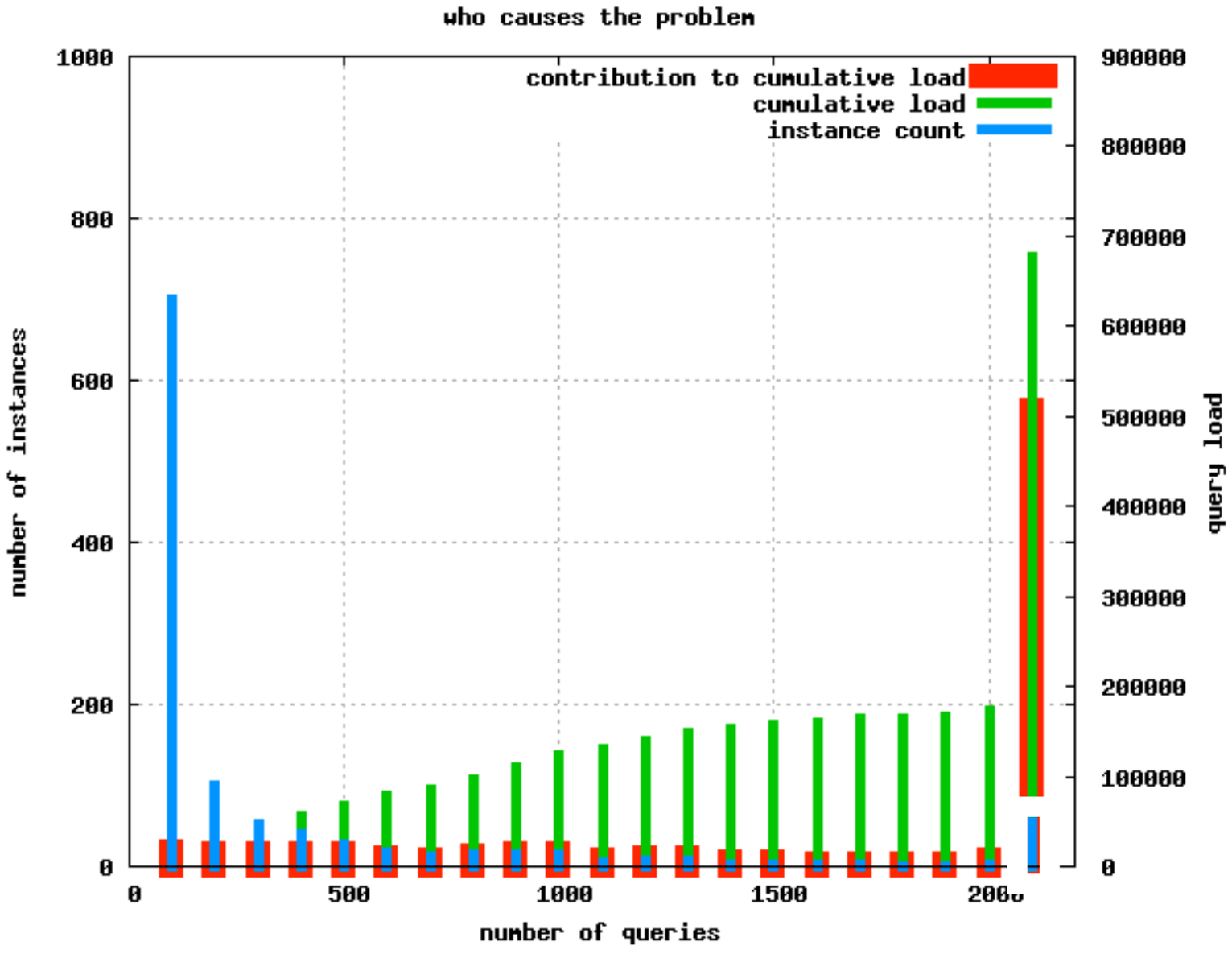
15.8 Mbps

Additional load

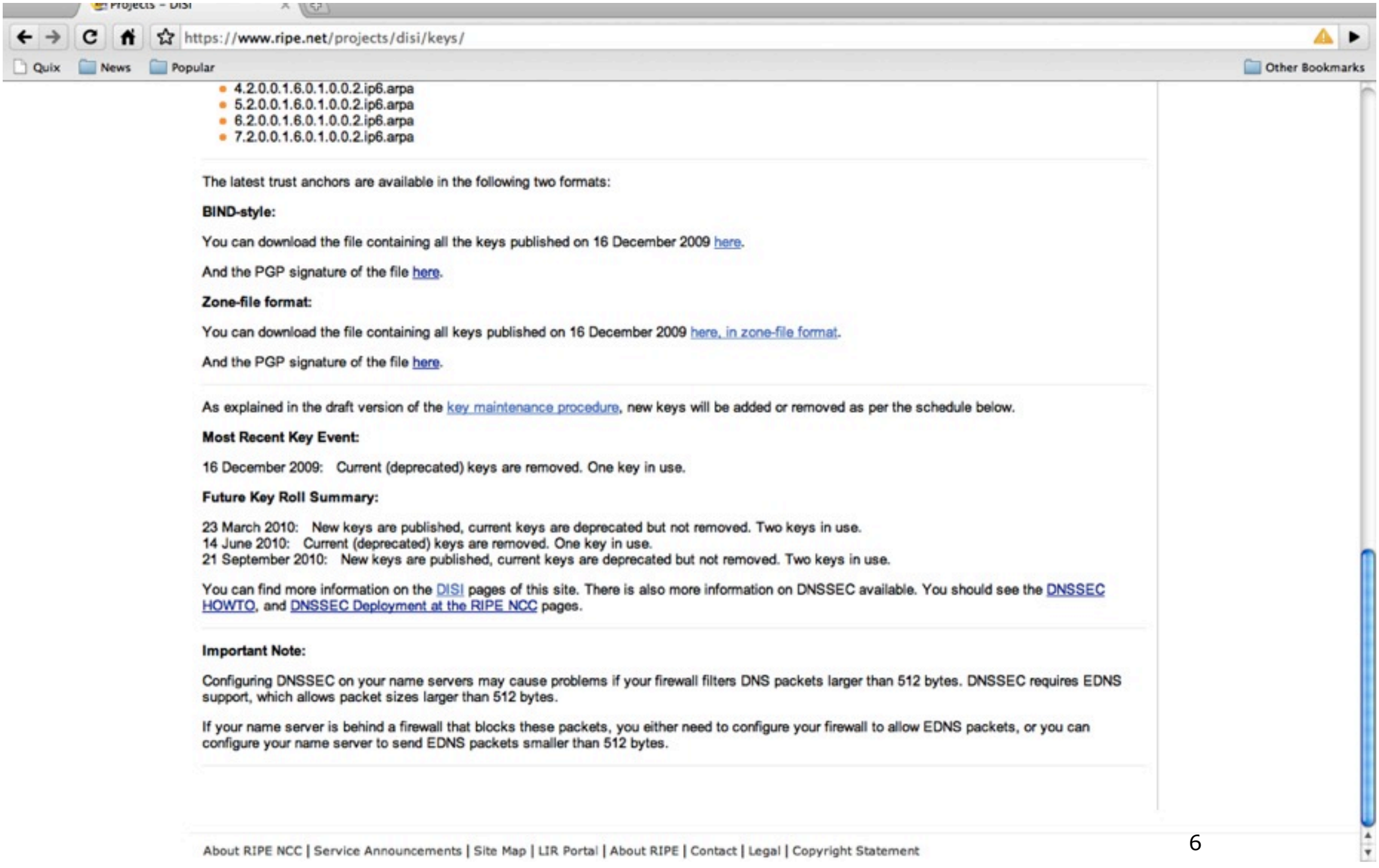
Who does this?



Who does this?



What was special about the 16th?



What was special about the 16th?

Zone-file format:

You can download the file containing all keys published on 16 December 2009 here, in zone-file format.

And the PGP signature of the file here.

As explained in the draft version of the key maintenance procedure, new keys will be added or removed a

Most Recent Key Event:

16 December 2009: Current (deprecated) keys are removed. One key in use.

Future Key Roll Summary:

23 March 2010: New keys are published, current keys are deprecated but not removed. Two keys in use
14 June 2010: Current (deprecated) keys are removed. One key in use.
21 September 2010: New keys are published, current keys are deprecated but not removed. Two keys ir

You can find more information on the DISI pages of this site. There is also more information on DNSSEC
HOWTO, and DNSSEC Deployment at the RIPE NCC pages.

Hanlon’s razor

Never attribute to **malice** that which can be explained by **stupidity**.

Why so many clients?

- Fedora bug report 17th Jan 2010
  - (1 month after the roll)
- operator reports getting 240.000 log entries in 24hr
  - "no valid key"
- dnssec-conf tool contained a hard-configured trust anchor file
  - obsolete after the 16th.

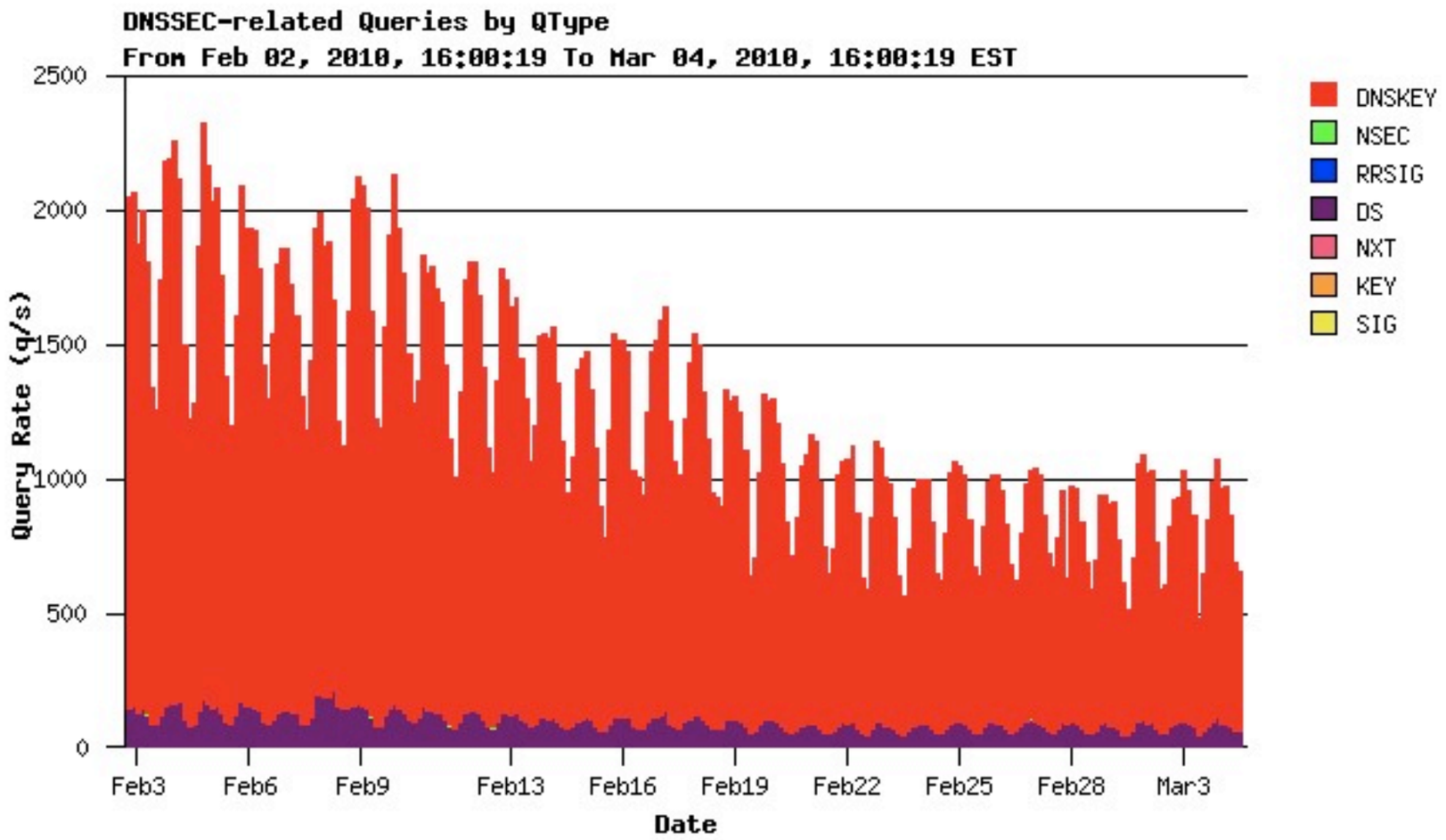
What was special about the 16th?

What was special about the 16th?

what a great lesson

Randy Bush's response

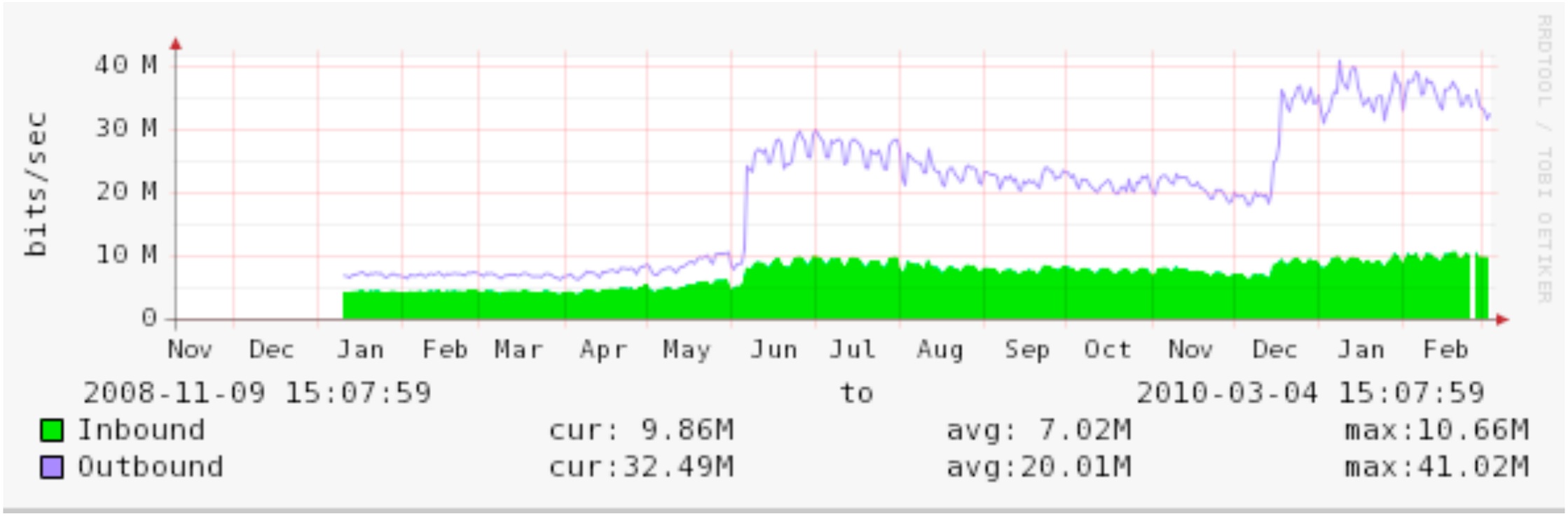
Current load for in-addr.arpa



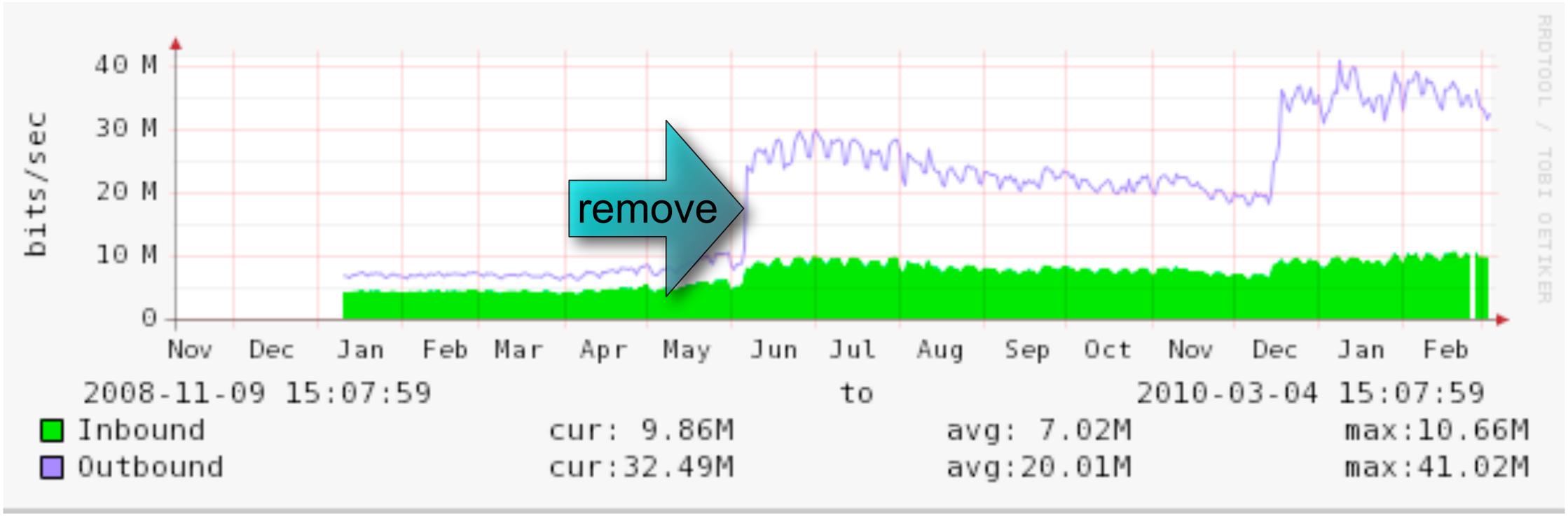
getting better, below 1000 qps right now

But decline not fast enough before new roll

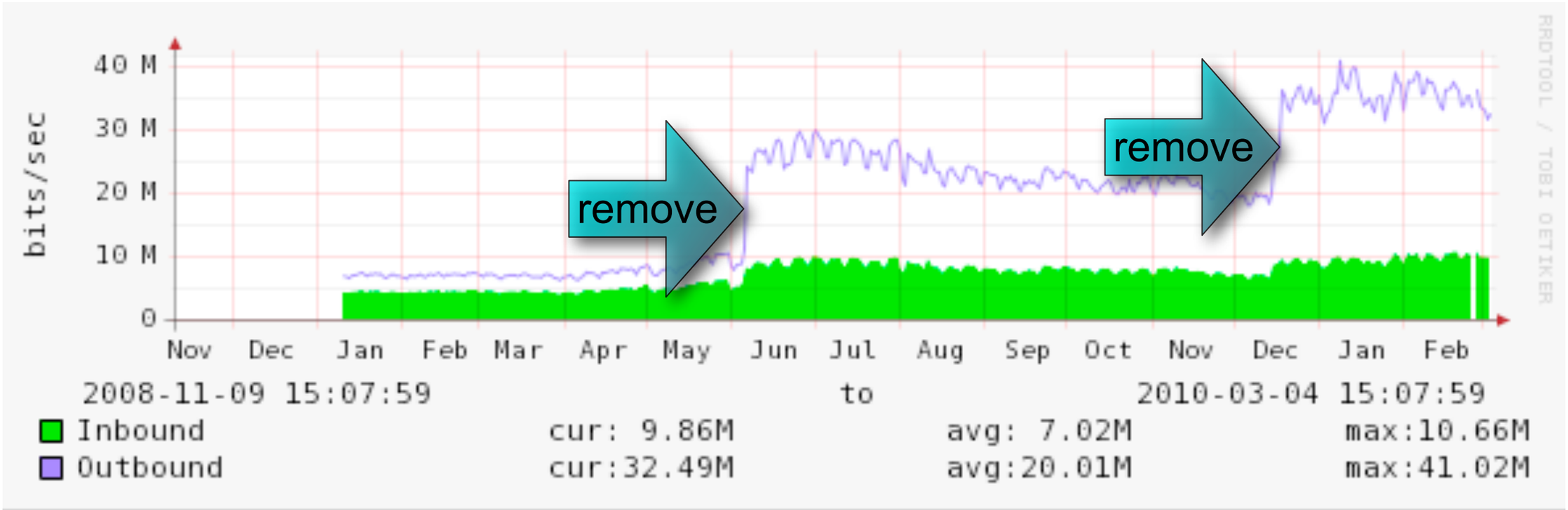
The Load Projection



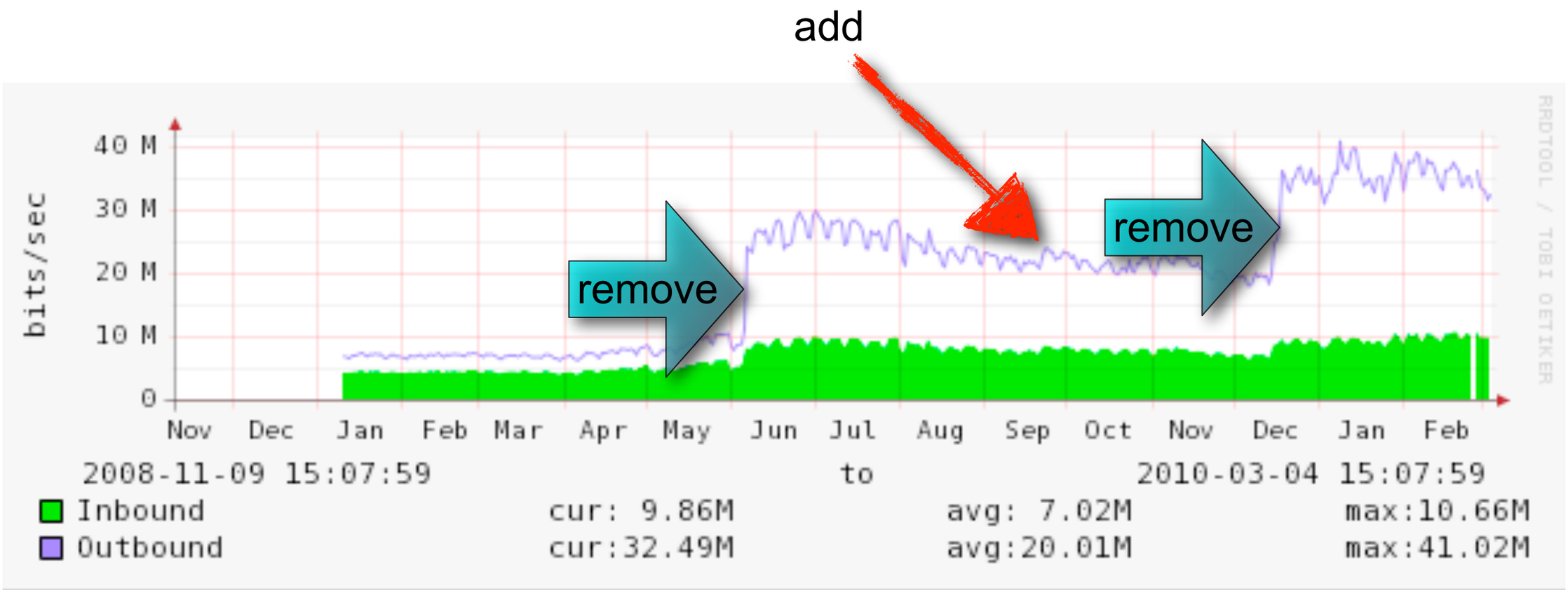
The Load Projection



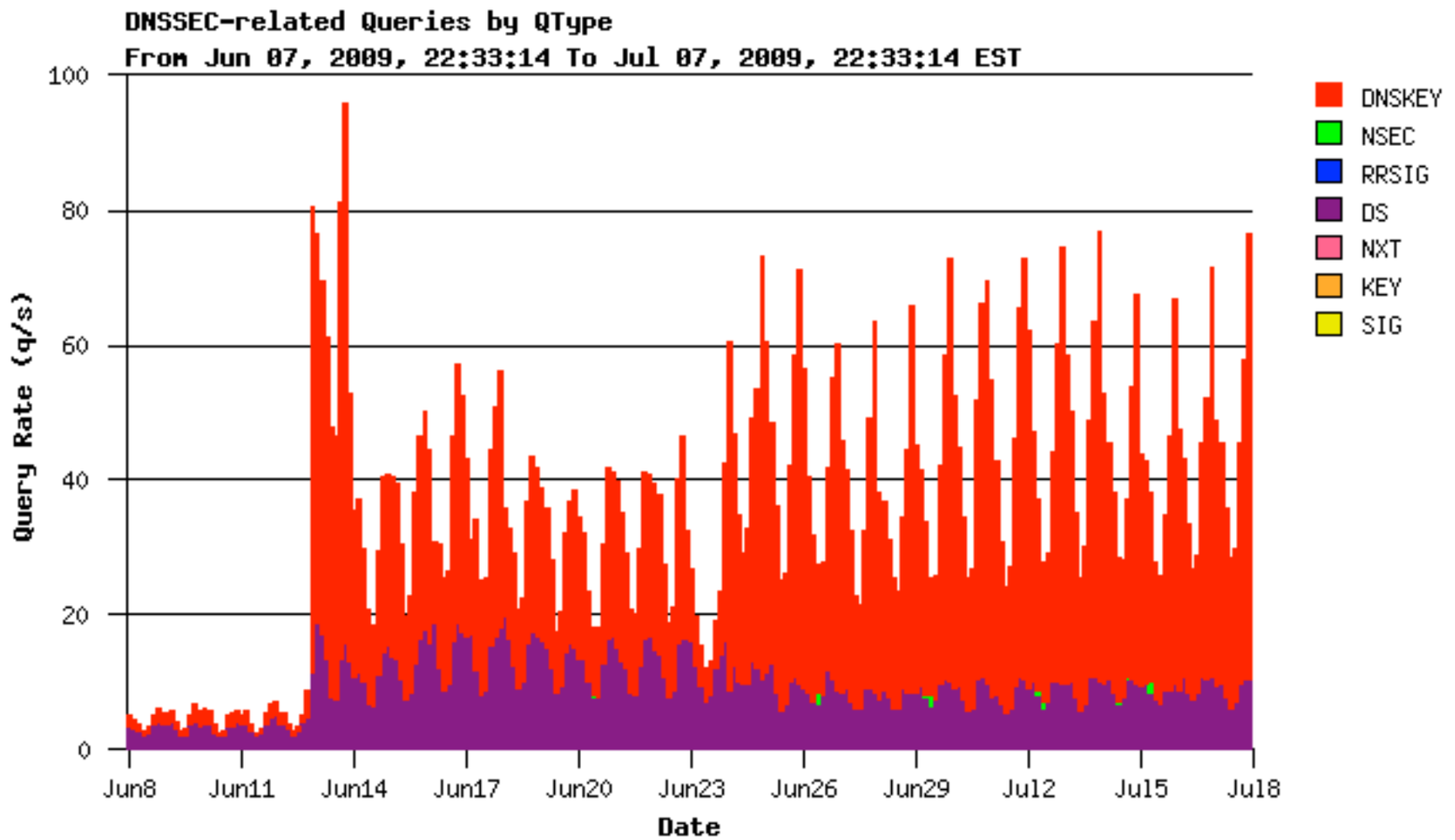
The Load Projection



The Load Projection

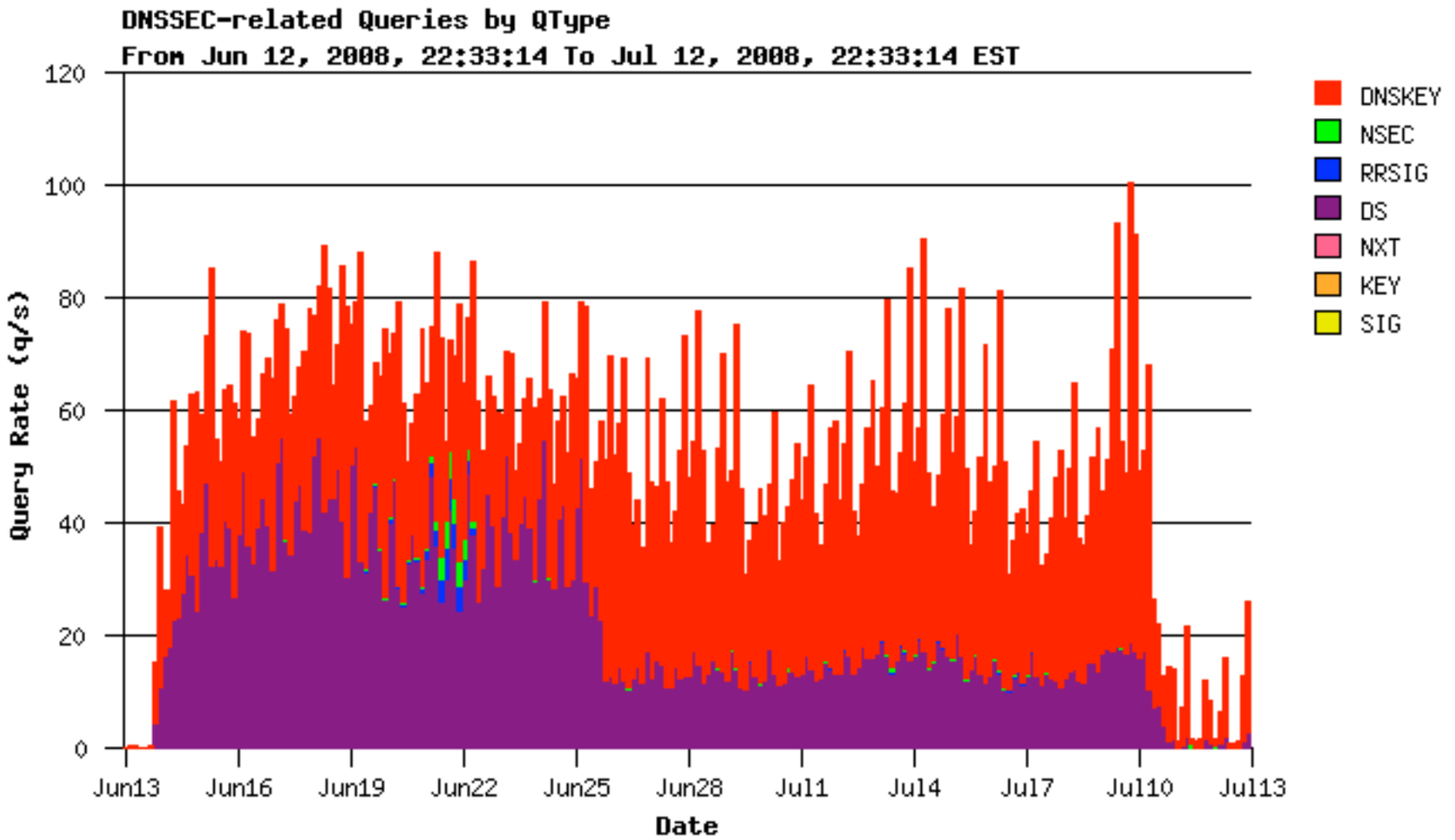


Was this a one off event?



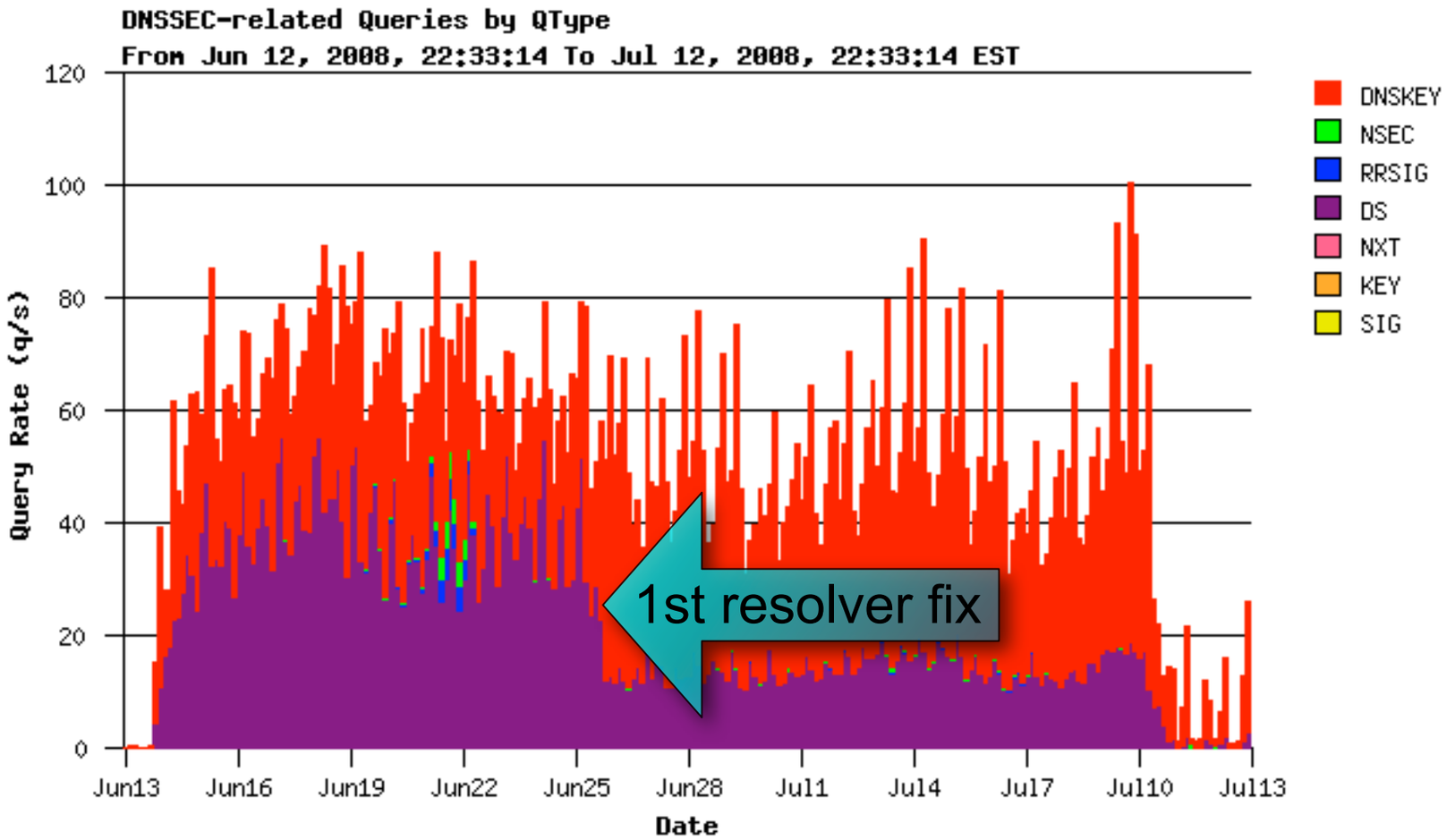
Sweden, june 2009

Was this a one off event?



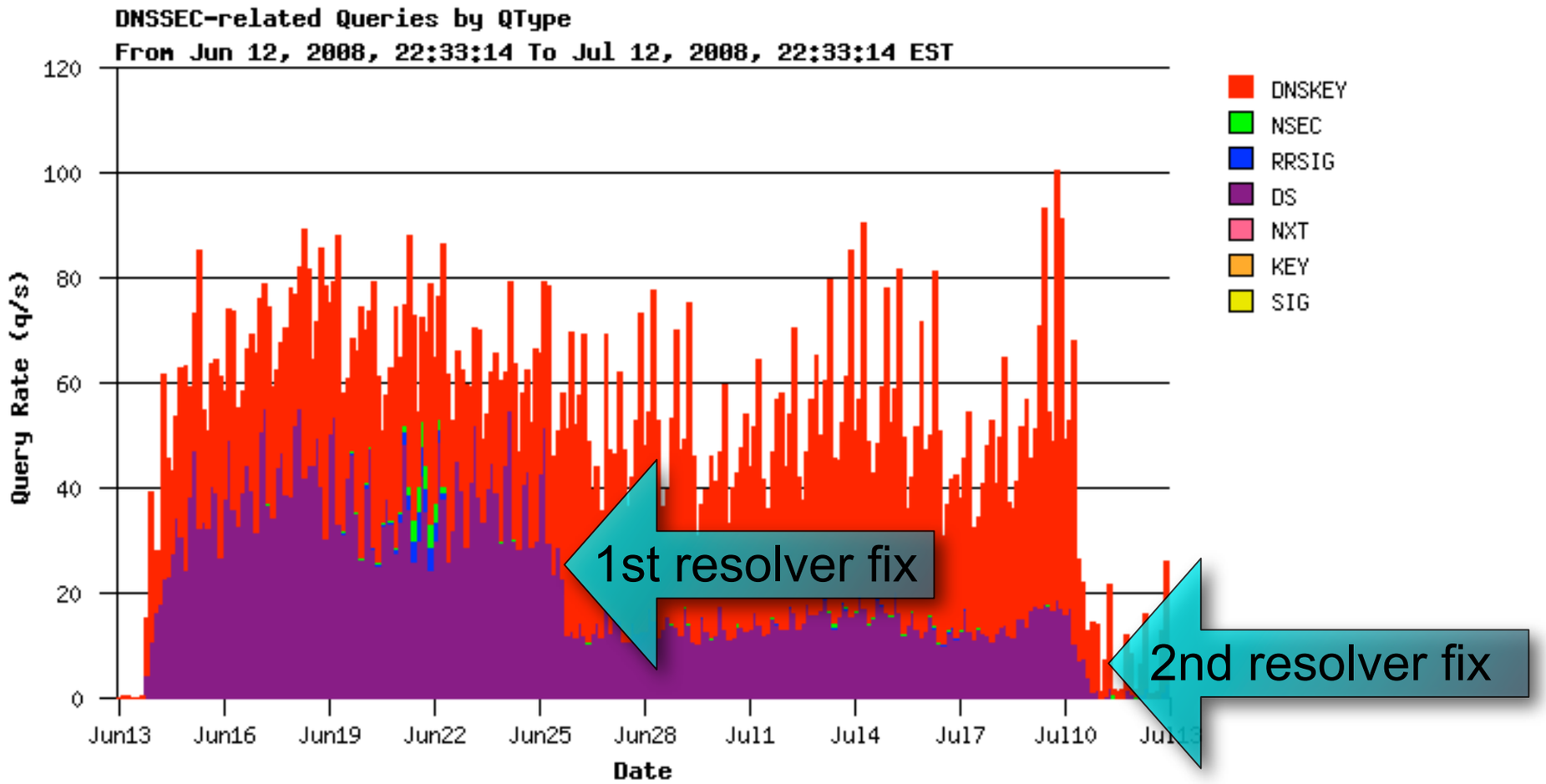
Sweden, june 2008

Was this a one off event?



Sweden, june 2008

Was this a one off event?



Sweden, june 2008

Why so many Queries?

- Resolvers are supposed to cache dnskey
- Even when those are bad
- Resolvers should be nice, not aggressive
- So many resolvers, so few servers

Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

www.dnssec.se

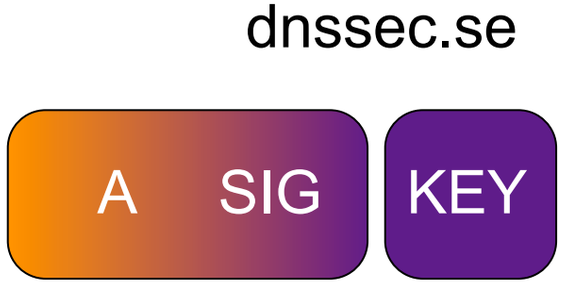
A SIG

root

TA

Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:



Why so many Queries?

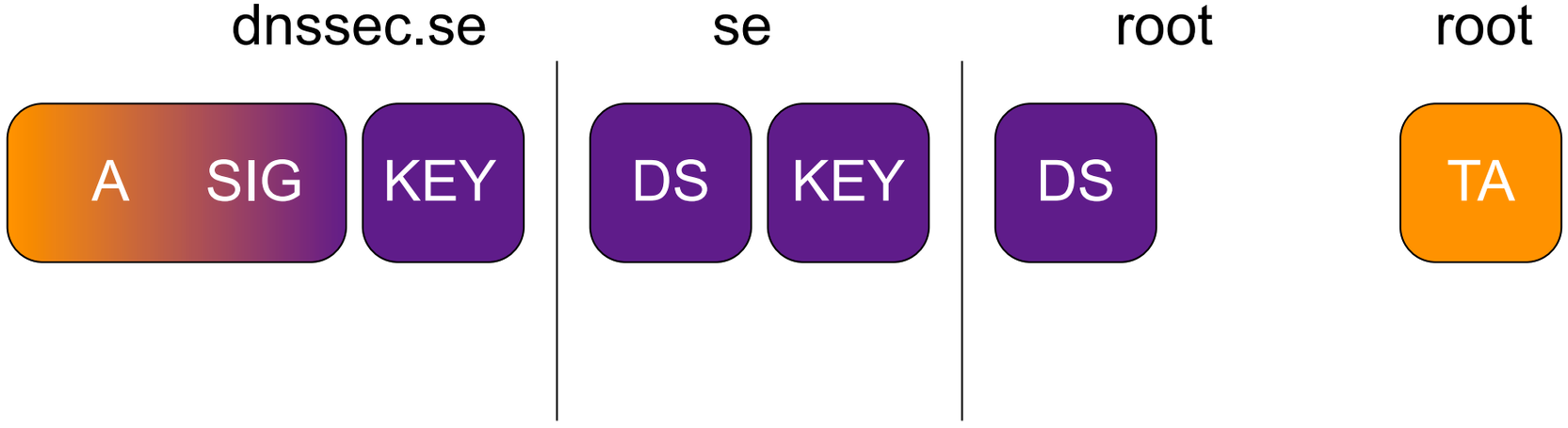
- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

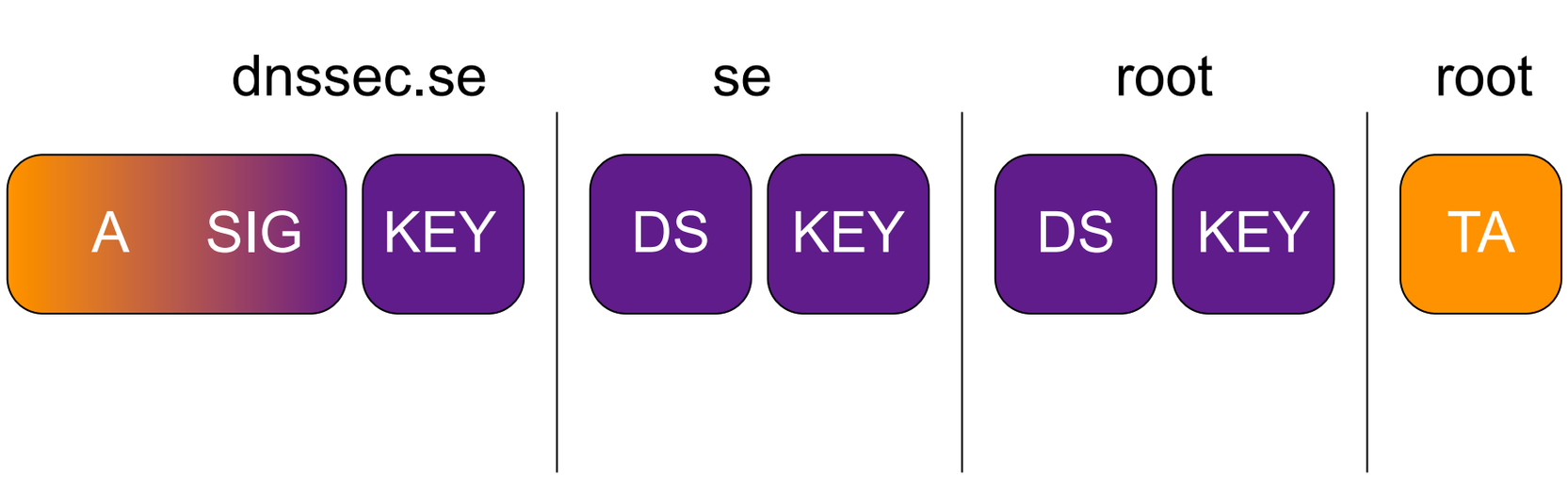
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:



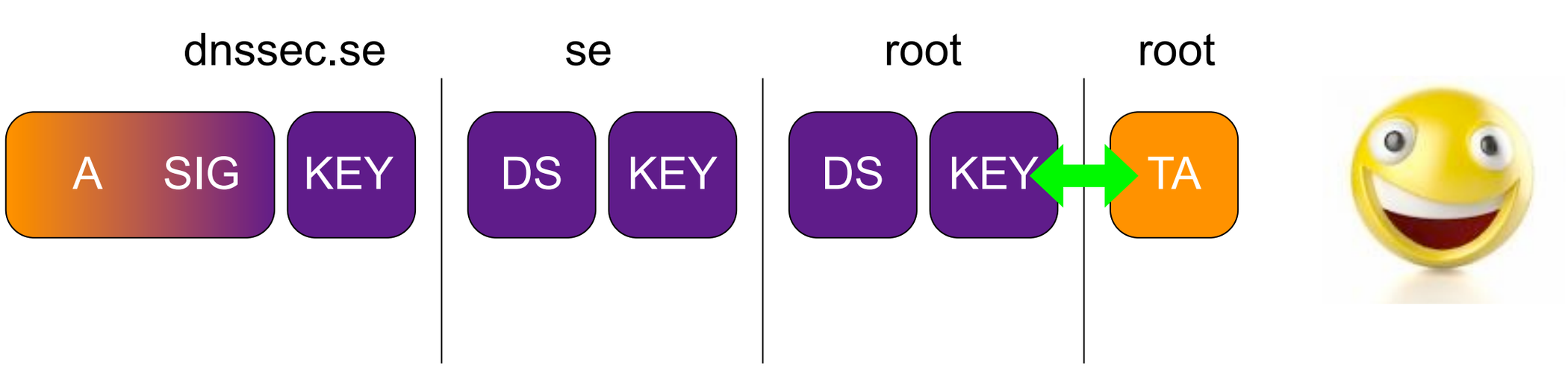
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:



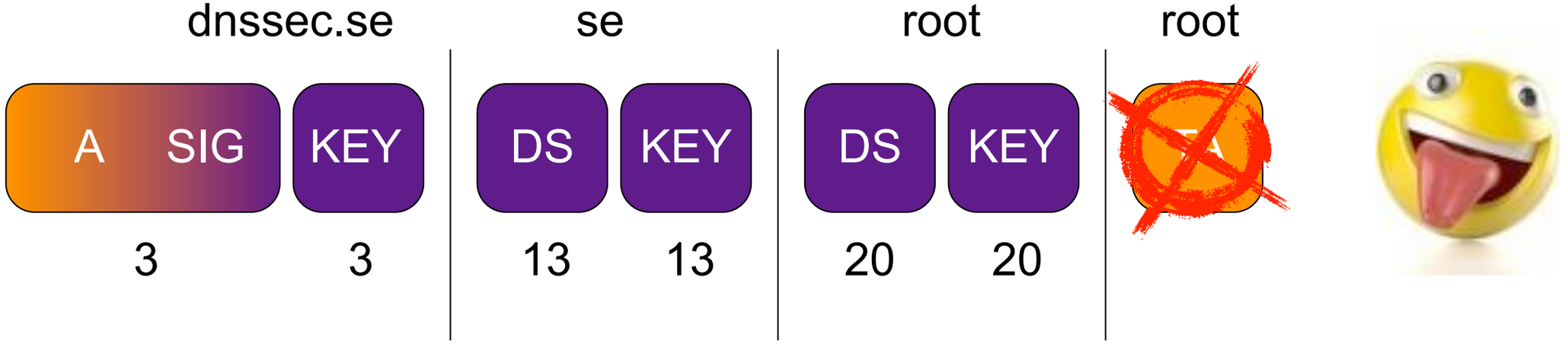
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:



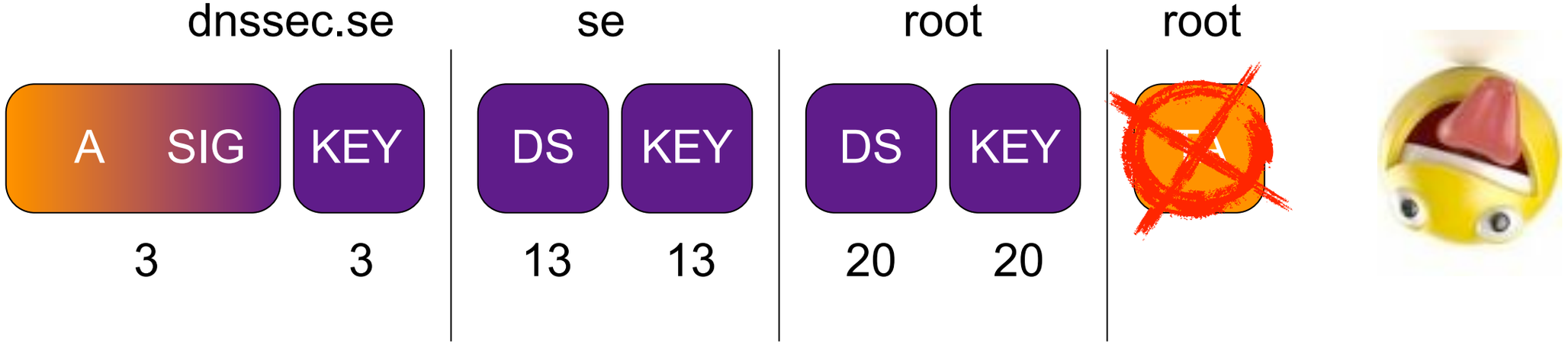
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:



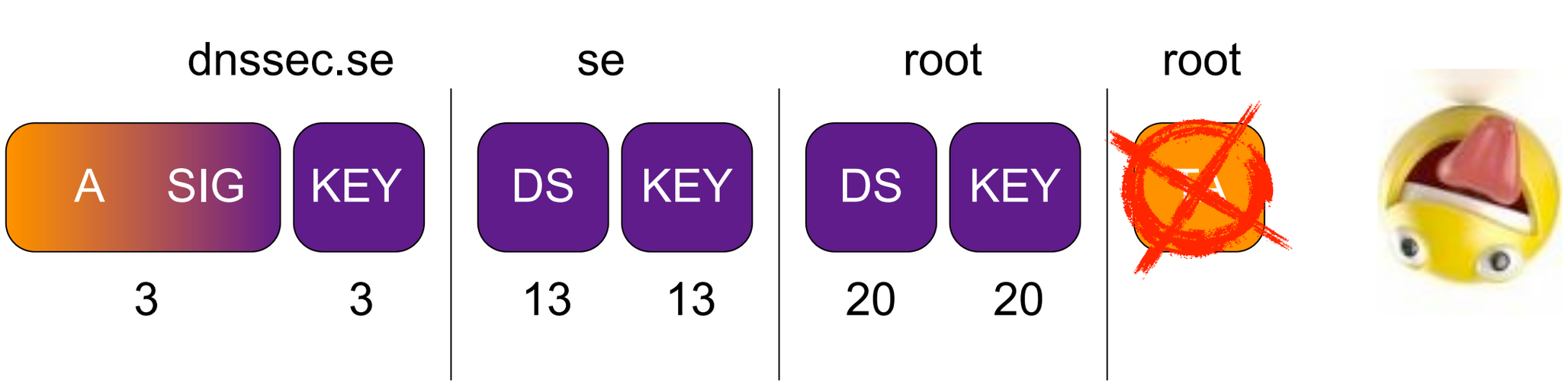
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:



Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:



3 * 3 * 13 * 13 * 20 * 20 = 608400 queries

ISC

- Reported the depth first search bug on februari 8th

ISC

- Reported the depth first search bug on februari 8th
- Acknowledged the problem
  - fundamental fix, needs thorough testing.

ISC

- Reported the depth first search bug on februari 8th
- Acknowledged the problem
  - fundamental fix, needs thorough testing.
- released BIND 9.7.0 with bug
  - first version that can validate the root
  - “Exercise caution”, ignores the lame DS issue

ISC

- Reported the depth first search bug on februari 8th
- Acknowledged the problem
  - fundamental fix, needs thorough testing.
- released BIND 9.7.0 with bug
  - first version that can validate the root
  - “Exercise caution”, ignores the lame DS issue
- released BIND 9.6.2 with bug
  - root-validation back ported, no 5011
    - tick tock

ISC

- Reported the depth first search bug on februari 8th
- Acknowledged the problem
  - fundamental fix, needs thorough testing.
- released BIND 9.7.0 with bug
  - first version that can validate the root
  - “Exercise caution”, ignores the lame DS issue
- released BIND 9.6.2 with bug
  - root-validation back ported, no 5011
    - tick tock
- Announced a patch as soon as possible.
  - still waiting
  - folks are deploying 9.7.0 and 9.6.2 right now

The Perfect Storm

- DNSSEC deployment at root (DURZ)
  - guess what: lame trust-anchor, don’t configure

The Perfect Storm

- DNSSEC deployment at root (DURZ)
  - guess what: lame trust-anchor, don’t configure

The Perfect Storm

The Perfect Storm

- No automatic trust anchor roll (5011)
  - 9.7.0 implementation is buggy
    - promised fix in 9.7.1
  - 9.6.2 not planned

The Perfect Storm

- No automatic trust anchor roll (5011)
  - 9.7.0 implementation is buggy
    - promised fix in 9.7.1
  - 9.6.2 not planned
- DLV mishaps:
  - DLV registry promiscuously scrapes TLD keys
    - Just another chain of trust
  - .PR rolled its key
    - was unavailable to DLV users for days
    - caused a major packet storm

The Perfect Storm

- Multiple trust anchor problem
  - TLD Trust Anchors trump Root Trust Anchor
    - stale TLD Trust Anchor trumps valid Root Trust Anchor

The Perfect Storm

- Multiple trust anchor problem
  - TLD Trust Anchors trump Root Trust Anchor
    - stale TLD Trust Anchor trumps valid Root Trust Anchor

- Doom scenario:
  - TLD registers DS in root
  - new policy: don’t announce rolls, depend on root
    - That is the way NS records works as well
  - Operators won’t update TLD trust anchor anymore
    - Why would they, they’ve configured root trust-anchor

A Series Of Unfortunate Events

A Series Of Unfortunate Events

- buggy software

A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root

A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
- multiple trust anchor problem

A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
- multiple trust anchor problem
- no 5011 deployment

A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
- multiple trust anchor problem
- no 5011 deployment
- opportunistic DLV scraping

A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
- multiple trust anchor problem
- no 5011 deployment
- opportunistic DLV scraping
- Frequent Rollover Syndrome
  - rolling rolling rolling, keep them DNSKEYs rolling.

Frequent Rollover Syndrome

- Advice seems to be:
  - roll the key as often as you can
  - Some roll twice a year, some roll monthly

Frequent Rollover Syndrome

- Advice seems to be:
  - roll the key as often as you can
  - Some roll twice a year, some roll monthly
- Advice is completely misguided:
  - too many sigs do not leak the key.
  - Intention is to mitigate a compromised key fallout
  - but there is no perfect forward security

Frequent Rollover Syndrome

- Advice seems to be:
  - roll the key as often as you can
  - Some roll twice a year, some roll monthly
- Advice is completely misguided:
  - too many sigs do not leak the key.
  - Intention is to mitigate a compromised key fallout
  - but there is no perfect forward security
- If a key can be compromised in 1 year, it can be compromised in 6 months for twice the cost

Frequent Rollover Syndrome

- Advice seems to be:
  - roll the key as often as you can
  - Some roll twice a year, some roll monthly
- Advice is completely misguided:
  - too many sigs do not leak the key.
  - Intention is to mitigate a compromised key fallout
  - but there is no perfect forward security
- If a key can be compromised in 1 year, it can be compromised in 6 months for twice the cost
- Other reasons: educate operators, exercise procedures
  - all irrelevant, never mess with a critical production system

Solution

- Fix the buggy software already
  - stop releasing versions that have problems
  - (Help fund BIND-10)
- Don’t roll keys (too often)
  - be practical
- Do not endorse configuration of trust-anchors when parent is signed.
  - no 5011, no web-page with listed keys, no DLV, no ITAR
  - Manage all through a signed parent.
- When parent is not signed:
  - Use proper 5011. Use ISC’s DLV.

Questions ? Remarks ? Observations ?

http://www.potaroo.net/ispcol/2010-02/rollover.html

Thanks to
Anand Buddhdev
Patrik Wallström
George Michaelson
Geoff Huston
David Conrad
Folks at ISC

Questions ? Remarks ? Observations ?

http://www.potaroo.net/ispcol/2010-02/rollover.html

Thanks to
Anand Buddhdev
Patrik Wallström
George Michaelson
Geoff Huston
David Conrad
Folks at ISC

Question: If you've deployed DNSSEC and rolled your (ksk) key, look at the stats around that period, and (pretty) please report them back to us.