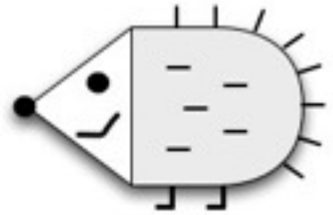
Hedgehog



OARC
Amsterdam, May 2015

John Dickinson
jad@sinodun.com

ICANN DNS Operations Team

Hedgehog History

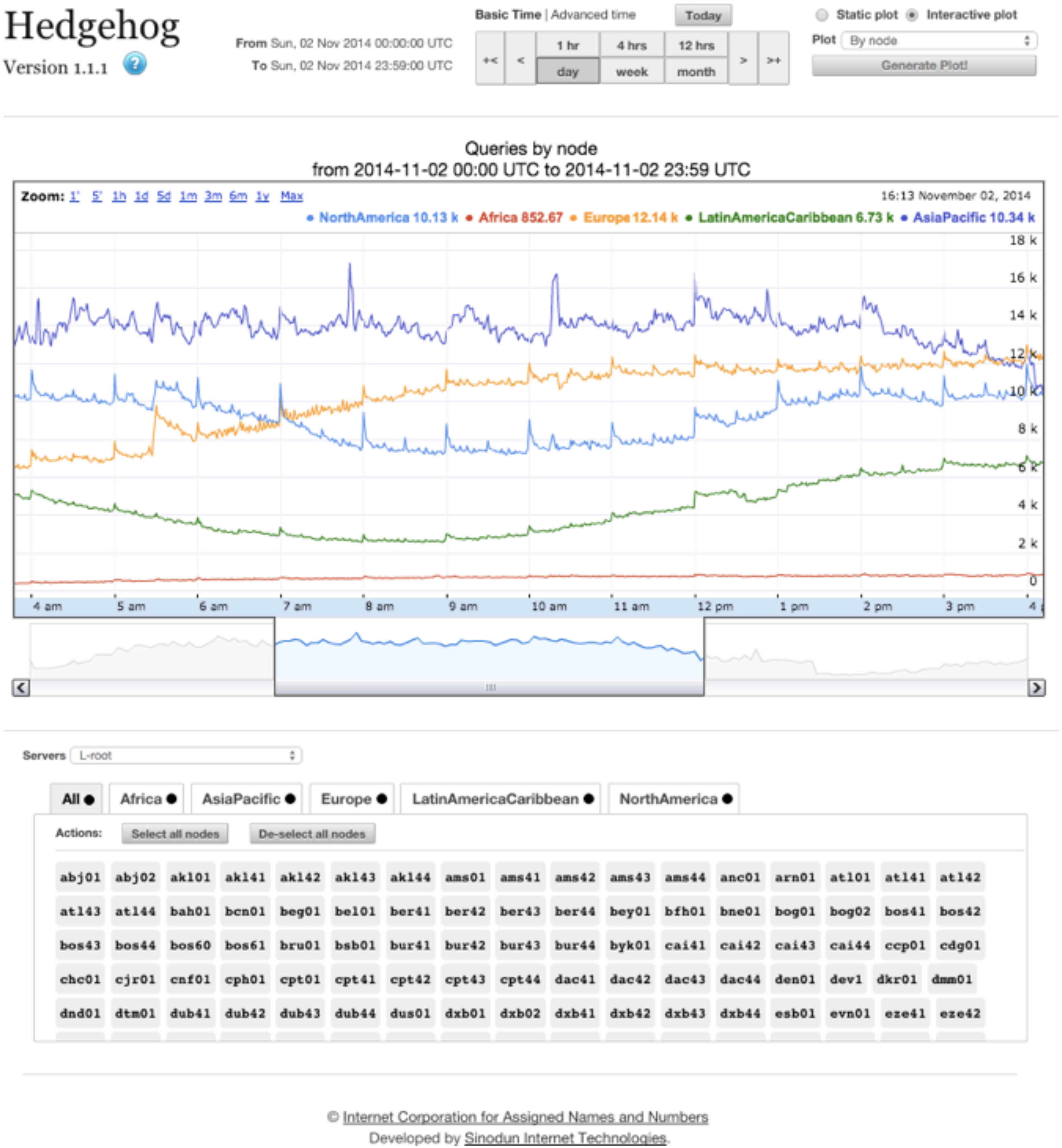
- Developed originally for ICANN.
  - Looking at root health
  - L-root has many nodes. (>300 rsync over ssh connections every minute!)
  - Old DSC presenter unable to scale - needed solution that could be extended to do further analysis of data
- ICANN using 1.x in production since mid 2013:
  - http://hedgehog.dns.icann.org/hedgehog/hedgehog.html

What is Hedgehog Today?

- A new web interface for DNS real-time traffic data
- Powered by R, jquery and Google Charts
    - R is a statistical analysis language
- Choice of Google charts or static PNG plots
    - Choice of SVG or Flash for the Google charts
- RSSAC reports in YAML (and plots) for 4 traffic metrics

What is Hedgehog Today?

- A “drop in” consumer of DSC XML files written in C++ (STL and Boost)
    - Uses PostgreSQL storage
- Able to Import DSC XML or DCS DAT to PostgreSQL
- Can still do XML to DAT for those who really want it



Hedgehog
Version 1.1.1
Basic Time | Advanced time
Today
○ Static plot ● Interactive plot
Plot By node
+< < 1 hr 4 hrs 12 hrs > >+
day week month
Generate Plot!

From Sun, 02 Nov 2014 00:00:00 UTC
To Sun, 02 Nov 2014 23:59:00 UTC

Queries by node
from 2014-11-02 00:00 UTC to 2014-11-02 23:59 UTC

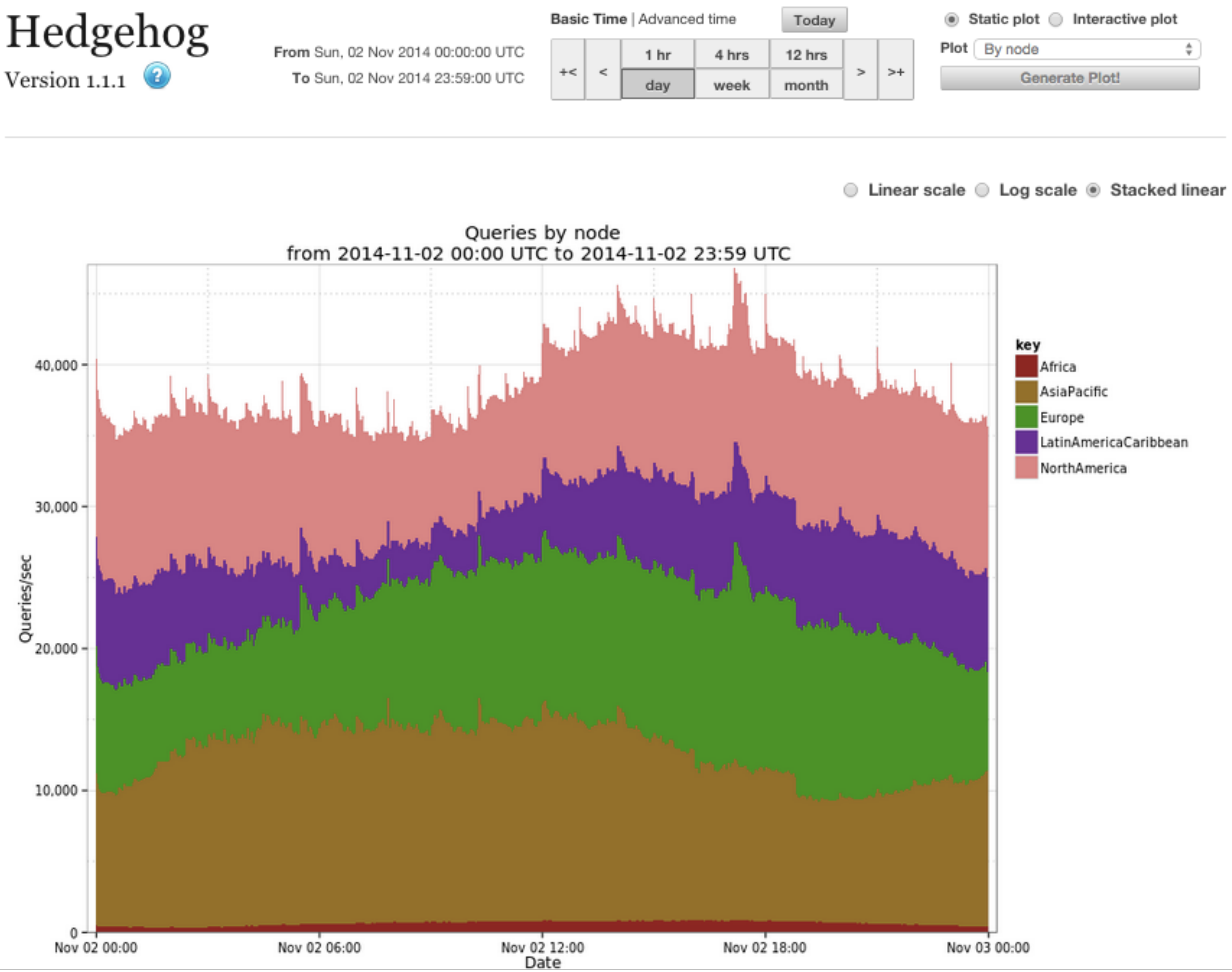
Zoom: 1' 5' 1h 1d 5d 1m 3m 6m 1y Max
16:13 November 02, 2014
● NorthAmerica 10.13 k ● Africa 852.67 ● Europe 12.14 k ● LatinAmericaCaribbean 6.73 k ● AsiaPacific 10.34 k
18 k
16 k
14 k
12 k
10 k
8 k
6 k
4 k
2 k
0
4 am
5 am
6 am
7 am
8 am
9 am
10 am
11 am
12 pm
1 pm
2 pm
3 pm
4

Servers L-root

All ● Africa ● AsiaPacific ● Europe ● LatinAmericaCaribbean ● NorthAmerica ●
Actions: Select all nodes De-select all nodes

abj01 abj02 akl01 akl41 akl42 akl43 akl44 ams01 ams41 ams42 ams43 ams44 anc01 arn01 atl01 atl41 atl42
atl43 atl44 bah01 bcn01 beg01 bel01 ber41 ber42 ber43 ber44 bey01 bfh01 bne01 bog01 bog02 bos41 bos42
bos43 bos44 bos60 bos61 bru01 bsb01 bur41 bur42 bur43 bur44 byk01 cai41 cai42 cai43 cai44 ccp01 cdg01
chc01 cjr01 cnf01 cph01 cpt01 cpt41 cpt42 cpt43 cpt44 dac41 dac42 dac43 dac44 den01 dev1 dkr01 dmm01
dnd01 dtm01 dub41 dub42 dub43 dub44 dus01 dxb01 dxb02 dxb41 dxb42 dxb43 dxb44 esb01 evn01 eze41 eze42

© Internet Corporation for Assigned Names and Numbers
Developed by Sinodun Internet Technologies.



Hedgehog

Version 1.1.1

From Sun, 02 Nov 2014 00:00:00 UTC

To Sun, 02 Nov 2014 23:59:00 UTC

Basic Time | Advanced time

● Static plot ○ Interactive plot

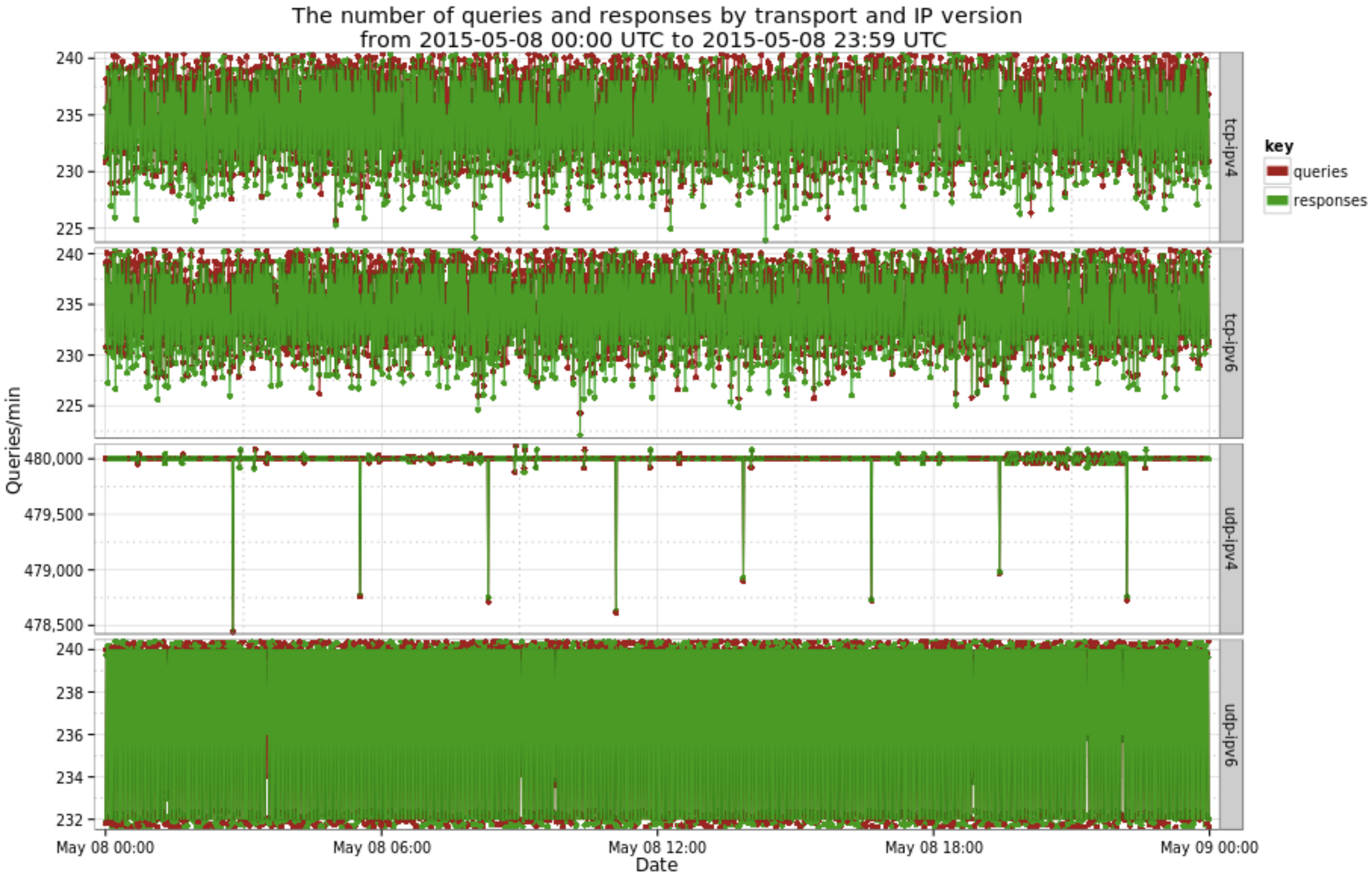
Plot By node

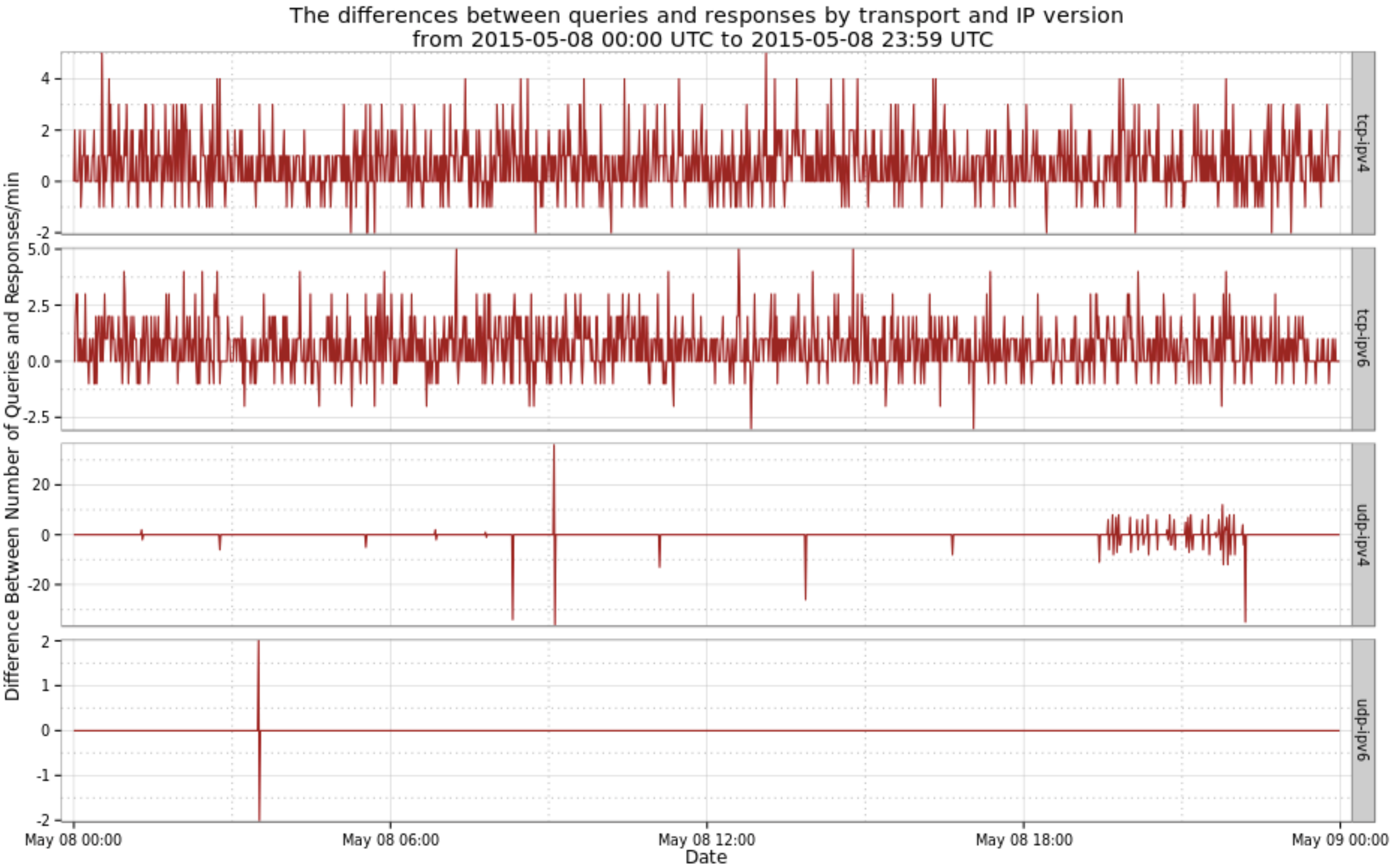
○ Linear scale ○ Log scale ● Stacked linear

Queries by node
from 2014-11-02 00:00 UTC to 2014-11-02 23:59 UTC

Hedgehog 2.0

- Now at version 2.0.0b2 (http://demo.sinodun.com)
  - Traffic volume plots now faceted
  - New Traffic Query/Response Difference plots
  - Support for Vagrant Provisioning (thanks melalj)
  - Better configuration and a few bug fixes
- Release candidate soon (weeks)


The number of queries and responses by transport and IP version
from 2015-05-08 00:00 UTC to 2015-05-08 23:59 UTC
Queries/min
240
235
230
225
tcp-ipv4
240
235
230
225
tcp-ipv6
480,000
479,500
479,000
478,500
udp-ipv4
240
238
236
234
232
udp-ipv6
May 08 00:00
May 08 06:00
May 08 12:00
May 08 18:00
May 09 00:00
Date
key
🟥 queries
🟩 responses


The differences between queries and responses by transport and IP version
from 2015-05-08 00:00 UTC to 2015-05-08 23:59 UTC
Difference Between Number of Queries and Responses/min
Date
tcp-ipv4
4
2
0
-2
tcp-ipv6
5.0
2.5
0.0
-2.5
udp-ipv4
20
0
-20
udp-ipv6
2
1
0
-1
-2
May 08 00:00
May 08 06:00
May 08 12:00
May 08 18:00
May 09 00:00

Hedgehog 2.1

- Improved TLD monitoring
- Make use of R to analyse the data
  - Want to “learn” what is normal and ‘healthy’
- Support non-traffic RSSAC metrics
- Add geo reporting features
- Packaging

Hedgehog Future…

- Further enhance statistical analysis of data
- Make the web interface more of a dash board
- Add data access API
- Test and port to other platforms.
- Add generic database layer

Data collection

- Currently consumes DSC generated data (XML, DAT)
- Requirements for replacement collector include (prototyping in progress):
    - Collector capable of running on the same machine as the nameserver
        - Resource management (e.g. throttle CPU, upload)
        - Support for some data processing on collector nodes

Data collection

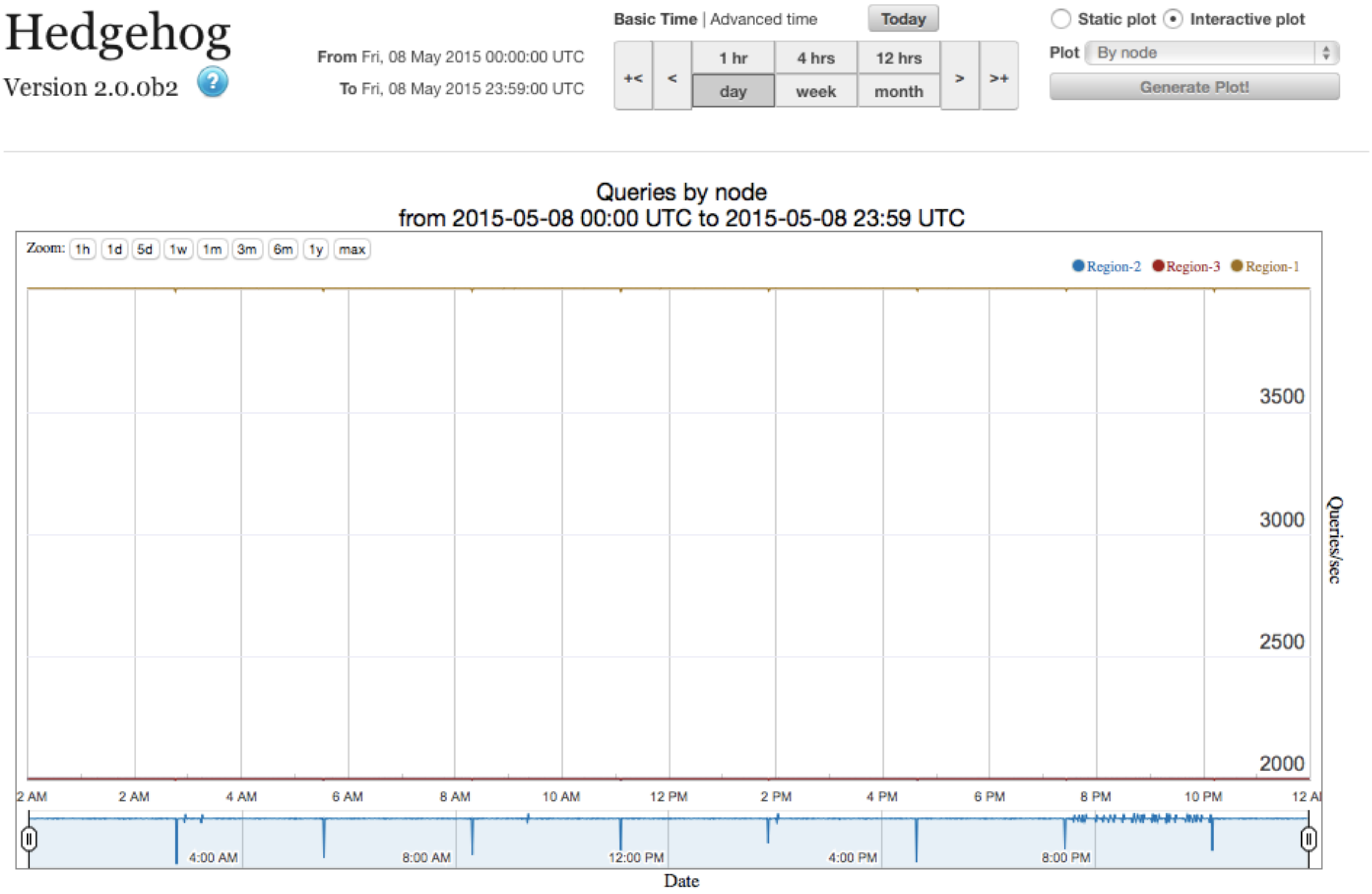
- Drill down to PCAP files
- Dynamic configuration (change what collected on demand)
- Standard data model
  - Intend to publish draft(s) on this soon
- Open Source
- Ubuntu and FreeBSD support at first

Open Source status

- Open source beta release of 2.0.0b2
  - Apache v2.0 license
  - website & mailing list: www.dns-stats.org
  - code: https://github.com/dns-stats/hedgehog
- Production release and active development ongoing

Appendix

- Screen shots…



Hedgehog

Version 2.0.0b2

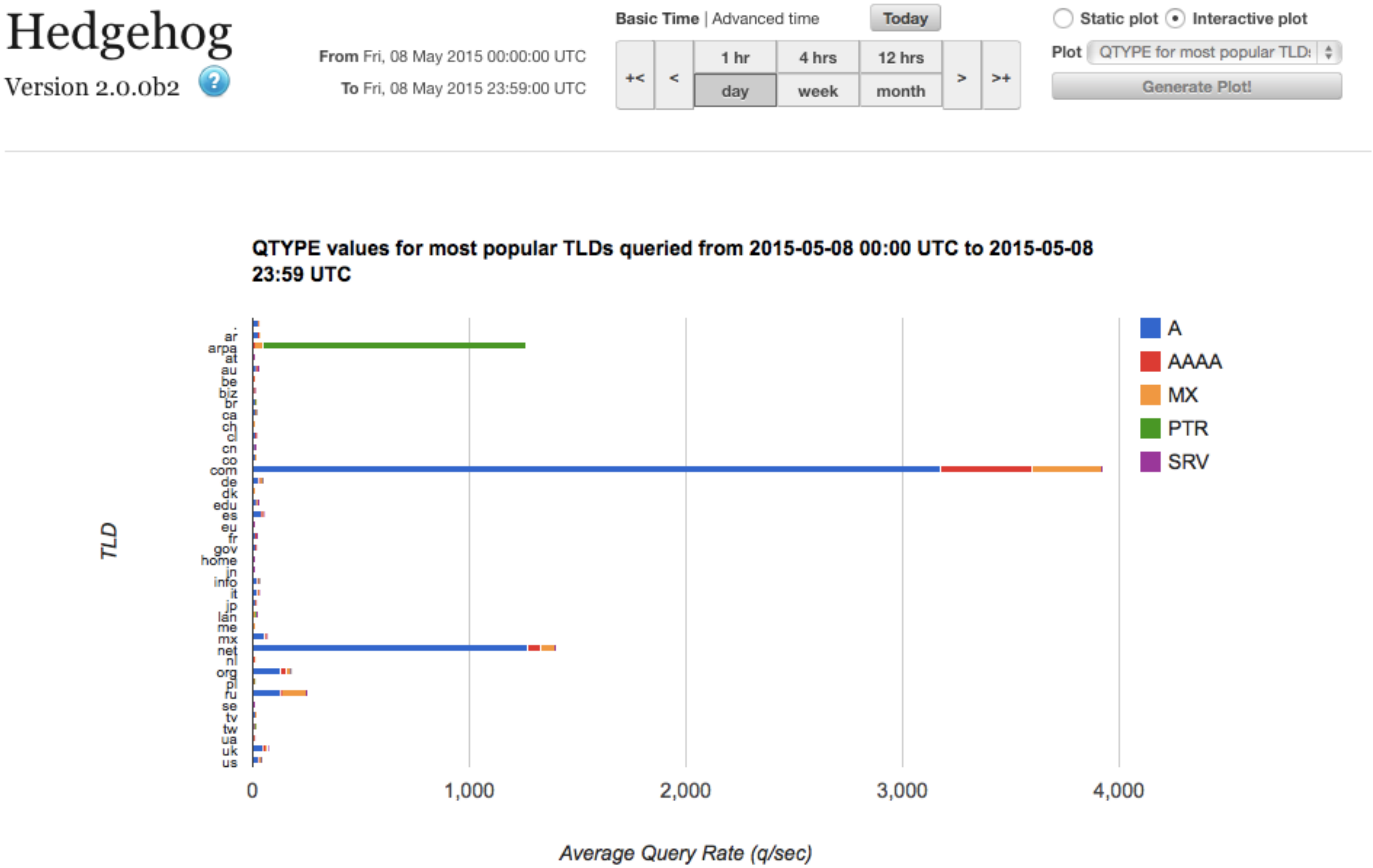
From Fri, 08 May 2015 00:00:00 UTC

To Fri, 08 May 2015 23:59:00 UTC

○ Static plot ● Interactive plot

Plot: By node

Queries by node
from 2015-05-08 00:00 UTC to 2015-05-08 23:59 UTC



Hedgehog

Version 2.0.0b2

From Fri, 08 May 2015 00:00:00 UTC

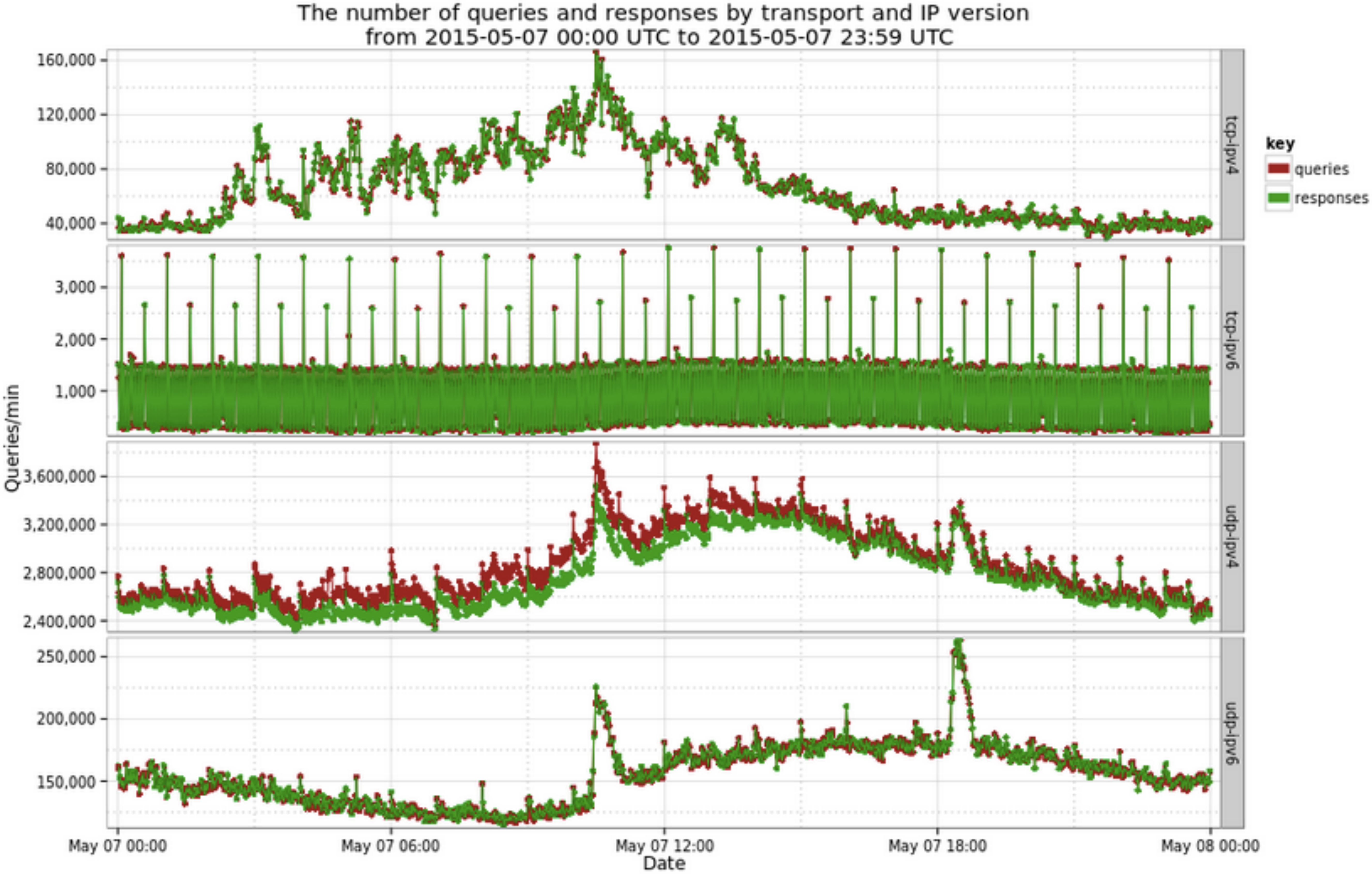
To Fri, 08 May 2015 23:59:00 UTC

Basic Time | Advanced time

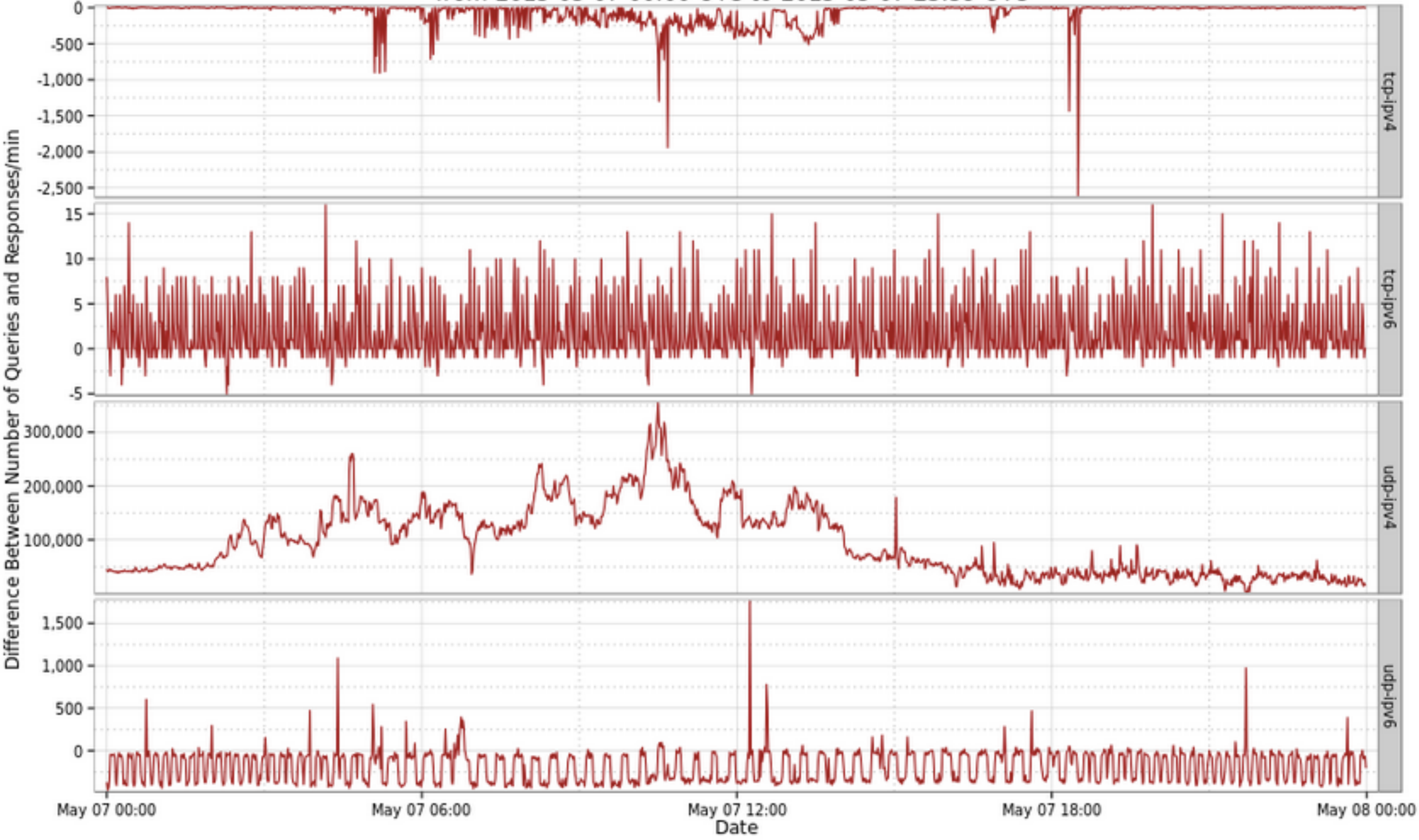
○ Static plot ● Interactive plot

Plot: QTYPE for most popular TLD:

QTYPE values for most popular TLDs queried from 2015-05-08 00:00 UTC to 2015-05-08 23:59 UTC


The number of queries and responses by transport and IP version
from 2015-05-07 00:00 UTC to 2015-05-07 23:59 UTC
160,000
120,000
80,000
40,000
tcp-ipv4
3,000
2,000
1,000
tcp-ipv6
3,600,000
3,200,000
2,800,000
2,400,000
udp-ipv4
250,000
200,000
150,000
udp-ipv6
Queries/min
May 07 00:00
May 07 06:00
May 07 12:00
May 07 18:00
May 08 00:00
Date
key
queries
responses

The differences between queries and responses by transport and IP version
from 2015-05-07 00:00 UTC to 2015-05-07 23:59 UTC


Difference Between Number of Queries and Responses/min
tcp-ipv4
tcp-ipv6
udp-ipv4
udp-ipv6
May 07 00:00
May 07 06:00
May 07 12:00
May 07 18:00
May 08 00:00
Date