Asia Pacific Network Information Centre

APNIC

DITL 2008-2009

George Michaelson

APNIC

ggm@apnic.net

Asia Pacific Network Information Centre

APNIC

ABOUT APNIC

The DG

The Chief Scientist

Asia Pacific Network Information Centre

APNIC

Office life at APNIC

Apologies to ESNOG attendees

- You've seen (most) of it before.
- …but there are some new bits.

Apologies to Everyone else

- You've seen (most) of it before.
- …but there are some new bits.
- But this is the 4th outing for this slidepack
  - Probably the last
- Many thanks to Rob B. who watched me crash-and-burn in Beijing and offered me a chance to redeem myself.

Belem is cool:
lambda calculus on the water

Belem is cool
matrix-maths in the streets

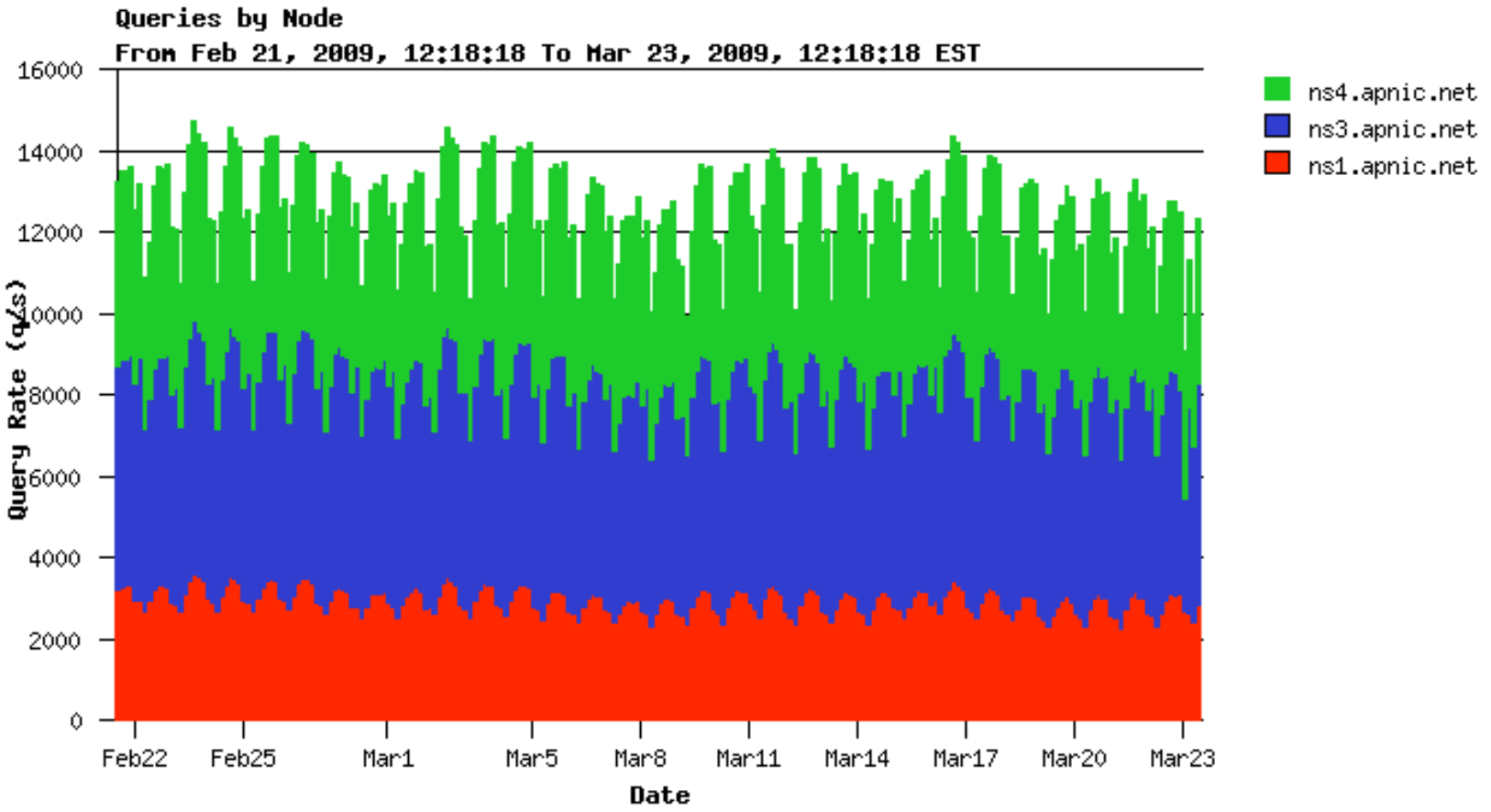
Madrid (ESNOG) was cool too!

Madrid (ESNOG) was cool too!

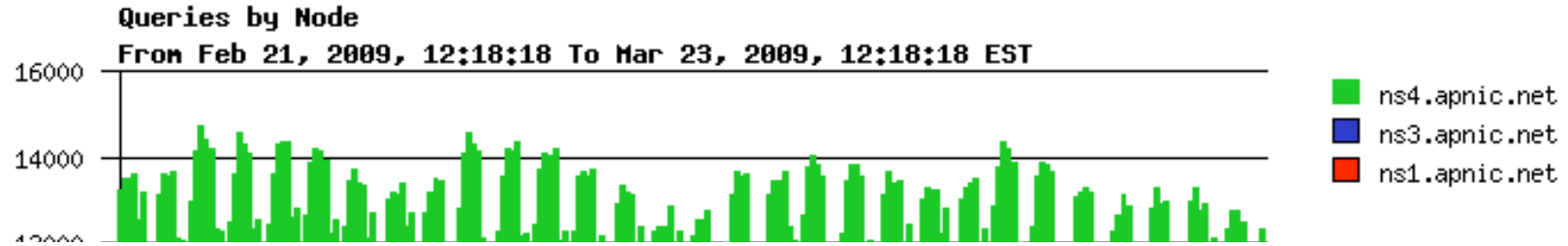
APNIC's DNS

- RIR's are the delegation point for in-addr, ip6 .arpa.
  - APNIC Master DNS for the Asia-Pacific reverse-DNS
    - Has secondary servers for other RIR in AP region. Lower RTT
- DNS @ APNIC, two 'flavours'
  - The 'NS' hosts
    - APNIC's primary NS for its in-addr.arpa/ip6.arpa duty
    - The entire Asia-Pacific managed IP address space
  - The 'SEC' hosts
    - Secondary NS for the other RIR (AfriNIC, LacNIC, RIPE)
    - A range of ccTLD, other forward namespaces of interest
- 3 locations: Brisbane, Tokyo, Hong Kong
  - Co Located, 100mbit switching fabric, good local connectivity

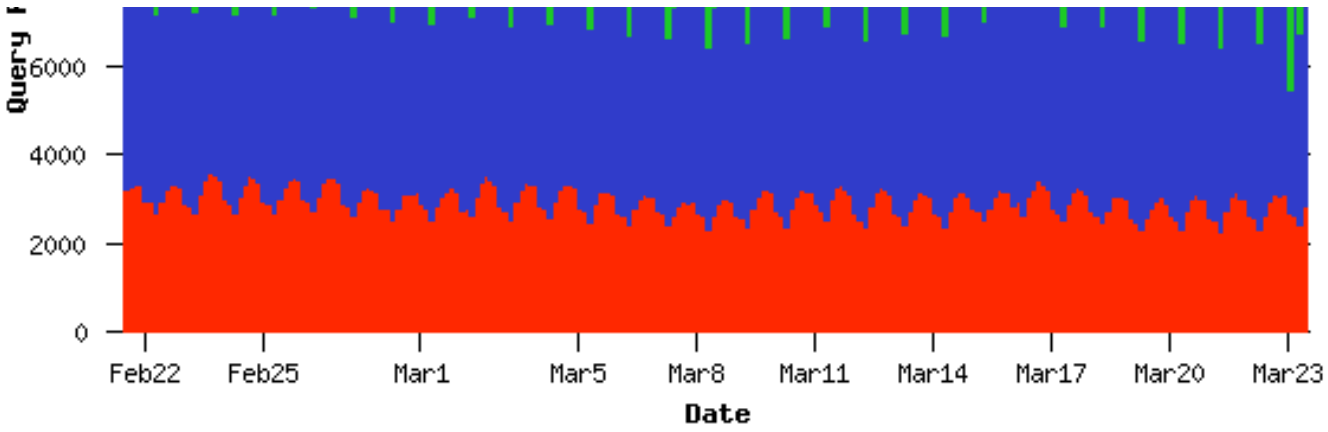
One month…



One month…



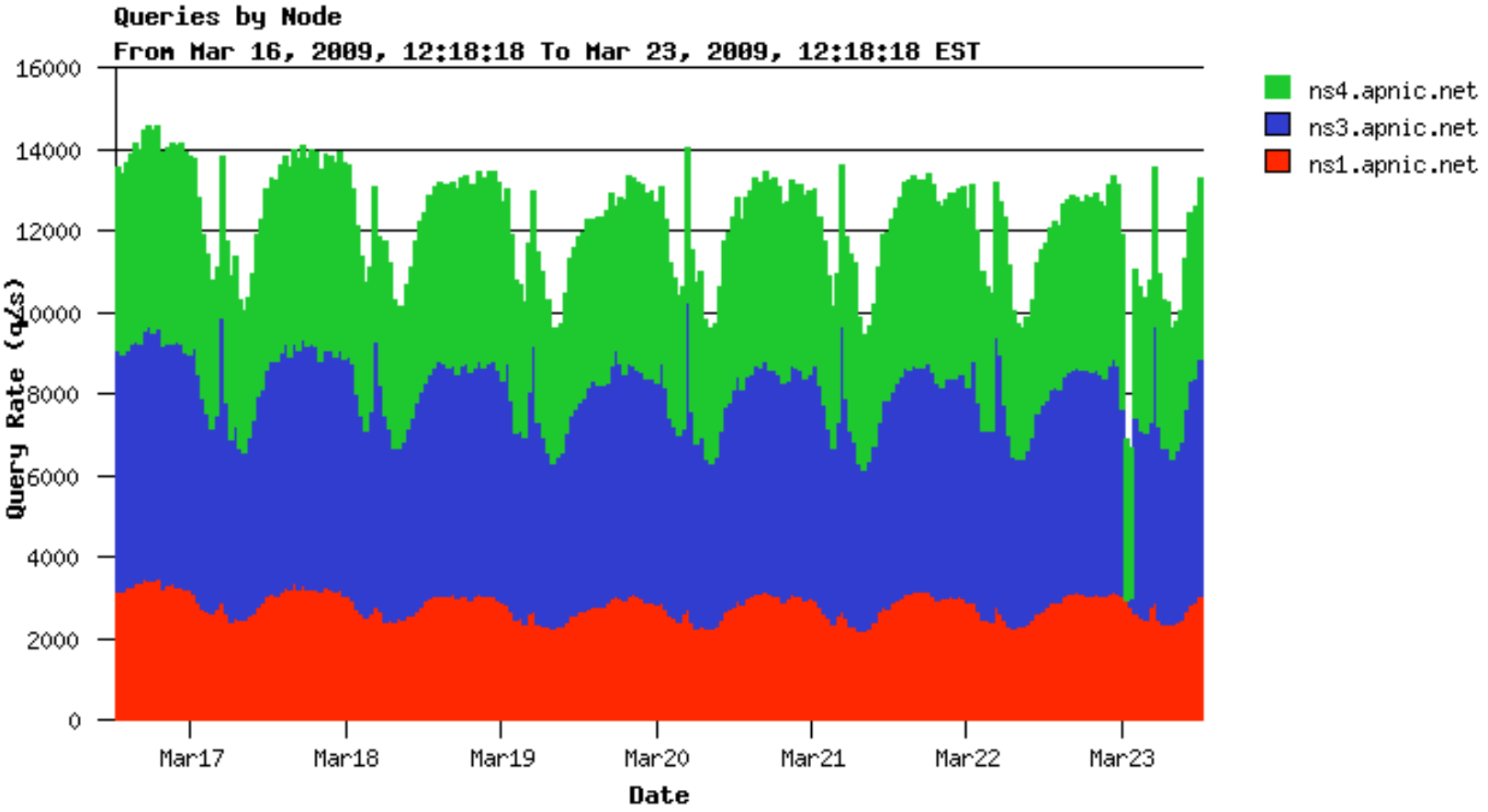
Most days look the same……



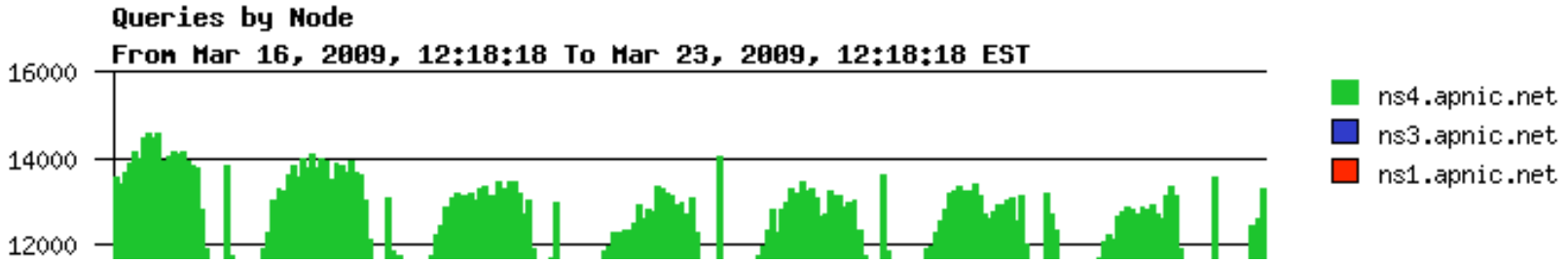
Asia Pacific Network Information Centre

APNIC

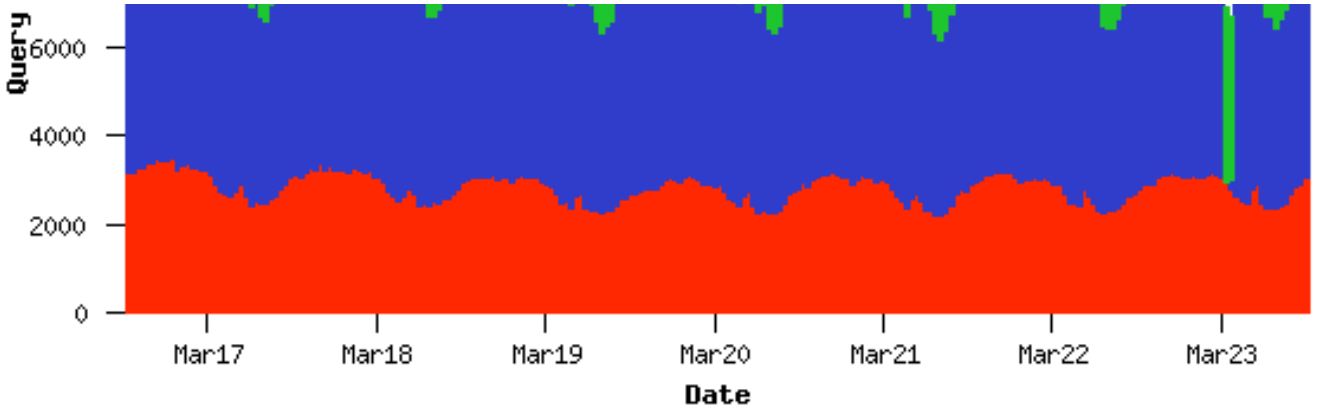
One Week…



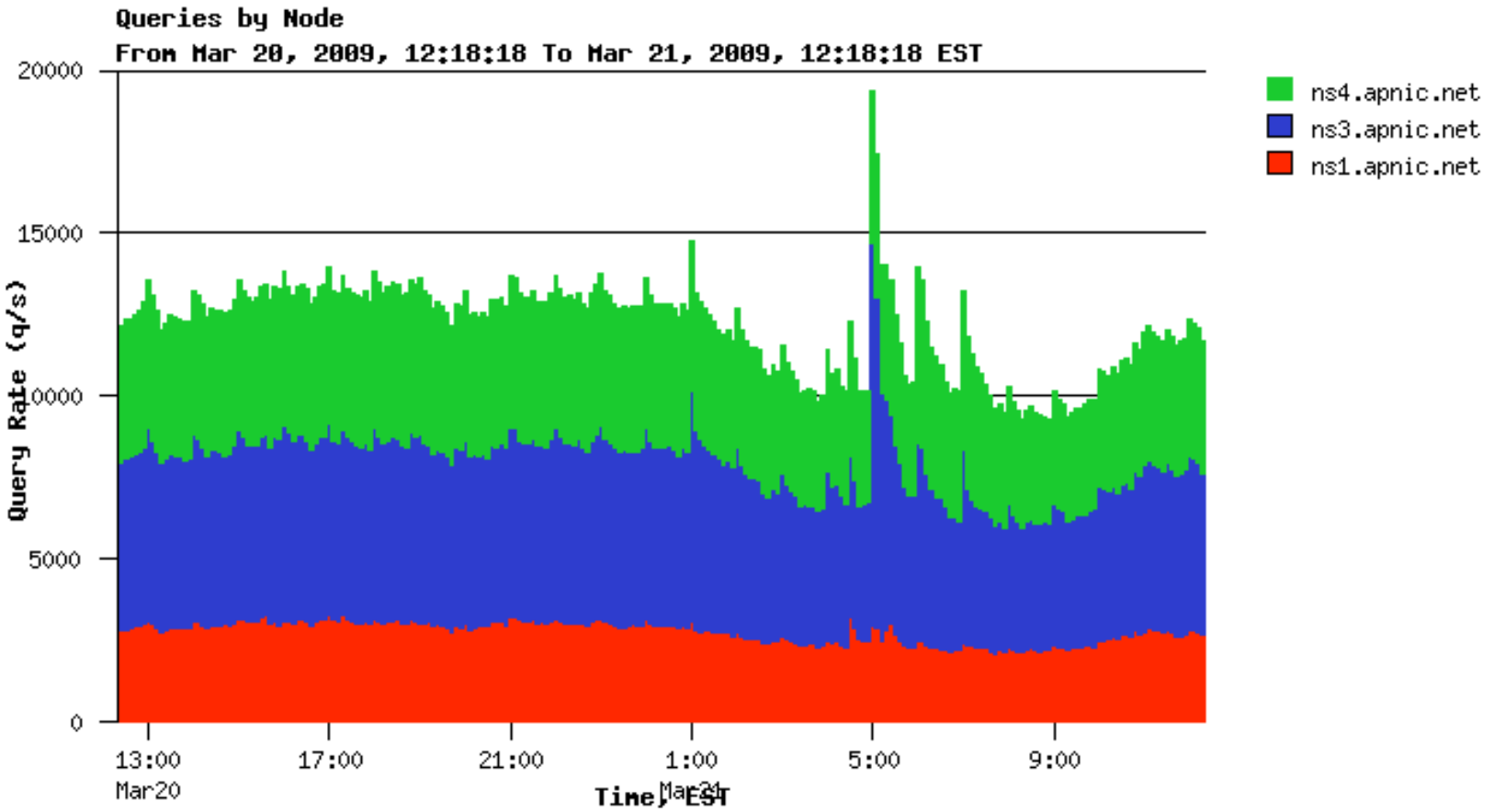
One Week…



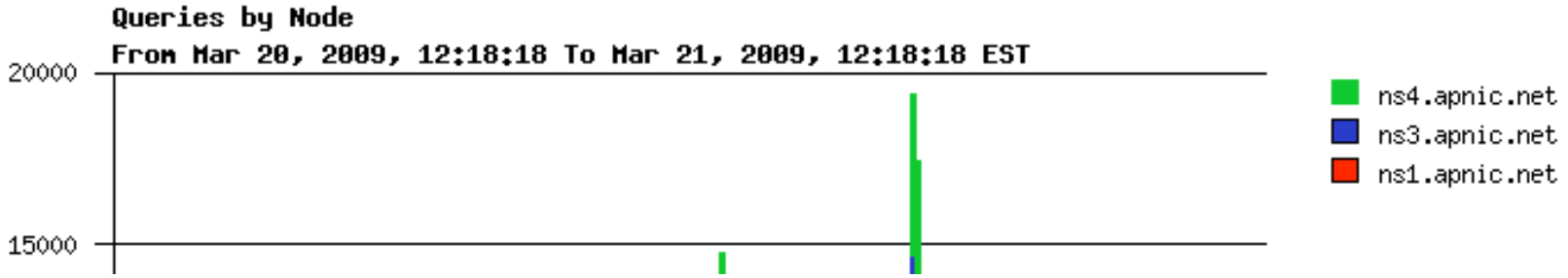
Regular behaviour in a day…



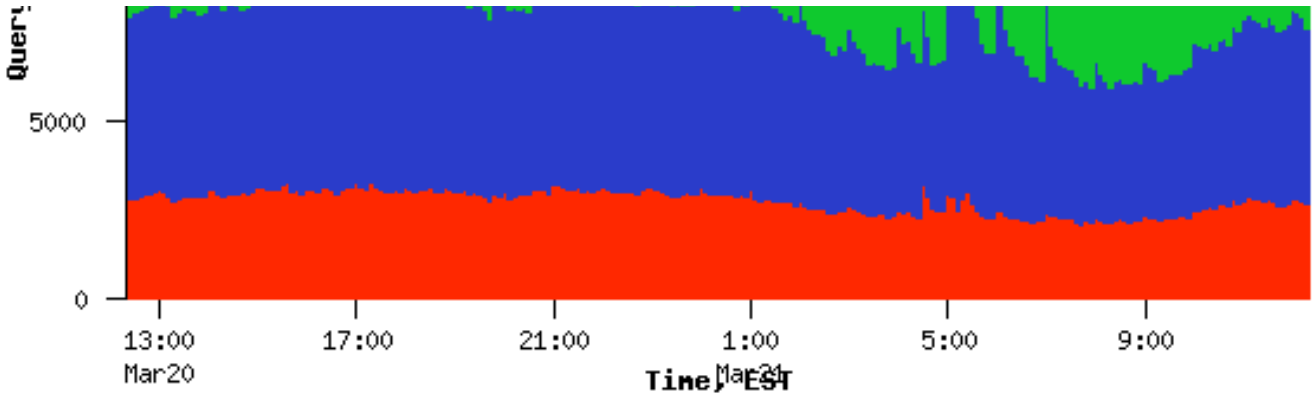
One Day …



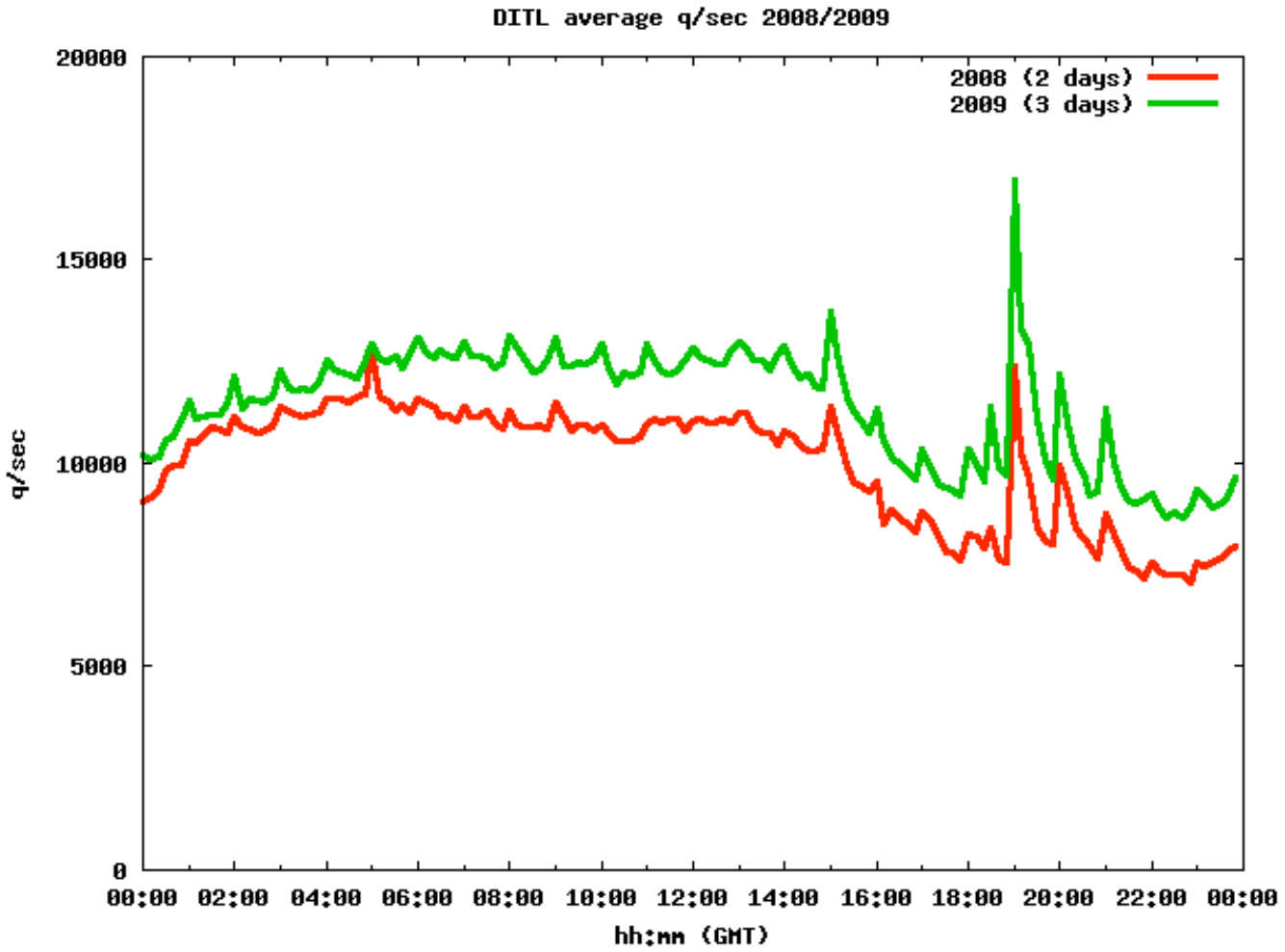
One Day …



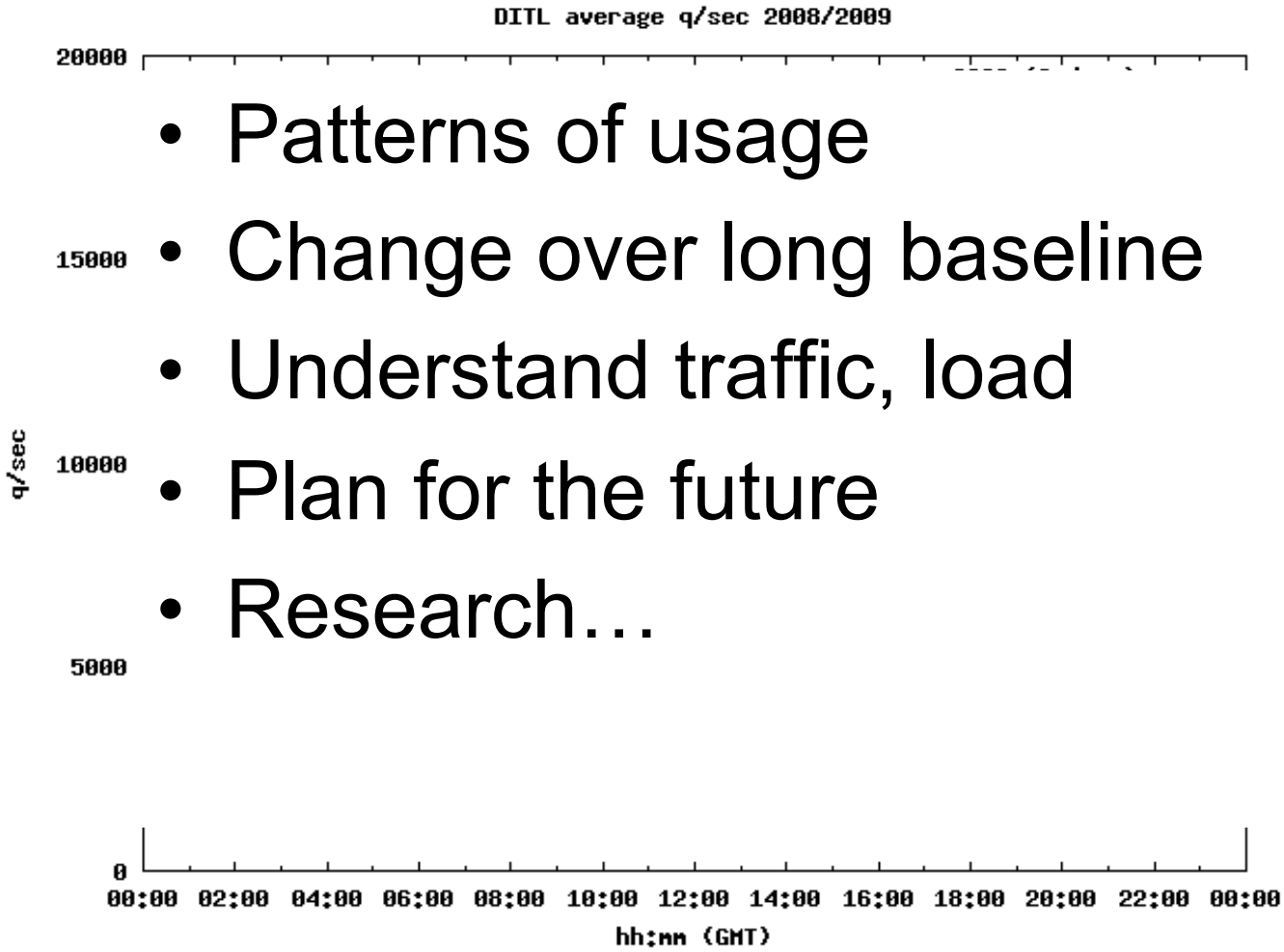
Interesting events in a day?



DITL 2008-2009 AP region



DITL 2008-2009 AP region



- Patterns of usage
- Change over long baseline
- Understand traffic, load
- Plan for the future
- Research…

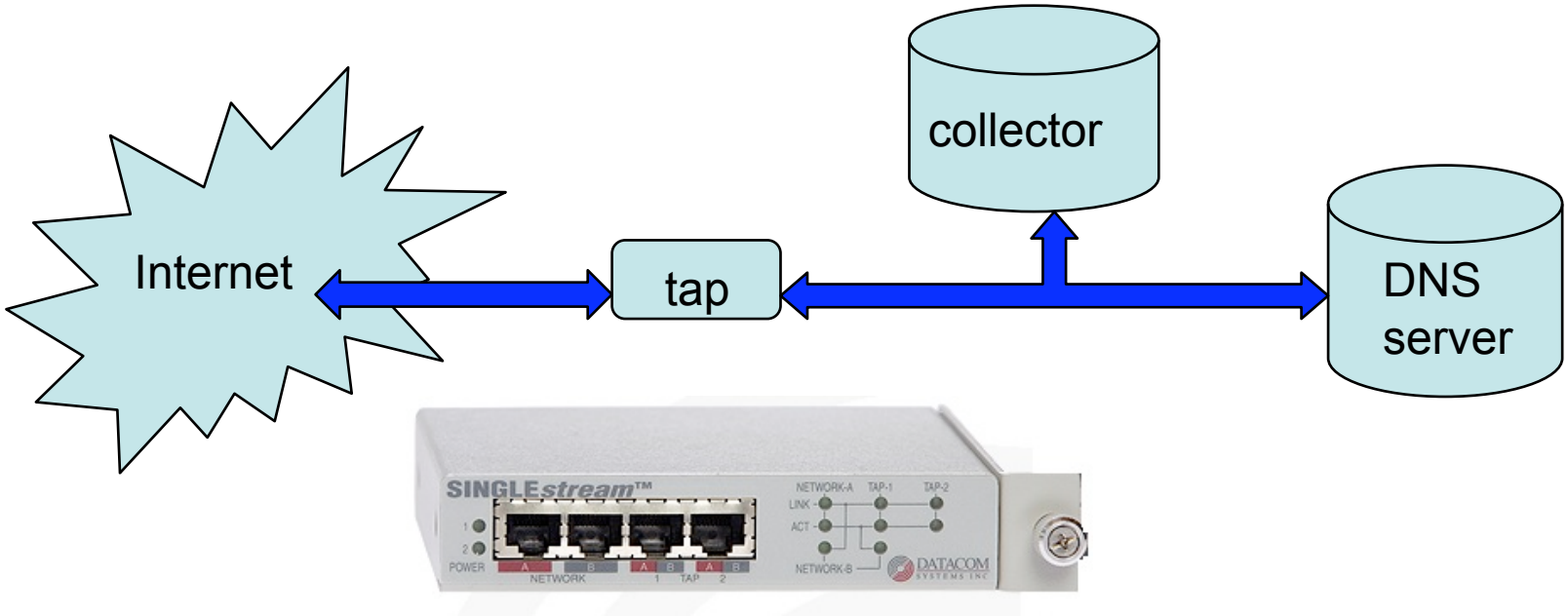
Day In The Life

- Continuous packet capture of DNS servers, IX, other places of interest
- Organized by CAIDA/OARC
- Provides resource for longer term analysis
  - Data archive warehouse
  - Opportunity for retrospective/review of data
- First collection 2006
  - 4 DNS participants, selected campus/local IX
- Fourth event (March 29-April2)
  - 37 participants, ~190 nodes of collection
  - Of the order 4Tb data (!)
- APNIC contributing since 2008 from all operated DNS servers
  - this only represents a subset of APNIC NS serve for its own domains. (secondary NS at other RIR)

Participants

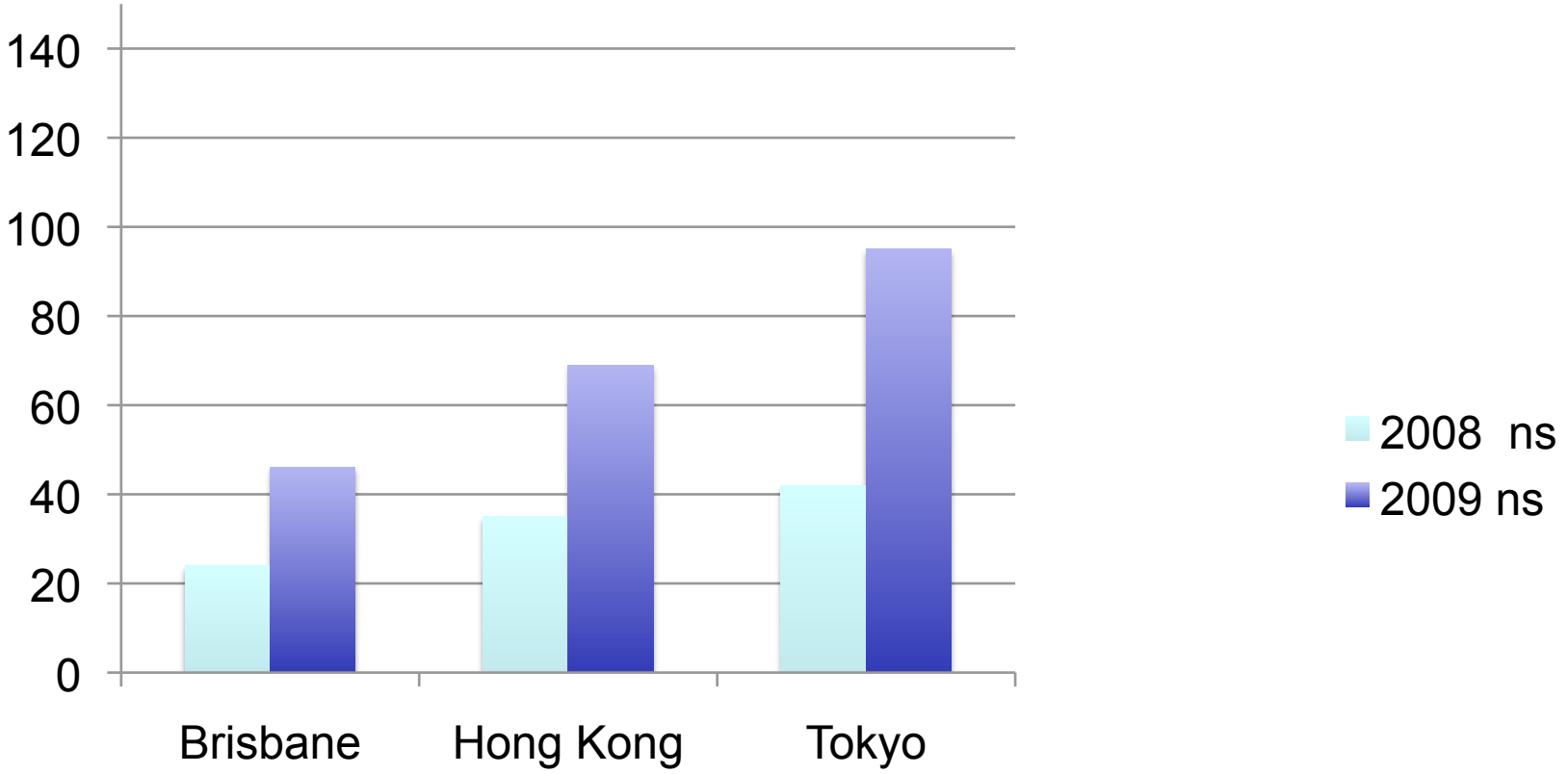
- afilias apnic arin arl as112-gf
- brave caida camel cira cogent
- cznic everydns icann iis isc
- isi lacnic level3 namex nasa
- nethelp niccl nixcz nominet nrcca
- oarc orsnb pktpush qwest regbr
- ripe switch ultradns uninett uniroma2
- verisign wide

Data Capture



- no packet loss data collection
  - 1 packet switchover to passive if power loss
- Collector doesn't impact DNS server cpu & disk cycles
- Offline storage, long term data retention

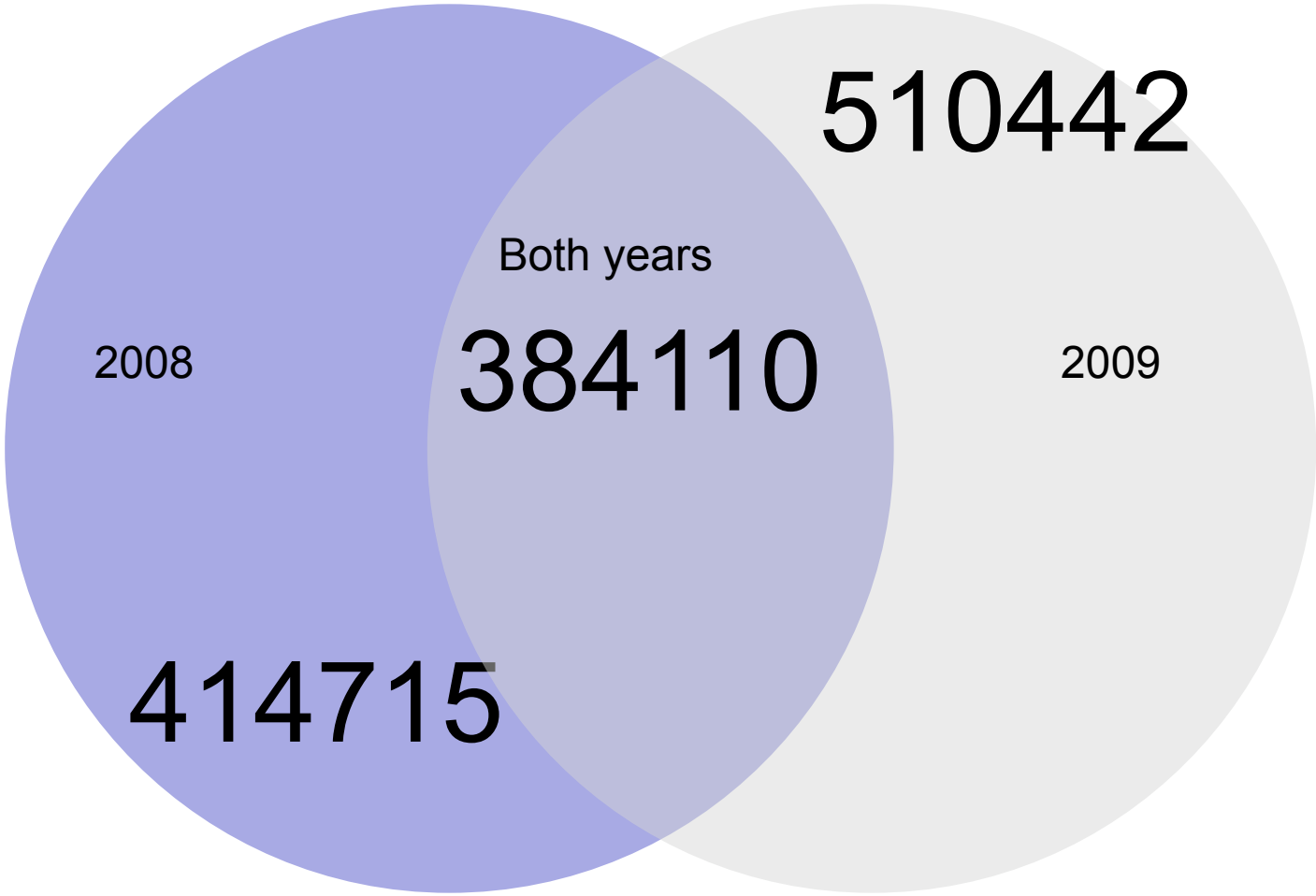
AP DiTL Data Capture (gb)



Brief quiz

- If you had DNS in 2008…
- Would you use the same IP address to do DNS in 2009?
  - (I would: I don't change my resolver that much)
- How many unique IP addresses seen in 2008 do you expect to see in 2009?
  - (I expected to see a lot. The majority in fact)
- …….

Unique IPs in 24h



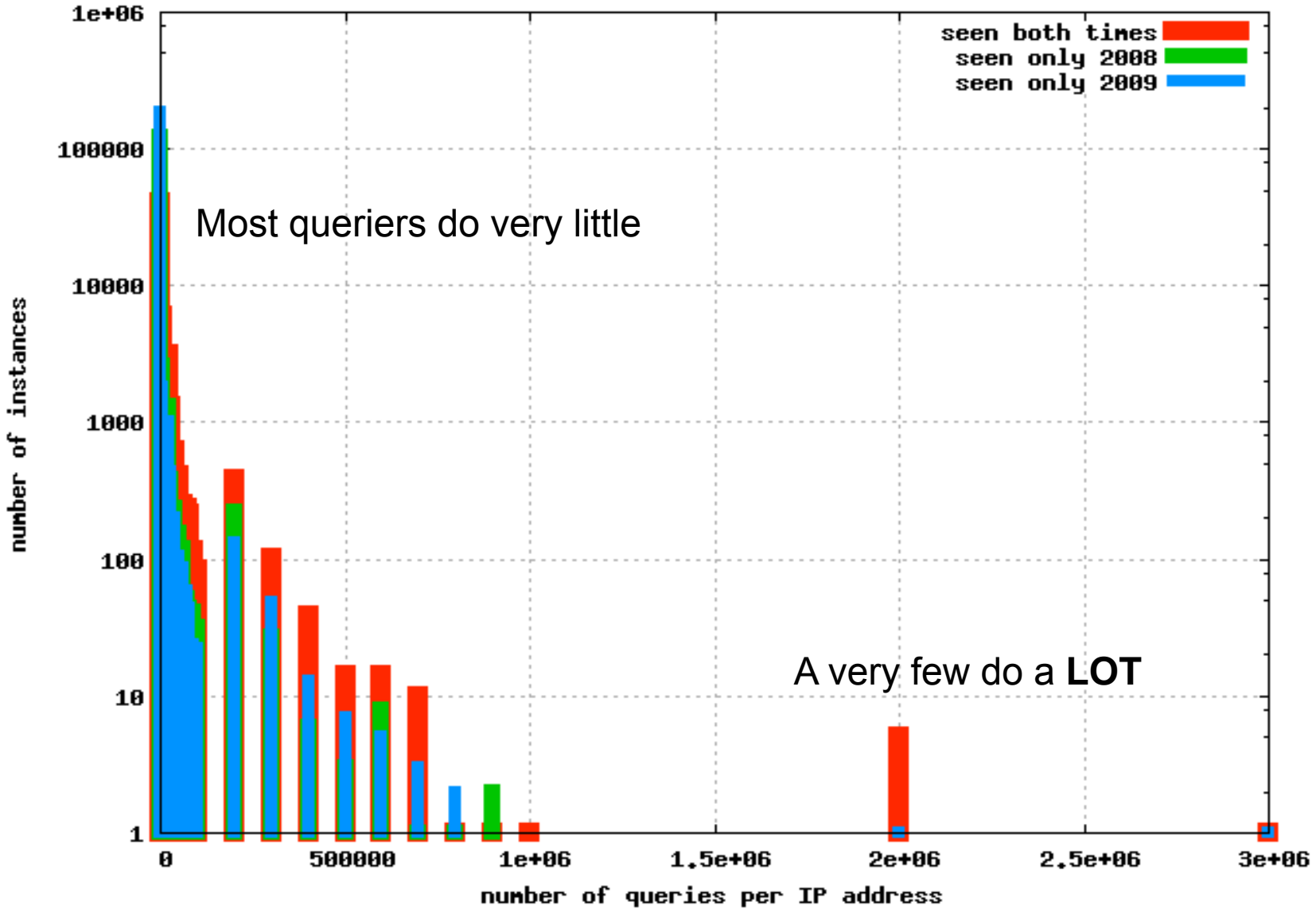
Not a lot of Address re-use

- Slightly less than 1/3 of the IP addresses seen, were seen the year before.
- Seems counter-intuitive:
  - infrastructure DNS is believed to be machine driven, and from company/internal DNS servers, resolvers
    - Which are expected to be on stable IP addresses
- For further study
  - Large numbers of non-infrastructure clients?

Brief quiz

- If a DNS server queries for reverse-DNS…
- Would you not expect it to query for a lot of reverse DNS?
  - (I would: applications which do reverse seem to do a lot)
- What sort of curve-shape of #lookups do you expect?
  - (I expected to see a lot of lookups from most hosts. The majority in fact)
- …….

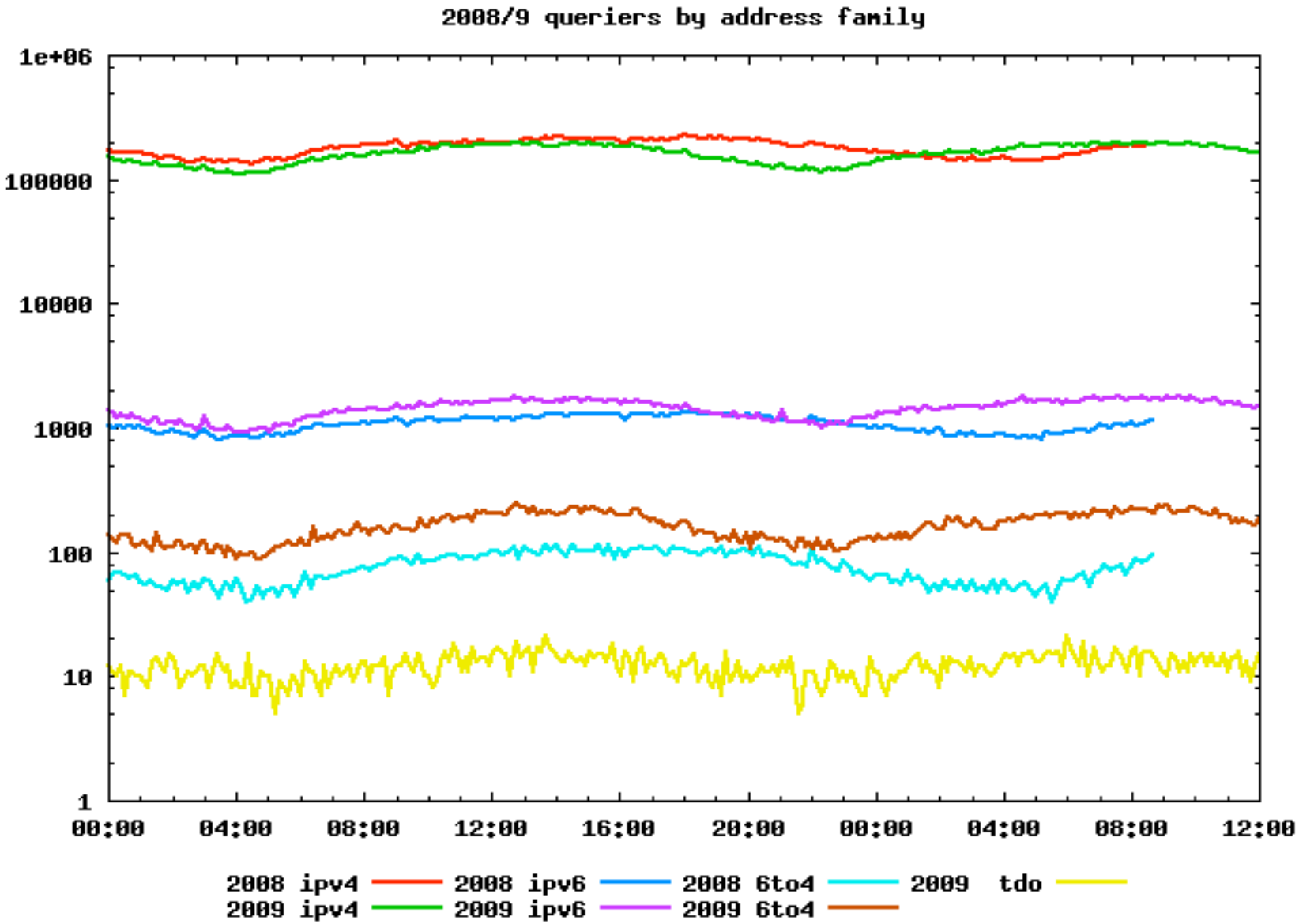
How often do people query?



This is strange…

- The majority of seen IP addresses do 1, or a few queries.
  - Only a very few addresses to hundreds of thousands
  - <10 do millions.
- PTR: ‘infrastructure’ DNS?
  - If its infrastructure, why so much volatility in the IP addresses doing DNS querying?
  - Expected to see far more persistent IP addresses across 2008/2009.
- End-user boxes doing reverse-DNS?
  - Firewalls, probe-tests, other applications?
  - For further study.
- Suggests the ‘real’ count of infrastructure resolvers hitting APNIC is lower than thought
  - <millions. Most hits from ‘singletons’

Queries by IP protocol



Queries by IP protocol

- Rather pretty 10:100:1000:10000 ratio.
- Some Infrastructure DNS now flows over V6
  - Some even flows over tunneling technology
  - Might indicate V6 uptake
  - 6rd countable
    - suggests deploying 6to4 internally can encourage uptake
- Signs of Increased V6 usage
  - But not enough to head off a problem in the context of V4 exhaustion.. Yet.

Tunneled V6 for DNS?

- Strong evidence the Teredo DNS is p2p
  - Clients embed DNS resolver, do reverse-DNS on display of peer sets
    - (N.Ward, Google-IPv6 workshop)
- Not a good choice for service dependency!
- 6to4 very likely to be combination of
  - Linux/FreeBSD
  - Mac, eg airport @home and other OSX 6to4

Its not Just the Asia-Pacific!

- Even noting the RTT, Many EU located economies use A-P located DNS servers to resolve PTR queries.
- Interesting to speculate if the lookup ratios reflect traffic, other measures of inter-economy dataflow
- For further study

Lessons learned 2008-2009

- 2008: 1hour captures
  - Huge risks if capture failed
  - Harder to upload to OARC (serialized)
  - 2009: 10 minute captures, parallel upload
- 2008: ran capture hosts on localtime
  - …but NTP was broken (2+hr offset) ☹
  - 2009: ran capture hosts on UTC, NTP checked!
- 2008: full capture, query + response
  - 2009: unable to capture responses on sec3
    - Too much data. Need to rethink what the value is in reply

Observations

- Infrastructure DNS is very odd.
  - More volatility in the query IP address than expected
  - Use of Teredo, other tunnels increasing
  - Use of IPv6 increasing
  - Some indications day-on-day comparison 2008/9 that V4 is not increasing significantly
  - Per economy, results can be confusing
- Worth further study!

How many prefixes being seen?

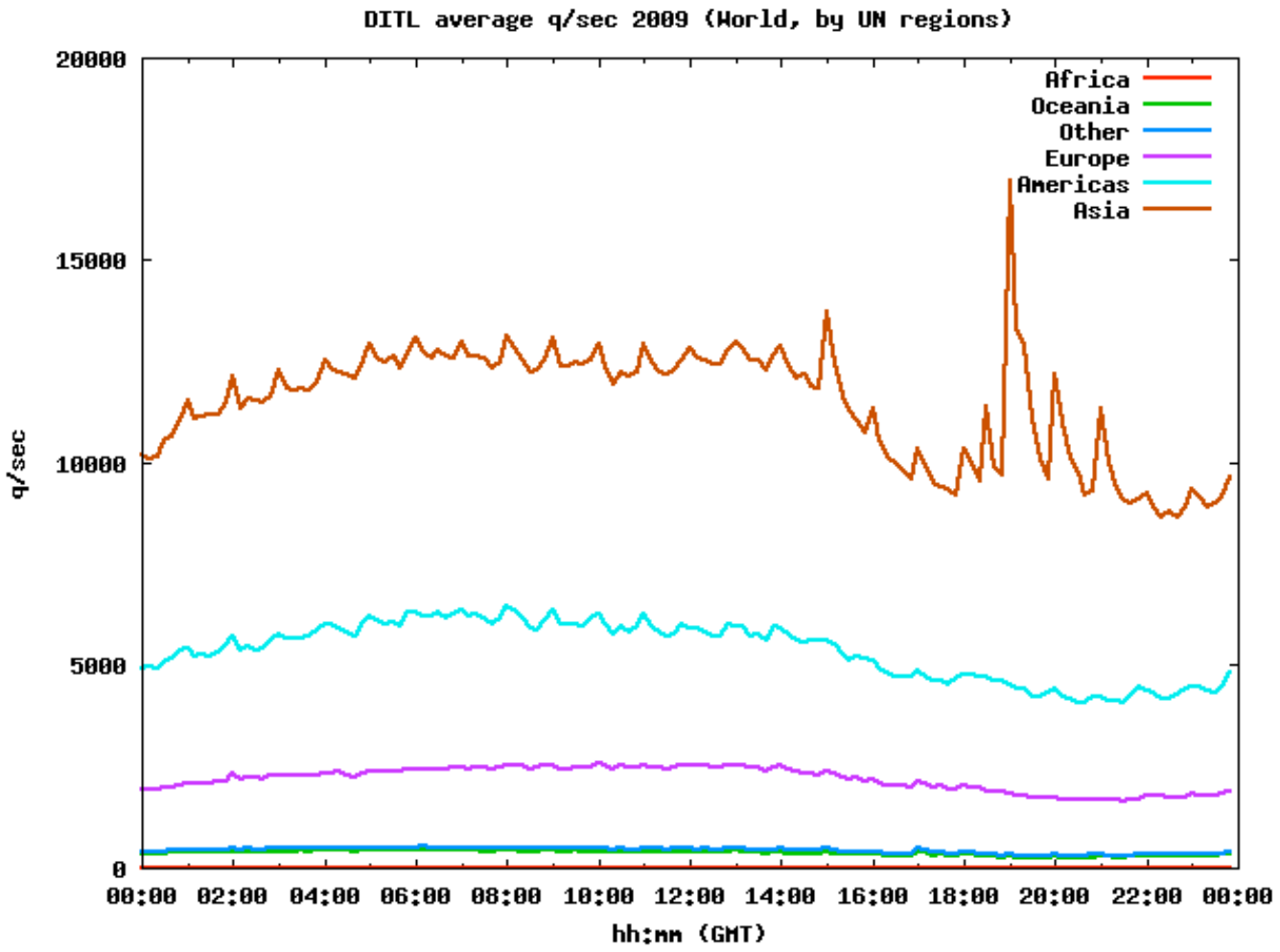
- Portugal:
  - Of 148 allocations listed in RIPE-NCC stats
  - 117 seen in DITL 2009.
  - Circa 77%
- Global Internet, closer to 40%
  - Legacy net overhang? Sampling issues?
    - APNIC nodes don't service a lot of US reverse
- Significant numbers of worldwide, distributed resolvers are being measured

What are we seeing?

- Resolvers of the networks of the world
  - Making PTR queries out TO the world
- So the ‘From’ measure is
  - Resolver making query from a network in..
- And the ‘TO’ measure is
  - What the PTR represents as a network in ...
- We are seeing the world talking to itself

DITL by regions overall query rate

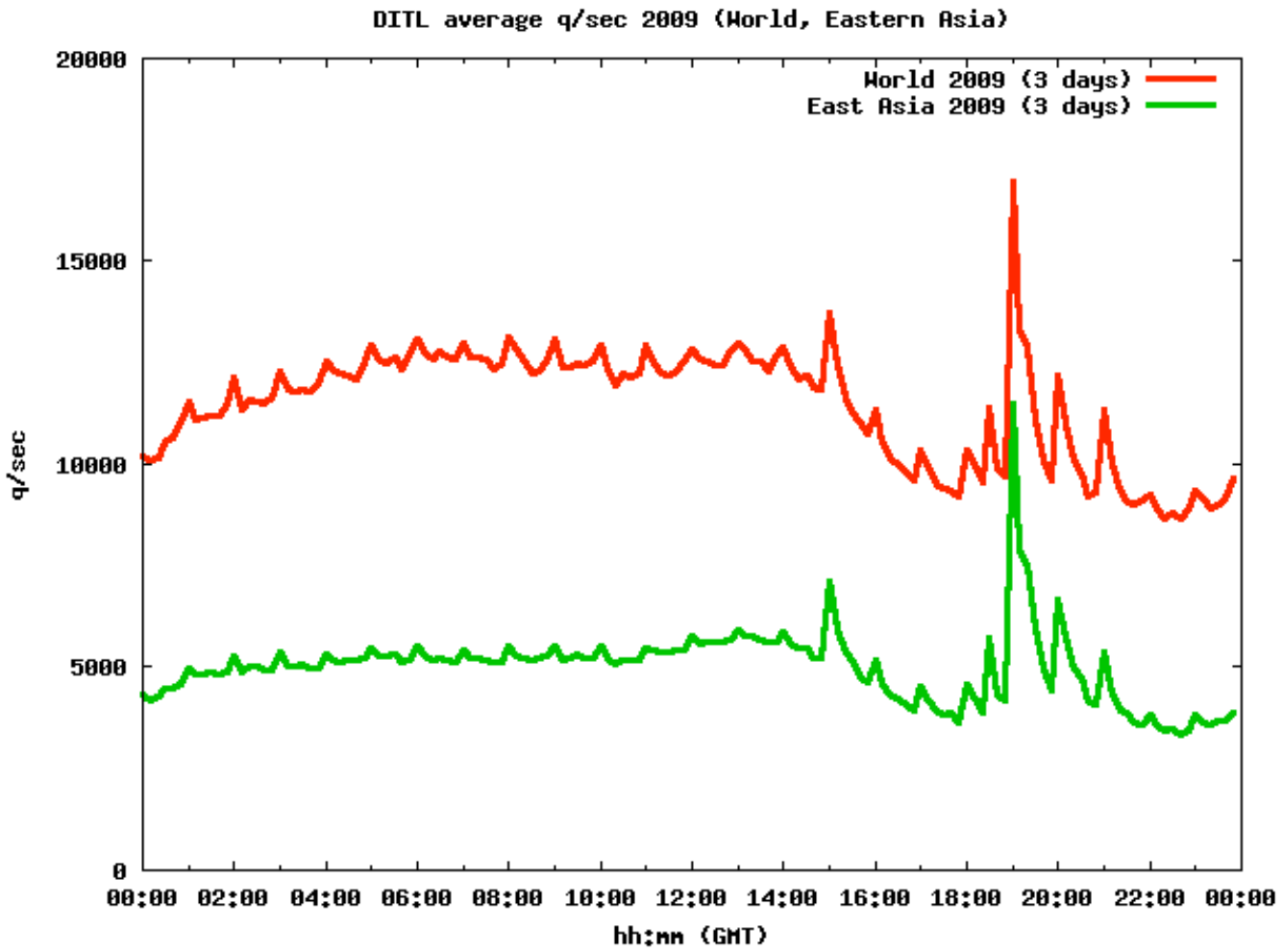
UN Region breakdowns



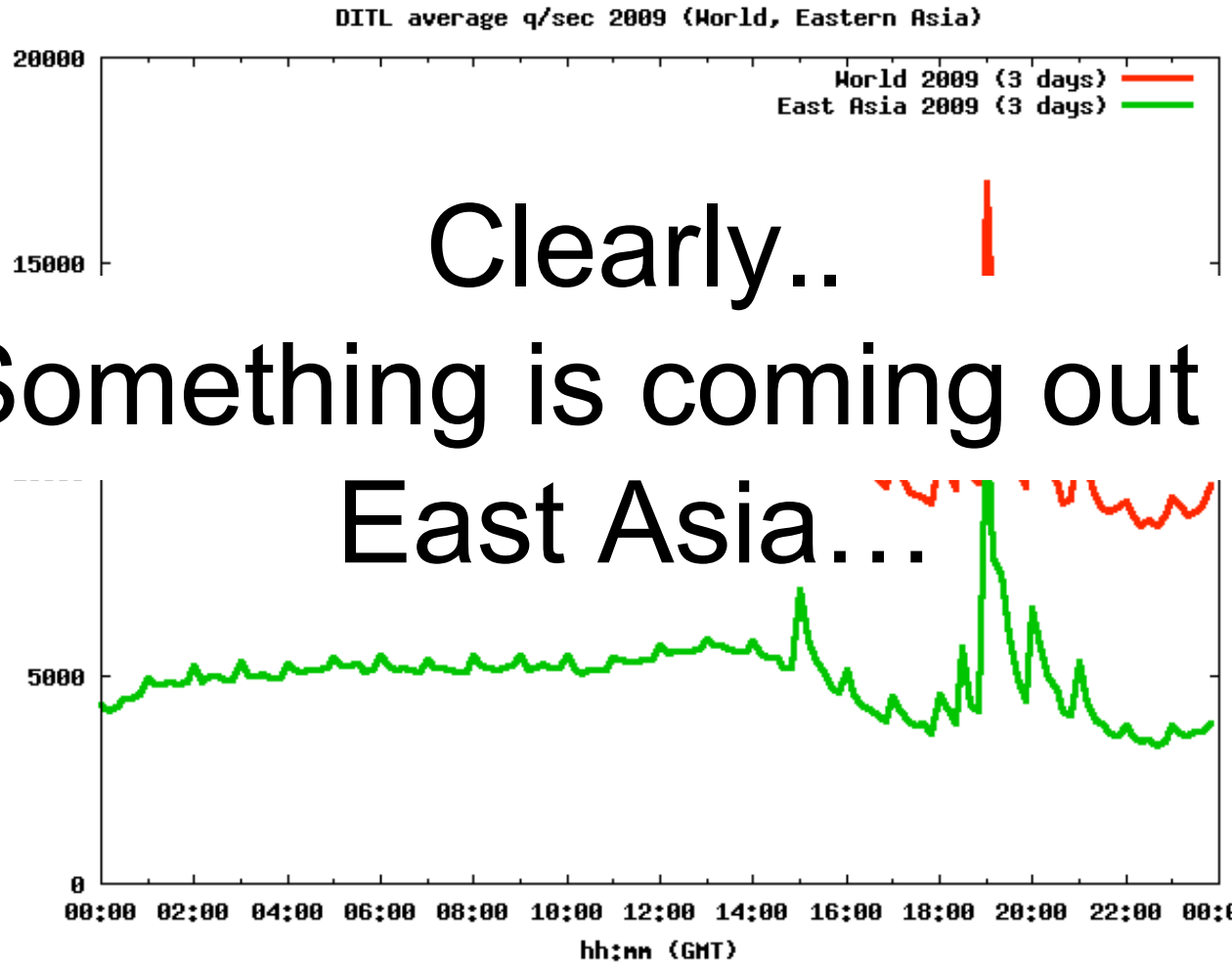
UN Region breakdowns

- Use of Reverse-DNS is not equal worldwide
  - Strong use in specific economies, regions
  - Data volume variations swamp individual economies (US, JP excepted)
  - Some strong signals evident that relate to specific regions
    - Logfile processing, cron-jobs, DNS polling?
- What is happening in Asia?

E. Asia in the World of DNS



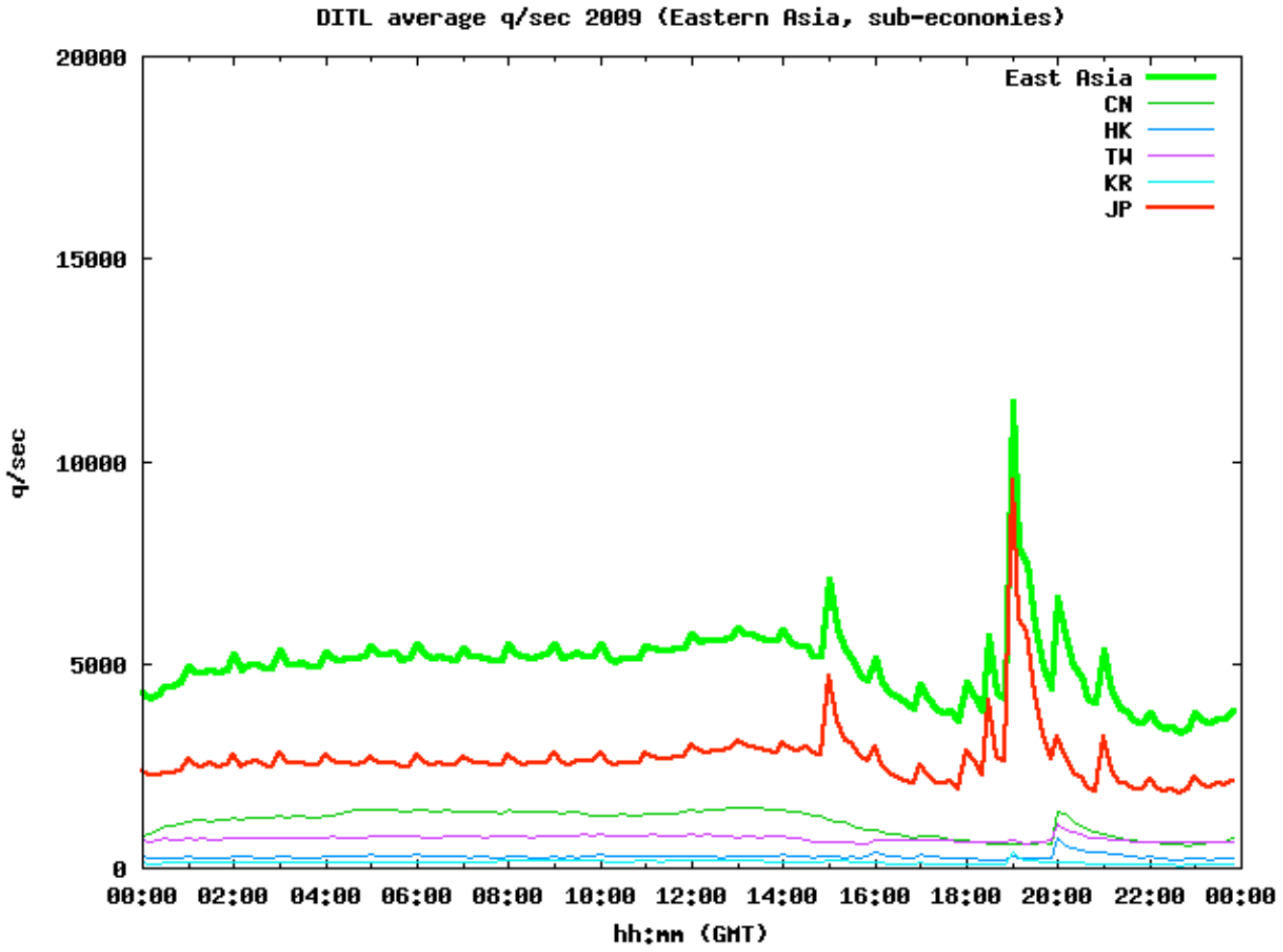
E. Asia in the World of DNS



Clearly..

Something is coming out of East Asia…

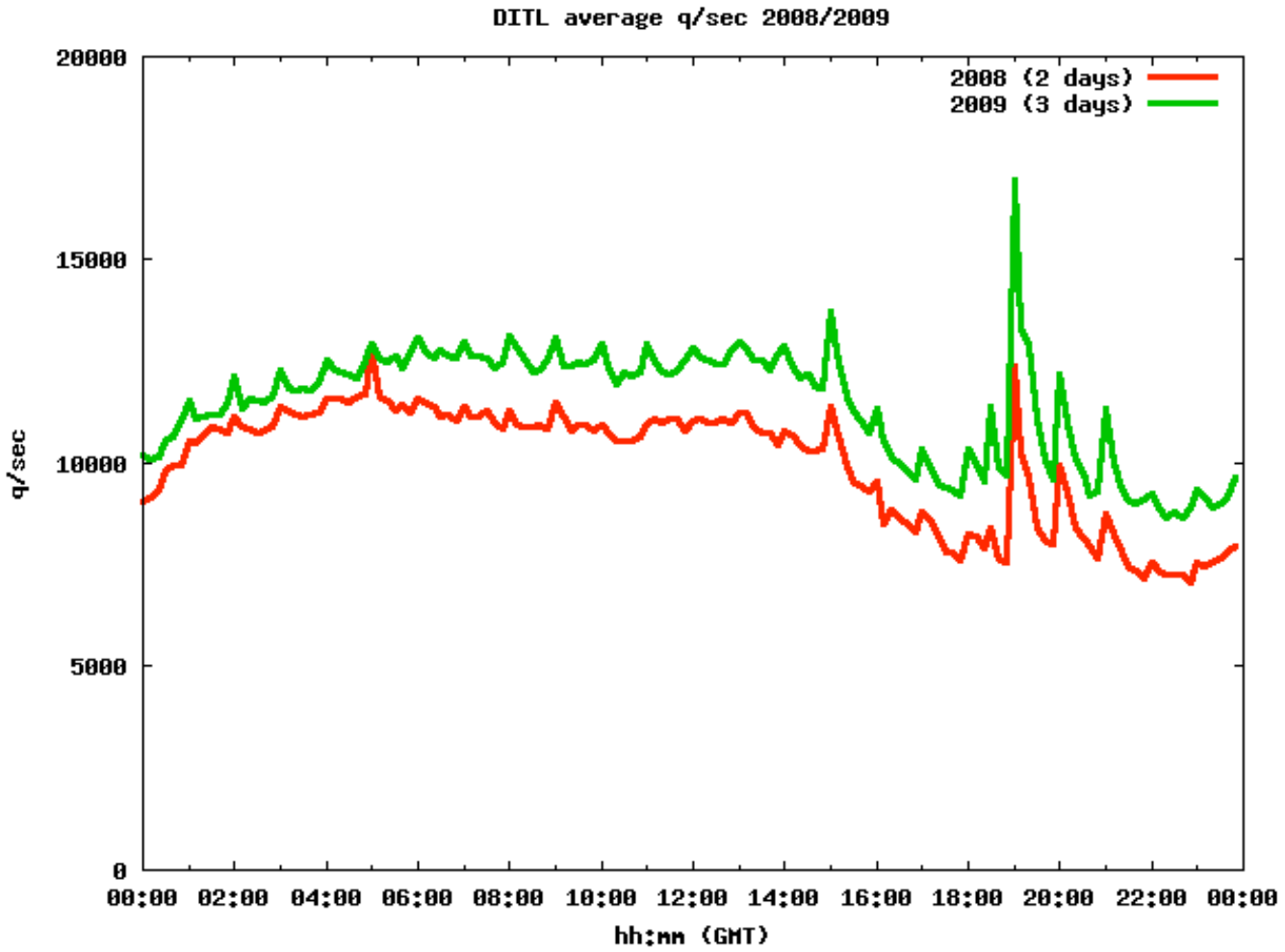
E. Asia breakdowns



East Asia breakdowns

- Very strong indications that specific daily events tie to specific (sub)region
  - Almost all of the significant ‘spike’ in worldwide DNS load comes from East Asia
  - Almost all of the spike within East Asia comes from Japan

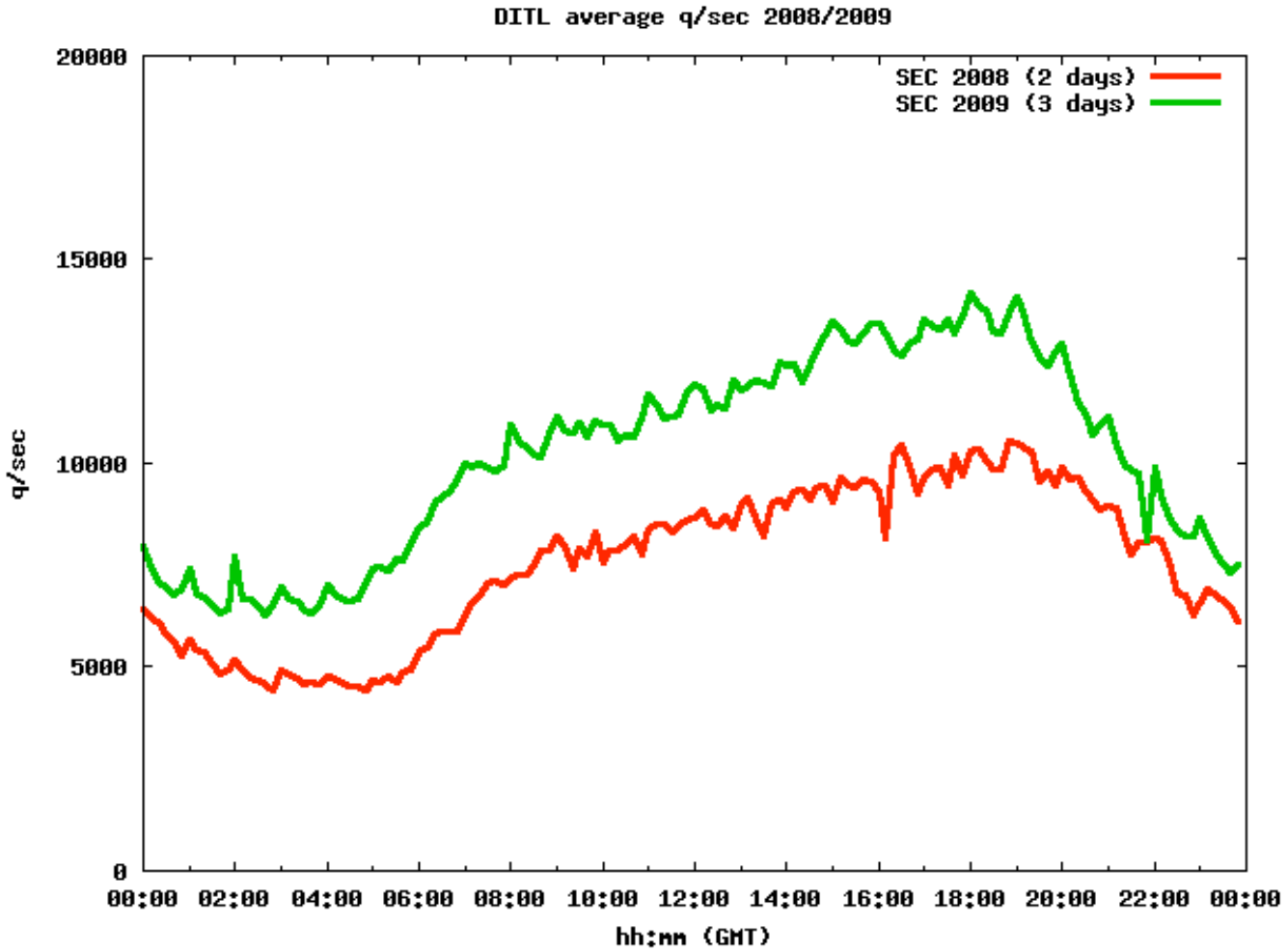
DITL 2008-2009 AP region



DITL 2008-2009 AP region

- Consistent behavior visible
  - Overall trend across 24h
  - Per-day significant events
    - Whatever these are, they are long-term behaviors
- Consistent growth in DNS traffic
  - 10-20% year on year growth in overall DNS load

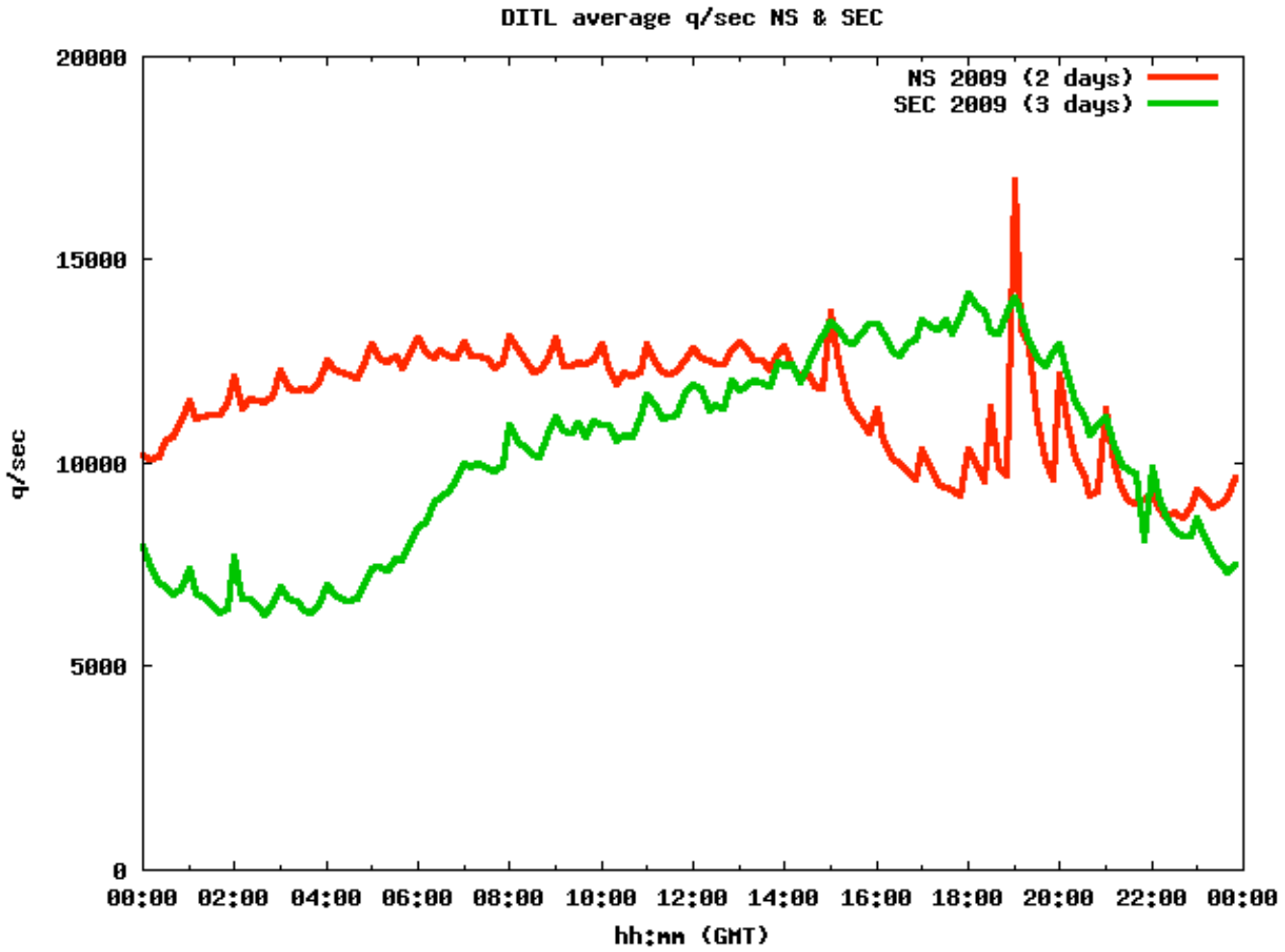
DITL 2008-2009
rest of the world



DITL 2008-2009
rest of the world

- Consistent behavior visible
  - But different to Asia-Pacific NS
  - JP ‘spike’ not visible year on year
- Also consistent growth in traffic
  - 15%-20% bigger than Asia-Pacific NS

Asia & Rest of World Time shift

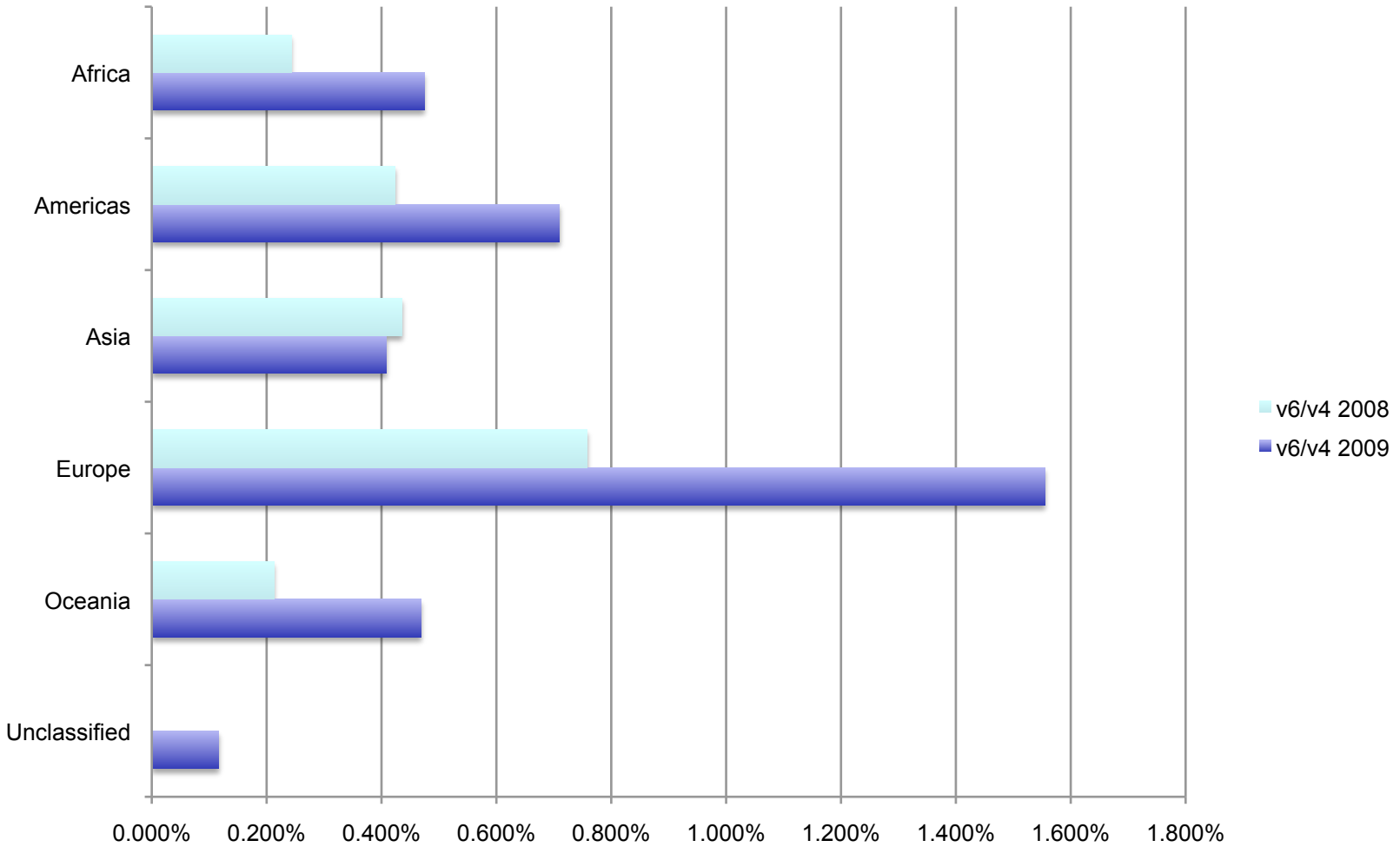


Asia & Rest of World
Time shift

- Distinct time-phase differences for each category
- Rest of World amalgamates many distinct local timezones
- Asia-Pacific dominated by a few closely aligned timezones

Inter-Regional V4/V6 Comparisons

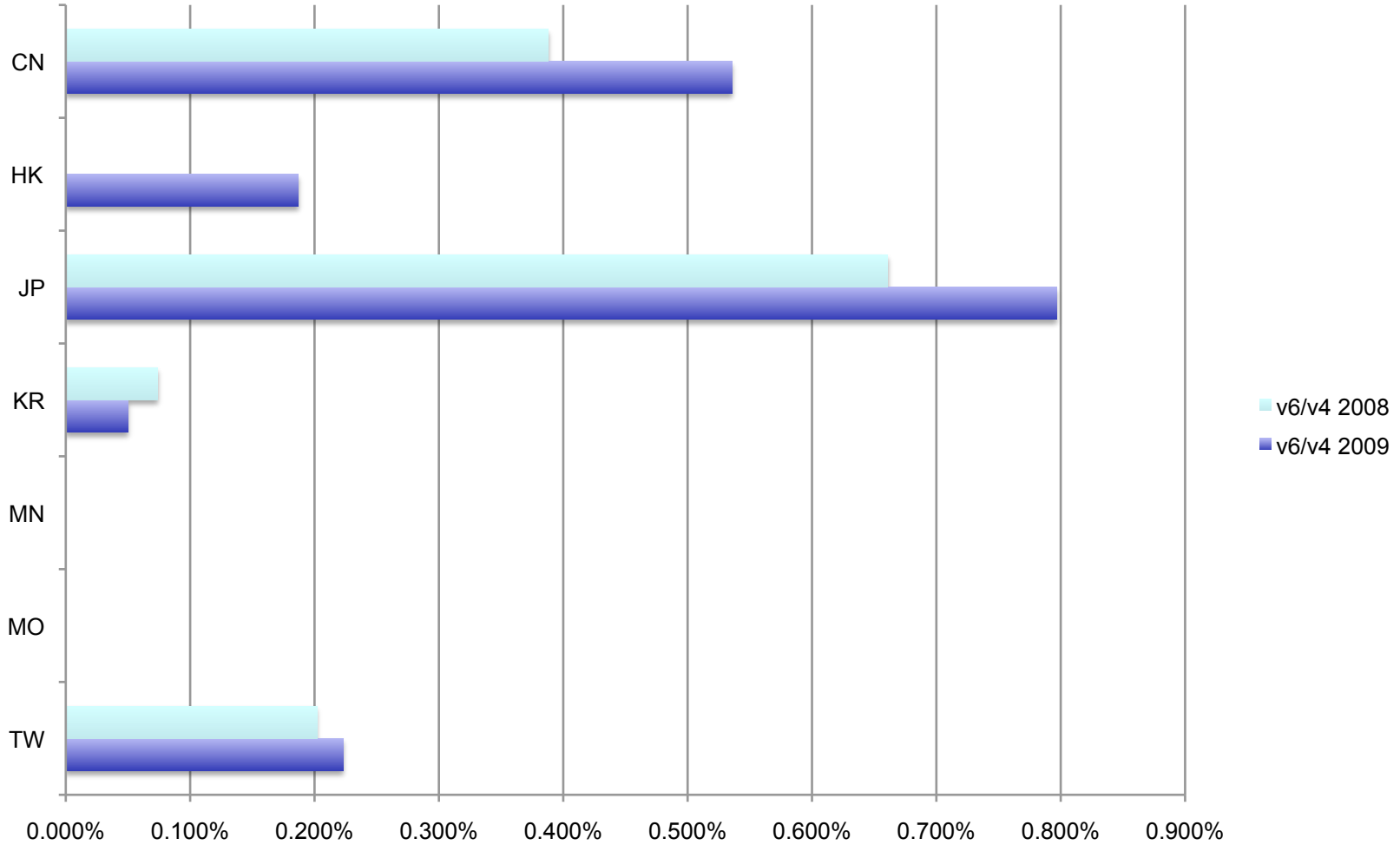
UN Regions v6/v4 usage



UN Regions observations

- All regions except Asia saw IPV6 growth in DNS transport
- Significant growth in European use of IPv6 as transport
- …but V6 usage still a low percentage of V4, of the order 0.2% to 1.5%

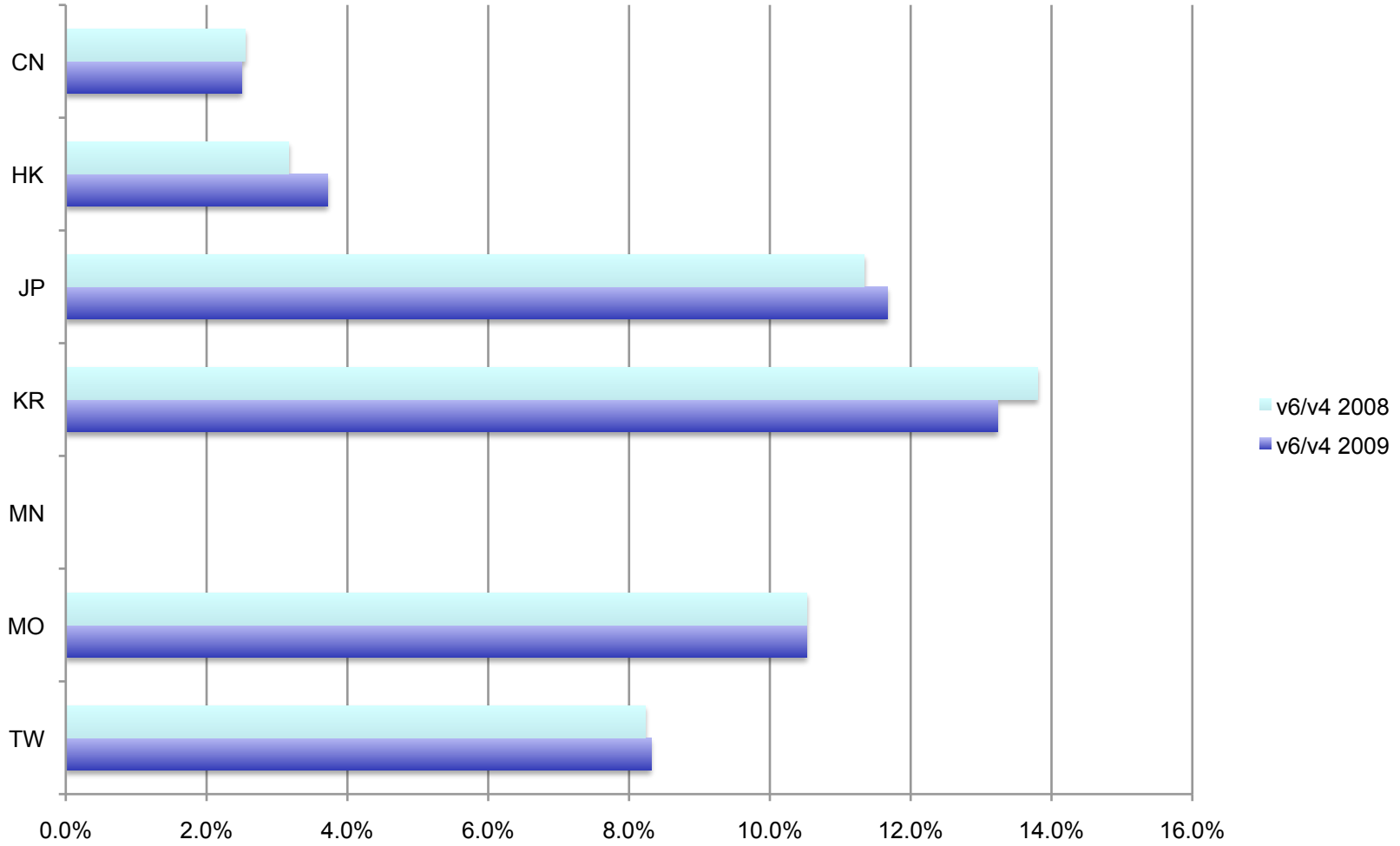
East Asia V6/V4 usage



East Asia observations

- Asia overall had declining IPv6 but East Asia did have some growth in use of IPv6
- Less than UN ‘rest of world’ regions
- Overall V6 usage also a low percentage of V4, of the order 0.2% to 0.8%

East Asia V6/V4 assignments



East Asia assignment obs.

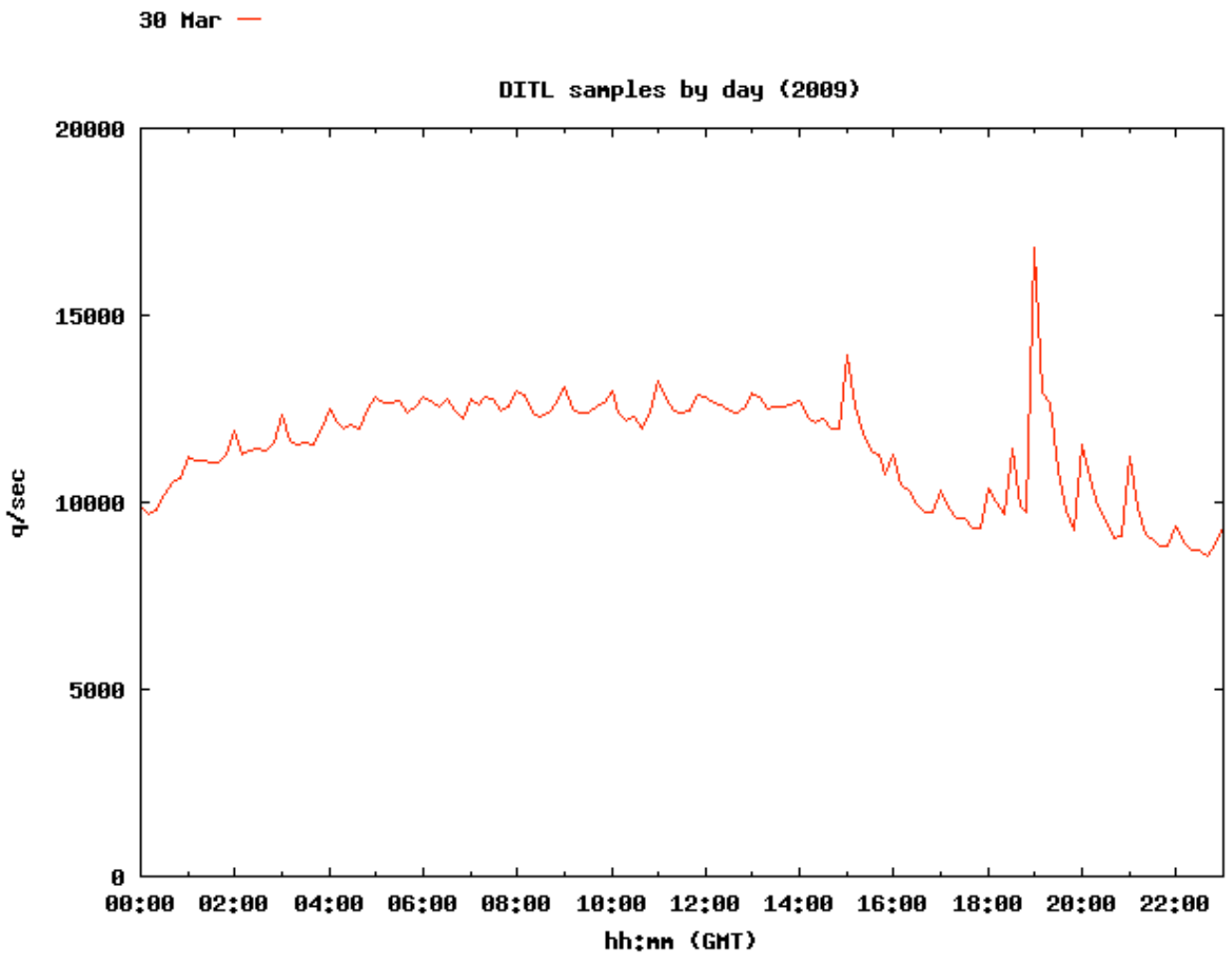
- Assignment counts for East Asia do not correlate with observed address use in DNS
- V6/V4 ratios in assignment counts do not correlate with observed V6/V4 usage
  - Higher ratios of V6 assigned than seen in use
  - No relationship per-economy

How the data was processed

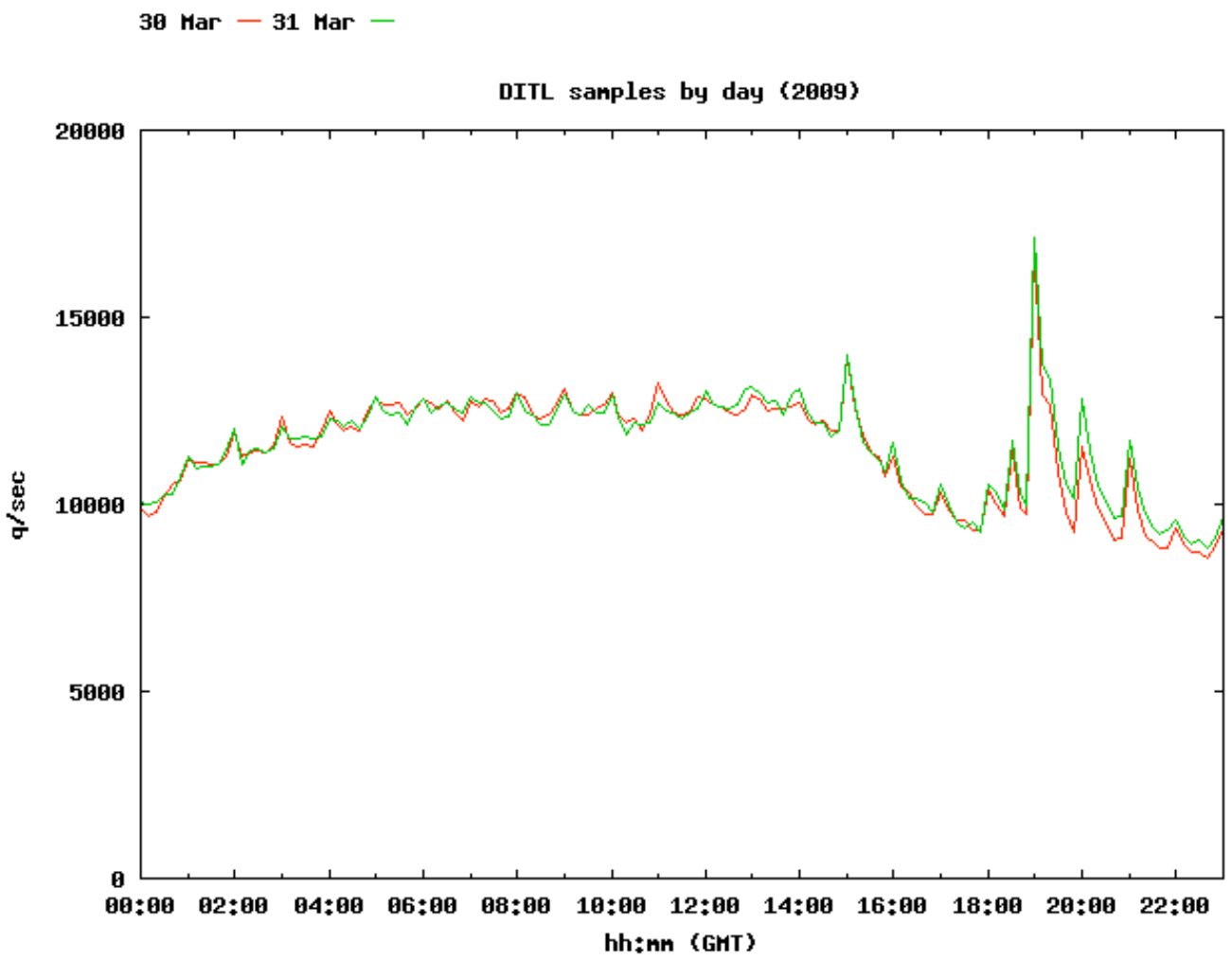
Technology

Lots of perl map { …. } over data

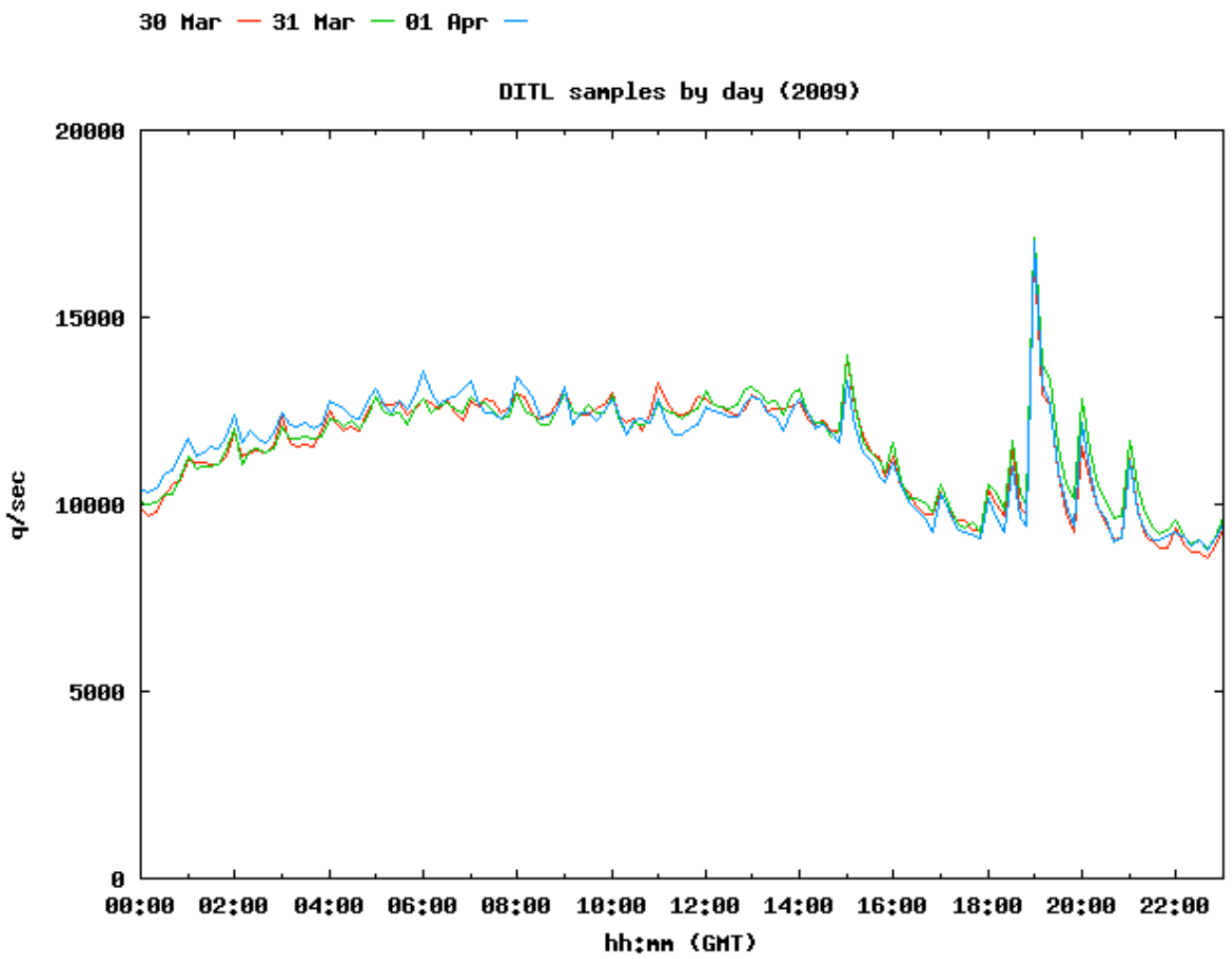
Day Samples



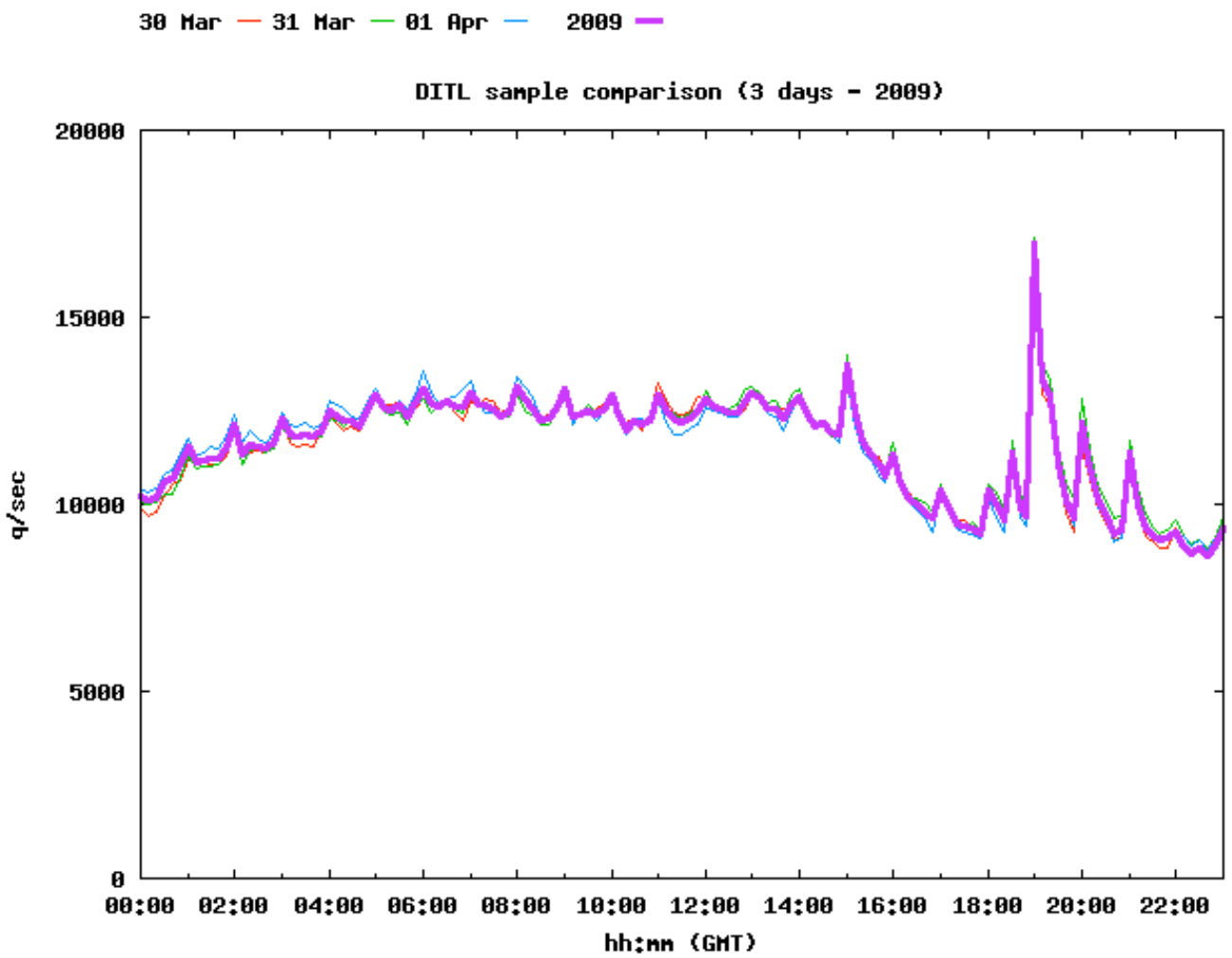
Day Samples line up



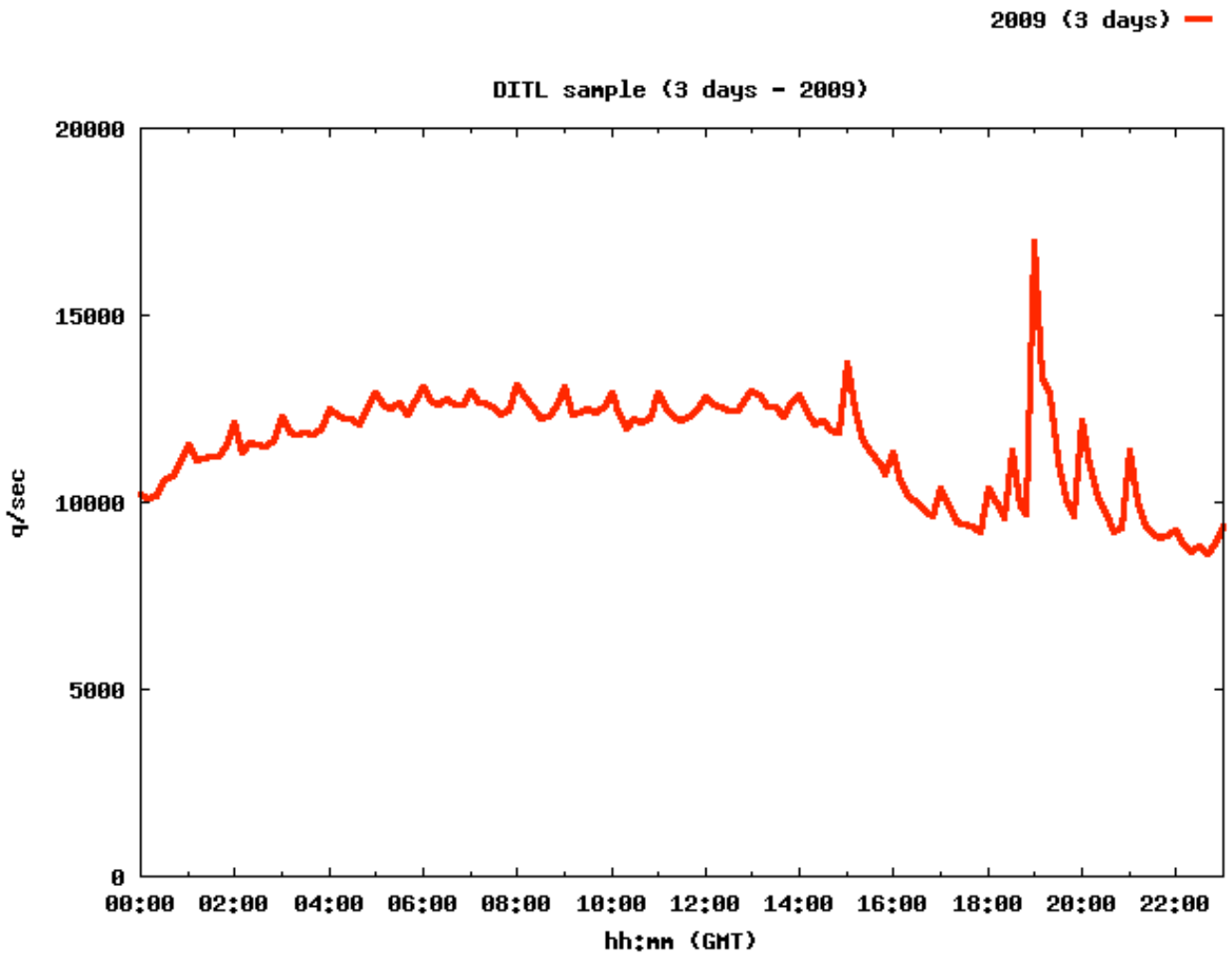
Day Samples line up strongly!



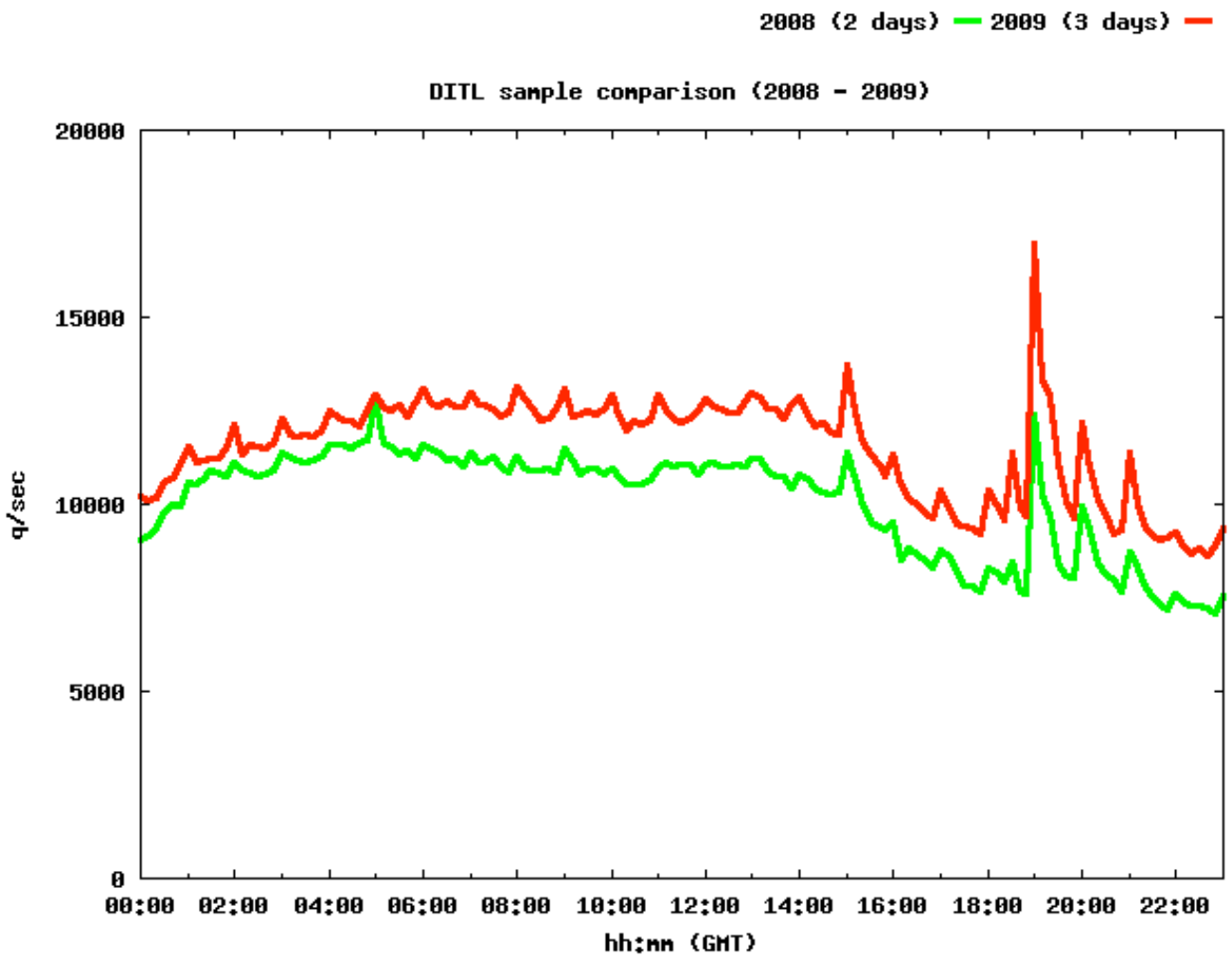
Average shows core ‘shape’



Averages can be compared



Result: year-on-year trends



DITL 2010

- 2 points make a line
  - 3 data series makes a strong trend!
  - V4/V6 relativities, ties to EU 25% V6 measurements?
- Re-use existing infrastructure
  - Possibly needs re-investment for DITL2011
- APNIC deploying DNSSEC/Anycast
  - Monitor change during deployment
  - Expected 2x traffic growth from DNSSEC

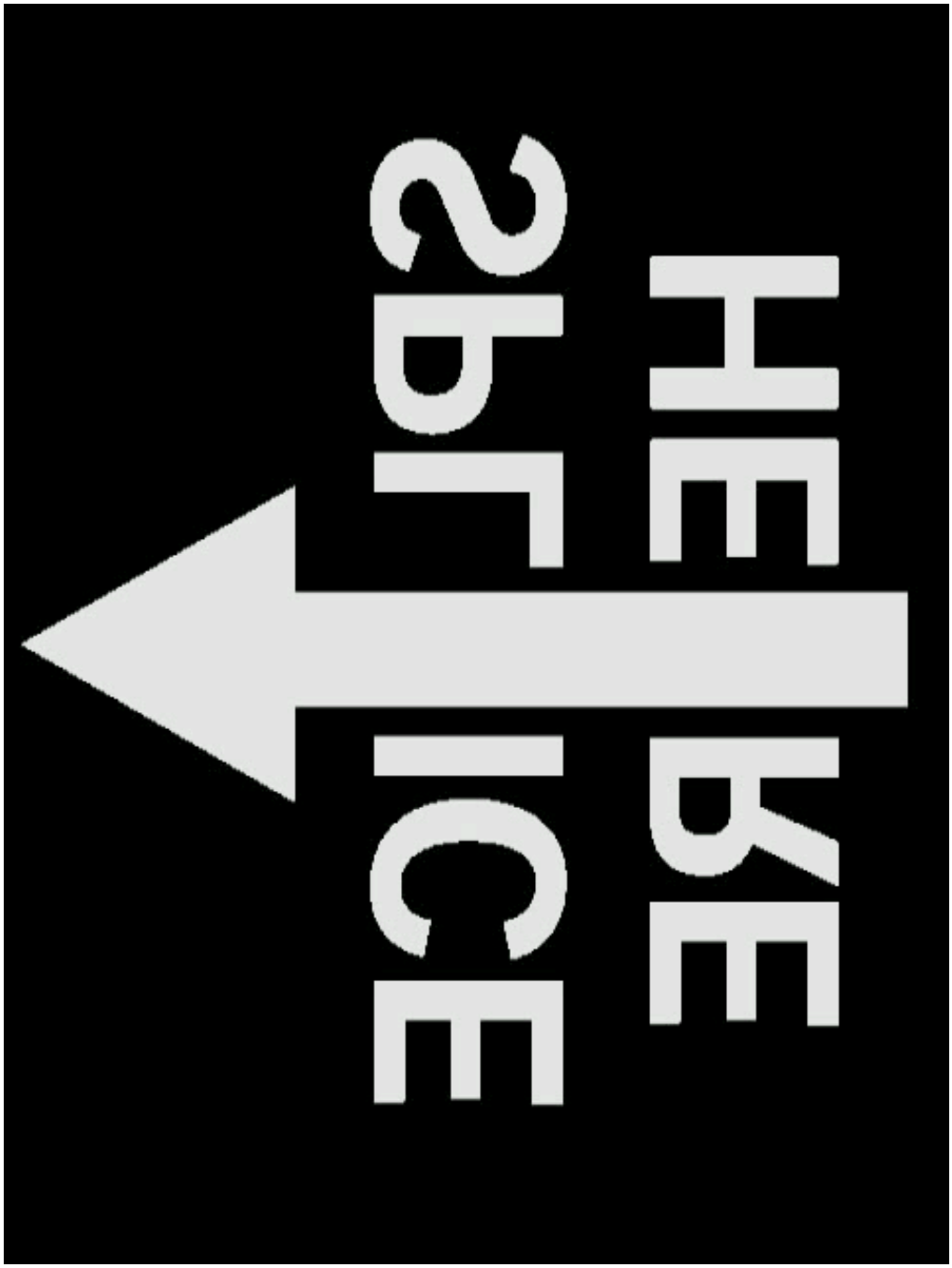
Thank You!

Questions?

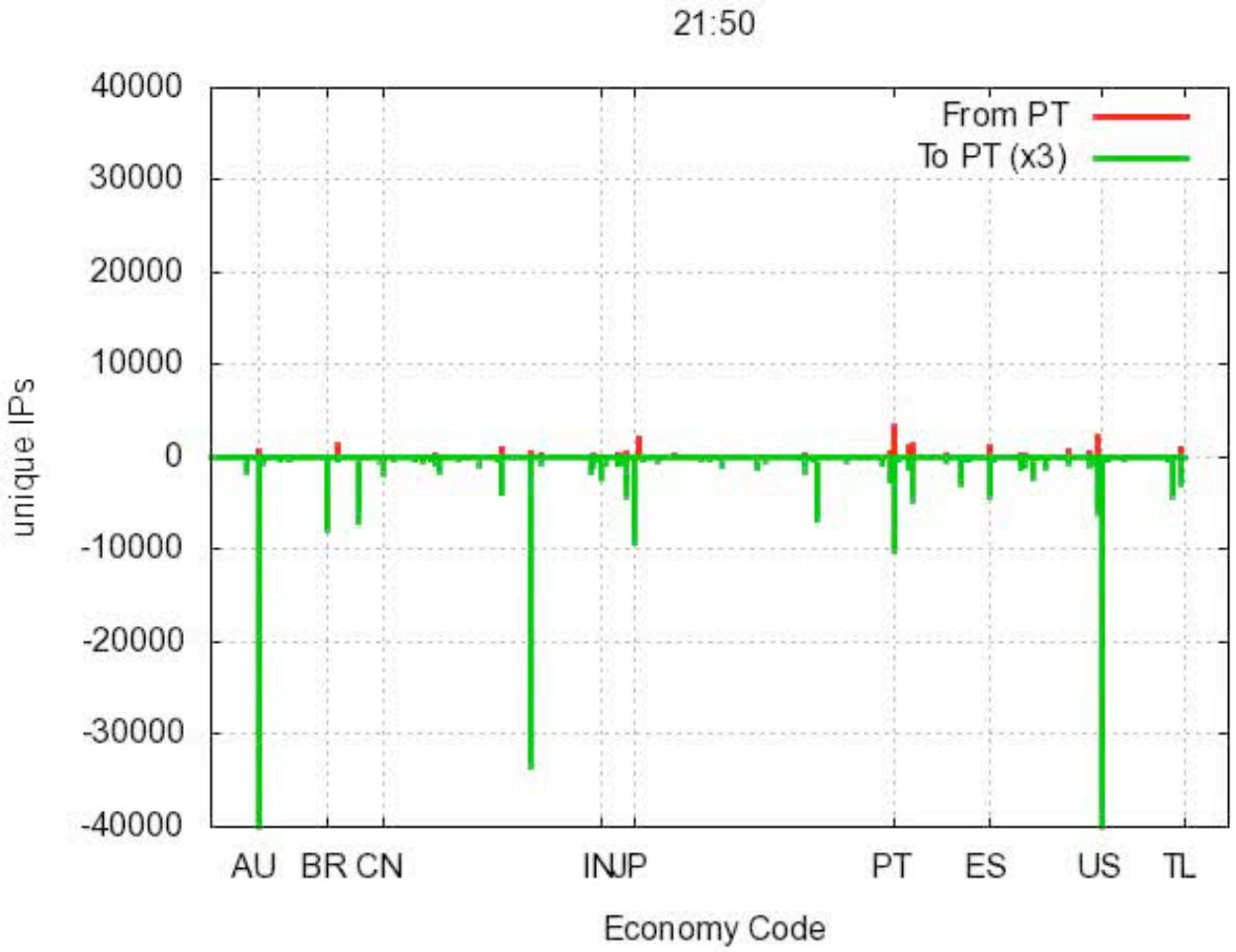
Boring..

Lets go to the movies..

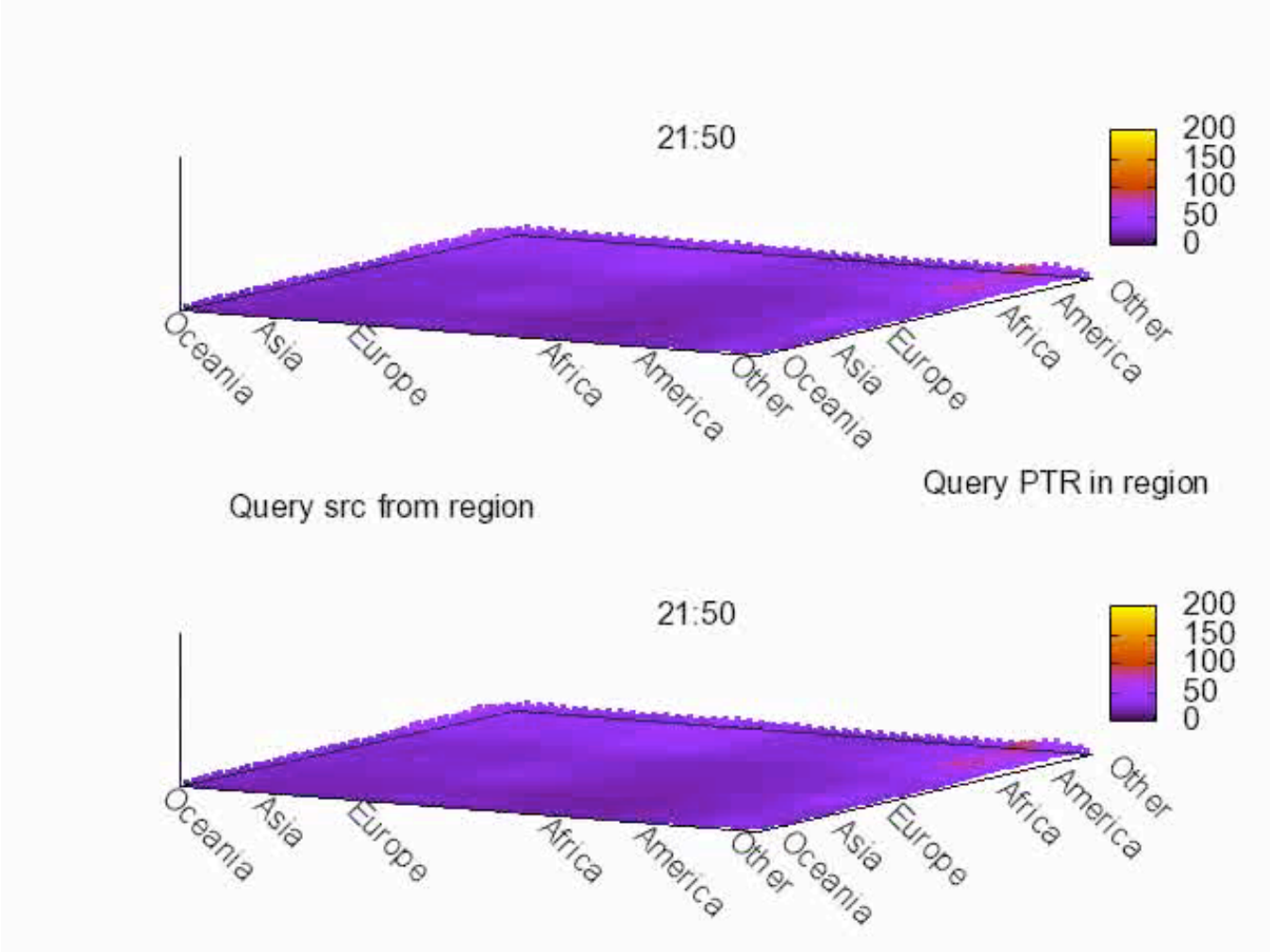
Lets go to the movies.. Again


HERE
2pl
IOE

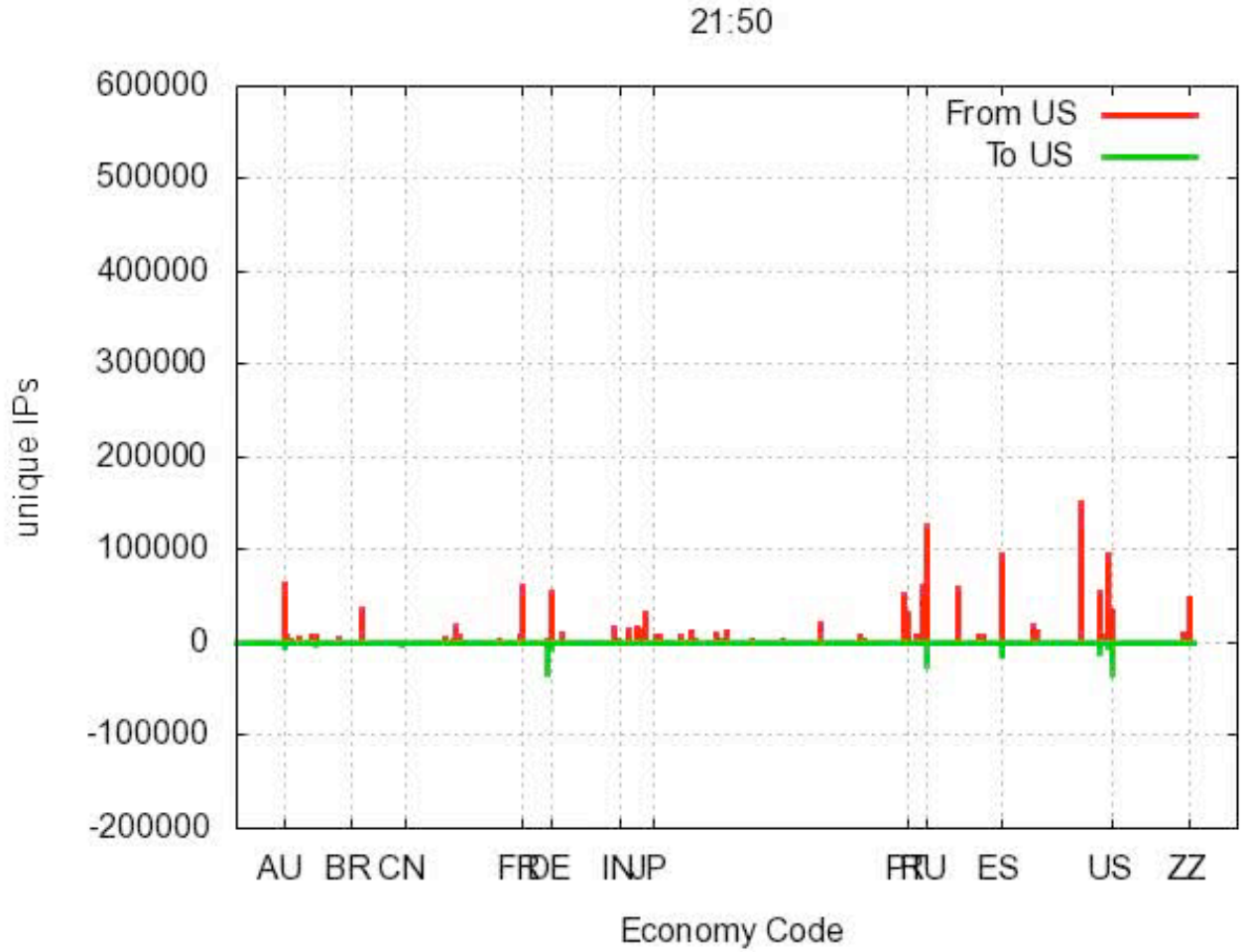
Portugal DNS DITL 2009



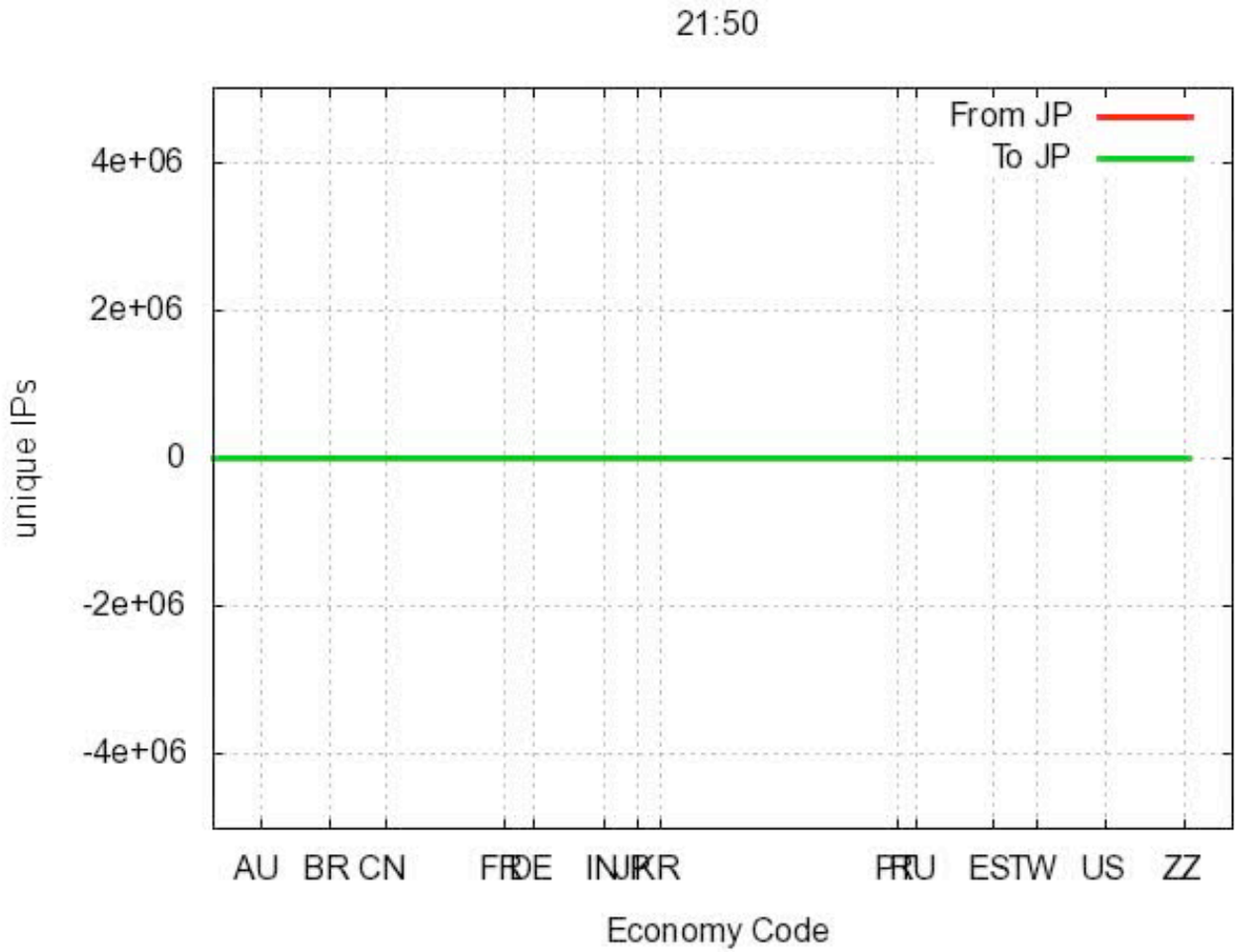
Asia-Pacific vs Rest-of-World



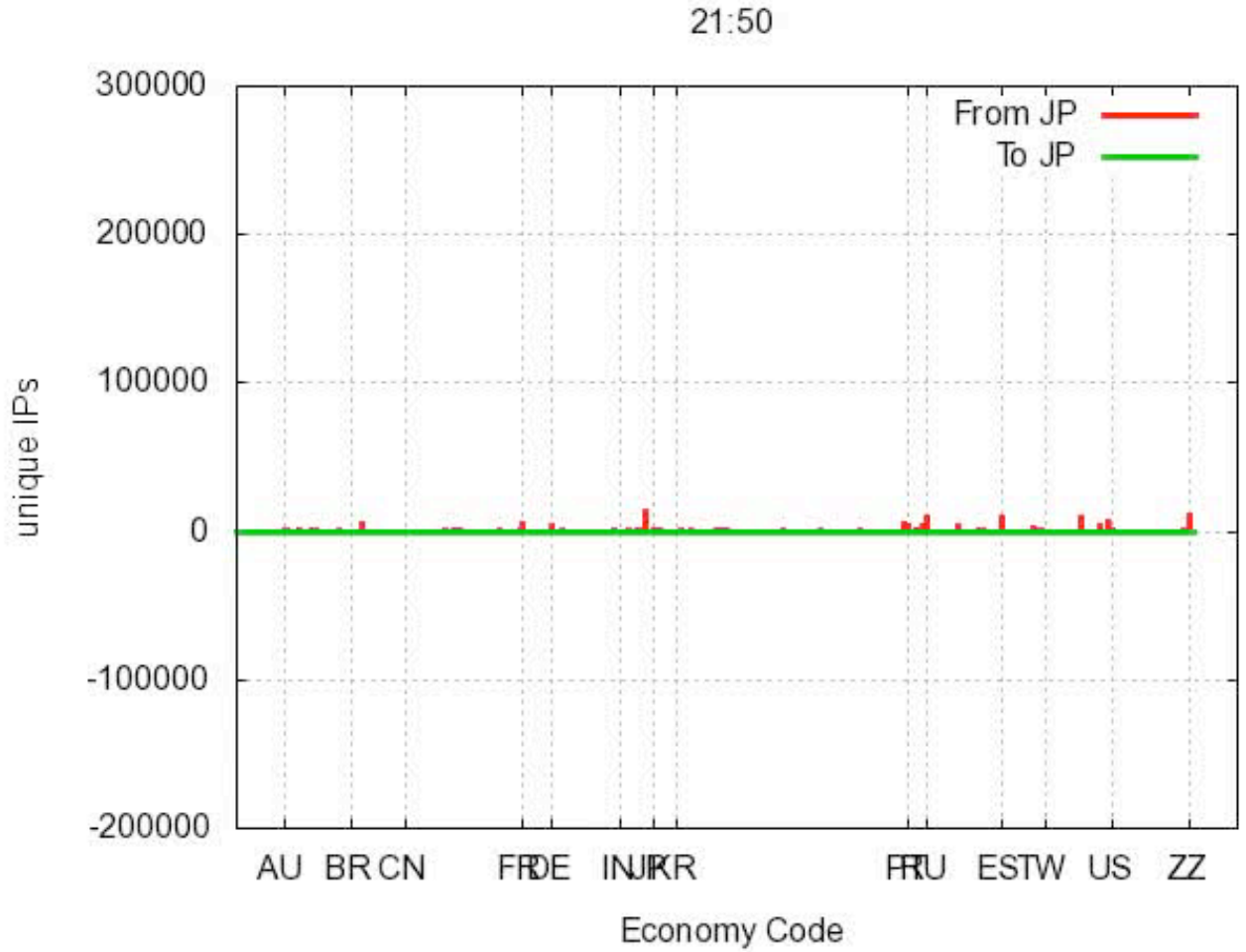
US looking everywhere (we don't secondary US reverse)



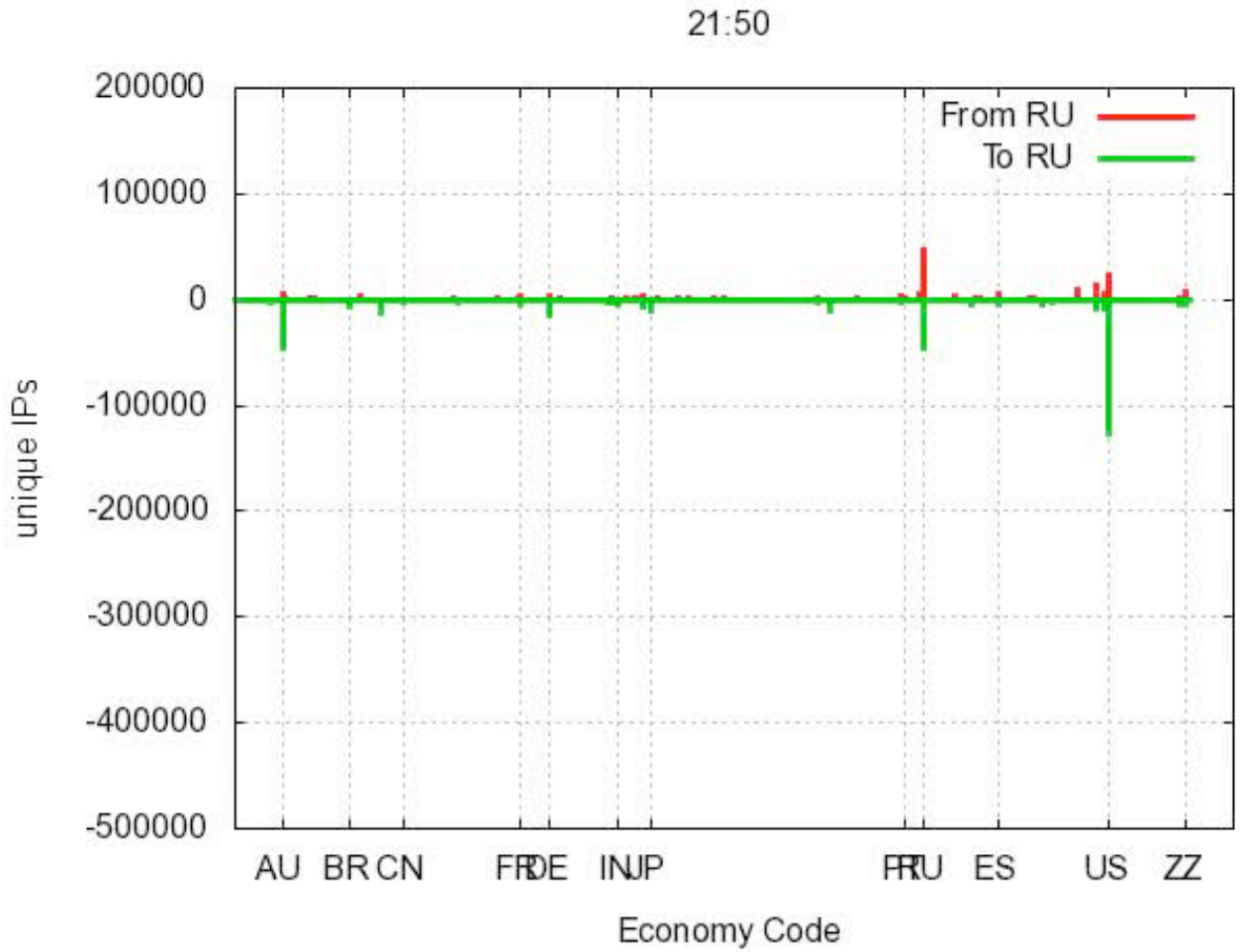
Japan looks at itself



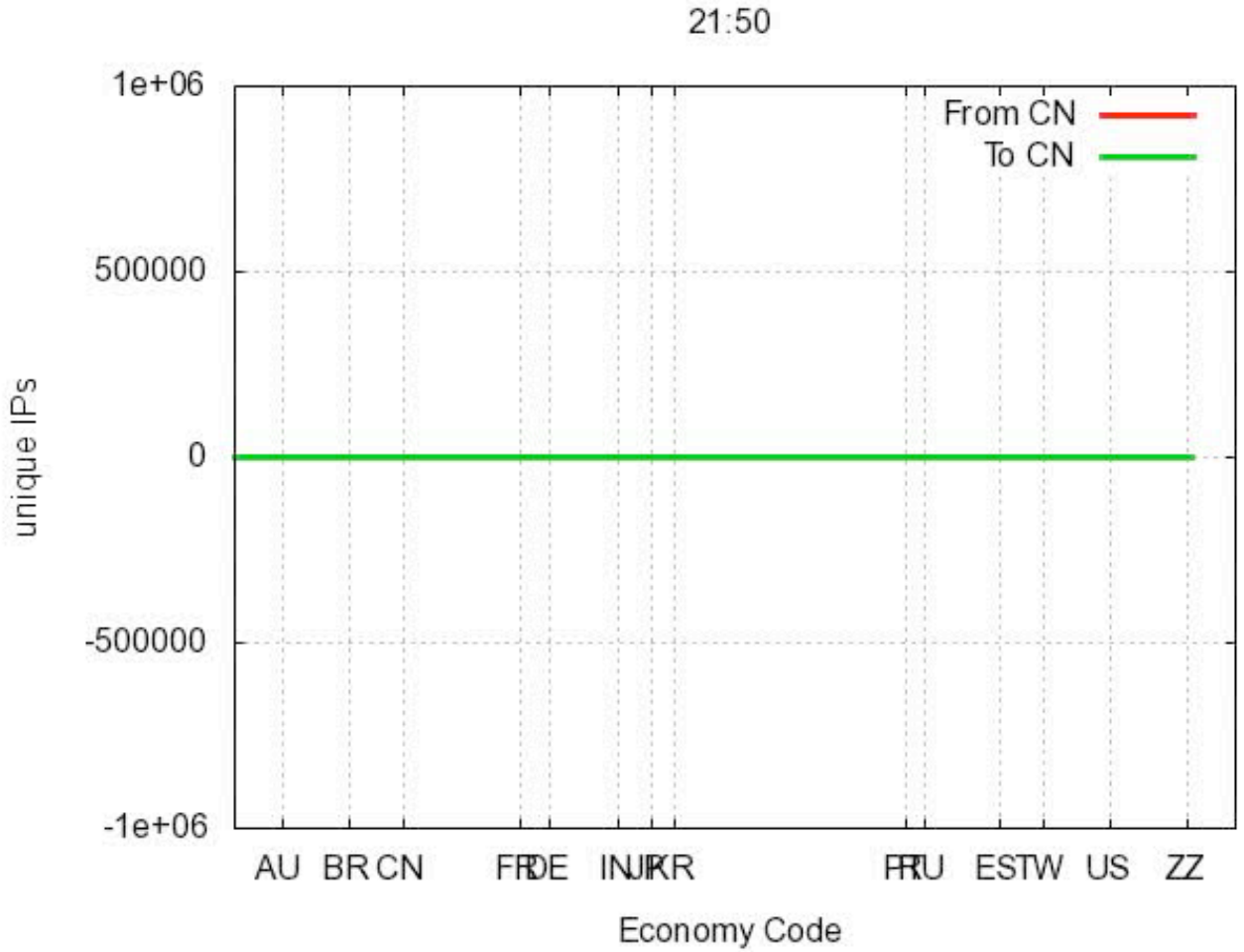
Ok. Japan looks everywhere (but mainly at itself)



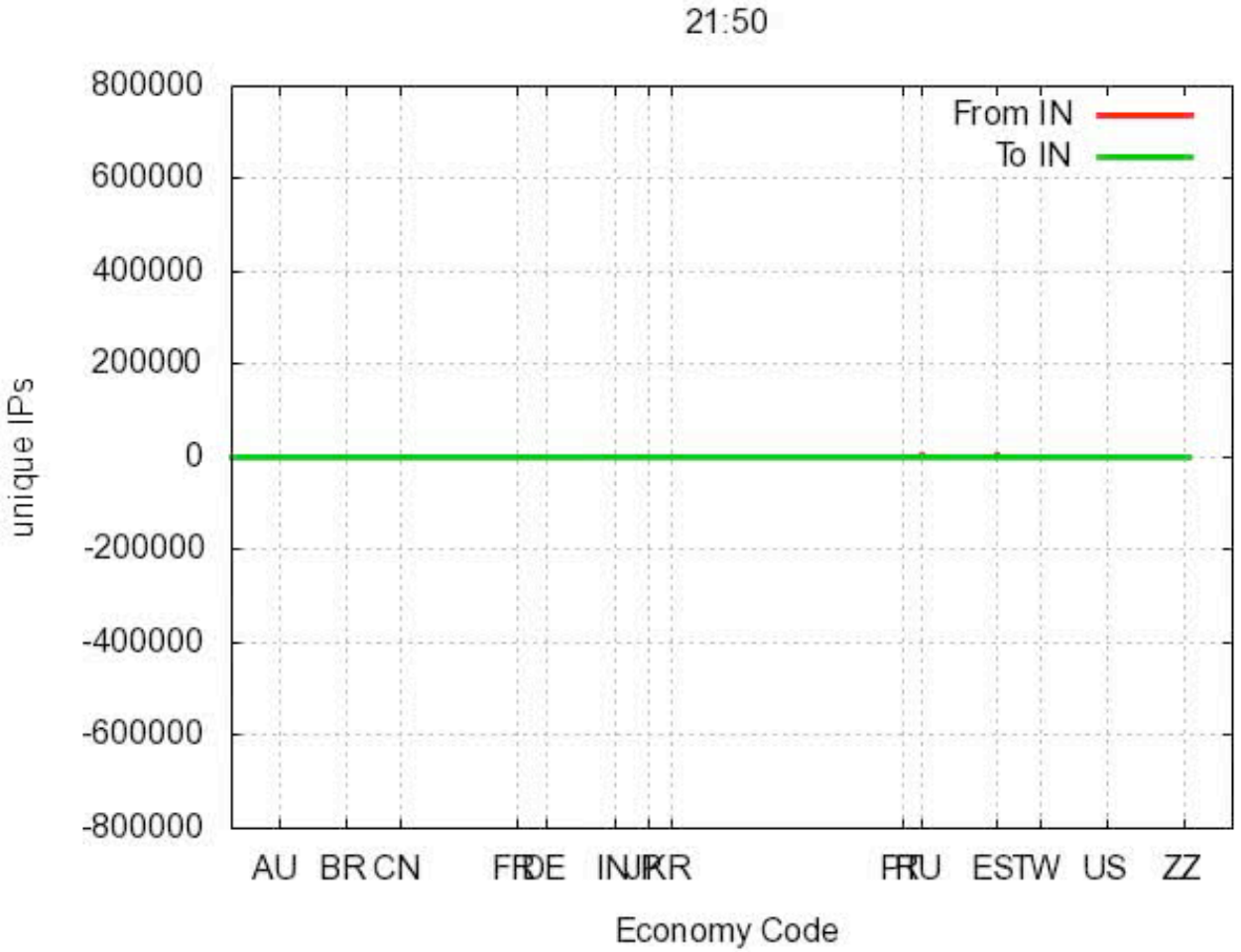
Everyone looks at Russia



China looks at Itself



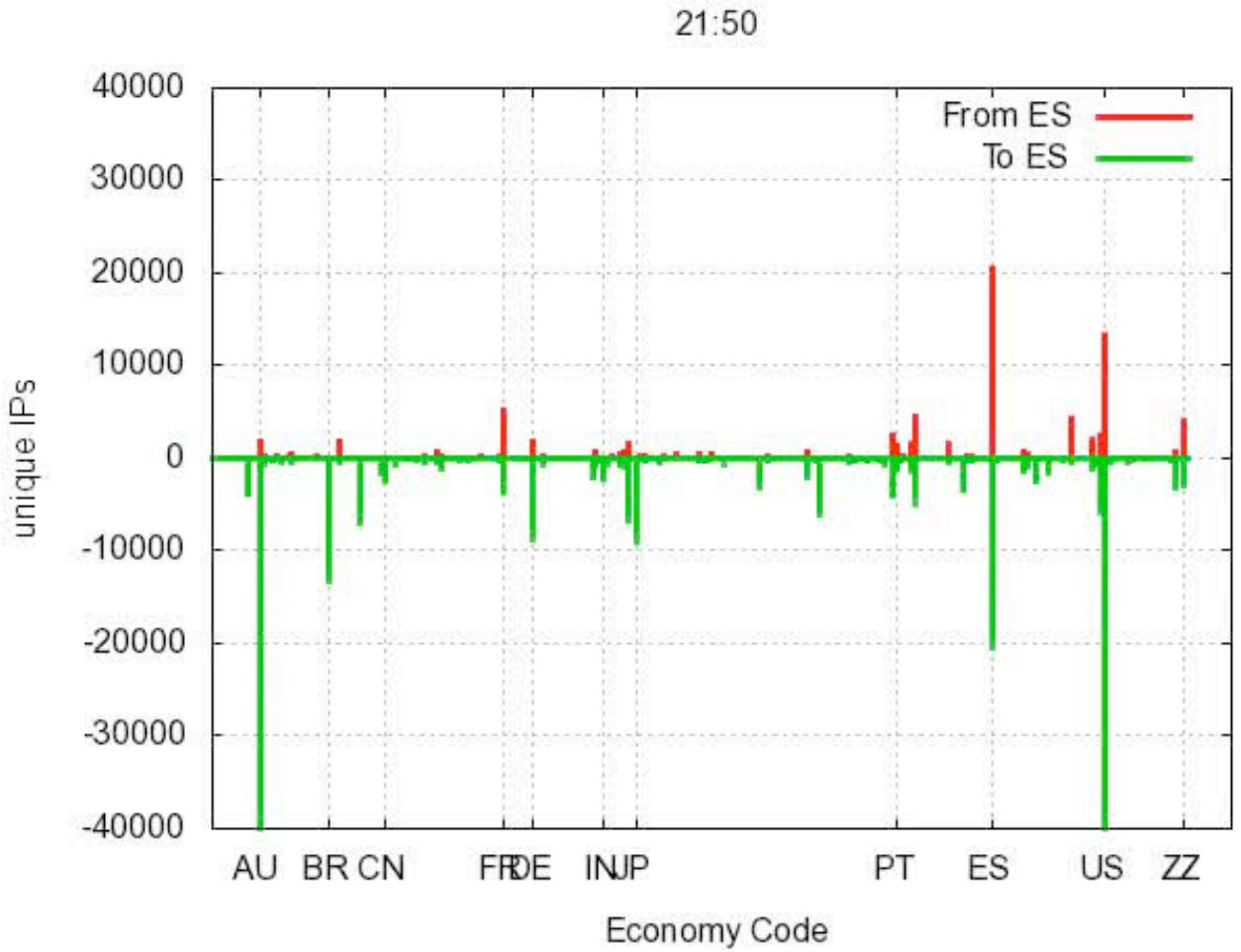
Everyone looks at India



Asia Pacific Network Information Centre

APNIC

For ESNOG Attendees



Germany looks at India