APNIC 28 Beijing, China 24-28 August 2009

DITL 2008-2009

George Michaelson
APNIC
ggm@apnic.net

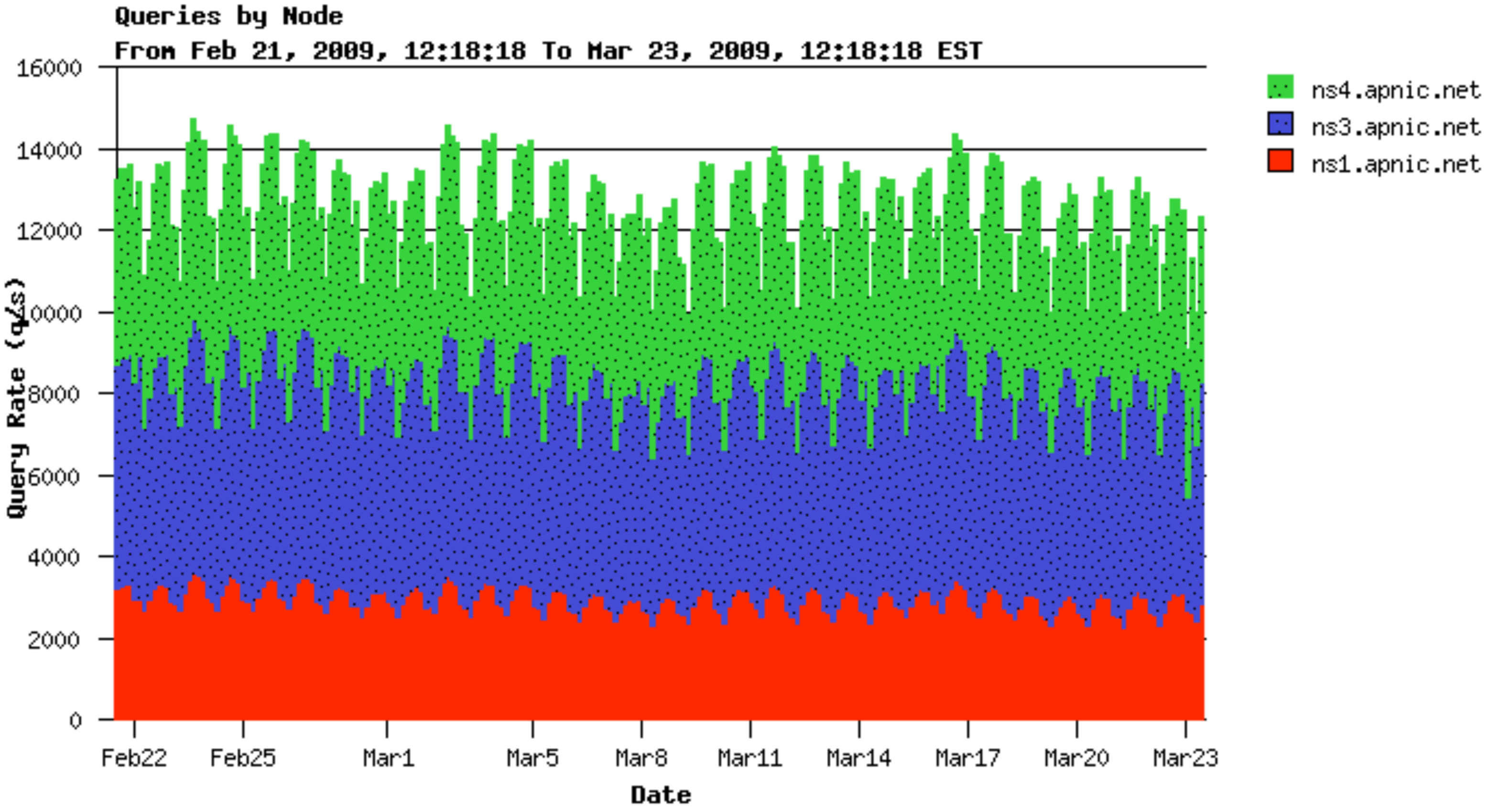
APNIC’s DNS

- RIRs are the delegation points for in-addr, ip6 .arpa. zones.
  - APNIC is the master DNS for the Asia-Pacific reverse-DNS
    - Supplies secondary DNS servers for other RIR in the AP region. Lowers RTT for lookups within region.
- 3 locations: Brisbane, Tokyo, Hong Kong
  - Co Located, 100mbit switching fabric
  - Good local & international connectivity

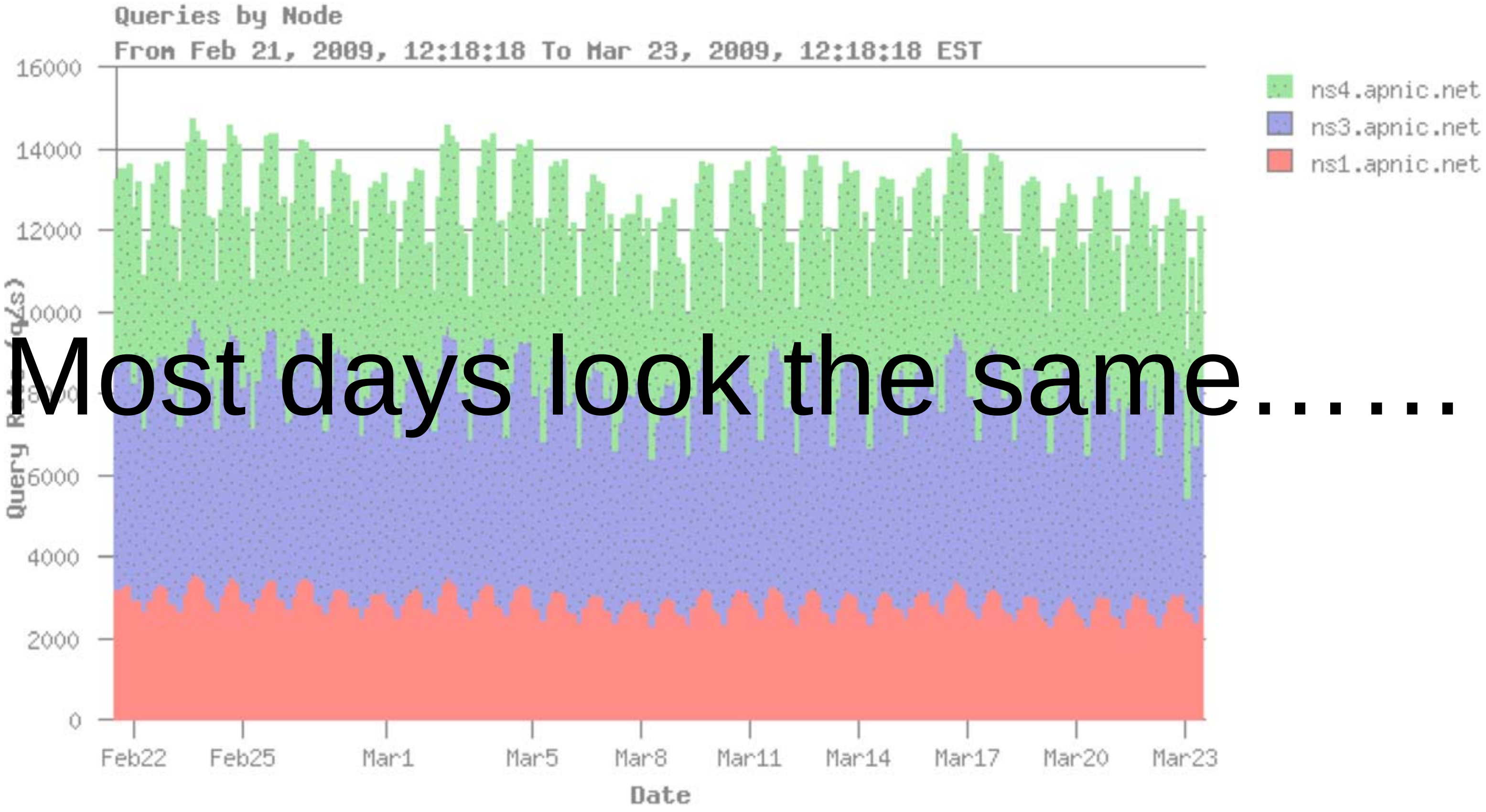
APNIC’s DNS

- DNS @ APNIC has two ‘forms’
  - The ‘NS’ hosts (ns1, ns3, ns4)
    - APNIC’s primary NS for its in-addr.arpa/ip6.arpa
    - The entire Asia-Pacific managed IP address space
  - The ‘SEC’ hosts (sec1, sec3)
    - Secondary NS for the other RIR
    - Also hosts a range of ccTLD, other forward namespaces
- Whats the behavior of these services? What do they do?

One month…

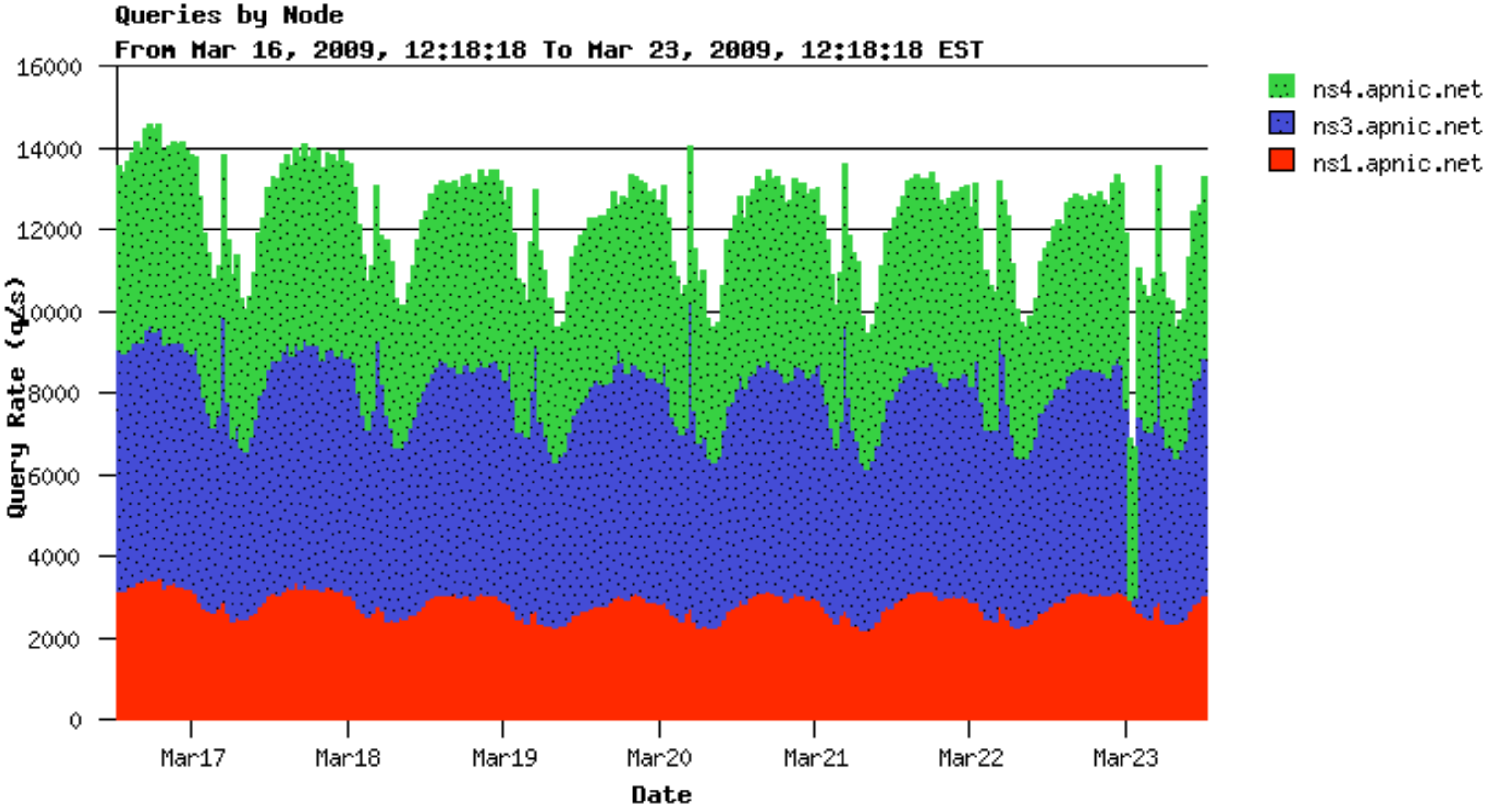

Queries by Node
From Feb 21, 2009, 12:18:18 To Mar 23, 2009, 12:18:18 EST
Query Rate (q/s)
16000
14000
12000
10000
8000
6000
4000
2000
0
Feb22
Feb25
Mar1
Mar5
Mar8
Mar11
Mar14
Mar17
Mar20
Mar23
Date
🟩 ns4.apnic.net
🟦 ns3.apnic.net
🟥 ns1.apnic.net

One month…

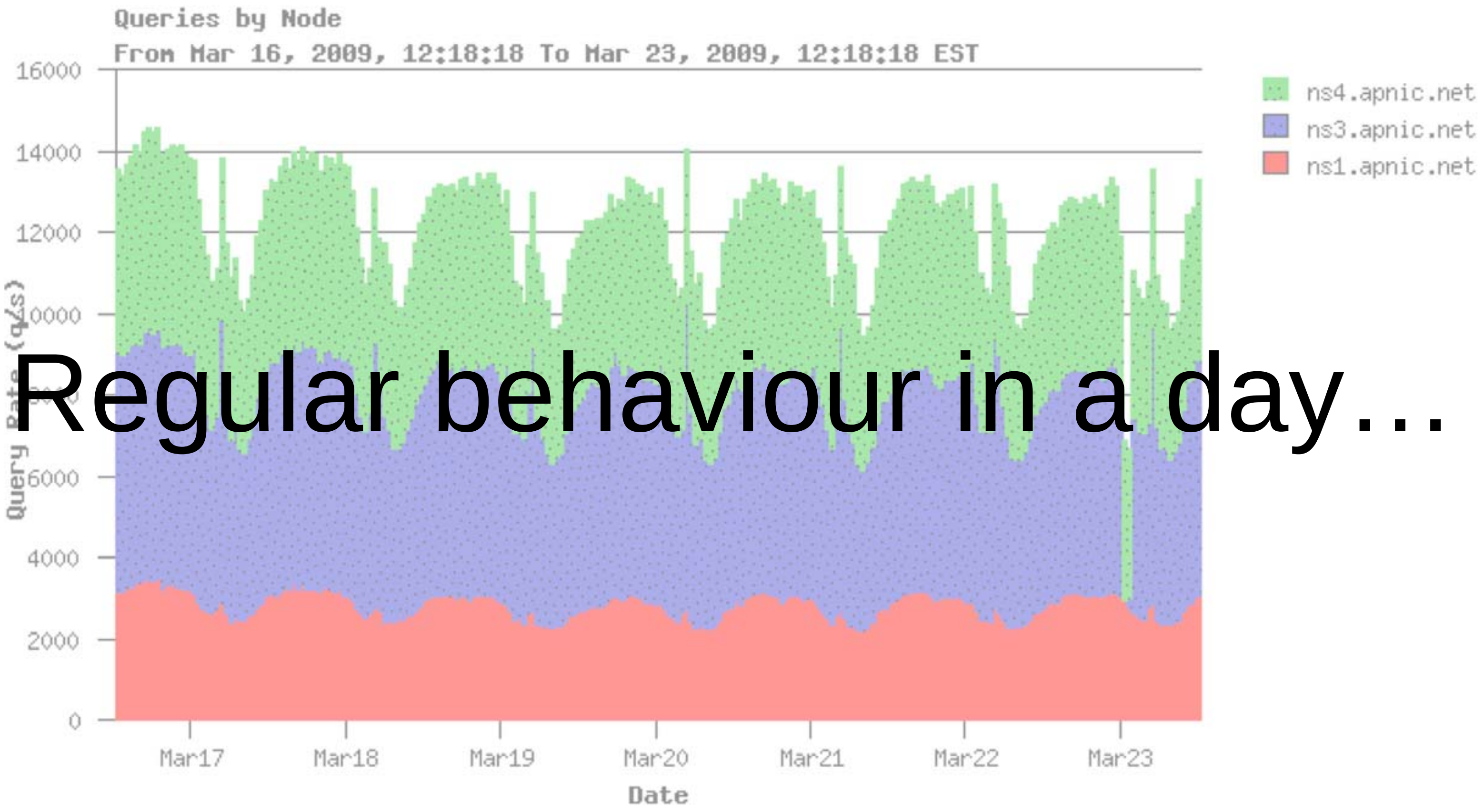


Most days look the same……

One Week…

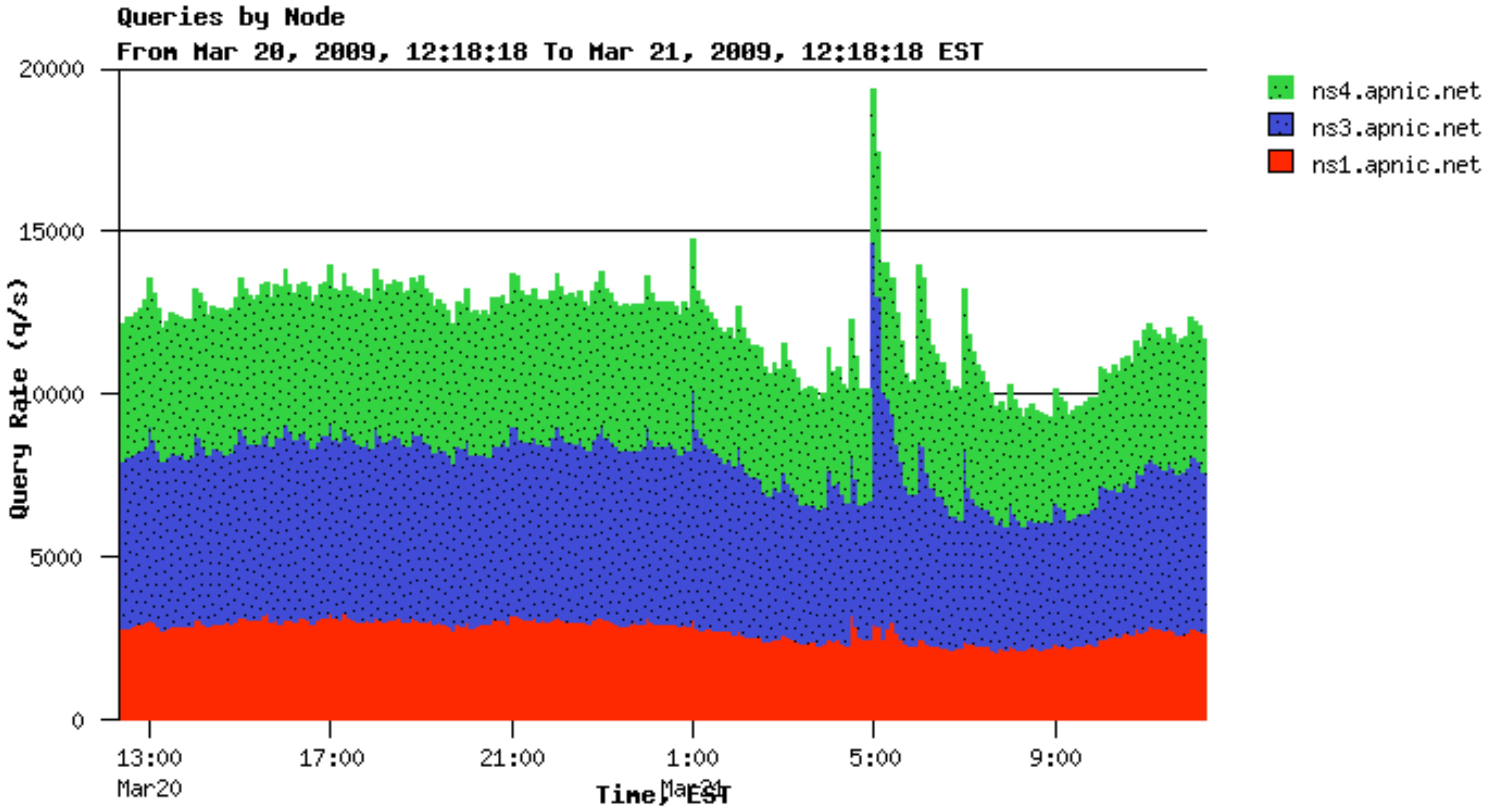

Queries by Node
From Mar 16, 2009, 12:18:18 To Mar 23, 2009, 12:18:18 EST
16000
14000
12000
10000
8000
6000
4000
2000
0
Query Rate (q/s)
Mar17
Mar18
Mar19
Mar20
Mar21
Mar22
Mar23
Date
ns4.apnic.net
ns3.apnic.net
ns1.apnic.net

One Week…

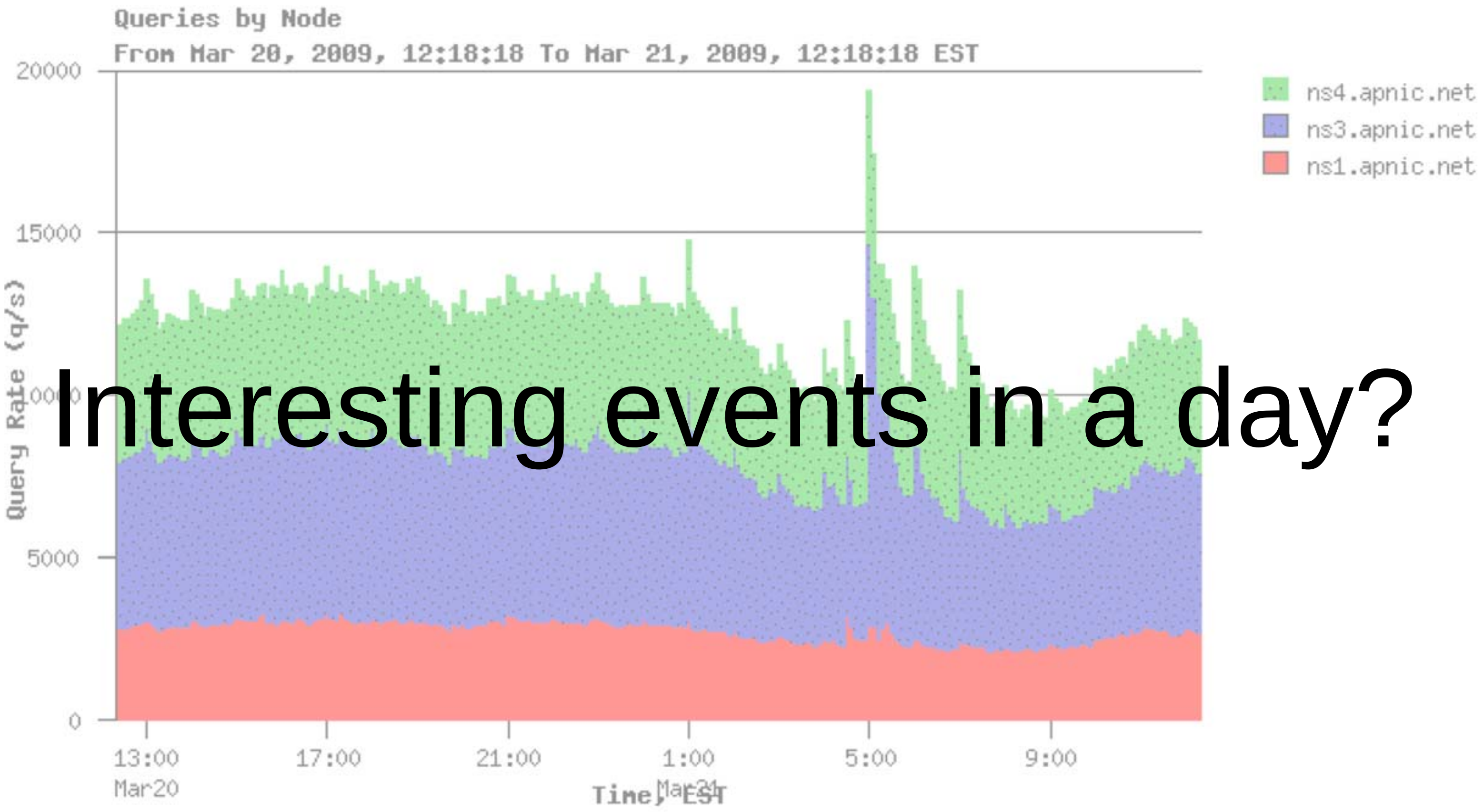


Regular behaviour in a day…

One Day …

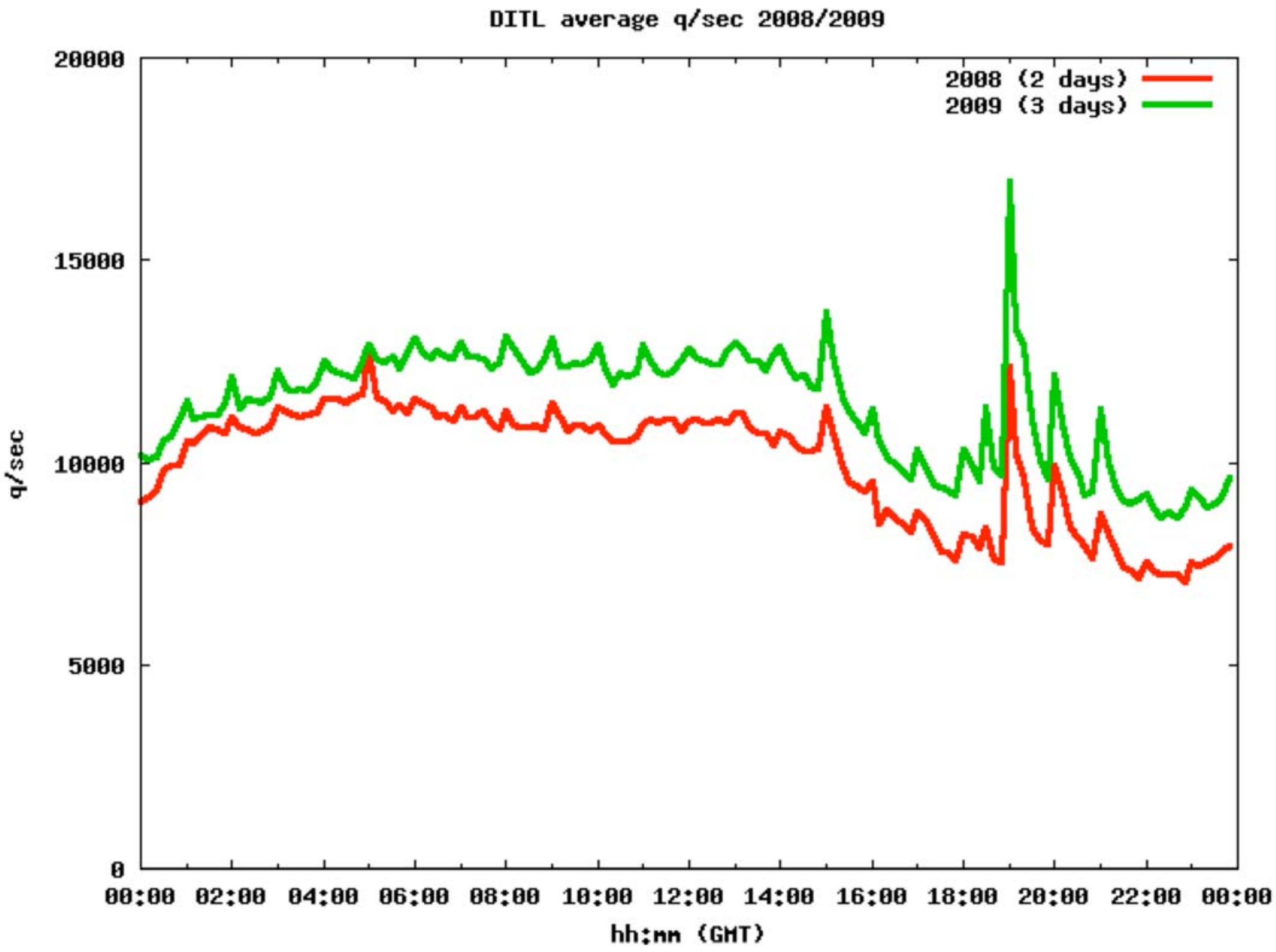

Queries by Node
From Mar 20, 2009, 12:18:18 To Mar 21, 2009, 12:18:18 EST
20000
15000
10000
5000
0
Query Rate (q/s)
13:00
Mar20
17:00
21:00
1:00
Mar21
5:00
9:00
Time, EST
ns4.apnic.net
ns3.apnic.net
ns1.apnic.net

One Day …

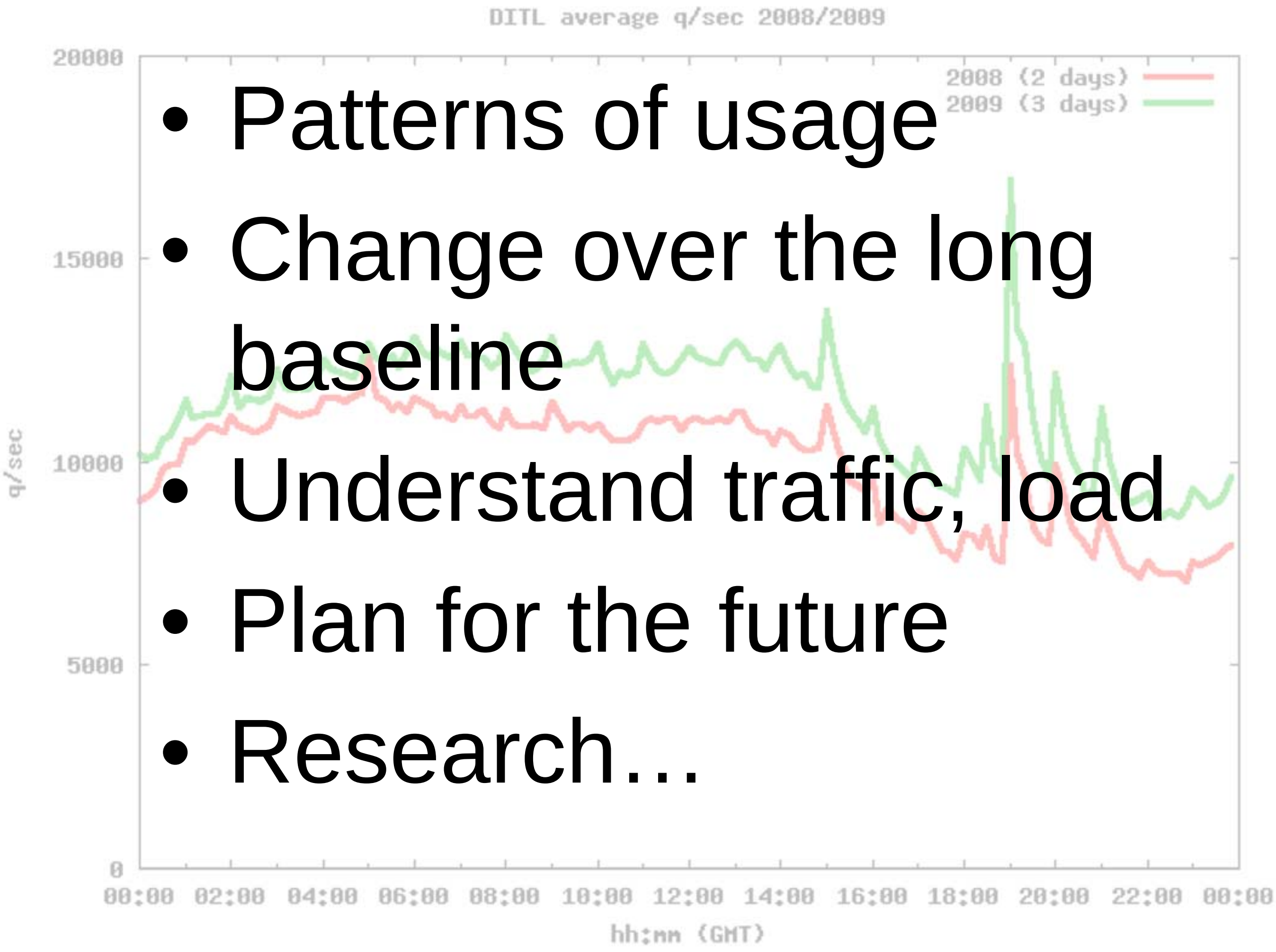


Interesting events in a day?

DITL 2008-2009 AP region



DITL 2008-2009 AP region



- Patterns of usage
- Change over the 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
  - across at least one 24h period.
- Organized by CAIDA
  - Data warehouse provided by OARC
  - Tools from OARC, ISC, ‘the measurement factory’
- Provides resource for longer term analysis
  - Data archive warehouse
  - Opportunity for retrospective/review of data
- Long baseline resource

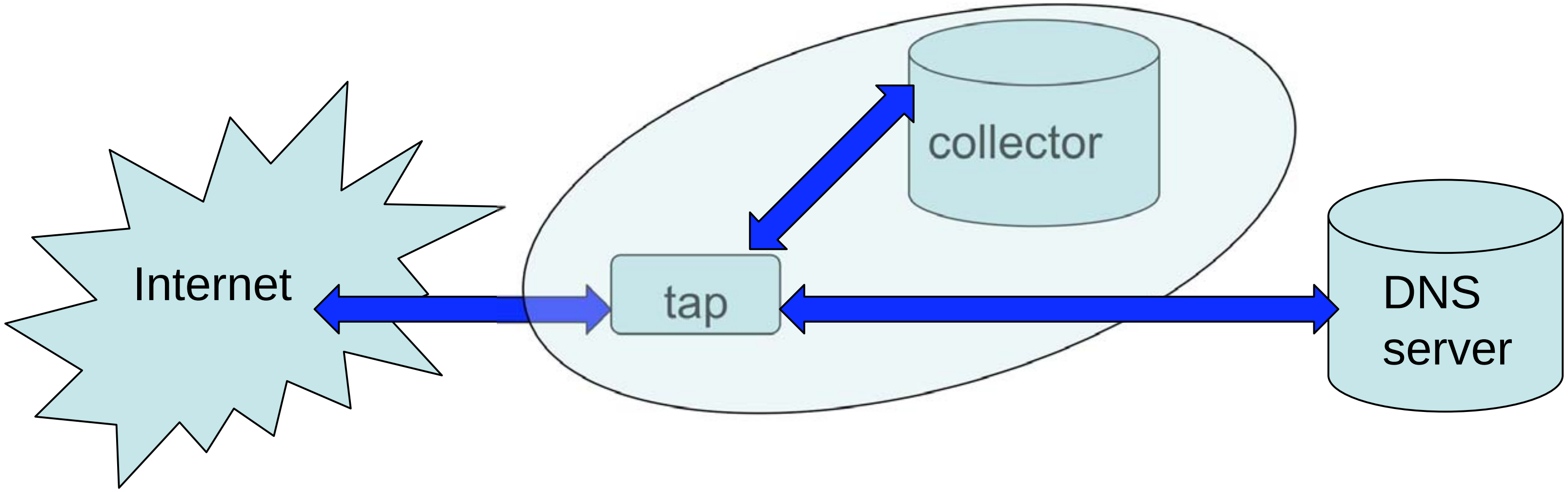
Day In The Life

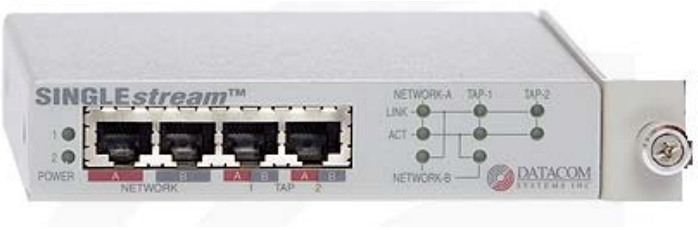
- First collection 2006
  - 4 DNS participants, selected campus/local IX
- Fourth event (March 29-April2)
  - 37 participants, ~190 nodes of collection
  - Of the order 4Tb data (!)
- APNIC contributing since 2008
  - from all operated DNS servers
  - this only represents a subset of APNIC NS serve, for its own domains.
    - secondary NS of APNIC ranges are hosted at other RIR
  - DITL data capture system provides APNIC internal logging/measurement on an ongoing basis

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

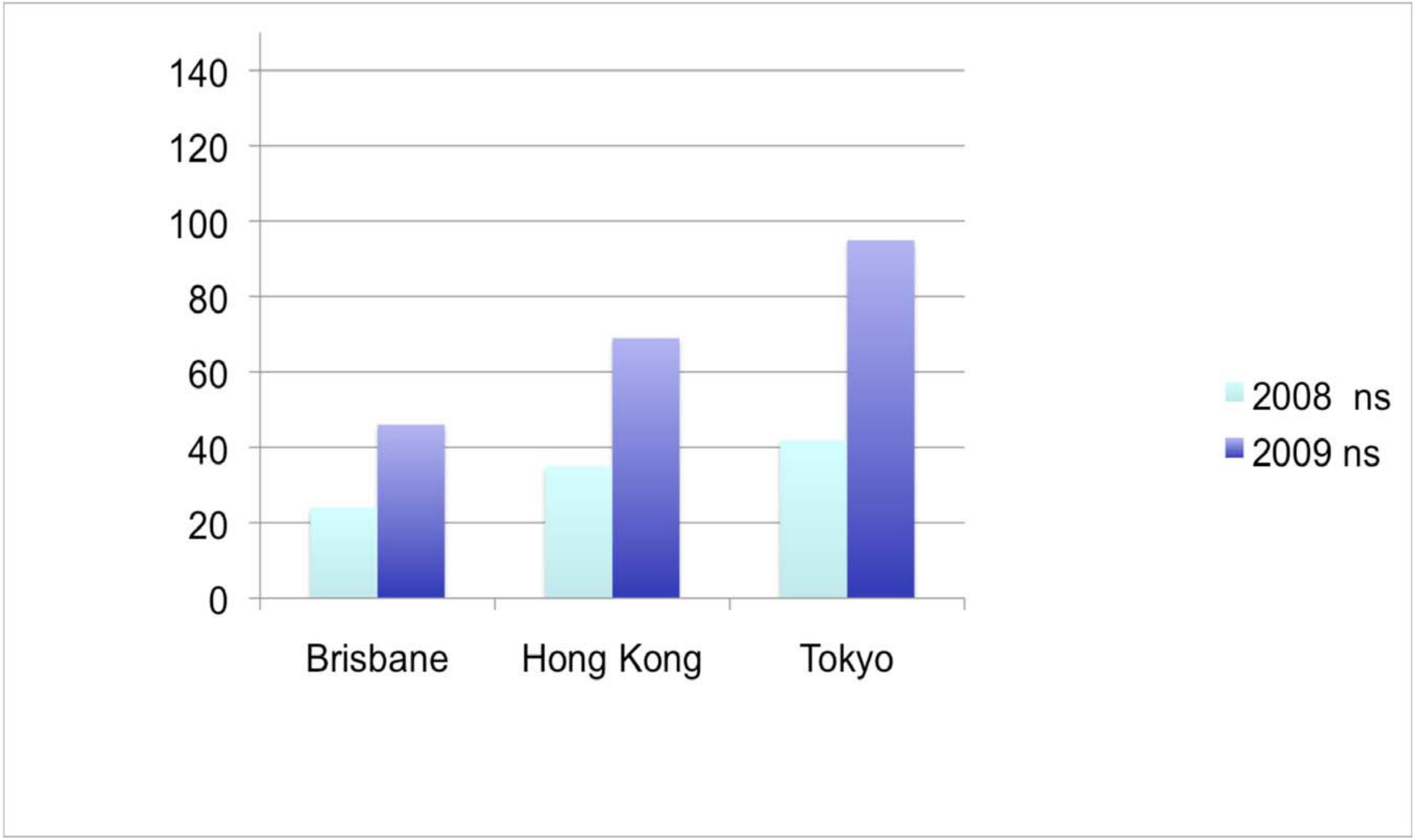
Data Capture





- 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

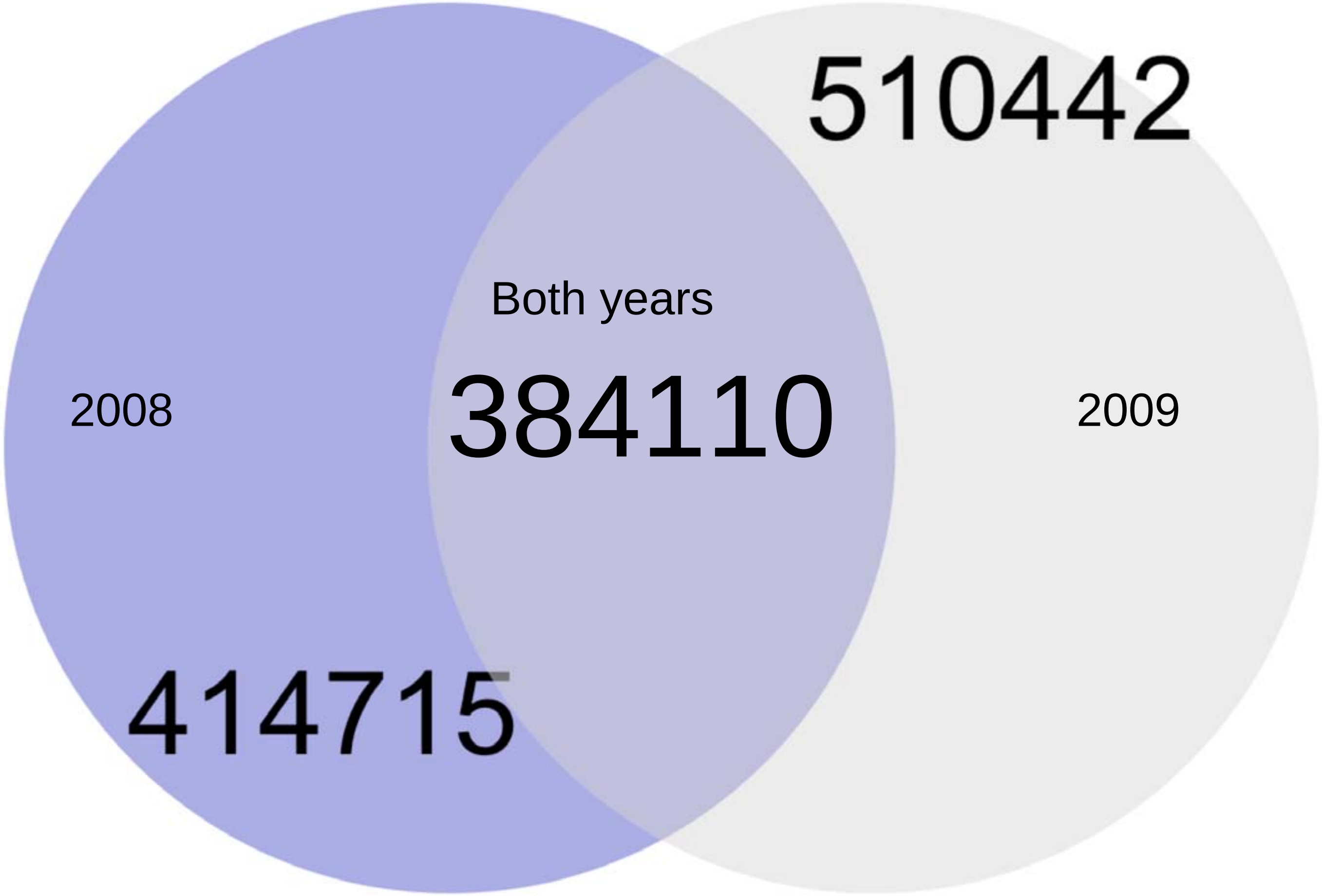
AP DiTL Data Capture (gb)



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



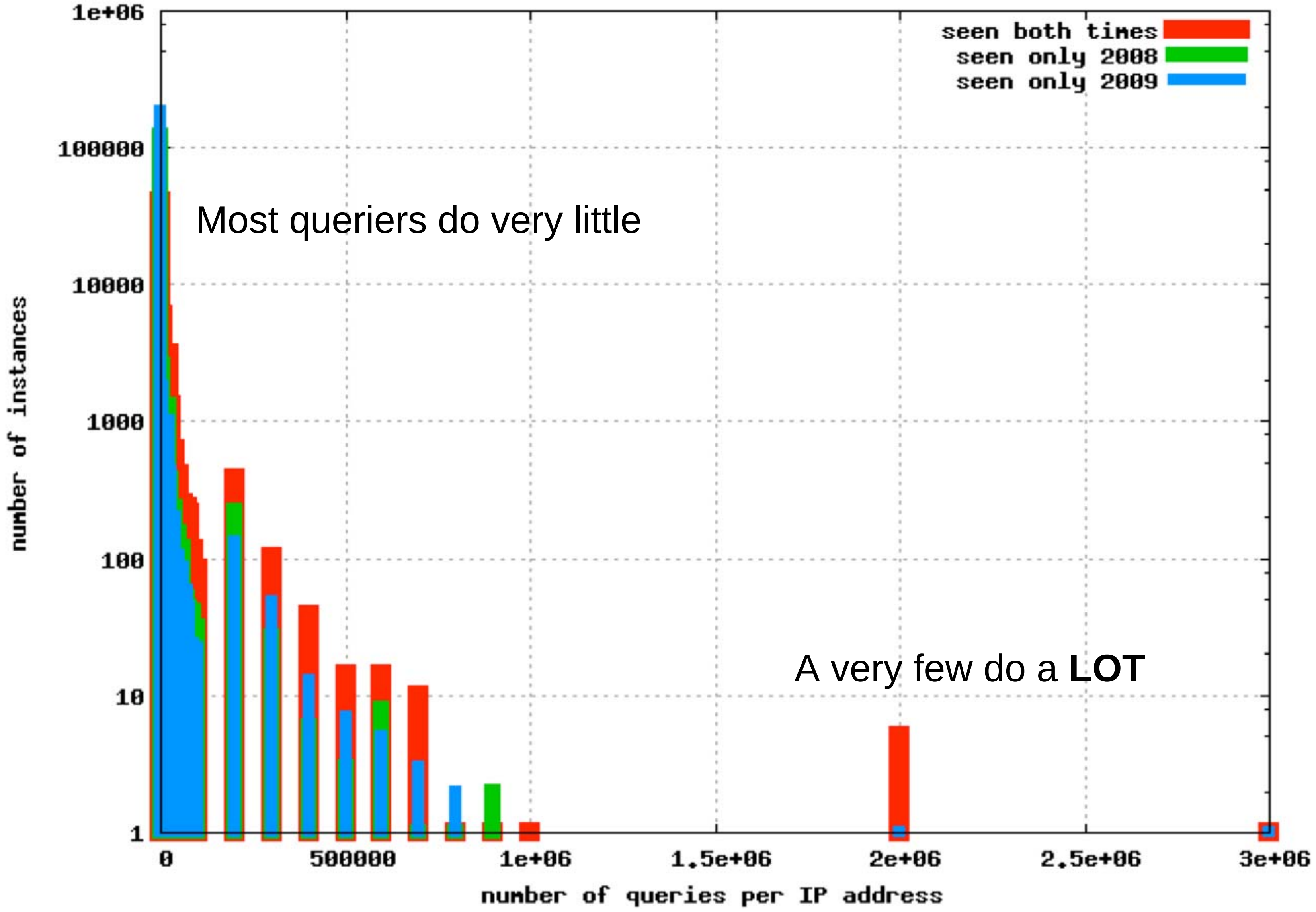
Not a lot of Address re-use

- 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?



Most queriers do very little

A very few do a **LOT**

This is strange…

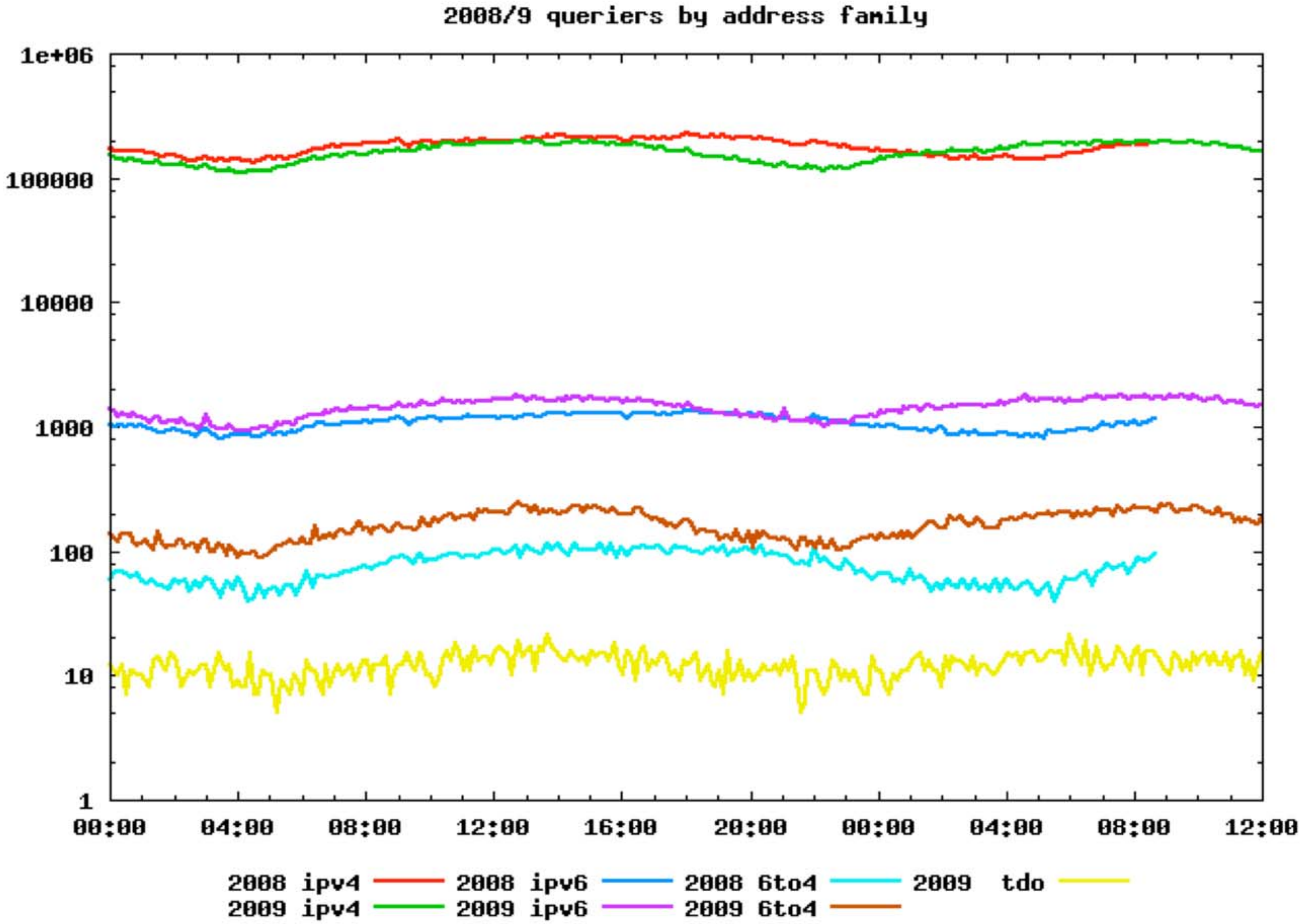
- The majority of seen IP addresses do one, or only a few queries.
  - A very few addresses seen, do hundreds or thousands of queries
  - <10 do millions.
- PTR: ‘infrastructure’ DNS?
  - If its infrastructure, why so much volatility in the IP addresses doing DNS querying?
    - Its not SOA fetching. Most queries are PTR
  - Expected to see far more persistent IP addresses across 2008/2009.

This is strange…

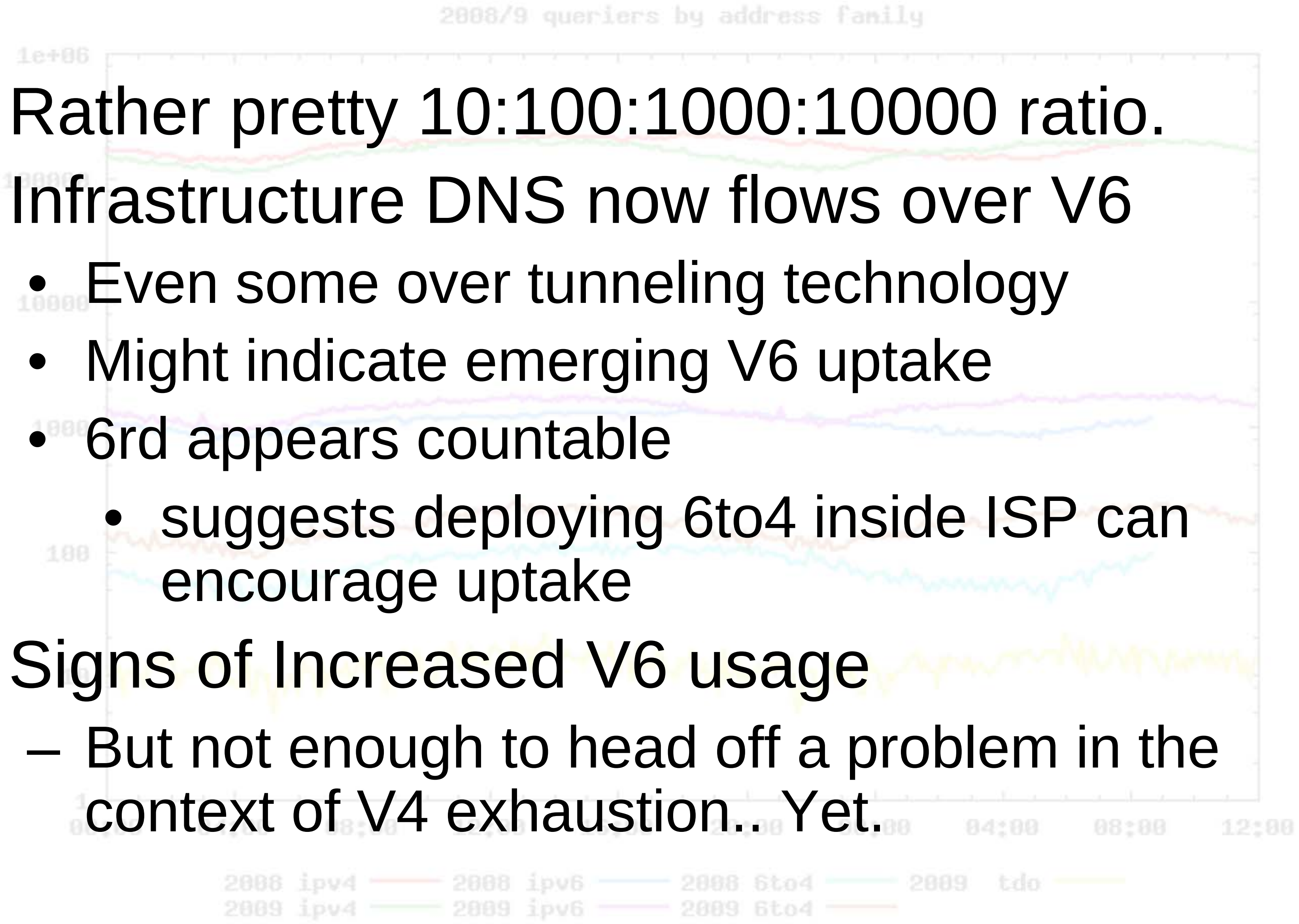
- End-user boxes doing reverse-DNS?
  - – Firewalls, probe-tests, other applications?
  - – For further study.
- Suggests the ‘real’ count of deployed infrastructure resolvers hitting APNIC DNS servers is lower than we thought
  - – <millions. Most hits from ‘singletons’
  - – Still, traffic is traffic: people want DNS from us

V4/V6 comparisons

Queries by IP protocol



Queries by IP protocol

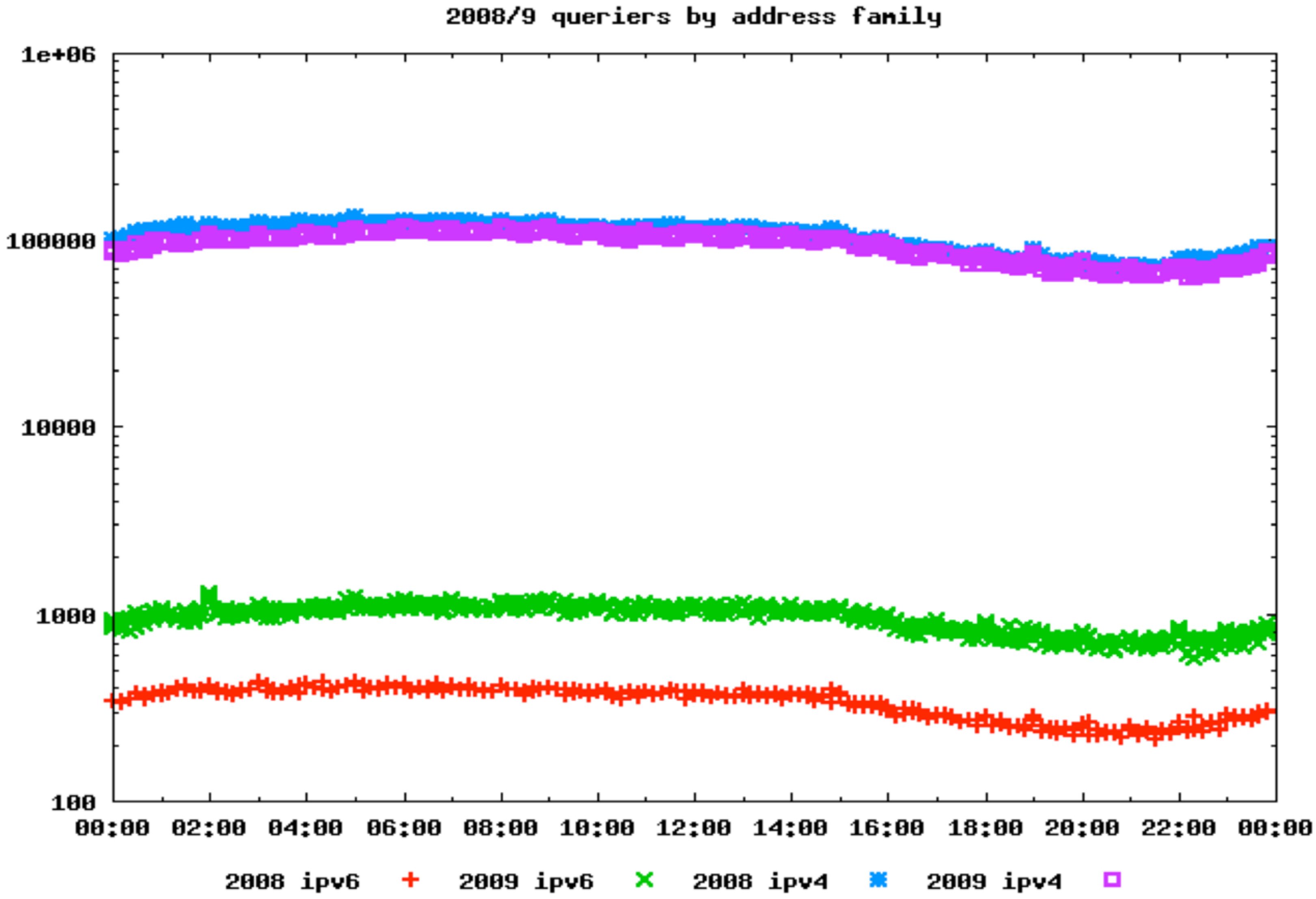


- Rather pretty 10:100:1000:10000 ratio.
- Infrastructure DNS now flows over V6
  - Even some over tunneling technology
  - Might indicate emerging V6 uptake
  - 6rd appears countable
    - suggests deploying 6to4 inside ISP can encourage uptake
- Signs of Increased V6 usage
  – But not enough to head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

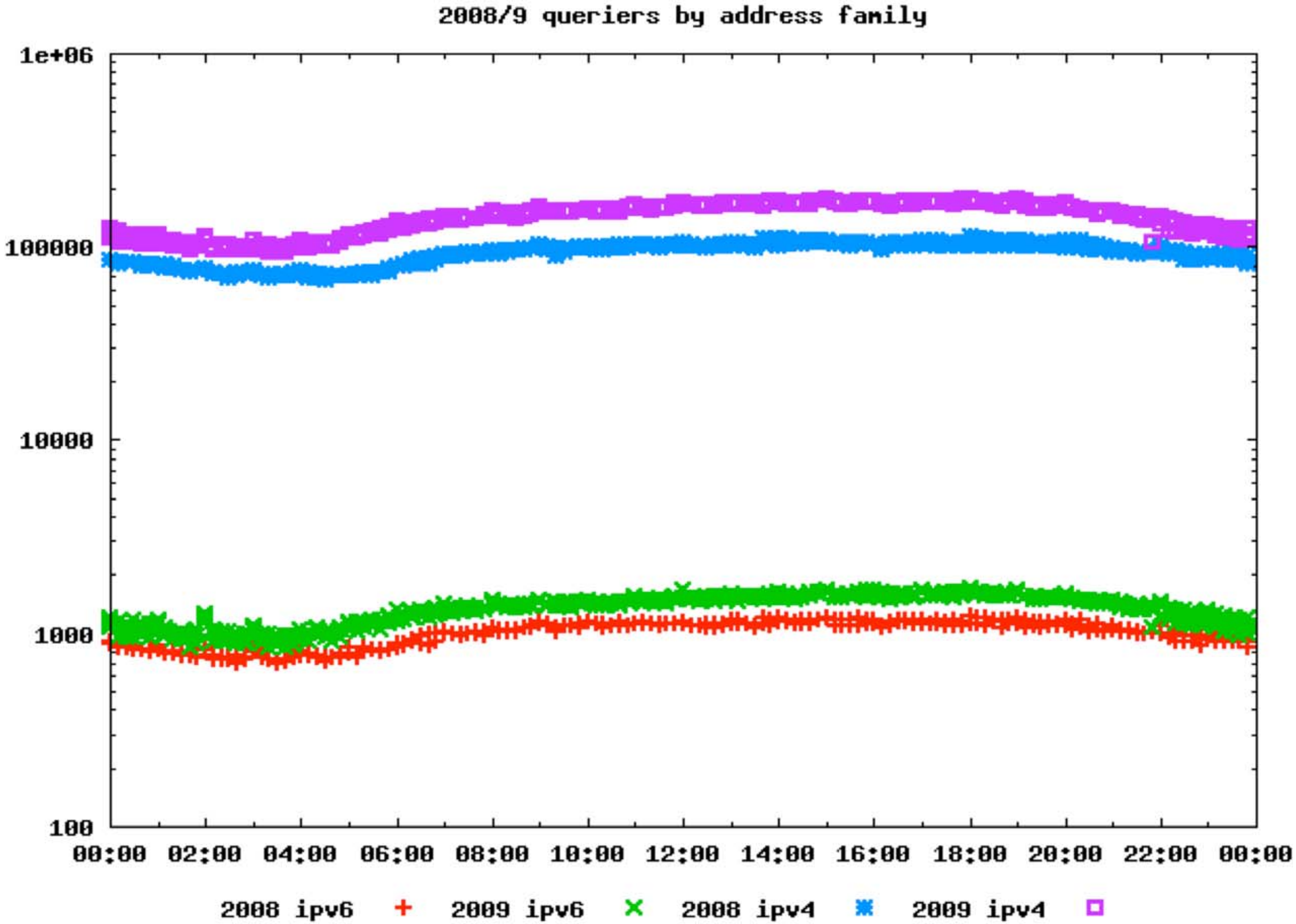
Tunneled V6 for DNS?

- 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
  - Approx 1500 registered reverse 6to4 zones

Overall V4/V6 NS



Overall V4/V6 SEC



V4/V6 Relativities changing

- Overall, IPv4 unique IP address counts fairly constant
  - of the order 100,000 per 10min sample window
    - but with some increase in SEC 08-09
- IPv6 saw an increase for the NS hosts
  - Addition of IPv6 in Hong Kong probably attracted traffic into region
  - Overall IPv6 levels consistent NS/SEC now
- Still 2 orders of magnitude smaller than IPv4

Its not Just the Asia-Pacific!

- Even noting the RTT, Many EU located economies use Asia Pacific located DNS servers to resolve PTR queries.
  - – Ie, SEC queries in both V4 and V6 include Europe, Africa, Americas
- Interesting to speculate if the lookup ratios reflect traffic, other measures of inter-economy dataflow
- For further study

Lessons learned 2008-2009

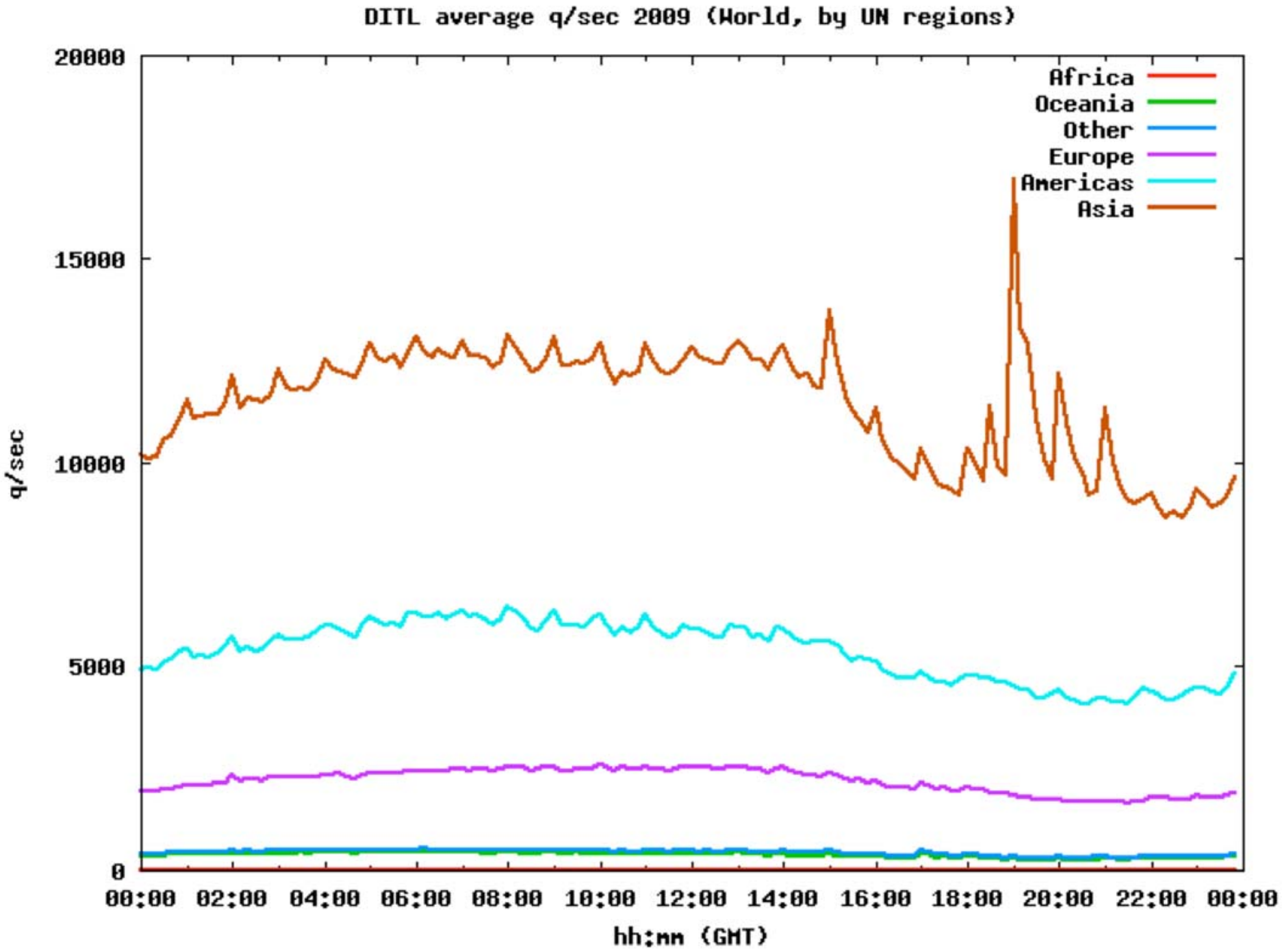
- 2008: 1hour captures
  - Huge risks if capture failed
  - Harder to upload to OARC (serialized)
  - 2009: 10 minute captures, parallel upload
- 2008: ran capture hosts on localtime
  - …but NTP was broken (2+hr offset) ☹
  - 2009: ran capture hosts on UTC, NTP checked!
- 2008: full capture, query + 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!

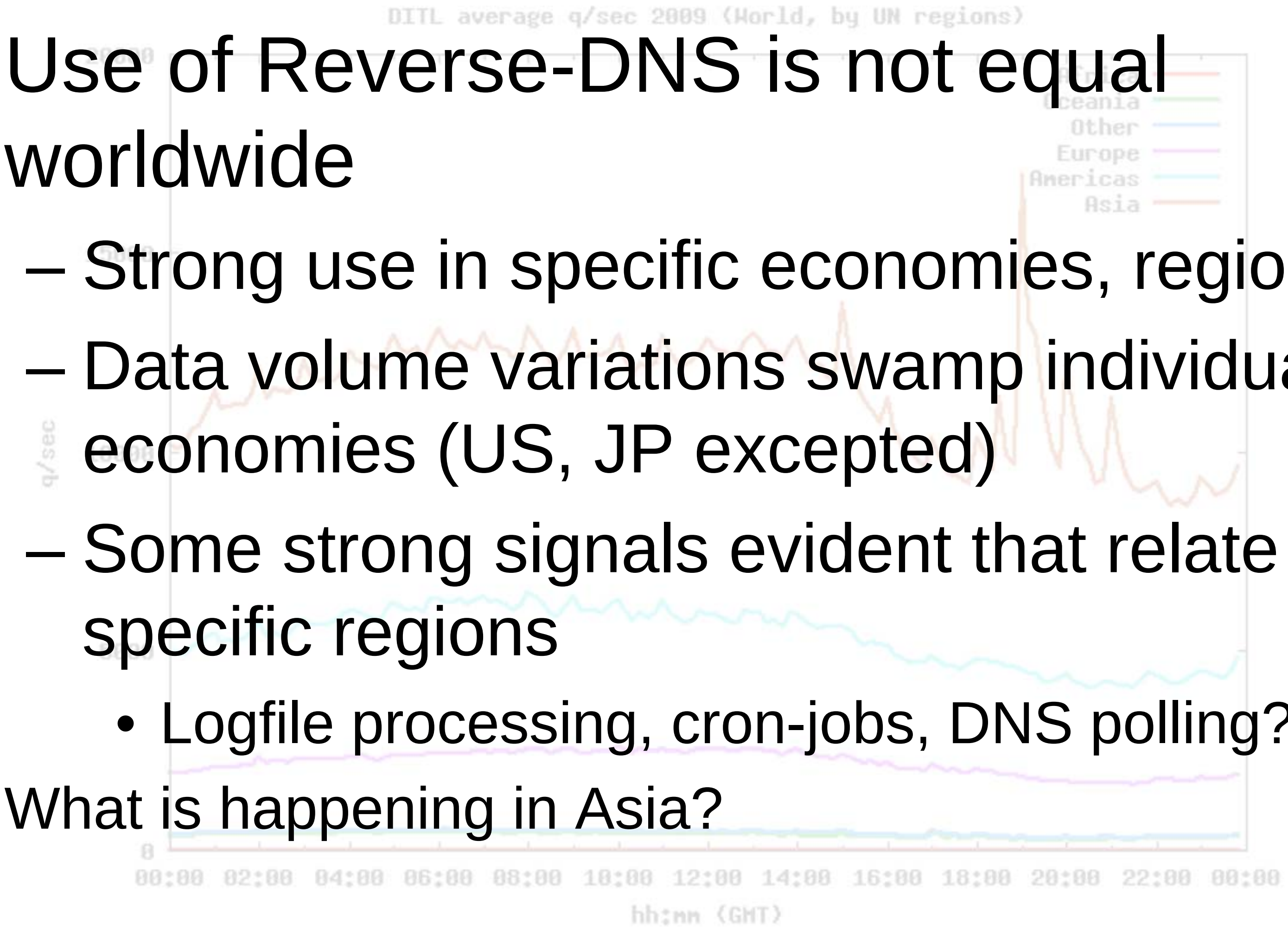
DITL by regions overall query rate

UN Region breakdowns

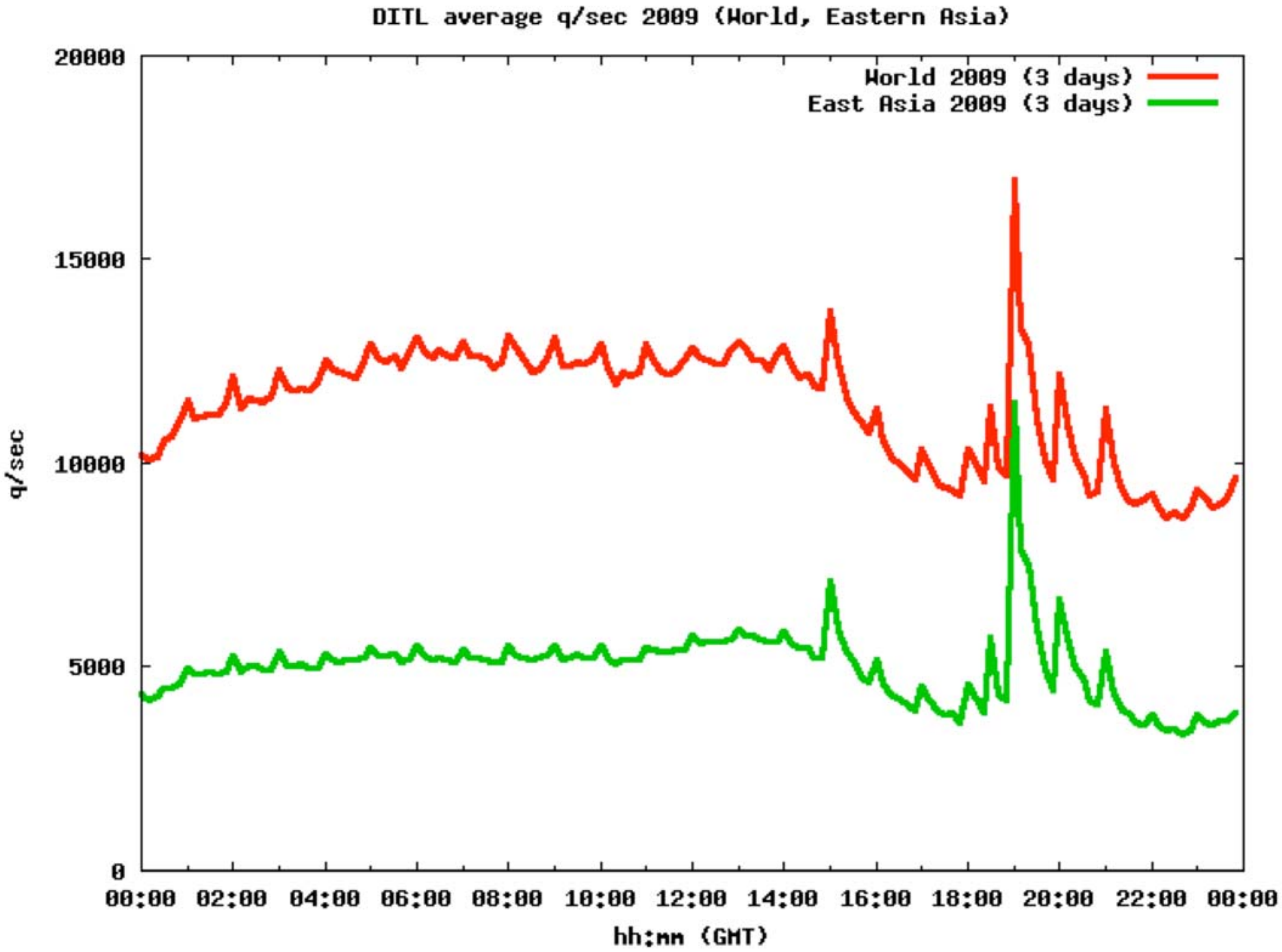


UN Region breakdowns

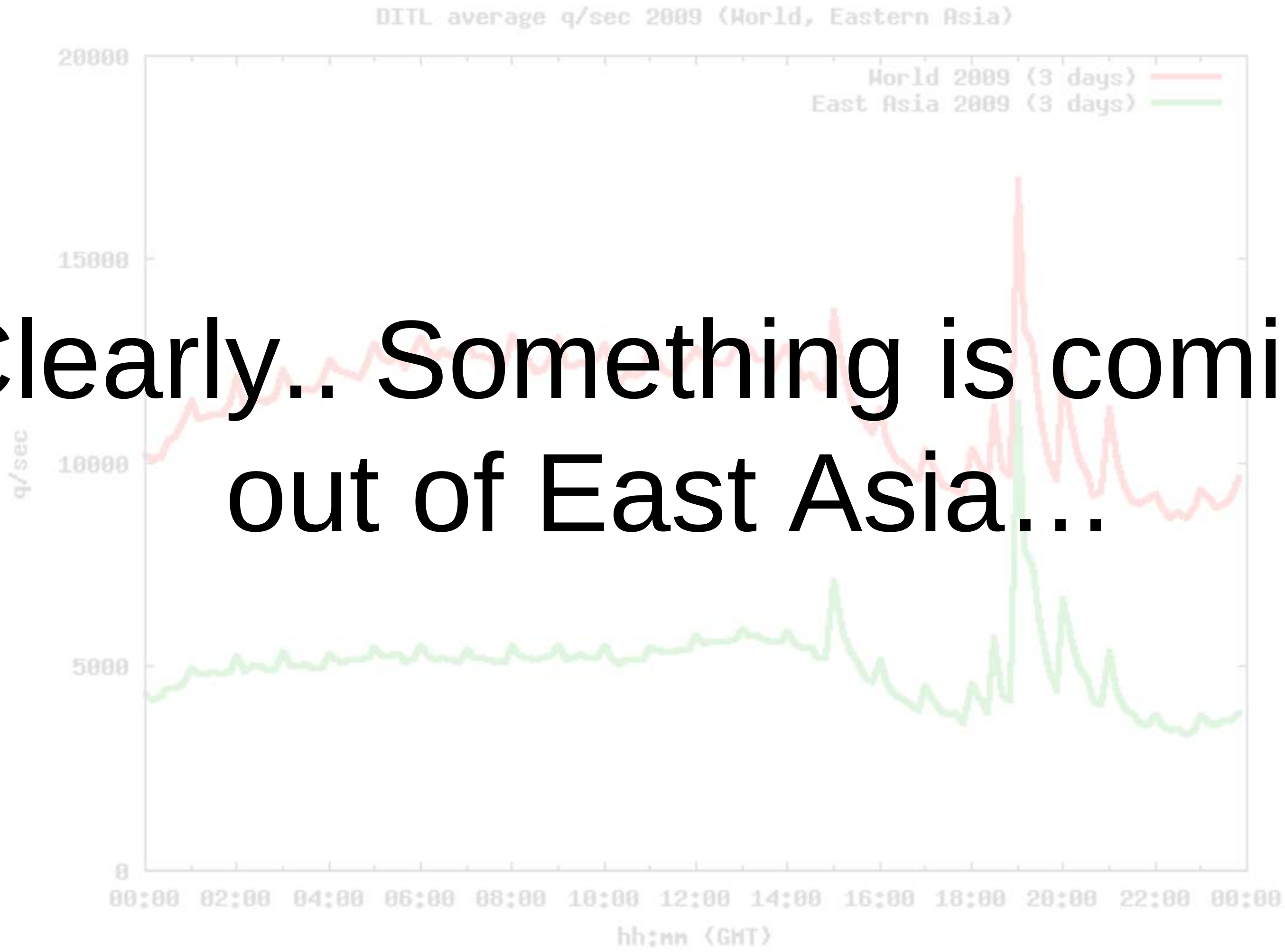
- Use of Reverse-DNS is not equal worldwide
  - Strong use in specific economies, regions
  - Data volume variations swamp individual economies (US, JP excepted)
  - Some strong signals evident that relate to specific regions
    - Logfile processing, cron-jobs, DNS polling?
- What is happening in Asia?



E. Asia in the World of DNS

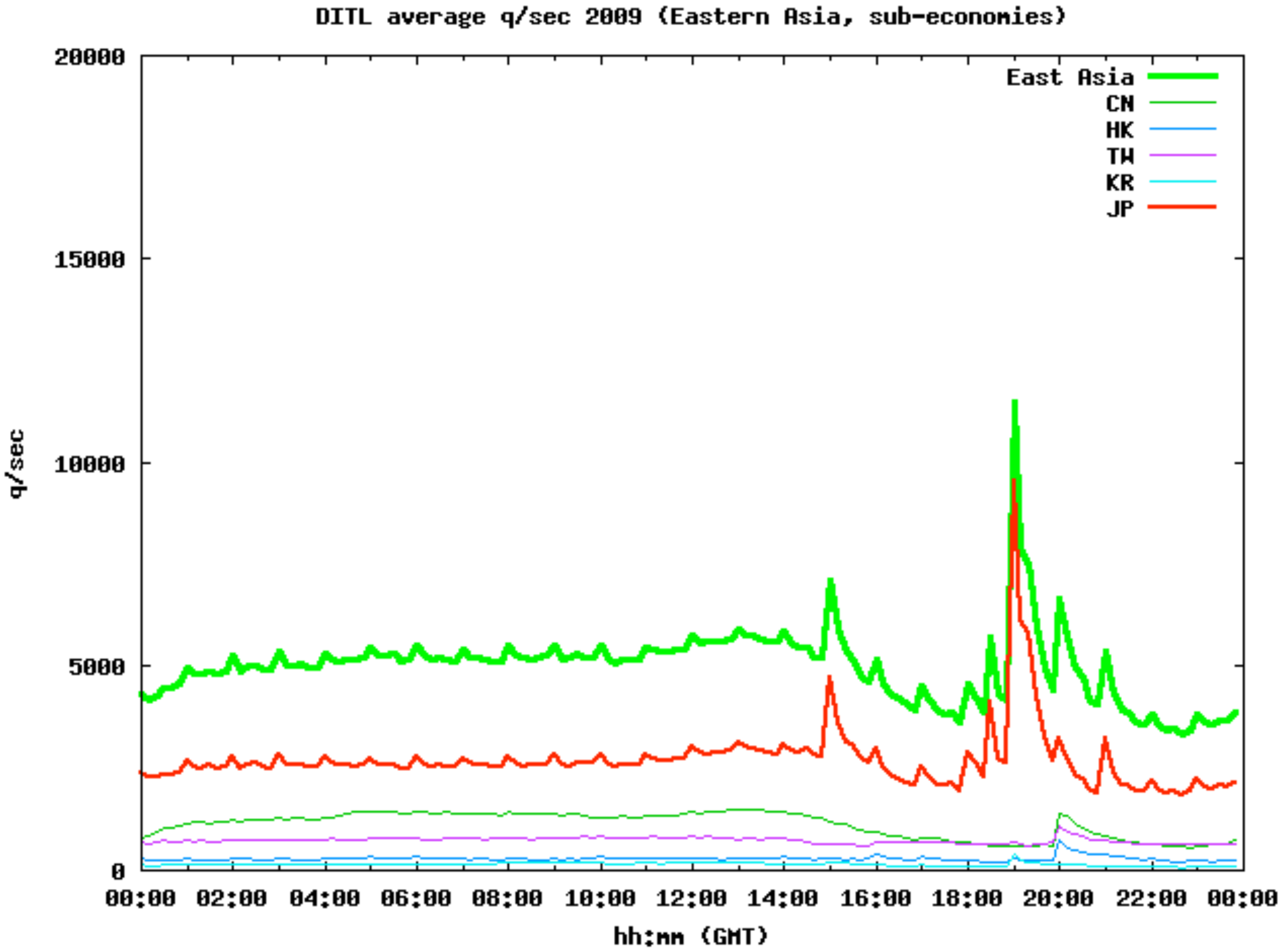


E. Asia in the World of DNS



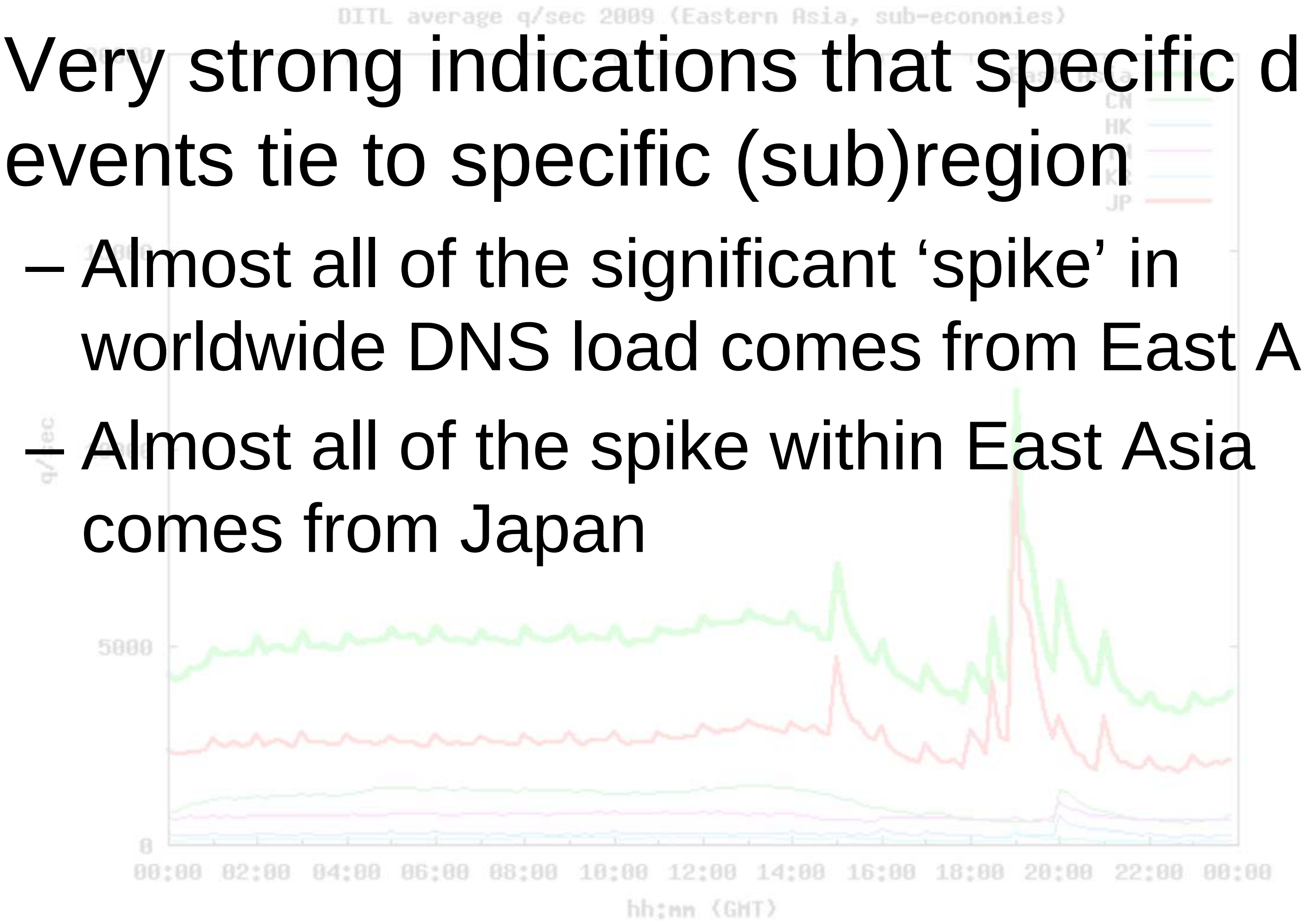
Clearly.. Something is coming out of East Asia…

E. Asia breakdowns

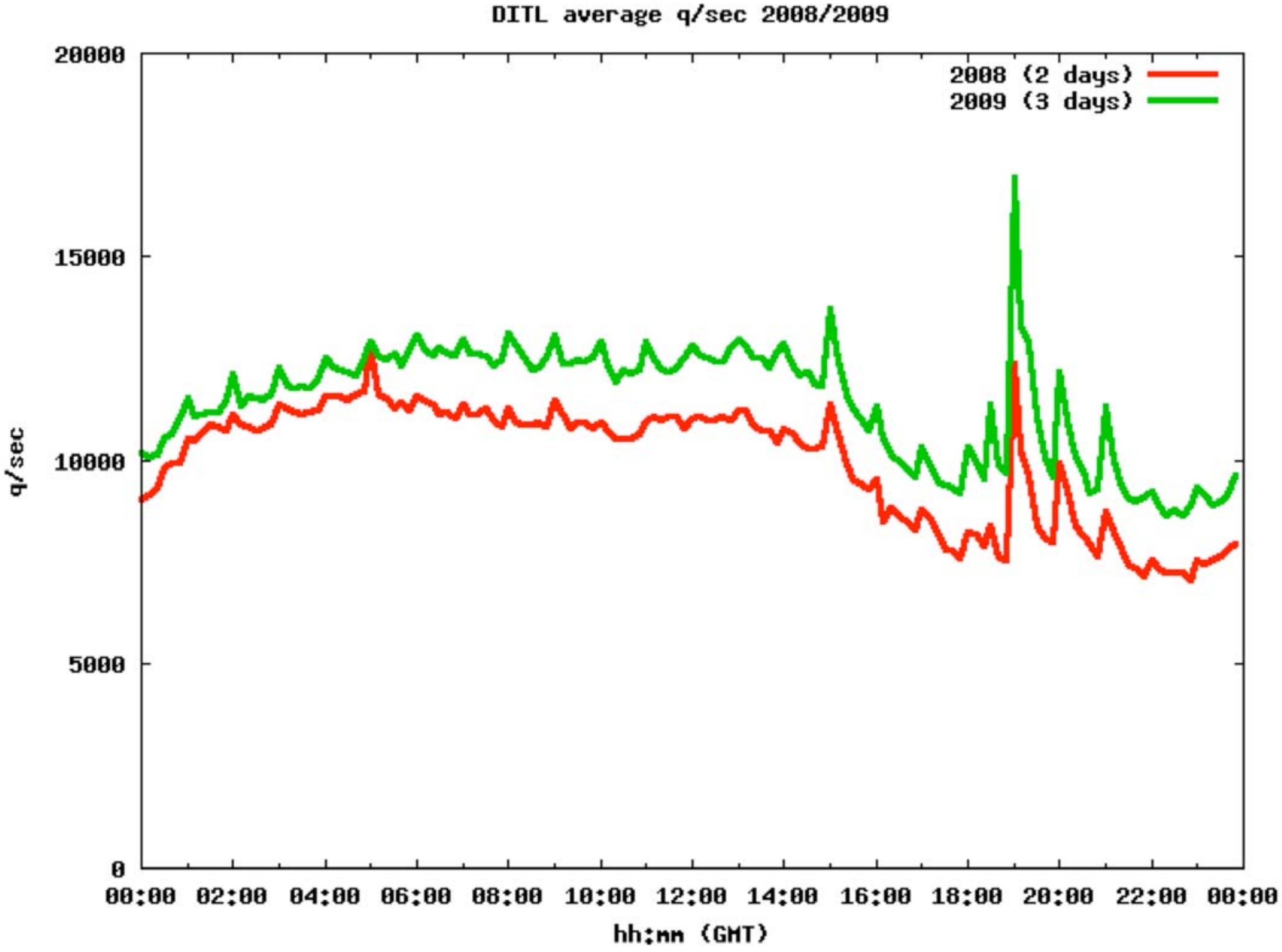


East Asia breakdowns

- 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

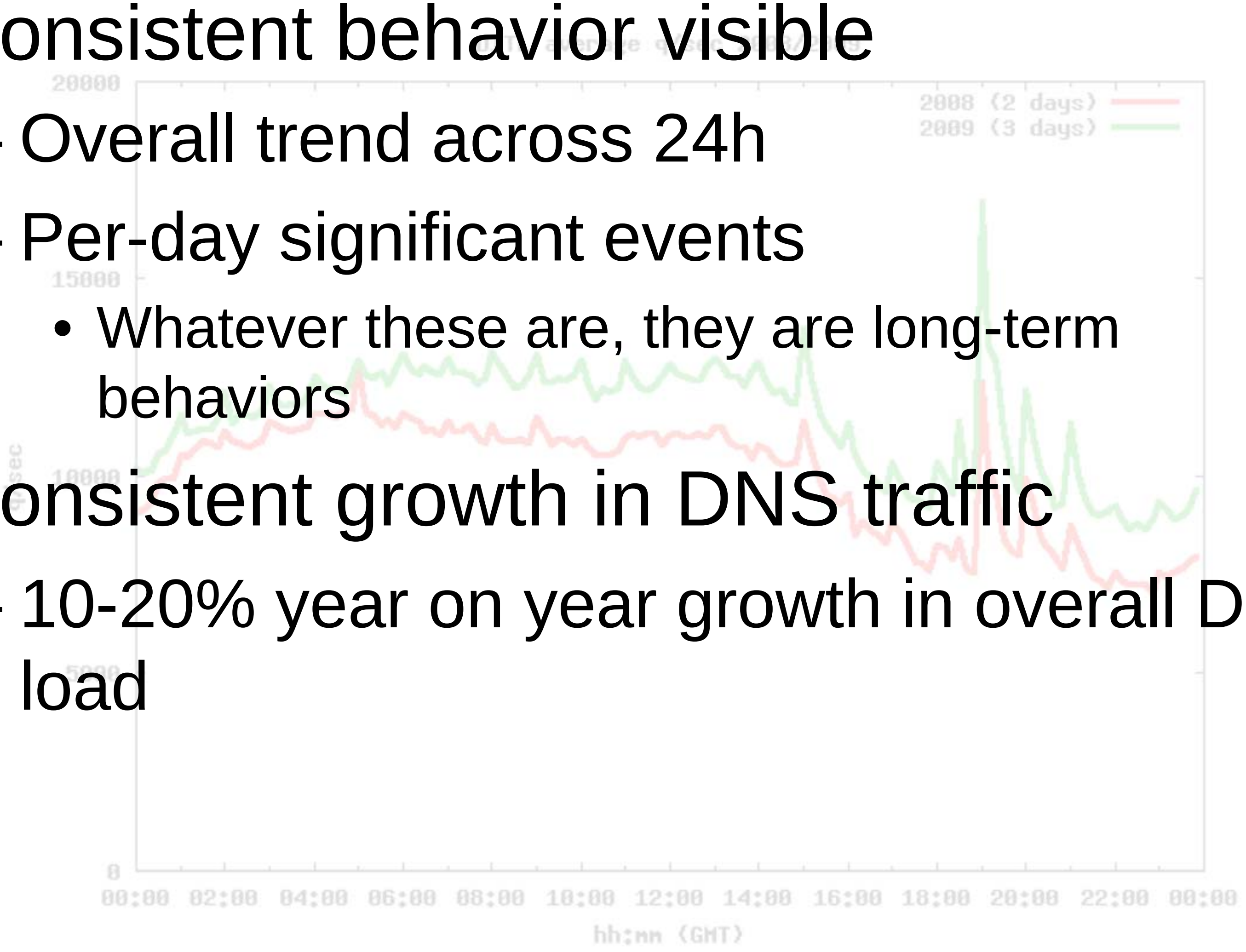


DITL 2008-2009 AP region



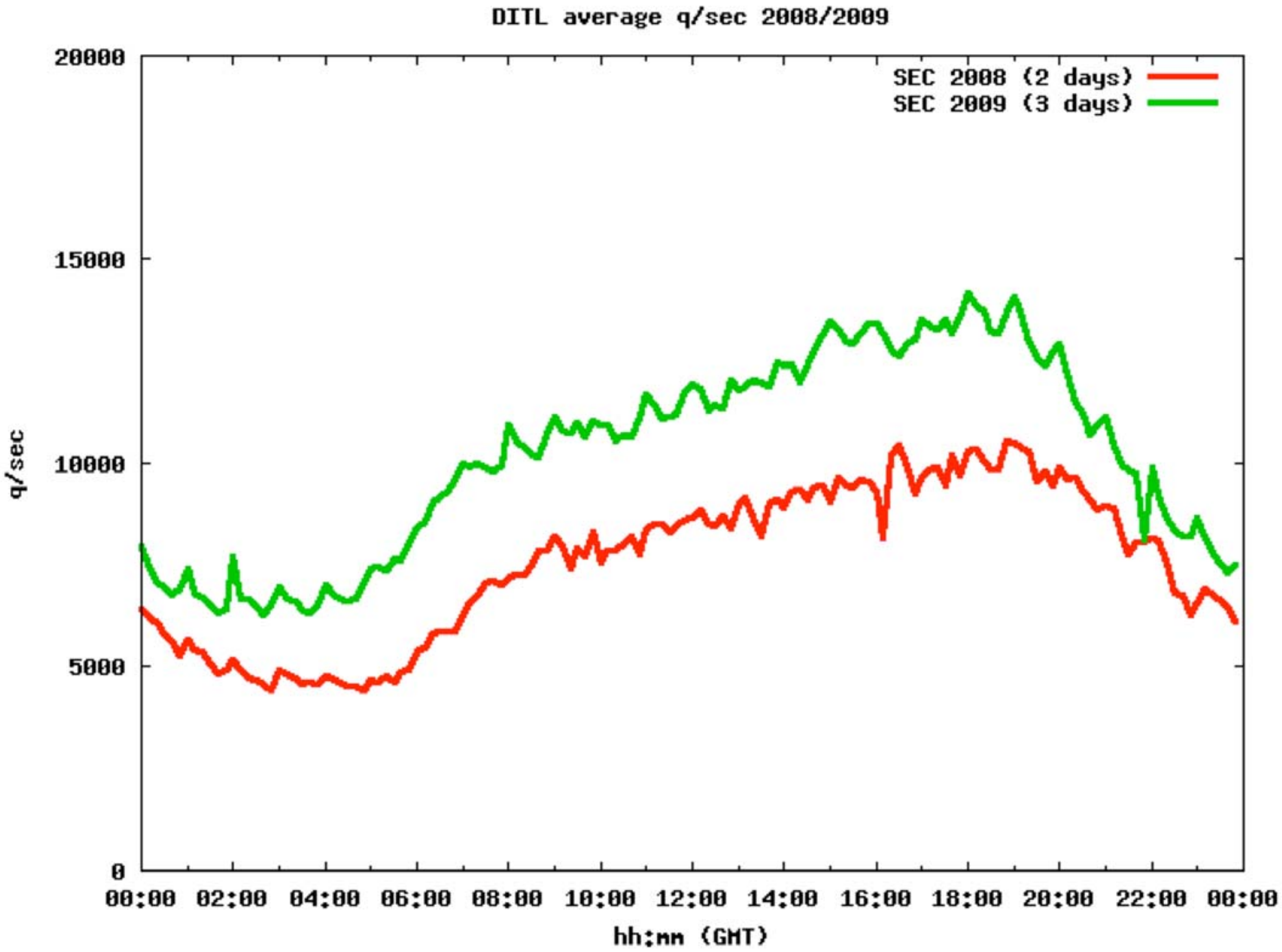
DITL 2008-2009 AP region

- 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



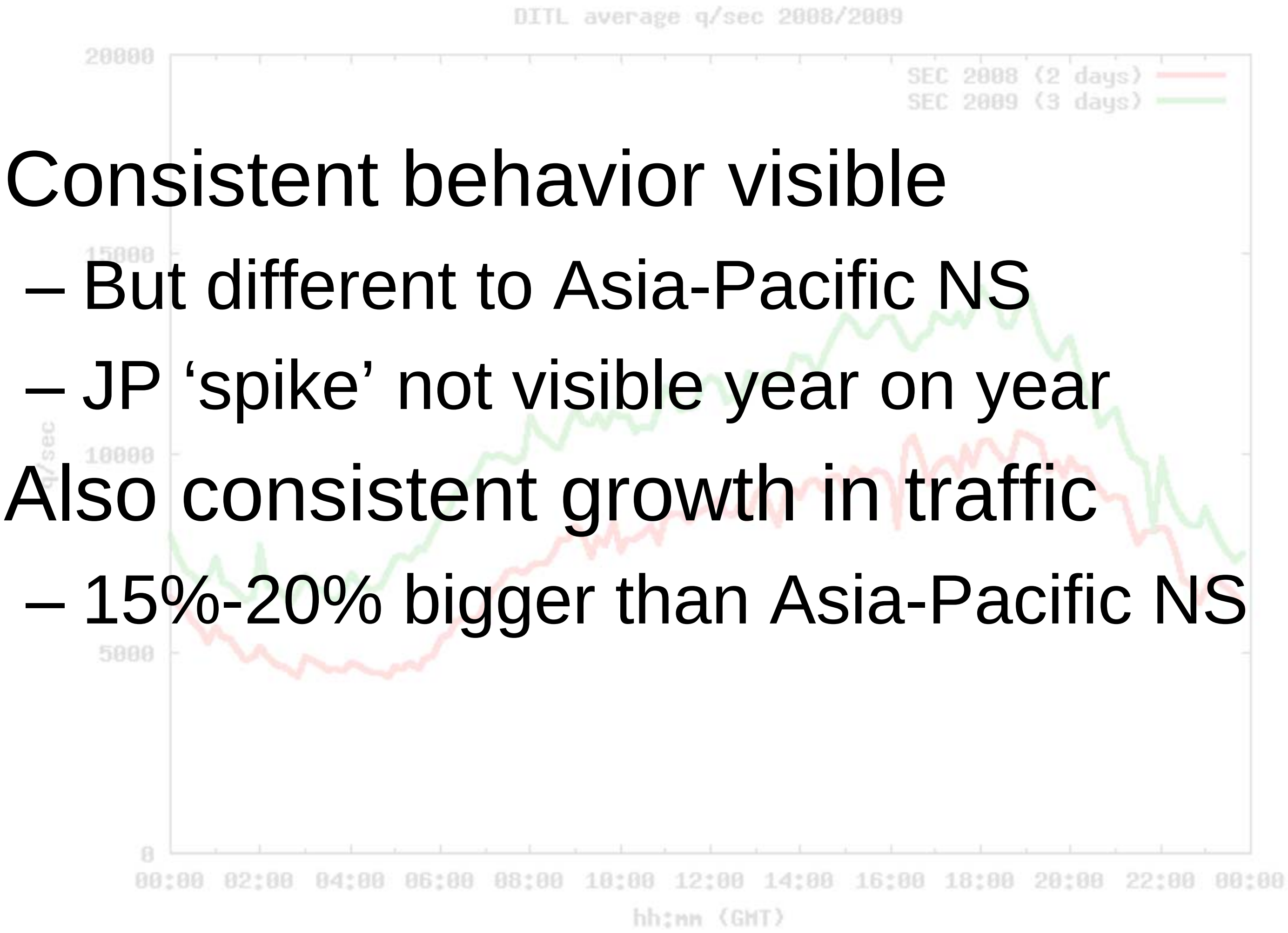
APNIC 28 Beijing, China 24-28 August 2009

DITL 2008-2009
rest of the world



APNIC 28 Beijing, China 24-28 August 2009

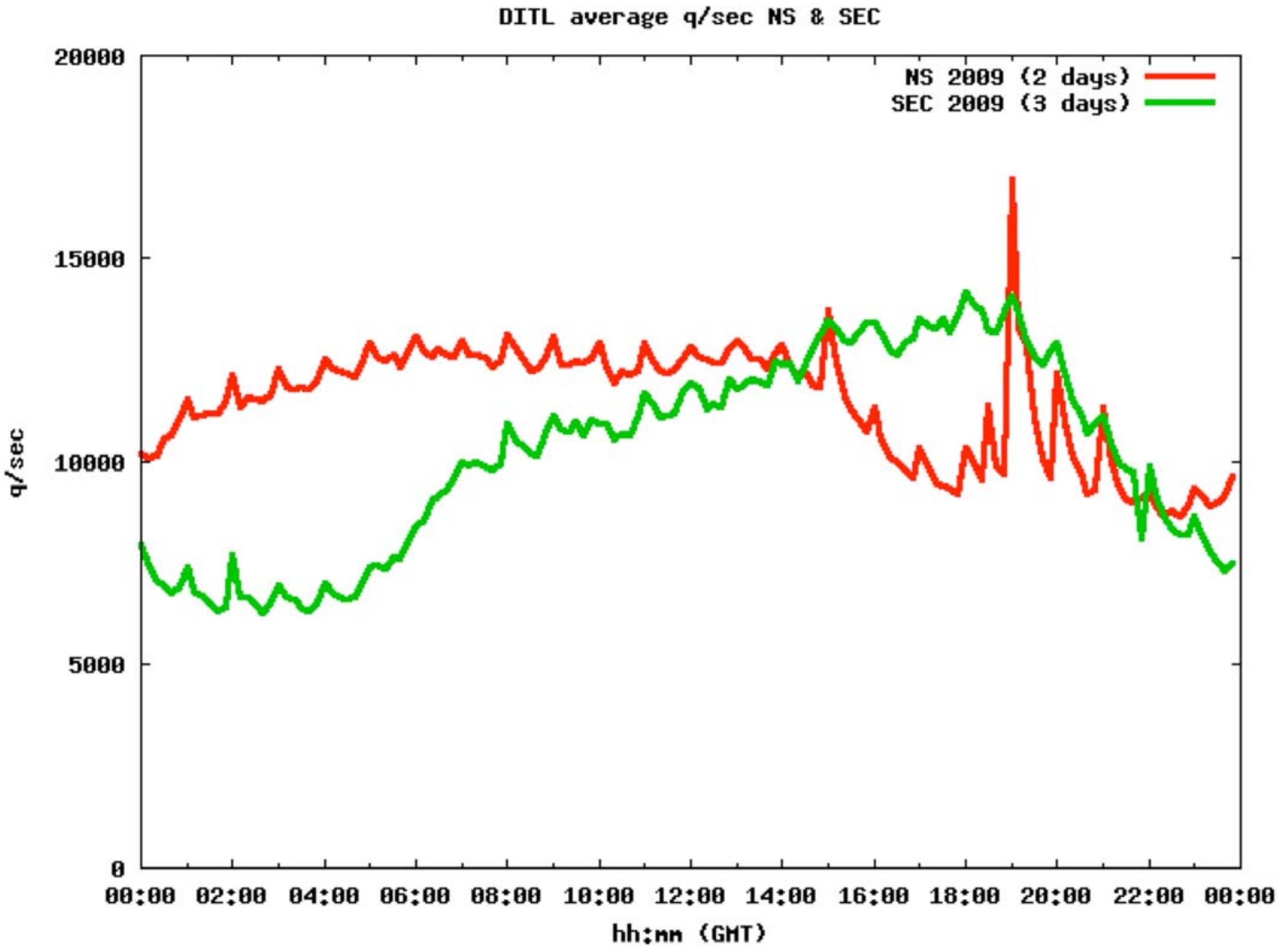
DITL 2008-2009 rest of the world



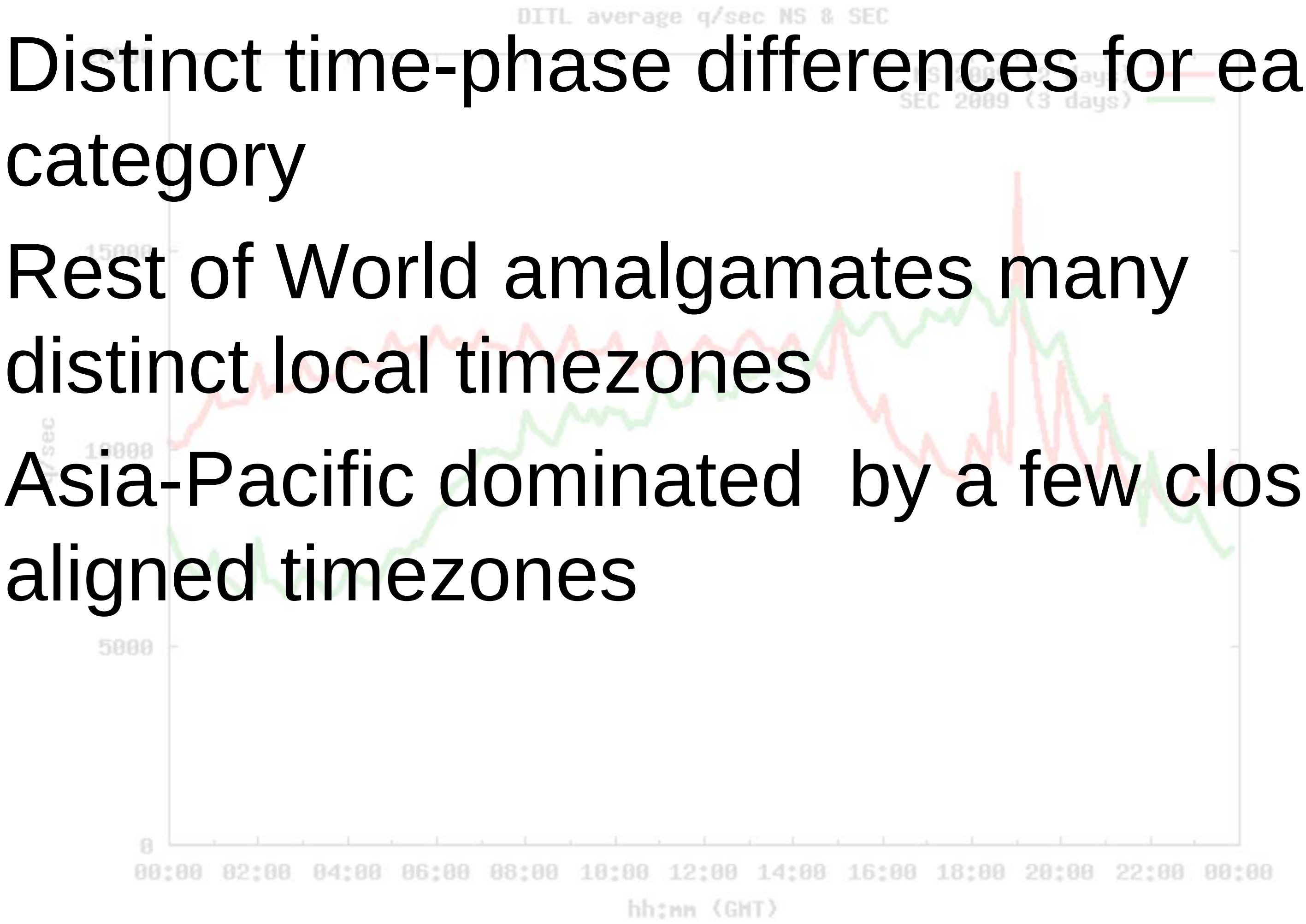
- Consistent behavior visible
  - – But different to Asia-Pacific NS
  - – JP ‘spike’ not visible year on year
- Also consistent growth in traffic
  - – 15%-20% bigger than Asia-Pacific NS

APNIC 28 Beijing, China 24-28 August 2009

Asia & Rest of World Time shift



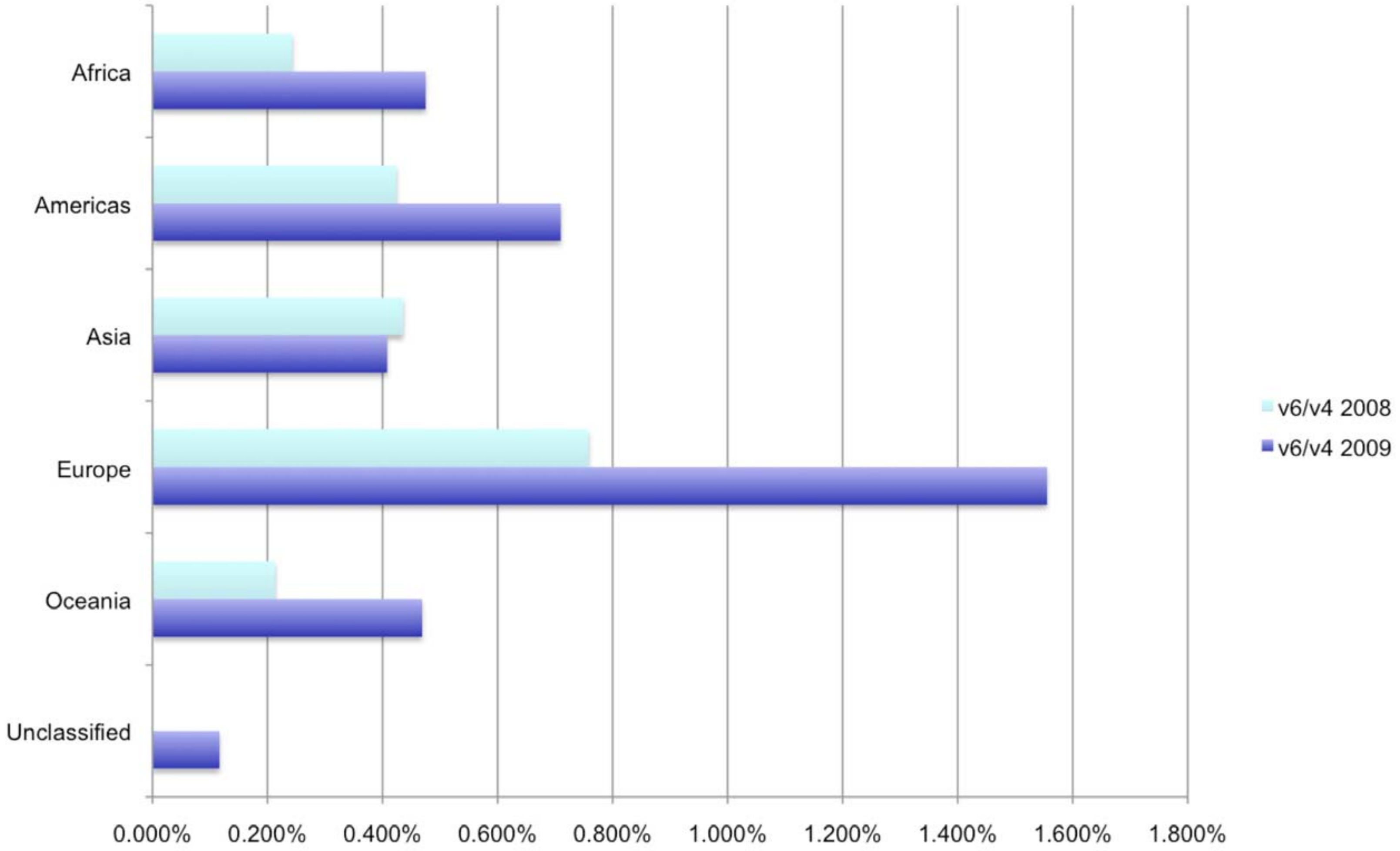
Asia & Rest of World
Time shift



- 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

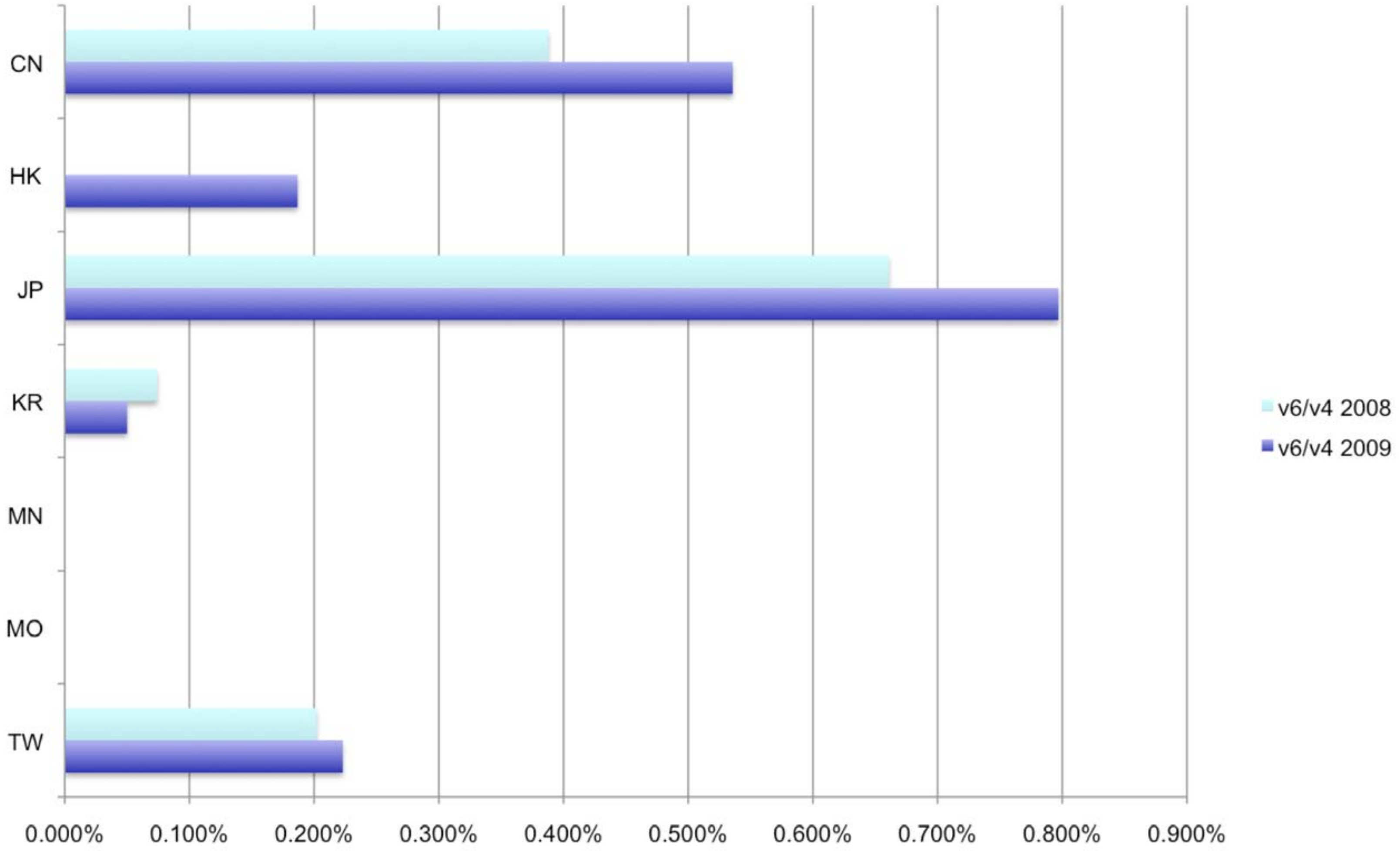
UN Regions v6/v4 usage



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%

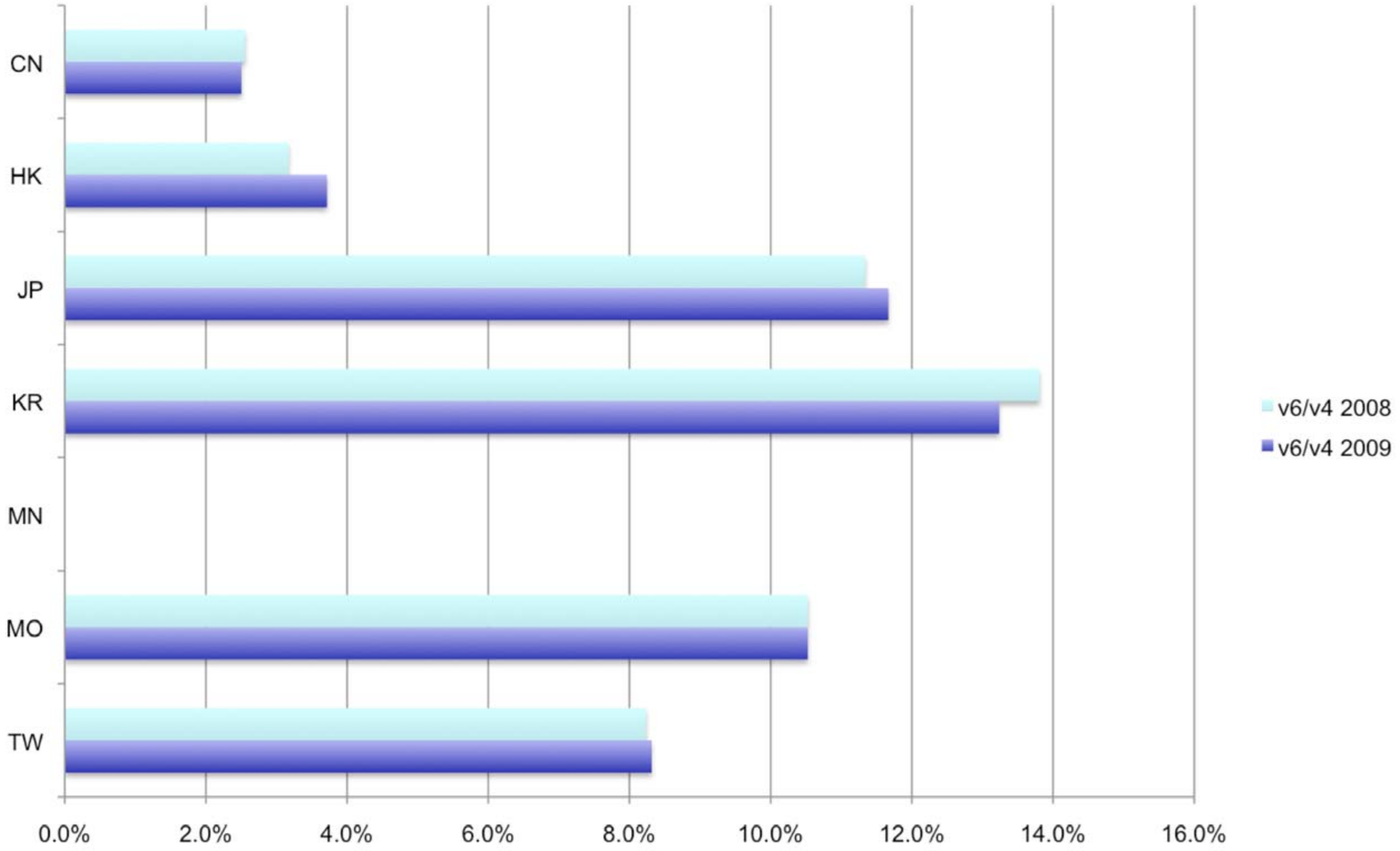
East Asia V6/V4 usage



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

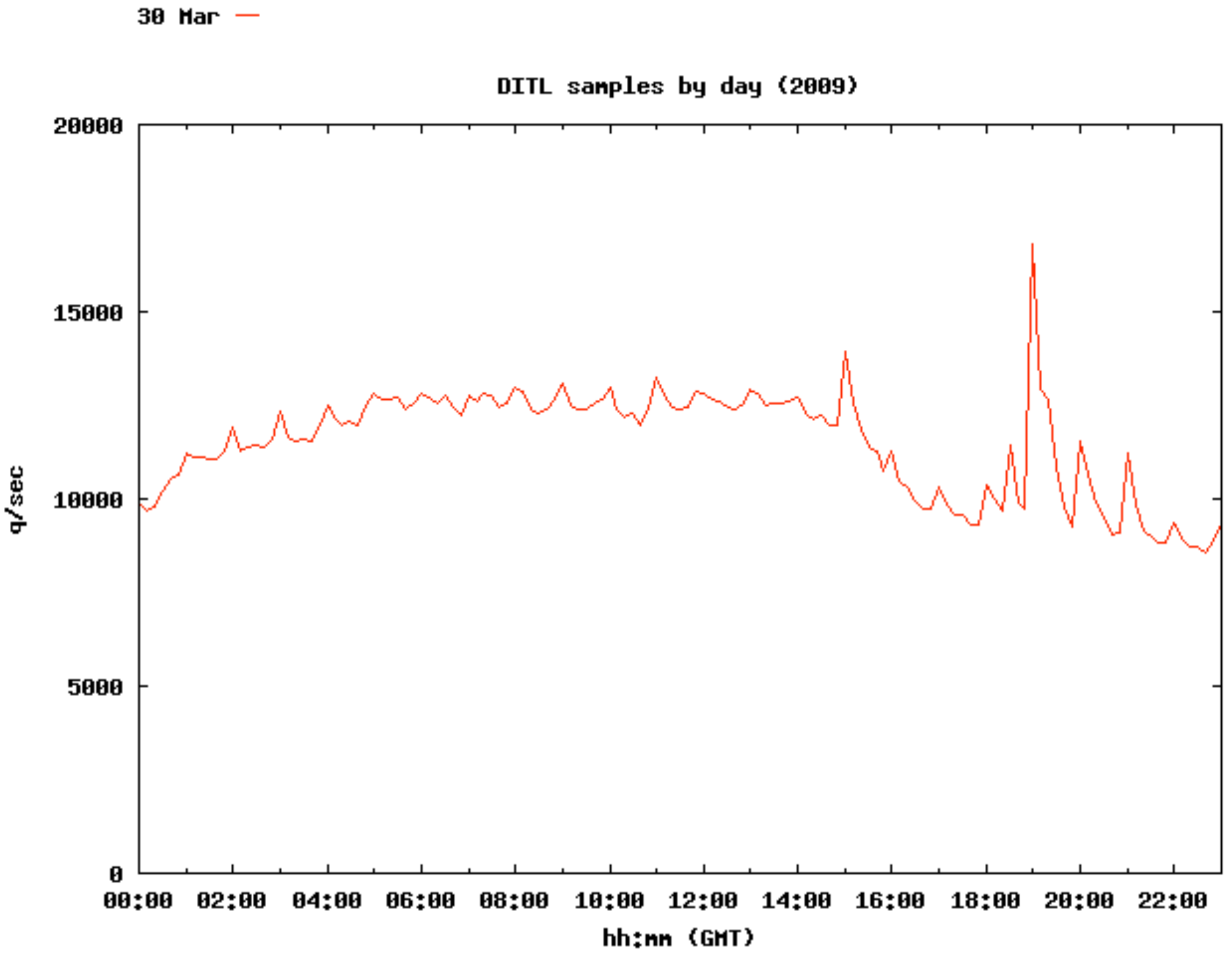


East Asia assignment obs.

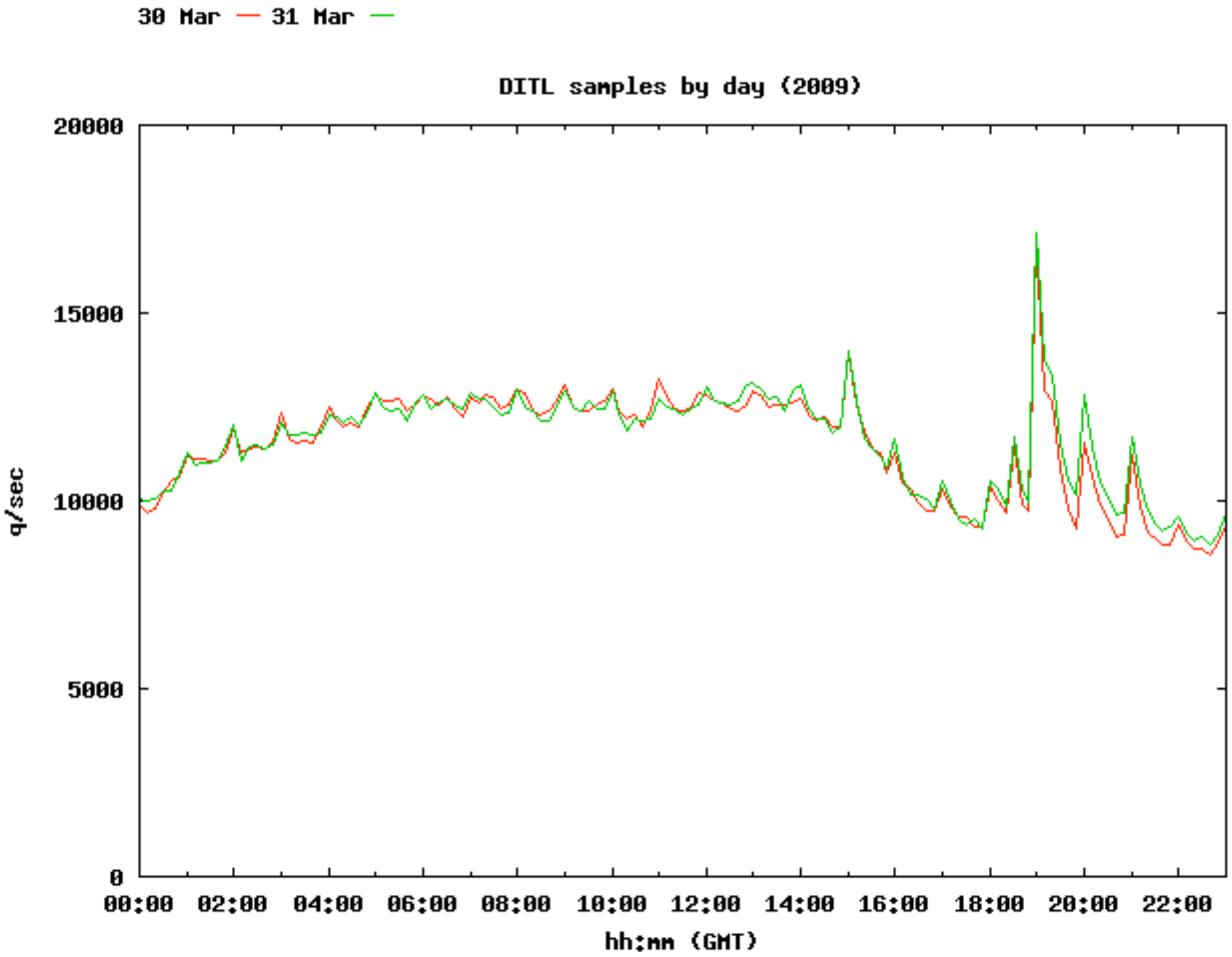
- Assignment counts for East Asia do not correlate with observed address use in DNS
- V6/V4 ratios in assignment counts do not correlate with observed V6/V4 usage
  - Higher ratios of V6 assigned than seen in use
  - No relationship per-economy

How the data was processed

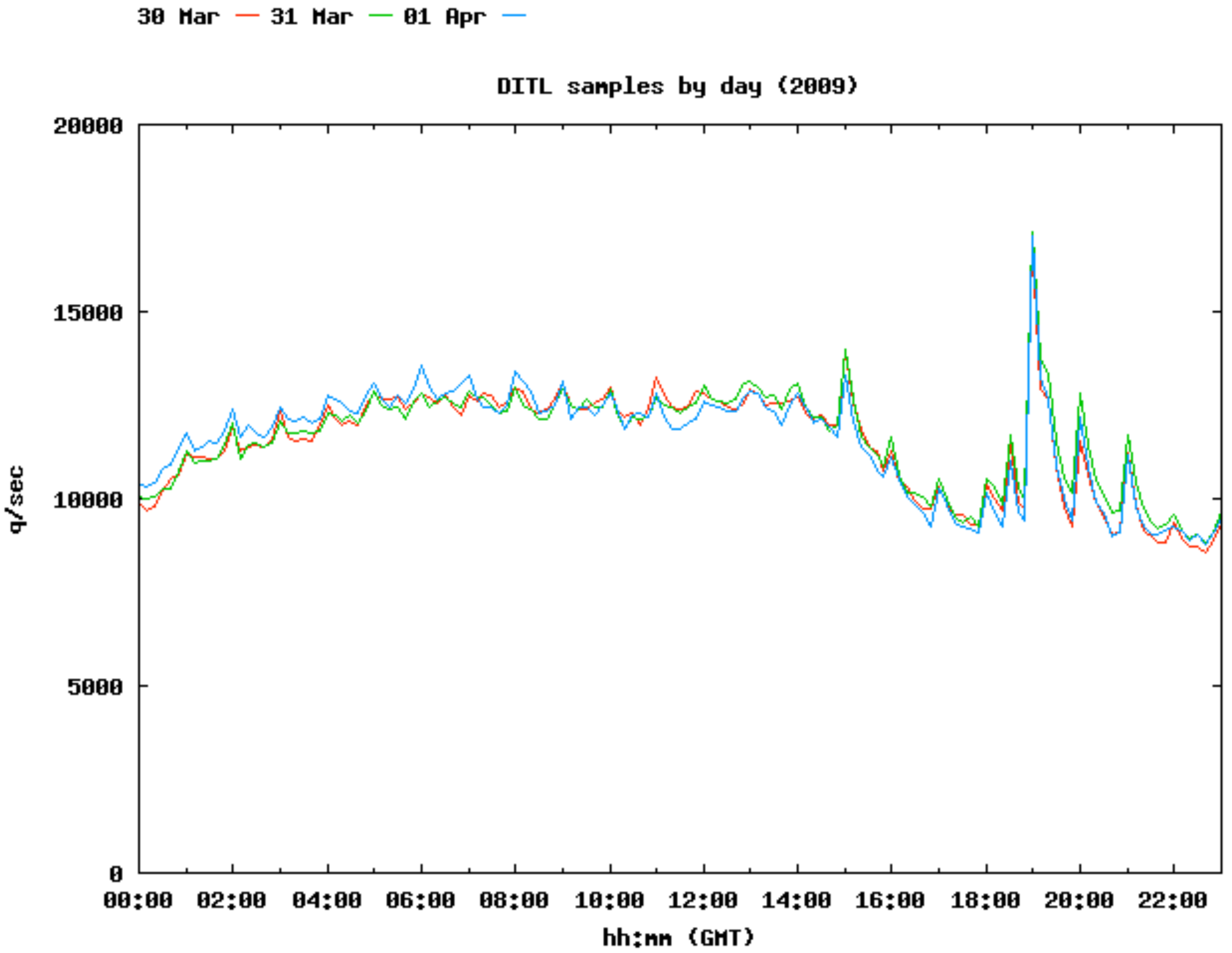
Day Samples


30 Mar
DITL samples by day (2009)
20000
15000
10000
5000
0
q/sec
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
hh:mm (GMT)

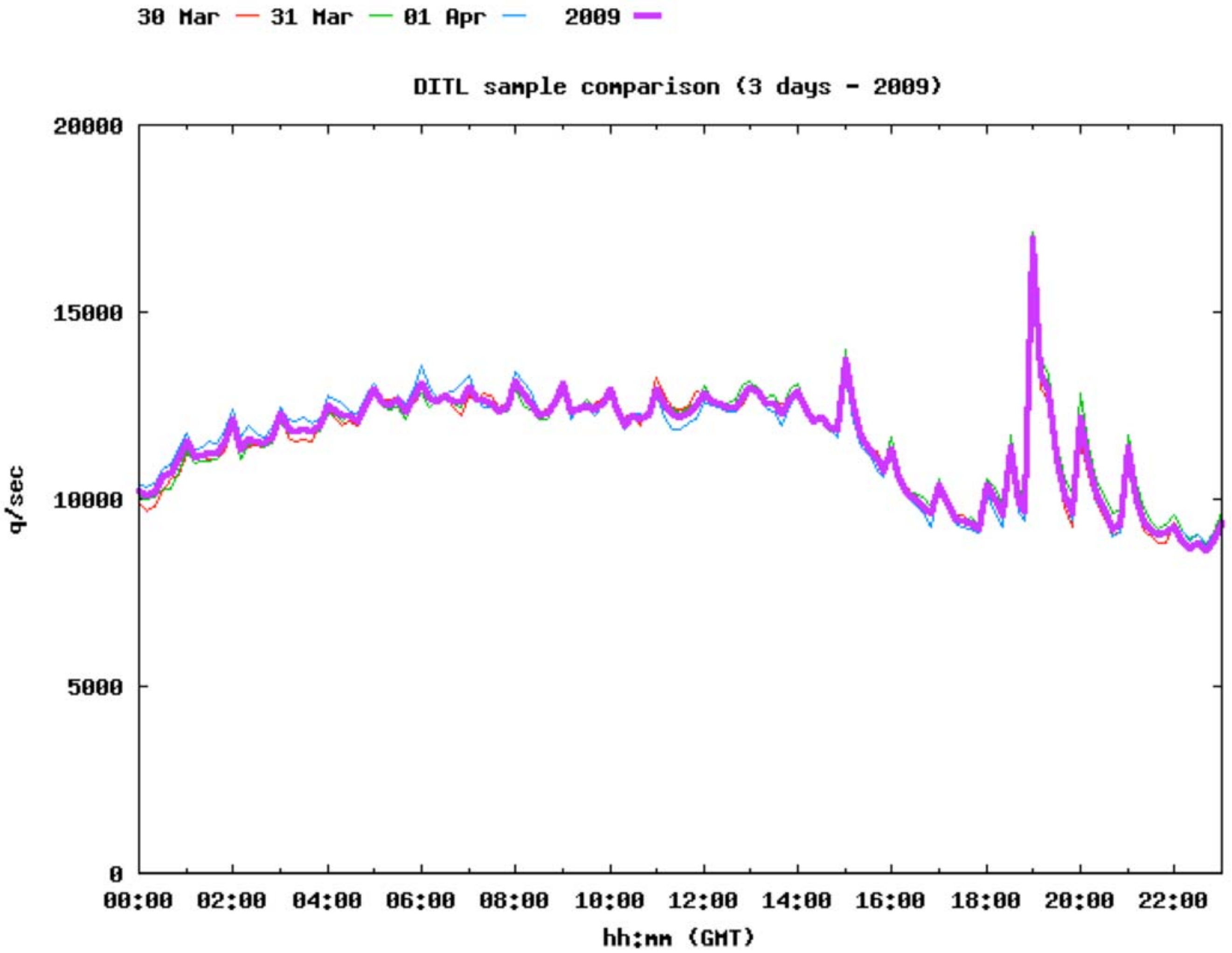
Day Samples line up



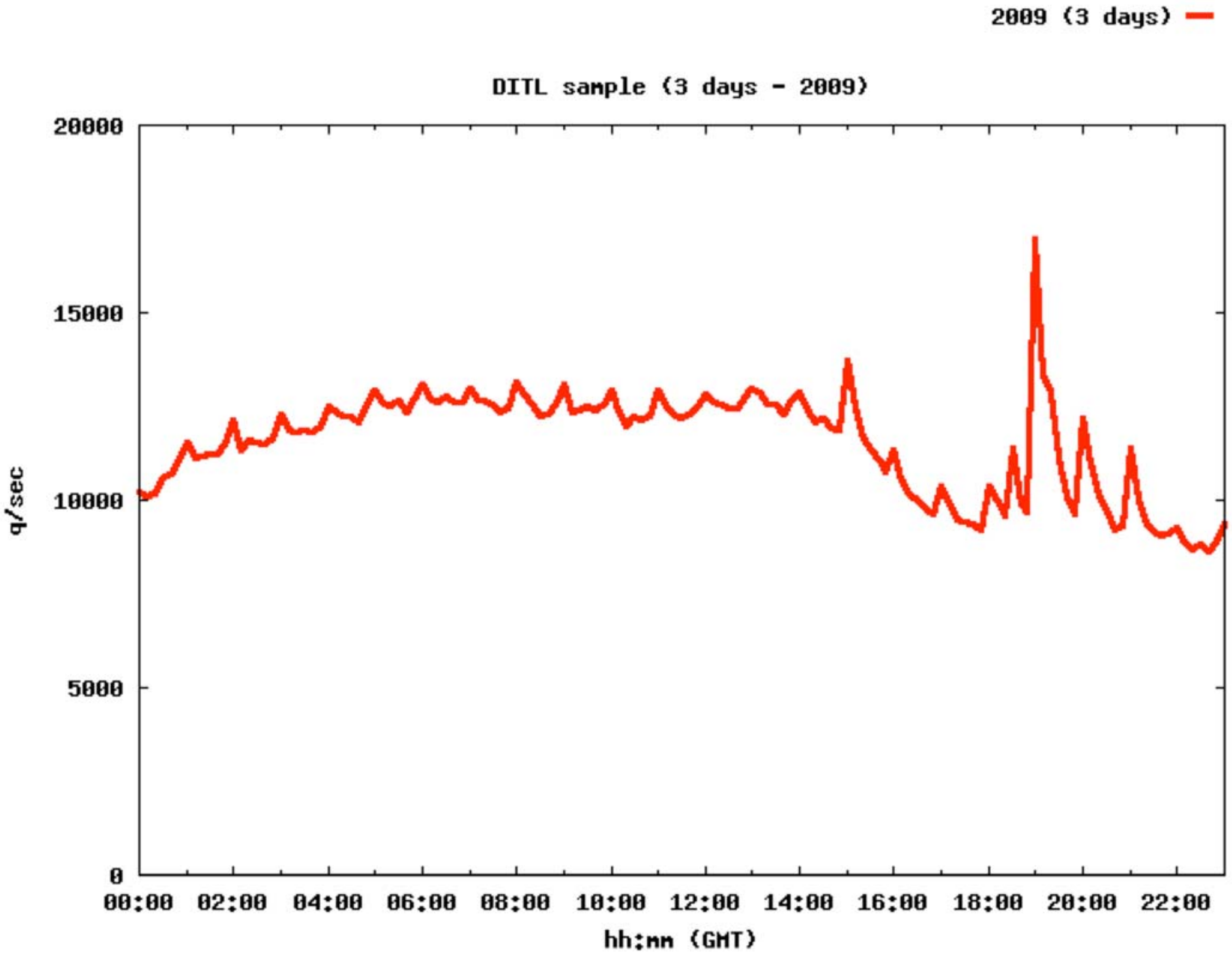
Day Samples line up strongly!



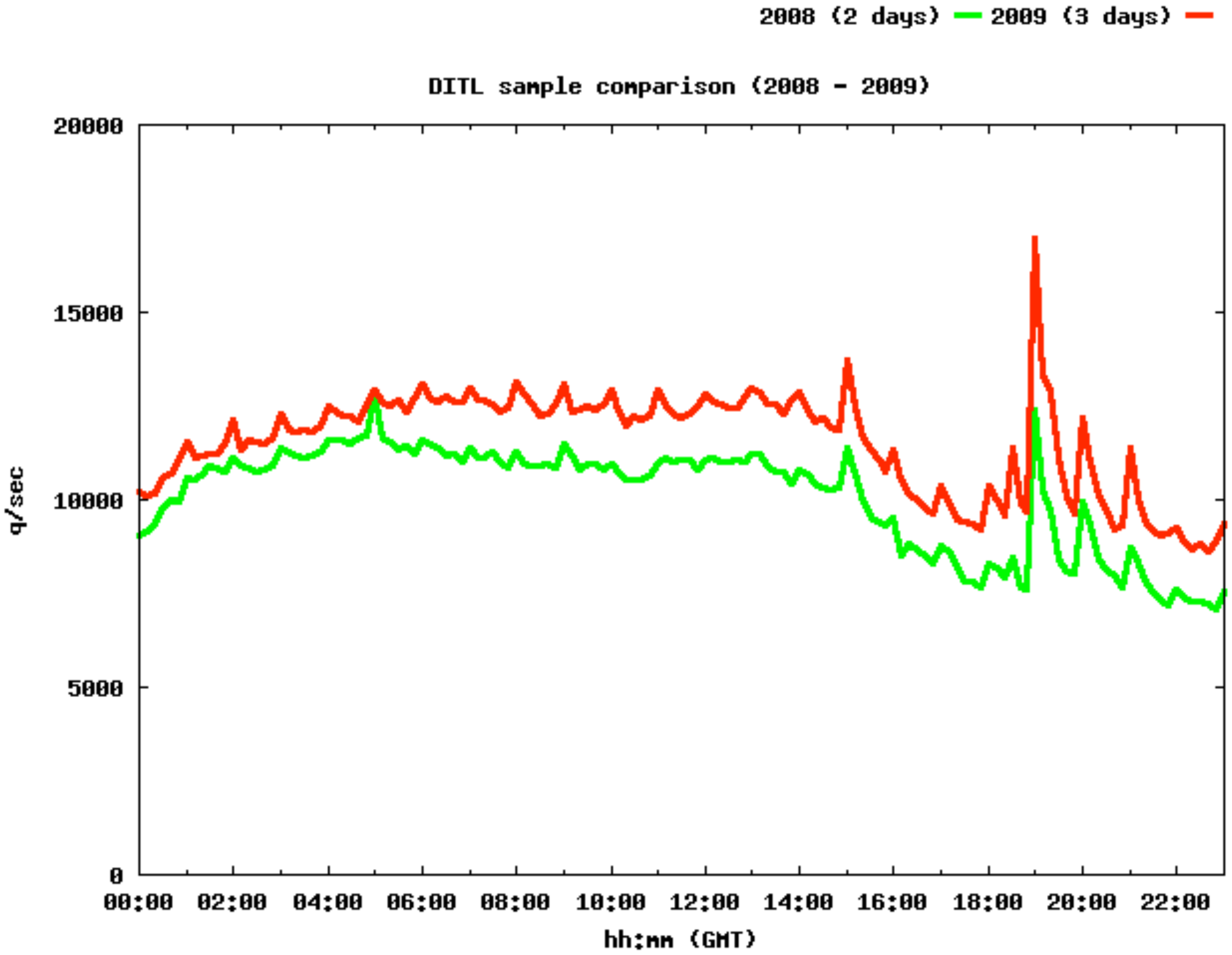
Average shows core 'shape'



Averages can be compared



Result: year-on-year trends



DITL 2010

- 2 points make a line
  - – 3 data series makes a trend!
    - V4/V6 relativities could aide EU V6 measurement activity
    - DITL data informs our input to OECD, wider community.
- Re-use existing infrastructure
  - – Possibly needs re-investment for DITL2011
- APNIC deploying DNSSEC & Anycast 2010
  - – Monitor change during deployment
  - – Predicting 2x traffic growth from DNSSEC
    - RRSIG/NSEC costs, 40% NXDOMAIN response rate

Thank You!

Questions?