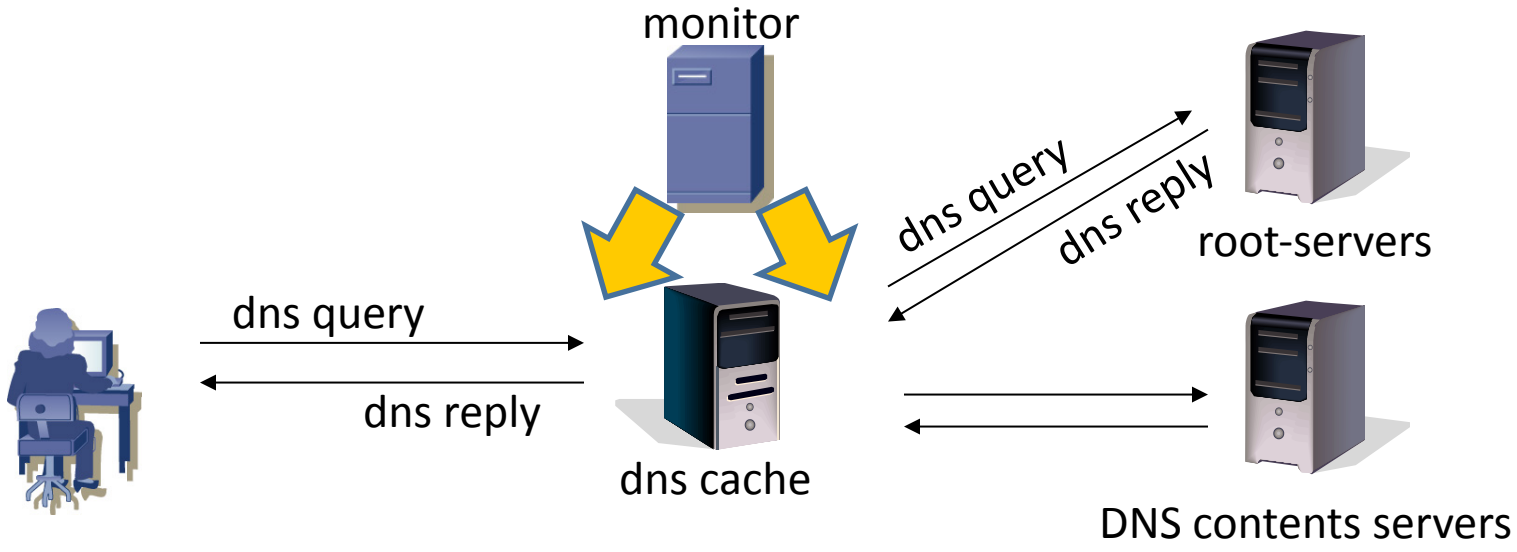
DNS cache stat

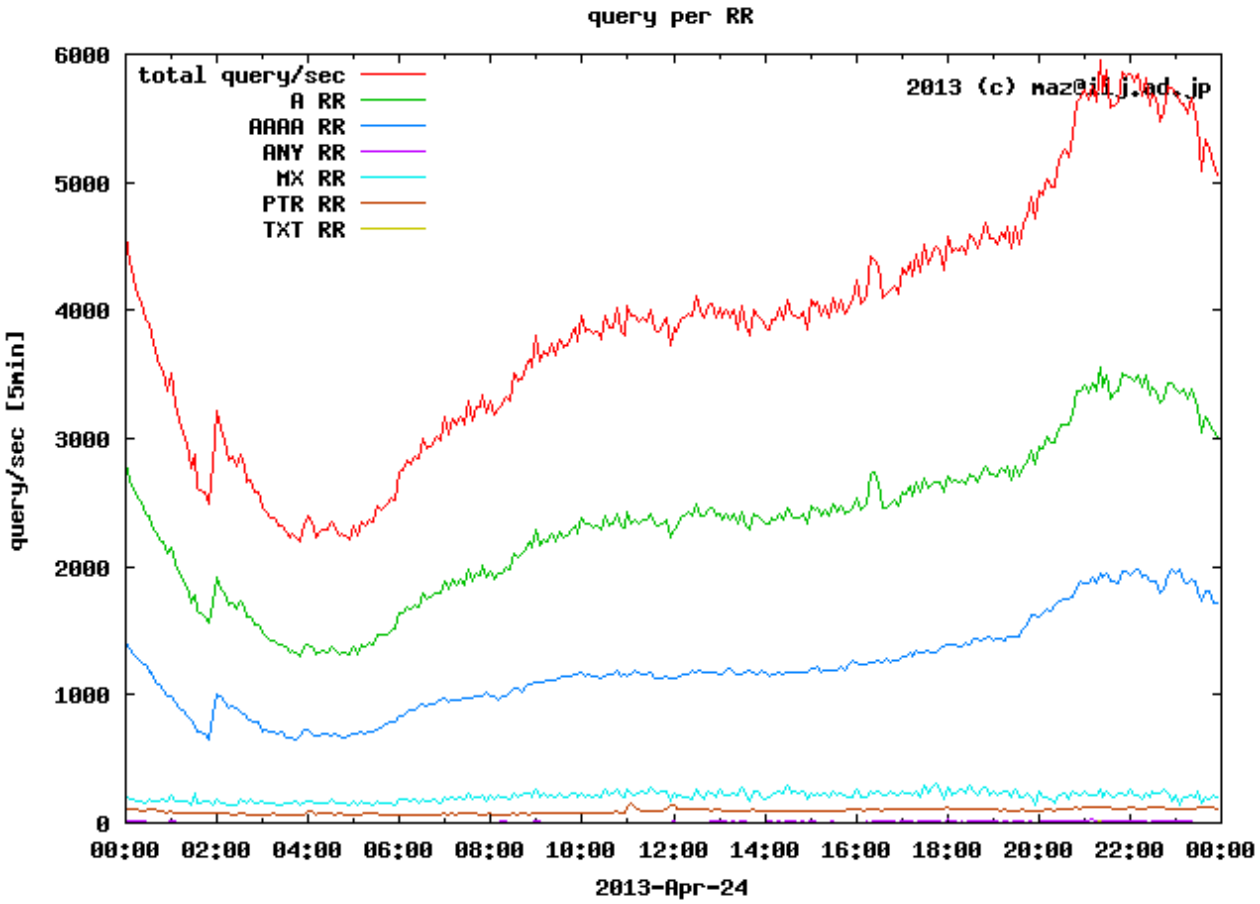
Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

DNS passive monitoring

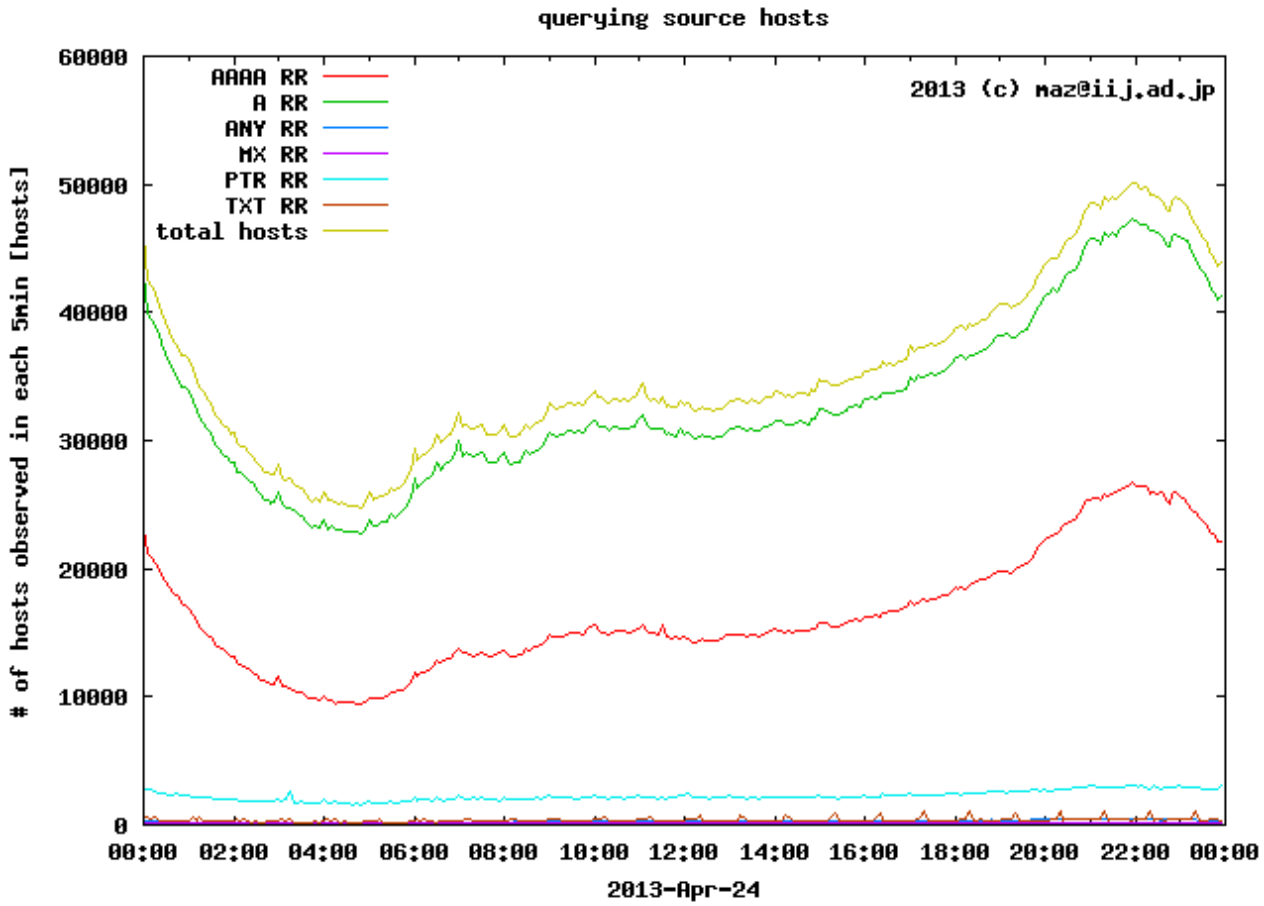
- at a dns cache server for consumer



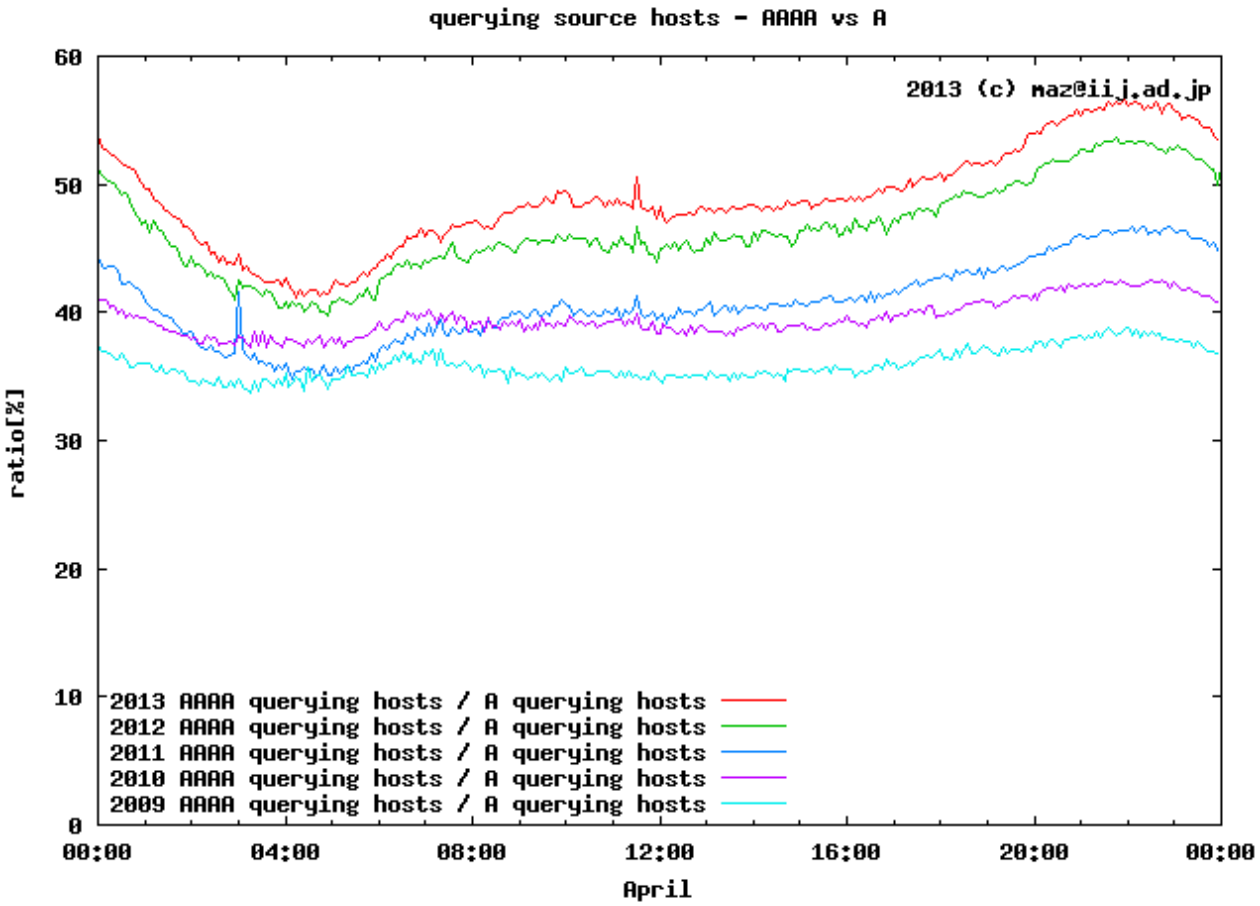
distribution of Resource Record



distribution per querying host



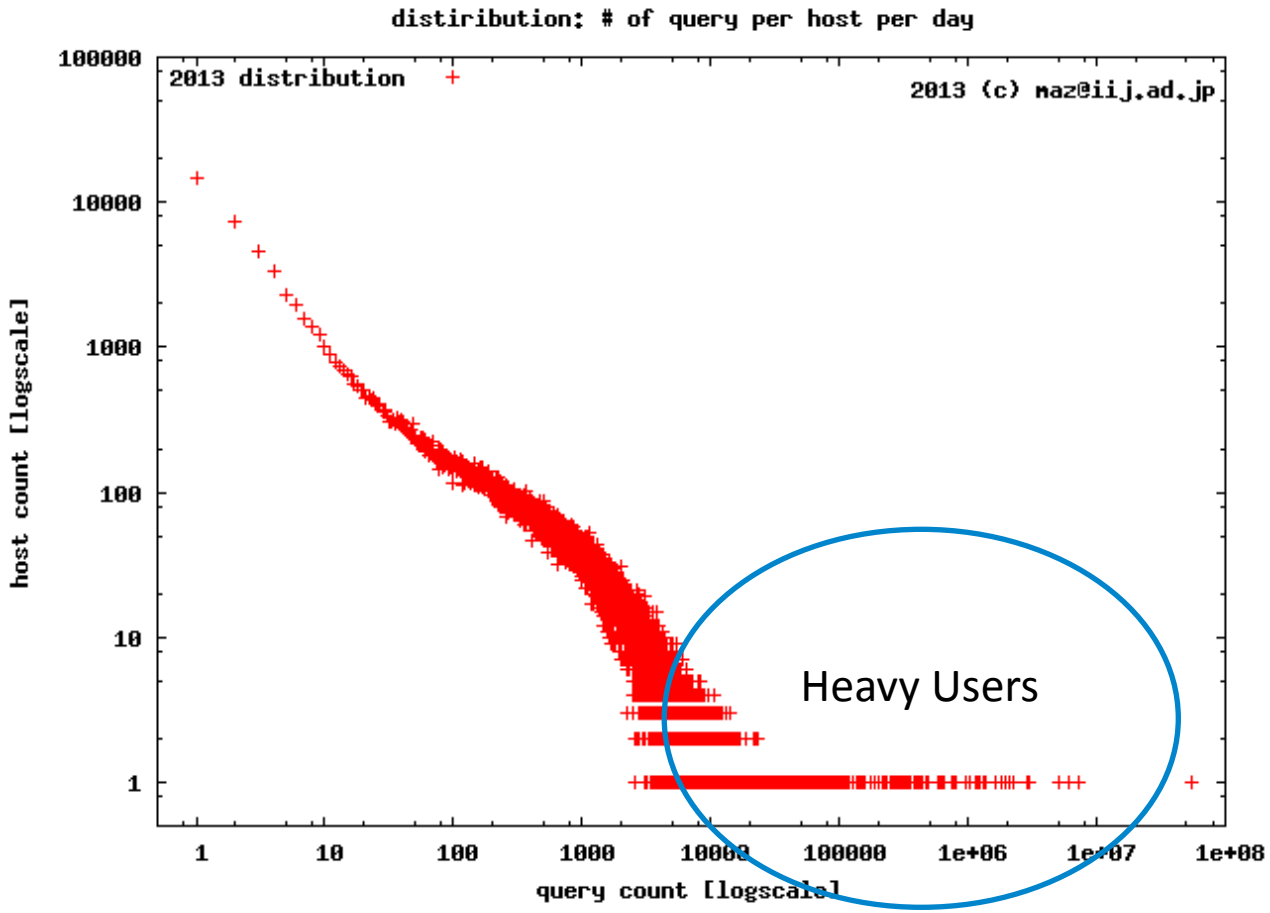
AAAA vs A


querying source hosts - AAAA vs A
2013 (c) maz@iij.ad.jp
ratio[%]
60
50
40
30
20
10
0
2013 AAAA querying hosts / A querying hosts
2012 AAAA querying hosts / A querying hosts
2011 AAAA querying hosts / A querying hosts
2010 AAAA querying hosts / A querying hosts
2009 AAAA querying hosts / A querying hosts
00:00
04:00
08:00
12:00
16:00
20:00
00:00
April

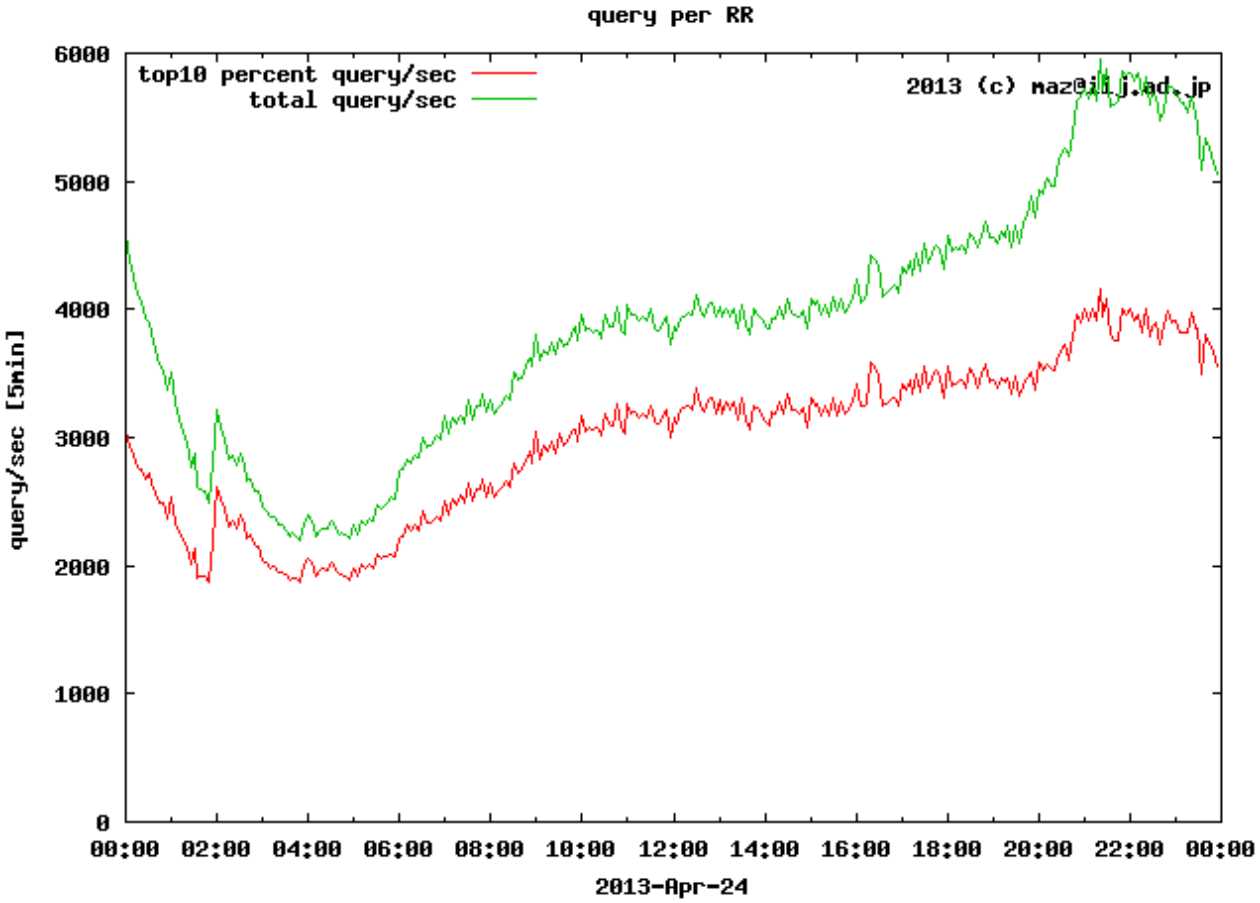
End Users' Devices

- more IPv6 capable devices
  - about 56% users also send AAAA query
  - +3 point growth since last year
- peak time at night (21:00-22:00)
  - more IPv6 capable devices at home
    - windows/mac/smart phones

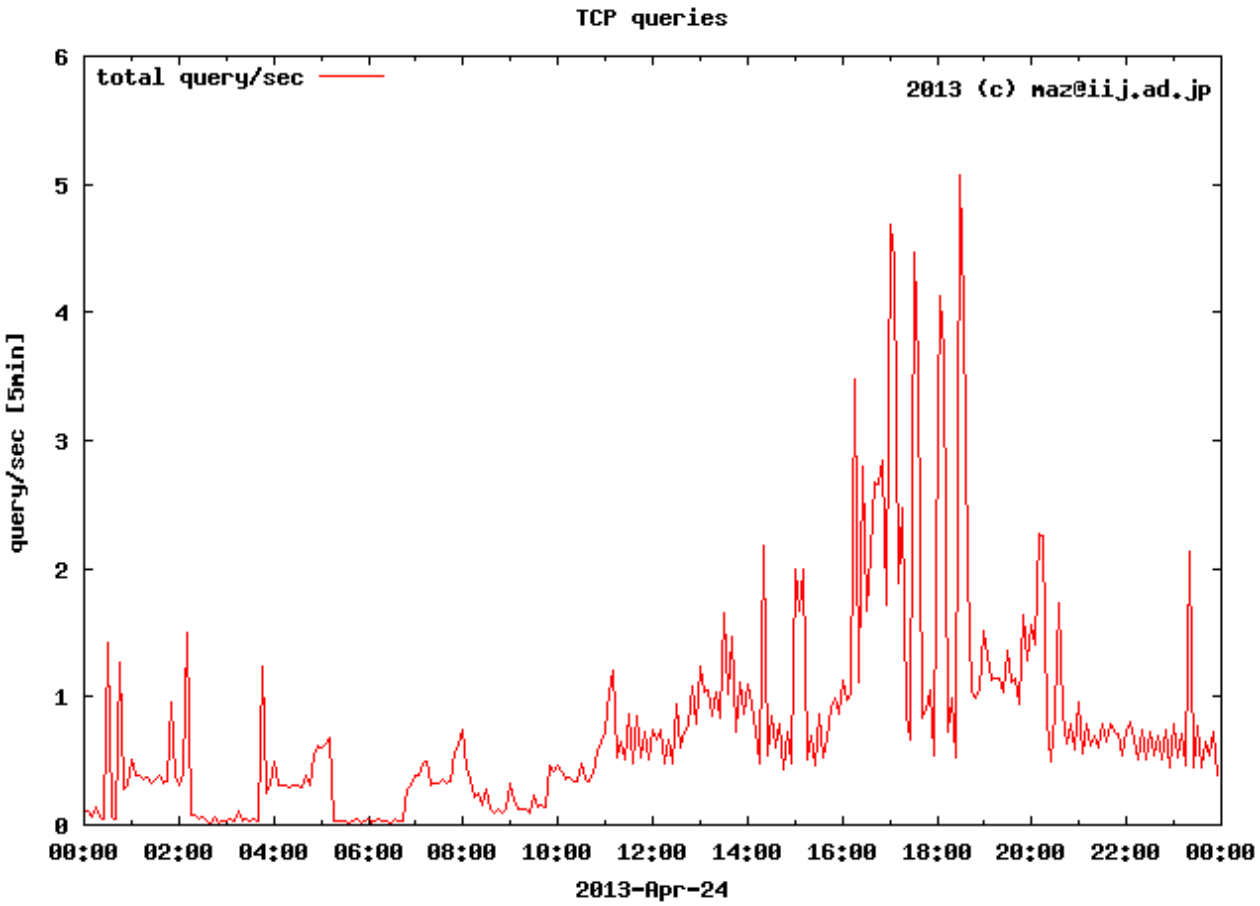
DNS and power law



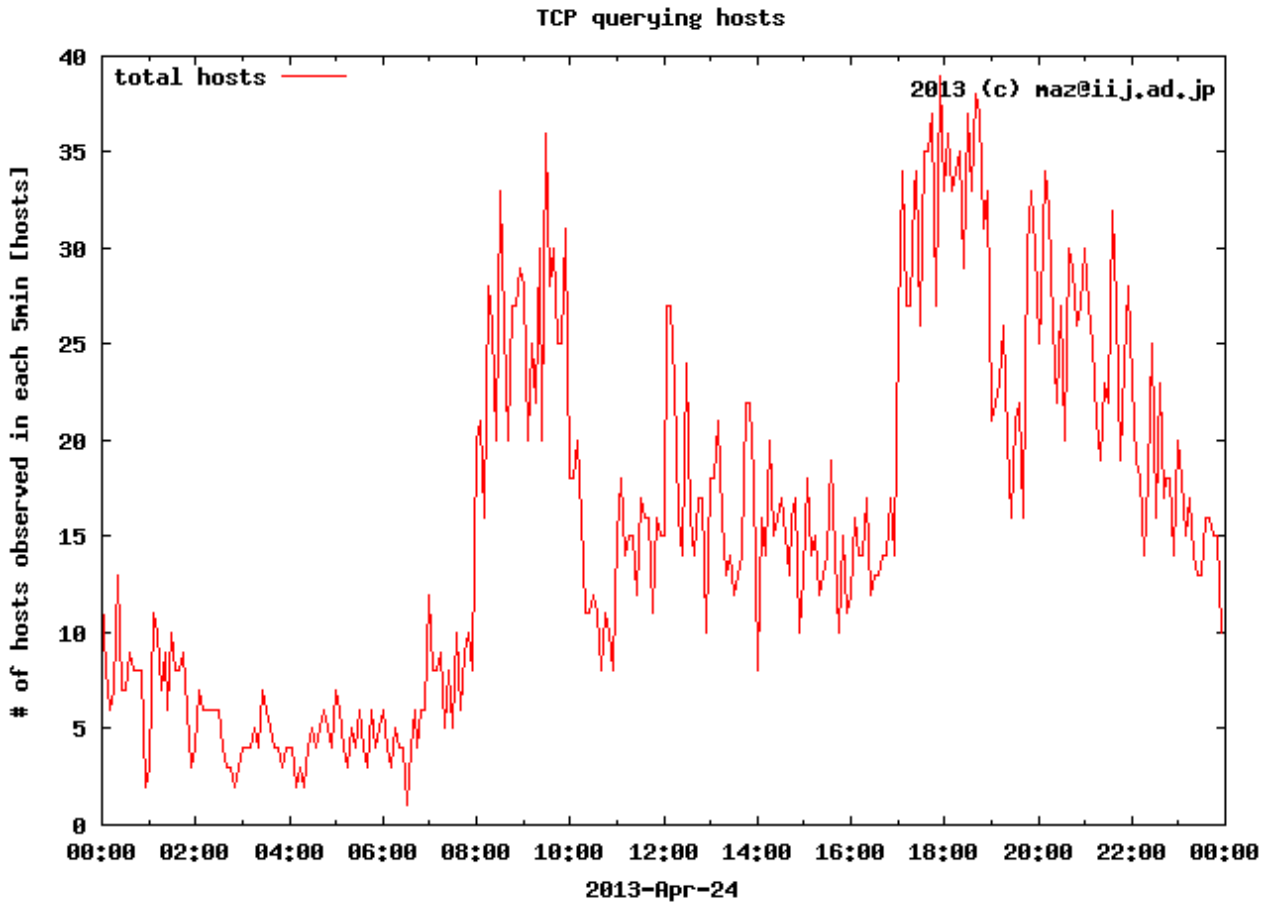
top 10% users produce 60-70% queries



TCP query


TCP queries
total query/sec
2013 (c) maz@iij.ad.jp
query/sec [5min]
0
1
2
3
4
5
6
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
2013-Apr-24

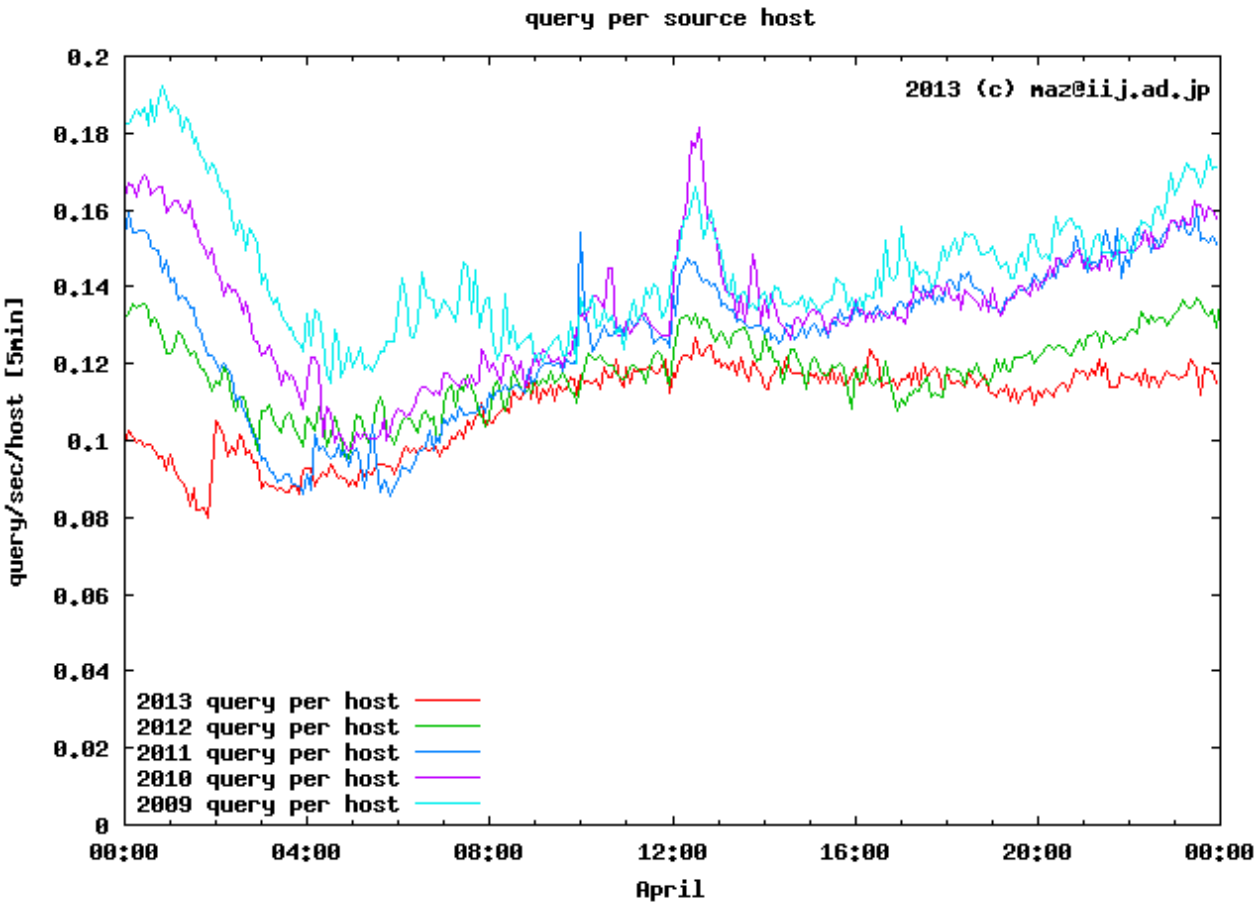
TCP querying hosts



TCP query

- more than 512 byte
  - e-mail distribution services
    - parallelize by many hosts (IP addresses)
  - messaging by DNS
    - version information of pattern files?
- some test?
  - example.com
- unknown implementation
  - always sending query by TCP

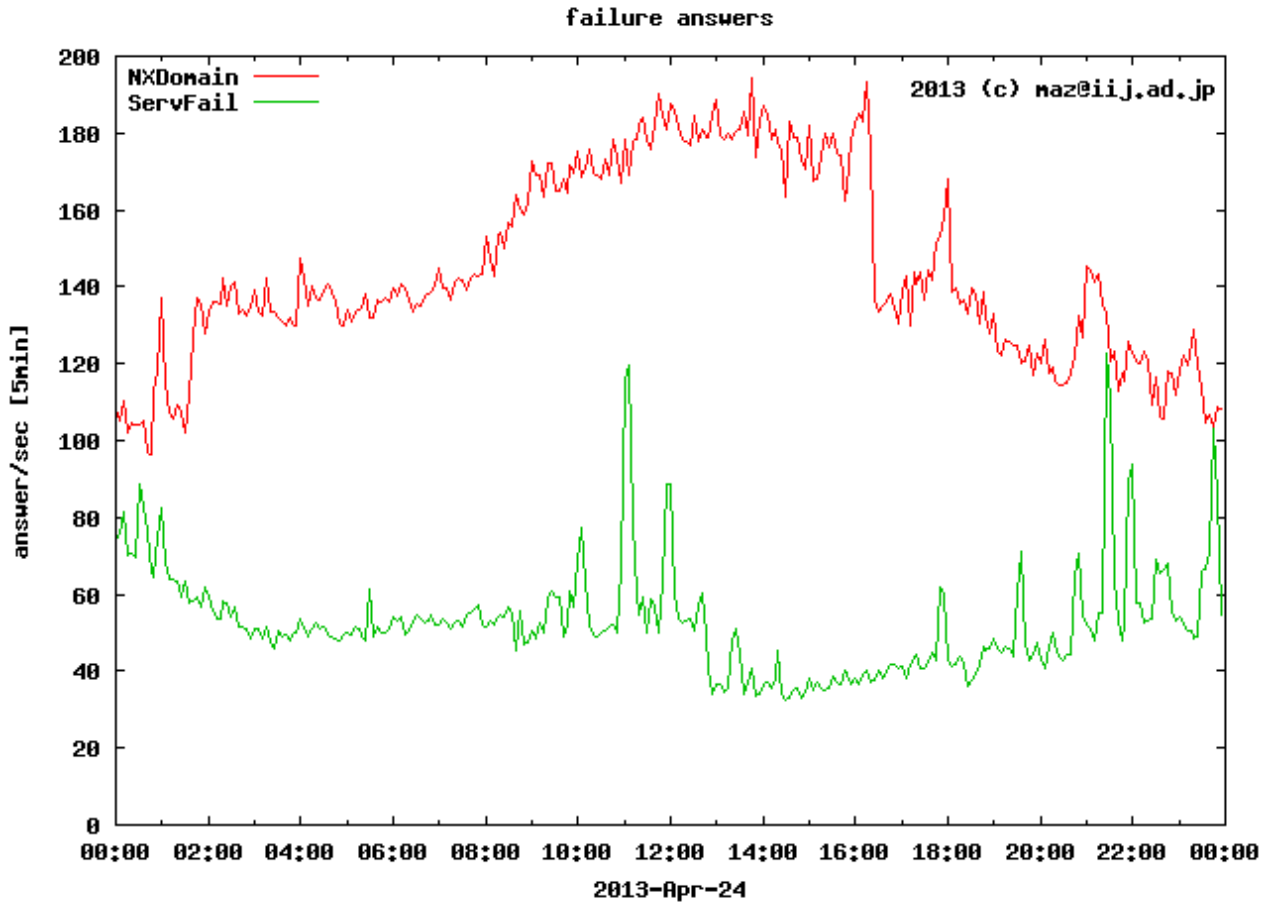
query per host



error trend

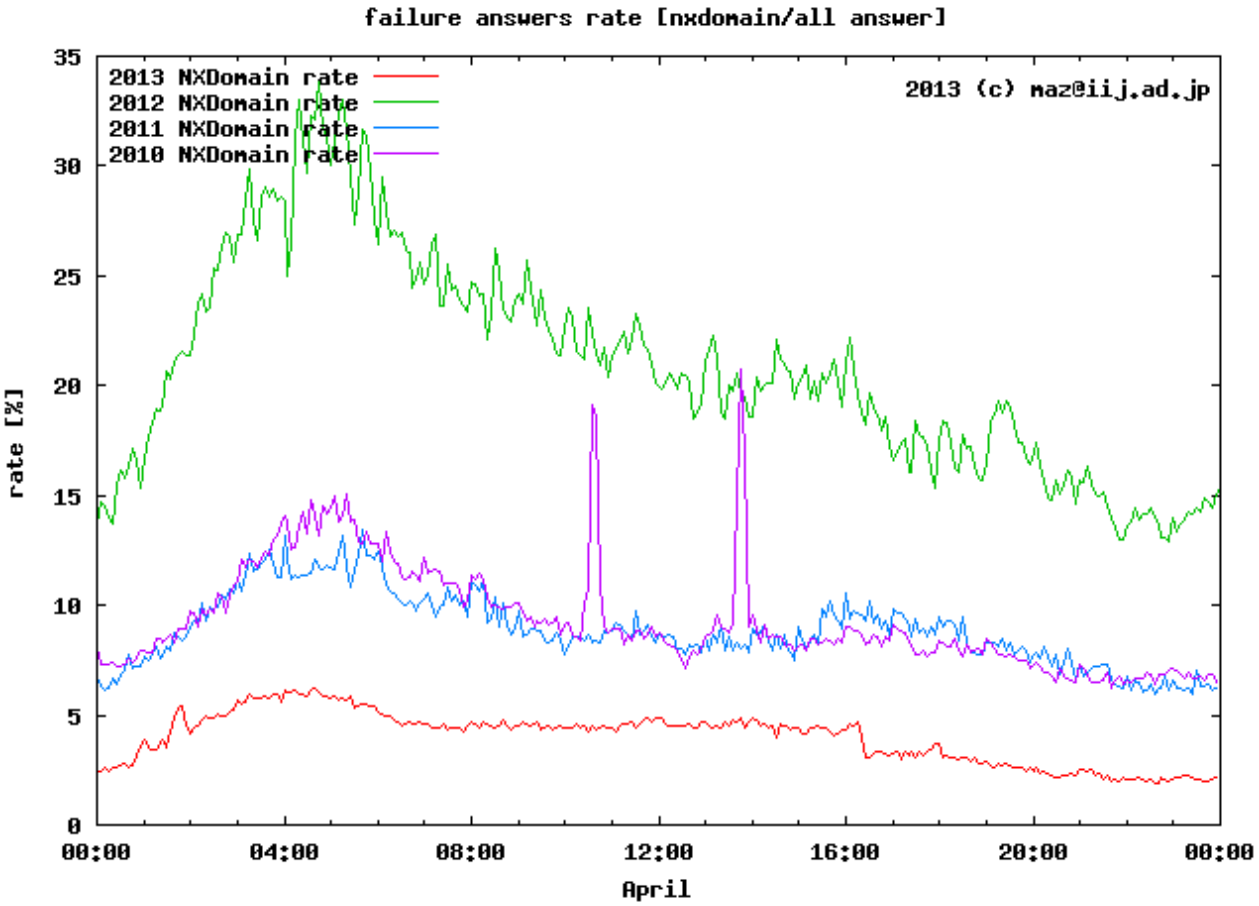
- NXDomain
  - no such record
  - mistype of URL
- ServFail
  - somehow resolution failed
  - configuration error on authoritative DNS servers
  - implementation errors

Error Rate

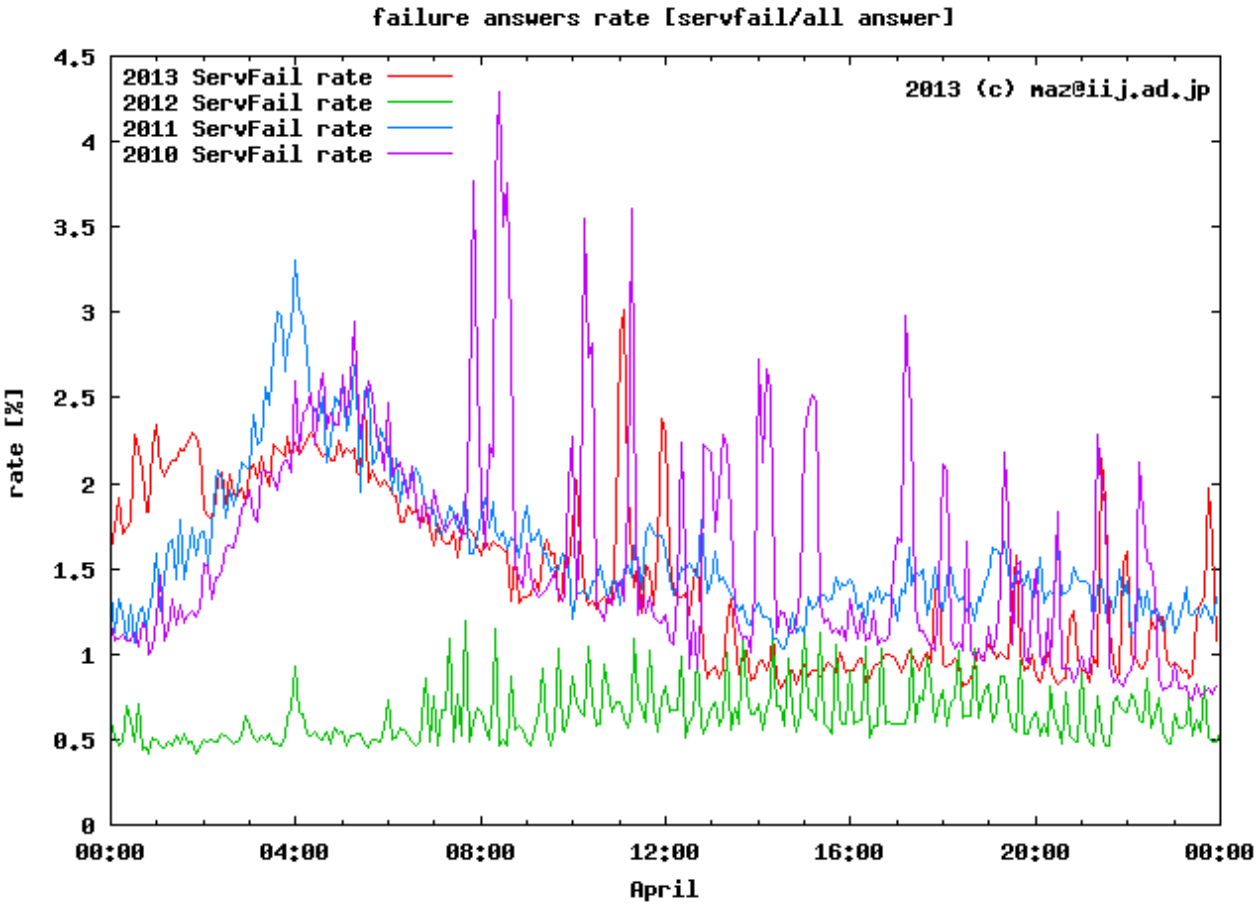

failure answers
NXDomain
ServFail
2013 (c) maz@iij.ad.jp
answer/sec [5min]
200
180
160
140
120
100
80
60
40
20
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
2013-Apr-24

Errors - querying hosts

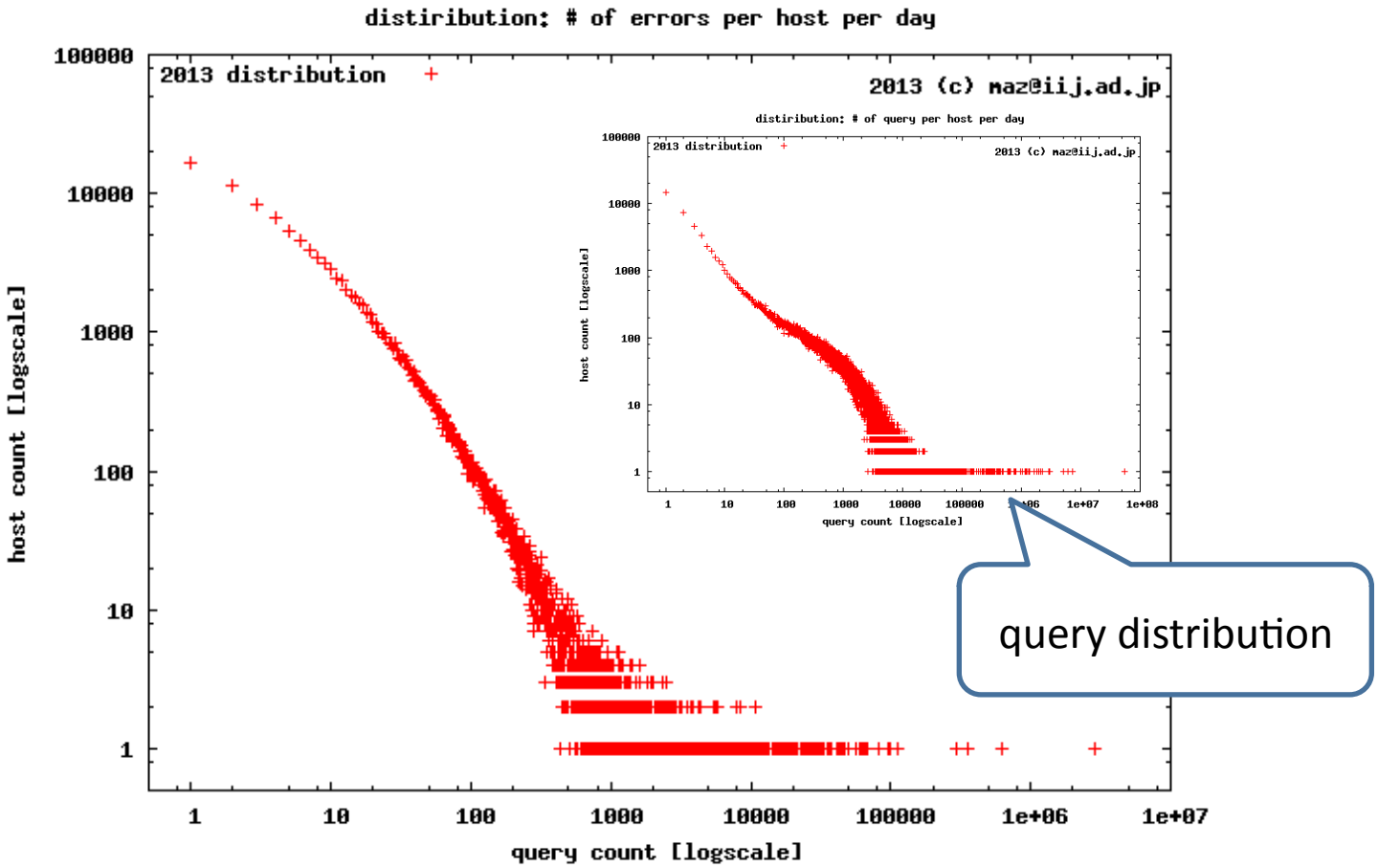
Trend of NXDomain rate



Trend of ServFail rate



Errors and power low



Trend of Erros

- NXDomain
  - the error rate was decreased
  - (some heavy users stopped mis-query)
- ServFail
  - a bit increased

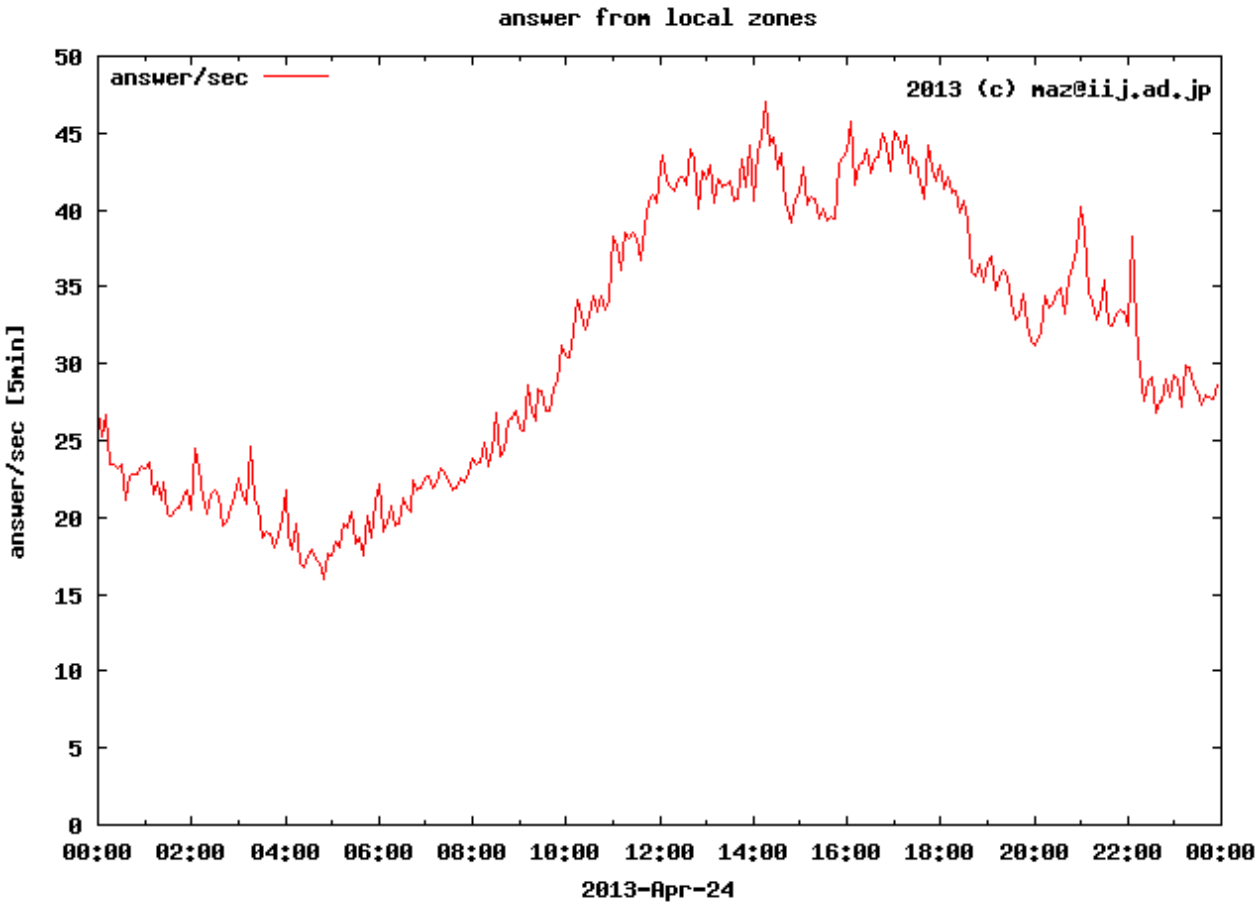
Observed NXDomain

- Private space
  - reverse zone, DNSSD, SOA? local
- Automation tools
  - wpad, VPN services?, a hash of a file?
- Discontinued services
  - DDNS services, SIP proxies
- bugs or mistakes
  - AforA, http, https, ssl

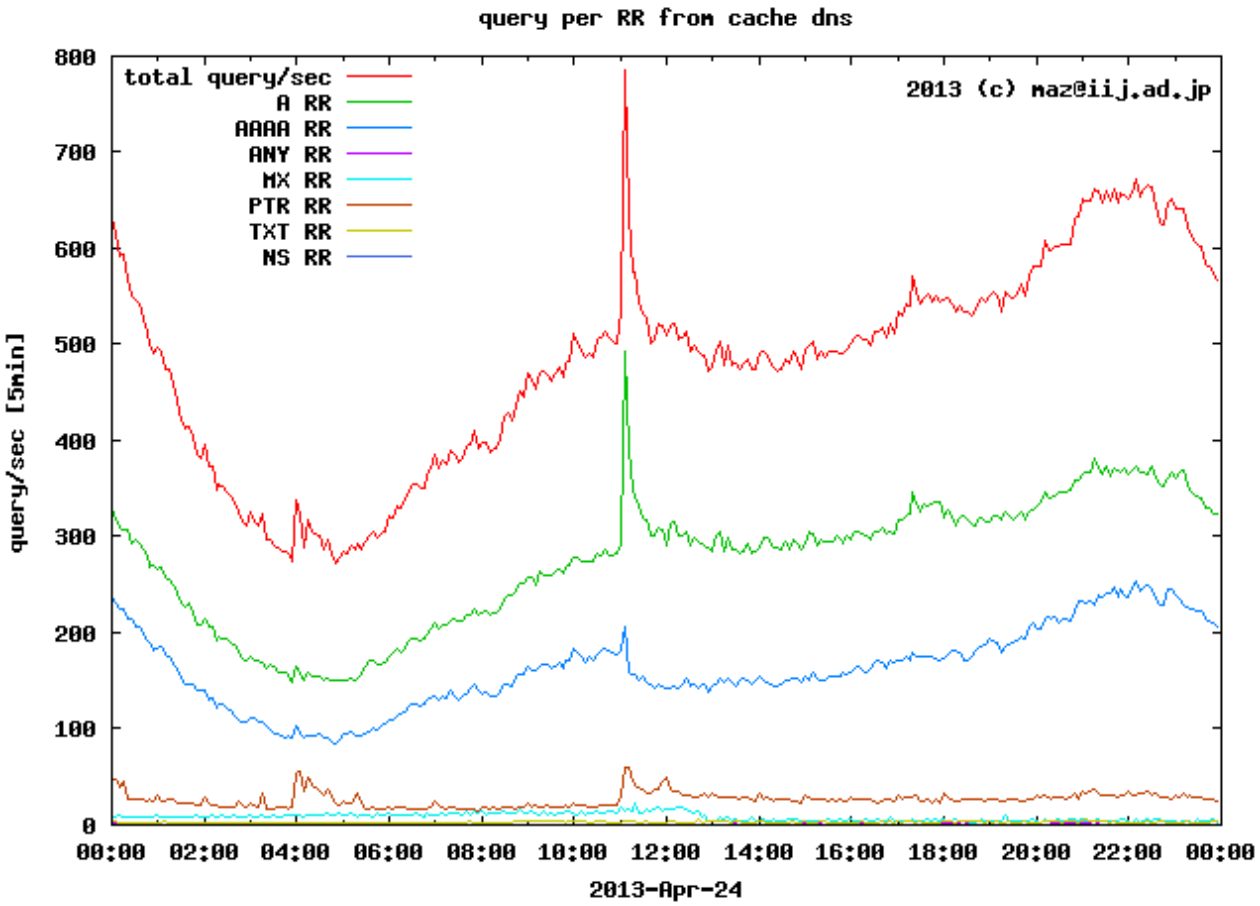
Observed ServFail

- Discontinued services
  - DDNS (lame delegation)
- Load balancers
  - answering ServFail for queries except A query
  - answering improper SOA for queries except A query
    - www.example.jp IN NS loadbalancer.example.jp
      - ‘www’ sub-domain is delegated to a load balancer
    - example.jp IN SOA …
      - If the FQDN exists, but no corresponding Resource Record is found, DNS server replies SOA. But the SOA is improper. ☹

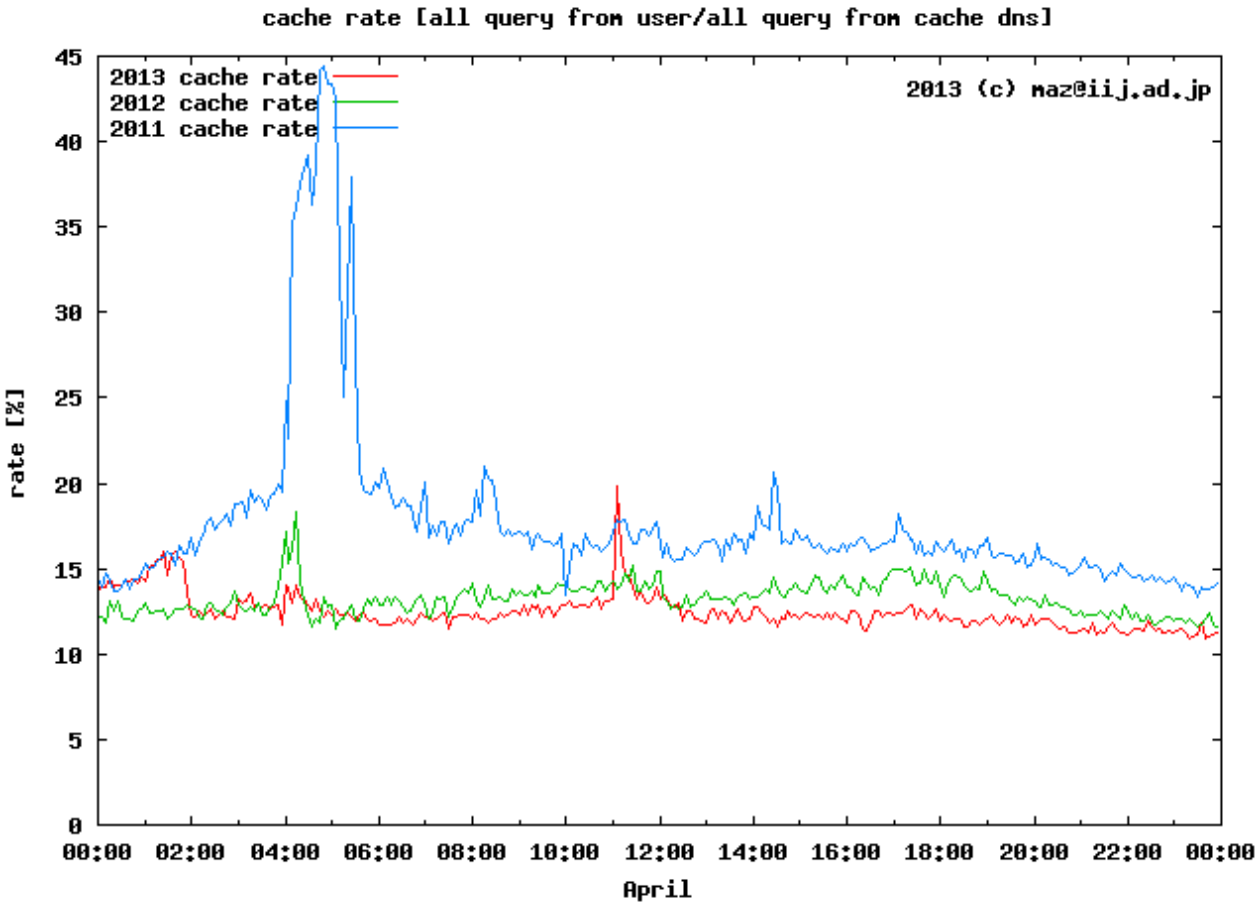
answer from local zones



query from the cache server

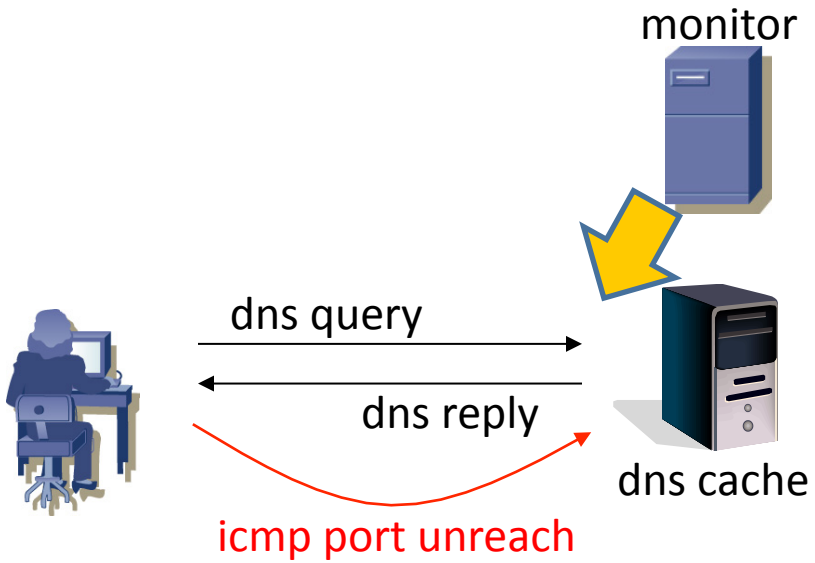


cache rate

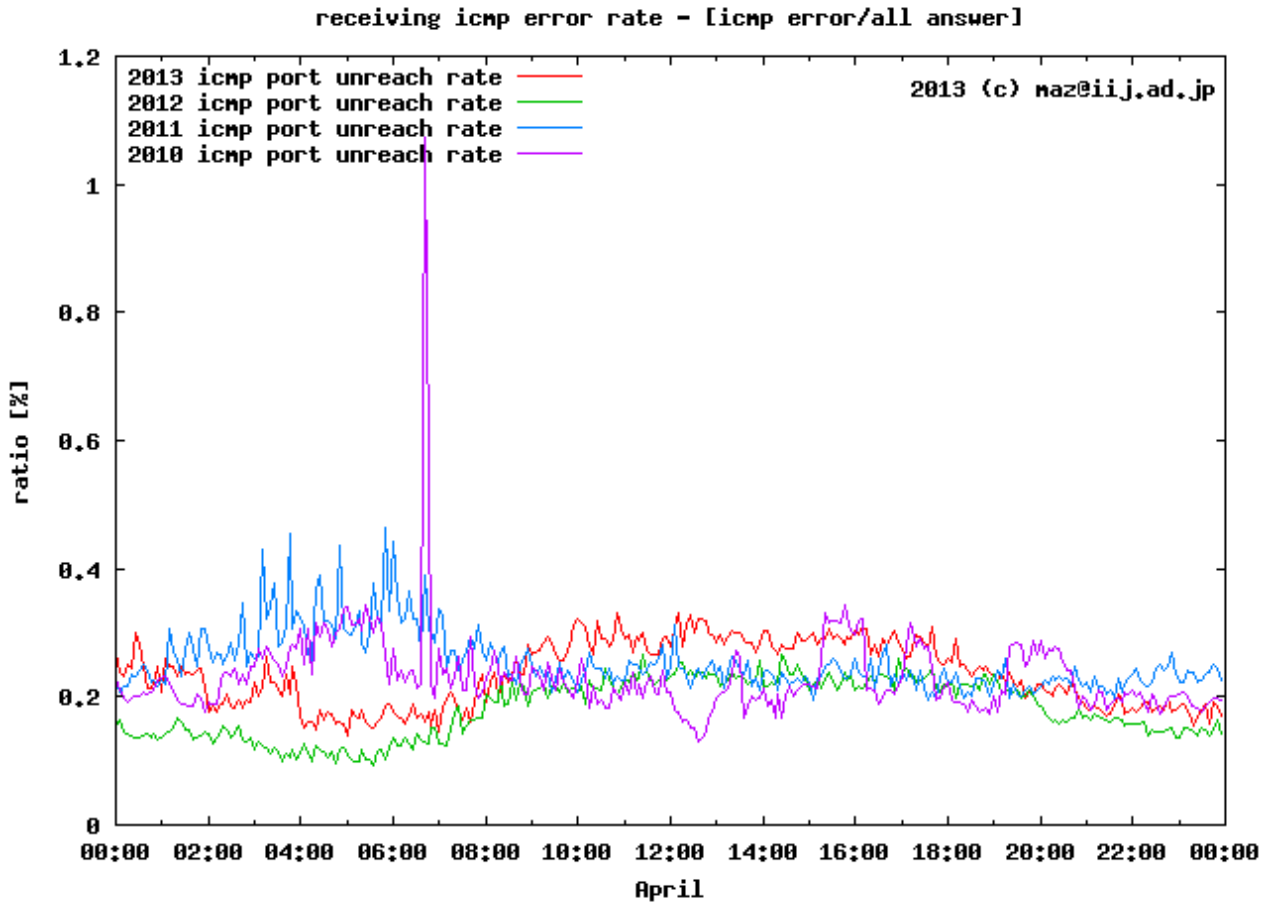

cache rate [all query from user/all query from cache dns]
2013 cache rate
2012 cache rate
2011 cache rate
2013 (c) maz@iij.ad.jp
rate [%]
45
40
35
30
25
20
15
10
5
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
April

other errors

- ICMP error (port unreachable) from users
  - It seems an answer couldn't reach the user



rate of port unreached



summary

- DNS is important in the internet
  - most services rely on DNS
  - it's also important to know the DNS stat
- Heavy users exist
  - as same as traffic trend