NTT

NTT Information Sharing Platform Laboratories

DNS Query Sent by Heavy Users and DNS Prefetch Effect

Kazumichi Sato, Keisuke Ishibashi, and Haruhiko Nishida (NTT Laboratories)

Kota Hashimoto (NTT Comunications)

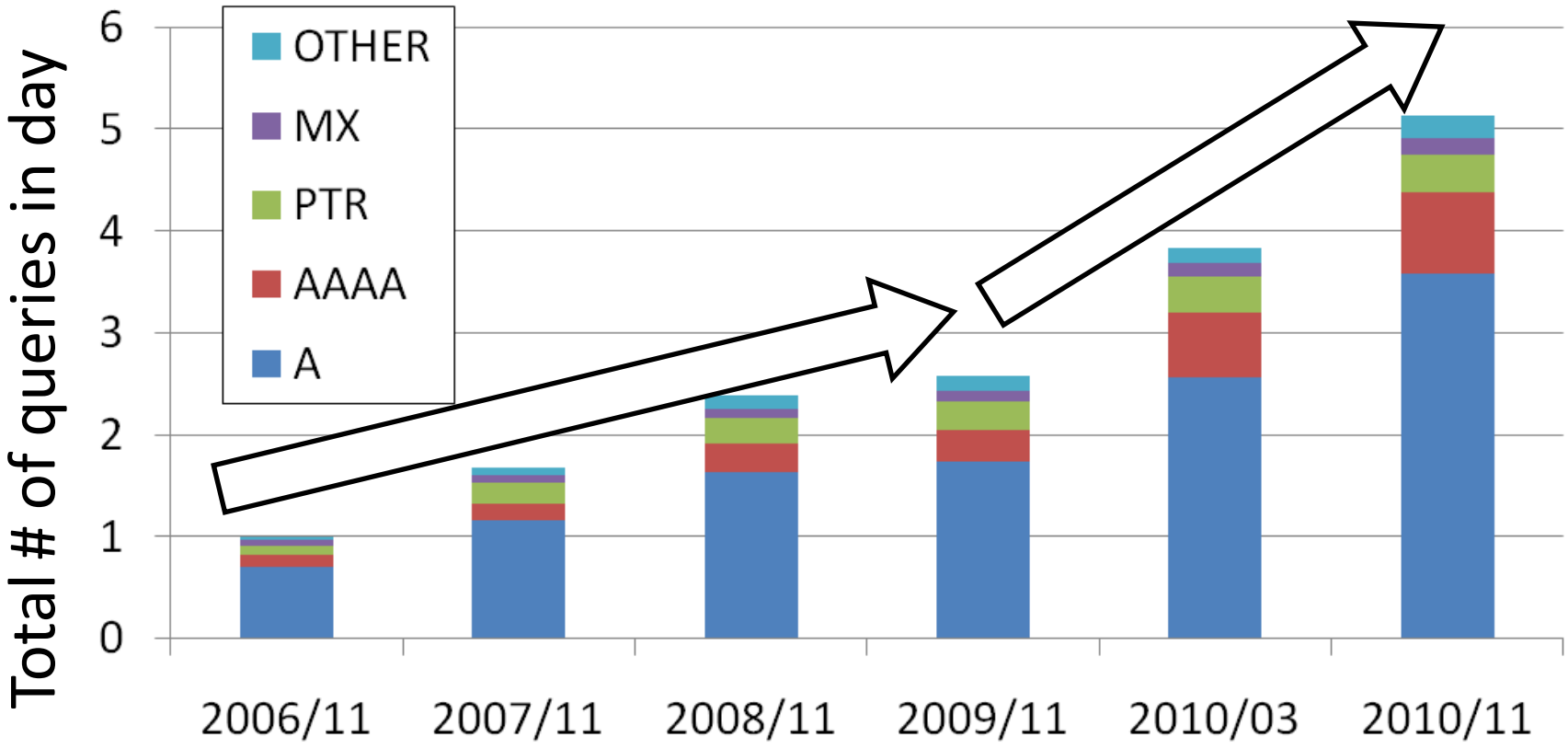
Agenda

- DNS Traffic Trends
  - Transition of total number of queries
  - Transition of number of queries sent by each user
    - Number of heavy users increased
- Cause of Increase: DNS Prefetch
- Discussion

1. DNS Traffic Trend

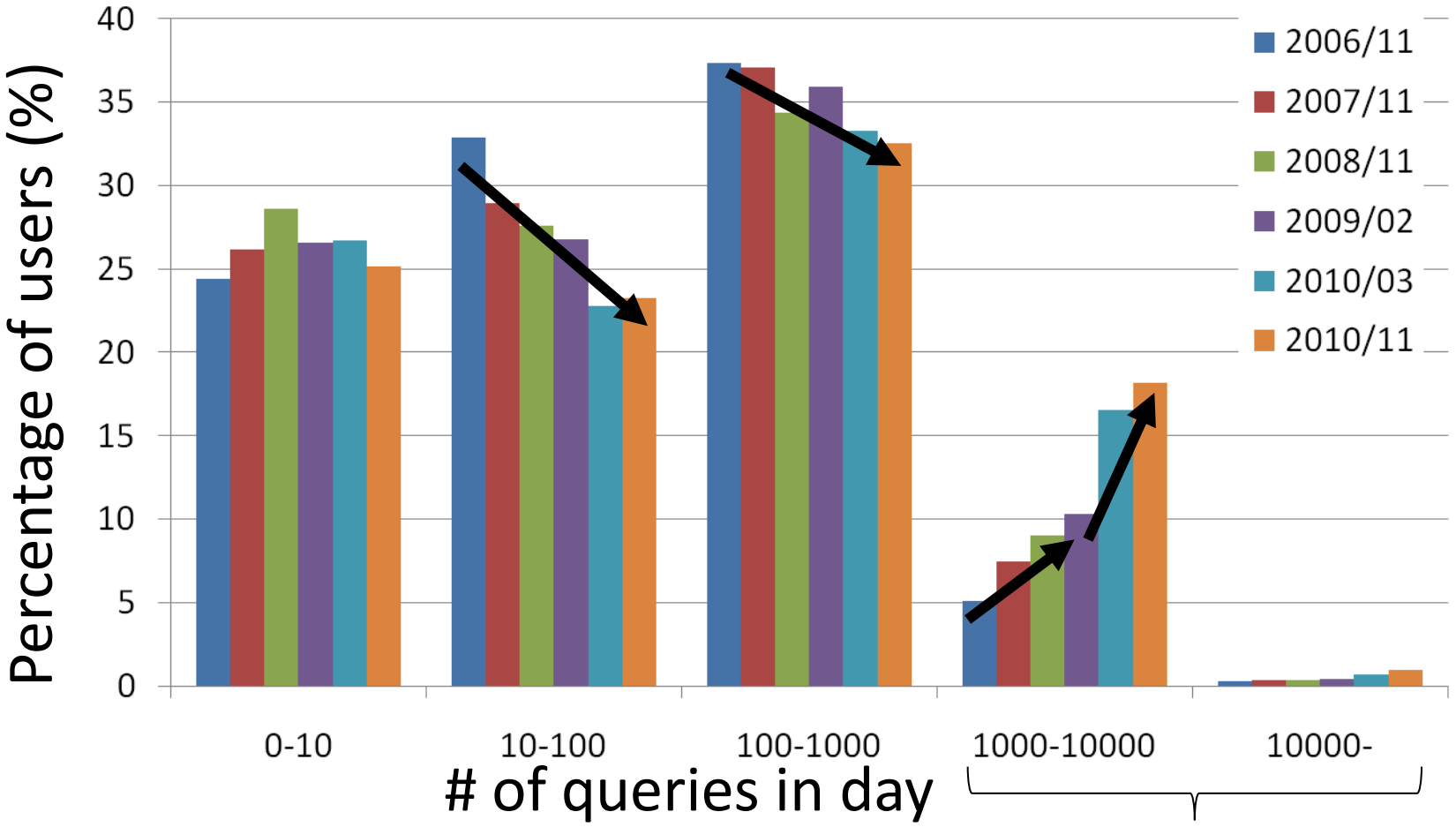
Total Number of Queries

- Queries sent by users have been increasing
- Inflection point during 2009/11 and 2010/03



Number of Queries Sent by Each User

- Number of Heavy users has been increasing
- Inflection point during 2009/11 and 2010/03



2. Cause of Increase

Cause of Increase in Heavy Users

- What caused increase?
  - DNS prefetch function was implemented in Firefox in June 2009
  - Number of Firefox users as heavy users increased

Suspect that DNS prefetch function increased number of heavy users

- DNS prefetch
  - Resolve domain names included in URLs in the browsed WEB page
  - Accelerate browsing the next page, but increase number of queries
  - Google Chrome, Firefox, and Safari implement DNS prefetch

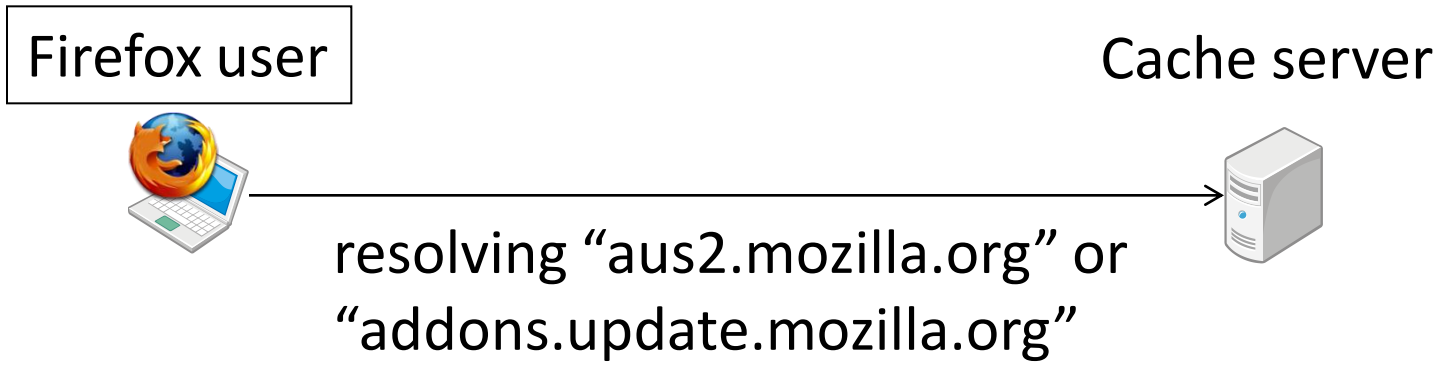
Validations of Suspected Cause

- Query increase analysis
  - Compared number of heavy users who use Firefox in Mar. 2010 with that in Feb. 2009
  - Compared number of queries sent by Firefox users in Mar. 2010 with that in Feb. 2009

- Firefox behavior inspection
  - Inspected prefetch queries by browsing Web pages with large number of links

Extract Firefox Users

- Find hosts that resolve domain names of Firefox or addons update server
  - –“aus2.mozilla.org”
  - –“addons.update.mozilla.org”



Note: We cannot extract all Firefox users. In addition, we might extract users who do not use Firefox

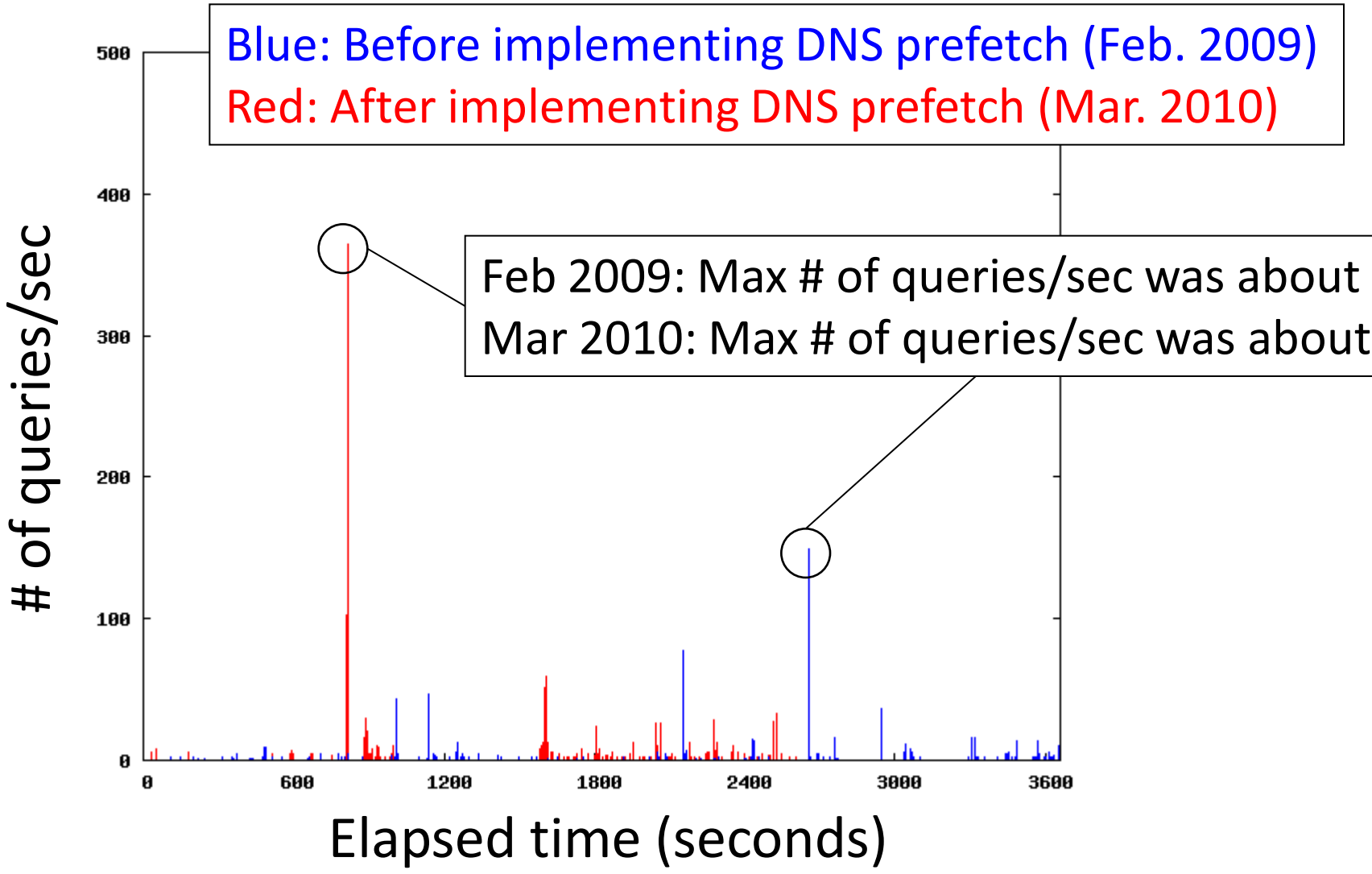
Number of Heavy Users Using Firefox

- Compared number of heavy users who use Firefox in Mar. 2010 with that in Feb. 2009
  - Found heavy users who sent more than 100 queries in one second
  - Pick up Firefox users from the above heavy users
- Comparison results
  - Heavy users quadrupled in one year
  - 28-times increase in heavy users who use Firefox in one year

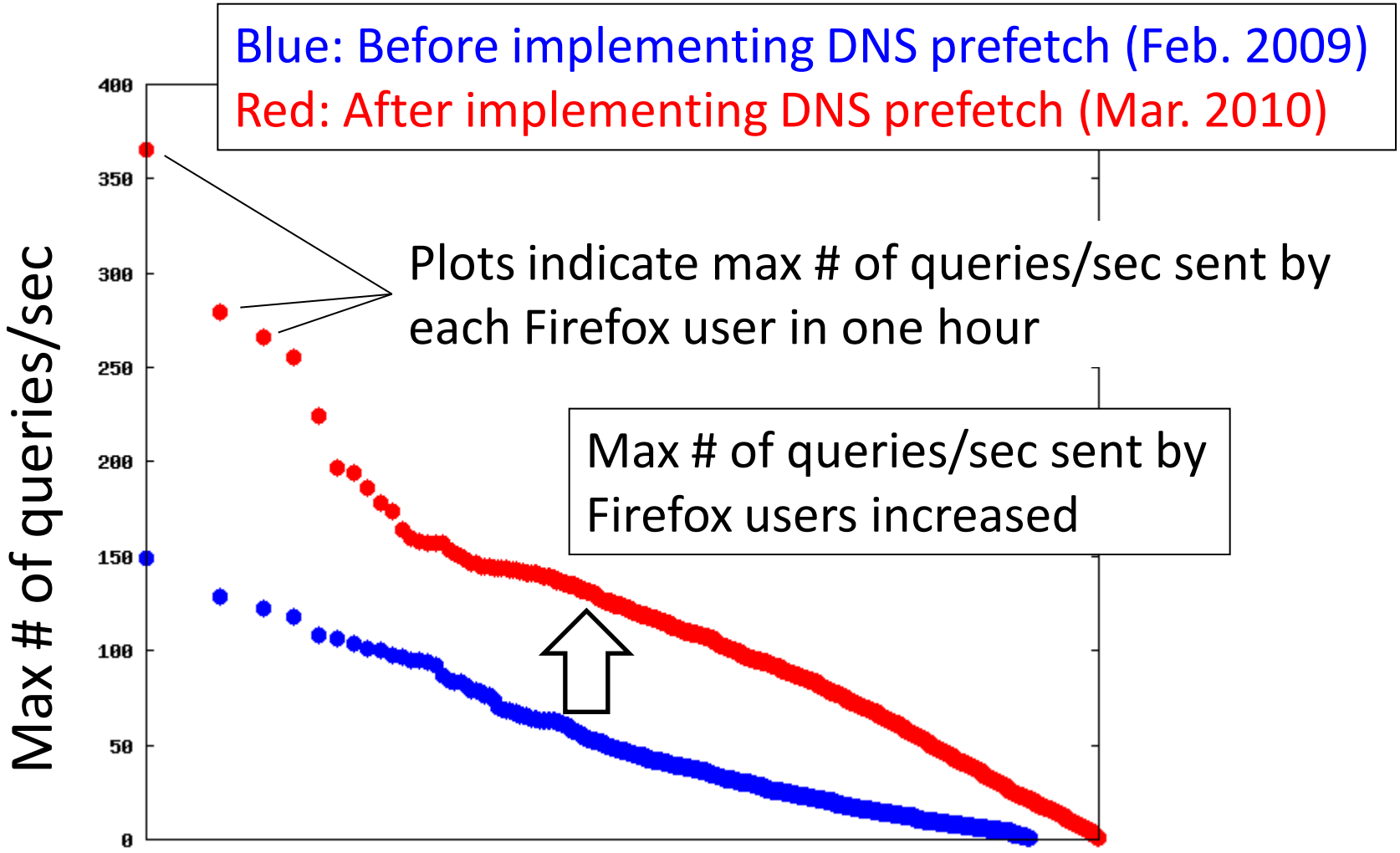
	Feb 2009	Mar 2010
Number of Heavy Users	1	4
Number of Heavy Firefox Users	0.02	0.55

Note: Data in table are normalized so that number Heavy Users at Feb 2009 as one.

Number of Queries Sent by Top Query Rate Firefox Users



Number of Queries per Second Sent by Firefox Users



Firefox users sorted in descending order of max # of queries/sec

Results of Query Increase Analysis

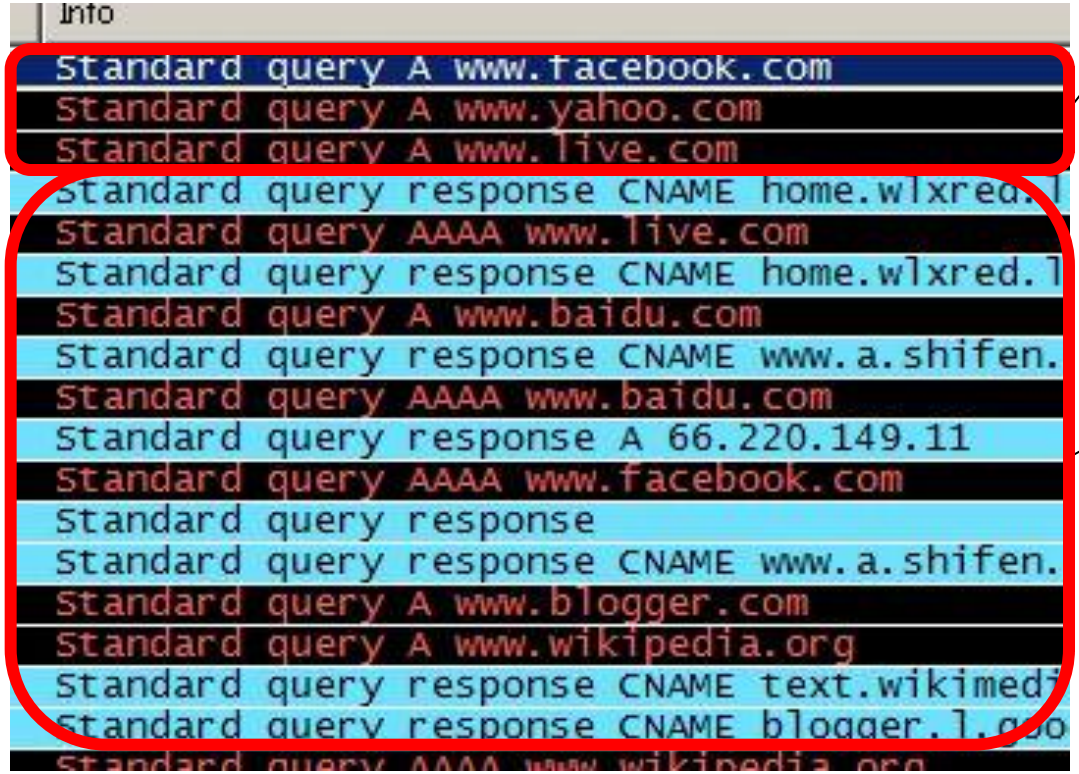
- Heavy users who use Firefox have been increasing
  - –28-times increase in one year
- Number of queries sent by each Firefox user increased after implementing DNS prefetch
  - –Feb. 2009: Max # of queries/sec is 150
  - –Mar. 2010: Max # of queries/sec is 350

# of queries may increase using DNS prefetch function

Firefox Behavior Inspection

- Prefetch query inspection
  - Create Web pages that include 300 links (unique URL)
  - Browse pages with Firefox
  - Capture and inspect prefetch queries
- Inspection Environment
  - Windows Vista SP2
  - Core 2 Duo 2.4 GHz、2 GB Memory
  - Firefox 3.6

Firefox Behavior



Send 3 prefetch queries and wait for response

Send next prefetch query as soon as response is returned

Stop sending query and wait for response when there are 3 threads

Resolve 150 out of 300 domain names

Results of Firefox Behavior Inspection

- Firefox seems to control prefetch rate
  - Max parallel queries was 3.
  - Max number of prefetch domain names was 150.
- However, number of prefetch queries may be double or more by OS resolvers.
  - Windows Vista/7 sends A and AAAA queries, and it also sends queries of domain names appended Domain Search Suffix [TOYONO]

[TOYONO] Tsuyoshi Toyono and Katsuyasu Toyama, “Clear and Present Increase of AAAA Queries”, NANOG 36.

`

3. Discussion

Discussion

- Filtering heavy users may block legitimate queries
  - So far, queries sent by heavy users have almost all been bogus[NAKAGAMI]
  - Difficult to distinguish whether queries sent by heavy users are bogus or not
- It may effect on stateful middle boxes provisioning such as FW, Large Scale NAT at ISP, enterprise networks
  - Session tables of those boxes may be fulfilled by small number of prefetch browser users
- If the IE implements DNS prefetch function, things may get worse

[NAKAGAMI]Shintaro NAKAGAMI, Tsuyoshi TOYONO, Keisuke ISHIBASHI, Haruhiko NISHIDA, and Haruhiko OHSHIMA, “Large-scale DNS Caching Servers Hot Topics/An Analysis of Anomalous Queries,” 2008 OARC DNS Ops Workshop