Clear and Present ~~Danger~~ Increase in Number of DNS AAAA Queries

NTT Information Sharing Platform Labs

Tsuyoshi Toyono,
Keisuke Ishibashi,
and Katsuyasu Toyama
{toyono, isibasi, toyama}@nttv6.net

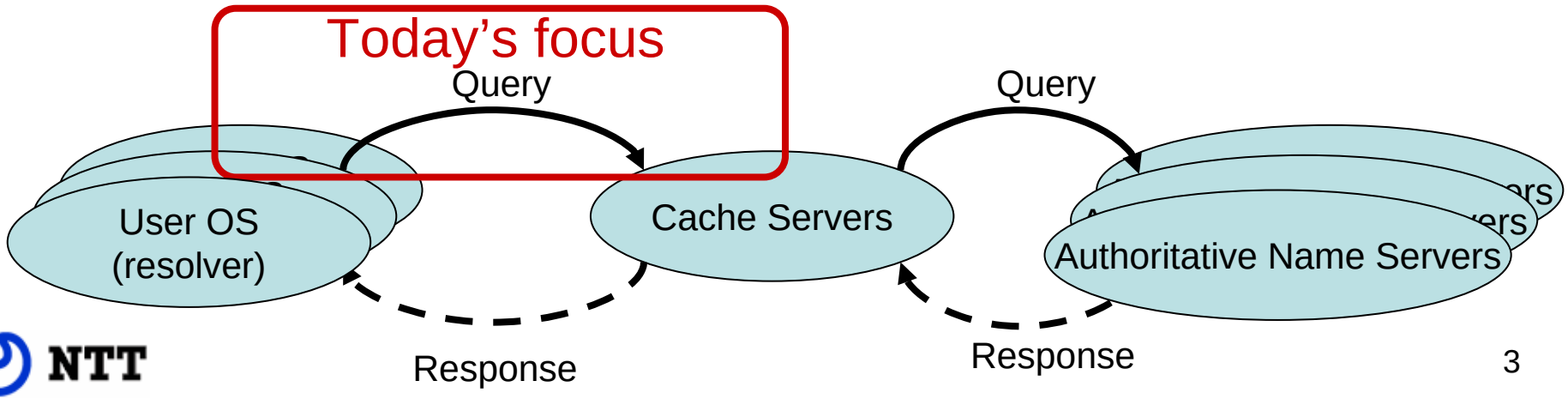
Outline

- Expect increase in number of DNS queries

- Discussion
  - Effect on cache server load and user response time
  - How can we decrease number of unnecessary queries?

Today's Topic

- We focus on increase in number of queries between users and cache servers caused by
  - 1. IPv6 support
    - Number of AAAA queries same as that of A queries
  - 2. Domain name completion
    - Domain name completion by operating system
    - Domain name completion by applications



(1) IPv6-enabled OS increases DNS queries

1. IPv6 and OS Resolver

- IPv6-enabled OSs send AAAA queries for every name resolution

- BSD / Windows
  - Sends both A and AAAA queries for every name resolution
    - Currently almost all applications do not specify “DNS Query Type”, therefore OS sends both.
    - Even if the response to AAAA query is “not exist such a domain name” (NXDomain), OS tries to send A query.

(2) Domain name completion increases DNS queries

2. Domain Name Completion

- When a name resolution fails, both OS and APP automatically resolve the domains with prefix/suffix completion.
  - e.g., when name resolution of “host” failed…
    → host.com → host.org → host.net ...

- OS using these domains to complete:
  - FreeBSD: specified by “search” in /etc/resolv.conf and distributed via DHCP
  - Windows: configured in control panel and distributed via DHCP
- Applications:
  - Mozilla: retries name resolution for a domain by adding “www. ” domain prefix
  - IE：searches domain using MSN search and then retries name resolutions for domains by adding .com➔.org ➔.net ➔.edu

And these combinations
increase queries more and more...

Combination in FreeBSD

- Combinations of AAAA queries and domain completions are different depending on OS
- FreeBSD
  - Tries domain completions for A and AAAA

(Ex) User Query: noexist-example.com

```
A     noexist-example.com
AAAA  noexist-example.com
A     noexist-example.com.com
AAAA  noexist-example.com.com
A     noexist-example.com.net
AAAA  noexist-example.com.net    .....
```

If IPv4 address is resolved, stop here.

Combination in Windows

- Combinations of AAAA queries and domain completions are different depending on OS
- Windows
  - Tries AAAA queries for all domain completions, and then A queries with domain completions

(Ex) User Query: noexist-example.com
AAAA noexist-example.com
AAAA noexist-example.com.com
AAAA noexist-example.com.net
A noexist-example.com
A noexist-example.com.com
A noexist-example.com.net .....

Current typical name resolution by IPv6-enabled Windows

- In the current Internet, almost domains
  - have IPv4 addresses
  - but does NOT have IPv6 addresses.
- IPv6-enabled Windows
  tries AAAA queries for all domain completions, and then sends A queries.

(Ex) User Query: no-v6addr.com

```
AAAA  no-v6addr.com
AAAA  no-v6addr.com.com
AAAA  no-v6addr.com.net
A     no-v6addr.com
```

Even if the domain has IPv4 addresses, firstly AAAA queries are sent!!!

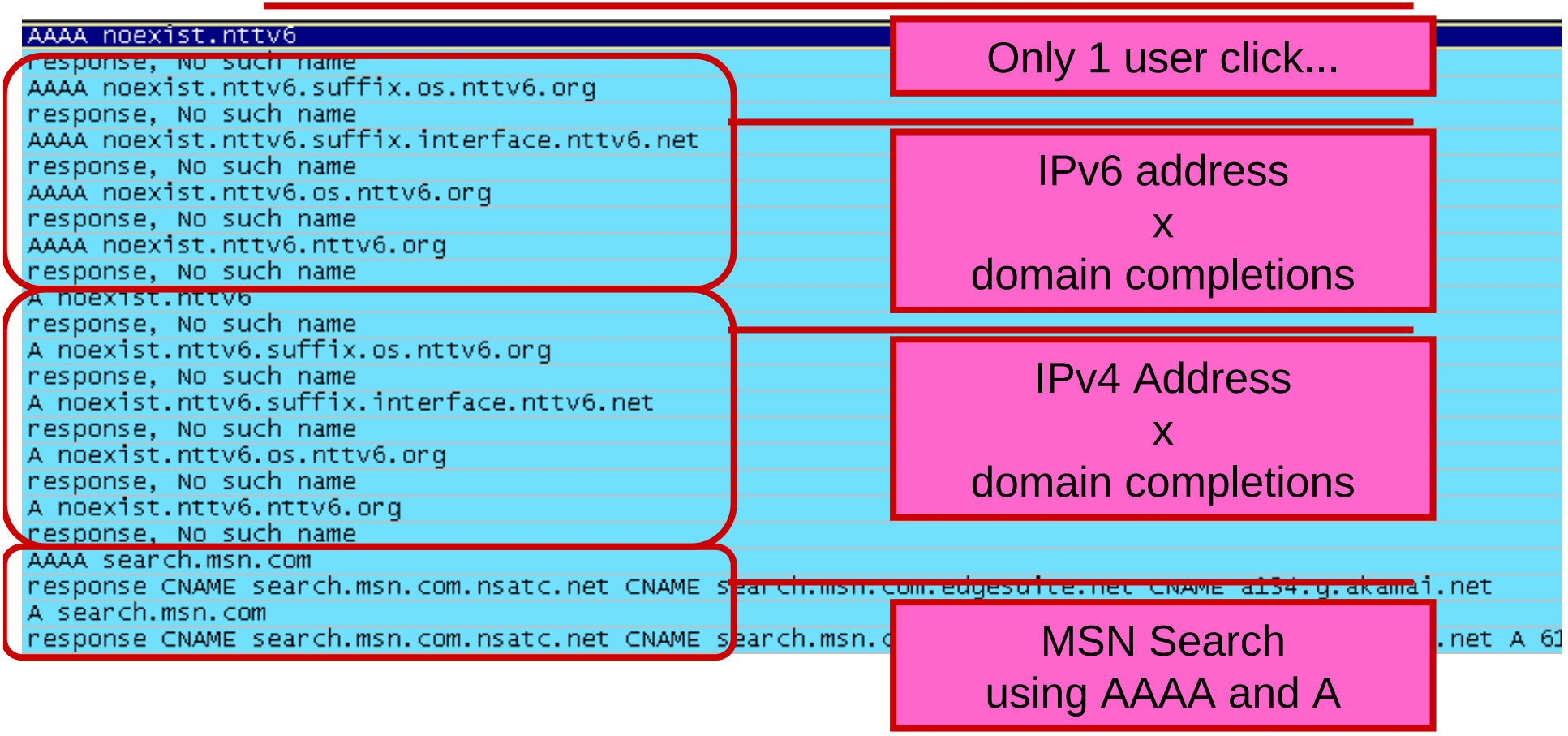
We examined
the forthcoming new Windows...

Longhorn (Windows Vista) β2 Build5270

- Default IPv6 enabled
  - Always try AAAA queries

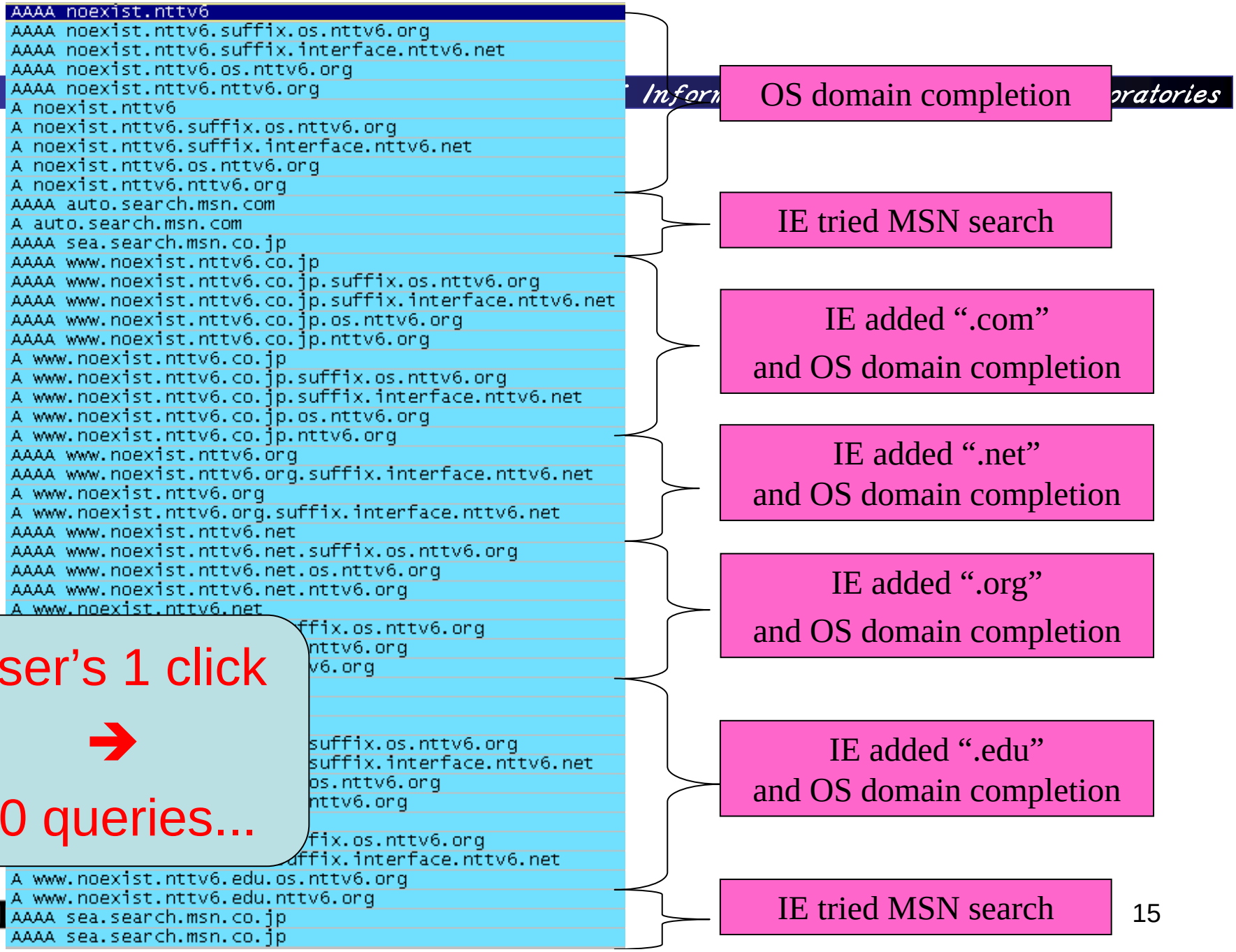
- OS/Application domain name completion
  - Behavior of OS resolver is same as Windows XP
    - OS and applications make (unnecessary) suffix/prefix completions for domain names

IPv6 enable + domain completion
A common case(IE7)



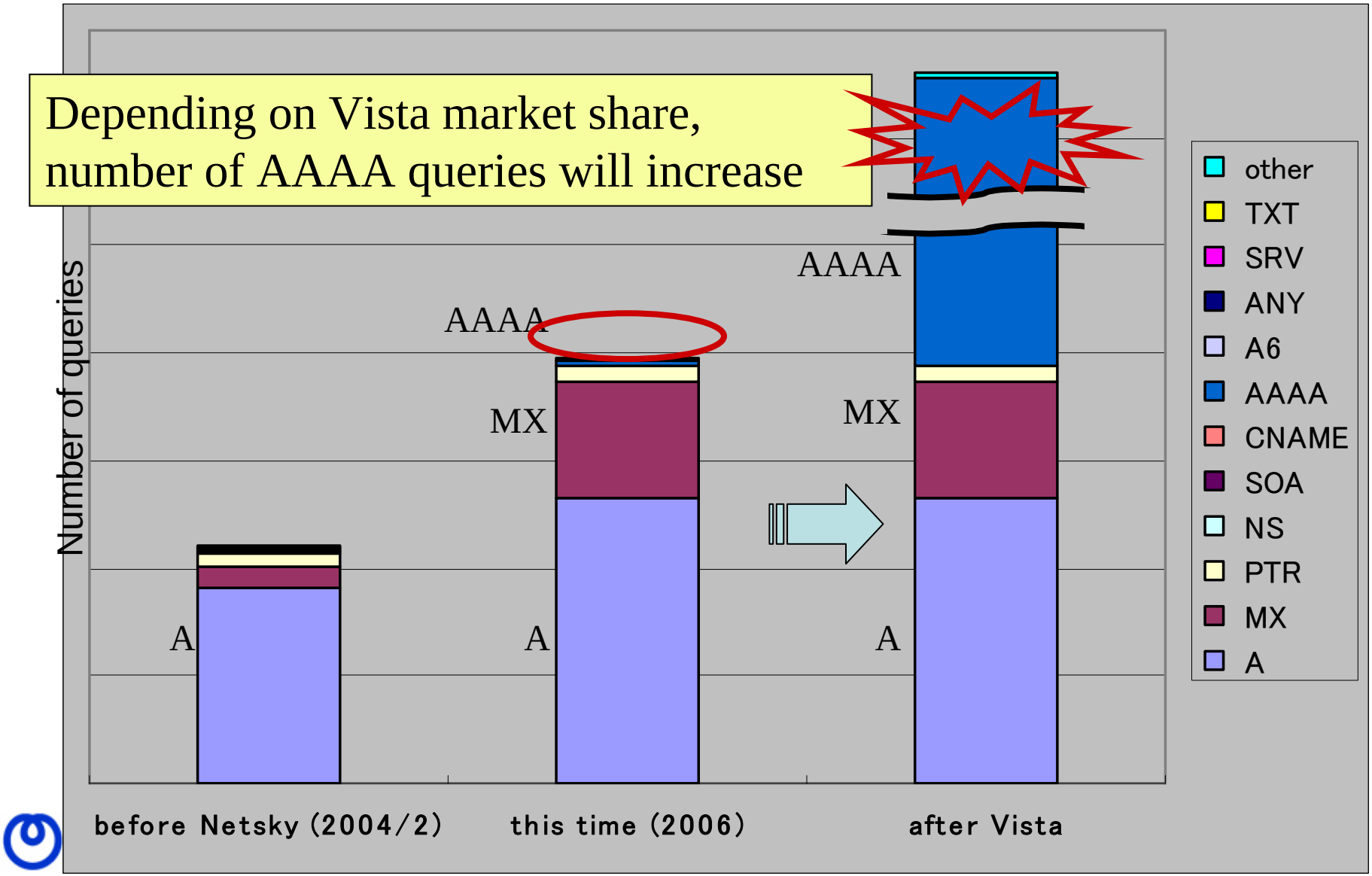
- 1 user click ➔ 12 DNS queries

In the worst case...



Consider these behaviors from the viewpoint of DNS cache servers...

Expected Increase in Number of User Queries



Conclusion

- Release of Windows Vista (IPv6 by default)
  - doubles the number of user queries
  - causes more queries in domain name completions and domain search sequence for AAAA and A queries

- Discussion
  - Operators
    - Cache servers should be prepared for those increases.
      - DNS response time has a serious impact on QoS to end users
    - e.g., stopping domain distribution to users by DHCP or PPPoE
  - Developers of OS
    - Is current search order of resolvers appropriate?
      - e.g., should “A” record be resolved before domain completion?

Questions or Comments?