DNS stub resolver behavior of IPv6 ready hosts

NTT
Information Sharing Platform Labs

Tsuyoshi Toyono, Haruhiko Nishida
{toyono, nishida}@nttv6.net

About our team

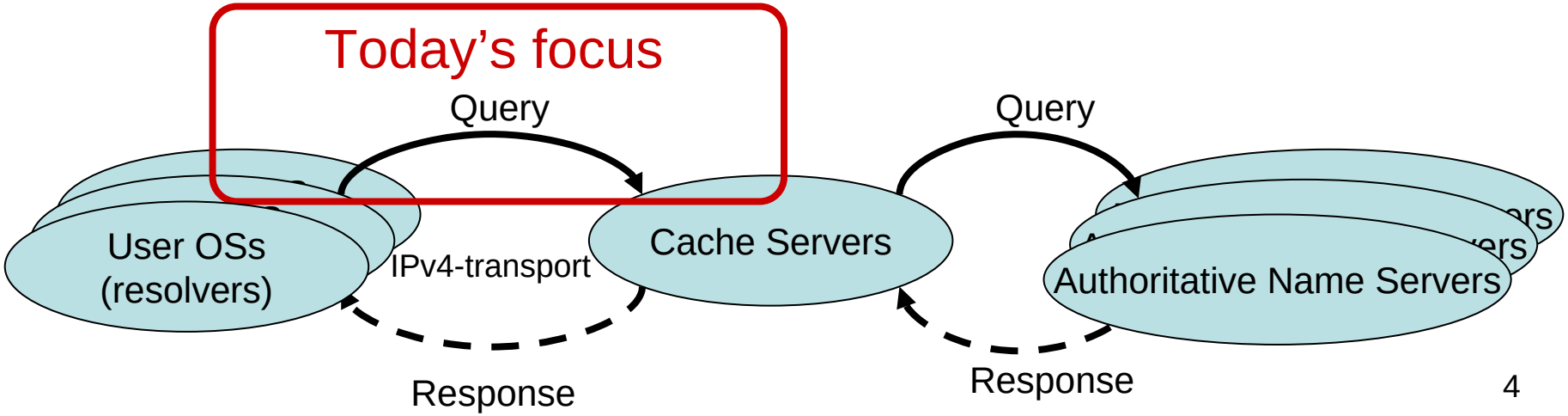
- Our team research on IPv6 deployment issues
  - IPv6 multi-homing
  - IPv4/IPv6 source address selection
  - IPv4 address exhaustion
    - 2011~2012 ?
  - IPv6 PI (Provider Independent) addresses
  - IPv6 impact on current network
  - host/server behavior in IPv4/IPv6 mixed environment

Outline

- DNS stub resolver behavior of IPv6 ready hosts causes increase in number of queries
  - Behaviors of IPv6-enabled hosts
  - Detailed behaviors of FreeBSD, Linux, MacOS X, Windows Vista (Beta and RC)
  - Prevention of unnecessary increase in number of AAAA queries
    - NANOG36: Our report
      - Expected increase in number of DNS AAAA queries
    - NANOG38: Microsoft report
      - Fix Windows Vista implementation of DNS reslover
- Other causes
  - Number of end users who have IPv6 reachability

Focus on

- User-Cache DNS queries, not on Cache-Authoritative queries
- 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 (API), and by applications
  - 3. These Combinations
    - Sequence of queries



(1) IPv6-enabled OS increases DNS queries

IPv6 and OS Resolver

- IPv6-enabled OSs ask for both A and AAAA records
  - "A" query = IPv4 name resolution
  - "AAAA" query = IPv6 name resolution

- Sends both A and AAAA queries for every name resolution
  - Currently, almost no application specifies "DNS Query Type"; therefore, OS sends both

(2) Domain name completion increases DNS queries

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” “domain” 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
  - IE6: using MSN search, then adds a domain suffix ".com" ".net" ".org" and ".edu"

(3) Combination of (1) and (2)

Combination in FreeBSD

- Sequence
  - Sends A query first, then AAAA query
- Domain Completion
  - Tries domain completions for every set of “A+AAAA”
- IPv6 address
  - Sends AAAA queries even if it doesn’t have an IPv6 address

(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

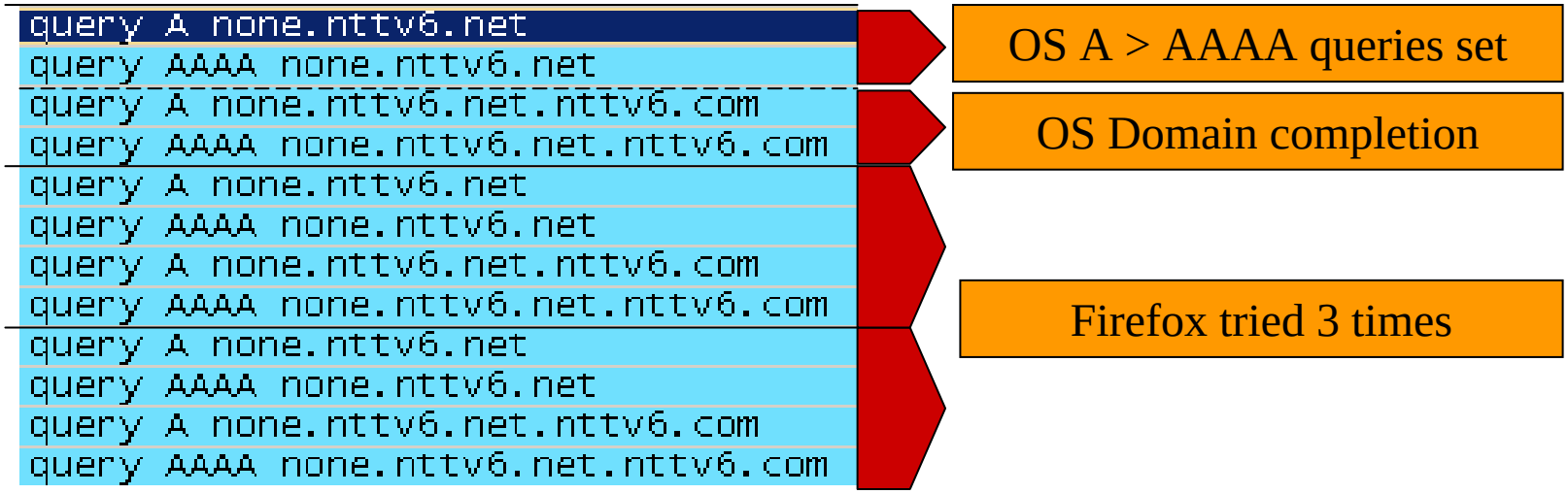
AAAA noexist-example.com.net .....

If IPv4 address is resolved, stop here.

FreeBSD 6.1R
+ Firefox 1.5.0.7

- NX-Domain
  - Tries A query first, then AAAA
  - Tries domain name completions (via DHCPd)
  - Application tries 2 times more

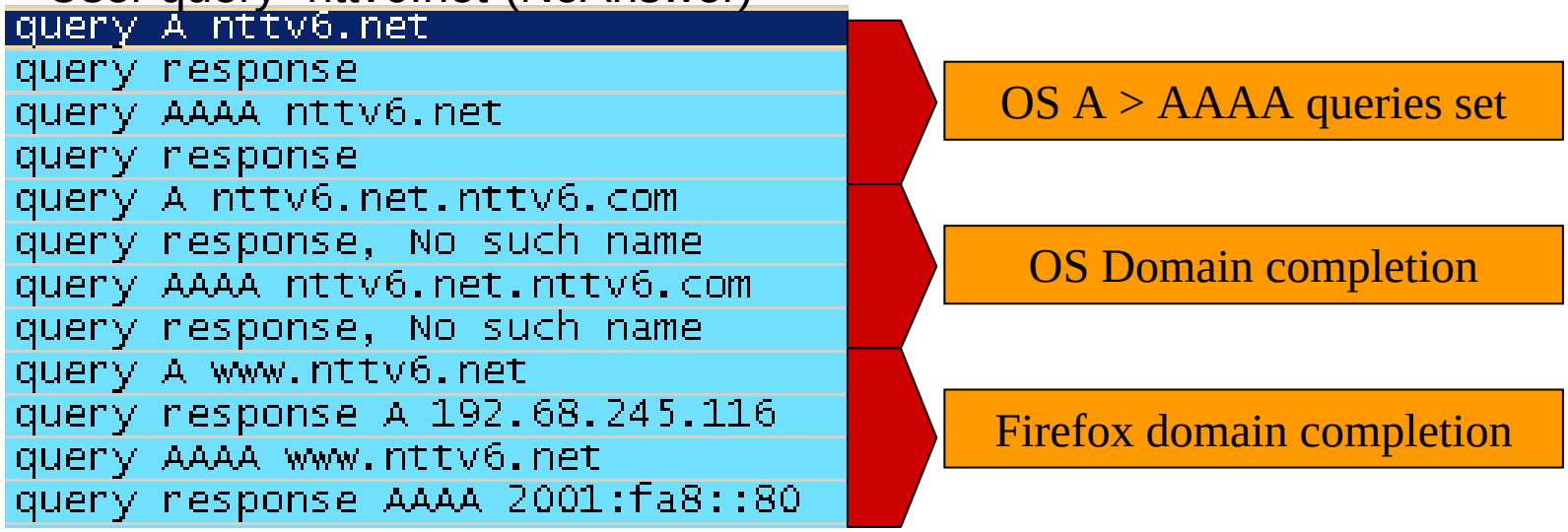
User query “none.nttv6.net”(NX)



FreeBSD 6.1R
+ Firefox 1.5.0.7

- No Answer
  - Tries A query first, then AAAA
  - Tries domain name completions
  - Application adds “www.” prefix and sends query to resolver again
  - Application displays “www.nttv6.net” page

User query “nttv6.net”(NoAnswer)



Combination in MacOS

- Sequence
  - Sends A query first, then AAAA query
- Domain Completion
  - Tries domain completions for every set of “A+AAAA”
- IPv6 address
  - Doesn’t send AAAA queries if it doesn’t have an IPv6 address

(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

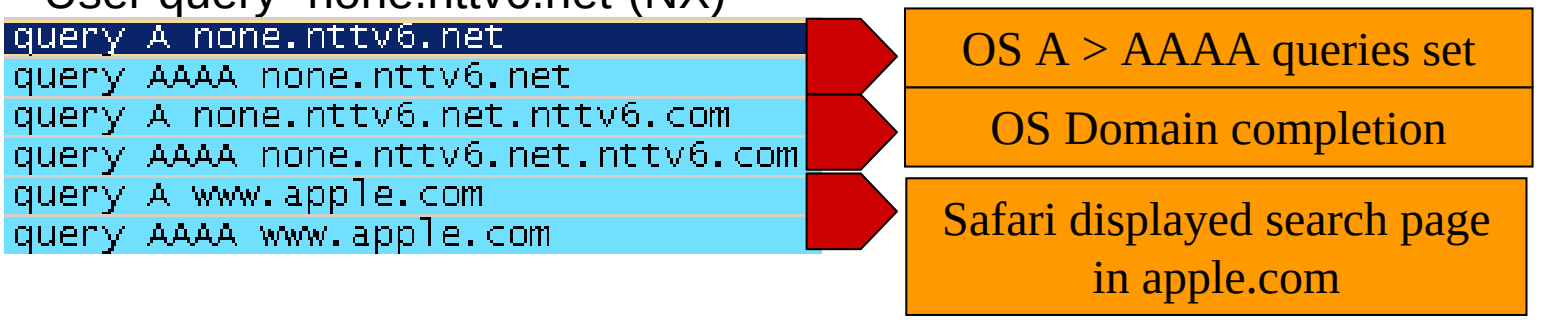
AAAA noexist-example.com.net .....

If IPv4 address is resolved, stop here.

MacOS 10.4.8 + Safari 2.0.4

- NX-Domain
  - Tries A query first, then AAAA
  - Tries domain name completions
  - Application displays search page in “www.apple.com”

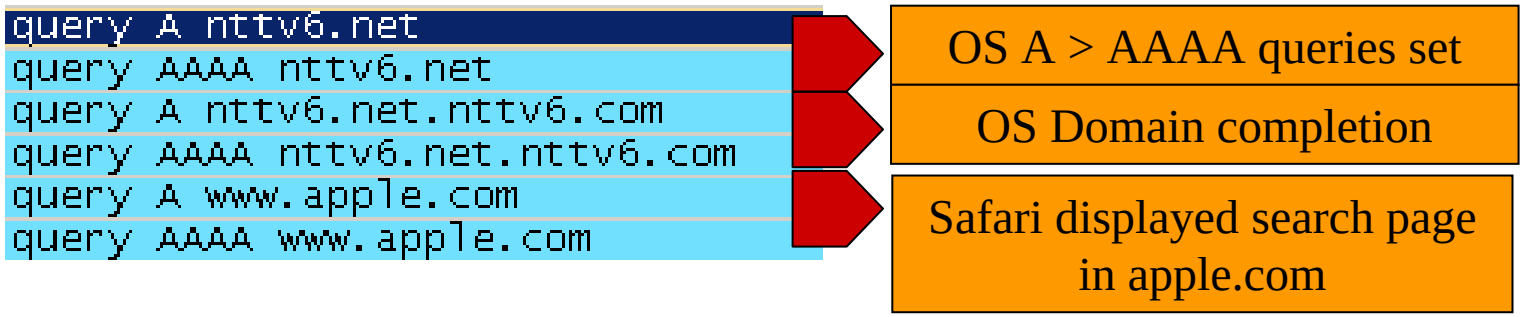
User query “none.nttv6.net”(NX)



MacOS 10.4.8
+ Safari 2.0.4

- No Answer
  - Same as “NX-Domain” pattern

User query “nttv6.net”(NoAnswer)



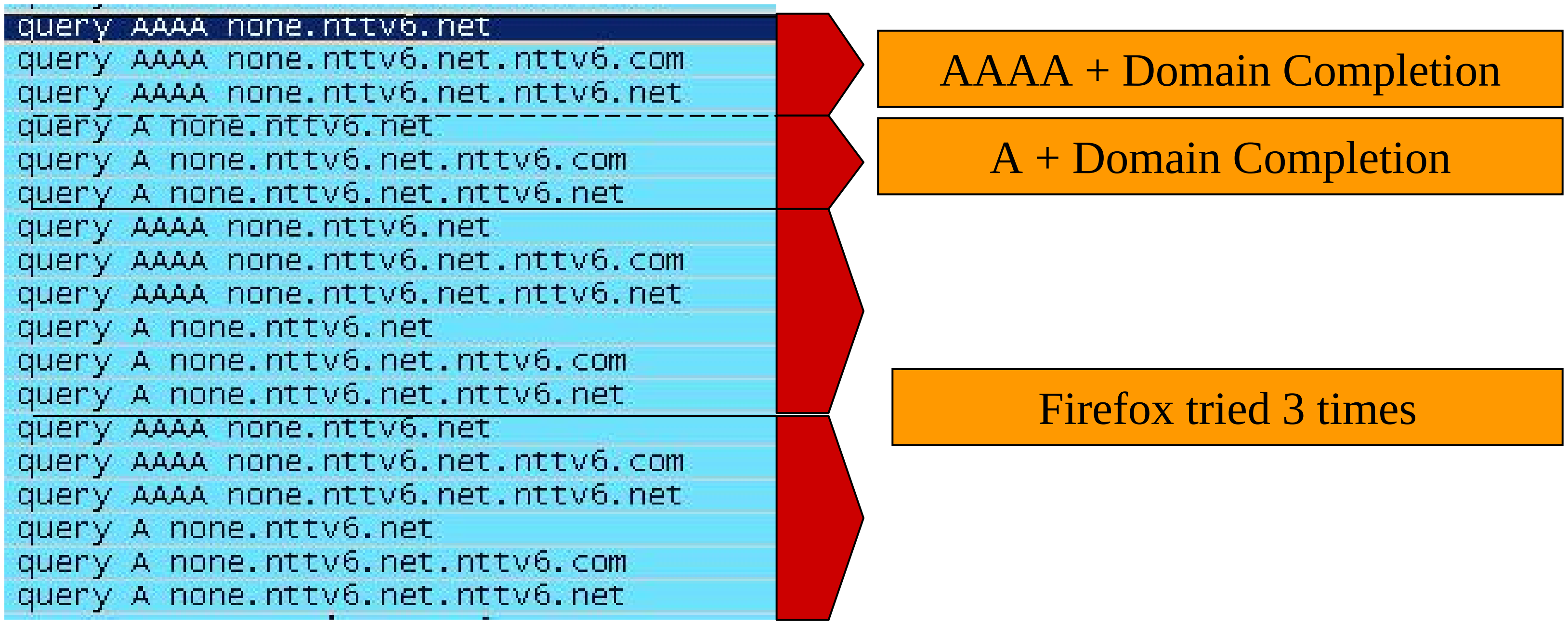
Combination in Linux

- Tries AAAA queries for all domain completions, then A queries with domain completions
- IPv6 address
  - Sends AAAA queries even if it doesn't have an IPv6 address

Fedora Core 5 (kernel2.6.15) + Firefox 1.5.0.7

- NX-Domain
  - Tries all patterns of AAAA Domain Name Completions
  - Then, tries A queries as same
  - Application tries 2 times more

User query “none.nttv6.net”(NX)



Fedora Core 5 (kernel2.6.15) + Firefox 1.5.0.7

- No Answer
  - Tries all patterns of AAAA Domain Name Completions
  - Then, tries A queries as same
  - Application adds “www.” prefix and sends query to resolver again
  - Application displays “www.nttv6.net” page

User query “nttv6.net”(NoAnswer)

```
query AAAA nttv6.net
query response
query AAAA nttv6.net.nttv6.com
query response, No such name
query AAAA nttv6.net.nttv6.net
query response, No such name
query A nttv6.net
query response
query A nttv6.net.nttv6.com
query response, No such name
query A nttv6.net.nttv6.net
query response, No such name
query AAAA www.nttv6.net
query response AAAA 2001:fa8::80
query A www.nttv6.net
query response A 192.68.245.116
```

AAAA + all domain completions

A + all domain completions

Firefox domain completion

Combination in Windows Vista (before β2 Build5270)

- Tries AAAA queries for all domain completions, then tries A queries with domain completions
- Same as Linux (kernel 2.6.15) behavior
- IPv6 address
  - Sends AAAA queries even if it doesn't have an IPv6 address

(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
```

Even if domain has IPv4 addresses, first, AAAA queries are sent.

Windows Vista (β2 Build5270)+IE7.0(at the time)

```
AAAA noexist.nttv6
AAAA noexist.nttv6.suffix.os.nttv6.org
AAAA noexist.nttv6.suffix.interface.nttv6.net
AAAA noexist.nttv6.os.nttv6.org
AAAA noexist.nttv6.nttv6.org
A noexist.nttv6
A noexist.nttv6.suffix.os.nttv6.org
A noexist.nttv6.suffix.interface.nttv6.net
A noexist.nttv6.os.nttv6.org
A noexist.nttv6.nttv6.org
AAAA auto.search.msn.com
A auto.search.msn.com
AAAA sea.search.msn.co.jp
AAAA www.noexist.nttv6.co.jp
AAAA www.noexist.nttv6.co.jp.suffix.os.nttv6.org
AAAA www.noexist.nttv6.co.jp.suffix.interface.nttv6.net
AAAA www.noexist.nttv6.co.jp.os.nttv6.org
AAAA www.noexist.nttv6.co.jp.nttv6.org
A www.noexist.nttv6.co.jp
A www.noexist.nttv6.co.jp.suffix.os.nttv6.org
A www.noexist.nttv6.co.jp.suffix.interface.nttv6.net
A www.noexist.nttv6.co.jp.os.nttv6.org
A www.noexist.nttv6.co.jp.nttv6.org
AAAA www.noexist.nttv6.org
AAAA www.noexist.nttv6.org.suffix.interface.nttv6.net
A www.noexist.nttv6.org
A www.noexist.nttv6.org.suffix.interface.nttv6.net
AAAA www.noexist.nttv6.net
AAAA www.noexist.nttv6.net.suffix.os.nttv6.org
AAAA www.noexist.nttv6.net.os.nttv6.org
AAAA www.noexist.nttv6.net.nttv6.org
A www.noexist.nttv6.net
A www.noexist.nttv6.net.suffix.os.nttv6.org
A www.noexist.nttv6.net.os.nttv6.org
A www.noexist.nttv6.net.nttv6.org
AAAA www.noexist.nttv6.edu
AAAA www.noexist.nttv6.edu
AAAA www.noexist.nttv6.edu
AAAA www.noexist.nttv6.edu.suffix.os.nttv6.org
AAAA www.noexist.nttv6.edu.suffix.interface.nttv6.net
AAAA www.noexist.nttv6.edu.os.nttv6.org
AAAA www.noexist.nttv6.edu.nttv6.org
A www.noexist.nttv6.edu
A www.noexist.nttv6.edu.suffix.os.nttv6.org
A www.noexist.nttv6.edu.suffix.interface.nttv6.net
A www.noexist.nttv6.edu.os.nttv6.org
A www.noexist.nttv6.edu.nttv6.org
AAAA sea.search.msn.co.jp
AAAA sea.search.msn.co.jp
```

OS domain completion

IE tried MSN search

IE added “.com”
and OS domain completion

IE added “.net”
and OS domain completion

IE added “.org”
and OS domain completion

IE added “.edu”
and OS domain completion

IE tried MSN search again

Our alert report and MS response

- NANOG36 (2006/2)
  - We reported this behaviors (Vista β) and alerted increase in number of DNS queries
- NANOG38 (2006/10)
  - Abolade Gbadegesin@Vista Internet Protocols team
  - "The NetIO Stack in Windows Vista: Functionality and Deployment"
    - "NTT Labs: NANOG36 report with preliminary analysis based on Windows Vista"

- In his slides:
  - "Deployments of new behavior are best undertaken as joint efforts between host software vendors and public network operators"

Reference:
NANOG36 "Clear and Present Increase of AAAA Queries"
NANOG38 "The NetIO Stack in Windows Vista: Functionality and Deployment"

Combination in Windows Vista (after RC1)

- Status in Vista RC1
  - "Vista doesn't send AAAA queries if the only global IPv6 addresses it has are Teredo addresses"
  - "DNS sends A query first, follows up with AAAA only to servers that have some info, then stops"

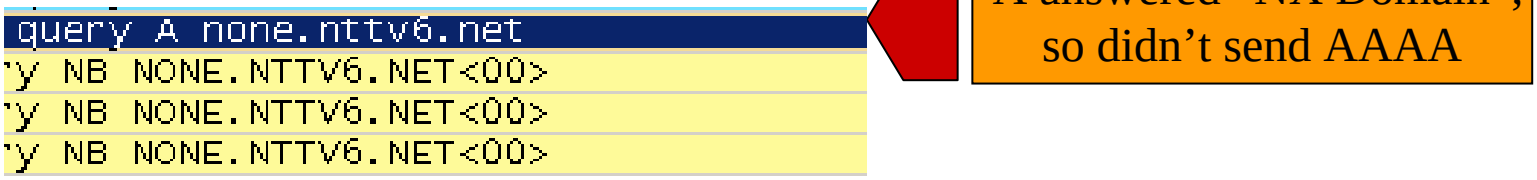
We appreciate this change by Microsoft!

Reference:
NANOG38 "The NetIO Stack in Windows Vista: Functionality and Deployment"

Windows Vista (RC2 Build5744) + IE 7.0.5744.16384

- NX-Domain
  - Sends A query first, and answer is “NX-Domain”, stops sending AAAA query
  - Doesn’t try domain name completions

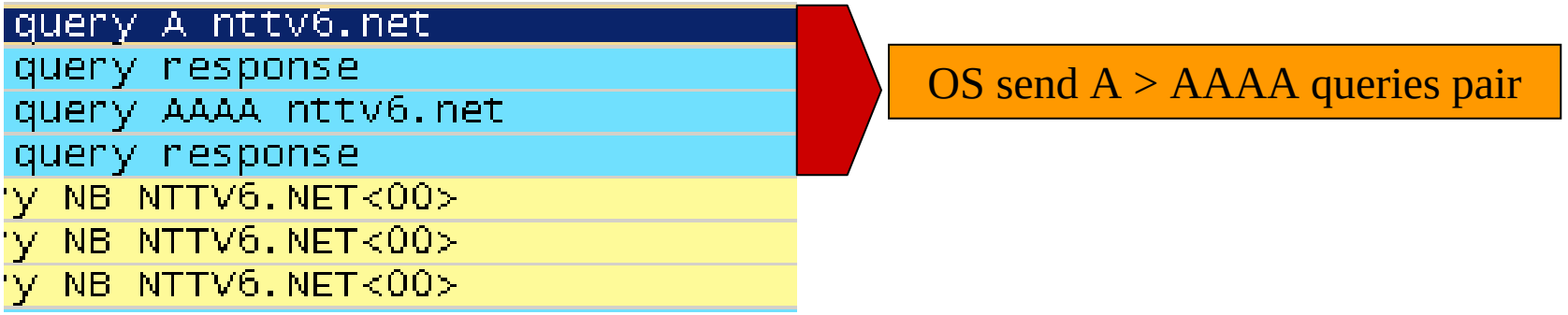
User query “none.nttv6.net”(NX)



Windows Vista (RC2 Build5744) + IE 7.0.5744.16384

- No Answer
  - sends A query first, and answer is “No Answer”, then sends AAAA query
  - Doesn’t try domain name completions
  - Application displays “Not found: nttv6.net” page

User query “nttv6.net”(NoAnswer)



Results

	FreeBSD	Linux	MacOS X	Vista (β)	Vista (RC2)
A & AAAA query sequence order	A first	AAAA first	A first	AAAA first	A first
When does domain name completion occur?	After A+AAAA	All AAAA completion first, then A	After A+AAAA	All AAAA completion first, then A	No completion
Send AAAA queries even if no IPv6 addresses assigned	Yes	Yes	No	Yes	No

- Linux send AAAA queries first
- Linux send all suffix completions of AAAA first, then A

- FreeBSD, Linux and old Vista send AAAA queries even if don't have IPv6 reachability

→ Now, if Vista doesn't have IPv6 address, they don't send AAAA queries

Network environment factors

Network environment factors for query increase

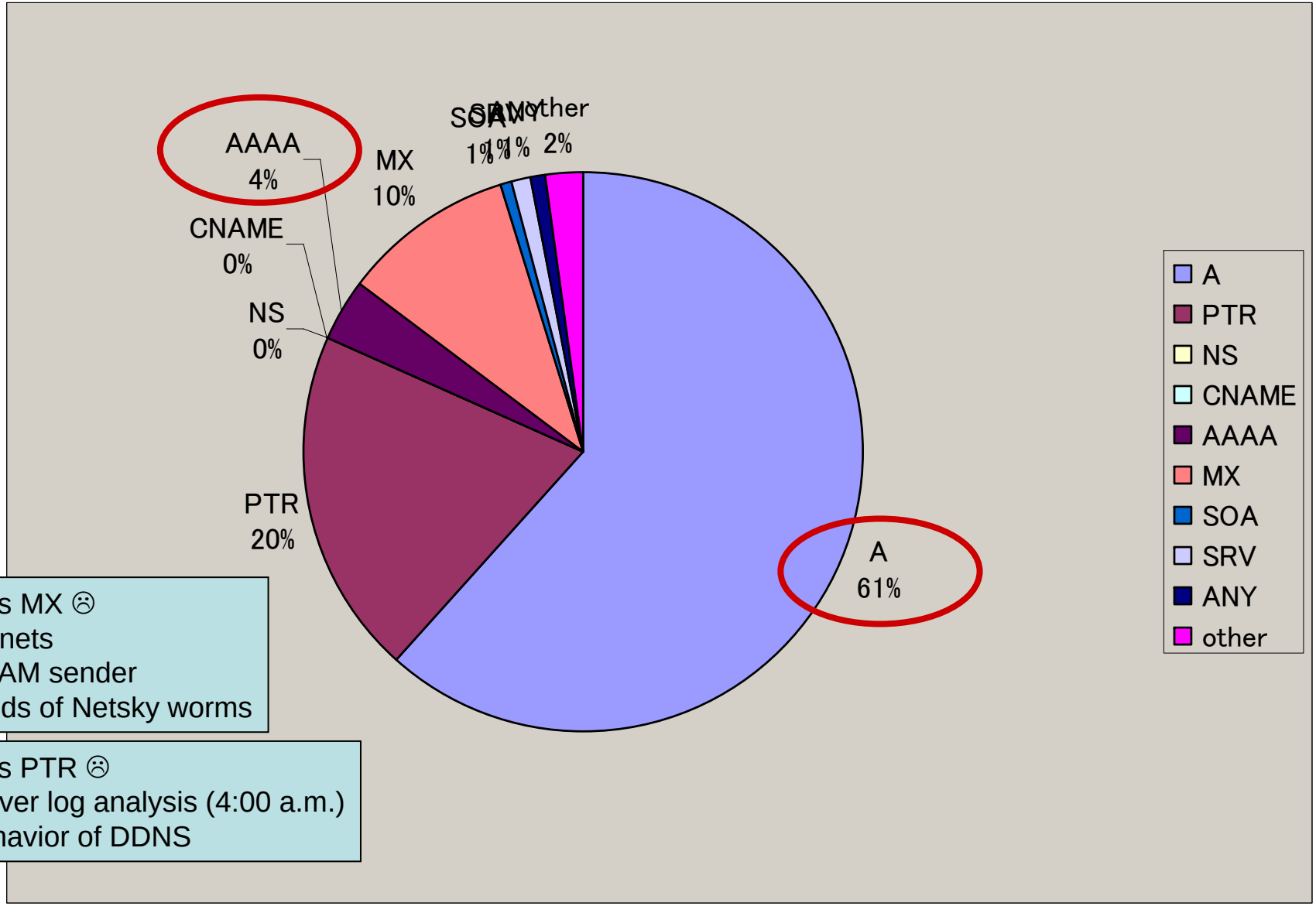
- Number of end users who have IPv6 addresses
- Some OSs send AAAA queries even if they don't have IPv6 reachability
  - Such as FreeBSD, Linux

- Others factors
  - If the answer was "NX-Domain"
  - Has A Resource Record, but don't have AAAA Resource Record
  - Domain suffix distribution to users by DHCP or PPPoE

Number of end users who have IPv6 addresses

- IPv6 environment in Japan
  - Many ISPs already provide IPv6 reachability services to end users
    - e.g., NTT, Yahoo, IIJ, KDDI, and nifty, for example
      (The market share of these large ISPs is about 60-70% of all broadband users)
  - ISPs use IPv6 for their streaming services and IP-phone services, for example.
  - Global IPv6 addresses were given to end hosts
    - Vista will send AAAA queries

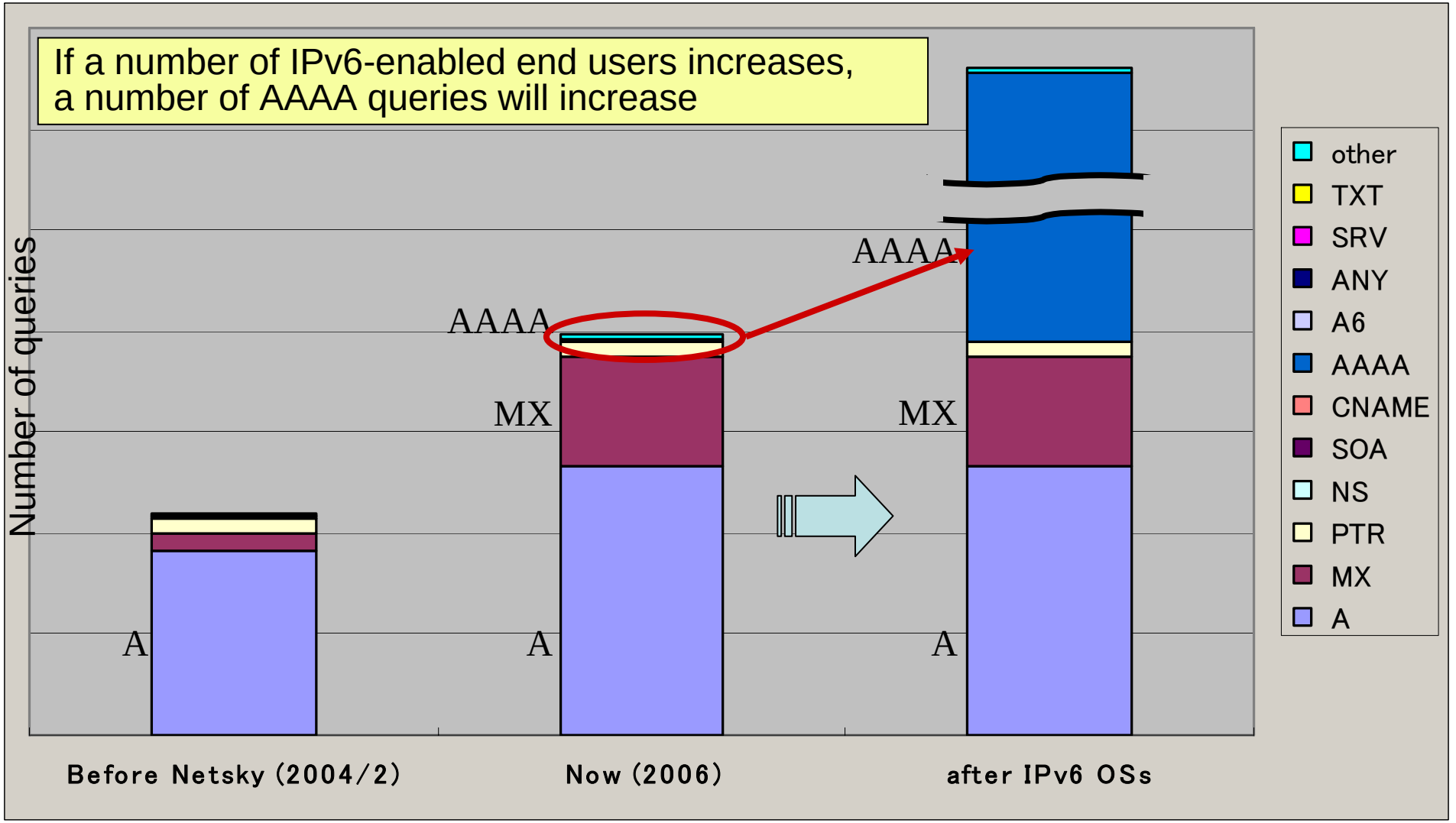
Share of large ISP's DNS cache queries, from users (2006/10 one day total)



User's MX ☹
- botnets
- SPAM sender
- Kinds of Netsky worms

User's PTR ☹
- server log analysis (4:00 a.m.)
- behavior of DDNS

Expected increase in number of user queries



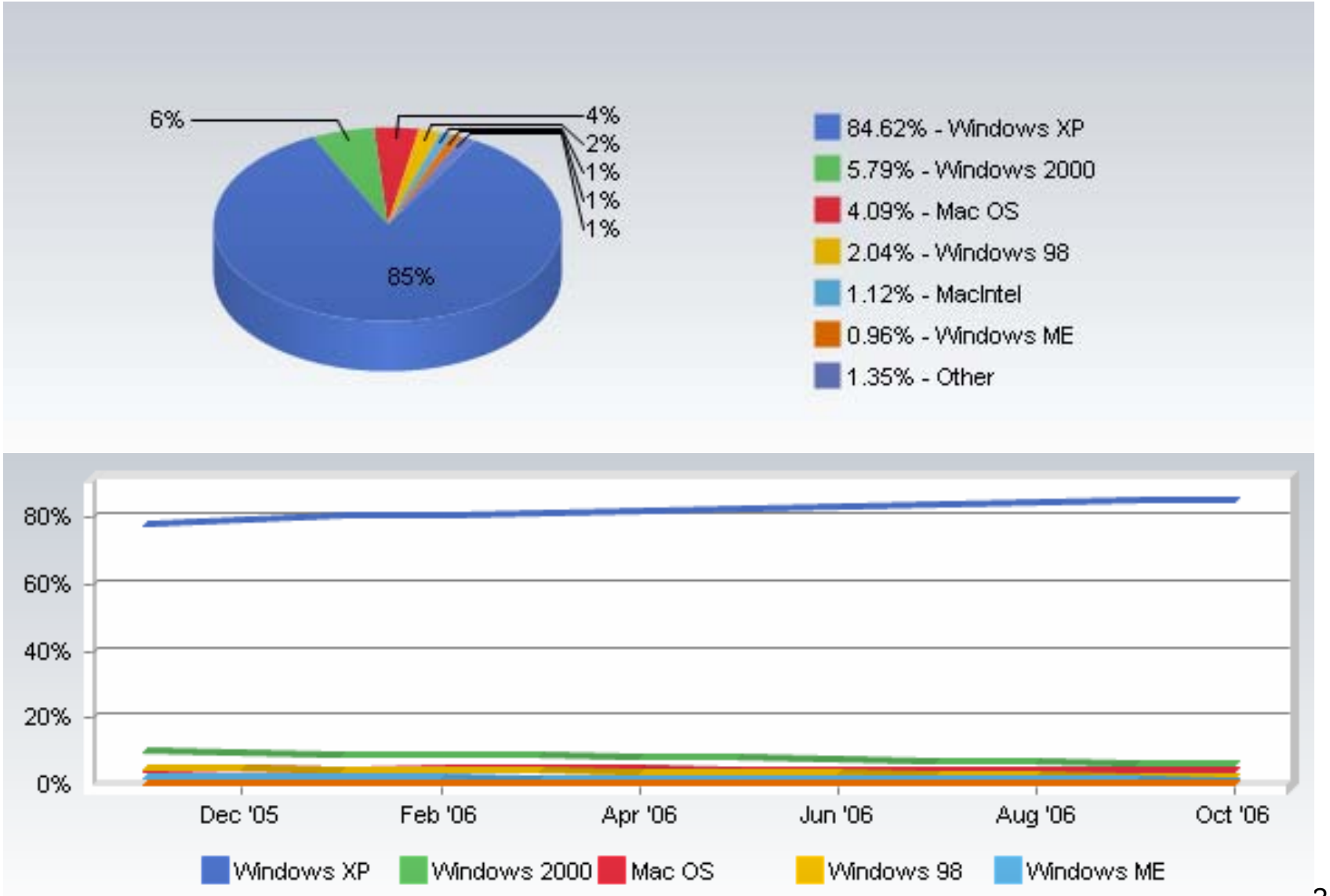
Conclusion

- If a number of IPv6-enabled end users increases, a number of AAAA queries will increase
  - The number of query Increase depends on IPv6-enabled OSs and Applications implementation
- Some OSs send AAAA queries even if hasn't IPv6 reachability
  - As for Vista, the impact was minimized

- We have to prepare increase in number of DNS queries
  - Cache servers should be prepared for those increases
    - Large ISPs Cache servers (that use load balancing) would be better off preparing for those increases
    - Preparing authoritative servers for increases would be better
  - Is current search order of resolvers & applications appropriate?
  - Should IPv6 transport DNS be used?

Thank you.

OS market share



reference: http://marketshare.hitslink.com/