Enabling Internet-Scale DNS-Based measurements

Bachelor Thesis Final Talk

Lennart Bader

Adviser: Dr. Oliver Hohlfeld

http://comsys.rwth-aachen.de

Aachen, 2017-04-27

Motivation

The Internet

Motivation

The Internet

- Evolving to fulfill changing requirements

Motivation

The Internet

- Evolving to fulfill changing requirements
  - IPv6

Motivation

The Internet

- Evolving to fulfill changing requirements
  - IPv6
  - Mobility, Security, QoS, ...

Motivation

The Internet

- Evolving to fulfill changing requirements
  - IPv6
  - Mobility, Security, QoS, ...
  - IoT, CDNs, Cloud Mail Providers, ...

Motivation

The Internet

- Evolving to fulfill changing requirements
  - IPv6
  - Mobility, Security, QoS, ...
  - IoT, CDNs, Cloud Mail Providers, ...

Current **state** of the Internet?

Motivation

The Internet

- Evolving to fulfill changing requirements
  - IPv6
  - Mobility, Security, QoS, ...
  - IoT, CDNs, Cloud Mail Providers, ...

Current **state** of the Internet?

Evolution of the Internet?

Motivation

The Internet

- Evolving to fulfill changing requirements
  - IPv6
  - Mobility, Security, QoS, ...
  - IoT, CDNs, Cloud Mail Providers, ...

Current **state** of the Internet?
Evolution of the Internet?

⇒ Use the Domain Name System to draw conclusions!

The DNS

The Domain Name System

The DNS

The Domain Name System

- Information about domains and their services

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?
- Security (`RRSIG`, `DS`, `TXT`, ...)

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?
- Security (`RRSIG`, `DS`, `TXT`, ...)
- Name Pointers (`CNAME`): CDNs?

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?
- Security (`RRSIG`, `DS`, `TXT`, ...)
- Name Pointers (`CNAME`): CDNs?

How to obtain these information?

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?
- Security (`RRSIG`, `DS`, `TXT`, ...)
- Name Pointers (`CNAME`): CDNs?

How to obtain these information? $\rightarrow$ iterative process

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?
- Security (`RRSIG`, `DS`, `TXT`, ...)
- Name Pointers (`CNAME`): CDNs?

How to obtain these information? $\rightarrow$ iterative process

Queries for specific information

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?
- Security (`RRSIG`, `DS`, `TXT`, ...)
- Name Pointers (`CNAME`): CDNs?

How to obtain these information? $\rightarrow$ iterative process
Queries for specific information – no "tell me everything"

The DNS

The Domain Name System

- Information about domains and their services
- Mail Exchangers (`MX`): Cloud Mail Provider?
- Name Servers (`NS`)
- Used IP addresses (`A`, `AAAA`): IPv6 deployment?
- Security (`RRSIG`, `DS`, `TXT`, ...)
- Name Pointers (`CNAME`): CDNs?

How to obtain these information? $\rightarrow$ iterative process
Queries for specific information – no "tell me everything"

Using the DNS: Not a new idea...

Related Work

Studies on the Internet involving the DNS

Related Work

Studies on the Internet involving the DNS

- Impact of Remote DNS on CDN Performance [IMC'12]
  $\approx$ 45000 users

Related Work

Studies on the Internet involving the DNS

- Impact of Remote DNS on CDN Performance [IMC'12]
  $\approx$ 45000 users
- Security of Web Servers [IMC'14]
  $\approx$ 20000 websites

Related Work

Studies on the Internet involving the DNS

- Impact of Remote DNS on CDN Performance [IMC'12]
  $\approx$ 45000 users
- Security of Web Servers [IMC'14]
  $\approx$ 20000 websites
- DDoS Potential of DNSSec [IMC'14]
  $\approx$ 2.5 million domains

Related Work

Studies on the Internet involving the DNS

- Impact of Remote DNS on CDN Performance [IMC'12]
  $\approx$ 45000 users
- Security of Web Servers [IMC'14]
  $\approx$ 20000 websites
- DDoS Potential of DNSSec [IMC'14]
  $\approx$ 2.5 million domains
- Large-Scale DNS Measurement Infrastructure [IMC'16]
  $\approx$ 150 million domains

Related Work

Studies on the Internet involving the DNS

- Impact of Remote DNS on CDN Performance [IMC'12]
  $\approx$ 45000 users
- Security of Web Servers [IMC'14]
  $\approx$ 20000 websites
- DDoS Potential of DNSSec [IMC'14]
  $\approx$ 2.5 million domains
- Large-Scale DNS Measurement Infrastructure [IMC'16]
  $\approx$ 150 million domains
- Passive DNS Measurements [SAC'12]
  `it`-zone

Related Work

Studies on the Internet involving the DNS

- Impact of Remote DNS on CDN Performance [IMC'12]
  $\approx$ 45000 users
- Security of Web Servers [IMC'14]
  $\approx$ 20000 websites
- DDoS Potential of DNSSec [IMC'14]
  $\approx$ 2.5 million domains
- Large-Scale DNS Measurement Infrastructure [IMC'16]
  $\approx$ 150 million domains
- Passive DNS Measurements [SAC'12]
  `it`-zone
- Client's IPv6 Adoption [PAM'10]
  Subset of Google's users

Related Work

Studies on the Internet involving the DNS

- Impact of Remote DNS on CDN Performance [IMC'12]
  $\approx$ 45000 users
- Security of Web Servers [IMC'14]
  $\approx$ 20000 websites
- DDoS Potential of DNSSec [IMC'14]
  $\approx$ 2.5 million domains
- Large-Scale DNS Measurement Infrastructure [IMC'16]
  $\approx$ 150 million domains
- Passive DNS Measurements [SAC'12]
  `it`-zone
- Client's IPv6 Adoption [PAM'10]
  Subset of Google's users

Goals

1. **Enable performant large-scale DNS measurements**

Goals

1. **Enable performant large-scale DNS measurements**
   - Large scale:
     Hundreds of millions of domains

Goals

1. **Enable performant large-scale DNS measurements**
   - Large scale:
     Hundreds of millions of domains
   - Performance and Scalability:
     Hundreds of millions of DNS queries per day

Goals

1. **Enable performant large-scale DNS measurements**
   - Large scale:
     Hundreds of millions of domains
   - Performance and Scalability:
     Hundreds of millions of DNS queries per day
   - Enable several analyses:
     IPv6 Deployment, Port Scans with SNI,
     Cloud Mail Providers, ... $\Rightarrow$ Iterative measurements

Goals

1. **Enable performant large-scale DNS measurements**
   - Large scale:
     Hundreds of millions of domains
   - Performance and Scalability:
     Hundreds of millions of DNS queries per day
   - Enable several analyses:
     IPv6 Deployment, Port Scans with SNI,
     Cloud Mail Providers, ... $\Rightarrow$ Iterative measurements
   - Data processing:
     Store and access collected data efficiently

Goals

1. **Enable performant large-scale DNS measurements**
   - Large scale:
     Hundreds of millions of domains
   - Performance and Scalability:
     Hundreds of millions of DNS queries per day
   - Enable several analyses:
     IPv6 Deployment, Port Scans with SNI,
     Cloud Mail Providers, ... $\Rightarrow$ Iterative measurements
   - Data processing:
     Store and access collected data efficiently
2. **Case Studies**
   - Enable SNI for port scan based measurements

Goals

1. **Enable performant large-scale DNS measurements**
   - Large scale:
     Hundreds of millions of domains
   - Performance and Scalability:
     Hundreds of millions of DNS queries per day
   - Enable several analyses:
     IPv6 Deployment, Port Scans with SNI,
     Cloud Mail Providers, ... $\Rightarrow$ Iterative measurements
   - Data processing:
     Store and access collected data efficiently
2. **Case Studies**
   - Enable SNI for port scan based measurements
   - Identifying misconfigured domains

Goals

1. **Enable performant large-scale DNS measurements**
   - Large scale:
     Hundreds of millions of domains
   - Performance and Scalability:
     Hundreds of millions of DNS queries per day
   - Enable several analyses:
     IPv6 Deployment, Port Scans with SNI,
     Cloud Mail Providers, ... $\Rightarrow$ Iterative measurements
   - Data processing:
     Store and access collected data efficiently
2. **Case Studies**
   - Enable SNI for port scan based measurements
   - Identifying misconfigured domains
   - IPv6-capability study

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

- \+ Multiple processes
- \- Not all RR-types supported
- \- No iterative measurements

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported
- No iterative measurements
- Does not support multiple hosts natively

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

- \+ Multiple processes
- \- Not all RR-types supported
- \- No iterative measurements
- \- Does not support multiple hosts natively

Pycares (Python library)

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

- \+ Multiple processes
- \- Not all RR-types supported
- \- No iterative measurements
- \- Does not support multiple hosts natively

Pycares (Python library)

- \+ Easy-to-use, fast

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported
- No iterative measurements
- Does not support multiple hosts natively

Pycares (Python library)

+ Easy-to-use, fast
- Not all RR-types supported

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported
- No iterative measurements
- Does not support multiple hosts natively

Pycares (Python library)

+ Easy-to-use, fast
- Not all RR-types supported
- Does not include all information (e.g. TTL)

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported
- No iterative measurements
- Does not support multiple hosts natively

Pycares (Python library)

+ Easy-to-use, fast
- Not all RR-types supported
- Does not include all information (e.g. TTL)

Twisted Framework (Python framework)

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported
- No iterative measurements
- Does not support multiple hosts natively

Pycares (Python library)

+ Easy-to-use, fast
- Not all RR-types supported
- Does not include all information (e.g. TTL)

Twisted Framework (Python framework)

+ Wide range of RR-types, multiple RR-classes supported

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported
- No iterative measurements
- Does not support multiple hosts natively

Pycares (Python library)

+ Easy-to-use, fast
- Not all RR-types supported
- Does not include all information (e.g. TTL)

Twisted Framework (Python framework)

+ Wide range of RR-types, multiple RR-classes supported
- Complex framework $\rightarrow$ overhead?

Large-Scale DNS Resolution

Existing Tools and Libraries

ZDNS (Go)

+ Multiple processes
- Not all RR-types supported
- No iterative measurements
- Does not support multiple hosts natively

Pycares (Python library)

+ Easy-to-use, fast
- Not all RR-types supported
- Does not include all information (e.g. TTL)

Twisted Framework (Python framework)

+ Wide range of RR-types, multiple RR-classes supported
- Complex framework → overhead?
- Performance?

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework
- Support multiple processes

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework
- Support multiple processes
- **Multiple hosts**

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework
- Support multiple processes
- **Multiple hosts**
- ZeroMQ

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework
- Support multiple processes
- **Multiple hosts**
- ZeroMQ
- JSON output

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework
- Support multiple processes
- **Multiple hosts**
- ZeroMQ
- JSON output
- Configurability: Rate Limiting, Server Load Limiting, . . .

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework
- Support multiple processes
- **Multiple hosts**
- ZeroMQ
- JSON output
- Configurability: Rate Limiting, Server Load Limiting, ...
- **Reactive Queuing**

Large-Scale DNS Resolution

TDNS (TwistedDNS)

- Uses the Twisted Framework
- Support multiple processes
- **Multiple hosts**
- ZeroMQ
- JSON output
- Configurability: Rate Limiting, Server Load Limiting, ...
- **Reactive Queuing**

```
cat domainlist.txt | ./tdns -ns 8.8.8.8 -t A
```

Large-Scale DNS Resolution

Performance: TDNS vs. ZDNS

Large-Scale DNS Resolution

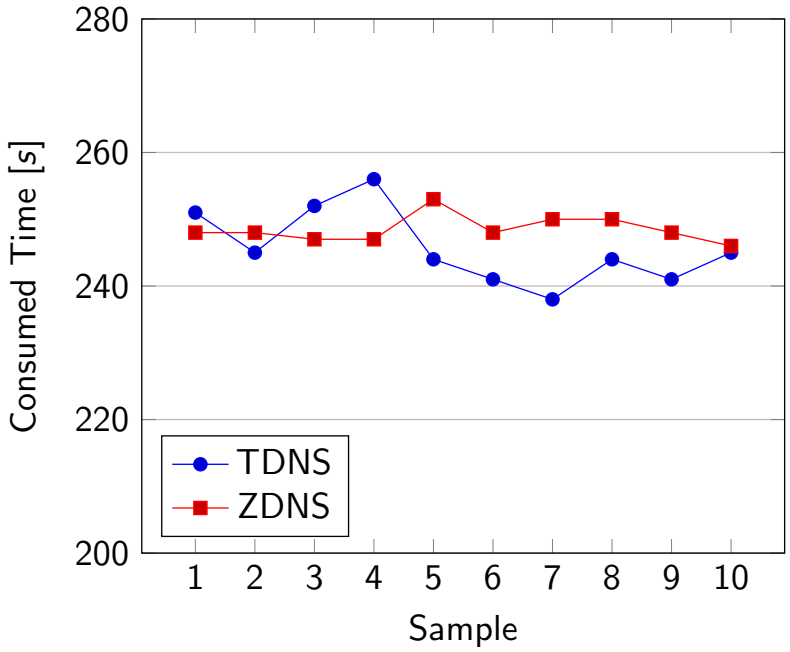
Performance: TDNS vs. ZDNS

- Consumed Time (1 million queries)
- Success Rate

Large-Scale DNS Resolution

Performance: TDNS vs. ZDNS

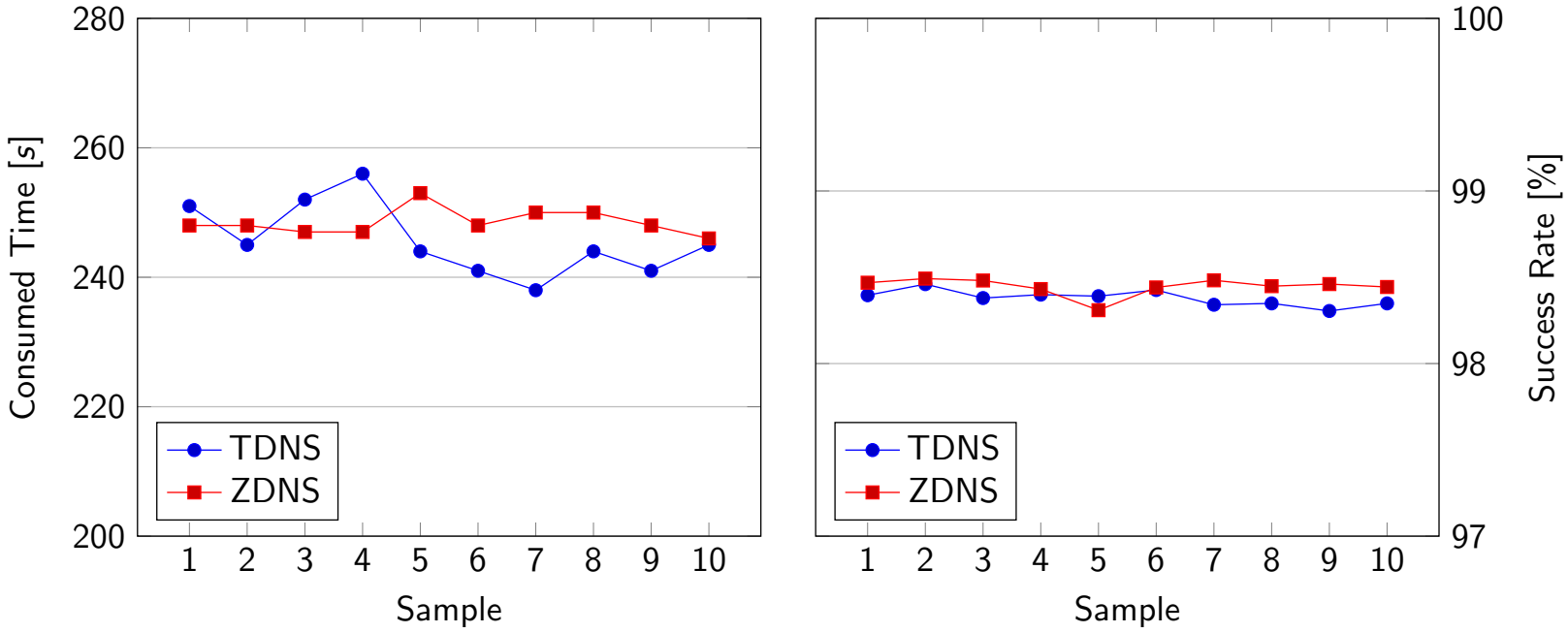
- Consumed Time (1 million queries)
- Success Rate



Large-Scale DNS Resolution

Performance: TDNS vs. ZDNS

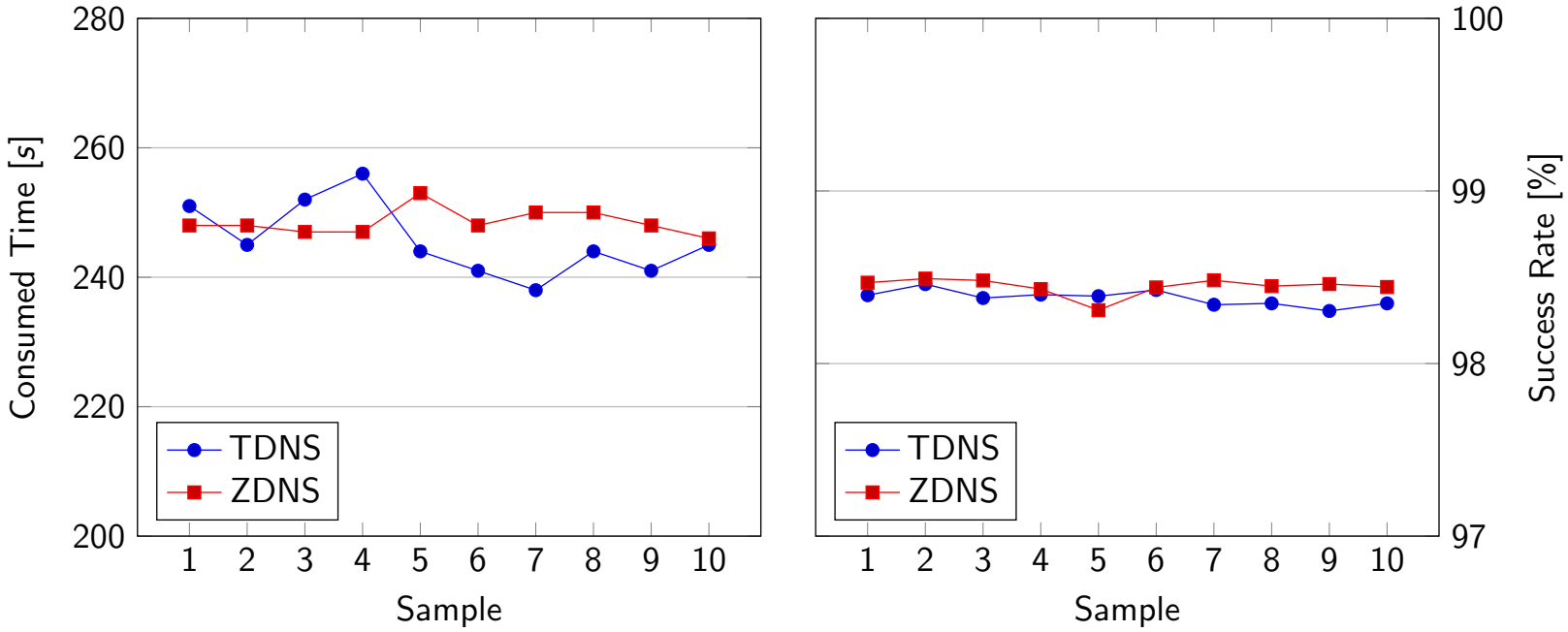
- Consumed Time (1 million queries)
- Success Rate



Large-Scale DNS Resolution

Performance: TDNS vs. ZDNS

- Consumed Time (1 million queries)
- Success Rate

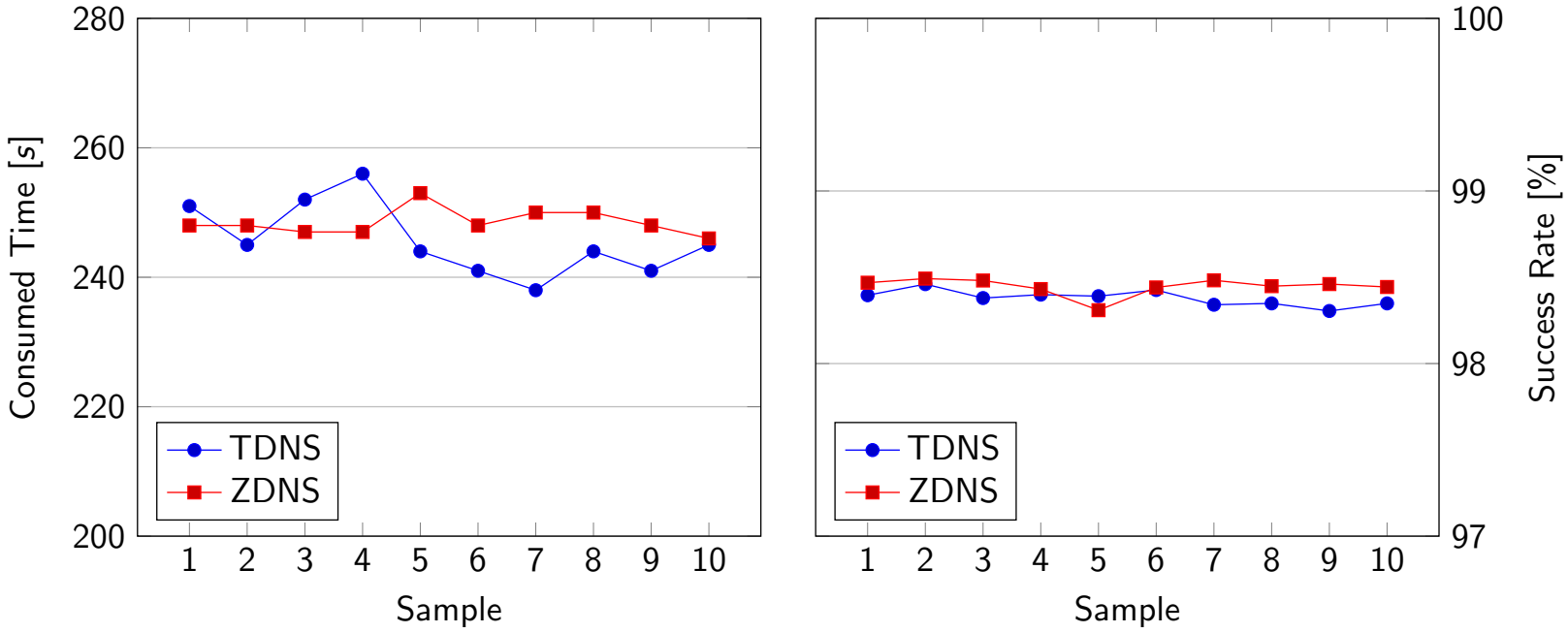


$249 \frac{\mu s}{succQ}$ vs. $252 \frac{\mu s}{succQ}$

Large-Scale DNS Resolution

Performance: TDNS vs. ZDNS

- Consumed Time (1 million queries)
- Success Rate



$249 \frac{\mu s}{succQ}$ vs. $252 \frac{\mu s}{succQ}$ $\Rightarrow$ Comparable performance

Use Cases

What can we do with this now?

Use Cases

What can we do with this now?
Use DNS information to...

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements
   - SNI for port scan based measurements

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements
   - SNI for port scan based measurements
2. ...draw conclusions about the Internet

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements
   - SNI for port scan based measurements
2. ...draw conclusions about the Internet
   - Identify misconfigured domains

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements
   - SNI for port scan based measurements
2. ...draw conclusions about the Internet
   - Identify misconfigured domains
   - Investigate IPv6 deployment

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements
   - SNI for port scan based measurements
2. ...draw conclusions about the Internet
   - Identify misconfigured domains
   - Investigate IPv6 deployment
   - Cloud Mail Providers, CDNs, Security, ...

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements
   - SNI for port scan based measurements
2. ...draw conclusions about the Internet
   - Identify misconfigured domains
   - Investigate IPv6 deployment
   - Cloud Mail Providers, CDNs, Security, ...

Required: **Storing** and **querying** local DNS data efficiently

Use Cases

What can we do with this now?

Use DNS information to...

1. ...improve other measurements
   - SNI for port scan based measurements
2. ...draw conclusions about the Internet
   - Identify misconfigured domains
   - Investigate IPv6 deployment
   - Cloud Mail Providers, CDNs, Security, ...

Required: **Storing** and **querying** local DNS data efficiently

- LevelDB, Radix Tree, Hashmap, SQLite, PostgreSQL, ...

Server Name Indication

Problem

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...),
  Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname?

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?
  - Not always identical to "forward" mapping, missing, ...

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?
  - Not always identical to "forward" mapping, missing, ...

Solution

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?
  - Not always identical to "forward" mapping, missing, ...

Solution

- Scan TLD-zone(s)

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?
  - Not always identical to "forward" mapping, missing, ...

Solution

- Scan TLD-zone(s): $\approx$ 9 hours for `com`-zone

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?
  - Not always identical to "forward" mapping, missing, ...

Solution

- Scan TLD-zone(s): $\approx$ 9 hours for `com`-zone
- Use a Hashmap to reverse the forward mapping

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?
  - Not always identical to "forward" mapping, missing, ...

Solution

- Scan TLD-zone(s): $\approx$ 9 hours for `com`-zone
- Use a Hashmap to reverse the forward mapping
- $\approx$ 2.1 minutes for 120 million lookups (Port 80)

Server Name Indication

Problem

- Port Scans using ZMap, ZGrab, nmap, ...
- Investigate TCP parameters (Initial Window, ...), Web Server Options (Certificates, Contents, ...)
- SNI: TLS extension that allows passing a Server Name
- Missing SNI: Connection might get closed immediately, "default" content $\Rightarrow$ Undesired behavior
- IP address $\rightarrow$ hostname? Reverse DNS (`PTR`)?
  - Not always identical to "forward" mapping, missing, ...

Solution

- Scan TLD-zone(s): $\approx$ 9 hours for `com`-zone
- Use a Hashmap to reverse the forward mapping
- $\approx$ 2.1 minutes for 120 million lookups (Port 80)

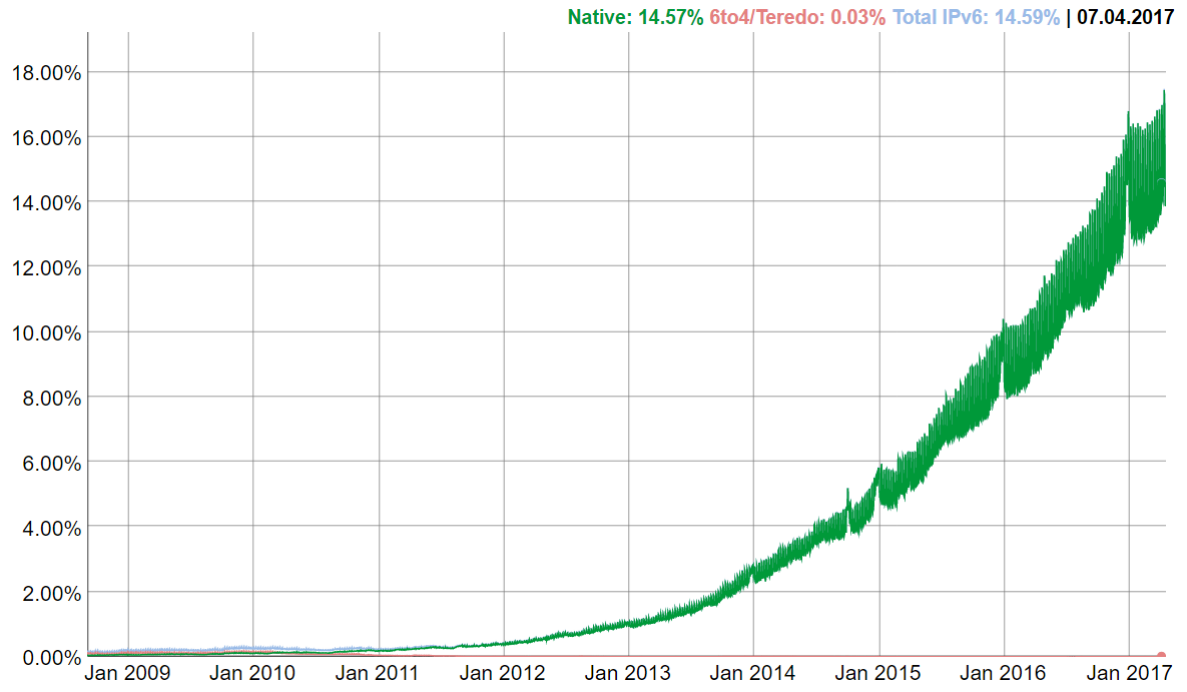
IPv6 Deployment

IPv6 Deployment

Don't we already know that?

IPv6 Deployment

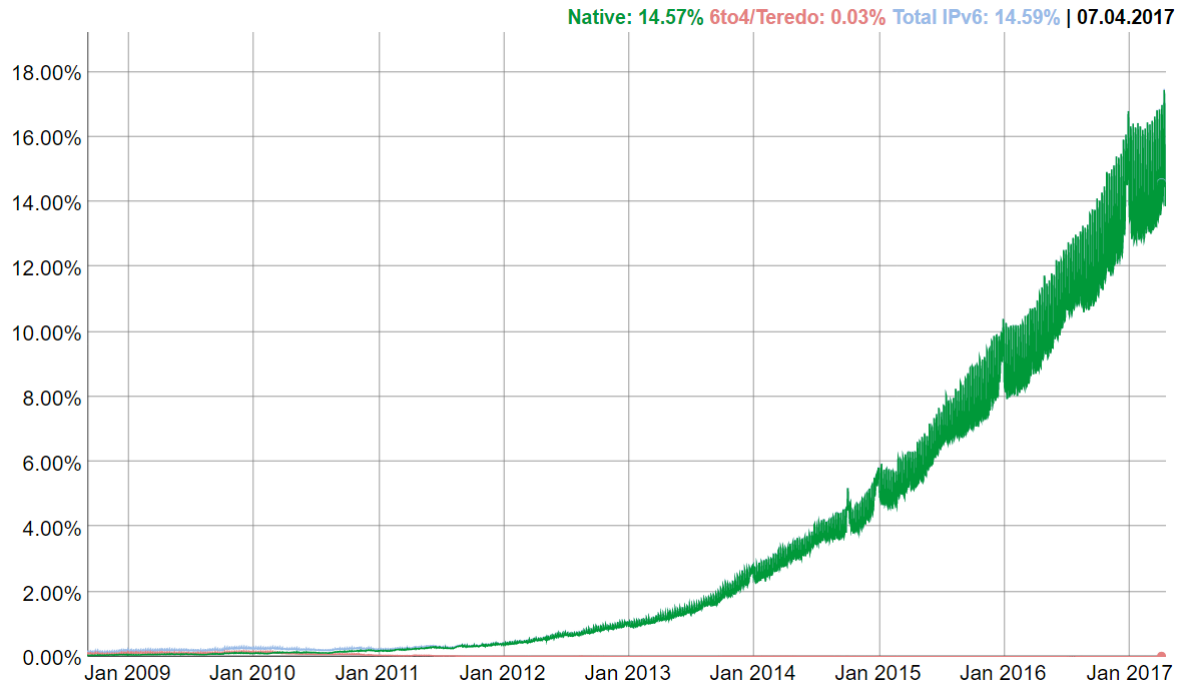
Don't we already know that? Yes, for the Client's side



`https://www.google.de/ipv6/statistics.html`

IPv6 Deployment

Don't we already know that? Yes, for the Client's side



`https://www.google.de/ipv6/statistics.html`

What about the Infrastructure?

IPv6-Capability Study

Problem

IPv6-Capability Study

Problem

- Domain: More than just a `AAAA`-record

IPv6-Capability Study

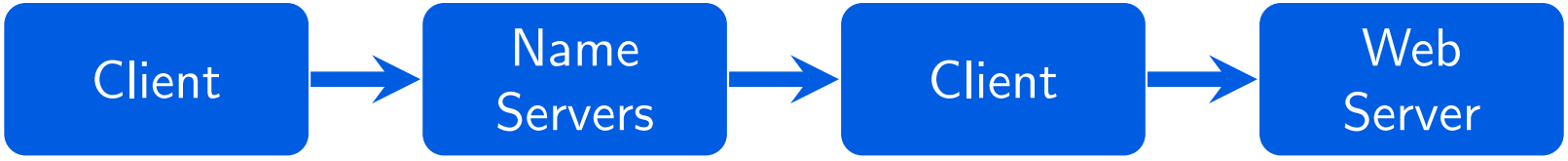
Problem

- Domain: More than just a `AAAA`-record
- Mail Exchangers, Name Servers, Subdomains, . . .

IPv6-Capability Study

Problem

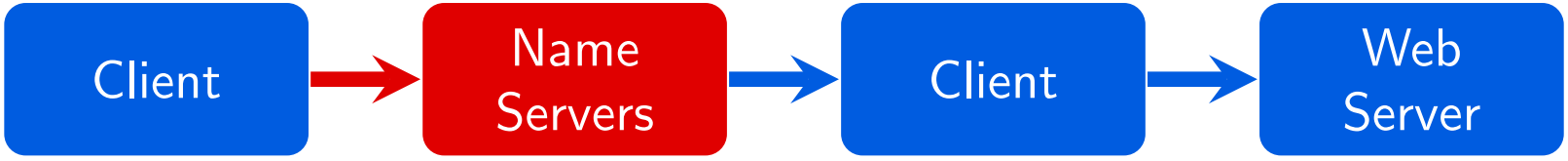
- Domain: More than just a `AAAA`-record
- Mail Exchangers, Name Servers, Subdomains, . . .



IPv6-Capability Study

Problem

- Domain: More than just a `AAAA`-record
- Mail Exchangers, Name Servers, Subdomains, . . .

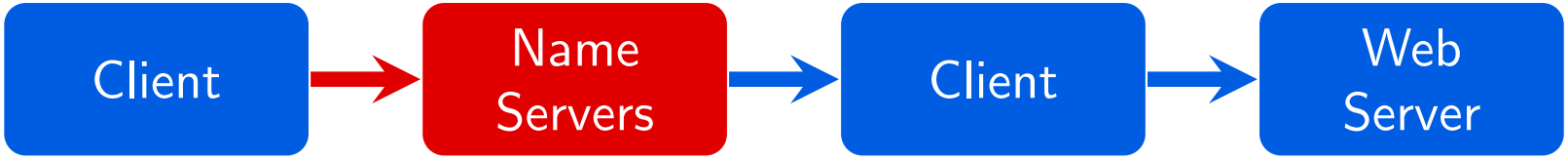


- Not IPv6-capable Name Servers affect other aspects

IPv6-Capability Study

Problem

- Domain: More than just a `AAAA`-record
- Mail Exchangers, Name Servers, Subdomains, . . .

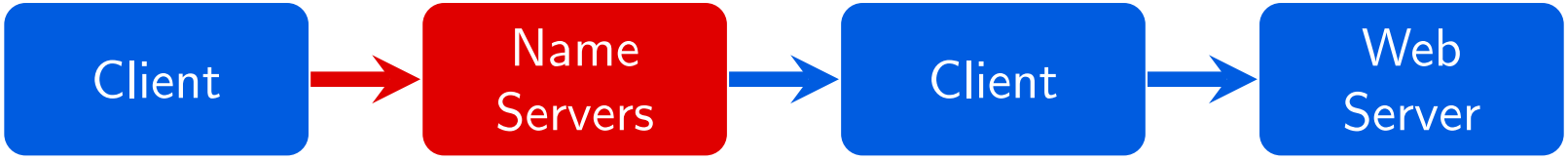


- Not IPv6-capable Name Servers affect other aspects
  $\Rightarrow$ Investigate multiple aspects

IPv6-Capability Study

Problem

- Domain: More than just a `AAAA`-record
- Mail Exchangers, Name Servers, Subdomains, . . .



- Not IPv6-capable Name Servers affect other aspects
  $\Rightarrow$ Investigate multiple aspects

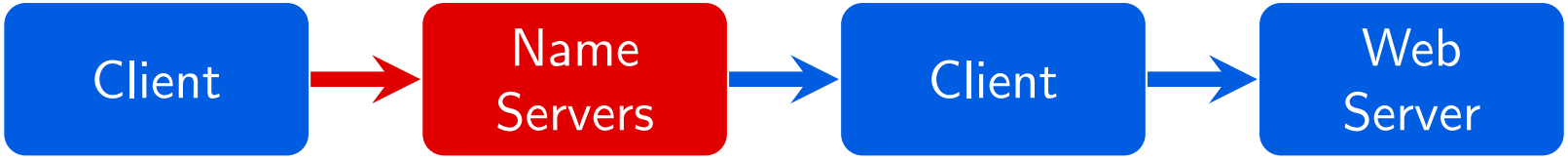
Approach

- Domain itself, Mail Exchangers, Name Servers, `www`-subdomain

IPv6-Capability Study

Problem

- Domain: More than just a `AAAA`-record
- Mail Exchangers, Name Servers, Subdomains, . . .

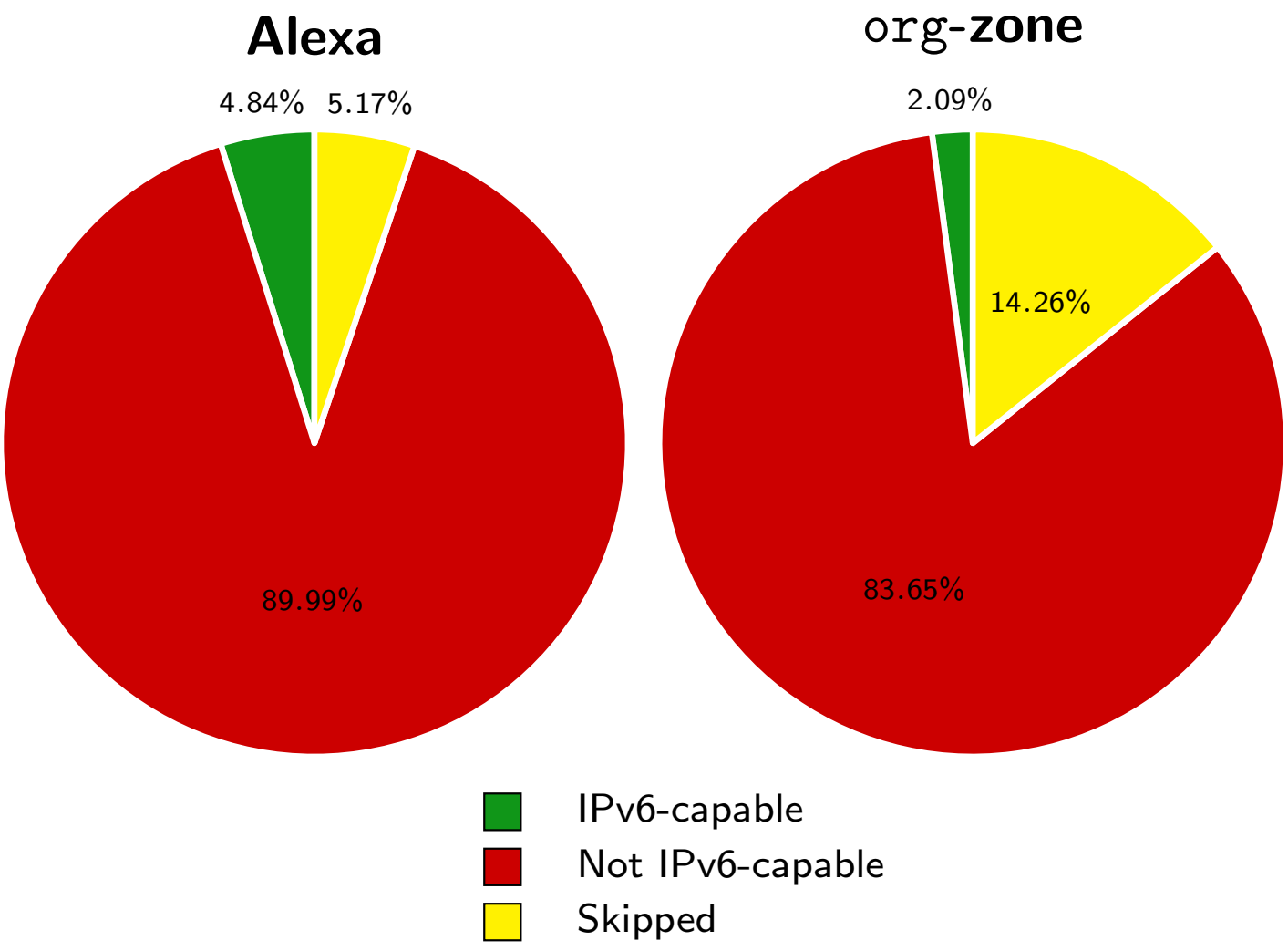


- Not IPv6-capable Name Servers affect other aspects
  $\Rightarrow$ Investigate multiple aspects

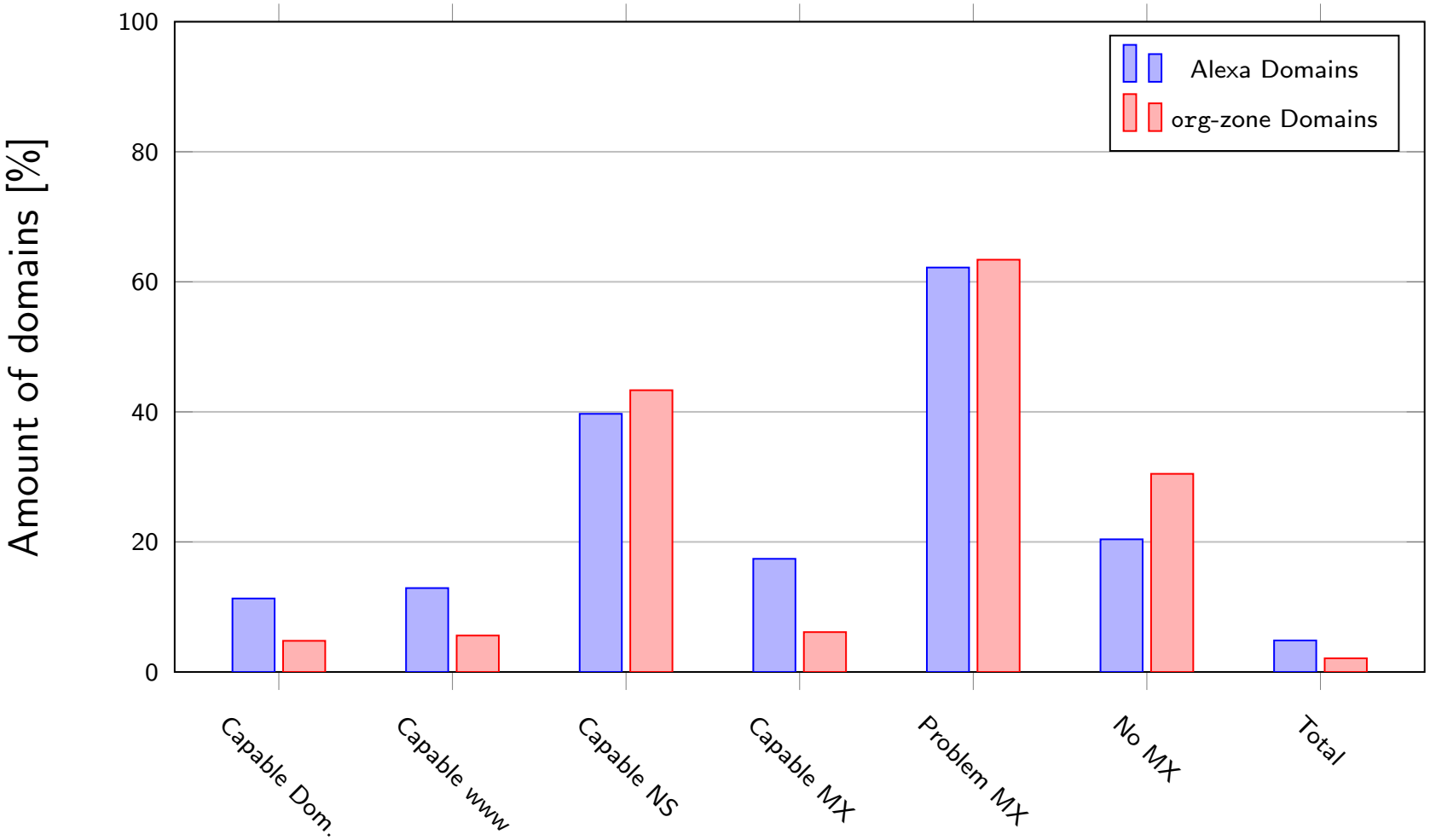
Approach

- Domain itself, Mail Exchangers, Name Servers, `www`-subdomain
- Alexa Top 1M & complete `org`-zone

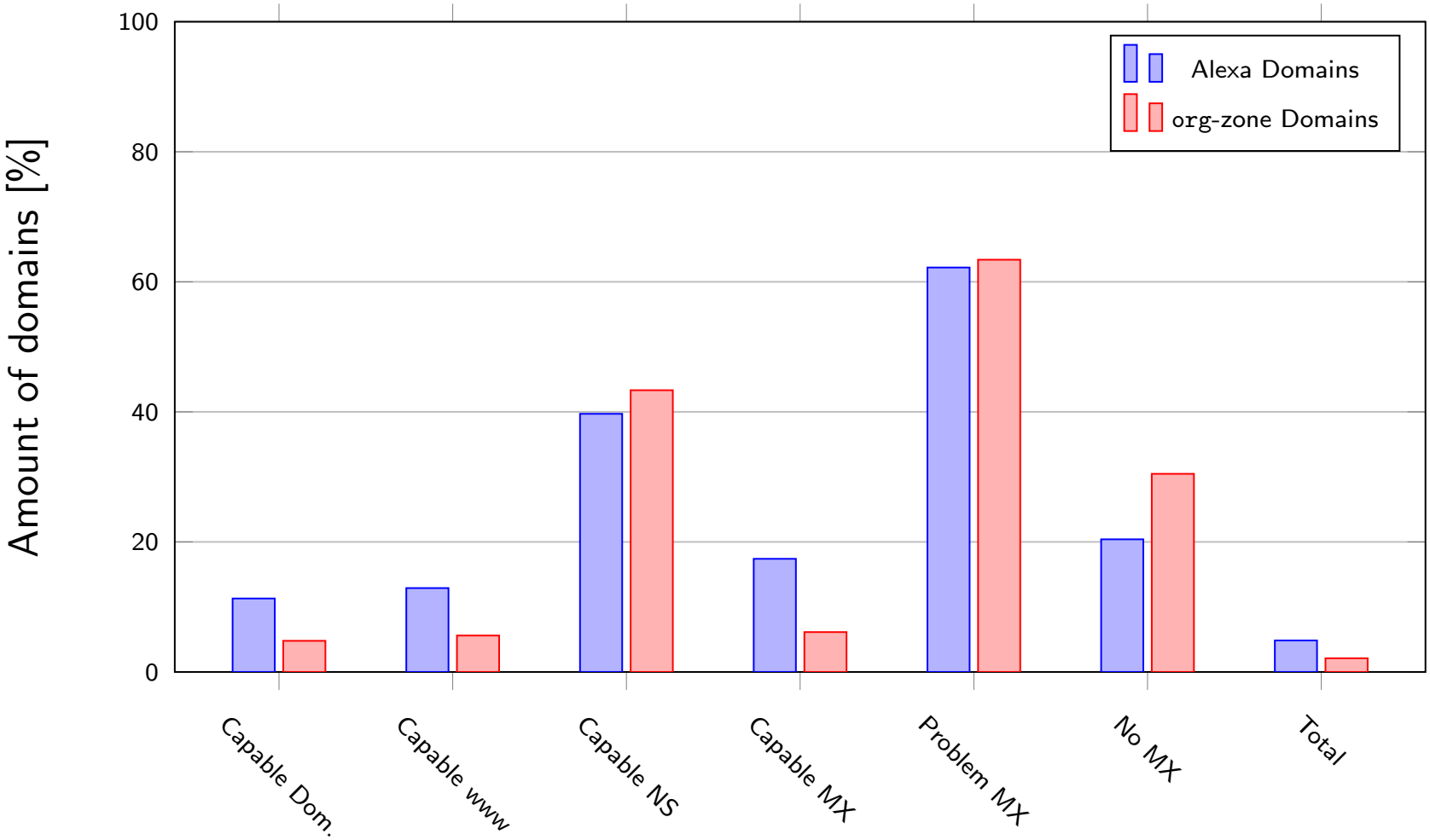
IPv6-Capability Study



IPv6-Capability Study



IPv6-Capability Study



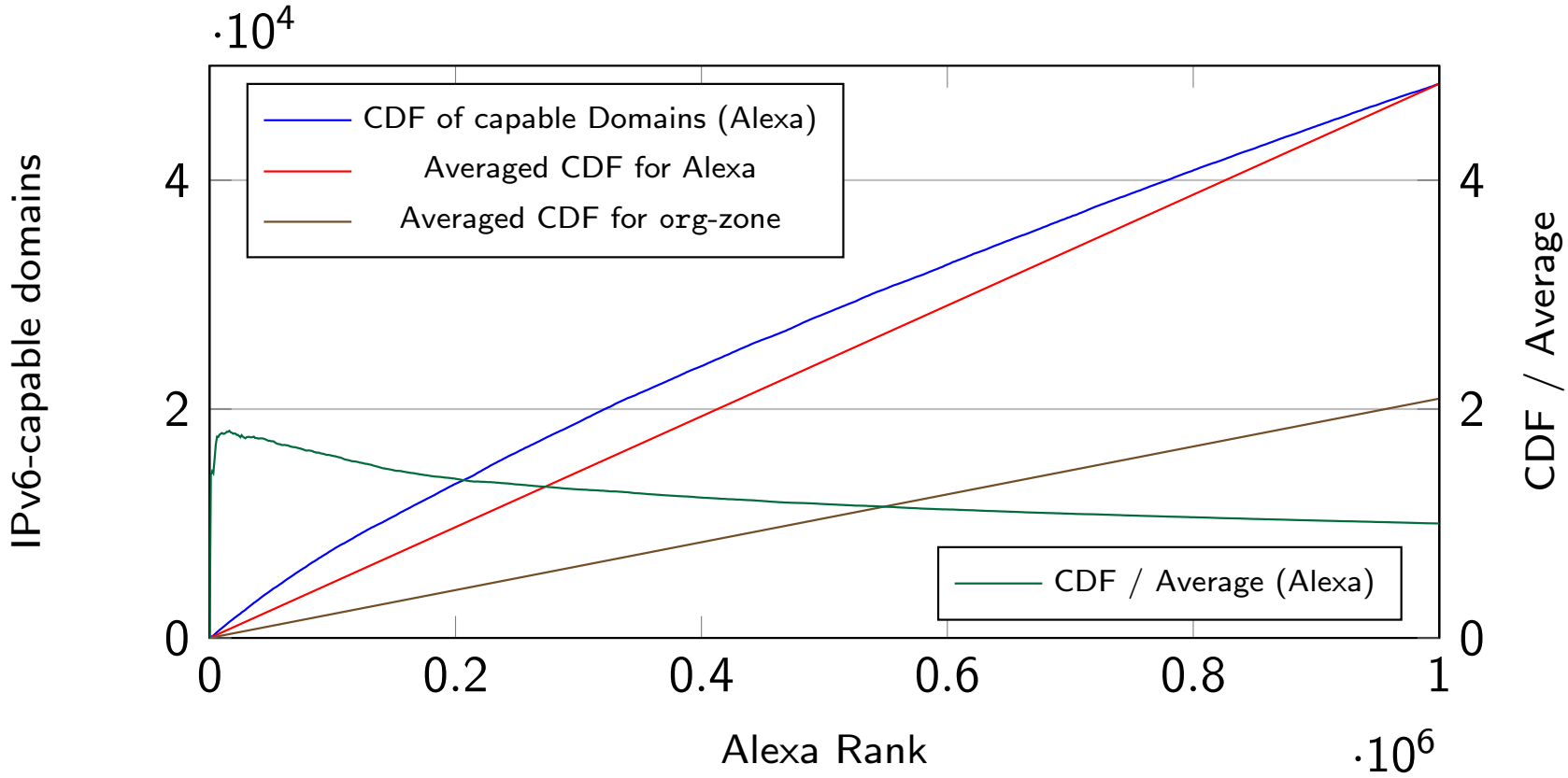
Misconfiguration or not IPv6-capable **infrastructure**. . . ?

IPv6-Capability Study

Is IPv6-capability linked to a domain's popularity?

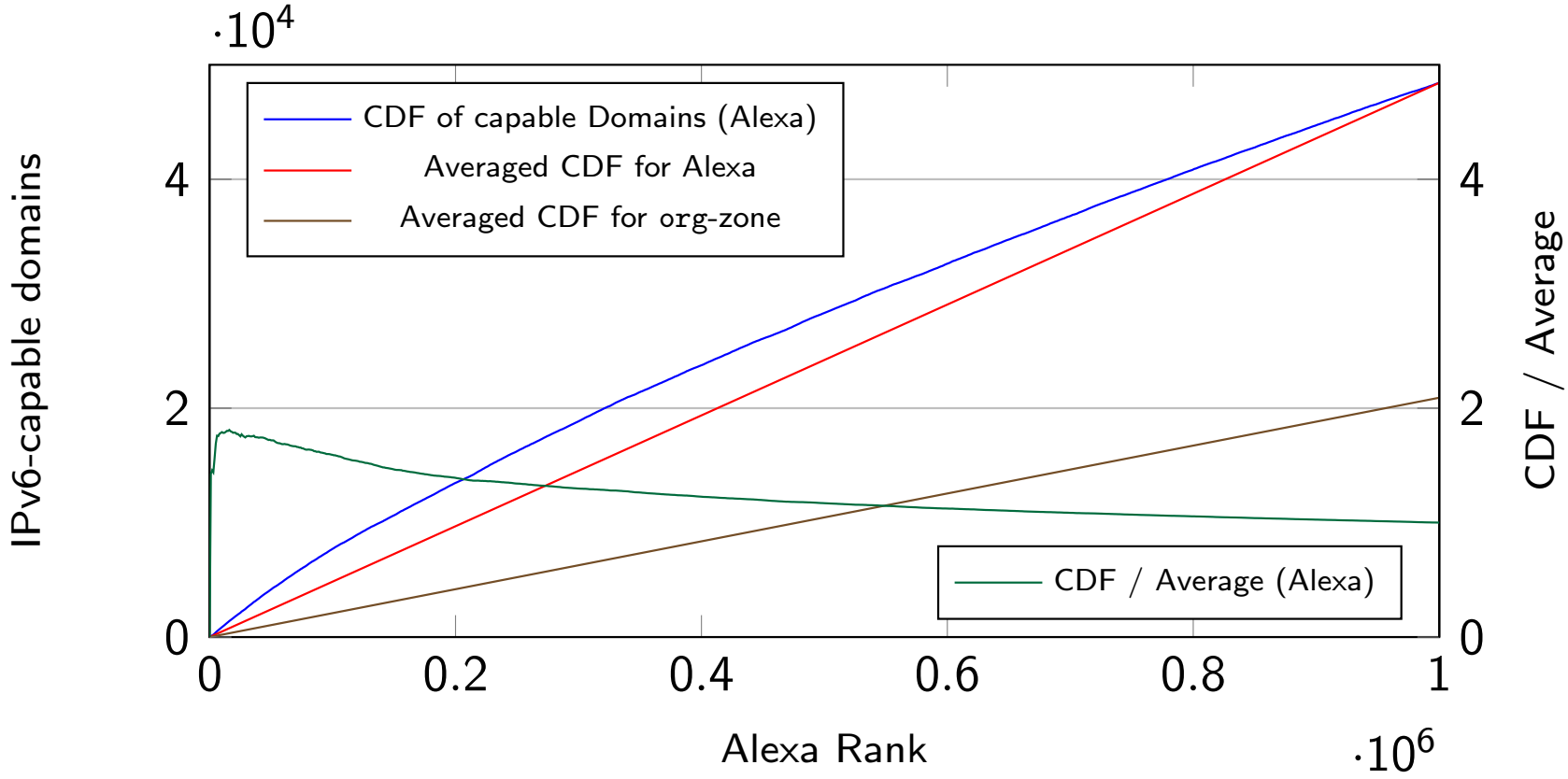
IPv6-Capability Study

Is IPv6-capability linked to a domain's popularity?



IPv6-Capability Study

Is IPv6-capability linked to a domain's popularity?



So the "big players" are v6-ready, right?

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...
- Only 18 out of the top 300 domains are IPv6-ready (6%)

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...
- Only 18 out of the top 300 domains are IPv6-ready (6%)

Which aspects are affected? (NS, MX, ...)

IPv6-Capability Study

Global Top Sites

- Google, Facebook, MSN, Yahoo, Bing, Twitter, Wikipedia, Amazon, Linkedin, ...
- Only 18 out of the top 300 domains are IPv6-ready (6%)

Which aspects are affected? (NS, MX, ...)
Is this just a **misconfiguration**?

Google's IPv6-Capability

The domain `google.com`

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record

`AAAA`-record for `www`

`AAAA`-record for any `MX`

`AAAA`-record for any `NS`

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record ✓

`AAAA`-record for `www`

`AAAA`-record for any `MX`

`AAAA`-record for any `NS`

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record ✓

`AAAA`-record for `www` ✓

`AAAA`-record for any `MX`

`AAAA`-record for any `NS`

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record	✓
`AAAA`-record for `www`	✓
`AAAA`-record for any `MX`	✓
`AAAA`-record for any `NS`	

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record	✓
`AAAA`-record for `www`	✓
`AAAA`-record for any `MX`	✓
`AAAA`-record for any `NS`	✗

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record	✓
`AAAA`-record for `www`	✓
`AAAA`-record for any `MX`	✓
`AAAA`-record for any `NS`	✗

	IPv4 address	**`AAAA`-record provided**	**ASN**
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record	✓
`AAAA`-record for `www`	✓
`AAAA`-record for any `MX`	✓
`AAAA`-record for any `NS`	✗

	IPv4 address	**`AAAA`-record provided**	**ASN**
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record	✓
`AAAA`-record for `www`	✓
`AAAA`-record for any `MX`	✓
`AAAA`-record for any `NS`	✗

	IPv4 address	`AAAA`-record provided	ASN
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record	✓
`AAAA`-record for `www`	✓
`AAAA`-record for any `MX`	✓
`AAAA`-record for any `NS`	✗

	IPv4 address	**`AAAA`-record provided**	**ASN**
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record ✓

`AAAA`-record for `www` ✓

`AAAA`-record for any `MX` ✓

`AAAA`-record for any `NS` ✗

	IPv4 address	**`AAAA`-record provided**	**ASN**
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record ✓

`AAAA`-record for `www` ✓

`AAAA`-record for any `MX` ✓

`AAAA`-record for any `NS` ✗

	IPv4 address	**`AAAA`-record provided**	**ASN**
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

⇒ Configuration mistake? Fixable?

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record ✓

`AAAA`-record for `www` ✓

`AAAA`-record for any `MX` ✓

`AAAA`-record for any `NS` ✗

	IPv4 address	**`AAAA`-record provided**	**ASN**
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

⇒ Configuration mistake? Fixable?

Ask Google! ☺

Google's IPv6-Capability

The domain `google.com`

`AAAA`-record ✓

`AAAA`-record for `www` ✓

`AAAA`-record for any `MX` ✓

`AAAA`-record for any `NS` ✗

	IPv4 address	**`AAAA`-record provided**	**ASN**
`google.com`	`172.217.22.238`	Yes	15169
`ns1.google.com`	`216.239.32.10`	No	15169
`ns3.google.com`	`216.239.36.10`	No	15169
`ns3ds.google.com`	`216.239.36.10`	Yes	15169

⇒ Configuration mistake? Fixable?

Ask Google! ☺

No answer yet...

IPv6-Capability Study

Summary

IPv6-Capability Study

Summary

- Only $\approx 3\%$ of domains would be usable in an IPv6-only Internet

IPv6-Capability Study

Summary

- Only $\approx 3\%$ of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support

IPv6-Capability Study

Summary

- Only $\approx$ 3% of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support
- More than 40% use IPv6-capable name servers

IPv6-Capability Study

Summary

- Only $\approx 3\%$ of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support
- More than 40% use IPv6-capable name servers
- 10% to 60% already use IPv6-capable infrastructure (“fixable”)

IPv6-Capability Study

Summary

- Only $\approx 3\%$ of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support
- More than 40% use IPv6-capable name servers
- 10% to 60% already use IPv6-capable infrastructure ("fixable")
- 95% of `org`-domains use 5% of name server providers

IPv6-Capability Study

Summary

- Only $\approx$ 3% of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support
- More than 40% use IPv6-capable name servers
- 10% to 60% already use IPv6-capable infrastructure ("fixable")
- 95% of `org`-domains use 5% of name server providers
- 80% of `org`-domains use 20% of cloud mail providers
  - Most used: Go Daddy Operating Company, LLC

IPv6-Capability Study

Summary

- Only $\approx$ 3% of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support
- More than 40% use IPv6-capable name servers
- 10% to 60% already use IPv6-capable infrastructure ("fixable")
- 95% of `org`-domains use 5% of name server providers
- 80% of `org`-domains use 20% of cloud mail providers
  - Most used: Go Daddy Operating Company, LLC

$\Rightarrow$ Small amount of providers affect large number of domains

IPv6-Capability Study

Summary

- Only $\approx$ 3% of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support
- More than 40% use IPv6-capable name servers
- 10% to 60% already use IPv6-capable infrastructure ("fixable")
- 95% of `org`-domains use 5% of name server providers
- 80% of `org`-domains use 20% of cloud mail providers
  - Most used: Go Daddy Operating Company, LLC

$\Rightarrow$ Small amount of providers affect large number of domains

There's still much to do...

IPv6-Capability Study

Summary

- Only $\approx 3\%$ of domains would be usable in an IPv6-only Internet
- Even the most prominent domains lack of IPv6 support
- More than 40% use IPv6-capable name servers
- 10% to 60% already use IPv6-capable infrastructure ("fixable")
- 95% of `org`-domains use 5% of name server providers
- 80% of `org`-domains use 20% of cloud mail providers
  - Most used: Go Daddy Operating Company, LLC

  $\Rightarrow$ Small amount of providers affect large number of domains

There's still much to do...
Worth repeating and improving these studies!

Conclusion and Future Work

Conclusion

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

- Improve TDNS

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

- Improve TDNS
- Share data

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

- Improve TDNS
- Share data
- Rate SNI performance and usefulness

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

- Improve TDNS
- Share data
- Rate SNI performance and usefulness
- Improve IPv6-capability study

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

- Improve TDNS
- Share data
- Rate SNI performance and usefulness
- Improve IPv6-capability study
  - Investigate more TLDs

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

- Improve TDNS
- Share data
- Rate SNI performance and usefulness
- Improve IPv6-capability study
  - Investigate more TLDs
  - Validate IPv6 addresses

Conclusion and Future Work

Conclusion

- Large-scale DNS measurements
- Data processing and evaluation
- Add SNI for port scan based measurements
- Identify misconfigured domains
- Rate the IPv6-capability of domains
- Cloud Mail Providers, CDNs, ...

Future Work

- Improve TDNS
- Share data
- Rate SNI performance and usefulness
- Improve IPv6-capability study
  - Investigate more TLDs
  - Validate IPv6 addresses
  - Improve casual analysis of non-capable domains

Thank You!

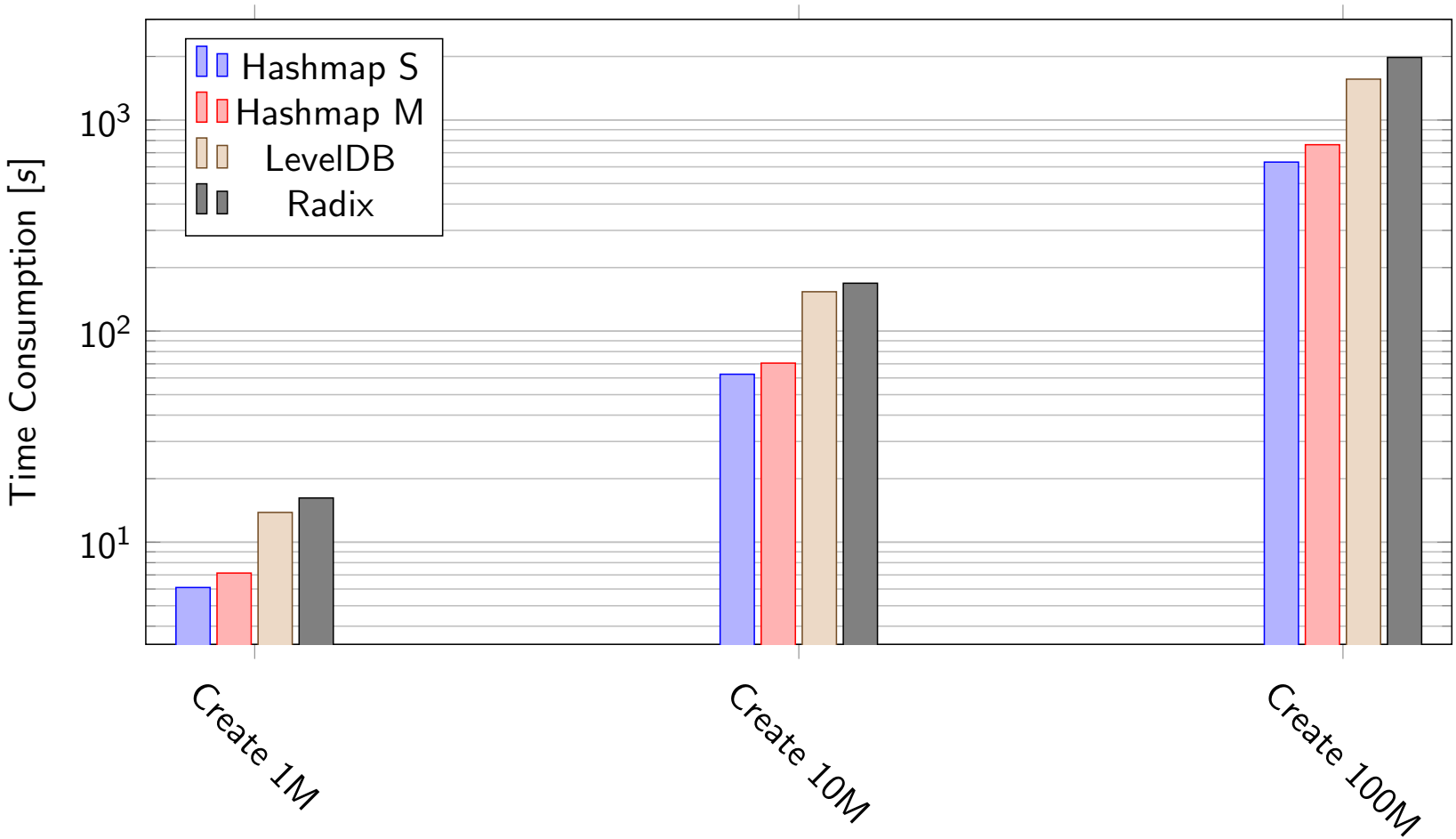
Thank you for your attention!

Do you have any questions?

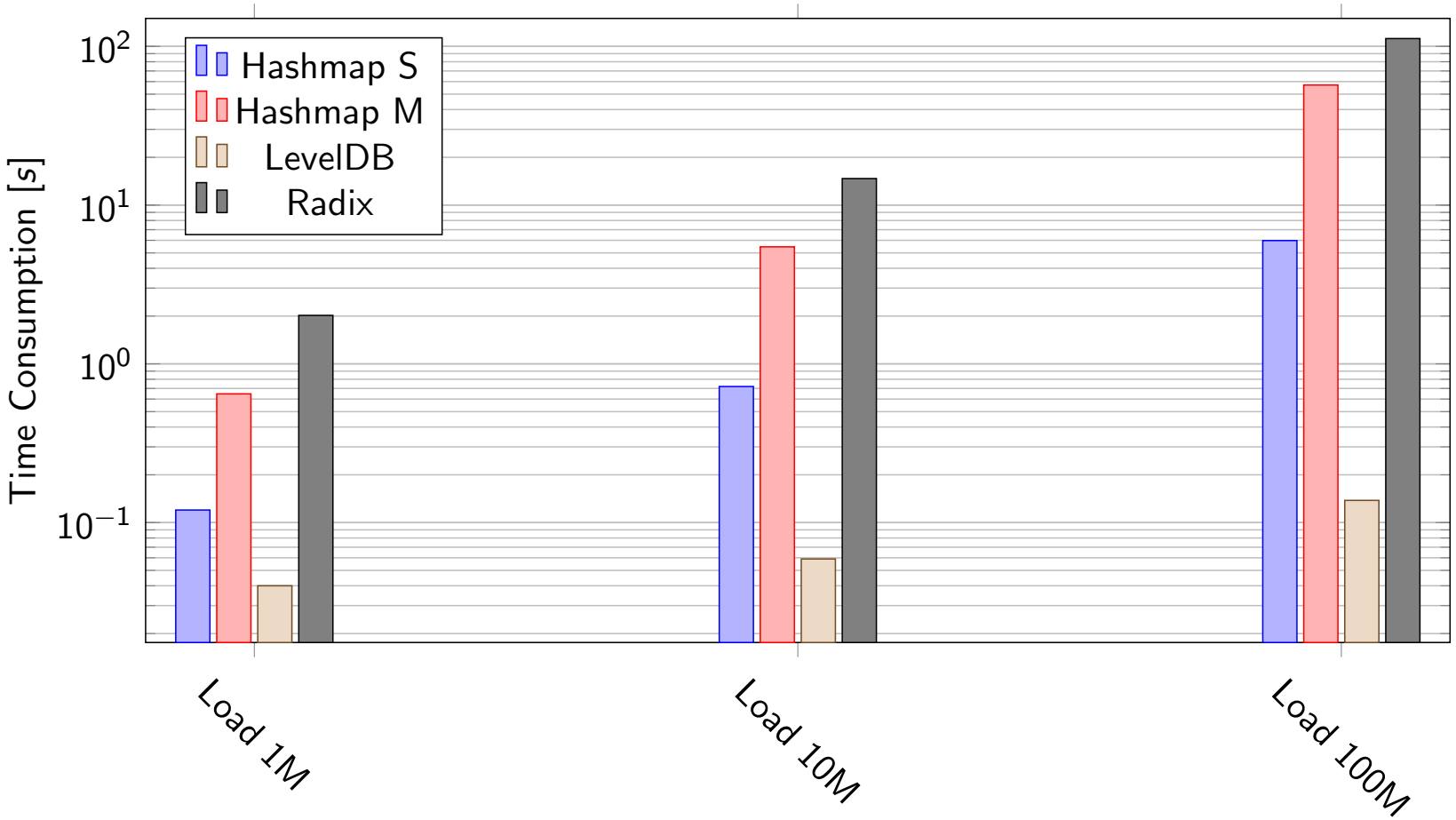
A: Reactive Queuing

```
{
    "rules": [
        {
            "desc": "AAAA for all A Records",
            "status": ["NOERROR"],
            "type": ["A"],
            "cont": [],
            "ncont": [],
            "format": [
                "{0} AAAA"
            ],
            "flags": [],
            "nflags": ["@ns", "@mx"]
        },
        {
            "desc": "MX for all A Records",
            "status": ["NOERROR"],
            "type": ["A"],
            "cont": [],
            "ncont": ["www."],
            "format": [
                "{0} MX"
            ],
            "flags": [],
            "nflags": ["@mx", "@ns"]
        },
    ...
    ]
}
```

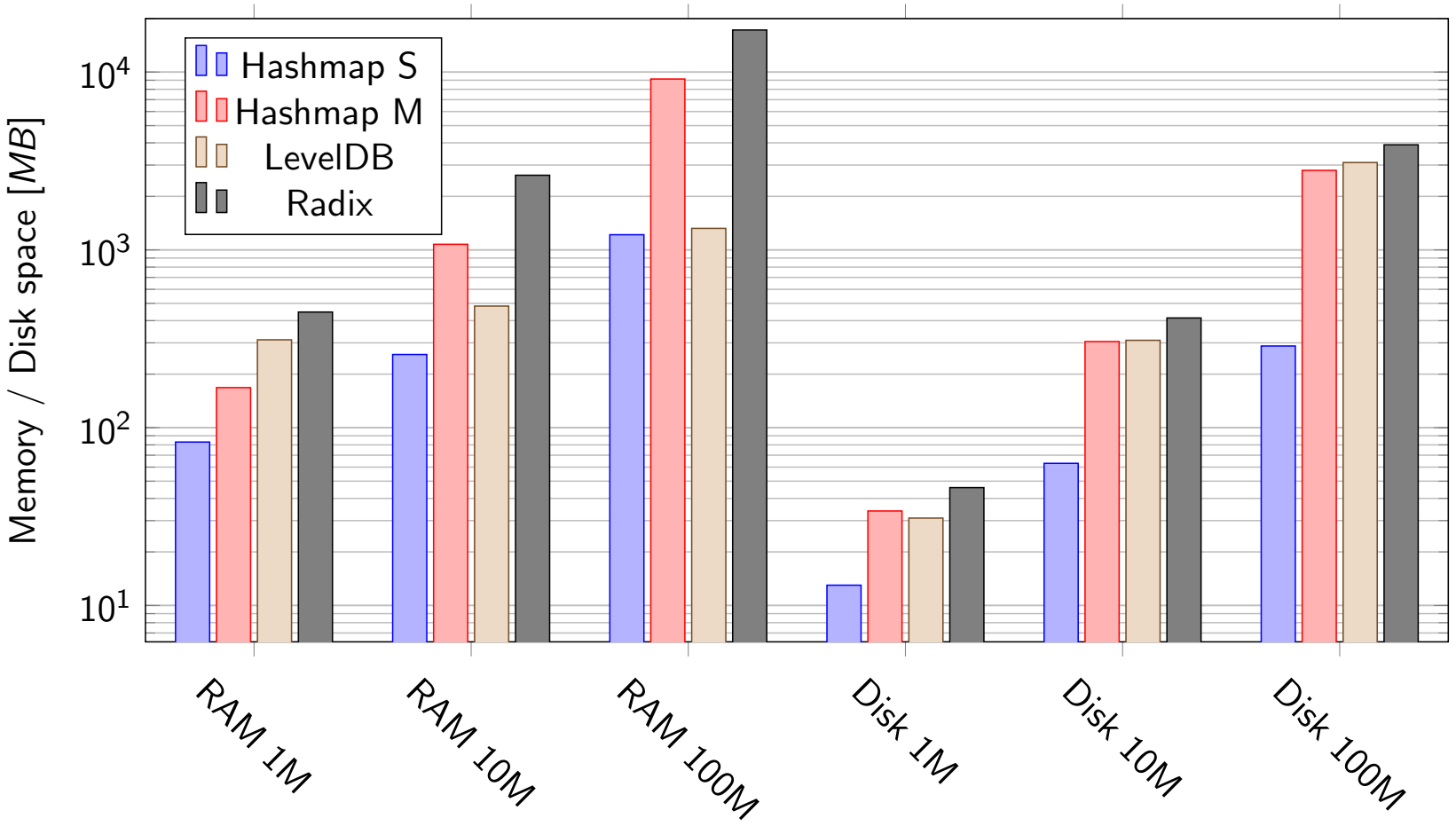
A: DB Create Performance



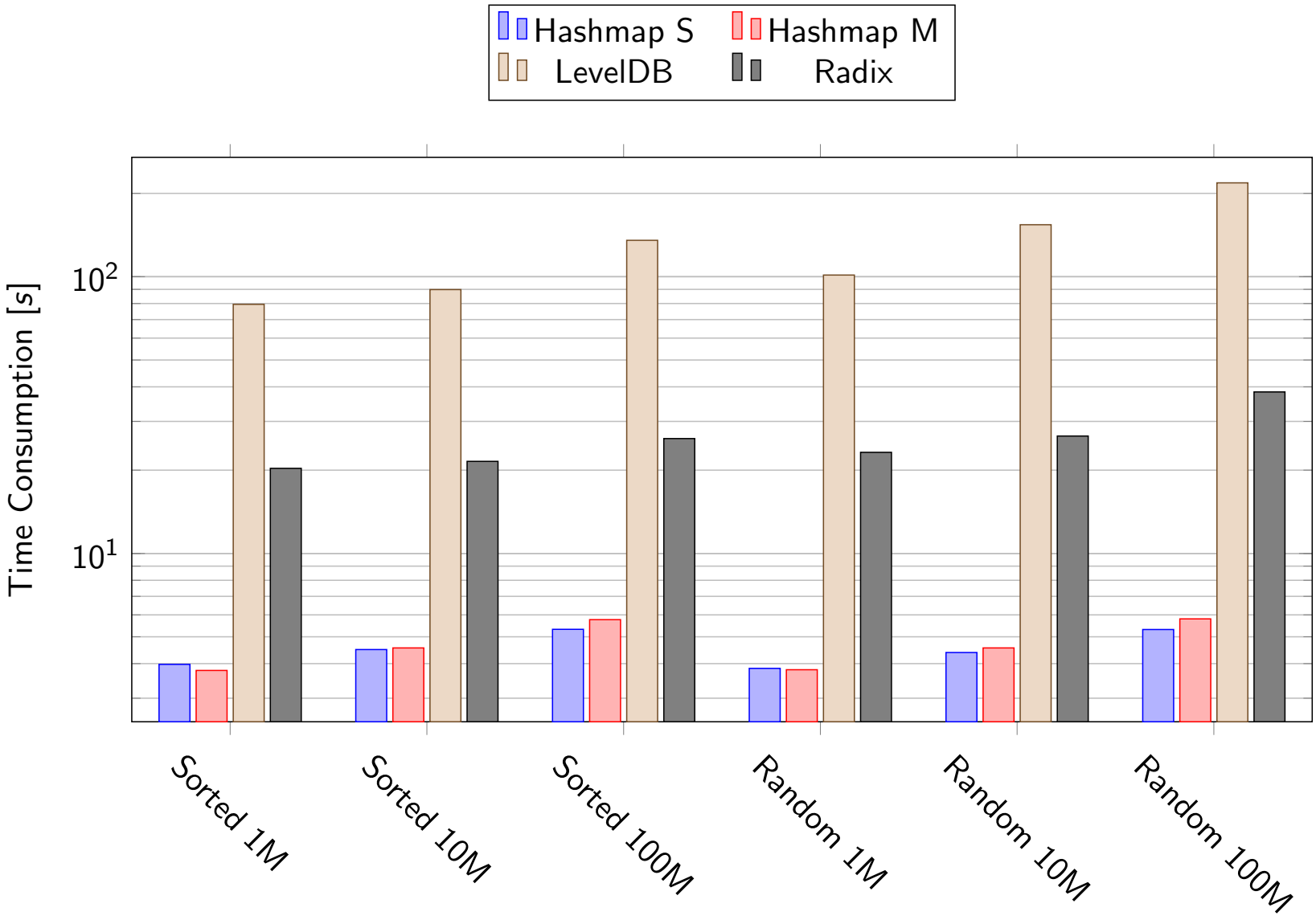
A: DB Load Performance



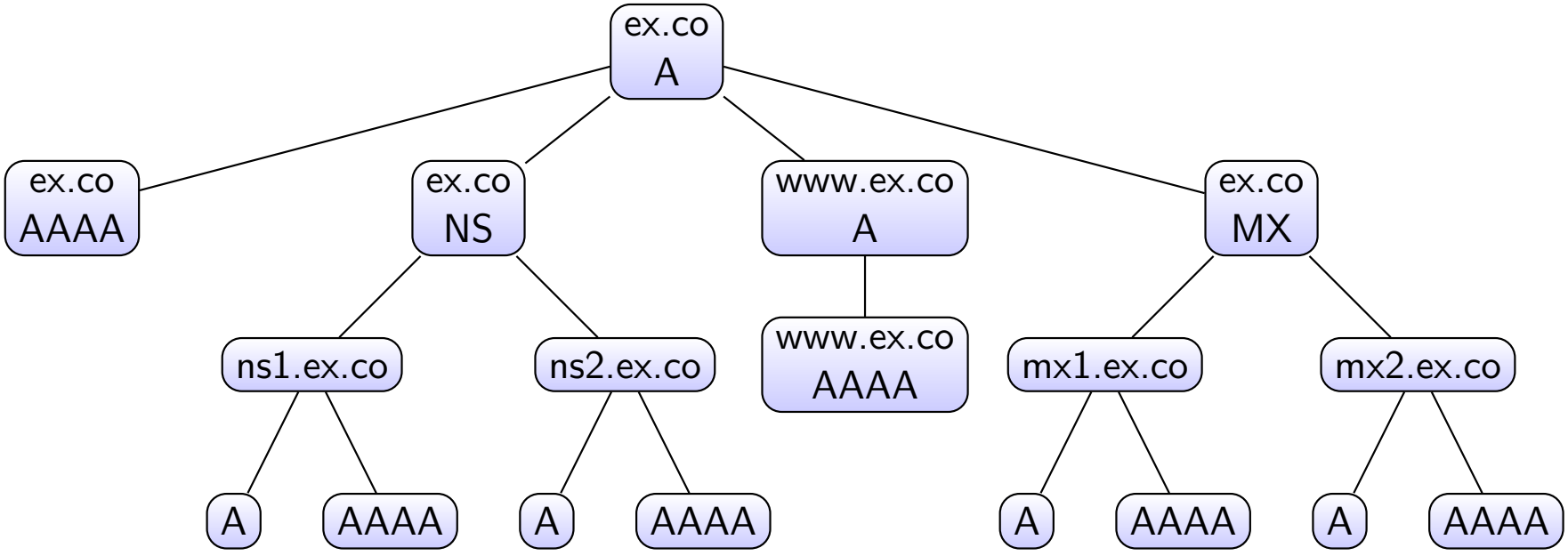
A: DB Memory Requirements



A: DB Query Performance



A: IPv6 Lookup Tree



A: MX Distribution (Org)

POS	Name (SLD)	V6	V4	V6 All	V4 All	DNUM	NSNUM
0	secureserver.net	False	True	False	False	2617311	203
1	google.com	True	True	False	False	302777	518
2	ctmail.com	True	True	False	False	235980	3
3	googlemail.com	True	True	False	False	228364	161
4	1and1.com	True	True	False	False	167140	17
5	outlook.com	True	True	False	False	127770	128052
6	GOOGLE.COM	True	True	False	False	124513	294
7	registrar-servers.com	False	True	False	False	109200	19
8	ovh.net	True	True	False	False	97814	109
9	co.uk	True	True	False	False	94123	2115
10	localhost	False	True	False	True	84105	1
11	GOOGLEMAIL.COM	True	True	False	False	81705	95
12	kundenserver.de	False	True	False	True	79481	5
13	rzone.de	True	True	False	True	63592	5
14	hostedemail.com	False	True	False	False	63415	28803
15	gandi.net	True	True	False	False	48952	13
16	m1bp.com	False	True	False	True	39871	6
17	mb5p.com	False	True	False	True	39775	6
18	dreamhost.com	False	True	False	False	36432	48
19	yahoodns.net	False	True	False	False	34638	8
20	1and1.fr	True	True	False	True	31171	4
21	udag.de	False	True	False	True	30622	6
22	one.com	False	True	False	True	30072	15
23	h-email.net	False	True	False	True	28233	1
24	emailsrvr.com	False	True	False	False	27695	21

A: NS Distribution (Org)

POS	Name (SLD)	V6	V4	V6 All	V4 All	DNUM	NSNUM
0	domaincontrol.com	True	True	False	False	2831306	118
1	worldnic.com	False	True	False	False	258121	105
2	co.uk	True	True	False	False	180370	6178
3	name-services.com	True	True	False	True	153477	7
4	registrar-servers.com	False	True	False	False	144099	184
5	1and1-dns.com	True	True	True	True	140994	9
6	1and1-dns.org	True	True	True	True	140073	9
7	bluehost.com	False	True	False	False	131958	78
8	wixdns.net	False	True	False	True	110342	24
9	cloudflare.com	True	True	False	False	105453	393
10	ovh.net	True	True	False	False	99184	840
11	register.com	True	True	False	False	98207	774
12	1and1.com	True	True	False	False	97133	18
13	1and1-dns.de	True	True	True	True	96183	2
14	hostgator.com	False	True	False	False	93570	5890
15	dreamhost.com	False	True	False	False	91566	6
16	sedoparking.com	False	True	False	True	83935	12
17	1and1-dns.biz	True	True	False	False	73603	9
18	1and1-dns.us	True	True	False	False	68904	2
19	wordpress.com	True	True	False	True	67070	16
20	gandi.net	True	True	False	False	61120	146
21	name.com	True	True	False	True	59780	135
22	cashparking.com	False	True	False	True	59309	2
23	rzone.de	True	True	True	True	55991	40
24	uniregistrymarket.link	False	True	False	True	55705	4

A: Misconfigured Domains

Motivation

A: Misconfigured Domains

Motivation

- Reserved IP address spaces

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?
  $\Rightarrow$ might indicate misconfiguration

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?
  $\Rightarrow$ might indicate misconfiguration

Findings

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?
  $\Rightarrow$ might indicate misconfiguration

Findings

- 94206 domains use reserved IP addresses
  (`com`-zone, 23-12-2016, 0.074% of `com`-domains)

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?
  $\Rightarrow$ might indicate misconfiguration

Findings

- 94206 domains use reserved IP addresses
  (`com`-zone, 23-12-2016, 0.074% of `com`-domains)
- Four months later:
  - 12100 domains no longer existed (`NXDOMAIN`)

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?
  $\Rightarrow$ might indicate misconfiguration

Findings

- 94206 domains use reserved IP addresses
  (`com`-zone, 23-12-2016, 0.074% of `com`-domains)
- Four months later:
  - 12100 domains no longer existed (`NXDOMAIN`)
  - **72760 (77%)** did not change anything...

A: Misconfigured Domains

Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?
  $\Rightarrow$ might indicate misconfiguration

Findings

- 94206 domains use reserved IP addresses
  (`com`-zone, 23-12-2016, 0.074% of `com`-domains)
- Four months later:
  - 12100 domains no longer existed (`NXDOMAIN`)
  - **72760 (77%)** did not change anything...
  - Only 9% fixed their `A`-records

A: Misconfigured Domains

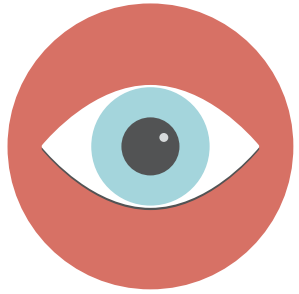
Motivation

- Reserved IP address spaces
  (`127.0.0.1`, `192.168.0.0/16`, ...)
- Domains using reserved IP addresses?
  $\Rightarrow$ might indicate misconfiguration

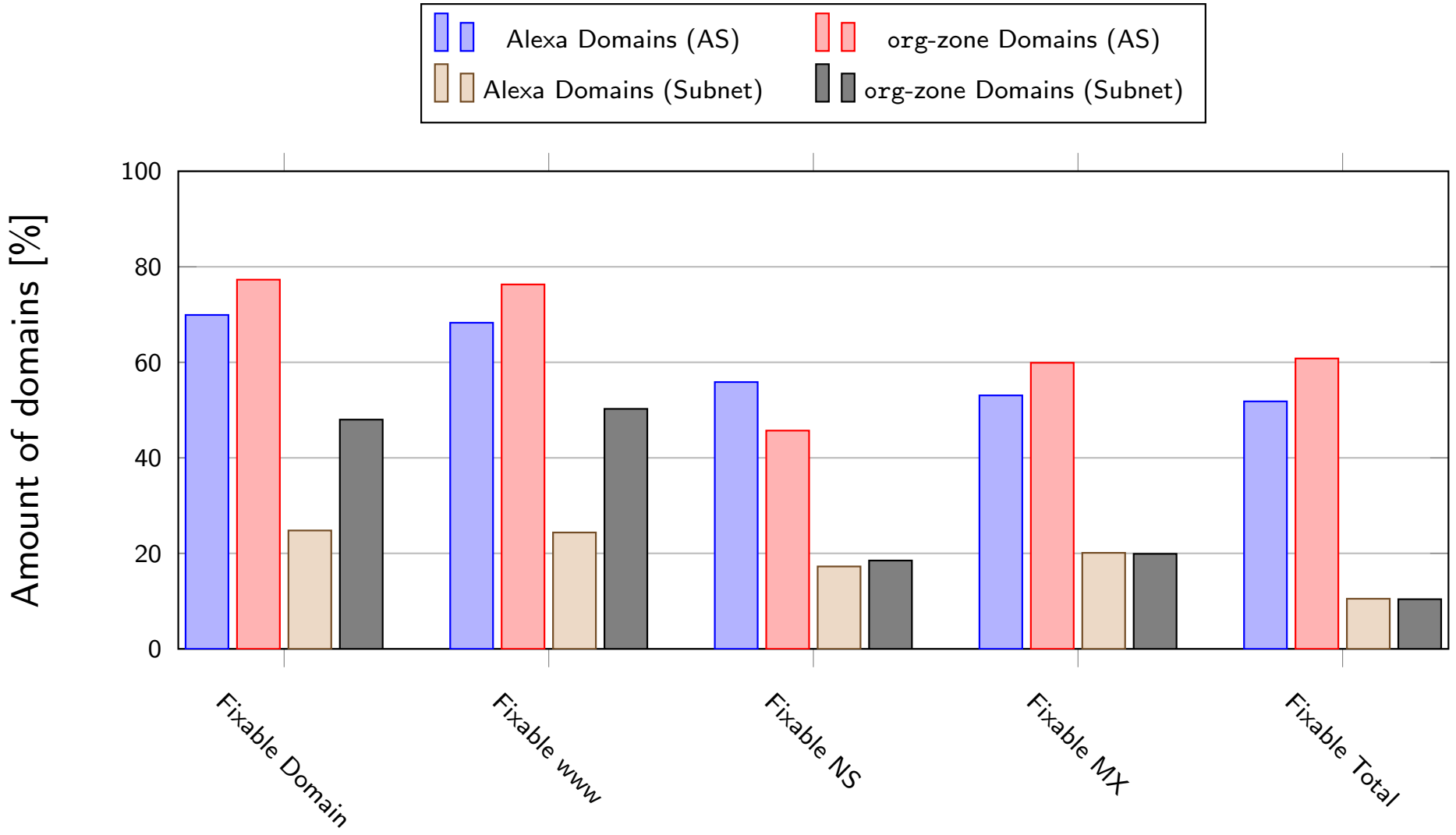
Findings

- 94206 domains use reserved IP addresses
  (`com`-zone, 23-12-2016, 0.074% of `com`-domains)
- Four months later:
  - 12100 domains no longer existed (`NXDOMAIN`)
  - **72760 (77%)** did not change anything...
  - Only 9% fixed their `A`-records

$\Rightarrow$ Misconfiguration does not just "disappear"



A: IPv6-Capability Study (Fixable Domains)



References I


Lorenzo Colitti, Steinar H. Gunderson, Erik Kline, and Tiziana Refice.
Evaluating ipv6 adoption in the internet.
In *PAM 2010*, 2010.


Luca Deri, Lorenzo Luconi Trombacchi, Maurizio Martinelli, and Daniele Vannozzi.
Towards a passive dns monitoring system.
In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, SAC '12, pages 629–630, New York, NY, USA, 2012. ACM.


John S. Otto, Mario A. Sánchez, John P. Rula, and Fabián E. Bustamante.
Content delivery and the natural evolution of dns.
2012.


Tom van Goethem, Ping Chen, Nick Nikiforakis, Lieven Desmet, and Wouter Joosen.
Large-scale security analysis of the web: Challenges and findings.
2014.

References II

Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto, and Aiko Pras.
A high-performance, scalable infrastructure for large-scale active dns measurements.
IEEE Journal on Selected Areas in Communications, 34(6):1877–1888, 2016.

Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras.
Dnssec and its potential for ddos attacks.
2014.