National Institute of Information and Communications Technology

Secure Glue A Cache and Update

○Yong Jin†, Kenji Fujikawa†, Hiroaki Harai†, Masataka Ohta‡

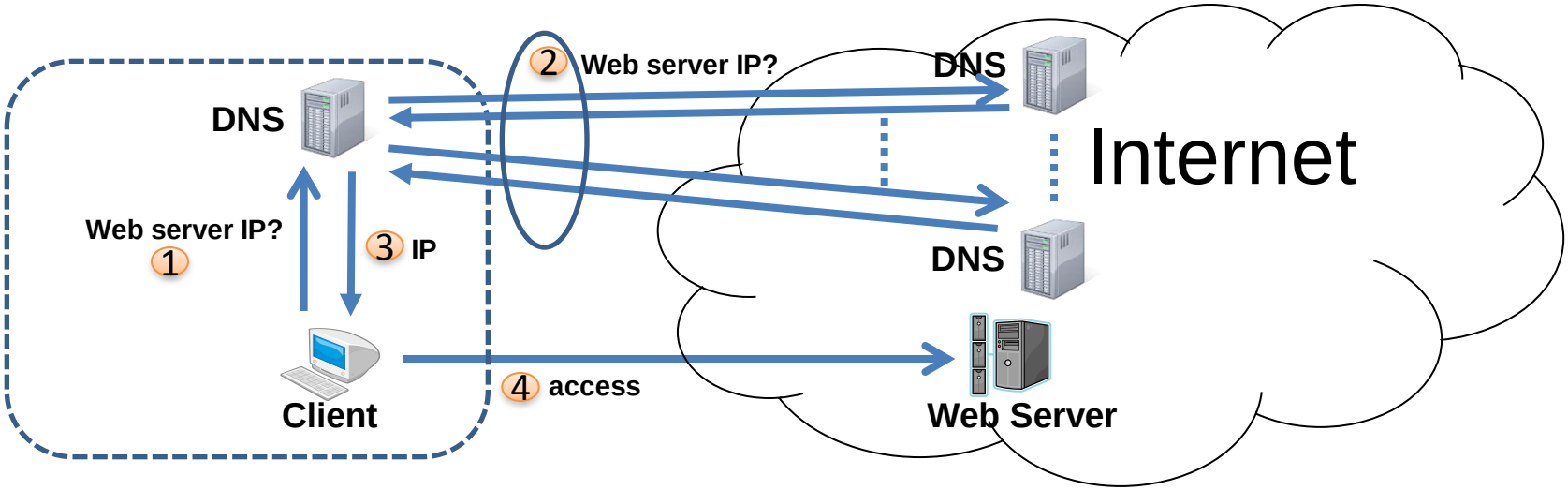
†National Institute of Information and Communications Technology
†Tokyo Institute of Technology

Abstract

- Introduction
- Problems in current DNS protocol
- Secure glue A cache and update
- Summary and future work

Introduction

- DNS (Domain Name System)
  - Name resolution protocol



- Key name resolution protocol in the Internet
  - Nobody uses IP addresses directly

Introduction

- DNS (Domain Name System)
  - Name resolution protocol

◆Problems:
Increase of delay in name resolution
Increase of DNS traffic
Lack of consideration for name servers' renumbering

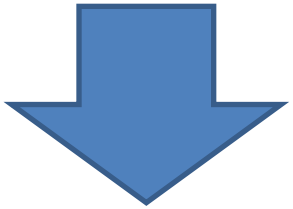
◆Need to:
Reduce DNS response time
Reduce network traffic caused by name resolution

◆Solution:
Secure glue A cache and update
Including in-bailiwick and out-of-bailiwick domain

What is glue A and why is it necessary?

- Indicates address of in-bailiwick domain NS record

Zone: example.com.	a.example.com.	NS	ns.a.example.com.	→ In-bailiwick NS record
	ns.a.example.com.	A	192.168.0.4	
	b.example.com.	NS	ns.example.net.	→ Out-of-bailiwick NS record
	ns.example.net.	A	192.168.0.2	→ Ignored



Name resolution fails if no glue A is configured
Glue A for out-of-bailiwick NS record is ignored

Pros and Cons of NS record

- Current NS record format
  - Out-of-bailiwick domain: sub1.example.com **IN NS** ns.example.net
  - In-bailiwick domain: sub1.example.com **IN NS** ns.sub1.example.com
  - **NOT LIKE**: sub1.example.com **IN NSA** 1.2.3.4
    sub1.example.com **IN NSIP** 1.2.3.4

Pros of NS record:

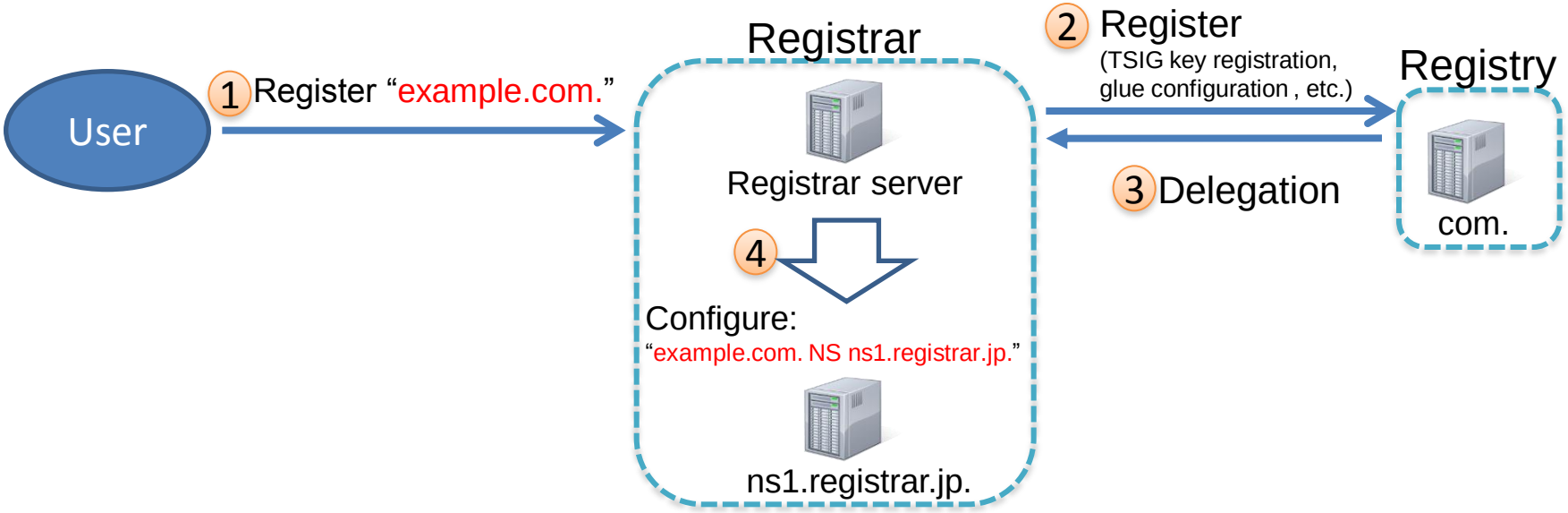
Out-of-bailiwick domain NS record is allowed

Cons of NS record:

Glue A for in-bailiwick NS record is required separately

Problems in current DNS -- (1)

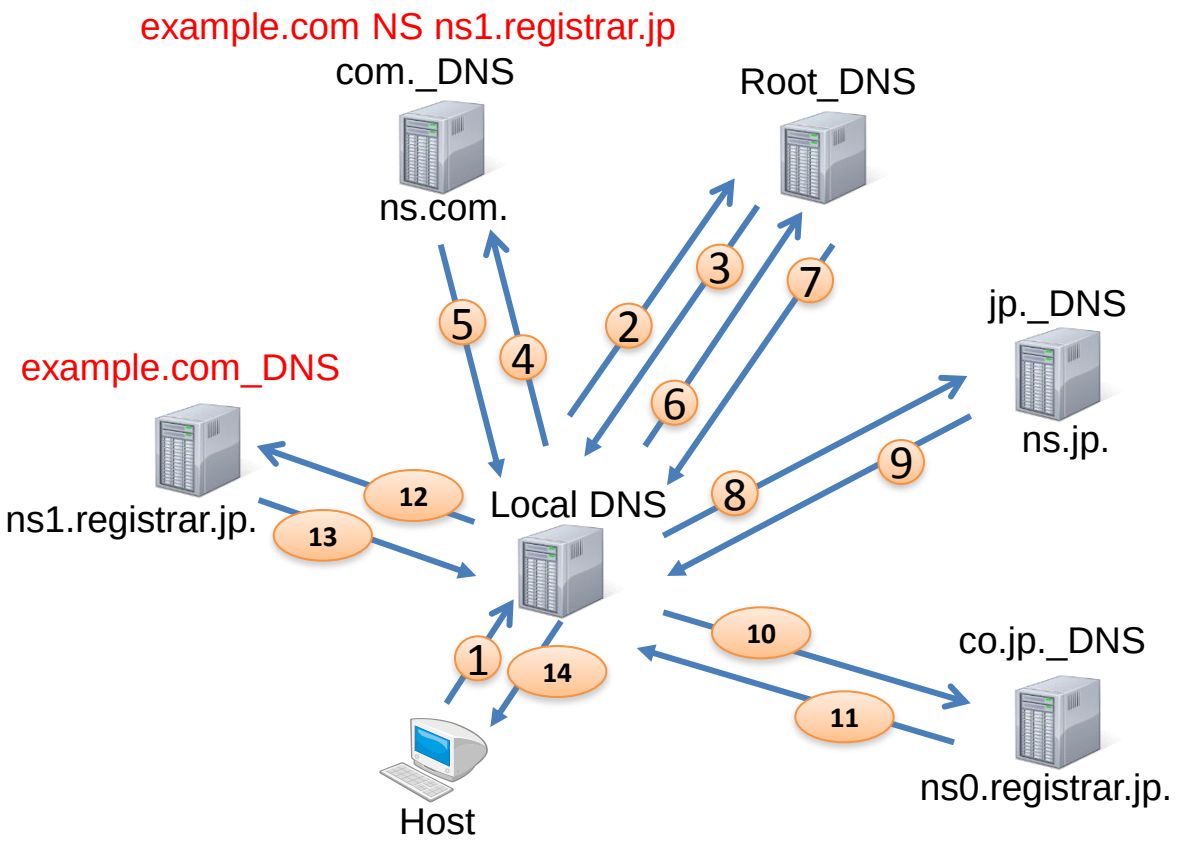
- What causes the problems?
  - » Increase of delay in name resolution
  - » Increase of DNS traffic
- Increasing use of out-of-bailiwick domain for ease of administration†
  - Example: “ns1.registrar.jp.” is the DNS server of a registrar



†Fujiwara, K.; Sato, A.; Yoshida, K.; , "DNS Traffic Analysis: Issues of IPv6 and CDN," *Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium on* , vol., no., pp.129-137, 16-20 July 2012doi: 10.1109/SAINT.2012.26

Problems in current DNS -- (2)

- Slow distribution of out-of-bailiwick domain
  - Example:

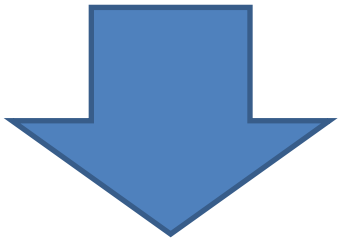


1. www.example.com. ?
2. www.example.com. ?
3. com. NS ns.com.
   ns.com. IP
4. www.example.com. ?
5. example.com. NS ns1.registrar.jp.
6. ns1.registrar.jp. ?
7. jp. NS ns.jp.
   ns.jp. IP
8. ns1.registrar.jp. ?
9. registrar.jp NS ns0.registrar.jp.
   ns0.registrar.jp. IP
10. ns1.registrar.jp. ?
11. ns1.registrar.jp. IP
12. www.example.com. ?
13. www.example.com. IP
14. www.example.com. IP

Access: http://www.example.com.

Solution: Secure Glue A Cache and Update

- Concept:
  - ➢Glue A only makes sense together with corresponding NS record
  - ➢No need to cache glue A individually



Making glue A cache and update secure:

- ●Cache and update glue A together with NS record
- ●Subsequent two records NS and A are bundled and handled as one set in cache

Solution: Secure Glue A Cache and Update

- Mechanism
  - DNS with out-of-bailiwick domain NS record previously queries the glue A and caches it together with the corresponding NS record at bootstrap time
  - For in-bailiwick domain NS record, DNS gets the glue A from the zone file and caches it together with the corresponding NS record at bootstrap time
  - If the TTL of cached glue A or NS record is expired re-fetch them
  - Only answer the cached glue A as referral record together with the corresponding NS record
  - When the glue A is changed put the new glue A in the additional section of the update message of the corresponding NS record and update the glue A
  - Update glue A in cache when receives the update message after checking its authoritative answer
  - Only change cache format of glue A and the corresponding NS record
  - Compatible with most other specifications of the current DNS protocol
  - Also can be used for AAAA record

Solution: Secure Glue A Cache and Update

- Cache format:

In-bailiwick domain

```
sub1.example.com       IN   NS   ns.sub1.example.com
ns.sub1.example.com    IN    A   1.2.3.4
```

Or

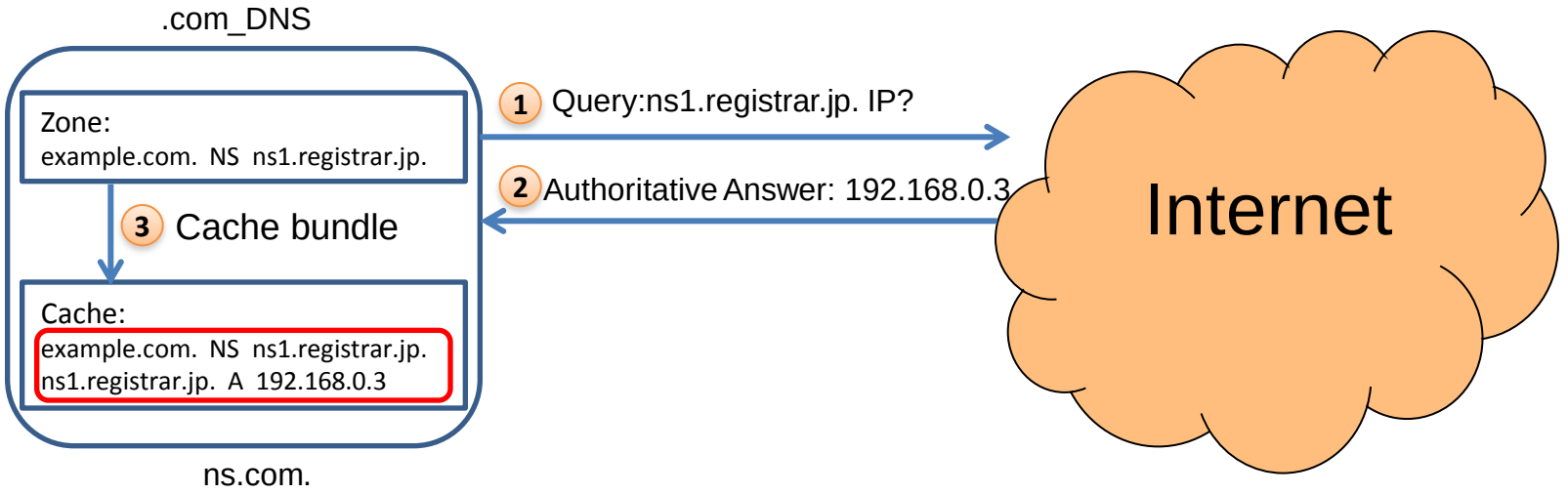
Out-of-bailiwick domain

```
sub1.example.com       IN  NS   ns.example.net
ns.example.net         IN   A   1.2.3.4
```

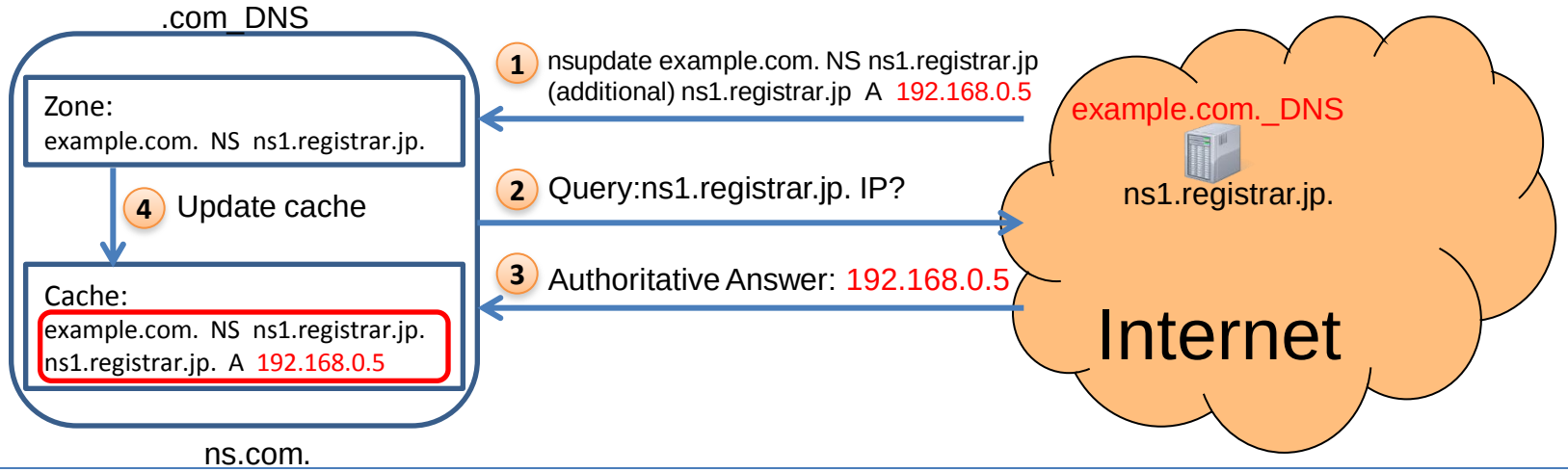
- Bundle glue A with corresponding NS record together and cache them as one record
- Only change the cache format of glue A and corresponding NS record

Solution: Secure Glue A Cache and Update

- Example: Caching

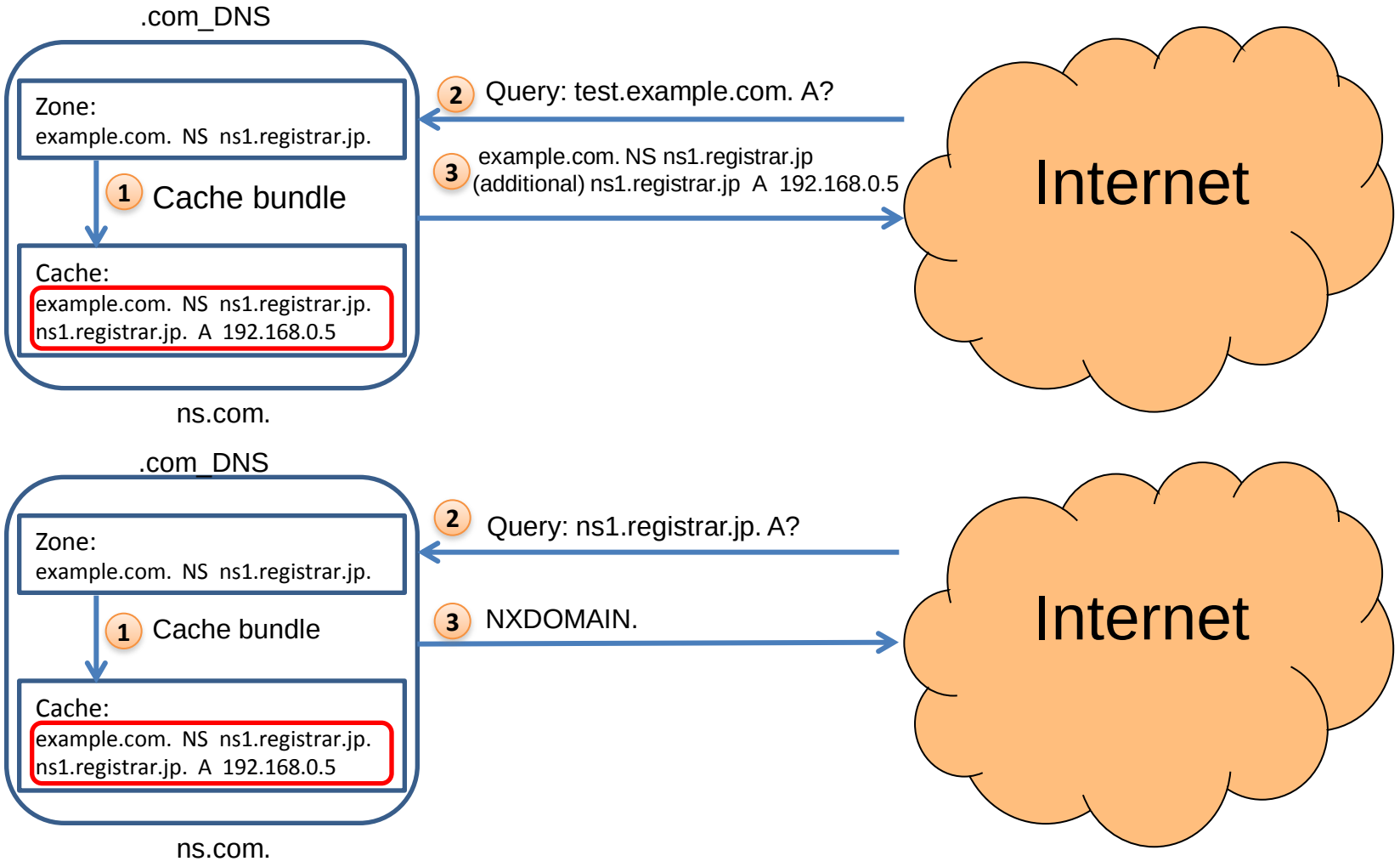


- Example: Updating



Solution: Secure Glue A Cache and Update

- Example: Answering



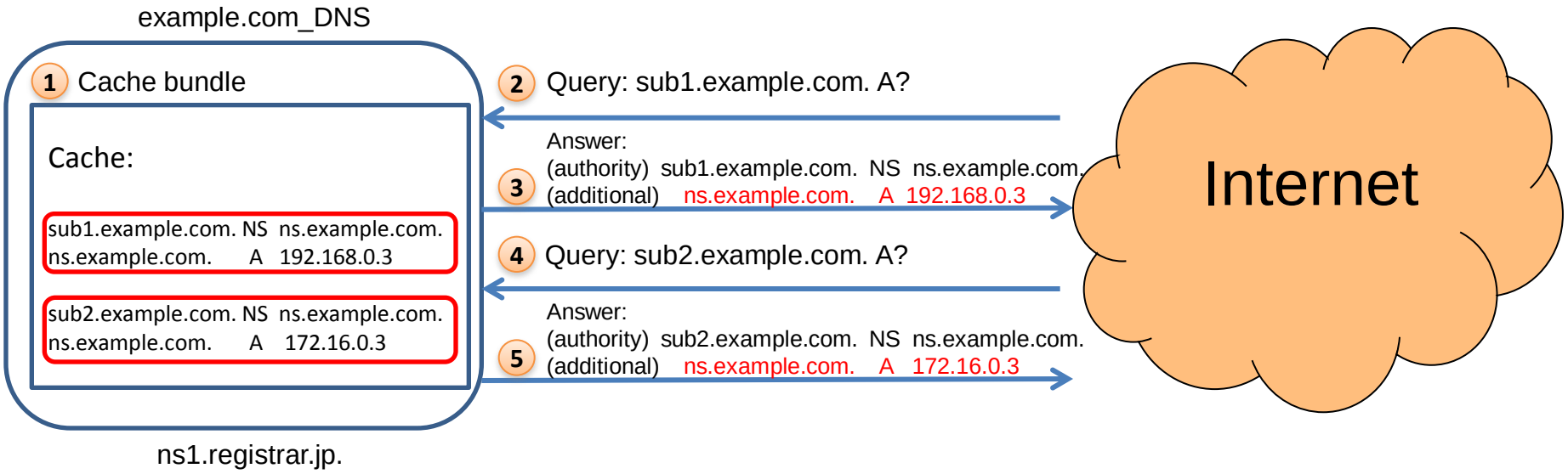
Solution: Secure Glue A Cache and Update

- Example: Zone delegation using inconsistent glue A records

Zone: “example.com.”

sub1.example.com. NS ns.example.com.
ns.example.com. A 192.168.0.3

sub2.example.com. NS ns.example.com.
ns.example.com. A 172.16.0.3



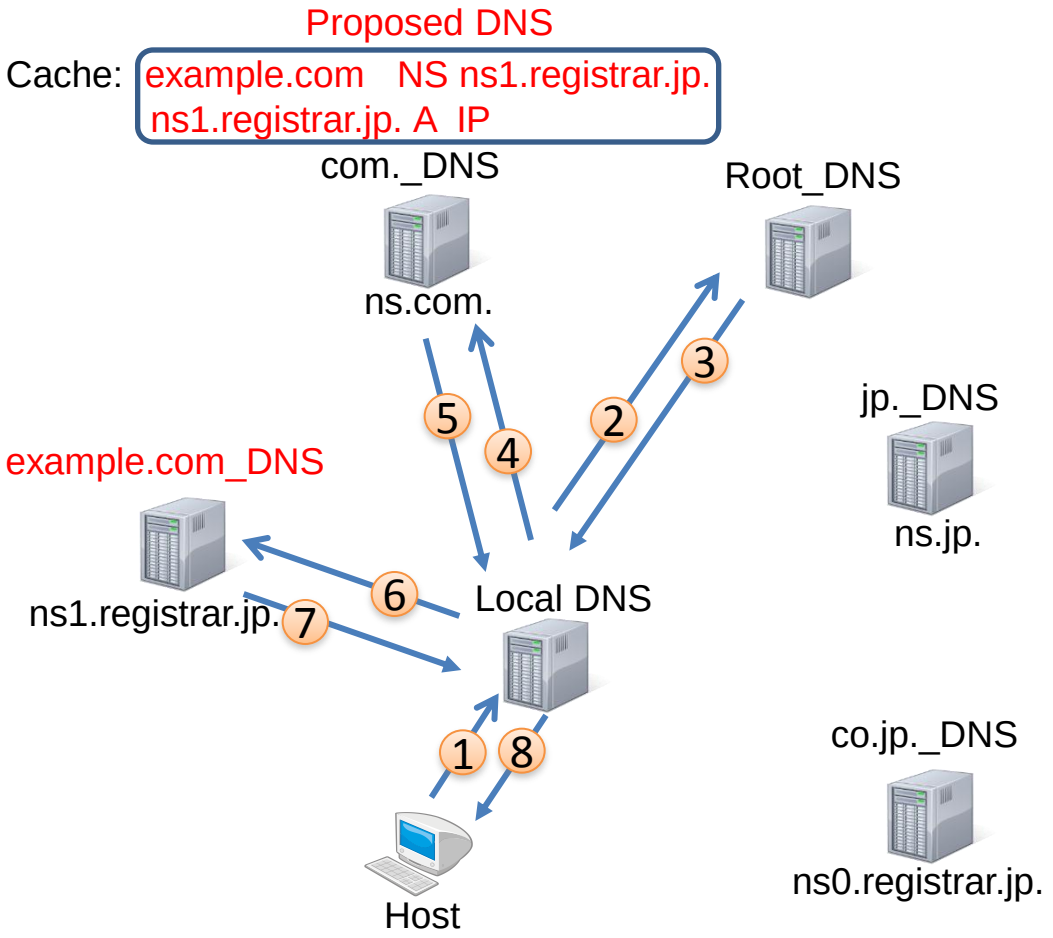
Solution: Secure Glue A Cache and Update

- Difference from **fetch-glue** substatement
  - Supported in BIND 4.9 and 8
  - Obsoleted in BIND 9
  - It makes the name server look up glue A records if it does not have when replies NS records

	Fetch-glue substatement	Secure glue A cache and update
Format	Individual glue record	Bundled with NS record
When achieve	Before reply response	At bootstrap time
Glue update	Not supported	Only support for updating with corresponding NS record (attach as additional record)
Availability	For any query	Only for query related to corresponding NS record

Solution: Secure Glue A Cache and Update

- Use of out-of-bailiwick domain NS record

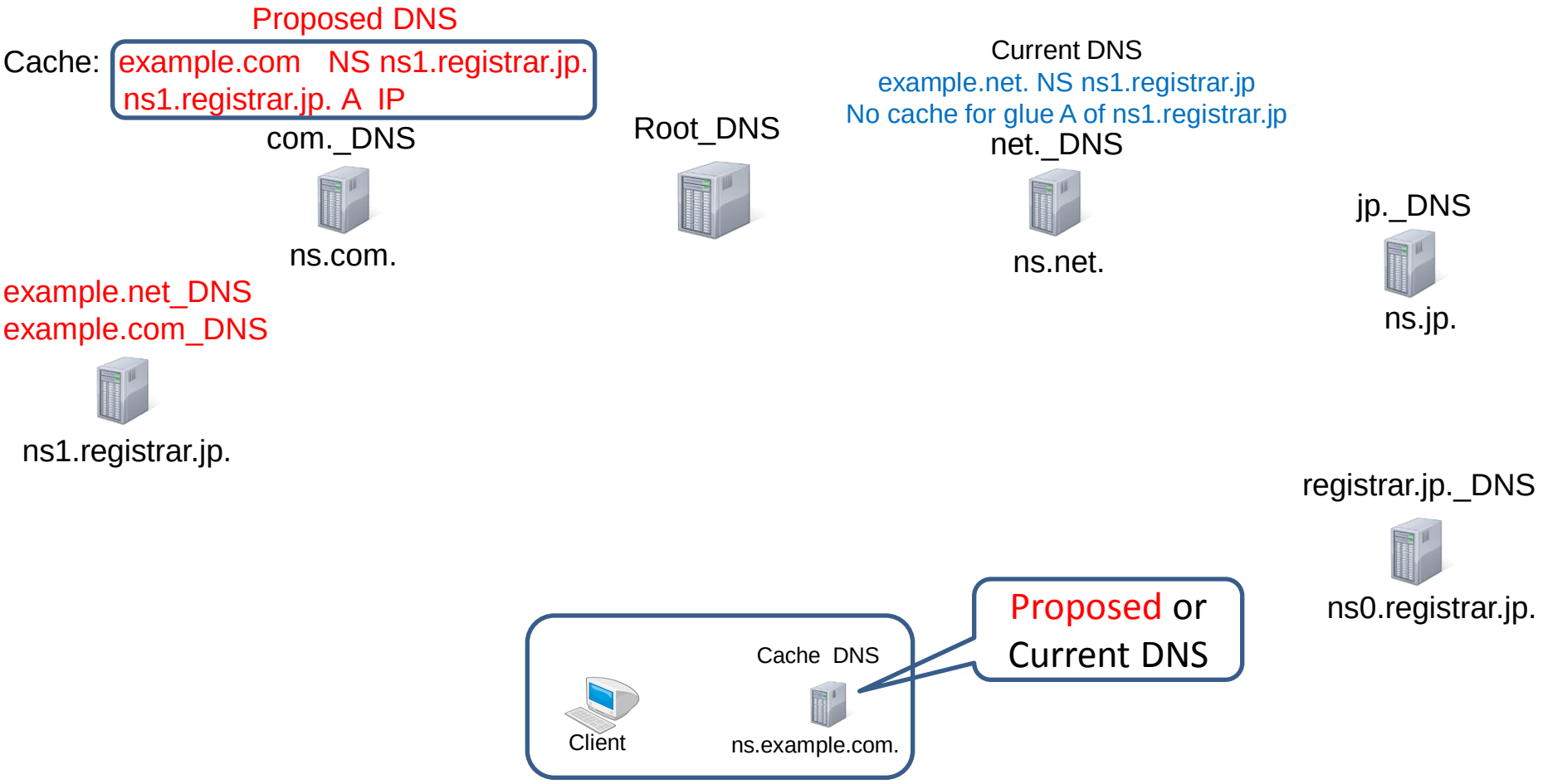


1. www.example.com. ?
2. www.example.com. ?
3. com. NS ns.com.
   ns.com. IP
4. www.example.com. ?
5. Reply cache:
   example.com. NS ns1.registrar.jp.
   ns1.registrar.jp. IP
6. www.example.com. ?
7. www.example.com. IP
8. www.example.com. IP

Solve problem: Reduces 6/14=43% of traffic in name resolution also can reduce DNS traffic in renumbering

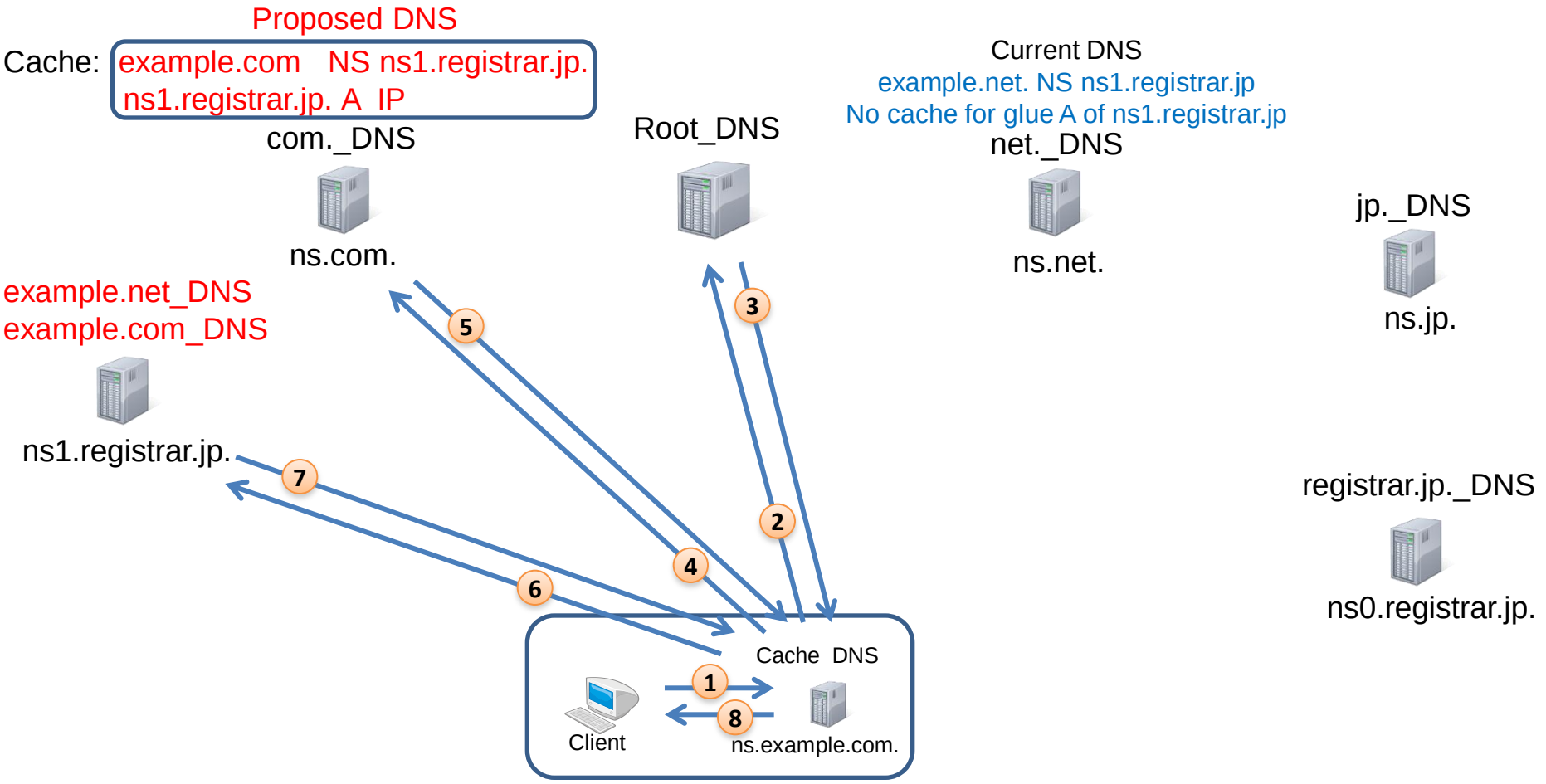
Apply to Current Internet

- Mixed environment



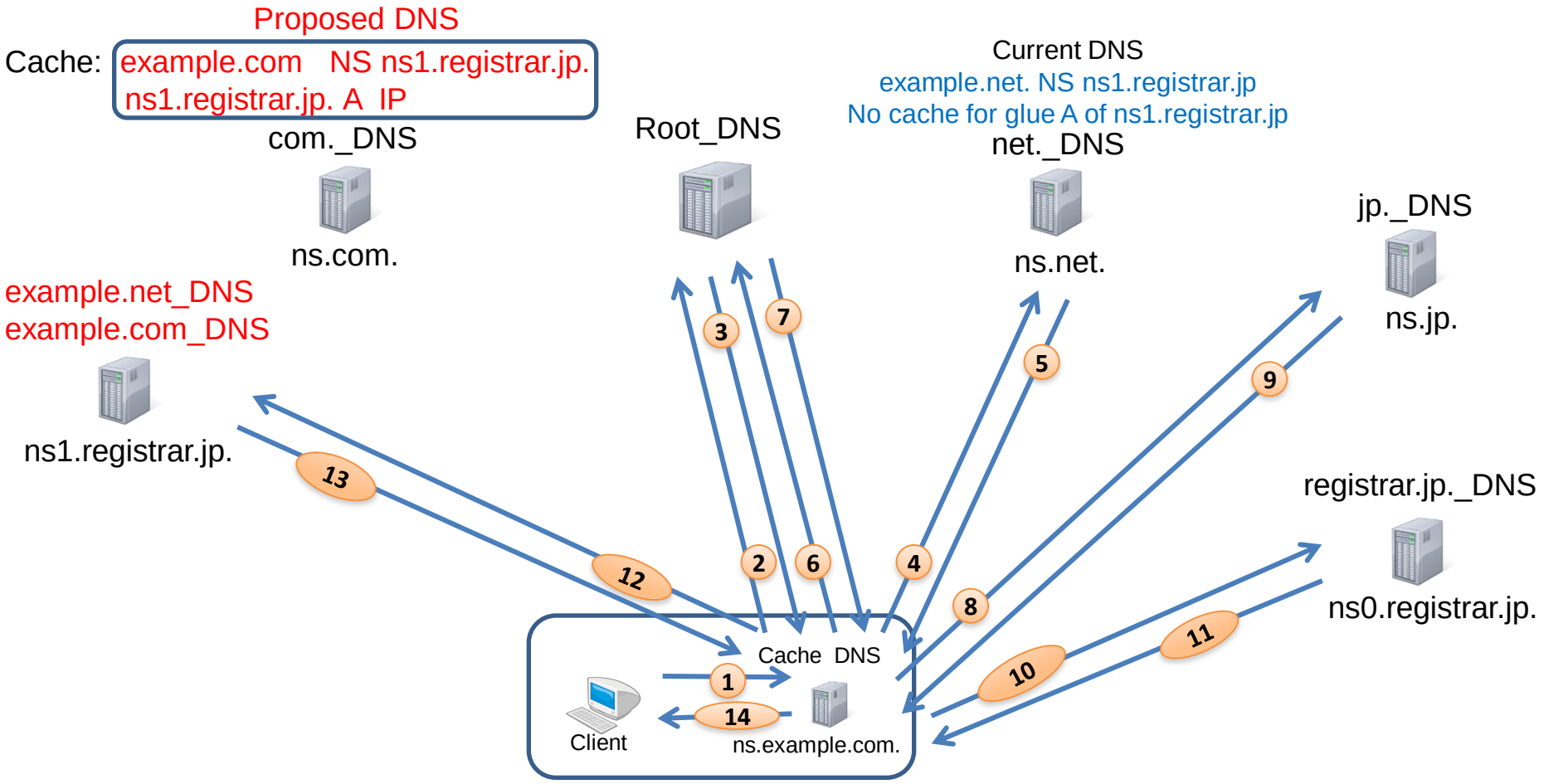
Apply to Current Internet

- Mixed environment – proposed DNS



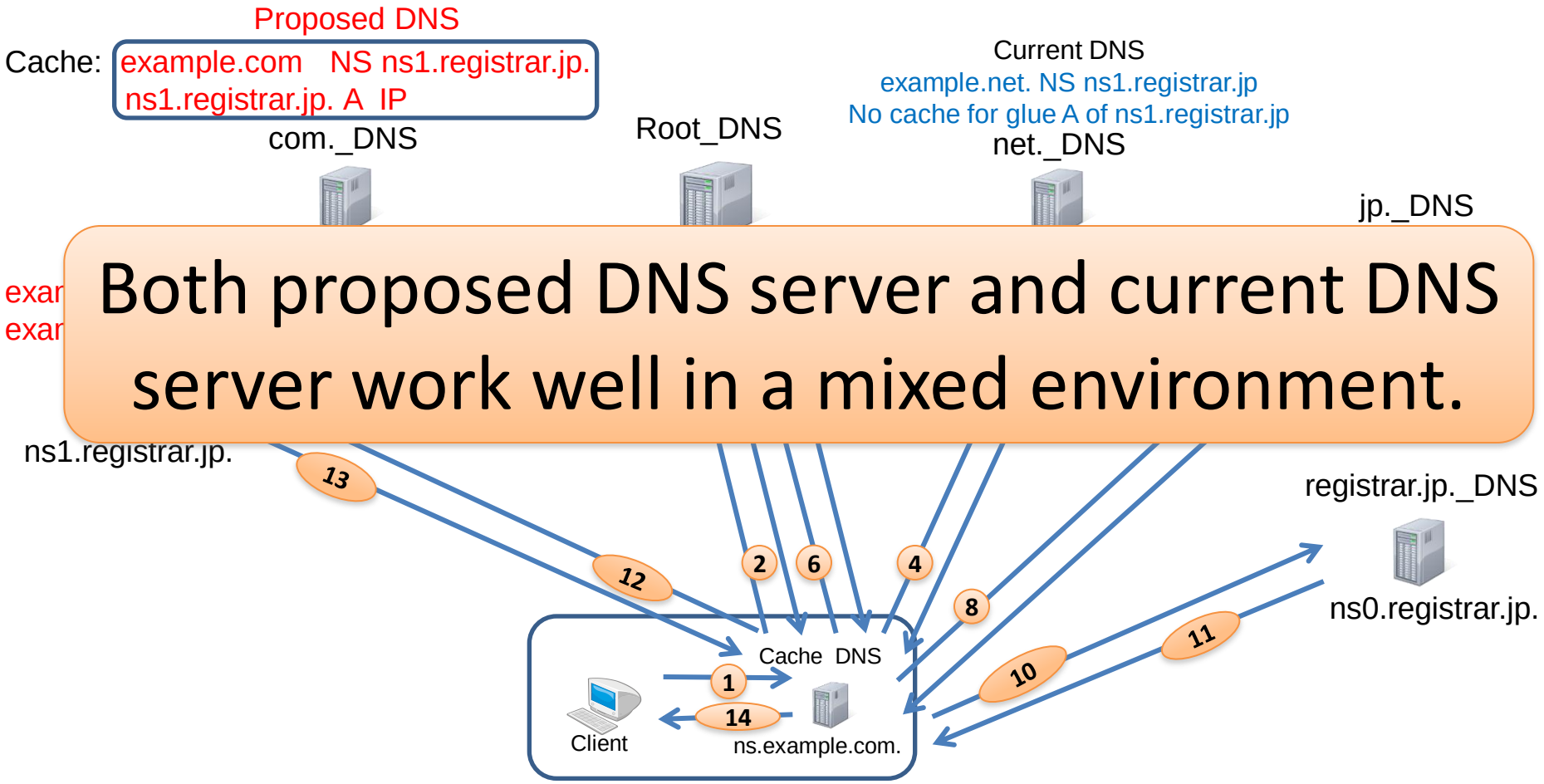
Apply to Current Internet

- Mixed environment – current DNS



Apply to Current Internet

- Mixed environment – current DNS



Implementation & Evaluation

- Development of HANA network
  - HANA(Hierarchical Automatic Number Allocation)†
    - IP address allocation architecture developed by NICT
    - In HANA, DNS servers may be also renumbered
  - Adapt DNS system to HANA network
    - Considering both name resolution and address update for renumbering including DNS servers
- Implementation & Evaluation
  - ➢ Implement and apply the proposal method on HANA network
  - ➢ Evaluate name resolution and dynamic address update for renumbering including DNS servers

†K. Fujikawa, H. Harai, and M. Ohta, "The Basic Procedures of Hierarchical Automatic Locator Number Allocation Protocol HANA," Proc. Asia Workshop on Future Internet Technologies (AWFIT 2011), pp. 124--131, October 2011

Summary and Future Work

- Propose secure cache and update glue A mechanism
  - Cache and update glue A together with corresponding NS record
  - Only answer glue A with corresponding NS record as referral record
- Plan to implement and evaluate on HANA network

- Expect to:
  - ➢Reduce latency of name resolution and dynamic dnsupdate
  - ➢Reduce DNS traffic
  - ➢Efficient dynamic dnsupdate for renumbering including DNS servers

Thanks!

Questions?