Universität Stuttgart

INSTITUT FÜR
KOMMUNIKATIONSNETZE
UND RECHNERSYSTEME
Prof. Dr.-Ing. Dr. h. c. mult. P. J. Kühn

Security Impact of DNS Delegation Structure and Configuration Problems

Jochen Kögel, Sebastian Kiesel
Institute of Communication Networks and Computer Engineering
University of Stuttgart
{koegel,kiesel}@ikr.uni-stuttgart.de

This work was funded by T-Com Corporate Security

October 11, 2006

Agenda

- Motivation
- DNS principles
- Problems - delegation structure and configuration
- Possible solutions
- Conclusion and Outlook

Motivation

DNS

- **Mainly used for**
  - Domain name ↔ IP address lookup (A records)
  - E-mail: application layer routing (MX records)
    - Load balancing
    - Backup servers
- **Proven scalability and flexibility**
- **Became one of the building blocks of the Internet**

➥ **Next to IP transport, it is something that "just works"**

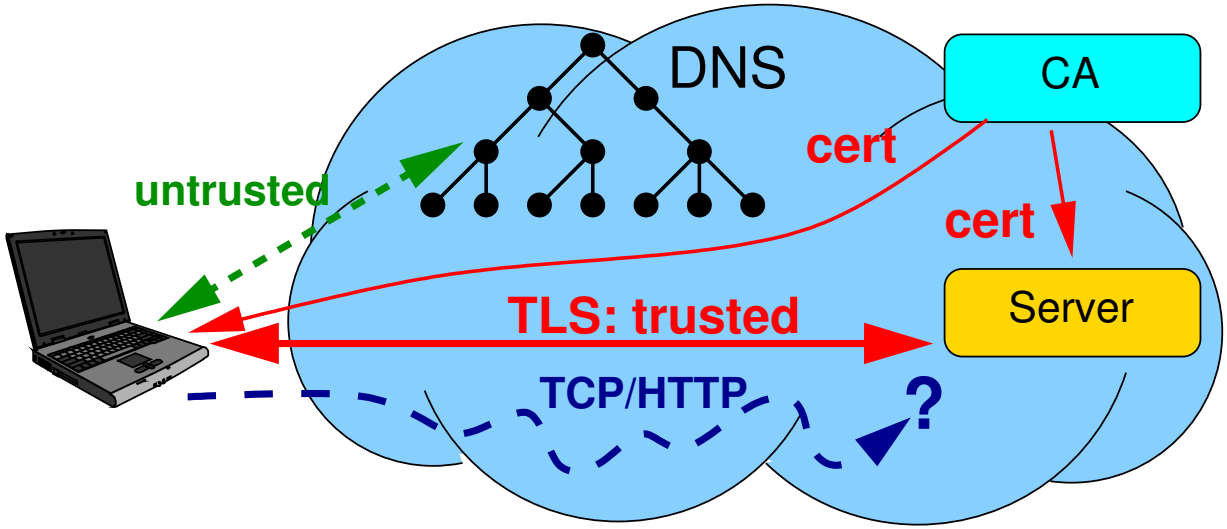
Motivation

Problems with DNS

- **No integrity protection in DNS replies (spoofing, cache poisoning, etc)**

Current security approach

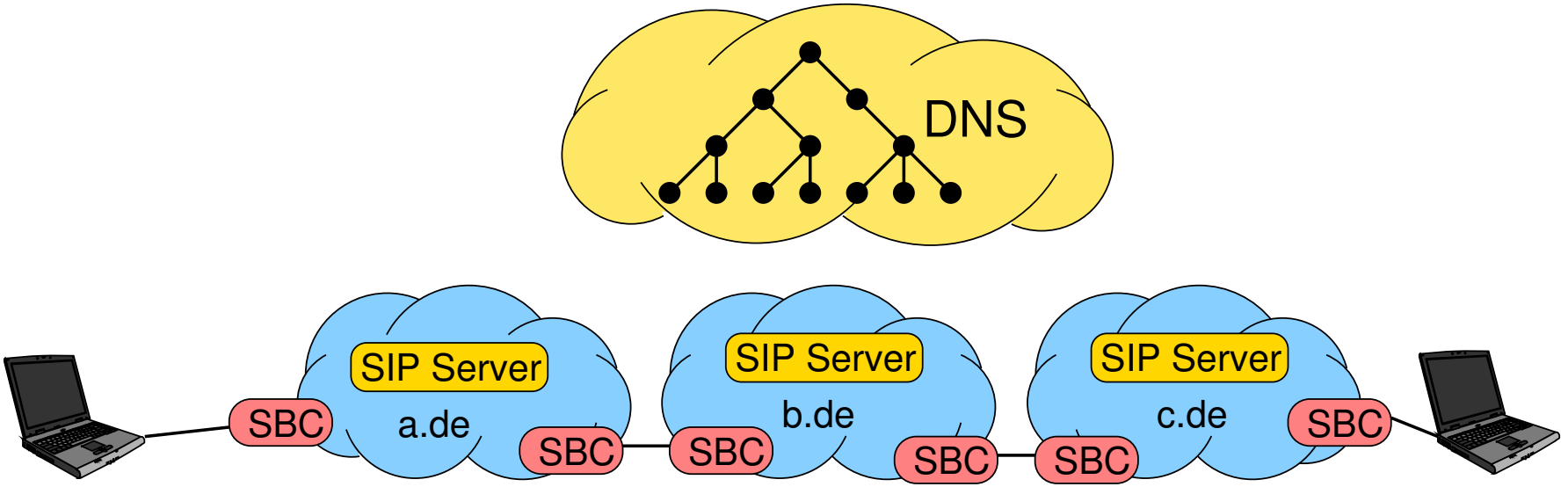
1. **Take DNS as untrusted lookup mechanism**
2. **For sensitive applications:**
   Use http over TLS for authenticating peers



➥ **This solution works. At least for web applications.**

Motivation

NGNs: new applications for DNS



Characteristics of NGNs (e.g., IMS): high security requirements

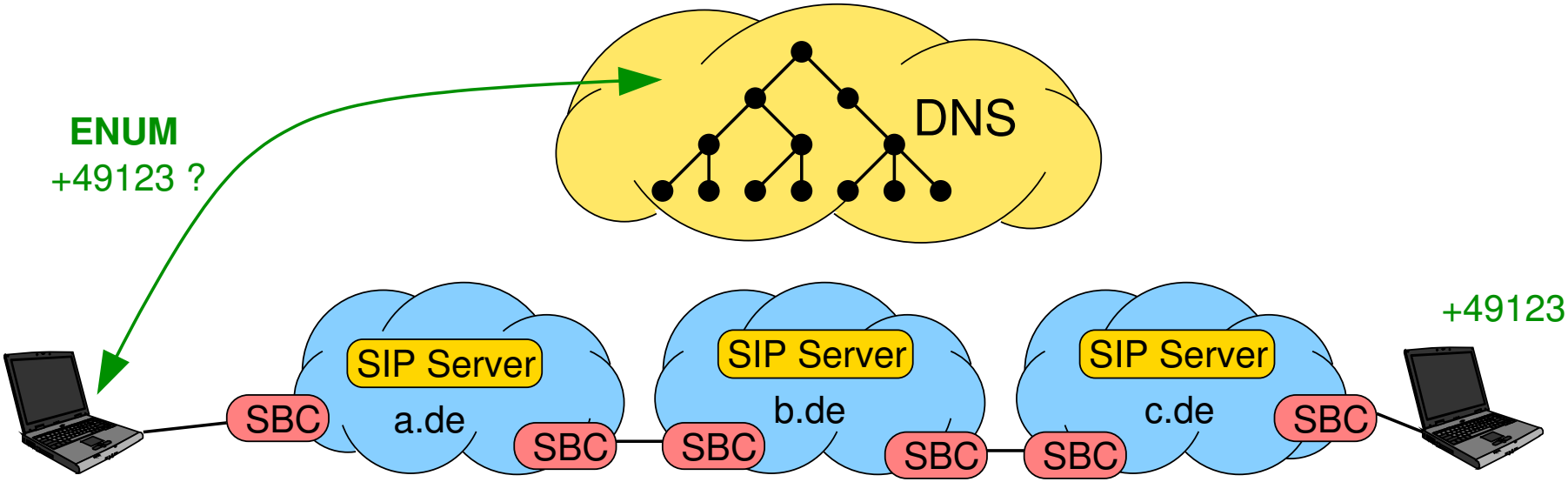
- **"Closed" platforms**
  - Policy enforcement by session based filtering at platform edge (Session Border Controllers)

➥ **No full IP connectivity to the Internet or other NGNs**

➥ **Application layer routing**

Motivation

NGNs: new applications for DNS



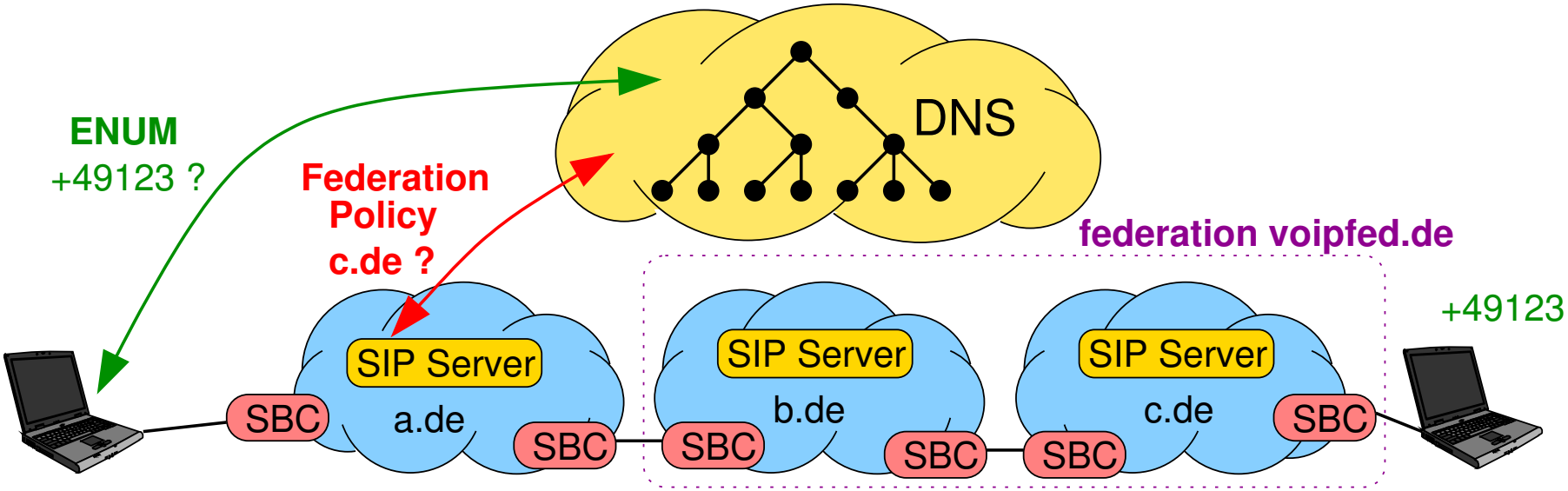
ENUM

Retrieve service URIs of based on phone number

```
3.2.1.9.4.e164.arpa.
14400 IN NAPTR 1 10 "u" "E2U+sip" "!^.*$!sip:+123@c.de!"
14400 IN NAPTR 1 20 "u" "E2U+msg" "!^.*$!mailto:bob@c.de!"
```

Motivation

NGNs: new applications for DNS



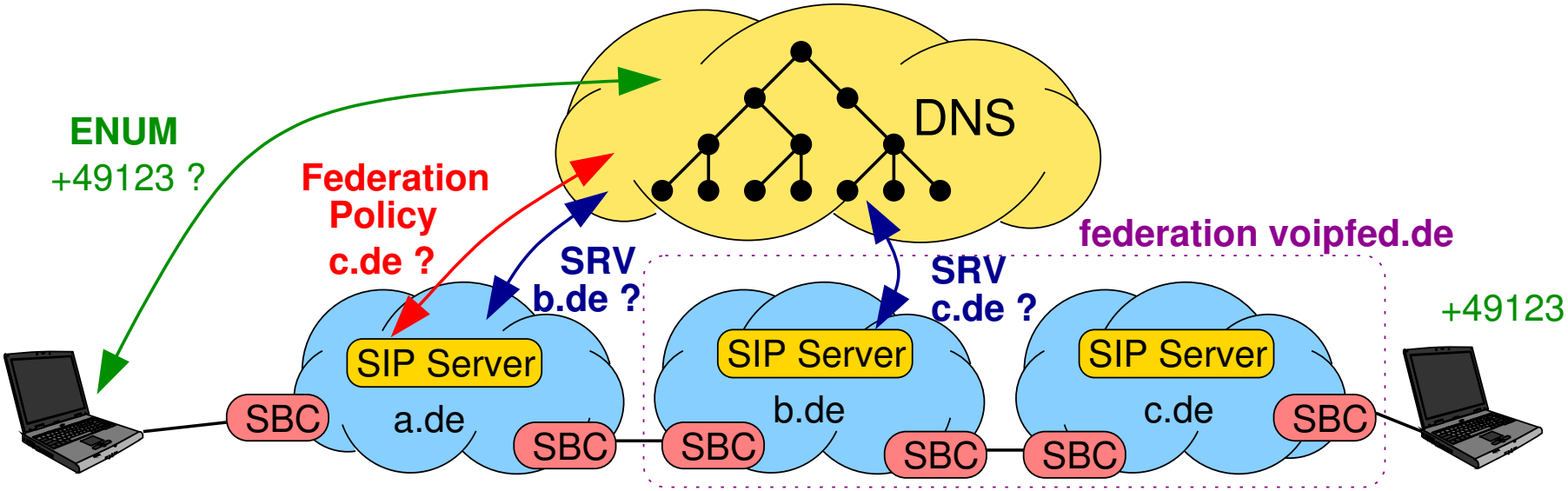
Federation policies

Provide policies for incoming connections (draft-lendl-domain-policy-ddds)

```
c.de.
IN NAPTR 10 10 "U" "D2P+SIP:fed "!^.*$!http://sip.voipfed.de/!"
```

Motivation

NGNs: new applications for DNS



SRV Records

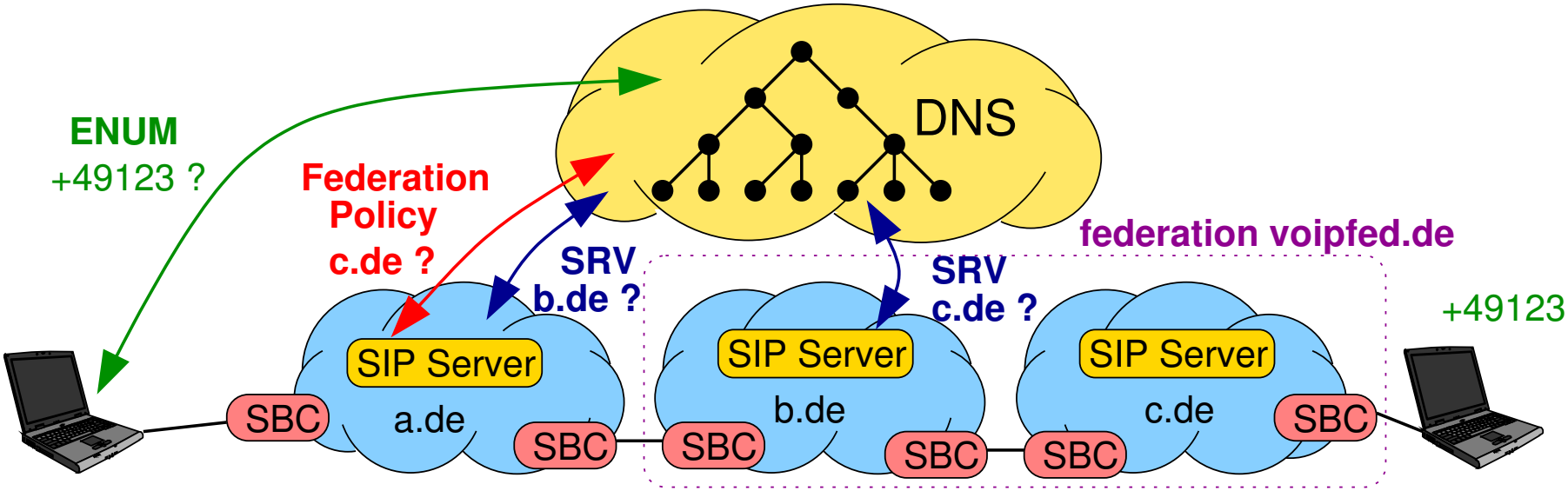
Generalized MX records for application layer routing

```
_sip._udp.b.de. 7200 IN SRV 0 0 5060 ingress-sbc.b.de.

_sip._udp.c.de. 7200 IN SRV 0 0 5060 sbc1.c.de.
```

Motivation

NGNs: new applications for DNS

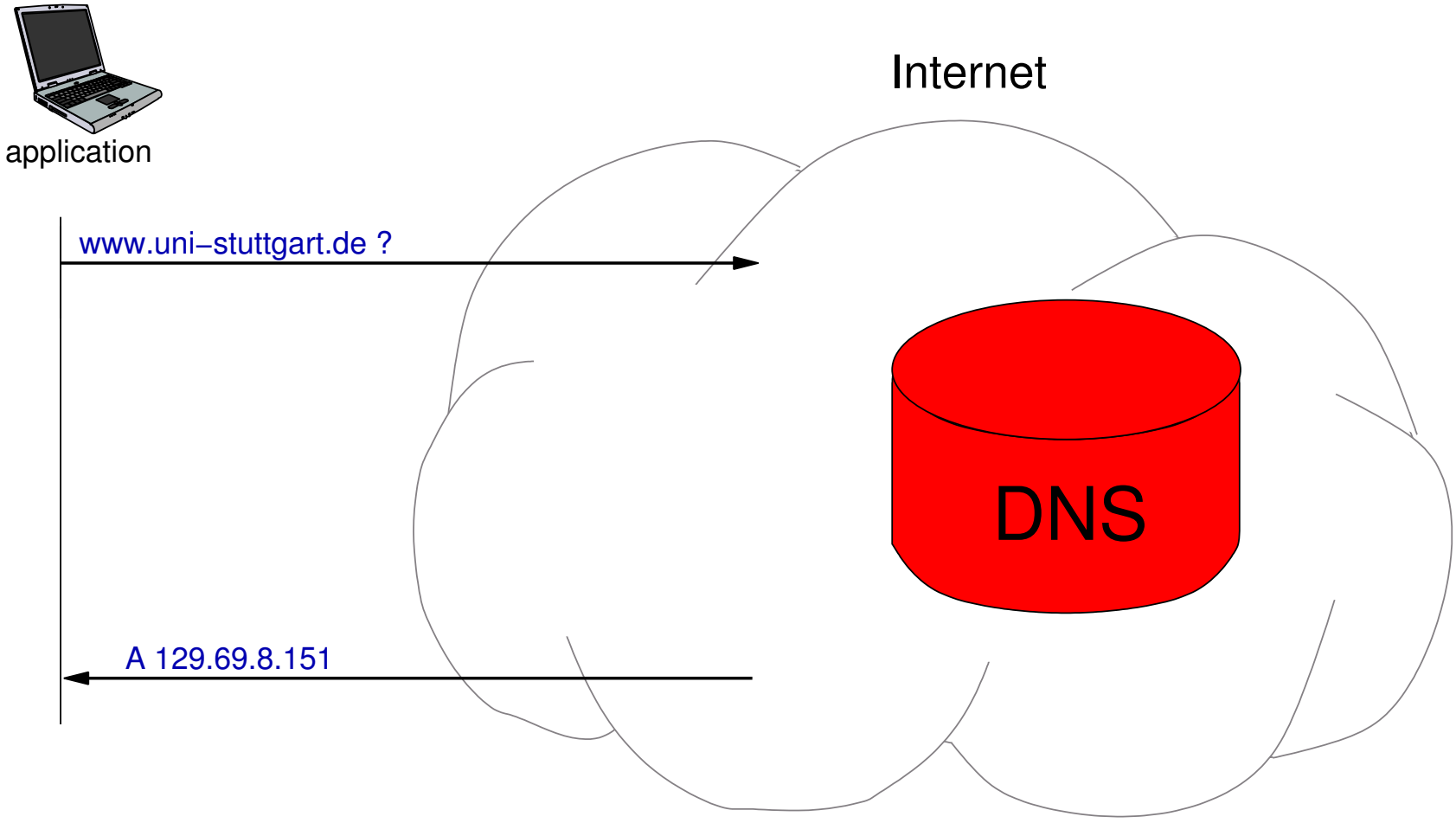


Essential routing information stored in DNS

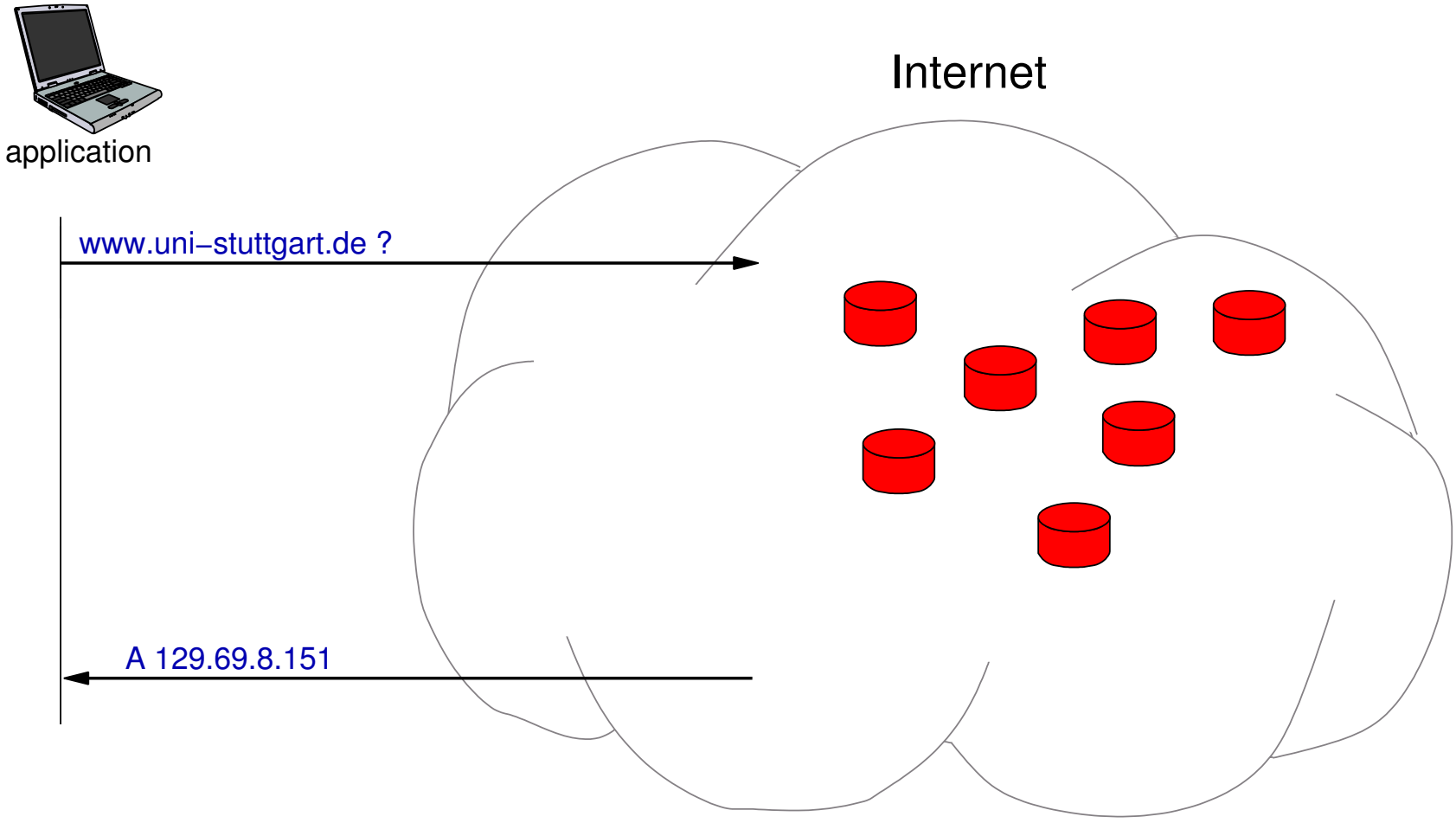
➥ **"http-over-TLS workaround" not sufficient anymore**

➥ **Security and reliabilty of the DNS itself becomes essential**

DNS Principles

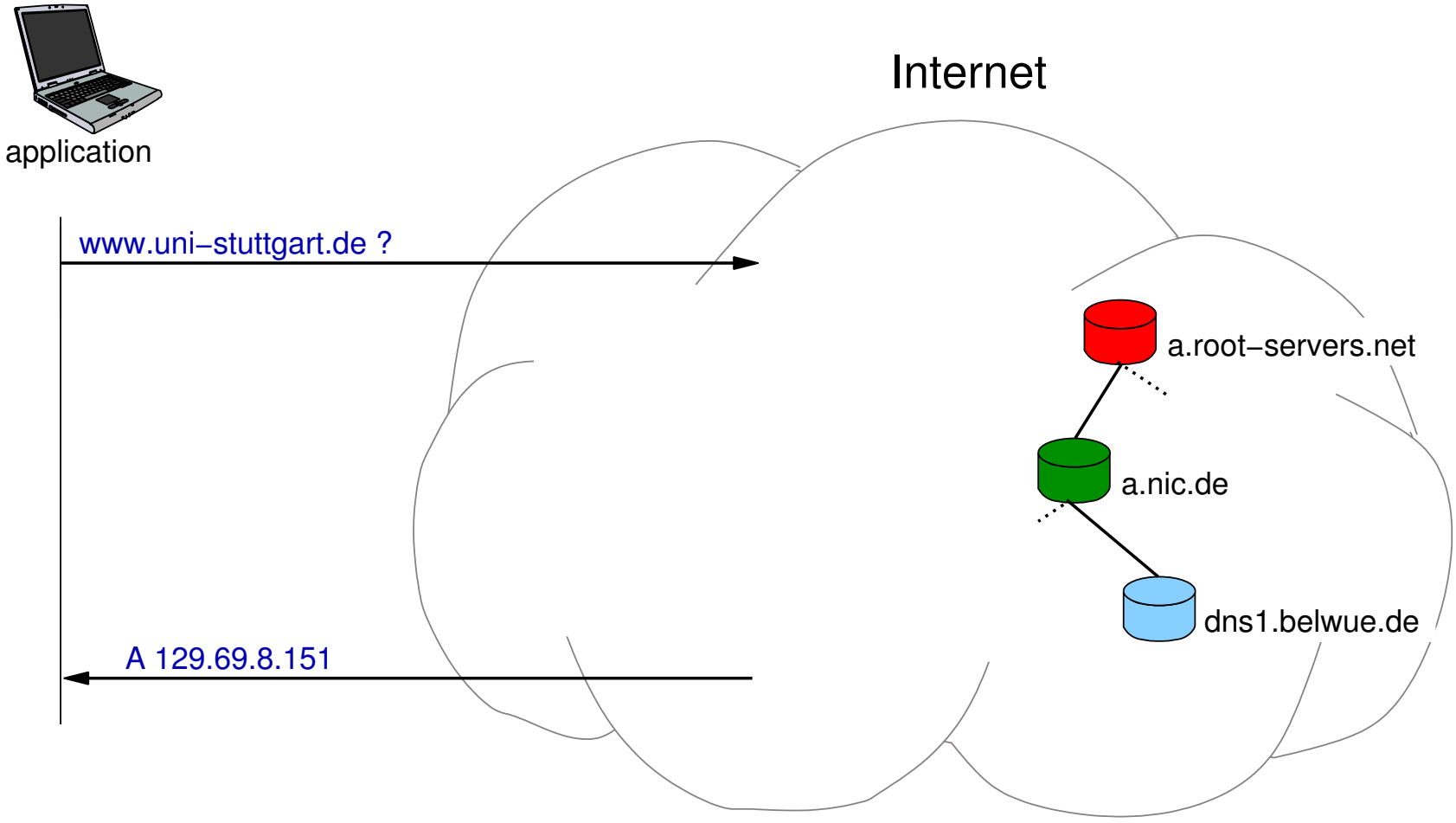


DNS Principles



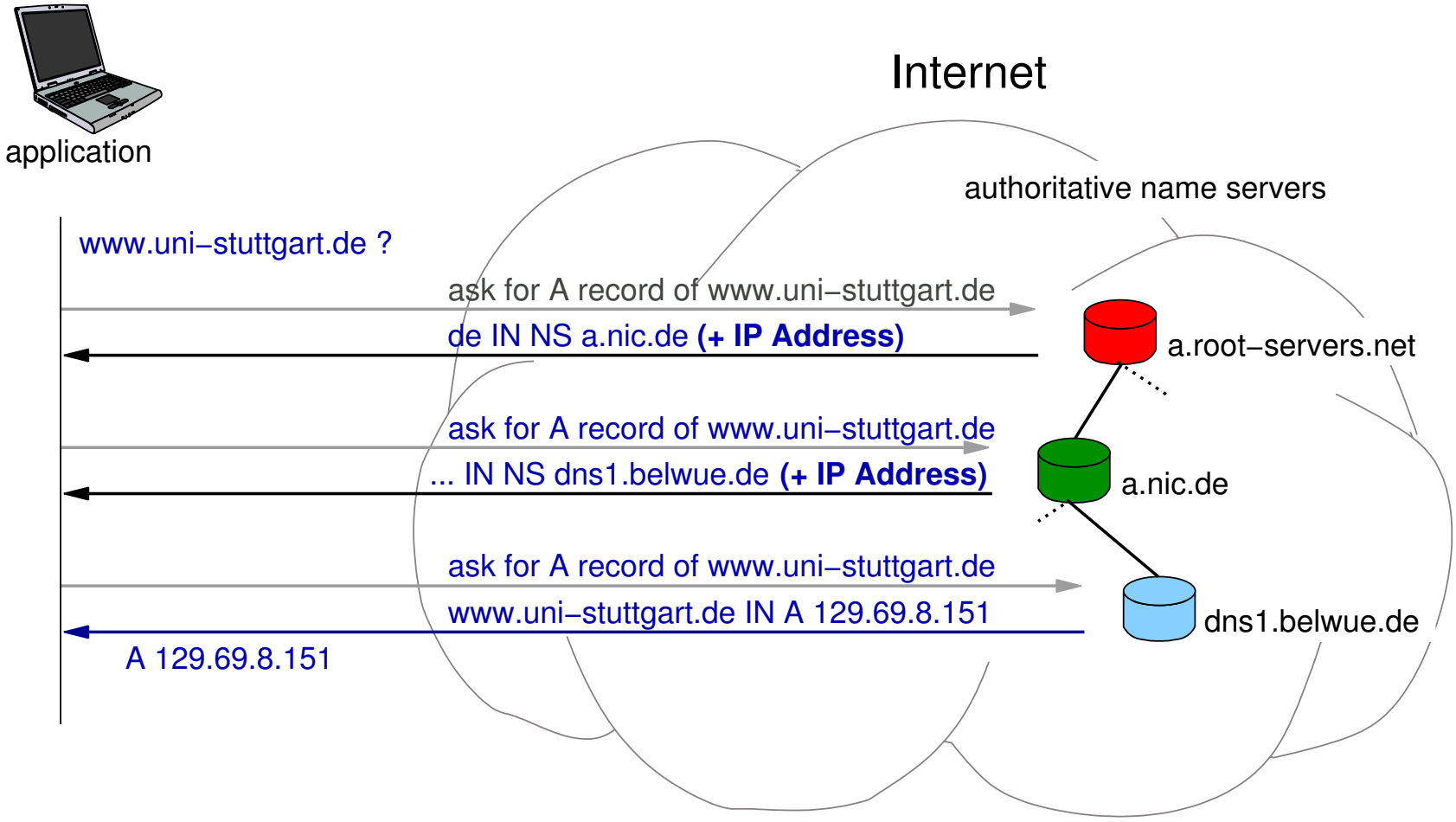
Replication – increased performance and availability

DNS Principles



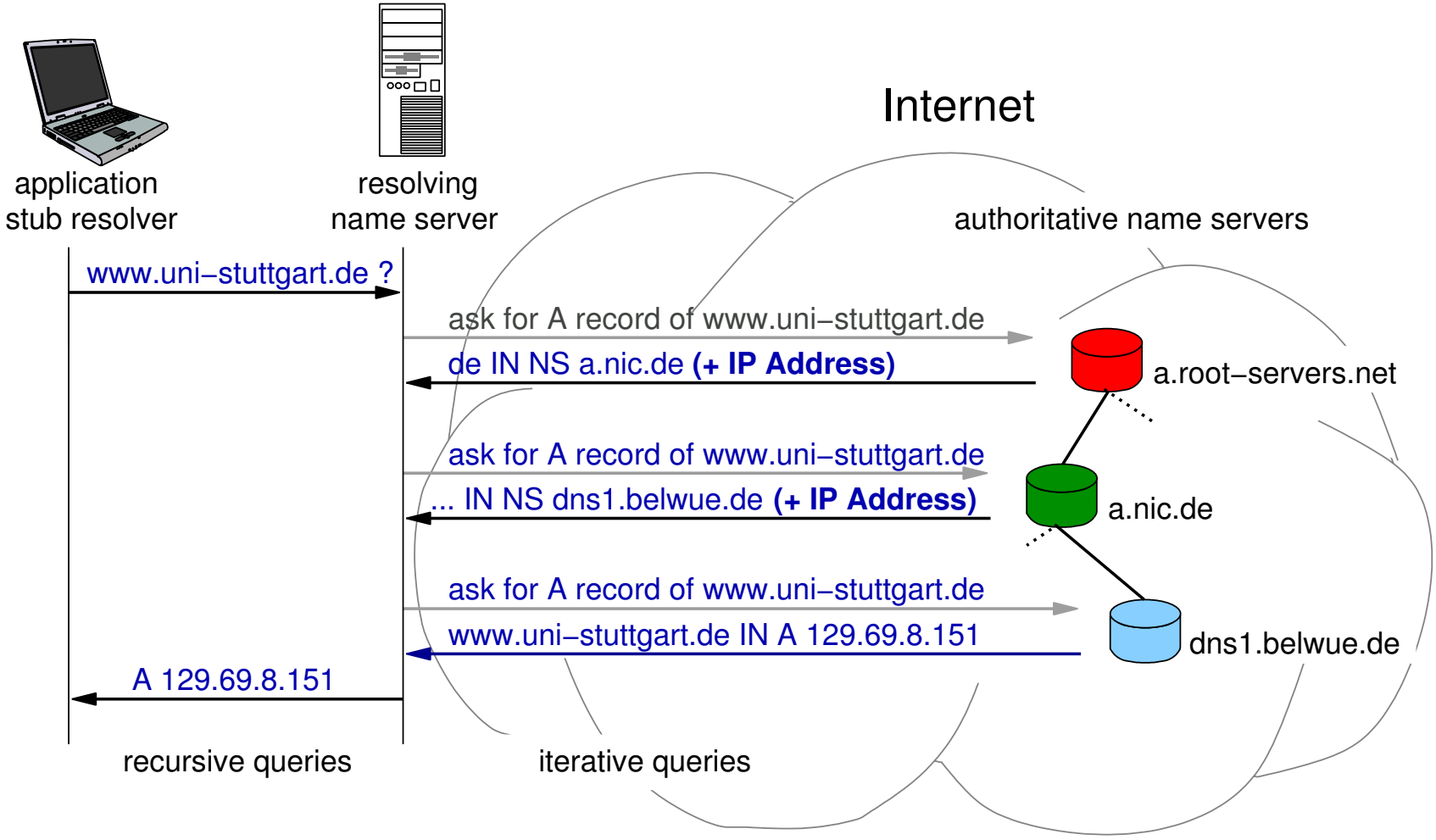
Delegation – each NS knows only parts of the data

DNS Principles



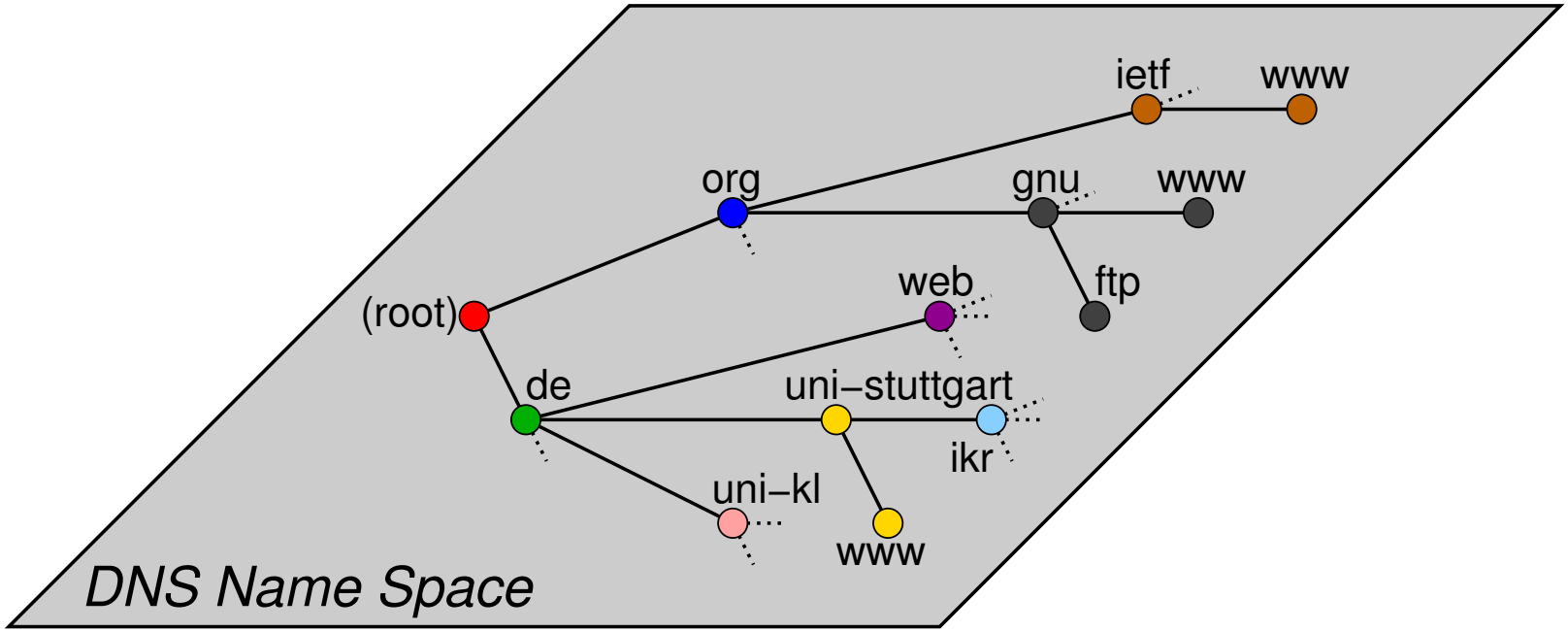
Delegation – each NS knows only parts of the data

DNS Principles

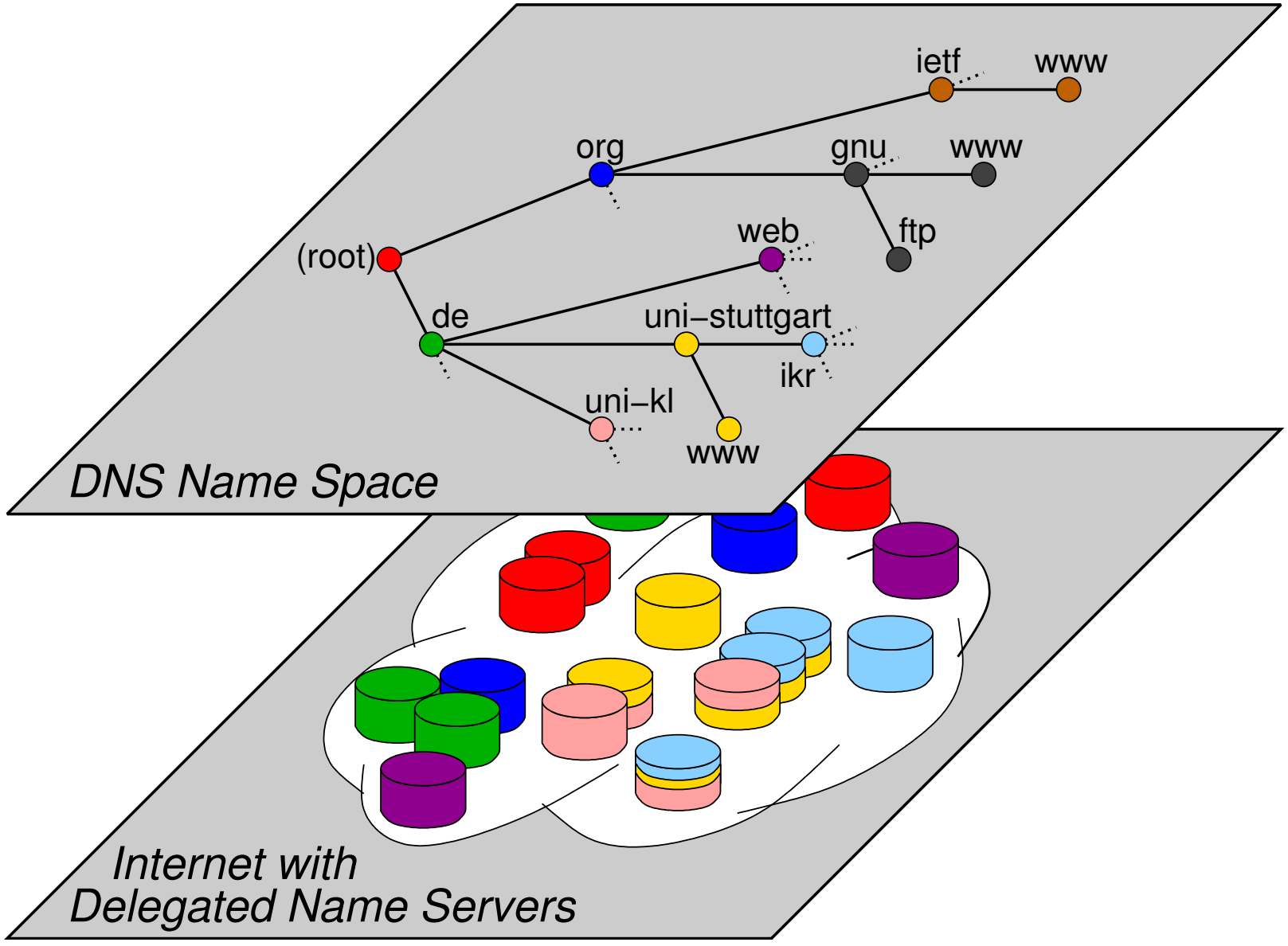


Query algorithm in Resolver – simpler clients & caching possible

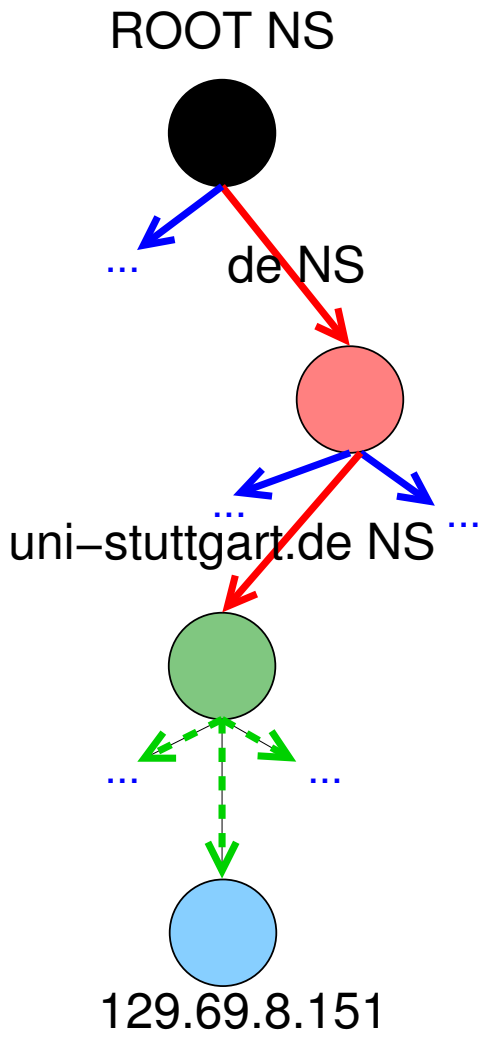
DNS Delegation and Server Structure



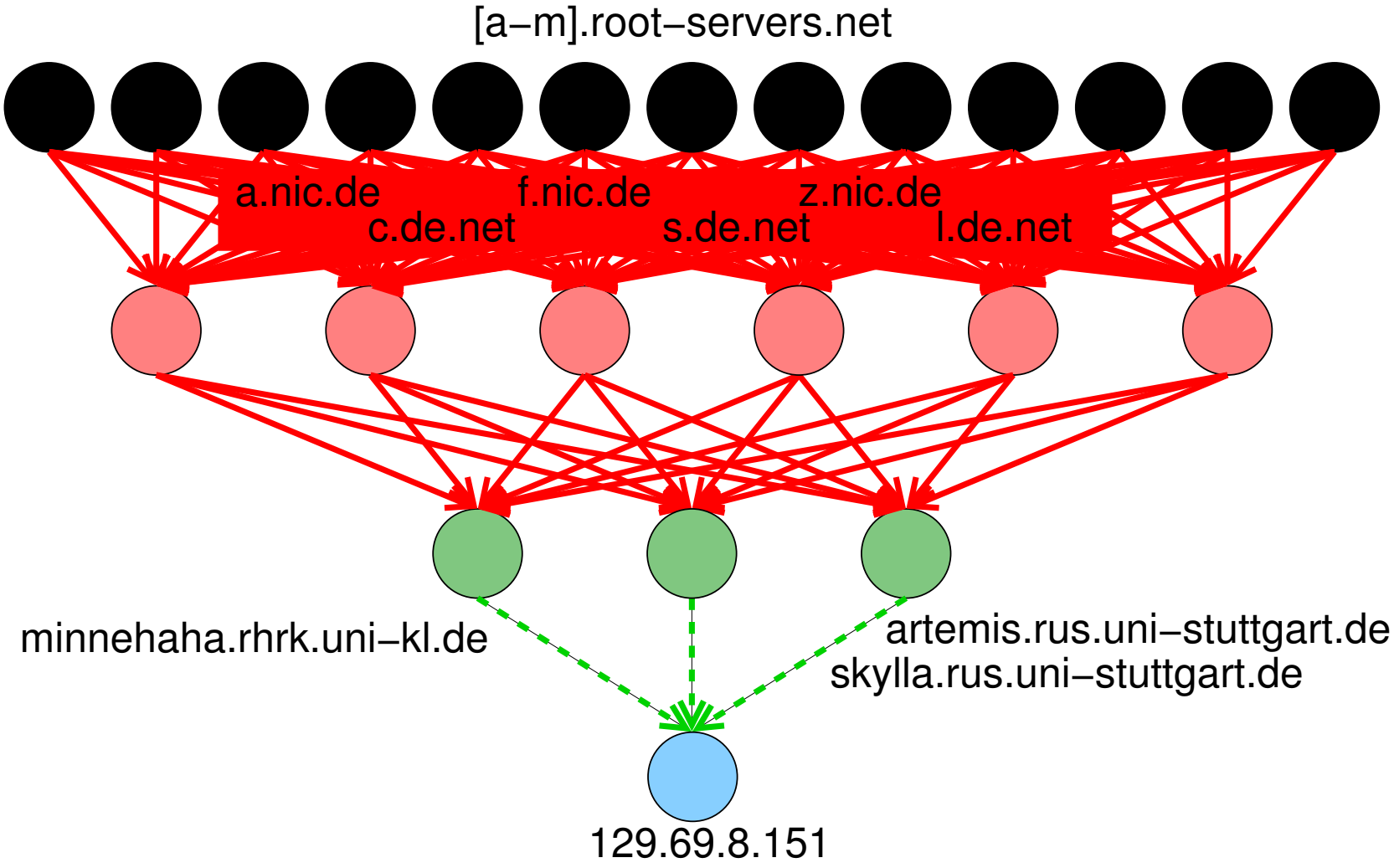
DNS Delegation and Server Structure



DNS Delegation



DNS Delegation



- **All potentially involved NS have to be trusted**

Impact of delegation: complex administration

Adminstrators of different domains are involved

- **Adminstrator of parent zone: needs to know for each delegated zone**
  - Names of delegated NS
  - IP addresses of delegated NS (glue records) – if in the same subdomain
- **Adminstrator of delegated zone: master server needs to know**
  - Addresses of slave servers that are allowed to copy data
- **Adminstrator of replicating (slave) servers need to know**
  - For which zones they act as delegated NS
  - Master server for retrieving zone data

Impact of delegation: problems

- **Outdated NS/IP address: Servers that are not responsible for the zone are queried: "Lame delegations"[1]**
  - NS might refuse to answer
  - NS might give wrong answer (NXDOMAIN, Fake A)
  - NS might serve as resolver and perform iterative queries for the name
- **Glue records not present**
  - Additional queries for NS's IP necessary

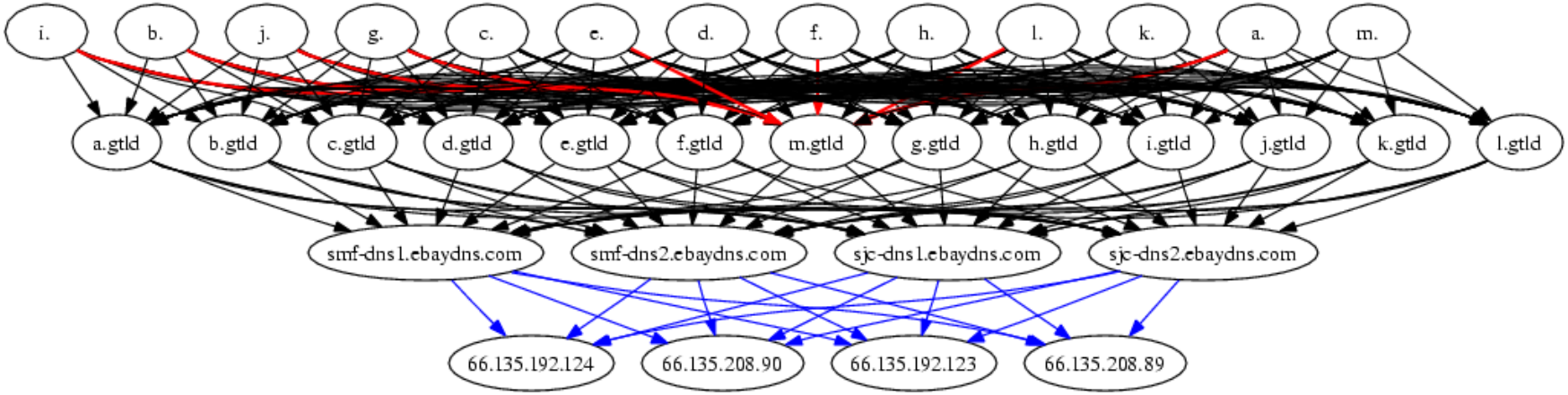
  ➥ Additional latency

  ➥ More (potentially compromised) servers contribute to answer

1. V. Pappas, Z. Xu, S. Lu, D. Massey, A. Terzis, L. Zhang: Impact of configuration errors on DNS robustness, ACM Press,2004.

Delegation - examples

www.ebay.com



- **Delegation structure without problems (almost)**

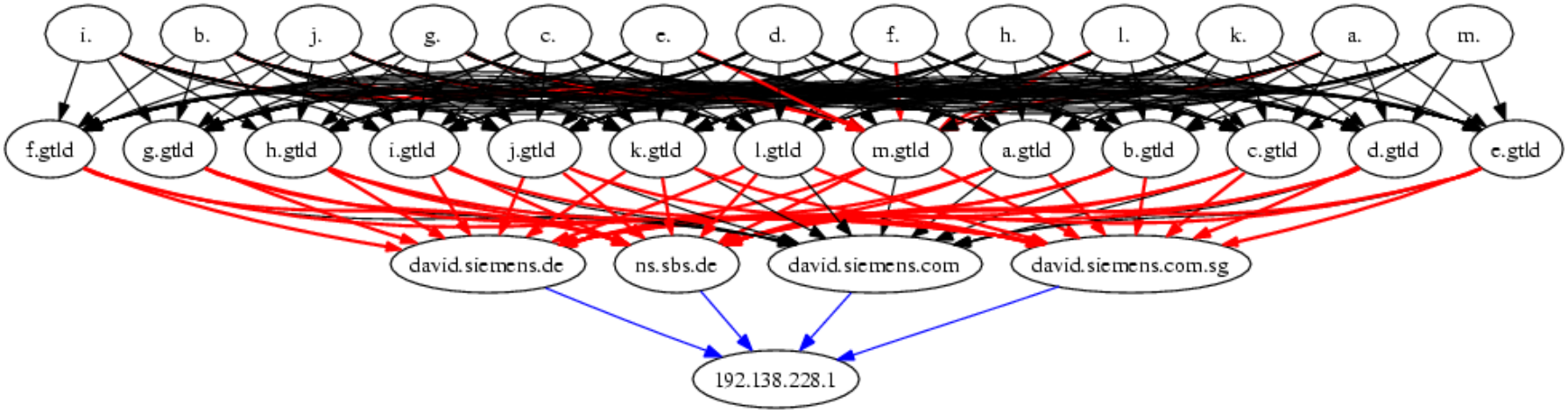
Black: Delegation with glue record

Red: Delegation without glue record

Blue: Answer

Delegation structure - examples

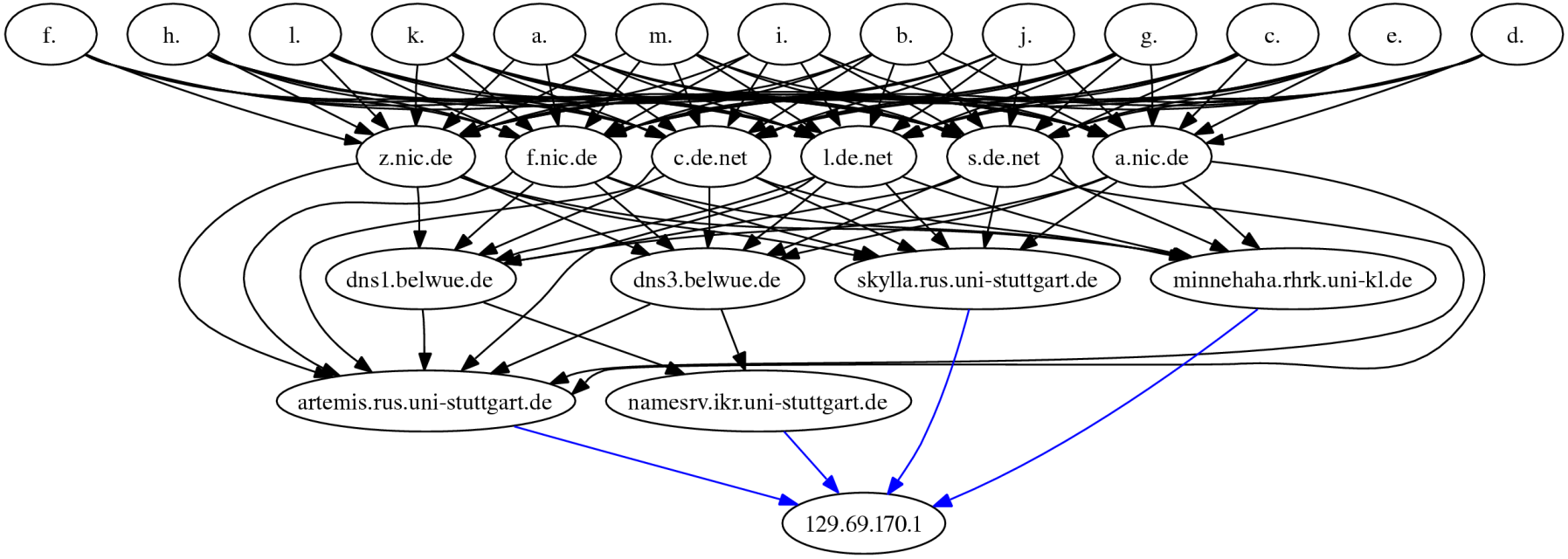
www.siemens.com



- **Missing glue for 3 of 4 NS**

Delegation structure - examples

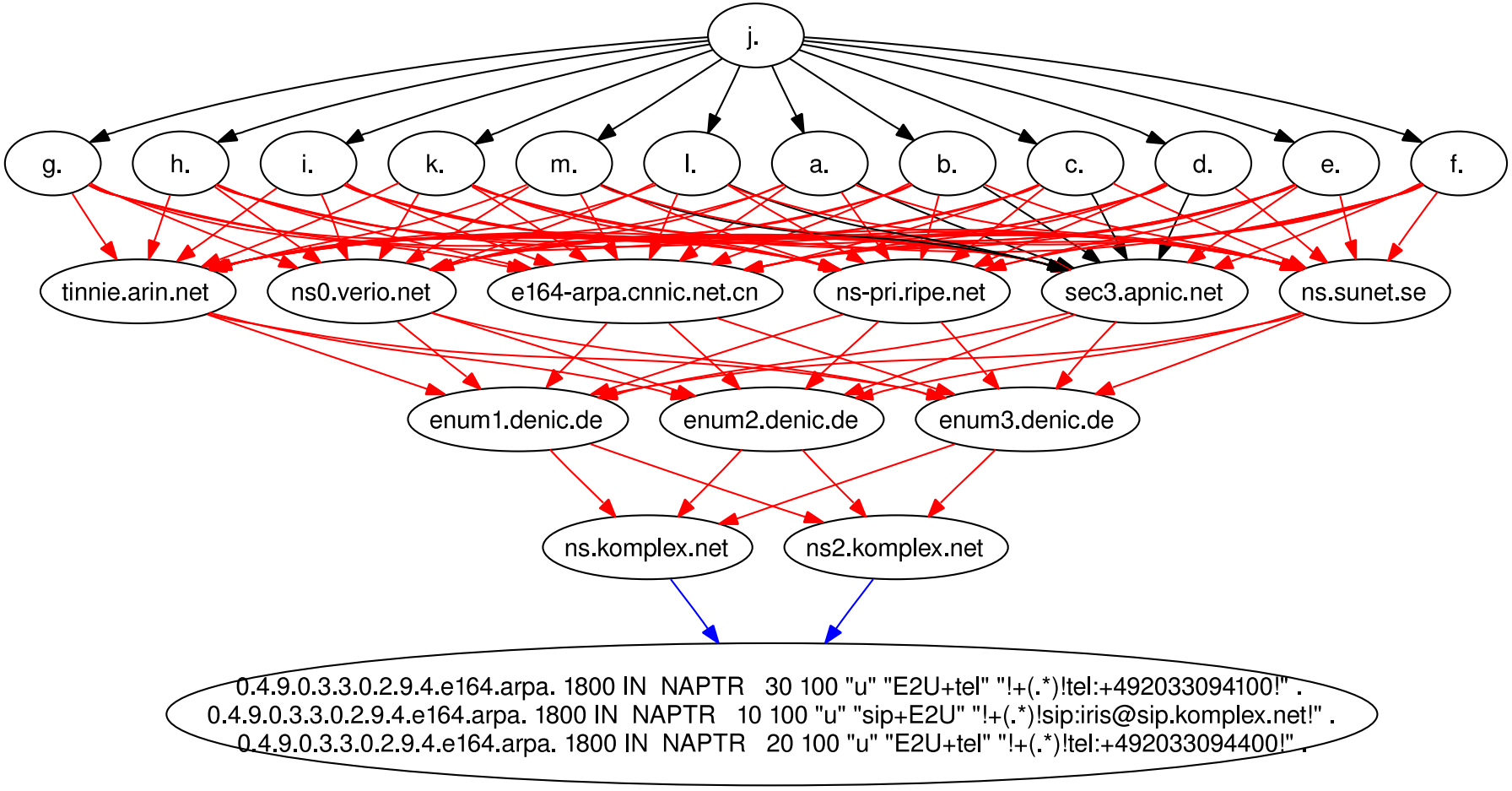
www.ikr.uni-stuttgart.de



- **Paths with different number of NS - inconsistent zone data**

Delegation structure - examples

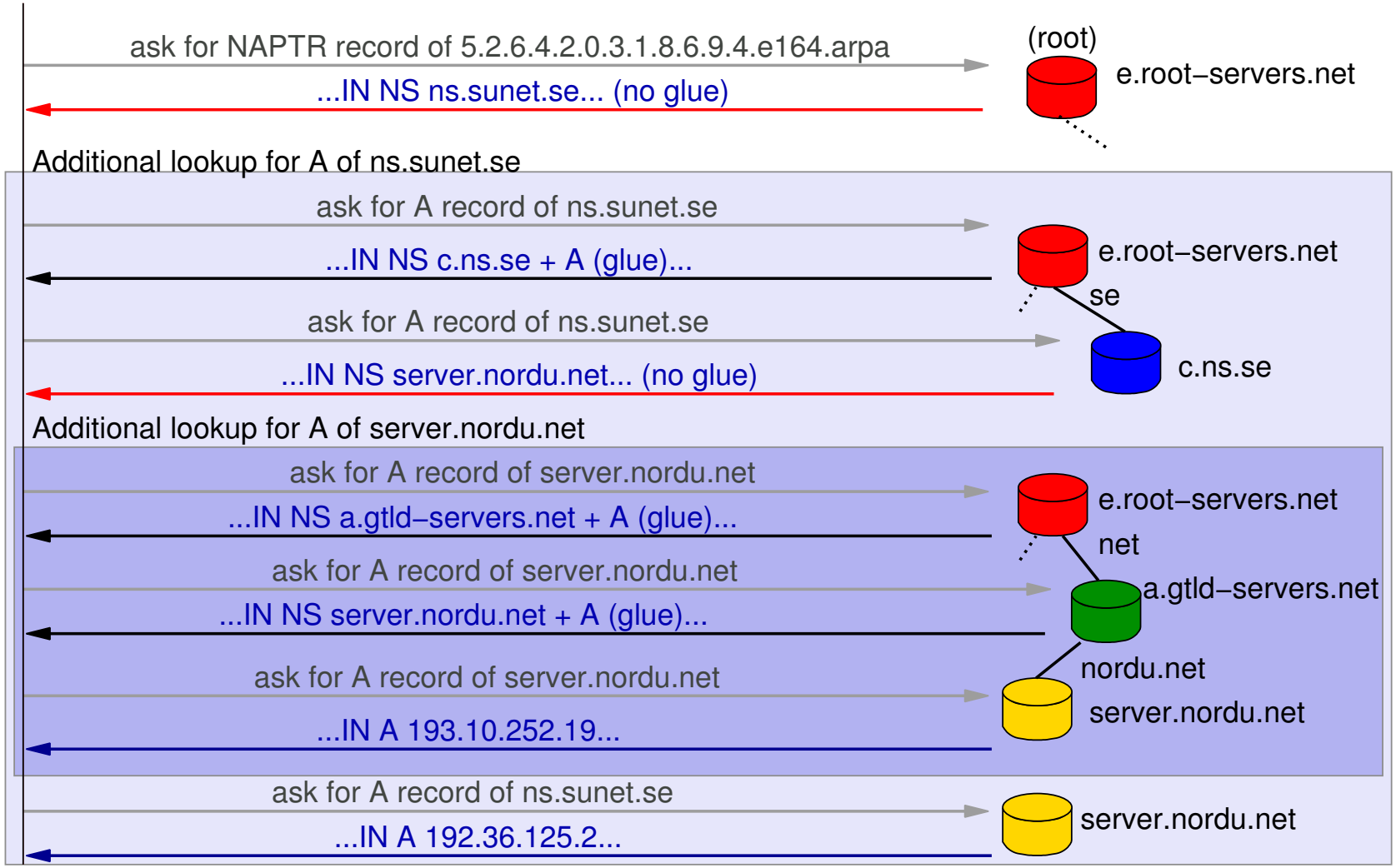
ENUM



- Root servers inconsistent – j.root-servers.net does not know e164.arpa
- Lots of glue records missing ➔ much more NS potentially involved

DNS - Missing glue records

Example: ENUM lookup



Summary

DNS Problems

- **DNS administration is evidently error-prone**
  - Even Root NS do not host the same data
  - Wrong information in parent zone causes "Lame Delegations"
- **Missing glue records**
  - Additional lookups to other NS required
  - Number of potentially involved servers unknown in advance
  - Every server that possibly can contribute to the result must be trusted

➥ **A high, unknown number of (potentially compromised) servers potentially contribute to answers**

➥ **Integrity of DNS?**

Possible solutions

DNSSEC

- **DNS Security Extensions RFC4033-4035 (March 2005)**
- **Protection of DNS Records by digital signatures**
- **Pre-configured public keys in Resolvers for establishing trust chain**
- **PKI-like administration required**
  - Distribution of new (Root-) Keys

  ➥ How to replace pre-configured keys in resolvers?
  - For each new zone: new keys have to signed by parent zone

➥ **Might lead to the same administrative problems**

➥ **Signatures expire, are invalid... → affects service availabilty**

Possible solutions

Local copy

Be Independent of the distributed DNS infrastructure

- Keep a local, verified copy of essential DNS data

➥ **Transfer of complete zone files required**

New DNS architecture

Build a centralized, replicated DNS architecture[1]

- Idea: keep all DNS data in "Root-Servers", no delegations
- For migration: delegation still possible

➥ **Paradigm shift**

➥ **Only a few servers have to be trusted**

➥ **Provisioning? ➔ For further study**

1. T. Deegan, J. Crowcroft, A. Warfield: The main name system: an exercise in centralized computing, SIGCOMM Comput. Commun. Rev., ACM Press, 2005

Conclusion and Outlook

Conclusion

- **New applications (e.g. VoIP Platforms): more than name-to-IP lookup**
  - ➥ Secure and reliable DNS required (http-over-TLS does not help)
- **Current DNS: complex, error-prone adminstration**
  - ➥ Integrity not guaranteed
- **DNSSEC might lead to the same administrative problems**

Outlook: Which is the best solution?

- **DNSSEC**
- **Local copy**
- **Paradigm shift: centralized DNS**

➥ **No general answer possible**

➥ **Further evaluation necessary**