

Rechnernetze und verteilte Systeme

Übungsblatt 12

Koenig.Noah@campus.lmu.de



Interpretation einer DNS-Antwort (H)

Ein nützliches Diagnosewerkzeug für den DNS ist das Programm `dig` (1), das auf vielen Unix-Derivaten (z.B. GNU/Linux Installationen) vorhanden ist. Nachfolgend sehen Sie die aus einer Anfrage resultierenden Resource Records. Beziehen Sie sich beim Bearbeiten der Aufgabe auf die relevanten Zeilnummern!

```
bash$ dig +trace +nodnssec mail.nm.ifi.lmu.de
```

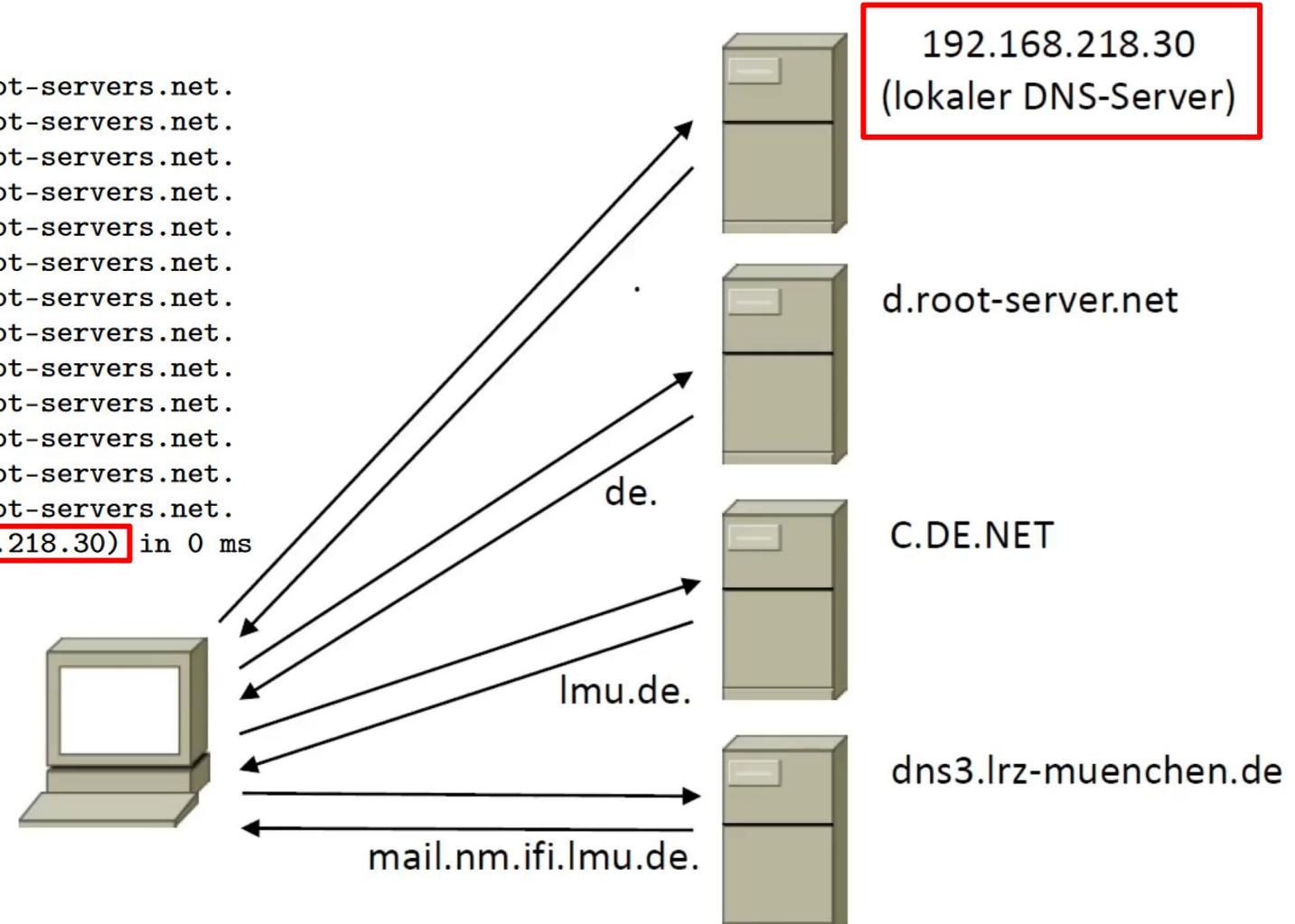
(a) Zeichnen Sie eine Skizze, die den DNS-Verkehr zur Anfrage darstellt, mit mindestens:

- dem anfragenden Host
- dem für diesen Host zuständigen DNS-Server (lokaler DNS-Server)
- dem DNS-Server, der die richtige IP-Adresse für `mail.nm.ifi.lmu.de` liefert
- eventuellen weiteren DNS-Servern, die Teile der Antwort liefern.
- den Nachrichten, die ausgetauscht wurden.

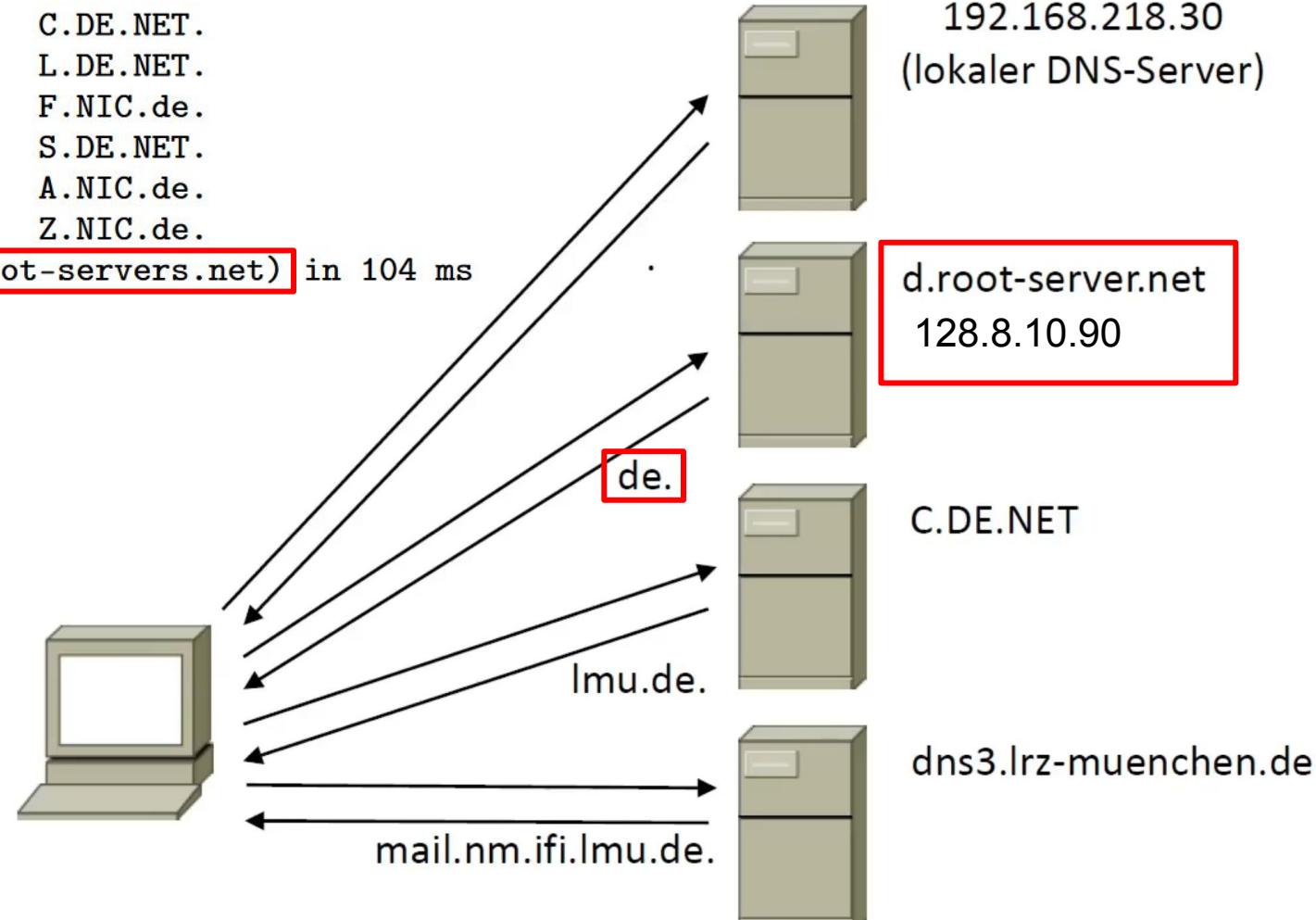
Geben Sie bei jedem Host in Ihrer Skizze, falls vorhanden, IP-Adresse und Hostname an.

```
1 ; <>> DiG 9.2.3 <>> +trace mail.nm.ifi.lmu.de
2 ;; global options: printcmd
3 .
4 .          80298 IN NS    d.root-servers.net.
5 .          80298 IN NS    e.root-servers.net.
6 .          80298 IN NS    f.root-servers.net.
7 .          80298 IN NS    j.root-servers.net.
8 .          80298 IN NS    g.root-servers.net.
9 .          80298 IN NS    h.root-servers.net.
10 .
11 .         80298 IN NS    b.root-servers.net.
12 .
13 .         80298 IN NS    l.root-servers.net.
14 .
15 .         80298 IN NS    i.root-servers.net.
16 .         80298 IN NS    c.root-servers.net.
17 .         80298 IN NS    m.root-servers.net.
18 .         80298 IN NS    a.root-servers.net.
19 .         80298 IN NS    k.root-servers.net.
20 .
21 ;; Received 500 bytes from 192.168.218.30#53(192.168.218.30) in 0 ms
```

lokaler DNS Server wird nach Root Servern gefragt



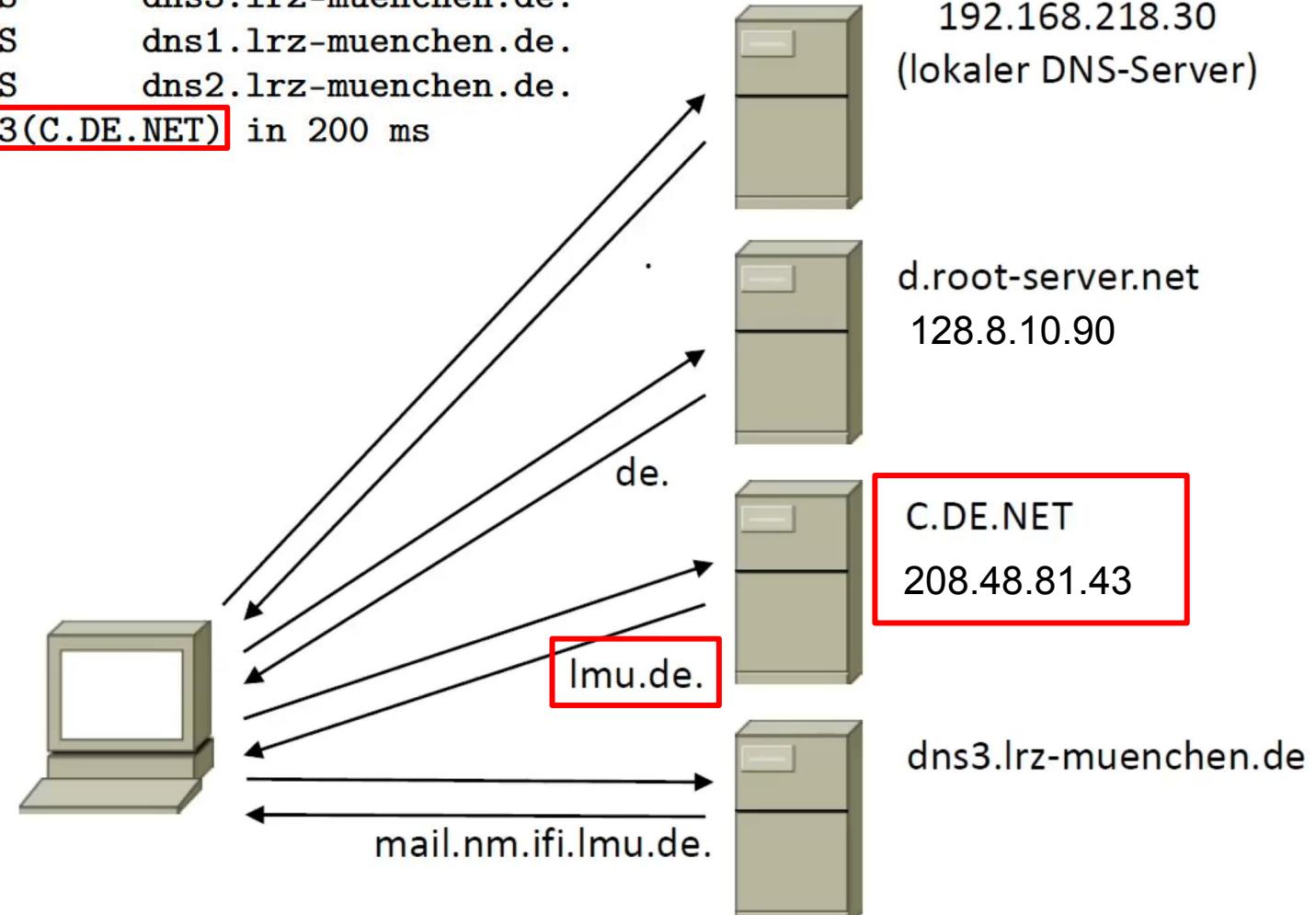
```
18 de.          172800 IN  NS  C.DE.NET.  
19 de.          172800 IN  NS  L.DE.NET.  
20 de.          172800 IN  NS  F.NIC.de.  
21 de.          172800 IN  NS  S.DE.NET.  
22 de.          172800 IN  NS  A.NIC.de.  
23 de.          172800 IN  NS  Z.NIC.de.  
24 ;; Received 294 bytes from 128.8.10.90#53(d.root-servers.net) in 104 ms
```



d.root-server.net wird nach Servern,
die für die Top Level Domain (TLD)
.de zuständig sind, gefragt

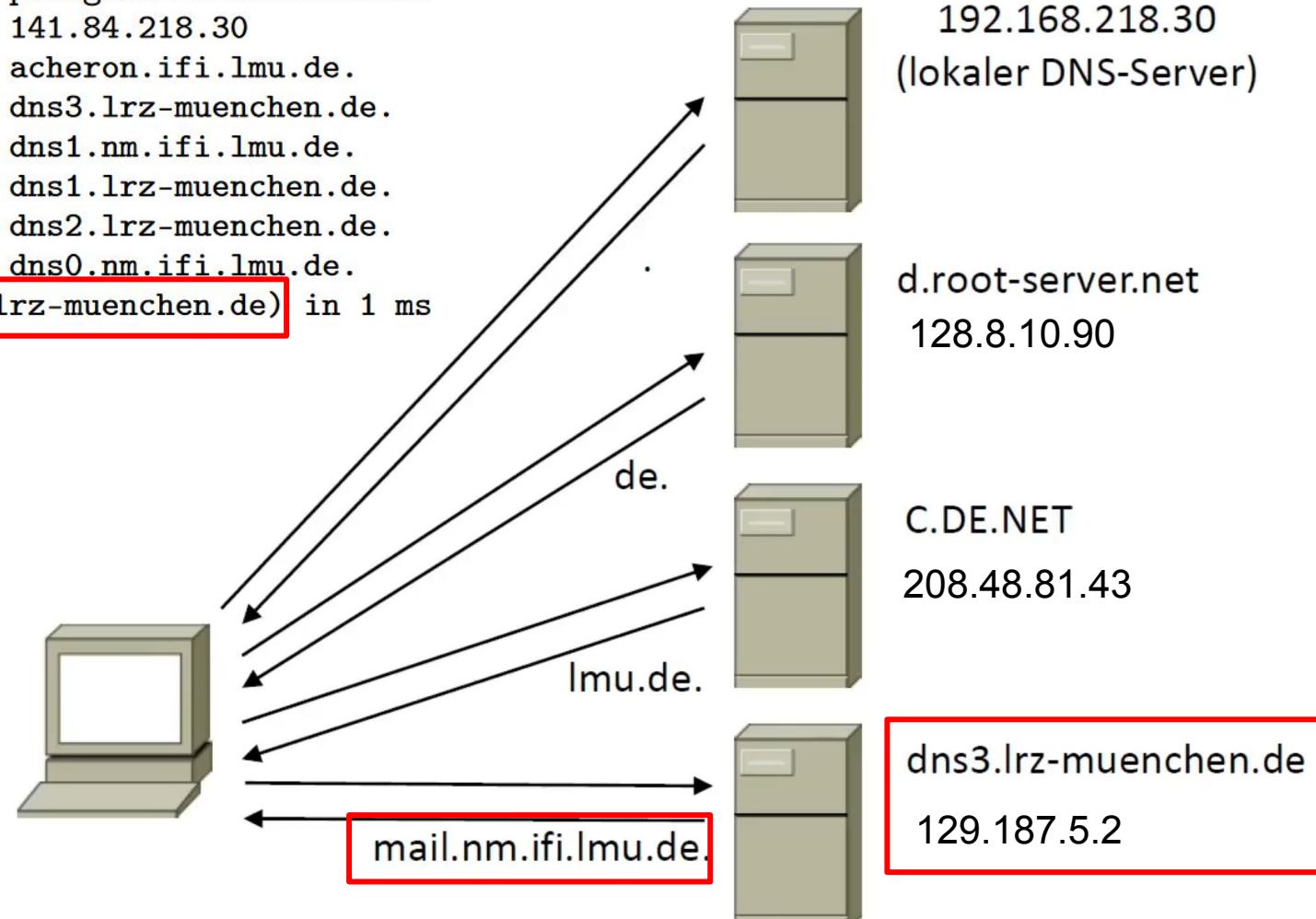
```
26 lmu.de.          86400  IN      NS      dns3.lrz-muenchen.de.  
27 lmu.de.          86400  IN      NS      dns1.lrz-muenchen.de.  
28 lmu.de.          86400  IN      NS      dns2.lrz-muenchen.de.  
29 ;; Received 210 bytes from 208.48.81.43#53(C.DE.NET) in 200 ms
```

C.DE.NET wird nach für lmu.de zuständige Server gefragt



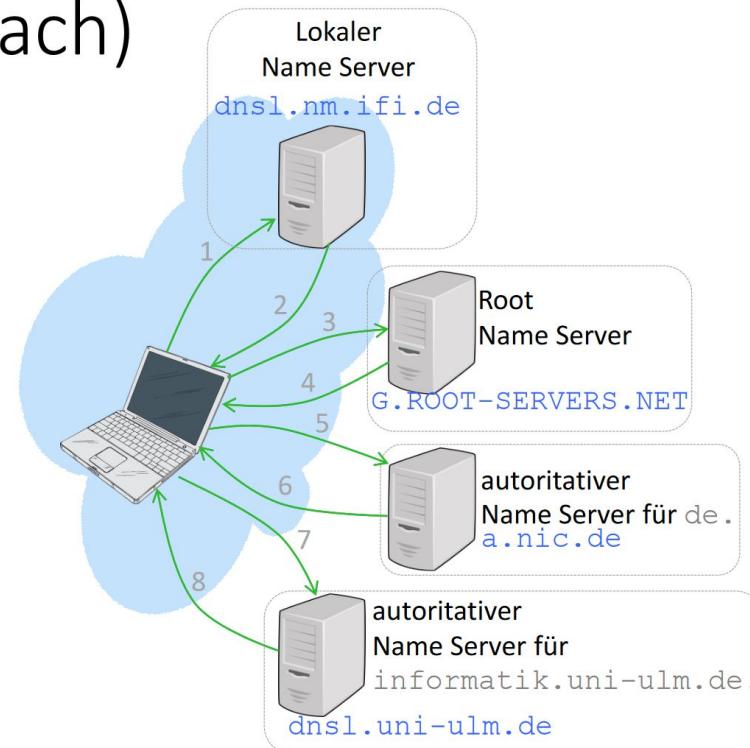
```
31 mail.nm.ifi.lmu.de. 86400 IN CNAME pcheger0.nm.ifi.lmu.de.  
32 pcheger0.nm.ifi.lmu.de. 86400 IN A 141.84.218.30  
33 nm.ifi.lmu.de. 86400 IN NS acheron.ifi.lmu.de.  
34 nm.ifi.lmu.de. 86400 IN NS dns3.lrz-muenchen.de.  
35 nm.ifi.lmu.de. 86400 IN NS dns1.nm.ifi.lmu.de.  
36 nm.ifi.lmu.de. 86400 IN NS dns1.lrz-muenchen.de.  
37 nm.ifi.lmu.de. 86400 IN NS dns2.lrz-muenchen.de.  
38 nm.ifi.lmu.de. 86400 IN NS dns0.nm.ifi.lmu.de.  
39 ;; Received 357 bytes from 129.187.5.2#53(dns3.lrz-muenchen.de) in 1 ms
```

dns3.lrz-muenchen.de wird nach für nm.ifi.lmu.de zuständigen Servern gefragt

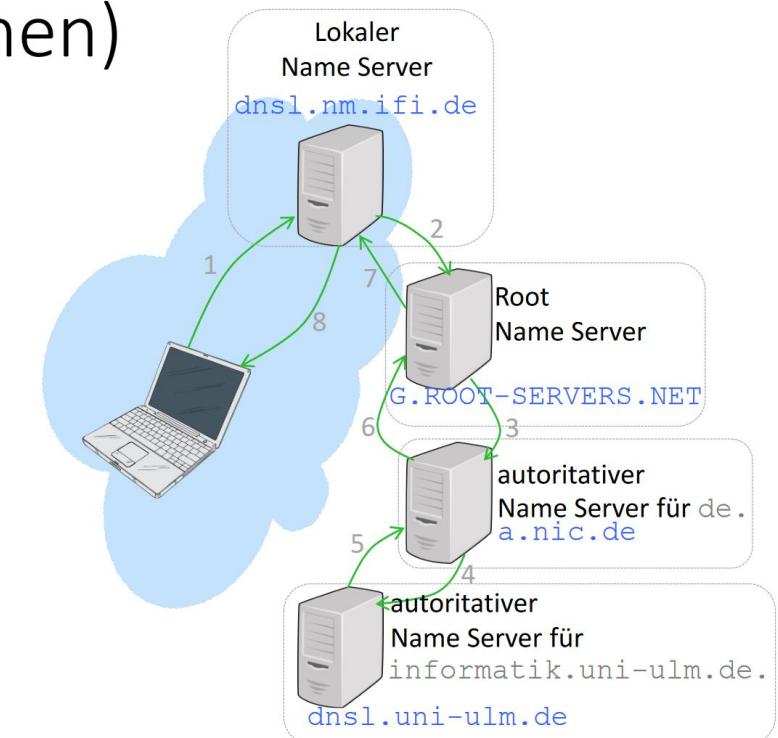


(b) Ist die Anfrage rekursiv oder iterativ?

DNS: Iterative Anfrage
(Der Reihe nach)



DNS: Rekursive Anfrage:
(Durchreichen)



→ iterativ (sonst würden wir nur die angefragte Info erhalten)

- (c) Die Ausgabe enthält eine Anfrage an einen der DNS-Root-Server. Wonach wird er gefragt?

Er wurde nach den für .de zuständigen Servern gefragt

```
18      de.          172800  IN      NS      C.DE.NET.  
19      de.          172800  IN      NS      L.DE.NET.  
20      de.          172800  IN      NS      F.NIC.de.  
21      de.          172800  IN      NS      S.DE.NET.  
22      de.          172800  IN      NS      A.NIC.de.  
23      de.          172800  IN      NS      Z.NIC.de.  
24  ;; Received 294 bytes from 128.8.10.90#53(d.root-servers.net) in 104 ms
```

(d) Der gesuchte Rechnername `mail.nm.ifi.lmu.de` ist ein Alias.

i. Wie heisst die Maschine wirklich?

pcheger0 (CNAME = Canonical (= true) Name)

ii. Welche IP-Adresse hat sie?

141.84.218.30 (A = (IPv4)-Adress)

```
31 mail.nm.ifi.lmu.de. 86400 IN CNAME pcheger0.nm.ifi.lmu.de.  
32 pcheger0.nm.ifi.lmu.de. 86400 IN A 141.84.218.30  
33 nm.ifi.lmu.de. 86400 IN NS acheron.ifi.lmu.de.  
34 nm.ifi.lmu.de. 86400 IN NS dns3.lrz-muenchen.de.  
35 nm.ifi.lmu.de. 86400 IN NS dns1.nm.ifi.lmu.de.  
36 nm.ifi.lmu.de. 86400 IN NS dns1.lrz-muenchen.de.  
37 nm.ifi.lmu.de. 86400 IN NS dns2.lrz-muenchen.de.  
38 nm.ifi.lmu.de. 86400 IN NS dns0.nm.ifi.lmu.de.  
39 ;; Received 357 bytes from 129.187.5.2#53(dns3.lrz-muenchen.de) in 1 ms
```

- (e) Anhand der Ausgabe können weitere Aussagen bezüglich der DNS-Server gemacht werden:
- Wer betreibt die DNS-Server, die für Anfragen über die Domäne `lmu.de`. zuständig sind?

Die DNS-Server für `lmu.de` betreibt das LRZ

```
26      lmu.de.          86400   IN      NS      dns3.lrz-muenchen.de.  
27      lmu.de.          86400   IN      NS      dns1.lrz-muenchen.de.  
28      lmu.de.          86400   IN      NS      dns2.lrz-muenchen.de.  
29      ;; Received 210 bytes from 208.48.81.43#53(C.DE.NET) in 200 ms
```

ii. Welche DNS-Server können Anfragen für die Domäne der gesuchten Maschine liefern?

```
31 mail.nm.ifi.lmu.de. 86400 IN CNAME pcheger0.nm.ifi.lmu.de.  
32 pcheger0.nm.ifi.lmu.de. 86400 IN A 141.84.218.30  
33 nm.ifi.lmu.de. 86400 IN NS acheron.ifi.lmu.de.  
34 nm.ifi.lmu.de. 86400 IN NS dns3.lrz-muenchen.de.  
35 nm.ifi.lmu.de. 86400 IN NS dns1.nm.ifi.lmu.de.  
36 nm.ifi.lmu.de. 86400 IN NS dns1.lrz-muenchen.de.  
37 nm.ifi.lmu.de. 86400 IN NS dns2.lrz-muenchen.de.  
38 nm.ifi.lmu.de. 86400 IN NS dns0.nm.ifi.lmu.de.  
39 ;; Received 357 bytes from 129.187.5.2#53(dns3.lrz-muenchen.de) in 1 ms
```

iii. Wurde die gesuchte IP-Adresse von einem autoritativen Server geliefert?

Ja, siehe “NS” (= Name Server, Hostname eines autoritativen Nameservers).
Primäre Server: Originalkopie der DNS-Infos; Sekundäre Server: Kopie der DNS-Infos

Nicht autorativ: Server speichert DNS-Infos temporär (*cachen*)

- (f) Angenommen Sie haben als Administrator Zugriff auf den DNS-Cache der lokalen DNS-Server im LRZ. Gibt es für Sie damit eine Möglichkeit, die von Nutzern meist besuchten Web-Server im Internet ausfindig zu machen Fassen Sie sich kurz.

Cache Snapshots in regelmäßigen Abständen abziehen und erkennen, welche Adressen von Web-Servern immer wieder im Cache auftauchen

HTTP Requests und Response (H)

Die folgende ASCII-Zeichenkette wurde mit Hilfe des Wireshark-Programms aufgezeichnet, als ein Web-Browser einen HTTP GET-Request sendete. Zu sehen ist also der komplette Request. Die Zeichen <cr><lf> stehen dabei für *Carriage Return* und *Line Feed*, wie es im Nachrichtenformat in der Vorlesung gekennzeichnet war.

```
GET /gnu/gnu.html HTTP/1.1<cr><lf>Host: www.gnu.org<cr><lf>User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0<cr><lf>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<cr><lf>Accept-Language: de-DE,en-US;q=0.7,en;q=0.3<cr><lf>Accept-Encoding: gzip, deflate, br<cr><lf>Connection: keep-alive<cr><lf><cr><lf>
```

(a) Wie lautet die URL des Dokuments, das vom Browser angefragt wurde?

```
GET /gnu/gnu.html HTTP/1.1<cr><lf>Host: www.gnu.org<cr><lf>User-Agent:  
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101  
Firefox/67.0<cr><lf>Accept: text/html,application/xhtml+xml,  
application/xml;q=0.9,*/*;q=0.8<cr><lf>Accept-Language: de-DE,en-US;  
q=0.7,en;q=0.3<cr><lf>Accept-Encoding: gzip, deflate, br<cr><lf>  
Connection: keep-alive<cr><lf><cr><lf>
```

Zusammensetzen aus Host-Header und Request-Zeile (GET...):

<http://www.gnu.org/gnu/gnu.html>

(b) Welche HTTP-Version nutzt der Browser?

HTTP 1.1

(c) Fragt der Browser eine persistente oder nicht-persistente Verbindung an?

persistent (Connection: keep-alive)

→ nachfolgende Requests werden über gleiche TCP-Verbindung gesendet

→ einmaliger Verbindungsaufbau

```
GET /gnu/gnu.html HTTP/1.1<cr><lf>Host: www.gnu.org<cr><lf>User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0<cr><lf>Accept: text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8<cr><lf>Accept-Language: de-DE,en-US;q=0.7,en;q=0.3<cr><lf>Accept-Encoding: gzip, deflate, br<cr><lf>Connection: keep-alive<cr><lf><cr><lf>
```

(d) Welche IP hat der Host, auf dem der Browser ausgeführt wird?

IP-Adresse ist nicht enthalten, da sie nicht benötigt wird (TCP-Verbindung besteht bereits)

```
GET /gnu/gnu.html HTTP/1.1<cr><lf>Host: www.gnu.org<cr><lf>User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0<cr><lf>Accept: text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8<cr><lf>Accept-Language: de-DE,en-US;q=0.7,en;q=0.3<cr><lf>Accept-Encoding: gzip, deflate, br<cr><lf>Connection: keep-alive<cr><lf><cr><lf>
```

(e) Welcher Browser-Typ hat den Request abgeschickt? Wozu dient die Übermittlung des Typs und ist sie notwendig?

- Browser-Typ: Firefox 67
- Übermittlung des Typs dient zur Anpassung der Server Antwort an den Browser, ist aber nicht notwendig, damit der Server eine korrekte Antwort schicken kann

```
GET /gnu/gnu.html HTTP/1.1<cr><lf>Host: www.gnu.org<cr><lf>User-Agent:  
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101  
Firefox/67.0<cr><lf>Accept: text/html, application/xhtml+xml,  
application/xml;q=0.9,*/*;q=0.8<cr><lf>Accept-Language: de-DE,en-US;  
q=0.7,en;q=0.3<cr><lf>Accept-Encoding: gzip, deflate, br<cr><lf>  
Connection: keep-alive<cr><lf><cr><lf>
```

Der Server antwortet nun mit der folgenden HTTP-Response auf die oben gezeigte Anfrage.

```
HTTP/1.1 200 OK<cr><lf>Date: Thu, 23 May 2019 08:27:34 GMT<cr><lf>Server: Apache/2.4.7<cr><lf>Content-Location: gnu.html<cr><lf>Accept-Ranges: bytes<cr><lf>Content-Encoding: gzip<cr><lf>Content-Length: 5751<cr><lf>Keep-Alive: timeout=3, max=98<cr><lf>Connection: Keep-Alive<cr><lf>Content-Type: text/html<cr><lf>Content-Language: en<cr><lf><cr><lf><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"<cr><lf>      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><cr><lf><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><cr><lf><head><cr><lf><!-- start of server/head - include -1.html --><... weitere Zeichen der Antwort wurden entfernt...>
```

(f) Konnte der Server das angefragte Dokument erfolgreich finden? Zu welcher Zeit wurde die Antwort generiert?

- “200 OK” gibt an, dass Request erfolgreich war
- Zeit: 23. Mai 2019 8:27 Uhr *Greenwich Mean Time* (standardisiertes Zeitformat)

(g) In welcher Sprache ist die Antwort formuliert?

Siehe Content-Language-Header: Englisch

```
HTTP/1.1 200 OK<cr><lf>Date: Thu, 23 May 2019 08:27:34 GMT<cr><lf>
Server: Apache/2.4.7<cr><lf>Content-Location: gnu.html<cr><lf>Accept-
Ranges: bytes<cr><lf>Content-Encoding: gzip<cr><lf>Content-Length:
5751<cr><lf>Keep-Alive: timeout=3, max=98<cr><lf>Connection: Keep-
Alive<cr><lf>Content-Type: text/html<cr><lf>Content-Language: en<cr>
```

(h) Wie viele Bytes enthält das zurück gegebende Dokument?

Siehe Content-Length-Header: 5751 Byte

```
HTTP/1.1 200 OK<cr><lf>Date: Thu, 23 May 2019 08:27:34 GMT<cr><lf>
Server: Apache/2.4.7<cr><lf>Content-Location: gnu.html<cr><lf>Accept-
Ranges: bytes<cr><lf>Content-Encoding: gzip<cr><lf>Content-Length:
5751<cr><lf>Keep-Alive: timeout=3, max=98<cr><lf>Connection: Keep-
Alive<cr><lf>Content-Type: text/html<cr><lf>Content-Language: en<cr><lf><cr><lf><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
```

(i) Wie lauten die ersten 5 Bytes des zurück gegebenen Dokuments? Hat der Server die Anfrage nach einer persistenten Verbindung bestätigt?

- Die ersten 5 ASCII-Zeichen entsprechen den ersten 5 Byte: <!DOC
- Der Server akzeptiert die persistente Verbindung

```
HTTP/1.1 200 OK<cr><lf>Date: Thu, 23 May 2019 08:27:34 GMT<cr><lf>
Server: Apache/2.4.7<cr><lf>Content-Location: gnu.html<cr><lf>Accept-
Ranges: bytes<cr><lf>Content-Encoding: gzip<cr><lf>Content-Length:
5751<cr><lf>Keep-Alive: timeout=3, max=98<cr><lf>Connection: Keep-
Alive<cr><lf>Content-Type: text/html<cr><lf>Content-Language: en<cr><lf><cr><lf><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN
"<cr><lf>      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><cr>
```

Zyklische Redundanzprüfung (CRC)

- Betrachte d Datenbits als Koeffizienten für ein Polynom mit d Termen.
- Sender und Empfänger vereinbaren ein $r+1$ bit-pattern, was als Generatorpolynom G aufgefasst wird.
- Der Sender berechnet r zusätzliche Bits (**R**) als Prüfsumme, sodass die Kombination aus d Datenbits und r teilbar durch G ist.
- Empfänger teilt empfangene Nachricht ebenfalls durch G.
- **Wenn Rest = 0, ist die Nachricht fehlerfrei übertragen.**

Kapitel 5
Hardwarenahe
Schichten
Folie 65

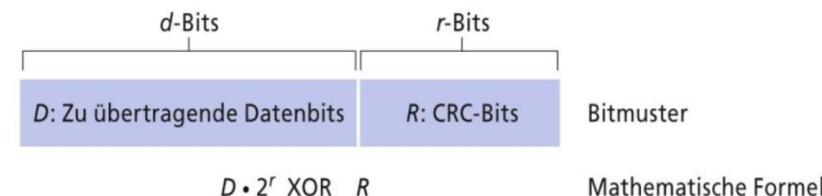


Abbildung 5.6: CRC-Codes.

CRC (H)

- (a) Gegeben sei das Generatorpolynom $G = x^3 + 1$.
- Durch wie viele Bits wird G bei CRC repräsentiert?

Grad von G r = 3
→ r + 1 = 4 Bit

- ii. Es soll die Nachricht 11 00 11 CRC-geschützt übertragen werden. Berechnen Sie die zu übertragende Bitfolge (inkl. CRC-Prüfsumme) unter Verwendung des Generatorpolynoms G .

- Füge r (= 3) Null-Bits an die **Nachricht**:

110011000

- Berechne G :

$$x^3 + 1 = 1 * x^3 + 0 * x^2 + 0 * x^1 + 1 * x^0$$

$$\rightarrow G = 1001$$

- Berechne **Rest** über XOR (siehe nächste Folie):

110011000 : 1001

- Hänge Rest an **Nachricht**, um zu übertragende Bitfolge zu erhalten:

110011101

110011000 : 1001
1001

01011

1001

001010

1001

001100

1001

101 \leftarrow Rest, Bitfolge ist 110011101

XOR Regeln:

0	XOR	0	\rightarrow	0
0	XOR	1	\rightarrow	1
1	XOR	0	\rightarrow	1
1	XOR	1	\rightarrow	0

- iii. Nehmen Sie an, dass Sie die CRC-geschützte Bitfolge 10 01 10 01 empfangen haben. Zeigen Sie, dass die empfangene Bitfolge unter Verwendung des Generatorpolynoms G korrekt ist (inkl. Rechnung). Markieren Sie in Ihrer Rechnung die Stelle, an der der Empfänger die Korrektheit ablesen kann.

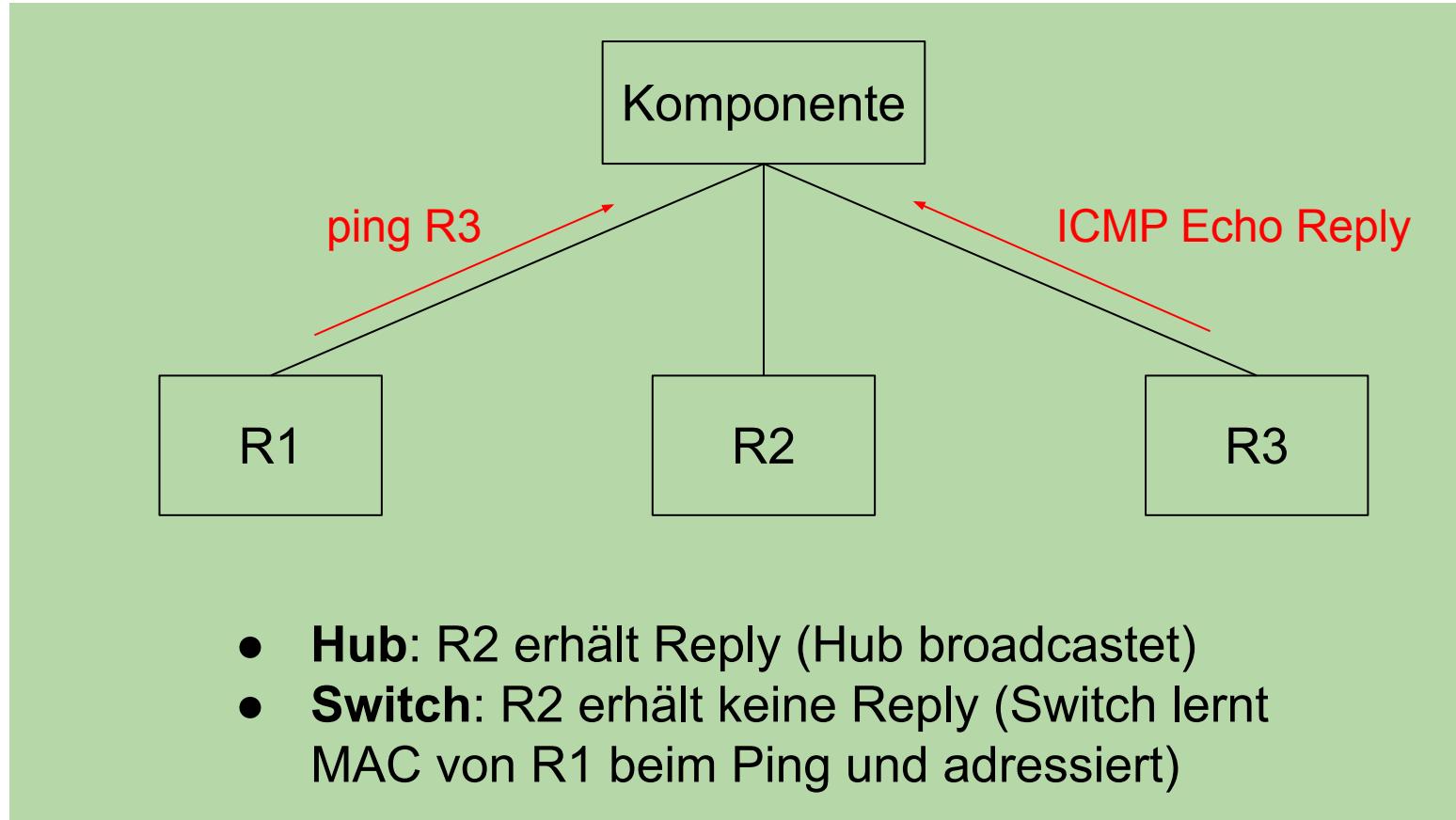
```
10011001 : 1001
 1001
 -----
 00001001
   1001
 -----
 0000 ← korrekt, da Rest 0
```

Was ist es, was kann es?

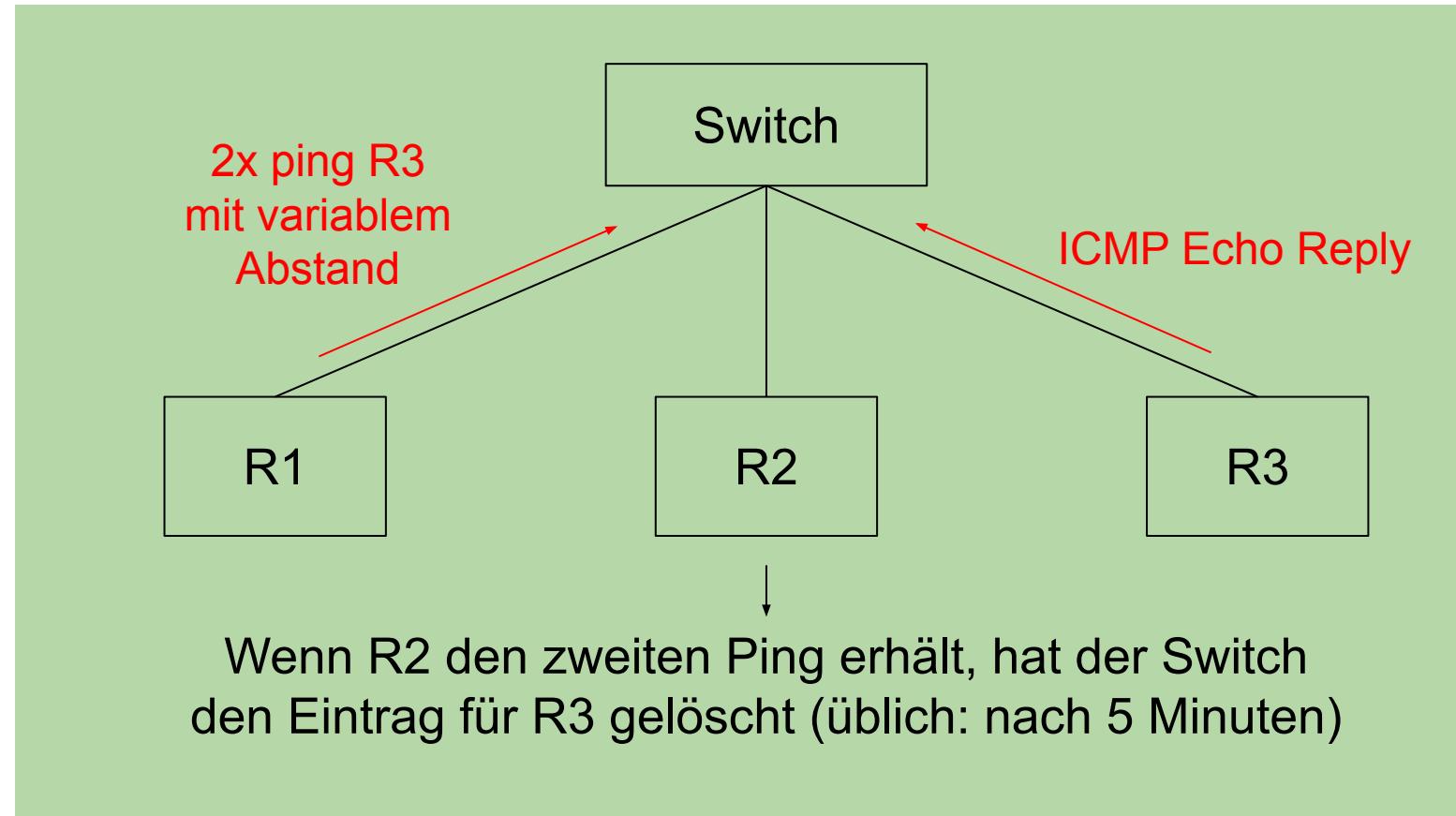
Sie finden in einem Büroschrank eine unbeschriftete Komponente mit 5 RJ45-Ports, von der Sie nur wissen, dass diese entweder ein Hub oder ein Switch ist. Sie haben außerdem drei Rechner mit je einer Netzschnittstelle und ausreichend Twisted-Pair-Kabel. Auf den Rechnern können Sie das Programm `ping` und/oder einen Protokoll-Analysator (z.B. `wireshark`) einsetzen, mit dem Sie sich alle eingehenden und ausgehenden Rahmen vollständig anzeigen lassen können.

Bei allen folgenden Untersuchungen soll das Ergebnis nur durch funktionale Tests und logisches Schlussfolgern bestimmt werden. Erstellen Sie eine Skizze Ihres Versuchsaufbaus und geben Sie die Sequenz der Aktionen (z.B. Programmaufrufe) an. Begründen Sie, warum Ihr Test das richtige Ergebnis liefert!

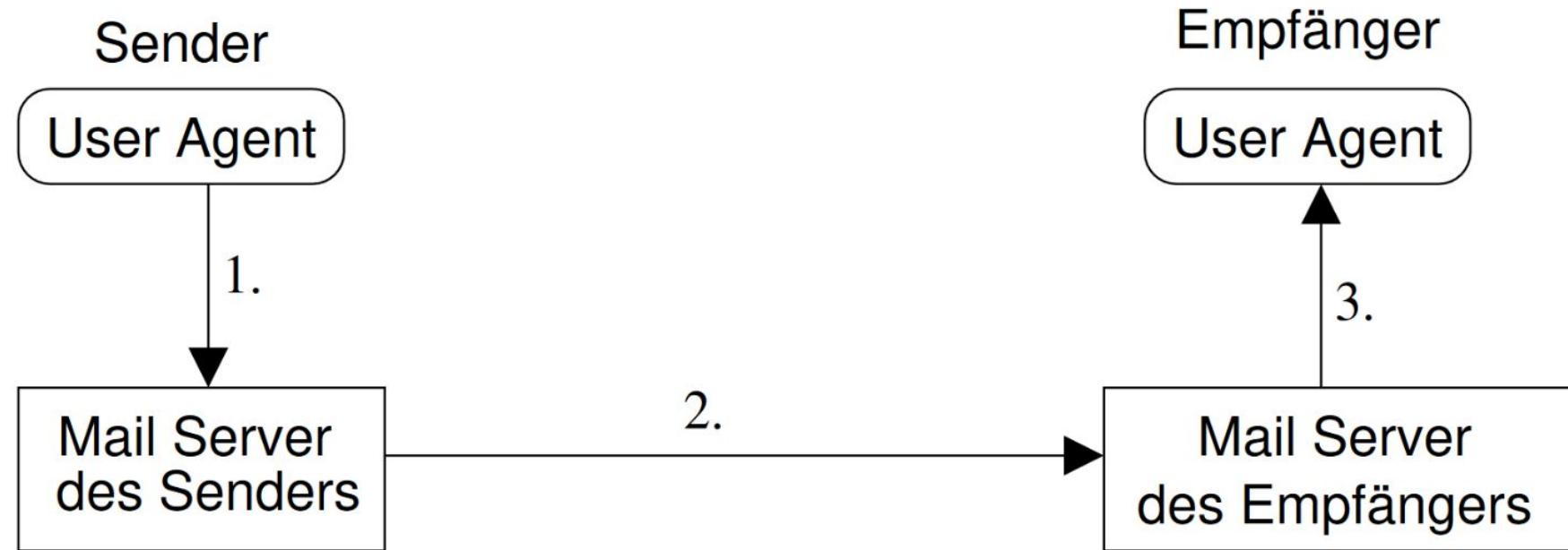
(a) Wie finden Sie heraus, ob das unbekannte Gerät ein Switch oder ein Hub ist?



- (b) Nehmen Sie an, es sei ein Switch. Wie bestimmen Sie möglichst genau und effizient die Zeit, nach der der Switch Einträge aus der Forwarding-Tabelle löscht?



Email (H)



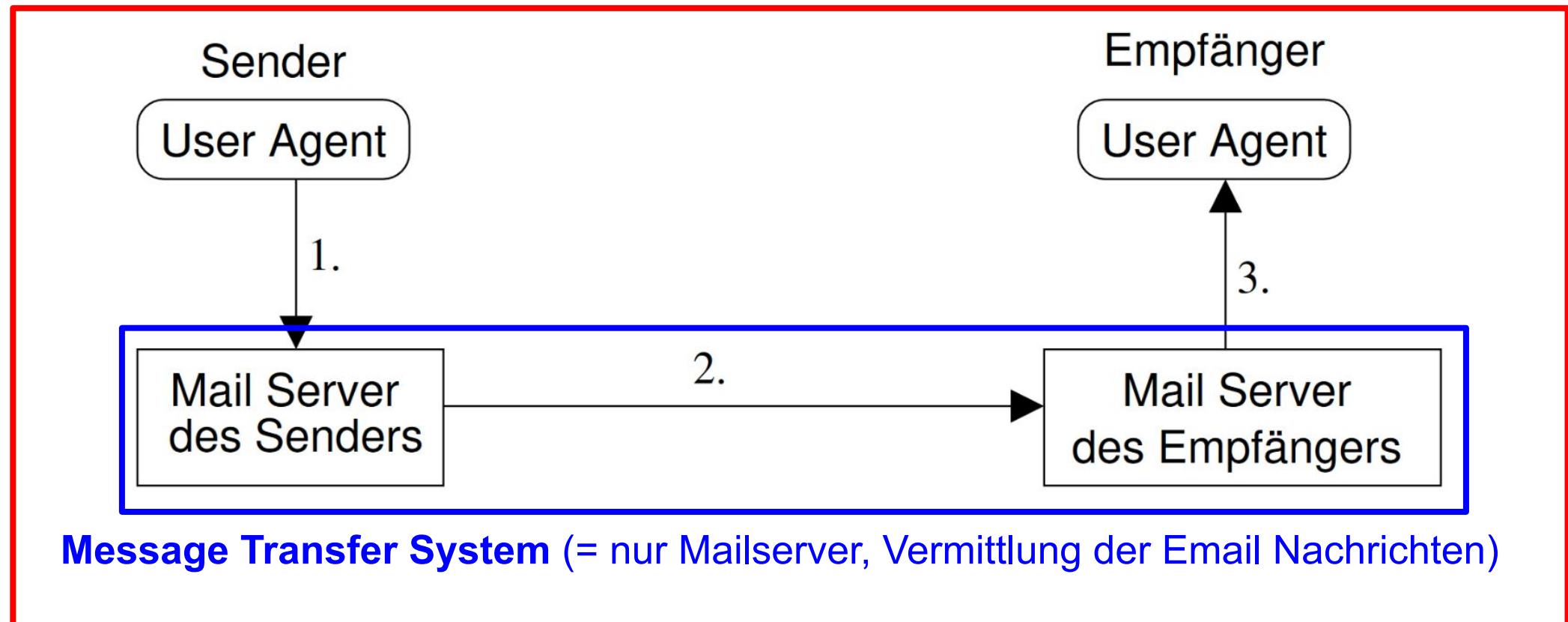
- (a) Die Abbildung skizziert den Weg einer Email vom Verfasser zum Adressaten. Welche Protokolle der Anwendungsschicht können auf den drei eingezeichneten Übertragungswegen eingesetzt werden?

1. und 2. SMTP, 3. IMAP oder POP3

- (b) Nehmen Sie nun an, dass der Sender mit einem webbasierten E-Mail Account (bspw. GMail oder GMX) eine E-Mail an den Empfänger verschickt. Welche (zusätzlichen) Protokolle im Vergleich zu Teilaufgabe (a) sind involviert?

HTTP bzw. bei verschlüsselter Verbindung HTTPS (= HTTP und TLS (früher SSL))

(c) Welche dargestellten Systeme sind Teil des *Message Transfer Systems*?



Message Handling System (ermöglicht Verfassen/Lesen/Verwalten von Mails)

- (d) Internet E-Mail ist empfindlich gegen den Dienstgüteparameter “Datenverlust” des Transportnetzes. Gibt es allgemeine Dienstgüteparameter, gegen die E-Mail unempfindlich ist? Begründen Sie Ihre Antwort!

Latenz

Email ist kein Echtzeitdienst. Sowohl auf Anwendungsebene als auch auf Ebene des Transportnetzes ist Email auch benutzbar, wenn eine Email etwas länger durch das Netz braucht.

Übertragungsrate

Email ist elastisch bezüglich Übertragungsrate. Es verschlechtert den Dienst nicht solange die vollständige Email korrekt zugestellt wird.