Lösung 12: Congestion Control, NAT, DNS

Aufgabe 1: Network Address Translation (NAT)

a) Beispiel:
- Home Router, externe bzw. öffentliche IP Adresse: 24.34.112.235
- Home Router, interne Adresse: 192.168.0.1
- Laptop 1: 192.168.0.101
- Laptop 2: 192.168.0.102
- Laptop 3: 192.168.0.103

b) Hierfür gibt es mehrere Möglichkeiten. Wichtig ist, dass jede HTTP Verbindung auf der WAN Seite eine eindeutige Portnummer hat. Für einen bestimmten Laptop darf nicht der gleiche Quell-Port für 2 verschiedene HTTP-Verbindungen gewählt werden. Eine mögliche gültige Belegung der Tabelle (auch wenn sie etwas unwahrscheinlich ist) könnte wie folgt aussehen:

LAN Seite/Heim-Netzwerk		*WAN Seite / Internet*	
IP Adresse	Port	IP Adresse	Port
192.168.0.101	18001	24.34.112.235	12000
192.168.0.101	18002	24.34.112.235	12001
192.168.0.102	53221	24.34.112.235	12002
192.168.0.102	53222	24.34.112.235	12003
192.168.0.103	49111	24.34.112.235	12004
192.168.0.103	49112	24.34.112.235	12005

Aufgabe 2: TCP Congestion Control

a) Flow Control verhindert eine Überlastung des Empfängers, Congestion Control verhindert eine Überlastung des Netzwerks.

b) [0; 6] und [23;26], exponentielles Wachstum von cwnd; jedes korrekt bestätigte Paket führt zur Vergrößerung von cwnd.

c) [6; 16] und [17;22]; lineares Wachstum von cwnd; erst nach jeder „Runde“ wird cwnd um 1 vergrößert.

d) Durch 3 ACK-Duplikate. Bei einem Timeout wäre cwnd auf 1 gesetzt worden.

e) Durch Timeout, da cwnd auf 1 gesetzt wird.

f) *ssthres* hat den Wert 32 (ca.), da bei diesem Wert der Slow Start aufhört und Congestion Avoidance startet.

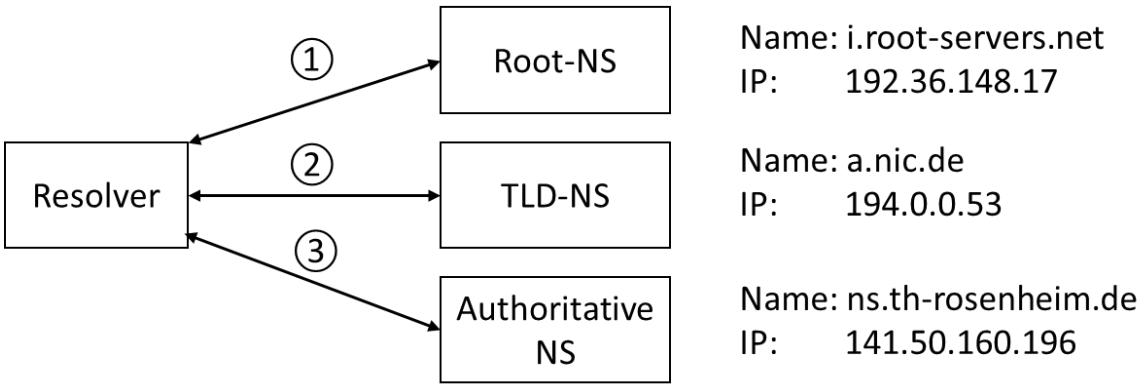
g) Der bisherige Wert von *ssthres* wird in Runde 16 verringert. Da *cwnd* zu diesem Zeitpunkt 42 ist, wird *ssthres* auf 21 gesetzt (halber cwnd-Wert).
Hinweis: In Runde 17/18 ändert sich daran nichts. Vielleicht wundert man sich, warum cwnd nicht auch auf 21 gesetzt wird, sondern gleich auf 24? Der Grund: Der Paketverlust wurde durch 3 Duplicate ACKs erkannt (also viermal das gleiche ACK). Man geht aus, dass nur 1 Paket verlorengegangen ist und nicht 4. Deshalb 21 + 3!

h) In Runde 22 wird ein Problem erkannt als das *cwnd*=28. Deshalb wird ssthres in der 24. Runde den Wert 14 haben. Hinweis: Nur beim ersten Slow Start einer TCP Verbindung ist ssthres fest durch die Implementierung vorgegeben.

i) Paket 1 wird in der 1. Runde gesendet, Paket 2 und 3 in der 2. Runde, Pakete 4-7 in der 3. Runde, Pakete 8-15 in der 4. Runde, Pakete 16-31 in der 5. Runde. Das Paket 17 wird also in der 5. Runde gesendet.

Aufgabe 3: DNS

a) Der Reihe nach ergeben sich z.B. die folgenden Ergebnisse:



Hinweis: Es gibt im Verlauf oft mehrere Nameserver, die weiterhelfen können. Beim letzten DNS Server (`ns.fh-rosenheim.de`) handelt es sich um den *Authoritative DNS Server*, der für den Namen www.th-rosenheim.de maßgeblich ist. Das Ergebnis, dass dieser Server zurückliefert entspricht der IP Adresse von www.th-rosenheim.de.
Man sieht auch, dass es zwei DNS Server gibt, die Hostnamen für IP Adressen der TH Rosenheim auflösen können, nämlich: `ns.fh-rosenheim.de` und `deneb.dfn.de`.

```
dev@OS-dev /etc $ dig @141.60.160.2 www.th-rosenheim.de

; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> @141.60.160.2 www.th-rosenheim.de
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43803
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1bdd36f2e139bcd54d91ed635dfb98c23c24b0d6b85e2bc6 (good)
;; QUESTION SECTION:
;www.th-rosenheim.de.           IN      A

;; ANSWER SECTION:
www.th-rosenheim.de.    86400   IN      A       141.60.160.196

;; AUTHORITY SECTION:
th-rosenheim.de.        86400   IN      NS      ns.fh-rosenheim.de.
th-rosenheim.de.        86400   IN      NS      dns-3.dfn.de.

;; ADDITIONAL SECTION:
ns.fh-rosenheim.de.     600     IN      A       141.60.160.2
dns-3.dfn.de.           72865   IN      A       193.174.75.58
dns-3.dfn.de.           72865   IN      AAAA    2001:638:d:b103::1

;; Query time: 3 msec
;; SERVER: 141.60.160.2#53(141.60.160.2)
;; WHEN: Thu Dec 19 16:35:30 CET 2019
;; MSG SIZE  rcvd: 206
```

b) Man erkennt, dass für www.berlin.de bereits eine IPv6 Adresse zurückgeliefert wird, aber für www.muenchen.de nicht. Das legt den Schluss nahe, dass die Webseite von www.muenchen.de noch nicht IPv6-fähig ist.

```
;; ANSWER SECTION:
www.berlin.de.          86352   IN      A       212.45.111.17
www.berlin.de.          2774    IN      AAAA    2a00:cd0:1002:1::17

;; ANSWER SECTION:
www.muenchen.de.        3542    IN      A       188.164.238.46
```

c) `dig MX th-rosenheim.de` liefert

```
;; ANSWER SECTION:
th-rosenheim.de.        7110    IN      MX      90 sophos-app-prim.th-rosenheim.de.
th-rosenheim.de.        7110    IN      MX      90 sophos-app-sec.th-rosenheim.de.
```

Diese Namen könnte man durch eine weitere Anfrage in IP Adressen auflösen.

d) Es werden mehrere IP Adresse zurückgegeben, z.B. 4 verschieden IP Adressen. Die Reihenfolge der IP Adressen kann sich dabei ändern. In der Regel wird eine Anwendung (z.B. Webrowser) immer die 1. Adresse verwenden. Auf diese Weise erreicht man Load Balancing.
Man erkennt auch wie lange DNS Anfragen gültig sind.