

Grundlagen Rechnernetze und Verteilte Systeme

IN0010, SoSe 2019

Übungsblatt 12

22. Juli – 26. Juli 2019

Hinweis: Mit * gekennzeichnete Teilaufgaben sind ohne Lösung vorhergehender Teilaufgaben lösbar.

Aufgabe 1 Domain Name System (DNS)

Hinweis: Angelehnt an Endterm 2015

Zentrale Aufgabe des Domain Name Systems (DNS) ist es, menschenlesbare Namen auf IP-Adressen abzubilden, die dann für die Wegwahl auf der Netzwerkschicht verwendet werden können. Bei dem Namen asciiart.grnvs.net. handelt es sich um einen sog. *Fully Qualified Domain Name (FQDN)*.

a)* Was ist der Unterschied zwischen einem vollqualifizierten Domain Name (FQDN) und einem nicht-(voll)qualifizierten?

mit . hinten ist FQDN

b)* Benennen Sie die einzelnen Bestandteile des FQDNs, sofern es dafür gängige Bezeichnungen gibt.

Subdomain
asciiart.grnvs.
Second level
grnvs.
Top level
net.
Root
durch

In Abbildung 1 sind ein PC sowie eine Reihe von Servern dargestellt. Wir nehmen an, dass PC1 den Router als Resolver nutzt. Der Router wiederum nutzt einen Resolver von Google unter der IP-Adresse 8.8.8.8 zur Namensauflösung. Ferner nehmen wir an, dass der Google-Resolver gerade neu gestartet wurde (also insbesondere keine Resource Records gecached hat) und rekursive Namensauflösung anbietet.

Die autoritativen Nameserver für die jeweiligen Zonen sind in Tabelle 1 gegeben.

Zone	autoritativer Nameserver
.	d.root-servers.net.
com., net.	a.gtld-servers.net.
google.com.	ns1.google.com.
grnvs.net.	bifrost.grnvs.net.

Tabelle 1: Zonen mit zugehörigen autoritativen Nameservern

c)* Erläutern Sie den Unterschied zwischen einem *Resolver* und einem *Nameserver*.

d)* Welche Funktion erfüllen d.root-servers.net und a.gtld-servers.net?

Root Zone

second level domains

e)* Erklären Sie den Unterschied zwischen iterativer und rekursiver Namensauflösung.

f) Zeichnen Sie in Abbildung 1 alle DNS-Nachrichten (Requests / Responses) ein, die ausgetauscht werden, sobald PC1 auf asciiart.grnvs.net. zugreift. Nummerieren Sie die Nachrichten gemäß der Reihenfolge, in der sie zwischen den einzelnen Knoten ausgetauscht werden.

g)* Wie wird im DNS sichergestellt, dass kein bössartiger Nameserver Anfragen für andere Domänen beantwortet? (Wir gehen davon aus, dass keine Man-in-the-Middle-Angriffe möglich sind.)

dem root muss vertraut werden

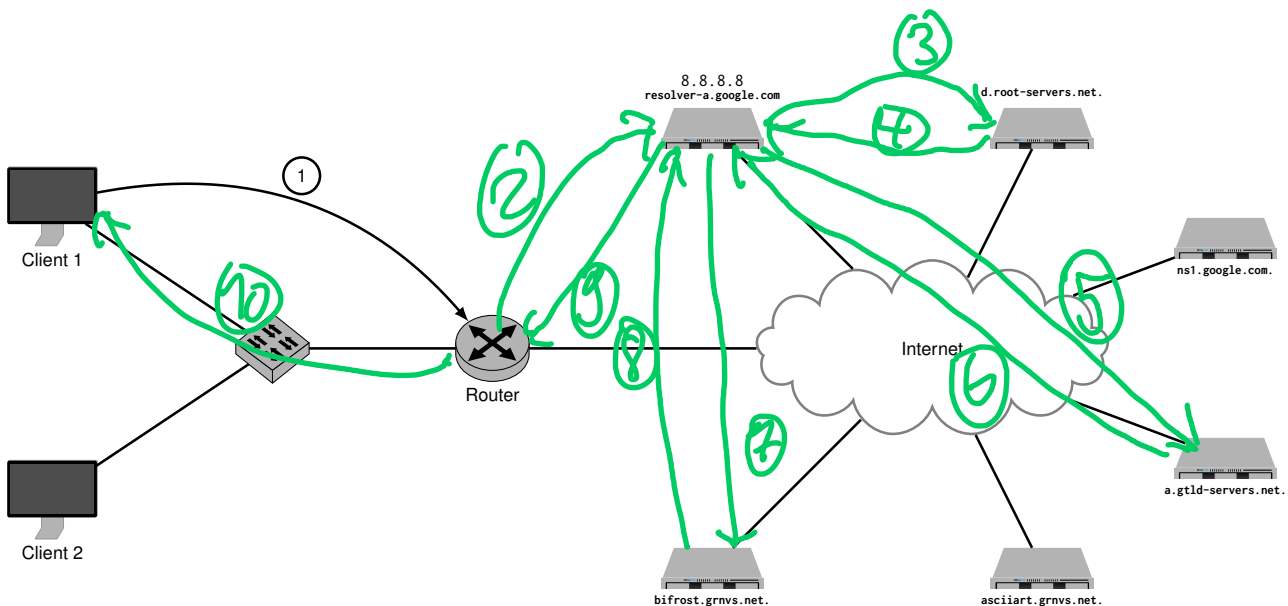


Abbildung 1: Vorlage zu Aufgabe 1f)

Aufgabe 2 All in a nutshell

In dieser Aufgabe wollen wir noch einmal alles nachvollziehen, was geschieht, wenn Sie auf Ihrem Computer die Webseite `www.google.de` aufrufen. Wir treffen dabei lediglich die Annahme, dass in Ihrem privaten Netz ARP- und DNS-Caches noch leer sind (d. h. etwaige Caches ab dem ersten Router können als gefüllt angenommen werden). Die Netzwerktopologie ist in Abbildung 2 dargestellt. Ihr Router übersetzt bei Bedarf private in öffentliche IP-Adressen sowie Portnummern (NAT). Auf Ihrem Computer sei der Google-Resolver mit der IPv4-Adresse 8.8.8.8 konfiguriert, der rekursive Anfragen erlaubt.

Es sollen nun für **jeden Link** – also jeden Abschnitt zwischen jeweils zwei Geräten (z. B. von PC zu SW) – einige ausgewählte Felder der Nachrichten notiert werden, die im jeweiligen Schritt über diesen Link versendet werden. Da dies insbesondere für MAC-Adressen etwas Schreibarbeit ist, kürzen wir Adressen mit der Bezeichnung `<Gerätename>.<Interface>.<Typ>` ab, z. B. `stehe RA.eth0.MAC` für die MAC-Adresse von Interface `eth0` an Router `RA`.

Sie finden in den Abbildungen 3 – 6 vorgedruckte Tabellen. Eine Zeile entspricht dabei einer Nachricht, die über den jeweiligen Link gesendet wird. Die erste Spalte bezeichnet den Link, also z. B. vom PC zum Switch oder vom Switch zum Router. Die übrigen Spalten entsprechen verschiedenen Schichten des ISO/OSI-Modells. Diese sind jeweils in die relevanten Headerfelder der üblicherweise verwendeten Protokolle unterteilt. Je nach Nachricht sind nicht alle Spalten oder Unterzeilen pro Spalte auszufüllen. **Streichen Sie deutlich nicht benötigte Felder.** Ein Beispiel ist bereits in der Tabelle eingetragen.

Einige Header verfügen über ein Protokoll-Feld, in dem das Protokoll der nächsthöheren Schicht angegeben wird. Üblicherweise stehen Zahlencodes für die jeweiligen Protokolle. Es ist nicht notwendig, diese Zahlencodes anzugeben. Stattdessen reicht es, das verwendete Protokoll anzugeben, z. B. IPv4, TCP oder UDP. Bei einigen Header-Feldern gibt es gewisse Freiheiten, z. B. bei Portnummern oder der initialen TTL. Wählen Sie in diesen Fällen **sinnvolle** Werte.

a)* Füllen Sie nun die Vordrucke in den Abbildungen 3 – 6 aus. Brechen Sie **nach dem ersten** an `www.google.de` übermittelten Paket auf dem Link von PC an SW ab.

Hinweise:

- Der Well-Known Port für DNS ist UDP 53.
- Wir nehmen an, dass sich zwischen Router RB und RC insgesamt 10 weitere Router befinden. Dies ist für die Bestimmung der TTL entscheidend.
- In die Spalte „Schicht 7“ tragen sie einfach das Anwendungsprotokoll, ggf. den Typ der Nachricht (z. B.

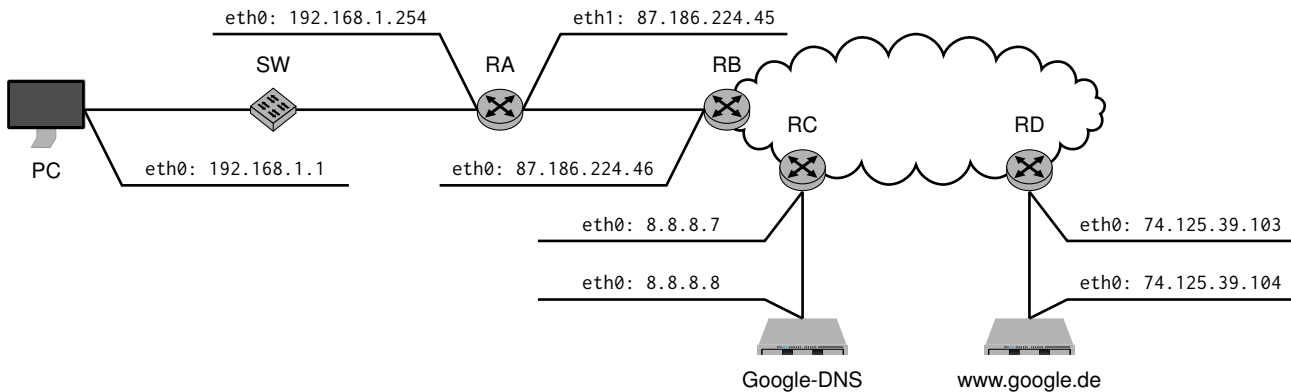
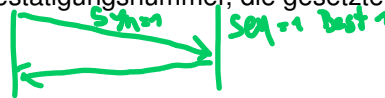


Abbildung 2: Netztopologie zu Aufgabe 2. Die relevanten Links sind mit den Ziffern 1 – 5 gekennzeichnet.

Request / Reply) sowie stichpunktartig den Inhalt der übermittelten Nachricht ein (z. B. „DNS-Request“ oder „DNS-Response“).

Die vorangegangene Teilaufgabe hat detailliert die Vorgänge bis zum Beginn des TCP-Verbindungsaufbaus dargestellt. Im Folgenden wollen wir uns auf die TCP-Verbindung und Datenübertragung konzentrieren. Aus diesem Grund betrachten wir ab jetzt nur noch die logische Verbindung zwischen dem PC und `www.google.de` in Form eines einfachen Weg-Zeit-Diagramms **ohne** die dazwischenliegenden Knoten. Sie können Serialisierungszeiten vernachlässigen. Gehen Sie außerdem davon aus, dass während der gesamten Übertragung keine Segmentverluste auftreten.

b)* Skizzieren Sie ein Weg-Zeit-Diagramm, welches den TCP-Verbindungsaufbau darstellt. Geben Sie für jedes übermittelte Segment die Sequenznummer, Bestätigungsnummer, die gesetzten¹ Flags sowie die Länge l der transportierten Nutzdaten an.



Der PC fordert nun die Webseite an, die auf `www.google.de` gehostet wird. Dazu sendet der PC eine HTTP-GET-Nachricht, welche aus Sicht von Schicht 4 eine Nutzdatenlänge von $l_1 = 50$ B habe. Der Webserver wird daraufhin die Webseite an den PC senden, welche eine Länge $l_2 = 1000$ B habe. Die ausgehandelte MSS² sei größer als l_2 .

c) Skizzieren Sie ein Weg-Zeit-Diagramm, welches die TCP-Verbindungsphase darstellt. Gehen Sie von den in Teilaufgabe b) ausgehandelten Sequenznummern aus. Geben Sie für jedes übermittelte Segment die Sequenznummer, Bestätigungsnummer, die gesetzten Flags sowie die Länge l der im Segment transportierten Nutzdaten an.

d) Skizzieren Sie ein Weg-Zeit-Diagramm, welches den TCP-Verbindungsabbau darstellt. Dieser werde vom PC initiiert. Gehen Sie dabei von den in Teilaufgabe c) ausgehandelten Sequenznummern aus. Geben Sie für jedes übermittelte Segment die Sequenznummer, Bestätigungsnummer, die gesetzten Flags sowie die Länge l der im Segment transportierten Nutzdaten an.

¹Ein Bit-Flag gilt als „gesetzt“, wenn es logisch 1 ist.

²Die MSS (Maximum Segment Size) gibt die maximale Größe eines Segments an. Sie bezieht sich dabei lediglich auf die Nutzdaten. Bestätigungen beispielsweise sind Segmente der Länge null, welche lediglich aus einem TCP-Header bestehen.

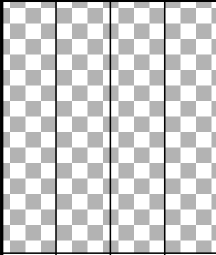
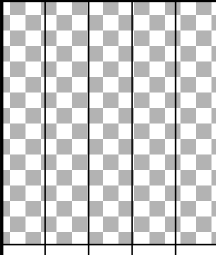
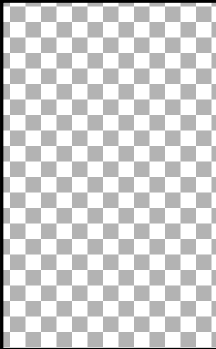
Link		Schicht 2				Schicht 3				Schicht 4					Schicht 7				
From	PC	Src	PC.eth0.MAC			Src				Src									
		Dst	ff:ff:ff:ff:ff:ff			Dst				Dst									
To	SW	Prot	ARP			Prot				Flags									
		Op	Request			TTL				SEQ									
From		Src				Src				Src									
		Dst				Dst				Dst									
To		Prot				Prot				Flags									
						TTL				SEQ									
From		Src				Src				Src									
		Dst				Dst				Dst									
To		Prot				Prot				Flags									
						TTL				SEQ									
From		Src				Src				Src									
		Dst				Dst				Dst									
To		Prot				Prot				Flags									
						TTL				SEQ									
From		Src				Src				Src									
		Dst				Dst				Dst									
To		Prot				Prot				Flags									
						TTL				SEQ									

Abbildung 3: Vordruck zu Aufgabe 2

Link		Schicht 2				Schicht 3				Schicht 4					Schicht 7				
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									

Abbildung 4: Vordruck zu Aufgabe 2

Link		Schicht 2				Schicht 3				Schicht 4					Schicht 7				
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									

Abbildung 5: Vordruck zu Aufgabe 2

Link		Schicht 2				Schicht 3				Schicht 4					Schicht 7				
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									
From		Src				Src				Src									
		Dst				Dst				Dst									
		Prot				Prot				Flags									
						TTL				SEQ									
To										ACK									

Abbildung 6: Vordruck zu Aufgabe 2

Aufgabe 3 SMTP (Hausaufgabe)

Für daheim: Mailversand von der Kommandozeile

Sie haben in der Vorlesung gelernt, dass mithilfe des Programms `telnet` bzw. mit dem `s_client` von OpenSSL Verbindungen zu Webservern aufgebaut werden können.

a) * Ihre Aufgabe ist nun, sich mithilfe des `s_client` mit dem SMTP-Servers Ihres Mailproviders zu verbinden und sich selbst eine e-Mail zu schicken. Die notwendigen Schritte können Sie sich aus dem RFC 5321 erschließen. Alternativ ist es auch möglich entsprechende Tutorials zu konsultieren. Der initiale Befehl könnte folgendermaßen aussehen: `openssl s_client -crlf -connect <smtp.server.org>:465`

Sollten Sie CRAM-MD5 verwenden wollen, könnte Ihnen die folgende Bash-Funktion zur Berechnung der Response auf eine vom Server gegebene Challenge helfen:

```
cram() {  
    challenge=$1  
    username=$2  
    challenge=$(echo -n $challenge|base64 -d)  
    echo "Challenge is: $challenge"  
    read -sp "Password for $username: " password  
    echo ""  
    hash=$(echo -n "$challenge" |openssl md5 -hmac "$password" -hex|cut -d" " -f 2 )  
    response=$(echo -n "$username $hash" |base64)  
    echo "Response for server is: "  
    echo $response  
}
```

Rufen sie Sie dann folgendermaßen auf:

```
cram <CHALLENGE> <USERNAME>
```

b) Ermitteln Sie, welche Authentifizierungsmethoden der von Ihnen gewählte SMTP-Server anbietet und machen Sie sich den Unterschied zwischen ihnen klar. **c)** * Warum ist überhaupt eine Authentifizierung notwendig? Welche Probleme werden dadurch behoben oder zumindest verringert?