



Hinweise zur Personalisierung:

- Ihre Prüfung wird bei der Anwesenheitskontrolle durch Aufkleben eines Codes personalisiert.
- Dieser enthält lediglich eine fortlaufende Nummer, welche auch auf der Anwesenheitsliste neben dem Unterschriftenfeld vermerkt ist.
- Diese wird als Pseudonym verwendet, um eine eindeutige Zuordnung Ihrer Prüfung zu ermöglichen.

Grundlagen Rechnernetze und Verteilte Systeme

Klausur: IN0010 / Endterm

Datum: Dienstag, 27. Juli 2021

Prüfer: Prof. Dr.-Ing. Georg Carle

Uhrzeit: 08:00 – 09:30

Unterschreiben Sie die Verhaltensregeln oben rechts neben Ihrem Sticker.

Andernfalls wird Ihre Elektronische Übungsleistung nicht gewertet!

Bearbeitungshinweise

- Diese Klausur umfasst **16 Seiten** mit insgesamt **6 Aufgaben**.
- Die Gesamtpunktzahl in dieser Prüfung beträgt 90 Punkte.
- Das Heraustrennen von Seiten aus der Prüfung ist untersagt.
- Als Hilfsmittel sind zugelassen:
 - ein **nicht-programmierbarer Taschenrechner (keine Taschenrechner-App!)**
 - der **vom Lehrstuhl bereitgestellte Cheatsheet ohne Modifikationen in ausgedruckter Form**
 - ein Wörterbuch Deutsch ↔ Muttersprache in Papierform ohne jedwede Anmerkungen
- Mit * gekennzeichnete Teilaufgaben sind ohne Kenntnis der Ergebnisse vorheriger Teilaufgaben lösbar.
- **Es werden nur solche Ergebnisse gewertet, bei denen der Lösungsweg erkennbar ist.** Auch Textaufgaben sind **grundsätzlich zu begründen**, sofern es in der jeweiligen Teilaufgabe nicht ausdrücklich anders vermerkt ist.
- Schreiben Sie weder mit roter / grüner Farbe noch mit Bleistift.
- Zum Ausdrucken und Einscannen Ihrer Prüfung (falls zutreffend) dürfen Sie den Raum verlassen. Ob Sie Ihre Kamera mitnehmen oder nicht, bleibt Ihnen überlassen. Wie auf Moodle aber bereits bekanntgegeben, könnte es von Vorteil sein, bei etwaigen Problemen eine Kommunikationsmöglichkeit zu haben.
- Sollten Sie während der Prüfung auf Toilette müssen, informieren Sie bitte die Aufsicht vorher mittels privater Nachricht in BBB und warten auf eine Bestätigung. Bitte nehmen Sie Smartphone / Webcam nicht mit.

Aufgabe 1 Multiple Choice (12 Punkte)

Die folgenden Aufgaben sind Multiple Choice / Multiple Answer, d. h. es ist jeweils mind. eine Antwortoption korrekt. Teilaufgaben mit nur einer richtigen Antwort werden mit 1 Punkt bewertet, wenn richtig. Teilaufgaben mit mehr als einer richtigen Antwort werden mit 0,5 Punkten pro richtigem Kreuz und $-0,5$ Punkten pro falschem Kreuz bewertet. Die minimale Punktzahl pro Teilaufgabe beträgt 0 Punkte.

Kreuzen Sie richtige Antworten an

Kreuze können durch vollständiges Ausfüllen gestrichen werden

Gestrichene Antworten können durch nebenstehende Markierung erneut angekreuzt werden



a)* Welcher PTR-Record gehört zur IP Adresse 133.35.3.31?

- 35.133.31.3.in-addr.arpa. 133.35.3.31.in-addr.arpa. 31.3.35.133.in-addr.arpa.
 8.8.4.4.in-addr.arpa. 4.4.8.8.in-addr.arpa. 31.3.35.31.in-addr.arpa.

b)* Welcher der folgenden Begriffe passt nicht dazu?

- RZ NRZ SDF MLT3 Manchester

c)* Welches sind keine geregelten Medienzugriffsverfahren?

- Token Passing CSMA/CD CSMA/CA ohne RTS/CTS CSMA/CA mit RTS/CTS ALOHA

d)* Welche Resource Record Typen beinhalten IP-Adressinformation:

- AAAA NS MX CNAME PTR TXT

e)* In einer URL ermöglicht die query ...

- ... Abschnitte in einem Dokument zu referenzieren ... die relative Angabe einer Lokalität auf dem Ziel
 ... die Übergabe von Variablen ... das Spezifizieren des Anwendungsprotokolls

f)* Welches sind keine gültigen HTTP Kommandos?

- POST DELETE SET PUT GET

g)* Wie viele DNS-Zonen muss man unterhalb der Zonen 251 und 23 mindestens anlegen, um damit einen Reverse-Lookup aller IP-Adressen des Netzes 251.23.224.0/19 zu ermöglichen?

- 172 1 184 194 246 32 34 256

h)* Wie viele PTR Records muss man anlegen, um damit einen Reverse-Lookup aller IP-Adressen des Netzes 251.23.224.0/19 zu ermöglichen?

- 256 1 2356 65536 4495 38 8192

i)* Die Quelle Q emittiert die Zeichen $\{S, C, P, G\}$ mit den angegebenen Auftrittswahrscheinlichkeiten. Bestimmen Sie die Entropie von Q . S: 0,06 C: 0,26 P: 0,32 G: 0,36

- 0,00 -2,79 0,21 2,75 1,55 1,66 1,81

j)* Welche der folgenden Faktoren kann ein Signal in einem Übertragungskanal beeinflussen?

- Tiefpassfilterung Interferenzen Verzerrungen
 Dämpfung Rauschen Gruselfaktor

Aufgabe 2 Kurzaufgaben (12 Punkte)

a)* Beschreiben Sie kurz, was man unter einem DNS-Server versteht.

Entweder einen Resolver oder einen Nameserver.



b)* Beschreiben Sie kurz den Prozess der iterativen Namensauflösung.

Ein Resolver löst DNS Requests Zone für Zone beginnend beim Root durch iterative Anfragen an die jeweils autoritativen Nameserver auf, welche jeweils entweder mit den autoritativen Nameservern der nächsten Zone oder (sofern schlussendlich bekannt) die Antwort auf die die Anfrage liefern.



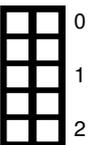
c)* Wie ist das Domain Name System hinsichtlich der Privatsphäre der Nutzer zu bewerten?

Das DNS arbeitet unverschlüsselt und erlaubt es so allen Parteien, die Netzwerkverkehr mitschneiden können, umfangreiche Nutzungsprofile zu erstellen. Insbesondere der jeweilige ISP sowie der Betreiber des genutzten Resolvers sind so trivial in der Lage, Nutzerprofile Ihrer Kunden zu erstellen. Mit relativ einfachen Methoden ist dies aber auch anderen Nutzern im selben (privaten) Netzwerk möglich.



d)* Wie ist eine iterativen Namensauflösung hinsichtlich Vertrauenswürdigkeit und Resistenz gegen Manipulation zu bewerten?

Da ein Resolver prinzipiell nur vertrauenswürdige Nameserver anfragt (ausgehend von den Root Hints, die fest hinterlegt sind), sollte auch die Namensauflösung vertrauenswürdig sein. Eine Manipulation auf dem Weg durch das Internet der Anfragen/Antworten kann dabei natürlich nicht ausgeschlossen werden.



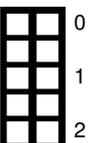
e)* Welche Auswirkung könnte eine komplette Verschlüsselung des DNS-Datenverkehrs auf die verschiedenen Parteien im Internet haben?

Nur noch Resolver können Nutzerprofile erstellen. Durch diese Zentralisierung der Daten werden diese wertvoller.

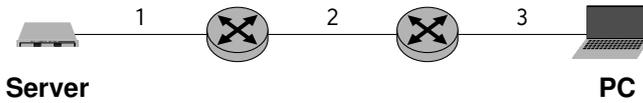
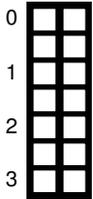


f)* Wozu benötigt man Glue Records im DNS?

Wenn sich ein Nameserver in der Zone befindet, für die er selbst autoritativ ist, muss die darüber befindliche Zone zusätzlich zum Domain Name des Nameservers (NS Record) dessen IP Adresse (A oder AAAA Record) als Glue Record schicken. Ansonsten ist eine Namensauflösung nicht möglich.



g)* Gegeben sei folgende Netztopologie. Sie empfangen an Ihrem PC drei Fragmente eines IPv4-Datenpakets mit den angegebenen Größen. Das Do-Not-Fragment bit ist nicht gesetzt. Gehen Sie davon aus, dass der Server die MTU auf Abschnitt 1 kennt und Segmentgrößen entsprechend anpasst, um nicht selber fragmentieren zu müssen. Bestimmen Sie die MTU jedes Pfadabschnitts so gut wie möglich. Geben Sie einen nachvollziehbaren Rechenweg an.



Fragment 1:	5888 B	Offset:	0
Fragment 2:	2056 B	Offset:	736
Fragment 3:	1047 B	Offset:	993

$MTU \text{ Abschnitt 1} \geq (5888 + 2056 + 1047)B = 8991 B$
 $MTU \text{ Abschnitt 2} \geq (5888 + 2056)B = 7944 B$
 $MTU \text{ Abschnitt 3} \geq \max(5888, 2056, 1047)B = 5888 B$



h)* Erläutern Sie, weswegen man OSPF der Schicht 3 des ISO/OSI-Modells zuordnen könnte.

Routingprotokolle tauschen Pfadinformationen aus und ermöglichen so erst die Wegwahl auf Schicht 3. Deswegen werden Routingprotokolle häufig dieser Schicht zugeordnet.

Gleichzeitig definieren sie aber Abläufe, die von Anwendungen umgesetzt werden, welche wieder eingehende Daten auf bestimmten Adressen oder sogar Ports (BGP) erwarten und verarbeiten. Dies unterscheidet sie nicht von Protokollen der Anwendungsschicht wie DHCP oder SMTP, weswegen man sie durchaus Schicht 7 zuordnen kann. Besonders deutlich wird das bei BGP, das selbst auf TCP aufbaut und somit streng genommen eigentlich gar nicht Schicht 3 zugeordnet werden kann.

Aufgabe 3 IPv4+ (16 Punkte)

Adressknappheit ist ein Problem bei IPv4. Um dieses Problem zu lösen wurde IPv4+¹ als *IPv4-kompatible Lösung* entwickelt. IPv4+ erweitert IPv4 um das Konzept einer „Door“ (Türe) mit zugehöriger „Door Address“ (Türadresse).

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0B	Version		IHL			TOS			Total Length																							
4B	Identification									Flags			Fragment Offset																			
8B	TTL			Protocol			Header Checksum																									
12B	Source Address																															
16B	Destination Address																															
20B	Source Door Address								Destination Door Address																							
24B	Options / Padding (optional)																															

Door	Region
0.00	Reserviert
1.23	Burundi
1.50	Cuba
1.56	Deutschland
1.69	EU
1.99	Haiti

Abbildung 3.1: IPv4+-Header und eine Auswahl von Door Address Zuweisungsvorschlägen

Der IPv4+-Header und einige Türadressen sind in Abbildung 3.1 abgebildet. Im sprachlichen Bild steckt „hinter“ jeder IPv4+-Türe ein *unabhängiger* IPv4-Adressbereich. Türadressen werden, wie IPv4-Adressen, in Dotted Decimal Notation angegeben.

Notationsbeispiel: Die IPv4+-Adresse der IPv4-Adresse 2.3.4.5/30 hinter Tür 0.1 ist 0.1|2.3.4.5/30.

a)* Wie viele IPv4+-Adressen gibt es? (Begründung!)

Eine IPv4+-Adresse besteht aus einer 32 bit IPv4-Adresse und einer 16 bit Türadresse, demnach gibt es $2^{32 \text{ bit} + 16 \text{ bit}} = 281\,474\,976\,710\,656$ Adressen.



b)* Wofür steht IHL und was bedeutet es?

Die Abkürzung steht für Internet-Header-Length. Bedeutung: Länge des IPv4(+)-Headers in Vielfachen von 4 B.



c)* Woran kann ein IPv4+-fähiger Router erkennen, ob es sich bei einer Nachricht um IPv4+ handelt?

Das IHL Feld hat den Wert 6 B. Durch die längeren, in den Optionen gespeicherten Adressen ändert sich der Wert von IHL. Ansonsten ist der Header nicht von IPv4 unterscheidbar.



RFC 791 (Titel: „Internet Protocol“) schreibt:

```
No Operation
+-----+
|00000001|
+-----+
Type=1
```

This option may be used between options, for example, to align the beginning of a subsequent option on a 32 bit boundary.
May be copied, introduced, or deleted on fragmentation, or for any other reason.

d)* Warum ist es problematisch, die Türadressen 1.0/8 zu verwenden?

Weil es bereits eine IPv4 Option gibt, die an der betreffenden Stelle auftauchen kann aber nichts mit IPv4+ zu tun hat.



¹IETF Standardisierungsvorschlag: <https://datatracker.ietf.org/doc/draft-tang-ipv4plus/>



e)* Warum ist die Türadresse 0.00 reserviert?

Der IPv4-Adressbereich hinter dieser Türadresse wird gerade verwendet. Um Kompatibilität mit IPv4 zu bewahren darf dieser nicht erneut vergeben werden. (Zudem gibt es auch hier bereits eine IPv4 Option gibt, die an der betreffenden Stelle auftauchen kann aber nichts mit IPv4+ zu tun hat.)



f)* Was ist ein Vorteil von IPv4+ gegenüber IPv6?

IPv4+ ist theoretisch transparent für existierende IPv4 Hardware. Existierende Hardware kann also weiter verwendet werden.



g)* Was ist ein Vorteil von IPv6 gegenüber IPv4+?

Mit IPv6 ist keine Fragmentierung im Netzwerk mehr notwendig. Fragmentierung erfolgt stattdessen durch den Absender. Dies entlastet Router.

Nachfolgend soll das IPv4/IPv4+-Mischnetzwerk in Abbildung 3.2 betrachtet werden.

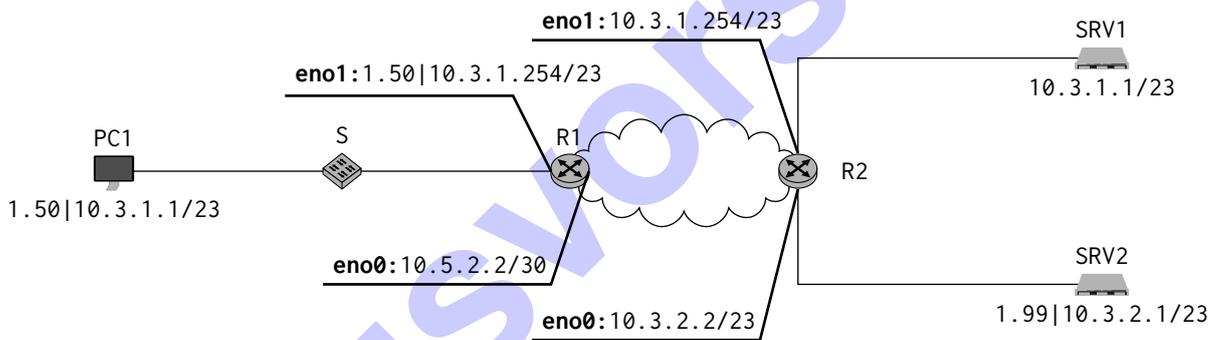


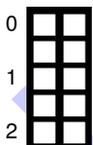
Abbildung 3.2: IPv4/IPv4+ Mischnetzwerk



h)* Zeichnen Sie alle Kollisionsdomänen, die nicht zugleich auch eine Broadcastdomäne darstellen, in Abbildung 3.2 ein. (Die das Internet darstellende Wolke kann ignoriert werden, die beiden Router R1 und R2 jedoch nicht.)
{PC1, S}, sowie {S, R1}



i)* Zeichnen Sie alle Broadcastdomänen, die zudem Kollisionsdomänen sind, in Abbildung 3.2 ein. (Die das Internet darstellende Wolke kann ignoriert werden, die beiden Router R1 und R2 jedoch nicht.)
{R2, SRV1}, sowie {R2, SRV2}



j)* Welche Routing-Einträge braucht der IPv4-Router R2, um die Netze von SRV1 und SRV2 zu erreichen?

Ziel	Next Hop	Interface
10.3.0.0/23	0.0.0.0	eno1
10.3.2.0/23	0.0.0.0	eno0



k)* PC1 sendet eine IPv4+-Paket an 1.99|10.3.2.1. Dieses erreicht nun den IPv4-Router R2. Was passiert?

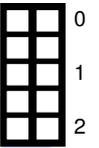
IPv4-Router R2 deutet das Paket als IPv4 Paket. R2 leitet das Paket an SRV2 weiter.

l)* SRV2 schickt ein IPv4+-Paket an 1.50|10.3.1.1. Dieses Paket erreicht nun den IPv4-Router R2. Was passiert?



IPv4-Router R2 deutet das Paket als IPv4 Paket. R2 leitet das Paket an SRV1 weiter.

m)* Erläutern Sie, inwieweit ein Wechsel von IPv4 auf IPv4+ Änderungen in anderen Schichten erfordert.



Zwei Beispiel:

Layer 2: ARP „funktioniert“ zwar weiterhin, solange die IPv4-Adressen verschieden sind. Bei gleichen IPv4-Adressen mit anderer Türadresse gäbe es jedoch Probleme. (Hier wäre dann ein Erweitern der ARP-Implementierung für IPv4+ notwendig.)

Layer 4: Aktuelle Implementierungen die ein TCP/UDP 5-Tupel bestimmen würde Türadresse ignorieren. Ebenso die Prüfsummenberechnungen.

n)* Lassen sich die IPv4+-Netzwerke 1.56|10.2.3.0/24 und 1.59|10.2.4.0/24 zusammenfassen? (Begründung!)



Nein, verschiedene Türadressen können nicht zusammengefasst werden. (Betrachtet man nur IPv4: Nein, da 3 und 4 in den dritten Oktetten der IPv4-Adressen nicht in einem /23 Netz liegen.)

Aufgabe 4 The WWNAT64 - World Wide NAT64 (20 Punkte)

Sie sind zuständig für die interplanetare Internetinfrastruktur auf dem Mars. Da die Erdlinge zu verschwenderisch mit den IPv4-Adressen umgegangen sind, wurde beschlossen, auf IPv4 zu verzichten und stattdessen nur IPv6 zu verwenden. Dafür konnten Sie das komplette IPv6-Präfix $1000::/4$ ergattern. Für das Solarlink Satellitennetzwerk, welches das ganze Sonnensystem mit Internet versorgt, benötigen Sie davon allerdings ein $/62$ Präfix.

Damit die Marsianer trotzdem ihre veralteten IPv4-Liebingsseiten der Erde besuchen können, bauen Sie ein WWNAT64 um die Erde auf. Dieses dient als Gateway zur Erde und ist in der Lage, IPv6- in IPv4-Adressen zu übersetzen. Damit ein Rechner auf dem Mars mit einer IPv4-Adresse auf der Erde kommunizieren kann, muss er nur die letzten 32 bit der angefragten IPv4-Adresse im IPv6-Präfix $64:ff9b::/96$ setzen und stattdessen diese Adresse verwenden. Ihr WWNAT64 ist von der Erde aus unter den Adressen $15.23.218.93$ und $982::71:898a$ erreichbar.

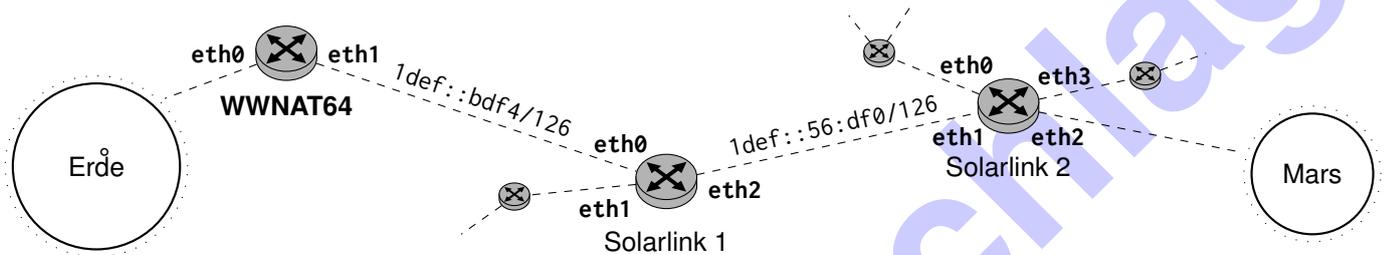


Abbildung 4.1: Solarlink Netz-Topologie

0 1 a)* Wie viele Adressen verbleiben Ihnen für das IPv6-Netz auf dem Mars?

$$2^{128-4} - 2^{128-62} = 2^{124} - 2^{66}$$

0 1 2 3 b)* Bestimmen Sie alle IP-Adressen der Interfaces **WWNAT64.eth0**, **WWNAT64.eth1**, **Solarlink 1.eth0**, **Solarlink 1.eth2** und **Solarlink 2.eth1**. Das numerisch kleinere Interface soll dabei auch die kleiner IP-Adresse erhalten.

Interface	Adresse	Interface	Adresse
WWNAT64.eth0	15.23.218.93	Solarlink 1.eth0	1def::bdf5
WWNAT64.eth0	982::71:898a	Solarlink 1.eth2	1def::56:df2
WWNAT64.eth1	1def::bdf6	Solarlink 2.eth1	1def::56:df1

0 1 c)* Es gibt auf dem Mars noch ältere Geräte, die die Übersetzung der IPv4- in IPv6-Adressen nicht implementiert haben. Zudem dient ihr WWNAT64 auch als DNS-Resolver. Wie können Sie diesen Umstand ausnutzen, damit diese alten Geräte trotzdem reine IPv4-fähige Erdlingsseiten aufrufen können?

Der Resolver kann die Übersetzung der Adressen übernehmen. Für reine IPv4 befähigten Server (erkennbar daran, dass im DNS nur ein A-Record hinterlegt ist), kann der DNS-Resolver vom WWNAT64 zusätzlich die übersetzten IPv6-Adressen als AAAA-Records ausliefern.

Als Sie Ihren PC auf dem Mars einschalten, hat dieser noch keine IP-Adresse. Sie wollen aber im Internet kommunizieren und brauchen eine. Dank IPv6 und SLAAC ist dies kein Problem. Ihre MAC-Adresse ist die 5d:38:20:bb:e3:0c und Ihr Router hat das globale Präfix 1aff:e:de::/64 zugeteilt bekommen.

d)* Wie heißt die erste IPv6-Adresse, die sich Ihr Rechner automatisch generiert?



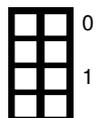
Der PC wird sich erst eine Link-Local Adresse generieren

e)* Wozu benötigt Ihr Rechner diese Adresse?



Er benötigt sie, damit er mit dem Router im lokalen Direktverbindungsnetz kommunizieren kann und so unter anderem das globale Präfix von dem aktuellen Subnetz erfragen kann.

f)* Bestimmen Sie die erste generierte Adresse.



Die durch SLAAC generierte Link-Local Adresse ist fe80::5f38:20ff:febb:e30c

g)* Wie heißt die zweite IPv6-Adresse, die sich Ihr PC automatisch generiert?



Der PC wird sich eine Global-Unique Adresse generieren

h)* Wozu dient diese zweite Adresse?



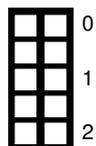
Der PC benötigt die Global-Unique Adresse, um global im Internet erreichbar zu sein und kommunizieren zu können.

i)* Bestimmen Sie die zweite automatisch generierte IPv6-Adresse.



Die generierte Global-Unique Adresse ist 1aff:e:de::5f38:20ff:febb:e30c

j)* Sie wollen die Domain iam.always.online von der Erde aufrufen, allerdings erhalten Sie nur die Adresse 60.239.113.11 bei der Namensauflösung als Antwort. Welche IPv6-Adresse müssen Sie als Ziel definieren, um eine Verbindung aufzubauen? Machen Sie deutlich, wie die einzelnen Bestandteile der Adresse zustande kommen.



Erst muss die Dezimalschreibweise der IPv4 Adresse in ein Hex Format gebracht werden. Die Hex Ziffern können dann direkt in die letzten 4 Byte der IPv6-Adresse übernommen werden.

NAT64 Prefix 64:ff9b::/96
⇒ 64:ff9b::3cef:710b
IPv4-Adresse im HEX Format

Nehmen Sie im Folgenden an, Ihr PC hat die IPv6-Adresse `1aff:e:de::42`. Sie bauen eine HTTPS Verbindung mit der IPv4-Adresse `60.239.113.11` auf.

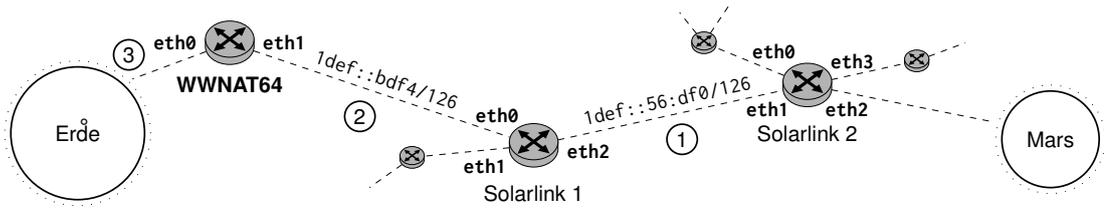


Abbildung 4.2: Kopie von Abbildung 4.1 (damit man nicht blättern muss)

0

 k) Geben Sie geforderten Daten an den Stellen 1, 2 und 3 aus Abb. 4.2 von dem ersten Segment an, das Ihr Rechner verschickt.

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Src. IP: <code>1aff:e:de::42</code></td></tr> <tr><td>Src. Port: <code>3608</code></td></tr> <tr><td>Dst. IP: <code>64:ff9b::3cef:710b</code></td></tr> <tr><td>Dst. Port: <code>443</code></td></tr> <tr><td>TTL: <code>64</code></td></tr> </table>	Src. IP: <code>1aff:e:de::42</code>	Src. Port: <code>3608</code>	Dst. IP: <code>64:ff9b::3cef:710b</code>	Dst. Port: <code>443</code>	TTL: <code>64</code>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Src. IP: <code>1aff:e:de::42</code></td></tr> <tr><td>Src. Port: <code>3608</code></td></tr> <tr><td>Dst. IP: <code>64:ff9b::3cef:710b</code></td></tr> <tr><td>Dst. Port: <code>443</code></td></tr> <tr><td>TTL: <code>63</code></td></tr> </table>	Src. IP: <code>1aff:e:de::42</code>	Src. Port: <code>3608</code>	Dst. IP: <code>64:ff9b::3cef:710b</code>	Dst. Port: <code>443</code>	TTL: <code>63</code>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Src. IP: <code>15.23.218.93</code></td></tr> <tr><td>Src. Port: <code>3608</code></td></tr> <tr><td>Dst. IP: <code>60.239.113.11</code></td></tr> <tr><td>Dst. Port: <code>443</code></td></tr> <tr><td>TTL: <code>62</code></td></tr> </table>	Src. IP: <code>15.23.218.93</code>	Src. Port: <code>3608</code>	Dst. IP: <code>60.239.113.11</code>	Dst. Port: <code>443</code>	TTL: <code>62</code>
Src. IP: <code>1aff:e:de::42</code>																	
Src. Port: <code>3608</code>																	
Dst. IP: <code>64:ff9b::3cef:710b</code>																	
Dst. Port: <code>443</code>																	
TTL: <code>64</code>																	
Src. IP: <code>1aff:e:de::42</code>																	
Src. Port: <code>3608</code>																	
Dst. IP: <code>64:ff9b::3cef:710b</code>																	
Dst. Port: <code>443</code>																	
TTL: <code>63</code>																	
Src. IP: <code>15.23.218.93</code>																	
Src. Port: <code>3608</code>																	
Dst. IP: <code>60.239.113.11</code>																	
Dst. Port: <code>443</code>																	
TTL: <code>62</code>																	
1: Solarlink 2 → Solarlink 1	2: Solarlink 1 → WWNAT64	3: WWNAT64 → Erde															

0

 l) Machen Sie den/die benötigten Einträge in der folgenden NAT-Tabelle von dem WWNAT64, die für die HTTPS Verbindung aus der vorherige Aufgabe k) notwendig sind.

Lokale IP	Lokaler Port	Protokoll	Globaler Port	Ziel IP	Ziel Port
<code>1aff:e:de::42</code>	<code>3608</code>	<code>TCP</code>	<code>3608</code>	<code>60.239.113.11</code>	<code>443</code>

0

 m)* Es gibt $2^{16} = 65\,536$ verschiedene Port Nummern. Bedeutet dies, dass Ihr WWNAT64 nur maximal 65 536 IPv6-zu-IPv4-Verbindungen von dem Mars zur Erde versorgen kann? Begründen Sie!

Laut NAT-Tabelle berücksichtigt das WWNAT64 auch das Protokoll, die Ziel IPv4-Adresse und den Ziel Port auf der Erde. Dies bedeutet es ist nicht durch die maximale Menge an eigenen Ports limitiert und kann somit pro Ziel auf der Erde und Protokoll bis zu 2^{16} (abzüglich reservierter Ports) Verbindungen von Clients versorgen.

Aufgabe 5 Packet Pair Probing (16 Punkte)

Gegeben sei die in Abbildung 5 dargestellte Situation. 1 und 2 sowie 3 und 4 bilden jeweils ein lokales Netzwerk mit Gigabit-Ethernet. Der Uplink des Routers 2 zu seinem ISP stellt gewöhnlich den limitierenden Faktor dar² und begrenzt damit die Übertragungsrate r_{23} und damit natürlich auch r_{14} .

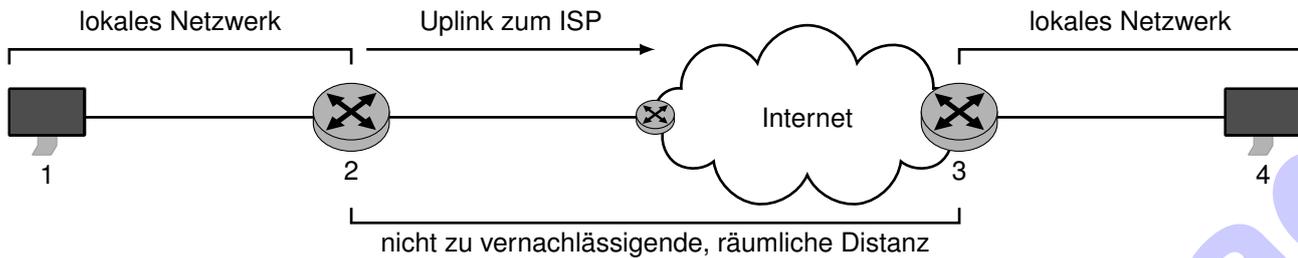


Abbildung 5.1: Netztopologie

Wir schicken nun ICMPv4 Echo Requests der Länge L von 1 nach 4 und wollen durch Messung und geschickte Ausnutzung entstehender Zeitverzögerungen an 4 die Uplink-Bandbreite bestimmen (die ja der erzielbaren Datenrate r_{23} entspricht).

a)* Geben Sie allgemein die Serialisierungszeit s_{ij} sowie die Ausbreitungsverzögerung p_{ij} zwischen zwei benachbarten Knoten an.

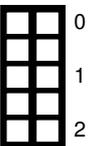
$s_{ij} = \frac{L}{r_{ij}} \quad p_{ij} = \frac{d_{ij}}{\nu c}, \text{ wobei } d_{ij} \text{ die Distanz zwischen } i \text{ und } j \text{ in } m \text{ beschreibt.}$



Für eine möglichst genaue Bestimmung ist es wichtig, dass die Echo Requests (und damit auch die Echo Replies) möglichst groß sind, die einzelnen Pakete aber nicht fragmentiert werden.

b)* Erläutern Sie kurz, wie 1 die maximale MTU auf dem Pfad von 1 nach 4 bestimmen kann.

1 sendet ein Paket mit der lokalen MTU, in dem das DF-Bit gesetzt ist. Sollte ein dazwischen liegender Link limitierend sein, wird 1 ein ICMP Destination Unreachable / Fragmentation Need erhalten. Dies wiederholt sich ggf., falls ein nachfolgender Link eine noch kleinere MTU aufweist.



c) Stellt das Verfahren aus Teilaufgabe b) auch sicher, dass Pakete von 4 an 1 nicht fragmentiert werden?

Nein, da die Pakete von 4 nach 1 über eine andere Route im Internet geroutet werden könnten und infolge dessen auch eine andere Path-MTU gelten könnte.



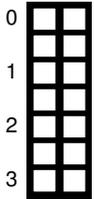
²Bei privaten Internetanschlüssen ist der Uplink üblicher Weise sehr viel langsamer als der Downlink.

Knoten 1 sende nun unmittelbar nacheinander zwei ICMP Echo Requests der Länge L an 4. Wir gehen vereinfachend davon aus, dass eventuelle andere Übertragungen an den Routern 2 und 3 nicht ins Gewicht fallen. Verarbeitungszeiten an den Knoten werden vernachlässigt.

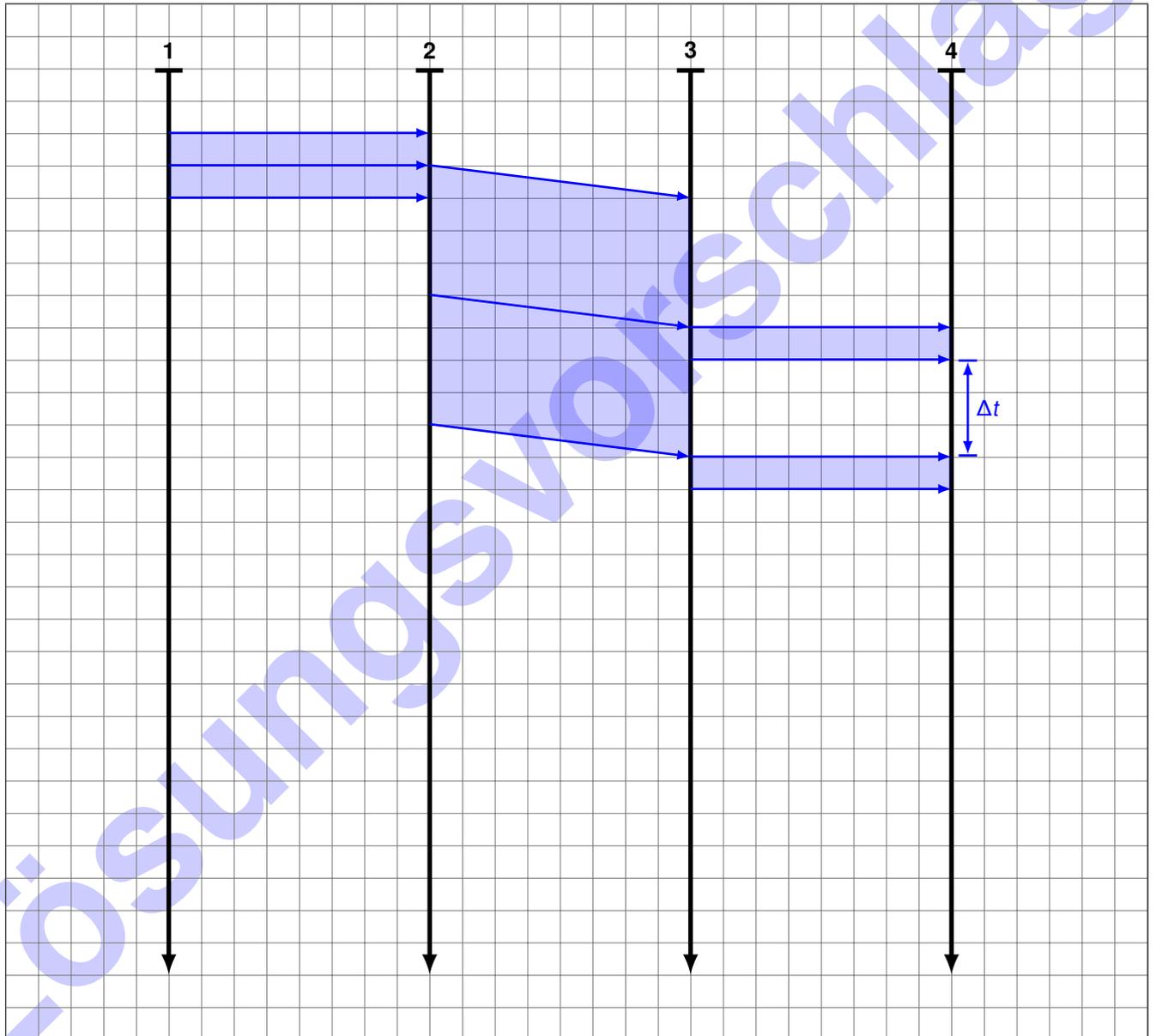


d)* Wie wird 4 reagieren, wenn er den Request erhält.

Er sollte mit einem ICMP Echo Reply derselben Größe antworten. (Payload des Requests wird gewöhnlich im Reply zurückgeschickt.)



e) Ergänzen Sie das unten stehende Weg-Zeit-Diagramm (nur für Pakete von 1 nach 4). Die Ausbreitungsverzögerung innerhalb der lokalen Netze sei zu vernachlässigen.



Durch den vergleichsweise langsamen Uplink entsteht ein Empfangspause Δt . Diese kann 4 messen.

f) Markieren Sie die Empfangspause an 4 in der Lösung von Teilaufgabe e).

g) Von welchen Größen hängt Δt ab?



Von L und r_{23} bzw. r_{34} .

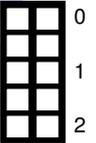


h) Geben Sie einen Ausdruck für Δt an.

$$\Delta t = s_{23} - s_{34} = \frac{L}{r_{23}} - \frac{L}{r_{34}}$$

(Vereinfachen nicht notwendig)

Keine Wertung, wenn Teilaufgaben e), f) und g) nicht oder falsch gelöst wurden (da eine Herleitung ohne diese nicht möglich ist).

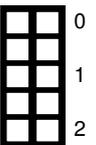


i) Geben Sie einen Ausdruck für die gesuchte Datenrate r_{23} an. Vereinfachen Sie das Ergebnis soweit möglich.

Auflösen des Ergebnisses aus Teilaufgabe h) ergibt:

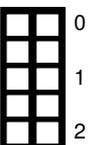
$$r_{23} = \frac{L}{\Delta t + \frac{L}{r_{34}}}$$

Keine Wertung, wenn Teilaufgaben e), f) und g) nicht oder falsch gelöst wurden (da eine Herleitung ohne diese nicht möglich ist).



j) Angenommen es gilt $r_{12} \neq r_{34}$. Begründen Sie, unter welcher Bedingung das Verfahren noch wie gewünscht funktioniert.

Solange $r_{34} \geq r_{23}$, da sonst kein Δt an 4 mehr entsteht, **und** $r_{12} \geq r_{23}$, da sonst der Uplink nicht vollständig ausgenutzt wird.



Aufgabe 6 Wireshark (14 Punkte)

Gegeben sei der Ethernet-Rahmen aus Abbildung 6, welcher im Folgenden analysiert werden soll.

```
0x0000  0c  c4  7a  80  52  58  00  25      90  57  22  4a  86  dd  60  00
0x0010  00  00  04  d8  3a  3c  20  01      06  38  00  0c  c0  71  00  00
0x0020  00  00  00  00  00  01  20  01      4c  a0  20  01  00  11  31  a0
0x0030  6d  28  d9  38  75  0c  03  00      14  00  9a  00  00  00  60  05
0x0040  5d  d6  05  3a  11  01  20  01      4c  a0  20  01  00  11  31  a0
0x0050  6d  28  d9  38  75  0c  2a  00      14  50  40  01  08  08  00  00
0x0060  00  00  00  00  20  03  ae  36      01  bb  05  3a  2f  ef  c8  ff
0x0070  00  42
```

Abbildung 6.1: Ethernet-Rahmen einschließlich Checksumme

Beachten Sie, dass für alle nachfolgenden Teileingaben Begründungen erforderlich sind. Diese kann z. B. durch Markierung der entsprechenden Felder im Hexdump und unter Nennung des Feldnamens erfolgen. Achten Sie darauf, dass Markierungen eindeutig einzelnen Teilaufgaben zugeordnet werden können. Nicht nachvollziehbare Aussagen **werden nicht bewertet**.



a)* Markieren Sie in Abbildung 6 die Absenderadresse auf Schicht 2.



b)* Markieren Sie in Abbildung 6 die Empfängeradresse auf Schicht 2.



c)* Begründen Sie, von welchem Typ ist die L3-PDU ist.

Ethertype 0x86dd ⇒ IPv6



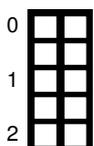
d) Geben Sie die Absenderadresse auf Schicht 3 in ihrer üblichen und ggf. gekürzten Schreibweise an.

2001:638:c:c071::1



e) Geben Sie die Empfängeradresse auf Schicht 3 in ihrer üblichen und ggf. gekürzten Schreibweise an.

2001:4ca0:2001:11:31a0:6d28:d938:750c



f) Begründen Sie, ob die Adressen aus den Teilaufgaben d) und e) dynamisch zugewiesen oder statisch konfiguriert sind.

Beide Adressen sind sehr wahrscheinlich statisch konfiguriert, da der für SLAAC übliche Einschub ff:fe in den Oktetten 11 und 12 fehlt.
Hinweis: Die Adresse 2001:4ca0:2001:11:31a0:6d28:d938:750c könnte auch über DHCPv6 zugewiesen worden sein.

Von der L3-SDU sei bekannt, dass sie an Offset $0x0036$ beginnt und es sich um ICMPv6 handelt.

g)* Bestimmen Sie Type und Code des ICMP-Pakets.

Type $0x03 \Rightarrow$ Time Exceeded
Code $0x00 \Rightarrow$ Hop Limit Exceeded



h) Unter welchen Umständen erhält ein Host eine solche Nachricht? Nennen Sie einen möglichen Grund, welches Problem wahrscheinlich zugrunde liegt!

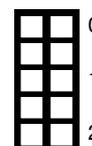
Wenn das Hop Limit eines Pakets bei der Weiterleitung 0 erreicht. Dies geschieht i. d. R. nur, wenn eine Routing Schleife existiert.



i) Welcher Knoten ist der Absender dieser ICMPv6 Nachricht?

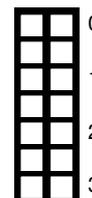
Hinweis: Hier ist nicht nach einer Adresse gefragt sondern allgemein danach, welcher Knoten im Netzwerk / Internet der Absender sein muss.

Ein Router auf dem Weg von $2001:638:c:c071::1$ zu einem (noch unbekanntem) Ziel.



j) Begründen Sie, ob sich bestimmen lässt, welches Paket bzw. welche Anwendung diese Nachricht ausgelöst hat.

Dem ICMPv6 Header folgt der IPv6 Header sowie die ersten 8 B Payload desjenigen Pakets, das wegen des Hop Limits verworfen wurde. Darin sind insbesondere die ursprünglichen L3-Adressen (Quelle und Ziel), der Typ der L4-Payload sowie im Fall von TCP/UDP die Portnummern enthalten.



Zusätzlicher Platz für Lösungen. Markieren Sie deutlich die Zuordnung zur jeweiligen Teilaufgabe. Vergessen Sie nicht, ungültige Lösungen zu streichen.

