

Klausur - Musterlösung Telematik

Prof. Dr. Martina Zitterbart
Institut für Telematik
KIT-Fakultät für Informatik
Karlsruher Institut für Technologie (KIT)

Montag, 27.03.2023

- Diese Klausur umfasst **22 Seiten** und insgesamt **6 Aufgaben**. Bitte kontrollieren Sie jetzt, ob Sie eine vollständige Ausgabe erhalten haben.
 - Sie dürfen Ihre Antworten in Deutsch oder Englisch formulieren. Der Wechsel der Sprache innerhalb einer Teilaufgabe ist nicht erlaubt.
 - Schreiben Sie mit blauer oder schwarzer Farbe und mit einem permanenten Stift.
 - Beachten Sie, dass die vorgegebenen Antwortfelder großzügig dimensioniert sind. In vordruckten Tabellen müssen nicht unbedingt alle freien Einträge für eine korrekte Lösung genutzt werden.
 - **Es werden nur solche Ergebnisse gewertet, bei denen ein Lösungsweg eindeutig erkennbar ist.** Antworten sind **grundsätzlich zu begründen**, falls es in der jeweiligen Teilaufgabe nicht ausdrücklich anders vermerkt ist.
 - Wenn Sie Ergebnisse aus einer Teilaufgabe in eine andere Teilaufgabe übernehmen, machen Sie dies bitte kenntlich.
 - Insgesamt sind **60 Punkte** zu erreichen.
- *This exam consists of 22 pages and a total of 6 tasks. Please check now if you have received a complete edition.*
 - *You may provide your answers in German or English. Changing the language within a subtask is not allowed.*
 - *Write in black or blue color and use a permanent pen.*
 - *Note that the provided answer fields are generously dimensioned. In preprinted tables not all free entries have to be used for a correct solution.*
 - *Only those results are evaluated in which the solution path is clearly recognizable. Answers have to be justified in principle unless explicitly stated otherwise in the respective subtask.*
 - *If you transfer results from one subtask to another subtask, please indicate this.*
 - *A total of 60 points can be achieved.*

A1	A2	A3	A4	A5	A6	Σ
9	11	10	9	10	11	60

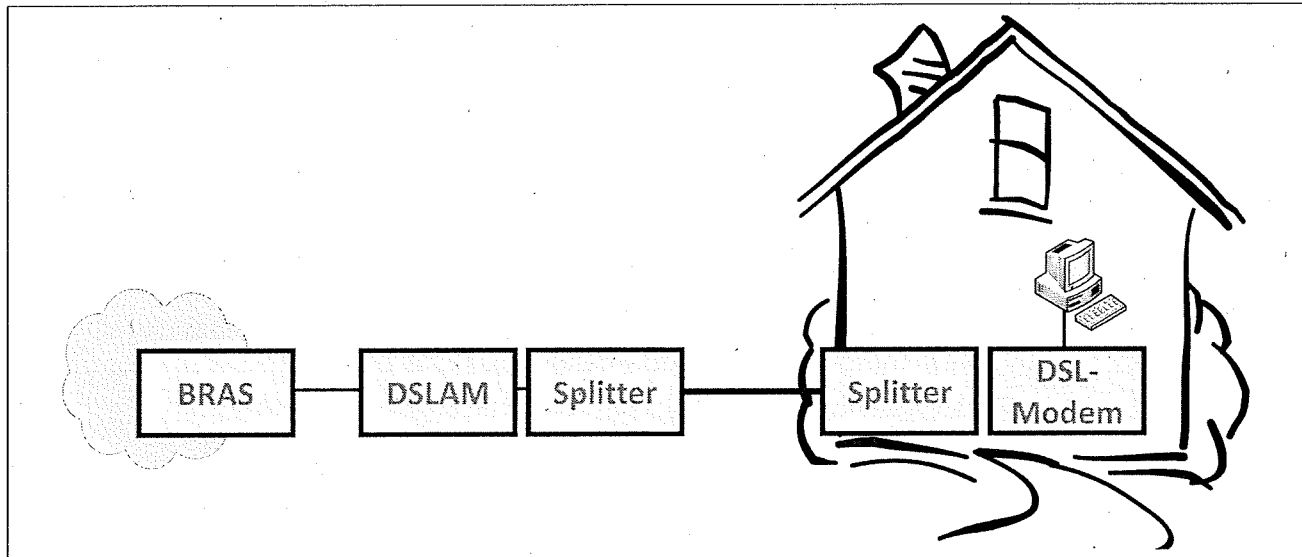
Aufgabe 1 Allgemein (9 Punkte)

9

a) Benennen Sie die Komponenten eines DSL-Netzes in den freien Feldern der nachfolgenden Abbildung.

2

Label the components of a DSL network in the empty fields of the following figure.



b) Zu welchem Zweck wurde Carrier Extension eingeführt und wie funktioniert es? Bei welcher Variante von Ethernet wurde es eingeführt? Wieso ist Carrier Extension bei 10-Gigabit-Ethernet nicht mehr erforderlich und wird deshalb auch nicht mehr unterstützt?

2

For what purpose was Carrier Extension introduced and how does it work? What variant of Ethernet introduced it? Why is Carrier Extension no longer required and therefore no longer supported with 10 Gigabit Ethernet?

Carrier Extension wurde zum Zweck der Kollisionserkennung eingeführt.
 Carrier Extension sendet zusätzliche Bytes nach dem Ende eines Ethernet Rahmens.
 Carrier Extension wurde bei Gigabit-Ethernet (1 Gbit/s) eingeführt.
 10-Gigabit-Ethernet unterstützt keine Halbduplex-Links mehr, weshalb Kollisionserkennung nicht mehr erforderlich ist.

2 c) Wie funktioniert Flusskontrolle auf Vollduplex-Links bei Ethernet? Welche zusätzliche Funktionalität bietet die Erweiterung *Priority-based Flow Control*? In welchem Paketkopf werden die für diese Erweiterung notwendigen Informationen übertragen?

How does flow control work on full-duplex links in Ethernet? What additional functionality does the extension Priority-based Flow Control offer? In which header is the information required for this extension transmitted?

Flusskontrolle auf Vollduplex-Links:

Ein empfangendes System sendet einen PAUSE-Rahmen.

Beim Empfang des PAUSE-Rahmens unterbricht das sendende System das Senden für das im PAUSE-Rahmen angegebene Zeitintervall.

Priority-based Flow Control:

Priority-based Flow Control gestattet das Pausieren von Verkehrsklassen differenziert nach Priorität.

Header:

Q-Header

1 d) Um die Größe des Staukontrollfensters zu bestimmen, berechnet Data Center TCP (DCTCP) die Variable DCTCP.Alpha wie unten angegeben. Erläutern Sie, wofür der Faktor M steht.

To determine the size of the congestion window, Data Center TCP (DCTCP) calculates the variable DCTCP.Alpha as shown below. Explain what the factor M stands for.

$$\text{DCTCP.Alpha} = (1 - g) \cdot \text{DCTCP.Alpha} + g \cdot M$$

Anteil der Bytes die eine Stausituation während eines Beobachtungsfensters (*observation window*) erfahren haben.

e) Welche zwei Skalierbarkeitsprobleme treten in großen OSPF-Domänen mit einer einzelnen Area auf? Welchen Vorteil hat die Einteilung in mehrere OSPF-Areas im Kontext dieser Probleme? Welche Informationen beinhalten Summary-LSAs?

Which two scalability issues arise in large single-area OSPF domains? What advantage does the division into multiple OSPF areas have in the context of these issues? What information do summary LSAs contain?

Skalierbarkeitsprobleme:

- Overhead of LSA Flooding
- Overhead of (re-)calculation of shortest paths

Vorteil mehrerer OSPF-Areas:

LSA-Fluten und die Berechnung der kürzesten Pfade ist beschränkt auf Router in derselben Area.

Inhalt von Summary-LSAs:

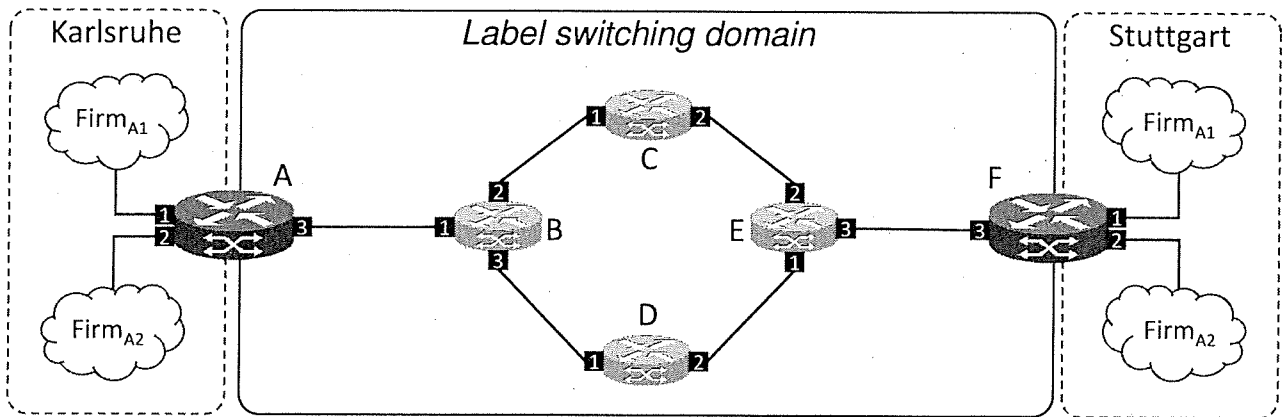
Liste von Zielen die in einer Area erreichbar sind und deren Pfadkosten.

Aufgabe 2 Label Switching (11 Punkte)

11

Die folgende Abbildung zeigt eine Label Switching Domäne, die die Standorte zweier Firmen, $Firm_{A1}$ und $Firm_{A2}$, verbindet. Es wurde bereits ein Label Switching Pfad (LSP) von Karlsruhe nach Stuttgart für $Firm_{A1}$ etabliert. Für diesen LSP relevante Auszüge aus den Label Forwarding Information Bases (LFIB) sind in der folgenden Abbildung dargestellt.

The following figure shows a label switching domain that connects the sites of two companies, $Firm_{A1}$ and $Firm_{A2}$. A label switching path (LSP) from Karlsruhe to Stuttgart for $Firm_{A1}$ has already been established. Relevant excerpts from the label forwarding information bases (LFIB) for this LSP are shown in the following figure.



LFIB Router A			
Interface in	Label in	Interface out	Label out
1	-	3	1

LFIB Router E			
Interface in	Label in	Interface out	Label out
2	4	3	5

LFIB Router B			
Interface in	Label in	Interface out	Label out
1	1	2	2

LFIB Router F			
Interface in	Label in	Interface out	Label out
3	5	1	-

- 1 a) Vervollständigen Sie die folgende LFIB von Router C mit den nötigen Regeln des bereits etablierten LSPs von Karlsruhe nach Stuttgart der $Firm_{A1}$.
 Complete the following LFIB of router C with the necessary rules of the already established LSP from Karlsruhe to Stuttgart of $Firm_{A1}$.

LFIB Router C			
Interface in	Label in	Interface out	Label out
1	2	2	4

b) Erklären Sie die Aufgabe von Label Edge Devices und Label Switching Devices.

Explain the task of label edge devices and label switching devices.

1

Label Edge Device:

Zuweisung und Entfernen von Labeln an/von ein eingehendes Paket passend zum jeweiligen Flow, und Weiterleitung.

Label Switching Device:

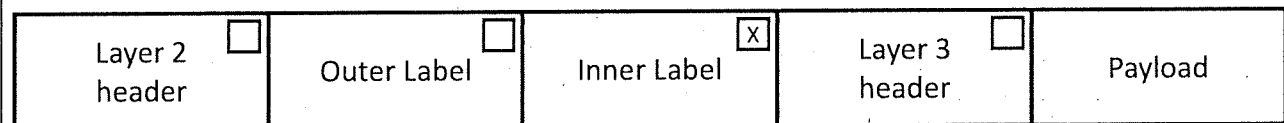
Weiterleitung von Paketen auf Basis von Labeln und Austauschen der Labeln (label swapping).

c) Erklären Sie die Struktur des Label Stacks im Kontext von VPNs mittels MPLS und den Zweck der einzelnen Labels. Tragen Sie die Labelarten des Label Stacks sowie die Header der Layer 2 und 3 in die nachfolgende Abbildung ein. Kennzeichnen Sie außerdem den Bottom of Stack durch Ankreuzen.

2,5

Explain the structure of the label stack in the context of VPNs using MPLS and the purpose of the individual labels. Enter the label types of the label stack in the following figure, as well as the headers of layer 2 and 3. Also mark the bottom of stack by crossing.

Label Stack beinhaltet im Kontext des VPN ein inneres und ein äußeres Label. Das innere Label identifiziert das VPN, das Äußere den LSP.



d) Welche beiden Nachrichtentypen kommen bei RSVP-TE bei der Labelverteilung zum Einsatz? Nennen Sie die beiden Typen und erklären Sie kurz deren Zweck.

Which message types are available in RSVP-TE for label distribution? Name the two message types and explain their application purpose.

Path message

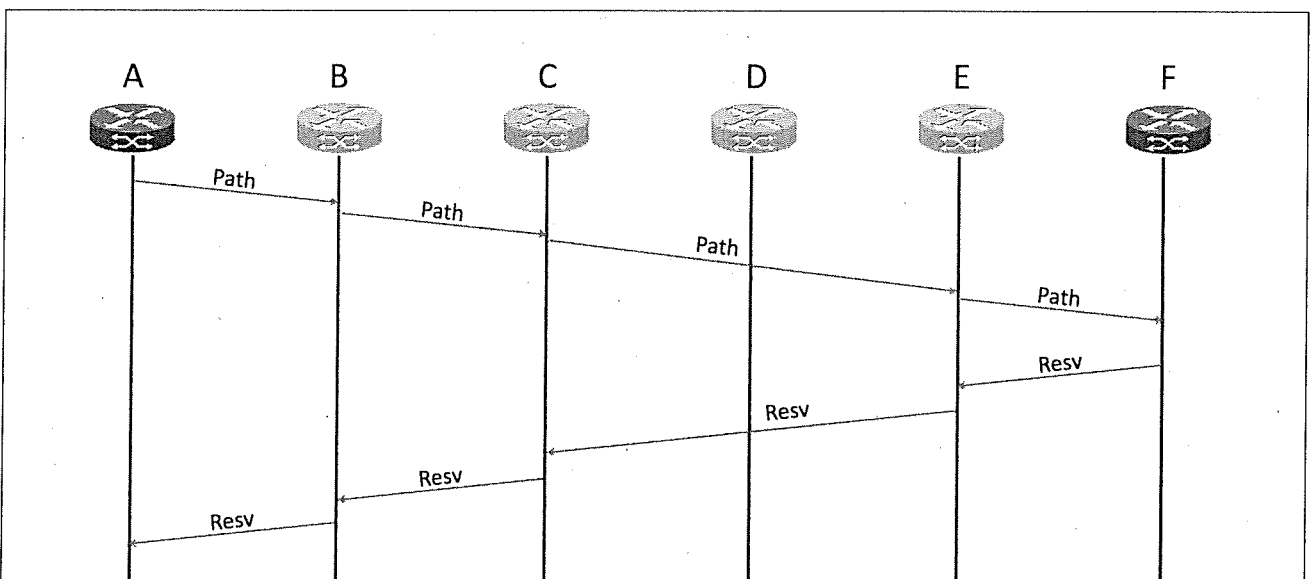
Von Upstream-LER zu Downstream-LER, Label-Anforderung

Resv message

Antwort auf eine Path Message, von Downstream-LER zu Upstream-LER, Label Binding

e) Die Labelverteilung des bereits etablierten LSPs wurde mittels RSVP-TE durchgeführt. Zeichnen Sie diese Labelverteilung in das folgende Weg-Zeit-Diagramm ein. Geben Sie zu jeder Nachricht ihren Typ an. Durch welches Zwischensystem wird jeweils "Label in" und "Label out" von Router E für den gegebenen LSP bestimmt? Handelt es sich bei dieser Art der Labelverteilung um die Strategie *Unsolicited Downstream* oder *Downstream on Demand*? Erklären Sie Ihre Entscheidung.

The label distribution of the already established LSP was carried out using RSVP-TE. Draw this label distribution into the following distance-time diagram. Which intermediate system determines "Label in" and "Label out" of router E for the given LSP? Is this kind of label distribution strategy Unsolicited Downstream or Downstream on Demand? Explain your decision.



"Label in" an Router E bestimmt durch? Router E

"Label out" an Router E bestimmt durch? Router F

Strategie der Labelverteilung? Erklären Sie Ihre Entscheidung.

Downstream on Demand, denn Downstream-Router generieren Labels nachdem Upstream-Router Labels für die Bindung der FEC anfordern.

f) Geben Sie für jede Regel in der folgenden LFIB an, mit welchen anderen Regeln sie in Konflikt steht. Erklären Sie Ihre Entscheidung.

For each rule in the following LFIB, state which other rules it is in conflict with. Explain your decision.

LFIB Router X					
Rule Nr.	Interface in	Label in	Interface out	Label out	Conflict with
1	1	1	2	1	3
2	2	1	1	1	
3	1	1	2	2	1
4	2	2	1	1	
5	1	2	2	1	

Erklärung:

Mapping von Interfaces und Labels muss lokal eindeutig sein.

Aufgabe 3 Longest Prefix Matching (10 Punkte)

10

1,5

a) Erklären Sie, warum Datenstrukturen, die Longest Prefix Matching im Kontext der Paketweiterleitung implementieren, die folgenden drei Anforderungen erfüllen müssen.

Explain why data structures that implement longest prefix matching in the context of packet forwarding need to satisfy the following three requirements.

Anforderung (requirement)	Erklärung (explanation)
Schnelle Suche (fast lookup)	Low time budget for processing small packets at high data rates
Geringer Speicherbedarf (low memory requirements)	Memory required per forwarding entry → scalability
Schnelle Aktualisierungen (fast updates)	Update required when routes change → Routes can change frequently. Therefore updates should be fast

2,5

b) Sie implementieren Longest Prefix Matching in Hardware mit TCAM. Wofür steht TCAM? Wie schnell ist die Regelauswertung mit TCAM? Nennen Sie drei Nachteile, die mit der Nutzung von TCAM einhergehen.

You implement longest prefix matching in hardware with TCAM. What does TCAM stand for? How fast is TCAM rule evaluation? Name three disadvantages of TCAM usage.

TCAM: Ternary Content Addressable Memory
Rule evaluation speed of TCAM: One clock cycle

- Hoher Energieverbrauch
- Hohe Kosten
- limitierte Kapazität
- Strikte Ordnung erforderlich

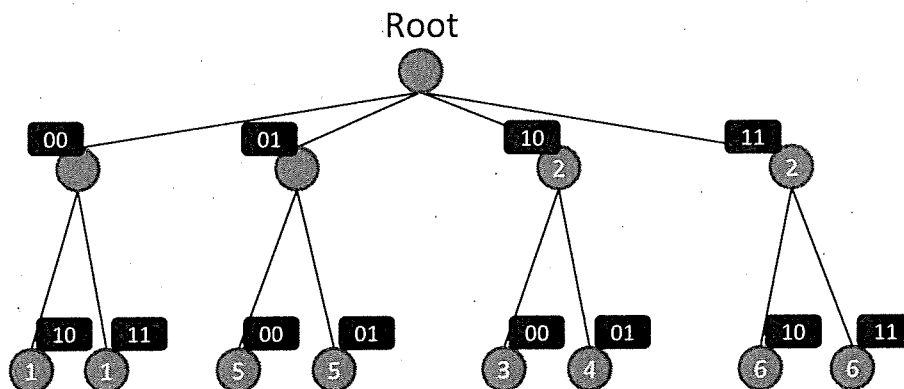
c) Geben Sie das Ergebnis der Prefix Expansion mit Stride $k = 2$ für jedes Präfix in Tabelle P1 an. Konstruieren Sie einen Multibit Trie mit festem Stride $k = 2$ für die Präfixe in Tabelle P1.

3

Give the result of prefix expansion with stride $k = 2$ for each prefix in table P1. Construct a multibit trie with fixed stride $k = 2$ for the prefixes in table P1.

Tabelle (table) P1

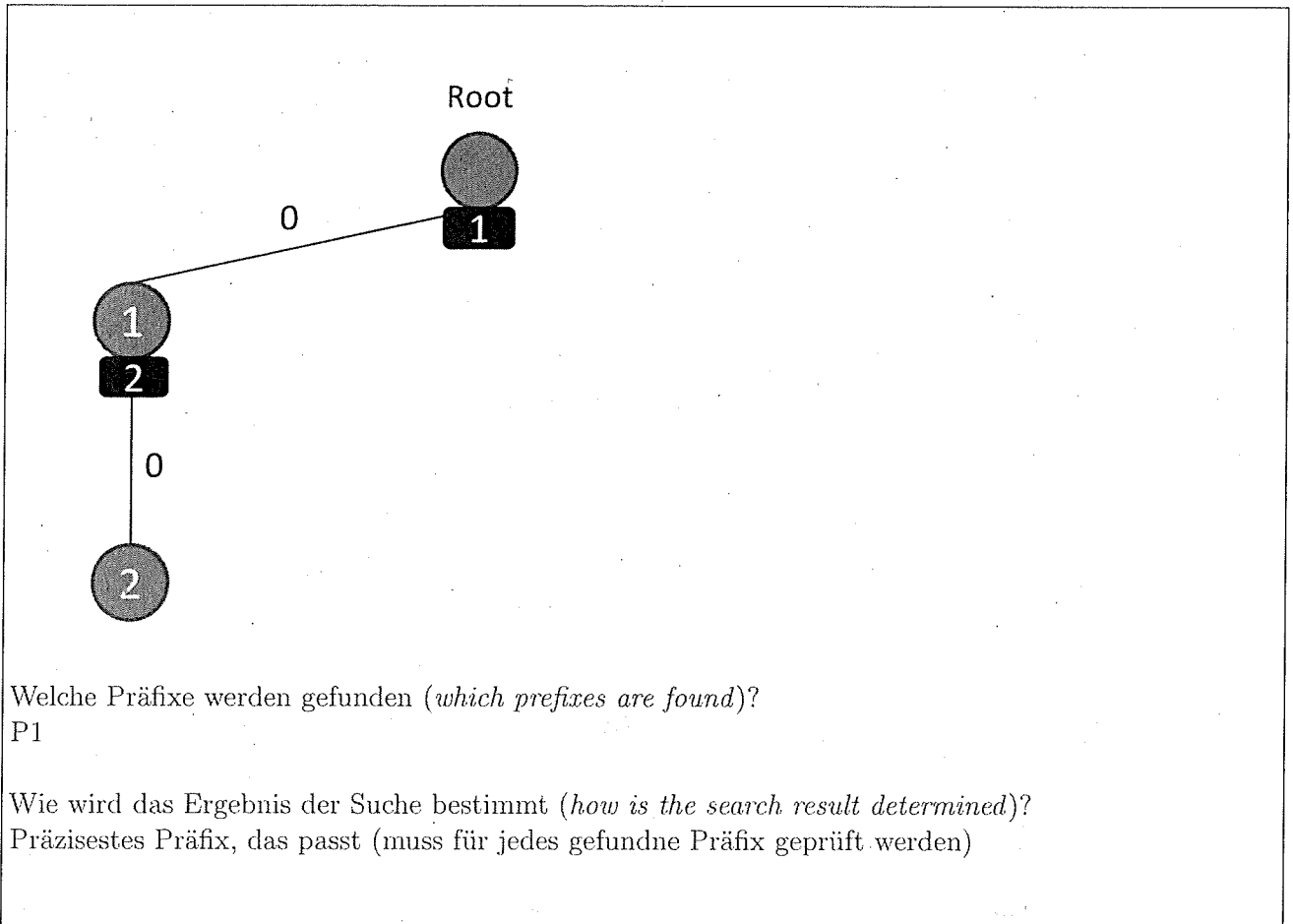
Präfixe (prefixes)		Prefix expansions
P1	001*	0011, 0010
P2	1*	10, 11
P3	1000*	leer oder 1000
P4	1001*	leer oder 1001
P5	010*	0101, 0100
P6	111*	1110, 1111



2

d) Konstruieren Sie einen Binary Trie mit Pfadkompression für die Präfixe 0^* (P1) und 000^* (P2). Erklären Sie, welche Präfixe bei einer Suche nach dem Wort 0100 gefunden werden und wie das Ergebnis der Suche bestimmt wird.

Construct a binary trie with path compression for the prefixes 0^ (P1) and 000^* (P2). Explain which prefixes are found during a search for the word 0100 and how the search result is determined.*



1 e) Bei welchen Verkehrsmustern ist es nützlich Hash Tabellen als Ergänzung für das Longest Prefix Matching einzusetzen?

For which traffic patterns is implementing hash tables as an extension for longest prefix matching useful?

Funktioniert gut, wenn IP-Adressen Lokalitäts-Charakteristiken (locality characteristics) aufweisen. Die Auswirkung der Hash-Tabelle hängt von der zugrunde liegenden Verkehrsverteilung ab.

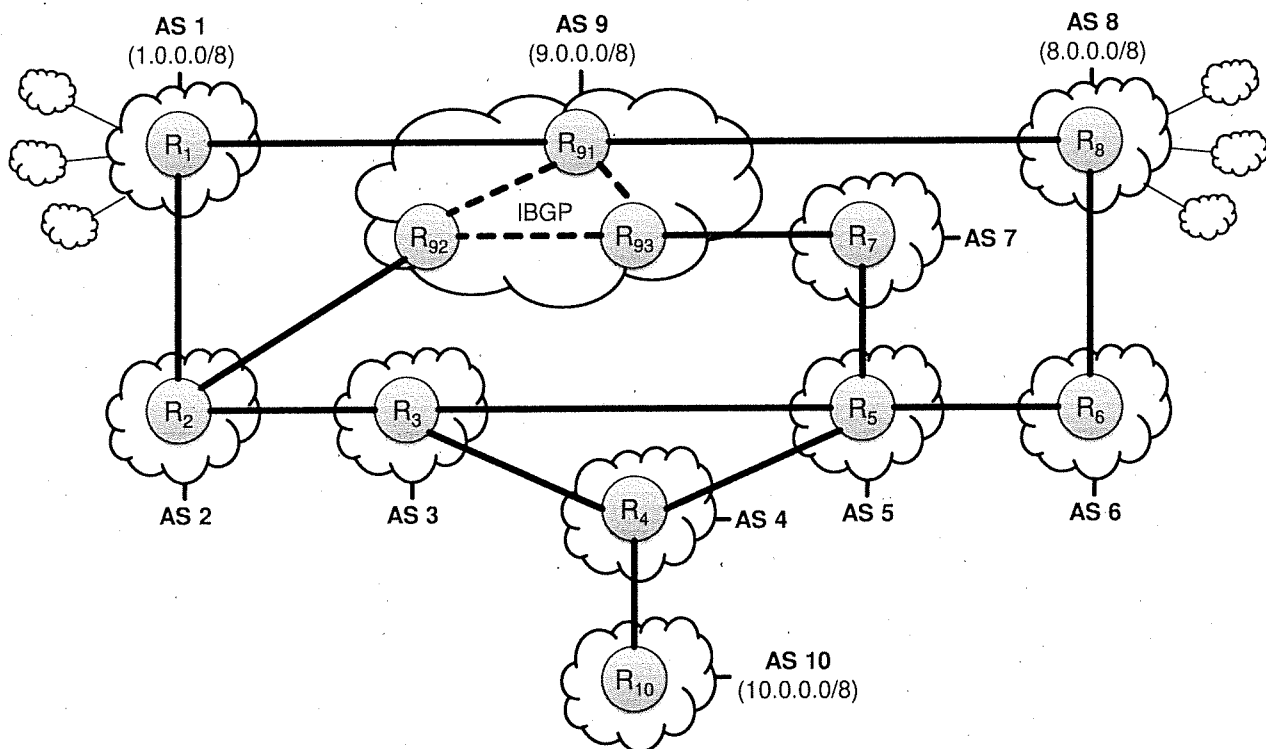
Aufgabe 4 BGP (9 Punkte)

Gegeben ist die abgebildete Topologie, bestehend aus autonomen Systemen AS_1, \dots, AS_{10} und BGP-Routern $R_1, \dots, R_8, R_{91}, R_{92}, R_{93}, R_{10}$. AS_1 und AS_8 stellen Netze mit Verbindungen zu vielen anderen Netzen dar. Durchgezogene Linien kennzeichnen physische Verbindungen und gestrichelte Linien kennzeichnen IBGP-Verbindungen (in AS_9). Verbindungen repräsentieren zudem etablierte BGP-Sitzungen. Für alle Teilaufgaben gilt das Folgende:

1. Alle autonomen Systeme außer AS_{10} sind Transit-ASes.
2. Jedes AS gibt nur die kürzesten Routen an alle Nachbarn bekannt.

The following topology is given, consisting of autonomous systems AS_1, \dots, AS_{10} and BGP routers $R_1, \dots, R_8, R_{91}, R_{92}, R_{93}, R_{10}$. AS_1 and AS_8 represent networks with connections to many other networks. Solid lines indicate physical connections and dashed lines indicate IBGP connections (in AS_9). Connections also represent established BGP sessions. The following applies to all subtasks:

1. All autonomous systems except AS_{10} are transit ASes.
2. Each AS announces only the shortest routes to all its neighbors.



a) Erläutern Sie wofür die Abkürzung IBGP steht und wozu der Einsatz von IBGP dient.

1

Explain what the abbreviation IBGP stands for and what IBGP is used for.

IBGP: Internal Border Gateway Protocol

Einsatz von IBGP: Synchronisation von BGP-Routern innerhalb eines autonomen Systems.

2

b) Geben Sie die kürzesten Routen in der BGP-Routingtabelle von Router R_2 für die Präfixe in der unten angegebenen Tabelle an, nachdem diese von ihren jeweiligen autonomen Systemen bekannt gegeben wurden. Beachten Sie, dass AS_9 IBGP einsetzt.

Specify the shortest routes in the BGP routing table of router R_2 for the prefixes in the table below after they were announced by their respective autonomous systems. Note that AS_9 uses IBGP.

Routingtabelle von R_2 (*routing table of R_2*)

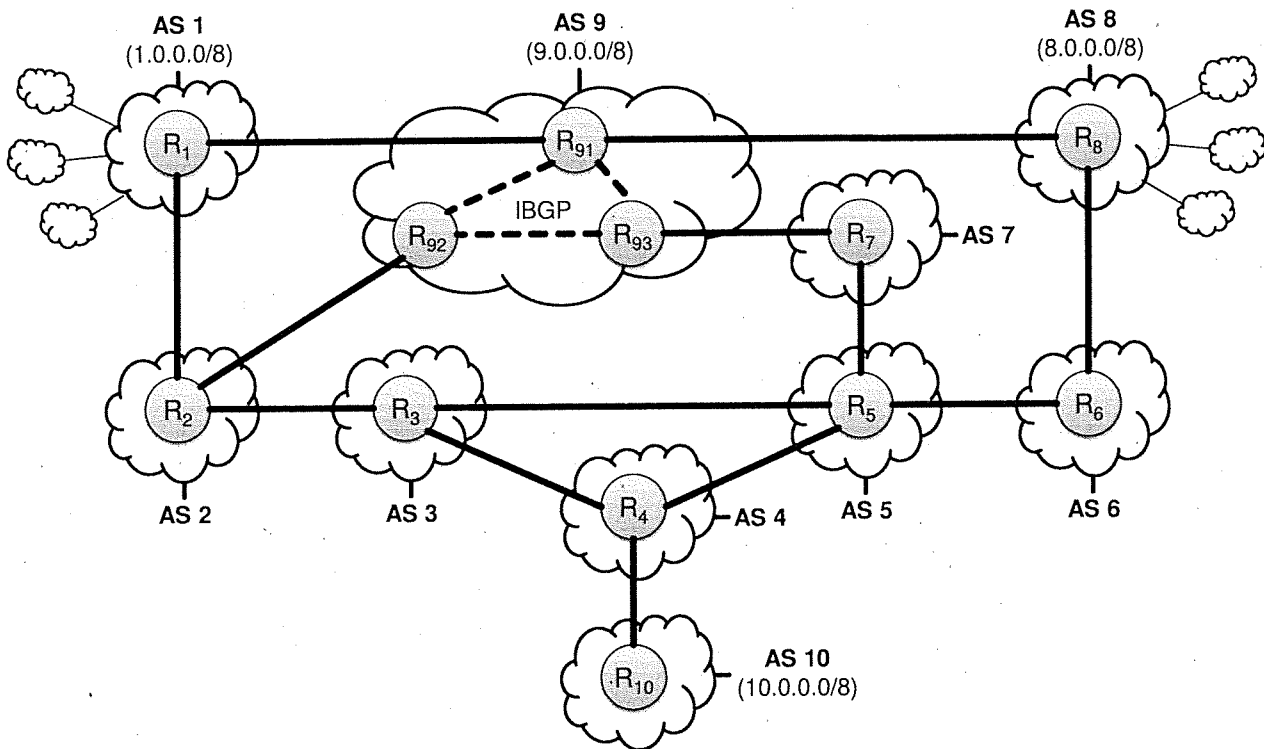
Präfix (<i>prefix</i>)	Next Hop	Pfad (<i>path</i>)
1.0.0.0/8	R_1	1
8.0.0.0/8	R_{92}	9 8
9.0.0.0/8	R_{92}	9
10.0.0.0/8	R_3	3 4 10

AS₁₀ empfängt Angriffsverkehr mit hohen Datenraten, der von AS₁ und AS₈ ungehindert weitergeleitet wird. AS₁₀ bittet AS₉ um Hilfe, da dieses Angriffsverkehr erkennen und verwerfen kann. AS₉ nutzt hierzu seine direkten Verbindungen zu AS₁ und AS₈, um den an AS₁₀ adressierten Verkehr zu sich umzuleiten. Hierzu verfährt AS₉ folgendermaßen:

1. AS₉ deaktiviert den Einsatz von IBGP.
2. AS₉ gibt das Präfix 10.0.0.0/8 über Router R₉₁ bekannt.

AS₁₀ receives attack traffic with high data rates, which is forwarded unhindered by AS₁ and AS₈. AS₁₀ asks AS₉ for help as that can detect and drop attack traffic. AS₉ uses its direct connections to AS₁ and AS₈ to redirect traffic addressed to AS₁₀ to itself. For this, AS₉ proceeds as follows:

1. AS₉ disables the use of IBGP.
2. AS₉ announces the prefix 10.0.0.0/8 through router R₉₁.



Wiederholung (*repetition*)

2 c) Geben Sie die kürzesten Routen in der BGP-Routingtabelle von Router R_2 für die Präfixe in der unten angegebenen Tabelle an, nachdem AS_9 den an AS_{10} adressierten Verkehr zu sich umgeleitet hat.

Specify the shortest routes in the BGP routing table of router R_2 for the prefixes in the table below after AS_9 has redirected the traffic addressed to AS_{10} to itself.

Routingtabelle von R_2 nach Umleiten des Verkehrs durch AS_9
(routing table of R_2 after traffic redirection by AS_9)

Präfix (<i>prefix</i>)	Next Hop	Pfad (<i>path</i>)
1.0.0.0/8	R_1	1
8.0.0.0/8	R_1	1 9 8
9.0.0.0/8	R_{92}	9
10.0.0.0/8	R_1	1 9

2 d) Über welchen seiner Router muss AS_9 den vom Angriffsverkehr bereinigten verbleibenden Verkehr weiterleiten, damit AS_{10} diesen erhält? Geben Sie den zutreffenden BGP-Routingtabelleneintrag des Routers an. Begründen Sie Ihre Wahl des Routers.

Over which of its router must AS_9 forward the remaining traffic that has been cleaned of the attack traffic, so that AS_{10} receives it? Specify the applying BGP routing table entry of the router. Justify your choice of the router.

Router: R_{93}

BGP-Routingtabelleneintrag (*BGP routing table entry*):

Präfix (<i>prefix</i>)	Next Hop	Pfad (<i>path</i>)
10.0.0.0/8	R_7	7 5 4 10

Begründung:

Eine Weiterleitung über Router R_{91} und R_{92} ist nicht möglich. Die Bekanntgabe des Präfix 10.0.0.0/8 von Router R_{91} führt dazu, dass der Verkehr bei Weiterleitung über einen der beiden Router wieder zu AS_9 zurück gesendet wird.

e) Weshalb musste AS₉ IBGP deaktivieren, um AS₁₀ zu helfen?

Why did AS₉ have to disable IBGP to help AS₁₀?

Das Präfix 10.0.0.0/8 würde bei Nutzung von IBGP auch von Router R₉₃ bekannt gegeben werden. AS₇ würde den AS-Pfad zu AS₉ präferieren, wodurch kein Weg zur Weiterleitung des bereinigten Verkehrs übrig bleibt.

f) Nennen Sie einen Vorteil, der sich durch den Einsatz eines Route-Reflectors bei BGP ergibt und erläutern Sie, wodurch dieser entsteht.

Name an advantage that results from using a route reflector with BGP and explain how it arises.

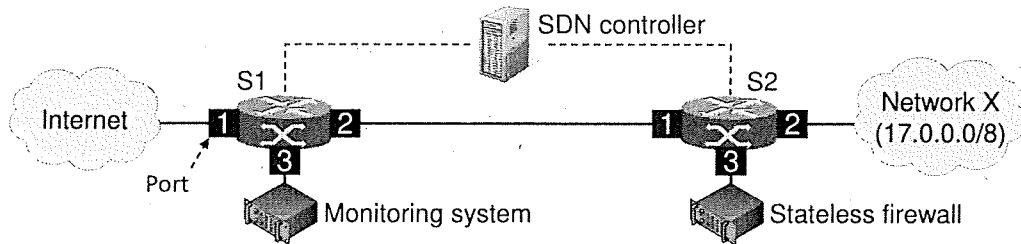
Verbesserte Skalierbarkeit

Es müssen lediglich BGP-Sitzungen zum Route-Reflector aufrecht erhalten werden, wodurch eine Vollvermaschung von BGP-Routern vermieden werden kann.

Aufgabe 5 Software Defined Networking (10 Punkte)

Sie sollen eine App für das abgebildete SDN-Netz mit den Switches S1 und S2 programmieren. Bei der Weiterleitung vom Internet zum Netz X (IP-Subnetz 17.0.0.0/8) sollen IP-Datagramme von einem Monitoring-System aufgezeichnet und/oder durch eine zustandslose Firewall verarbeitet werden. Die Weiterleitung von Netz X zum Internet soll direkt erfolgen.

You shall program an app for the depicted SDN network with switches S1 and S2. When forwarding from the Internet to network X (IP subnet 17.0.0.0/8), IP datagrams shall be recorded by a monitoring system and/or processed by a stateless firewall. Forwarding from network X to the Internet shall be done directly.



a) Geben Sie zunächst Flowtable-Einträge für S1 und S2 an, die Folgendes umsetzen:

1. S1 verwirft Datagramme aus dem Internet mit Quell-IP-Adressen im Subnetz 17.0.0.0/8.
2. S2 verwirft Datagramme aus Netz X mit Quell-IP-Adressen außerhalb des Subnetz 17.0.0.0/8.
3. S1 und S2 leiten alle anderen Datagramme aus Netz X direkt ins Internet weiter.
4. S1 und S2 leiten Datagramme ohne zutreffende Flowtable-Einträge an den SDN-Controller weiter.

First, provide flowtable entries for S1 and S2 that implement the following:

1. S1 discards datagrams from the Internet with source IP addresses in the subnet 17.0.0.0/8.
2. S2 discards datagrams from network X with source IP addresses outside the subnet 17.0.0.0/8.
3. S1 and S2 forward all other datagrams from network X directly to the Internet.
4. S1 and S2 forward datagrams without matching flow table entries to the SDN controller.

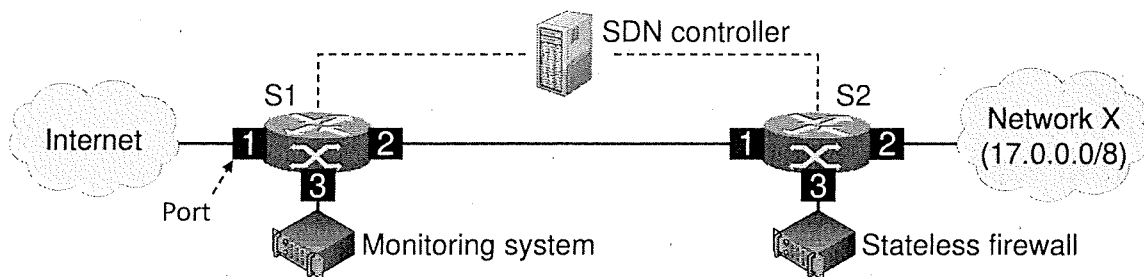
Flowtable von S1 (flow table of S1)		
Priorität (priority)	Match-Felder (match fields)	Aktion (action)
1	IN_PORT = 1, IP_SRC = 17.0.0.0/8	DROP
1	IN_PORT = 2	OUTPUT 1
0	*	CONTROLLER
Flowtable von S2 (flow table of S2)		
Priorität (priority)	Match-Felder (match fields)	Aktion (action)
2	IN_PORT = 2, IP_SRC = 17.0.0.0/8	OUTPUT 1
1	IN_PORT = 2	DROP
0	*	CONTROLLER

b) Beim Empfang von Datagrammen von S1 und S2 nutzt Ihre App die Methode `getDecision`, welche anhand von Quell- und Ziel-IP-Adressen über die Weiterleitung von Datagrammen vom Internet zu Netz X entscheidet. Die in Aufgabenteil a) beschriebenen Flowtable-Einträge sind bereits programmiert. Vervollständigen Sie nun die vorgegebene `onPacketIn`-Methode, um die in der unten stehenden Tabelle zusammengefassten Entscheidungen von `getDecision` umzusetzen.

6

When receiving datagrams from S1 and S2, your app uses the `getDecision` method, which decides on the forwarding of datagrams from the Internet to network X based on source and destination IP addresses. The flow table entries described in subtask a) are already programmed. Now complete the provided `onPacketIn` method to implement the decisions of `getDecision` summarized in the table below.

Rückgabewert (return value)	Entscheidung von <code>getDecision</code> (decision of <code>getDecision</code>)
FORWARD	Direkte Weiterleitung zu Netz X <i>Direct forwarding to network X</i>
FIREWALL	Weiterleitung zur Firewall und zu Netz X <i>Forwarding to the firewall and to network X</i>
RECORD	Weiterleitung zum Monitoring-System, zur Firewall und zu Netz X <i>Forwarding to the monitoring system, the firewall, and network X</i>



Wiederholung (repetition)

```
import S1, S2; // References to switches
import getDecision;

onPacketIn(packet, switch, inport) {
    decision = getDecision(packet.IP_SRC, packet.IP_DST)

    r1 = Rule();
    r1.PRIORITY(3);
    r1.MATCH( 'INPORT', inport );
    r1.MATCH( 'IP_SRC', packet.IP_SRC );
    r1.MATCH( 'IP_DST', packet.IP_DST );

    // Default (decision == FORWARD): forward to network X
    outport = 2 ;
    if (decision == FIREWALL) {
        // Forward to firewall and network X
        if (switch == S1 )
            outport = 2 ;
        else {
            if (inport == 1)
                outport = 3 ;
            else
                outport = 2 ;
        }
    }
    else if (decision == RECORD) {
        // Forward to monitoring system, firewall, and network X
        if (inport == 1)
            outport = 3 ;
        else
            outport = 2 ;
    }

    r1.ACTION( 'OUTPUT', outport );
    send_rule(r1, switch);
    send_packet(packet, switch);
}
```

c) Die zustandslose Firewall wird später durch eine Firewall ersetzt, die den Verbindungszustand von TCP-Verbindungen überwachen kann. Kann das Netz bei Verwendung der neuen Firewall wie zuvor beschrieben weiterbetrieben werden? Begründen Sie Ihre Antwort.

The stateless firewall is later replaced by a firewall that can monitor the connection state of TCP connections. Can the network continue to operate as previously described when using the new firewall? Justify your answer.

Die Überwachung des Verbindungszustands erfordert die Weiterleitung *aller* TCP-Segmente einer Verbindung zur Firewall.
Von Netz X zum Internet ist keine Weiterleitung über die Firewall vorgesehen, weshalb die neue Firewall nicht eingesetzt werden kann.

Aufgabe 6 HTTP and Transport (11 Punkte)

11 Sie sind die Betreiberin eines Webservers S , der eine Datei `index.html` über HTTPS bereitstellt. Der Webserver verwendet einen traditionellen HTTPS Protokollstack. Die Datei ist 20 MSS groß. Gehen Sie davon aus, dass alle übrigen erforderlichen Daten jeweils in eine MSS passen.

Gehen Sie, wenn nicht explizit anders angegeben, davon aus, dass es keine vorangegangene Verbindung gab. Die IP-Adresse des Webservers ist bereits bekannt.

You are the operator of a web server S , that hosts a file `index.html` over HTTPS. The web server uses a traditional HTTPS protocol stack. The file has a size of 20 MSS. Assume that all remaining data that is required fits into one MSS each.

Assume that there was no previous connection unless explicitly stated otherwise. Furthermore assume, that the IP address of the server has already been retrieved over DNS.

3 a) Client C sendet eine HTTPS-Anfrage für `index.html` an Webserver S . Geben Sie die chronologische Abfolge der von C gesendeten bzw. empfangenen IP-Pakete an, bis die HTTPS-Anfrage bei S vorliegt. Befüllen Sie die erste Spalte der Tabelle mit der Quelle des IP-Pakets (C oder S) und die zweite Spalte mit den Protokollen, die im Nutzdatenfeld des IP-Pakets übertragen werden. Geben Sie, falls nötig, jeweils die verwendete Protokollversion an.

Nach wie vielen RTTs liegt die HTTPS-Anfrage frühestens beim Server vor?

Client C sends a HTTPS request for `index.html` to server S . Write down a chronological sequence of IP packets sent or received by client C until the HTTPS request is available at S . Fill the first column of the table with source of the IP packet (C or S) and the second column with all protocols contained in the IP payload. If necessary also state the used protocol version.

After how many RTTs is the request available at the server at the earliest.

	Quelle (<i>source</i>)	Protokolle im Payload (<i>protocols in payload</i>)
1	C	TCP
2	S	TCP
3	C	TCP
4	C	TCP, TLS1.3
5	S	TCP, TLS1.3
6	C	TCP, TLS1.3
7	C	TCP, TLS1.3, HTTP

Anzahl RTTs: 2.5

b) Mit welcher TCP-Erweiterung kann die Anzahl der erforderlichen RTTs für nachfolgende Anfragen reduziert werden? Wie funktioniert diese?

2,5

Which TCP extension can reduce the number of required RTTs for subsequent connections? How does this extension work?

TCP-Fast-Open:
 In the first connection, the server sends a TFO cookie + data.
 In subsequent connections, the client sends the cookie and application data with the first SYN packet. Server validates the TFO cookie and, if correct, delivers the application data immediately.

c) Die HTTPS-Verbindung ist nun aufgebaut. Wie viele RTTs werden für die Übertragung von index.html (20 MSS) benötigt? Die initiale Staukontrollfenstergröße (IW) beträgt: $IW = 2 \text{ MSS}$ beziehungsweise $IW = 8 \text{ MSS}$.

2,5

Tragen Sie in die beiden Tabellen für jede RTT die Größe des aktuellen Staukontrollfensters des Servers und die bis zum Beginn der RTT insgesamt übertragenen Daten gemessen in MSS ein. Geben Sie die Größe des Staukontrollfensters auch für die RTT nach Abschluss der Übertragung an.

Server S beginnt die Übertragung der Datei in RTT 1 mit $CW_{nd} = IW$. Es treten keine Paketverluste auf und es existiert kein Bottleneck. Die Verbindung nutzt TCP Reno.

Wie viel kürzer (in Prozent) ist die Dauer der Übertragung ohne Verbindungsaufbau mit $IW = 8$?

The HTTPS connection is now established. How many RTTs are needed to transmit index.html (20 MSS)? The initial congestion window size (IW) is: $IW = 2 \text{ MSS}$ respectively $IW = 8 \text{ MSS}$.

Fill the two tables below for each RTT with the congestion window size of the server and the total amount of transmitted data (in MSS) at the beginning of the RTT. Also fill in the size of the congestion window for the RTT after the file transfer is completed.

Server S starts transmitting the file in RTT 1 with $CW_{nd} = IW$. There are no packet losses and no bottleneck. The connection uses TCP Reno.

How much shorter (in percent) is the duration of the transmission without connection establishment with $IW = 8$?

IW = 2	RTT	1	2	3	4	5	6	7
	CW _{nd} (Server)	2	4	8	16	22		
	übertragene MSS (transmitted MSS)	0	2	6	14	20		

IW = 8	RTT	1	2	3	4	5	6	7
	CW _{nd} (Server)	8	16	28				
	übertragene MSS (transmitted MSS)	0	8	20				

$1 - \frac{2}{4} = 50\%$

3

d) Der Webserver unterstützt nun HTTP/3. Beschreiben Sie, warum dies die Anzahl erforderlicher RTTs im Vergleich zu Teilaufgabe a) reduziert.

Geben Sie analog zu Teilaufgabe a) den Ablauf einer HTTP/3-Anfrage (C an S) als Abfolge von IP-Paketen an. Verwenden Sie dabei so wenige Pakete wie möglich. Nach wie vielen RTTs kann ein Client eine HTTP/3-Anfrage bei einer nachfolgenden Verbindung frühestens verschicken?

You switch to using HTTP/3. Describe how this reduces the number of RTTs required in comparison to sub-problem a). Similar to sub-problem a), give a chronological sequence of IP packets of an HTTP/3 request (C to S). Use as few packets as possible.

After how many RTTs can a client send an HTTP/3 request in a subsequent connection at the earliest?

Erklärung der RTT-Reduktion:

HTTP/3 verwendet QUIC

QUIC ermöglicht einen einzigen kombinierten Handshake (Transport + Verschlüsselung)

	IP	Protokolle im Nutzdatenfeld von IP (<i>protocols in payload</i>)
1	C → S	UDP, QUIC
2	S → C	UDP, QUIC
3	C → S	UDP, QUIC, HTTP

Anzahl RTTs bei nachfolgender Verbindung: 0-RTT / Mit dem ersten Paket