

Informatik – Biber

*Lehrmittel für die informatische
Bildung an der Sekundarstufe I*

Kommentar für Lehrpersonen



Inhaltsverzeichnis

Routing – meine Daten auf der Reise durchs Internet	3
Umsetzungsvorschläge (bis 4 Lektionen)	4
Hintergrundwissen zum Routing	5
<i>Wo kommt Routing vor?</i>	5
<i>Wie werden Informationen weitergeleitet?</i>	5
Hintergrundwissen zu «Datenpakete weiterleiten»	7
<i>Wie finden die Informationen das richtige Ziel?</i>	7
<i>Was lässt sich aus der IP-Adresse 192.168.10.20/24 ablesen?</i>	8
<i>Wie viele Hostadressen gibt es in einem Netzwerk?</i>	10
<i>Weshalb braucht es kleinere Netzwerke (Subnetze)?</i>	11
<i>Wo beginnt ein Subnetz, und wo hört es auf?</i>	11
<i>Wie findet das Datenpaket den schnellsten Weg?</i>	13
Hintergrundwissen zu «Datenpakete zusammensetzen»	16
<i>Wer verpackt die Daten? Wer packt sie wieder aus?</i>	16
<i>Wie werden Transport und Vermittlung des Datenpakets sichergestellt?</i>	16
Hintergrundwissen zu «Datenpakete priorisieren»	18
Umsetzungshilfen	19
Reflexion Lernfilm / Perspektiven der Lernenden	19
Arbeitsblatt 1: „Datenpakete weiterleiten“	19
Arbeitsblatt 2: „Datenpakete zusammensetzen“	20
Arbeitsblatt 3: „Datenpakete priorisieren“	20
Informatik-Biberaufgaben zum Thema Routing	21
Mögliche Vertiefungen	22
Lösungen	23
Arbeitsblatt 1: „Datenpakete weiterleiten“	23
Arbeitsblatt 2: „Datenpakete zusammensetzen“	27
Arbeitsblatt 3: „Datenpakete priorisieren“	29

Routing – meine Daten auf der Reise durchs Internet

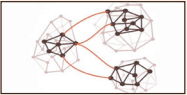


Eingangskompetenz

- Schülerinnen und Schüler haben eine Vorstellung vom binären Zahlenraum (1 und 0).
- Schülerinnen und Schüler haben bereits Erfahrung gesammelt mit dem Internet (Webrecherchen, Webseiten besucht, E-Mails verschickt o.a.).
- Schülerinnen und Schüler können den kürzesten (optimalsten) Weg berechnen oder haben eine Vorstellung davon, was es heisst, aus mehreren Wegen den kürzesten auszuwählen.

Ausgangskompetenzen

- Schülerinnen und Schüler kennen den Begriff des „Routings“ und können erklären, wie Datenpakete weitergeleitet werden.
- Schülerinnen und Schüler können eine IP-Adresse von der Dezimalschreibweise in die Binärform umwandeln und umgekehrt.
- Schülerinnen und Schüler können mit der Subnetzmaske oder der CIDR-Schreibweise ein Teilnetz identifizieren.
- Schülerinnen und Schüler können TCP-Segmente erkennen und die Pakete ihren Empfängern zuordnen.
- Schülerinnen und Schüler kennen Unterschiede von verschiedenen Webanwendungen, die den Fluss der TCP-IP-Pakete durch das Internet messen.

Umsetzungsvorschläge (bis 4 Lektionen)

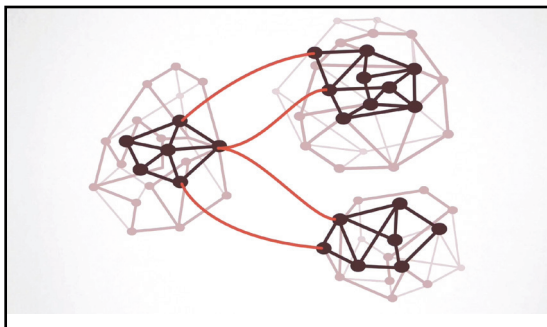
Lernenden-Perspektiven	<p>Anschauen des Lernfilms Routing – Meine Daten auf der Reise durchs Internet Thema: Netzwerke – Internet Metapher Autoverkehr besprechen</p>	
Vorwissen	<p>Schülerinnen und Schüler wissen bereits, dass Computer im Binärsystem rechnen (siehe auch Biber-Modul „Musik“). Schülerinnen und Schüler haben bereits Erfahrung mit dem Internet gesammelt und eine Vorstellung davon, was es ist. Schülerinnen und Schüler können sich vorstellen, wie man den optimalen Weg berechnet (siehe auch Biber-Modul „Verkehr“).</p>	
Arbeitsblatt 1	<p>Wie kommen meine Daten am schnellsten durchs Netz? Bezug Lernfilm: Verbund von Netzwerken (02:44)</p>	
Arbeitsblatt 2	<p>Wer kümmert sich darum, dass alle Daten ankommen? Bezug Lernfilm: Protokoll (03:17)</p>	
Arbeitsblatt 3	<p>Werden alle Daten gleich behandelt? Bezug Lernfilm: Ausstiegsfragen (04:51)</p>	
Biberaufgaben	<p>Verschiedene Aufgaben zum Thema Routing und Netzwerke selbstständig lösen.</p>	
Mögliche Vertiefung	<p>Interaktive Materialien zum Routing Interaktive Grafik: So laufen Datenströme aus der Schweiz, Deutschland und Frankreich in Richtung USA, http://homment.com/internet-routing</p>	

Hintergrundwissen zum Routing

Haben Sie sich schon einmal überlegt, wieso man von zu Hause über das Internet eine Webseite öffnen kann? Wie geht das? Wieso weiss die Videoplattform Youtube, welches Video ich aufgerufen habe? Und wie kann es bei all diesen Millionen von Daten, die durchs Internet geschickt werden, funktionieren, dass ich keine falschen Informationen dargestellt bekomme und die Informationen an die richtige Adresse gelangen?

In diesem Modul möchten wir den Fragen nachgehen, wie die Daten ihr Ziel erreichen und wie Nachrichtenpakete weitergeleitet werden. Hier kommt das „Routing“ ins Spiel.

Wo kommt Routing vor?



Routing meint die Weiterleitung von Dingen entlang von Wegen und über Kreuzungen. Im Bild sind die Kreuzungen als Punkte und die Wege als Strecken ersichtlich. Dabei muss meistens bei einem Knoten entschieden werden, wie der Weg der Nachricht weitergeht. Zum Beispiel kommt Routing bei Paketsystemen im Internet vor, wo Informationen verschickt werden. Oder auch – wie der Film zeigt – beim Autoverkehr: Hier leiten Verkehrspolizisten oder Ampeln den Verkehr bei Kreuzungen.

Wie werden Informationen weitergeleitet?

Die Kommunikation über das Internet basiert auf einem dezentral organisierten Internet, das man sich als Netz von Netzen vorstellen kann. Jedes Netz ist ebenfalls dezentral organisiert und wird in der Internetsprache als „AS Autonomic System“ bezeichnet. Fällt ein Netz aus, kann ein anderes einspringen, da die Netze untereinander verknüpft sind. Als Beispiel im Verkehr: Autos werden bei einem Unfall auf eine andere Strasse umgeleitet, welche ebenfalls zum Ziel führt.



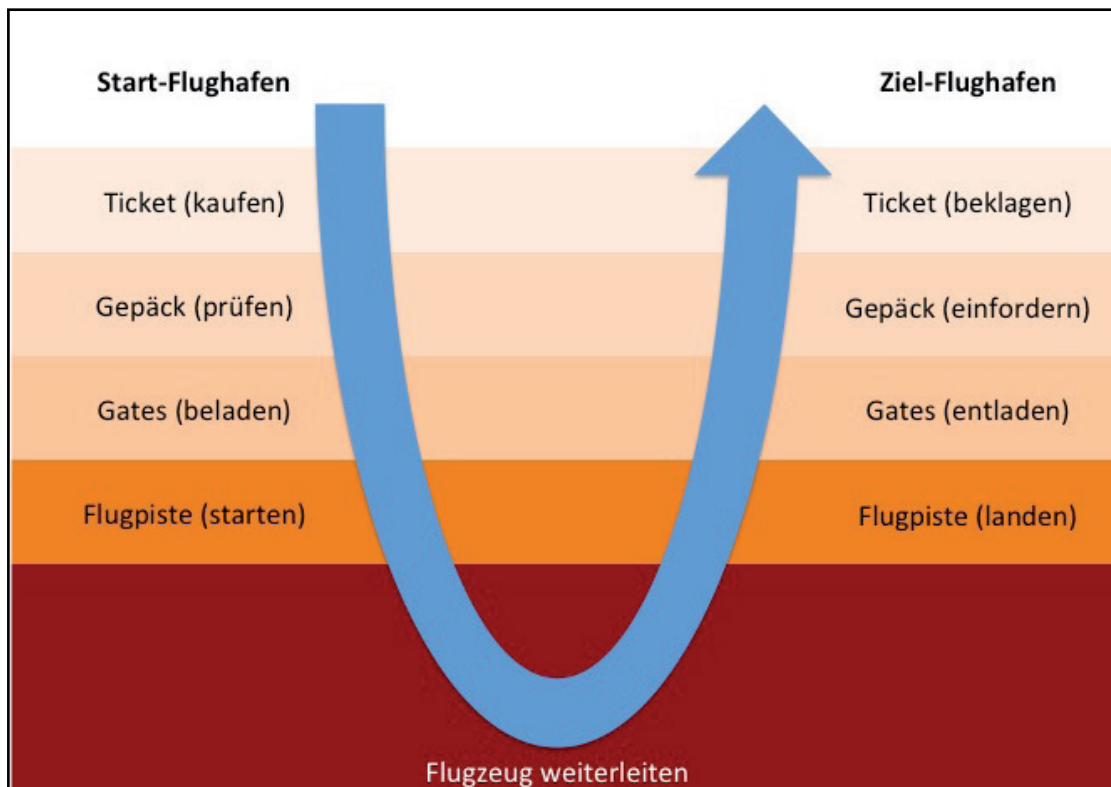
Damit ein so komplexes dezentrales System wie das Internet funktioniert, braucht es eine robuste Bauweise. Im Straßenverkehr sind ja auch gut gebaute Strassen notwendig, damit der Verkehr flüssig läuft. Ein wesentlicher Punkt dabei ist das Internetschichten-Modell, welches verschiedene Aufgaben verschiedenen Schichten zuordnet:

Die oberste Schicht, die Applikationsschicht, wird von den uns bekannten Programmen (z.B. Browser, E-Mail) genutzt, um Informationen über das Internet zu schicken und zu empfangen. Die Programme halten sich an Regeln, welche in einem Protokoll festgehalten sind (wie die Regeln, an welche sich die englische Königsfamilie halten sollte, welche auch in Protokollen zu den verschiedenen Anlässen festgehalten ist). Die Regeln,

an welche sich die Programme halten, bestimmen, welche Informationen und Angaben in welcher Form auf die Pakete geschrieben werden müssen, damit diese an den richtigen Ort gelan-

gen. Die Detailaufgabe des Verschickens, Transportierens und Empfangens wird von den unteren Schichten übernommen.

Wird Information von einem Ort bzw. von einem Programm zu einem anderen geschickt, wird diese in jeder Schicht nach einem fest vorgeschriebenem Protokoll verpackt und weitergeleitet. Damit man sich diesen Ablauf besser vorstellen kann, hilft eine Metapher zum Reisen in einem Flugzeug: Die folgende Figur schematisiert das schichtweise Durchlaufen eines Passagiers bei einem Flug von A nach B.



Der Ablauf am Flughafen ist stark strukturiert. Es muss jede Schicht durchlaufen werden, bis der Passagier am Schluss in seinem Reiseland ankommt und aus dem Flughafen gehen kann.

1. Ich kaufe ein Ticket.
2. Dann wird das Gepäck aufgegeben und geprüft.
3. Das Flugzeug wird mit Passagieren und Gepäck beladen.
4. Die Pilotinnen und Piloten folgen der Abheberoutine und fliegen ab an den Zielflughafen.

Am Ziel-Flughafen wird jede Schicht in umgekehrter Reihenfolge wieder durchlaufen, d.h. in jeder Schicht wird kontrolliert, ob alles richtig protokolliert wurde:

4. Das Flugzeug ist abgehoben, d.h. jetzt muss es landen.
3. Am Gate wurde es beladen, d.h. jetzt muss es entladen werden.
2. Ich habe mein Gepäck aufgegeben, d.h. jetzt hole ich mein Gepäck wieder ab.
1. Und (falls nötig) kann man sich z.B. über eine Verspätung beschweren.

Jede Schicht hat ihre eigenen Dienste und einen bestimmten Ablauf. Diese Abläufe halten fest, zu welchem Zeitpunkt oder in welcher Reihenfolge welcher Vorgang durch wen oder durch was veranlasst wurde. Es wird somit genauestens protokolliert, wo sich der Passagier befindet, und er wird zur nächsten Schicht weitergeleitet. Beim Entladen des Flugzeugs werden die Protokolle kontrolliert.

Wie beim Modell eines Flugs durchlaufen auch die Informationen im Schichtenmodell des Internets jede Schicht einzeln. Dabei hat jede Schicht ihre eigene Aufgabe und ihr eigenes Protokoll, das festhält, wann die Information die Schicht passiert hat oder von wem der Vorgang veranlasst wurde. Beim Empfang der Informationen wird mithilfe des Protokolls überprüft, ob alle Informationen korrekt angekommen sind.

Zusammenfassend:

- **Das TCP/IP-Schichtenmodell des Internets besteht aus fünf Schichten.**
- **Die Schichten helfen dabei, das Paketsystem anhand verschiedener Zuständigkeiten zu steuern.**
- **Jede Schicht bietet eigene Dienste an und vermittelt zur nächsten Schicht.**
- **Die Kommunikation zwischen den gleichen Schichten basiert auf Protokollen.**

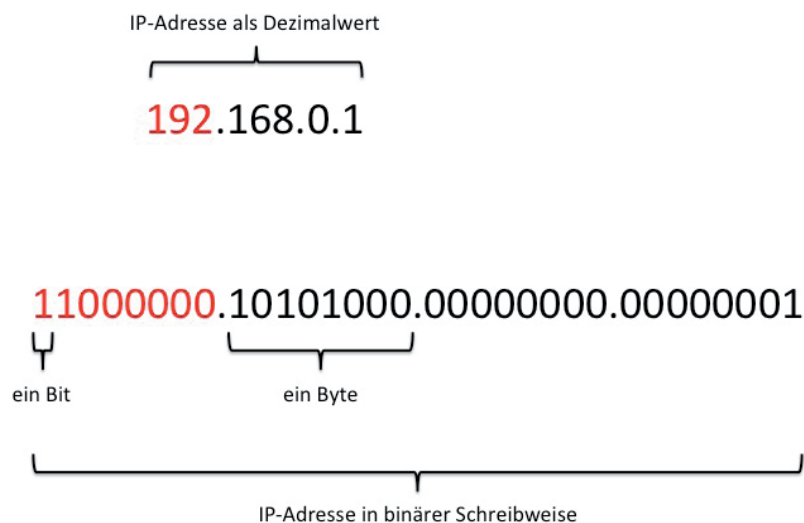
Die Fragen des Moduls beziehen sich auf die Transportschicht und die Netzwerkschicht.

Hintergrundwissen zu «Datenpakete weiterleiten»

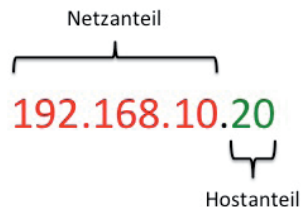
Wie finden die Informationen das richtige Ziel?

Innerhalb der Netzwerkschicht ist ein mit dem Netzwerk verbundener Computer, ein Router oder ein anderes mobiles Gerät durch eine eindeutige Adresse identifiziert: Die IP-Adresse. Eine IPv4-Adresse besteht aus 4 Bytes (4 mal 8 Bits) und der Punktnotation. Sie kann ganze Zahlen von 0 bis 255 darstellen. Eine IPv4-Adresse sieht z.B. so aus: 192.168.0.1

Da ein Computer nur im binären Zahlenraum rechnen kann und nur 0 und 1 versteht, sieht die IP-Adresse für ihn wie folgt aus:



Eine IP-Adresse besteht aus zwei Teilen: Der erste Teil bestimmt den Netzanteil und der zweite Teil den Hostanteil (auch Geräteadresse). Das ist wie bei einer Telefonnummer: Die Ortswahl bestimmt die Netzwerk-Adresse, die Telefonnummer die Host-Adresse.



Das Datenpaket wird über verschiedene IP-Adressen zum richtigen Netzwerk und zum richtigen Host (Gerät) geschickt. D.h. es muss erkannt werden, welche Teile von dieser Adresse das Netzwerk und welche Teile den Host definieren. Dies wird durch die Netzmaske festgelegt. Um diese zu berechnen, benötigen wir das Wissen über die Binärform von IP-Adressen.

Computer rechnen mit 1 und 0 (Binärform¹)

Schauen wir uns die Umrechnung vom ersten Byte der IP-Adresse 192.168.0.1 an: Wir wollen die Dezimalzahl 192 als binäre Zahl darstellen. Binäre Zahlen berechnen sich mit Potenzen der Basis 2. Dabei ist der kleinste Wert 2^0 und wird rechts aussen notiert. Da $128 + 64 = 192$ ergibt, benötigen wir die beiden Potenzen 2^7 und 2^6 . Dies drücken wir mit einer 1 aus. Die restlichen Potenzen benötigen wir nicht, daher erhalten sie eine 0.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	Potenz
128	64	32	16	8	4	2	1	Dezimalwert
128	+64							= 192
1	1	0	0	0	0	0	0	binär

192 entspricht in der binären Darstellung 1100 0000 (zur besseren Lesbarkeit können wir die ersten 4 Bits mit einer Lücke trennen).

Was lässt sich aus der IP-Adresse 192.168.10.20/24 ablesen?

Die Länge der IP-Adresse ist auf 32 Bits beschränkt (32 mal 1 oder 0 in der Binärschreibweise bzw. 4 mal 8 Bits = $8 + 8 + 8 + 8 = 32$). Die Anzahl IP-Adressen ist beschränkt, da jedes Ge-

¹ Eine gute Einführung ins Binärsystem befindet sich im Biber-Modul „Musik“.

² Quelle: http://de.wikipedia.org/wiki/Classless_Inter-Domain_Routing

rät in einem Netzwerk eine eindeutige IP-Adresse aufweisen muss. Da immer mehr Geräte mit einem Netzwerk verbunden sind, gehen diese IP-Adressen allmählich aus. Um die verfügbaren Adressbereiche besser auszunutzen, wurde mit dem CIDR (Classless Inter-Domain-Routing) ein Verfahren eingeführt, damit der 32-Bit-IP-Adressraum für IPv4 effizienter genutzt werden kann. Der Vorteil dieser Notation ist, dass die Netzmaske direkt abgelesen werden kann.

Beispiel 1:

Die Notation 192.168.10.20/24 entspricht der Adresse 192.168.10.20 mit der Netzmaske 255.255.255.0. *Warum?*

Die Netzmaske in binärer Schreibweise zeigt es auf:

11111111.11111111.11111111.00000000

Es sind 3 mal 8 = 24 gesetzte Bits (alle 1) vorhanden. Diese Anzahl gesetzter Bits wird in der CIDR-Notation mit einem Schrägstrich angegeben, daher: 192.168.10.20/24

Beispiel 2:

Die Notation 10.43.8.67/28 entspricht der IP-Adresse 10.43.8.67. Die 28 Bits zeigen die Netzmaske mit 28 mal 1 in binärer Schreibweise, d.h.: 11111111.11111111.11111111.11110000 (3 mal 8 + 4 = 28 gesetzte Bits).

Wie gross ist der Adressbereich dieses Netzwerks?

Da von 32 bereits 28 Bits belegt sind (28 mal 1), bleiben 4 Bits zur freien Verfügung. Damit lassen sich $2^4 = 16$ unterschiedliche Werte darstellen, nämlich von 0 bis 15. Da die Broadcast- und Netzwerkadresse eine eigene Adresse besitzen müssen, bleiben $16 - 2 = 14$ IPv4-Adressen, die an Hosts zu vergeben sind.

Wie lautet die Netzadresse und wie die Broadcastadresse?

Die Netzwerkadresse (die erste Adresse in diesem Netzwerk) lässt sich über die logische UND-Verknüpfung³ berechnen. Da wir 14 IP-Adressen für die Hosts zu vergeben haben und eine zusätzliche die Broadcast-Adresse (die letzte Adresse in diesem Netzwerk) ist, können wir zur Netzwerkadresse 15 addieren und erhalten die Broadcast-Adresse.⁴

IPv4-Adresse		00001010.00101011.00001000 .01000011	10.43.8.67
Netzmaske	/28	11111111.11111111.11111111 .11110000	255.255.255.240
Netzwerkadresse	IPv4 UND Netzmaske	00001010.00101011.00001000 .01000000	10.43.8.64
Broadcast-Adresse	Netzwerkadresse + 15		10.43.8.79

³ Die logische UND-Verknüpfung kommt aus der Booleschen Algebra. Nur wenn zwei 1 vorhanden sind, bleibt es eine 1, ansonsten ist das Resultat eine 0.

⁴ Die Broadcast-Adresse lässt sich auch mit einer ODER-Verknüpfung (wenn ein Bit 1 vorhanden, dann ergibt es 1, sonst 0) zwischen IPv4 und negierter Netzwerkadresse (0 wird eine 1, 1 wird eine 0) berechnen. Die Binärschreibweise muss anschliessend noch in Dezimalschreibweise umgewandelt werden.

Wie ist der Adressbereich dieses Netzwerks aufgeteilt?

Der Adressbereich erstreckt sich von 10.43.8.64 bis 10.43.8.79. Davon können folgende IPv4-Adressen für Endgeräte verwendet werden: 10.43.8.65 bis 10.43.8.78 (ohne Netzwerk- und Broadcast-Adresse).

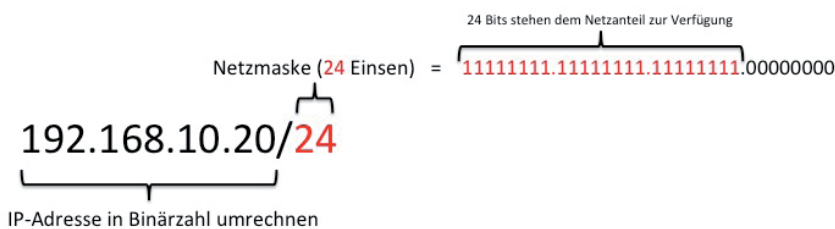
Was teilt mir die Netzmaske mit?

Die Netzmaske hilft dem Computer, die Netzwerkadresse herauszufinden. Das Kennen der Netzwerkadresse ist eine Grundlage dafür, dass das Datenpaket an den richtigen Ort gelangt. Alle Bits einer Netzmaske, die auf 1 stehen, bezeichnen den Netzanteil der Adresse. Der andere Teil ist die Hostadresse.

Je nach Anzahl der Einsen sind diese Teilnetze grösser oder kleiner.

Netzmaske	Binär
255.0.0.0	11111111.00000000.00000000.00000000
255.255.0.0	11111111.11111111.00000000.00000000
255.255.255.0	11111111.11111111.11111111.00000000

Die Netzmaske kann zum Beispiel aus der CIDR-Notation herausgelesen werden. Mit der IP-Adresse und der Netzmaske kann nun (mit einer logischen UND-Verknüpfung) die Netzwerkadresse bestimmt werden:



IP-Adresse: 11000000.10101000.00001010.00010100 } UND-Verknüpfung

Netzmaske: 11111111.11111111.11111111.00000000 }

Netzwerkadresse: 11000000.10101000.00001010.00000000



Wie viele Hostadressen gibt es in einem Netzwerk?

Dies soll mit einem Beispiel verdeutlicht werden: Mit der Netzmaske 255.255.255.0 bzw.

11111111.11111111.11111111.00000000

können nur 8 Bits (alle 0) zur Adressierung eines Geräts (Host) verwendet werden. Aus diesen 8 Bits ergeben sich $2^8 = 256$ mögliche binäre Zahlenkombinationen. Es bleiben somit 254 Hostadressen übrig, die in diesem Subnetz verwendet werden können.

Weshalb braucht es kleinere Netzwerke (Subnetze)?

Die Anzahl IP-Adressen, die zu vergeben sind, sind beschränkt. Ein Privatanwender hat meistens nicht mehr als 32 Geräte, deshalb genügt ihm ein /27 Netzwerk ($2^5 - 2 = 30$ Hosts) oder ein /28 Netzwerk ($2^4 - 2 = 14$ Hosts). Mit Subnetzen wird die Last der Netzwerke verteilt, und Fehler oder Störungen treten nur in diesen kleinen Teilnetzen auf und beeinflussen das gesamte Netzwerk nicht. Das ist das Prinzip der Dezentralisierung. Mit den Subnetzen können mehr Hosts in ein Netzwerk eingebunden werden, weil mehr IP-Adressen zur Verfügung stehen.

Beispiel:

Für ein privates Subnetz haben wir einen Adressbereich von 192.168.0.0/24 bis 192.168.255.255/24 zur Verfügung. Die ersten drei Bytes bilden die Netzwerkadresse (da die Netzmaske 255.255.255.0 ist), zwei davon sind festgelegt (192.168). Das dritte Byte kann den Wert von 0 bis 255 annehmen, d.h. in diesem Subnetz können bereits 256 verschiedene Netzwerke mit je 254 Hosts aufgebaut werden.

Wo beginnt ein Subnetz, und wo hört es auf?

Um ein Netzwerk in Subnetze zu unterteilen, wird der Netzanteil erweitert. Dabei wird ein Teil des Hostanteils sozusagen dem Netzanteil zugewiesen.

Beispiel:

Ein Netzwerk soll in vier Subnetze unterteilt werden.

IP-Adresse: 192.168.168.0

Netzmaske: 255.255.255.0

Zuerst wird bestimmt, um wie viele Bits die Netzmaske erweitert werden muss. Das letzte Byte wird dazu in vier Binärzahl umgerechnet. Um vier Subnetze erstellen zu können, benötigen wir 2 Bits, da mit 2 Bits $2^2 = 4$ Subnetze aufgebaut werden können. Der Netzteil der Adresse muss somit um 2 Bits erweitert werden, d.h. zwei Bits vom bisherigen Hostanteil werden besetzt, und das wird in der Netzmaske mit einer 1 festgelegt.

IP-Adresse: 192.168.168.00000000

Netzmaske: aus 255.255.255.00000000 wird 255.255.255.11000000

Netzanteil Hostanteil

192.168.168.0
255.255.255.0

Netzanteil Hostanteil (8 Bits)

192.168.168.00000000
255.255.255.00000000

4 Subnetze nötig: Da $2^2 = 4$ ist, wird der Netzanteil um 2 Bits erweitert.

Netzanteil Hostanteil (6 Bits)

192.168.168.00000000
255.255.255.11000000

Wir bezeichnen mit 1, dass die zwei Bits neu zum Netzanteil gehören.

Für die vier Subnetze wurden 2 Bits dem Netzanteil zugeschrieben. Mit 2 Bits können wir vier unterschiedliche Varianten an Binärzahlen kombinieren: 00, 01, 10, 11.

Subnetz 1: 192.168.168.00000000 bis 192.168.168.00111111

Subnetz 2: 192.168.168.01000000 bis 192.168.168.01111111

Subnetz 3: 192.168.168.10000000 bis 192.168.168.10111111

Subnetz 4: 192.168.168.11000000 bis 192.168.168.11111111

Der Hostanteil besteht nun noch aus 6 Bits. D.h. dem Subnetz stehen $2^6 = 64$ IP-Adressen zur Verfügung. Dabei fällt eine noch der Netzwerkadresse und eine der Broadcast-Adresse zu. Es können somit 62 Host-IPs pro Subnetz vergeben werden.

Nun können die Subnetzadressen berechnet werden. Das letzte Byte wird wieder in eine Dezimalzahl umgerechnet.

Subnetz 1: 192.168.168.00000000 → 192.168.168.0

Netzmaske: 255.255.255.11000000 → 255.255.255.192

Broadcast-Adresse (höchste Adresse im Subnetz 1): 192.168.168.00111111 → 192.168.168.63

Damit ergibt sich folgende IP-Adressen-Verteilung:

	Subnetzadresse	Host-IP-Range	Broadcast
Subnetz 1	192.168.168.0	192.168.168.1 bis 192.168.168.62	192.168.168.63

Erhöht man die Broadcast-IP um 1, erhält man die Subnetzadresse vom nächsten Subnetz. Da wir 62 IPs für die Hosts haben und 1 IP die Broadcast-Adresse definiert, gilt: $192.168.168.64 + 62 + 1 = 127$. Die neue Broadcast-Adresse ist somit 192.168.168.127.

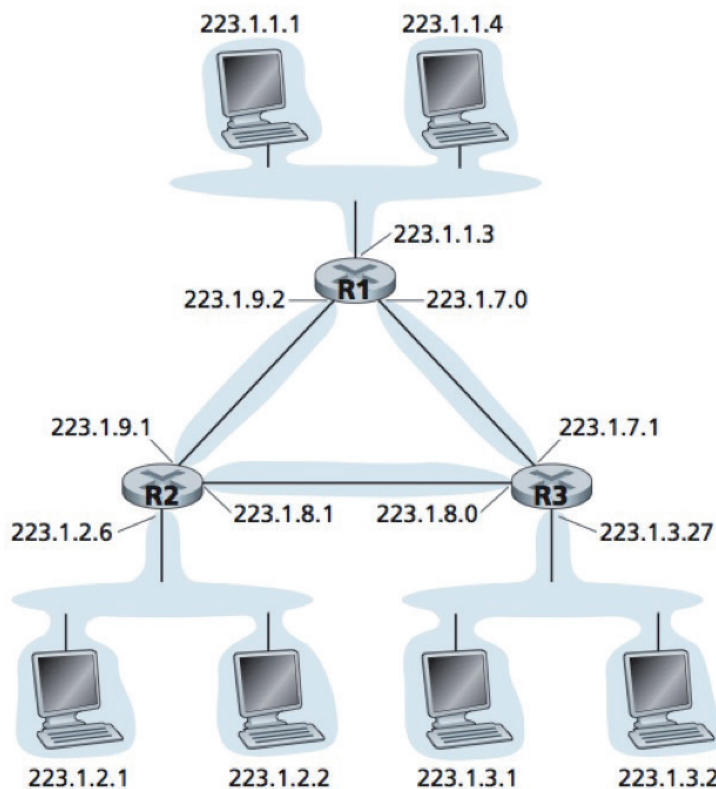
	Subnetzadresse	Host-IP-Range	Broadcast
Subnetz 1	192.168.168.0	192.168.168.1 bis 192.168.168.62	192.168.168.63
Subnetz 2	192.168.168.64	192.168.168.65 bis 192.168.168.126	192.168.168.127

Dies kann nun für die zwei weiteren Subnetze wiederholt werden:

- **Broadcast + 1 = Subnetzadresse des neuen Subnetzes**
- **Subnetzadresse + 62 + 1 = neue Broadcast-Adresse**
- **Host-IP-Range = alle dazwischenliegenden IPs**

Wie findet das Datenpaket den schnellsten Weg?

Ein Router ist ein Netzwerkgerät, welches Datenpakete von einem Netz zu einem nächsten weiterleitet. Router besitzen mehrere Netzwerkkarten und sind somit Teil mehrerer Netzwerke (mindestens 2). Jede Netzwerkkarte des Routers hat eine eigene IP-Adresse. Über diese Anschlüsse kann der Router Kontakt zu seinen umliegenden Netzwerken aufnehmen und seine Routingtabelle vervollständigen. Die Routingtabelle enthält Angaben darüber, welche Wege ein Datenpaket nehmen kann und wie viel es „kostet“. Jeder Knoten tauscht sich nur mit dem nächsten Nachbarn aus. Ein Datenpaket wird somit von Knoten zu Knoten geschickt. Dank der Routingtabelle kann ein optimaler Weg berechnet werden.

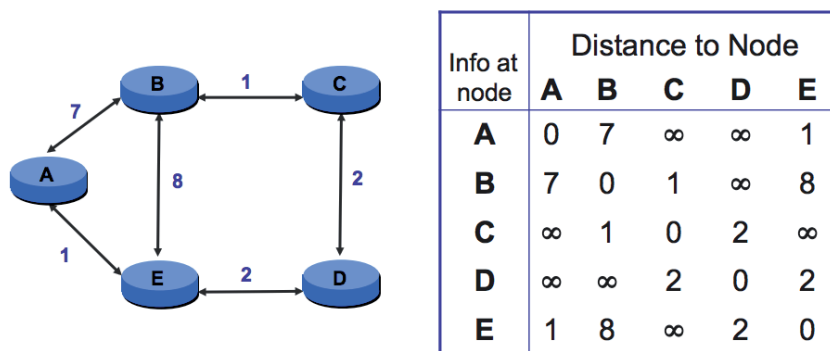


Beispiel: 3 Router verbinden 6 Subnetze (jede Netzwerkkarte des Routers hat eine eigene IP-Adresse)

Der Distanz-Vektor-Routing-Algorithmus ist eine Möglichkeit, dass ein Router an die Routingtabelle⁵ kommt. Dabei befolgt der Algorithmus folgendes Prinzip:

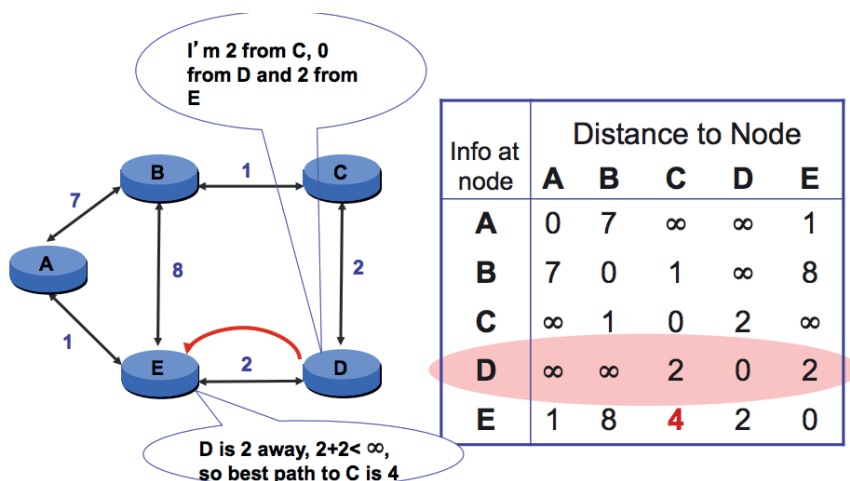
- Erstelle eine Kostenmatrix, die zeigt, welche Router über welche Nachbarn und zu welchen Kosten erreichbar sind. Zuerst sind nur die bekannten Kosten zu den direkten Nachbarn vorhanden: 0 für sich, die direkten Verbindungen werden eingetragen, alles andere wird auf unendlich gesetzt.
- Schicke diese Tabelle regelmässig an die Nachbarn.
- Warte auf die Tabellen der Nachbarn und vervollständige die eigene Tabelle.
- Vergleiche bei Erhalt einer Tabelle die Werte und behalte die besten (minimale Kosten).

An folgendem Beispiel soll dieser Algorithmus erklärt werden:



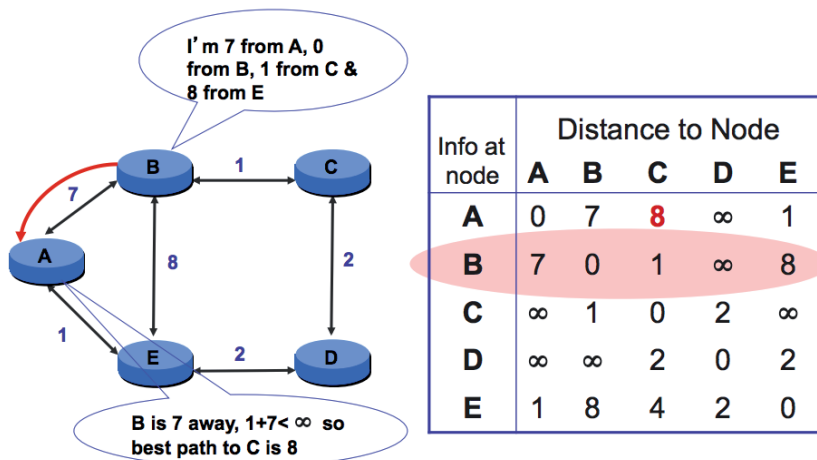
Die Knoten schicken ihre Tabelle zu den Nachbarn.

Z.B. meldet der Knoten D: „Meine Distanz zu E und C beträgt 2, zu D 0.“



Knoten B informiert A: „Meine Distanz ist 7 zu A, 0 zu B und 1 zu C.“

⁵ Mehr Informationen, <https://www.youtube.com/watch?v=ylzAefKENXY>



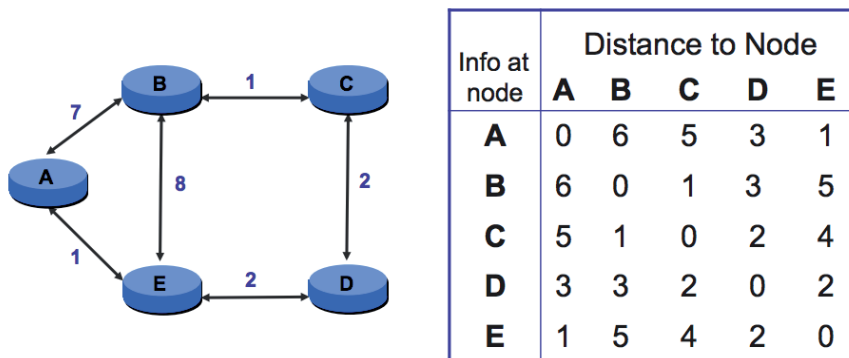
Und so weiter, bis alle Distanzen in diesem Netzwerk bekannt sind.

A kann nun den besten Weg errechnen. Um von A nach C zu gelangen, hat er zwei Wege: Über B oder über E.

Wenn er das Datenpaket über B schickt, kostet es $7 + 1 = 8$.

Wenn er das Datenpaket über E schickt, kostet es $1 + \infty$ (unendlich) = 1 mehr als unendlich.

Da $8 < \infty$ ist, wählt A den Weg über C.



So wird die gesamte Tabelle vervollständigt.

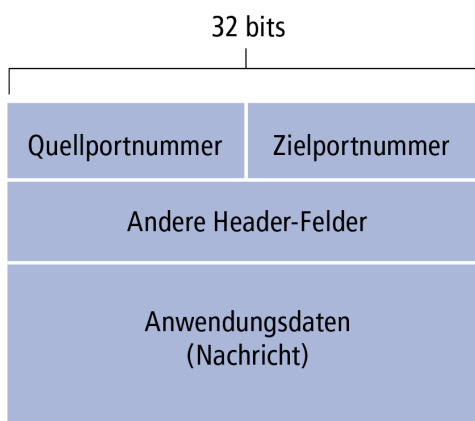
Der verwendete DV-Routing-Algorithmus ist iterativ, asynchron und verteilt:

- Iterativ im Sinn, dass mit jeder Meldung die eigene Tabelle besser wird, bis alle Distanzen im Netzwerk bekannt sind.
- Asynchron: Jeder Knoten meldet periodisch, jedoch selbstständig seine aktuelle Tabelle seinen Nachbarn.
- Verteilt: Jeder Knoten muss sich aus den empfangenen Informationen eine eigene Routing-Tabelle erstellen.

Hintergrundwissen zu «Datenpakete zusammensetzen»

Wer verpackt die Daten? Wer packt sie wieder aus?

Das Transmission Control Protocol (TCP) ist ein zuverlässiges, verbindungsorientiertes, paketvermittelndes Transportprotokoll in Computernetzwerken und gibt die entsprechenden Regeln vor, damit ein sicherer Transport von Daten gewährleistet wird. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets. Entwickelt wurde TCP von Robert E. Kahn und Vinton G. Cerf. Ihre Forschungsarbeit, die sie im Jahre 1973 begannen, hat mehrere Jahre gedauert. Auf der Seite des Senders werden die Daten durch die Transportschicht in Pakete, sog. Segmente, zerteilt und entsprechend im Header angeschrieben, damit diese auf der Empfängerseite wieder richtig zugeordnet werden können. Dieses Eintragen der Headerinformationen („Beipackzettel“) und das Weiterreichen an die Netzwerkschicht wird „Multiplexing“ genannt.



Aufbau eines Segments

Quellport: 143	Zielport: 5039
Sequenznummer: 0	
ACK-Nummer: 104	
Inhalt / ASCII-Daten	
01001000 01100001 01101100 01101100	
01101111 00100000 01000011 01101000	

Beispiel eines Segments

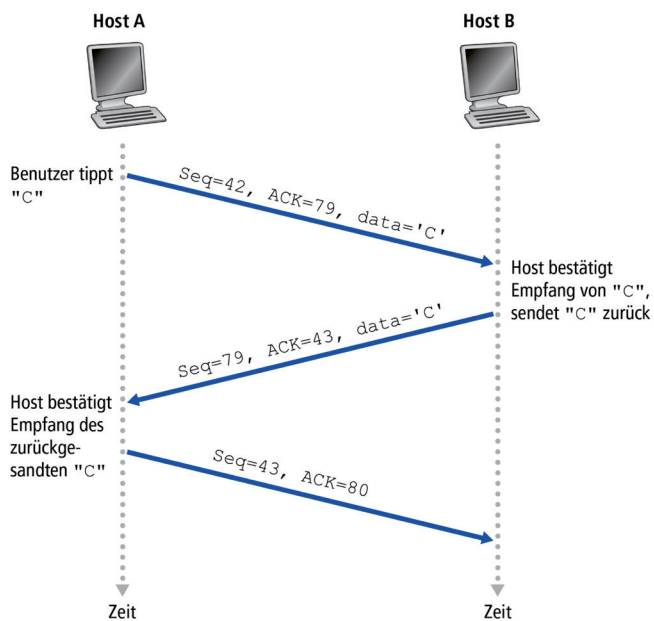
Die Quellportnummer gibt die Portnummer des Senders an. Die Zielportnummer definiert die Anwendung auf der Empfängerseite, an die das Segment geschickt wird. Die Sequenznummer dient der Sortierung der TCP-Segmente, da diese in unterschiedlicher Reihenfolge beim Empfänger ankommen können. Die Acknowledgement-Nummer gibt die Sequenznummer des nächsten TCP-Segments an.

Die Informationen des Headers werden von den Zwischenstationen im Netz (Router) nicht beachtet. Erst auf der Empfängerseite erhält die Transportschicht die eintreffenden Pakete und baut die Segmente in der richtigen Reihenfolge und vollständig für die empfangende Anwendung zusammen („Demultiplexing“).

Wie werden Transport und Vermittlung des Datenpakets sichergestellt?

TCP ist ein verbindungsorientierter Dienst. TCP heisst verbindungsorientiert, weil zwei Anwendungen zunächst ein „Handshake“ durchführen müssen, bevor ein Anwendungsprozess beginnen kann, Daten zu senden. Jedes empfangene Segment wird durch ein „Acknowledge ACK“ bestätigt.

Beispiel: Der Sender schickt ein TCP-Segment mit der Sequenznummer Seq = 42. Der Empfänger bestätigt mit einem ACK = 43 den Erhalt dieses Segments und fordert damit das nächste Segment an. Das nächste Segment des Senders enthält nun dieselbe Nummer wie das letzte ACK, hier also Seq = 43. Zudem bestätigt der Sender den Erhalt des ACK 43 mit einem erneuten ACK = 80 und fordert damit ebenfalls die nächste Sequenz ein. Fehlt bei der nächsten Übertragung die fortlaufende Nummer, so ging ein Paket verloren.



Hintergrundwissen zu «Datenpakete priorisieren»

Internet-Provider (z.B. Swisscom, Cablecom, Sunrise) haben alle Arten von Datenverkehr gleich zu behandeln – Videotelefonate, Livestreams von Bundestagsdebatten, Downloads bezahlter Filme bei iTunes, Youtube-Clips Skateboard fahrender Hunde, Nachrichtenseiten wie SPIEGEL ONLINE, E-Mails, den Datenfluss von Online-Rollenspielen und Bittorrent-Verbindungen.

In letzter Zeit bemühen sich Mobilfunkunternehmen, diese Praxis zu ändern. Datenpakete von Konkurrenz-Diensten, wie z.B. Skype, werden schon heute gefiltert, sodass Skype nicht zur Konkurrenz werden kann. Wer die abgerufenen Webseiten nicht auf dem winzigen Telefonbildschirm, sondern an einem angeschlossenen Notebook sehen will, muss auch dafür extra bezahlen.

Diese Diskussion wird unter dem Begriff „Netzneutralität“ geführt. Hier einige Verweise mit mehr Informationen dazu:

- Was ist Netzneutralität, <https://www.youtube.com/watch?v=MjUSZLi6Kho>
- Das Internet ist unabhängig, <https://www.youtube.com/watch?v=i5oe63pOhLI>

Umsetzungshilfen

Reflexion Lernfilm / Perspektiven der Lernenden

Im Plenum wird der Lernfilm „Routing – Meine Daten auf der Reise durchs Internet“ angeschaut.

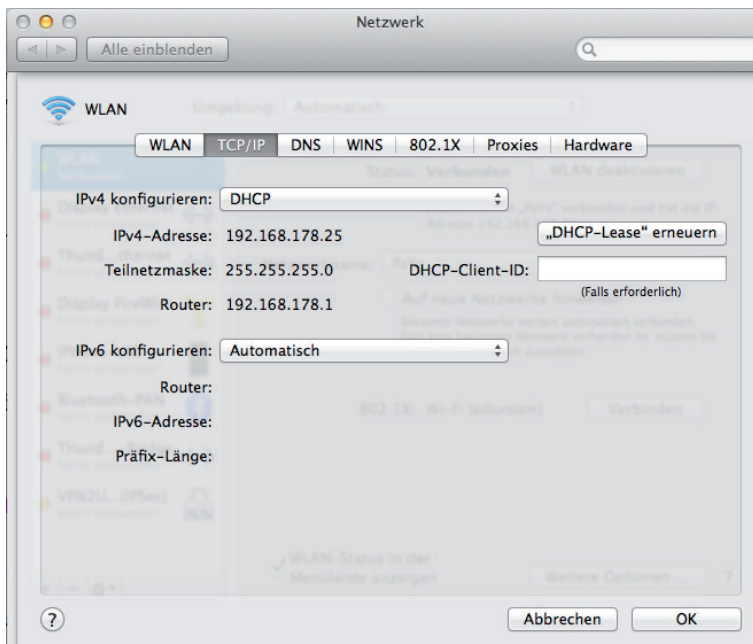
Zur Reflexion des Lernfilms können folgende Fragen in der Klasse aufgenommen werden:

- Nach welchen Regeln werden Datenpakete weitergeleitet?
- Wie werden die eintreffenden Pakete richtig zusammengesetzt?
- Wie schnell ist unser Internet? Wie lange braucht ein Paket von Europa nach Neuseeland?

Diese und ähnliche Fragen werden in den Arbeitsblättern thematisiert.

Arbeitsblatt 1: „Datenpakete weiterleiten“

Damit die Schülerinnen und Schüler das Thema IP-Adresse und Netzmaske angehen können, müssen sie zuerst wissen, wie sie Dezimalzahlen in die Binärform umwandeln können (siehe Hintergrundwissen oder Biber-Modul „Verkehr“).



Ausgang zu diesem Thema können die Netzwerk-Einstellungen des Computers sein. Hier kommen die im Hintergrundwissen und in dem Arbeitsblatt erwähnten Begriffe vor, und es kann gemeinsam erarbeitet werden, worum es sich handelt, bzw. was die einzelnen Begriffe im Zusammenhang mit „Datenpakete weiterleiten“ bedeuten.

Im Arbeitsblatt 1 befassen sich die Schülerinnen und Schüler mit der Struktur der IP-Adressen. Sie lernen, eine IP-Adresse in ihre Binärform umzuwandeln. Sie lernen, dass man mit der Subnetzmas-

ke oder CIDR-Notation herausfinden kann, welche Bits der IP-Adresse das Teilnetz identifizieren können und welche Bits dem Rechner eine eindeutige Nummer im Teilnetz zuordnen.

Anhand eines konkreten Routing-Beispiels lernen die Schülerinnen und Schüler in der Aufgabe 4 wie eine asynchrone und parallele Weiterleitung der Pakete durchgeführt werden kann.

Für einen einfacheren Einstieg oder als Alternative zu Arbeitsblatt 1 kann auch folgende Aufgabe (z.B. in Gruppen) bearbeitet werden:

- Wie sieht ein Verkehrssystem aus, wenn Datenpakete weitergeleitet werden? Versucht, mithilfe des Lernfilms und dem Beispiel „Verkehr“ aufzuzeichnen, wie das Internet Datenpakete weiterleitet. Könnt ihr verschiedene Begriffe des „Routings“ eurer Zeichnung zuordnen? Z.B. Netzwerk, Datenpaket, TCP-Protokoll, IPv4-Adresse, Router, ...
- Vergleicht nun eure Zeichnungen: Was stellt ihr euch gleich vor? Was muss in einem Netzwerk mindestens vorhanden sein, damit es ein Netzwerk ist?

Arbeitsblatt 2: „Datenpakete zusammensetzen“

Nachrichtenpakete enthalten mehr Informationen als nur den reinen Inhalt, z.B. die Angaben über den Sender und Informationen, welche die einzelnen Schichten zur Weiterverarbeitung benötigen. Diese Informationen werden für die Weiterleitung voneinander getrennt. Die Datenpakete müssen dann beim Empfänger der Nachricht wieder zusammengesetzt werden.

Beim Arbeitsblatt 2 beginnen die Schülerinnen und Schüler mit 16 TCP-Segmenten. Anhand der Angaben im Kopf (blauer Hintergrund) können die Schülerinnen und Schüler die Pakete ihren Empfängern zuordnen. Mithilfe der Sequenznummer kann die ursprüngliche Reihenfolge der Pakete rekonstruiert werden.

Der Inhalt der Pakete ist eine Bytefolge, welche in diesem Beispiel als ASCII kodiert ist. Mithilfe der ASCII-Tabelle können die Schülerinnen den Inhalt Bytes (1 Byte = 8 Bits) jeweils einem ASCII-Charakter zuordnen. So entspricht **00100000** zum Beispiel einer Lücke (Leertaste).

Arbeitsblatt 3: „Datenpakete priorisieren“

Im Verkehr haben Sanitäts- und Polizeiautos Vortritt vor anderen Verkehrsteilnehmenden. Wie ist das im Internet? Werden hier ebenfalls Datenpakete priorisiert?

Beim Arbeitsblatt 3 lernen die Schülerinnen und Schüler verschiedene Webanwendungen kennen, welche als Messinstrumente den Fluss der TCP-IP-Pakete durch das Internet messen können. Mit den Aufgaben versuchen die Schülerinnen und Schüler herauszufinden, welche IP-Nummer ein Webserver oder Webdienst hat.

In weiteren Aufgaben sollen die Schülerinnen und Schüler den weiten Weg eines IP-Pakets nach Neuseeland verfolgen und dabei feststellen, dass es nicht mehr als eine halbe Sekunde braucht, auch wenn es über mehr als 20 Stationen geleitet wurde.

Informatik-Biberaufgaben zum Thema Routing

Die Biberaufgaben stellen konkrete Fragen zu Themen im Umfeld des Routings. Sie wurden den drei Schwierigkeitsstufen einfach, mittel, schwierig zugeordnet und liegen in den entsprechenden Verzeichnissen vor.

Weitere Informationen zum Informatik-Biber Wettbewerb finden Sie auf der Webseite <http://www.informatik-biber.ch/>

Mögliche Vertiefungen

Im Arbeitsblatt 1 wird über das Weiterleiten von Datenpaketen gesprochen. Folgende Verweise geben einen visuellen Einblick in die Routing-Mechanismen. Die interaktive CIDR-Übung kann Schülerinnen und Schülern helfen, Rechenwege einzuüben.

- Routing-Animation, http://members.gaponline.de/afj/rechnernetze/whiteboard/rn_course_16.2.1.html
- Interaktive CIDR-Übung, <http://www.eex-online.de/informatik/cidr.html>
- Distance-Vector-Routing-Animation, https://www-rnks.informatik.tu-cottbus.de/content/unrestricted/animations/Distance_Vector_Routing.swf

Zum besseren Verständnis, in welchen Schichten Pakete zusammengesetzt werden und welche Funktion dabei das TCP-Protokoll hat, werden folgende Erklärungsvideos für Lehrpersonen empfohlen:

- Video zur Funktionsweise von TCP/IP, <https://www.youtube.com/watch?v=LDmcWVxX5TA>
- Video zu TCP/IP, <https://www.youtube.com/watch?v=APm7goBdBrE>
- Video zum Schichtenmodell, <https://www.youtube.com/watch?v=oLQUqWicU5Y>

Die folgenden Verweise führen zu englischsprachigen Erklärungen zum Thema „Datenpakete weiterleiten“ und „Pakete zusammensetzen“.

- Erklärungsvideo CIDR (<http://www.youtube.com/watch?v=Q1U9wVXRuHA>)
- Erklärungsvideo Subnetting (<http://www.youtube.com/watch?v=GtoRQX3QCO8>)
- Video Transport Protocols UDP and TCP (<https://www.youtube.com/watch?v=Vdc8TCESlg8>)

Weiterführende Literatur

Kurose, James F., and Keith W. Ross. Computernetzwerke: der Top-Down-Ansatz. Pearson Deutschland GmbH, 2008.

Tanenbaum A. S. (2010). Computer Networks. Prentice Hall, ISBN-13: 978-0132126953

Naughton, J. (1999). A brief history of the future. Weidenfeld & Nicolson.

Unterrichtsmaterial für den Informatikunterricht

- <http://www.swisseduc.ch/informatik/>
- <http://www.educ.ethz.ch/unt/um/inf>

Lösungen

Arbeitsblatt 1: „Datenpakete weiterleiten“

1a) 10.11.20.0 → 00001010 00001011 00010100 00000000
(<http://www.csgnetwork.com/ipaddconv.html>)

1b) 10.11.20.0/25

Subnetzmaske binär (25 mal 1) 11111111 11111111 11111111 10000000
→ 255.255.255.128

2a/b) Vier gültige Subnetzmasken <i>binär</i>	/	<i>Dezimalschreibweise</i>
11111111 11111111 11111111 00000000		255.255.255.0
11111111 11111111 11111111 11111000		255.255.255.248
11111111 11111111 11111111 11000000		255.255.255.112
11111111 11111111 11111100 00000000		255.255.192.0

3) Der Adressblock 101.101.128.0/17 beinhaltet alle IP-Nummern von 101.101.128.0 bis 101.101.255.255.

/17 heisst, die ersten 17 Bits identifizieren das Netzwerk. Die Subnetzmaske ist somit 11111111 1.11111111.10000000.00000000 (17 mal 1). Damit hat der ISP $32 - 17 = 15$ Bits zur freien Verfügung. Die Bits 18 und 19 können für die Adressierung von vier gleich grossen Subnetzen verwendet werden. Die neue Subnetzmaske ist nun 11111111.11111111.11100000.00000000 (19 mal 1; 13 mal 0).

Damit gibt es in den vier Teilnetzen jeweils $2^{13} - 2 = 8190$ mögliche IP-Adressen. – 2 kommt daher, dass in einem Netzwerk eine IP für die Netzwerkadresse und eine IP für die Broadcast-Adresse reserviert ist.

IP-Adressen der Teilnetze in der Form a.b.c.d/x

Die ersten beiden Bytes des Adressblockes sind definiert: 101.101

Beim 3. Byte ist nur das erste Bit vergeben und in diesem Fall auf 1 gesetzt (128). Die anderen 7 Bits können frei gewählt werden. Das 3. Byte kann von 1000 0000 bis 1111 1111, also von 128 bis 255 verwendet werden. Falls nur die ersten Bits des 3. Byte beachtet werden, würde das folgendes sein:

1000 0000	128
1010 0000	128 + 32 = 160
1100 0000	128 + 64 = 192
1110 0000	128 + 64 + 32 = 224

Teilnetz 1: 101.101.128.0/19 bis 101.101.128.255/19

Teilnetz 2: 101.101.160.0/19 bis 101.101.191.255/19

Teilnetz 3: 101.101.192.0/19 bis 101.101.223.255/19

Teilnetz 4: 101.101.224.0/19 bis 101.101.255.255/19

4) DV-Routing

1. Schritt

Routingtabelle

Von A	Nächster Hop	Kosten	Von B	Nächster Hop	Kosten	Von C	Nächster Hop	Kosten
B	B	1	A	A	1	A	A	4
C	C	4	C	C	1	B	B	1
			D	D	1	D	D	2

Von D	Nächster Hop	Kosten	Von E	Nächster Hop	Kosten
B	B	1	D	D	3
C	C	2			
E	E	3			

Distanzmatrix

	A	B	C	D	E
A	0	1	4		
B	1	0	1	1	
C	4	1	0	2	
D		1	2	0	3
E				3	0

2. Schritt

Routingtabelle

Von A	Nächster Hop	Kosten	Von B	Nächster Hop	Kosten	Von C	Nächster Hop	Kosten
B	B	1	A	A	1	A	B	2
C	B	2	C	C	1	B	B	1
D	B	2	D	D	1	D	D	2
			E	D	4	E	D	5

Von D	Nächster Hop	Kosten	Von E	Nächster Hop	Kosten
B	B	1	D	D	3
C	C	2	B	D	4
E	E	3	C	D	5
A	B	2			

Distanzmatrix

	A	B	C	D	E
A	0	1	2	2	
B	1	0	1	1	4
C	2	1	0	2	5
D	2	1	2	0	3
E		4	5	3	0

3. Schritt

Routingtabelle:

Von A	Nächster Hop	Kosten	Von B	Nächster Hop	Kosten	Von C	Nächster Hop	Kosten
B	B	1	A	A	1	A	B	2
C	B	2	C	C	1	B	B	1
D	B	2	D	D	1	D	D	2
E	B	5	E	D	4	E	D	5

Von D	Nächster Hop	Kosten	Von E	Nächster Hop	Kosten
B	B	1	D	D	3
C	C	2	B	D	4
E	E	3	C	D	5
A	B	2	A	D	5

Distanzmatrix

	A	B	C	D	E
A	0	1	2	2	5
B	1	0	1	1	4
C	2	1	0	2	5
D	2	1	2	0	3
E	5	4	5	3	0

Arbeitsblatt 2: „Datenpakete zusammensetzen“

Aufgabe: TCP-Pakete zusammenfügen

Eine Analyse ergibt, dass vier Segmente an den Zielport 5037 gesendet wurden. Diese können in eine richtige Reihenfolge gebracht werden. Die in ASCII kodierte Nachricht lautet: „@Christa let’s go out! now!“.

Es gibt weitere fünf Pakete, welche an den Zielport 5039 gesendet wurden. In die richtige Reihenfolge gebracht, erhält man die Nachricht: „Hallo Christa bist du schon im Weekend?“

Die restlichen Segmente wurden an verschiedene Zielports gesandt und können nicht nach Sequenznummern sortiert werden.

Der Quellport 143 deutet auf einen IMAP-Dienst wie z.B. ein Mailprogramm, über den Quellport 443 (https) kommen viele Informationen aus Webdiensten. Hier könnte es sich z.B. um einen Facebook-Chat handeln (wobei in einem konkreten Beispiel die Inhalte verschlüsselt wären).

Antworten zu den Fragen

- 1) Mit Multiplexing bezeichnet man den Vorgang, wenn man Informationen für verschiedene Ziele durch eine gemeinsame Leitung schickt. Das Demultiplexing bei TCP basiert darauf, dass jedes Segment an einen Zielport geschickt wird, was einer Zuordnung der Daten zum entsprechenden Programm entspricht.
- 2) Im Kopf eines TCP-Segments stehen der Quellport, der Zielport, die Sequenznummer und die Acknowledgement-Nummer. Zusätzlich gibt es weitere Informationen, welche zum Teil auch noch frei definiert werden können. Ein minimaler Header besteht aus 20 Bytes. (siehe Aufbau_TCP-KOPF.pdf in den Kopiervorlagen).
- 3) Der Empfänger bestätigt jedes eintreffende Segment mit einer ACK-Nummer. Diese ACK-Nummer entspricht der Länge der bis dahin aneinandergfügten Informationen. Im Fall, dass ein Paket verloren geht, kann die Information des übernächsten (eingetroffenen) Pakets nicht angefügt werden. Es wird also nochmals die Bestätigung mit der alten Länge der Information an den Sender geschickt. Dieser kann dann das fehlende Paket nachschicken

Quellport: 443	Zielport: 5037	X
Sequenznummer:	0	
ACK-Nummer:	120	
Inhalt / ASCII-Daten		
01000000 01000011 01101000 01110010		
@ c h r		
01101001 01110011 01110100 01100001		
i s t a		

Quellport: 143	Zielport: 5039	X
Sequenznummer:	0	
ACK-Nummer:	104	
Inhalt / ASCII-Daten		
01001000 01100001 01101100 01101100		
H a l l		
01101111 00100000 01000011 01101000		
o H c h		

H
Space
(hier)

Quellport: 443	Zielport: 5037	X
Sequenznummer:	8	
ACK-Nummer:	128	
Inhalt / ASCII-Daten		
00100000 01101100 01100101 01110100		
H l e t		
00100111 01110011 00100000 01100111		
s H g		

Quellport: 143	Zielport: 5039	X
Sequenznummer:	8	
ACK-Nummer:	112	
Inhalt / ASCII-Daten		
01110010 01101001 01110011 01110100		
r i s t		
01100001 00100000 01100010 01101001		
a H b i		

Quellport: 443	Zielport: 5037	X
Sequenznummer:	16	
ACK-Nummer:	136	
Inhalt / ASCII-Daten		
01101111 00100000 01101111 01110101		
o H o u		
01110100 00100000 00100001 00100000		
t H ! H		

Quellport: 143	Zielport: 5039	X
Sequenznummer:	16	
ACK-Nummer:	120	
Inhalt / ASCII-Daten		
01110011 01110100 00100000 01100100		
s t H d		
01110101 00100000 01110011 01100011		
u H s c		

Quellport: 443	Zielport: 5037	X
Sequenznummer:	24	
ACK-Nummer:	144	
Inhalt / ASCII-Daten		
01101110 01101111 01110111 00100001		
n o w !		

Quellport: 143	Zielport: 5039	X
Sequenznummer:	24	
ACK-Nummer:	128	
Inhalt / ASCII-Daten		
01101000 01101111 01101110 00100000		
h o n H		
01101001 01101101 00100000 01010111		
i m H w		

@Christa let's
go out! now!

Quellport: 143	Zielport: 5039	X
Sequenznummer:	32	
ACK-Nummer:	136	
Inhalt / ASCII-Daten		
01100101 01100101 01101011 01100101		
e e k e		
01101110 01100100 00100000 00111111		
n a H ?		

Hallo Christa bist
du schon im
weekend?

Arbeitsblatt 3: „Datenpakete priorisieren“

1) Wie lautet die IP-Adresse?

<http://www.tincheungcamera.com.hk>

180.92.181.12

<http://180.92.181.12/>

<http://www.nyc.com>

66.111.11.23

<http://66.111.11.23/>

mit <http://ping.eu/nslookup/>

2) Wo befinden sich die folgenden Webserver?

Die Antwortzeiten können variieren!

a) <http://www.places.co.za> (Webserver in Südafrika)

Die Pakete brauchen

- 290 ms von Amerika
- 161 ms von Europa
- 470 ms von Asien



a)

b) <http://www.charterlink.co.nz> (Webserver in Neuseeland)

Die Pakete brauchen

- 128 ms von Amerika
- 278 ms von Europa
- 166 ms von Asien

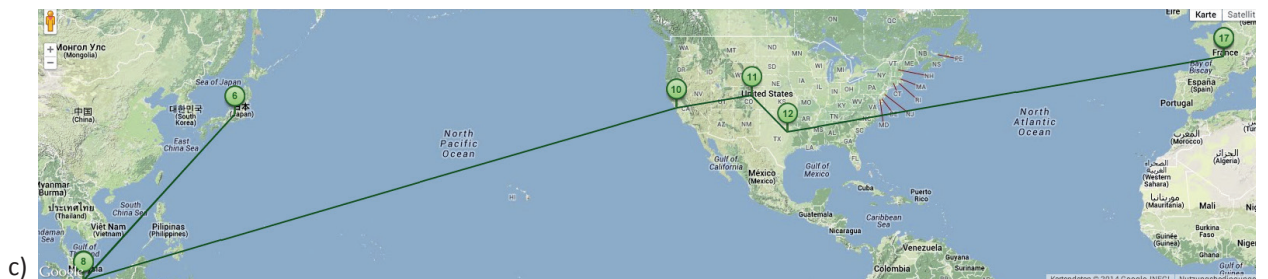


b)

c) <http://www.parishotels.com> (Webserver in Paris)

Die Pakete brauchen

- 147 ms von Amerika
- 16 ms von Europa
- 248 ms von Asien



c)

3) Mit Google Maps lassen sich auf der ganzen Welt Angebote finden. Z.B. ein Skigebiet im Himalaya. Die Webseite der Auli-Hotels in diesem Skigebiet läuft jedoch auf einem Server www.hotelsinauli.co.in in Singapur.

Impressum

Herausgeber	SVIA, Schweizerischer Verein für Informatik in der Ausbildung
Partner	Hasler Stiftung ICT Berufsbildung SWITCH
Konzeption / Umsetzung	Lernetz AG
Autorenschaft	Martin Guggisberg, PH FHNW Yvonne Seiler