

Kommunikation und Datenhaltung Sommersemester 2009

3. K-Übungsblatt

Aufgabe 1: Vermittlungsschicht und Segmentierung

- (a) Das Internet Protocol (IP) bietet die Möglichkeit, Dateneinheiten für den Transport über ein Medium der Sicherungsschicht mit geringer *Maximum Transfer Unit* (MTU) zu fragmentieren und auch wieder zu reassemblieren. Was könnten Gründe dafür sein, es als nicht sinnvoll zu erachten, die Reassemblierung schon in zwischenliegenden Routern vornehmen zu lassen?

Routen können sich im Internet im Laufe der Zeit ändern, so dass ein Router, der bereits einen Teil der zu reassemblierenden Dateneinheiten bekommen hat, nicht mehr auf dem Datenpfad der neuen Route liegt. Desweiteren ist effizientes Reassemblieren auf IP-Schicht schwierig, da IP – im Gegensatz zu bspw. TCP – im Protokollkopf keine Möglichkeit vorsieht anzuzeigen, wieviele Fragmente noch folgen oder wie groß die Dateneinheit insgesamt ist.

- (b) Nennen Sie Möglichkeiten, wie man Fragmentierung auf IP-Schicht vermeiden könnte, wenn man davon ausgeht, dass auf einem Datenpfad MTUs unterschiedlicher Größe existieren.
- Immer die kleinstmögliche maximale Datagrammgröße wählen: Dazu muss eine kleinstmögliche Größe definiert worden sein. Die IP Spezifikation erlaubt das Senden 576 Bytes großer Dateneinheiten als maximale Größe eines Senders, ohne dass dieser eine explizite Erlaubnis des Empfängers dafür bräuchte.
 - Erraten der minimalen MTU eines Pfads: Man könnte eine Heuristik verwenden, mit der die minimale MTU eines Datenpfads bestimmt wird.
 - Tatsächliche minimale MTU ermitteln: Mittels eines Protokolls könnte man die minimale MTU auf dem Datenpfad ermitteln. Für Messmechanismen (*Probing*) benötigte man die Unterstützung der zwischenliegenden Router, die entweder eine Liste aller MTUs ergänzen oder die Größe der minimalen MTU anpassen.
 - Raten oder Entdecken der MTU und Zurückverfolgen falls falsch: Da eine Schätzung falsch sein könnte und sich eine entdeckte MTU aufgrund von Routingänderungen verändern könnte, muss die MTU Größe manchmal angepasst werden. Man könnte Messungen mit speziellen ICMP Nachrichten (*»Probe Path«*) durchführen. Alternativ können Messungen im Piggyback-Verfahren im IP-Kopf von regulären Dateneinheiten durchgeführt werden.

Dabei passt jeder zwischenliegende Router bei Bedarf den Wert einer *Probe MTU* Option an. Sobald die Dateneinheit den Empfänger erreicht hat kopiert dieser den Wert in das Feld einer *MTU Reply* Option und fügt diese an die nächste Dateneinheit, die zurück zum ursprünglichen Sender geschickt wird, an.

Eine ausführliche Diskussion dazu findet sich in der Veröffentlichung von Kent und Mogul »Fragmentation Considered Harmful« und dem RFC 1063. Das heutzutage eingesetzte Verfahren ist in RFC 1191 beschrieben. Hierbei schickt der Sender eine Dateneinheit mit der maximal möglichen MTU-Größe, die ihm anhand des eigenen Netzzugangspunkts bekannt ist, bei der im IP-Kopf das »*Don't Fragment*« (DF) Bit gesetzt ist. Sollte die Größe der IP-Dateneinheit von einem zwischenliegenden Router nicht ohne Fragmentierung weitergeleitet werden können, verwirft dieser die Dateneinheit und antwortet mit einer ICMP Nachricht »*Destination unreachable. Fragmentation needed and DF bit set.*«. Empfängt der ursprüngliche Sender eine solche Nachricht, muss er folgende Dateneinheiten auf dieser Route mit kleinerer Größe verschicken. Damit der Sender weiß, um wieviel er die MTU verringern muss, haben Router die Möglichkeit, in der ICMP Nachricht die Größe der gewünschten MTU anzugeben.

Es sei eine Vermittlungsschichtinstanz angenommen, welche die Dienste einer Sicherungsschicht nutzt, die folgende Beschränkungen aufweist:

- Die maximale Nutzdatenlänge, mit der die Sicherungsschicht umgehen kann, beträgt 1 500 Byte
- Die angebotene Bitübertragungsrate ist 7 Mbit/s
- Die Sicherungsschicht verwendet das *Stop-and-Wait*-Verfahren
- Die Sicherungsschicht garantiert am Dienstzugangspunkt eine reihenfolgegetreue Auslieferung

Die Vermittlungsschicht muss Nutzdaten der Länge 0,9 MByte verschicken.

- (c) Die Quittung selbst hat eine Länge von 1 kbit. Wie lange dauert der gesamte Datentransfer von Anlieferung der zu sendenden Daten am Dienstzugangspunkt der Vermittlungsschicht des Senders bis zur Anzeige der vollständig empfangenen Daten am Dienstzugangspunkt der Vermittlungsschicht des Empfängers? Dabei seien Ausbreitungsverzögerung und die Verarbeitungszeiten in den jeweiligen Instanzen selbst zu vernachlässigen.

Im ersten Schritt sind die entsprechenden Umrechnungen durchzuführen, woraus sich die Anzahl der benötigten Dateneinheiten berechnen lässt:

$$0,9 \text{ MByte} = 7,2 \text{ Mbit} = 7\,200 \text{ kbit}$$

$$1\,500 \text{ Byte} = 12\,000 \text{ bit} = 12 \text{ kbit}$$

Daraus errechnet sich die Anzahl der Dateneinheiten durch

$$\frac{7\,200 \text{ kbit}}{12 \text{ kbit / Dateneinheit}} = 600 \text{ Dateneinheiten}$$

Bei einer Größe der Quittungen von 1 kbit müssen somit $1 \text{ kbit/Dateneinheit} \cdot 600 \text{ Dateneinheiten} = 600 \text{ kbit}$ zusätzlich übertragen werden. Es müssen insgesamt $(7200 + 600) \text{ kbit} = 7800 \text{ kbit} = 7,8 \text{ Mbit}$ übertragen werden. Bei einer Verbindung mit der Geschwindigkeit von 7 Mbit/s sind dafür $7,8 \text{ Mbit} / 7 \text{ Mbit/s} = 1,1 \text{ s}$ notwendig.

- (d) Illustrieren Sie mittels eines Weg-Zeit-Diagramms, in dem Sicherungs- und Vermittlungsschicht aufgeführt sind, sowie den entsprechenden Dienstprimitiven den Datenaustausch.

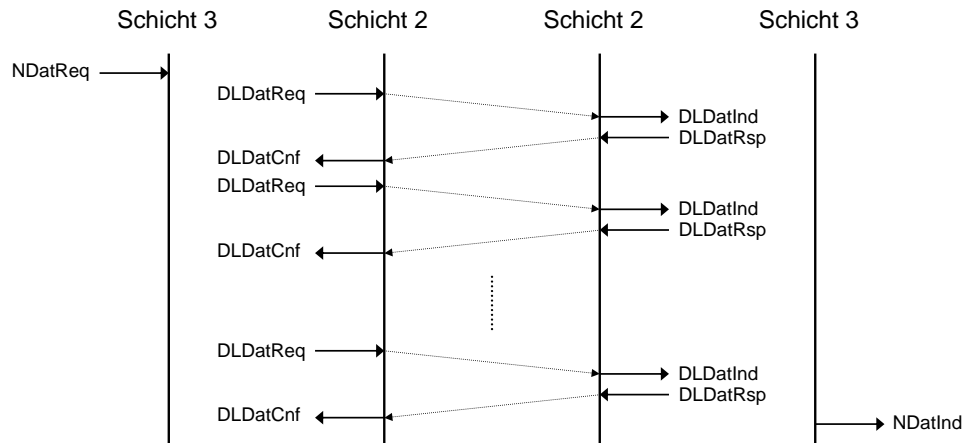


Abbildung 1: Weg-Zeit Diagramm für den Datenaustausch über Vermittlungs- und Sicherungsschicht

Das Weg-Zeit-Diagramm für das in dieser Aufgabe beschriebene Szenario ist in Abbildung 1 aufgeführt. Das Stop-and-Wait-Verfahren wird durch die protokollseitige Bestätigung mittels einer ACK-PDU realisiert. Bevor weitere Dateneinheiten mittels `DLDatReq` verschickt werden können, muss diese ACK-PDU für die vorangegangene Übertragung beim Sender eingetroffen sein.

- (e) Eine Anwendung möchte eine Dateneinheit von 1742 Bit über TCP/IP übertragen. TCP fügt dieser einen Kopf von 160 Bit hinzu. Auf der Vermittlungsschicht fügt IP einen Paketkopf mit ebenfalls 160 Bit hinzu. Auf der Sicherungsschicht werden jeder Dateneinheit 24 Bit Kopf und 8 Bit Prüfsumme hinzugefügt. Allerdings ist die maximale Größe einer Dateneinheit auf Sicherungsschicht auf 800 Bit beschränkt und es ist nicht möglich, ankommende Dateneinheiten auf Schicht 2 zu segmentieren. Wie viele Bit (inklusive den Köpfen) werden letztendlich mindestens über das Netzwerk übertragen?

Insgesamt möchte eine Anwendung 1742 Bit übertragen. TCP fügt diesen einen Kopf von 160 Bit hinzu, wodurch die Vermittlungsschicht (IP) insgesamt 1902 Bit übertragen muss. Da die Sicherungsschicht keine Segmentierung vornehmen kann, muss bereits in der Vermittlungsschicht dafür gesorgt werden, dass die zu übertragenden IP-Dateneinheiten diese Größenbeschränkung einhalten. Auf Schicht 2 können insgesamt $(800 - 24 - 8) \text{ Bit} = 768 \text{ Bit}$ übertragen werden, d. h. auf Vermittlungsschicht dürfen in eine Dateneinheit maximal $(768 - 160) \text{ Bit} = 608 \text{ Bit}$ Nutzdaten gepackt werden. Daher sind $1902 \text{ Bit} / 608 \text{ Bit/Dateneinheit} = 3,13$ Dateneinheiten, also 4 IP-Dateneinheiten notwendig. Daher müssen von der

Vermittlungsschicht insgesamt $(1902 + 4 \cdot 160)$ Bit = 2542 Bit übertragen werden. Auf der Sicherungsschicht werden weitere $(24 + 8)$ Bit pro Dateneinheit hinzugefügt, so dass summa summarum $(2542 + 4 \cdot (24 + 8))$ Bit = 2670 Bit zu übertragen sind. Abbildung 2 verdeutlicht diesen Sachverhalt.

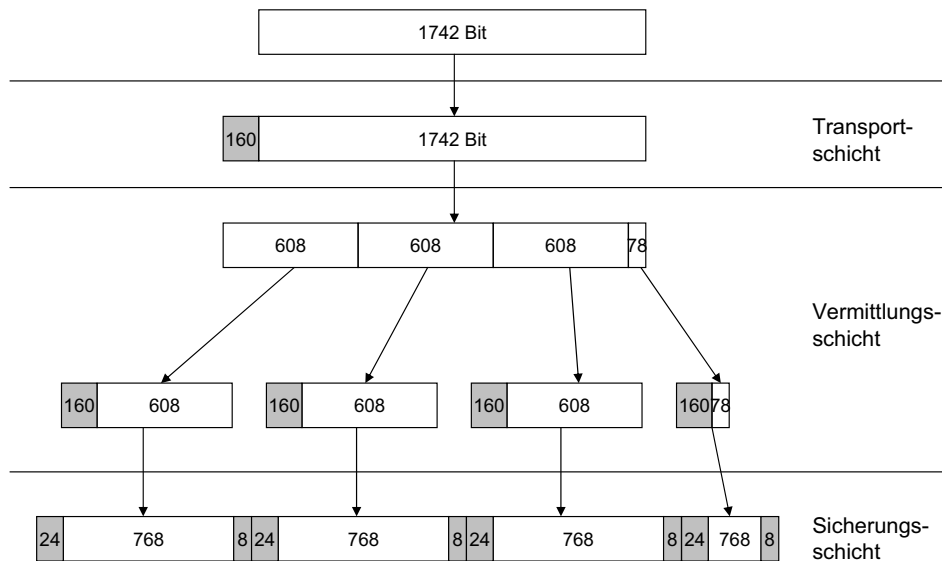


Abbildung 2: Segmentierung

- (f) Wie viele Dateneinheiten müssen erneut gesendet werden, falls eine Dateneinheit auf der Vermittlungsschicht verfälscht wird?

Auf Schicht 3 sind mit IP keinerlei Sicherungsmaßnahmen gegen den Verlust von Dateneinheiten gegeben. Das bedeutet, dass ein auftretender Fehler nicht von der Vermittlungsschicht, sondern von der darüberliegenden Transportschicht erkannt wird. In diesem Fall wird die (verfälschte) Nachricht vom Empfänger erneut angefordert, d. h. es sind 4 weitere IP-Dateneinheiten zu übertragen, welche die gesamte Nachricht beinhalten.

- (g) Die im Internet eingesetzten Protokolle TCP und IP bieten beide die Möglichkeit zur Segmentierung. Welche Möglichkeit wäre hierbei zu bevorzugen? Erläutern Sie entsprechende Vor- und Nachteile.

TCP ist Byte-Strom orientiert und sieht eine maximale Segmentgröße (MSS) vor. Eine Segmentierung auf TCP-Ebene ist daher zu bevorzugen, da auf dieser Ebene auch Sicherungsmechanismen, wie Wiederholung von Dateneinheiten, vorgesehen sind. Wenn in der IP-Schicht segmentiert wird und ein IP-Fragment verloren geht, muss hingegen die komplette IP-Dateneinheit, d. h. alle Fragmente erneut gesendet werden. Zudem ist eine Segmentierung bei IPv6 auf Routern nicht mehr möglich, daher muss diese ohnehin im Endsystem stattfinden.

Aufgabe 2: Routing

- (a) Was versteht man unter adaptiven/dynamischen Routing-Algorithmen?

Im Gegensatz zum *statischen* Routing, bei dem die Wegewahltabelle für längere Zeit fixiert ist, werden bei dynamischen bzw. adaptiven Verfahren die Wegewahl-
tabellen laufend den aktuellen Verkehrserfordernissen angepasst.

Abbildung 3 stellt ein Netzwerk aus sechs Zwischensystemen dar, wobei an den einzelnen Ver-
bindungsleitungen Kostenfaktoren angegeben sind. Der eingesetzte Routingalgorithmus soll den
kostengünstigsten Weg finden. Bei gleichen Kosten soll der Weg ausgewählt werden, der die we-
nigsten Zwischensysteme enthält.

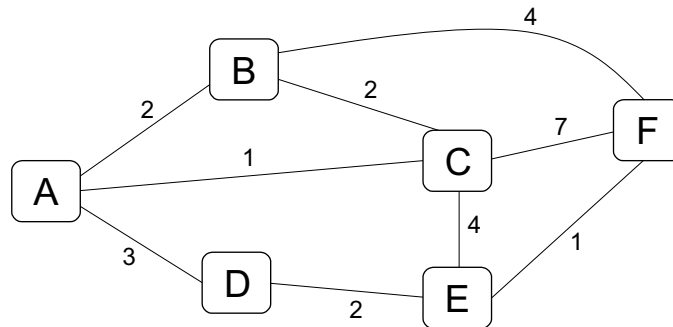


Abbildung 3: Netzwerk mit Zwischensystemen

(b) Erstellen Sie die Wegewahltabelle für Router C gemäß dem Dijkstra-Algorithmus und der
in der Vorlesung eingeführten Notation.

Schritt	N	D(A), p(A)	D(B), p(B)	D(D), p(D)	D(E), p(E)	D(F), p(F)
0	C	1, C	2, C	∞	4, C	7, C
1	CA			4, A		
2	CAB					6, B
3	CABD					
4	CABDE					5, E
5	CABDEF					

Tabelle 1: Wegewahlberechnung gemäß Dijkstra-Algorithmus aus Sicht von Knoten C

- (c) Die Leitung, die die Zwischensysteme A und C verbindet, sei gestört. Welche Veränderungen ergeben sich in den Wegewahltabellen?

Schritt	N	D(A), p(A)	D(B), p(B)	D(D), p(D)	D(E), p(E)	D(F), p(F)
0	C	∞	2, C	∞	4, C	7, C
1	CB	4, B				6, B
2	CBA			7, A		
3	CBAE			6, E		5, F
4	CBAEF					
5	CBAEFD					

Tabelle 2: Wegewahlberechnung gemäß Dijkstra-Algorithmus aus Sicht von Knoten C nach Leitungsstörung

- (d) Wovon kann der Netzbetreiber die Kosten einzelner Verbindungen abhängig machen?

Die Kosten können auf vielfältige Art und Weise ihre Ursache finden, bspw. gegeben durch

- das physikalische Medium (Glasfaser, Koaxialkabel, verdrehtes Kupferadernpaar)
- das Verkehrsaufkommen, also der Belastung der Verbindung
- »politischen« Bestrebungen der Netzbetreiber
- Dienstgütemerkmalen wie bspw. zugesicherten Bandbreiten, maximalen Latenzen oder Zuverlässigkeitsgarantien

Aufgabe 3: IP-Adresskonfiguration

Nachdem sich die ursprüngliche Einteilung von IP-Adressen in feste Klassen (am wichtigsten davon Netzwerk-Klassen A – C mit festgelegter Anzahl Endsysteme pro Klasse) als zu unflexibel und verschwenderisch herausgestellt hatte, wurde 1993 das in RFC 1519 spezifizierte Verfahren *Classless Inter-Domain Routing* (CIDR) eingeführt. Mit CIDR wird die feste Aufteilung der alten Adressklassen in Netzwerk-Teil und lokalen Teil durch eine flexible Zuordnung ersetzt. Die Subnetzmaske, welche in ihrer Bitdarstellung festlegt, welche Bit der IP-Adresse das Netzwerk und welche Bit den Endsystem-Teil repräsentieren, kann mit CIDR eine beliebige Länge haben. Zudem wurde eine neue Notation eingeführt, bei der die Anzahl Einser-Bits der Subnetzmaske als »/Anzahl« hinter die IP-Adresse geschrieben wird.

Beispiel: 13.12.11.10/28 entspricht der IP-Adresse 13.12.11.10 mit Subnetzmaske 11111111.11111111.11111111.11110000 (28 Einsen) und somit 255.255.255.240 (Subnetzmaske in Dezimal-Schreibweise). In diesem Fall bestimmen daher die ersten 28 Bit der binären IP-Adresse den Netzwerk-Teil, während die letzten 4 Bit den Endsystem-Teil repräsentieren. Aufgrund des 4 Bit langen Endsystem-Teils können daher mit dieser Subnetzmaske maximal 2^4 und damit 16 Adressen im zugehörigen Netzwerk verwendet werden. (Als Besonderheit ist noch zu beachten, dass

davon i. A. zwei Adressen für die Netzwerk- und die Broadcast-Adresse reserviert sind, es können also tatsächlich nur 14 Rechner in diesem Netzwerk mit eindeutigen IP-Adressen versehen werden.)

- (a) Gegeben sei der IP-Adressbereich 141.22.67.0/24. Liegt die Adresse 141.22.70.198 im zugehörigen Netzwerk oder nicht?

Der Netzwerk-Teil von Adressen, die sich im zugehörigen Netzwerk eines Adressbereichs befinden, stimmt mit dem Netzwerk-Teil des Adressbereichs überein.

Die 24 Bit der Subnetzmaske von 141.22.67.0/24 »decken« genau die ersten drei Bytes des Adressbereichs ab, das bedeutet, nur alle Adressen, die mit 141.22.67.x beginnen, befinden sich im zugehörigen Netzwerk. Die fragliche Adresse 141.22.70.198 liegt daher *nicht* im zugehörigen Netzwerk.

- (b) Gegeben sei der IP-Adressbereich 141.22.67.0/20. Liegt die Adresse 141.22.70.198 im zugehörigen Netzwerk oder nicht?

Untersucht werden muss, ob die ersten 20 Bit der Adresse 141.22.70.198 mit den ersten 20 Bit des Adressbereichs 141.22.67.0/20 übereinstimmen:

141.22.70.198 in Binärschreibweise: 10001101.00010110.0100 0110.11000110

141.22.67.0 in Binärschreibweise: 10001101.00010110.0100 0011.00000000

Die ersten 20 Bit (Netzwerkteil, grau unterlegt) stimmen überein, d. h. die fragliche Adresse befindet sich im zugehörigen Netzwerk.

- (c) Gegeben sei der IP-Adressbereich 141.22.67.0/22. Welche IP-Adressen bilden den Anfang und das Ende dieses Adressbereichs, bzw. welche IP-Adressen liegen im zugehörigen Netzwerk?

Die ersten 22 Bit des Adressbereichs (grau unterlegt) stellen mit angehängten binären Nullen den Anfang des Adressbereichs dar und mit angehängten binären Einsen das Ende:

141.22.67.0 binär: 10001101.00010110.010000 11.00000000

Anfang Adr.bereich: 10001101.00010110.010000 00.00000000 = 141.22.64.0

Ende Adr.bereich: 10001101.00010110.010000 11.11111111 = 141.22.67.255

(Alternativ kann das Ende des Adressbereichs auch über den Anfang des Adressbereichs und die mögliche Anzahl an, mit den restlichen $32 - 22 = 10$ Bit erzeugbaren, Hostadressen gefunden werden.)

- (d) Ihnen sei von Ihrem Netzbetreiber der IP-Adressbereich 141.22.67.0/26 zur freien Verfügung zugeteilt worden. Sie möchten diese Adressen getrennt auf drei Netzwerk-Standorte verteilen. Am ersten Standort sind 10 Endsysteme anzubinden, am zweiten 13 und am dritten 21. Mit welchen Adressen und Subnetzmasken konfigurieren Sie die einzelnen Standorte?

Zur eindeutigen Adressierung von 10 Endsystemen werden mindestens 4 Bit für den Endsystem-Adressteil benötigt, für 13 Endsysteme ebenfalls, für 21 Endsysteme 5 Bit. Weniger ist jeweils nicht ausreichend, mehr wird nicht benötigt. D. h.

der zugeteilte Adressbereich muss in zwei Teile mit $32 - 4 = 28$ Bit Subnetzmaske und einen Teil mit $32 - 5 = 27$ Bit Subnetzmaske aufgeteilt werden. Eine beispielhafte, mögliche Aufteilung wäre die folgende:

1. Standort: Adressbereich 141.22.67.0/28 mit Adressen 141.22.67.0 bis 141.22.67.15
2. Standort: Adressbereich 141.22.67.16/28 mit Adressen 141.22.67.16 bis 141.22.67.31
3. Standort: Adressbereich 141.22.67.32/27 mit Adressen 141.22.67.32 bis 141.22.67.63

Der insgesamt zugeteilte Adressbereich von 141.22.67.0 bis 141.22.67.63 wurde hierbei nicht überschritten, keine Adresse wurde an mehr als einem Standort genutzt und an jedem Standort sind genug Adressen für die Endsysteme vorhanden.

Aufgabe 4: Domain Name System

- (a) Die Protokolle ARP und DNS machen beide Gebrauch von Caches. Die Lebensdauer von Einträgen im ARP-Cache beträgt normalerweise 20 Minuten und die im DNS-Cache mehrere Tage. Nennen Sie eine Rechtfertigung für diesen Unterschied. Welche unerwünschten Konsequenzen können entstehen, wenn die Lebensdauer von Einträgen im DNS-Cache zu lang ist?

Obwohl sich die Zuordnung MAC-Adresse \leftrightarrow IP-Adresse normalerweise selten ändert (z. B. beim Austausch einer Netzwerkkarte), ist es kein Problem ARP-Anfragen relativ häufig zu verschicken (die typische Lebenszeit eines Eintrags innerhalb des ARP-Caches beträgt 20 Minuten), da diese auf das lokale und meist schnelle Netz beschränkt sind. DNS-Anfragen müssen hingegen über das Internet versendet werden, was durch eine längere Lebensdauer der Cache-Einträge (meist mehrere Tage) seltener geschehen soll. Normalerweise ist dies kaum ein Problem, da auch die Zuordnung DNS-Name (Rechnername) \leftrightarrow IP-Adresse üblicherweise relativ konstant ist. Sollte dies nicht der Fall sein, verursacht die lange Lebensdauer die Nutzung einer veralteten IP-Adresse für einen Rechnernamen, so dass der gewünschte Rechner in diesem Zeitraum nicht erreicht werden kann.

- (b) Beschreiben Sie den grundsätzlichen Ablauf einer DNS-Anfrage und benennen Sie die beteiligten Systeme.

Im Rahmen einer Namensauflösung via DNS wird zunächst auf dem anfragenden System überprüft, ob die Antwort bereits bekannt ist, d.h. ob sie sich bereits im lokalen DNS-Cache befindet. Falls dies nicht der Fall ist, wird der lokal definierte DNS-Server angefragt. Dort läuft der gleiche Algorithmus ab: Liegt die Antwort bereits im eigenen DNS-Cache vor, wird diese zurückgeliefert. Andernfalls befragt der DNS-Server je nach Konfiguration entweder eine Menge an fest definierten anderen DNS-Servern oder er führt eine sukzessive Auflösung beginnend bei den fest definierten DNS-Rootservern durch.

- (c) Angenommen, ein Endsystem entscheidet sich bezüglich der Adressauflösung für die Benutzung eines Nameservers, der sich nicht innerhalb seiner Organisation befindet. In welchem Szenario könnte dies im Vergleich zur Nutzung des lokalen Nameservers aufgrund von Anfragen, die in einem DNS-Cache nicht gefunden werden, zu mehr DNS-Gesamtverkehr führen?

DNS-Server speichern Antworten auf Anfragen in einem eigenen Cache, um so oft wie möglich Anfragen direkt ohne internetweite Kommunikation beantworten zu können. Nutzt ein Endsystem nun einen externen Nameserver anstelle desjenigen innerhalb seiner lokalen Organisation, kann er nicht vom Cache des internen DNS-Servers profitieren. Wenn das Nutzungsprofil innerhalb der Organisation relativ gleichartig ist und daher viele interne Nutzer die gleichen Adressen (be)suchen, handelt es sich hierbei um einen Nachteil, weil der externe Cache diese Adressen evtl. noch nicht kennt und erst (durch weitere Anfragen) ermitteln muss. (Wird dagegen angenommen, dass der externe DNS-Server über einen »passenderen« Cache verfügt, könnte dies evtl. insgesamt DNS-Abfragen sparen.)

Da bei DNS-Abfragen aber eigentlich die Laufzeit eine entscheidende Rolle spielt, sollte im Allgemeinen stets der topologisch naheliegendste Nameserver verwendet werden. Die angefragten Adressen wird er nach der ersten Anfrage cachen und ab dann am schnellsten (aufgrund der geringen Laufzeit) antworten können.

Aufgabe 5: Zusammenspiel der Schichten

Das Ziel dieser (etwas umfangreicheren) Aufgabe ist es, das Zusammenspiel zwischen den einzelnen Schichten anhand eines einfachen realen Beispiels nachzuspielen. Dabei sollen sämtliche für das Internet relevanten Schichten einbezogen werden: Anwendungsorientierte Schicht, Transportschicht (TCP), Vermittlungsschicht (IP) und Sicherungsschicht (PPP, s. u.).

Angenommen sei das folgende Beispiel aus dem Leben einer Studentin bzw. eines Studenten: Sie sitzen zuhause vor Ihrem Computer (mit Modem bzw. ISDN-Adapter, ausnahmsweise kein DSL oder WLAN) und möchten zur WWW-Seite des Instituts für Telematik surfen (<http://www.tm.uka.de>). Sie starten daher Ihren Webbrowser und tippen die angeführte URL ein, um die gewünschte Anfrage abzusetzen (direkt den HTTP-Get.Req, die Namensauflösung sei an dieser Stelle einmal vernachlässigt). Der Webbrowser veranlasst das TCP/IP daraufhin, über das Modem bzw. den ISDN-Adapter eine PPP-Verbindung (*Point to Point Protocol*, ein Protokoll der Sicherungsschicht, das hauptsächlich zur Einwahl bei Providern verwendet wird) zum Rechenzentrum der Universität Karlsruhe aufzubauen, um die gewünschte Seite zu laden. Sie haben sich bisher noch nicht in das Rechenzentrum eingewählt.

Hinweis: TCP verwendet beim Verbindungsaufbau einen Drei-Wege-Handshake. Für die gesicherte Übertragung der Daten sorgt TCP durch das Schicken einer ACK-Dateneinheit als Bestätigung für die korrekte Ankunft der Daten.

- (a) Wie viele Verbindungen auf Transportschicht werden in diesem (vereinfachten) Beispiellauf aufgebaut?

Es wird i.d.R. genau eine TCP-Verbindung aufgebaut, da eine TCP-Verbindung immer einen Kanal zwischen Sender und Empfänger bereitstellt. Es ist allerdings durchaus möglich, dass mehrere TCP-Verbindungen zwischen dem Webbrowser und dem Webserver bestehen.

- (b) Skizzieren Sie den Ablauf bis zum Empfang der WWW-Seite (HTTP-Rsp.Ind) in Form eines Weg-Zeit-Diagramms, welches Anwendungsschicht, Transportschicht, Vermittlungsschicht und die Sicherungsschicht umfasst. Dazu sind die jeweiligen Dienste und die ausgetauschten Protokollateneinheiten in das Weg-Zeit-Diagramm einzuzeichnen. Der Abbau der Transportschichtverbindung bleibt der Einfachheit halber unberücksichtigt.

siehe Abbildung 4

Hinweis: Im dargestellten Ablauf werden im letzten Schritt des TCP-Verbindungsaufbaus (ACK) auch gleich Daten (die Dateneinheit $\langle H-R \rangle$) übermittelt, um die Abbildung kompakt zu halten. Dies ist laut RFC 793 möglich, wird allerdings von typischen Implementierungen nicht so gehandhabt, sondern es wird ein separates ACK übermittelt und die eigentlichen Daten dann direkt im Anschluss in weiteren Dateneinheiten.

- (c) Wozu dient das Protokoll ARP? Bei welcher Anfrage in Ihrem Schaubild würde dieses Protokoll in Aktion treten, falls sich der Webserver in Ihrem lokalen Netzwerk befindet?

ARP ist auf der Vermittlungsschicht angesiedelt. Es wird dazu verwendet, IP-Adressen auf zugehörige Schicht 2-Adressen (MAC-Adressen) abzubilden. Es tritt in Aktion bevor die erste Dateneinheit auf der Sicherungsschicht (*DataLink*, DL) gesendet wird.

- (d) Was müsste die Anwendung als Grundlage für die Abfrage der entsprechenden WWW-Seite normalerweise noch durchführen (falls nicht, wie oben, vernachlässigt)? An welcher Stelle im Ablauf, würde diese Tätigkeit stattfinden?

Bevor die Anwendung den Webserver kontaktieren kann, muss sie die IP-Adresse des gewünschten Webservers kennen. In unserem Beispiel ist es also erforderlich, aus dem URL (*Uniform Resource Locator*), im Beispiel *http://www.tm.uka.de*, die zugehörige IP-Adresse herauszufinden. Diese wird über *Domain Name System* (DNS) Server ermittelt, die zur Namensauflösung kontaktiert werden müssen. Dies geschieht vor dem Verbindungsaufbau zum Webserver, dessen IP-Adresse bis dahin ja noch unbekannt ist. Die DNS-Abfrage im Szenario würde den Namen *www.tm.uka.de* zur IP-Adresse des Webservers des Instituts für Telematik auflösen.

- (e) Wie wird die bestehende Verbindung auf der Sicherungsschicht aufgelöst, bzw. durch was wird sie nicht aufgelöst?

Ein Abbau der TCP-Verbindung bewirkt *keinen* Abbau der Verbindung auf der Sicherungsschicht. Der Grund ist darin zu sehen, dass die PDUs für den Verbindungsabbau als transparente Daten über die Sicherungsschicht übertragen werden. Auf Schicht 2 ist also nicht erkennbar, ob von der Transportschicht ein Verbindungsabbau kommt. Stattdessen wird die Verbindung auf der Sicherungsschicht auf viel »brutalere« Weise beendet: Durch Auflegen (=Beenden der Verbindung), wie dies vom Telefon her bekannt ist.

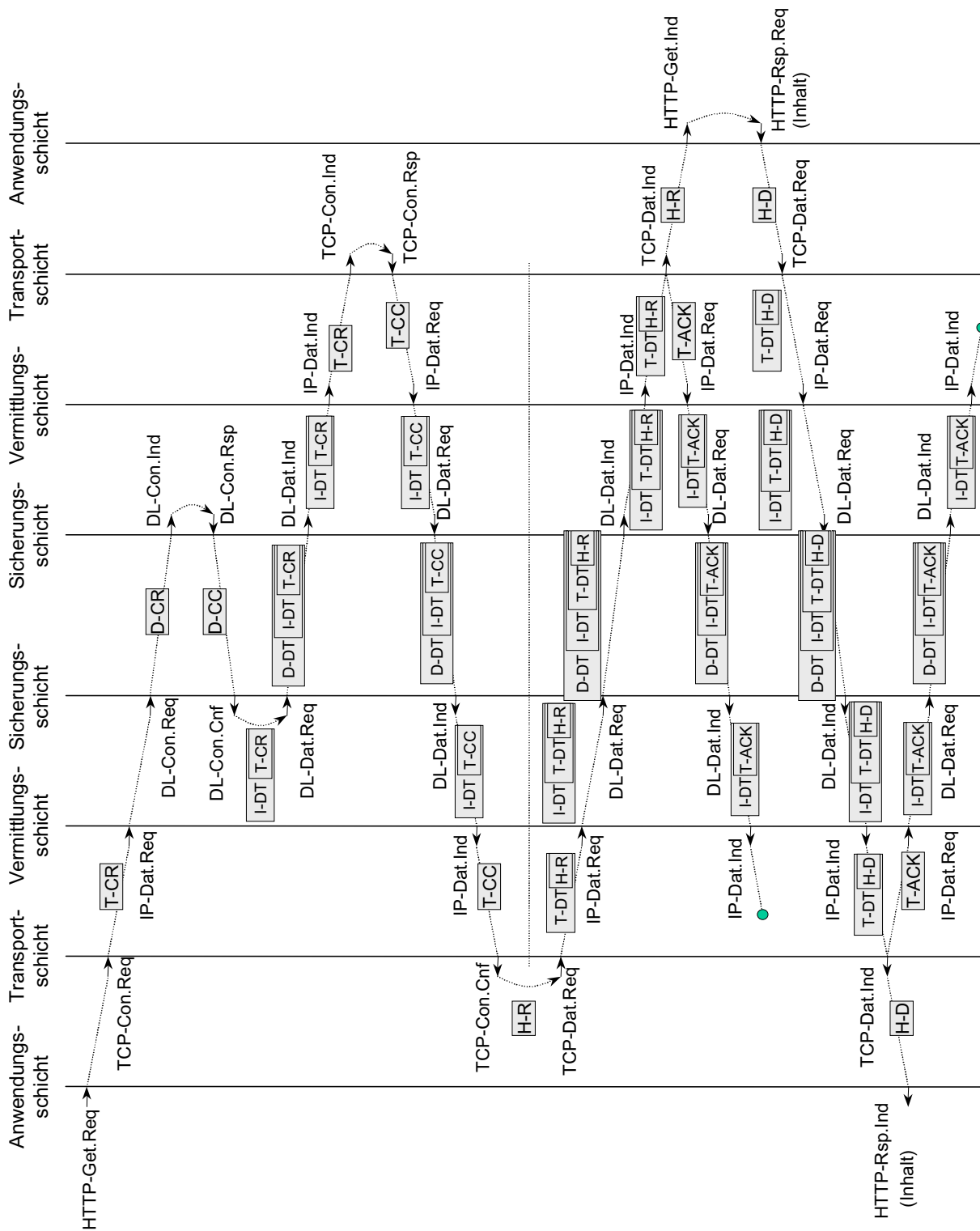


Abbildung 4: Beispielablauf beim Zusammenspiel der Schichten