
1 Grundlagen — Die TCP/IP-Protokollfamilie

In diesem Kapitel lernen Sie

- ▶ die Architektur von TCP/IP kennen.
- ▶ die Bedeutung der Standard-Netzwerkprotokolle kennen.
- ▶ die Schichtenmodelle zur Beschreibung von Netzwerk-Software kennen.
- ▶ die TCP/IP-Protokollfamilie kennen.
- ▶ die Bedeutung von IPv6.

1.1 Übersicht über die Standard-Netzwerkprotokolle und -Dienste

In Computernetzwerken kann ein Rechner einen Dienst anbieten (*Server*), oder einen Dienst eines anderen Rechners in Anspruch nehmen (*Client*). Die Begriffe von Protokoll und Dienst sind eng miteinander verknüpft. Der *Dienst* besagt dabei, *welche Art* von Leistung erbracht wird und das *Protokoll* legt dabei fest, *wie* diese Leistung erbracht, bzw. kommuniziert wird.



Beispiel: Ein Mittagessen in einem Restaurant ist ein gutes Beispiel für die Begriffe Protokoll und Dienst. Dabei besteht der Dienst darin, dass der Gast (*Client*) in einem Restaurant (*Server*) mit Getränken und Essen versorgt wird (*Dienst*). Das Protokoll legt eine Standardvorgehensweise fest, wie der Dienst erbracht wird. Das hat den Vorteil, dass der Gast und der Kellner genau wissen, wie sie miteinander kommunizieren können. Immer dann, wenn einer der beiden (Gast oder Kellner) vom Protokoll abweichen, ist die Gefahr von Missverständnissen oder Unbehagen gegeben.

Das Protokoll zur Bestellung in einem Restaurant lässt sich in etwa wie folgt definieren:

1. Der Gast betritt das Restaurant und belegt einen freien Tisch.
2. Der Kellner kommt an den Tisch und fragt die Gäste, welches Getränk sie bestellen möchten.
3. Die Gäste nennen ein Getränk aus der Getränkekarte. Falls ein Gast ein Getränk bestellt, das nicht auf der Getränkekarte steht, so tritt folgendes Unterprotokoll in Kraft, mit dem Kellner und Gast ein verfügbares Getränk aushandeln:
 - (a) Kellner nimmt an. In diesem Fall ist das Unterprotokoll beendet. Falls nicht gegeben, so schlägt der Kellner eventuell eine Alternative vor.

- (b) Falls der Kellner eine Alternative vorgeschlagen hat, nimmt der Kunde an, womit wiederum das Unterprotokoll beendet ist. Falls nicht, schlägt der Kunde eine Alternative vor, womit das Unterprotokoll von neuem abläuft.
4. Der Kellner bringt die bestellten Getränke.
5. Die Gäste bestellen die Speisen.
6. Der Kellner bringt die Speisen.
7. Optional erfolgt die Bestellung von weiteren Speisen (z.B. Desserts) oder Getränken nach folgendem Muster:
 - (a) Der Kellner kommt (eventuell auf Hinweis des Gastes).
 - (b) Der Gast bestellt eine Speise/ein Getränk.
 - (c) Der Kellner bringt die Speise/das Getränk.
8. Die Gäste fordern den Kellner auf, die Rechnung zu bringen.
9. Der Kellner bringt die Rechnung und fragt: „Zusammen oder getrennt?“.
10. Die Gäste zahlen entweder jeder für sich oder ein Gast zahlt für alle zusammen.
11. Die Gäste verlassen das Restaurant.

In diesem Beispiel wissen alle Beteiligten, wie das Protokoll abläuft. Das gibt allen Beteiligten die Sicherheit, dass sie sich verstehen.

Wollen zwei Rechner im Netz miteinander kommunizieren, so geschieht das mit Hilfe eines *Netzwerkprotokolls*. Ein Protokoll ist eine genaue Spezifikation, wie die Daten auszusehen haben, die über das Netzwerk ausgetauscht werden. Dazu zählt unter anderem das Datenformat (z.B. Text oder Binär), die Struktur der Nachrichten oder die Abfolge der Nachrichten. Dadurch, dass das Protokoll genau definiert ist, ist es letztendlich egal, welche Betriebssysteme oder Hardwarearchitekturen miteinander verbunden sind, sofern sie nur die Sprache des Protokolls beherrschen.

Das Internet basiert auf *offenen Protokollen*, also Protokollen, deren Spezifikation jedem zugänglich ist. Diese Protokolle werden von der *Internet Engineering Task Force (IETF)* definiert. Will eine Person oder eine Firma ein neues Protokoll vorschlagen, so entwickelt es das Protokoll zunächst in Form von Internet-Drafts (Entwürfen).

Ist ein Draft dann ausgereift, so wird er im Erfolgsfall zu einem *Proposed Internet Standard*, der in einem *RFC* (Request for Comment) definiert wird. Einem RFC ist ein Status zugeordnet, der besagt, inwiefern der Inhalt des RFCs maßgeblich ist:

INFORMATIONAL Nicht bindend, nur zur Information.

1.1 Übersicht über die Standard-Netzwerkprotokolle und -Dienste

BEST CURRENT PRACTICE (Bestes derzeitiges Vorgehen) Zu dem Thema ist noch keine endgültige Entscheidung gefallen. Das vorliegende Dokument stellt die beste derzeit bekannte Vorgehensweise dar.

EXPERIMENTAL (Experimentell) Das in dem betreffenden Dokument beschriebene Protokoll ist noch nicht ausgereift.

DRAFT STANDARD (Standard-Entwurf) Das vorliegende Dokument beschreibt den Entwurf für einen kommenden Standard.

PROPOSED STANDARD (Vorgeschlagener Standard) Das betreffende Dokument definiert einen Vorschlag für einen Internet-Standard.

STANDARD Das vorliegende Dokument definiert einen offiziellen Internet-Standard.

Ein Protokoll ist das Mittel zum Zweck, im Internet einen bestimmten Dienst zu erbringen. Wie im Restaurant-Beispiel gibt es für jeden Dienst ein für diesen Dienst zugeschnittenes Protokoll. Fast immer erbringt eine Seite (der *Server*) einen Dienst, und die andere Seite (der *Client*) nimmt den Dienst des Servers in Anspruch. Im Falle des Restaurants ist der Kellner der Server und die Gäste sind die Clients.

Im Folgenden lernen wir, welche Protokolle für den Ablauf der bekanntesten Internet-Dienste zuständig sind.

Standard-Netzwerkdienste

Benutzer	System
HTTP (Web)	DHCP
SMTP (E-Mail)	SNMP
FTP	DNS
NNTP (News)	NFS
Telnet	NIS
SSH (Secure Shell)	LPD

Diese Protokolle lassen sich in Benutzer- und System-Protokolle unterteilen.

Benutzer-Protokolle gehören zu Diensten, mit denen der Benutzer direkt in Kontakt kommt, während System-Protokolle zu Diensten gehören, die im Hintergrund für das System wichtige Dienste leisten, ohne dass der Benutzer etwas bewusst davon wahrnimmt.

HTTP (*Hypertext-Transfer-Protocol*) Das wohl bekannteste und meistgenutzte Protokoll im Internet.

Mittels der Seitenbeschreibungssprache *HTML* lassen sich aus Bildern, Text und Multimediaobjekten Web-Seiten mit Hyperlinks erzeugen. HTTP dient als

Übertragungsprotokoll für diese Web-Seiten. Alle Web-Seiten im Internet bilden das *World Wide Web* (WWW).

Web-Seiten können über Verweise, die so genannten Hyperlinks, auf andere Web-Seiten verweisen, die auf der anderen Seite des Globus gespeichert sind.

Die Anwendungsmöglichkeiten im Unternehmen sind sehr vielfältig: Präsentationen, Werbung, Wissensaustausch und -management, Schnittstelle für Datenbankabfragen, und so weiter. Dadurch, dass man Web-Seiten bequem per Mausklicks bedienen kann, ist das WWW neben E-Mail der wohl am häufigsten genutzte Internetdienst.

SMTP, POP3 und IMAP Diese drei Protokolle haben mit dem Versenden (SMTP) und der Auslieferung (POP3 oder IMAP) von E-Mails zu tun. Über E-Mail lassen sich nicht nur Texte verschicken, sondern Bilder, Klänge, Videos, etc. Bei der Fülle dieser Möglichkeiten kommt noch der Vorteil hinzu, dass die Nachricht oft nach einigen Minuten beim Empfänger angelangt ist. Dadurch, dass E-Mail so schnell und günstig ist (wenn man es mit der Papier-Post vergleicht), ist es einer der meist genutzten Dienste im Internet.

Es gibt eigentlich kein Unternehmen, das ohne E-Mail auskommt, denn für die Kommunikation im Unternehmen ist es unentbehrlich; beispielsweise lassen sich für Teams bequem Mailinglisten einrichten, d.h. schickt ein Teilnehmer eine Mail an diese Liste, wird sie automatisch allen Mitgliedern zugestellt.

Zum Senden von E-Mail dient das *Simple Mail Transfer Protocol* (SMTP) und zum Empfang wird oft das *Post Office Protocol* (POP3) oder IMAP verwendet.

FTP Das *File Transfer Protocol* ist für die Übertragung von Dateien zuständig. Häufigster Anwendungsfall: Die Einrichtung so genannter *anonymous-ftp-server*, auf denen man allen Mitgliedern eines Netzwerks (auch des Internet) Dateien zum Download anbieten kann. Jedoch kann man es auch zur Dateiübertragung privater Dateien verwenden. (Zum Beispiel Hochladen der eigenen Web-Seite zum Provider.) Dafür ist aber ein gültiges Benutzerkonto mit Usernamen und Passwort auf dem entfernten Rechner notwendig.

Vorsicht ist jedoch geboten: alle übertragenen Daten, einschließlich der Passworte werden unverschlüsselt übertragen. In unsicheren Netzwerken sind sichere Protokolle wie *Secure FTP* (SFTP) oder *Secure Copy* (SCP) vorzuziehen.

NNTP ist das zugrundeliegende Protokoll der Newsgroups. Sie werden oft mit „schwarzen Brettern“ verglichen. In diesen Diskussionsforen unterhalten sich die Menschen jeweils zu einem bestimmten Thema. Da es mittlerweile über 20.000 solcher Newsgroups gibt, kann man quasi auf Knopfdruck eine Antwort auf fast jede erdenkliche Frage bekommen. *Aber Vorsicht:* Da einige Fragen besonders häufig vorkommen, sind es die Abonnenten einer solchen Newsgroup

1.1 Übersicht über die Standard-Netzwerkprotokolle und -Dienste

längst leid, sie immer wieder beantworten zu müssen. Daher existieren Textdateien, die so genannten *FAQs* (Frequently Asked Questions), in denen die häufig gestellten Fragen und Antworten zusammengefasst sind.

Dieser Protokoll ist besonders für Systemadministratoren interessant, die sich immer über die Neuigkeiten zu den Themen Sicherheit, Konfiguration, usw. informieren können.



Beispiele:

```
comp.os.linux.security
comp.os.linux.setup
comp.os.linux.networking
```

Telnet und SSH sind zwei Protokolle, mit deren Hilfe man via Netzwerk einen anderen Rechner im Textterminal fernbedienen kann. Warum gibt es jetzt *zwei* Protokolle? Das hat historische Gründe; **telnet** war zuerst da, hatte jedoch den gravierenden Nachteil, dass jedwede Datenübertragung unverschlüsselt abläuft. Mittels eines Netzwerkmonitors wie **tcpdump**, oder komfortabler, **wireshark** lassen sich also alle Ein- und Ausgaben mitlesen, insbesondere Passwörter. Deswegen soll **telnet** möglichst nicht mehr verwendet werden.

Die Secure Shell **ssh** benutzt stattdessen starke Verschlüsselung. Es ist eine freie Version von **ssh**-Server und Client verfügbar. Noch ein weiteres Feature ist sehr interessant: Man kann das X-Window-System (die netzwerkfähige grafische Oberfläche von UNIX) durch eine mit **ssh** verschlüsselte Leitung tunneln, so dass man einen Rechner per grafische Oberfläche im Netz fernsteuern kann.

DHCP *Dynamic Host Configuration Protocol*. Die Netzwerkkonfiguration von Rechnern lässt sich damit zentral auf einem Rechner bewerkstelligen. Das erspart einem die lästige „Turnschuh-Administration“, nämlich von Rechner zu Rechner laufen zu müssen, um deren Konfiguration umzustellen.

SNMP *Simple Network Management Protocol* ist ebenfalls ein Segen für den Netzwerkadministrator. Damit ist es möglich, die Auslastung und Statusinformationen (System läuft, Uptime des Systems, laufende Systemdienste) eines ganzen Netzwerks zu überwachen und die Konfiguration einzelner Rechner bequem zu ändern. Aber Vorsicht: ein schlecht konfigurierter SNMP-Dienst zählt zu den häufigsten Sicherheitslücken überhaupt.

DNS *Domain Name Service*. Da sich Menschen (zumindest normale Menschen...) IP-Adressen schlecht merken können, wurde der DNS erfunden. Er wirkt wie ein elektronisches Telefonbuch, in dem anhand des Rechnernamens die IP-Adresse¹

¹IP-Adressen sind die „Hausnummern“ von Rechnern im Internet

des Zielrechners nachgeschlagen werden kann. Auch der umgekehrte Weg (IP-Adresse→Rechnername) ist möglich. Schließlich spielt der DNS für die Auslieferung von E-Mails eine wichtige Rolle, da im DNS die zu einer E-Mail-Adresse zugehörigen Mailserver nachgeschlagen werden können.

RPC Entfernte Funktionsaufrufe (*RPC: Remote Procedure Calls*), werden durch das **rpc.portmap**-Programm implementiert, welcher dynamisch IP-Ports für diese Prozeduraufrufe zuweist (daher der Name). RPC ist für den Betrieb von NFS und NIS notwendig.

NFS Das von Sun entwickelte *Networking File System* stellt den de-facto-Standard dar, um Dateisysteme in der UNIX-Welt freizugeben. Jedoch auch für die Windows-Welt existieren NFS-Clients.

NIS Ebenfalls von Sun entwickelt wurde der *Network Information Service*. Er wird ausschließlich in UNIX-Netzen verwendet und dient meist dazu, Konfigurationsdatenbanken wie, z.B., die `/etc/passwd` netzwerkweit zentral zu verwalten. Damit wird es möglich, dass man die Benutzerinformationen und die Passwörter nur noch in einer einzigen, zentralen Benutzerdatenbank pflegen muss. Ein NIS-Server ist damit ein Authentifizierungsserver, was die Standardanwendung von NIS ist. Ein NIS-Server kann auch noch andere Daten, wie zum Beispiel die Standard-Zeitzone oder beliebige, benutzerdefinierte Daten zur Verfügung stellen. NIS findet man meistens nur in reinen UNIX/Linux-Umgebungen.

Das Protokoll *LDAP (Lightweight Directory Access Protocol)*² ist derzeit sehr stark als Nachfolger von NIS auf dem Vormarsch. Es ist sowohl deutlich flexibler als auch sicherer und ist in heterogenen Netzwerken als gemeinsamer Standard sehr verbreitet. Nicht zuletzt ist LDAP die Schnittstelle zum Microsoft Active Directory und zu den Novell Directory Services, die eine ähnliche, wenn auch komplexere, Aufgabe wie NIS erfüllen.

LPD Ist der Standard-Druckserver unter UNIX (*line printer daemon*). Mit diesem ist es möglich, Druckerwarteschlangen zu importieren und zu exportieren. `lpd` kümmert sich natürlich auch um lokale Druckaufträge. Das Protokoll ist in RFC 1179 beschrieben. Als Nachfolger dieses sehr betagten Protokolls setzt sich das sehr moderne, auf HTTP basierende *Internet Printing Protokoll (IPP)* durch, das Features wie automatische Druckservererkennung oder Verschlüsselung bietet.

²Zu LDAP siehe www.verzeichnisdienst.de

1.2 TCP/IP-Architektur

1.2.1 Schichtenmodelle

Schicken wir einen Brief mit der Post weg, so packen wir unsere „Daten“ in einen Umschlag, versehen diesen mit der Adresse des Absenders und Empfängers und werfen ihn in den Briefkasten. Dass der Brief dann ankommt, scheint für uns heute ganz normal zu sein. Das funktioniert aber nur, weil verschiedene Abteilungen der Post dafür sorgen:

- das Fahrrad/der Transporter („*Hardware*“)
- die Logistikabteilung („*Data Link*“)
- die Zustellung („*Vermittlung*“)

Ablauf: Der Absender braucht den Umschlag nur zu beschriften, ausreichend zu frankieren, alles andere erledigt die Post.

Entsprechend braucht die Zustellung nur das Porto zu prüfen und den Brief an die zuständige Zielpoststelle weiterzuleiten.

Die Logistikabteilung kümmert sich darum, dass die Briefe von Postamt zu Postamt, vom Briefkasten zum Postamt oder vom Postamt zum Empfänger gefahren werden. Der Postbote mit seinem Fahrrad kümmert sich beispielsweise um den physischen Transport zum Empfänger. Den Transport von Postamt zu Postamt übernimmt dabei ein Transporter, der größere Volumina enthalten kann („*unterschiedliche Hardware*“).

Computernetzwerke funktionieren sehr ähnlich:

- Die *Abteilungen* der Post entsprechen den *Schichten* des Netzwerkmodells.
- Wer die Protokolle einer Schicht verwendet, braucht sich um die Aufgaben der darunterliegenden Schichten nicht mehr zu kümmern.
- Innerhalb einer Schicht gibt es unterschiedliche Wege zum Ziel.

Den Brief beispielsweise interessiert es nicht, ob er mit dem Fahrrad oder mit dem Auto transportiert wird. Entsprechend interessiert es ein IP-Paket nicht, ob es über Ethernet- oder Token Ring- Netzwerkhardware zugestellt wird.

Ebenso ist ihm der Briefträger egal, entsprechend dem Ethernet- oder Token-Ring-Kommunikationsprotokoll.

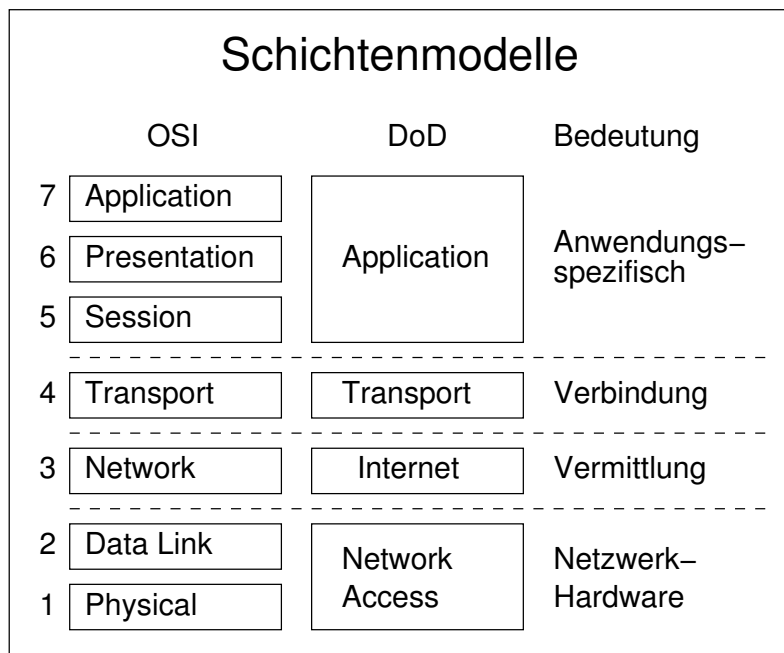
Die Ursprünge des TCP/IP-Netzwerks stammen aus dem amerikanischen Verteidigungsministerium, das Ende der 60er Jahre mit dem DARPA-Projekt den Auftrag

zur Vereinheitlichung der unterschiedlichen, bis dahin verwendeten Netzwerklösungen gab.

Später wurde daraus, unter BSD-UNIX, das TCP/IP-Protokoll. Da BSD-UNIX frei verfügbar ist und deshalb besonders an den Hochschulen eingesetzt wurde, die wiederum das Internet begründet haben, ist TCP/IP das Internetprotokoll geworden.

TCP/IP ist, wie schon der Name vermuten lässt, mehr als nur ein einziges Protokoll. Ein Netzwerkprotokoll wird i.A. immer durch mehrere Einzelprotokolle auf verschiedenen Ebenen („Schichten“) beschrieben.

Die Arbeitsteilung in der Netzwerkwelt wurde von der *ISO*, der *International Organization for Standardization* im Standard *OSI (Open Systems Interconnection)* festgelegt. Eine einfachere Aufteilung fand das amerikanische Verteidigungsministerium (*Department of Defense*), nach der die Architektur des TCP/IP-Protokolls gestaltet ist:



Das OSI-Modell wird immer verwendet, um die Funktionen zu erläutern, die ein Netzwerk klassischerweise übernimmt. Jedoch hat es sich herausgestellt, dass dieses Modell zwar sehr sauber implementiert werden kann, jedoch das Modell wegen der vielen übereinanderliegenden Schichten langsam und schwerfällig wird. Das einfachere DoD-Modell dagegen ist schneller, weil einfacher, und wurde deshalb für das Design von TCP/IP verwendet.

Physical Die *Physikalische Schicht* oder *Bitübertragungsschicht* definiert die physikalischen Eigenschaften der Übertragungswege, wie z.B.:

- Leitungen: elektrisch, optisch, Funkstrecke
- Signalpegel
- Bandbreite
- Bit-Kodierung

Data Link Die *Sicherungsschicht* sorgt für die zuverlässige Übertragung der Daten über die physikalischen Verbindungen. Sie

- stellt die zuverlässige Übertragung von *Datenpaketen (Frames)* sicher
- bildet Prüfsummen, synchronisiert, erkennt/bereinigt Fehler
- stellt Hardware-Adressen zur Verfügung, durch die alle an das physikalische Medium angeschlossenen Stationen eindeutig angesprochen werden können
- meist in zwei Ebenen unterteilt:

MAC *Medium Access Control* regelt den Zugriff auf die Leitung

LLC oder *Logical Link Control* bildet die logische Datenverbindung und agiert als Bindeglied zu Schicht 3

Network Die *Netzwerkschicht* oder *Vermittlungsschicht* verwaltet die Verbindungen zwischen Rechnern im Netz für höhere Schichten. Sie

- findet für jedes einzelne Paket den Weg vom Absender zum Empfänger übers Netz (*Routing*)
- trennt die Protokolle der oberen Schichten von den Details des darunterliegenden Netzwerks und seiner Hardware; durch diese Abstraktion erreicht man die Unabhängigkeit von der Netzwerkhardware

Transport Die *Transportschicht* garantiert die fehlerfreie Datenübertragung durch Fehlererkennung und -korrektur. Da über Computernetzwerke in der Regel nur Datenpakete (so genannte *Frames*) versendet werden können, sind auf dieser Schicht gewöhnlich zwei Protokolltypen zu Hause:

- Ein *verbindungsorientiertes Protokoll*, bei dem der Empfänger den korrekten Erhalt aller Daten quittiert. Für die meisten Zwecke werden verbindungsorientierte Protokolle verwendet. Ein Nachteil dieses Protokolltyps ist der etwas höhere Aufwand.
- Ein *verbindungsloses Protokoll*, bei dem der Empfänger den Erhalt der Daten nicht quittiert. Es wird meist nur für die Zustellung kurzer Datenpakete verwendet, bei der eine Antwort des Empfängers als Empfangsbestätigung genügt. Trifft keine Antwort ein, wird die Anfrage nochmals gesendet. Verbindungslose Protokolle sind etwas performanter.

Session oder *Kommunikationssteuerschicht*: Sie verwaltet die Verbindungen (Sessions) zwischen kooperierenden Anwendungen. Im TCP/IP-Modell (= DoD) tritt die Session-Schicht gar nicht auf, deren Aufgaben werden von der Anwendungsschicht übernommen.

Presentation Damit kooperierende Anwendungen Informationen austauschen können, müssen sie sich darüber einig sein, wie diese Daten dargestellt werden. Beim OSI-Modell stellt diese Schicht Standardroutinen bereit. Bei TCP/IP wird diese Funktion häufig innerhalb der Anwendungen ausgeführt. Zunehmend wird diese Aufgabe auch von XDR, XML oder MIME übernommen.

Application oder Anwendungsschicht. Hier tummeln sich die meisten Protokolle wie HTTP, FTP, SMTP, DNS, und so weiter. Diese nehmen die Protokolle aller unteren Schichten in Anspruch, ohne sich jedoch darum kümmern zu müssen.

Diese beiden Schichtenmodelle haben einige Gemeinsamkeiten:

- Eine Schicht bietet der darüberliegenden Schicht immer fest definierte Dienste an
- Die darüberliegende Schicht baut immer auf diesen Diensten auf, sie realisiert *nie* selbst Aufgaben, die einer anderen Schicht zuzuordnen sind
- Die Kommunikation zwischen den Schichten geschieht mittels festgelegter Protokolle (*Dienstschnittstelle*)
- Bei der Datenübertragung „unterhalten“ sich jeweils die korrespondierenden Schichten der beteiligten Netzwerkimplementationen
- Auch diese Kommunikation erfolgt nach festen Protokollen