

Kommunikations- & Netztechnik

Verbinden – Verknüpfen – Verteilen

Roman Wetenkamp

23. Oktober 2021



Inhaltsverzeichnis

I. Grundlegendes	4
1. Netzwerk	4
1.1. Kommunikationsmodelle	5
1.2. Zuverlässigkeit	5
1.3. Vermittlungskonzepte	6
1.3.1. Multiplexing	6
1.4. Aufgaben	7
2. Terminologie	7
2.1. Datenübertragungsmodi	7
2.2. Kommunikationsmodi	8
2.3. Topologien	8
2.3.1. Busnetz	8
2.3.2. Ringnetz	8
2.3.3. Sternnetz	9
2.3.4. Maschennetz	9
2.3.5. Baumnetze	9
2.3.6. Zellnetze	10
2.4. Aufgaben	11
3. Geschichte des Internets	11
4. Standardisierung	11
5. Schichtenmodelle	13
5.1. TCP/IP-Referenzmodell	13
5.2. Hybrides Referenzmodell	13
5.3. ISO/OSI-Referenzmodell	13

Vorwort

In guter Tradition zum letzten Semester wage ich mich auch jetzt wieder an ein Skript für ein Modul, für das ich es als sinnvoll erachte – Kommunikations- und Netztechnik. Hier beschäftigen wir uns mit den Grundlagen des Internets, finden heraus, durch welche Protokolle und auf welchen Ebenen Daten übertragen werden und wie wir Unternehmen und Organisationen mit einem sicheren Netzwerk ausstatten. Dieses Skript greift die Inhalte der Vorlesung auf, fasst sie zusammen und ergänzt sie dort, wo es sinnvoll ist, durch Erklärungen und Übungen. Idealerweise sind wir beide dann gut auf die Klausur vorbereitet. *Viel Erfolg!*

Roman Wetenkamp
Mannheim, den 23. Oktober 2021

Warnung Das Studium an einer Dualen Hochschule unterscheidet sich von dem Studium an Universitäten oder regulären Fachhochschulen insbesondere dadurch, dass aufgrund der Dualität von Theorie und Praxis meist nur die Hälfte der Zeit zur Vermittlung des Stoffes zur Verfügung steht (wenn dann auch intensiver). Daher gehen Sie bitte nicht davon aus, dass Sie dieses Skript ausreichend auf Klausuren in regulären Vollzeitstudiengängen vorbereitet!

Hinweis Dieses Dokument ist kein Vorlesungsmaterial, hat nicht den Anspruch auf Vollständigkeit und enthält mit Sicherheit Fehler. Desweiteren ist es noch lange nicht vollendet (es ist infrage zu stellen, ob es das je sein wird), und doch möchte ich Sie ermutigen, beizutragen! Jegliche Fehler, Probleme oder Anmerkungen können Sie mir gerne über das dazugehörige GitHub-Repository unter der URL <https://github.com/RWetenkamp/kommnet> zukommen lassen. Danke!

Einführung

Das Internet ist für uns alle Neuland – Klar, was auch sonst, dieses unförmige, kaum verständliche Ding, das uns ermöglicht, uns über Länder- und Kontinentalgrenzen zu vernetzen und Informationen von überall auf der Welt zu beziehen, muss Neuland sein. Sicherlich auch für alle und nicht nur für eine konservative, leicht hinterherhinkende Regierungspartei. Doch genug der politischen Spitzen, besinnen wir uns lieber darauf, was es wirklich ist: Längst ist das Internet fundamentaler und integraler Bestandteil unseres Alltags. Gerade durch die Corona-Pandemie zeigte es sich auf so eindrucksvolle Weise: Online-Konzerte, Online-Unterricht, Online-Konferenzen. Längst wurde es für quasi alle Teile der Bevölkerung unabdingbar, sich einen Zugang zum Internet zu einzurichten und teilzunehmen.

Für Anwender*innen reicht es dabei völlig aus, einen Webbrowser oder internetfähige Applikationen bedienen zu können – zumindest bis irgendetwas nicht funktioniert. „Oh je, ich habe das Internet gelöscht!“ und „Mein WLAN funktioniert nicht mehr!“, vielleicht kennen Sie diese oder ähnliche sonderbare Aussprüche aus Ihrem Familien- oder Bekanntenkreis.

Mit diesem Modul und Skript wollen wir einen Blick hinter die Kulissen wagen und verstehen, wo die Unterschiede zwischen 404, 500 und 201 liegen, wann UDP TCP vorzuziehen ist und warum es sich wirklich nicht lohnt, in einem Elektronikmarkt nach einem WLAN-Kabel zu fragen. Doch beginnen wir mit den grundlegenden Begriffen und Definitionen.

Teil I. Grundlegendes

1. Netzwerk

Definition 1. *Ein Netzwerk besteht aus mindestens zwei **Endgeräten** mit Netzwerkdiensten, einem **Übertragungsmedium** und **Netzwerkprotokollen**.*

Das Übertragungsmedium kann dabei leitungsgebunden (z.B. Kupferkabel oder Glasfaser) oder nicht-leitungsgebunden (z.B. durch Funkwellen) sein. Die Art und Weise, wie die Endgeräte über dieses Medium kommunizieren, ist in Netzwerkprotokollen festgelegt – fast wie überregulierte Dating-Konventionen: Wer geht den ersten Schritt? Wie muss ich dich nach einem Treffen fragen? Und muss ich jedes Mal nachhaken, ob du noch an mir interessiert bist oder sind wir das solange, bis du widersprichst?

Definition 2. *Protokolle definieren das Format und die Reihenfolge, in der Nachrichten von Systemen im Netzwerk gesendet und empfangen werden sowie die Aktionen, die durch die Nachrichten ausgelöst werden.*

Für verschiedenste Anwendungsfälle kommen unterschiedliche Protokolle zum Einsatz – manche mit dem Ziel, möglichst schnell viele Informationen zu übertragen, manche mit dem Ziel, verlustfrei ganz sicher zu gehen und nichts zu riskieren. Wir werden die verschiedenen Protokolle später in aller Ausführlichkeit thematisieren.

Definition 3. *Das Internet ist ein hierarchisch aufgebautes Netzwerk von Netzwerken.*

Des Weiteren lassen sich die Begriffe Internet und Intranet unterscheiden:

- **Intranet** bezeichnet ein von außen nicht zugängliches, abgeschlossenes Netzwerk eines Unternehmens oder einer Institution (Zugang z.B. über VPN)
- **Internet** bezeichnet das öffentlich zugängliche, von überall aus erreichbare Netzwerk von Netzwerken.

Definition 4. *Ein Dienst bezeichnet eine Kommunikationsinfrastruktur, die verteilte Anwendungen ermöglicht.*

Beispiele für Dienste sind E-Mail, Voice-over-IP oder Streaming. Diese Dienste kommunizieren dabei meistens über TCP oder UDP.

1.1. Kommunikationsmodelle

1. Client-Server-Modell

Im Client-Server-Modell ist genau festgelegt, welches Gerät anfragend und welches antwortend ist. Der **Client** ist hierbei das Endgerät, z.B. ein Laptop, ein Smartphone oder ein Desktop-Rechner, von dem eine Anfrage nach einer bestimmten Ressource abgeschickt wird. Der **Server** ist ein dauerhaft betriebener Rechner, der von sich aus keine Anfragen an Clients absendet, sondern lediglich die Anfragen der Clients beantwortet und die angefragten Ressourcen zurücksendet. Ein Beispiel für dieses Modell ist die Kommunikation per E-Mail.

2. Peer-to-Peer-Kommunikation

In diesem Modell kommunizieren zwei typidentische Endgeräte miteinander. Beide Geräte können Anfragen stellen und ebenso auch angefragte Daten / Ressourcen zurücksenden. Hierbei werden (fast) keine zentralen Server eingesetzt, die Kommunikation zwischen den Geräten erfolgt weitgehend autonom. Ein Beispiel für dieses Modell liefert die Internettelefonie per Skype.

1.2. Zuverlässigkeit

Protokolle besitzen verschiedene Eigenschaften. Je nach beabsichtigtem Einsatzzweck entscheiden diese Eigenschaften, welches Protokoll verwendet wird. Eine wesentliche Eigenschaft ist die **Übertragungszuverlässigkeit**.

TCP-Dienste Bei TCP wird eine zuverlässige Datenübertragung gewährleistet, die auch die Reihenfolge von Paketen erhält. Sollte ein Paket verloren werden, wird die entsprechende Übertragung wiederholt. Dafür ist ein vorgeschaltetes Handshaking nötig. TCP enthält außerdem eine Fluss- und Überlastkontrolle, um den Netzverkehr steuern zu können. TCP wird in vielen Fällen eingesetzt, wo die Zuverlässigkeit der Übertragung einen höheren Stellenwert als die Geschwindigkeit (also die Bandbreite) hat. [**RFC793**]

UDP-Dienste Das Protokoll UDP ist hingegen verbindungslos, folglich findet auch kein Handshaking statt. Der Datenverkehr mittels UDP verläuft unzuverlässiger. Ebenso ist keine Fluss- oder Überlastkontrolle enthalten. UDP wird insbesondere dann eingesetzt, wenn die Übertragungszeit wichtiger ist als die Vollständigkeit und Verlustfreiheit, beispielsweise bei (Video-)telefonie- oder Gaming-Anwendungen. Dieses Prinzip bezeichnen wir auch als **best effort**-Konzept. [**RFC768**]

1.3. Vermittlungskonzepte

Neben verschiedenen Protokollen muss auch ein Vermittlungskonzept gewählt werden, dass insbesondere dann zum Einsatz kommt, wenn mehrere Clients gleichzeitig einen Übermittlungskanal nutzen (können). Wir unterscheiden hierbei zwei wesentliche Konzepte:

- **Leitungsbasierte Vermittlung:** Für jede Verbindung ist eine eigene Leitung erforderlich, also können nicht mehrere Endgeräte gleichzeitig über eine Leitung kommunizieren. Dies ist beispielsweise im Telefonnetz der Fall: Dass ein Endgerät gleichzeitig mit mehreren anderen Endgeräten kommuniziert ist hier weder erwünscht noch möglich.
Grundlage für die Kommunikation ist das Reservieren der Ressourcen von Ende-zu-Ende. Diese Ressourcen sind fest dieser Verbindung zugeordnet und stehen somit nur für diese zur Verfügung. Dadurch wird die Dienstgüte (Quality of Service) garantiert.
- **Paketbasierte Vermittlung:** Im Gegensatz dazu wird in diesem Ansatz die Kommunikation in Datenpakete eingeteilt, die einzeln übertragen werden. So können sich mehrere Verbindungen eine Leitung teilen, da jedes Paket Informationen enthält, um es später zuzuordnen zu können. Bei diesem Ansatz kann die volle Bandbreite ausgenutzt werden.

1.3.1. Multiplexing

Für die paketbasierte Vermittlung ist das Konzept Multiplexing entscheidend. Hier werden Netzwerkressourcen in Einheiten aufgeteilt und diese jeweils den Verbindungen zugeteilt. Dafür gibt es zwei unterschiedliche Ansätze:

- **Frequency Division Multiplex (FDM)** Bei diesem Ansatz wird die zur Verfügung stehende Frequenz aufgeteilt, sodass Pakete zwar parallel und gleichförmig übertragen werden können, jedoch nur mit einem Bruchteil der zur Verfügung stehenden Bandbreite.

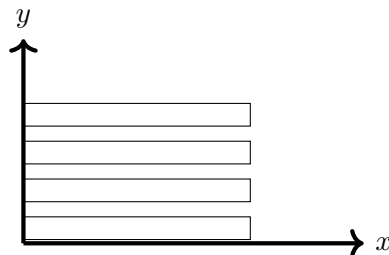


Abbildung 1: Frequency Division Multiplex

- **Time Division Multiplex (TDM)** Alternativ dazu kann auch die Zeit geteilt werden: Pakete erhalten nun die volle Bandbreite, können jedoch nicht kontinuierlich unterbrechungsfrei aneinandergereiht versendet werden, sondern werden mit Paketen anderer Verbindungen in einer Reihenfolge abwechselnd übertragen. Das Verfahren der Paketvermittlung ist insbesondere für unregelmäßigen Datenverkehr geeigneter, da die Aufteilung der Ressourcen dort flexibler gehandhabt werden kann. Ein Router empfängt ein Paket komplett, bevor es in einer Warteschlange zwischengespeichert wird und bei Freigabe der Leitung weitergesendet wird. Beim **statistischen Multiplexing** gibt es kein festes Muster der Paketfolge.

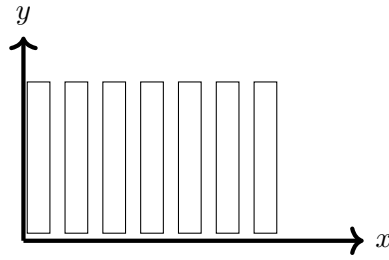


Abbildung 2: Time Division Multiplex

Als **Teilstreckenverfahren** oder **Store and Forward** wird die Technik bezeichnet, bei der ein Paket von Knoten zu Knoten gesendet wird und an jedem Knoten erneut auf die Freigabe der nachfolgenden Teilstrecke warten muss. Ein Paket erhält folglich nicht die Freigabe, den gesamten Weg zurückzulegen, sondern wird in einzelnen Teilstrecken übertragen. Erst nachdem ein Paket vollständig übertragen wurde, wird es auf die nächste Leitung übertragen. Die Dauer einer Paketübertragung lässt sich berechnen:

$$\frac{\text{Paketgröße in Bits}}{\text{Übertragungsrate in Bits pro Sekunde}} = \text{Zeitdauer in Sekunden}$$

1.4. Aufgaben

Aufgabe 1 Berechnen Sie die Übertragungsdauer bzw. Dateigröße jeweils.

- 256 Megabit auf einer 1 GBit/s-Leitung
- 32 Megabyte auf einer 16 MBit/s-Leitung
- 12 Sekunden Übertragungsdauer auf einer 250 MBit/s-Leitung

Aufgabe 2 Erläutern Sie die Unterschiede zwischen FDM und TDM.

Aufgabe 3 Sie entwickeln eine Webanwendung für Online-Vorlesungen in Echtzeit. Wählen Sie ein geeignetes Protokoll und begründen Sie Ihre Wahl.

2. Terminologie

In diesem nun folgenden Teil widmen wir uns einigen, relevanten Begrifflichkeiten.

2.1. Datenübertragungsmodi

Parallele Datenübertragung bezeichnet das Verfahren, bei dem die Übertragung der Bits auf mehreren Datenleitungen parallel erfolgt. Zusätzlich sind Steuerleitungen vorhanden. Dadurch kann ein hoher Datendurchsatz erreicht werden, wobei jedoch viele Leitungen nötig sind. Dieses Verfahren findet in internen und lokalen Bus-Systemen Anwendung.

Serielle Datenübertragung hingegen bezeichnet das Verfahren, bei dem die Daten auf einer Leitung nacheinander übertragen werden. Dieses Verfahren erreicht logischerweise einen geringeren Datendurchsatz, ist jedoch auch für größere Distanzen geeignet. Es findet Anwendung in internen Bus-Systemen und Computernetzwerken.

2.2. Kommunikationsmodi

simplex bezeichnet eine Übertragung, die nur in eine Richtung stattfindet. Also beispielsweise Radio oder Fernsehen. Die Daten können empfangen werden, doch es können keine Daten zurückgesendet werden.

half-duplex hingegen ist die Möglichkeit, Daten in beide Richtungen zu übertragen, jedoch nicht gleichzeitig. Das ist beispielsweise bei Netzwerken mit Twisted-Pair-Verkabelung der Fall.

duplex ist nun die Königsklasse: Übertragung gleichzeitig in beide Richtungen, wie beispielsweise durch ein Glasfaserkabel.

2.3. Topologien

Als Topologien bezeichnen wir Strukturen der Anordnung und Verkabelung von Kommunikationspartnern mit dem Ziel, die Ausfallsicherheit und auch die Verfügbarkeit eines Netzes zu maximieren. Häufig werden die klassischen Strukturen - insbesondere in größeren Netzen - vermischt.

Wir unterscheiden die **physische** und die **logische Topologie**. Während die physische Topologie den Aufbau der Verkabelung beschreibt, bestimmt die logische Topologie den Datenfluss zwischen den Endgeräten.

2.3.1. Busnetz

In einem Bus-Netz sind alle Knoten über ein Medium verbunden. Fällt ein Knoten aus, führt das nicht zum Ausfall des gesamten Netzes. Allerdings kann in dieser Topologie immer nur ein Teilnehmer Daten senden. Die Kosten für ein Busnetz sind vergleichsweise gering, allerdings ist das Netz fehleranfällig und die Bandbreite wird auf alle Teilnehmer aufgeteilt. Wird der Bus an einem Punkt unterbrochen, führt das zum Ausfall des Netzes.

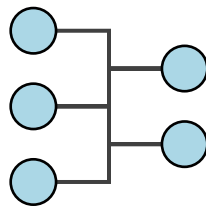


Abbildung 3: Busnetz-Topologie

2.3.2. Ringnetz

In einem Ringnetz hingegen gibt es kein zentrales Medium, über den der Datenverkehr weitergeleitet wird. Stattdessen ist jeder Knoten mit seinen Nachbarn verbunden, sodass ein Ring entsteht. Der Datenverkehr passiert nun alle erforderlichen Endpunkte bei der Übertragung. Dadurch wird das Signal verstärkt und kann sich regenerieren, gleichzeitig ist diese Vorgehensweise sehr störanfällig. Ebenso wird die Bandbreite währenddessen geteilt. Das Ringnetz findet beispielsweise im Token-Ring-LAN Anwendung.

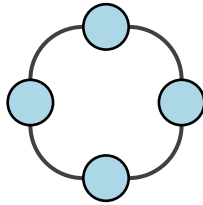


Abbildung 4: Ringnetz-Topologie

2.3.3. Sternnetz

Die dritte mögliche Topologie verläuft nun über eine zentrale Komponente, einen Switch. Jeder Knoten unterhält eine eigenständige Verbindung zur zentralen Komponente und diese ist nun dafür verantwortlich, die Datenpakete passend weiterzuleiten. Der Vorteil dieser Topologie liegt in der Übersichtlichkeit. Gleichzeitig besteht eine Abhängigkeit von der zentralen Komponente: Fällt diese aus, ist logischerweise kein Datenverkehr mehr möglich. Diese Topologie wird in Datennetzen häufig eingesetzt.

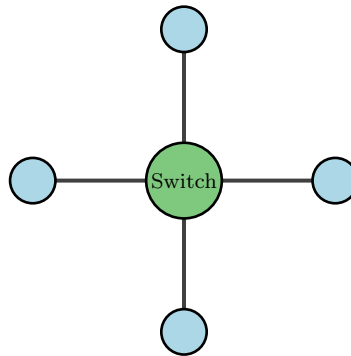


Abbildung 5: Sternnetz-Topologie

2.3.4. Maschennetz

Um die Ausfallsicherheit zu erhöhen, bleibt als Ansatz noch die Vermaschung, entweder vollständig oder teilweise. Hierbei werden zusätzliche Redundanzen eingefügt und entweder jeder Knoten mit jedem übrigen verbunden oder zumindest die am stärksten frequentierten miteinander. Hierfür sind mehr Datenverbindungen erforderlich, jedoch führt der Ausfall eines Knotens nicht zum Totalausfall des gesamten Netzes, da alternative Wege gefunden werden können.

2.3.5. Baumnetze

Als nächste Topologieoption betrachten wir die Verknüpfung mehrerer Maschennetze zu sogenannten Baumnetzen. Der Gedanke hier ist, die Verbindung zwischen mehreren Netzen über Koppelglieder herzustellen, um Kosten zu sparen. Der Nachteil hierbei liegt in der Fehleranfälligkeit. Ebenso wird die Bandbreite geteilt und der Vorteil des Maschennetzes, über Redundanzen die Ausfallsicherheit zu gewährleisten, entfällt. Diese Topologie findet beispielsweise in Breitbandkabelnetzen Einsatz.

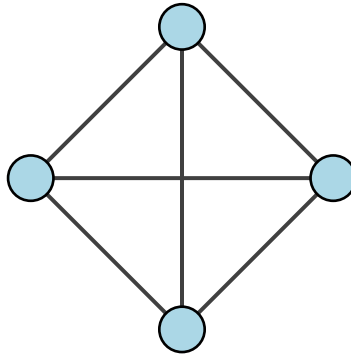


Abbildung 6: Maschennetz-Topologie (teilvermascht)

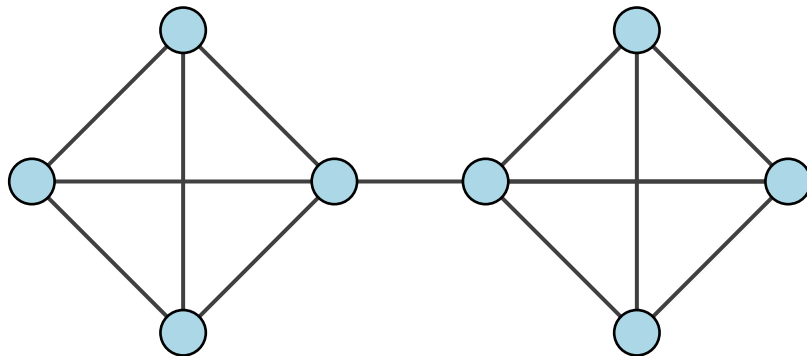


Abbildung 7: Baumnetz-Topologie

2.3.6. Zellnetze

Während die vorangegangenen Topologien Leitungen als Verbindungsmedium nutzen, betrachten wir nun eine Topologie, die Funkwellen nutzt. Diese Topologie samt ihrer Vor- und Nachteile ist vermutlich dem Großteil der Bevölkerung bekannt, da sowohl das Mobilfunknetz als auch WLANs auf diese Weise aufgebaut sind. Mehrere Basisstationen senden radial Funkwellen aus und überlappen sich gegenseitig, um die Vernetzung herzustellen. Dabei ist die Reichweite jeder Basisstation begrenzt. Der Vorteil liegt darin, dass keine Leitungen nötig sind und auch hier durch das Überlappen mehrerer Zellen Redundanzen geschaffen werden können. Während früher häufig Bus- und Ringnetze zum Einsatz kamen,

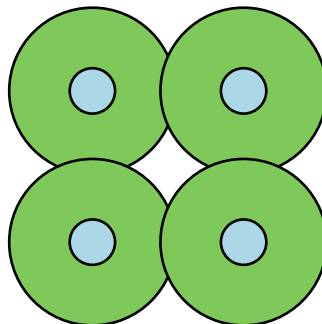


Abbildung 8: Zellnetz-Topologie

werden heute häufig Maschennetze für Funknetze und Routerverbindungen genutzt, für Ethernet finden Stern- und Baumnetze Einsatz. Je nach Anwendungsfall und Rahmenbe-

dingungen bieten sich andere Topologien an. Die „ideale“ Topologie für alle Einsatzzwecke gibt es folglich nicht.

PAN	Personal Area Network	Bis zu 100 Meter Ausdehnung (z.B. Bluetooth)
LAN	Local Area Network	Bis zu 10 Kilometer Ausdehnung (z.B. Verkabelung innerhalb von Gebäuden)
MAN	Metropolitan Area Network	Bis zu 50 Kilometer Ausdehnung (z.B. städtisches Netz)
WAN	Wide Area Network	Ausdehnung über 10 Kilometer (z.B. Campus-Netze großer Firmen)
GAN	Global Area Network	Interkontinentale Netzwerke (z.B. Internet)

Tabelle 1: Typische Ausdehnungen von Netzwerken

2.4. Aufgaben

Aufgabe 1 Entscheiden und begründen Sie, welche Kommunikationsmodi in folgenden Szenarien verwendet werden.

- Menschliche Kommunikation im Zwiegespräch
- Spannungsübertragung zwischen Plus- und Minuspol einer Batterie
- Kommunikation über Funkgeräte (Walkie-Talkies)

Aufgabe 2 Erläutern Sie die Begriffe Redundanz und Ausfallsicherheit anhand der dargestellten Netztopologien.

Aufgabe 3 Entscheiden und begründen Sie, inwiefern sich Baumnetze auch aus anderen Netztopologien als vermaschten Netzen zusammensetzen ließen. Gehen Sie auf mögliche Vor- und Nachteile ein.

3. Geschichte des Internets

Nun betrachten wir kurz die Geschichte des Internets anhand einer Zeittafel.

4. Standardisierung

Was wäre das Internet, wenn jeder Server und jeder Client eine eigene, andere Sprache spräche? Interkulturelle Differenzen und Missverständnisse bezögen sich nicht mehr ausschließlich auf den Inhalt unserer Datenpakete, sondern wir wären gar nicht mehr in der Lage, jene zu erkennen, da die Datenpakete mit relativ hoher Wahrscheinlichkeit gar nicht korrekt übermittelt und empfangen werden würden. Deshalb wurde das Internet hochgradig standardisiert. Im Folgenden werden kurz vier relevante Organisationen vorgestellt, die an der Normung und Definition von Standards im Internet mitwirken.

- 1967 Die Advanced Research Projects Agency plant das ARPANet, danach rein universitäre Ziele.
- 1969 Der erste ARPANet-Knoten geht in Betrieb
- 1972 Das ARPANet wird vorgestellt, mitsamt des NCP (Network Control Protocol) als erstes Protokoll zwischen Hosts
- 1979 Das ARPANet wächst weiter und hat nun 200 Knoten. Parallel dazu entstehen proprietäre Architekturen wie DECnet, SNA und XNA
- 1981 TCP/IP wird eingeführt
- 1982 Das SMTP-Protokoll für E-Mails wird definiert
- 1983 Das DNS zur Übersetzung von Namen zu IP-Adressen wird definiert
- 1990 Das ARPANet wird eingestellt, Hypertext (damit HTML, HTTP) wird entwickelt
- 2007 Das Internet verzeichnet 1.4 Millionen Nutzer und Anwendungen wie VoIP entstehen
- 2019 Nun nutzen > 4 Millionen Menschen das Internet und das Anwendungsspektrum hat sich signifikant erweitert.

Tabelle 2: Geschichte des Internets

International Organization for Standardization (ISO) ist eine Agentur der vereinten Nationen, die in einer Vielzahl verschiedenster Bereiche Normen und Standards festlegt, so zum Beispiel auch im Bereich der IT-Sicherheit oder bei Spannungsschutzvorrichtungen bei elektronischen Geräten. In Bezug auf Telekommunikationssysteme sollte vorrangig das **ISO/OSI-Modell** genannt werden, dass als Referenzmodell verschiedene Schichten unterscheidet, in die sich die Kommunikation einteilen lässt. Dieses Modell betrachten wir später genauer.

International Telecommunications Union (ITU) ist ebenfalls ein UN-Organ, das weltweit die Koordination der Telekommunikation übernimmt. Zur ITU gehören die Definitionen von ATM, ISDN, V.24 und Carrier Ethernet.

Institute of Electrical and Electronics Engineering (IEEE) ist eines der wichtigsten Standardisierungsgremien für das Internet. Vermutlich haben Sie in Ihrem Studium auch bereits mindestens ein IEEE-Paper gelesen. Die IEEE standardisiert insbesondere auch WLAN, dort beispielsweise im Standard IEEE 802.11n.

Internet Engineering Task Force (IETF) definiert Internet-Standards, insbesondere Protokolle, in sogenannten RFC (Request for Comments). Hier sind Protokolle wie TCP, HTTP, FTP, Telnet, SSH oder VXLAN definiert und standardisiert.

Eine klare Trennung und Zuordnung wäre sicher wünschenswert, gelingt aber nur mit mittlerem Erfolg. Vereinfacht kann festgehalten werden, dass die ISO auf abstrakter Ebene Normen festlegt, die ITU sich hauptsächlich auf Telefonie und Telekommunikation beschränkt, die IEEE hardwarenähere Standards wie WLAN definiert und die IETF Dienste und Protokolle beschreibt.

5. Schichtenmodelle

Wir wollen die Betrachtung von Netzwerken und Kommunikationsvorgängen nun dadurch vereinfachen und strukturieren, dass wir verschiedene Schichten unterscheiden, denen mehrere spezifizierte Aufgaben und Protokolle zugeordnet sind. Diese Strukturierung erleichtert einerseits unsere Kommunikation über die Prozesse, sorgt jedoch auch dafür, dass die Sicherheit und Wartbarkeit des Netzes insgesamt erhöht wird, da die Daten der einzelnen Schichten gekapselt werden. Beginnen wir mit dem ältesten und einfachsten Referenzmodell, dem TCP/IP-Modell.

5.1. TCP/IP-Referenzmodell

Dieses Modell entstammt dem Department of Defense der USA und wurde im Rahmen des ARPAnets entwickelt. Es werden vier Schichten unterschieden: Ein Datenpaket wird

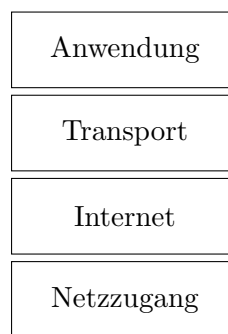


Abbildung 9: TCP/IP-Referenzmodell

in der Anwendungsschicht erzeugt und nun mittels eines Protokolls wie HTTP, FTP, SMTP, POP3 oder SMTP an die Transportschicht übertragen. Hier wird dem Paket ein zusätzlicher TCP- oder UDP-Header hinzugefügt, bevor es an die physische Infrastruktur weitergeleitet wird. Das Datenpaket wird nun zum IP-Paket und betritt die Netzwerkinfrastruktur zwischen Client und Server, wo es mittels Ethernet, WLAN oder weiteren Protokollen weiter übertragen wird. Erreicht es den Zielservers, werden die Schichten dort in umgekehrter Reihenfolge erneut durchlaufen, bis die Zielanwendung das Paket verarbeiten kann.

5.2. Hybrides Referenzmodell

Um noch genauer zu werden und detailliertere Aussagen zu treffen, erweitern wir das TCP/IP-Modell, indem die Netzzugangsschicht nun in zwei Schichten aufgeteilt wird. Die Sicherungsschicht beschreibt nun den Datentransfer zwischen benachbarten Netzwerksystemen, zum Beispiel über Ethernet. Die Bitübertragungsschicht stellt nun ganz rudimentär nur die tatsächliche Übertragung einzelner Bits auf einer Leitung dar.

5.3. ISO/OSI-Referenzmodell

Um zum heute noch verbreiteten Standardmodell zu gelangen, fügen wir ebenfalls zwei weitere Schichten in das Modell hinzu.

- Die **Darstellungsschicht** ermöglicht es Anwendungen, die Daten zu interpretieren und zu modifizieren, also beispielsweise zu verschlüsseln oder zu komprimieren.

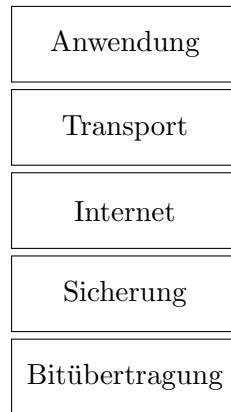


Abbildung 10: Hybrides Referenzmodell

- Die **Kommunikationssteuerschicht** synchronisiert die Daten und setzt beispielsweise Wiederherstellungspunkte.

Diese Funktionalitäten müssen jeweils von den Anwendungen implementiert werden, da sie nicht zum eigentlichen Protokollstapel des Internets gehören. Wie erhalten das folgende Modell:



Abbildung 11: ISO/OSI-Referenzmodell