Die Internetprotokollfamilie

Werner-von-Siemens-Gymnasium Magdeburg
Schuljahr: 2014 / 2015
Fach: Informatik
Fachlehrer: Herr Thormeyer
Verfasser: Jonas Pietsch
Facharbeit zum Thema: Die Internetprotokollfamilie

Gliederung

1 Einleitung

Die Internetprotokollfamilie ist eine Familie von rund 500 Netzwerkprotokollen, die alle miteinander in einer hierarchisch-vernetzten Beziehung zueinander stehen. Diese Protokolle bilden die Basis für die Netzwerkkommunikation im Internet. Synonym dazu wird auch die Bezeichnung TCP/IP-Protokoll-Familie verwendet. Die Abkürzung TCP/IP steht für das Transmission Control Protocol (TCP) und das Internet Protocol (IP).

Das Zusammenspiel und die Struktur der "Generationenprotokolle" (Schichten) erhalten ihre Strukturierung durch das ISO/OSI-7-Schichtenmodell. Vor ca. 30 Jahren startete eine Studie zur Entwicklung von Protokollen zur Datenkommunikation. Im Rahmen dieser Forschungen entstand das DoD-Schichtenmodell. Dieses Modell bildet die Basis der Internetprotokollfamilie. Im DoD-Modell werden die einzelnen Aufgaben bei der Datenübertragung im Internet in aufeinander aufbauende Schichten eingeteilt. Dabei existiert für jede einzelne Schicht eine Vielzahl von Protokollen. Diese Protokolle stehen zur unterschiedlichen Lösung der Aufgaben jeder einzelnen Schicht zur Verfügung.

Ich habe mein Projekt nach dem TCP/IP-Modell gegliedert, da dieses Modell einen allgemeinen Überblick über die Internetprotokollfamilie zeigt und trotzdem jedes einzelne Protokoll sich in einer hierarchisch vernetzten Schicht befindet.

2 Allgemeine Informationen

Der Begriff Internetprotokollfamilie bezeichnet eine Sammlung von rund 500 Netzwerkprotokollen, die es möglich machen, dass Netzwerke miteinander kommunizieren können und verbunden sind. Die Protokolle bewirken zuerst eine Verbindung und dann eine Datenübertragung zwischen den Netzwerken. Außerdem lassen sich damit auch Netzwerke verschlüsseln.

Die Internetprotokollfamilie wird auch als TCP/IP-Protokoll-Familie bezeichnet. Allgemein gilt die Bezeichnung nicht nur als Oberbegriff für die rund 500 Protokolle, sondern auch als Einzelbezeichnung für das eine Protokoll für die Datenübertragung zwischen Netzwerken.

Hierbei steht TCP für Transmission Control Protocol und IP für Internet Protokoll. Das sogenannte OSI-Schichtenmodell beschreibt den Aufbau der Protokollfamilie. Dabei handelt es sich um sieben verschiedene Schichten, von denen jede einzelne der Lösung einer bestimmten Aufgabe dient. So kann zum Beispiel eine Schicht die Übertragung der Daten auf Vollständigkeit oder Fehler überprüfen. Jede Schicht dient der jeweils höheren Schicht und kann wiederum Dienste der niedrigeren Schicht verwenden.

Neben diesen Internetprotokollen existieren zusätzlich noch Transportprotokolle sowie Hilfsprotokolle. /I1/

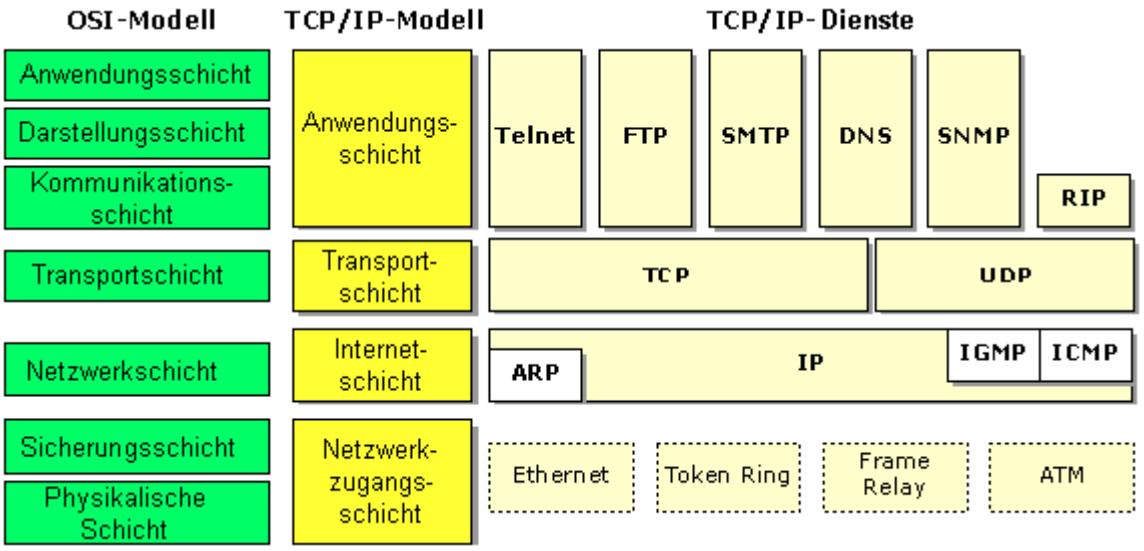


Abbildung 1: OSI-Schichtenmodell /B1/

3 Anwendungsschicht

3.1 Definition

Die Anwendungsschicht (engl.: Application Layer) umfasst alle Protokolle, die mit Anwendungsprogrammen zusammenarbeiten und die Netzwerkinfrastruktur für den Austausch anwendungsspezifischer Daten nutzen. /I2/

3.2 DNS

Um einen Server im Internet adressieren zu können, benötigt man seine IP-Adresse. Normalerweise sind aber nur Domain-Namen und/oder Computernamen der Server bekannt. Also ist das DNS ein System zur Auflösung von Computernamen in IP-Adressen und umgekehrt.

3.2.1 Domain-Name

Domain-Namen dienen dazu Computern/Servern richtige Namen zu geben und gleichzeitig in eine hierarchische Struktur zu unterteilen. Das DNS kümmert sich im Hintergrund um die Zuordnung von IP-Adresse zu Domain-Name und umgekehrt.

Domain-Namen haben eine bestimmte Struktur und sind Teil einem Uniform Resource Locator (en: einheitliche Angabeform für Ressourcen) (URL). Die für DNS verwendete Struktur (URL) besteht aus drei oder mehr Teilen:

Computername (Host oder Dienst)	Second-Level-Domain (SLD)	Top-Level-Domain (TLD)
www. ftp.	jonaspietsch. jonaspietsch.	de de

Manchmal befindet sich zwischen der Second-Level-Domain (SLD) und dem Computernamen eine Sub-Level-Domain (Subdomain).

Computername (Host oder Dienst)	Sub-Level-Domain (Subdomain)	Second-Level-Domain (SLD)	Top-Level-Domain (TLD)
www. ftp.	files. files.	jonaspietsch. jonaspietsch.	de de

Eine URL wird immer von hinten nach vorne gelesen. Die Adresse beginnt dort mit der Top-Level-Domain (TLD). Man unterscheidet zwischen zwei Typen von TLDs:

- Country-Code Top-Level-Domains (ccTLD): Ländercodes z.B. .de .at
- Generic Top-Level-Domain (gTLD): z.B. .com .info

An letzter Stelle, jedoch nicht zwingend erforderlich, steht der Computername oder Hostname, der meistens auf einen Dienst ist.
Die einzelnen Unterteilungen bzw. Ebenen werden durch Punkte voneinander getrennt. Zur Vervollständigung hat eine URL ein vorangestelltes Kürzel, das den verwendeten Dienst kennzeichnet (http:// oder ftp://). /I3/

3.2.2 DNS-Server

Ein Nameserver/DNS-Server ist ein Server, der die Namensauflösung anbietet. Namensauflösung ist das Verfahren, dass es ermöglicht, Namen von Rechnern bzw. Diensten in eine vom Computer bearbeitbare Adresse aufzulösen (z.B. siemens.md.st.schule.de in 141.44.122.232 oder jonaspietsch.de in 81.169.145.161). /I4/

Ein DNS-Server tritt selten alleine auf. Es gibt immer einen Primary und einen Secondary Nameserver. Sie sind voneinander unabhängig und so ausgelegt, dass mindestens ein Server verfügbar ist. Der Secondary Nameserver gleicht in regelmäßigen Abständen seine Daten mit dem Primary Nameserver ab und dient so als Backup-Server.

Damit nicht bei jeder DNS-Anfrage das Netzwerk belastet werden muss, hat jeder DNS-Server einen Cache, in dem er erfolgreiche DNS-Anfragen speichert. Bei einem wiederholten Aufruf holt er die jeweilige IP-Adresse der angeforderten Domain aus seinem Cache. Die gespeicherten Informationen haben eine Speicherdauer von ca. 2 Tagen. /I3/

3.3 FTP

Das File Transfer Protocol (FTP, englisch für Dateiübertragungsverfahren) ist ein spezifiziertes Netzwerkprotokoll zur Übertragung von Dateien über IP-Netzwerke. FTP befindet sich in der Anwendungsschicht des TCP/IP-Modells. Es wird benutzt für Downloads, für Uploads oder für das File Exchange Protocol. Außerdem können mit FTP Verzeichnisse angelegt und ausgelesen, sowie Verzeichnisse und Dateien umbenannt oder gelöscht werden.

Das FTP verwendet für die Steuerung und Datenübertragung jeweils unterschiedliche Ports/Verbindungen: Eine FTP-Sitzung beginnt, indem vom Client zum Control Port des Servers (Standard: 21) eine TCP-Verbindung aufgebaut wird. Über diese Verbindung werden Befehle zum Server gesendet. Der Server antwortet auf jeden Befehl mit einem Statuscode, oft mit einem angehängten, erklärenden Text. Die meisten Befehle sind allerdings erst nach einer erfolgreichen Authentifizierung zulässig. Daten werden dann über den Port 20 übertragen.

3.3.1 Verbindungsarten

Zum Senden und Empfangen von Dateien und zur Übertragung von Verzeichnislisten wird pro Vorgang jeweils eine separate TCP-Verbindung verwendet. Das FTP-Protokoll kennt für den Aufbau der Verbindungen zwei verschiedene Modi:

3.3.1.1 Aktives FTP

Beim aktiven FTP öffnet der Client einen zufälligen Port und teilt dies dem Server mit der eigenen IP-Adresse über das PORT- oder des EPRT-Kommando mit. Dies ist standartmäßig ein Port des Clients, der höher als 1023 liegt. Die Datenübertragung von dem Server erfolgt dabei über den Port 20. Die Kommunikation mit Befehlen erfolgt nur auf dem Control/Kommando Port. Man spricht auch von der Steuerung „Out of Band“. Somit ist es möglich, dass während der Datenübertragung die Partner miteinander kommunizieren können.

3.3.1.2 Passives FTP

Beim passiven FTP sendet der Client ein PASV- oder ein EPSV-Kommando. Danach öffnet der Server einen Port und übermittelt diesen inklusive der IP-Adresse an den Client. Hier wird beim Client ein Port höher als 1023 verwendet und beim Server der zuvor an den Client übermittelte Port. Diese Technik wird eingesetzt, wenn der Server keine Verbindung zum Client aufbauen kann, das heißt, dass der Client sich hinter einem Router befindet, der die Adresse des Clients über das NAT-Verfahren umschreibt, oder wenn eine Firewall das Netzwerk vom Clienten vor Zugriffen von außen schützt. /I5/

3.4 HTTP/HTTPS

Das Hypertext Transfer Protocol (HTTP) ist ein allgemeines, statusloses, objektorientiertes Protokoll zur Datenübertragung im World Wide Web (WWW). Es ist im RFC 2616 aus dem Jahr 1999 beschrieben und definiert einen bestimmten Satz von Nachrichten (Request) und Antworten (Response) mit denen ein Web-Client und ein Webserver während einer HTML-Sitzung miteinander kommunizieren. /I6/

3.4.1 HTTP-Übertragung/Struktur

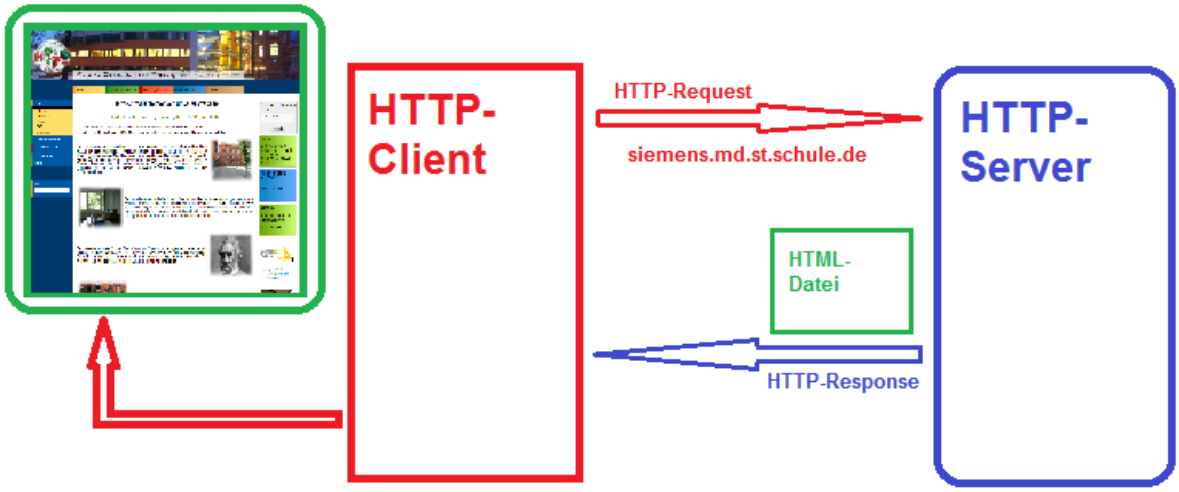


Abbildung 2: Client –Server-Prinzip /B2/

Bei HTTP geht es um die Übertragung von Hypertextinformationen. Dazu gehören Text-Dateien im HTML-Format, Bilder in den Formaten GIF, PNG und JPG/JPEG, sowie Audio- und Video-Aufnahmen.

Der Austausch dieser Dateien erfolgt, wie in Abbildung 2 zu sehen. Der HTTP-Client sendet einen HTTP-Request an einen Webserver. Dieser antwortet dann mit dem HTTP-Response und der jeweiligen angeforderten Datei. /I7/

3.4.2 Sonderform: HTTPS

HTTPS steht für Hypertext Transfer Protocol über SSL (Secure Socket Layer). Es ist ein von Webservern verwendetes Protokoll zur sicheren Datenübertragung. Die übertragenen Daten sind so verschlüsselt, und können nur vom Empfänger gelesen werden.

HTTPS wird von jeder Website genutzt, die sensible Kundendaten sammelt oder verwaltet, z.B. Bankinformationen oder Kaufinformationen. /I8/

3.5 IMAP

IMAP bedeutet Internet Message Access Protocol und ist ein Protokoll, dass die Übertragung/Verwaltung der E-Mails erlaubt. Beim nutzen des IMAP Protokolls verbleiben die E-Mails in der Regel auf dem Server (sie werden nur zum Lesen geladen), was erlaubt, dass die E-Mails an jeden internetfähigen Computer abrufbar sind. /I9/

3.5.1 Vorteile/Nachteile

Vorteile	Nachteile
• Nachrichten bleiben auf dem Server gespeichert • Schnellerer Zugriff auf das Postfach ist möglich • Der Inhalt des Postfaches ist immer auf dem neusten Stand	• Lesen einer Nachricht braucht eine Internetverbindung • Um eine Kopie zu speichern, muss sie erneut hochgeladen werden • Erhöhte Serverbelastung

/I10/

3.6 POP3

POP3 steht für "Post Office Protocol". POP3, das auch in seltenen Fällen nur "POP" genannt wird, ist eine einfache, standardisierte Methode zur Bereitstellung von E-Mails. Ein POP3-Mail-Server empfängt E-Mails und filtert sie in die entsprechenden Benutzerordner bzw. hauptsächlich in den Posteingang. Wenn ein Benutzer eine Verbindung mit dem Mail-Server herstellt, um seine Mails abzurufen, werden die Nachrichten vom Mail-Server auf die Festplatte des Benutzers heruntergeladen. /I11/

3.6.1 Vorteile/Nachteile

Vorteile	Nachteile
• Keine ständige Verbindung zum Server ist notwendig • Die Verbindung wird nur bei Bedarf aufgebaut • Alle Emails werden nach Anmeldung automatisch heruntergeladen	• Eine Kommunikation mit dem Server findet nach dem Download nicht statt → Alle Tätigkeiten nach dem Download sind nur auf dem Clienten gespeichert

/I12/

3.7 SMTP

SMTP ist ein Kommunikationsprotokoll für die Übertragung von E-Mails. Die Kommunikation erfolgt zwischen einem E-Mail-Client und einem SMTP-Server oder zwischen zwei SMTP-Server.

Für den Austausch der E-Mails sind die Mail Transfer Agents (MTAs) zuständig. Untereinander verständigen sich die MTAs mit Kommandos. Dabei sendet der SMTP-Client dem SMTP-Server ein Kommando, und dieser antwortet mit einem Status-Code und einer Klartext-Meldung.

3.7.1 E-Mail-Routing über SMTP und DNS

Nachdem der SMTP-Server eine E-Mail von einem E-Mail-Client (SMTP-Client) entgegengenommen hat, ist er für das Weiterleiten an den Ziel-SMTP-Server verantwortlich. Das DNS spielt wie bei den Protokollen HTTP und FTP eine zentrale Rolle. Im DNS sind spezielle Einträge für die elektronische Post vorhanden. Das sind die Mail Exchange Records (MX-Records). Über diese Einträge identifiziert der SMTP-Server den Ziel-SMTP-Server der Domain, die in der E-Mail-Adresse des Empfängers angegeben ist.

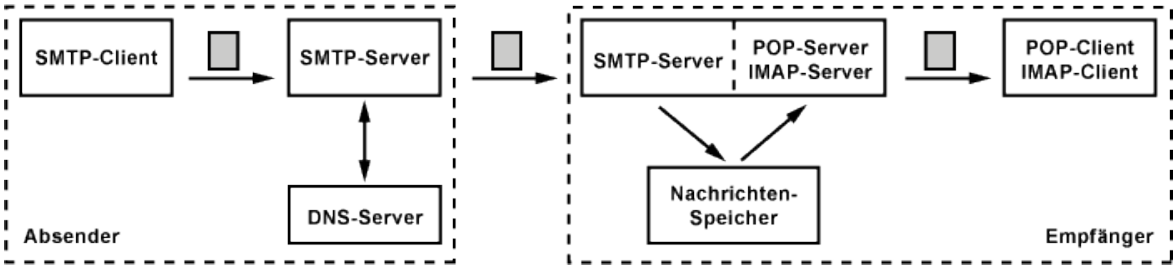


Abbildung 3: Versand von E-Mails /B3/

Der Ablauf des E-Mail-Routings sieht in etwa so aus: Der SMTP-Server fragt einen DNS-Server ab und erhält eine Aufstellung von Mail-Servern, die E-Mails für den Ziel-SMTP-Server entgegennehmen. Jeder dieser Mail-Server (Mail Exchanger) ist mit einer Priorität versehen. Der SMTP-Server versucht die Mail-Server in der vorgegebenen Reihenfolge zu kontaktieren, um die E-Mail zu übermitteln. Theoretisch ist es möglich, dass eine E-Mail über mehrere dieser Mail Exchanger läuft. Die MX-Records sollen das Entstehen dieser Mail-Schleifen verhindern. Trotzdem kann es zu Mail-Schleifen kommen, wenn die MX-Records unvollständig sind oder die Domain zu einem anderen Hoster oder Provider umgezogen ist. /I13/

3.8 NTP

Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. NTP verwendet das verbindungslose Transportprotokoll UDP. NTP wurde speziell entwickelt, um eine zuverlässige Zeitangabe über Netzwerke zu ermöglichen.

3.8.1 Genauigkeit/Algorithmus

NTP benutzt den Marzullo-Algorithmus (von Keith Marzullo an der Universität San Diego entwickelt) und einen Algorithmus, um Byzantinische Fehler zu beheben. NTP benutzt eine UTC-Zeitskala.

NTP unterstützt Schaltsekunden. Durch die Betrachtung der Schaltsekunden im Protokoll kommt es dazu, dass mit jeder Schaltsekunde eine neue Sekundenskala benutzt wird. Für die Skala der Systemzeit wird jedoch für gewöhnlich die tatsächlich vergangene Zeit seit einem bestimmten Zeitpunkt benutzt. Schaltsekunden kommen erst bei der Darstellung der Zeit ins Spiel.

NTP überträgt die Zeit über das Internet mit einer Genauigkeit von 10 Millisekunden. In lokalen Netzwerken ist eine Genauigkeit von bis zu 200 Mikrosekunden möglich. /I14/

3.9 Telnet

Das Telnet-Protokoll gehört zu den ARPA-Diensten und bietet Funktionen eines virtuellen Terminals. Dadurch ermöglicht Telnet den Fernzugriff vom eigenen Computer auf andere Computersysteme in seinem Netzwerk. /I15/

3.9.1 Nutzung

Telnet wird zur Fernsteuerung von Computern eingesetzt. Diese Steuerung geschieht in Form von textbasierten Ein- und Ausgaben.

Sobald die Verbindung zwischen dem Telnet-Client und dem Telnet-Server hergestellt wurde, werden die Tastatureingaben vom steuernden Endgerät zum fernen Computer gesendet und von dort wiederum Texte an das Endgerät zurück übertragen. Der ferne Computer überträgt so z. B. die textbasierten Ausgaben eines Programmes. Auf diese Weise lässt sich von einem Computer aus ein anderer Computer fernbedienen. Dieser Fernzugriff kann sogar über mehr als zwei Stufen erfolgen.

Da der Datenaustausch über Telnet unverschlüsselt erfolgt und leicht mitgelesen werden kann, wird zum Fernzugriff auf andere Rechner heute im Regelfall der verschlüsselte Dienst Secure Shell (SSH) statt des Telnet-Dienstes verwendet. Wobei es mit SSH möglich ist, einen ähnlichen Zugriff auf ein entferntes System zu erlangen, mit dem sich gleichermaßen arbeiten lässt.

Der Telnet-Dienst selbst wird heute in erster Linie noch eingesetzt, um einen Zugriff auf netzwerkfähige Firmwares verschiedenster Geräte oder auf Kleinstcomputer zu erlangen, die aufgrund von technischen Beschränkungen Betriebssysteme mit minimalem Funktionsumfang nutzen, die den Betrieb eines SSH-Servers nicht ermöglichen. /I16/

4 Transportschicht

4.1 Definition

Die Transportschicht ist die Schicht im TCP/IP-Modell, in der eine direkte und logische Ende-zu-Ende-Kommunikation zwischen zwei Clienten/Servern möglich wird. Der transparente Datentransport über die Netzwerkverbindungen kann durch Mechanismen für die Flusskontrolle gesteuert werden. /I17/

4.2 TCP

Das Transmission Control Protocol ist ein verbindungsorientiertes Transportprotokoll für den Einsatz in paketvermittelten Netzen und ist ein Teil der Protokollfamilie TCP/IP. Das Protokoll baut auf dem IP-Protokoll auf und stellt vor der Datenübertragung eine gesicherte Verbindung zwischen den Instanzen her. Dieses Protokoll soll Datenverluste verhindern, Dateien und Datenströme aufteilen und Datenpakete Anwendungen zuordnen können. /I18,I19/

4.2.1 TCP-Funktionen

- Ende-zu-Ende-Kontrolle
  - Alle Datenpakete werden bestätigt
  - Nicht empfangene Datenpakete werden erneut gesendet
- Verbindungsmanagement
  - Gesicherter Verbindungsaufbau mit Handshake-Verfahren
- Flusskontrolle
  - Verhinderung des Verlustes von Datenpaketen
- Zeitkontrolle
  - Nichtbestätigte Datenpakete nach einer bestimmten Zeit werden erneut gesendet
- Multiplexen von Verbindungen
  - Möglichmachen von Verbindungen über mehreren Ports
- Fehlerbehandlung
  - Fordert fehlerhafte Datensegmente erneut

/I18/

4.2.2 Verbindungsauf/-abbau

4.2.2.1 Verbindungsaufbau

Der Host 1 sendet ein Anfragepaket (SYN mit SEQ=X) an Host 2. → Host 2 nimmt die Anfrage an und sendet seine Zustimmung (SYN-ACK mit ACK=X+1 und SEQ=Y) → Host 1 bestätig dies mit einem Erhalt (ACK mit ACK=Y+1 und SEQ=X+1) /L1/

4.2.2.2 Verbindungsabbau

Der Host 1 sendet ein Paket (FIN mit SEQ=X) an Host 2 → Host 2 sendet daraufhin seine Zustimmung (ACK mit ACK=X+1 und FIN SEQ mit SEQ=Y) → Dies bestätigt dann Host 1 (ACK mit ACK=Y+1) /L1/

4.3 UDP

UDP bedeutet User Datagramm Protokoll und arbeitet ohne das Aufbauen, Überwachen und Abbauen einer Verbindung. Die beteiligte Anwendung ist selbst für die Fehlererkennung und -behebung dieser zuständig. Der Verzicht auf jegliche Verbindungs- und Transportprotokolle ermöglicht Anwendungen, die mit TCP nicht möglich wären, z.B. die Übertragung von Ton und Video, da es hierbei nicht darauf ankommt, dass alle Datenpakete auf Richtigkeit und Vollständigkeit überprüft werden. /L1/

4.4 SSL/TLS

SSL und TLS bezeichnen beide das gleiche Verschlüsselungsprotokoll. Der einzige Unterschied zwischen diesen Beiden, ist der, dass SSL die Bezeichnung vor der Version 3.0 war, und TLS für die Versionen danach. /L1/

4.4.1 Sicherheitsschaffung

Das SSL-Protokoll schafft unter drei Gesichtspunkten sichere Verbindungen:

- Die Verbindung ist privat, weil ihr Inhalt nur verschlüsselt über das Netz geht.
- Die Identität des Servers steht fest.
- Wirkungsvolle Algorithmen prüfen, ob die Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen.

/I20/

5 Internetschicht

5.1 Definition

Eine weitere Schicht des TCP/IP-Referenzmodells ist die Internetschicht. Sie übernimmt die Adressierung der verschiedenen Systeme im Internet und ist verantwortlich, dass die Daten richtig versendet werden (Routing). Da direkte Leitungen zwischen allen Kommunikationspartnern im Internet wirtschaftlich oder technisch nicht zu erwägen wären, erfolgt der Datenaustausch zwischen nicht direkt miteinander verbundenen Kommunikationspartnern über Zwischenstationen (Router). In diesen Zwischenstationen, wo lediglich die Subnetzschicht und die Internetschicht implementiert sind, erfolgt die Entscheidung über den richtigen Weg der Datenpakete. /I21/

5.2 IP/IPsec

Das Internetprotokoll stellt nur die grundlegenden Transportmechanismen bereit, die für die Sendung von Datagrammen über Netzwerkgrenzen hinweg benötigt werden. Das Internetprotokoll arbeitet verbindungslos, das bedeutet, dass keine Verbindung im technischen Sinne aufgebaut wird. /L1/

Es gibt aktuell die zwei nachfolgenden Versionen von IP. Die wichtigste Neuerung, weshalb man IPv6 entwickelt hat, war das, dass man nun 128 Bit-Adressen hat (ca. 340 Sextillionen Adressen) im Gegensatz zu IPv4: 32.Bit-Adressen (ca. 4 Milliarden Adressen) /I22/

5.2.1 IPv4 und IPv6

	IPv4	IPv6
Adressraum	4 294 967 296 Adressen	~3,4 x 1038 Adressen
Konfiguration	Manuell oder via DHCP	Manuell oder über Autokonfiguration via SLAAC
Header	• Checksumme • variable Länge • Fragmentierung im Header • keine Sicherheit	• Überprüfung auf höherer Schicht • fest vorgeschriebene Größe • Fragmentierung im Extension Header • IPsec über Extension Header
Sicherheit	Für Verschlüsselung bei IPv4 wie zum Beispiel bei VPN benötigt, müssen immer die höheren Schichten bemüht werden	IPv6 bringt mit IPsec über die Extension Header eine direkte Integration

/I23/

5.2.2 Sonderform: IPsec

IPsec besteht aus 2 Teilen. Der erste Teil ist der, der einen Header an die Pakete anfügt, für die Sicherheitskennung, für Daten zur Integritätskontrolle und für andere

Informationen. Der andere Teil ist der, der sich mit der Vergabe von Schlüsseln befasst (ISAKMP).

IPsec kann in 2 Modi eingesetzt werden: Der Transportmodus und der Tunnelmodus.

Im Transportmodus wird im IP-Header das Feld „Protokoll“ geändert, um anzugeben, dass ein IPsec-Header folgt.

Im Tunnelmodus werden der gesamte IP-Header und alle Daten eines neuen IP-Pakets mit einem neuen IP-Header gekapselt. Der Tunnelmodus ist nützlich, wenn der Tunnel an einem anderen Ort landet als das Ziel.

/L2/

6 Netzwerk-Zugangsschicht

6.1 Definition

Die unterste Schicht in dem TCP/IP-Modell ist die Netzwerk-Zugangsschicht. Die darin enthaltenen Protokolle machen eine Versendung von Daten in einem direkt angeschlossenen Netzwerk möglich. Dabei müssen die Protokolle die zugrundeliegende Netzwerkstruktur kennen. Ein Beispiel für ein solches Protokoll ist das Address Resolution Protocol (ARP), welches IP-Adressen auf Ethernet-Adressen abbildet. /I24/

6.2 Ethernet

Ethernet entstand aus einem Projekt von Digital Equipment, Intel und Xerox in den siebziger Jahren, das unter der Bezeichnung DIX bekannt wurde. Dieses Projekt zielte auf die gemeinsame Nutzung eines Übertragungsmediums durch mehrere gleichberechtigte Datenstationen und war für den lokalen Bereich konzipiert. Die Struktur dieses lokalen Netzes war die eines Busses an den alle Datenstationen angeschlossen werden konnten. Das Buskonzept war in seiner Ausdehnung, in der Anzahl der anschließbaren Stationen und in Datenrate auf 3 Mbit/s begrenzt und daher nur für den lokalen Bereich geeignet. Aus dem DIX-Projekt wurde 1982 Ethernet. Die Spezifizierung und Standardisierung übernahm das IEEE, das die Spezifikationen DIX Ethernet V2.0 veröffentlichte. /I25/

6.2.1 Übertragungstechnik

Ethernet transportiert Daten paketweise ohne festes Zugriffsraster. Dabei unterscheidet es sich von anderen paketorientierten Systemen, wie zum Beispiel ATM oder SDH/Sonet, in einem festgelegtem Zeitraster jedem Teilnehmer eine Mindestbandbreite zusichern können. Deshalb bereitet Ethernet vor allem allen zeitkritischen Anwendungen Probleme. Bei Ethernet gibt es keine Garantie, dass die Daten innerhalb einer bestimmten Zeit den Empfänger erreichen. Dagegen spricht aber, dass Ethernet eine einfach zu implementierende Vernetzungstechnik ist, die sich über die Jahrzehnte hinweg in lokalen Netzwerken bewährt hat. /I26/

6.3 WLAN

Wireless Local Area Network (WLAN) ist ein Oberbegriff für alle auf dem Markt befindlichen drahtlosen lokalen Datennetze. Darunter fallen auch Bluetooth, HomeRF und HiperLAN. Und selbstverständlich alle anderen Techniken und Standards mit denen sich drahtlose Funknetzwerke aufbauen lassen. Allerdings bezeichnet "WLAN" im allgemeinen Sprachgebrauch ein Funknetzwerk nach IEEE 802.11. /I27/

6.3.1 Übertragungstechnik

Der Funknetz-Standard IEEE 802.11 definiert einen gemeinsamen MAC-Layer (Medium Access Control) für drei spezifische Physical Layer (PHY). Zwei davon sind den Funk-LANs, einer dem Infrarotnetz zugeordnet. Im Funknetz wird als Frequenzbereich das ISM-Band (2,4 GHz) von 2,400 bis 2,4835 GHz genutzt.

Die Infrarot-Variante ist so gut wie unbekannt. Sie nutzt die Frequenzen mit einer Wellenlänge von 850nm bis 950nm. /I28/

6.4 ARP

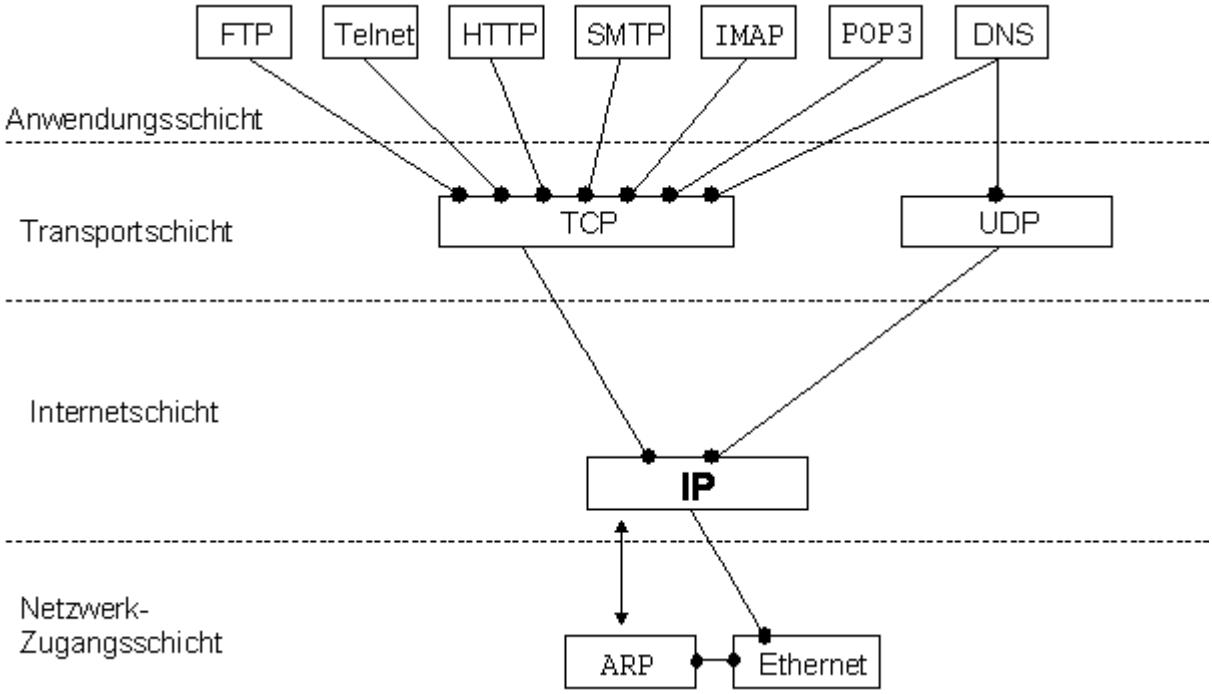
Das Address Resolution Protocol (ARP) ist ein Netzwerkprotokoll, dass zu einer Netzwerkadresse der Internetschicht die physikalische Adresse (Hardwareadresse) der Netzwerkzugangsschicht ermittelt. Die Zuordnung speichert es in den so genannten ARP-Tabellen der beteiligten Rechner und macht sie aufrufbar. Es wird fast nur im Zusammenhang mit IPv4-Adressierung auf Ethernet-Netzen, obwohl es auch anders nutzbar ist, aber nicht für IPv6.

6.4.1 Funktion am Beispiel Ethernet

Es wird eine ARP-Anforderung (ARP Request) mit der MAC-Adresse und der IP-Adresse des anfragenden Computers als Senderadresse und der IP-Adresse des gesuchten Computers als Empfänger-IP-Adresse an alle Computer des lokalen Netzwerkes gesendet. Als Empfänger-MAC-Adresse wird dazu die Broadcast-Adresse ff-ff-ff-ff-ff-ff_{16} verwendet. Empfängt ein Computer ein solches Paket, sieht er nach, ob dieses Paket seine IP-Adresse als Empfänger-IP-Adresse enthält. Wenn dies der Fall ist, antwortet er mit dem Zurücksenden seiner MAC-Adresse und IP-Adresse (ARP-Antwort oder ARP-Reply) an die MAC-Quelladresse des Anfragenden. Dieser trägt nach Empfang der Antwort die empfangene Kombination von IP- und MAC-Adresse in seine ARP-Tabelle, den sogenannten ARP-Cache, ein. Für ARP-Request und ARP-Reply wird das gleiche Paket-Format verwendet.

Zusätzlich können die Empfänger des ARP-Requests ebenfalls die Kombination von IP-Adresse und MAC-Adresse des anfragenden Computers in ihre ARP-Tabelle eintragen bzw. einen bestehenden Eintrag aktualisieren. Insbesondere der Rechner mit der im ARP-Request angefragten IP-Adresse sollte diese Eintragung vornehmen, da anzunehmen ist, dass der ARP-Request als Vorbereitung für weitere Kommunikation auf höherer Protokollebene dienen soll, wofür er dann für eventuelle Antworten ebenfalls die MAC-Adresse des Anfragenden benötigt. /I29/

7 Fazit



Der Austausch von Nachrichten erfordert häufig ein Zusammenspiel verschiedener Protokolle, die unterschiedliche Aufgaben übernehmen. Um die damit verbundene Komplexität beherrschen zu können, werden die einzelnen Protokolle in Schichten organisiert. Im Rahmen einer solchen Architektur gehört jedes Protokoll einer bestimmten Schicht an und ist für die Erledigung der speziellen Aufgaben zuständig. Protokolle höherer Schichten verwenden Dienste von Protokollen tieferer Schichten. Zusammen bilden die, so strukturierten, Protokolle einen Protokollstapel.

8 Quellen

Textquellen aus dem Internet

I1 http://www.deine-ip-adresse.de/internetprotokollfamilie.html 23.12.14

I2 http://fakten-uber.de/tcp/ip-referenzmodell 23.12.14

I3 http://www.elektronik-kompendium.de/sites/net/0901141.htm 23.12.14

I4 https://de.wikipedia.org/wiki/Domain_Name_System 23.12.14

I5 https://de.wikipedia.org/wiki/File_Transfer_Protocol 23.12.14

I6 http://www.itwissen.info/definition/lexikon/hypertext-transfer-protocol-HTTP-HTTP-Protokoll.html 16.01.15

I7 http://www.elektronik.info/was-ist-http/ 16.01.15

I8 http://webdesign.about.com/od/http/g/bldefhttps.htm 16.01.15

I9 http://www.webhosting-anleitung.de/glossar-definition/imap-internet-message-access-protocol 16.01.15

I10 http://de.wikipedia.org/wiki/Internet_Message_Access_Protocol 17.01.15

I11 http://techterms.com/definition/pop3 17.01.15

I12 http://de.wikipedia.org/wiki/Post_Office_Protocol 17.01.15

I13 http://www.ssl.de/ssl.html 10.03.15

I14 http://de.wikipedia.org/wiki/Network_Time_Protocol 17.01.15

I15 http://www.itwissen.info/definition/lexikon/Telnet-Protokoll-telnet.html 18.01.15

I16 https://de.wikipedia.org/wiki/Telnet 18.01.15

I17 http://www.itwissen.info/definition/lexikon/Transportschicht-transport-layer.html 01.02.15

I18 http://www.itwissen.info/definition/lexikon/transmission-control-protocol-TCP-TCP-Protokoll.html 01.02.15

I19 http://www.elektronik-kompendium.de/sites/net/0812271.htm 01.02.15

I20 http://www.ssl.de/ssl.html 10.03.15

I21 http://www.gym1.at/informatik/unterlagen/netzwerk/node23.html 18.02.15

I22 http://de.wikipedia.org/wiki/Internet_Protocol 07.03.15

I23 http://www.ipv6-portal.de/informationen/unterschiede-ipv4-ipv6.html 07.03.15

I24 http://www.informatik.uni-hamburg.de/TKRN/world/lernmodule/LMint/Popup/netzzugangsschicht.htm 07.03.15

I25 http://www.itwissen.info/definition/lexikon/Ethernet-Ethernet.html 10.03.15

I26 http://www.elektronik-kompendium.de/sites/net/0603201.htm 10.03.15

I27 http://www.elektronik-kompendium.de/sites/net/0907021.htm 10.03.15

I28 http://www.elektronik-kompendium.de/sites/net/0907101.htm 10.03.15

I29 http://de.wikipedia.org/wiki/Address_Resolution_Protocol 10.03.15

Bildquellen

B1 http://www.trojaner-und-sicherheit.de/glossar/tcp-ip-modell-vs-osi-modell.gif 23.12.14

B2 http://www.elektronik.info/was-ist-http/ (Bild: Video bei 1:12min+Bearbeitung) 16.01.15

B3 http://www.elektronik-kompendium.de/sites/net/bilder/09022611.gif 10.03.15

Literaturquellen

L1 Harald Zisler: Computer-Netzwerke, Galileo-Computing, 2012, S. 104-105; 190-193

L2 Andrew S. Tanenbaum: Computernetzwerke, Pearson-Studium, 2003, S. 833