

# Zusammenfassung - Kryptographie

Marc Meier

6. November 2015

Korrektheit und Vollständigkeit der Informationen sind nicht gewährleistet. Macht euch eigene Notizen oder ergänzt/korrigiert meine Ausführungen!

## Inhaltsverzeichnis

<b>1 Grundlagen</b>	<b>2</b>
<b>2 Protokolle</b>	<b>3</b>
<b>3 Adressierung</b>	<b>7</b>
<b>4 ARP, RARP</b>	<b>7</b>
<b>5 DNS und WHOIS</b>	<b>7</b>
<b>6 Migration von IPv4 nach IPv6</b>	<b>7</b>
<b>7 Timeouts, ACK, Bestätigungen</b>	<b>7</b>
<b>8 Routingkonzepte</b>	<b>7</b>
<b>9 Quality of Service</b>	<b>7</b>
<b>10 Multicasts</b>	<b>7</b>
<b>11 Zeitsynchronisation</b>	<b>7</b>
<b>12 Internet Control Message Protocol</b>	<b>7</b>
<b>13 Voice over IP</b>	<b>7</b>
<b>14 World Wide Web und HTTP</b>	<b>7</b>
<b>15 Peer-to-Peer</b>	<b>7</b>
<b>16 E-Mail</b>	<b>7</b>
<b>17 Autokonfiguration</b>	<b>7</b>
<b>18 Dateien und Drucken</b>	<b>7</b>
<b>19 Telnet, SSH und rlogin</b>	<b>7</b>
<b>20 Extensible Messaging and Presence Protocol (XMPP)</b>	<b>7</b>
<b>21 LDAP</b>	<b>7</b>
<b>22 Authentication Protocols</b>	<b>7</b>
<b>23 Simple Network Management Protocol</b>	<b>7</b>
<b>24 Mac-Sublayer</b>	<b>7</b>

25 Mobile Netzwerke	7
26 HTTP2 und SCTP	7
Literatur	8
Glossar	9

# 1 Grundlagen

## 1.1 Grundprinzipien und Entwicklung des Internets

Das Internet entwickelte sich ab den 1960er Jahren. Es ging aus dem am Ende des Jahrzehnts entstandenen, vornehmlich militärisch und akademisch geprägten ARPA-Net hervor. Heutzutage wird es international kommerziell, industriell und auch akademisch (Katzenbilder) genutzt. Bei seiner Entstehung war vor allem eine dezentrale Struktur ohne zentrale Verwaltung von Interesse. Grund hierfür war die Angst des amerikanischen Department of Defense, dass eine atomarer Angriff zentrale Kommunikationspunkte außer Kraft setzen könnte. Die Kommunikation findet über hochgradig vernetzte Knoten mithilfe von Paketen statt.

Literatur: [1, 2]

## 1.2 Packet Switching

Paketvermittelte Übertragung bedeutet die Abkehr von der leitungsbasierten Vermittlung. Dabei werden längere Nachrichten in Datenpakete aufgeteilt und voneinander unabhängig versendet. Dies ermöglicht eine faire Verteilung der Leistungskapazität und redundante Wege bei einem Ausfall von Knoten oder Verbindungen. Im Gegenzug können konstante Bandbreiten nicht ohne Weiteres (Abschnitt 9) gewährleistet werden, ebenso ergeben sich unterschiedliche Laufzeiten von Paketen.

## 1.3 Dezentrale Verwaltung des Internets

### 1.3.1 Prinzipien

- Keine zentrale Verwaltung oder Behörde (trotz Einflussnahme)
- Demokratisches Zusammenwirken der Beteiligten / Wahlen
- Selbstorganisation
- Standards dort, wo sie erforderlich sind
- Dynamisch, offen für Neuigkeiten

### 1.3.2 Organisationen

**ICANN:** Vergibt IP-Adressen und betreibt die DNS-Rootserver.

**IETF:** Standardisierung von Protokollen in RFCs [3]

**RIPE:** Administration und technische Koordination

**RIPE NCC:** Adressvergabe in Europa und Zentralasien, Verwaltung der WHOIS-Datenbank.

**DENIC eG:** Domain-Verwaltung für die Zone .de

## 1.4 Standards

Standards ermöglichen die Kooperation im Netzwerk, nur durch sie können Geräte verschiedener Hersteller miteinander kommunizieren. Sie können textuell, mithilfe einer Referenzimplementierung oder anhand von Automaten (meist für zustandsbehaftete Protokolle) festgelegt werden.

**Protokoll** Standardisierte Regeln (Vorschriften) und Vereinbarungen zu Form, Ablauf, Steuerung und Sicherung (Fehler) der Datenübertragung in und zwischen Rechnernetzen, zwischen Einzel-Rechnern und zwischen Rechnern und Peripheriegeräten.

**Standard** Ein Standard wird von den verschiedensten internationalen und nationalen Organisationen sowie von großen Firmen erstellt. Ein Standard wird als verbindliche oder unverbindliche (empfohlene) Festlegungen schriftlich niedergelegt.

Ablauf einer Standardisierung bei RFCs:

1. **Proposed Standard:** Vollständige, konsistente Spezifikation vorhanden
2. **Draft Standard:** Mindestens 2 unabhängige, interoperable Implementierungen
3. **Standard:** Operationell stabil

**Weitere Status:** *Experimental*, *Informational* und *Historic*.

## 1.5 Netze, Autonome Systeme und Schichten

Große Teile des Internet-Backbones werden von wenigen Firmen bereitgestellt (Tier-1). Diese werden an einigen Knotenpunkten verbunden. Wichtiger Knotenpunkt in Deutschland ist DE-CIX in Frankfurt/Main. Man unterteilt folgende **Netzwerk-Schichten**:

**Tier 1** : Ein Netzwerk, das mit allen anderen Tier-1-Netzwerken verbunden ist; *Internet-Backbone*; z.B. ATDN, GX, AT&T...

**Tier 2** : Netzwerk, das mit vielen Netzwerken verbunden ist, aber Transit *einkauft*, um einige Bereiche des Internets zu erreichen; z.B. Deutsche Telekom

**Tier 3** : Ein Netzwerk, das ausschließlich Transit *einkauft*, um das Internet zu erreichen

**Autonome Systeme** sind Ansammlungen von IP-Netzen, die als Einheit verwaltet werden. Innerhalb kommt ein einheitliches Routing-Protokoll zum Einsatz. Autonome Systeme sind untereinander verbunden und bilden das Internet.

## 2 Protokolle

### 2.1 Zustandslose und zustandsbehaftete Protokolle

Bei **zustandslosen Protokollen** wird jede Anfrage in einer eigenständigen Transaktion ausgeführt, es existieren keine Vorbedingungen oder Sitzungsinformationen (UDP, HTTP, TFTP). **Zustandsbehaftete Protokolle** hingegen merken sich den aktuellen Zustand mithilfe einer Sitzung. Nachfolgende Anfragen können auf die Sitzungsinformationen zugreifen. Diese Zustandsübergänge können durch endliche Automaten dargestellt werden. Beispiele sind FTP, TCP und SMTP.

### 2.2 OSI-7-Schichten-Modell

1. Physical Layer / Bitübertragung
2. Data Link Layer / Sicherungsschicht / Datenübertragungsschicht
3. Network Layer / Vermittlungsschicht
4. Transport Layer
5. Session Layer / Sitzungsschicht
6. Presentation Layer / Darstellungsschicht
7. Application Layer / Anwendungsschicht

Gute **Eselsbrücken** sind:

- Alle deutschen Studenten trinken verschiedene Sorten Bier (deutsche Bezeichnungen, 7-1)
- An dem Samstag trug Verena 'nen String in Blau (deutsche Bezeichnungen, 7-1)
- Alle poppen Susis Tante nach der Party (deutsche Bezeichnungen, 7-1)
- Physiker, die nicht trinken sind potentielle Attentäter (deutsche/englische Bezeichnungen, 1-7)
- Alibaba präsentiert sich täglich nackt dem Personal
- Please Do Not Throw Salami Pizza Away (englisch, 1-7)

Jede Schicht  $n$  nutzt die darunterliegende Schicht  $n - 1$  um mit dem Kommunikationspartner zu kommunizieren. Daten höherer Schichten werden in niederen Schichten umkapselt. Die Bezeichnung der Pakete ist je nach Schicht unterschiedlich:

**Data Link Layer** : (Ethernet-)Frame

**Network Layer** : Paket

**Transport Layer** : Fragment

## 2.3 Ethernet

Das Ethernet-Protokoll wirkt auf den Layern 1 + 2 und wird im Standard **IEEE 802.3** definiert. Es kümmert sich um Elektrokrams (Physikalische Eigenschaften, Stecker, Stromversorgung, Kabel etc.), Zugriffsverfahren auf das Medium, Adressierung (MAC), Protocol-Multiplexing, Flow Control (Logical Link Control) und Fehlererkennung (CRC). Es ähnelt den Standards **802.11** (WLAN), **802.15.1** (Bluetooth) und **802.16** (WiMAX).

Ein **Ethernet-Frame** hat eine Größe von 64 - 1518 Byte. Davon ausgenommen sind die Präambel und der SFD. Wird das VLAN-Tag genutzt, sind 1522 Byte möglich. Das **Ethernet-Paket** (Offensichtlich Präambel + SFD + Ethernet-Frame) umfasst folgende Felder:

Preamble								Destination MAC						Source MAC						EtherType/ Size	PayLoad				CRC				
1	2	3	4	5	6	7	8	1	2	3	4	5	6	1	2	3	4	5	6	1	2					1	2	3	4

**Präambel** : Zum Synchronisieren von Sender und Empfänger, *Einschwingphase* (8 Byte)

**SFD** : Festgelegte Sequenz 10101011 (1 Byte)

**Ziel-Mac-Adresse** : Adresse des Empfängers (8 Byte)

**Quell-Mac-Adresse** : Adresse des Senders (8 Byte)

**VLAN-Tag** : Nach IEEE 802.1q, optional (4 Byte)

**Typ-Feld** : Identifiziert die Art des nachfolgenden Inhalts, z.B. IP, ARP, etc...

**Nutzlast**

**PAD-Füllfeld** : Wird optional benötigt, um die Mindestlänge von 64 Byte einzuhalten <sup>1</sup>

**CRC-Prüfsumme** : Zur Fehlererkennung (4 Byte)

### 2.3.1 CSMA/CD

CSMA/CD regelt den Zugriff auf ein von mehreren Teilnehmern genutztes Medium (Kabel). Dazu prüft der sendende Host, ob das Medium frei ist, bevor er sendet. Beim Übertragen von Daten können Kollisionen erkannt werden. Der Sendevorgang wird dann nach einer zufälligen Zeit wiederholt. Aufgrund der verbreiteten Nutzung von Switches sind echte geteilte Medien inzwischen eher die Ausnahme.

⇒ Jeder Port am Switch bildet eine eigene *Kollisionsdomäne*. Die Bustopologie mit Koaxialkabeln (aber auch mit Hubs) wird nicht mehr genutzt.

### 2.3.2 Duplex / Half Duplex

Beim **Full Duplex** sind beide Seiten in der Lage, gleichzeitig zu Senden und zu Empfangen. Im Falle von **Half Duplex** ist dies nur wechselseitig möglich (vgl Walkie Talkie). Es sind verschiedene Realisierungen einer geteilten Nutzung eines Mediums möglich:

**Zeitduplex (TDD)** : Übertragung in verschiedenen Zeitschlitzten

**Frequenzduplex (FDD)** : Übertragung auf verschiedenen Frequenzen

**Codeduplex** : (nicht im Skript)

## 2.4 Switching

**Switches** sind Geräte auf dem OSI-Layer 2. Sie empfangen Ethernet-Frames und leiten sie anhand ihrer Empfänger-MAC-Adresse weiter. Im Gegensatz zum Hub wird dabei nur über den Port ausgegeben, hinter dem sich der Empfänger befindet. Die Ausnahme ist hierbei, wenn der Port des Empfängers nicht bekannt ist. Anhand der empfangenen Frames lernt ein Switch, wo sich Geräte befinden.

<sup>1</sup>Rausfinden, warum mindestens 64 Byte nötig. Vermutung: Kollisionserkennung

### 2.4.1 Realisierungsmöglichkeiten

### 2.4.2 Cut-Through und Store-and-Forward

Beim **Cut-Through** (auch *On The Fly Forwarding*) werden Pakete sofort nach Empfang der Empfängeradresse auf dem entsprechenden Port weitergeleitet, sofern dieser frei ist. Diese Methode ist sehr schnell (Verzögerung ca.  $40\mu s$ ), leitet jedoch gegebenenfalls auch fehlerhafte Frames weiter, da CRC umgangen wird.

**Store-and-Forward** hingegen empfängt zuerst den gesamten Frame, prüft diesen und leitet ihn anschließend weiter. Offensichtlich werden keine fehlerhaften Pakete mehr in benachbarte Segmente weitergeleitet, dies wird jedoch durch erhöhte Latenz erkauft.

In der Praxis arbeiten Switches häufig im Cut-Through-Modus und schalten bei erhöhter Fehlerrate in den Store-and-Forward-Modus.

### 2.4.3 VLAN

Ermöglicht die Aufteilung von Switches in mehrere virtuelle LANs. Den Ports werden dabei einzelne VLANs zugeordnet. Auf diese Weise kann Hardware eingespart werden. Realisiert wird dies mit einem 4 Byte langen Feld im Ethernet-Frame:

- 2 Bytes **TPID** - Tag Protocol Identifier – Fester Wert 0x8100. Frame trägt die 802.1Q/802.1p-Tag-Information
- 3 Bit **Priorität** (user\_priority) – Benutzer-Prioritätsinformationen
- 1 Bit **CFI** - Canonical Format Indicator – Gilt für alle vorhandenen MAC-Adressinformationen im MAC-Datenpaket des Frames. Wert 0 das Format ist kanonisch (am wenigsten signifikante Bit zuerst); Wert 1 Format nicht-kanonisch. Benutzung im Token Ring/Source-Routed- FDDI-Media-Zugang, um die Bit-Order der Adressinformationen des verkapselten Frames festzulegen
- 12 Bit **VID** - VLAN Identifier – Identifizierung des VLANs zu dem der Frame gehört



2.5	Asynchronous Transfer Mode
2.6	Internet Protocol
2.6.1	IPv4
2.6.2	IPv6
2.7	User Datagram Protocol
2.8	Transmission Control Protocol
3	Adressierung
4	ARP, RARP
5	DNS und WHOIS
6	Migration von IPv4 nach IPv6
7	Timeouts, ACK, Bestätigungen
8	Routingkonzepte
9	Quality of Service
10	Multicasts
11	Zeitsynchronisation
12	Internet Control Message Protocol
13	Voice over IP
14	World Wide Web und HTTP
15	Peer-to-Peer
16	E-Mail
17	Autokonfiguration
18	Dateien und Drucken
19	Telnet, SSH und rlogin
20	Extensible Messaging and Presence Protocol (XMPP)
21	LDAP
22	Authentication Protocols
23	Simple Network Management Protocol
24	Mac-Sublayer
25	Mobile Netzwerke
26	HTTP2 und SCTP

## Literatur

- [1] Janet Abbate. *Inventing the internet*. MIT press, 2000.
- [2] Paul Baran et al. On distributed communications. *Volumes I-XI, RAND Corporation Research Documents, August*, pages 637–648, 1964.
- [3] Paul Hoffman and Scott Bradner. Defining the ietf. 2002. <http://www.ietf.org/rfc/rfc3233.txt>.



