Netzwerke, Teil 1: Schichten und Ethernet

Handout zum Vortrag im CCC Freiburg

Balrog

2026-10-06

Schichtenmodelle

OSI	Name	TCP/IP	Einheit	Adresse	Beispiele	Gerät
7	Anwendung	Anwendung	Daten		HTTP, DNS, SSH, SMTP	
6	Darstellung	Anwendung	Daten		TLS, Zeichensätze	
5	Sitzung	Anwendung	Daten		(in der Praxis Teil der Anwendung)	
4	Transport	Transport	Segment	Port	TCP, UDP, QUIC	Firewall, Load Balancer
3	Vermittlung	Internet	Paket	IP-Adresse	IPv4, IPv6, ICMP	Router
2	Sicherung	Netzzugang	Frame	MAC-Adresse	Ethernet, WLAN, VLAN	Switch, Access Point
1	Bitübertragung	Netzzugang	Bit		Kupfer, Glasfaser, Funk	Kabel, Transceiver

Eselsbrücke von oben nach unten: **A**lle **P**riester **S**aufen **T**equila **N**ach **D**er **P**redigt.

Das Internet ist nach dem TCP/IP-Modell gebaut (RFC 1122). Es hat vier Schichten: OSI 5 bis 7 sind dort eine einzige Anwendungsschicht, OSI 1 und 2 heißen zusammen Netzzugang. Die OSI-Nummern sind das gemeinsame Vokabular: „Layer-2-Problem" heißt, es hakt zwischen Gerät und Switch; „Layer-3-Problem" heißt Adressen oder Routing.

Kapselung

Jede Schicht setzt ihren Header vor die Daten der Schicht darüber und gibt das Ganze nach unten weiter. Beim Empfänger packt jede Schicht ihren Teil wieder aus.

```
Anwendung                                [ Daten           ]
Transport                       [TCP-Hdr][ Daten           ]
Internet              [IP-Hdr ][TCP-Hdr][ Daten           ]
Netzzugang  [Eth-Hdr][IP-Hdr ][TCP-Hdr][ Daten           ][FCS]
```

Ein Switch liest nur den Ethernet-Header, ein Router zusätzlich den IP-Header.

Ethernet

Vom Bus zum Switch

Aufbau	Verkabelung	Zugriff auf die Leitung	Kollisionen
Koaxkabel (ab 1983)	ein Kabel für alle	Bus	alle Geräte in einer Collision Domain
Hub (ab 1990)	Stern	Bus im Kasten: Signal geht elektrisch an alle Ports	alle Ports in einer Collision Domain
Switch, Half-Duplex	Stern	je Port ein Bus mit zwei Teilnehmern	möglich, nur innerhalb des Ports
Switch, Full-Duplex	Stern	Punkt-zu-Punkt, beide Richtungen gleichzeitig	keine

Auf einem Bus regelt **CSMA/CD** den Zugriff: horchen, ob frei; senden; bei Kollision abbrechen und eine Zufallszeit warten. Mit Full-Duplex ist das abgeschaltet, ab 10 Gbit/s gibt es nur noch Full-Duplex.

Ein Switch ist eine Bridge mit vielen Ports. Daher heißt er unter Linux (`br0`), in Proxmox (`vmbr0`) und bei MikroTik (`/interface bridge`) auch so. Er nimmt jeden Frame vollständig an, prüft die Prüfsumme und sendet ihn neu. Aus den Absenderadressen lernt er, an welchem Port welches Gerät hängt, und schickt Frames nur dorthin.

Broadcasts und Frames an unbekannte Ziele gehen an alle Ports. Für diese Frames verhält sich das Netz bis heute wie ein Bus: einer ruft, alle hören.

MAC-Tabelle

Der Switch merkt sich zu jeder Absender-MAC den Port, an dem sie hereinkam. Beispiel aus dem Vortrag: A an Port 1, B an Port 3, C und D an Port 2 und 4, Tabelle anfangs leer.

Schritt	Frame	Switch lernt	Frame geht an
1	A an B	A hängt an Port 1	Port 2, 3, 4 (B unbekannt, *Flooding*)
2	B an A	B hängt an Port 3	nur Port 1
3	A an B	nichts Neues	nur Port 3

C und D bekommen den ersten Frame auch und verwerfen ihn, weil die Ziel-MAC nicht ihre ist. Ab Schritt 2 sehen sie vom Verkehr zwischen A und B nichts mehr.

Einträge ohne Verkehr verfallen, meist nach 300 Sekunden. Steckt ein Gerät um, lernt der Switch den neuen Port beim nächsten Frame. Ist die Tabelle voll, flutet der Switch alles wie ein Hub; genau das nutzt der Angriff *MAC-Flooding* aus.

Zwei Wege zwischen denselben Switches ergeben eine Schleife: Broadcasts kreisen ohne Ende (*Broadcast-Sturm*). Das *Spanning Tree Protocol* (STP) schaltet überzählige Wege ab.

Tabelle anzeigen: Linux `bridge fdb show`, MikroTik `/interface bridge host print`.

Kupferkabel dürfen pro Strecke höchstens **100 m** lang sein.

Collision Domain und Broadcast-Domain

- **Collision Domain:** Geräte, deren Signale sich auf der Leitung stören können. Am Switch höchstens ein Port, bei Full-Duplex gibt es keine.
- **Broadcast-Domain:** Geräte, die ein Broadcast erreicht. Alle Ports aller Switches im selben Netz bzw. VLAN, bis zum nächsten Router. In diesem Bereich gelten MAC-Adressen.

MAC-Adressen

48 Bit, geschrieben als sechs Byte hexadezimal: `d0:ea:11:dc:66:b5`.

Teil	Bedeutung
Byte 1 bis 3	Herstellerkennung (OUI), von der IEEE vergeben. `d0:ea:11` = Routerboard.com (MikroTik)
Byte 4 bis 6	vom Hersteller vergeben
Bit 0 von Byte 1	0 = einzelnes Gerät (Unicast), 1 = Gruppe (Multicast)
Bit 1 von Byte 1	0 = vom Hersteller, 1 = lokal vergeben

Besondere Adressen:

Adresse	Bedeutung
`ff:ff:ff:ff:ff:ff`	Broadcast, an alle in der Broadcast-Domain
`01:00:5e:…`	IPv4-Multicast
`33:33:…`	IPv6-Multicast

Handys und Laptops verwenden heute pro WLAN eine **zufällige, lokal vergebene MAC**, damit man sie nicht von Netz zu Netz verfolgen kann. Erkennbar an der zweiten Hex-Ziffer **2, 6, A oder E** (z. B. `a6:…` oder `3e:…`).

MAC-Adressen sind nicht routebar: Der Adressraum ist flach, aus der Adresse lässt sich kein Standort ablesen. Für den Weg über mehrere Netze gibt es IP-Adressen.

Aufbau eines Frames

Feld	Byte	Inhalt
Präambel + Start of Frame	8	Takt-Synchronisation, im Mitschnitt nicht sichtbar
Ziel-MAC	6	steht vorne, damit der Switch früh entscheiden kann
Absender-MAC	6	daraus lernt der Switch
802.1Q-Tag (optional)	4	`81 00` + Priorität + VLAN-Nummer
EtherType	2	was in der Nutzlast steckt
Nutzlast	46 bis 1500	z. B. ein IP-Paket. 1500 = **MTU**
Prüfsumme (FCS)	4	CRC32. Falsch → Frame wird verworfen. Im Mitschnitt meist nicht sichtbar
Pause (Interframe Gap)	12	Ruhezeit auf der Leitung

Ein Frame ist mindestens 64 und höchstens 1518 Byte lang (mit VLAN-Tag 1522), jeweils ohne Präambel und Pause.

Häufige EtherTypes:

Wert	Protokoll
`0x0800`	IPv4
`0x0806`	ARP
`0x86DD`	IPv6
`0x8100`	VLAN-Tag (802.1Q)
`0x88CC`	LLDP (Nachbarerkennung)

Beispiel aus dem Vortrag

Ein MikroTik-Switch meldet sich per Broadcast bei seinen Nachbarn (MNDP):

```
0000  ff ff ff ff ff ff  d0 ea 11 dc 66 b5  81 00 00 01
      Ziel: Broadcast    Absender: MikroTik VLAN 1
0010  08 00  45 00 00 69 ...
      IPv4   ab hier IP-Header
...
0040  73 77 2d 6b 30 2d 67 6c 61 73 31 ...   "sw-k0-glas1"
```

Begriffe

Begriff	Erklärung
Autonegotiation	Beide Seiten eines Kabels handeln Geschwindigkeit und Duplex aus. Schlägt das fehl, wird die Leitung langsam
Duplex	Half: abwechselnd senden. Full: beide Richtungen gleichzeitig
Flooding	Switch schickt einen Frame an alle Ports außer dem Eingangsport, weil er das Ziel nicht kennt
Frame	Dateneinheit auf Schicht 2
MAC-Tabelle	Liste im Switch: MAC-Adresse → Port, gelernt aus den Absenderadressen
MTU	Größte Nutzlast eines Frames, bei Ethernet 1500 Byte
OUI	Herstellerkennung, erste drei Byte der MAC
STP	Spanning Tree Protocol, schaltet Schleifen zwischen Switches ab
Trunk	Switch-Verbindung, die mehrere VLANs getaggt transportiert
VLAN	Logisch getrenntes Netz auf denselben Switches. Jedes VLAN ist eine eigene Broadcast-Domain

Zum Weiterlesen

- W. Richard Stevens, Kevin R. Fall, *TCP/IP Illustrated, Volume 1: The Protocols*, 2. Auflage 2011. Das Standardwerk, jedes Protokoll an echten Mitschnitten erklärt. Zu diesem Teil: Kapitel 1 (Schichten und Kapselung) und 3 (Link Layer, Ethernet, VLAN, Bridges).
- Charles E. Spurgeon, Joann Zimmerman, *Ethernet: The Definitive Guide*, 2. Auflage 2014. Alles über Kabel, Stecker, Geschwindigkeiten und Autonegotiation.
- Radia Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, 2. Auflage 1999. Von der Erfinderin des Spanning Tree, erklärt Bridges und Schleifen von Grund auf.
- RFC 1122 (TCP/IP-Schichten für Hosts), IEEE 802.3 (Ethernet) und IEEE 802.1Q (VLAN, Bridges). Die IEEE-Standards gibt es nach Registrierung kostenlos im Programm *IEEE GET*.

Bildquelle Schichtenmodell im Vortrag: Wikimedia Commons, `OSI_Model_v2.svg`, CC BY-SA 4.0. Frame-Tabelle nach de.wikipedia.org/wiki/Datenframe, CC BY-SA 4.0.