Kapitel 6: Layer 2

Aufgaben Layer 2

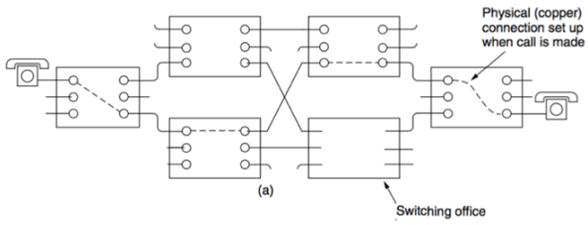
- Aufgaben Bitübertragungs- und Sicherungsschicht

Ziel: Übertrage einen Datenrahmen fehlerfrei von einem Gerät (Absender) am physischen Netz zu einem anderen Gerät (Empfänger) am selben physischen Netz.

Leitungsvermittlung oder Paketvermittlung

Leitungsvermittlung (engl. circuit switching)

Idee: Beim Verbindungsaufbau wird eine dedizierte Leitung für genau diese Verbindung geschaltet



Vorteile:

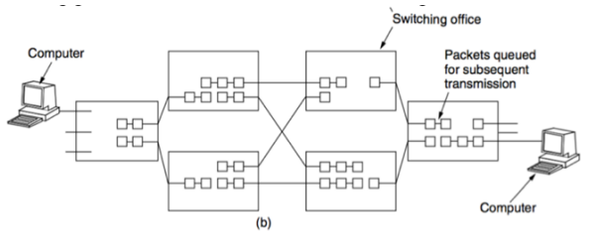
- Nach erfolgtem Verbindungsaufbau schnelle Datenübertragung.
- Garantierte Bandbreite für jede Verbindung.

Nachteile:

- Verbindungsaufbau erforderlich, bevor Daten transportiert werden.
- Verbindungsaufbau ist komplex und dauert.
- Verbindungsaufbau kann schief gehen („Besetzt“)
- Ungenutzte Übertragungskapazitäten

Paketvermittlung (engl. packet switching)

Idee: Teile Datenstrom in einzelne Pakete, die dann nacheinander auf den Weg gebracht werden. Jedes Paket muss den Weg zum Ziel „alleine“ finden.



Vorteile:

- Kein Verbindungsaufbau erforderlich.
- Bei Leitungsstörungen können „Umwege“ gewählt werden.
- Vermittlungsstelle kann Paket 1 weiterleiten, während parallel Paket 2 gerade eintrifft.
- Übertragungskapazitäten besser ausnutzbar.

Nachteile:

- Pakete können verloren gehen oder sich gegenseitig überholen.
- Keine garantierte Bandbreite (Dienstgüte) möglich.
- Jedes Paket muss adressiert werden.

- Layer 2 beschäftigt sich mit der Kommunikation zweier Stationen, die durch einen direkten Übertragungskanal (z. B. ein Kabel) verbunden sind.
- Heute wird Paketvermittlung statt Leitungsvermittlung bevorzugt, da es flexibler ist und eine bessere Auslastung der Übertragungskapazitäten erlaubt. Je nach Netztopologie existieren verschiedene Medienzugriffsverfahren. Bei gemeinsam genutzten Medien wird eine Zugriffssteuerung benötigt.
- Statt Bitstrom werden auf Layer 2 Daten-Rahmen (engl. frame) versendet. Es gibt verschiedene Rahmenstandards. In ihnen werden Hardware-Adressen (MAC-Adressen) der jeweiligen Netzwerkhardware verwendet.
- Ethernet und WLAN sind zwei häufig benutzte Techniken in lokalen Netzen. Aktive Netzkomponenten wie Repeater, Hubs, Switches oder Bridges verbinden Stationen in einem LAN.

Paketerkennung

Trennung einzelner Pakete

(1) Pause zwischen Paketen

- **Einfügen von Begrenzungslücken**: Pause zwischen den Paketen.
- **Problem mit Begrenzungslücken**: Bei den Übertragungen kann es zu Verzögerungen kommen, so dass neue Lücken entstehen oder bestehende Lücken verschwinden. Zeitabläufe sind daher nicht verlässlich.

(2) Zählen der Bytes

- Benutze ein Längenfeld (Zahl der Zeichen im Paket) am Beginn eines Pakets. **Beispiel:**
- Was passiert wenn bspw. ein Bit kippt?
- Im Beispiel ist im zweiten Datenrahmen im Zähler für die Anzahl der Bytes ein Bit gekippt. Statt der 5 wurde 7 übertragen. Die empfangende Station geht daher von 7 Zeichen im zweiten Datenrahmen aus.

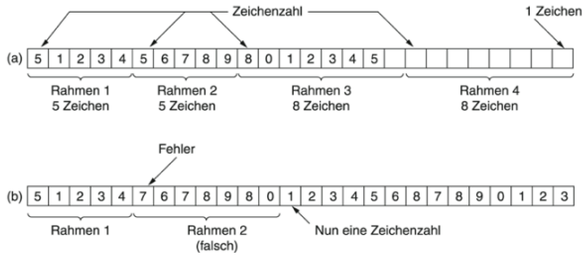
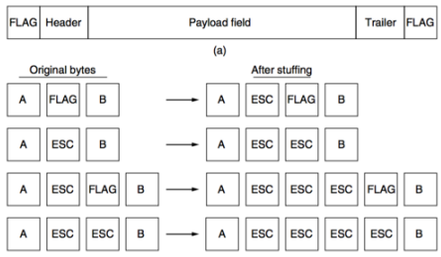


Abbildung 3.4: Ein Zeichenstrom: (a) ohne Fehler (b) mit einem Fehler

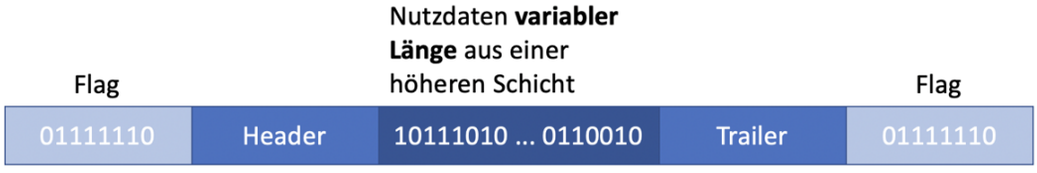
(3) Byte Stuffing

- **Idee**: Jeder Rahmen beginnt und endet mit einem speziellen Byte, genannt FLAG.
- **Problem**: Was ist, wenn dieses Byte irgendwo im Rahmen vorkommt?
  Lösung: Maskiere FLAG-Byte im Rahmen mit einem anderen speziellen Byte, genannt ESC.



(4) Bit Stuffing

- **Idee**: Jeder Rahmen beginnt und endet mit demselben Byte, nämlich: 011111102 oder 7E16.
- **Problem**: Was ist, wenn dieses Byte irgendwo im Rahmen vorkommt? Lösung: Füge nach fünf 1-Bits im Rahmen ein 0-Bit ein.



Medienzugriff

Grundsätzliche Eigenschaften von Topologien

Gemeinsames Medium:

- Hierbei teilen sich alle angeschlossenen Stationen (Rechner) dasselbe Übertragungsmedium.
  Beispiele: klassisches Ethernet, WLAN, Internet über Fernsehkabel

Probleme: Durcheinander senden ergibt unverständlichen „Funksalat“.
Lösung: Steuere (engl. to control) den Zugriff auf das Übertragungsmedium.
Im ISO-Protokollstack ist dafür im Layer 2 der Sublayer Medium Access Control (MAC) zuständig.

Dediziertes Medium:

- Hierbei steht ein Übertragungsmedium einer Station exklusiv zur Verfügung.
  Beispiele: Telefonleitung, switched Ethernet

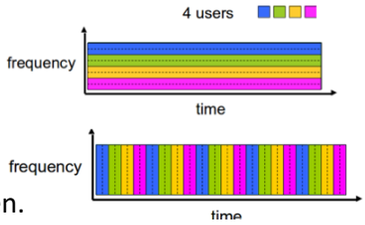
Grundsätzliche Steuerungsmöglichkeiten

Feste Kanalaufteilung, d. h. das Medium wird nach bestimmter Vorschrift fest aufgeteilt.
  - Verschwendet Bandbreite. (FDM|TDM)

Zufallszugriffsverfahren, d. h. bei Bedarf greift die Station einfach auf das Medium zu.
  - Kollisionen (zwei Stationen senden gleichzeitig) müssen behandelt werden.
  - Bessere Nutzung der Bandbreite.

Zyklische Zuteilung, Zugriffsberechtigung geht reihum. Stationen senden erst wenn sie die Sendeberechtigung haben.
  - Realisierung durch spezielles token. Nur der Besitzer darf senden.
  - Das Token geht reihum, es liegt ein token ring vor.

Feste Kanalaufteilung

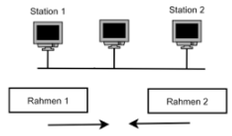


Frequency Division Multiplexing (FDM): Die verfügbaren Frequenzen werden auf die Stationen verteilt. Station kann jederzeit auf „ihrer" Frequenz senden.

Time Division Multiplexing (TDM): Das Frequenzspektrum wird in Zeitscheiben eingeteilt. Die Zeitscheiben werden auf die Stationen verteilt, z. B. Round Robin. Station muss ggf. warten.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

Ablauf des Verfahrens:



- **Prüfe, ob Medium belegt**. Sende nur bei freiem Medium.
- **Während des Sendens:** Lese parallel mit, um Kollisionen zu erkennen.
- **Falls Kollision erkannt**: Abbruch der Übertragung und warte eine „zufällig" gewählte Zeit (engl. backoff).

Entstehung einer Kollision: Eine Station beginnt mit Senden, da Medium frei. Zweite Station beginnt mit Senden, während die Signale der ersten Station noch unterwegs sind.

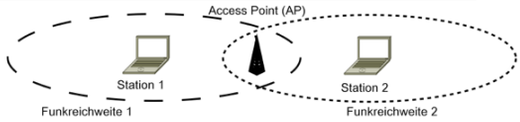
Wartezeit mit Exponential Backoff

Ziel:

- **Stationen warten unterschiedlich lang**, damit nicht alle zur gleichen Zeit einen erneuten Sendeversuch starten.
- **Wartezeit steigt mit Anzahl der Sendeversuche**, da häufige Kollisionen ein Zeichen für Netzüberlastung sind. Dann sollte länger gewartet werden, bis die Überlast vorbei ist.

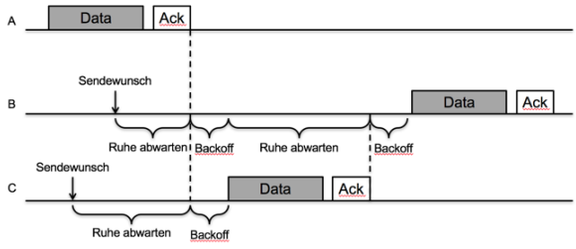
Voraussetzungen und Eigenschaften von CSMA/CD

- Stationen müssen während des Sendens auch Empfangen können (kann WLAN nicht)
- Mit Kollisionsdomäne wird der Teil eines Netzes bezeichnet, in dem mehrere Stationen angeschlossen sind, die um den Zugriff konkurrieren und wo Kollisionen entstehen können.
- Je mehr Stationen in einer Kollisionsdomäne sind, umso größer wird die Kollisionswahrscheinlichkeit.
- ~~Kollisionen sind kein Fehler im Netz, sondern ein Normalfall. Allerdings sollten sie nicht zu häufig auftreten.~~
- ~~Die Länge eines Netzes darf nicht zu groß werden, da 2 x τ gewartet werden muss, bevor klar ist, dass die Übertragung kollisionsfrei war.~~



WLAN-Problem: Station 1 kann eine Kollision mit Station 2 nicht erkennen. Auch als **Hidden-Station-Problem** bezeichnet.
Lösung: Empfänger muss bei kollisionsfreiem Empfang immer eine Bestätigung (engl. acknowledge) senden. Erst nach Empfang der Bestätigung weiss der Absender, dass es gut gegangen ist.

Ablauf CSMA/CA (ohne Hidden Station)



1) Sender wartet auf Ruhe (carrier sense)
2) Sender wartet zufällige backoff-Zeit.
3) Falls inzwischen belegt, goto 1 sonst senden.
4) Auf Bestätigung warten.

Verbesserung für Hidden-Station-Problem

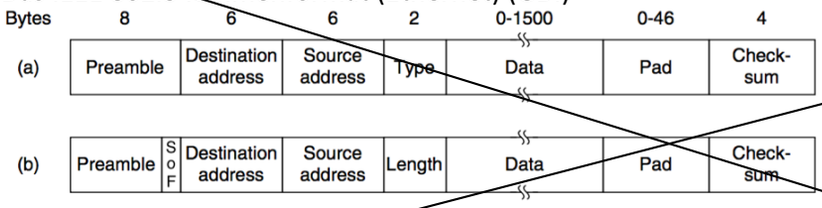
Idee: Bevor der ganze Rahmen gesendet wird, vorher testen, ob es auch gut gehen wird.
Beispiel Station 1 will Rahmen X an AP senden:

- Station 1 sendet Request to send (RTS) mit Rahmenlänge von X.
- Alle Nachbarn von Station 1 inkl. AP hören das RTS. Sie machen Pause bis Clear to send (CTS) angekommen ist.
- AP sendet ein CTS mit der erwarteten Sendezeit an Station 1.
- Alle Nachbarn von AP hören das CTS und pausieren die angegebene Zeit. Station 1 sendet jetzt den geplanten Rahmen X an AP.
- AP sendet ACK an Station 1.

Kollisionen entstehen nur noch bei zwei gleichzeitigen RTS. Der Access Point sendet dann kein oder nur ein CTS.

Ethernet und WLAN Rahmenformate

Das IEEE 802.3 Rahmenformat (Ethernet) (GDI)



- Die Präambel (engl. preamble) besteht aus 8 Bytes und dient der Synchronisierung mit dem Empfänger.
- Empfänger (engl. destination) und Absender (engl. source) Adressen sind jeweils 6 Bytes lang.
- Zu kurze Rahmen werden im Padding-Feld auf die Mindestlänge von 64 Bytes gebracht.

Ethernet-Adressen / MAC-Adresse Media Access Control

- 6 Bytes lang *(Hexadezimal)*

Beispiel: Mac-Adresse: 00:15:c5:60:7c:8a

Herstelleranteil: 00:15:c5 (entspricht Firma Dell)

Kartenadresse: 60:7c:8a

- **Einzeladressen** *(normale)* beginnen mit **0**
- **Gruppenadressen** beginnen mit 1 (nur als Ziel)
- **Multicast-Adressen**: spricht eine Gruppe von Rechnern an
- **Broadcast-Adresse**: FF:FF:FF:FF:FF:FF => spricht alle Rechner im Netzwerk an (alle Bits auf 1 gesetzt)

→ In lokalen Netzen sollten Ethernet-Adressen eindeutig sein

Einige wichtige Ethernetstandards

- **10BASE-T**: Bietet 10 MBit/s auf Twisted Pair Kabeln
- **100BASE-TX**: Bietet 100 MBit/s auf CAT 5 Twisted Pair Kabeln (auch Fast-Ethernet genannt; IEEE 802.3u)
- **1000BASE-T**: Bietet 1.000 MBit/s auf CAT 5 Twisted Pair Kabeln (auch Gigabit-Ethernet genannt; IEEE 802.3ab)
- **1000BASE-TX**: Bietet 1.000 MBit/s auf CAT 6 Twisted Pair Kabeln
- **1000BASE-LX**: Bietet 1.000 MBit/s auf Glasfaser (IEEE 802.3z)
- **10GBASE-T**: Bietet 10.000 MBit/s auf CAT 6e Twisted Pair Kabeln (IEEE 802.3an)
- **10GBASE-SR**: Bietet 10.000 MBit/s auf Multimode Glasfaser

WLAN-Betriebsmodi

Ad-hoc Modus 2 WLAN-Stationen kommunizieren direkt miteinander

Point-to-Point-Modus: Hierbei kommunizieren zwei Access Points über ein WLAN miteinander

***Point-to-Point-Modus**: Wireless Bridge*

***Point-to-Multipoint-Modus**: Wireless Repeater*

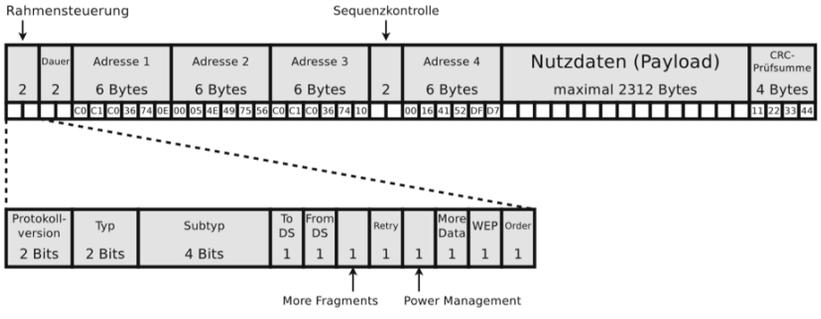
Infrastruktur-Modus 2 WLAN-Stationen kommunizieren nicht direkt miteinander, sondern über einen Access Point

WLAN Rahmenformat

Mehrere Adressen, da über Access Point die Pakete vermittelt werden und die Access Points müssen auch adressiert werden

WLAN-Rahmen haben Maximalgröße von 2346 Bytes (Ethernet: 1518 Bytes).

Es gibt verschiedene WLAN-Rahmentypen: Management, Control, Data und Extension



Einige wichtige WLAN-Standards

IEEE 802.11: Normenfamilie für WLAN

- **802.11**: ursprünglicher Standard, 1997, bis zu 2 Mbit/s brutto
- **802.11a und 802.11b**: 1999 (802.11a mit 5 GHz seit 2002 in Deutschland freigegeben), bis zu 54 Mbit/s brutto für 5 GHz
- **802.11n**: 2009, bis zu 150 Mbit/s brutto
- **802.11ac**: Erweiterung von 802.11n, 2013, rechnerisch bis zu 6936 Mbit/s mit MIMO (verwendet mehrere Antennen gleichzeitig) möglich, nur 5 GHz
- **802.11ad**: Entwurf aus 2012, auch Wireless Gigabit genannt, 60 GHz, bis zu 6930 Mbit/s möglich
- **802.11ah**: 2016, auch Wi-Fi HaLow genannt, 900 MHz (!), für Smart Homes und Maschine-zu-Maschine-Kommunikation gedacht

Wichtigsten Eigenschaften

- Komplexere Zugriffskontrollen auf das Übertragungsmedium und eine Kollisionserkennung sind erforderlich
  → Niedrigere Datenübertragungsraten als bei kabelgebundenen Netzen
- Sicherheitsprobleme

Fehlererkennung

Zweck der Fehlererkennung:

- Erkenne solche Störungen sicher.
- Reagiere sinnvoll auf Fehler

Mögliche **Reaktion bei Fehlern**:

- Ignoriere Fehler (Sehr schlecht)
- Behebe Fehler, wenn möglich.
- Verwerfe fehlerhafte Datenrahmen.
- Übertrage fehlerhafte Rahmen erneut.

Single Bit Parity

Idee: Füge redundante Daten in einen Datenrahmen ein, mit denen dann Fehler erkannt werden.

Beispiel: Benutze ein zusätzliches Bit, das immer so gesetzt wird, dass die Zahl der Einsen gerade ist *(gerade Parität).*

- *Das ist der Grund, warum im ASCII-Code nur 7-Bit eines Bytes für die Zeichencodierung benutzt werden. Das oberste (achte) Bit kann als Paritätsbit benutzt werden.*

Eigenschaften:

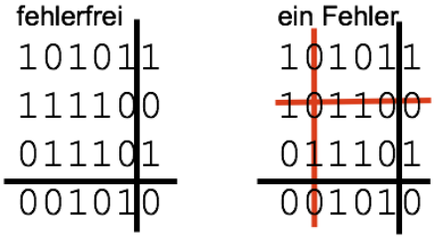
- Erkennt ein falsches (umgekipptes) Bit.
- Zwei umgekippte Bits werden nicht erkannt.
- Die Position des gekippten Bits ist unklar.

Zweidimensionale Bitparität

Idee: Betrachte den Datenrahmen als zweidimensionale Matrix und berechne Paritätsbits für jede Zeile und jede Spalte.

Eigenschaften:

- Einzelne Bitfehler kann lokalisiert und korrigiert werden.
- Mehrbit-Fehler können nur teilweise erkannt werden.



Cyclic Redundancy Check (CRC)

Bei Funkübertragungen häufig benutzes Verfahren zur Fehlererkennung.

Idee: Prüfe Korrektheit durch Polynomdivision mit Rest.

Benutze eine Funktion und nehme die Bit im Rahmen und berechne darüber ein Polynom und übertrage diesen CRC-Wert.

Ablauf:

- Voraussetzung: Algebra in Polynomringen, Polynome über Z2
- Interpretiere den Datenrahmen D als Binärzahl. Jede Ziffer der Binärzahl ist der Koeffizient eines Polynoms D(x). Bei k Bit im Rahmen hat das Polynom den Grad k − 1.
- Sender und Empfänger vereinbaren eine Generatorzahl G und damit auch ein Generatorpolynom G(x).
- Eine Prüfsumme P ergänzt Binärzahl D so, dass sie ohne Rest durch G teilbar wird.
- Sei D = 1101011011. Dann ist D(x) = x9 + x8 + x6 + x4 + x3 + x + 1. Für
- G = 10011 ist G(x) = x4 + x + 1. (Die Kunst besteht in der Auswahl des Generatorpolynoms.)
- Polynomdivison mit Rest durchführen: Rest entspricht CRC-Wert.

Anwendung in Ethernet, Bluetooth, ext4, gzip, PNG, GSM, ISDN, AES, etc.

Aktive Netzkomponenten

Repeater, Hub und Bridge

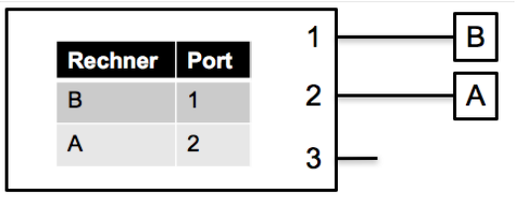
- **Signalverstärker** (engl. repeater) kompensieren die Leitungsdämpfung, indem sie die Signale wieder „auffrischen“. Dabei werden aber auch Störungen „aufgefrischt“.
- **Ein Hub** ist ein Gerat, dass ein klassisches Bus-Ethernet in sternförmiger Verkabelung erlaubt.
- **Ein Hub** übertragt empfangene Datenrahmen an alle an den Hub angeschlossenen Stationen.
- **Eine Bridge** nimmt ganze Rahmen entgegen, prüft diese mit Hilfe der Prüfsummen auf Fehler und leitet nur fehlerfreie Rahmen weiter.
- **Eine Bridge** kann auch unterschiedliche Rahmenformate umwandeln oder unterschiedliche Geschwindigkeiten ausgleichen.
- **Einfache Bridges haben 2 Anschlüsse. Multiport-Bridges mit mehr als 2 Anschlüssen werden auch Switch genannt**.

(Layer-2-)Switch

- **Switche** nehmen Datenrahmen entgegen und leiten diese i. d. R. **nur** an den **adressierten Empfänger weiter**.
- Anhand der MAC-Zieladresse wird der Port ausgewählt, an den weitergeleitet wird.
- Zwei Ports (Anschlüsse) zwischen denen Daten fließen sollen werden direkt miteinander „verbunden“.
- Ist an jeden Switch-Port nur ein Rechner angeschlossen, so können keine Kollisionen mehr auftreten.
- Broadcasts sind aber nach wie vor möglich.
- Problem: Woher weiß ein Switch, an welchem Port eine Station mit einer gegebenen MAC-Adresse angeschlossen ist?

Funktionsweise eines Switch

- Weiß der Switch nicht, an welchen Port welche Station angeschlossen ist, dann leitet er den Rahmen einfach an alle Ports weiter. (Broadcast)
- Anhand der Absender-MAC-Adresse eines Rahmens lernt der Switch welche Station an welchen Port angeschlossen ist.



Ein Switch benutzt eine interne Tabelle mit MAC-Adresse und Port-Zuordnung.

Layer-n-Switch

Layer-3-Switch

- Multifunktionsgerät: Kombination aus Layer-2-Switch und einem Router (Ein Router arbeitet auf Layer 3).
- Meist als Hochleistungs-Switches entwickelt
- Beherrscht das Zuweisen von einzelnen Switch-Ports (Layer 2) und zusätzlich das Routing von Paketen (Layer 3).

Layer-4-Switch

- Kann zwischen TCP und UDP unterscheiden.
- Kennt das Konzept von Ports.
- Ermöglicht bspw. die Priorisierung von Datenverkehr je nach Applikation.

Layer-4-7-Switch

- Versteht Protokolle bis Layer 7
- Ermöglicht bspw. Lastverteilung

Layer-7-Switch:

- Lastverteilung auf Basis von URLs bspw. in CDNs.