

Inhalt der Vorlesung „Rechnerkommunikation“

- ✓ Einführung
- ✓ Anwendungsschicht
- ✓ Transportschicht
- ✓ Netzwerkschicht
- **Sicherungsschicht**
- Physikalische Schicht

Sicherungsschicht

- Einführung
- Adressierung
- Datensicherung
- Medienzugriff
- Ethernet
- Drahtlose LANs

Einführung

■ Terminologie

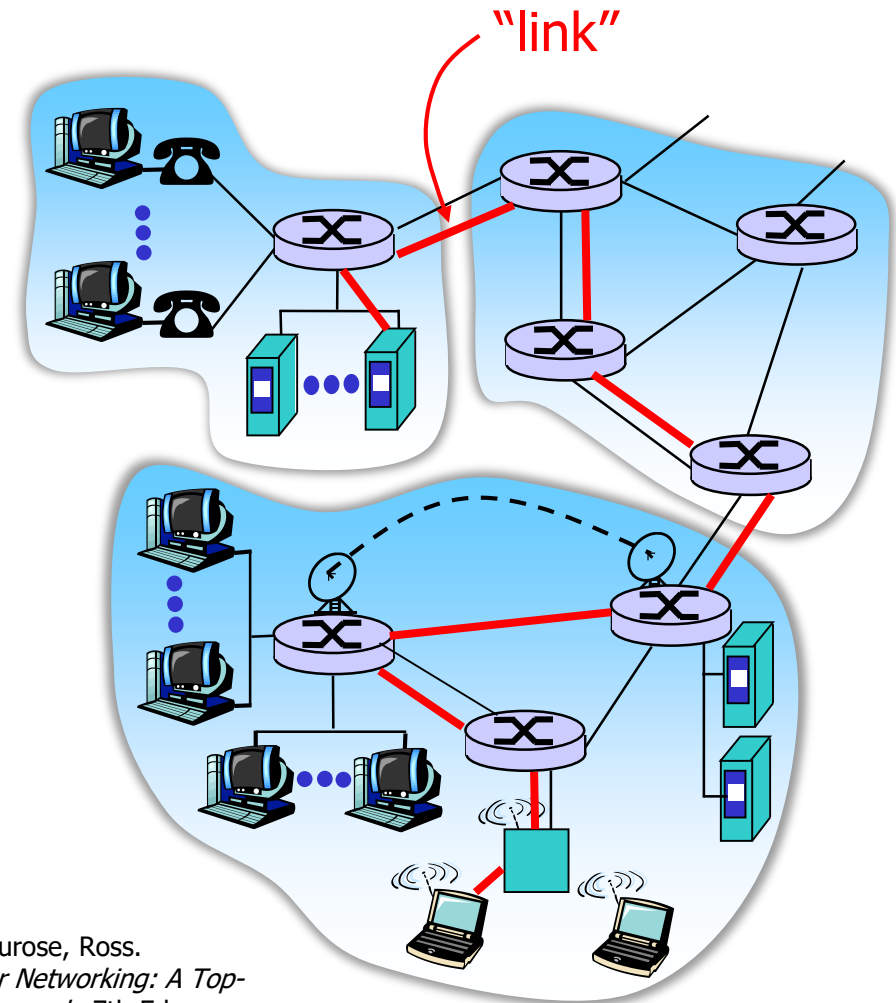
- Host, Router sind **Knoten (Nodes)**
- Kommunikationskanäle (**Links**)
- Dateneinheiten sind **Rahmen (Frames)**

■ Beispiele

- lokales Netz, Ethernet
- lokales Netz, WLAN
- Router über optisches Transportnetz
- Router über DSL

■ Aufgabe der Sicherungsschicht

- **Transfer der Rahmen zwischen Knoten über Links**



Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Einführung

■ Dienste der Sicherungsschicht

- Datagramm der Netzwerkschicht in Rahmen ein-/auspacken
- Adressierung: Rahmen enthält **physikalische Adresse** der Knoten
- **Datensicherung**
- **Medienzugriff (Medium Access, MAC)**
- eventuell Flusskontrolle

keine doppelte flusskontrolle auf 2 und d3

■ Adapter

- Funktionalität meistens in Netzwerkadapter bzw. -karte
- Schnittstellen zum Systembus des Knotens und zum Netzwerk
- Funktion in HW/SW/FPGA
- **Programmed I/O (PIO)**: CPU transferiert Daten zwischen Speicher und Adapter unter Verwendung von Statusregistern und Unterbrechungen
- **Direct Memory Access (DMA)**: Adapter liest und schreibt selbst
- Gerätetreiber im Betriebssystem

Einführung

■ Entwicklung von LANs, MANs und PANs (u.a.)

● Local Area Networks (LANs)

- klassisches Ethernet mit Bustopologie, Koaxialkabel, IEEE 802.3, veraltet
- Token Ring mit Ringtopologie, IEEE 802.5, veraltet
- Switched Ethernet (Stern- und Baumtopologie, Hubs, Switches, Twisted Pair, Glasfaser), IEEE 802.3
- Time Sensitive Networks (TSN), Industrial Ethernet, Erweiterung von Ethernet für Echtzeit, IEEE 802.1 Working Group
- Drahtlose LANs, IEEE 802.11

● Metropolitan Area Networks (MANs)

- Fiber Distributed Data Interface (FDDI): Doppelring, ISO 9314, veraltet
- Carrier Ethernet, Metropolitan Ethernet, basierend auf Ethernet, Metro Ethernet Forum
- Worldwide Interoperability for Microwave Access (WiMAX): Fixed (Versorgung von Hotspots, drahtloser Hausanschluss), Mobile (Versorgung mobiler Nutzer), IEEE 802.16
- Mobilfunk gemäß 4G (LTE), bzw. 5G

←
konkurrenten

Einführung

- Personal Area Networks (PANs)
 - Bluetooth, IEEE 802.15.1, „Kabelersatz“ für die Verknüpfung von Geräten, Daten- und Sprachkanäle
 - ZigBee, IEEE 802.15.4, preiswerter, geringe Datenraten, lange Batterielebensdauern, kleine Codegröße, für Heim-, Gebäude-, Industrieautomatisierung, eingebettete Geräte
 - Ultra-Wideband (UWB), große Datenraten (> 500 Mbps) über kurze Entfernungen, Hindernisse (wie Wände) können durchdrungen werden, IEEE 802.15.3a, 802.15.4a
- Außerdem positionsfinden
 - Low Power Wide Area Networks (LPWAN), für Internet-of-Things (IoT), z.B. LoRaWAN
 - Power-line Communication (PLC), z.B. Broadband over Power Lines (BPL), Narrowband
 - Near Field Communication (NFC), für RFIDs, Abstand wenige Zentimeter
 - Satellitenkommunikation
 - ...

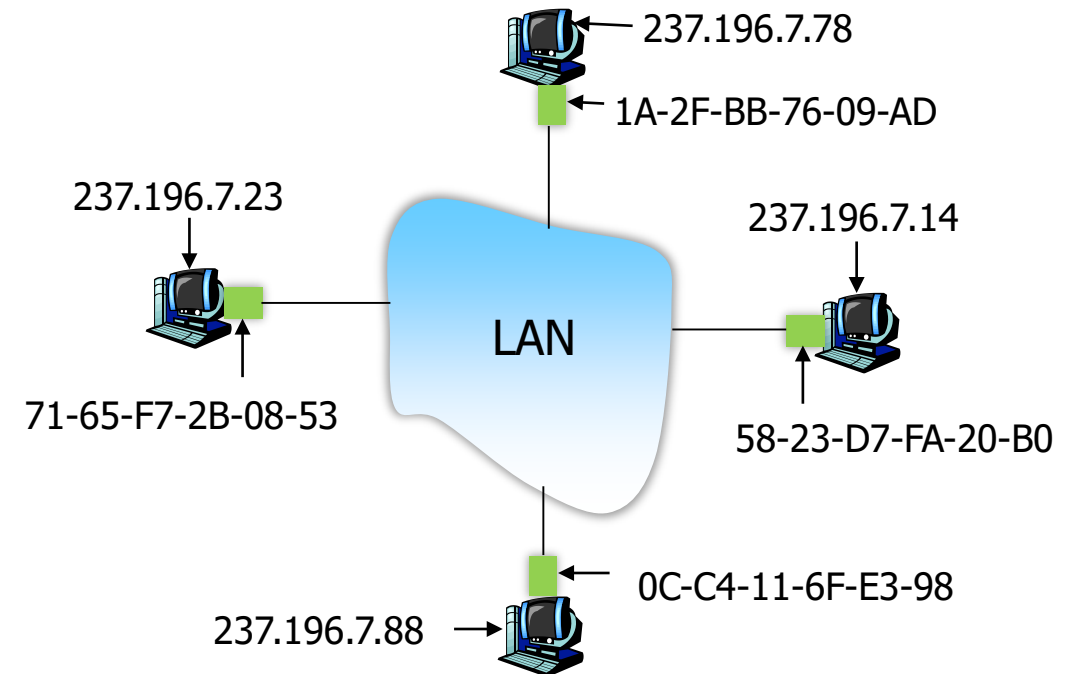
Sicherungsschicht

- ✓ Einführung
- Adressierung
- Datensicherung
- Medienzugriff
- Ethernet
- Drahtlose LANs

Adressierung

■ Physikalische Adresse

- auch MAC-Adresse, LAN-Adresse
- 48 Bits, 6 Bytes, 12 Hexadezimalziffern
- in den ROM des Adapters eingebrannt
- Verwaltung durch IEEE, kann von Herstellern gekauft werden
- global eindeutig
- keine Strukturierung es gibt aber "typische Formen"
- ≠ IP-Adresse
- Frage: IP-Adresse eines Zielknotens bekannt, wie wird physikalische Adresse gefunden?



Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Adressierung

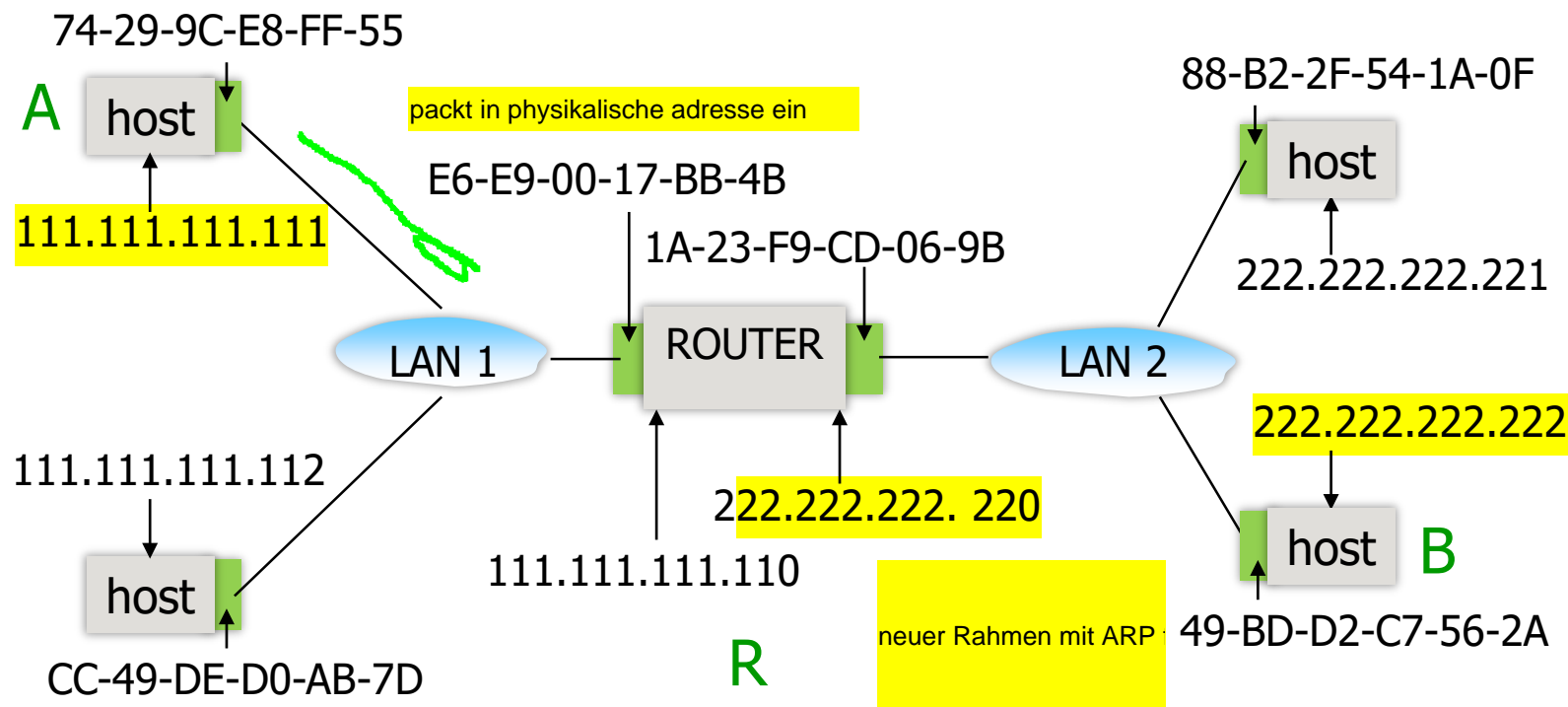
■ Address Resolution Protocol (ARP)

- jeder Knoten besitzt ARP-Tabelle mit Zuordnungen (IP-Adresse, physikalischer Adresse, TTL)
- Time To Live (TTL): Dauer der Gültigkeit des Eintrags, z.B. 20 Minuten
- Knoten A möchte an B Rahmen schicken, kennt IP-Adresse, aber nicht physikalische Adresse von B
- A sendet ARP-Anfrage als Broadcast (Adresse FF-FF-FF-FF-FF) mit seiner physikalischen Adresse und der IP-Adresse von B
- B erkennt sich als Ziel an IP-Adresse in der ARP-Anfrage und sendet in ARP-Antwort seine physikalische Adresse an die physikalische Adresse von A
- A speichert die Zuordnung der Adressen von B in seiner ARP-Tabelle
- Autonomie, „Soft State“

Adressierung

■ Beispiel

- A in LAN1 sendet IP-Datagramm von A über R zu B in LAN2
- A kennt IP-Adresse von B
- R benötigt für jedes LAN eine ARP-Tabelle



Quelle: Kurose, Ross.
*Computer Networking:
A Top-Down Approach*,
7th Ed., Pearson
Education, 2017.

Adressierung

- A erzeugt Datagramm mit IP-Quelladresse A und IP-Zieladresse B
- A findet R in seiner Routingtabelle
- A benutzt ARP um die physikalische Adresse des Adapters von R an LAN1 zu finden
- A erzeugt einen Rahmen mit sich als physikalischer Quelladresse, physikalische Zieladresse ist der Adapter von R an LAN1 (die IP-Zieladresse im eingepackten Datagramm bleibt B!)
- der Adapter von A sendet den Rahmen auf LAN1
- R's Adapter in LAN1 empfängt den Rahmen und packt das Datagramm aus, liest die IP-Zieladresse B, findet in der Routingtabelle heraus, dass B in LAN2 ist
- R benutzt ARP um die physikalische Adresse von B zu finden
- R erzeugt einen Rahmen mit seinem Adapter in LAN2 als physikalischer Quelladresse und B als physikalischer Zieladresse (die IP-Quelladresse bleibt A!)
- R's Adapter in LAN2 versendet den Rahmen
- B's Adapter empfängt den Rahmen und liefert das Datagramm aus

Sicherungsschicht

- ✓ Einführung
- ✓ Adressierung
- **Datensicherung**
- Medienzugriff
- Ethernet
- Drahtlose LANs

Datensicherung

■ Fehlercharakteristika

- thermisches Rauschen, elektromagnetische Einstrahlung (Übersprechen, Motoren, Zündanlagen), radioaktive Einstrahlung
- typische Bitfehlerwahrscheinlichkeiten: 10^{-3} (Funk) bis 10^{-12} (Glasfaser)
- oft treten Fehler als **Bursts** (Schübe, Bündel) auf

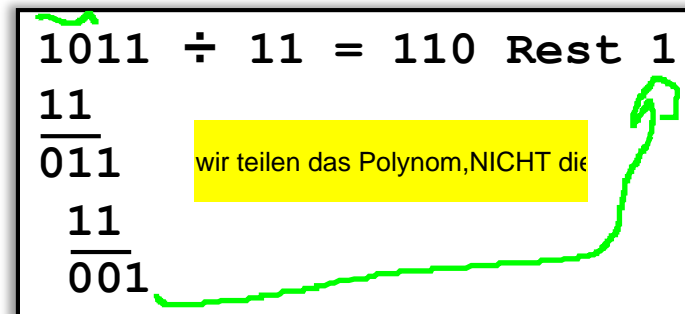
■ Ansätze zur Datensicherung

- **Fehlererkennung**: den Nutzdaten werden zusätzlich Prüfdaten zugefügt, um Fehler beim Empfänger zu erkennen und eine Sendewiederholung zu veranlassen, z.B. **Paritätsprüfung**, **zyklische Redundanzprüfung**
- **Fehlerkorrektur**: die Nutzdaten werden redundant kodiert, der Empfänger kann Fehler erkennen und korrigieren
 - n Bits Nutzdaten in m Bits gesendete Daten, $m > n$, z.B. mit **Block- und Faltungs-Codes**
 - Redundanz größer als für Fehlererkennung, wird typisch in **stärker gestörten Kanälen und bei hohen Latenzanforderungen verwendet**
- hybride Verfahren, z.B. **Hybrid ARQ**

Datensicherung

■ Zyklische Redundanzprüfung (Cyclic Redundancy Check, CRC)

- Bitfolgen werden als **Koeffizienten eines binären Polynoms** interpretiert:
 $(b_{n-1}, b_{n-2}, \dots, b_1, b_0)$ entspricht $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x^1 + b_0x^0$
z.B. (10011001) entspricht $x^7 + x^4 + x^3 + x^0$ die 1 an siebter stelle (beginnend bei 0!) liefert x^7
- algebraisch: Polynomring über $(0,1)$ -Körper mit Modulo-2-Arithmetik
- Operationen
 - Addition = Subtraktion = XOR (jeweils stellenweise, ohne Übertrag)
z.B.: $(0011) + (0101) = (0110)$
 - Multiplikation mit Potenz x^n entspricht Multiplikation der Binärzahl mit 2^n bzw. einer **Schiebeoperation um n Bits**
z.B. $(x^2 + x) \cdot x^4 = x^6 + x^5$ entspricht $(0110)_2 \cdot 2^4 = (01100000)_2$
 - **Division wie im 10er-System (euklidische Division):**

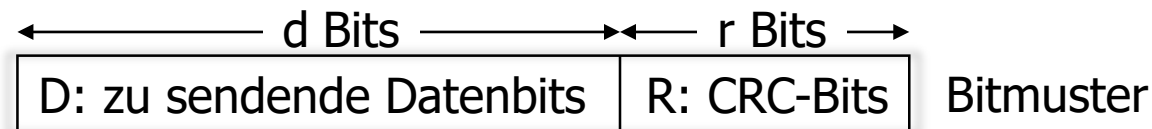

$$\begin{array}{r} 1011 \div 11 = 110 \text{ Rest } 1 \\ \underline{11} \\ 011 \\ \underline{11} \\ 001 \end{array}$$

wir teilen das Polynom, NICHT die

Datensicherung

■ Prinzip bei CRC

- Nutzdaten D mit d Bits, Prüfdaten R mit r Bits, Senden von (D,R)
- Generatorpolynom G , $r+1$ Bits
- Sender wählt R so, dass (D,R) ohne Rest durch G teilbar ist:
 - R ist Rest bei $D \cdot 2^r \div G$
 - (D,R) entspricht $D \cdot 2^r + R$ und ist ohne Rest durch G teilbar
 - Beweis: $D \cdot 2^r = n \cdot G + R$, also $D \cdot 2^r + R = n \cdot G$ ($n > 0$ natürliche Zahl) weil hier plus=minus
- Empfänger teilt (D,R) durch G , kein Fehler falls Rest = 0



$$D * 2^r \text{ XOR } R$$

Formel

Datensicherung

■ Beispiel

- $D = (101110)$, $G = (1001)$, $r = 3$

- $D \cdot 2^r = (101110000)$

wir schieben um 3 stellen

- $R = (011)$

- $D \cdot 2^r + R = (101110011)$

wir wollen drei redundanzen hinzufügen also p

$$101110000 \div 1001 = 101011 \text{ Rest } 011$$

$$\begin{array}{r} 1001 \\ \underline{00101} \\ 0000 \\ \underline{01010} \\ 1001 \\ \underline{00110} \\ 0000 \\ \underline{01100} \\ 1001 \\ \underline{01010} \\ 1001 \\ \underline{0011} \end{array}$$

Datensicherung

■ Implementierung

- euklidische Division kann leicht und effizient durch Schieberegister und XOR-Gatter in HW durchgeführt werden
- verbreitete genormte Generatorpolynome z.B.
 - CRC-8 (ITU-T) = $x^8 + x^2 + x + 1$
 - CRC-16 (IBM) = $x^{16} + x^{15} + x^2 + 1$
 - CRC-16 (ITU-T) = $x^{16} + x^{12} + x^5 + 1$
 - CRC-32 (IEEE 802.3) = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

■ Eigenschaften bei der Fehlererkennung

- alle Einzelbitfehler, wenn Koeffizienten von x^r und x^0 gleich Eins
- alle Doppelbitfehler, falls G unzerlegbaren Faktor mit mindestens 3 Termen enthält
- jede ungerade Bitfehlerzahl, falls G den Faktor $(x+1)$ enthält
- jeder Fehlerburst, der kürzer als r Bits ist (die meisten längeren Fehlerbursts können ebenfalls erkannt werden)

Sicherungsschicht

- ✓ Einführung
- ✓ Adressierung
- ✓ Datensicherung
- **Medienzugriff**
 - feste Kanalaufteilung
 - Zufallszugriff
 - zyklische Zuteilung
- Ethernet
- Drahtlose LANs

Medienzugriff

■ Punkt-zu-Punkt-Verbindungen

- nur die zwei Endpunkte greifen auf das Medium zu, z.B.
 - Point-to-Point Protocol (PPP) zwischen Router und Internet Service Provider über Telefonverbindung exklusives medium
 - Verbindung zweier Router über anderes Netz (z.B. Transportnetz)
- keine komplizierte Koordination notwendig

■ Medien mit Mehrfachzugriff

- z.B.
 - gemeinsamer Bus: früher bei Ethernet, in Bussen für die Fahrzeug- und Automatisierungstechnik (z.B. CAN), Systembus (z.B. PCI), Peripheriebus (z.B. SCSI)
 - gemeinsamer Funkkanal: WLAN 802.11, Bluetooth, ZigBee
 - Internetzugang über Kabel
- benötigt verteilte Koordination des Medienzugriffs (Medium Access Control, MAC)

Medienzugriff

■ Möglichkeiten für den Mehrfachzugriff

● feste Kanalaufteilung

- durch geeignetes Multiplexverfahren wird das Medium in feste Kanäle für Knotenpaare aufgeteilt
- bekannt: Frequenz-, Zeit-, Raum-, Codemultiplex
- für Sprachkommunikation (früher) verbreitet
- Nachteil für Datenkommunikation: Daten werden typischerweise sporadisch versendet, ineffiziente Nutzung des Mediums

● Zufallszugriffverfahren

- Stationen greifen zufällig auf Medium zu, eventuelle gleichzeitige Übertragungen (Kollisionen) müssen beachtet werden
- Urform: ALOHA, abgeleitet: MAC bei Ethernet und WLAN

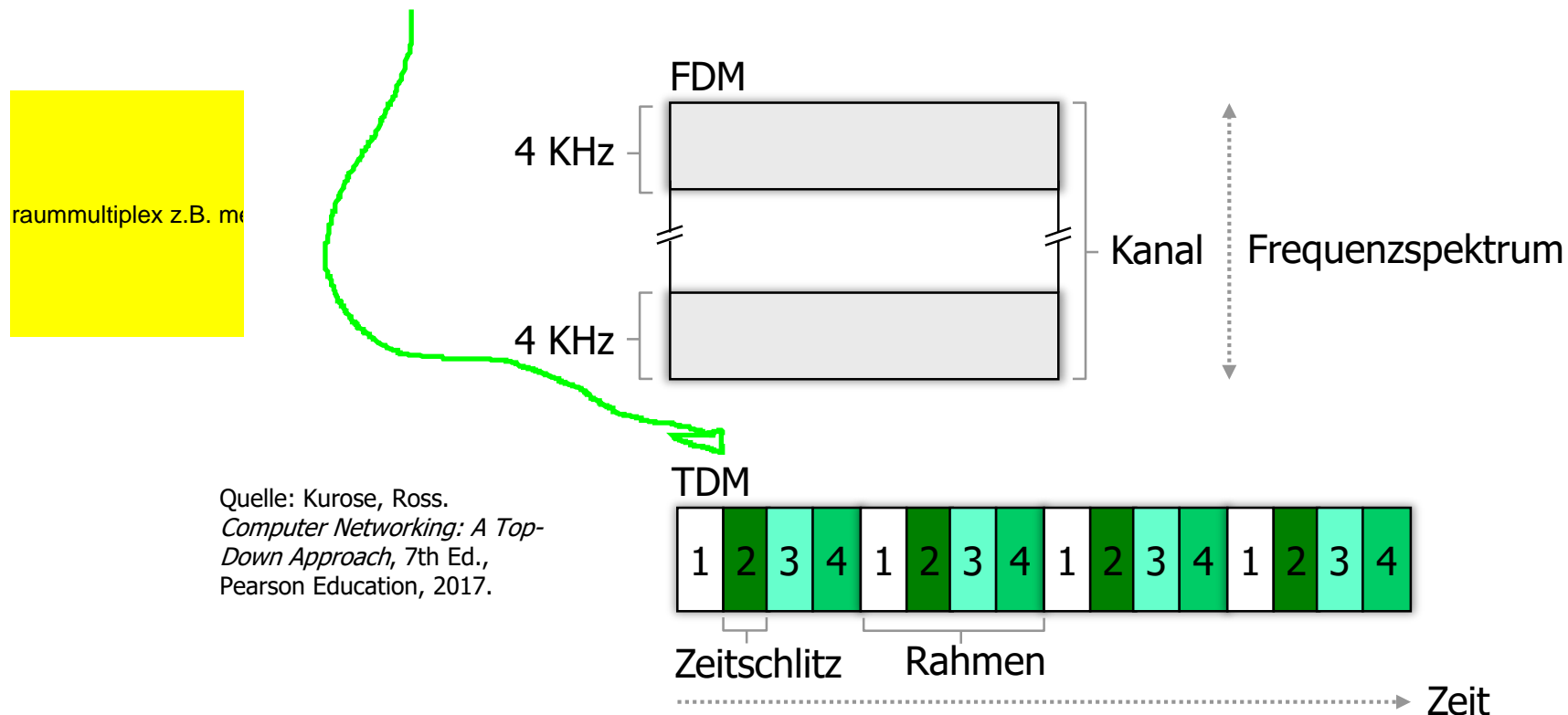
● zyklische Zuteilung

- zentralisiert: Polling durch zentralen Knoten
- verteilt: Sendeerlaubnis durch rotierendes Bitmuster (Token), z.B. Token Ring, FDDI, USB, Profibus

Medienzugriff

■ Feste Kanalaufteilung

- Frequenzmultiplex (Frequency Division Multiplex Access, FDMA): Geräte verwenden verschiedene Teile des Frequenzspektrums
- Zeitmultiplex (Time Division Multiplex Access, TDMA): Geräte wechseln sich zeitlich ab



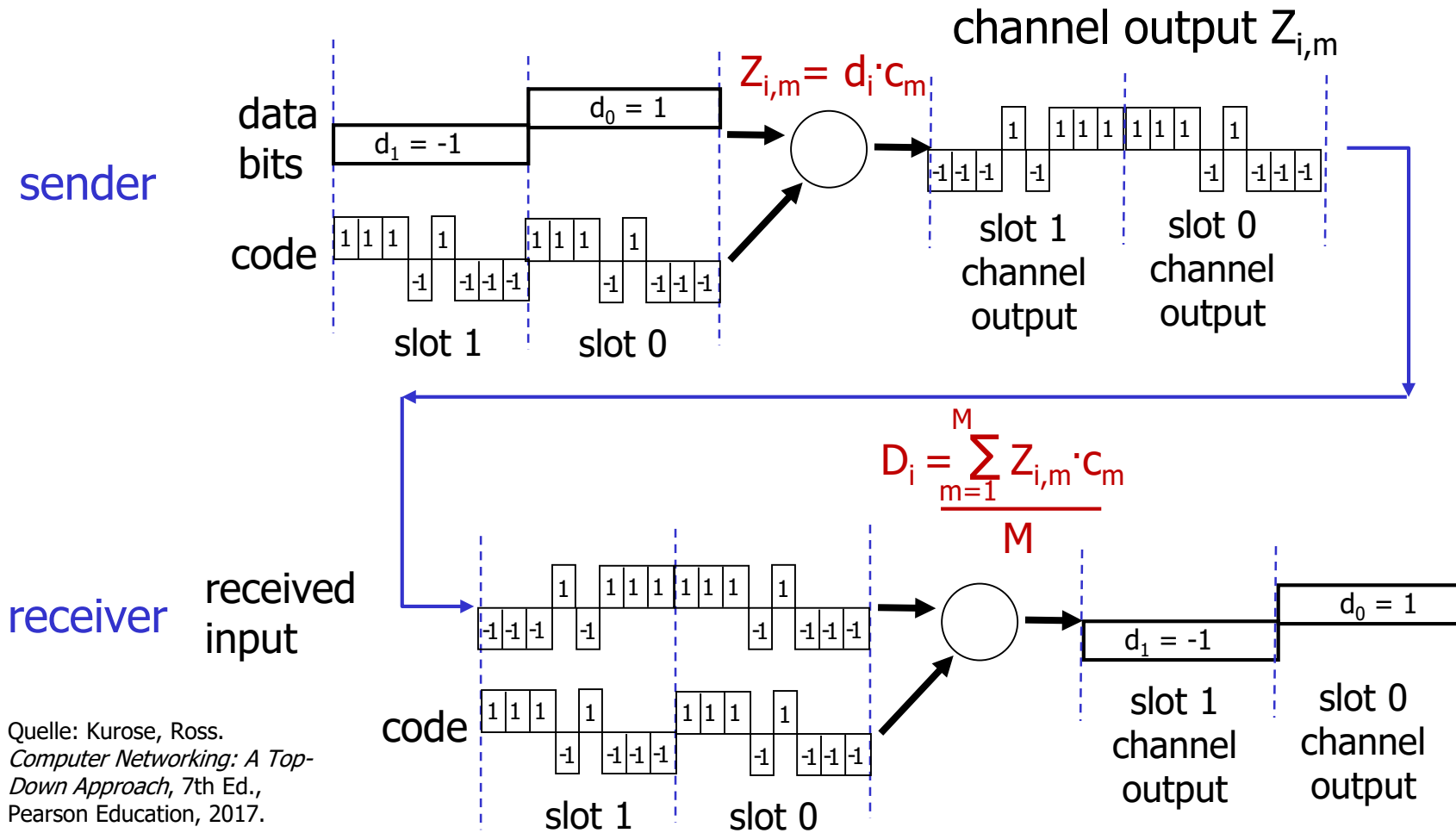
Medienzugriff

■ Weitere Möglichkeit für feste Kanalaufteilung: Codemultiplex (Code Division Multiplex Access, CDMA)

- Spreiztechnik: der Sender multipliziert jedes Bit mit einem Chipping-Code hochfrequentes signal
- er erzeugt dadurch ein Signal mit höherer Frequenz und sendet dieses auf das Medium (er benutzt dazu das volle Spektrum und die gesamte Zeit)
- die gespreizten Signale überlagern sich auf dem Medium wir führen künstlich eine Frequenz ein
- der Empfänger kann hieraus mit dem Chipping-Code das einzelne gesendete Signal extrahieren
- andere Variante: Frequenzsprungverfahren, der Sender springt (während des Sendens eines Bits oder nach mehreren Bits) zwischen verschiedenen Frequenzen, dies erlaubt die Überlagerung vieler Signale auf dem Kanal, durch Kenntnis des Sprungmusters kann das Signal empfangen werden
- Ursprung: Militärtechnik, bekannt aus Mobilfunk

Medienzugriff

- **Beispiel:** Chipping, ein Sender, ein Empfänger

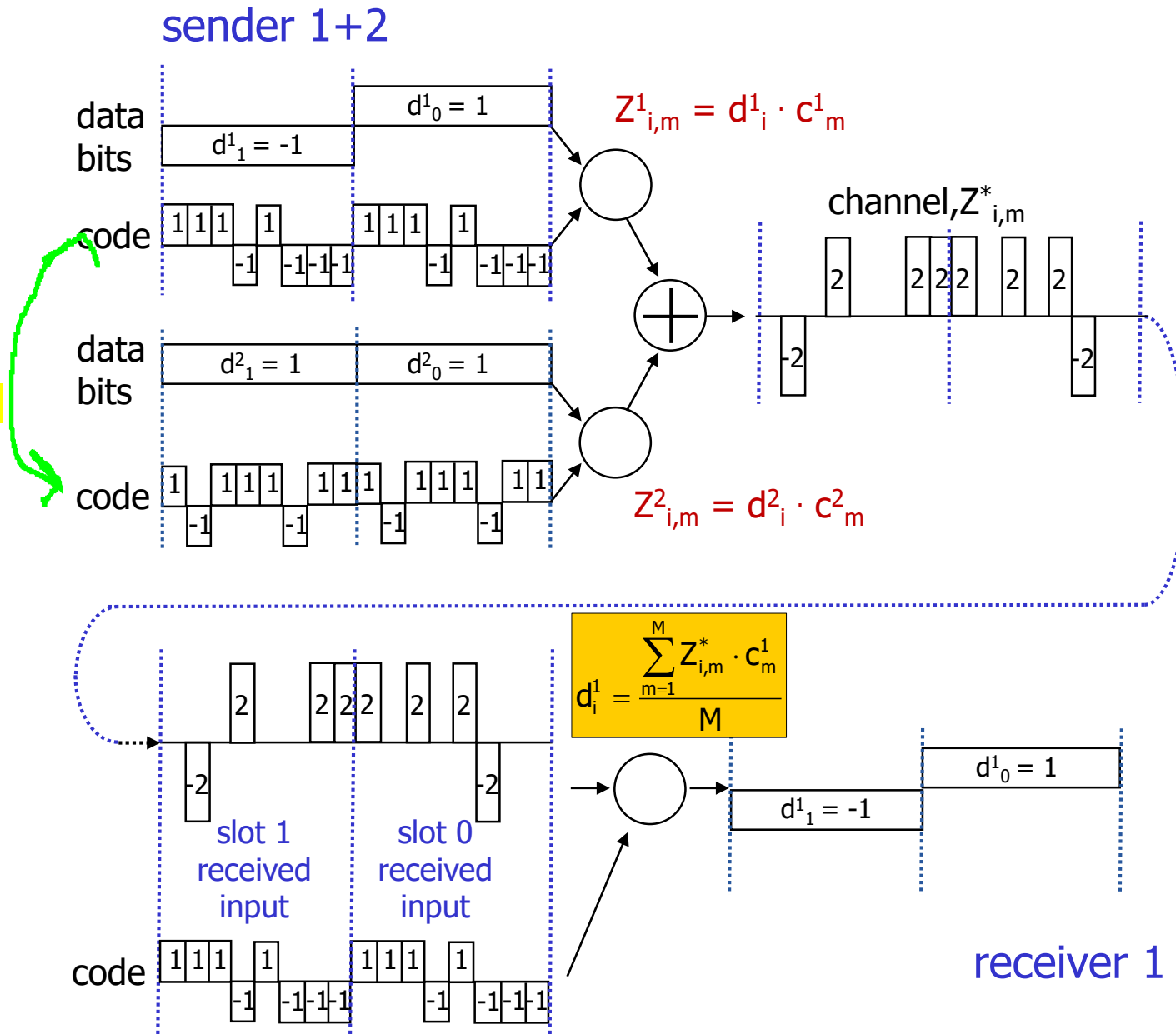


Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Medienzugriff

- Beispiel:
Chipping,
zwei Sender, Überlagerung,
Rückgewinnung der
Information

ungleich



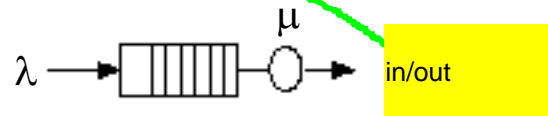
Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Medienzugriff

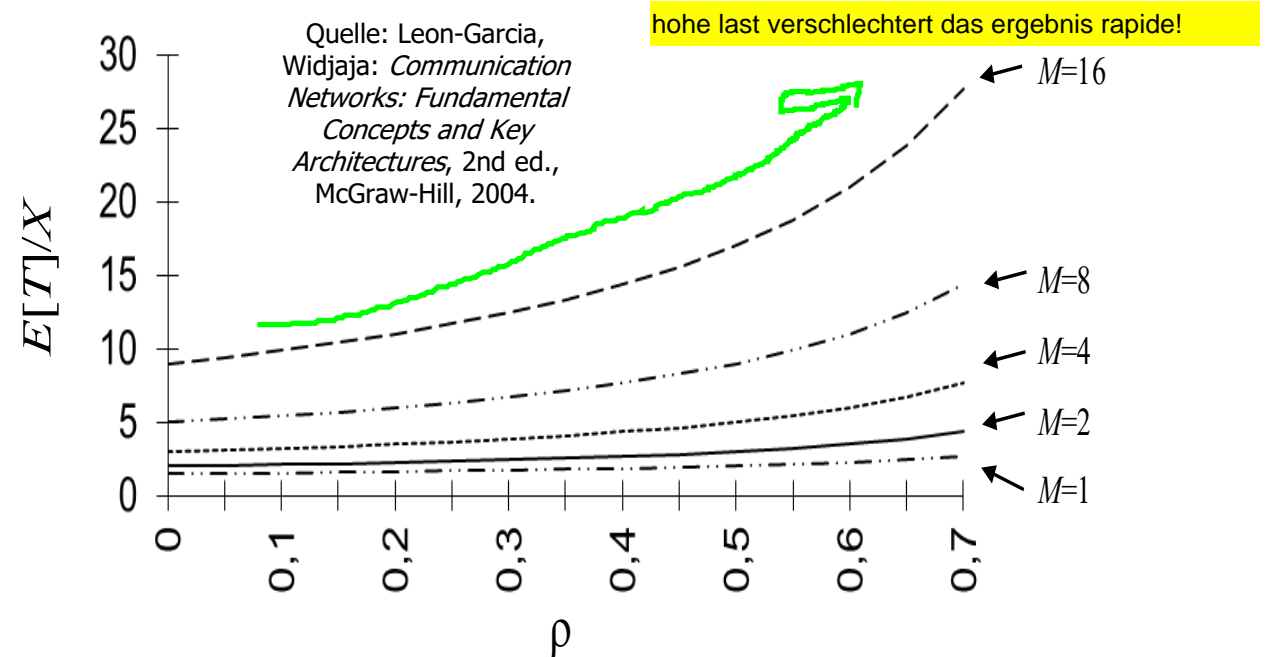
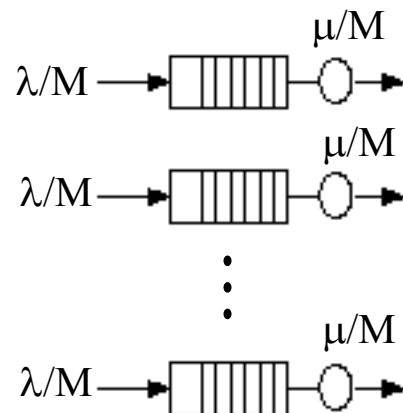
■ Effizienz fester Kanalaufteilung

- Datenkommunikation ist **bursty** (\approx schubartig), feste Kanalaufteilung ist ineffizient
- Bsp.: Kanal mit Puffer und zufälligen Zwischenankunftszeiten (exponentiell verteilt mit Rate λ), zufälligen Paketlängen (exponentiell verteilt, **Sendezeit ist Paketlänge geteilt durch Bitrate, ergibt Bedienrate μ**), Last ist $\rho = \lambda/\mu$. Eine feste **Aufteilung in M Kanäle** ergibt zwar gleiche Last pro Kanal, aber M-fach größere mittlere Verzögerung im Puffer (Warteschlangentheorie)

ungeteilter
Kanal:



feste Unterteilung
in M Kanäle:



Sicherungsschicht

- ✓ Einführung
- ✓ Adressierung
- ✓ Datensicherung
- ✓ Medienzugriff
 - ✓ feste Kanalaufteilung
 - Zufallszugriff
 - zyklische Zuteilung
- Ethernet
- Drahtlose LANs

Medienzugriff

■ Zufälliger Medienzugriff

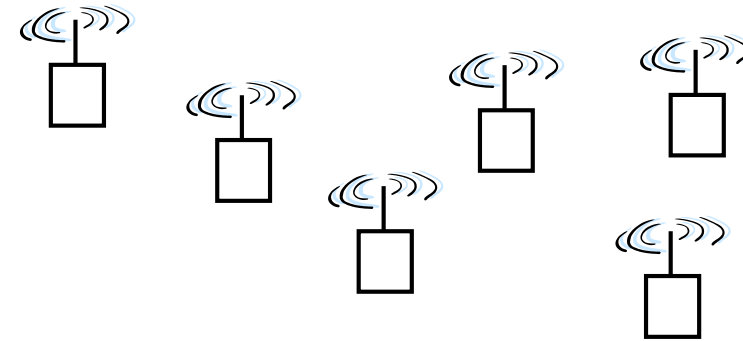
- wenn Knoten Rahmen zum Senden hat, sendet er mit der vollen Bitrate des Mediums
- wenn Knoten gleichzeitig senden, **überlagern sich die Signale auf dem Medium und zerstören sich gegenseitig**: es kommt zur **Kollision**, die durch Sendewiederholung behoben wird
- Grundidee: bei schwacher Last ist dies selten
- unterschiedliche Verfahren zur Vermeidung und Erkennung von Kollisionen
 - **ALOHA, slotted ALOHA** schlechte ausnutzung
 - Carrier Sense Multiple Access (CSMA) wir schauen, ob schon jemand sendet
 - mit Collision Detection: CSMA/CD (in Ethernet) während des sendens wird gefunden, dass jemand anderes sendet (Ethernet)
 - mit Collision Avoidance: CSMA/CA (in WLANs) Wlan wird versucht collisionen zu umgehen, weil CSMA/CD nicht umsetzbar ist
- Neuere Verfahren beherrschen auch **Successive Interference Cancellation (SIC)**, hierbei wird das **stärkste Signal abgezogen**, damit können auch Signale mit Kollisionen empfangen werden, wird hier nicht betrachtet

-summensignal

Medienzugriff

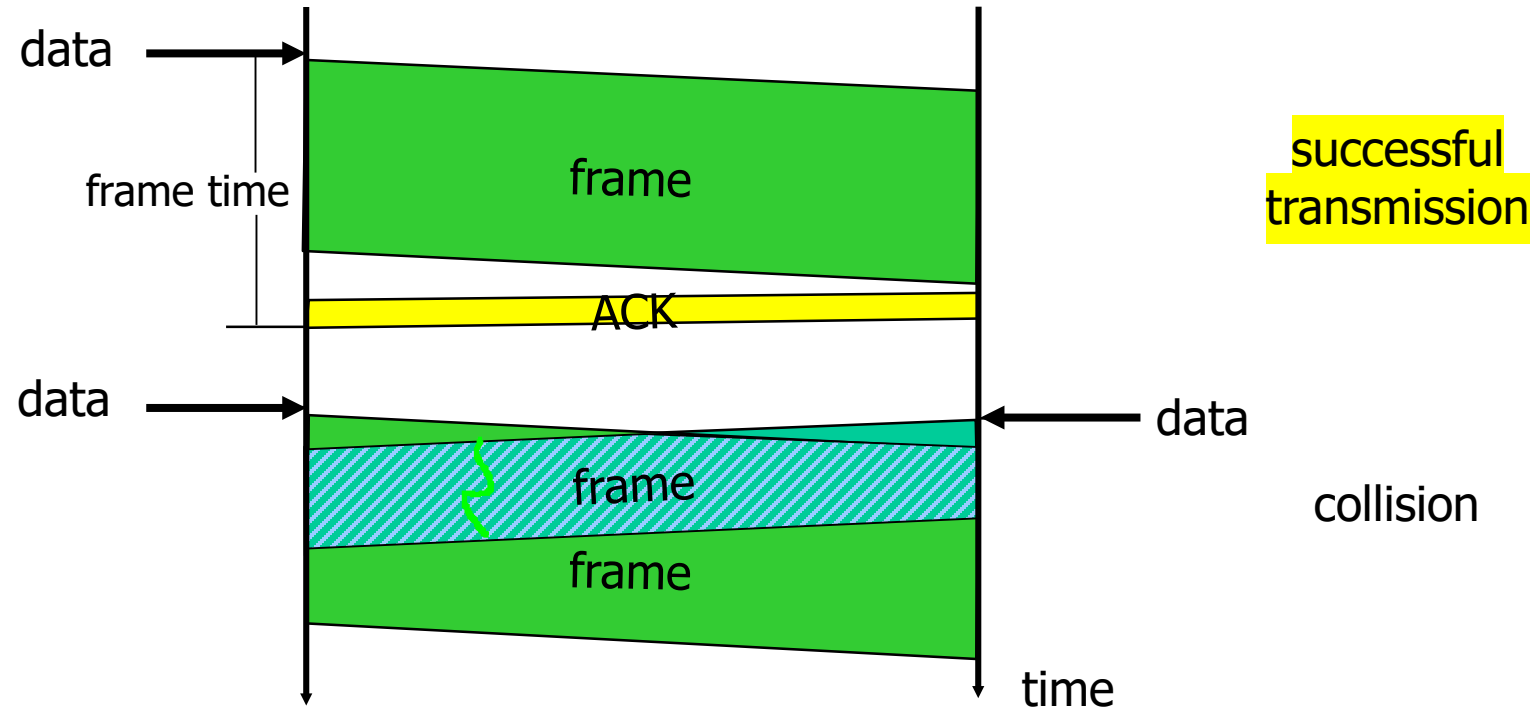
■ ALOHA

- in den 1970ern zur Vernetzung von Rechnern der Uni Hawaii
- gemeinsamer Funkkanal für alle Knoten
- Verfahren:
 - wenn die MAC-Schicht eines Knotens von der Netzwerkschicht ein Datagramm erhält, wird der Rahmen **sofort gesendet**
 - wenn der Empfänger ihn fehlerlos erhält, sendet er eine positive Bestätigung (ACK) zurück
 - wenn nach einem **Timeout** kein ACK zurückkommt, wartet der Sender eine zufällige Wartezeit (**Backoff**) und wiederholt dann das Senden
- Kollisionen werden wie Fehler bei der Fehlerkontrolle behandelt
- das Protokoll ist einfach, verteilt, es gibt keine Absprachen zwischen den Knoten



Medienzugriff

■ Beispielhafter Ablauf von ALOHA:



- hier ist Produkt aus Bitrate und Verzögerung klein ($a < 1$)
- Ähnlichkeit zu Stop-and-Wait

produkt aus bitrate und verzögerungman s

Medienzugriff

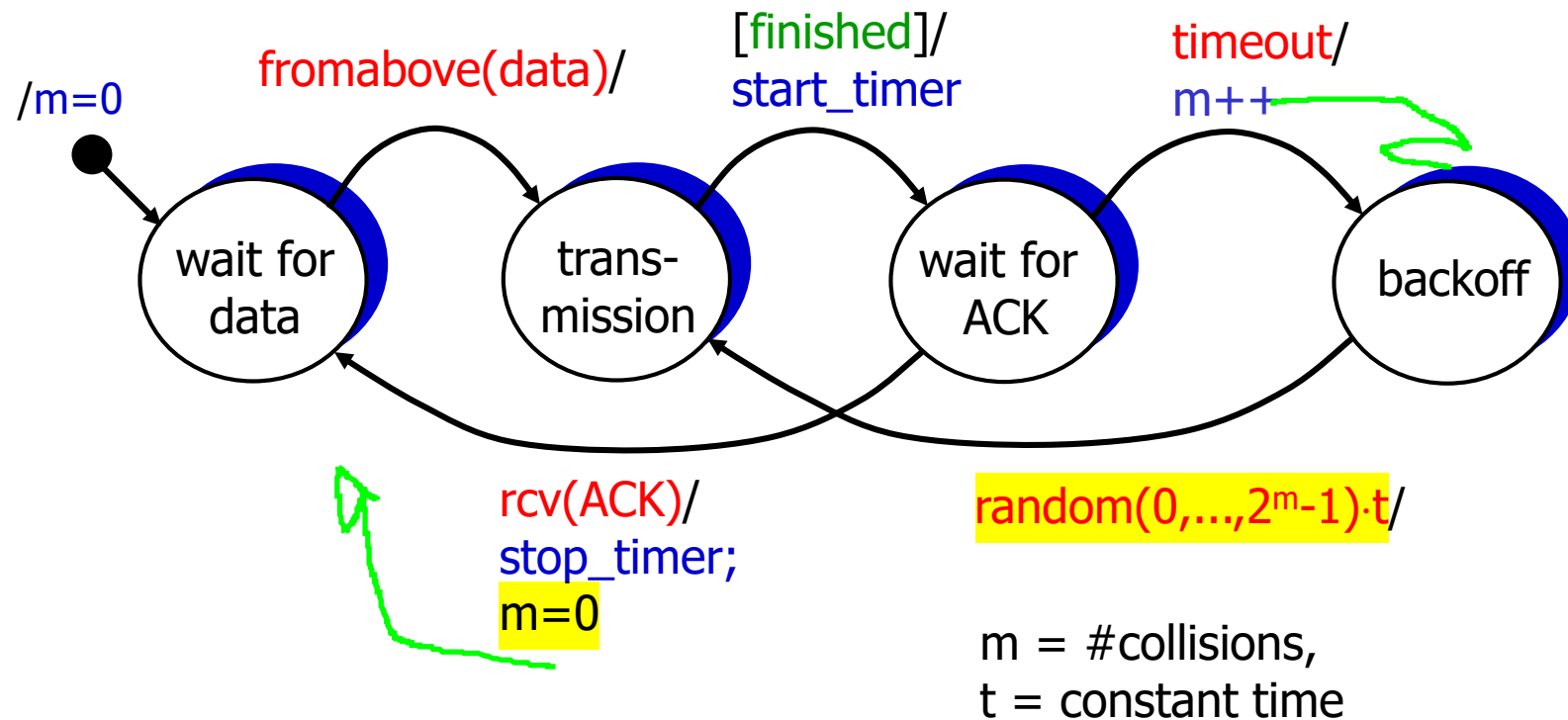
■ Binärer exponentieller Backoff

- erste Kollision: gleichverteilte Auswahl von K aus $\{0,1\}$
- zweite Kollision: gleichverteilte Auswahl von K aus $\{0,1,2,3\}$
- ...
- m-te Kollision: gleichverteilte Auswahl von K aus $\{0,1,2,3,4,\dots, 2^m-1\}$
- Backoffzeit ist $K \cdot t$
- nach einer maximalen Zahl M von Kollisionen (z.B. $M = 10$), bricht die MAC-Schicht ab und meldet einen Fehler an die Netzwerkschicht
- Idee:
 - Backoffzeit an aktuelle Last anpassen
 - niedrige Last: vermutlich sind nur wenige Knoten an der Kollision beteiligt, Auswahl von K aus wenigen Möglichkeiten reicht
 - höhere Last: mehr kollidierende Knoten, Auswahl von K aus mehr Möglichkeiten, größere mittlere Backoffzeit

Medienzugriff

■ ALOHA Sender als Statechart

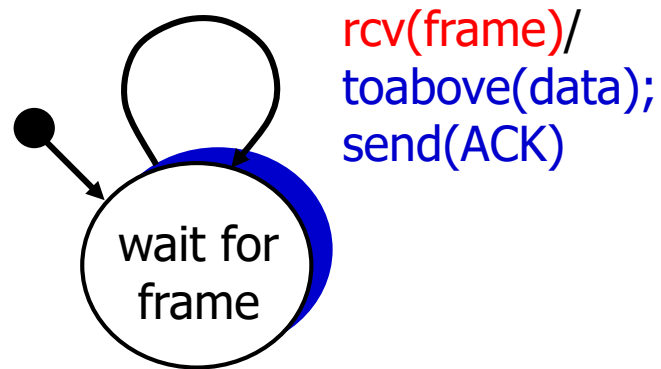
- Bitfehler und Verluste sind nicht berücksichtigt



Medienzugriff

■ ALOHA Empfänger als Statechart

- einfach: muss nur Daten ausliefern und mit ACK antworten

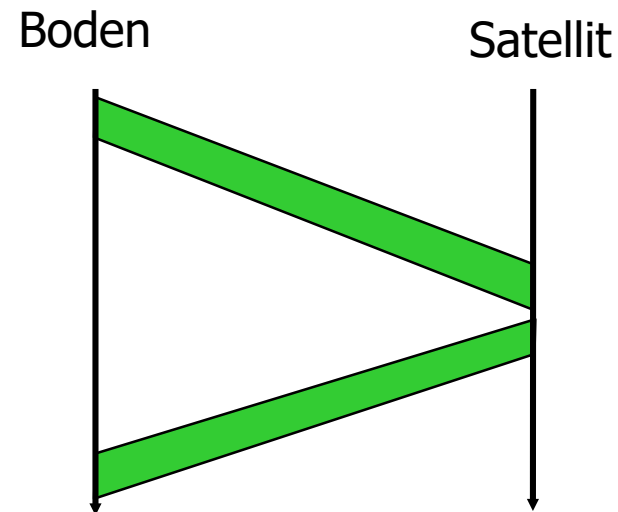
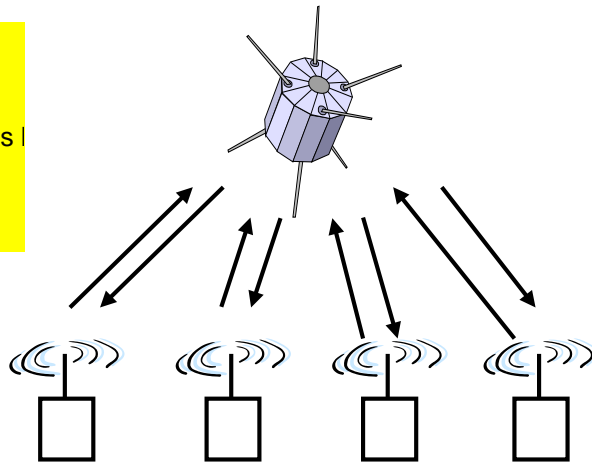


Medienzugriff

■ ALOHA über Satellit

- Bodenstationen haben keine Möglichkeit zur Koordination
- Bodenstationen senden in Uplink-Kanal an Satellit, Satellit reflektiert in Broadcast-Downlink-Kanal
- Kollisionen treten im Uplink-Kanal auf
- Verzögerung groß (0,27 s RTT bei geostationärem Satellit), Produkt von Bitrate und Verzögerung groß ($a > 1$)
- sendende Bodenstation erkennt an ausbleibendem ACK Kollision

hier ist Aloha immernoch das I



Medienzugriff

■ Leistungsanalyse von ALOHA

- Verschwendung durch Kollisionen und Backoffzeiten
- aus Literatur ist eine einfache Analyse sehr bekannt, durch Simulation bestätigt

■ Vereinfachende Annahmen

- alle Rahmen besitzen konstante Länge, zum Senden wird eine Slotzeit benötigt, die Slotzeit wird als Zeiteinheit verwendet
- jeder Knoten besitzt die gleiche Wahrscheinlichkeit p , einen Rahmen zu senden (das erste Mal oder als Wiederholung), dies ist die wesentliche Einschränkung hier!
- Nah-/Ferneffekt (eigentlich werden in Funkkanälen Signale bei Kollisionen nicht immer zerstört) oder SIC unberücksichtigt
- keine Bitfehler, kein Verlust

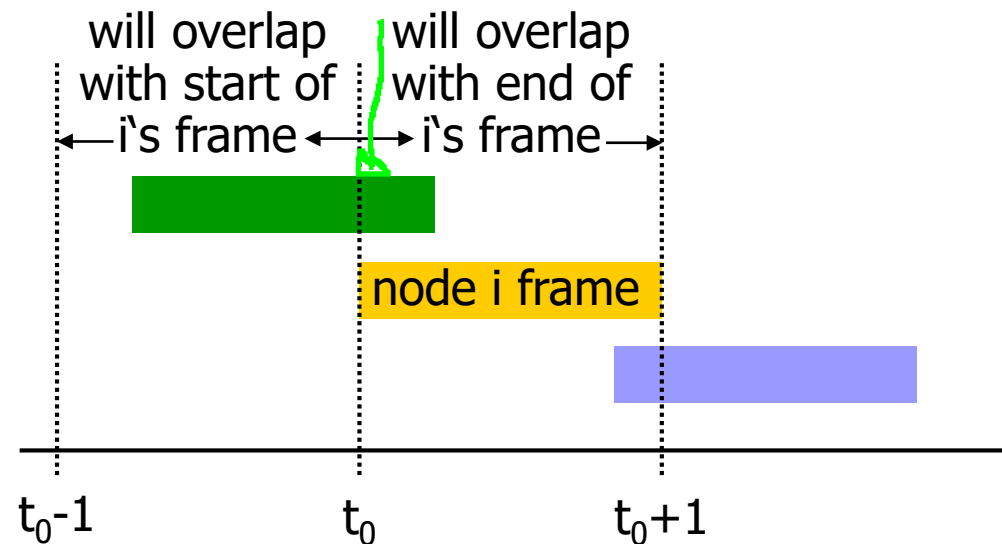
z.B. wlan versendung von "zwei richtungen" zerstört das signal nicht

Medienzugriff

■ Bedingung für Kollision

- wenn ein Knoten zum Zeitpunkt t_0 mit dem Senden beginnt und ein weiterer Knoten im Intervall $[t_0-1, t_0+1]$ beginnt, entsteht eine Kollision

Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.



Medienzugriff

■ Durchsatzberechnung

- N Stationen
- Wahrscheinlichkeit, dass ein ausgewählter Knoten in einem beliebigen Slot ohne Kollision sendet

$$\begin{aligned} &= P(\text{der Knoten sendet}) \cdot \\ &\quad P(\text{kein anderer Knoten sendet in } [t_0-1, t_0]) \cdot \\ &\quad P(\text{kein anderer Knoten sendet in } [t_0, t_0+1]) \quad \text{Teilweise im 2-ten Intervall} \\ &= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1} \\ &= p \cdot (1-p)^{2(N-1)} \end{aligned}$$

- Wahrscheinlichkeit, dass ein beliebiger Knoten in einem beliebigen Slot ohne Kollision sendet

$$\begin{aligned} &= N \cdot p(1-p)^{2(N-1)} \\ &= \text{durchschnittliche Anzahl erfolgreicher Slots} \\ &= \text{normalisierter Durchsatz } S \end{aligned}$$

Medienzugriff

- sei $G = Np$ (Offered Load, die Rate von Sendeversuchen von Rahmen in einem Slot),
damit ist $p = G/N$ anzahl stationen und sendewahrscheinlichkeit eines Teilnehmers

- Einsetzen in den Durchsatz ergibt $S = Np(1-p)^{2(N-1)} = G \left(1 - \frac{G}{N}\right)^{2(N-1)}$

- schnelle Konvergenz für große N , es gilt $\lim_{n \rightarrow \infty} (1+x/n)^n = e^x$

- damit wird $\lim_{N \rightarrow \infty} S = \lim_{N \rightarrow \infty} G \left(1 - \frac{G}{N}\right)^{2(N-1)} = \lim_{N \rightarrow \infty} G \left(1 - \frac{G}{N}\right)^{2N} \left(1 - \frac{G}{N}\right)^{-2} = Ge^{-2G}$

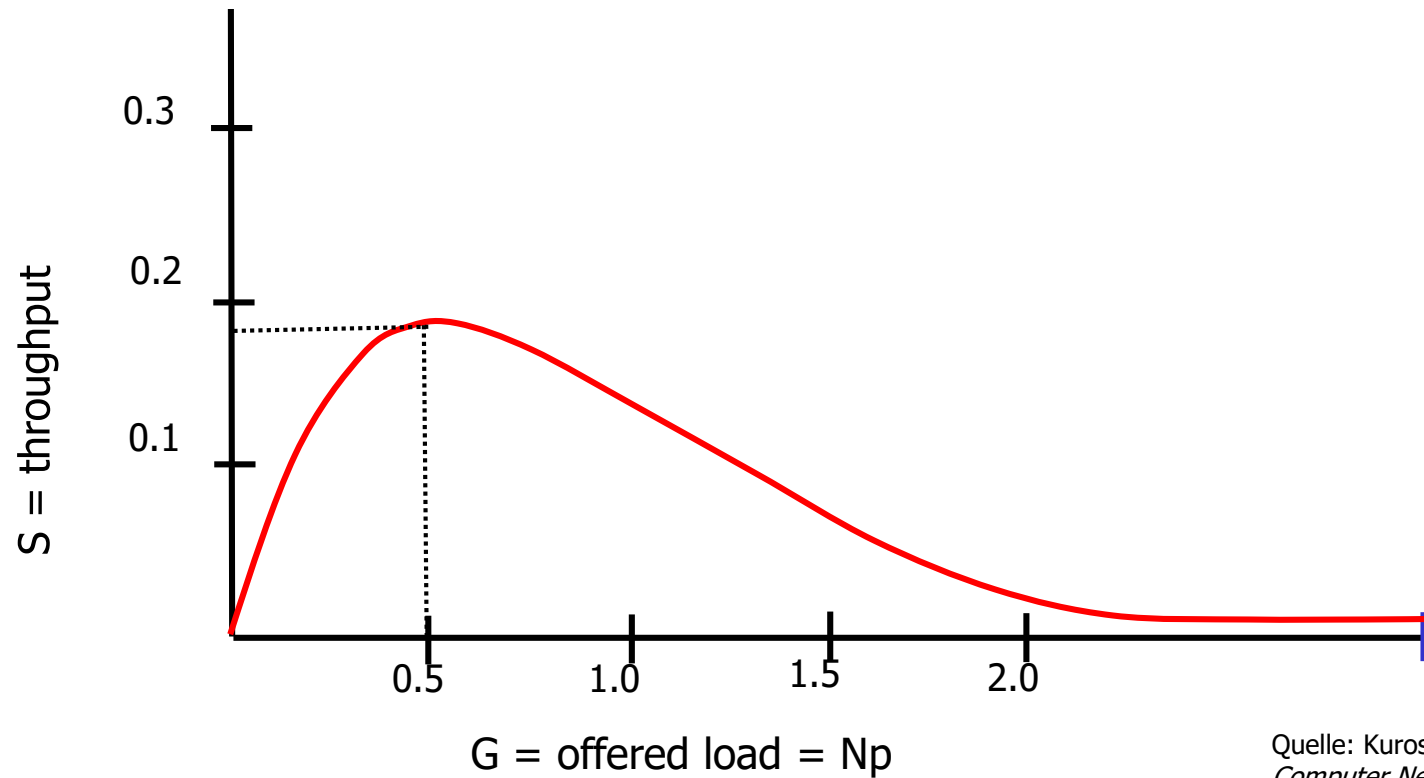
- aus $\frac{d}{dG} Ge^{-2G} = (1-2G)e^{-2G} \stackrel{!}{=} 0$

folgt das Maximum $S_{\max} = 1/2e \approx 0.18$ bei $G = 0.5$

- **Interpretation:** selbst bei optimaler Einstellung der Last kann maximal 18% Durchsatz erreicht werden!

Medienzugriff

■ Durchsatz vs. Offered Load bei ALOHA:

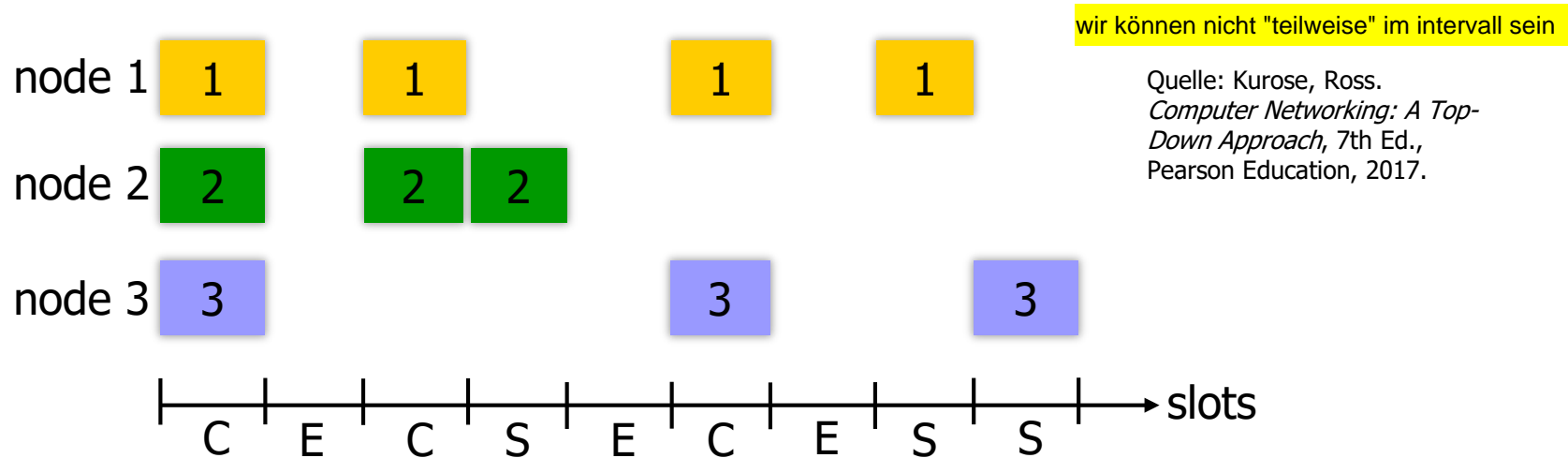


Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Medienzugriff

■ Slotted ALOHA

- alle Knoten synchronisieren ihre Slots (z.B. durch zentrales Zeitsignal)
- Sendebeginn nur zu Beginn eines Slots, Kollisionsintervall verkürzt sich auf einen Slot

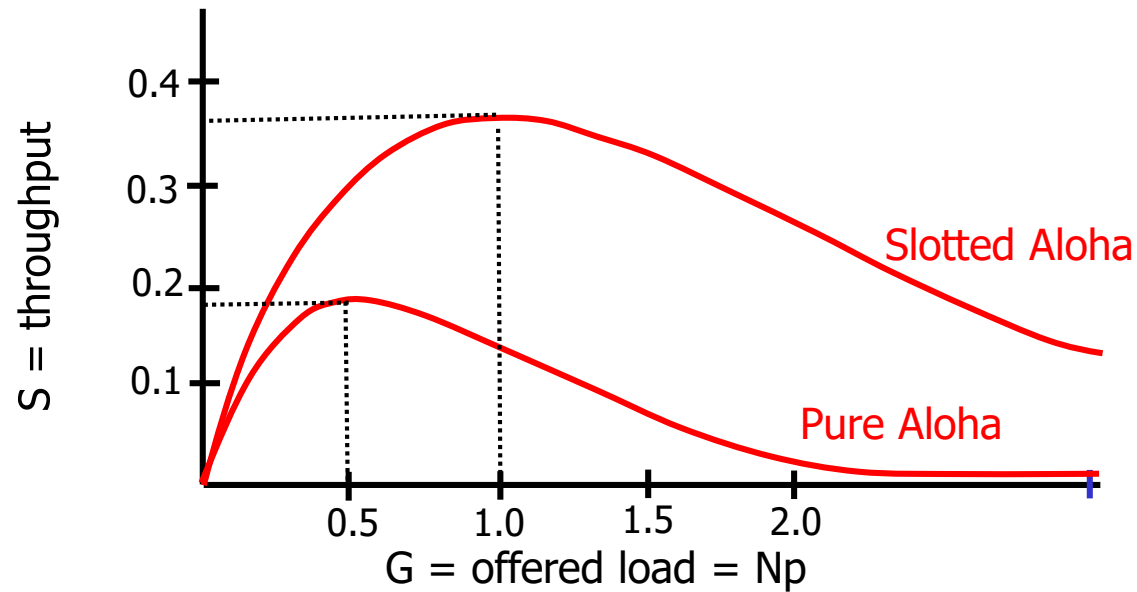


- Wahrscheinlichkeit, dass von allen Knoten ein beliebiger Knoten in einem beliebigen Slot ohne Kollision sendet = $Np(1-p)^{(N-1)}$
- die gleichen Überlegungen wie bei ALOHA führen zu $S = G \cdot e^{-G}$ und $S_{\max} = 1/e \approx 0.37$ bei $G = 1$ (Verdoppelung) verdoppelung der effizienz!

Medienzugriff

■ Vergleich von ALOHA und Slotted ALOHA

- Durchsatz vs. Offered Load:

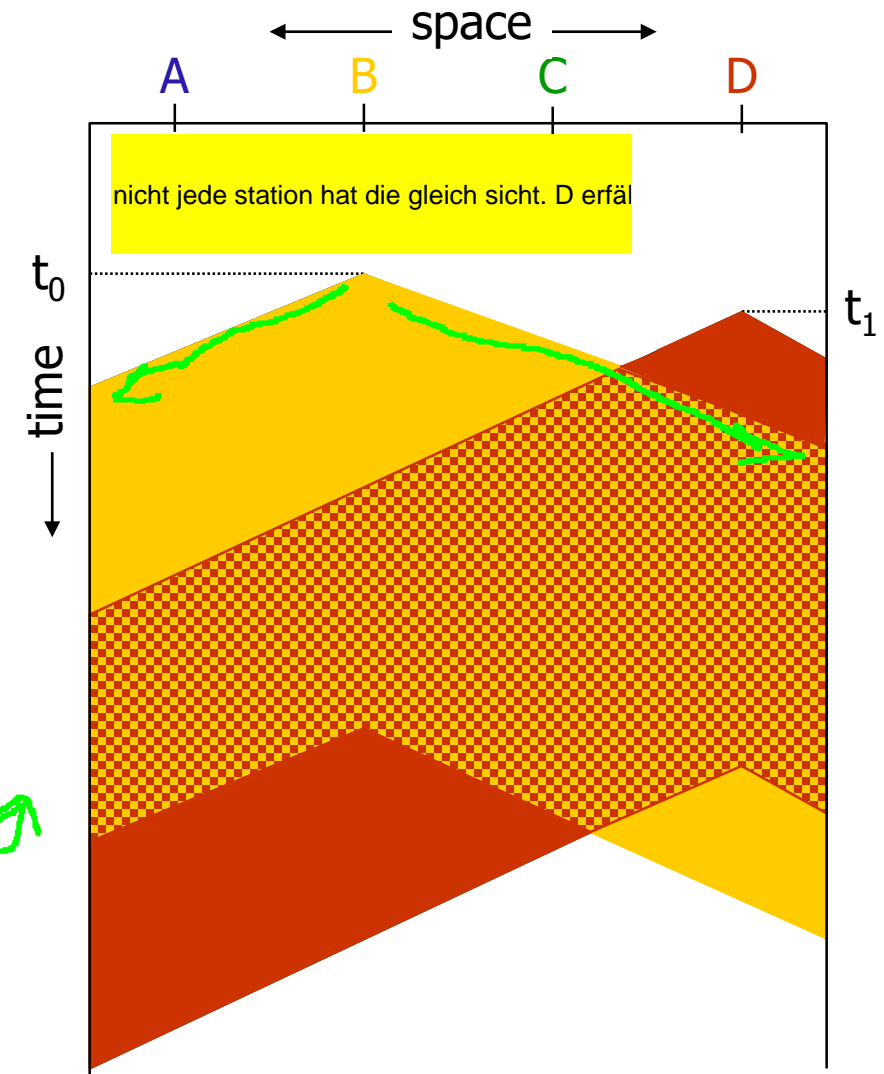


Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Medienzugriff

■ Carrier Sense Multiple Access (CSMA)

- Knoten prüfen vor dem Senden, ob Medium belegt (listen before talking)
macht sinn (wenn das listening funktioniert!)
- reduziert Kollisionen
- Voraussetzung:
Ausbreitungsverzögerung < Rahmensendezeit
(sonst ist die Information des belegten Kanals veraltet und das Verfahren sinnlos) satelliteneffekt
- Kollisionen immer noch möglich: wenn anderer Knoten startet, bevor sich das Signal auf dem Medium zu ihm ausgebreitet hat



Medienzugriff

■ CSMA-Verfahren allgemein

- wenn die MAC-Schicht eines Knotens von der Netzwerkschicht ein Datagramm erhält, überprüft sie das Medium (listen before talking); wenn es frei ist, wird der Rahmen gesendet, sonst wird gewartet
- wenn der Empfänger ihn fehlerlos erhält, sendet er eine positive Bestätigung (ACK) zurück
- wenn nach einem Timeout kein ACK zurückkommt, wartet der Sender eine zufällige Wartezeit (Backoff) und wiederholt dann das Senden

Medienzugriff

■ CSMA-Varianten

● 1-persistent

- 1. wenn das Medium frei ist, sendet der Knoten sofort
- 2. wenn das Medium belegt ist, wartet der Knoten bis es frei ist und geht dann zu 1.
- 3. wenn nach Senden kein ACK kommt, geht der Knoten der Knoten in Backoff, danach zu 1.
- geringe Wartezeit, aber sichere Kollision, wenn mehrere Knoten auf freies Medium warten

● nicht-persistent

jeder Knoten ist greedy!

- 1. wenn das Medium frei ist, sendet der Knoten sofort
- 2. wenn das Medium belegt ist oder nach Senden kein ACK kommt, geht der Knoten in Backoff, danach zu 1.
- weniger Kollisionen, aber längere Wartezeit

wir haben kein 2. es gibt keinen Surge auf den Bus nach freigabe

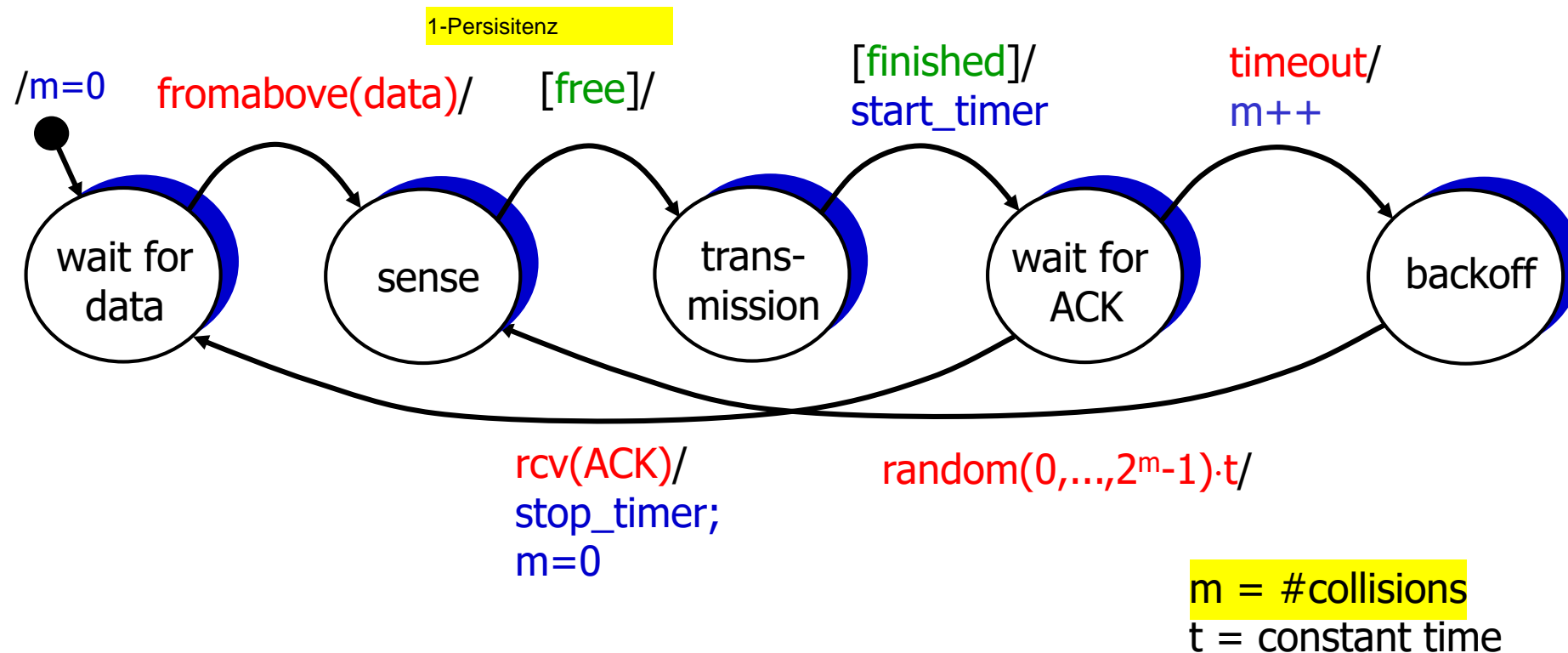
● p-persistent

- 1. wenn das Medium frei ist, sendet der Knoten jeweils mit Wahrscheinlichkeit p oder wartet noch einen Slot mit Wahrscheinlichkeit $1-p$
- 2. wenn das Medium belegt ist, wartet der Knoten bis es frei ist
- 3. wenn nach Senden kein ACK kommt, geht der Knoten der Knoten in Backoff, danach zu 1.
- Kompromiss

das obere ist präzise, wenn man $p=1$ wählt...

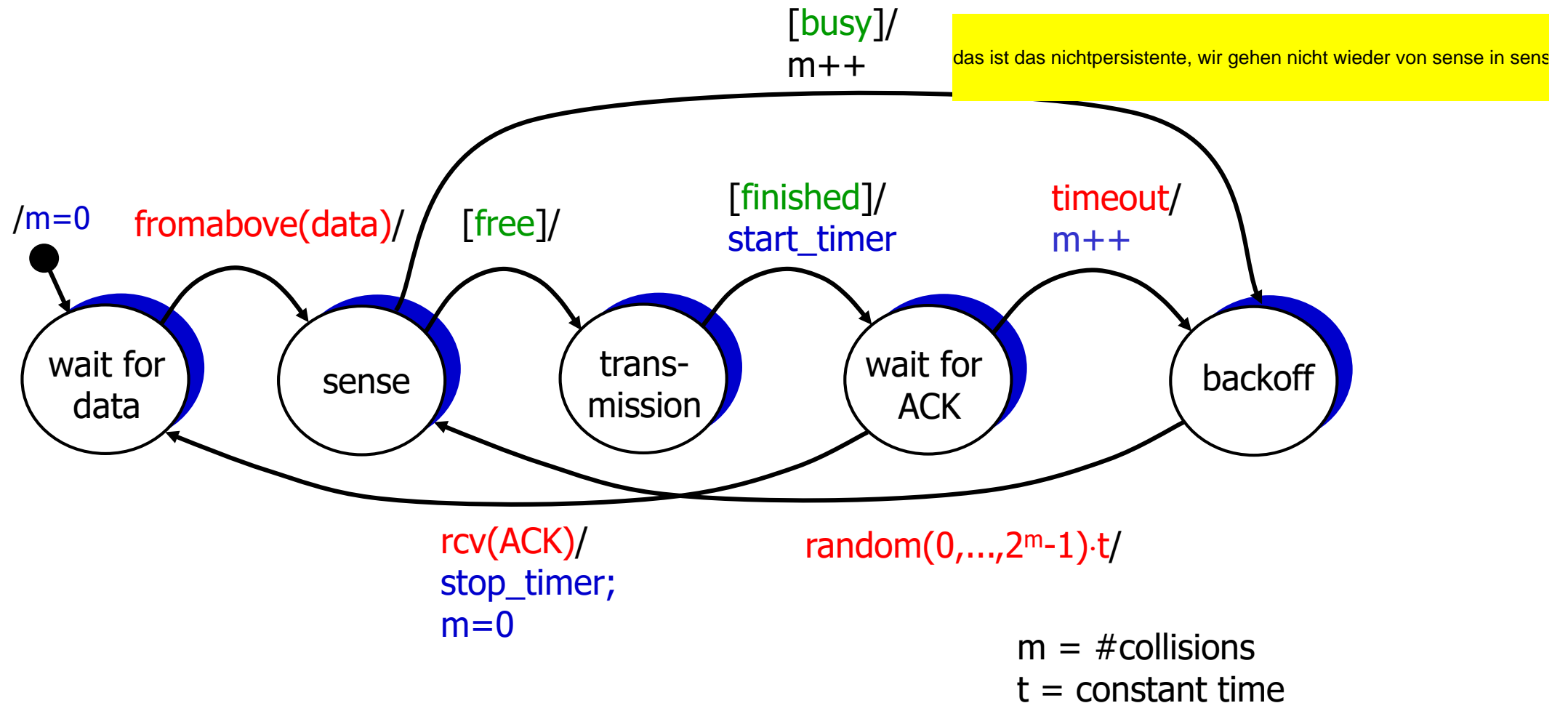
Medienzugriff

■ Statechart des 1-persistenten Senders



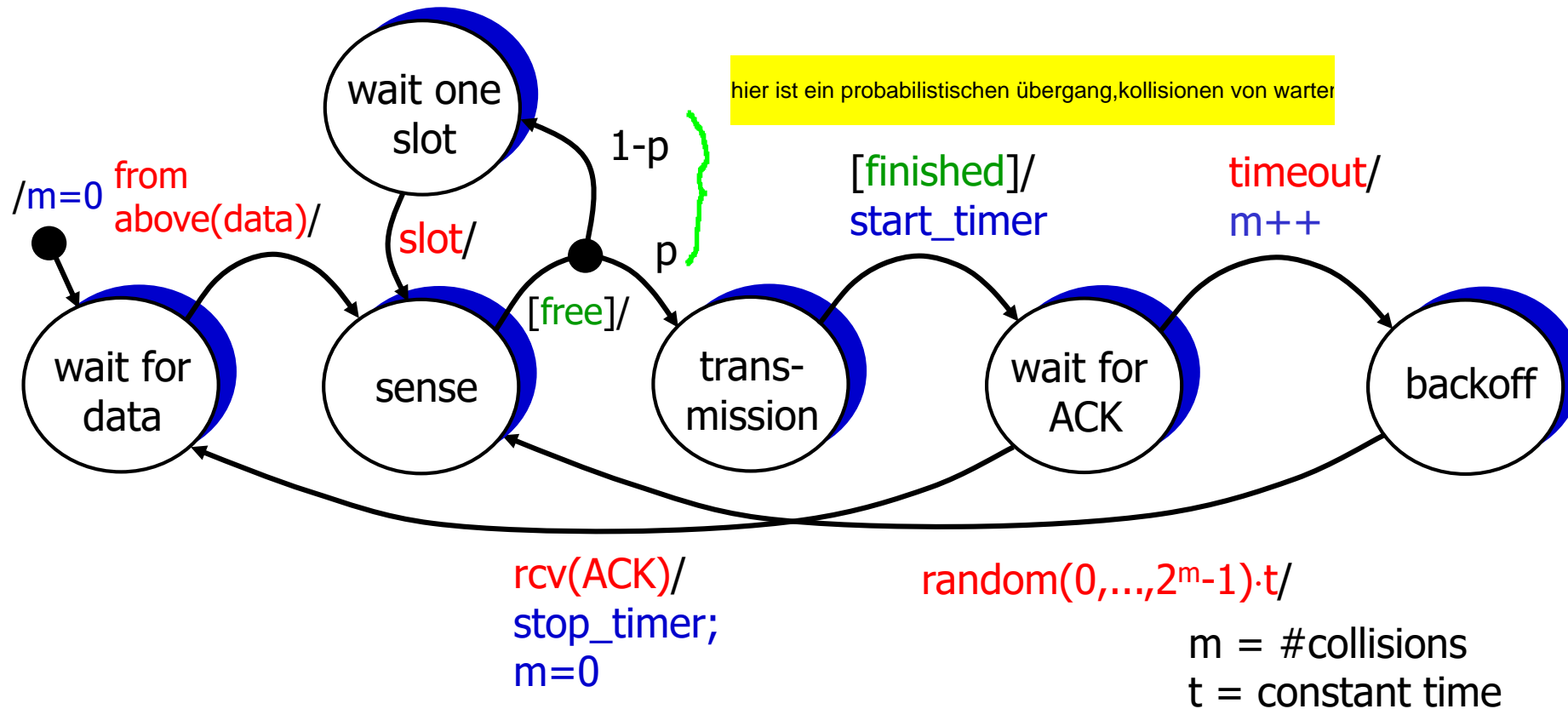
Medienzugriff

■ Statechart des nicht-persistenten Senders



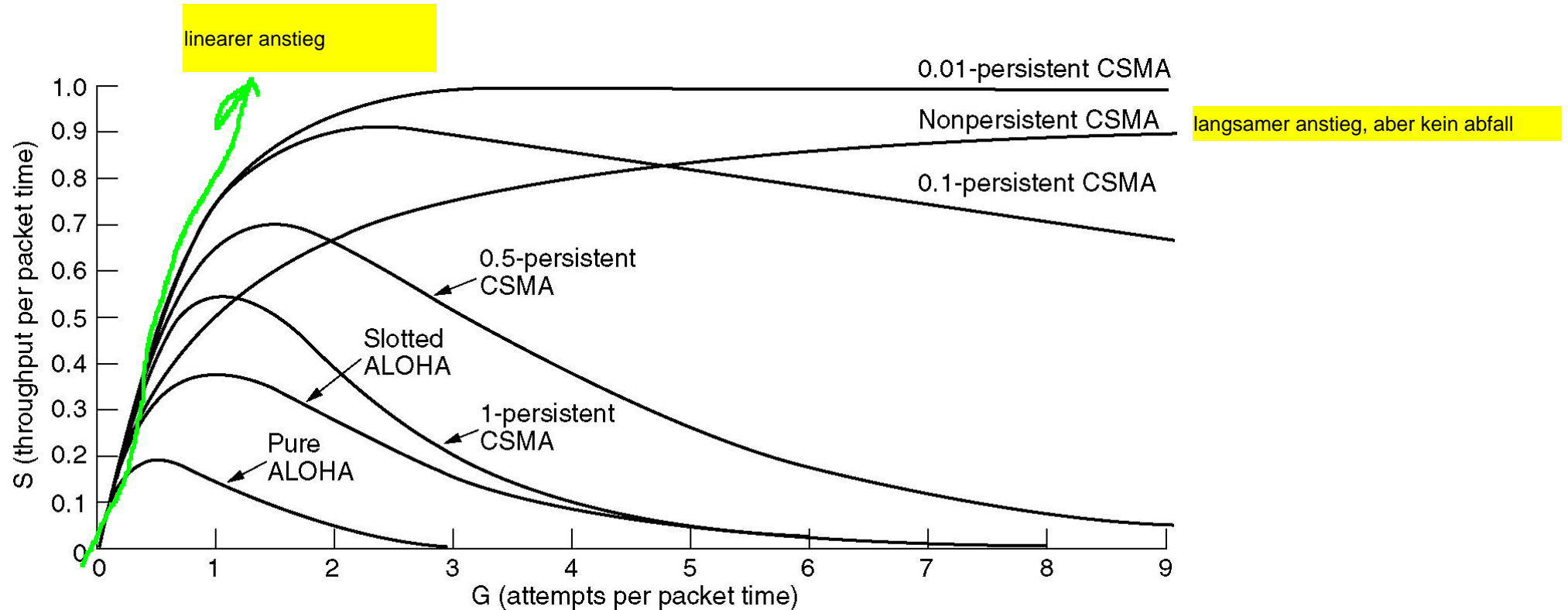
Medienzugriff

■ Statechart des p-persistenten Senders



Medienzugriff

■ Durchsatz für verschiedene CSMA-Varianten



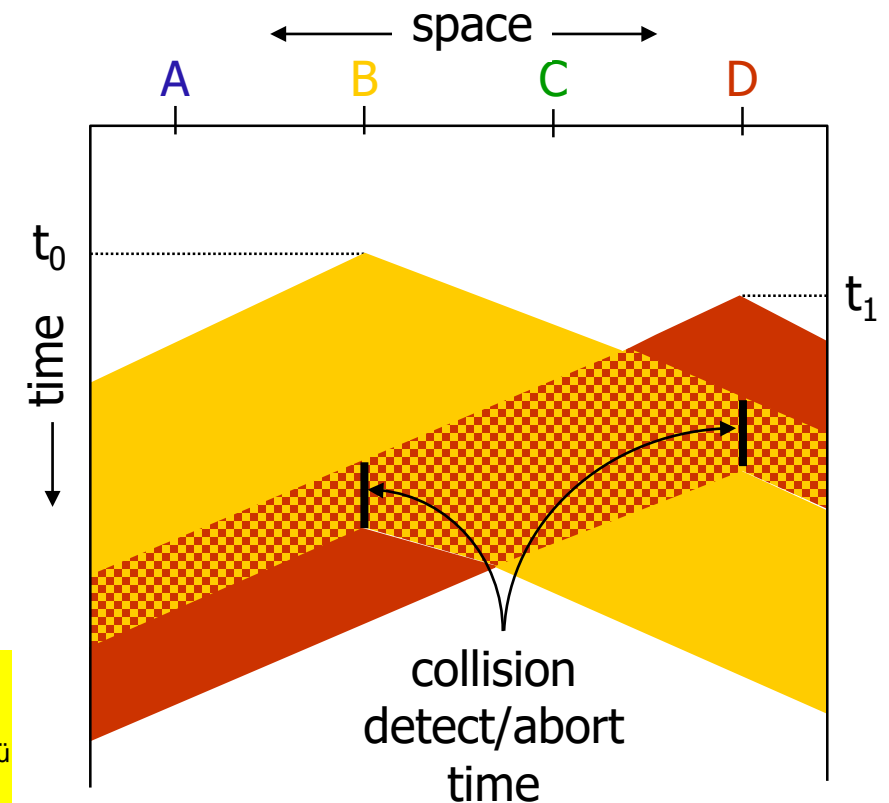
- aus Tanenbaum: Computer Networks. 5th Ed., Prentice Hall, 2011, Herleitung geht über Inhalt der VL hinaus

Medienzugriff

■ Kollisionserkennung, CSMA/CD

- Knoten besitzen HW, um während des Sendens Kollision zu erkennen (listen while talking)
- nach Kollisionserkennung wird Senden abgebrochen (weniger Verschwendung), ein Jamming-Signal wird gesendet, damit alle Knoten Kollision sicher erkennen
- keine ACKs ethernet
- kombinierbar mit allen CSMA-Varianten

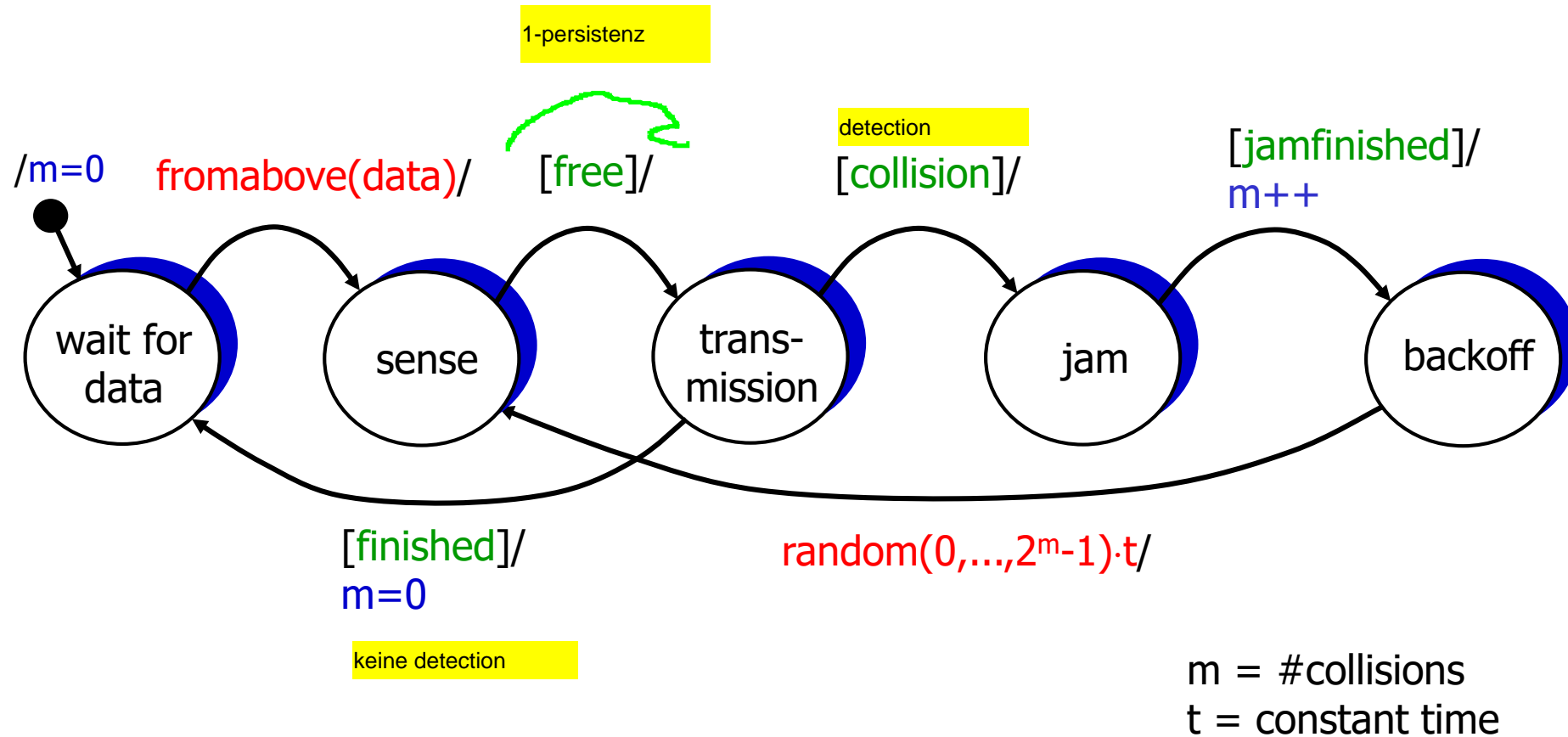
D weiss noch nichts von A, während des sendens wird das ü



Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Medienzugriff

■ Statechart des 1-persistenten CSMA/CD-Senders

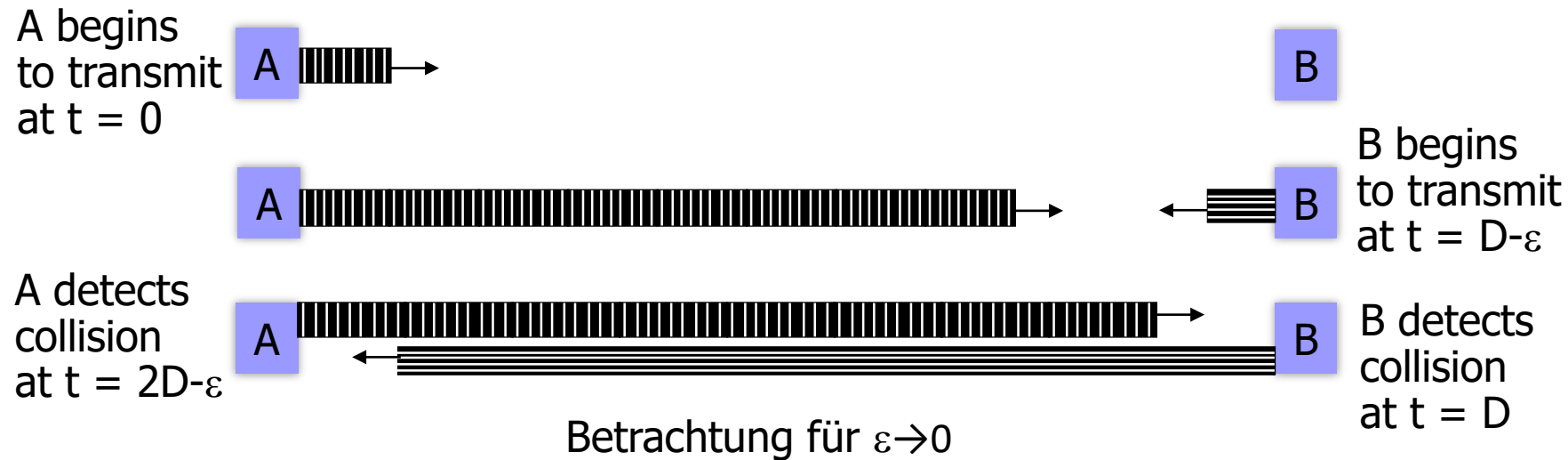


Medienzugriff

■ Minimale Rahmengröße bei CSMA/CD

- sei D die maximale Ausbreitungsverzögerung zwischen zwei Knoten
- es dauert höchstens $2D$, bis eine Kollision von allen Knoten bemerkt wird
- bei Bitrate R **muss** minimale Rahmengröße L groß genug sein, so dass $L/R > 2D$, damit Kollision sicher erkannt wird

sonst gibt es Fragement, für die Kollisionen nicht sicher erkannt werden können (sie werden von großen blöcken aufgefressen!)

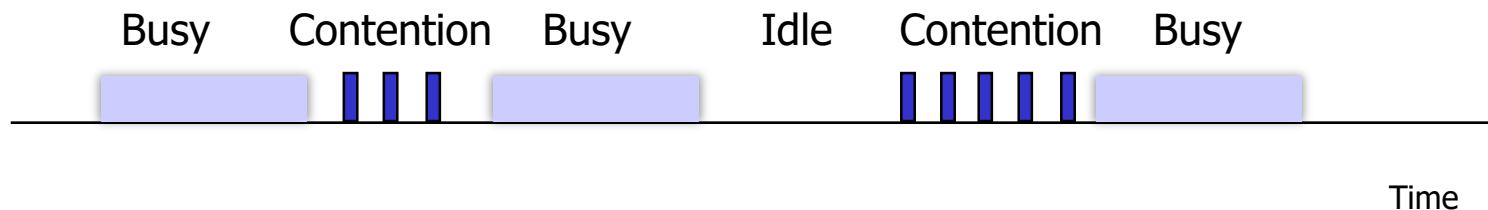


Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

Medienzugriff

■ Leistung von CSMA/CD

- Wechsel von Sende-, Leerlauf- und Wettbewerbsphasen
- Sendephase dauert L/R Zeiteinheiten
- Kollisionen werden nach Intervallen der Länge $2D$ behoben (Zeit für Jamming wird vernachlässigt)
- Wettbewerbsphase wird in Slots der Länge $2D$ unterteilt
- N Knoten, jeder versucht mit Wahrscheinlichk. p in einem Slot zu senden
- Wettbewerb ist beendet, wenn genau ein Knoten sendet: $P_{\text{Erfolg}} = Np \cdot (1-p)^{N-1}$
- wie bei Slotted ALOHA kann man herleiten, dass für $p = 1/N$ die Erfolgswahrscheinlichkeit maximal wird: $P_{\text{Erfolg}}^{\text{max}} = 1/e$
- im Mittel ist ein Knoten also einmal pro $1/P_{\text{Erfolg}}^{\text{max}} = e$ Slots erfolgreich
erwartungswert für erfolg



Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

Medienzugriff

- somit ist die Wettbewerbsphase im Mittel $e - 1 \approx 1,718$ Slots lang, da der letzte Slot erfolgreich ist, also bereits zum Senden genutzt wird
- für maximalen Durchsatz wird die Leerlaufphase auf Null gesetzt, das System alterniert nur zwischen Sende- und Wettbewerbsphase
- nach dem Senden dauert es noch eine Ausbreitungsverzögerung D , bis das Ende überall bemerkt ist
- also:

*RTT

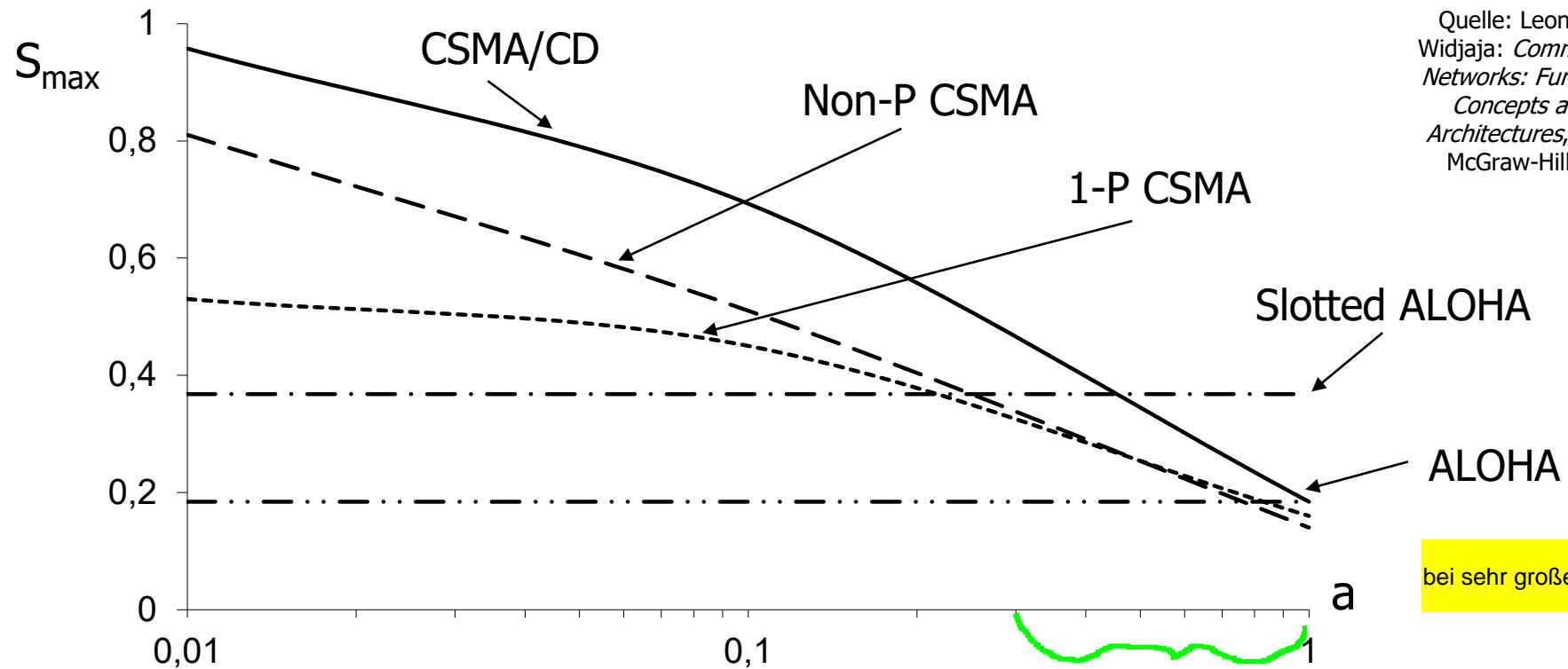
$$\begin{aligned} S_{\max} &= \frac{\text{Sendephase}}{\text{Sendephase} + \text{Ausbreitung} + \text{Wettbewerbsphase}} \\ &= \frac{\frac{L}{R}}{\frac{L}{R} + D + \frac{1}{1 + [1 + 2 \cdot (e - 1)] \cdot \frac{RD}{L}}} \\ &= \frac{1}{1 + [1 + 2 \cdot (e - 1)] \cdot a} = \frac{1}{1 + 4.4a} \end{aligned}$$

prozentualer anteil des Sendens pro gesamtzeit

- $a = RD/L$ ist die Kanalpuffergröße in Rahmen, wie in der Transportschicht definiert, die Leistung hängt kritisch von dieser Größe ab

Medienzugriff

■ Maximaler Durchsatz von Zufallszugriffverfahren vs. a



bei sehr großen a wird Slotted ALOHA besser

- kleines a : CSMA/CD am besten
- ALOHA, Slotted ALOHA unabhängig von a , besser für großes a

Sicherungsschicht

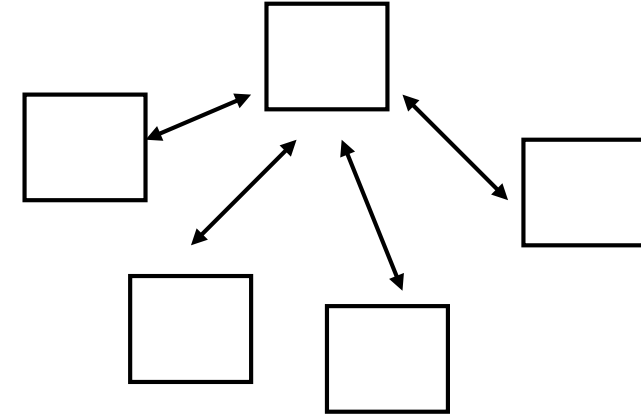
- ✓ Einführung
- ✓ Adressierung
- ✓ Datensicherung
- ✓ Medienzugriff
 - ✓ feste Kanalaufteilung
 - ✓ Zufallszugriff
 - zyklische Zuteilung
- Ethernet
- Drahtlose LANs

Medienzugriff

■ Zyklische Zuteilung

● Polling

- Sendeerlaubnis wird den Knoten sukzessive zugewiesen
- durch
 - zentralen Knoten
 - zufällig ausgewählten Knoten
 - ein verteiltes Protokoll
- Reihenfolge zyklisch oder anders (z.B. prioritätsgesteuert)
- **Zykluszeit**: Zeit bis Sendeerlaubnis zu Knoten zurückkommt =
für jeden Knoten: Sendezeit für Sendeerlaubnis + Ausbreitungszeiten + Verarbeitungszeiten +
Sendezeit für Daten echtzeitfähig (im gegensatz zu Zufallsprotokoll)
- Nachteile: **Overhead**, zentraler Knoten ist „Single-Point-of-Failure“

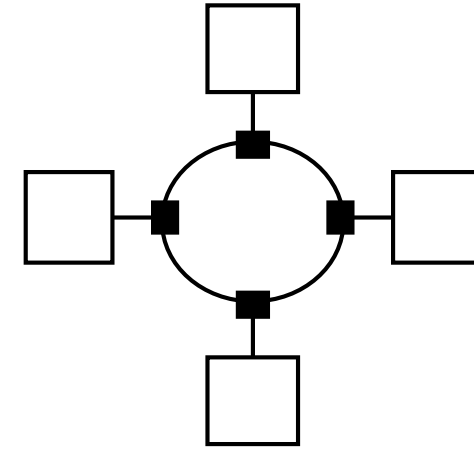


Medienzugriff

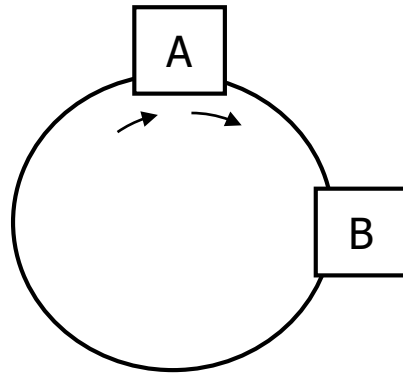
■ Zyklische Zuteilung

● Token Ring

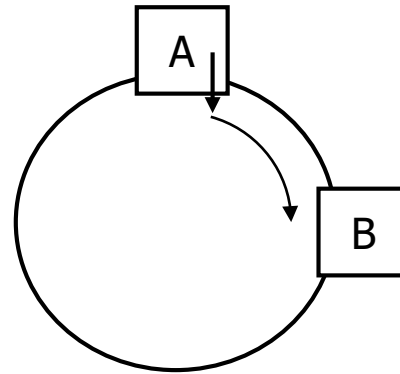
- die Knoten sind ringförmig vernetzt
- Knotenadapter hat Eingang und Ausgang, 2 Modi:
 - **Listen Mode:** Bits vom Eingang werden mit Pufferung (typisch 1 Bit) weitergereicht, Knoten erhält Kopie
 - **Transmit Mode:** Bits vom Eingang werden an Knoten geleitet, Bits zum Ausgang kommen vom Knoten
- ein Bitmuster (**Token**) zirkuliert auf Ring, 2 Zustände (**frei**, **belegt**), z.B.: frei = 0111111**0**, belegt = 0111111**1**
- wenn Knoten freies Token empfängt und Sendewunsch vorliegt, verändert er das Token durch Umsetzen des Bits in belegt und sendet Daten
- der Empfänger erhält die Daten
- nach Ringumlauf entfernt der Sender das belegte Token und die Daten wieder vom Ring und sendet das freie Token weiter



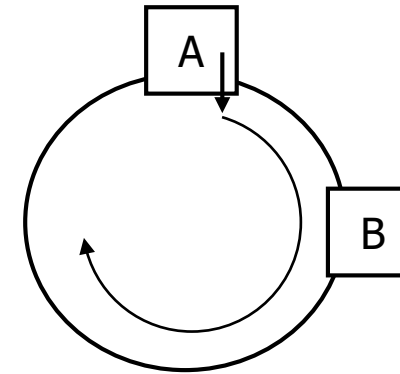
Medienzugriff



t_0 : A erhält freies Token,
sendet belegtes Token

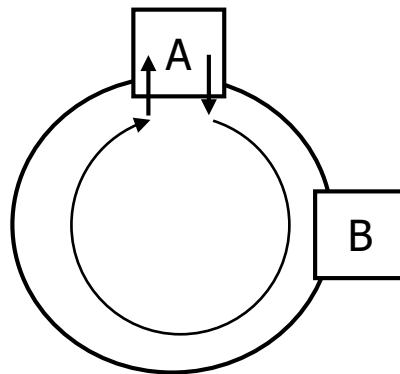


t_1 : Token erreicht B,
A sendet Rahmen

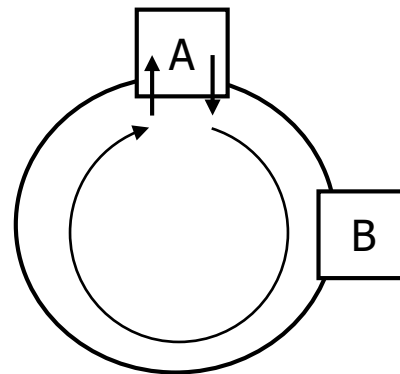


t_2 : Token und Rahmen
zirkulieren auf Ring

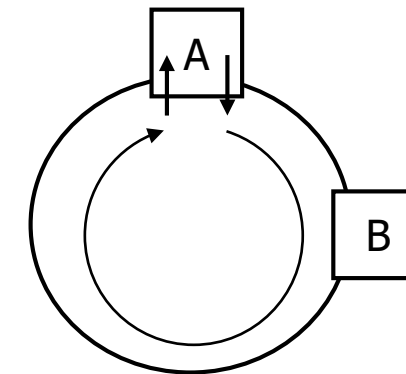
der Token switched also v



t_3 : Token kommt zu A zurück,
Token + Anfang des Rahmens
auf Ring



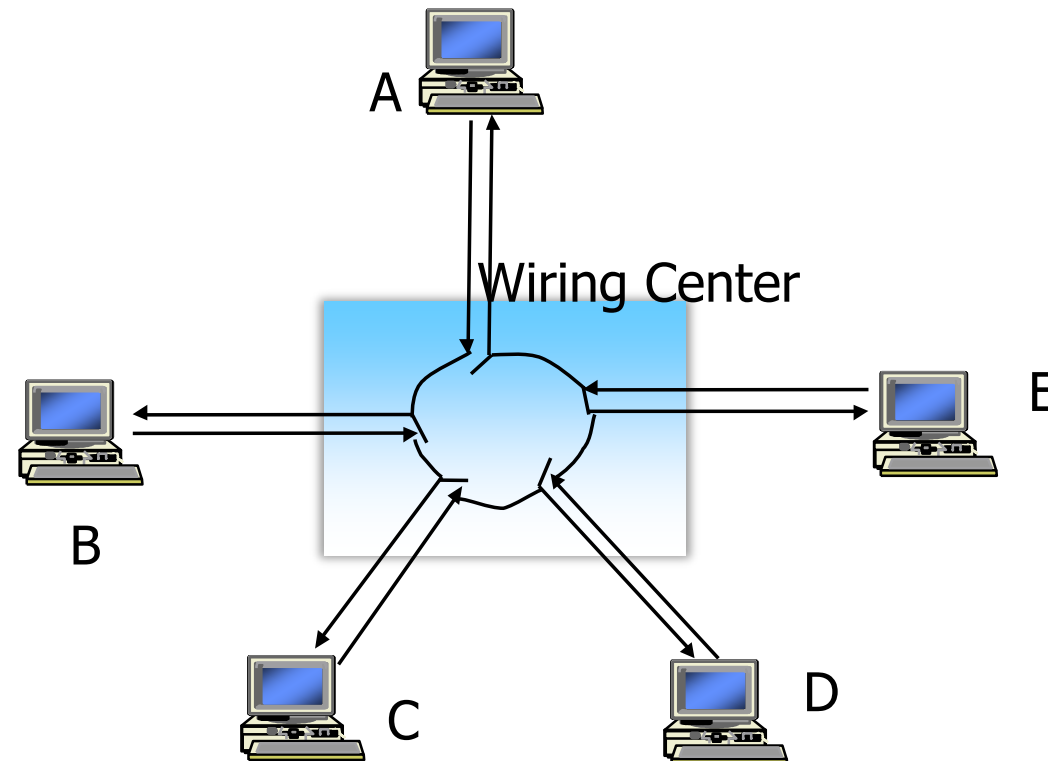
t_4 : Rahmenende
wird gesendet



t_5 : A sendet freies Token,
Ende des Rahmens +
Token auf Ring

Medienzugriff

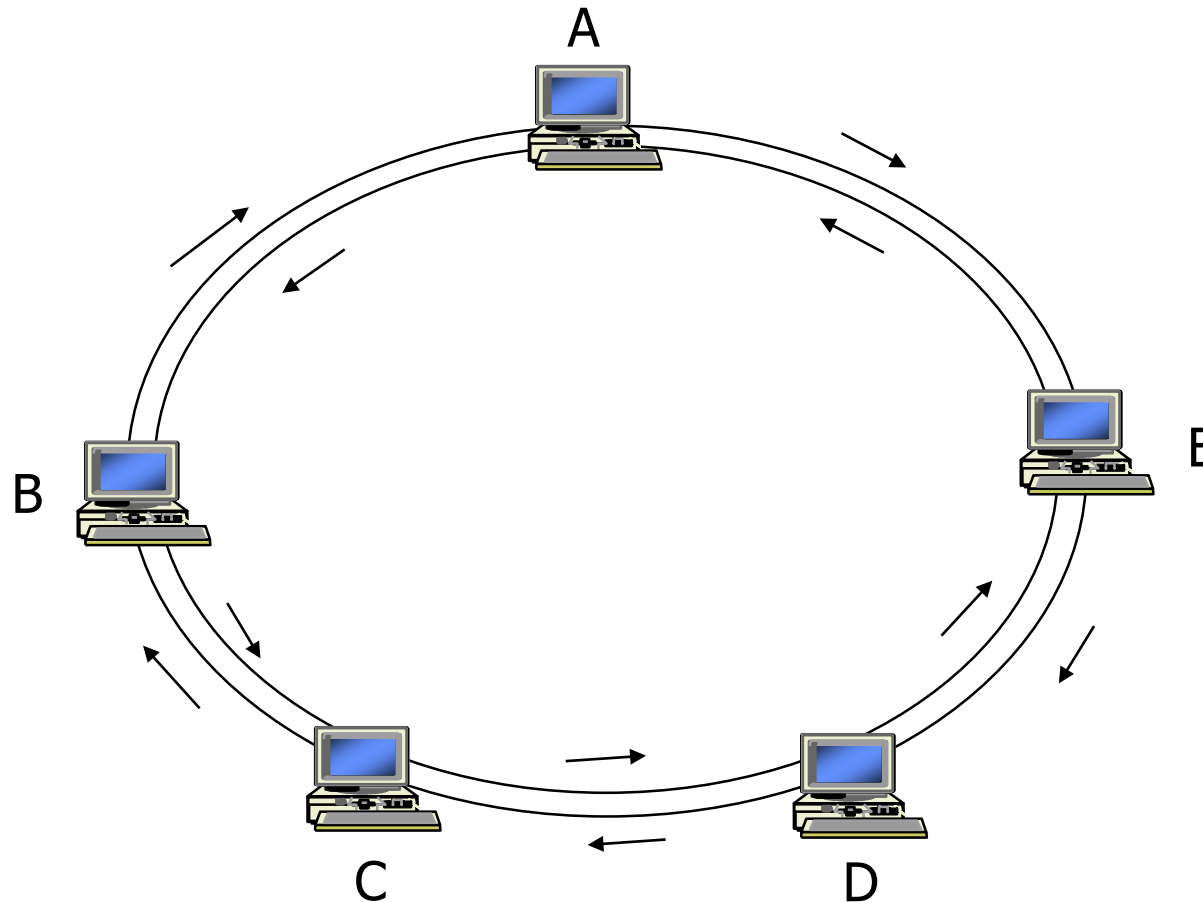
- Verkabelung: Ring mit sternförmiger Topologie



Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

Medienzugriff

- Verkabelung: gegenläufige Ringe für Fehlertoleranz bei Ausfall



Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

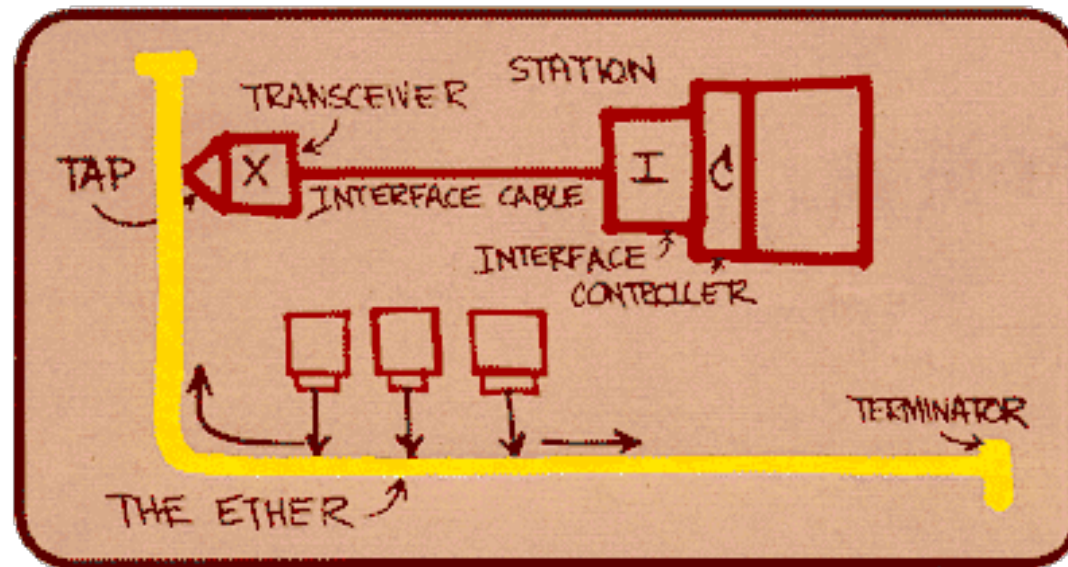
Sicherungsschicht

- ✓ Einführung
- ✓ Adressierung
- ✓ Datensicherung
- ✓ Medienzugriff
- Ethernet
- Drahtlose LANs

Ethernet

■ Ethernet

- dominierende Technologie für kabelgebundene LANs
- durchgesetzt gegen Token Ring, ATM u.a.
- durch Massenmarkt preiswerte Adapter
- Evolution der Bitraten: 10 Mbps – 100 Gbps
- Rahmenformat jeweils gleich, Kompatibilität

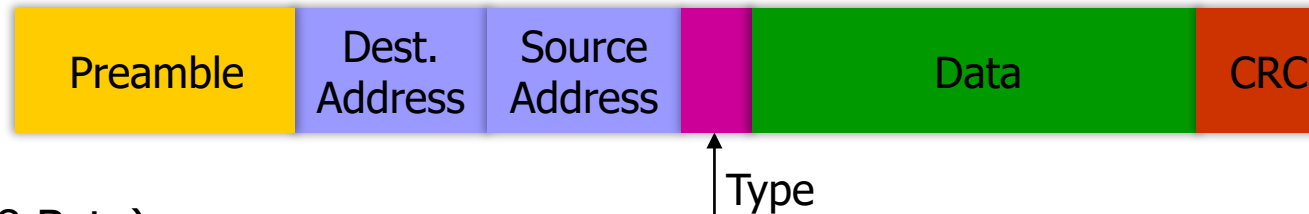


Metcalf's Ethernet-Skizze

Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Ethernet

■ Rahmenformat



Quelle: Kurose, Ross.
*Computer Networking:
A Top-Down Approach*,
7th Ed., Pearson
Education, 2017.

- Präambel (8 Byte)
 - 7 Bytes mit Muster 10101010, zur Synchronisation der Taktfrequenz (Ausgleich der Drift) vom Empfänger mit dem Sender
 - ein Byte mit Muster 10101011 zur Anzeige des Beginns der Zieladresse
- Quell- und Zieladresse (6 Byte): physikalische Adresse
- Type (2 Bytes): Nummer für Protokoll der Nutzdaten (IP, Appletalk, ...)
- Nutzdaten (46-1500 Byte)
- CRC (4 Bytes): CCITT-32
- Gesamtgröße: minimal 64 Byte (ohne Präambel)

Ethernet

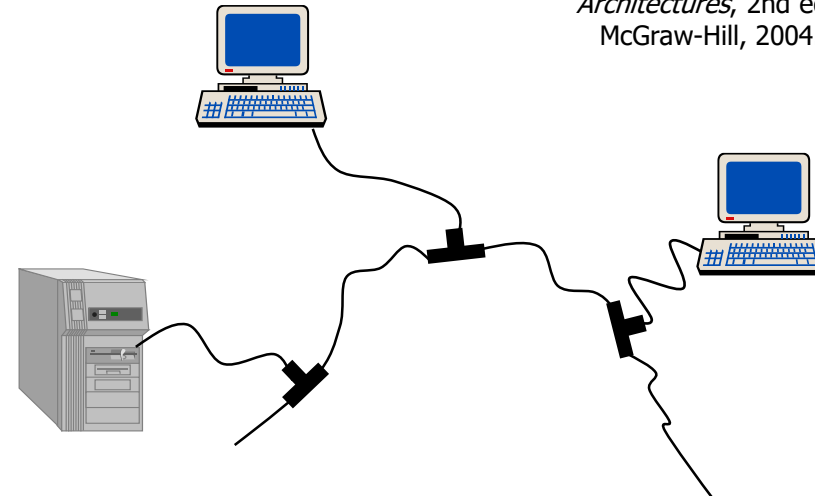
■ Medienzugriff

- 1-persistentes CSMA/CD
- Jam-Signal: 32-48 Bit
- binärer exponentieller Backoff
 - nach m-ter Wiederholung gleichverteilte Auswahl von K aus $[0, 2^n - 1]$ mit $n = \min(m, 10)$
 - Aufgabe nach 16 Wiederholungen
 - Backoffzeit von $K \cdot 512$ Bitzeiten
- verbindungslos: kein Handshaking erforderlich
- unzuverlässig: kein Versenden von Bestätigungen
- Erinnerung: minimale Sendezeit muss größer gleich zweifacher maximaler Ausbreitungszeit in Medium sein

Ethernet

■ Ursprüngliche Bus-Topologie (10Base5)

- Koaxialkabel ist Bus, Knoten über Transceiver angeschlossen
- Datenrate 10 Mbps
- maximale Segmentgröße: 500 m, max. 4 Repeater → max. Entfernung 2.500 m
- maximale RTT (mit Zeit in Repeatern): knapp 50 μ s
- Zeit zum Senden eines Bits: 0,1 μ s
- minimale Rahmengröße 512 Bits = 64 Bytes
- minimale Rahmen-Sendezeit: 51,2 μ s
- max. Durchsatz: $S_{\max} \approx 1/(1+4.4a)$
 - 64 Byte Rahmen \Rightarrow
 $a=0.48 \Rightarrow S_{\max} \approx 32 \%$
 - 640 Byte Rahmen \Rightarrow
 $a=0.048 \Rightarrow S_{\max} \approx 83 \%$
 - 6400 Byte Rahmen \Rightarrow
 $a=0.0048 \Rightarrow S_{\max} \approx 98 \%$



Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

Ethernet

■ Repeater

- zur Auffrischung von Signalen
- operiert auf physikalischer Schicht, transparent für Medienzugriffsschicht

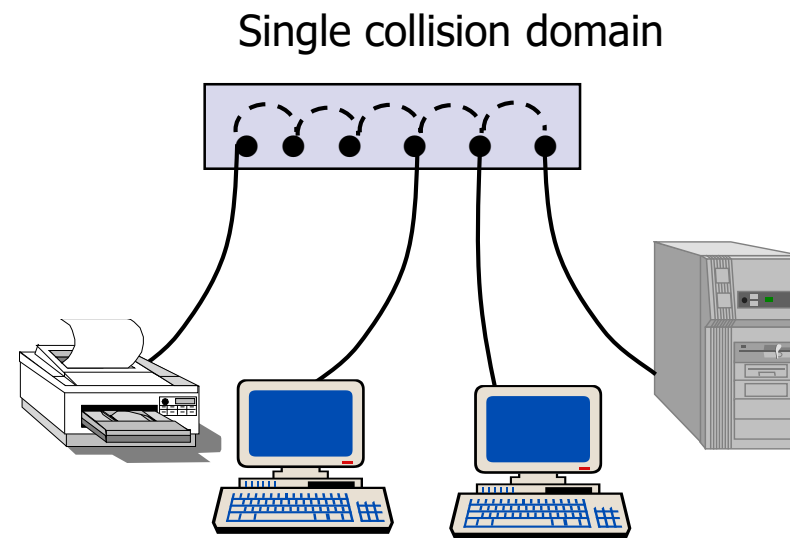
■ Bridge

- Verbindung von Ethernet-Segmenten
- bei jedem Empfang eines Rahmens an einem Eingangsport wird entschieden, an welchen Ausgangsport der Rahmen weitergeleitet wird und mittels CSMA/CD auf das Medium dieses Segments gegeben
- operiert auf Medienzugriffsschicht
- Aufteilung in verschiedene Kollisionsdomänen

Ethernet

■ Sterntopologie mit Hub (10BaseT)

- Hub: Repeater mit vielen Ports, keine Pufferung, aber Managementfunktion
- alle Knoten werden an zentralen Hub angeschlossen, das Signal auf jedem eingehenden Port wird auf jeden ausgehenden Port weitergegeben
- eine Kollisionsdomäne, CSMA/CD
- Twisted-Pair, RJ-45 (wie bei Telefon)
- Bitrate 10 Mbps
- Entfernung Hub-Knoten max. 100 m (200 m bei Kat. 5-Kabel)

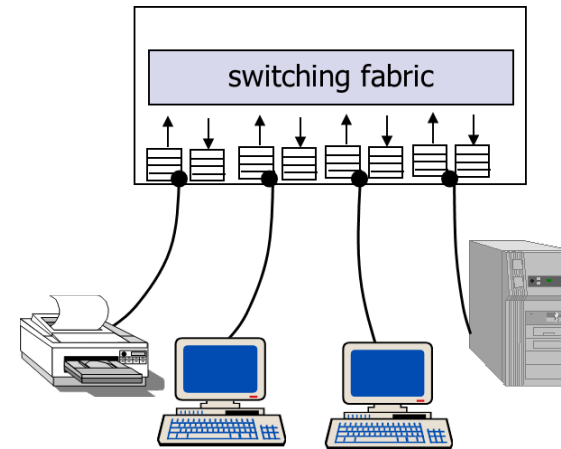


Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

Ethernet

■ Sterntopologie mit Switch

- Switch: Bridge mit vielen Ports, Pufferung an jedem Port, Store-and-Forward, voll-duplex
- Knoten führen noch CSMA/CD durch, Kollisionen treten aber nicht mehr auf
- Kaskadierung möglich
- Heterogenität von Bitraten möglich
- Kombination mit Hubs möglich



Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

Ethernet

■ Fast Ethernet

- Sterntopologie, Hubs, Switches
- Bitrate 100 Mbps
- 2 Modi: mit CSMA/CD für Hubs, ohne CSMA/CD für Switches
- Rahmenformat gleich
- Entfernung Hub-Knoten
 - Twisted Pair: max. 100 m (100BaseT)
 - Glasfaser: max. 2.000 m (100BaseFX)
- Kodierung 4B/5B-NRZI (mit Modifikationen für jedes Medium)
- Kaskadierung, Kombination Switches/Hubs möglich
- Kombination 10BaseT/100BaseT möglich: Switches mit Dual-Speed-Anschlüssen, die sowohl 10BaseT als auch 100BaseT beherrschen

Ethernet

■ Gigabit Ethernet

- Bitrate 1 Gbps, gleiches Rahmenformat, Kodierung 8B/10B
- Hubs (Buffered Distributers) mit Kollisionen, minimale Rahmengröße 512 Bytes (um Bedingung für Sendezeit und Ausbreitungszeit zu genügen)
- Switches ohne CSMA/CD
- 1000BaseT: Twisted Pair, 100 m
- 1000BaseSX: Multimode-Glasfaser (550 m)
- 1000BaseLX: Singlemode-Glasfaser (5 Km)

■ 10 Gigabit Ethernet

- Bitrate 10 Gbps, gleiches Rahmenformat, Kodierung 64B/66B
- CSMA/CD aufgegeben, nur Switches
- Entfernungen Multimode bis 300 m, Singlemode bis 40 Km

■ 40 und 100 Gigabit Ethernet

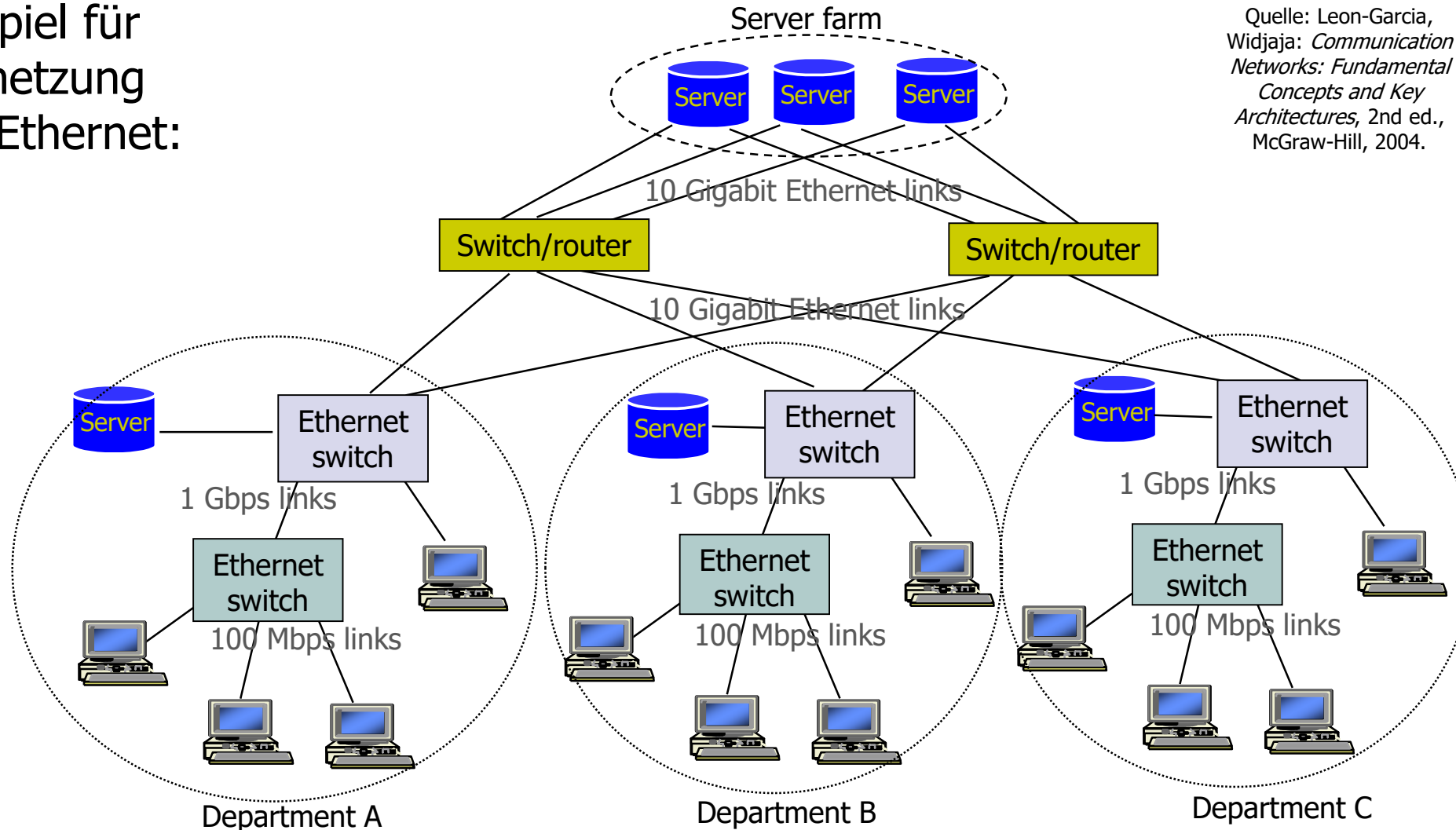
- Bitrate 40 und 100 Gbps, gleiches Rahmenformat, Kodierung 64B/66B
- Multilane Distribution: mehrere physikalische Kanäle
- Entfernungen Multimode bis 100 m, Singlemode bis 40 Km

■ Terabit Ethernet

- Standardisierungsaktivitäten für Bitraten > 100 Gbps

Ethernet

■ Beispiel für Vernetzung mit Ethernet:



Quelle: Leon-Garcia,
Widjaja: *Communication
Networks: Fundamental
Concepts and Key
Architectures*, 2nd ed.,
McGraw-Hill, 2004.

Ethernet

■ Selbstlernen

- wenn Switch Rahmen erhält, muss er Entscheidung treffen, wohin Rahmen weitergeleitet werden soll
- wenn die physikalische Zieladresse an dem Port ist, von dem der Rahmen kommt, wird er verworfen
- wenn der Port der physikalischen Adresse unbekannt ist, wird der Rahmen an alle Ports geflutet
- für einen eingehenden Rahmen wird die Zuordnung von physikalischer Adresse und Portnummer in Tabelle gespeichert
- Soft State, TTL z.B. 60 Minuten

■ Spanning Tree Protocol

- mit Switches können zyklische Strukturen aufgebaut werden, dann funktioniert Selbstlernen nicht
- alle Switches in einem LAN führen verteilten Algorithmus durch, so dass ein aufspannenden Baum entsteht (STP, IEEE 802.1D)
- Idee: Root Switch mit kleinster MAC-Adresse bestimmen, jeder Switch bestimmt kürzesten Pfad zu Root Switch, jeder Switch leitet nur auf den Ports auf dem kürzesten Pfad weiter
- Rapid Spanning Tree Protocol (RSTP, IEEE 801.1D-2004) konvergiert schneller (von 30 s unter 1 s)

Ethernet

■ Virtuelle LANs (VLANs)

- über Switches verbundene Knoten bilden Broadcastdomäne (z.B. für ARP, DHCP)
- VLANs: Aufteilung in scheinbar verschiedene LANs mit verschiedenen Subnetzen
- Ziele: Aufteilung, Lastoptimierung, Anpassung der logischen Netztopologie an Unternehmensorganisation (z.B. Arbeitsgruppen, Benutzermobilität)
- Konfiguration der Switches über Management-Software, basierend auf Ports, MAC-Adressen oder Protokollinformation
- Port-basiert
 - Endgeräte an bestimmten Ports bilden VLAN
 - Rahmen werden von Switch nur innerhalb VLAN weitergeleitet, Inter-VLAN-Verkehr geht über Router
- Tagging (Markierung)
 - Standard IEEE 802.1Q beschreibt VLAN-Tags in Ethernet-Rahmen
 - Rahmen mit VLAN-Tag werden zwischen Switches ausgetauscht
 - ermöglicht VLANs über mehrere Switches

Ethernet

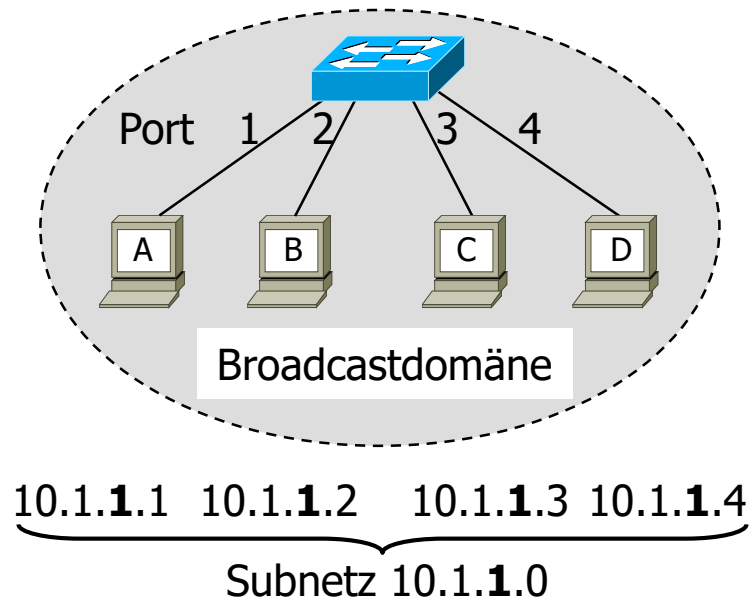
■ Beispiel für Port-basierte VLANs:

VLAN als Broadcastdomäne

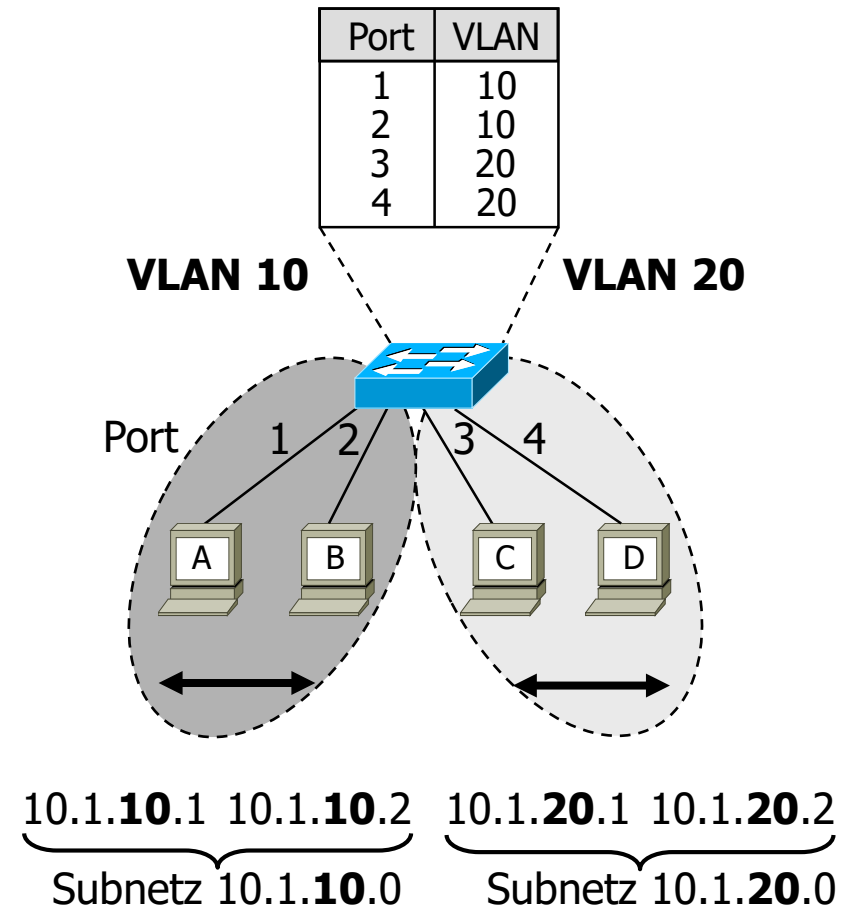
Anmerkungen:

- Standardmäßig gehören alle Interfaces eines Switches zum VLAN 1.
- Alle Geräte desselben VLANs ordnet man auch demselben Subnetz zu.

VLAN 1 (= LAN)



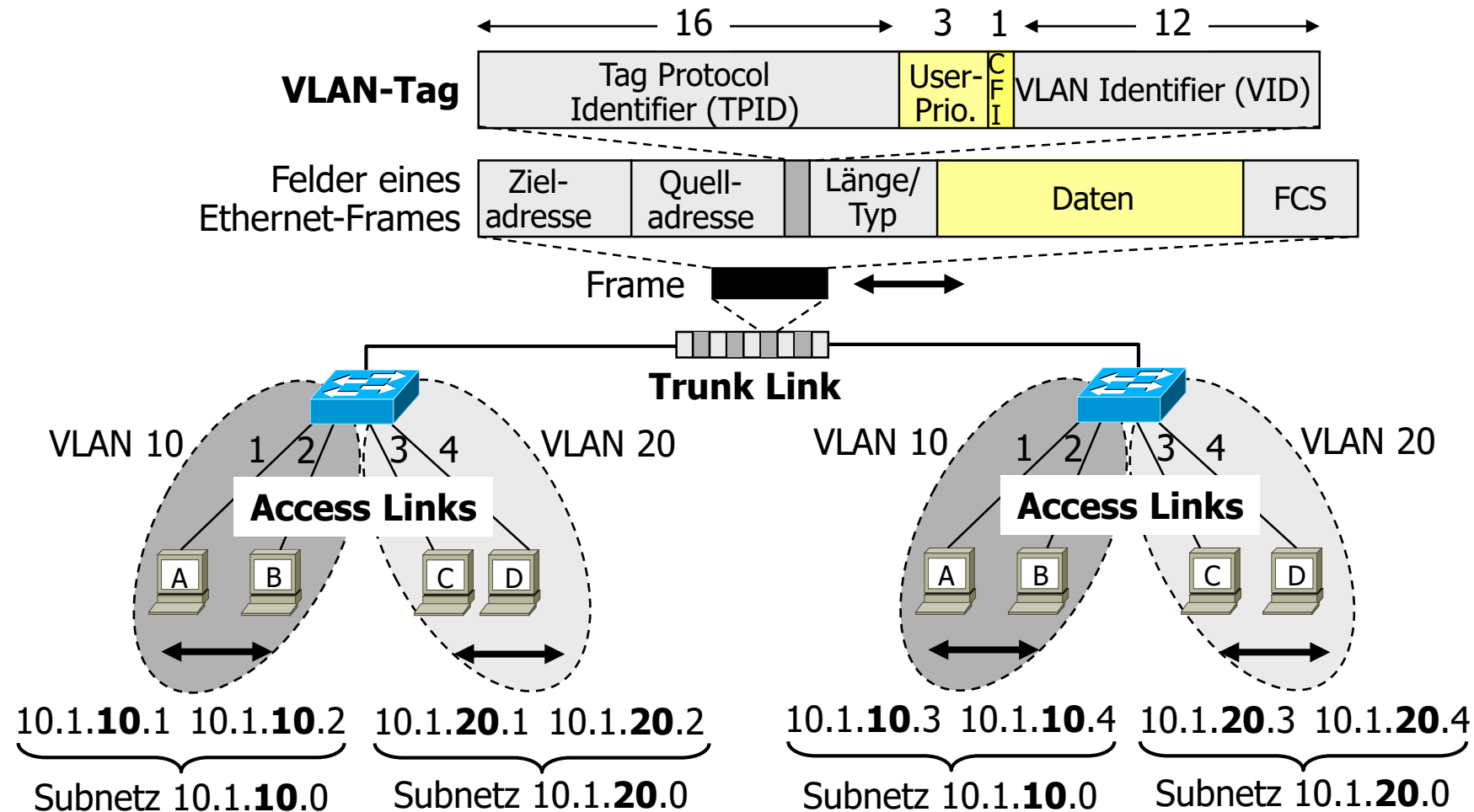
2 VLANs mit Intra-VLAN-Verkehr



aus J. Scherf:
Grundkurs
Computernetze,
Vieweg 2006

Ethernet

■ Beispiel für VLAN-Tagging:

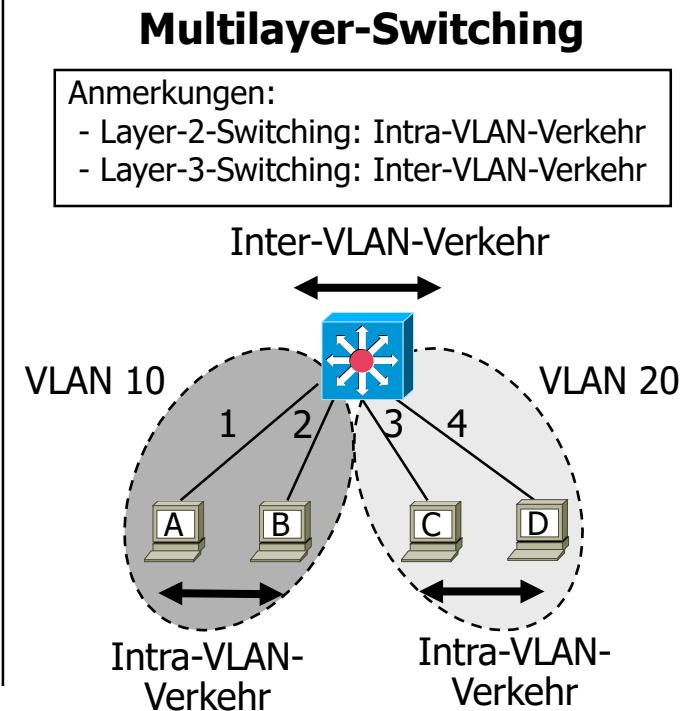
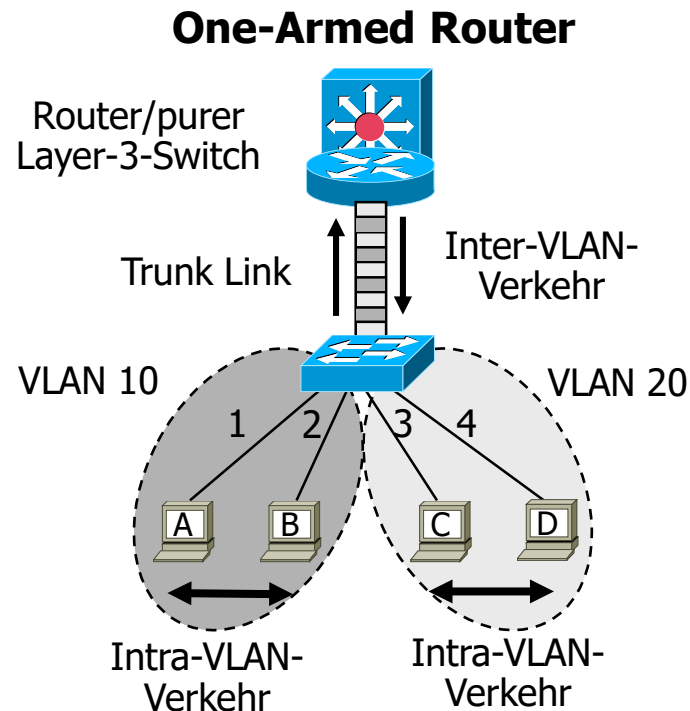


aus J. Scherf:
Grundkurs
Computernetze,
Vieweg 2006

Ethernet

■ Multilayer-Switching

- Intra-VLAN-Verkehr möglich mit Layer-2-Switching
- für Inter-VLAN-Verkehr wird Layer-3-Switching (IP-Forwarding) benötigt
- **Multilayer-Switching**: Integration Layer-3-Funktionalität in Layer-2-Switch



aus J. Scherf:
Grundkurs
Computernetze,
Vieweg 2006

Rechenzentrens (Data Center)-Netzwerke

- 10.000 – 100.000 Hosts, meist stark vernetzt und nahe beieinander
 - E-business (z.B. Amazon)
 - Content-server (z.B. YouTube, Akamai, Apple, Microsoft)
 - Suchmaschinen, Data Mining (z.B. Google)
- Herausforderungen
 - verschiedene Anwendungen, von denen jede eine enorme Anzahl von Nutzern hat
 - Lasten balancieren und managen, Verhinderung von Verarbeitungs-, Übertragungs- und Daten-Flaschenhälsen

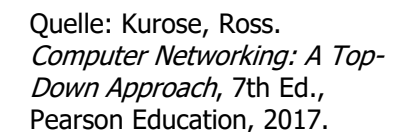


Innenansicht eines 40-ft Containers von Microsoft im Chicago Data-Center

Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

- Lastverteiler (Load Balancer)

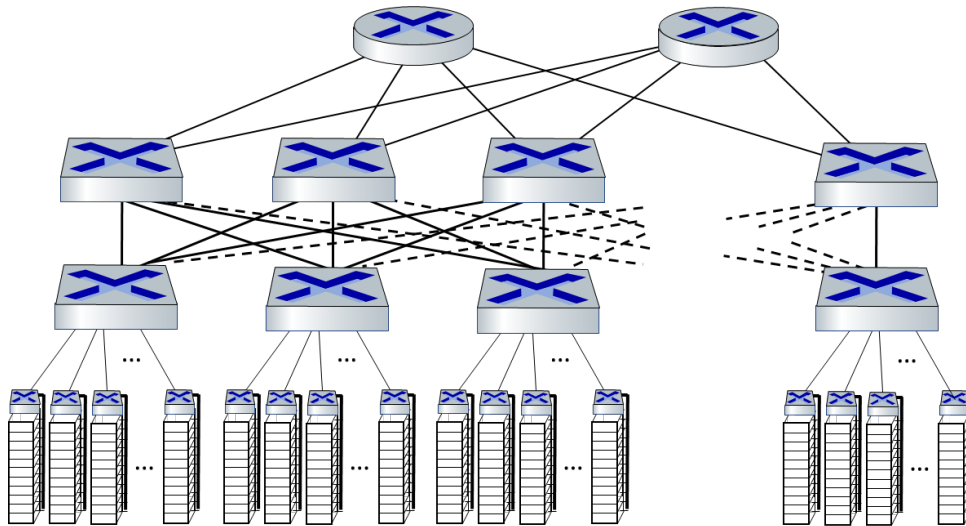
- nimmt externe Anfrage entgegen
- delegiert Arbeit innerhalb des Rechenzentrums
- übermittelt Resultat an externen Klienten (verbirgt interne Strukturen)



Rechenzentrs (Data Center)-Netzwerke

■ Motivation für SDN: Data Center Anforderungen

- z.B. 120.000 Server, jeweils 20 virtuelle Maschinen: 2.400.000 Hosts
- 80 % Ost-West-Verkehr, 20 % Nord-Süd-Verkehr
- Unterschied zu bisherigen Netzen: Stabilität der Topologie, Verkehrsmuster, Skalierung
- einige Probleme: Begrenzung von MAC-Tabellen, Broadcast falls kein Eintrag in MAC-Tabelle, zu kleine Anzahl möglicher VLANs (4096), Konvergenzzeit des Spanning-Tree-Protokolls, kein Multipath, ...



Border routers

- connections outside datacenter

Tier-1 switches

- connecting to ~16 T-2s below

Tier-2 switches

- connecting to ~16 TORs below

Top of Rack (TOR) switch

- one per rack
- 40-100Gbps Ethernet to blades

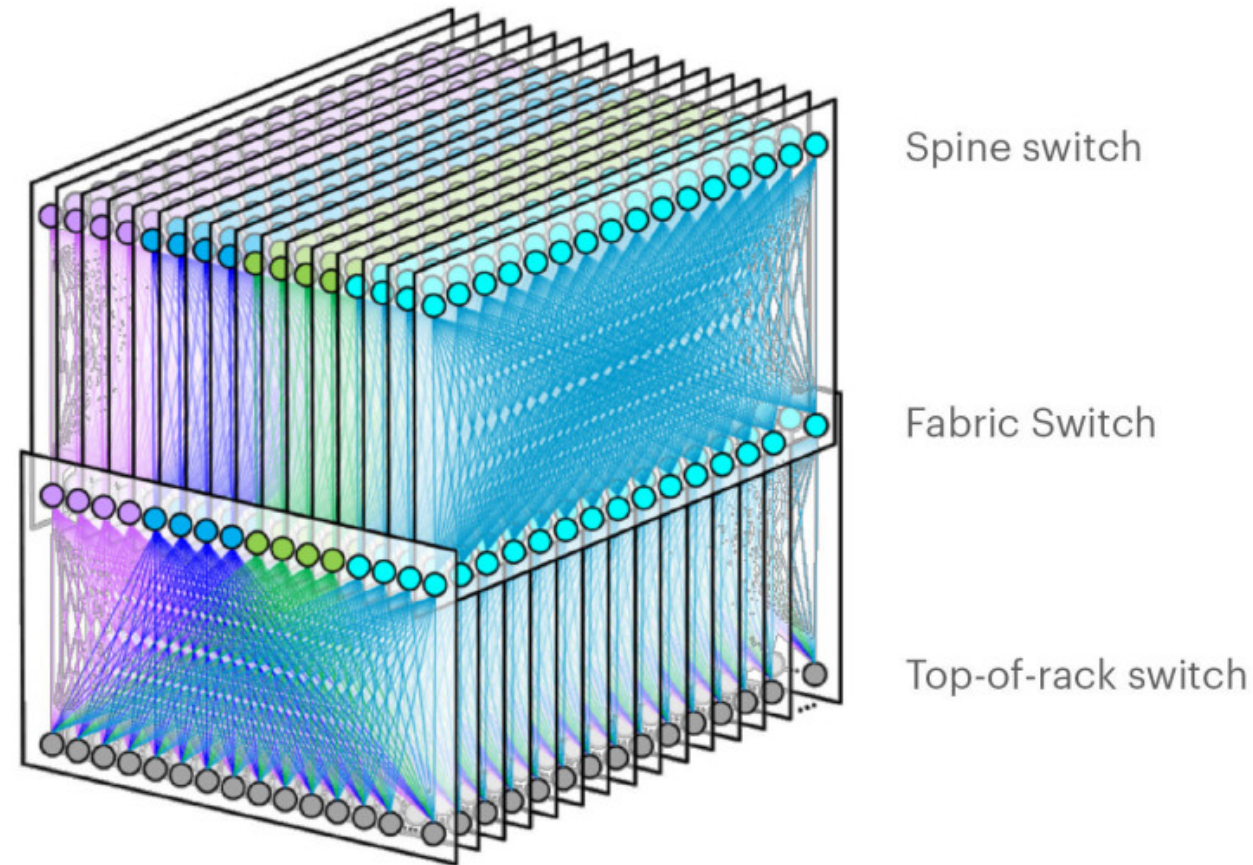
Server racks

- 20- 40 server blades: hosts

Quelle: Kurose, Ross.
*Computer Networking:
A Top-Down Approach*,
7th Ed., Pearson
Education, 2020.

Rechenzentrens (Data Center)-Netzwerke

■ Facebook F16 data center network topology:



<https://engineering.fb.com/data-center-engineering/f16-minipack/> (posted 3/2019)

Sicherungsschicht

- ✓ Einführung
- ✓ Adressierung
- ✓ Datensicherung
- ✓ Medienzugriff
- ✓ Ethernet
- Drahtlose LANs

Drahtlose LANs

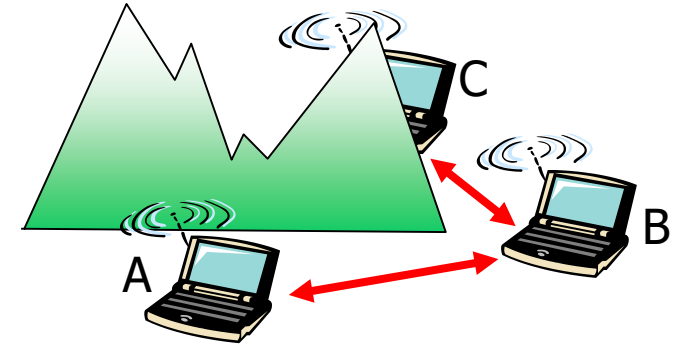
■ Charakteristika von Funkkommunikation

- Dämpfung: Abnahme der Signalstärke ca. quadratisch mit Entfernung, abhängig von Umgebung
- Interferenzen durch andere Sender (drahtlose Netze, schnurlose und mobile Telefone, Mikrowellenöfen, Motoren, ...)
- Mehrwegausbreitung: Funkwellen werden reflektiert, phasenverschobene Wellen überlagern sich und schwächen sich kurzfristig ab bzw. löschen sich aus (Short-Range Fading)
- höhere Fehlerrate, insbesondere als Bursts

Drahtlose LANs

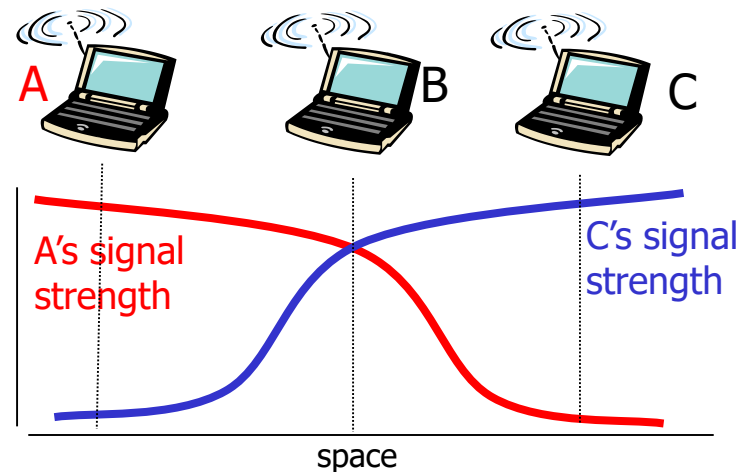
■ Hidden-Terminal Problem:

- A, B hören sich
- C, B hören sich
- A, C hören sich nicht,
A und C wissen nichts von möglichen Kollisionen bei B



Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

■ genauso möglich durch Signaldämpfung:



Drahtlose LANs

■ Drahtlose LANs nach IEEE 802.11

- 90er Jahre Beginn der Standardisierung: ETSI HIPERLAN und IEEE 802.11
- 802.11-1997 mit Infrarot und Funk (FHSS, DSSS) bei 1 und 2 Mbps (Brutto)
- Amendments in diversen Task Groups, 11b (11 Mbps), 11g (54 Mbps), 11n (600 Mbps), 11i (Sicherheit), 11e (Quality-of-Service), 11p (Vehicular), 11ac (Very High Throughput < 6 GHz), 11ad (Wireless Gigabit bei 60 GHz, WiGig) ...
- Aufnahme in konsolidierte Standards: 802.11-2003, 802.11-2007, 802.11-2012 (2.793 Seiten), 802.11-2016 (3.534 Seiten)
- **Wi-Fi-Alliance**: Industrieforum zur Zertifizierung interoperabler Produkte
- Betriebsmodi: Infrastrukturnetz (Access Points, Distribution Service), Ad-Hoc-Netz, Mesh Network (drahtlose Multi-Hop-Weiterleitung)
- Adressierung: 4 physikalische Adressen
- Medienzugriff: CSMA/CA (Collision Avoidance)
 - Kollisionserkennung würde 2. Antenne benötigen, die während des Sendens empfängt, schwieriger, teurer
 - 2 Varianten: Basic Access, RTS/CTS-Austausch
- Energiesparen: Schlafphasen, synchronisiertes Aufwachen

Drahtlose LANs: Architektur eines Infrastrukturnetzes

■ Station (STA)

- System mit Zugriffsfunktion auf das drahtlose Medium und Funkkontakt zum Access Point

■ Zugangspunkt, Access Point (AP)

- Station, die sowohl in das Funk-LAN als auch das verbindende Netz (Distribution System) integriert ist

■ Basic Service Set (BSS)

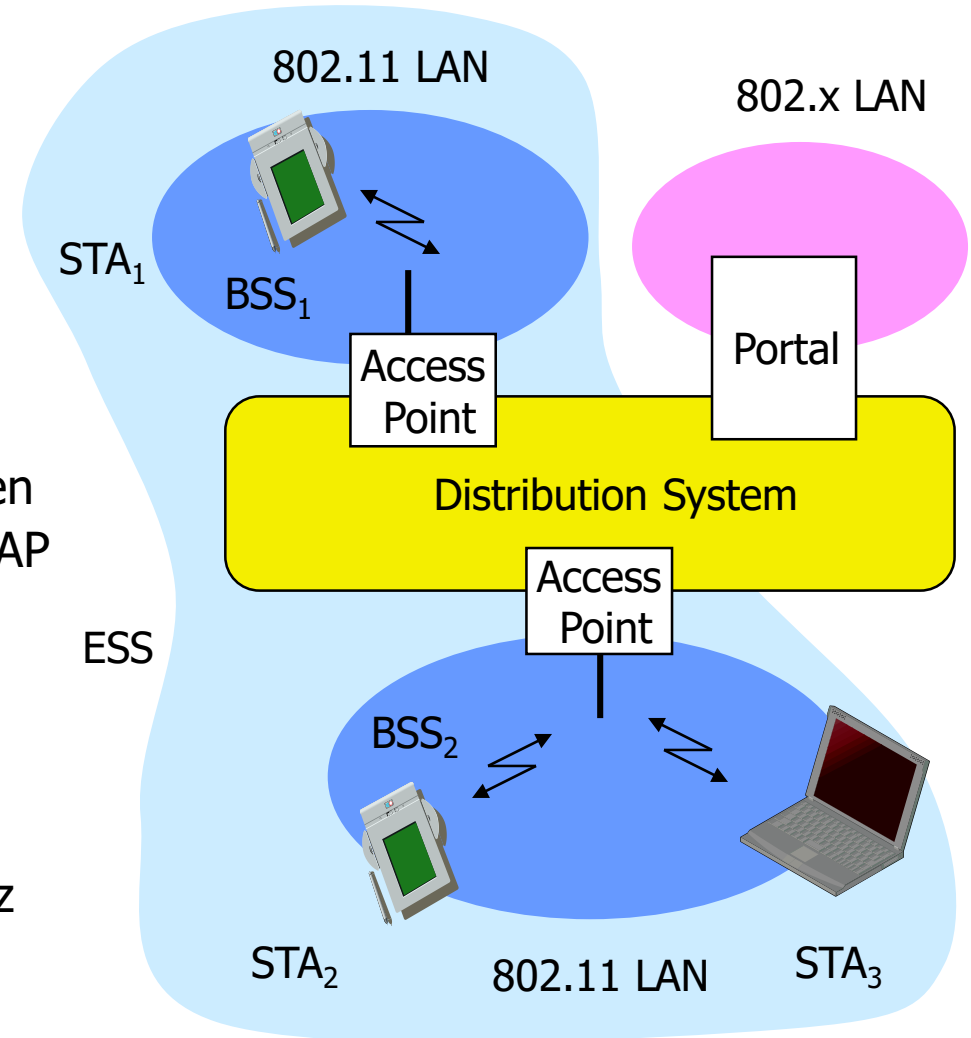
- Gruppe von Stationen, die dieselbe Funkfrequenz nutzen
- Basic Service Set Identifier (BSSID): MAC-Adresse des AP
- SSID: Zeichenkette

■ Portal

- Übergang in ein anderes Netz

■ Distribution System (DS)

- Verbindung der APs über Schicht 2, gleiches IP-Subnetz
- Extended Service Set (ESS): Vereinigung von BSSs mit gleicher SSID



Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

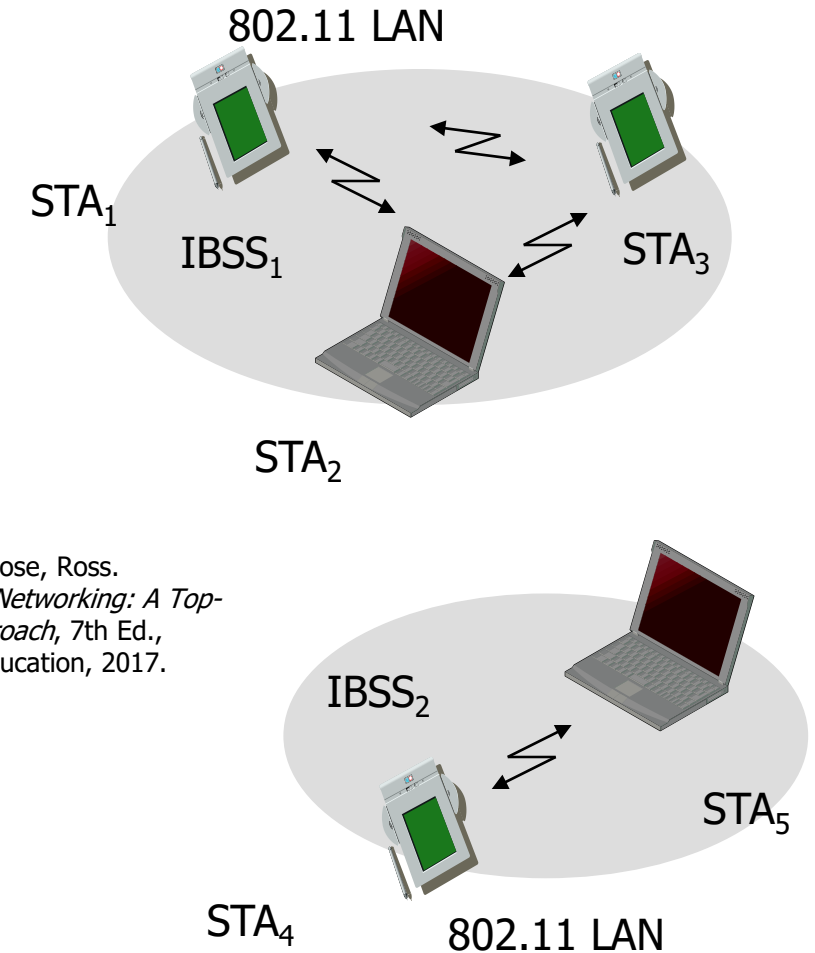
Drahtlose LANs: Architektur eines Ad-Hoc-Netzes

■ Station (STA)

- System mit Zugriffsfunktion auf das drahtlose Medium

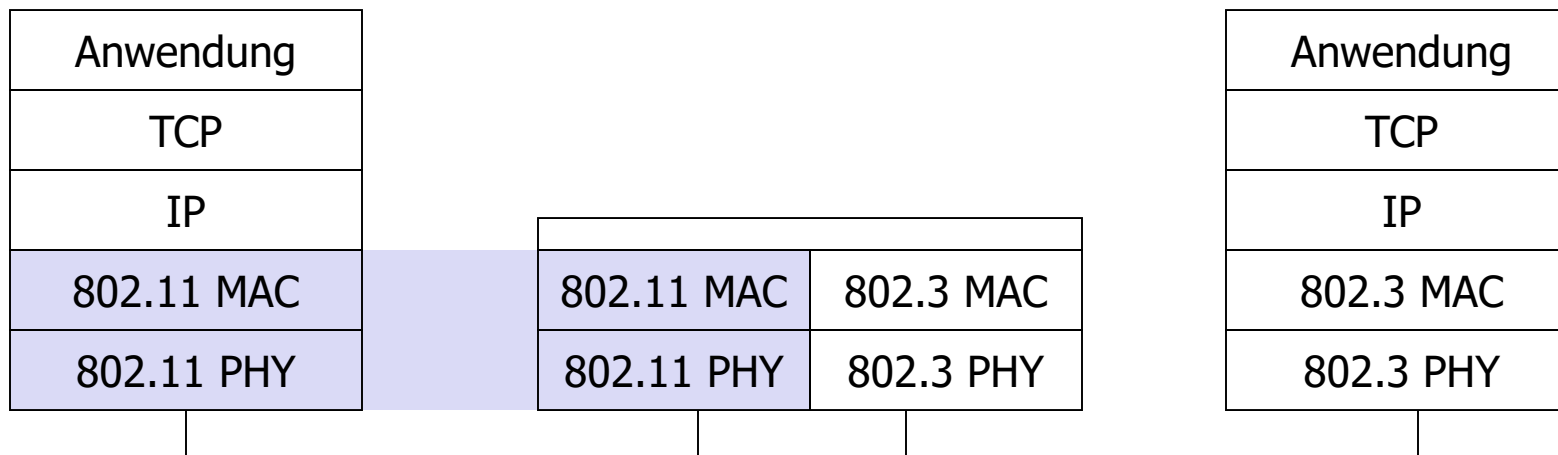
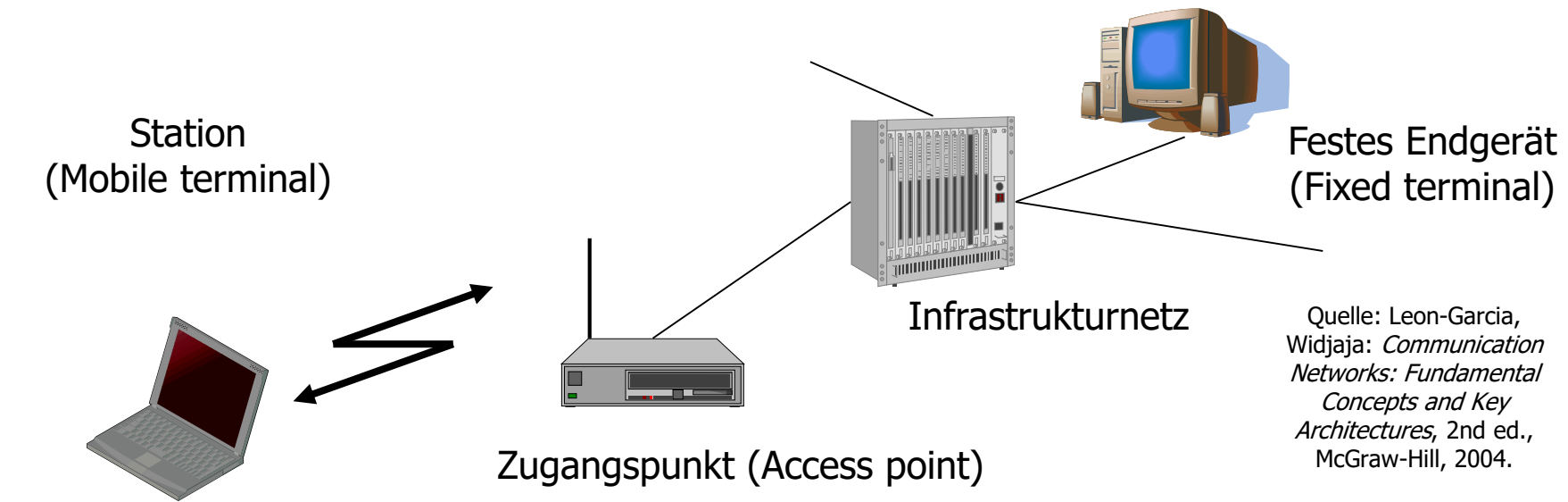
■ Independent Basic Service Set (IBSS)

- Gruppe von Stationen, die dieselbe Funkfrequenz nutzen
- zufällige MAC-Adresse als BSSID



Quelle: Kurose, Ross.
Computer Networking: A Top-Down Approach, 7th Ed.,
Pearson Education, 2017.

Drahtlose LANs: Protokollarchitektur bei Infrastrukturnetz



Drahtlose LANs

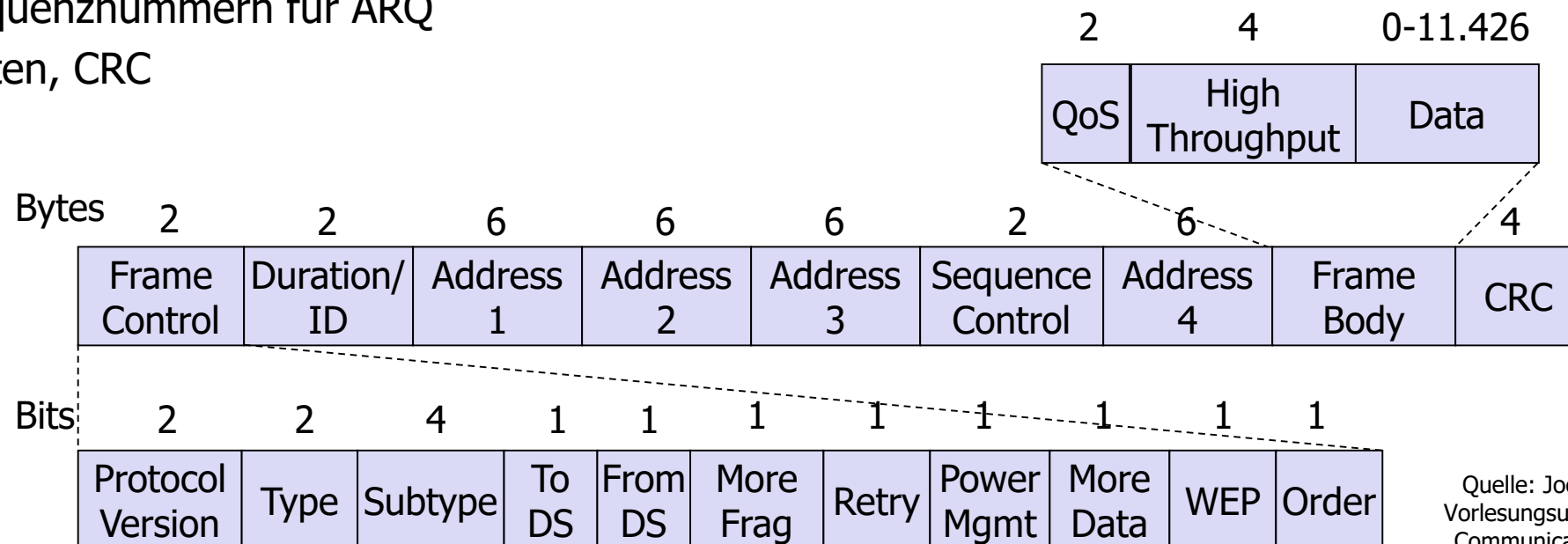
■ Physikalische Varianten u.a.

| | Frequenz | max. Bitrate | PHY-Technologien, Bemerkungen |
|--------------------------|---------------|--------------|---|
| 802.11-1997 | 2,4 GHz | 1-2 Mbps | Frequency-Hopping Spread Spectrum & Direct Sequence Spread Spectrum |
| 802.11b (1999) | 2,4 GHz | 11 Mbps | Complementary Code Keying (CCK) & QPSK |
| 802.11a (1999) | 5 GHz | 54 Mbps | OFDM |
| 802.11g (2003) | 2,4 GHz | 54 Mbps | Orthogonal Frequency Division Multiplexing (OFDM) & CCK für Rückwärtskompatibilität mit 802.11b |
| 802.11n (2009) | 2,4 und 5 GHz | 600 Mbps | OFDM, Multiple Input Multiple Output (MIMO), Frameaggregation |
| 802.11ac (2012) | 5 GHz | 3,2 Gbps | Bandwidth Expansion (max. 160 MHz), Multiuser MIMO, Frameaggregation |
| 802.11ad (2014) | 60 GHz | 6,76 Gbps | 2.160 MHz Bandbreite, Millimeterwellen, keine Objektdurchdringung, Beamforming |
| 802.11ax (2020 erwartet) | 2,4 und 5 GHz | 14 Gbps | OFDM, Multiuser MIMO, Spatial Reuse |

Drahtlose LANs: MAC

■ MAC-Rahmenformat

- Rahmensteuerung
 - Type: Management (00), Steuerung (01), Daten (10)
 - Subtype: Association Request, Data, ACK, RTS, CTS, ...
- Belegungsdauer des Mediums in μs (für RTS/CTS) oder ID
- 4 physikalische Adressen: Empfänger, Sender, weitere Adressen
- Sequenznummern für ARQ
- Daten, CRC



Quelle: Jochen H. Schiller,
Vorlesungsunterlagen "Mobile
Communications", FU Berlin

Drahtlose LANs: MAC

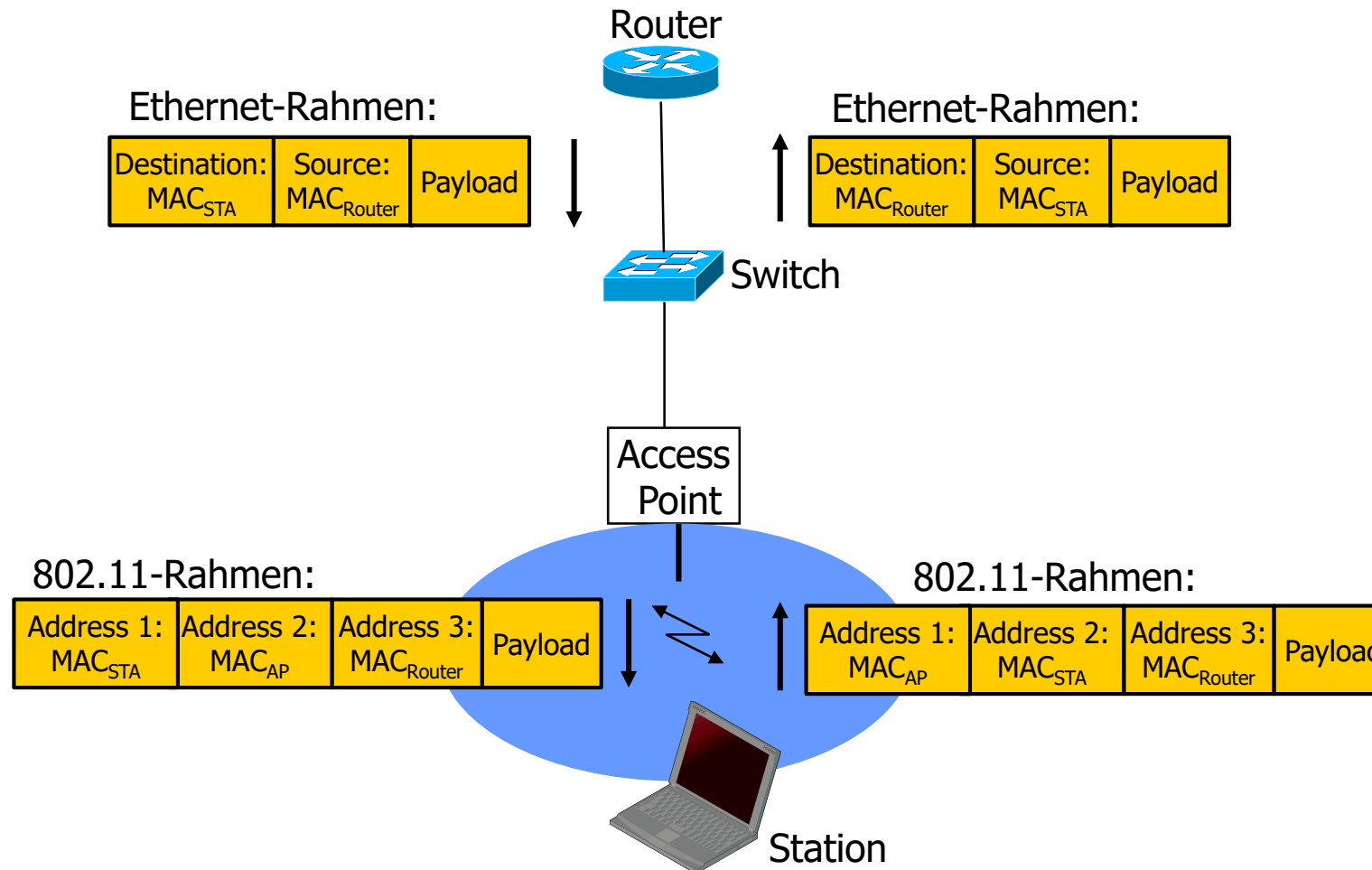
■ Interpretation der 4 Adressen

- Identifikation der STAs und APs durch physikalische Adresse
- Service Set IDs (BSSIDs): Identifikation des BSS: zufällige physikalische Adresse bei Ad-Hoc-Netzen, Adressen der APs in Infrastrukturnetzen
- abhängig von der Rahmenart werden DS-Bits gesetzt und Adressen unterschiedlich interpretiert:

| Rahmenart | to DS | from DS | Address 1 (Empfänger) | Address 2 (Sender) | Address 3 (zusätzlich) | Address 4 |
|----------------------------------|-------|---------|-------------------------|----------------------|------------------------|-----------|
| Ad-Hoc-Netz, STA → STA | 0 | 0 | Empfänger-STA | Sender-STA | (zufällige) BSSID | - |
| Infrastrukturnetz, STA → AP | 1 | 0 | AP | Sender-STA | Ziel, z.B. Router | - |
| Infrastrukturnetz, AP → STA | 0 | 1 | Empfänger-STA | AP | Quelle, z.B. Router | - |
| 4 Adressen, nur für Mesh Network | 1 | 1 | Empfänger aktueller Hop | Sender aktueller Hop | Quelle | Ziel |

Drahtlose LANs: MAC

- Verwendung der Adressen, Kommunikation zwischen Router und Station:



Drahtlose LANs: MAC

■ Medienzugriff gemäß Basic Access

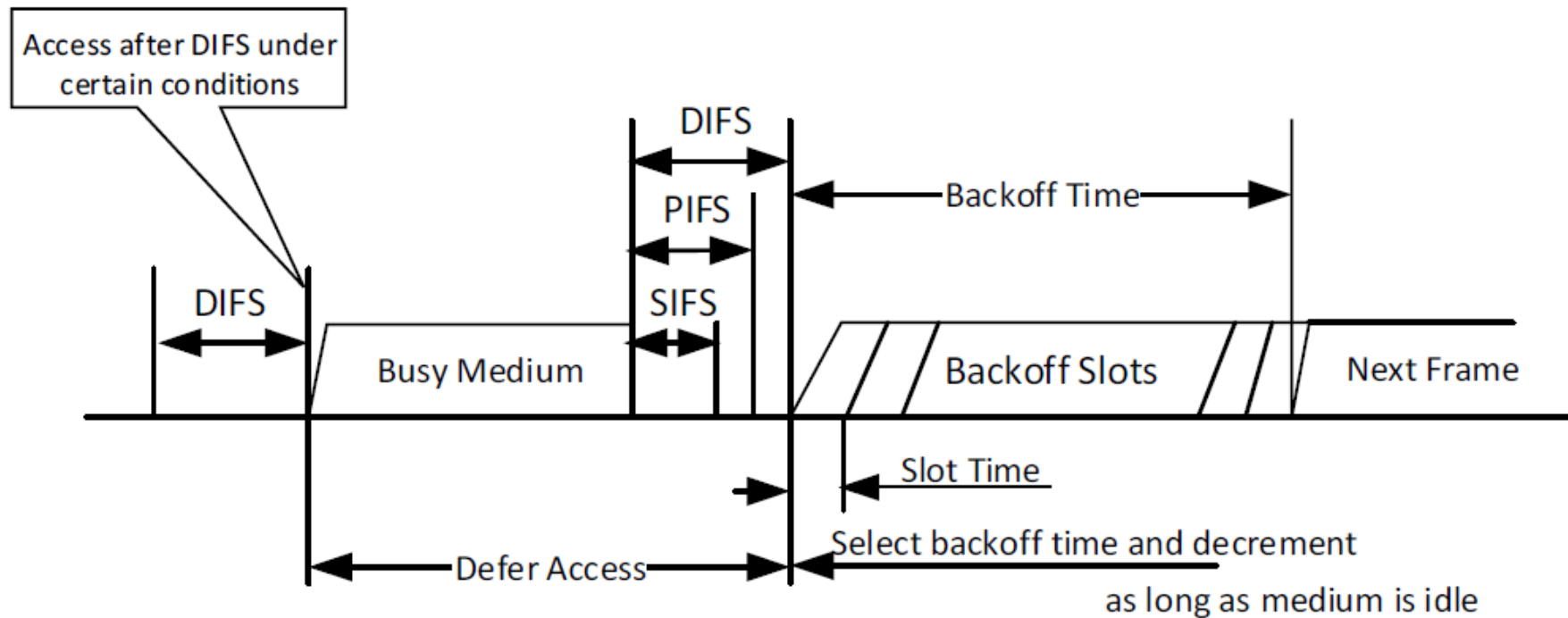
- wenn die MAC-Schicht einer Station von der Netzwerkschicht ein Datagramm erhält, überprüft sie das Medium (listen before talking); wenn es eine Zeitdauer **DIFS (Distribution Interframe Space)** frei ist, wird der Rahmen gesendet, sonst geht sie in Backoff
 - wenn der Empfänger ihn fehlerlos erhält, wartet er eine Zeitdauer **SIFS (Short Interframe Space)**, dann sendet er eine positive Bestätigung (ACK) zurück
 - wenn nach einem Timeout kein ACK zurückkommt, geht der Sender in Backoff
 - Truncated Binary Exponential Backoff: abhängig von Anzahl der Kollisionen würfelt der Sender eine zufällige Wartezeit, **reduziert sie solange das Medium frei ist** und wiederholt dann die Sendung
- Variante von nicht-persistentem CSMA/CA (DIFS, SIFS ist neuer Aspekt)

Drahtlose LANs: MAC

■ Zeitablauf beim Medienzugriff:

Backoff-Mechanismus:

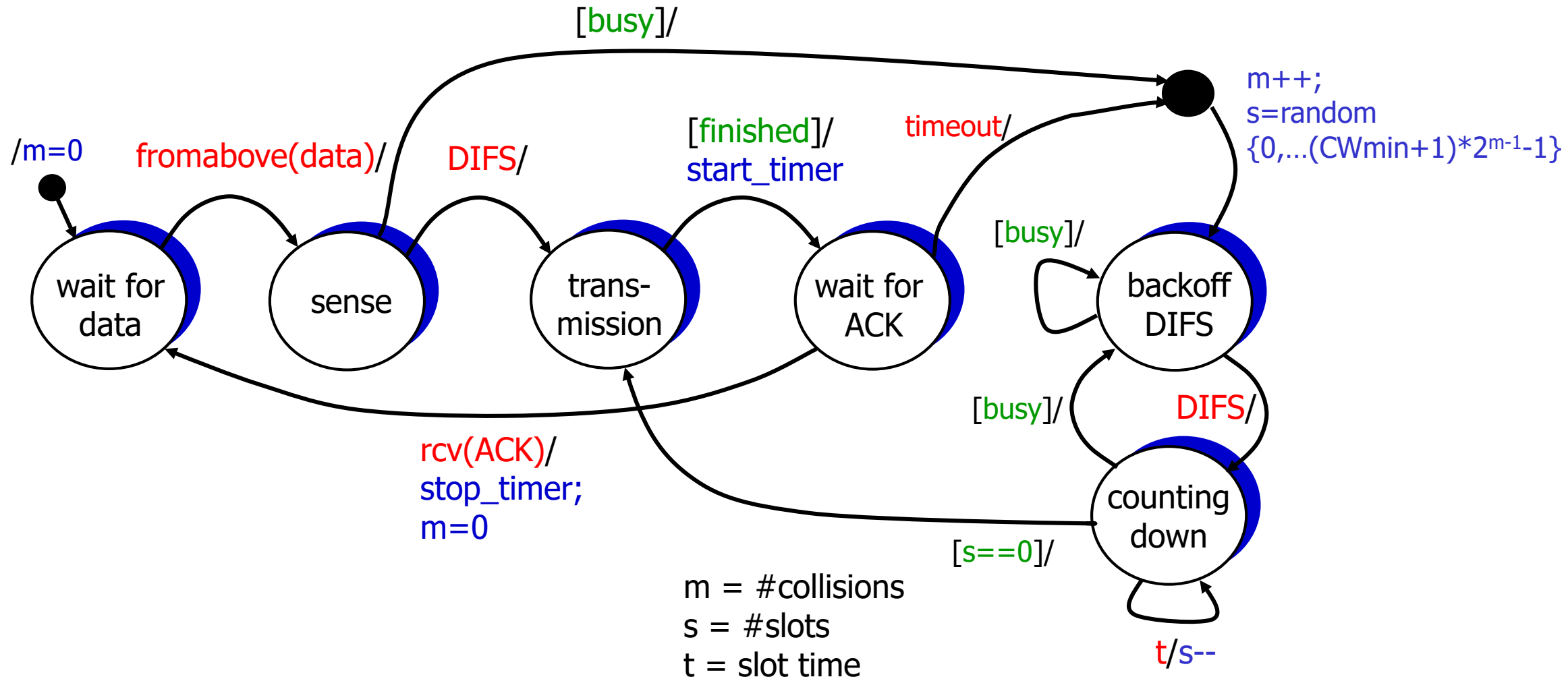
- initial Contention Window $CW = CW_{min}$
- nach jedem Sendeversuch $CW := (CW+1)*2-1$
- bis $CW = CW_{max}$, dann bleibt CW konstant
- Wartezeit: gleichverteilte Auswahl aus $\{0, \dots, CW\}$ Slot Times
- Unterbrechung des Dekrementierens wenn Medium belegt
- z.B. für OFDM: $CW_{min} = 15$, $CW_{max} = 1023$, Slot Time = 13 μs



Quelle: IEEE 802.11-2016

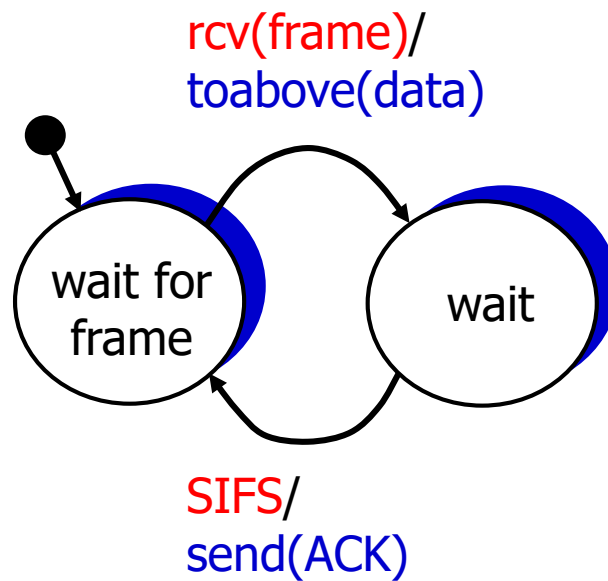
Drahtlose LANs: MAC

■ Statechart des Senders:



Drahtlose LANs: MAC

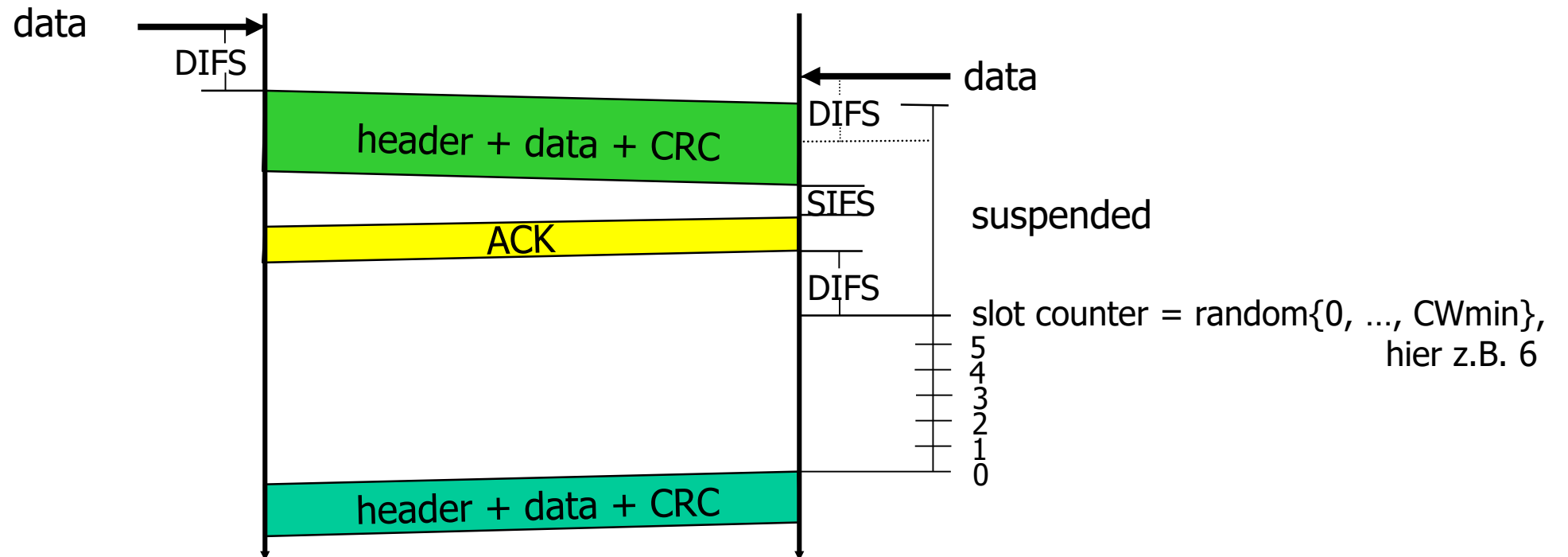
■ Statechart des Empfängers:



Drahtlose LANs: MAC

■ Beispielablauf 1

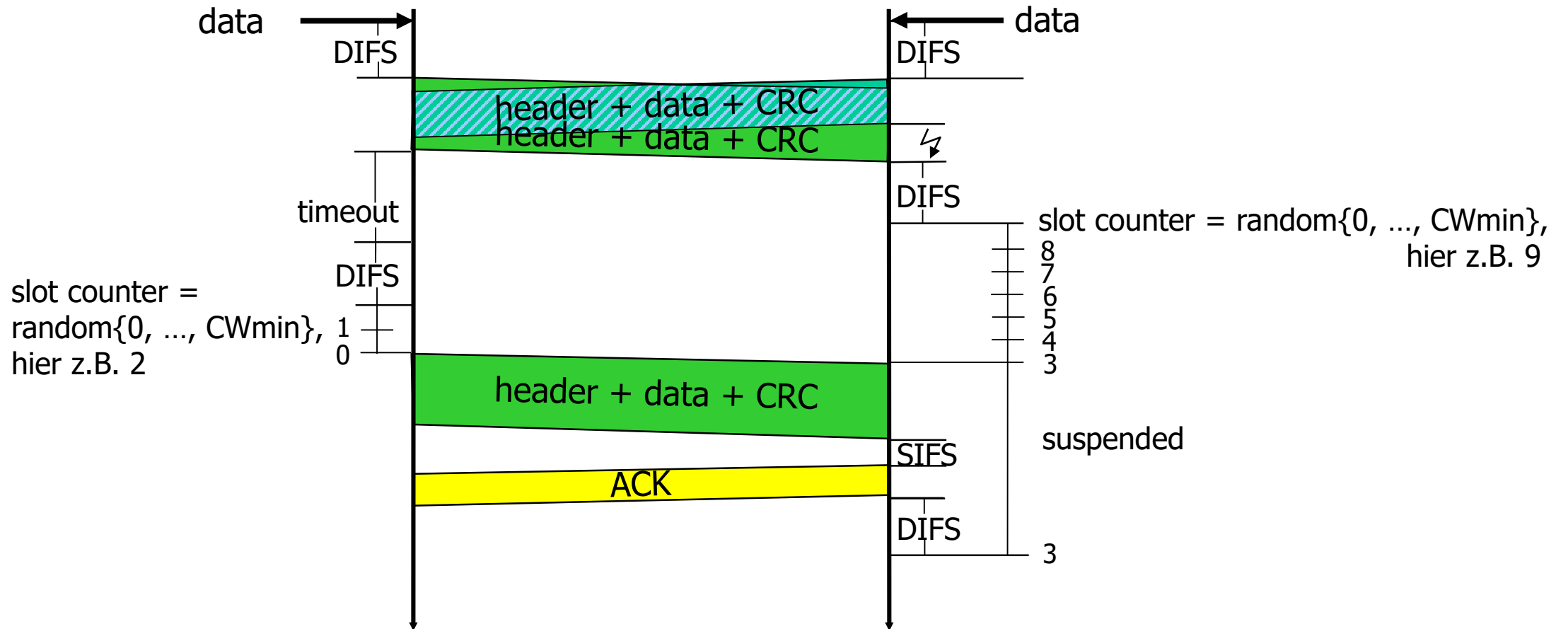
- zwei Stationen wollen zu ähnlicher Zeit senden, durch DIFS wird Kollision vermieden:



Drahtlose LANs: MAC

■ Beispielablauf 2

- zwei Stationen wollen fast gleichzeitig senden, Unterschied kleiner als Ausbreitungsverzögerung, eine Kollision entsteht und wird aufgelöst:



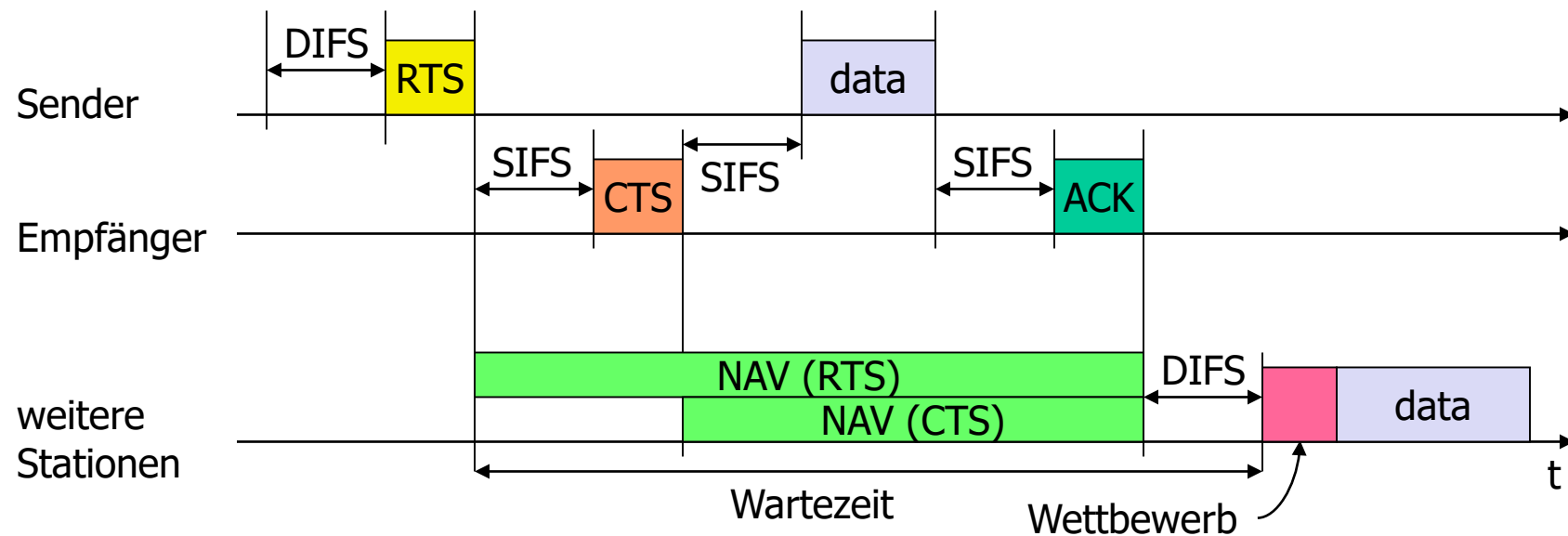
Drahtlose LANs: MAC

■ RTS/CTS-Austausch

- vorheriger Austausch von kurzen Reservierungsnachrichten
- Sender sendet Request-To-Send (RTS) mit Länge des Rahmens, Empfänger (Station bei Ad-Hoc-Netz, AP bei Infrastrukturnetz) antwortet mit Clear-To-Send (CTS), in der Länge auch steht
- Medienzugriff für RTS mit Basic Access
- Nachteil: größerer Overhead
- Vorteile:
 - wenn keine Kollision auftritt, ist Medium reserviert, wenn Kollision auftritt, dauert diese nicht lange (RTS kurz)
 - Hidden-Terminal-Problem teilweise gelöst: die Stationen, die Sender nicht hören, erfahren vom Empfänger Reservierung

Drahtlose LANs: MAC

- Zeitablauf beim Medienzugriff mit RTS/CTS-Austausch:



Quelle: Jochen H. Schiller,
Vorlesungsunterlagen "Mobile
Communications", FU Berlin

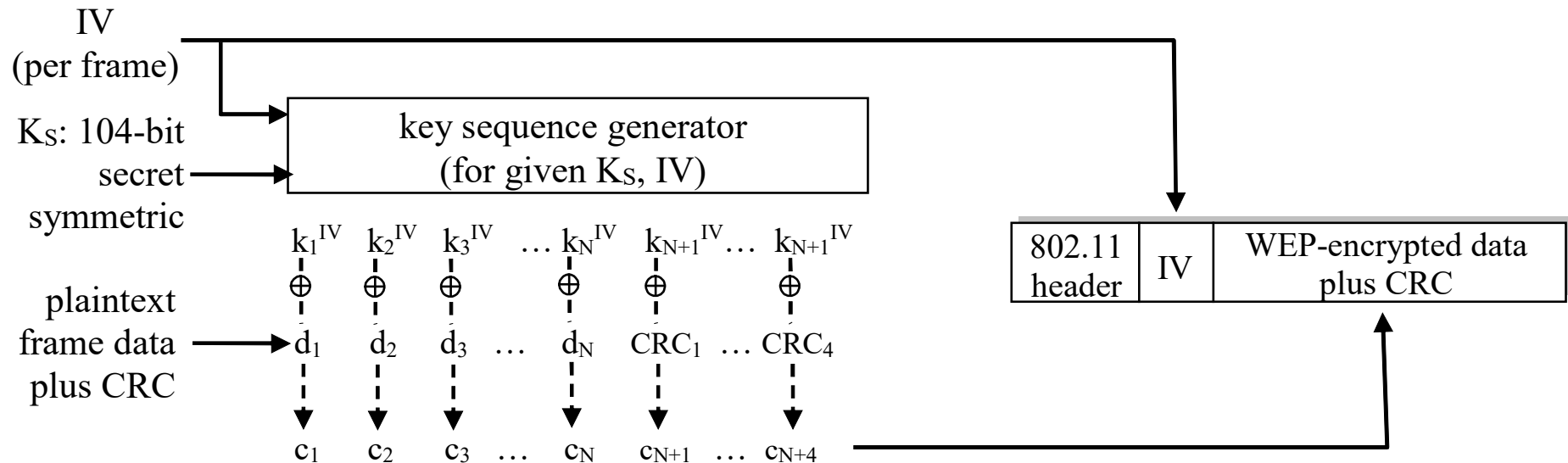
Drahtlose LANs: Sicherheit

■ Wired Equivalent Privacy (WEP)

- im initialen WLAN 802.11-1997-Standard: Ziel war ähnliche Sicherheit wie bei leitungsgebundener Kommunikation
- Schlüsselaustausch: nicht festgelegt
- Authentifikation zwischen Station und Zugangspunkt: symmetrisches Challenge-Response-Verfahren
- Verschlüsselung
 - symmetrischer 40-Bit oder 104-Bit Schlüssel K_S in Station und Zugangspunkt
 - für jedes Paket wird 24-Bit **Initialisierungsvektor IV** erzeugt und im Klartext im Rahmen gesendet
 - für Daten wird 4-Byte **Integrity Check Value (ICV)** mittels CRC berechnet
 - aus $K_S + IV$ wird mit RC4 pseudozufällige Bitsequenz erzeugt, Daten + ICV werden mit XOR bitweise verknüpft
 - wg. nur 2^{24} möglichen IVs sind Angriffe möglich, weitere Sicherheitsprobleme bestehen

Drahtlose LANs: Sicherheit

■ Versenden eines Frames mit WEP (Encapsulation):



Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

Drahtlose LANs: Sicherheit

■ Weiterentwicklung der Sicherheit

- Arbeitsgruppe [IEEE 802.11i](#), aufgenommen in 802.11-2007
- WiFi-Alliance: [WiFi Protected Access \(WPA\)](#)
 - 1. Version vor Fertigstellung von 802.11i
 - erfordert nur Aktualisierung der Firmware von Stationen, aber neue Zugangspunkte
 - gegenseitige Authentifikation über Pre-Shared Key (PSK) oder über Authentifikations-Server (z.B. RADIUS)
 - [Temporal Key Integrity Protocol \(TKIP\)](#): verbesserte Version der WEP Encapsulation
 - RC4 mit wirklich neuem 128-Bit Schlüssel pro Frame
 - statt CRC Frame-Authentifikation: [Message Integrity Code \(MIC\)](#)

Drahtlose LANs: Sicherheit

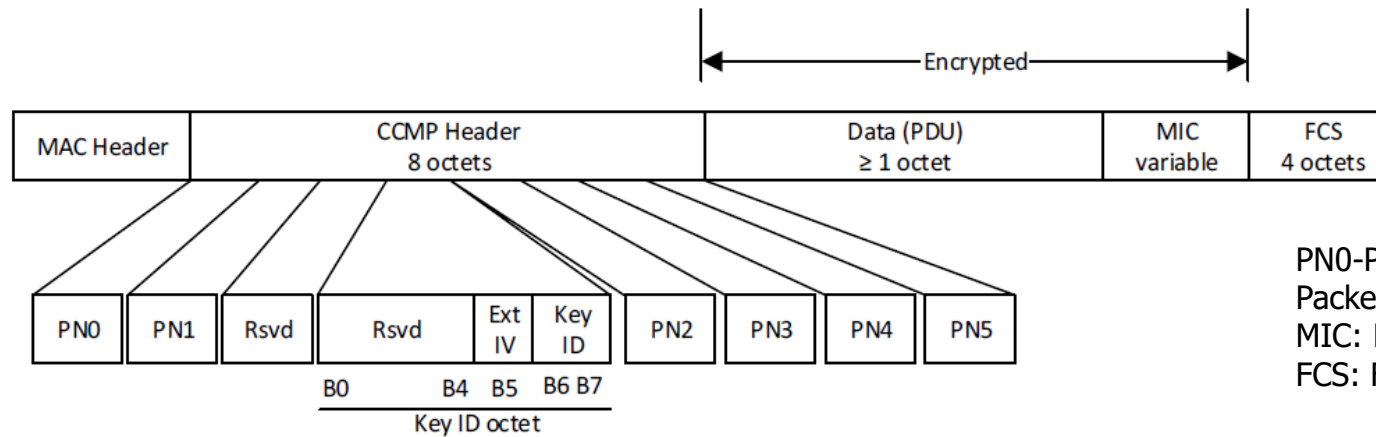
■ Weiterentwicklung der Sicherheit (Fortsetzung)

- WEP und TKIP weiter in 802.11-2016, aber „obsolet“
- WPA2
 - gegenseitige Authentifikation über Pre-Shared Key (PSK) oder über Authentifikations-Server (z.B. RADIUS, DIAMETER)
 - Encapsulation: Counter Mode with Cipher Block Chaining Message Authentication Protocol (CTR with CBC-MAC Protocol, CCMP)
 - Counter (Packet Number), wird bei jedem Frame inkrementiert, dient Erstellung einer Nonce pro Frame
 - Verwendung von AES
- 2017 wird Sicherheitslücke in WPA2 bekannt (Krack), Abhilfe durch WPA3 seit 2018

Drahtlose LANs: Sicherheit

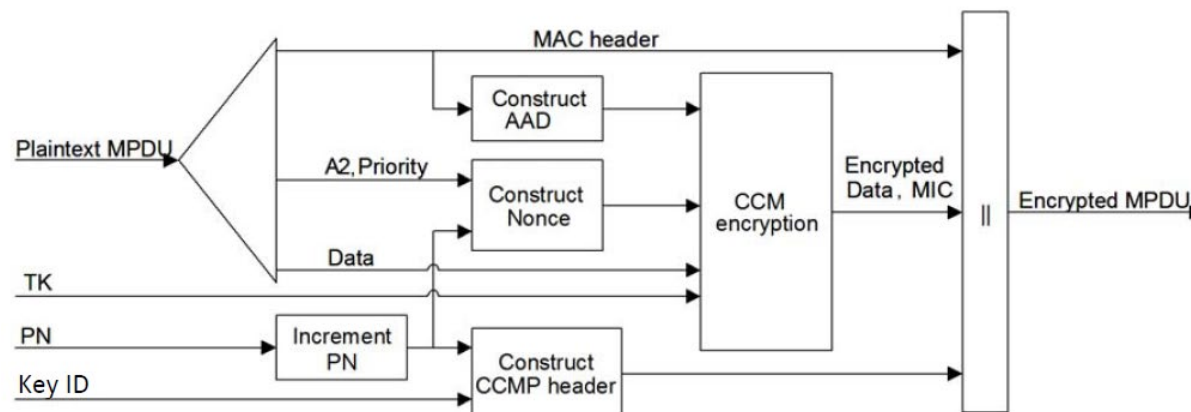
■ CCMP Paket Format:

Quelle: IEEE802.11-2016



PN0-PN5:
Packet Number, 48 Bit
MIC: Message Integrity Code
FCS: Frame Check Sequence

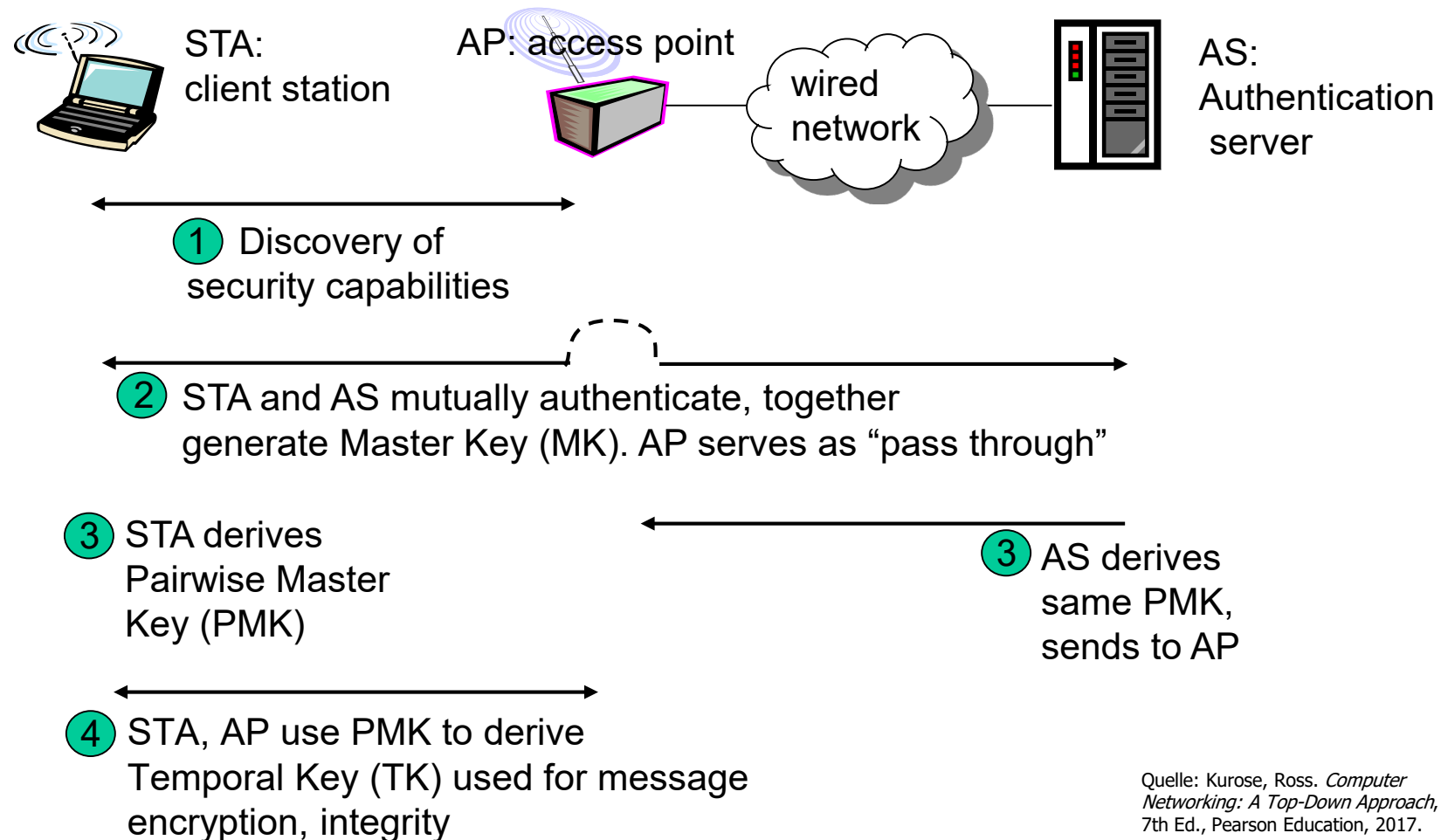
■ CCMP Encapsulation:



TK: Temporal Key
(neu für jede Session)
PN: Packet Number
Key ID:
A2: 2. Adresse im MAC-Header
Priority: ggfs. QoS-Priorität aus
MAC-Header
AAD: Additional Authentication Data

Drahtlose LANs: Sicherheit

■ Authentifizierung über Authentifikations-Server:



Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.