Sicherungsschicht

NETZWERKTECHNIK / SEMESTER 1 UND 2

1

AGENDA

01 ZWECK DER SICHERUNGSSCHICHT

02 TOPOLOGIEN

03 MEDIENZUGRIFF

04 RAHMENBILDUNG, ADRESSIERUNG UND FEHLERERKENNUNG

05 VERBINDUNG AUF SCHICHT 1 UND 2

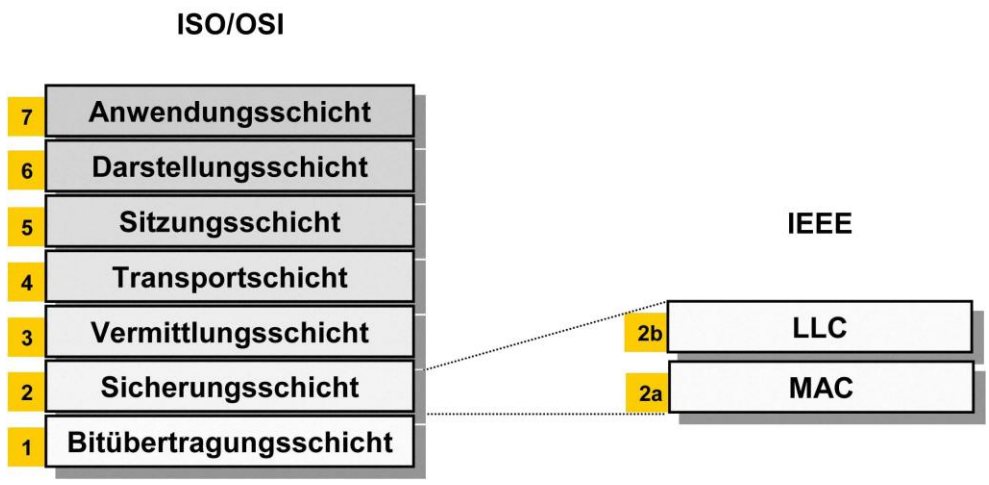
2

01

Zweck der Sicherungs-schicht

4

Einordnung im ISO/OSI Modell



[Quelle: https://www.airnet.de/cr1-gfe/de/html/TrFddiIEEE802_learningObject6.xml - letzter Abruf 21.07.2025]

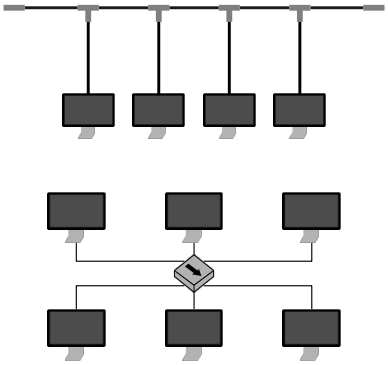
5

Direktverbindungsnetze

- d. h. **alle angeschlossenen Knoten sind direkt erreichbar und werden mittels einfacher Adressen der Schicht 2 identifiziert**
- es findet **keine Vermittlung** statt,
- eine **einfache Weiterleitung** (in Form von „Bridging“ oder „Switching“) ist aber möglich.

Beispiele:

- einzelne lokale Netzwerke (hier Verbindung mittels Bus / Hub, aber auch mittels Switch möglich)
- Verbindung zwischen Basisstation und Mobiltelefon
- Bus-Systeme innerhalb eines Computers, z. B. USB, PCIe etc.



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

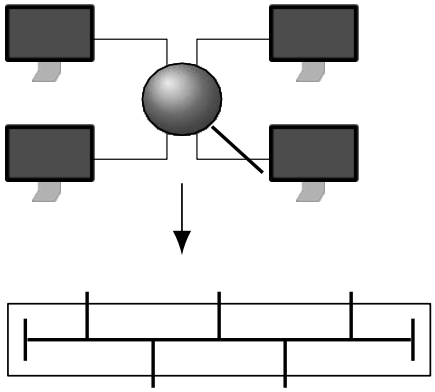
Wesentliche Aufgaben der Sicherungsschicht

- die Steuerung des **Medienzugriffs**,
- die Prüfung übertragener Nachrichten auf **Fehler** und
- die **Adressierung** innerhalb von Direktverbindungsnetzen.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Medienzugriff

- Hubs z. B. erzeugen nur auf den ersten Blick eine Sterntopologie
- Intern werden alle angeschlossenen Computer zu einem Bus verbunden
- **Gleichzeitiges Senden von zwei Stationen führt zu Kollisionen und daher zum Verlust von Nachrichten**

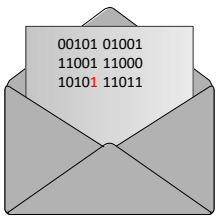


[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

8

Prüfung

- Trotz Kanalkodierung treten **Übertragungsfehler** auf
- Diese müssen erkannt werden
- **Defekte Nachrichten werden nicht an höhere Schichten weitergegeben**
- **Die Wiederholung einer Übertragung ist häufig Aufgabe höherer Schichten**

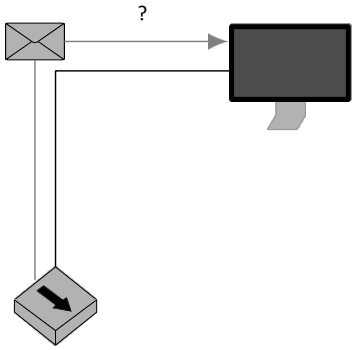


[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

9

Addressierung

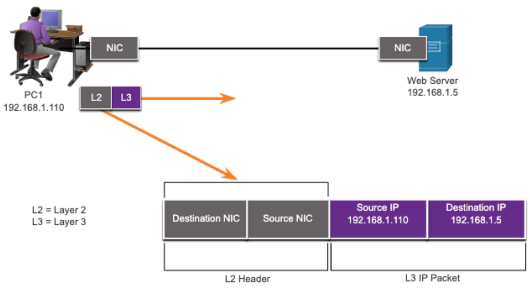
- Eine Nachricht kann von vielen Knoten empfangen werden, z. B. bei Bus-Verbindungen oder Funknetzwerken
- Der jeweilige Empfänger muss entscheiden können, ob eine Nachricht für ihn bestimmt ist

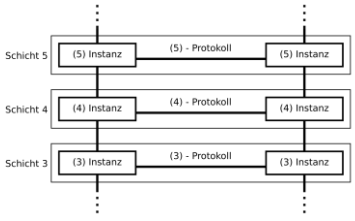


[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Die Sicherungsschicht

- Die Datenverbindungsschicht ist für die **Kommunikation zwischen den Netzwerkkarten der Endgeräte** verantwortlich.
- Es ermöglicht Protokollen der oberen Schicht den Zugriff auf die Medien der Bitübertragungsschicht und **kapselt Layer-3-Pakete (IPv4 und IPv6) in Layer-2-Frames**.
- Es führt auch eine **Fehlererkennung** durch und lehnt beschädigte Frames ab.



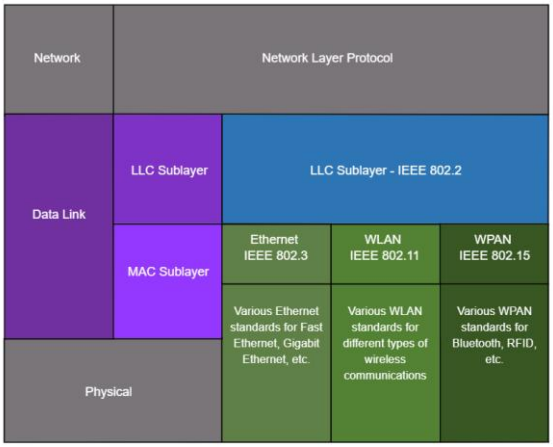


[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

NETZWERKTECHNIK / SEMESTER 1 und 2

IEEE 802 LAN/MAN Data Link Sublayers

- **IEEE 802 LAN/MAN-Standards** sind spezifisch für die Art des Netzwerks (Ethernet, WLAN, WPAN usw.).
- Der Data Link Layer **besteht aus zwei Sublayern**. Logical Link Control (**LLC**) und Media Access Control (**MAC**).
- Die **LLC-Unterschicht** kommuniziert zwischen der **Netzwerksoftware auf den oberen Schichten und der Gerätehardware** auf den unteren Schichten.
- Die **MAC-Unterschicht** ist für die Datenkapselung und die **Medienzugriffskontrolle** verantwortlich.



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

12

NETZWERKTECHNIK / SEMESTER 1 und 2

Medienzugriff

Pakete, die zwischen Knoten ausgetauscht werden, können zahlreiche Sicherungsschichten und Medienübergänge erfahren.

Bei jedem Hop entlang des Pfads führt ein Router vier grundlegende Layer-2-Funktionen aus:

1. Akzeptiert einen Frame vom Netzwerkmedium.
2. Entkapselt den Frame, um das gekapselte Paket verfügbar zu machen.
3. Kapselt das Paket erneut in einen neuen Frame.
4. Leitet den neuen Frame auf dem Medium des nächsten Netzwerksegments weiter.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

13

Standardisierung der Sicherungsschicht

Protokolle der Sicherungsschicht werden von technischen Organisationen definiert:

- Institut für Elektro- und Elektronikingenieure (IEEE) z.B. Ethernet
- Internationale Fernmeldeunion (ITU) z.B. ISDN
- Internationale Organisationen für Normung (ISO) z.B. HDLC
- Amerikanisches Nationales Normungsinstitut (ANSI) z.B. BacNet

02

Topologien

QUELLE:

INTRODUCTION TO NETWORKS V7.0 (ITN)

NETZWERKTECHNIK / SEMESTER 1 und 2

Physikalische und logische Topologien

- Die Topologie eines Netzwerks ist die Anordnung und Beziehung der Netzwerkgeräte und die Verbindungen zwischen ihnen.
- Es gibt zwei Arten von Topologien, die beim Beschreiben von Netzwerken verwendet werden:
  - **Physische Topologie** – zeigt physische Verbindungen und wie Geräte miteinander verbunden sind.
  - **Logische Topologie** – identifiziert die virtuellen Verbindungen zwischen Geräten mithilfe von Geräteschnittstellen und IP-Adressierungsschemata.

NETZWERKTECHNIK / SEMESTER 1 und 2

WAN Topologien

Es gibt drei gängige physische WAN-Topologien:

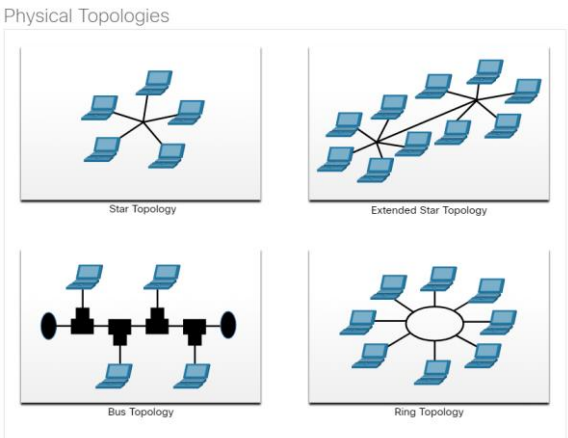
- **Punkt-zu-Punkt** – die einfachste und gebräuchlichste WAN-Topologie. Besteht aus einer permanenten Verknüpfung zwischen zwei Endpunkten.
- **Hub and Spoke** – ähnlich einer Sterntopologie, bei der ein zentraler Standort Zweigstellen über Punkt-zu-Punkt-Verbindungen miteinander verbindet.
- **Mesh** – bietet hohe Verfügbarkeit, erfordert jedoch, dass jedes Endsystem mit jedem anderen Endsystem verbunden ist.

Point-to-Point WAN Topologie

- Physische **Punkt-zu-Punkt**-Topologien verbinden zwei Knoten direkt.
- Die Knoten dürfen die **Medien nicht für andere Hosts freigeben**.
- Da alle Frames auf dem Medium nur zu oder von den beiden Knoten übertragen werden können, können **Punkt-zu-Punkt-WAN-Protokolle sehr einfach** sein.

LAN Topologien

- Endgeräte in LANs werden in der Regel über eine **Stern- oder Extended-Stern-Topologie** miteinander verbunden.
- Stern- und erweiterte Sterntopologien sind einfach zu installieren, sehr skalierbar und leicht zu beheben.
- Frühe Ethernet- und Legacy-Token-Ring-Technologien bieten zwei zusätzliche Topologien:
  - **Bus** – Alle Endsysteme, die miteinander verkettet und an jedem Ende abgeschlossen sind.
  - **Ring** – Jedes Endsystem ist mit seinen jeweiligen Nachbarn verbunden, um einen Ring zu bilden.



03

Medienzugriff

20

20

Übertragungsrichtung

21

21

Übertragungsrichtung

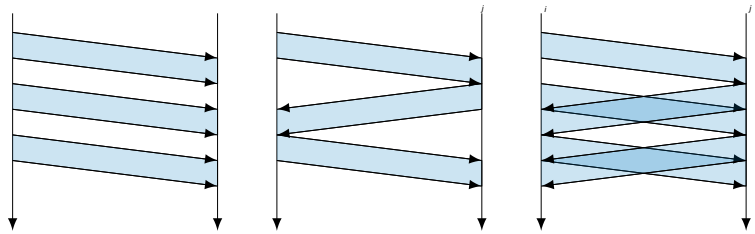
- **Halbduplex-Kommunikation**
  - Es kann jeweils nur ein Gerät auf einem freigegebenen Medium senden oder empfangen.
  - Wird in WLANs und Legacy-Bustopologien mit Ethernet-Hubs verwendet.
- **Vollduplex-Kommunikation**
  - Ermöglicht beiden Geräten das gleichzeitige Senden und Empfangen auf einem gemeinsam genutzten Medium.
  - Ethernet-Switches arbeiten im Vollduplex-Modus.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

Halb- und Voll-Duplex Kommunikation

Die Art der Verbindung hängt dabei ab von

- den Fähigkeiten des Übertragungskanals,
- dem Medienzugriffsverfahren und
- den Anforderungen der Kommunikationspartner.



(a) Simplex **(b) Halbduplex** **(c) Vollduplex**

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Multiplexing

24

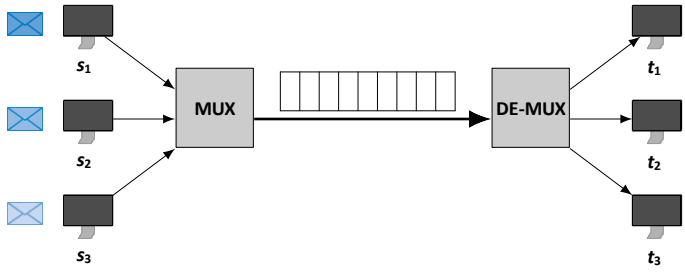
24

Mehrfachzugriff (Multiplexing)

Häufig ist es von Vorteil, **Nachrichten unterschiedlicher Teilnehmer gemeinsam über eine Leitung zu übertragen**:

- **Einfaches Beispiel:** Werden mehrere Computer mittels eines Hubs miteinander verbunden, so bildet der Hub ein gemeinsames geteiltes Medium, auf das die Computer mittels eines nicht-deterministischen Medienzugriffsverfahrens abwechselnd zugreifen.

Deterministisches Zeitmultiplex-Verfahren:



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

25

NETZWERKTECHNIK / SEMESTER 1 und 2

Übersicht über Multiplex-Verfahren

- **Zeitmultiplex (Time Division Multiplex, TDM)**
  - Deterministische Verfahren z. B. im Telefonnetz, bei ISDN-Verbindungen und im Mobilfunk
  - Nichtdeterministische Verfahren (konkurrierender Zugriff) in paketbasierten Netzwerken (z. B. Ethernet, WLAN)
- **Frequenzmultiplex (Frequency Division Multiplex, FDM)**
  - Aufteilung des Kanals in unterschiedliche Frequenzbänder (spektrale Zerlegung) und Zuweisung der Frequenzbänder an Kommunikationspartner.
  - Omnipräsent bei Funkübertragungen (z. B. unterschiedliche Radiosender)
  - Einsatz bei Glasfaserübertragungen („Modes“ mit unterschiedlicher Farbe)
  - Koexistenz von ISDN und DSL auf derselben Leitung

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

26

NETZWERKTECHNIK / SEMESTER 1 und 2

Übersicht über Multiplex-Verfahren

- **Raummultiplex (Space Division Multiplex, SDM)**
  - Verwendung mehrerer paralleler Übertragungskanäle.
  - „Kanalbündelung“ (Link Aggregation) bei Ethernet
  - MIMO (Multiple-In Multiple-Out) bei kabellosen Übertragungen (Verwendung mehrerer Antennen schafft mehrere Übertragungskanäle)
- **Codemultiplex (Code Division Multiplex, CDM)**
  - Verwendung orthogonaler Alphabete und Zuweisung der Alphabete an Kommunikationspartner.
  - Die Mobilfunktechnologie UMTS repräsentiert eine Variante von CDMA

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

27

NETZWERKTECHNIK / SEMESTER 1 und 2

TDM (Time Division Multiplexing)

- Die zur Verfügung stehende Ressource „Zeit“ wird auf mehrere Aufgaben aufgeteilt
- Die Zeit in der ein einzelner Kanal durchgeschaltet wird die **Kanaldauer t_c** oder auch Zeitschlitz (slot time) genannt.
- Bei n Kanälen ist die **Rahmenzeit $t_f = n * t_c$**
- Stationen die keine Daten zum übertragen haben belegen trotzdem einen Zeitschlitz

=> **Verbesserung durch asynchrones Zeitmultiplex**

- Kanäle nicht nach festem Zeitraster sondern nach Bedarf durchgeschaltet
- Zeitschlitze werden mit einer Kanalkennung versehen => Header

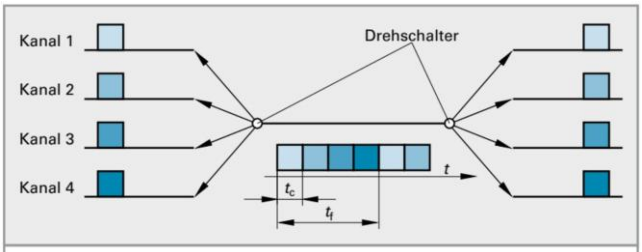


Bild 1.27: Zeitmultiplex mit festem Zeitraster

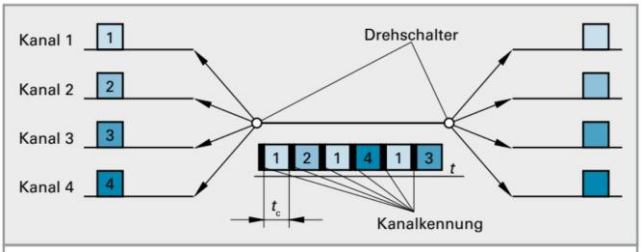


Bild 1.28: Asynchrones Zeitmultiplex

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

28

NETZWERKTECHNIK / SEMESTER 1 und 2

FDM (Frequency Division Multiplexing)

- Verfügung stehende Bandbreite des Mediums oder Übertragungskanals wird in mehrere Teilbereiche aufgeteilt
- **Beispiel**: Radio mit verschiedenen Sendefrequenzen der Stationen innerhalb eines Frequenzbandes
- Jedem Kanal zugewiesene Bandbreite wird als **Kanalbandbreite f_{ch}** bezeichnet
- Die Kanäle haben einen „Sicherheitsabstand“ den **Kanalabstand f_s** zueinander.

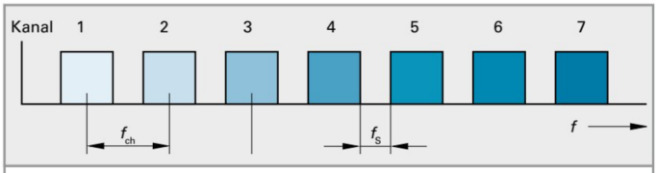


Bild 1.29: Frequenzmultiplex

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

29

SDM (Space Division Multiplexing)

- Verfügung stehender Raum in verschiedene Bereiche für die verschiedenen Kanäle aufgeteilt
- **Beispiel:** Mobilfunk Basisstation mit mehreren Funkzellen
- Funkzellen benachbarter Basisstationen können bzw. sollen sich überlappen damit keine Funklöcher auftreten

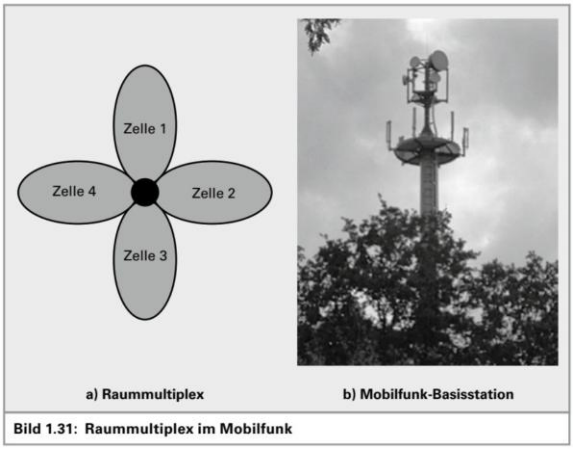


Bild 1.31: Raummultiplex im Mobilfunk

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

CDM (Code Division Multiplexing)

- Bei **Funkübertragungen** um mehrere Funkkanäle gleichzeitig auf derselben Frequenz zu übertragen (UMTS, LTE, CDMA, …)
- Die zu sendenden Datenbits werden vor dem Senden mit **Code Sequenzen** verknüpft
- Beim Empfangen wieder mittels gleicher Code-Sequenzen zurückgewonnen
- Der **Chipcode** wird bitweise mit den Datenbits multipliziert
- $z_{i,m} = d_i \cdot c_m$

Beispiel Chipcode: +1 -1 +1 +1 -1 +1 +1 +1

- HIGH Datenbit = +1 -1 +1 +1 -1 +1 +1 +1
- LOW Datenbit = -1 +1 -1 -1 +1 -1 -1 -1 (also invertiert)

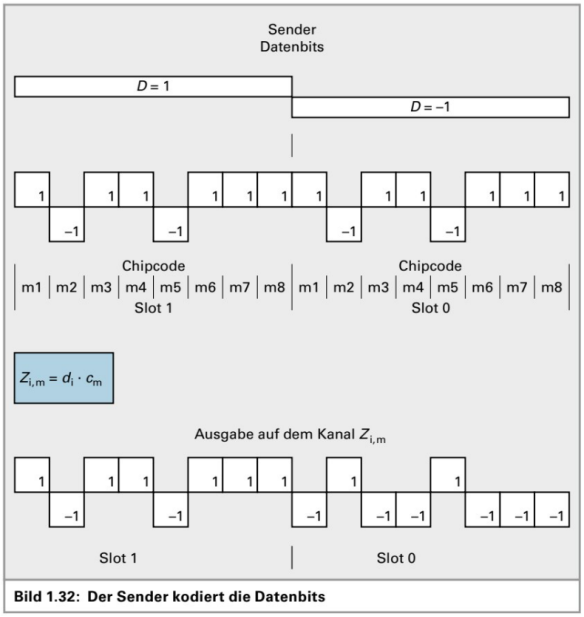


Bild 1.32: Der Sender kodiert die Datenbits

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

CDM (Code Division Multiplexing)

Jedem Kanal wird ein anderer Chipcode zugewiesen. Senden mehrere Kanäle gleichzeitig so überlagern sich die Signale.

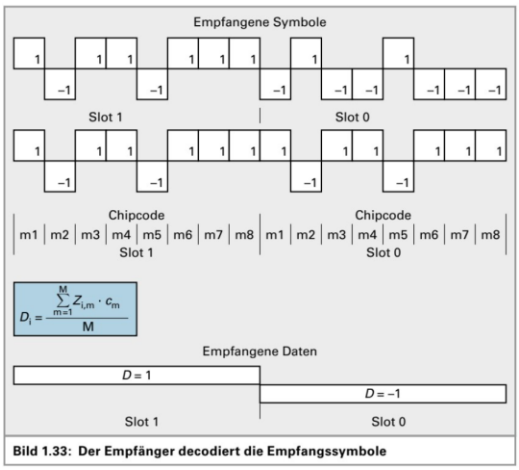


Bild 1.33: Der Empfänger decodiert die Empfangssymbole

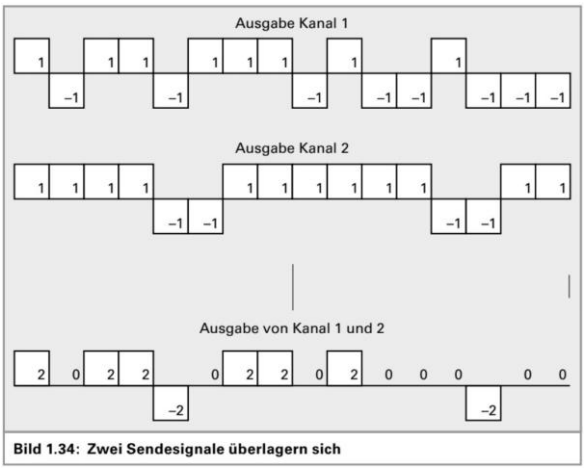


Bild 1.34: Zwei Sendesignale überlagern sich

[Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

32

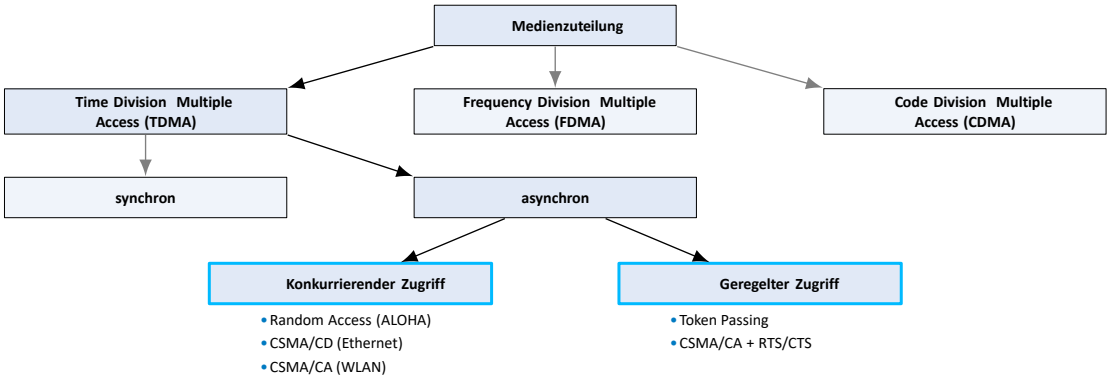
Mehrfachzugriff

34

NETZWERKTECHNIK / SEMESTER 1 und 2

Mehrfachzugriff und Medienzugriffskontrolle

Einige der (statistischen) Multiplexing-Verfahren eignen sich auch als Mehrfachzugriffsverfahren:



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

NETZWERKTECHNIK / SEMESTER 1 und 2

Medienzugriff

- **Konkurrierender Zugriff (Contention-based access)**
  - Alle Knoten, die im Halbduplex-Modus arbeiten und um die Nutzung des Mediums konkurrieren.
    - **Carrier Sense Multiple Access mit Collision Detection (CSMA/CD)**, wie bei Ethernet verwendet
    - **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**, wie in Wireless LANs verwendet
- **Geregelter Zugriff (Controlled Access)**
  - Deterministischer Zugriff, bei dem **jeder Knoten seine eigene Zeit auf dem Medium hat**.
  - Wird in älteren Netzwerken wie **Token Ring und ARCNET** verwendet.

NETZWERKTECHNIK / SEMESTER 1 und 2

Contention-Based Access – CSMA/CD

- Wird von älteren **Ethernet-LANs** verwendet.
- Arbeitet im **Halbduplex-Modus**, bei dem jeweils nur ein Gerät sendet oder empfängt.
- Verwendet einen **Kollisionserkennungsprozess, um zu steuern, wann ein Gerät senden kann,** und was passiert, wenn mehrere Geräte gleichzeitig senden.

Prozess der CSMA/CD-Kollisionserkennung:

1. Geräte, die gleichzeitig senden, führen zu einer Signalkollision auf den gemeinsam genutzten Medien.
2. Geräte erkennen die Kollision.
3. Geräte warten eine zufällige Zeit und übertragen Daten erneut.

NETZWERKTECHNIK / SEMESTER 1 und 2

Contention-Based Access – CSMA/CA

- Wird von **IEEE 802.11 WLANs** verwendet.
- Arbeitet im **Halbduplex-Modus**, bei dem jeweils nur ein Gerät sendet oder empfängt.
- Verwendet einen **Kollisionsvermeidungsprozess, um zu steuern, wann ein Gerät senden kann,** und was passiert, wenn mehrere Geräte gleichzeitig senden.

CSMA/CA-Kollisionsvermeidungsprozess:

1. Bei der Übertragung **beziehen Geräte auch die Zeitdauer mit ein**, die für die Übertragung benötigt wird.
2. Andere Geräte auf dem freigegebenen Medium erhalten die Informationen zur Zeitdauer und **wissen, wie lange das Medium nicht verfügbar sein wird.**

Medienzugriff

Bewertungskriterien für Medienzugriffsverfahren sind unter anderem:

- **Durchsatz**, d. h. Gesamtanzahl an Nachrichten pro Zeiteinheit, die übertragen werden können
- **Verzögerung** für einzelne Nachrichten
- **Fairness** zwischen Teilnehmern, die sich dasselbe Medium teilen
- **Implementierungsaufwand** für Sender und Empfänger

Problem bei synchronem TDMA

- Der Kanal **wird statisch zwischen Teilnehmern aufgeteilt**
- **Datenverkehr ist aber stossartig** bzw. **burst-artig**, d. h. ein Teilnehmer überträgt kurz mit hoher Bandbreite und danach längere Zeit nicht mehr
- Bandbreite steht während Ruhepausen anderen Teilnehmern nicht zur Verfügung

Lösungsansatz: Asynchrones (flexibles) TDMA

- **Keine statische Aufteilung** / Zuweisung von Zeitslots
- **Stattdessen: Zufälliger, konkurrierender** oder dynamisch geregelter Medienzugriff

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

39

ALOHA und Slotted ALOHA

Random Access (ALOHA)

- Entwickelt an der Universität von Hawaii (1971), cf. Prof. Abramson
- Ursprünglich für kabellose Datenübertragungen
- Ziel: Verbindung von Oahu mit den anderen hawaiianischen Inseln

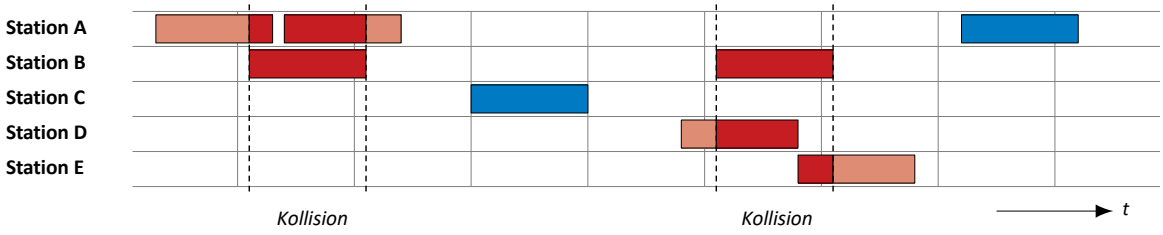
Funktionsweise

- Jede Station sendet an eine zentrale Station (vgl. „Basisstation“ in WLANs), sobald Daten vorliegen
- Senden zwei Stationen gleichzeitig, kommt es zu Kollisionen
- Erfolgreich übertragene Nachrichten werden vom Empfänger auf anderer Frequenz quittiert („out-of-band“ Bestätigungsverfahren auf Link-Layer, keine Kollisionen zwischen Nachrichten und Bestätigungen)

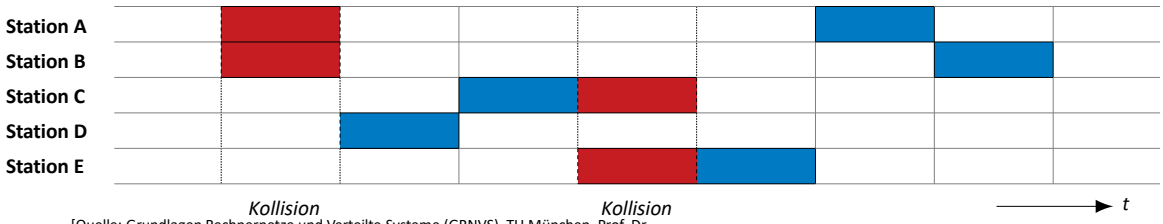
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

40

ALOHA



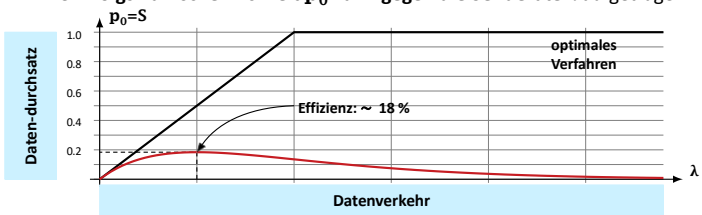
Bei Slotted ALOHA dürfen Stationen nicht mehr zu beliebigen Zeitpunkten mit einer Übertragung beginnen, sondern nur noch zu den Zeitpunkten $t = nT$, $n = 0,1, \ldots$



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Erreichbarer Durchsatz mit Aloha

- Die **Erfolgswahrscheinlichkeit p_0 kann gegen die Senderate λ** aufgetragen werden:



Dieses Ergebnis ist nicht sehr ermutigend. Wenn aber jeder Daten dann überträgt, wann er will, ist kaum eine Erfolgsrate von 100% zu erwarten.

- Innerhalb eines **beliebigen Intervalls $[t, t + T]$ kann höchstens eine Übertragung** erfolgreich sein kann.
- Dementsprechend entspricht die Anzahl S der erfolgreichen Nachrichten pro Intervall gleichzeitig der Wahrscheinlichkeit für eine erfolgreiche Übertragung.
- Bei einem **optimalen Verfahren** würde die Anzahl. erfolgreicher Nachrichten **S linear mit der Senderate ansteigen, bis die maximale Anzahl von Nachrichten pro Zeitintervall erreicht ist** (1 Nachricht pro Intervall).
- Steigt die Senderate weiter, würde dies ein optimales Verfahren nicht beeinträchtigen.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

CSMA, CSMA/CD, CSMA/CA

Carrier Sense Multiple Access (CSMA)

- Eine einfache Verbesserung von Slotted ALOHA: „Listen Before Talk“
- Höre das Medium ab
- Beginne erst dann zu senden, wenn das Medium frei ist

Verschiedene Varianten:

1-persistentes CSMA

Wenn Medium frei, beginne Übertragung

Wenn Medium belegt, warte bis frei und beginne dann Übertragung

p-persistentes CSMA

Wenn Medium frei, übertrage mit Wahrscheinlichkeit p oder verzögere mit Wahrscheinlichkeit $1 - p$ um eine feste Zeit dann 1.

Wenn Medium belegt, warte bis frei, dann 1.

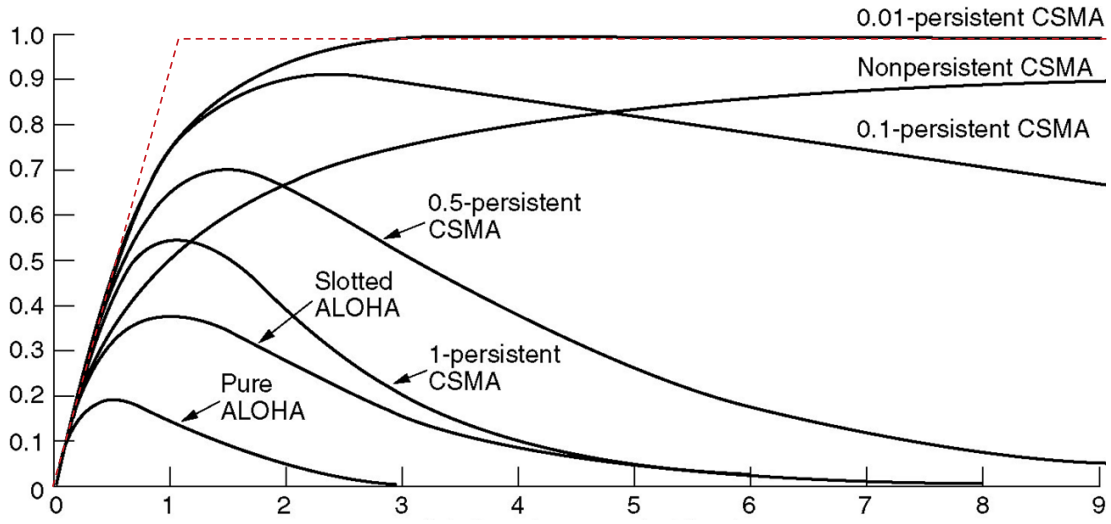
nicht-persistentes CSMA

Wenn Medium frei, beginne Übertragung

Wenn belegt, warte eine zufällig gewählte Zeitspanne dann 1.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Verfahren im Vergleich

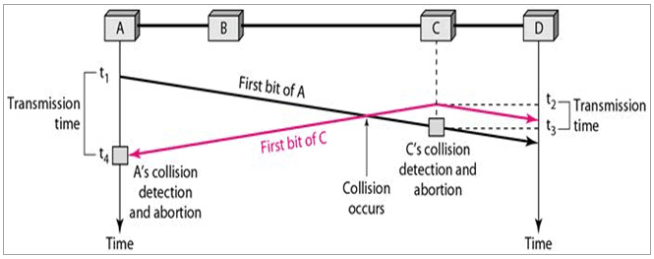


tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

CSMA mit Kollisionserkennung (CD = Collision Detection)

- **Erkenne Kollisionen und wiederhole die Übertragung**, wenn eine Kollision erkannt wird
- Verzichte auf das Senden von Bestätigungen
- Wird keine Kollision erkannt, gilt die Übertragung als erfolgreich

Problem: Der Sender muss die Kollision erkennen, während er noch überträgt



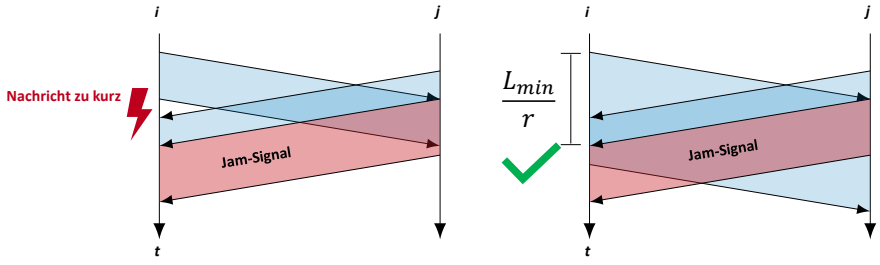
[Quelle: https://www.softwaretestinghelp.com/what-is-csma-cd/ - letzter Abruf 21.07.2025]

Voraussetzung für CSMA/CD

Angenommen zwei Stationen i und j kommunizieren über eine Distanz d mittels CSMA/CD. **Damit Kollisionen erkannt werden können, müssen Nachrichten folgende Mindestlänge L_{min} [bit] aufweisen**:

$$T_t >= 2 \cdot T_p$$
$$T_t = L_{min}[bit] \cdot \frac{1}{r}$$
$$L_{min}[bit] >= 2 \cdot T_p \cdot r$$
$$L_{min}[bit] = 2 \cdot \frac{d}{v \cdot c_0} \cdot r$$

r = Übertragungsrate [bit/s]
v = Ausbreitungsgeschwindigkeit



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Back-Off-Zeit (Binary Exponential Backoff)

Wird 1-persistentes CSMA mit Kollisionserkennung verwendet, ergibt sich folgendes Problem:

- Die **Kollision zerstört die Nachrichten** beider in die Kollision verwickelten Stationen.
- Mind. eine der Stationen sendet ein **JAM-Signal**.
- Nachdem das Medium frei wird, **wiederholen beide Stationen die Übertragung**
  - ➢ **Es kommt sofort wieder zu einer Kollision.**

Lösung: Warte „zufällige" Zeit nach einer Kollision

Durch die Wartezeiten, die

- zufällig gewählt und
- situationsabhängig größer werden,
- wird die Kollisionswahrscheinlichkeit bei Wiederholungen reduziert.

Binary Exponential Backoff
Beim k-ten Sendeversuch einer Nachricht

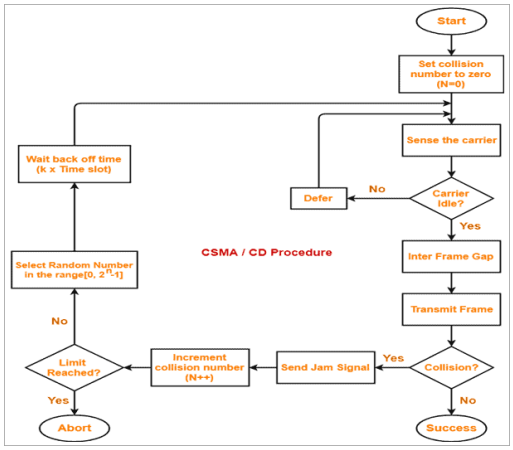
- wählt der Sender zufällig $n \epsilon \{0, \dots, min\{2^{k-1} - 1{,}1023\}\}$aus und
- wartet *n* Slotzeiten vor einem erneuten Sendeversuch.

Die maximale Wartezeit ergibt sich bei $k = 11$ (also bei 10 Wiederholungen) und beträgt 1023 Slotzeiten.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

CSMA mit Kollisionserkennung (CD = Collision Detection)

1. Zuerst **erkennt** die Station, die die Daten übertragen möchte, den Träger, ob dieser belegt oder inaktiv ist. Wenn ein Träger inaktiv ist, wird die Übertragung durchgeführt.
2. Die Übertragungsstation erkennt eine Kollision, falls vorhanden, unter der folgenden **Bedingung:** $\mathbf{T_t >= 2 * T_p}$, wobei T_t die Übertragungsverzögerung und T_p die Laufzeitverzögerung ist.
3. Die Station gibt das **Stausignal** frei, sobald sie eine Kollision erkennt.
4. Nachdem es zu einer Kollision gekommen ist, stoppt die Sendestation die Übertragung und wartet eine zufällige Zeitspanne, die als "**Back-Off-Zeit**" bezeichnet wird. Nach dieser Zeit sendet der Sender erneut.



tgm [Quelle: https://www.softwaretestinghelp.com/what-is-csma-cd/ - letzter Abruf 21.07.2025]

CSMA/CA (Collision Avoidance)

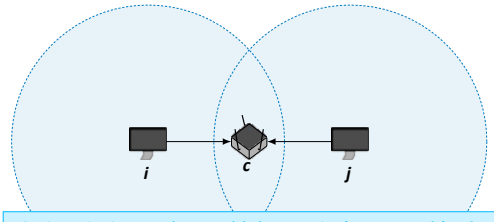
In **Funknetzwerken funktioniert CSMA/CD nicht**, da der Sender einer Nachricht eine Kollision auch bei ausreichender Nachrichtenlänge nicht immer detektieren kann.

„Hidden Station“:

Knoten i und j senden gleichzeitig

Knoten c erkennt die Kollision

Weder i noch j bemerken die Kollision



Stationen in einem Funknetzwerk haben nur eine **begrenzte Reichweite**. So kann es passieren, dass sich Teilnehmer in einem Netzwerk gegenseitig nicht wahrnehmen.

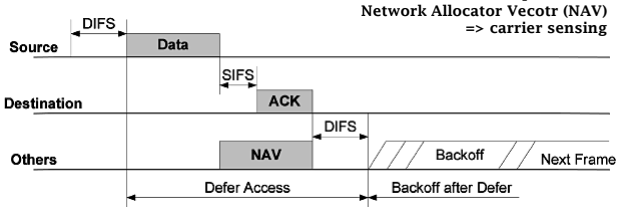
CSMA/CA basiert auf p-persistentem CSMA, d. h.

1. Wenn Medium frei, übertrage mit Wahrscheinlichkeit p oder verzögere mit Wahrscheinlichkeit $1 - p$ um eine feste Zeit dann 1.
2. Wenn Medium belegt, warte bis frei, dann 1.

Fallbeispiel: IEEE 802.11 DCF (Distributed Coordination Function)

- Festes Zeitintervall zwischen Rahmen: **DIFS (DCF Interframe Spacing).**
- **Wenn Medium mind. für DIFS unbelegt** ist, dann wähle unabhängig und gleichverteilt eine **Anzahl von Backoff-Slots** aus dem Intervall $\{0,1,2,\dots,min\{2^{c+k-1}-1,255\}\}$
- c ist abhängig vom PHY (z. B. $c = 4$), k ist die Anzahl der Sendeversuche (siehe Binary Exponential Backoff).
- Medienzugriff hat durch festes $c > 0$ **stets ein Contention Window**.
- Ein Rahmen gilt in IEEE 802.11 als **erfolgreich übertragen, wenn**
- im Fall von Unicasts der **Empfänger eine Bestätigung schickt** (Link-Layer Acknowledgements) oder
- im Fall von Broadcasts die **Übertragung eines Frames störungsfrei** abgeschlossen wird.

Short Interframe Space (SIFS)
DCF Interframe Space (DIFS)
Network Allocator Vecotr (NAV)
=> carrier sensing



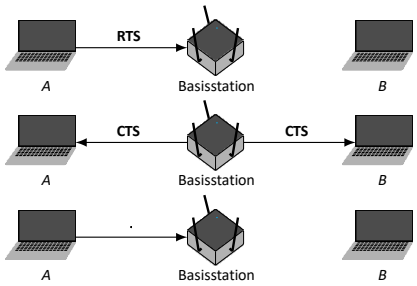
- Da i. d. R. nicht gleichzeitig gesendet und das Medium geprüft werden kann (anders bei Ethernet), ist die zweite Bedingung praktisch bereits erfüllt, wenn ein Knoten zu senden beginnt.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Erweiterung: RTS/CTS (Request to Send / Clear to Send)

- Übertragungen werden i. d. R. von einer Basisstation gesteuert
- Bevor ein Knoten eine Nachricht überträgt, wird ein RTS (Ready to Send) an die Basisstation geschickt
- Nur wenn die Basisstation mit einem CTS (Clear to Send) antwortet, darf die Übertragung beginnen

1. A sendet RTS, welches von B aufgrund der Distanz nicht
2. Basistation antwortet mit CTS, welches von A und B
3. A darf senden, B muss eine im CTS definierte Zeitspanne abwarten, bevor überhaupt ein RTS gesendet werden darf.



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Erweiterung: RTS/CTS (Request to Send / Clear to Send)

Vorteile:

- Kollisionen mit **Hidden Stations** werden vermieden, aber nicht gänzlich verhindert.
- Insgesamt **weniger Kollisionen**, auch ohne Hidden Stations.

Nachteile:

- Es können **noch immer Kollisionen** auftreten, z. B. wenn B das CTS nicht empfängt.
- RTS/CTS nimmt **vorab Zeit in Anspruch**, was die maximal erzielbare Datenrate reduziert.

Anmerkungen:

- RTS/CTS ist Bestandteil des sog. **Virtual Carrier Sensing**, da mit CTS das Medium für eine bestimmte Zeitspanne für eine Übertragung reserviert wird.
- Um die Verlustwahrscheinlichkeit von RTS/CTS-Nachrichten zu minimieren, werden diese mit der **robustesten Kodierung übertragen**, was i. d. R. der niedrigsten unterstützten Datenrate entspricht. Im Gegenzug sind RTS/CTS-Nachrichten sehr klein.
- Es ist streng genommen für RTS/CTS nicht notwendig, dass ein Netzwerk durch eine Basisstation kontrolliert wird. Es funktioniert auch im ad-hoc Modus oder (mit Einschränkungen) in Mesh-Netzwerken.
- Alle Geräte, unabhängig davon ob sie zum selben Service Set gehören oder nicht, sollten CTS-Nachrichten verarbeiten.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

04

Rahmenbildung, Adressierung und Fehlererkennung

Der Frame

- **Aus Sicht der physikalischen Schicht ist eine Nachricht lediglich eine Folge von Bits**.
- Für eine Betrachtung der Sicherungsschicht reicht diese Vorstellung aber nicht mehr aus.

Daher

- Wie werden einzelne Nachrichten auseinandergehalten?
- Welche zusätzlichen Informationen benötigen Protokolle der Sicherungsschicht?
- Wie werden Übertragungsfehler, die trotz Kanalkodierung auftreten, erkannt?

- **Im Kontext der Sicherungsschicht bezeichnen wir Nachrichten fortan als Rahmen (engl. Frame).**

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Der Frame

- Die Daten werden von der Sicherungsschicht mit einem Header und einem Trailer gekapselt, um einen Rahmen zu bilden.
  - Header
  - Daten
  - Trailer
- Die Felder des Headers und des Trailers variieren je nach Protokoll der Sicherungsschicht.
- Die Menge der im Frame übertragenen Steuerungsinformationen variiert je nach Zugriffssteuerungsinformationen und logischer Topologie.

LAN und WAN Frames

- **Die logische Topologie und das physische Medium bestimmen das verwendete Data Link Protocol:**
  - Ethernet
  - 802.11 Drahtlos
  - Punkt-zu-Punkt-Verfahren (PPP)
  - High-Level-Datenverbindungssteuerung (HDLC)
  - Frame Relay
- **Jedes Protokoll führt die Medienzugriffssteuerung für bestimmte logische Topologien aus.**

NETZWERKTECHNIK / SEMESTER 1 und 2

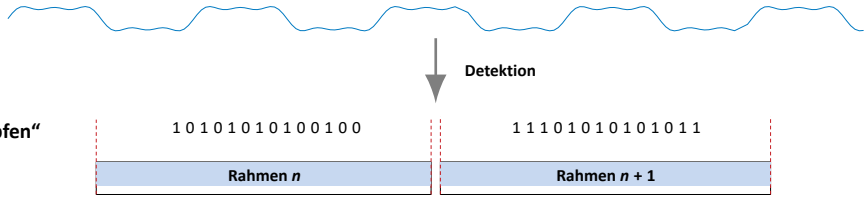
Erkennen von Rahmengrenzen

Wie kann der Empfänger Rahmen erkennen, insbesondere wenn

- Rahmen unterschiedliche Größen haben und
- nicht ständig Nutzdaten auf der Leitung liegen (Idle-Perioden)?

Es gibt viele Möglichkeiten:

- **Längenangabe der Nutzdaten**
- **Steuerzeichen (Start / Ende)**
- **Begrenzungsfelder und „Bit-Stopfen“**
- **Coderegelverletzung**



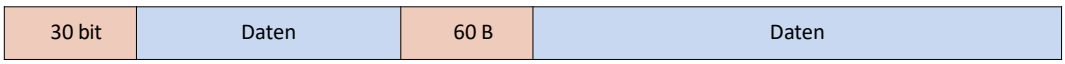
Ziel aller Verfahren zur Rahmenbegrenzung ist die Erhaltung der Codetransparenz, d. h. die Übertragung beliebiger Zeichenfolgen zu ermöglichen.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

NETZWERKTECHNIK / SEMESTER 1 und 2

Längenangabe der Nutzdaten

- Am Anfang des Rahmens steht die **Länge der nachfolgenden Nutzdaten** (oder die Gesamtlänge des Rahmens).
- Voraussetzung: Das Längenfeld und damit der Beginn einer Nachricht muss eindeutig zu erkennen sein



Wie kann der Beginn eines Rahmens erkannt werden?

- Durch Steuerzeichen (Start / Ende)
- Durch Voranstellen von Begrenzungsfeldern
- Durch Verlust des Trägersignals zwischen den Rahmen (Coderegelverletzung, siehe Kapitel 1)

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

NETZWERKTECHNIK / SEMESTER 1 und 2

Steuerzeichen

- **Beispiel: 4B5B-Code**, den man in Kombination mit Leitungscodes wie MLT-3 auf der phys. Schicht einsetzt.
- **Je 4 bit Eingabe werden auf 5 bit Ausgabe abgebildet**
- Einem Rahmen werden die **Startsymbole J/K** vorangestellt
- Nach einem Rahmen werden die **Endsymbole T/R** eingefügt

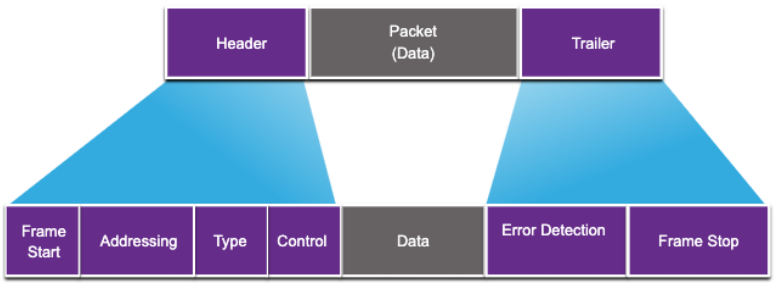
Eingabe	Ausgabe	Bedeutung	Eingabe	Ausgabe	Bedeutung
0000	11110	Hex data 0	-	00000	Quiet (Signalverlust)
0001	01001	Hex data 1	-	11111	Idle (Pause)
0010	10100	Hex data 2	-	11000	Start #1 (J)
0011	10101	Hex data 3	-	10001	Start #2 (K)
0100	01010	Hex data 4	-	01101	End (T)
0101	01011	Hex data 5	-	00111	Reset (R)
-	-	-	-	-	
-	-	-	-	-	
-	-	-	-	11001	Set
1111	11101	Hex data F	-	00100	Halt

Beispiel	Eingabe			1011	0101	0110		
	Ausgabe	11000	10001	10111	01011	01110	01101	00111
		Start #1	Start #2	Data	Data	Data	End	Reset

63

NETZWERKTECHNIK / SEMESTER 1 und 2

Felder eines Frame



Feld	Beschreibung
Frame Start and Stop	Identifiziert Anfang und Ende des Frames
Addressing	Gibt Quell- und Zielknoten an
Type	Identifiziert das gekapselte Layer-3-Protokoll
Control	Identifiziert Flusssteuerungsdienste
Data	Enthält die Frame-Nutzlast
Error Detection	Wird verwendet, um Übertragungsfehler zu ermitteln

[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

64

Begrenzungsfelder und Bit-Stopfen

- **Markiere Start und Ende einer Nachricht mit einer bestimmten Bitfolge**
- Stelle sicher, dass die Markierung nicht zufällig in den Nutzdaten vorkommt („Bit-Stopfen“, engl. Bit Stuffing)

Beispiel:

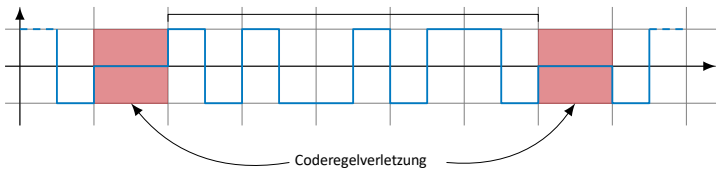
- Start- / Endemarkierung sei 01111110
- Um das Auftreten der Markierung in Nutzdaten zu verhindern, füge in Nutzdaten nach fünf aufeinanderfolgenden 1-en eine 0 ein
- Eingabe: 1100101111110111111
- Ausgabe: 01111110 11001011111**0**10111110**1** 01111110
- Empfänger entfernt nach fünf aufeinanderfolgenden 1-en die darauf folgende 0
- Praktischer Einsatz z. B. bei HDLC (High Level Data Link Control), einem Protokoll auf Schicht 2 für serielle Verbindungen.

Codeverletzung

- Viele Leitungscodes (z. B. Return-to-Zero und Manchester) besitzen unabhängig von den zu übertragenden Daten bestimmte Signalwechsel.

Idee:

- Lasse bestimmte Signalwechsel aus.
- Auf diese Art wird ein **ungültiges (im Code nicht existierendes) Symbol** erzeugt.
- Dieses kann verwendet werden, um Start und Ende von Rahmen zu markieren.
- **Beispiel:**
  Manchester-Code
  Rahmen: 11001



Fallbeispiele

IEEE 802.3a/i (Ethernet): 10 Mbit/s

- Als Leitungscode wird der **Manchester-Code** verwendet.
- Das Ende eines Frames wird durch **Coderegelverletzung** angezeigt.

IEEE 802.3u (FastEthernet): 100 Mbit/s

- Als Leitungscode wird **MLT-3** in Kombination mit dem **4B5B**-Code verwendet.
- Start und Ende von Rahmen werden durch **Steuerzeichen des 4B5B-Codes** markiert.

IEEE 802.3z (Gigabit Ethernet over Fiber): 1000 Mbit/s

- Als Leitungscode wird **NRZ** in Kombination mit dem **8B10B-Code** verwendet.
- Start und Ende von Rahmen werden durch **Steuerzeichen des 8B10B-Codes** markiert.
- IEEE 802.3ab (Gigabit Ethernet over Copper) verwendet andere Leitungscodes, da die Dämpfung andernfalls zu groß wäre.

Zusätzlich wird bei all diesen Beispielen jedem Rahmen noch eine Präambel vorangestellt. Diese dient allerdings nur der Taktsynchronisierung zwischen Sender und Empfänger.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Adressierung und Fehlererkennung

Bisher

- wie wird ein binärer Datenstrom übertragen und
- wie der Empfänger Rahmengrenzen wiedererkennt.

Wir wissen aber noch nicht,

- wie Nutzdaten, die von Schicht 3 und höher kommen, von der Sicherungsschicht behandelt werden,
- wie der Empfänger eines Rahmens adressiert wird und
- wie aus den Nutzdaten und protokollspezifischen Informationen ein Rahmen entsteht.

Anmerkung: Alle folgenden Konzepte werden anhand der IEEE 802-Standards erklärt. Die wesentlichen Punkte sind mit kleinen Modifikationen auf andere Verfahren übertragbar.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Adressierung in Direktverbindungsnetzen:

Adressierung in Direktverbindungsnetzen:

- sind angeschlossene **Knoten direkt erreichbar**,
- es findet also **keine Vermittlung (engl. Routing)** zwischen Knoten statt.

Anforderungen an Adressen auf Schicht 2:

- **Eindeutige Identifizierung der Knoten** innerhalb des Direktverbindungsnetzes.
- Zumeist existiert eine **Broadcast-Adresse**, welche alle Knoten im Direktverbindungsnetz anspricht.
- Zusätzlich kann es **Multicast-Adressen** geben, die bestimmte Gruppen von Knoten ansprechen.
- Adressen auf Schicht 2 bezeichnet man allgemein als **MAC-Adressen**, wobei MAC für Media Access Control steht.
- Beispiel:

RA	TA	(Control)	L3-PDU (Data)

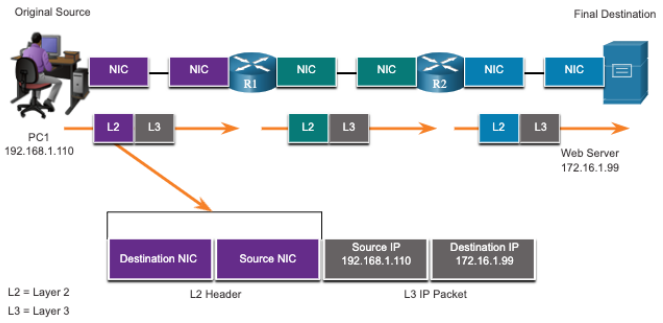
(RA = Receiver Address, TA = Transmitter Address)

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

70

Layer 2 Adressen

- Wird auch als **physische Adresse** bezeichnet.
- Enthalten im **Header** des Frame.
- Wird nur für die **lokale Übermittlung** eines Frames auf dem Link verwendet.
- **Wird von jedem Gerät aktualisiert, das den Frame weiterleitet.**



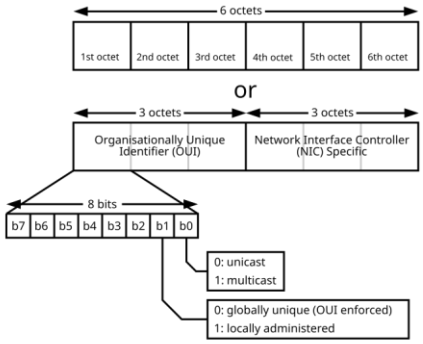
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

71

MAC-Adressen aller IEEE 802-Standards

- Netzwerkkarten besitzen eine ab Werk im **ROM (Read Only Memory) hinterlegte MAC-Adresse**.
- Auftrennung in **OUI (Organizationally Unique Identifier)** und **Device ID** ermöglicht es den Herstellern von Netzwerkkarten, eindeutige MAC-Adressen zu vergeben.
- Der Hersteller einer Netzwerkkarte kann folglich anhand deren MAC-Adresse identifiziert werden (z. B. 7c:6d:62 = Apple)
- Als **Broadcast-Adresse ist ff:ff:ff:ff:ff:ff** („all ones“) definiert
- Ob es sich bei einer Adresse um eine Unicast- oder Multicast-Adresse handelt, bestimmt das lowest order Bit des ersten Oktetts.

Anmerkung: Für bestimmte Anwendungen ist es sinnvoll, auf die herstellerübergreifende Eindeutigkeit zu verzichten, z. B. bei virtualisierten Netzwerkadaptern. Hierfür sind die sog. lokal-administrierten Adressen (zweites Bit des ersten Oktetts) vorgesehen.



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Fehlererkennung

- **Trotz Kanalkodierung können Übertragungsfehler (Bitfehler) auftreten.**
- Es kann daher passieren, dass eine fehlerhafte Payload an höhere Schichten weitergeleitet wird.
- Um die Wahrscheinlichkeit für derartige Fehler zu weiter zu reduzieren, werden **zusätzlich fehlererkennende Codes eingesetzt** (sog. Prüf- summen, engl. Checksums):
- Im Gegensatz zur Kanalkodierung (fehlerkorrigierende Codes) dient die Prüfsumme eines Schicht-2-Protokolls üblicherweise **nicht der Fehlerkorrektur sondern lediglich der Fehlererkennung**.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

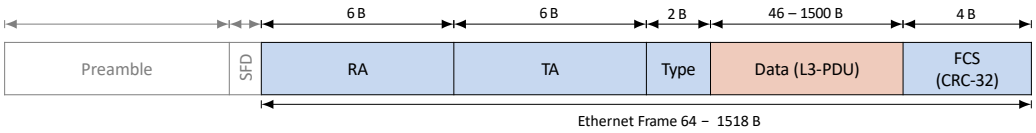
Cyclic Redundancy Check (CRC)

- Im Gegensatz zu fehlerkorrigierenden Codes, handelt sich sich bei **CRC um eine Familie fehlererkennender Codes**. Mit ihrem Einsatz werden folgende Ziele verfolgt:
- Eine **grosse Anzahl von Fehlern** (Einbit-, Mehrbit-, Burstfehler) sollen erkannt werden.
- Die zugefügte **Redundanz soll gering** sein.
- Fehler sollen **lediglich erkannt aber nicht korrigiert** werden können.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Fallbeispiel: IEEE 802.3u (FastEthernet)

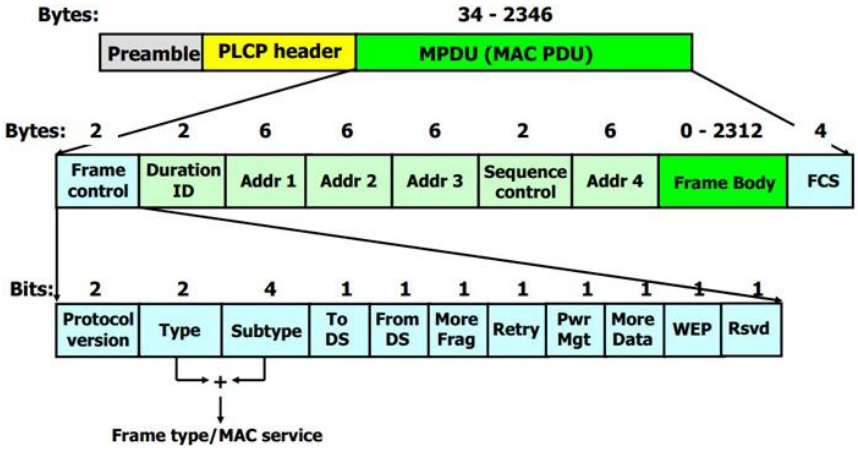
- Frame vor der 4B5B-Kodierung:



- Präambel und Start Frame Delimiter (SFD) dienen der **Taktsynchronisation**.
- Ein Byte der Präambel wird durch das J/K-Symbol des 4B5B-Codes ersetzt (Start Frame Delimiter).
- Nach der **Frame Check Sequence (FCS)** wird das T/R-Symbol des 4B5B-Codes eingefügt (End of Frame).
- Zwischen J/K und T/R liegende **Daten** werden gemäß des 4B5B-Codes kodiert.
- Das **Typfeld** gibt die Art des Frames an (z. B. 0x0800 =^ IPv4 Payload, 0x0806 =^ ARP).
- Das Datenfeld muss (vor der Kodierung) mind. 46 B lang sein – andernfalls wird es bis zu diesem Wert gepadded.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Fallbeispiel: IEEE 802.11a/g (WLAN)



[Quelle: https://www.engineersgarage.com/wi-fi-protocol-networking-frame-formats-security-attributes/ - letzter Abruf 22.07.2025]

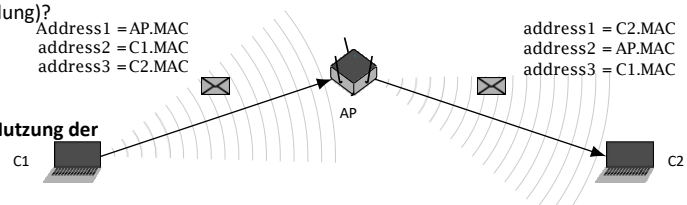
Fallbeispiel: IEEE 802.11a/g (WLAN)

Frame Control (FC)

- Gibt den Typ des Rahmens an (Data, Management oder Control)
- Definiert, wie die im Rahmen enthaltenen Adressen zu interpretieren sind (ToDS / FromDS Bits)
- Verschiedene weitere Parameter:
  - Folgen weitere Fragmente, die zum selben Rahmen gehören?
  - Handelt es sich um einen Retransmit (Wiederholung)?
  - Liegen am Sender noch weitere Rahmen vor?

MAC-Adressen (variable Anzahl, nachfolgend typische Nutzung der Felder)

- Address 1 gibt den direkten Empfänger (Receiver Address, RA) an
- Address 2 gibt die Adresse der übertragenden Station (Transmitter Address, TA) an
- Address 3 gibt den Sender (Source Address, SA) bzw. das Ziel (Destination Address, DA) an



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Fallbeispiel: IEEE 802.11a/g (WLAN)

Sequence Control

- Sequenznummer des Rahmens
- Dient der Erkennung von fehlenden Rahmen und der Sortierung empfangener Rahmen
- Hinweis: Im Gegensatz zu Ethernet werden im WLAN sog. Quittungsverfahren auf Schicht 2 eingesetzt, da das Übertragungsmedium selbst zu unzuverlässig ist.
- Dies ist kein Ersatz für Bestätigungen höherer Schichten,

Subnetwork Access Protocol (SNAP)

- Header variabler Länge zur Angabe des Typs der L3-PDU
- Entfernt vergleichbar mit dem Ethertype

- Daten variabler Länge
- Die maximale Rahmengröße in IEEE 802.11-Netzen ist um ein Vielfaches größer als bei Ethernet
- Der Medienzugriff benötigt hier sehr viel Zeit
- Je kleiner die einzelnen Rahmen, desto mehr Zeit geht durch den Medienzugriff verloren
- Tendenz zu größeren Rahmen trotz höherer Bitfehlerwahrscheinlichkeit

Frame Check Sequence (FCS)

- 32-bit CRC-Prüfsumme (bis auf Implementierungsdetails identisch zu Ethernet)
- FCS wird mit anderem Polynom als bei Ethernet berechnet

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Daten (L3-PDU)

78

05

Verbindung auf Schicht 1 und 2

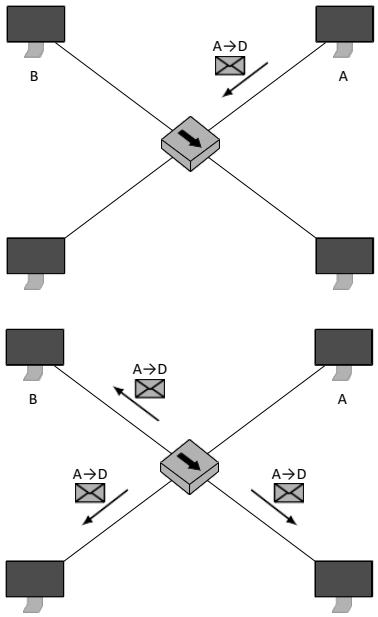
79

79

NETZWERKTECHNIK / SEMESTER 1 und 2

Verbindung auf Schicht 1: Hub

- **Knoten A sendet einen Rahmen an Knoten D**
- Der **Hub** verbindet die einzelnen Links **zu einem gemeinsamen Bus**
- Der Rahmen erreicht alle Knoten
- Es darf folglich zu jedem Zeitpunkt nur ein Knoten senden, andernfalls treten **Kollisionen** auf
- Wichtig: **Bis auf wenige Ausnahmen arbeitet Schicht 2 verbindungslos**, d. h. es wird keine logische Verbindung zwischen den Kommunikationspartnern aufgebaut.



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

80

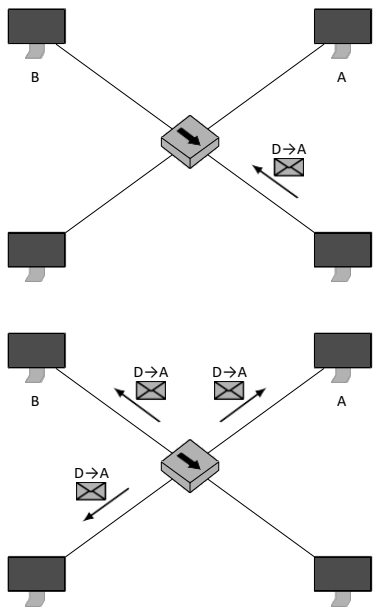
NETZWERKTECHNIK / SEMESTER 1 und 2

Verbindung auf Schicht 1: Hub

- Knoten D antwortet auf den Rahmen von A
- Auch die Antwort erreicht alle Knoten

Definition (Collision Domain)

Unter einer Kollisions-Domäne versteht man den Teil eines Direktverbindungsnetzes, innerhalb dem eine Kollision bei gleichzeitiger Über- tragung mehrerer Knoten auftreten kann. Dieser wird häufig auch als Segment bezeichnet.



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

81

Verbindung auf Schicht 1: Hub

Sind Hubs mehr als nur Sternverteiler?

- **Aktive Hubs (Repeater) verstärken die Signale** auf der physikalischen Schicht, ohne dabei die in Rahmen enthaltenen Felder wie Adressen oder Checksummen zu prüfen
- **Passive Hubs sind wirklich nur Sternverteiler**

Kann man Hubs kaskadieren?

- Ja, aber es gilt bei Ethernet mit Baumtopologie (802.3a/i) die 5-4-3-Regel:
- Nicht mehr als 5 Abschnitte, verbunden durch 4 Repeater, wobei nur in 3 Abschnitten aktive Endgeräte enthalten sein dürfen.

Können Hubs unterschiedliche Medientypen miteinander verbinden?

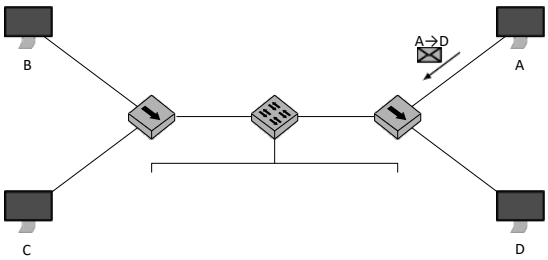
- Ja, wenn auf allen Abschnitten dasselbe Medienzugriffsverfahren genutzt wird (beispielsweise Verbindung Ethernet über BNC- und Patch-Kabel mit jeweils gleicher Datenrate).
- Unterschiedliche Zugriffsverfahren können nicht gekoppelt werden.

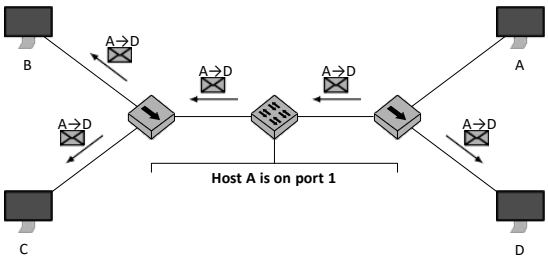
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

82

Verbindung auf Schicht 2: Switch

- Zwei Gruppen von Hosts, die jeweils über Hubs verbunden sind, werden durch einen Switch gekoppelt.
- Der Switch arbeitet zunächst wie ein Hub mit 2 Ports (Learning-Phase).
- Dabei merkt sich der Switch, über welchen Port ein Rahmen empfangen wurde.
- So ordnet er den Ports 0 und 1 die MAC-Adressen der Knoten zu, die an den jeweiligen Port angeschlossen sind.
- Ein Switch mit nur zwei Ports, nennt man auch Bridge.



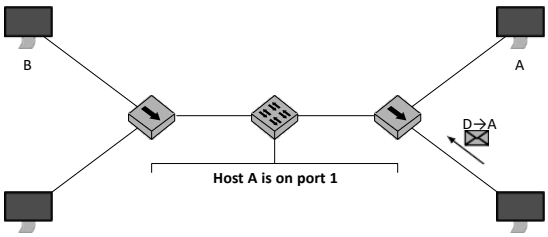


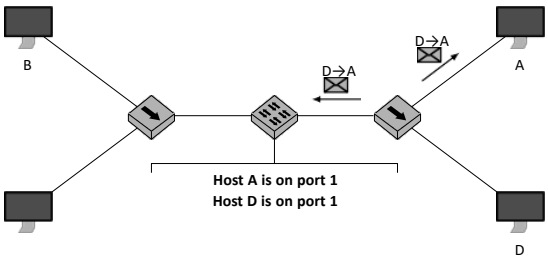
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

83

Verbindung auf Schicht 2: Switch

- Die Ziel-Adresse eingehender Rahmen wird mit den Einträgen in der Switching-Table verglichen.
- Ist ein Eintrag vorhanden, wir der Rahmen nur an den betreffenden Ziel-Port weitergeleitet.
- Ist kein Eintrag vorhanden, so wird der Rahmen an alle Ports weitergeleitet.
- Einträge erhalten einen Zeitstempel (Timestamp) und werden nach einem festen Zeitintervall invalidiert.

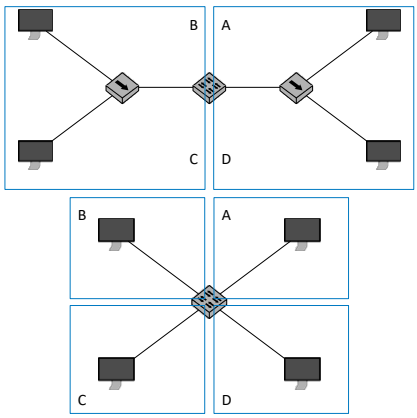




tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Verbindung auf Schicht 2: Switch

- Ein Switch bzw. eine Bridge unterbricht Kollisionsdomänen (auch als Segmentierung bezeichnet).
- Wenn ein Switch alle angeschlossenen Geräte kennt, darf in jedem der beiden Segmente jeweils ein Knoten zur selben Zeit senden.
- Ist pro Switchport genau ein Host angeschlossen, spricht man von Microsegmentation oder einem vollständig geswitchtem Netz (heute der Regelfall).
- In diesem Fall können jeweils zwei beliebige Hosts gleichzeitig miteineinander kommunizieren.



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

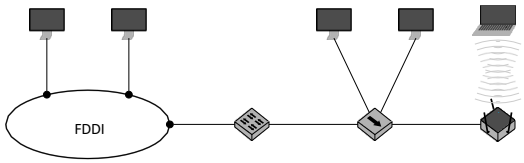
Verbindung auf Schicht 2: Switch

Switches können auch genutzt werden, um **Netzsegmente mit unterschiedlichen Zugriffsverfahren zu koppeln**:

- FDDI-Ethernet-Switch zwischen Token Passing und CSMA/CD
- WLAN Access Point zwischen CSMA/CD und CSMA/CA

Diese Kopplung ist transparent, d. h.

- angeschlossene Stationen bemerken nicht, dass ein Switch verwendet wird und
- im normalen Betrieb wird ein Host niemals direkt mit einem Switch kommunizieren.



Voraussetzung: Die MAC-Adressen müssen „kompatibel“ sein, um den jeweiligen Empfänger über seine MAC-Adresse identifizieren zu können.

Verbindung auf Schicht 2: Switch

- **Switches sind für Hosts transparent**, d. h. ein Host weiß nicht, dass er über einen Switch mit anderen Hosts kommuniziert.
- **Sender- und Empfänger-Adresse werden von Switches nicht verändert**.
- Switches **schränken nicht die Erreichbarkeit** innerhalb des Direktverbindungsnetzes ein.
- Ein **Broadcast (MAC-Adresse ff:ff:ff:ff:ff:ff)** wird von allen Hosts empfangen (man spricht daher auch von Broadcast-Domänen im Unterschied zu einer Kollisions-Domäne).
- Ein Switch benötigt zur Erfüllung seiner grundlegenden Aufgaben **keine eigene MAC-Adresse**.
- **Weiterleitungsentscheidungen werden auf Basis der Ziel-Adresse** und der Switching-Tabelle getroffen.

Ferner unterscheidet man zwischen zwei unterschiedlichen Switching-Arten:

- **Store-and-Forward:** Eingehende Rahmen werden vollständig empfangen und deren FCS geprüft. Falls der Ausgangsport belegt ist, kann eine begrenzte Anzahl von Rahmen gepuffert werden.
- **Cut-Through:** Beginne mit der Serialisierung des Rahmens, sobald der Ausgangsport bestimmt wurde. Die FCS wird in diesem Fall nicht geprüft.

Schleifen auf Schicht 2

Schleifen auf Schicht 2 führen dazu, dass **mehrere Kopien eines Rahmens erzeugt werden** und im Netzwerk zirkulieren.

Wie entstehen **Schleifen**?

- Auch wenn Direktverbindungsnetze räumlich begrenzt sind, kann man schnell den Überblick verlieren und ungewollt Schleifen erzeugen.
- Um robuste lokale Netze aufzubauen werden Topologien mit **redundanten Pfaden** verwendet. Fällt eine Verbindung oder ein Knoten aus, kann der Verkehr umgeleitet werden. **Aus redundanten Pfaden können Schleifen entstehen.**

Wie werden **Schleifen** vermieden?

- Switches unterstützen das sog. **Spanning Tree Protocol (STP)**.
- **Ziel ist die Deaktivierung redundanter Pfade, so dass alle Netzsegmente schleifenfrei erreichbar sind.**
- **Fällt eine Verbindung aus, wird ggf. einer dieser Pfade reaktiviert.**

WLAN Access Points

WLAN Access Points sind im wesentlichen Brücken zwischen Twisted Pair und Funkübertragung:

- Ein **RJ45-Interface** in Richtung des kabelgebundenen Netzwerks
- Ein **Wireless Transceiver** in Richtung des Funknetzwerks

Allerdings besteht ein wesentlicher **Unterschied zu Brücken bzw. Switches**:

- WLAN Access Points sind für WLAN Clients **nicht transparent auf Schicht 2!**
  - Clients sind sich der Anwesenheit eines Access Points bewusst.
  - Zur Kommunikation untereinander wird der Access Point direkt adressiert.

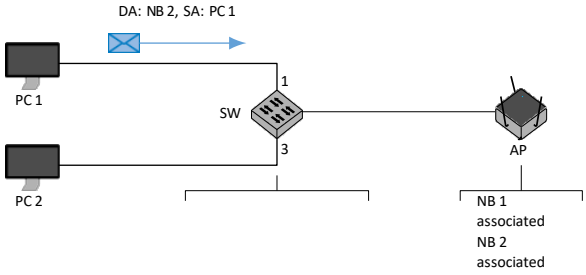
Gemeinsam mit Switches haben Access Points aber:

- Sie treffen **Weiterleitungsentscheidungen auf Basis von MAC-Adressen**.
- **Sie unterbrechen Kollisionsdomänen** auf logischer Ebene, d. h. ein Rahmen würde nicht weitergeleitet, sofern der betreffende Empfänger nicht mit dem jeweiligen AP assoziiert (verbunden) ist.
- Wichtig: Da Broadcast-Medium, nur eine Transmission gleichzeitig stattfinden, andernfalls Kollision

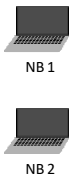
WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass

- NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und
- sonst noch keine Kommunikation im Netzwerk stattgefunden hat.



- PC 1 sendet einen Rahmen an NB 2.
- Source Address (SA) und Destination Address (DA) sind damit zunächst festgelegt.

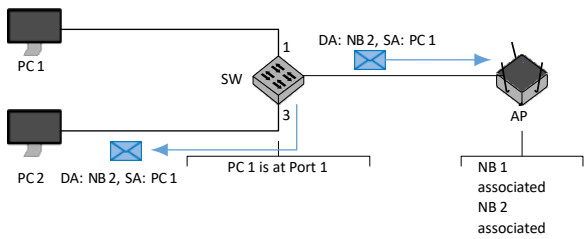


WLAN Access Points

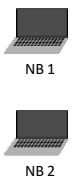
Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass

NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und

sonst noch keine Kommunikation im Netzwerk stattgefunden hat.



- Der Switch SW lernt, dass PC 1 an Port 1 angeschlossen ist.
- Der Empfänger NB 2 ist aber noch unbekannt, weswegen der Rahmen über alle Ports (außer dem, von dem er empfangen wurde) gesendet wird.

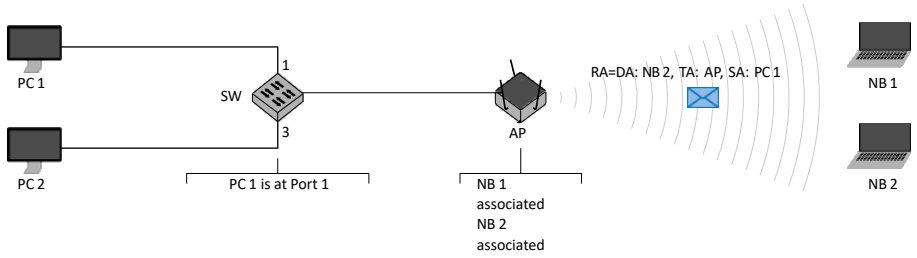


NETZWERKTECHNIK / SEMESTER 1 und 2

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

- AP empfängt den Rahmen - NB 2 assoziierte (verbundene) Station.
- Wandelt von IEEE 802.3 zu IEEE 802.11
- RA entspricht der Destination Address (DA).
- TA ist die MAC-Adresse des AP.
- SA bleibt die Adresse von PC 1.
- NB 2 wird den Rahmen akzeptieren, NB 1 wird ihn ignorieren.



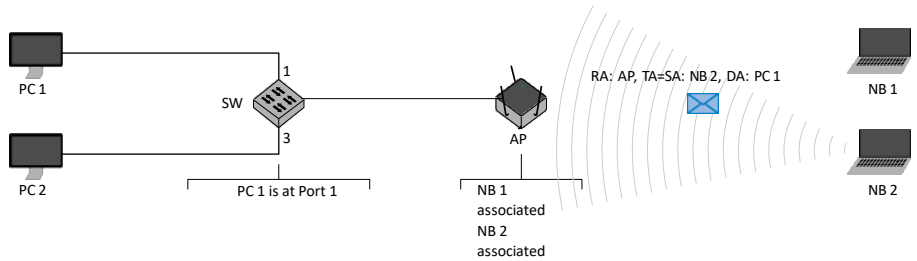
[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

NETZWERKTECHNIK / SEMESTER 1 und 2

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

- NB 2 antwortet mit einem neuen Rahmen.
- Receiver Address (RA) ist der AP.
- Transmitter Address (TA) entspricht der Source Address (SA).
- Destination Address (DA) ist PC 1.
- Der AP empfängt den Rahmen und akzeptiert ihn, da er an ihn gerichtet ist (RA)..

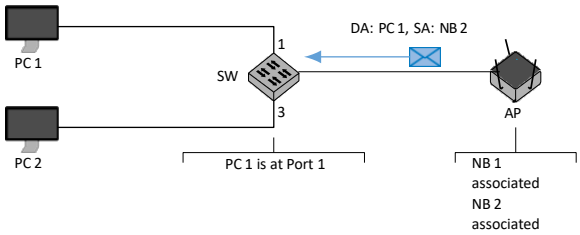


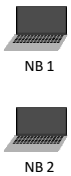
[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

- Der AP weiß, dass PC 1 keine assoziierte Station ist – sich also nicht im WLAN befindet.
- Der AP wird daher den Rahmen von IEEE 802.11 zu IEEE 802.3 zurückübersetzen.
- Source Address (SA) ist NB 2.
- Destination Address (DA) ist PC 1.



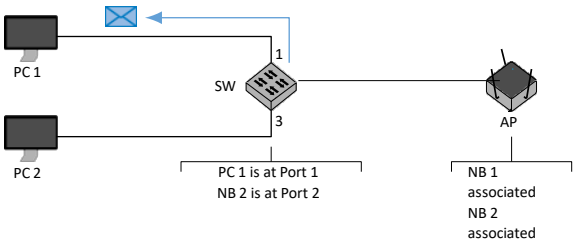


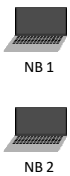
[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

- SW 1 lernt, dass NB 2 an über Port 2 erreichbar ist.
- Da PC 1 bekanntlich an Port 1 angeschlossen ist, wird der Rahmen auch nur dort weitergeleitet.
- PC 1 akzeptiert den Rahmen.
- Weder PC 1 noch NB 2 haben das andere Medienzugriffsverfahren bemerkt





[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Der Unsinn des „WLAN Routers“

Der Begriff „WLAN Router“ ist technisch falsch:

- Hersteller verkaufen hier Geräte, welche gleichzeitig
- DSL- oder Kabel-Modem,
- Ethernet Switch,
- Router (Ethernet ↔ DSL/Cable/etc.) und
- WLAN Access Point sind.

Tatsächlich sind **WLAN Access Points nicht mehr als Switches mit integrierten Medienkonvertern**, wobei meistens gleich noch ein Router integriert wird.

Routing findet innerhalb kabelloser Netzwerke im Infrastructure Mode nicht statt.