



Netzwerke und Internettechnologien 1





Zugriffs- und Fehlererkennungsverfahren

Netzwerke und Internettechnologien 1



Lernziele



1

Zugriffsverfahren



2

Fehlererkennung und
Fehlerkorrektur



Zugriffsverfahren

- Im Netzwerk kommunizieren die Stationen miteinander über physikalischen Verbindungswege, dem Übertragungsmedium.
- Das Zugriffsverfahren beschreibt die Art und Weise, wie die einzelnen Stationen auf das Übertragungsmedium zugreifen und es belegen.
- Das Zugriffsverfahren ist nicht von einer bestimmten Netzwerkstruktur abhängig.
- Grundsätzlich kann in zwei Arten unterschieden werden,
 - Stochastische Zugriffsverfahren (z.B. CSMA/CD und CSMA/CA) und
 - Deterministische Zugriffsverfahren (z.B. Token Passing).

Token-basierte Zugriffsverfahren

- Ein Zugriffsverfahren ist das Token Passing, ein deterministisches Verfahren.
- Nur der jeweilige Besitzer des Tokens darf senden.
- Ist seine Transaktion abgeschlossen, reicht er das Token wieder weiter.
- Es gibt zwei Realisierungsformen: Token Ring und Token Bus.

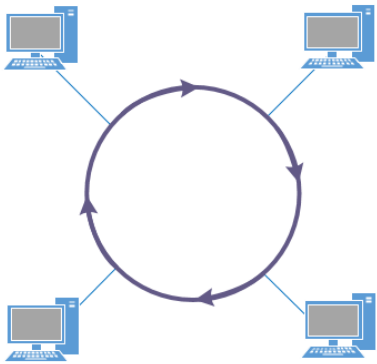


Abbildung 1: Token Ring (Eigene Darstellung)

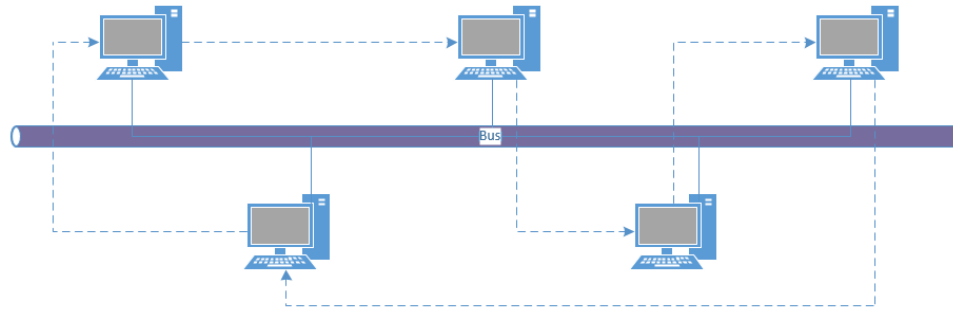


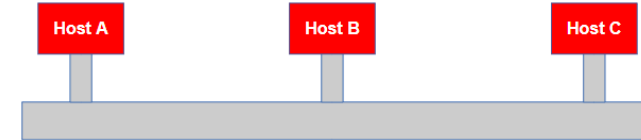
Abbildung 2: Token Bus (Eigene Darstellung)

CSMA/CD

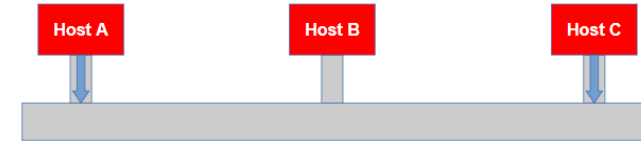
Carrier Sense Multiple Access with Collision Detection

- CSMA/CD ist ein stochastisches Zugriffsverfahren.
- **Carrier Sense** (Träger-Zustandserkennung): Jede Station prüft, ob das Übertragungsmedium frei ist.
- **Multiple Access** (Mehrfachzugriff): Mehrere Stationen teilen sich das Übertragungsmedium.
- **Collision Detection** (Kollisionserkennung): Wenn mehrere Stationen gleichzeitig senden, werden die Kollisionen erkannt.

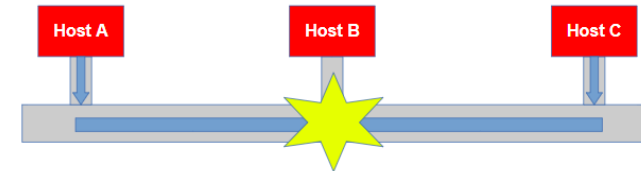
1) Carrier Sense



2) Multiple Access



3) Collision



4) Collision Detection (Back off Algorithmus)

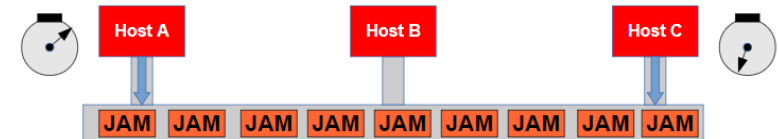


Abbildung 3: CSMA/CD-Verfahren (Deadlyhappen)
(https://commons.wikimedia.org/wiki/File:CSMA-CD_Verfahren.svg)

CSMA/CD

Kollisionen

- CSMA/CD konkurrieren mehrere Stationen um das Medium. Senden sie gleichzeitig, kommt es zu Kollisionen (Überlagerung der Signale).
- Zwischen Netzwerkausdehnung und Kollisionserkennung besteht ein Zusammenhang, aus diesem resultiert die Mindestlänge eines Frames (64 Byte).
- Kollisionen müssen, insbesondere vom Sender, erkannt werden.

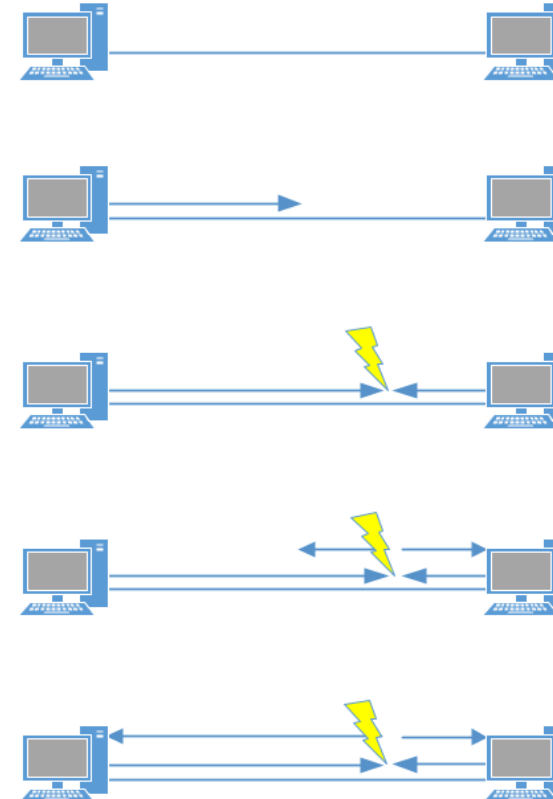


Abbildung 4: Kollision (Eigene Darstellung)

CSMA/CD

Kollisionen

- Bei Erkennung einer Kollision wird ein Jam-Signal gesendet, welches das Auftreten einer Kollision anzeigt.
- Danach wird eine zufällige Zeitdauer (Backoff) gewartet, ehe ein erneuter Sendeversuch gestartet wird.

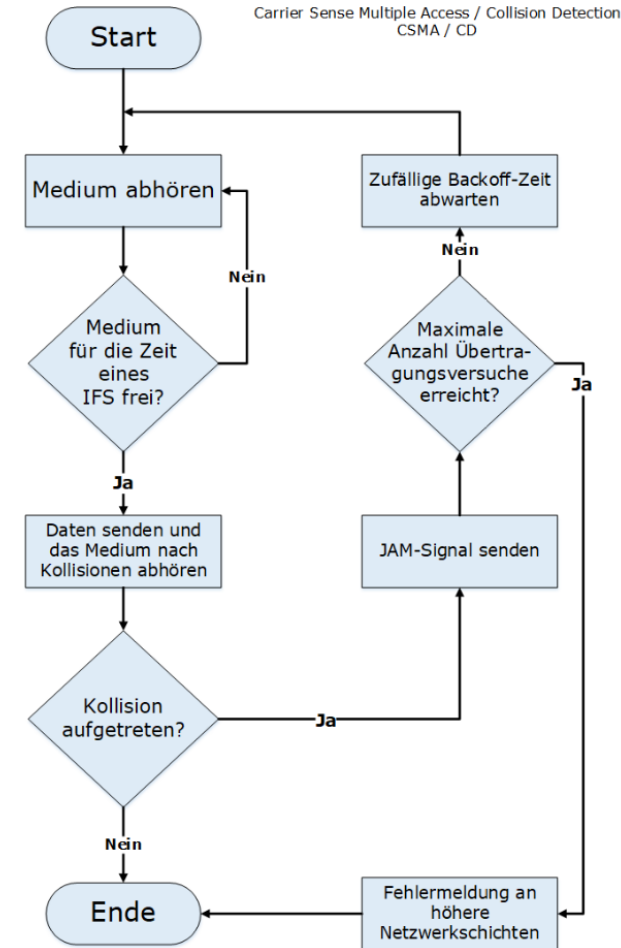


Abbildung 5: CSMACD (Heimdall793 (https://commons.wikimedia.org/wiki/File:CSMACDVisio_v2.png))

CSMA/CD

Kollisionen und Kollisionsdomäne

- Der Bereich, in dem Kollisionen empfangen werden können, wird als Kollisionsdomäne bezeichnet.
- Die heute gängigen Ethernet-Varianten können, da getrennte Sende- und Empfangsleitungen vorhanden sind, im Voll-Duplex Betrieb arbeiten.
- Kollisionen können im Voll-Duplex Betrieb nicht mehr auftreten.

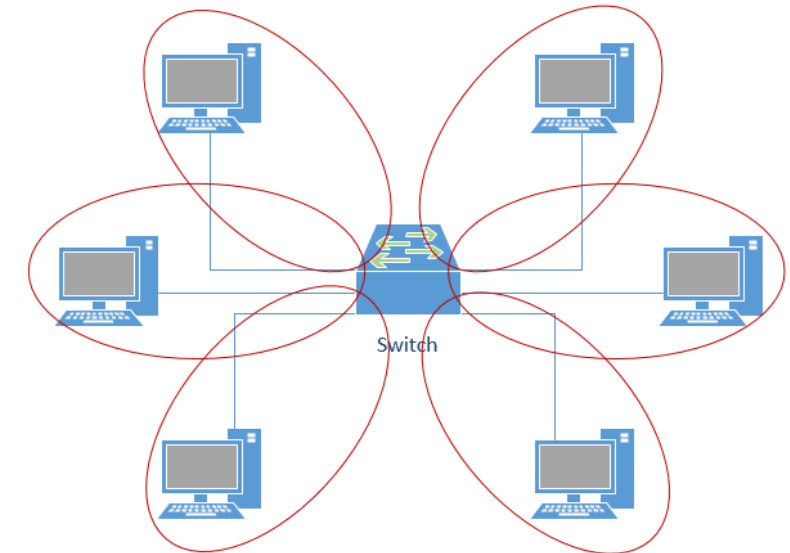
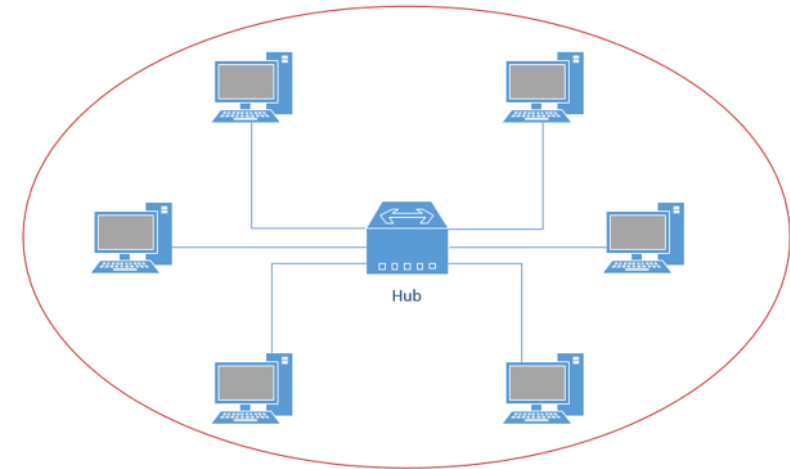


Abbildung 6: Kollisionsdomänen (eigene Darstellung)

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance

- CSMA/CA kommt im WLAN (IEEE 802.11) zum Einsatz.
- Auch hier teilen sich die Stationen das Medium.
- Es tritt aber das Hidden-Station-Problem auf, eine andere Station wird nicht erkannt.

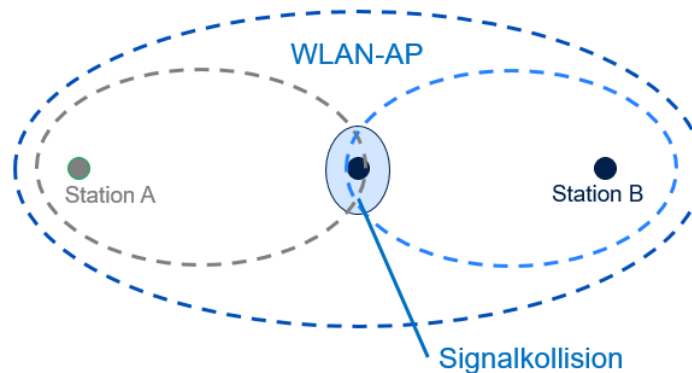


Abbildung 7: Hidden Station (Eigene Darstellung)

- Da hier Kollisionen nicht sicher erkannt werden können, wird auf Kollisionsvermeidung gesetzt.

CSMA/CA

Funktionsweise

- Ein WLAN-Client muß vor dem Senden sicherstellen, dass der Empfänger zum Empfang bereit und das Übertragungsmedium frei ist.
- Jede Station muß die Funkschnittstelle explizit reservieren, bevor sie sie belegen darf. Dieser Prozess wird als Listen-Before-Talk (LBT) bezeichnet.



Abbildung 8: LBT (Eigene Darstellung)

- CSMA/CA arbeitet mit Bestätigungspaketen (ACK), der Empfänger eines Pakets muss den Empfang beim Absender bestätigen.

CSMA/CA

Ablauf

1. Das Medium wird abgehört (Carrier Sense).
2. Ist das Medium frei, wird ein Request-to-Send (RTS) auf diesem Kanal gesendet.
3. Der Access Point (AP) sendet ein Clear-to-Send (CTS).
4. Die WLAN-Station sendet die Daten.
5. Der Access Point (AP) bestätigt den Empfang durch ein Acknowledgement (ACK).

Multiplex und Multiplexing

- Beim Multiplexverfahren werden mehrere Eingangssignale zusammengefasst und über ein Medium übertragen.
- Verfahren sind Raum-, Frequenz-, Zeit- und Codemultiplexing.
- Beim Zeitmultiplexverfahren werden in bestimmten Zeitabschnitten die Daten verschiedener Eingangskanäle, synchron (links) oder asynchron (rechts), auf einem Kanal übertragen.

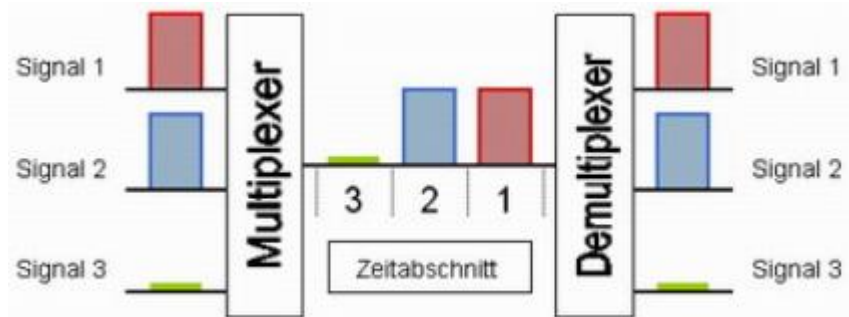


Abbildung 9: CSMACD (Matthias Bock (https://commons.wikimedia.org/wiki/File:Zeitmultiplex-synchron_1.jpg))

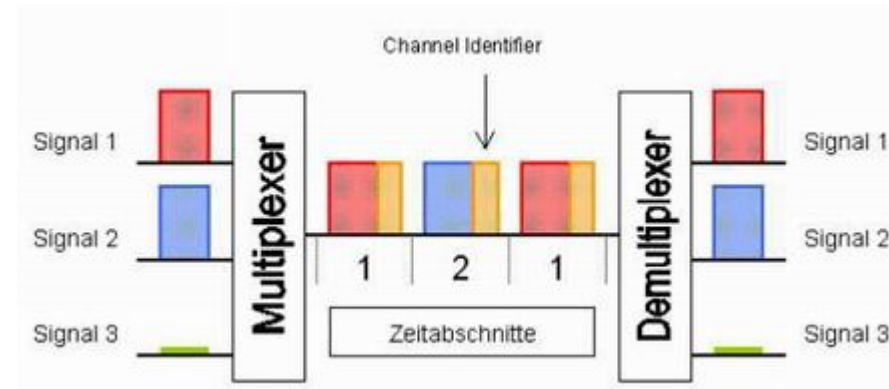


Abbildung 10: CSMACD (Matthias Bock (https://commons.wikimedia.org/wiki/File:Zeitmultiplex-asynchron_1.jpg))

Fehlererkennung und Fehlerkorrektur



Fehlerursachen

- Daten werden in Netzwerken im binäre Code in Form von Signalen übertragen.
- Während der Signalübertragung können Störungen (z.B. Verfälschung und Verlust) auftreten.
- Art und Häufigkeit der Fehler sind stark vom Übertragungsmedium abhängig.
- Bei Übertragung digitaler Daten führen Störeinflüsse (Fehlerquellen) zu falsch detektierten Bits.
- Typen:
 - Einzel-Bit-Fehler sind Fehler, die unabhängig von anderen auftreten.
 - Bündelfehler (Blockfehler), treten abhängig von anderen, durch Störeinflüsse, auf.
 - Synchronisierungsfehler: Alle Bits bzw. Zeichen werden falsch erkannt -> Informationsverlust.

Fehlerursachen

- Maß für die Fehlerhäufigkeit ist die Bitfehlerrate

$$\textit{Bitfehlerrate} = \frac{\textit{Summe der gestörten Bits}}{\textit{Summe der übertragenen Bits}}$$

- Typische Wahrscheinlichkeiten für Bitfehler:
 - Analoges Fernsprechnet $2 \cdot 10^{-4}$
 - Funkstrecke $10^{-3} - 10^{-4}$
 - Ethernet $10^{-10} - 10^{-12}$
 - Glasfaser $10^{-10} - 10^{-13}$

Fehlererkennung

- Die Datenübertragung ist im Allgemeinen nicht fehlerfrei.
- Die aufgetretenen Fehler müssen sicher erkannt werden.
- Fehlerkontrollsysteme basieren auf der Übertragung zusätzlicher Information (*Redundanz*), durch welche die Gültigkeit der Daten überprüft werden kann.
- Diese Redundanz verringert die Nettoübertragungsrate.
- Ziel ist daher die Verwendung einer Verfahrens, das mit wenig Zusatzinformationen eine sichere Fehlererkennung erlaubt.
- Das geeignete Verfahren hängt vom Übertragungskanal ab.

Fehlererkennung

Parität

- Eine Methode zur Fehlererkennung bei der Datenübertragung und -speicherung ist das Einfügen von *Paritätsbits*.
- Mittels des Paritätsbits können Einzelbitfehler erkannt aber nicht korrigiert werden.
- Bei der Paritätsprüfung wird auf gerade (even) oder ungerade (odd) Parität geprüft.
- Die Anzahl der »1«-Bits, incl. dem Paritätsbit, wird auf eine gerade oder ungerade Zahl ergänzt.



Abbildung 11: Parität (Eigene Darstellung)

Fehlererkennung und -korrektur

Mehrdimensionale Parität (Kreuz- oder Blockparität)

- Bei diesem Verfahren werden die Bytes zu einem Array zusammengefasst.
- Zu jeder Zeile und jeder Spalte wird ein Paritätsbit ermittelt.
- Mit dem Verfahren können 1-Bit-Fehler erkannt und korrigiert werden.
- Es ist ein Fehlererkennungs- und Fehlerkorrekturverfahren.
- Mehrbit-Fehler können u.U. erkannt, aber nicht korrigiert werden.

even

Paritätsbit

1	1	0	1	1	0	0	0
1	0	0	1	0	0	1	1
0	1	0	1	1	0	1	0
1	0	0	0	1	0	0	0
0	1	0	1	1	0	1	0
1	0	0	1	0	0	0	0
0	1	0	0	1	0	1	1
0	0	0	1	1	0	0	0

Paritätsbit

even

Paritätsbit

1	1	0	1	1	0	0	0
1	0	0	1	0	0	1	1
0	1	0	1	1	0	1	0
1	0	0	1	1	0	0	0
0	1	0	1	1	0	1	0
1	0	0	1	0	0	0	0
0	1	0	0	1	0	1	1
0	0	0	1	1	0	0	0

Paritätsbit

Abbildung 12: Kreuzparität (Eigene Darstellung)

Fehlererkennung und -korrektur

Zyklische Redundanzprüfung

- Englisch cyclic redundancy check (CRC) ist ein Fehlererkennungsverfahren, bei dem ein Prüfwert (Prüfsumme) für die Daten ermittelt wird, die an die Daten angehängt wird.
- Der Empfänger errechnet nach der gleichen Methode die Prüfsumme und vergleicht sie mit der übermittelten.
- Dient zur Erkennung von zufälligen Fehlern. 1-Bit- und unabhängige Mehrbit-Fehler werden erkannt.
- Anwendung zum Beispiel im Ethernet-Frame:

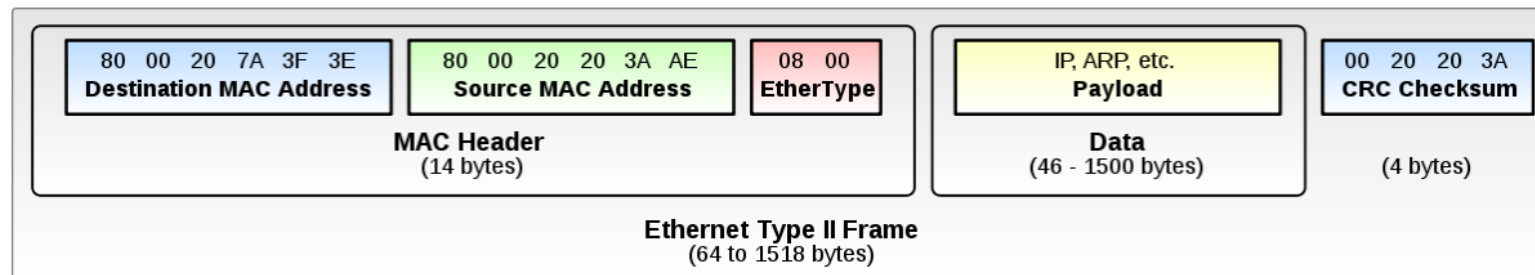


Abbildung 13: Ethernet Type II Frame format (Wikipedia)

Fehlerkorrektur

ECC (error-correcting code)

- ECC ist eine Kodierung zur Fehlerkorrektur.
- Bei dieser Kodierung werden auf 32 Bit 6 Check-Bits und auf 64 Bit 7 Check-Bits benötigt.
- ECC ist in der Lage, 1-Bit-Fehler zu korrigieren und 2-Bit-Fehler zu erkennen.
- Mehr-Bit-Fehler werden nicht mehr sicher erkannt.
- Das ECC-Verfahren wird häufig in RAM-Bausteinen für Server eingesetzt, die eine besonders hohe Datenintegrität benötigen.

Fehlerkorrektur

Hamming-Code

- Der Hamming-Code ist ein fehlerkorrigierender Blockcode.
- Bei diesem werden mehrere Paritätsbits eingefügt und ermöglichen es 1-Bit-Fehler zu erkennen und zu korrigieren sowie 2-Bit-Fehler zu erkennen.

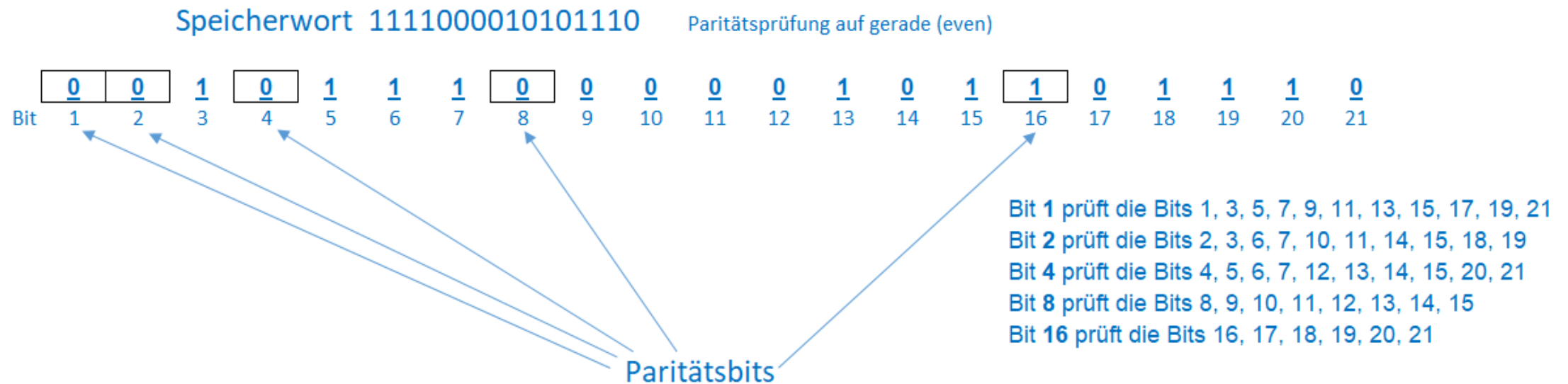


Abbildung 14: Hamming-Code (Eigene Darstellung)

Quellen

Buchquelle

2. Vorlesung Netzwerke - PDF Kostenfreier Download (2021). Online verfügbar unter <https://docplayer.org/17203729-2-vorlesung-netzwerke.html>, zuletzt aktualisiert am 07.05.2021, zuletzt geprüft am 07.05.2021.

ECC - Error Correcting Code (2021). Online verfügbar unter <https://www.elektronik-kompodium.de/sites/com/1504141.htm>, zuletzt aktualisiert am 14.05.2021, zuletzt geprüft am 14.05.2021.

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

PROF. DR. Stephan Euler (2005): Netzwerk-Grundlagen, Teil 2. In: TecChannel Workshop, 15.08.2005. Online verfügbar unter <https://www.tecchannel.de/a/netzwerk-grundlagen-teil-2,431454,8>, zuletzt geprüft am 14.05.2021.

Schnabel, Patrick (2013): Netzwerktechnik-Fibel. Grundlagen Netzwerktechnik ; Übertragungstechnik ; TCP/IP ; Anwendungen und Dienste ; Netzwerk-Sicherheit. 3. Aufl. Ludwigsburg.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

Wikipedia (Hg.) (2021): Carrier Sense Multiple Access/Collision Detection. Online verfügbar unter https://de.wikipedia.org/w/index.php?title=Carrier_Sense_Multiple_Access/Collision_Detection&oldid=211820540, zuletzt aktualisiert am 10.05.2021, zuletzt geprüft am 13.05.2021.

Wikipedia (Hg.) (2021): Ethernet. Online verfügbar unter <https://de.wikipedia.org/w/index.php?title=Ethernet&oldid=210943590>, zuletzt aktualisiert am 15.04.2021, zuletzt geprüft am 11.05.2021.

Wikipedia (Hg.) (2021): Multiplexverfahren. Online verfügbar unter <https://de.wikipedia.org/w/index.php?title=Multiplexverfahren&oldid=209368535>, zuletzt aktualisiert am 02.03.2021, zuletzt geprüft am 14.05.2021.

Wikipedia (Hg.) (2021): Paritätsbit. Online verfügbar unter <https://de.wikipedia.org/w/index.php?title=Paritätsbit&oldid=208134459>, zuletzt aktualisiert am 27.01.2021, zuletzt geprüft am 14.05.2021.

Abbildungen

3 „CSMA-CD Verfahren“ Lizenz: Deadlyhappen (https://commons.wikimedia.org/wiki/File:CSMA-CD_Verfahren.svg), „CSMA-CD Verfahren“, <https://creativecommons.org/licenses/by-sa/3.0/legalcode>

4 „CSMACD“ Lizenz: Heimdall793 (https://commons.wikimedia.org/wiki/File:CSMACDVisio_v2.png), <https://creativecommons.org/licenses/by-sa/4.0/legalcode>

9 „Zeitmultiplex-synchron“ Lizenz: Matthias Bock (https://commons.wikimedia.org/wiki/File:Zeitmultiplex-synchron_1.jpg), „Zeitmultiplex-synchron 1“, <https://creativecommons.org/licenses/by-sa/3.0/legalcode>

10 Lizenz: „Zeitmultiplex-synchron“ Lizenz: Matthias Bock (https://commons.wikimedia.org/wiki/File:Zeitmultiplex-asynchron_1.jpg), „Zeitmultiplex-asynchron 1“, <https://creativecommons.org/licenses/by-sa/3.0/legalcode>

Quellen

Buchquelle

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

Abbildungen

10 Lizenz: „Zeitmultiplex-synchron“ Lizenz: Matthias Bock (https://commons.wikimedia.org/wiki/File:Zeitmultiplex-asynchron_1.jpg), „Zeitmultiplex-asynchron 1“, <https://creativecommons.org/licenses/by-sa/3.0/legalcode>

VIELEN DANK!

