

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Vorlesung
Rechnernetze und Kommunikationssysteme
Kommunikationsnetze

Dr. Werner Otten, Fakultät für Informatik ■ Wintersemester 2025/2026

Kapitel 3:

Media Access Control (MAC) Teilschicht

Kapitelinhalt

- 3.1 Kanalzugriff
- 3.2 Multipler Zugriff
- 3.3 IEEE 802 LANs
- 3.4 Netzwerkkoppelung auf Sicherungsschicht

Kapitel 3.1:

Kanalzugriff

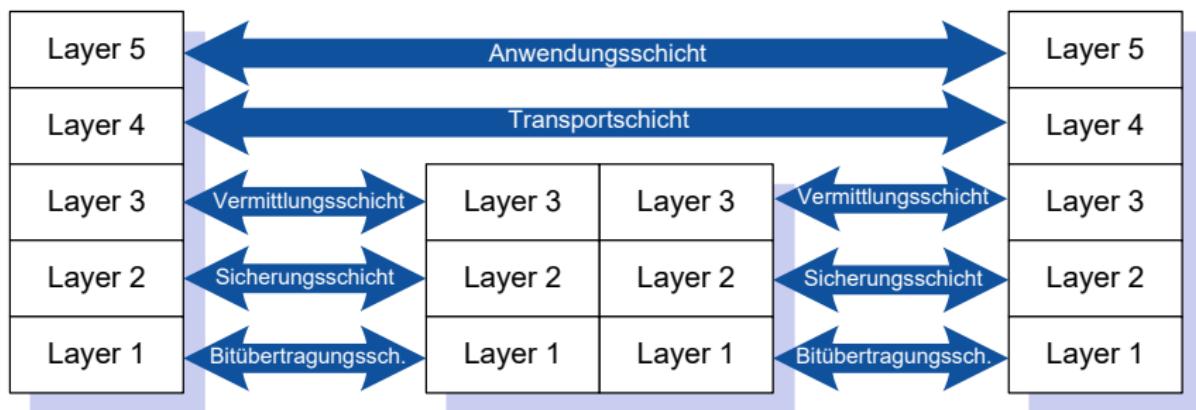
Zuordnung des Kommunikationskanals

- Ausgangssituation:
 - Mehrere Stationen nutzen den selben Kommunikationskanal (Broadcast Medium)
 - Es besteht die Möglichkeit, dass 2 oder mehr Stationen (quasi) gleichzeitig senden \rightsquigarrow Kollision
 - Wie kann man Kollisionen vermeiden?
- Zwei Ansätze denkbar
 - statische Kanalzuordnung \rightsquigarrow einfach zu implementieren
 - dynamische Kanalzuordnung \rightsquigarrow effiziente Verwendung der Bandbreite

Zuordnung des Kommunikationskanals

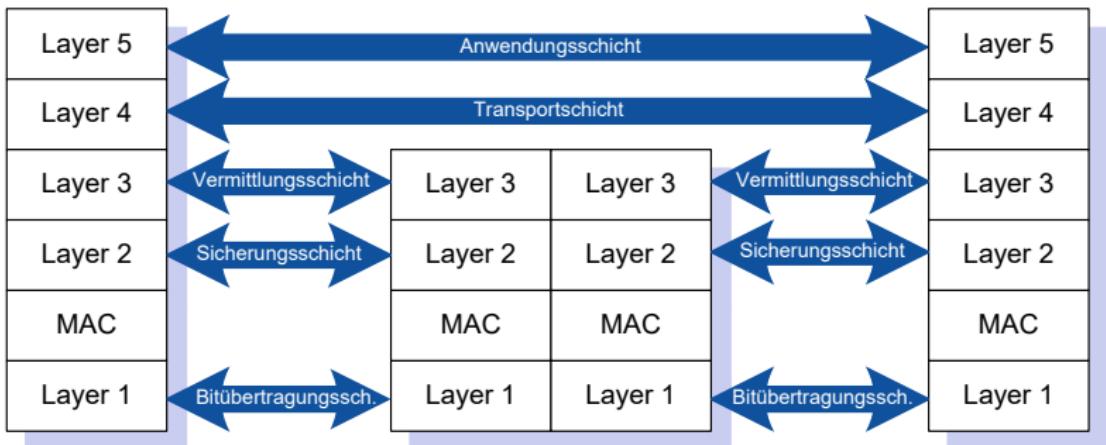
- wenn zwei oder mehr Nutzer zur selben Zeit senden, kommt es zu einer Kollision
- alle kollidierenden Pakete gehen in diesem Fall verloren \rightsquigarrow Verlust von Bandbreite
- ein Zugriffsprotokoll für ein Broadcast Medium mit Bandbreite R Bit/sec sollte idealerweise gewährleisten:
 - dass der Durchsatz R Bit/sec ist, falls nur eine Station sendet.
 - dass der Durchsatz R/M Bit/sec ist, falls M Stationen Daten senden möchten.
 - dass das Zugriffsprotokoll dezentralisiert abläuft, d.h. keine Station ausgezeichnet ist (Masterstation).
 - dass es einfach und günstig zu implementieren ist.

Protokolllayer



- der Data Link Layer (Sicherungsschicht) erzeugt die Frames und legt sie auf den Kanal
- falls mehrere Stationen gleichzeitig Frames auf den Kanal legen möchten ~ zusätzliche Media Access Control (MAC) notwendig

Media Access Control Teilschicht



- MAC–Schicht ist keine eigenständige Schicht im ISO/OSI Modell
- MAC ist in einer Teilschicht des Data Link Layers angesiedelt

Statische Kanalzuordnung

- Frequenzmultiplexing (FDM)
 - Kanal mit Bandbreite H wird bei n angeschlossenen Stationen in H/n Frequenzbänder aufgeteilt
 - jede Station erhält ein anderes Frequenzband
 - keine Kollision möglich, aber Bandbreite wird für jede einzelne Station um Faktor n reduziert
- Zeitmultiplexing (TDM)
 - Kanal mit Transferrate H Bit/sec und n angeschlossenen Stationen
 - bilden n Zeitslots der Länge t , jede Station überträgt pro Slot $B * t$ Bit
 - keine Kollision möglich, aber Bandbreite wird für jede einzelne Station um Faktor n reduziert

Dynamische Kanalzuordnung

- zur späteren Diskussion gehen wir von folgenden Annahmen aus:
- Stationsmodell
 - n unabhängige Stationen
 - jede Station ist in der Lage Frames zu erzeugen und möchte diese versenden
 - Ankunftsrate λ der Frames sei konstant
 - Wahrscheinlichkeit, dass im Zeitraum Δt ein Frame gesendet wird ist $\Delta t * \lambda$
 - wenn ein Frame erzeugt wurde, ist Station blockiert, bis dieser gesendet wurde

Dynamische Kanalzuordnung

- gemeinsamer Kanal
 - alle Stationen sind an einem gemeinsamen Kanal angeschlossen
 - alle Stationen sind gleichartig
 - jede Station kann sowohl senden als auch empfangen
 - Optional: es können Prioritäten vergeben werden
- Kollisionsannahme
 - zwei Stationen senden in einem überlappenden Zeitintervall gleichzeitig \rightsquigarrow Kollision
 - gesendete Informationen sind zerstört/verändert
 - nach einer Kollision müssen die Frames erneut gesendet werden
 - Stationen sind in der Lage, Kollisionen zu erkennen
 - außer Kollisionen passieren keine Fehler

Dynamische Kanalzuordnung

hinsichtlich des Zeitpunktes, wann gesendet wird, kann eine der folgenden Annahmen getroffen werden

- kontinuierliche Sendezeit
 - Zeit ist nicht in diskrete Abschnitte eingeteilt
 - jede Station kann zu einer beliebigen Zeit mit dem Senden beginnen
- diskrete Sendezeit
 - Zeit ist in diskrete Abschnitte (Slots) eingeteilt
 - Versendung der Rahmen beginnt am Anfang oder Ende eines Zeitslots

Dynamische Kanalzuordnung

eine weitere Unterscheidung besteht in der Möglichkeit der Kanalüberwachung

- Carrier Sense (Kanalüberwachung)
 - der Kanal ist entweder belegt oder frei
 - Stationen können den Kanal überwachen und erkennen, ob er belegt ist
 - vor dem Sendebeginn wird der Status des Kanals überprüft
- keine Kanalüberwachung
 - Stationen können den Kanal nicht überwachen
 - Station sendet einfach
 - nach dem Senden, weiß die Station anhand einer Bestätigung ob die Übertragung erfolgreich war oder nicht

Kapitel 3.2:

Mehrfacher Zugriff (Multiple Access)

Dynamische Kanalzuordnung – Verfahren

- ALOHA Protokolle
- Carrier Sense Multiple Access Protokolle
- kollisionsfreie Protokolle
- Zugriffsprotokolle für Wireless LAN

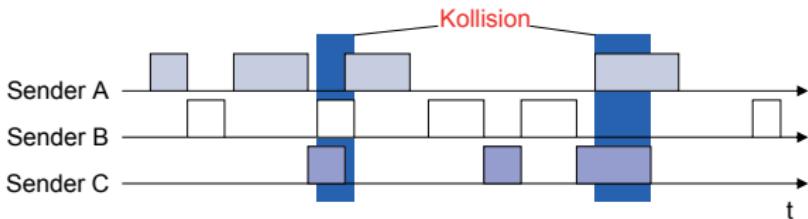
ALOHA Protokolle

- 1970 von N. Abramson an der Universität von Hawaii entwickelt
- diente zum Anschluss der diversen Hawaii Inseln per Funkkanal an die Universität von Hawaii
- auf einem gemeinsamen Kanal senden die Stationen zu einer Basisstation
- Basisstation bestätigt durch ein Acknowledgement auf anderer Frequenz
- falls es zu Kollisionen kommt, bleibt Acknowledgement aus
- Idee auf alle Übertragungen mit nicht koordinierten Benutzern und gemeinsamen Kanal übertragbar
- Varianten: Reines Aloha (ohne diskrete Zeitsteuerung) und Slotted Aloha (mit diskreten Zeitslots)

Reines ALOHA

- Benutzer dürfen zu jeder Zeit Daten übertragen
- die Rahmen haben alle die gleiche Größe
- falls mehrere Stationen gleichzeitig senden kommt es zu Kollisionen, die Rahmen werden beschädigt
- nach einer Kollision warten die Stationen eine zufällige Zeit und senden erneut

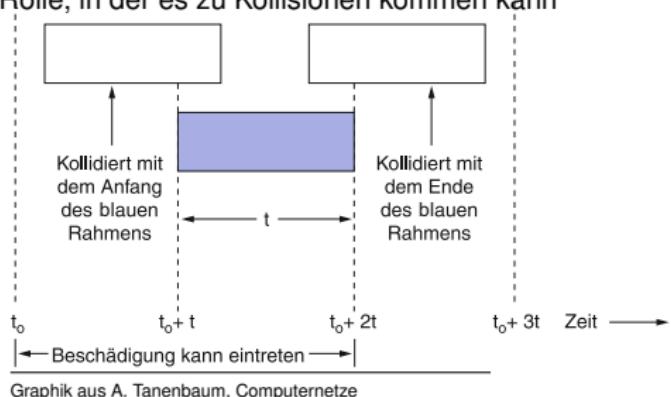
- Auftreten einer Kollision: zwei Rahmen überschneiden sich mindestens in einem Bit



Reines ALOHA – Effizienz

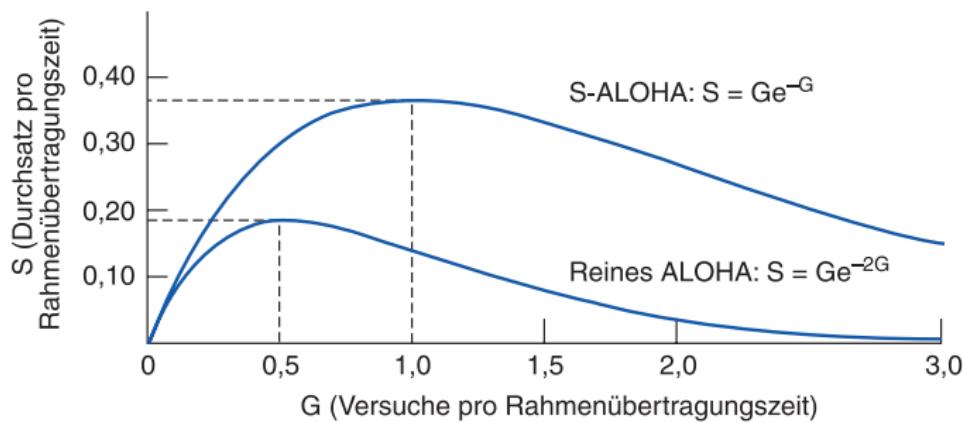
- für Effizienz ist die Kollisionswahrscheinlichkeit interessant
- hier spielt das Konkurrenzintervall eine Rolle, in der es zu Kollisionen kommen kann
- bei einer Rahmenübertragungszeit von t hat das Konkurrenzintervall bei reinem ALOHA eine Breite von $2 * t$
- ist S der Durchsatz pro Rahmenübertragungszeit und G die Anzahl der Versuche, so gilt:

$$S = Ge^{-2G}$$



ALOHA

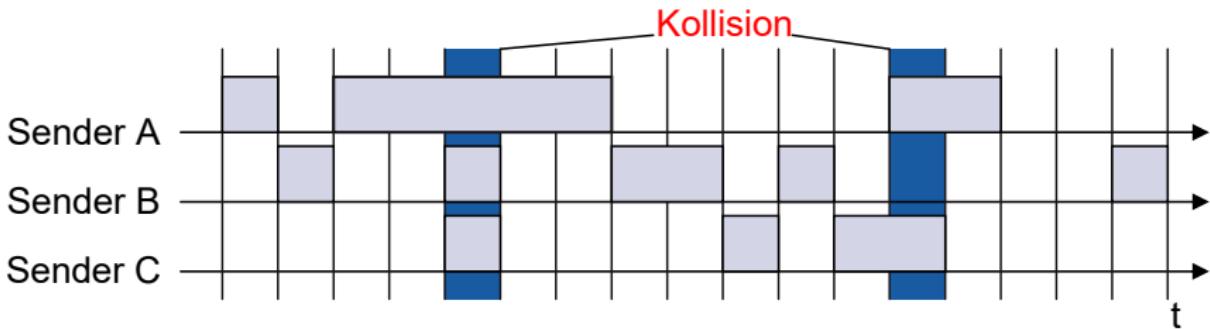
- maximaler Durchsatz bei reinem ALOHA ist für $G = 0,5$ mit $S = 1/(2e)$ gegeben
- damit ist die maximale Kanalnutzung von 18,4 % erreichbar



Graphik aus A. Tanenbaum, Computernetze

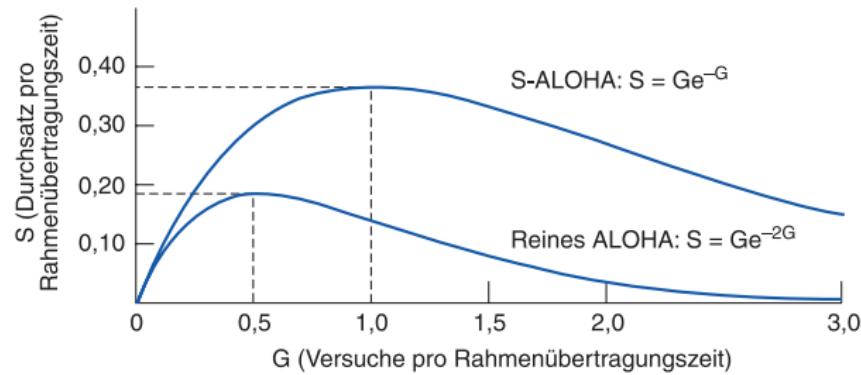
Slotted–ALOHA

- es werden Slots der Länge t gebildet (Länge der Rahmen)
- Übertragung kann nur am Anfang eines Slots beginnen
- dadurch wird das Konkurrenzintervall von $2t$ auf t reduziert, d.h. der Durchsatz wird verdoppelt



Effizienz ALOHA vs. S–ALOHA

- durch Reduktion des Konkurrenzintervalls bei Slotted–ALOHA auf t ist Durchsatz gegeben durch
$$S = Ge^{-G}$$
- in diesem Fall dann maximaler Durchsatz für $G = 1$ mit ca. 36,8 %



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

CSMA Protokolle (Carrier Sense Multiple Access)

- S–ALOHA erreicht eine maximale Kanalnutzung von 36,8 %
- bedingt durch die Tatsache, dass Stationen beginnen zu senden ohne sich dafür zu interessieren, ob andere Station sendet (d.h. es kommt häufig zu Kollisionen)
- Verbesserung: Station hört vor dem Senden den Kanal ab (Protokolle mit Trägerprüfung, Carrier Sense Multiple Access CSMA)
- hierzu gibt es verschiedene Varianten

1-persistentes CSMA

- Protokoll
 - sendewillige Station hört Kanal ab
 - falls bereits andere Station sendet, wartet sie bis Kanal frei ist
 - bei freiem Kanal wird der Rahmen übertragen
 - tritt Kollision auf, wird zufällige Zeit gewartet und dann von vorne begonnen
 - wenn Kanal frei ist, wird mit Wahrscheinlichkeit 1 gesendet, daher 1-persistent
- Leistungsfähigkeit/Kollisionshäufigkeit hängt von der Signalausbreitungsverzögerung ab (damit von der Länge des Mediums)
- Kollision auch bei Null Verzögerung möglich, wenn zwei Stationen auf das Freiwerden des Kanals warten

p-persistentes CSMA

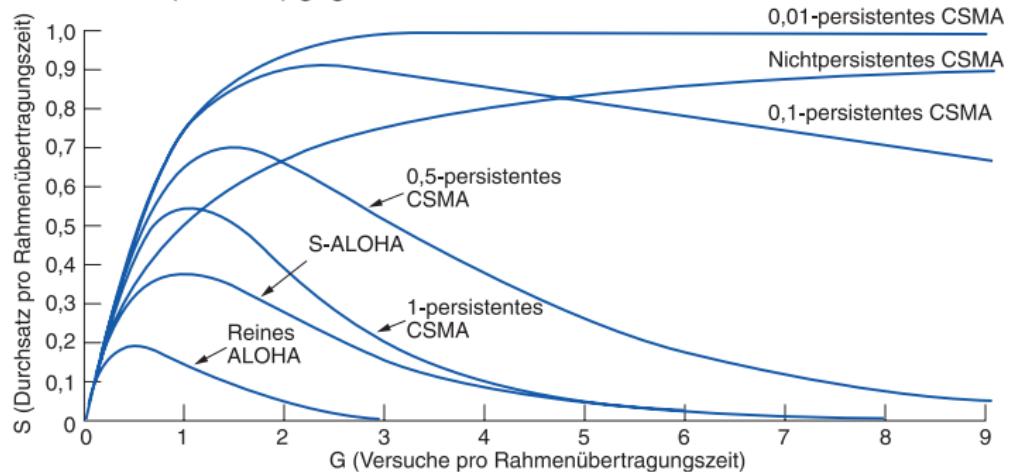
- Protokoll zur Anwendung bei Kanälen mit Zeitschlitten
 - sendewillige Station hört Kanal ab
 - bei freiem Kanal wird der Rahmen nur mit Wahrscheinlichkeit p übertragen und mit Wahrscheinlichkeit $q = 1 - p$ bis zum nächsten Zeitschlitz gewartet
 - ist nächster Zeitschlitz ebenfalls frei, wird wiederum mit Wahrscheinlichkeit p gesendet und mit Wahrscheinlichkeit q gewartet
 - Vorgang wird wiederholt, bis Rahmen gesendet wurde, oder in Zeitschlitz Kanal belegt war, dann behandelt wie bei Kollision
 - wenn Zeitschlitz bei erster Prüfung belegt, wird im nächsten Zeitschlitz wieder geprüft

nichtpersistentes CSMA

- Protokoll
 - sendewillige Station hört Kanal ab
 - falls bereits andere Station sendet, wartet sie eine zufällige Zeit und hört Kanal erneut ab
 - bei freiem Kanal wird der Rahmen übertragen
 - tritt Kollision auf, wird zufällige Zeit gewartet und dann von vorne begonnen
- Unterschied zu persistentem CSMA: bei belegtem Kanal wird nicht ständig weiter abgehört

Effizienz ALOHA vs. CSMA

ein Vergleich des Durchsatzes zeigt eine deutliche Steigerung bei 1-persistentem CSMA (ca. 55%) bzw. 0.5-persistentem CSMA (ca. 70%) gegenüber den ALOHA Verfahren



Graphik aus A. Tanenbaum, Computernetze

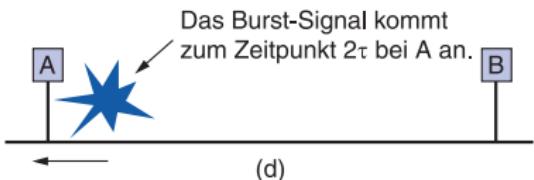
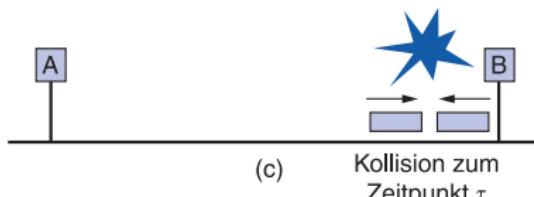
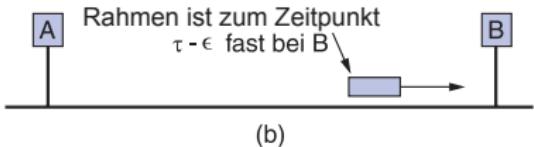
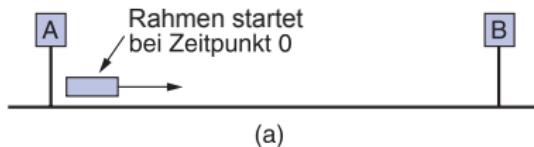
CSMA mit Kollisionserkennung (CD)

- Kollisionserkennung kann erfolgen durch
 1. abwarten einer Bestätigung (ACK)
 - ACK wird gesendet, falls der Rahmen korrekt empfangen wurde, d.h. Frames mit Kollisionen werden komplett übertragen
 - Warten auf das ACK kostet Zeit und Bandbreite (da alle Rahmen komplett übertragen werden)
 2. überwachen des Kanals während der Übertragung
 - sendende Station vergleicht das gesendete Signal mit Signal auf dem Kanal \rightsquigarrow Kollision kann früher erkannt werden
 - Verfahren wird "Collision Detection" (CD) genannt

CSMA mit Kollisionserkennung (CD)

- Kollision kann bei Signalvergleich durch Veränderung der Leistung oder Impulsbreite erkannt werden
- zu welchem Zeitpunkt kann Kollision erkannt werden?
 - Station A sendet zum Zeitpunkt t_0 einen Frame
 - Signal benötigt τ um die am weitesten entfernte Station X zu erreichen
 - zum Zeitpunkt $t_0 + \tau - \epsilon$ beginnt Station X auch zu senden
 - zu diesem Zeitpunkt erkennt X den Kanal als frei
 - Signal von X benötigt τ um Station A zu erreichen
 - Folgerung: A muss $2\tau - \epsilon$ warten, um die Kollision zu erkennen
 - Problem: der maximale Wert von τ hängt von der maximalen Entfernung der Stationen ab!

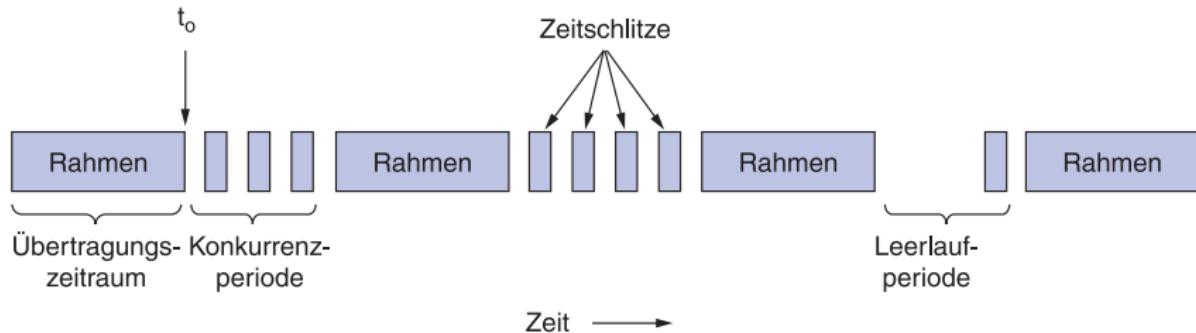
CSMA mit Kollisionserkennung (CD)



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

CSMA mit Kollisionserkennung (CD)

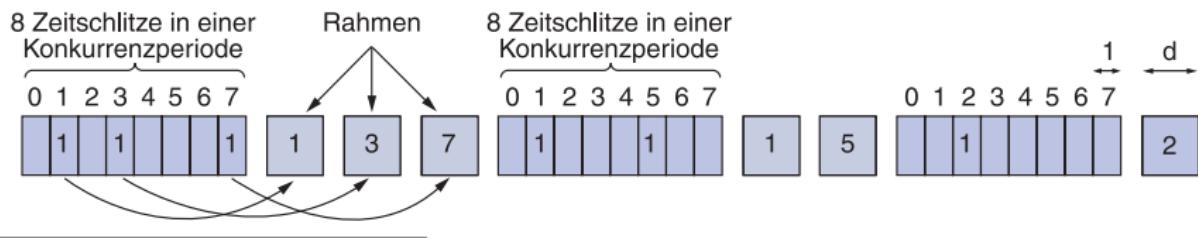
- CSMA/CD besteht aus abwechselnder Konkurrenzperiode (hier können Kollisionen auftreten) und Übertragungszeitraum
- zusätzlich kann es zu Leerlaufperioden kommen (keine Station überträgt)



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

Kollisionsfreie Protokolle – Bitmap

- bei N angeschlossenen Stationen besteht die Konkurrenzperiode aus N Zeitschlitten
- in diesen Zeitschlitten übertragen die N Stationen der Reihe nach eine 1 falls ein Rahmen zur Übertragung bereitsteht
- nach der Konkurrenzphase wissen alle Stationen wer übertragen möchte
- die Stationen übertragen der Reihe nach die Rahmen



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

Kollisionsfreie Protokolle – Bitmap

- das Bitmap Protokoll ist ein Reservierungsprotokoll
- für die Reservierung entsteht ein Overhead
 - falls jede der insgesamt N Stationen einen Rahmen senden möchte
~~ Overhead: eine Konkurrenzperiode für alle N Frames, jeweils 1 Bit

$$E = \frac{d}{d + 1} \approx 1$$

- nur eine Station möchte einen Frame senden
~~ Overhead: eine Konkurrenzperiode für 1 Frame, d.h. N Bit

$$E = \frac{d}{d + N}$$

Kollisionsfreie Protokolle – Binärer Countdown

- Nachteil Bitmusterprotokoll: pro Station wird eine 1 Bit Information als Overhead übertragen – führt bei vielen Stationen zu Verzögerungen
 - beim binären Countdown erhält je Station eine Nummer (Nummern haben in binärer Darstellung alle die gleiche Länge)
 - sendewillige Stationen senden per Broadcast jeweils 1 Bit ihrer Nummer, mit dem höchstwertigsten beginnend
 - alle Stationen, die eine 1 an der gerade aktuellen Stelle sehen und dort selber eine Null haben, geben auf
- | | Bitzeit |
|---------|---------|
| 0 0 1 0 | 0 - - - |
| 0 1 0 0 | 0 - - - |
| 1 0 0 1 | 1 0 0 - |
| 1 0 1 0 | 1 0 1 0 |
- Ergebnis: 1 0 1 0
- Die Stationen 0010 und 0100 erkennen diese 1 und geben auf
- Station 1001 erkennt diese 1 und gibt auf

Kollisionsfreie Protokolle – Binärer Countdown

- Binärer Countdown ist ebenfalls ein Reservierungsprotokoll
- Overheadberechnung:
 - insgesamt N Stationen
 - wenigstens eine Station möchte senden
 - Konkurrenzperiode hat eine Länge von $\log_2 N$

$$E = \frac{d}{d + \log_2 N}$$

Kollisionsfreie Protokolle – Binärer Countdown

- Binärer Countdown nutzt Prioritäten (Wert der Stationsnummer)
- eine hohe Adresse wird immer bevorzugt
- d.h. Stationen mit niedrigen Adressen können "verhungern"
- mögliche Abhilfe (Vorschlag von Mok und Ward)
 - Wechsle die Adressen der Stationen automatisch, d.h. Adressen der Stationen sind virtuell
 - wenn von Station A ein Frame gesendet wurde, bekommt A anschließend die virtuelle Nummer 0
 - virtuelle Stationsnummern aller Stationen, die vorher kleinere virtuelle Nummer als Station A hatten, werden um 1 inkrementiert

Beispiel: Binärer Countdown (nach Mok und Ward)

- aktuell seien Stationen nach virtuellen Nummern wie folgt angeordnet: C, H, D, A, G, B, E, F;
virtuelle Nummer 7, 6, 5, 4, 3, 2, 1 und 0
- höchste virtuelle Adresse gewinnt
- Station D möchte senden
- nach dem Senden erhält D die virtuelle Nummer 0
- Stationen mit kleinerer Nummer als 5 "rücken auf"
- Reihenfolge geordnet nach virtuellen Stationsnummern dann: C, H, A, G, B, E, F, D

Zugriff im WLAN

- Bisher betrachtet: Protokolle für kabelgestützte Netzwerke
 - CSMA, CSMA/CD
- für Drahtlose Netzwerke benötigen wird andere, speziellere Zugriffsprotokolle
 - MACA = Multiple Access Collision Avoidance
 - MACAW = MACA for Wireless
- zugehörige Technologien sind im Standard IEEE 802.11 beschrieben (später)

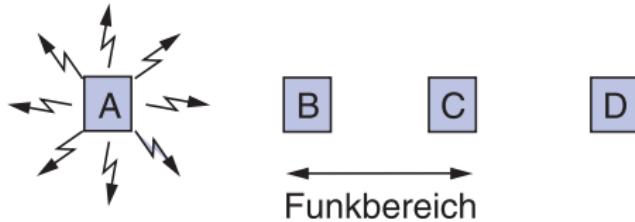
Zugriff im WLAN

- Warum kann CSMA oder CSMA/CD nicht im Wireless LAN angewendet werden?
 - hier ist der Träger die Luft, dieses Medium kann nicht so ohne weiteres abgehört werden
 - bei kabelgebundenen Netzwerken erreicht das Signal alle angeschlossenen Stationen, d.h. Signale werden überall "gehört"
 - Funkwellen haben nur eine begrenzte Reichweite, d.h. es ist nicht möglich, Signale aller anderen Stationen zu überwachen
- Warum interessieren Signale, die nicht überwacht werden können?

Zugriff im WLAN

■ 1. Problem: Hidden Station Problem

- z.B. könnte es sein, dass ein potenzieller Sender A eine bereits sendende Station C nicht bemerkt (außer Reichweite) \rightsquigarrow Carrier Sense würde daher das Senden erlauben
- der Empfänger B liegt aber in Reichweite von C, d.h. es kommt zur Kollision beim Empfänger
- weder Sender A noch C würden diese Kollision bei CSMA mitbekommen

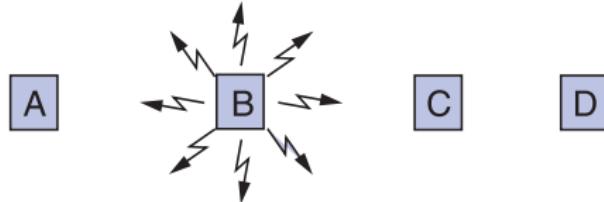


Graphik aus Tanenbaum, Wetherall: Computernetzwerke

Zugriff im WLAN

■ 2. Problem: Exposed Station Problem

- nun soll Station B an Station A senden
- C tastet den Kanal ab und erkennt ihn als belegt, schließt daraus, dass sie nicht an D senden darf
- die Sendung von C nach D würde aber nur die Zone zwischen B und C beeinflussen, nicht die zwischen A und B, daher wäre die Sendung möglich



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

Zugriff im WLAN

- Problem von CSMA im WLAN:
 - eine Station, die Kanal abhört, registriert nur Aktivität in der Umgebung des Senders
 - aber: für eine erfolgreiche Versendung ist die Aktivität in Umgebung des Empfängers von gleicher Bedeutung
- Lösungsansatz
 - bevor ein großes Datenpaket gesendet wird, wird der Empfänger aufgefordert, einen kleinen Datenrahmen zu senden (CTS)
 - Stationen in der Nähe des Empfängers registrieren das CTS und senden nicht während der eigentliche Datenrahmen versendet und empfangen wird
- Ansatz ist im MACA Protokoll verwirklicht

MACA – Multiple Access Collision Avoidance

- Ausgangssituation:

Station A möchte Datenrahmen an Station B senden

- falls A den Kanal in der eigenen Umgebung als frei erkennt wird ein kurzer Rahmen "Request to Send" (RTS) als Anfrage an B gesendet
- RTS enthält unter anderem Information über die Menge der eigentlich zu sendenden Daten
- Station B empfängt RTS Signal
- Station B antwortet seinerseits mit "Clear to Send" (CTS) Signal
- CTS Signal enthält ebenfalls die Information zur Datenmenge, die A senden möchte
- A erhält das CTS
- A sendet den Datenrahmen

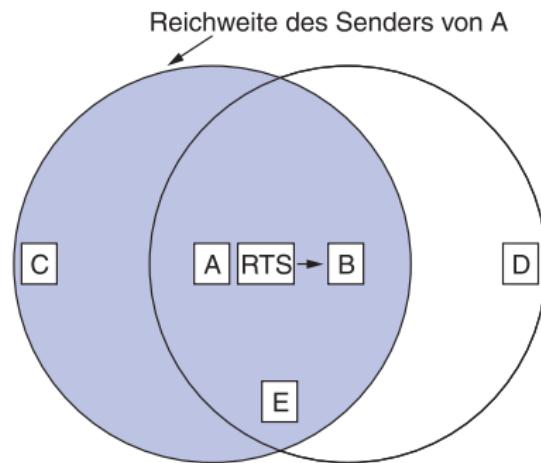
MACA – Multiple Access Collision Avoidance

Bedeutung der RTS und CTS Signale:

- RTS
 - Stationen, die RTS hören befinden sich in Nähe eines zukünftigen Senders
 - Stationen müssen solange "schweigen", bis das zugehörige CTS Signal zurückgekommen ist
- CTS
 - Stationen, die CTS hören befinden sich in Nähe eines Empfängers
 - Stationen müssen während der folgenden Datenübertragung schweigen
 - die zu übertragende Datenmenge (Größe des Rahmens) kann aus RTS bzw. CTS entnommen werden

MACA – Multiple Access Collision Avoidance

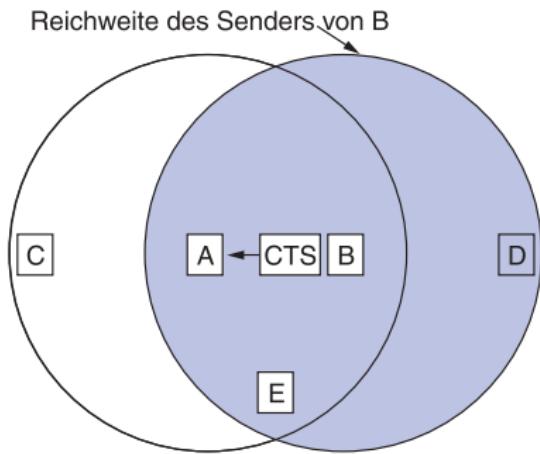
- C befindet sich innerhalb Bereich von A aber nicht im Bereich von B
- C hört RTS von A, aber nicht CTS von B
- solange CTS nicht gestört wird, kann C gleichzeitig senden



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

MACA – Multiple Access Collision Avoidance

- D befindet sich innerhalb Bereich von B aber nicht im Bereich von A
- D hört nur das CTS von B, aber nicht das RTS von A
- D hält sich zurück, bis der erwartete Datenrahmen empfangen wurde
- E hört beide Signale und muss ebenfalls stillhalten.



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

MACA – Multiple Access Collision Avoidance

- Kollisionen: falls zwei RTS Signale gleichzeitig gesendet werden
 - in diesem Fall warten beide Stationen, die RTS gesendet hatten, eine zufällige Zeit
 - Zeit wird nach dem "binären exponentiellen Back–Off" Algorithmus bestimmt (siehe später bei 802.3 Standard)
- MACAW (Multiple Access Collision Avoidance Wireless)
 - Verlust von Rahmen in MACA wird spät erkannt (höhere Schichten) \rightsquigarrow MACAW fügt ein ACK (Acknowledgement) Signal ein
 - mittels CSMA kann häufig vermieden werden, dass zweite Station RTS sendet, wenn bereits andere beim Senden des RTS ist
 - Back-off Algorithmus wird zur Erhöhung der Fairness getrennt für jeden Datenstrom (Quell/Zielpaar) angewendet
 - Austausch von Informationen zur Flußkontrolle

Kapitel 3.3:

IEEE 802 Standards

IEEE 802 Standards für LANs

Token Ring 802.5

Ethernet 802.3

Wireless LAN 802.11

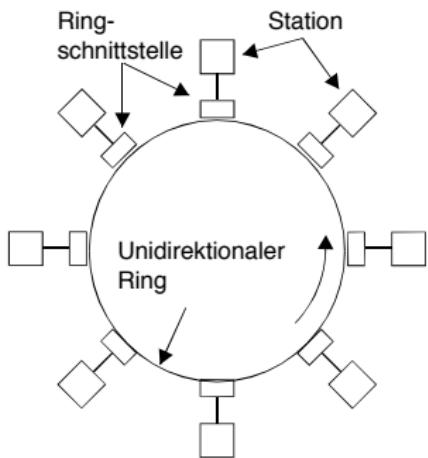
IEEE 802 Standards für LANs

Token Ring 802.5

(nicht prüfungsrelevant, zum Selbststudium für Interessierte)

IEEE 802.5 – Token Ring

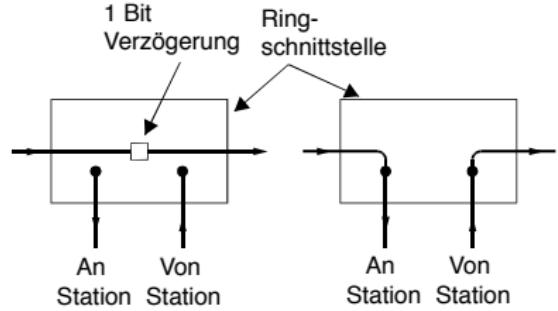
- der Token Ring ist ein unidirektonaler Ring
- die Ringschnittstellen sind mit Punkt-zu-Punkt Kabeln mit den Stationen verbunden
- Stationen dürfen nur Senden, wenn sie das Token (ein spezielles Bitmuster) vom Ring genommen haben
- damit keine Konkurrenzphase notwendig
- Zugriffsverfahren ist damit vorhersagbar (deterministisch)



Graphik aus A. Tanenbaum, Computernetze

IEEE 802.5 – Token Ring

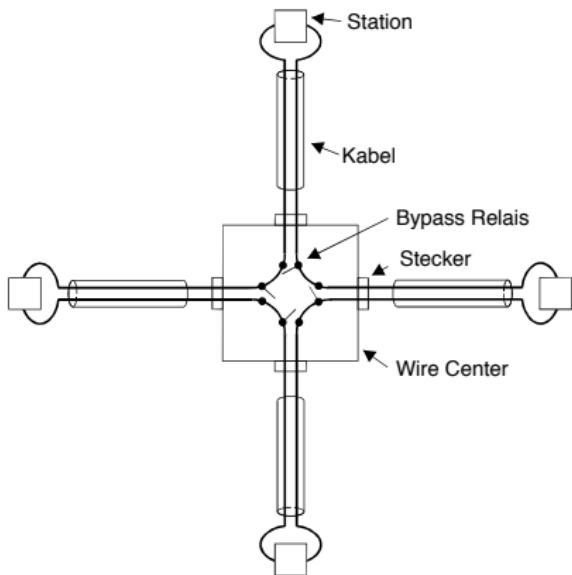
- Stationen können im Lesemodus oder im Sendemodus sein
- im Lesemodus werden die eingelesenen Bits zum Ausgang kopiert, damit Verzögerung um 1 Bit
- in den Sendemodus wird nur nach Erlangen des Tokens geschaltet
 - Schnittstelle unterbricht Verbindung zwischen Ein- und Ausgang
 - Station übergibt eigene Daten an den Ring



Graphik aus A. Tanenbaum, Computernetze

IEEE 802.5 – Token Ring

- Problem eines physikalischen Rings: Ausfall einer Verbindung legt gesamten Ring lahm
- potentielle Schwachstellen sind die Stationsanschlüsse
- Anschluss daher über Wire-Center und Punkt-zu-Punkt Kabel
- Stationen werden über Bypass Relais in den Ring eingeklinkt
- als Leitungscodierung wird differentielle Manchestercodierung verwendet



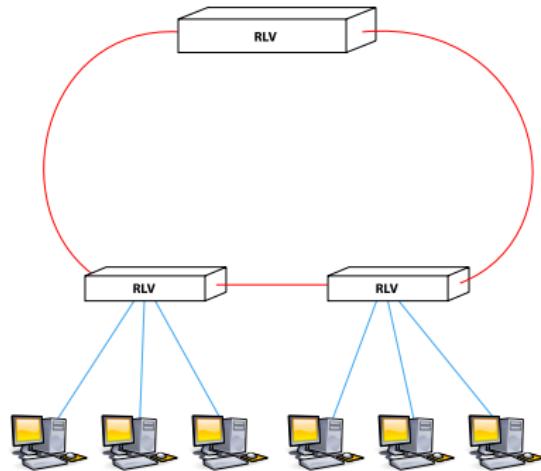
Graphik aus A. Tanenbaum, Computernetze

IEEE 802.5 – Physikalischer Aufbau

- Ringleitungsverteiler (MAU – Media Access Units) sind zu Ring zusammengeschaltet
- einzelne Stationen werden über Twisted Pair in den Ring eingebunden

Ringleitungsverteiler (RLV)

- Typ-1-Kabel oder Glasfaser
- Twisted Pair



IEEE 802.5 – Physikalischer Aufbau

- physikalische Topologie damit ein Stern
- Stationen durch "Hin–" und "Rückleitung" eingebunden
- dadurch logisch ein Ring



IEEE 802.5 – Zugriffsverfahren

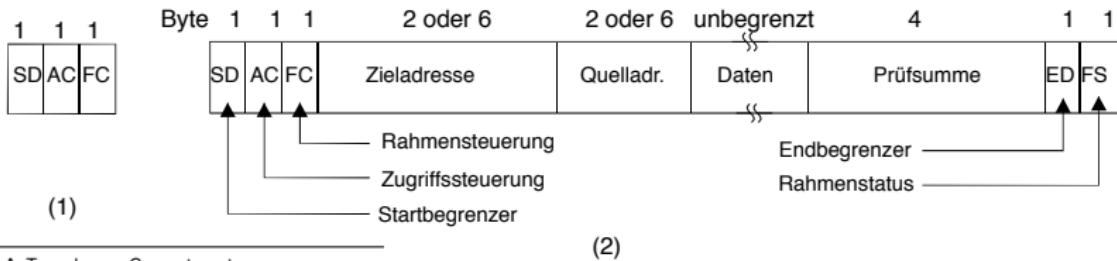
- eine sendewillige Station wartet das Token auf dem Ring ab
- Token wird vom Ring genommen in einem Bit verändert, und als Beginn eines Senderahmens verwendet, d.h. die eigenen Daten werden an das Token angeschlossen
- ist eine Nachricht auf dem Ring vergleichen alle Stationen ihre eigene Adresse mit der Empfängeradresse
 - Adressen stimmen überein: Empfänger kopiert Rahmen in eigenen Eingangspuffer
 - Adressen stimmen nicht überein: Rahmen wird weitergeleitet
- in jedem Fall kommt Nachricht wieder beim Sender an
- Sender entfernt Nachricht und gibt neues Token oder weiteren Rahmen auf den Ring
- Token Haltezeit ist begrenzt (10 ms), d.h. nächste Station kann in Besitz des Tokens kommen

IEEE 802.5 – Token Ring

- das Token besteht aus 3 Byte:

SD=Start Delimiter, AC=Acess Control, ED=End Delimiter

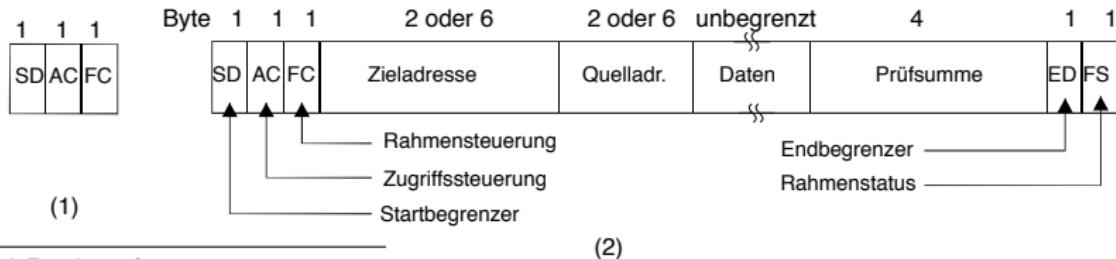
- AC Byte enthält ein Tokenbit T (Bit 4); T=0 Frei-Token; T=1 Rahmen
- weiter enthält AC ein Monitorbit und drei Bits zur Prioritätenvergabe



Graphik aus A. Tanenbaum, Computernetze

IEEE 802.5 – Token Ring

- Datenrahmen enthält ein Byte FS=Framestatus
- hier u.a. zwei Bits A und C, an denen der Sender erkennen kann, ob Rahmen vom Empfänger akzeptiert wurde
- A=0, C=1: Ziel nicht vorhanden oder ausgeschaltet,
A=1, C=0: Ziel vorhanden aber Rahmen nicht akzeptiert,
A=1, C=1: Ziel vorhanden und Rahmen kopiert



Graphik aus A. Tanenbaum, Computernetze

IEEE 802.5 – Ringüberwachung

- jeder Token Ring hat eine ausgezeichnete Station, die Ring überwacht ↳ Monitorstation
- fällt aktuelle Monitorstation aus, wird über ein Konkurrenzprotokoll eine andere Station zum Monitor (jede Station kann die Aufgabe übernehmen)
- Aufgaben der Monitorstation
 - dafür sorgen, dass Frei Token nicht verlorengeht
 - Ring von Rahmenbruchstücken säubern
 - kreisende Rahmen entfernen

IEEE 802 Standards für LANs

Ethernet 802.3

Ethernet 802.3 – Kabelarten

Name	Kabelart	max. Segmentlänge	max. Knoten pro Segment
10Base5	Dickes Koaxkabel (Yellow Cable)	500 m	100
10Base2	Dünnes Koaxkabel	185 m	30
10Base-T	Twisted Pair	100 m	1024
10Base-F	Lichtwellenleiter	2000 m	1024

Bezeichnung:

10 = Geschwindigkeit in MBit/sec

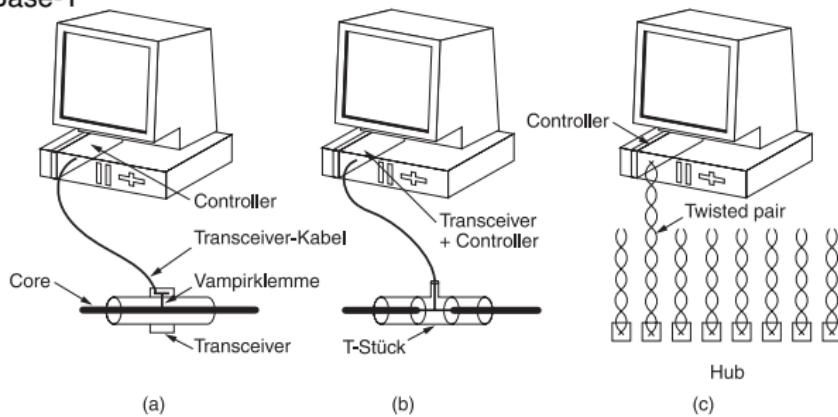
Base = Basisband

5, 2 = max. Länge in 100m

-T/F = Kabelart

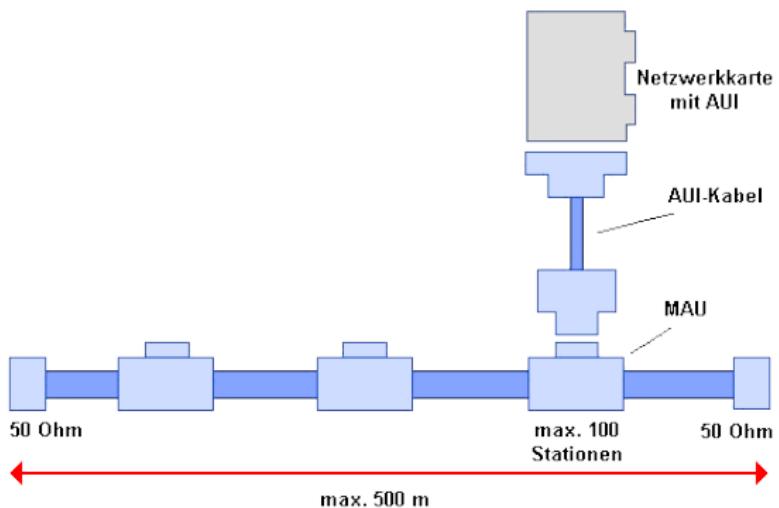
Ethernet 802.3 – Kabelarten

- a) Schema 10Base5
- b) Schema 10Base2
- c) Schema 10Base-T



Graphik aus A. Tanenbaum, Computernetze

Ethernet 802.3 – 10 Base5

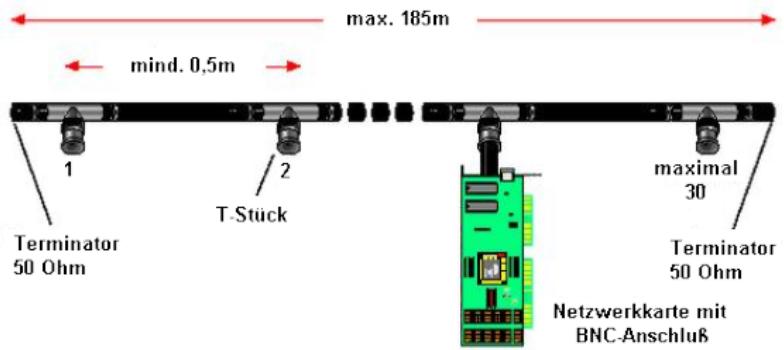


Yellow Cable Transceiver



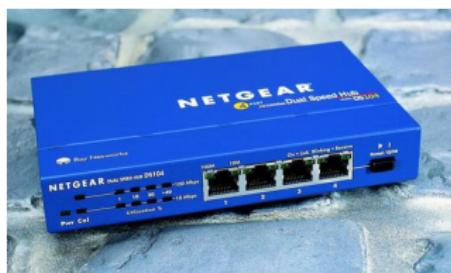
10Base-T Transceiver für 10Base5
Netzwerkarte

Ethernet 802.3 – 10 Base2



BNC Repeater

Ethernet 802.3 – 10 Base-T / 10 Base-F



10Base-T Hub



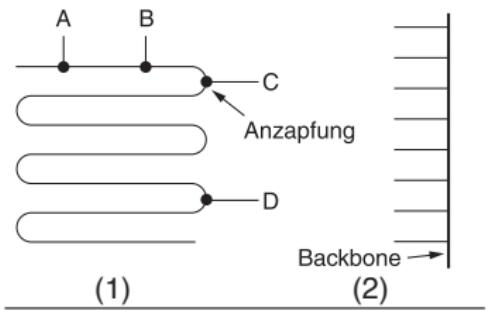
Medienkonverter
TwistesPair → LWL



Switch mit 10Base-T und 10Base-F Modul

Ethernet 802.3 – Netzarten

1. ein einzelnes Kabel bildet das Netzwerk
 - Stationen sind direkt an der nächstmöglichen Anzapfung angeschlossen
 - 10Base5 oder 10Base2 können so betrieben werden



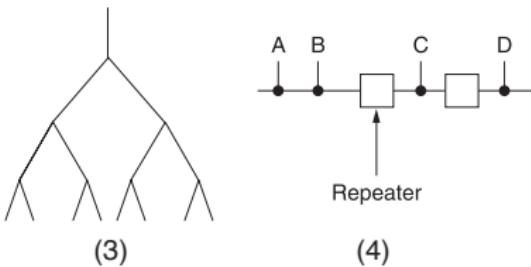
Graphik aus A. Tanenbaum, Computernetze

2. Backboneverbindung zwischen Etagennetzwerken
 - Backbone bildet vertikalen Strang
 - an diesen sind die horizontalen Stränge über Repeater angeschlossen
 - klassischerweise 10Base5 (wegen Länge) aber auch 10Base2 möglich

Ethernet 802.3 – Netzarten

3. Allg. Topologie als Baumstruktur

- Stationen dürfen nicht durch zwei Pfade verbunden sein
- 10Base-T kann als solche Struktur interpretiert werden



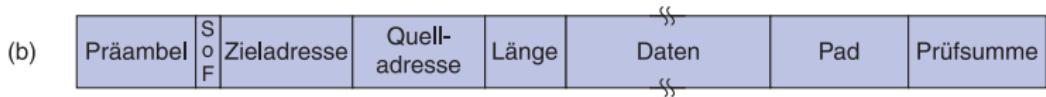
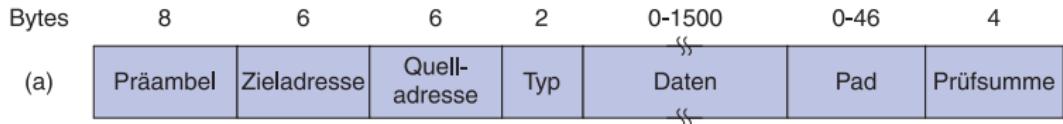
Graphik aus A. Tanenbaum, Computernetze

4. Verbindung von Segmenten mittels Repeatern

- Repeater arbeitet auf Bitübertragungsebene
- regeneriert und verstärkt das Signal in beide Richtungen
- für höhere Schichten transparent, d.h. alle Segmente wirken als Ganzes
- maximal 5 Segmente und 4 Repeater erlaubt ~ Länge 2.500 m

Ethernet 802.3 – Rahmenformat

- a) DIX–Rahmenformat
- b) IEEE 802.3 Rahmenformat



- wesentlicher Unterschied liegt im Typ bzw. Länge Feld
- Type–Feld: Prozess/Protokoll an den Rahmen zu übergeben ist
- im Ethernet auf höheren Schichten geregelt (siehe später)

Graphik aus Tanenbaum, Wetherall: Computernetzwerke

Ethernet 802.3 – Rahmenformat

PRE	SFD	DA	SA	LE	DATA	PAD	FCS	IFG
7 Byte	1 Byte	2 oder 6 Byte	2 oder 6 Byte	2 Byte	≥ 0 Byte	≤ 46 Byte	4 Byte	\geq 96 Bitzeiten
Gesamt: ≥ 64 Byte (512 Bitzeiten) ≤ 1518 Byte (1 Bitzeit = $0.1\mu\text{sec}$ bei 10MBit/sec)								

- PRE: Präambel; jedes Byte hat Muster 10101010 zur Synchronisation des Taktes für eine Manchester Kodierung
- SFD: Start Frame Delimiter; markiert den eigentlichen Beginn
- DA: Zieladresse (Gerätekennung des Empfängers)
- SA: Quelladresse (Gerätekennung des Senders)
- LE: length; Länge der Nutzdaten des Datenfeldes (≤ 1500 als Länge interpretiert, > 1500 als Typfeld nach DIX Standard)

Ethernet 802.3 – Rahmenformat

PRE	SFD	DA	SA	LE	DATA	PAD	FCS	IFG
7 Byte	1 Byte	2 oder 6 Byte	2 oder 6 Byte	2 Byte	≥ 0 Byte	≤ 46 Byte	4 Byte	\geq 96 Bitzeiten
Gesamt: ≥ 64 Byte (512 Bitzeiten) ≤ 1518 Byte (1 Bitzeit = $0.1\mu\text{sec}$ bei 10MBit/sec)								

- DATA: Nutzdaten, also echte auszuwertende Daten
- PAD: padding bits; sog. Stopfbits, die bei wenigen Nutzdaten den Rahmen künstlich auf 64 Byte Länge ausdehnen
- FCS: frame check sequence; CRC Prüfsumme zur Fehlererkennung, keine Fehlerkorrektur (siehe nächstes Kapitel)
- IFG: inter frame gap; Mindestabstand zum nächsten Rahmen

Daten im Rechner und auf der Leitung

- bei Datenübertragung ist Byte- und Bitordnung zu berücksichtigen
- in Protokollen wird die Netzwerk-Byte-Ordnung festgelegt
- Bytereihenfolge: In welcher Reihenfolge werden die Bytes eines Rahmens auf die Leitung gebracht?
 - Konvention: Byte mit der niedrigen Adresse zuerst
- Bitreihenfolgen: In welcher Reihenfolge werden die Bits eines Bytes auf die Leitung gebracht?
 - Konvention 1: Most Significant Bit First (Big Endian): das im Speicher höchstwertigste Bit kommt zuerst auf die Leitung; z.B. bei FDDI oder Token Ring
 - Konvention 2: Least Significant Bit First (Little Endian): das im Speicher niederwertigste Bit kommt zuerst auf die Leitung; z.B. bei Ethernet

Ethernet 802.3 – MAC Adressen

- MAC Adressen = Media Access Control Adressen
- jede Netzwerkkarte muss eine eindeutige Adresse besitzen
 - Empfänger erkennt daran für ihn bestimmte Frames
- IEEE Standard im 10MHz Basisband nutzt nur die 6 Byte Adressen (MAC-48)
- MAC-48 Adressen werden meist im kanonischer Form (Ethernet format, LSB Format) angegeben (vgl. RFC 2469)

Beispiel: 12-34-56-78-9A-BC

Im Speicher, 12 34 56 78 9A BC
kanonisch: 00010010 00110100 01010110 01111000 10011010 10111100
 1. Bit auf dem LAN
 |

auf LAN: 01001000 00101100 01101010 00011110 01011001 00111101

Im Speicher,
MSB format: 01001000 00101100 01101010 00011110 01011001 00111101
 48 2C 6A 1E 59 3D

Ethernet 802.3 – MAC Adressen

- eine MAC Adresse kann eine lokale oder globale Adresse sein
 - Unterscheidung am 2. Bit auf der Leitung (zweit niederwertigstes Bit im Speicher) \rightsquigarrow G/L Bit
 - globale Adressen sind weltweit eindeutig und von der IEEE vergeben \rightsquigarrow G/L = 0
 - lokale Adressen können vom Netzwerkadministrator vergeben werden \rightsquigarrow G/L = 1
- die ersten 3 Byte der Adresse geben bei einer globalen Adresse den Hersteller an (OUI)
(=Organisation Unique Identifier) Anteil von der IEEE vergeben)
- die letzten 3 Byte vergibt der Hersteller selber

Ethernet 802.3 – MAC Adressen

- 1. Bit (G/I Bit) auf der Leitung legt fest, ob es sich um eine einzelne oder Gruppenadresse handelt
- G/I = 0 \rightsquigarrow einzelne Adresse; G/I = 1 \rightsquigarrow Gruppenadresse
 - über Gruppenadresse (Multicastadresse) als Zieladresse kann Frame an mehrere Empfänger gleichzeitig gesendet werden
 - besondere Gruppenadresse, die nur aus "1" besteht \rightsquigarrow Broadcastadresse
 - Broadcast: Rundsenden eines Frames an alle Stationen im lokalen Netzwerk
 - Broadcasts werden für viele Mechanismen im Netzwerk verwendet
 - Broadcasts dürfen sich nicht beliebig ausbreiten (erzeugen hohe Last) \rightsquigarrow Broadcastdomäne
 - Broadcastdomäne endet an einem Router

Beispiele: MAC Adressen

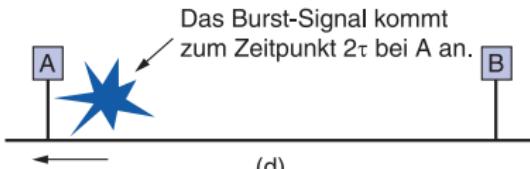
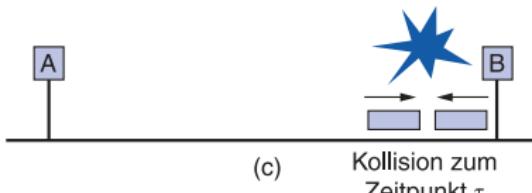
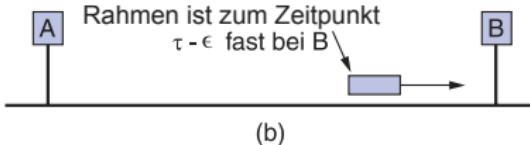
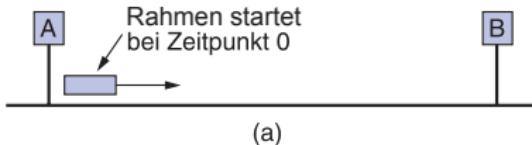
- 6 Byte Adresse mit einem herstellerabhängigen Teil (die ersten 3 Bytes) und einem vom Hersteller zu vergebenden Teil
- herstellerabhängigen Teil vergibt die IEEE \rightsquigarrow Eindeutigkeit
 - 00:60:B0:2B:FE:E9 für einen HP-Printserver
 - F4:AC:C1:17:4B:28 für eine Cisco Komponente
- Aber: bei modernen Karten sind die Adressen nicht mehr fest "eingebrannt" sondern in einem EEPROM gespeichert
- Adresse kann softwaremäßig geändert werden

Ethernet 802.3 – Eigenschaften

- Ethernet nutzt die Kabel als Broadcast Medium
- Zugriffskontrolle erfolgt über den CSMA/CD (Carrier Sense with Collision detection) Algorithmus
- falls das Medium in Benutzung ist, wird ständig überprüft
 - ~~ 1-persistentes CSMA
- bei einer Kollision wird zufällige Zeit gewartet
 - Zeit wird nach dem binären exponentiellen Back-off Algorithmus bestimmt
- Kollisionserkennung hat Einfluss auf Gesamtlänge des Mediums und minimale Framegröße

Ethernet 802.3 – Kollisionen

- Warum ist eine Rahmenmindestgröße von 64 Byte erforderlich?



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

Ethernet 802.3 – Kollisionen

- Station A sendet zum Zeitpunkt 0 einen Rahmen
- zum Zeitpunkt $\tau - \epsilon$ hat die maximal entfernte Station B diesen Rahmen noch nicht gesehen \rightsquigarrow für B erscheint der Kanal frei
- zum Zeitpunkt $\tau - \epsilon$ beginnt B zu senden, es kommt zur Kollision
 - B bricht Sendung ab, erzeugt ein spezielles 48 Bit Burst-Signal
- das Burst-Signal ist erst zum Zeitpunkt 2τ wieder bei A angekommen, erst dann bricht A das Senden ab
- Kanalüberwachung durch A findet nur während der Zeit statt, wo A Rahmen sendet,
 - letztes Bit des kürzesten Rahmens darf A erst nach 2τ verlassen (erstes Bit des Rahmens hat Kollision ausgelöst)

Ethernet 802.3 – Kollisionen

- bei IEEE 802.3 mit 10MBit/sec und 10Base5
 - maximale Entfernung 2500 m inkl. 4 Repeater
- Signallaufzeit 2τ hin und zurück inkl. Verarbeitungszeit in den Repeatern ist $50 \mu\text{sec}$ (oder 500 Bitzeiten) (IEEE Standard legt fest, wie hoch die Verarbeitungszeit in den Komponenten maximal sein darf)
- bei 10 MBit/sec Datentransferrate benötigt ein Bit 100 nsec
- es müssen mind. 500 Bit gesendet werden bis das erste Bit die gesamte Strecke hin und zurück gelaufen ist
- \rightsquigarrow mit etwas Sicherheit wurde kürzester Rahmen auf 512 Bit = 64 Byte festgelegt.
- bei Gigabit-Ethernet müsste der Rahmen 6400 Byte lang sein

Ethernet 802.3 – binärer exponentieller Back–off Algorithmus

- Was geschieht nach einer Kollision?
 - Stationen warten (Back–off)
 - konstante Wartezeit (d.h. insbesondere gleiche Wartezeit für beide Stationen) \rightsquigarrow erneute Kollision
 - daher zufällige Wartezeit nötig
 - aber: falls Wartezeit zu lang, unnötig ineffizient

Ethernet 802.3 – binärer exponentieller Back–off Algorithmus

- Binärer exponentieller Back–off Algorithmus
 - die Round–Trip Signalübertragungszeit 2τ und die minimale Rahmengröße führt zu Zeitschlitten von 512 Bitzeiten
 - 1. Kollision: Stationen wählen Wartezeit aus $\{0, 1\}$ Zeitschlitten
 - 2. Kollision: Stationen wählen Wartezeit aus $\{0, 1, 2, 3\}$ Zeitschlitten
 - i -te Kollision: Stationen wählen Wartezeit aus $\{0, 1, \dots, 2^i - 1\}$ Zeitschlitten
 - nach der 16. Kollision
 - Sendevorschuss wird aufgegeben
 - Fehler wird höheren Protokollen gemeldet

Ethernet 802.3 – Fast Ethernet

Name	Kabel	Max. Segment	Vorteile
100Base-T4	Twisted Pair	100 m	verwendet Cat 3 UTP
100Base-TX	Twisted Pair	100 m	Vollduplex mit 100Mbps
100Base-FX	Glasfaser	2000 m	Vollduplex mit 100Mbps, grössere Entferungen

- Fast Ethernet nutzt Hubs und Switches mit Sternverkabelung
- keine Bustopologie vergleichbar 10Base2 oder 10Base5 möglich
- 100Base-T4 für Nutzung mit Telefonnetzwerk in Gebäuden
- 100Base-TX nutzt eine 4B/5B Leitungskodierung
- 100Base-TX erlaubt bei gleicher minimaler Rahmenlänge von 64 Byte Kabel von maximal 100 m
- 100Base-FX nur in Verbindung mit Switches bei 2000 m möglich

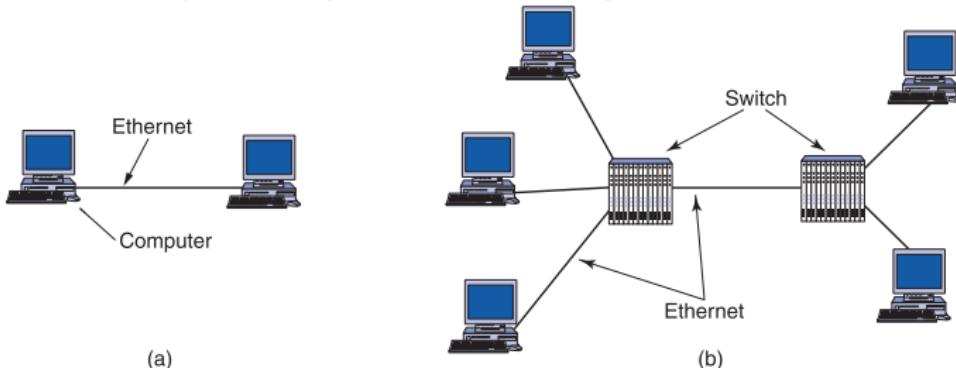
Ethernet 802.3 – Gigabit Ethernet

- Gigabit Ethernet von der IEEE unter 802.3z spezifiziert
- Forderungen
 - kompatibel mit den bisherigen 802.3 Standards
 - insbesondere gleiches Adressierungsschema mit 48 Bit MAC–Adressen
 - gleiche minimale und maximale Rahmenlängen

Name	Kabel	Max. Segm.	Vorteile
1000Base–SX	Glasfaser	550 m	Multimode Faser (50, 62,5 μ)
1000Base–LX	Glasfaser	5000 m	Single (10 μ) oder multimode (50, 62,5 μ)
1000Base–CX	2 Paare STP	25 m	Shielded Twisted Pair
1000Base–T	4 Paare UTP	100 m	Standard Kat 5 UTP

Ethernet 802.3 – Gigabit Ethernet

- Gigabit-Ethernet Verbindungen sind Punkt-zu-Punkt Verbindungen
- entweder zwei Stationen oder mehrere Stationen über Switch
- an einem Kabel sind in jedem Fall genau zwei Geräte angeschlossen



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

Ethernet 802.3 – Gigabit Ethernet

- Gigabit Ethernet unterstützt zwei verschiedene Betriebsmodi
- Vollduplex
 - Datenverkehr jederzeit in beiden Richtungen möglich
 - Verwendung wenn zentraler Switch mit Rechnern oder anderen Switches verbunden ist
 - keine Kanalprüfung erforderlich, Daten können jederzeit gesendet werden und werden gepuffert
 - kein CSMA/CD nötig und damit Kabellänge im Wesentlichen durch Signaldämpfung bestimmt

Ethernet 802.3 – Gigabit Ethernet

- Halbduplex
 - Datentransfer nur in einer Richtung
 - Verwendung, wenn ein Hub zur Verbindung dient (alle Daten werden auf alle Eingänge geschaltet)
 - in diesem Fall muss CSMA/CD verwendet werden
 - da minimales Paket von 64 Byte die Kabellänge auf 25 m begrenzen würde in diesem Fall Rahmenerweiterung auf 512 Byte
 - Carrier Extension: auffüllen der Rahmen auf 512 Byte durch die Hardware; Software bekommt Rahmenänderung nicht mit
 - Frame Bursting: zusammenfassen mehrere Nutzdaten von einem Sender/Empfängerpaar in einen Rahmen

Ethernet 802.3 – 10 Gigabit Ethernet

- 10 GBit Ethernet unterstützt nur Vollduplexbetrieb, d.h. CSMA/CD spielt keine Rolle mehr
- durch Autonegotiation Rückfall auf geringere gemeinsame Geschwindigkeit möglich
- Bei Glasfaserverbindungen wird ein 64B/66B Leitungscode verwendet ~ weniger Overhead
- seit Ende 2007 auch Standardisierungen für 40 GBit und 100 GBit Ethernet im Gange

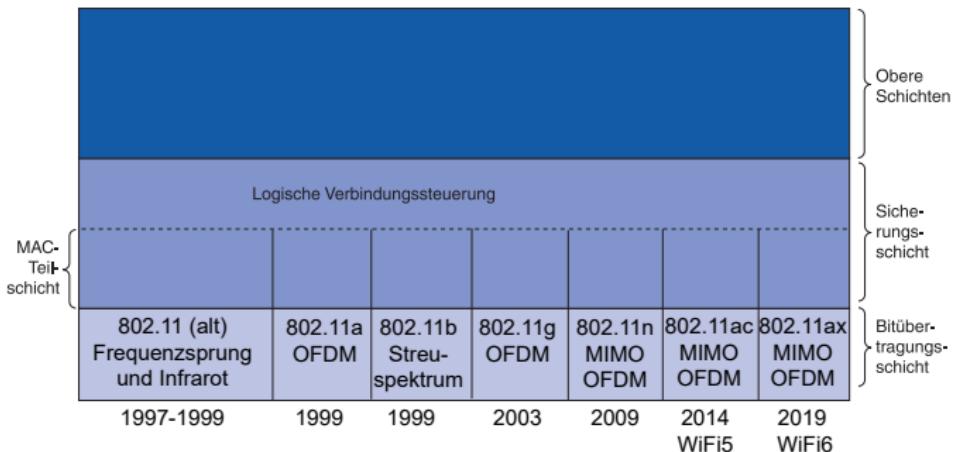
Name	Kabel	Max. Segm.	Vorteile
10GBase-SR	Glasfaser	bis zu 300m	Multimode Faser ($0,85 \mu m$)
10GBase-LR	Glasfaser	10 km	Singlemode Faser ($1.3 \mu m$)
10GBase-ER	Glasfaser	40 km	Singlemode Faser ($1.5 \mu m$)
10GBase-T	4 Paare UTP	100 m	Standard Kat 6a UTP

IEEE 802 Standards für LANs

Wireless LAN 802.11

802.11 – Protokollstapel

- WLAN arbeitet auf der Bitübertragungsschicht mit verschiedenen Standards
- Unterschied in den Modulationstechniken, aber insb. in den Frequenzbändern und Geschwindigkeiten



802.11a

- 802.11a nutzt OFDM (Orthogonal Frequency Division Multiplexing)
 - Datenübertragungsrate 54 MBit/sec
 - nutzt das 5 GHz Band
 - insgesamt 52 Kanäle, 4 zur Synchronisation
 - viele Kanäle können parallel auf verschiedenen Frequenzen genutzt werden
 - 216 Datenbit werden als 288 Bit kodiert

802.11b/g

- 802.11b nutzt HR-DSSS (High Rate Direct Sequence Spread Spectrum)
 - nutzt das 2.4 GHz ISM Band
 - Übertragungsraten 1, 2, 5.5 und 11 MBit/s
 - nutzt 1MBaud mit 1 bzw. 2 Bit pro Baud bzw. 1,375 MBaud bei 4 bzw. 8 Bit pro Baud mittels Walsh/Hadamard Code
 - Datenrate kann dynamisch an Last- und Rauschbedingungen angepasst werden
 - Reichweite ca. 7 mal höher als bei 802.11a
- 802.11g als verbesserte Version von 802.11b mittels OFDM
 - Datenrate mit 54 MBit/sec vergleichbar mit 802.11a
 - nutzt das 2.4 GHz Band, damit kompatibel zu 802.11b

802.11n

- 802.11n ist im 2.4 und 5 GHz Band verfügbar
- Die Kanalbreite wurde von 20 MHz auf 40 MHz verdoppelt
- Es nutzt die sog. MIMO (Multiple Input Multiple Output) Technik
 - Es werden mehrere (2-4) parallele Datenströme verwendet
 - Dazu sind mehrere (2-4) Sende- und Empfangsantennen nötig
 - Pro Datenstrom werden 150 MBit/sec (brutto) erreicht, d.h. bei 4 Antennen max. 600 MBit Datenrate
- Verbreiteste Datenrate ist 300 MBit/sec

802.11ac / WiFi-5

- 802.11ac ist nur im 5 GHz Band verfügbar
- Kanalbreiten von 80 MHz und 160 MHz möglich
- MIMO (Multiple Input Multiple Output) Technik mit bis zu acht MIMO Verbindungen
- Höhere Modulationsstufen bei sehr gutem Empfang
- Theoretisch bis zu 6936 MBit/sec möglich

802.11ax / WiFi-6

- 802.11ax ist sowohl im 2.4 als auch im 5 GHz Band verfügbar
- Kanalbreiten bis zu 160 MHz möglich
- MU-MIMO (Multi User Multiple Input Multiple Output) Technik mit bis zu acht MIMO Verbindungen
- nochmal Erhöhung der Modulationsstufen
- Datenraten bis 11 GBit/sec möglich

802.11be / WiFi-7

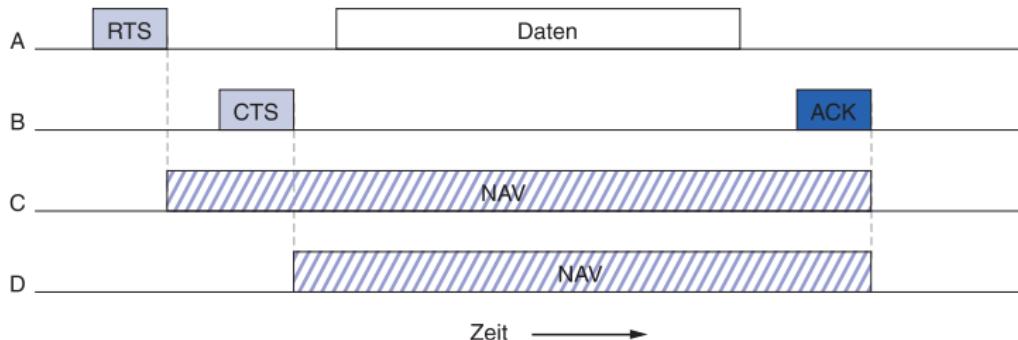
- 802.11be ist sowohl im 2.4 als auch im 5 GHz Band verfügbar, zusätzlich neues 6 GHz Band.
- spezifiziert seit 2024
- Kanalbreiten bis zu 320 MHz möglich
- MLO (Multi Link Operation): Senden und empfangen gleichzeitig über verschiedene Frequenzen
- Datenraten theoretisch bis 23 GBit/sec möglich

802.11 MAC Sublayer Protokoll

- 802.11 unterstützt zwei Betriebsmodi
 - DCF (Distributed Coordination Function): Verteilte Koordinierungsfunktion, keine ausgezeichnete Station, vergleichbar mit Ethernet
 - PCF (Point Coordination Function): verwendet die Basisstation zur Steuerung in einer Zelle
- der DCF Modus nutzt CSMA mit Kollisionsvermeidung (CA)
 - CSMA/CA basiert auf dem MACAW Protokoll
 - es nutzt RTS/CTS Signale
 - Protokoll nutzt Carrier Sense (CS) zur Vermeidung von Kollisionen der RTS Signale
 - CSMA/CA kann Kollisionen nicht vollständig vermeiden
 - nach Kollision wird nach binärem exponentiellen Back-Off gewartet

802.11 – Kanalprüfung

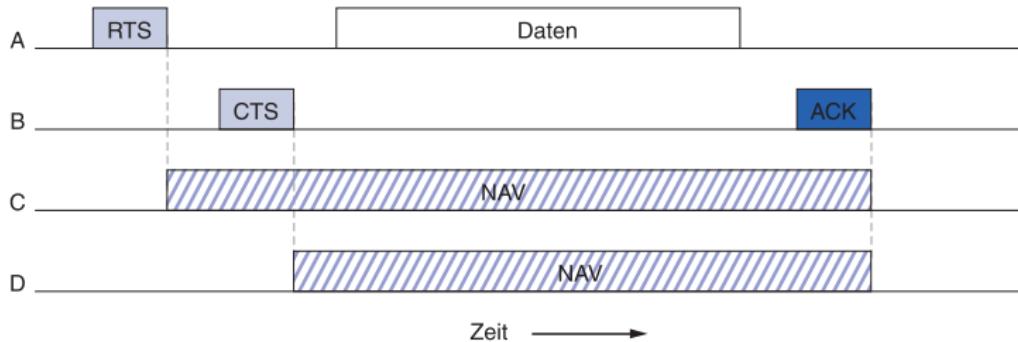
- mittels RTS/CTS wird der Kanal geprüft und belegt
- nach Senden der Daten wird ACK Timer gestartet
- falls Timer abläuft ohne das Empfänger ACK sendet \leadsto Protokoll läuft erneut ab



Graphik aus Tanenbaum, Wetherall: Computernetzwerke

802.11 – Kanalprüfung

- Stationen die RTS oder CTS hören, halten sich zurück
- aktivieren für sich selbst ein NAV "Signal" (Network Allocation Vector)
- kein wirkliches Signal, zeigt der Station (hier C und D) belegten Kanal an; endet beim zugehörigen ACK



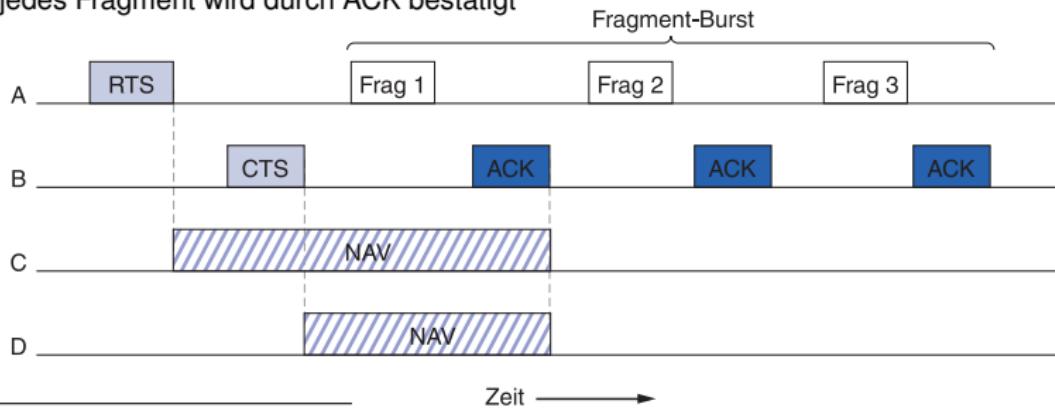
Graphik aus Tanenbaum, Wetherall: Computernetzwerke

802.11 MAC Sublayer Protokoll

- drahtlose Netzwerke sind mit stärkerem Rauschen behaftet als kabelgebundene Netzwerke
- Wahrscheinlichkeit von Bitfehlern steigt
- ist p die Wahrscheinlichkeit eines Einzelbitfehlers und n die Rahmenlänge \rightsquigarrow Wahrscheinlichkeit für korrekt gesendeten Rahmen ist $(1 - p)^n$
- Wahrscheinlichkeit, dass lange Rahmen fehlerfrei ankommen sinkt
- Beispiel: Etherenetrahmen der Länge 12.144 Bit
 - $p = 10^{-4} \Rightarrow$ Wahrscheinlichkeit für korrekten Rahmen 30 %
 - $p = 10^{-5} \Rightarrow$ Wahrscheinlichkeit für korrekten Rahmen 90 %
 - $p = 10^{-6} \Rightarrow$ Wahrscheinlichkeit für korrekten Rahmen 99 %
 - auch im letzten Fall noch 12 falsche Rahmen pro Sekunde

802.11 MAC Sublayer Protokoll – Fragment Burst

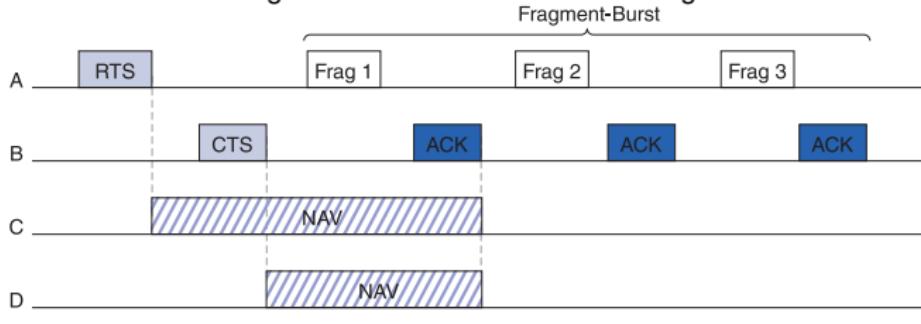
- 802.11 nutzt wegen der höheren Rauschempfindlichkeit sog. Fragment–Bursts
 - Rahmen werden in mehrere Fragmente aufgeteilt, die eigene Prüfsumme besitzen
 - jedes Fragment wird durch ACK bestätigt



Graphik aus A. Tanenbaum, Computernetze

802.11 MAC Sublayer Protokoll – Fragment Burst

- nur fehlerhafte Fragmente werden neu gesendet
- Fragmentgröße ist Parameter einer Funkzelle, die von Basisstation vorgegeben wird
- NAV Signal bei nicht beteiligten Stationen bis zum ersten ACK
- keine erneute Kanalreservierung durch RTS/CTS für weitere Fragmente

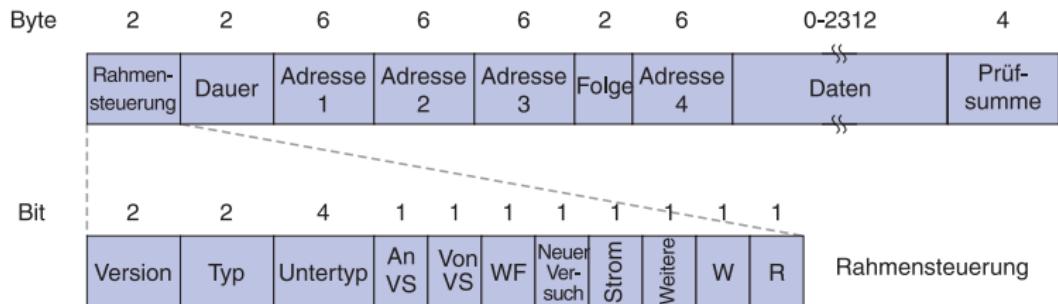


Graphik aus A. Tanenbaum, Computernetze

Zeit →

802.11 MAC Sublayer Protokoll – Rahmenstruktur

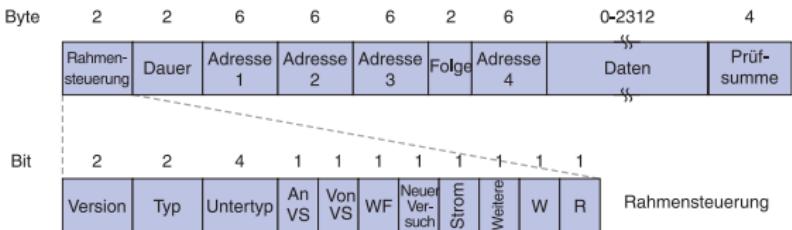
- 802.11 definiert drei Arten von Rahmen: Daten-, Steuerungs- und Verwaltungsrahmen
- Der Datenrahmen ist der umfangreichste
 - die ersten 2 Byte des Headers dienen zur Rahmensteuerung



Graphik aus A. Tanenbaum, Computernetze

802.11 MAC Sublayer Protokoll – Rahmenstruktur/Rahmensteuerung

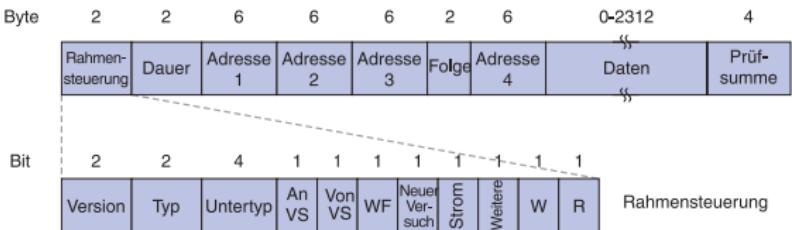
- *Protokollversion*: erlaubt zwei verschiedene Versionen in einer Zelle
- *Typ*: Daten-, Steuer- oder Verwaltungsrahmen
- *Untertyp*: CTS oder RTS
- *AnVS* und *VonVS*: Rahmen an oder von Verteilungsnetzwerk (z.B. Ethernet) zwischen Funkzellen
- *WF*: weitere Fragmente folgen



Graphik aus A. Tanenbaum, Computernetze

802.11 MAC Sublayer Protokoll – Rahmenstruktur/Rahmensteuerung

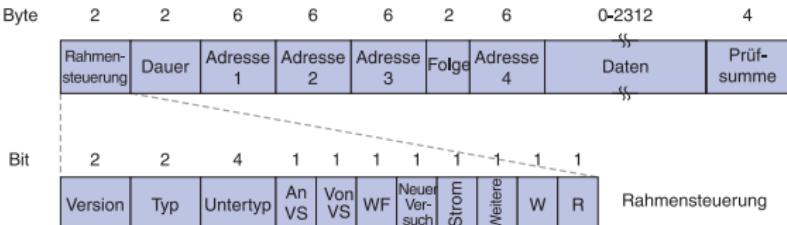
- *NeuerVersuch*: Rahmen wird erneut übertragen
- *Strom*: von Basisstation verwendet um Empfänger in Ruhezustand zu versetzen bzw. zu aktivieren
- *Weitere*: Sender hat weitere Rahmen für den Empfänger
- *W*: Rahmenhauptteil mittels WEP verschlüsselt
- *R*: Rahmenfolge muss in Reihenfolge verarbeitet werden



Graphik aus A. Tanenbaum, ComputerNetze

802.11 MAC Sublayer Protokoll – Rahmenstruktur

- **Dauer:** wie lange belegen Rahmen und Bestätigung den Kanal \rightsquigarrow NAV Mechanismus
- **Adressen 1-4:** IEEE 802 Adressen für Sender und Empfänger sowie für die zwei ggf. beteiligten Basisstationen
- **Folge:** Nummerierung von Fragmenten: 12 Bit zur Rahmenidentifikation, 4 Bit für Fragmentnummer
- **Daten:** bis zu 2.312 Byte Nutzdaten
- **Prüfsumme:** Erkennung von Bitfehlern



Graphik aus A. Tanenbaum, Computernetze

Kapitel 3.4:

Netzwerkkoppelung auf Sicherungsschicht

Link Layer vs. Network Layer LAN Koppelung

- im Moment besprechen wir die Verknüpfung von LANs auf der Sicherungsschicht (Schicht 2)
- später: Verbindung von LAN über die Netzwerk-Schicht (Schicht 3) (Routing)
- Unterschiede: Sicherungsschicht
 - Verbindung auf Sicherungsschicht bedeutet Verbindung von LANs der gleichen Organisation
 - LAN ist iAllg. logisch eine Einheit
- Netzwerkschicht
 - Verbindung auf Netzwerkschicht verbindet LANs die räumlich weit entfernt liegen
 - jedes LAN ist ein eigenständiges Netzwerk
 - Verbindung zwischen unterschiedlichen Netzwerken

LAN Koppelung auf Sicherungsschicht – Gründe

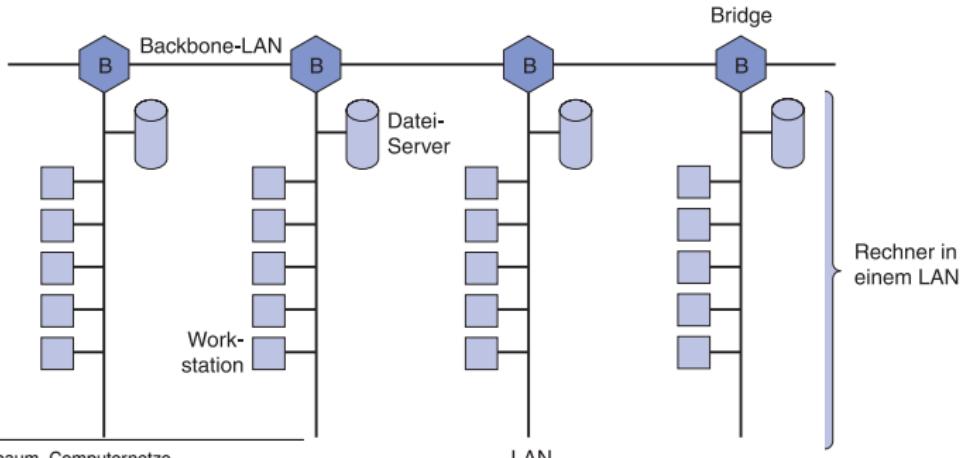
- Größe
 - Anzahl der Stationen ist zu groß für ein LAN
 - Stationen müssen die Bandbreite teilen
 - Anzahl der Ports an einem Koppelungselement nicht möglich
- Ausfallsicherheit
 - falls ein LAN ausfällt (z.B. Sternkoppler fällt aus) sind die anderen weiter funktionsfähig
- Zugriffssicherheit
 - LANs nutzen Broadcast Medien, d.h. Kommunikation kann abgehört werden

LAN Koppelung auf Sicherungsschicht

- Lasttrennung
 - häufig ist ein Großteil der Last auf ein Teilnetz beschränkt
 - andere Teilnetze sollten diese Last nicht "sehen" (insbesondere bei Broadcast Netzwerken)
- unabhängige Implementation von Teilnetzen
 - Teilnetze werden häufig lokal implementiert
 - später ergibt sich die Notwendigkeit des übergreifenden Zugriffs

Backbone

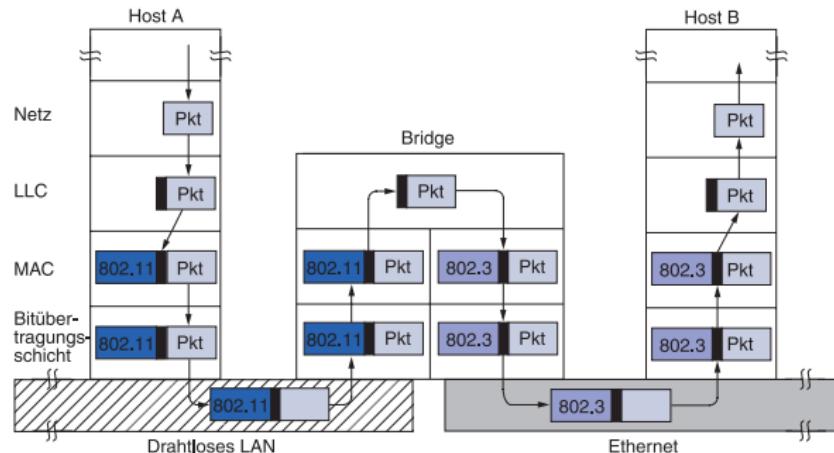
- mehrere LANs können durch ein Backbone und Bridges miteinander verbunden werden
- Bridges prüfen die Sicherungsschichtadressen und leiten Rahmen weiter



Graphik aus A. Tanenbaum, Computernetze

802.x Bridges

- Bridges können auch verschiedenartige Netzwerke miteinander verbinden
- Problem: Rahmen müssen angepasst werden



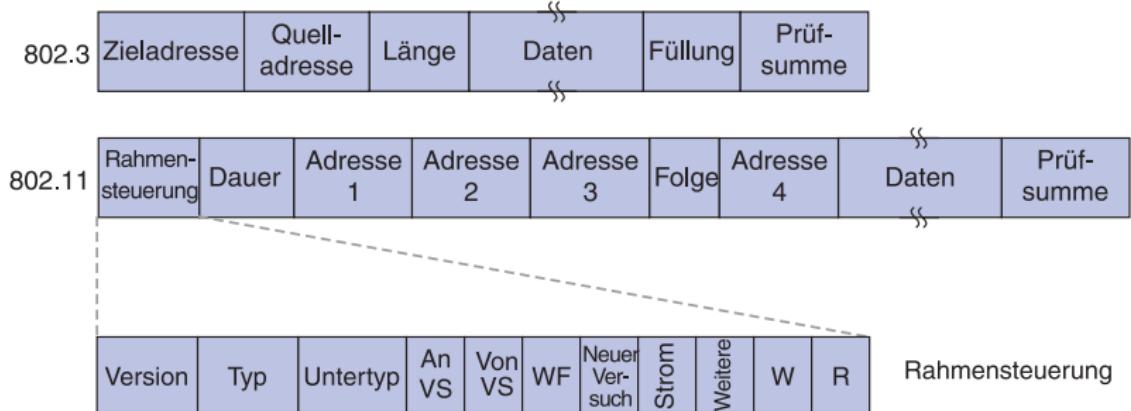
Graphik aus A. Tanenbaum, Computernetze

Bridges von 802.x in 802.y Netze

- Bridging von 802.x in 802.y Netze ist iAllg. schwierig
- Unterschiedliche Netzwerk Geschwindigkeiten
 - A sendet auf einem 1000 BaseT Ethernet an Station B
 - B ist in ein 10BaseT-Ethernet eingebunden
 - die Bridge muss die Daten puffern
 - Puffer laufen aber ggf. über, d.h. Rahmen gehen verloren
- Unterschiedliche Größen der Nutzlastfelder
 - A sendet aus einem 802.5 Netzwerk mit Nutzlast von z.B. 8.192 Byte (Nutzlast variabel); B empfängt in einem 802.3 Netzwerk ⇔ hier Begrenzung auf 1.500 Byte Nutzlast
 - Fragmentierung der Rahmen auf Sicherungsschicht nicht vorgesehen
- Unterschiedliche Rahmenformate

Rahmenformate von 802.3 und 802.11

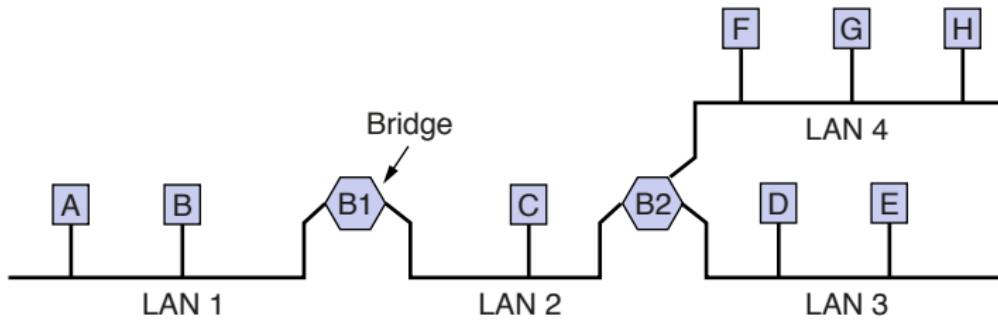
- Probleme der unterschiedlichen Rahmenformate zeigt der Vergleich von 802.3 und 802.11 Rahmen
- Bridge muss ggf. die fehlende Headerinformation erzeugen



Graphik aus A. Tanenbaum, Computernetze

Transparente Bridges im lokalen Netz

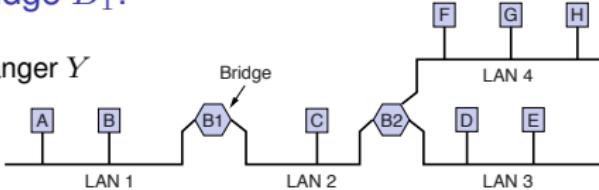
- Beispiel einer Konfiguration mit 4 LANs und 2 Bridges
- eine Bridge (Multiportbridge) kann mehrere Netzwerke anschließen



Graphik aus A. Tanenbaum, Computernetze

Voraussetzung: ein Rahmen erreicht eine Bridge B_1 :

- der Rahmen hat einen Sender X und einen Empfänger Y
- der Sender X befindet sich im LAN L_X
- falls Y ebenfalls in LAN L_X
 - verwerfe den Rahmen innerhalb der Bridge B_1
 - der Rahmen ist bereits im korrekten LAN (L_X)
 - Y kann den Rahmen ohne Mitwirkung von L_X empfangen
- falls Y in einem LAN L_Y mit $L_Y \neq L_X$
 - Bridge B_1 leitet Rahmen in ein anderes LAN weiter
 - falls L_Y direkt an die Bridge B_1 angeschlossen \rightsquigarrow unmittelbare Weiterleitung ins Ziel-LAN L_Y
 - anderenfalls finde ein LAN L_K , welches an B_1 angeschlossen und mit L_Y verbunden ist und leite Rahmen nach L_K weiter (ggf. L_Y nur über weitere Bridges mit L_K verbunden)



Bridging Algorithmen

- Frage: wie wird zu einer Station Y das zugehörige LAN bestimmt?
 - hierzu dient eine große Hashtabelle, die Source Adress Table (SAT)
 - falls n Knoten im LAN sind, muss die Tabelle n Einträge enthalten
- zu lösende Probleme
 - die Tabellen werden schnell sehr groß, d.h. keine Lösung für sehr sehr große Netze
 - die Tabellen müssen konfiguriert werden
 - Tabellen müssen aktualisiert werden (neue Stationen eintragen, entfallende Stationen entfernen)

Bridging Algorithmen – Aktualisierung der SAT

Entfernen von Einträgen

- Aging

- den Tabelleneinträgen können Zeitstempel mitgegeben werden
- periodisch werden alle zu alten Einträge entfernt

- Second Chance Algorithmus

- jeder Tabelleneintrag enthält ein 1 Bit Flag: (Knotenadresse, LAN, Flag)
- anfangs wird Flag auf 0 gesetzt
- falls Rahmen von Station Y über LAN L_Y empfangen wird

- $(Y, L_Y, 0) \rightarrow (Y, L_Y, 1)$

- periodische Ausführung von
 - für alle Y mit $(Y, L_Y, 0)$: lösche den Eintrag aus Tabelle
 - für alle Y mit $(Y, L_Y, 1)$: ändere Flag, d.h. $(Y, L_Y, 0)$

Bridging Algorithmen – Aktualisierung der SAT

Backward Learning

■ Bridging Phase

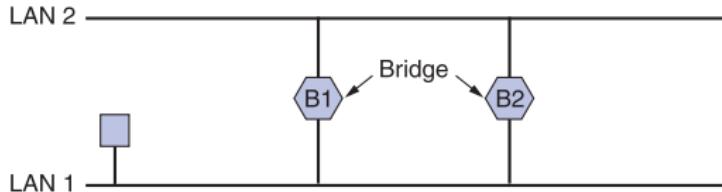
- ein Frame mit Zieladresse Y erreicht die Bridge aus L_X
- suche in SAT einen Eintrag zu (Y, L_Y)
- falls ein solcher existiert und $L_X \neq L_Y$, leite Frame nach L_Y weiter
- falls kein Eintrag existiert, leite Frame an alle Netzwerke mit Ausnahme von L_X weiter, die an Bridge angeschlossen sind (Flooding)

■ Lernphase

- Rahmen von Sender X erreicht eine Bridge über LAN L_X
- schreibe bzw. aktualisiere einen Eintrag (X, L_X)

Spanning Tree

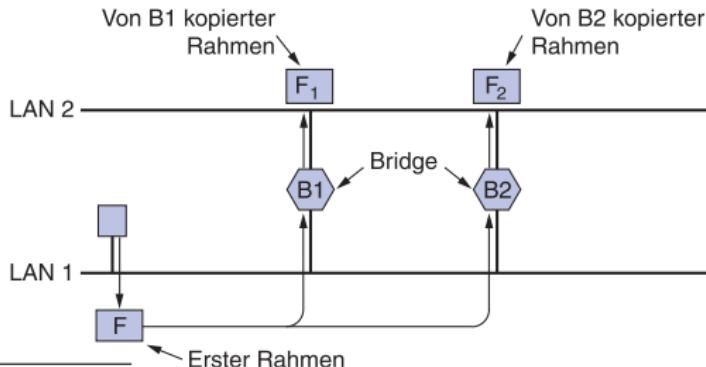
- zur Ausfallsicherheit können zwei oder mehrere Bridges parallel eingebaut sein
- diese Anordnung ruft allerdings Probleme hervor, da Schleifen entstehen können
- Schleifen können beliebig oft gebridegte Rahmen zur Folge haben



Graphik aus A. Tanenbaum, Computernetze

Spanning Tree

- Station in LAN 1 sendet Rahmen an eine Station F , die beiden Bridges unbekannt ist
- beide Bridges leiten den Rahmen per Flooding nach LAN 2 weiter (Rahmen F_1 und F_2)
- Bridge B_2 leitet F_1 wieder nach LAN 1 und B_1 den Rahmen F_2 nach LAN 1 usw.



Graphik aus A. Tanenbaum, Computernetze

Spanning Tree

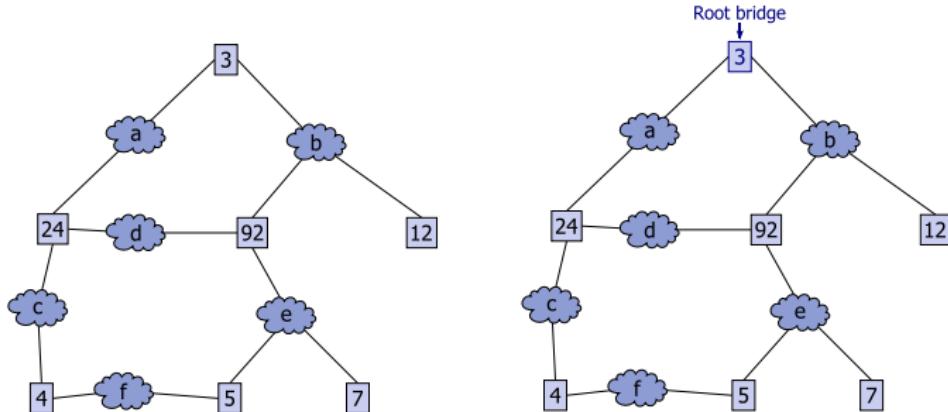
- es muss sichergestellt werden, dass zu einem Zeitpunkt nur eine der parallel liegenden Bridges arbeitet
- über die physikalische Topologie wird ein Spannbaum gelegt, der alle LANs beinhaltet
- Bridges tauschen Informationen aus (BPDU), um diesen Spannbaum aufzubauen
- Netzwerk wird als Graph angesehen,
 - Bridges und Netzwerke bilden die Knoten
 - Kanten sind Verbindungen zwischen Netzwerken und Bridges
- jede Bridge hat eine eindeutige BridgID (BID), 8 Byte, bestehend aus Priorität und MAC

Spanning Tree

- jeder Verbindung werden Kosten (Path Costs) zugeordnet, die sich z.B. aus der Geschwindigkeit der Verbindung ergeben
- Bridge mit der kleinsten BID wird zur RootBridge (Wurzel)
- von der gewählten Wurzel wird anhand der Kosten der Spannbaum aufgebaut
 - enthält die Verbindungen mit den geringsten Kosten von der RootBridge zu allen anderen Bridges
- bei einer Änderung der Topologie wird der Spannbaum neu berechnet
- Spannbaum Algorithmus für Bridges wurde nach IEEE 802.1D standardisiert (Spanning Tree Protokoll – STP)

Spanning Tree

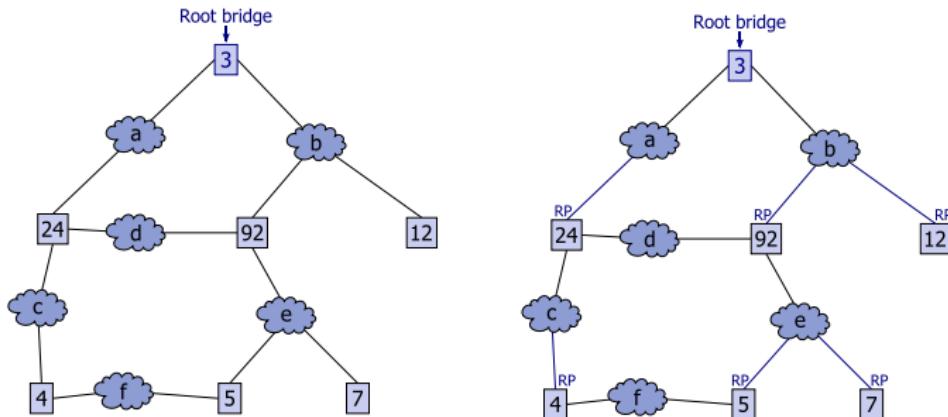
- Bridge mit kleinster BID wird zur RootBridge
- im Folgenden nehmen wir gleiche Pfadkosten von "1" für alle Pfade an



Graphik: http://en.wikipedia.org/wiki/Spanning_tree_protocol

Spanning Tree

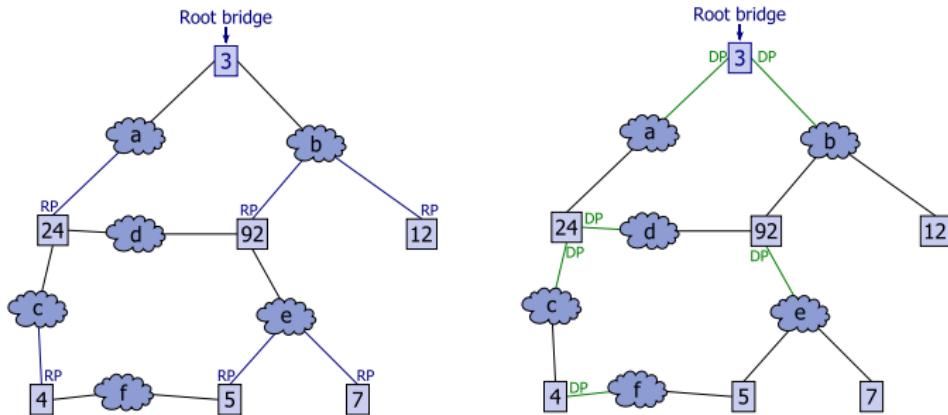
- zu jeder Bridge wird der RootPort (RP) bestimmt \rightsquigarrow geringste Pfadkosten zur RootBridge
- im Beispiel: für Bridge 4 der Port zu LAN c



Graphik: http://en.wikipedia.org/wiki/Spanning_tree_protocol

Spanning Tree

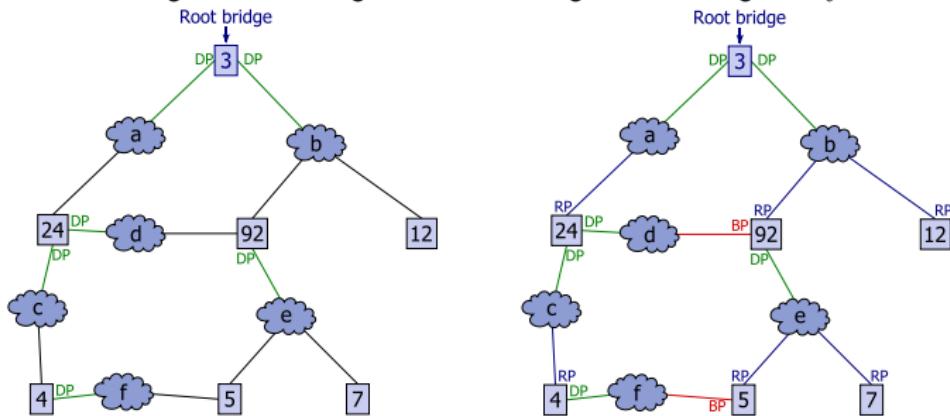
- zu jedem Netzwerk wird ein DesignatedPort (DP) bestimmt \rightsquigarrow der Port, der Segment mit geringsten Kosten mit RootBridge verbindet
- im Beispiel: für Segment e ist der kostengünstigste Weg über Bridge 92



Graphik: http://en.wikipedia.org/wiki/Spanning_tree_protocol

Spanning Tree

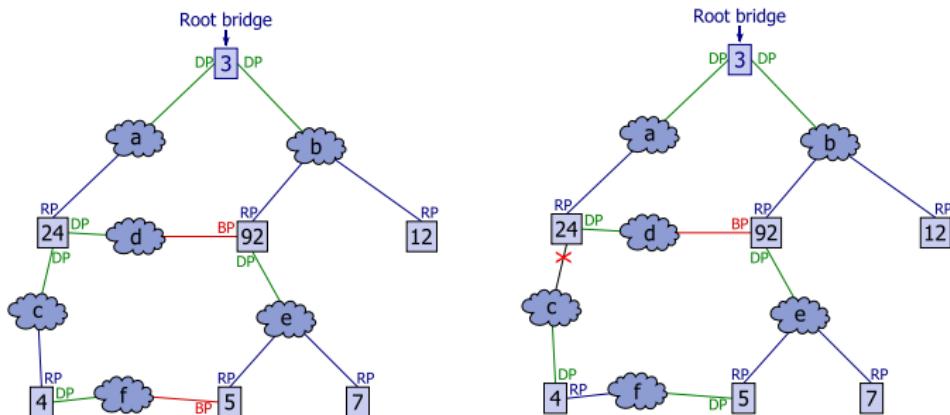
- Bridge Ports die weder RootPorts noch DesignedPorts sind werden deaktiviert (BlockedPorts BP)
- im Beispiel: Verbindung zwischen Segment d und Bridge 92 und Segment f und Bridge 5



Graphik: http://en.wikipedia.org/wiki/Spanning_tree_protocol

Spanning Tree

- bei einer ausfallenden Verbindung werden die RootPorts und DesignedPorts neu bestimmt
- Spannbaum ändert sich entsprechend der neuen günstigsten Verbindungen



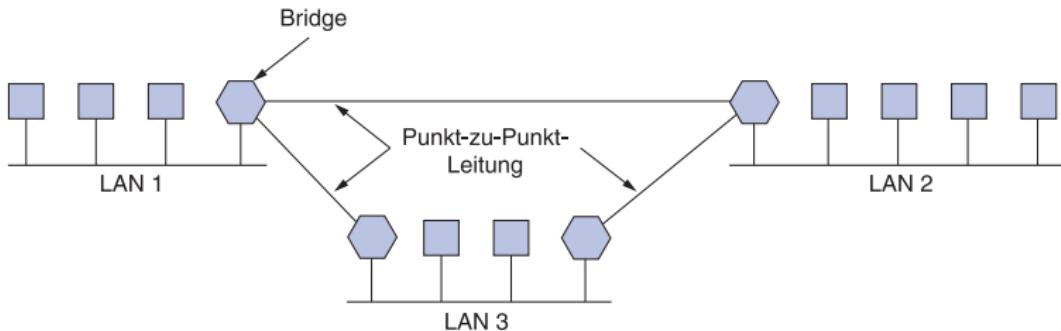
Graphik: http://en.wikipedia.org/wiki/Spanning_tree_protocol

Spanning Tree

- neben Pfadkosten auch den BridgePorts Kosten zuweisbar
- Entscheidung bei gleichen Kosten für Verbindungen nach
 1. niedrigster BID
 2. niedrigsten Pfadkosten zur RootBridge
 3. niedrigste SenderBID
 4. niedrigste PortId/Portkosten
- Bridges verschicken BPDUs um z.B. die Pfadkosten mitzuteilen
- RootBridge sendet alle 2 sec ein Hello Signal an direkt nachfolgende Bridges, diese senden dann ebenfalls an die direkt nachfolgenden usw.
- bleibt ein Hello aus, muss sich das Netz rekonfigurieren (kann bei STP bis zu 30 sec dauern)
- Verbesserung Rapid Spanning Tree Protokoll (RSTP, IEEE 802.1w) \rightsquigarrow Verzögerung nur 1 sec.

Remote Bridge

- Bridges können auch zur Koppelung entfernter Netze verwendet werden \rightsquigarrow Remote Bridges
- Remote Bridges bestehen aus zwei Teilen, die durch eine Punkt-zu-Punkt-Verbindung gekoppelt werden



Graphik aus A. Tanenbaum, Computernetze

Bridge – weitere Arten

- Translation Bridge
 - Koppelung von unterschiedlichen Netzwerken
 - es findet eine echte Übersetzung statt, die Rahmen der einen Netzart werden in die der zweiten Netzart umgewandelt
- Encapsulation Bridge
 - Datenrahmen werden nur vorübergehend über eine andere Netzart geleitet
 - Startnetz und Zielnetz sind von gleichem Typ aber ein Zwischennetz hat anderen Typ, z.B. Ethernet → Ethernet über ein FDDI Backbone.
 - Rahmen des sendenden Teilnetzes werden in Rahmen der Netzart des Koppelungsnetzes "eingepackt"
 - an einer Bridge im Zielnetzwerk wieder entpackt
 - häufigster Einsatz dieser Art ist im Backbone-Bereich

Einordnung ins Schichtenmodell

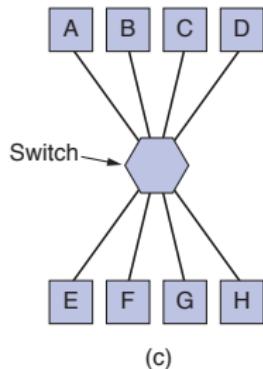
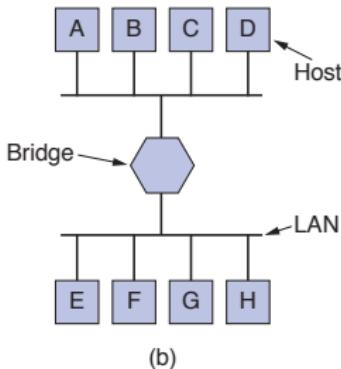
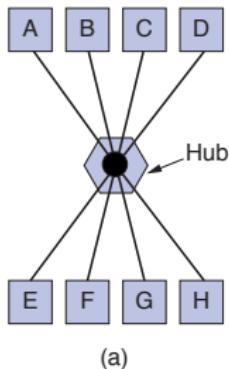
- Repeater dienen zur Signalgeneration und Netzwerkoppelung auf Schicht 1
- Hubs koppeln ebenfalls auf Schicht 1, da keine Adressen zur Weiterleitung herangezogen werden
- Bridges und Switches koppeln auf Schicht 2 (Adressen werden zum finden des Zielnetzwerkes verwendet)
- Switches erlauben mehrere gleichzeitige Verbindungen



Graphik aus A. Tanenbaum, Computernetze

Arten der Koppelung

- Hub: sternförmige Vernetzung, eingehende Daten an alle Ports
- Bridge: Koppelung unterschiedlicher Topologien, Zielnetzwerk wird gezielt adressiert
- Switch: Netzwerke und Stationen werden gezielt adressiert



Graphik aus A. Tanenbaum, Computernetze

Switches

- moderne Technik zur Sternvernetzung
- eingehende Daten werden nur an den Port weitergeleitet, an dem Empfängerstation angeschlossen ist
- erlauben mehrere gleichzeitige Verbindungen
- lesen je nach Art die Rahmen ganz oder teilweise aus



Switcharten

Cut-Through-Switching

- nur die Hardware-Adressen des Senders und des Empfängers werden aus dem Datenrahmen ausgelesen
- anhand dieser wird entschieden, an welchen Port der Rahmen zu senden ist
- es wird bei diesem Verfahren keinerlei Fehlerkontrolle für den Rahmen durchgeführt oder geprüft ob der Rahmen vollständig ist
- ist topologieabhängig, d.h. es kann nur innerhalb der gleichen Netzart geswitcht werden (Ethernet → Ethernet, Token Ring → Token Ring)

Switcharten

Store-and-Forward-Switching

- kompletter Rahmen inkl. Frame Check Sequence (FCS) wird gelesen
- eine Fehlerkontrolle wird durchgeführt.
- Hardware Adresse zur Entscheidung wohin geschaltet werden muss wird zugrunde gelegt
- Umsetzung in eine andere Netzart möglich
 - echte Umsetzung des Rahmens z.B. kann ein Token-Ring mit einem Ethernet oder FDDI Netz verbunden werden.
 - auch Encapsulation möglich
 - kompletter Rahmen der einen Netzart wird in einen Rahmen der zweiten Netzart eingepackt
 - z.B. Koppelung von Ethernetsegmenten über FDDI Backbone

Switcharten

Modified-Cut-Through-Switching

- arbeitet standardmäßig wie ein Cut–Through Switch, d.h. nur Hardwareadressen werden eingelesen
- Umschaltung auf Store–and–Forward–Switching wenn durch Protokolle höherer Schichten zu viele Fehler signalisiert werden

Switch vs. Bridge

- Switche treffen wie Bridges die Entscheidung über Ziel an den Hardwareadressen ↵ selbstlernende Tabelle
- Switche können Netzwerke verbinden und via Spanning Tree Kreise ausschließen
- Broadcasts werden an alle Switchports weitergeleitet