Rechnernetze & Verteilte Systeme

Ludwig-Maximilians-Universität München

Sommersemester 2019

Prof. Dr. D. Kranzlmüller

MNM TEAM

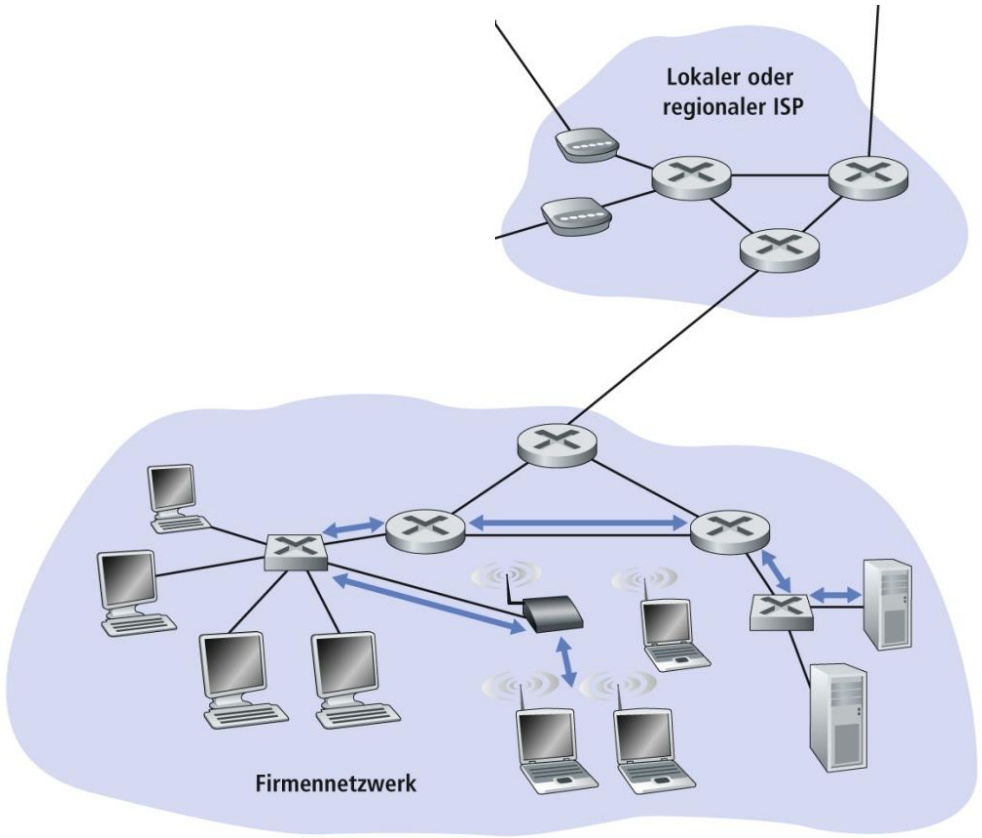
Erinnerung: Fragestunde

- Termin: 26.07.2019
- Einreichung von Fragen bis 24.07.2019
  - Per E-Mail an rnvs-fragen@nm.ifi.lmu.de

- Letztes Übungsblatt 12 vom 19.07. bis 26.07. zur **Klausurvorbereitung**
  - Besprechung sowie Diskussion in der Fragestunde.

Kapitel 6: Sicherungsschicht (engl. Link Layer)

Thematische Einordnung



Beispiel: 6 Hosts zwischen drahtlosem Client und kabelgebundenem Server

Aufgaben der Sicherungsschicht

- Rahmenbildung (Framing)
  - Kapselung von Pakete bzw. Datagrammen in Rahmen
  - Block/Frame–Synchronisation
- Medienzugriff
  - Problem: Medium (Kabel, Luft) **keine** exklusive Resource. → Vielfachzugriffsproblem.
  - Steuerung durch Vielfachzugriffsprotokolle
- Zuverlässige Übertragung
  - Medien haben inhärente Fehlerraten unterschiedlicher Größe (Kabel vs. Kabellos / Luft)
  - Statt sich nur auf Transportschicht zu verlassen (Retransmission zwischen verbundenen Endpunkten) wird versucht, Fehler unmittelbar auf Schicht 2 zu vermeiden.
- Fehlererkennung bzw. –Korrektur
  - Siehe separaten Foliensatz auf der Vorlesungswebseite.

Kapitel 6.1: Vielfachzugriffsverfahren

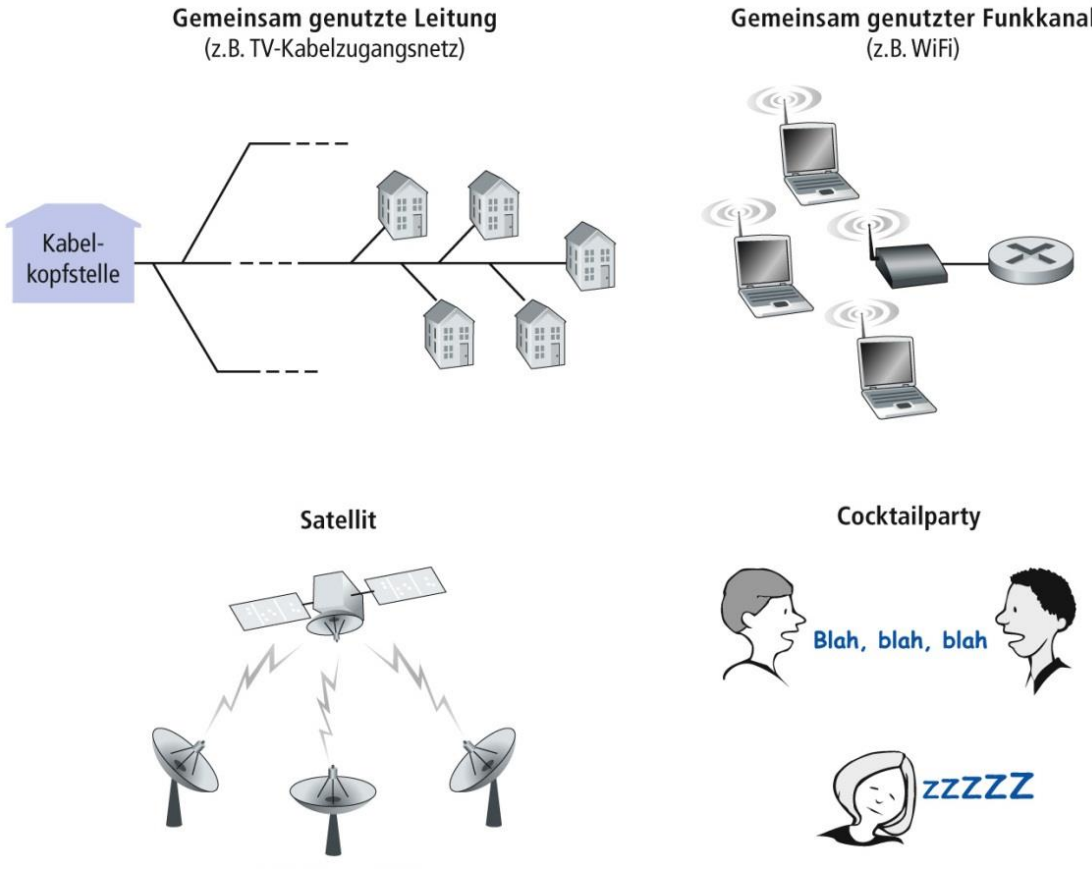
Vielfachzugriffsverfahren

- Zwei Verbindungsarten auf Sicherungsschicht
  - Punkt-zu-Punkt (1 Sender sowie 1 Empfänger)
  - Broadcast: Mehrere Sender sowie Empfänger. → Jeder am Medium angeschlossene Knoten erhält eine Kopie der übertragenen Rahmen. („Jeder hört alles“).
- Weiterer Fokus der Vorlesung liegt auf Broadcast-Channels mit den gängigen Protokollen
  - Ethernet
  - Wifi
- Grundsätzliches Problem: Wie wird koordinierter Zugriff auf ein geteiltes Medium mit mehreren Teilnehmern erreicht?

Kategorisierung: Vielfachzugriffsverfahren

- Wettbewerbsverfahren/Random Access Verfahren
  - Aloha-Verfahren (pure, slotted, reservation)
  - Carrier Sensing Verfahren (p-persistent, non persistent)
- Zuteilungsverfahren
  - zentral (Polling)
  - dezentral (Token Passing, Register Insertion, DQDB)
- Reservierungsverfahren
  - Fest (TDMA, FDMA, WDMA, CDMA, SDMA)
  - dynamisch

Vielfachzugriff: Beispiel-Szenarien



Beispiele für Links mit Mehrfachzugriff

Vielfachzugriff: Anforderungen

Ein Kanal (Medium) hat eine verfügbare Übertragungsrate von R Bits / Sekunde. Idealerweise werden dabei folgenden Anforderungen erfüllt:

- Falls nur 1 Sender: Durchsatz von R.
- Falls M Sender: Der gemittelte Durchsatz über die Zeit aller Sender ist R/M.
- Dezentralisiertes Protokoll: Kein Single Point of Failure (SPoF).
- Simples Protokoll → geringe Anforderungen der Implementierung. (Muss auf vielen verschiedenen Geräten lauffähig sein)

Random Access Verfahren: Überblick

- Ein Knoten sendet immer mit maximal möglichen Übertragungsrate R.
- Bei Auftreten einer **Kollision**
  1. **Zufällige** Zeitspanne warten
  2. Erneuter Sendeversuch
  3. Verfahren wiederholen, bis der Rahmen erfolgreich übertragen ist
- Durch Zufall ist Wahrscheinlichkeit geringer, dass mehrere Sender die exakte Wartezeit haben. → Geringere Kollisionswahrscheinlichkeit
- Protokolle
  - Slotted Aloha
  - Pures Aloha
  - Ethernet

Slotted Aloha: Voraussetzungen

- Jeder Rahmen hat eine fixe Größe von L Bits.
- Verfügbare Übertragungsrate ist R Bits / Sekunde
- Aufteilen der Sendezeit in diskrete Zeit-Intervalle
  - L / R Sekunden: Zeit um einen Rahmen der Größe L mit Übertragungsrate R zu versenden.
- Übertragung eines Rahmen wird immer bei Beginn eines Sende-Intervalls gestartet.
- Alle Sender sind zeitlich synchronisiert und wissen daher, wann ein Sende-Intervall beginnt / endet.
- Alle Sender erkennen eine mögliche Kollision.

Slotted Aloha: Protokollablauf

Sei *p* eine Wahrscheinlich (Zahlen zwischen 0 und 1).

- Tritt keine Kollision auf, ist der Rahmen erfolgreich übertragen.
- Bei Auftreten einer Kollision: Erkennen vor Ende des *aktuellen* Sende-Intervalls. Erneute Übertragung im *nächsten* Intervall mit Wahrscheinlichkeit *p*.

→ Nicht-Übertragung sowie erneutes Versuchen in späteren Zeitintervallen daher mit Wahrscheinlichkeit *(1-p)*.

Slotted Aloha (Bewertung)

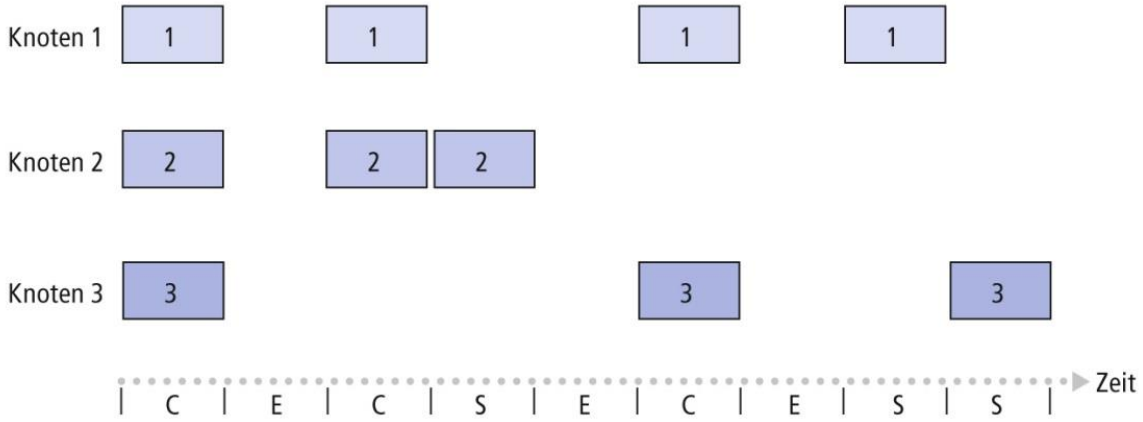
- Jeder Sender kann Übertragungsrate R voll ausschöpfen.
- Dezentralisiertes Protokoll durch unabhängiges Erkennen der Kollision und Wahrscheinlichkeit *p* für erneutes Übertragen im nächsten Intervall.
- Am effizientesten, wenn nur 1 Sender offene Rahmen zu versenden hat.

→ Wie effizient ist Aloha?

Slotted Aloha: Beispiel

4 Sender (Knoten):

- Knoten 1,2 und 3 kollidieren im ersten Intervall (Zeitscheibe).
- Knoten 2 versendet Rahmen erfolgreich in Intervall 4, Konten 1 in 8 sowie Knoten 3 in 9.



Legende:
C = Zeitscheibe mit Kollision (collision)
E = Leere Zeitscheibe (empty)
S = Erfolgreiche Zeitscheibe (success)

Slotted Aloha (Effizienz)

Vereinfachte Annahme mit: Sowohl neue (aus Schicht 3 ankommende) als auch kollidierende Rahmen werden mit Wahrscheinlich *p* versendet. Es gibt N Sender.

- Wahrscheinlichkeit für erfolgreichen Slot: Nur 1 Knoten (aus N) sendet.
  - Knoten versendet: p
  - N-1 Knoten senden nicht: $(1-p)^{N-1}$
  - Ein beliebiger Knoten erfolgreich: $\mathrm{p}(1-p)^{N-1}$
  - Wahrscheinlichkeit mit N Knoten: $\mathrm{Np}(1-p)^{N-1}$

→Finde p*, das den Term maximiert (Schrittweises Herleiten in der Übung).

→Ergebnis: Effizienz ist $\frac{1}{e} = 0.37\ (37\%)$.

→Durchsatz bei 100 Mbit/s nur 37 Mbit/s.

Pure Aloha

- Im Gegensatz zu slotted Aloha **Keine** Aufteilung in diskrete Zeitintervalle.
- Wenn ein Rahmen anfällt, wird unmittelbar versendet.
- Bei Auftreten einer Kollision unmittelbar erneutes Versenden mit Wahrscheinlichkeit *p* bzw. erneutes Abwarten für die Dauer einer Rahmenübertragungszeit mit *1-p*.
- Vorteil gegenüber Slotted Aloha: Keine Zeitsynchronisation notwendig.
- Nachteil: Noch geringere Effizienz mit $\frac{1}{2e}$ (halb so groß wie die von Slotted Aloha.

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

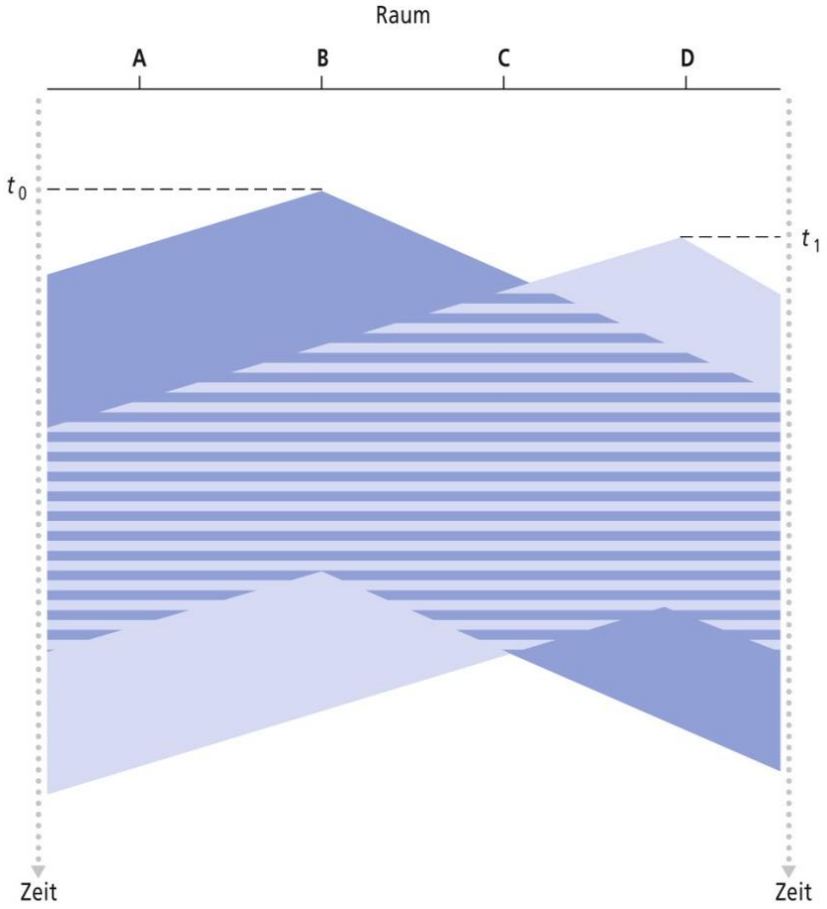
- Zugrundeliegendes Zugriffs-Protokoll in Ethernet 802.03
- Grundsätzliche Regeln (im Gegensatz zu Aloha)
  - **Carrier Sensing**: Bevor die Übertragung eines Rahmens initiiert wird, Kanal abhören. Falls Kanal „belegt“, warten bis Kanal frei ist.
  - Kollisionserkennung (**Collision Detection**): Tritt während der Übertragung eine Kollision auf, Übertragung abbrechen und zufällige Zeit warten bevor ein erneuter Versuch gestartet wird.

Frage: Warum kommt es zu einer Kollision, obwohl vor Beginn der Übertragung festgestellt wird, dass der Kanal frei ist (Carrier Sensing)?

Beispielszenario CSMA

Raum-Zeit-Diagramm zweier CSMA Konten (Sender) mit kollidierenden Übertragungen

Zeitpunkt *t0*: Knoten B hört Kanal ab und startet Übertragung^.

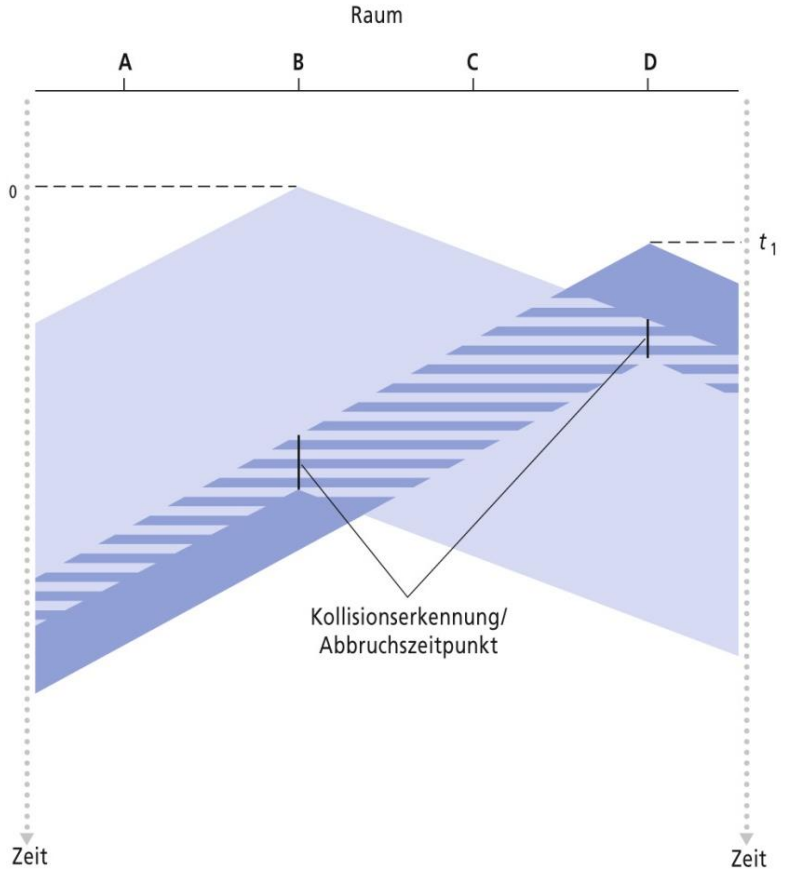


Zeitpunkt *t1*: Knoten D hört Kanal ab und stellt (fälschlicherweise) fest, dass Kanal frei ist. Knoten D beginnt daher ebenfalls mit der Übertragung.

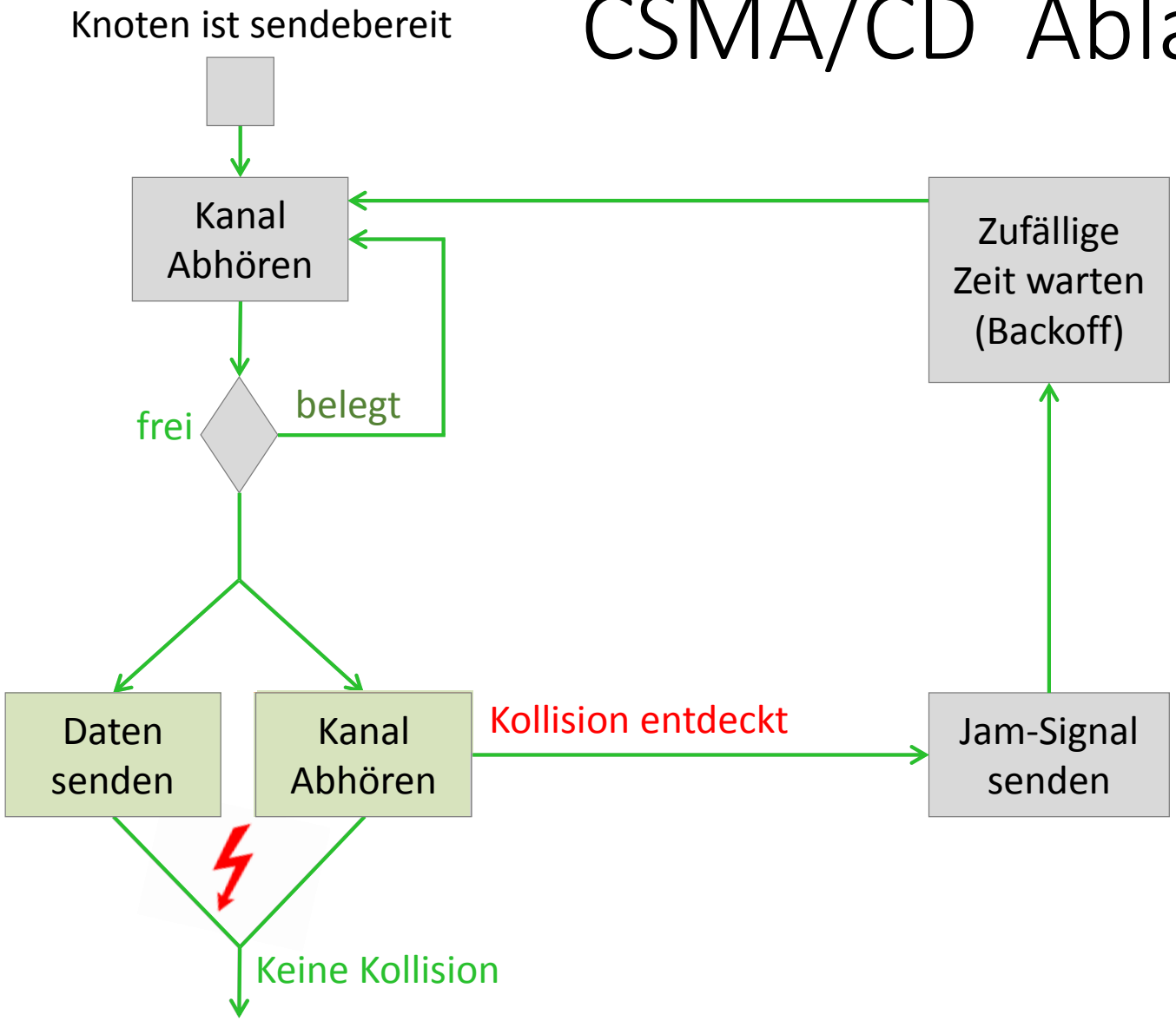
→ Kollision (Signal-Interferenz von B und D) tritt später auf.
→ Problem: Signal von B hat sich bei t1 noch nicht über das ganze Medium ausgebreitet. (**Ausbreitungs-verzögerung**)

Beispielszenario CMSA mit Kollisionserkennung

→ Entscheidende Rolle der Ausbreitungsverzögerung:
Je größer, umso höhere Wahrscheinlichkeit, dass Carrier Sensing eine spätere Kollision nicht vermeiden kann.



CSMA/CD Ablauf



CSMA: Wartezeit-Verfahren

- Es wird eine zufällige Wartezeit aus einem definierten Intervall gewählt. --> Was ist ein gutes Intervall
  - Zu kurz: Hohe Wahrscheinlichkeit für weiteres Auftreten einer Kollision
  - Zu lange: Zu geringe Auslastung des Mediums (Performance)
- Kompromiss: **Binary Exponential Backoff** (Ethernet)

CSMA: Binary Exponential Backoff

- Nach *N* Kollisionen bei Übertragung eines Rahmen wird eine zufällige Zeit *K* aus dem Intervall $\{0,1,2,\dots,2^N-1\}$ ausgewählt.
- Weiterhin gilt: $N = \min(N, 10)$

→Je mehr Kollisionen auftreten bei einem Rahmen, umso größer das Wartezeiten-Intervall.

- Die Wartezeiten-Einheit ist bei Ethernet 512 Bit-Zeiten
  - Zeit um einen Rahmen der Länge 512 Bits über die gesamte Leitungslänge mit Ethernet zu übertragen.

  → Siehe Kapitel 6.2

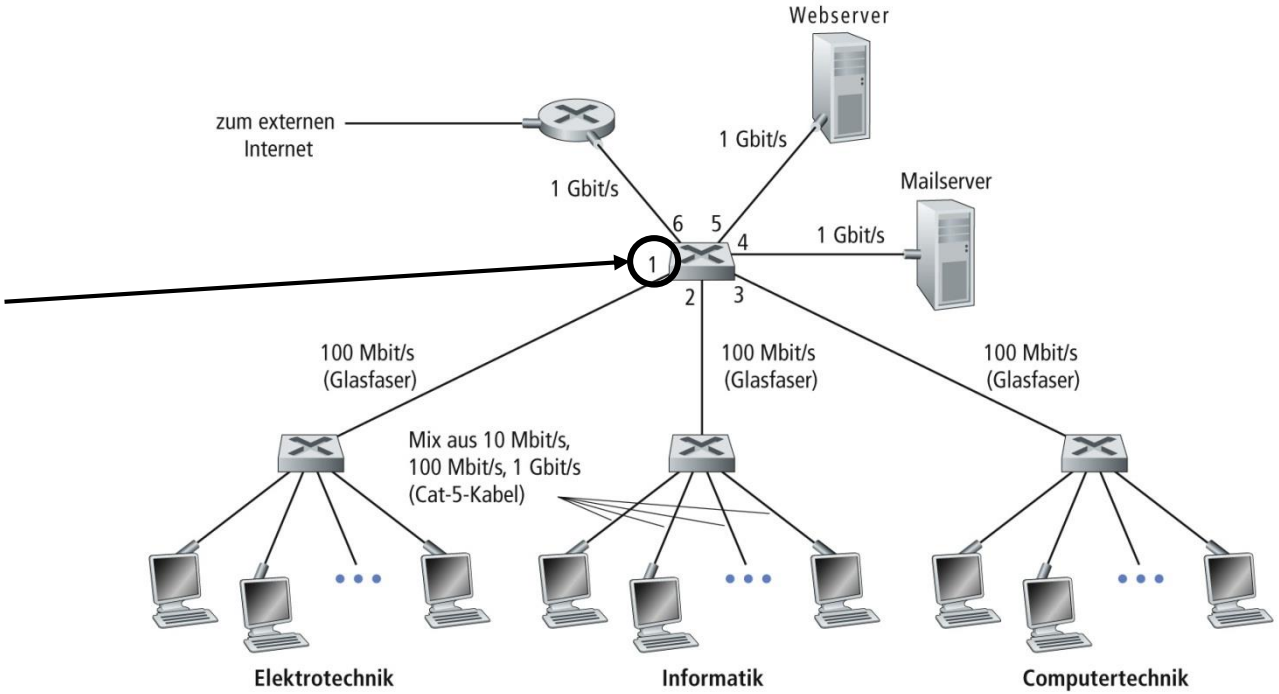
Kapitel 6.2
Adressierung in der Sicherungsschicht

Adressierung in Schicht 2

- Schicht verschickt ausschließlich **Rahmen**
  - Kein Konzept von IP-Paketen oder –Datagrammen
  - Kein Konzept von Routing-Verfahren
- Adressierung („Switching“) erfolgt anhand von MAC-Adressen (Media Access Control Address)
- Jede Schicht 3 Netz-Schnittstelle (Netzwerkkarte) hat eine eigene MAC Adresse
  - Ein Router hat daher mehrere MAC-Adressen.
  - Ein Host kann ebenfalls mehrere MAC-Adressen haben (bspw. je eine für LAN- und WiFi-Adapter)

Beispiel: Firmenetzwerk

Router mit 6
Layer 2
Schnittstellen



MAC Adressen

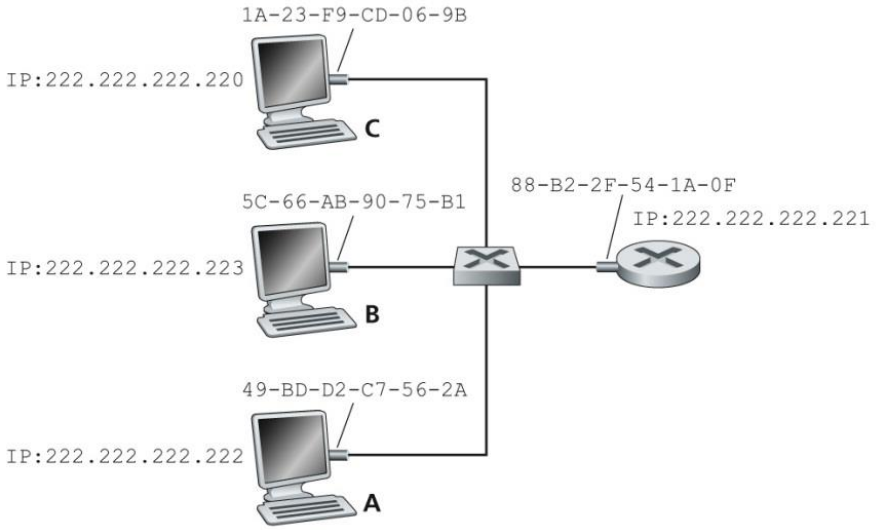
- Synonyme: LAN Adresse, physische Adresse
- Keine hierarchische Struktur (im Gegensatz zu IP)
- Länge: 6 Bytes → 2^{48}mögliche MAC Adressen
- MAC Adressen werden „ab Werk“vergeben und sind daher fest in der Hardware verankert.
- Zuweisung von MAC Adressen an Herstellen erfolgt zentral durch IEEE.
  - Die ersten 24 bit: Prefix für Hersteller (IEEE)
  - Die letzten 24 bit: definierbar vom Hersteller selbst.
- Broadcast MAC Adresse um ein Frame an alle Peers im selben LAN zu senden
  - FF-FF-FF-FF-FF-FF (48 aufeinanderfolgende Einsen)

Kapitel 6.2.1 Adressierung in lokalen Netzen

Adressauflösung in lokalen Netzen (LAN)

- Szenario: Host C sendet an Host A ein IP-Paket
  - Hosts C benötigt neben der IP-Adresse auch die MAC-Adresse von Host A.
  - Aus IP (Netz)-Sicht sind beide Hosts im selben Netz.
  - Woher kennt Host A die MAC-Adresse von Host C?

  → Address Resolution Protocol (**ARP**)



Address Resolution Protocol

- Tabellarische Zuordnung von IP-Adressen zu MAC-Adressen in einem LAN (ARP Table)
- Alle Hosts und Router haben eine eigene ARP Table
- Time To Live (Ablaufzeitpukt): Maximale Gültigkeit eines Eintrags

IP-Adresse	MAC-Adresse	Ablaufzeitpunkt
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

- Kann in Linux eingesehen werden via
  - `$ cat /proc/net/arp`, bzw.
  - `$ ip -statistics`

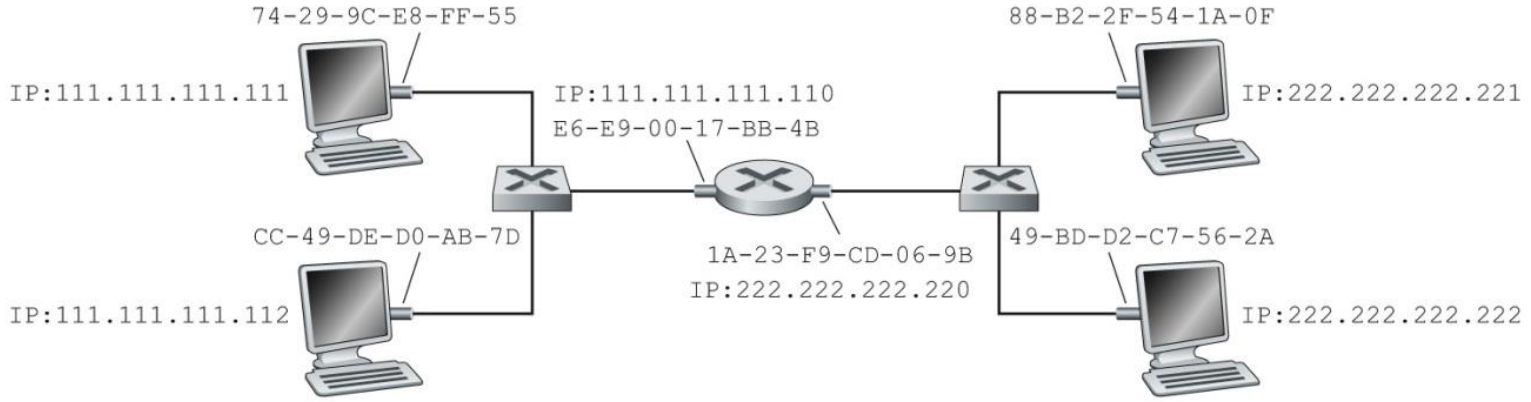
Ermitteln der ARP Einträge

Falls bei einem Host für eine bestimmte IP-Adresse keine MAC-Adresse vorliegt, wird sie zuerst via ARP ermittelt.

1. Der Host konstruiert eine ARP-Anfrage (Query)
   - Mit Quell-MAC sowie Quell-IP und Ziel-IP-Adresse
   - Ziel-MAC Adresse ist FF-FF-FF-FF-FF-FF, sodass alle Peers im lokalen Netz angesprochen werden (Broadcast).
2. Alle Hosts (Router) empfangen die ARP-Anfrage
3. Der Host (Router) auf den die Anfrage zutrifft, antwortet
   - Gesuchte MAC-Adresse wird in der ursprünglichen Anfrage ersetzt und an den Sender zurück geschickt.
4. Sender übernimmt die Antwort in seine lokale ARP Tabelle.

Adressauflösung zwischen Netzen

Szenario: Zwei Subnetze die durch einen Router verbunden sind.



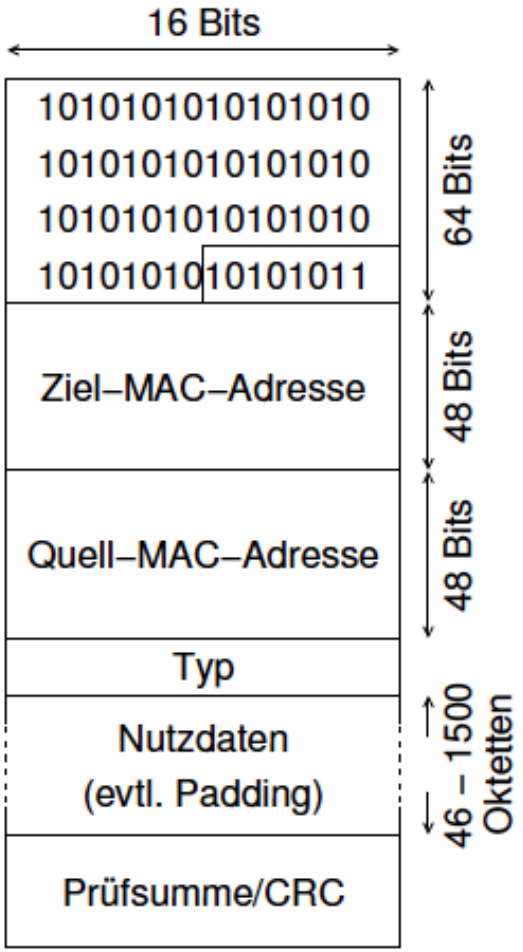
- Sender mit IP 111.111.111.111 übermittelt Rahmen an Empfänger mit IP 222.222.222.222
- An welche MAC Adresse adressiert der Sender den Rahmen? Wie ist der weitere Datenfluss?

Kapitel 6.2.2 Ethernet

Ethernet: Überblick

- Ethernet ist die wichtigste CSMA-Variante und marktdominant bei LANs
- Ethernet ist definiert in Standard IEEE 802.3.
- Es realisiert ein CSMA/CD-Verfahren
- Mit CD (Collision Detect) ist auch die Art der Kollisionserkennung festgelegt.
- Die Wartezeit bei Kollision ist durch Binary Exponential Backoff definiert.
- Verbindungsloses Protokolle (analog zu IP)
  - Kein Handshake Mechanismus
  - Keine Acknowledgements

Ethernet: Rahmenaufbau



- **Präambel** (7 Bytes): je 10101010
- **Start of Frame** (1Byte): 10101011
- **Ziel-, und Quell-MAC-Adresse**
- **Nutzdaten**
  - Ethernetframe muss min. 64 Bytes lang sein (inclusive MAC-Felder)
  - Maximale Länge: 1500 Bytes
  - Padding (bedarfsweise 0-46 Bytes)
- **Typ** (Ethertype)
  - IPv6, IPv4, ARP,…
- **Prüfsumme** (4Bytes): nach dem CRC-Verfahren
  - Fehlerhafte Rahmen werden beim Empfänger verworfen.

Ethernet Präambel

- Jedes Frame beginnt mit einer 8-byte langen Präambel
  - Die ersten 7 Bytes: 10101010
  - Das letzte Byte: 10101011
- Zweck ist eine Synchronisation von Sender und Empfänger
  - Woher erkennt Empfänger, wann ein Frame beginnt?

  → Letztes Byte signalisiert den Start mit relevanten Daten

Minimale Rahmenlänge

- Unterscheidung von unvollständigen, abgeschnittenen Frames (im Falle einer Kollision) von vollständigen Frames.
- Sendezeit vs. Übertragungszeit (Konfliktparameter K)
  - Vermeiden, dass ein Frame vollständig versendet ist bevor das erste Bit den Empfänger erreicht.
  - Andernfalls erhält der Sender bei einer Kollision keine rechtzeitige Rückmeldung um ein erneutes Senden des Frames zu veranlassen.

Ethernet: Rahmenlänge

- 10 Mbit/s LAN
- Max. 2500m Kabellänge
- Durchschnittlich gemessene RTD mit 4 Repeater: 50 µs

→ 1 Bit: 100 nsec

→ minimum 500 Bits

→Für Ethernet aufgerundet auf 512 bit (64 bytes)

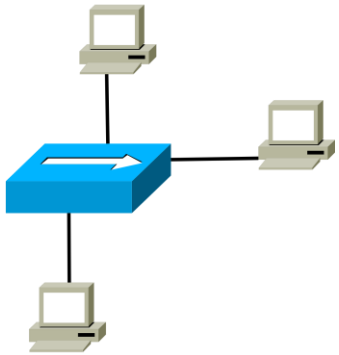
Ethernet: Jam Signal

- Erkennt ein Sender eine Kollision, wird ein Jam-Signal gesendet
- Maximale Distanz zwischen zwei Stationen (Diameter) in Ethernet: 232 Bits (Bit-Zeiten)
  →Round Trip Time: 464 Bits
- Mindest-Rahmenlänge in Ethernet: 512 Bits
- Differenz: 512 Bits – 464 Bits = **48 Bits** Jam-Signal

→ Jam Signal ist eine Abfolge von 16 „10“ Bit-Kombinationen

Switched Ethernet (1)

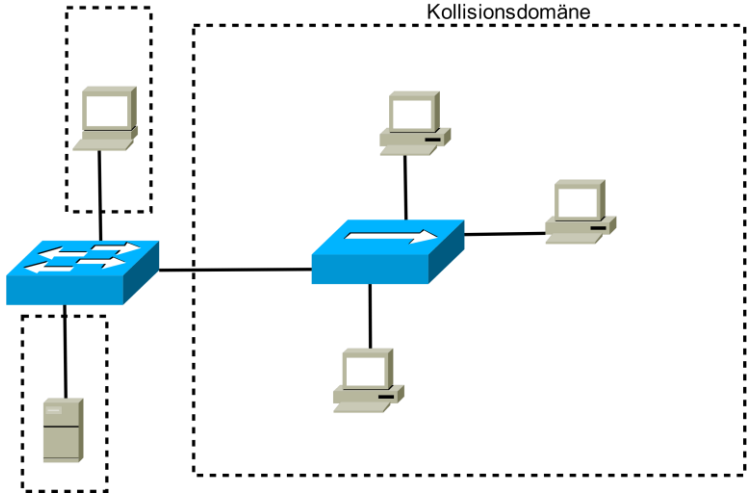
- Erste Weiterentwicklung: Einsatz von Hubs / Repeaters.



- Vorteil: Einfachere Wartung
- Nachteile
  - Immer noch **eine** Kollisionsdomäne.
  - Geräte teilen sich die verfügbare Kapazität

Switched Ethernet (2)

- Einsatz von Switches



- Jeder Port am Switch ist eine eigene Kollisionsdomäne
- Kollisionsvermeidung durch intelligentes Zwischenspeichern von Frames im Switch (kein CSMA/CD notwendig)

Kapitel 6.2.3
Virtuelle LANs

Motivation

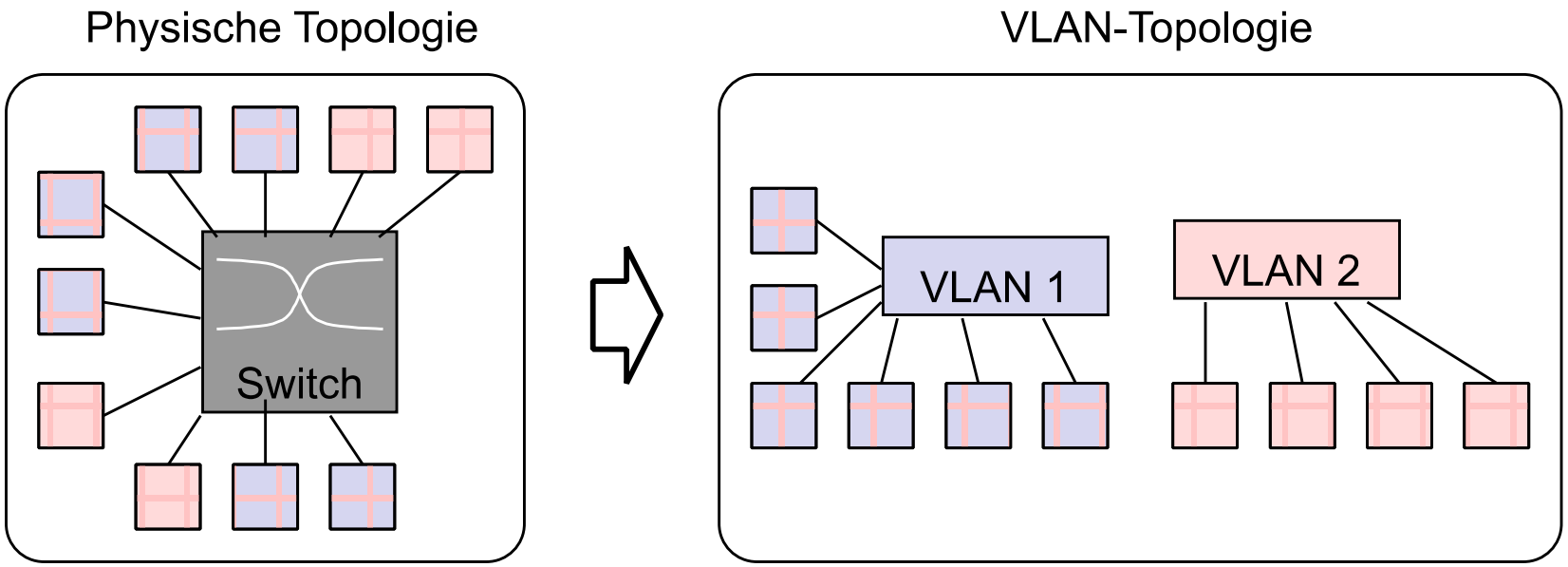
Normales LAN:

- LAN-Topologie folgt physischem Aufbau, und nicht Nutzungsanforderungen
- LAN ist Broadcastdomäne; LAN-Verkehr für alle DEE „sichtbar”
- Aber: Geschäftsprozesse und -strukturen ➔ Anforderungen an LAN-Struktur

Idee VLAN:

- Unterteilung eines LAN zur Isolation von DEE-Gruppen, die z.B. organisatorischen Einheiten entsprechen, Trennung des Datenverkehrs verschiedener Gruppen.
- Ziele:
  - Trennung von Verkehrslast
  - Sicherheit (z.B. Vertraulichkeit)
  - Trennung der Broadcastdomänen

Probleme und Aufgaben

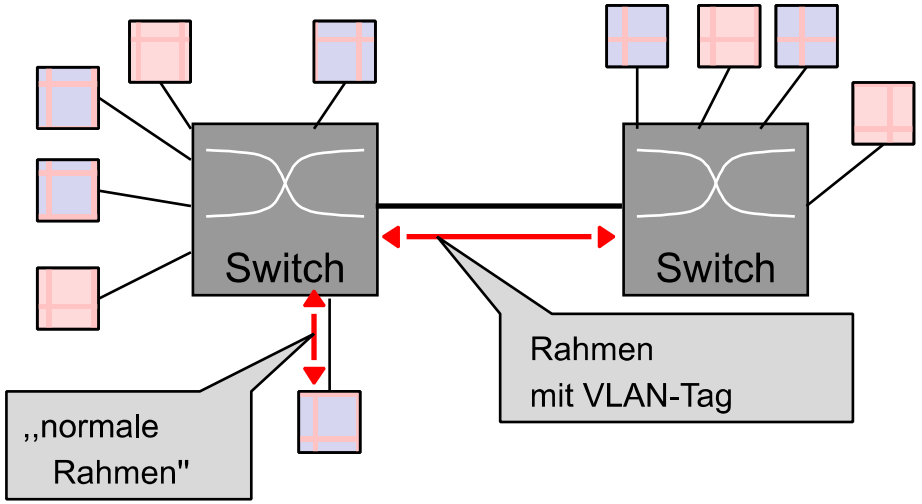


- Abstraktion von physischer (LAN) auf logische (VLAN) Topologie
- Herausforderung: Bildung von VLANs über Hubs/Switches hinweg
- Keine Änderungen an den Leitungsadaptern der DEE

Ansätze

- VLAN-bildung über Ports der Koppelkomponente (z.B. Switch-Ports)
  - Anforderung: alle DEE hinter einem Port gehören VLAN an
  - Einfache Konfiguration: Port-Bereiche werden VLAN fest zugeordnet
  - Mobilität der DEE problematisch: Portwechsel ➔ VLAN-Wechsel
- VLAN-bildung über MAC-Adressen der DEE
  - Anbindung einer DEE unabhängig von Port (MAC-Adresse bleibt gleich)
  - MAC-Adressen neuer DEE müssen VLAN zugeordnet werden ➔ Konfigurationsaufwand
- VLAN-bildung über Adressen der Vermittlungsschicht
  - Verletzung des Schichtenkonzeptes!
  - keine Transparenz bezüglich Schicht-3-Protokollen (z.B. verschiedene Versionen des Internet Protokolls)

Beispiel: „Tagging“

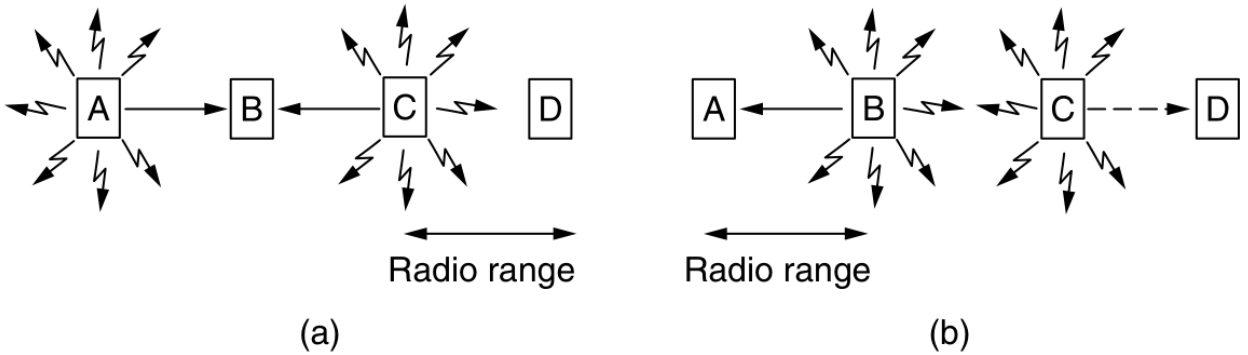


- Problem: Betrieb von VLANs über mehrere Switches hinweg bei VLAN-agnostischen Link-Adaptern der DEE
- Markierung der Rahmen (tagging)
  - in Abhängigkeit von VLAN-Zugehörigkeit des Senders
  - durch erste VLAN-fähige Koppelkomponente
  - Tags relevant für Vermittlung zwischen Switches
- bei Ethernet IEEE 802.1Q
  - zusätzliches Rahmenformat mit: VLAN-Protocol-ID und Tag (Prio, VLAN-ID)
  - dynamische Zuordnung Port zu VLAN (ähnlich „Anlernen” von MAC–Port-Paaren)

Kapitel 6.2.4
MACA (Multiple Access with Collision Avoidance)

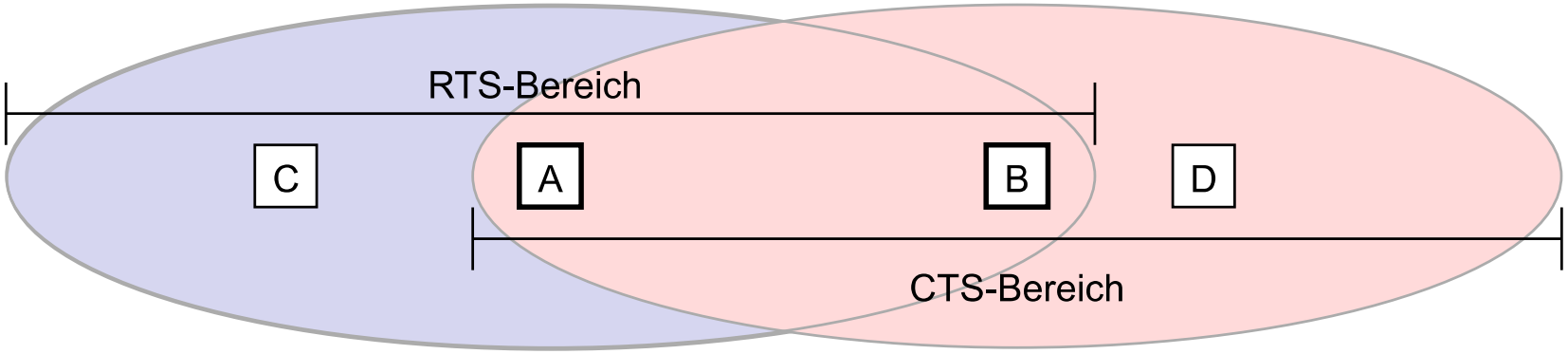
Motivation

- MACA: Multiple Access with Collision Avoidance
- Anwendung bei Funkkommunikation
- Hidden Station / Exposed Station Probleme
  a. Manche Stationen nur in Reichweite des Senders A oder nur des Empfängers B (A sowie C sind hidden stations)
  b. Manche Stationen interpretieren „fälschlicherweise“ ein irrelevantes Signal als besetzte Leitung.



MACA: Konzeptionelle Sicht

- Kommunikation über dedizierte Signale
  - Sender: RTS (ready to send)
  - Empfänger: CTS (clear to send)
- Inhalt von RTS-Paket
  - Empfänger
  - Nachrichtenlänge



Ablauf MACAW (MACA for Wireless)

- positive Quittungen
- CSMA vor Senden des RTS
- Sicht des Senders
  - Sendebereitschaft: prüfen, ob Kanal frei („lauschen“)
  - Kanal frei: senden, RTS (engl. request to send) markiert Sendeabsicht, Länge der Nachricht sowie Empfänger
  - Quittung CTS (engl. clear to send) empfangen: Nachricht kann gesendet werden
  - Nachbarn: Empfangen RTS, leiten aus Länge der Nachricht die Dauer der Reservierung ab
- Sicht des Empfängers
  - wenn RTS korrekt empfangen: senden CTS
  - Nachbarn: Empfangen CTS, leiten aus Länge der Nachricht die Dauer der Reservierung ab

Fragen zur MAC-Teilschicht

- Begründen Sie die Notwendigkeit von Vielfachzugriffsprotokollen.
- Was versteht man unter dem Konzept einer Kollisionsdomäne?
- Warum muss bei Ethernet eine untere Grenze für den kürzesten Frame festgelegt werden?
- Welche Protokollbestandteile sind für Ethernet festgelegt?
- Warum kann ein reines carrier sense Verfahren nicht Kollisionen vermeiden, wenn ein hidden station problem vorliegt ?