

Technische Grundlagen der Informatik 2

– Teil 7:

Sicherungsschicht (Layer 2)

Philipp Rettberg / Sebastian Harnau

Block 13-15/18

Sicherungsschicht (Layer 2)

MAC, ARP, Ethernet, Switches...

Einführung

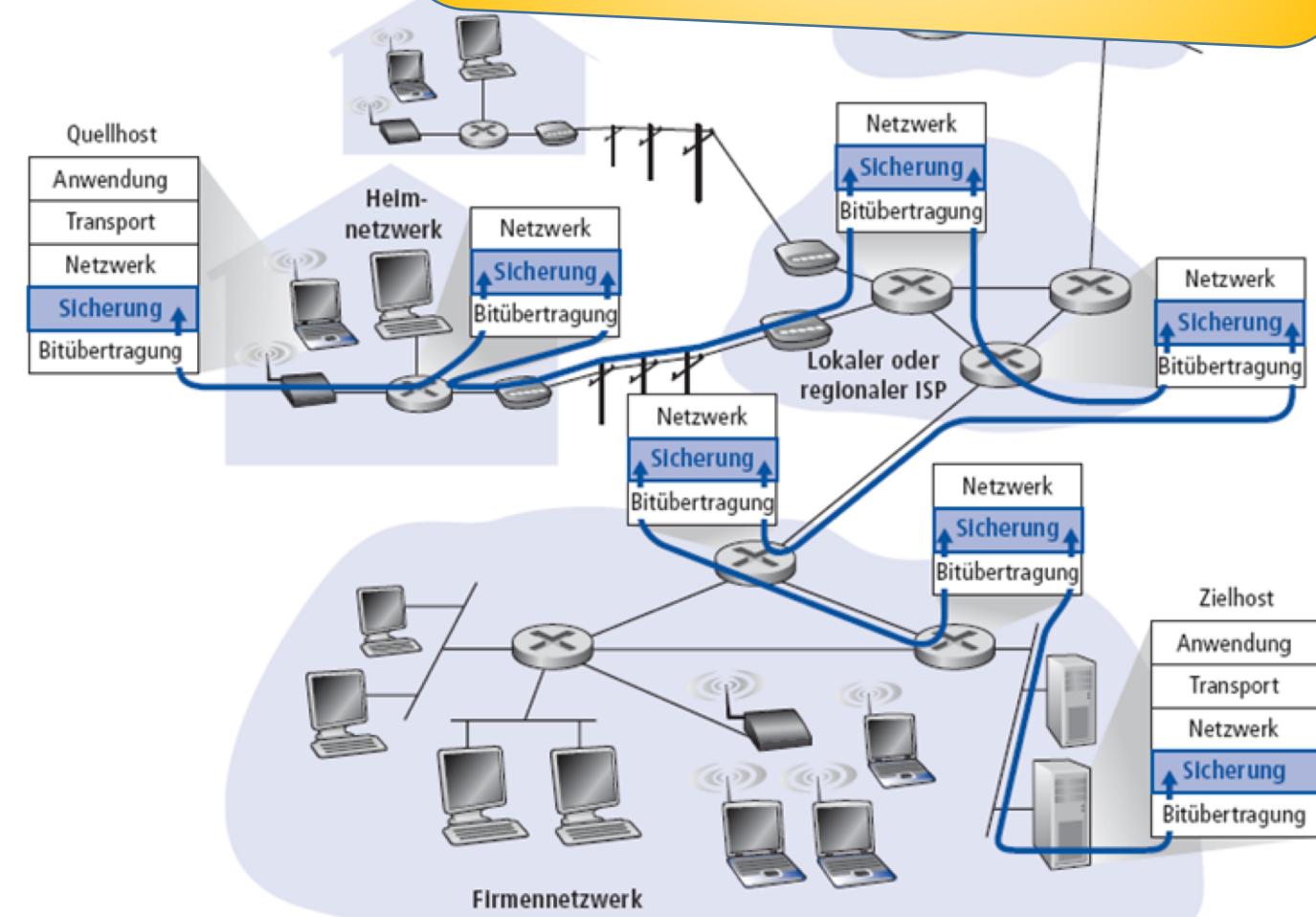


Sicherungsschicht

Terminologie:

- Hosts und Router sind **Knoten**
- Kommunikationskanäle auf dem Weg vom Sender zum Empfänger sind **Links**
- Ein Paket der Sicherungsschicht nennt man **Rahmen** (engl. **Frame**)
- Ein Rahmen enthält üblicherweise ein Datagramm der Netzwerkschicht

Die **Sicherungsschicht** (link layer) hat die Aufgabe, Rahmen von einem Knoten über einen Link zu einem direkt benachbarten Knoten zu transportieren.



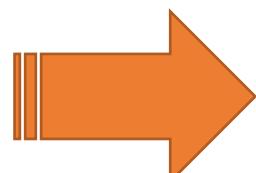
Adressierung von Hosts bzw. Routern

Namen/Alias
im DNS

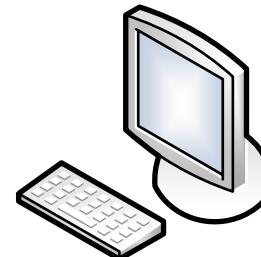


host.netzid.local

Layer 7
(Applikation)

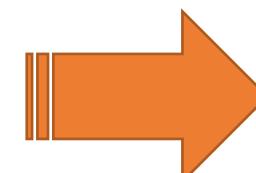


IP-Adresse stellt
„Ortsinformation“
über das Netzwerk
bereit



192.168.178.21

Layer 3
(Netzwerkschicht)



MAC-Adresse: keine
„Ortsinformationen“;
Eindeutigkeit im
lokalen Netzwerk!



C4-54-44-52-A3-85

Layer 2
(Sicherungsschicht)

Ethernet-Adressierung

MAC-Adresse

1A:2B:3C:22:48:F5

8 Bit 8 Bit 8 Bit 8 Bit 8 Bit 8 Bit = 48 Bit

hexadezimale Notation!

Organisationally Unique
Identifier -
herstellerspezifisch vom Hersteller vergeben

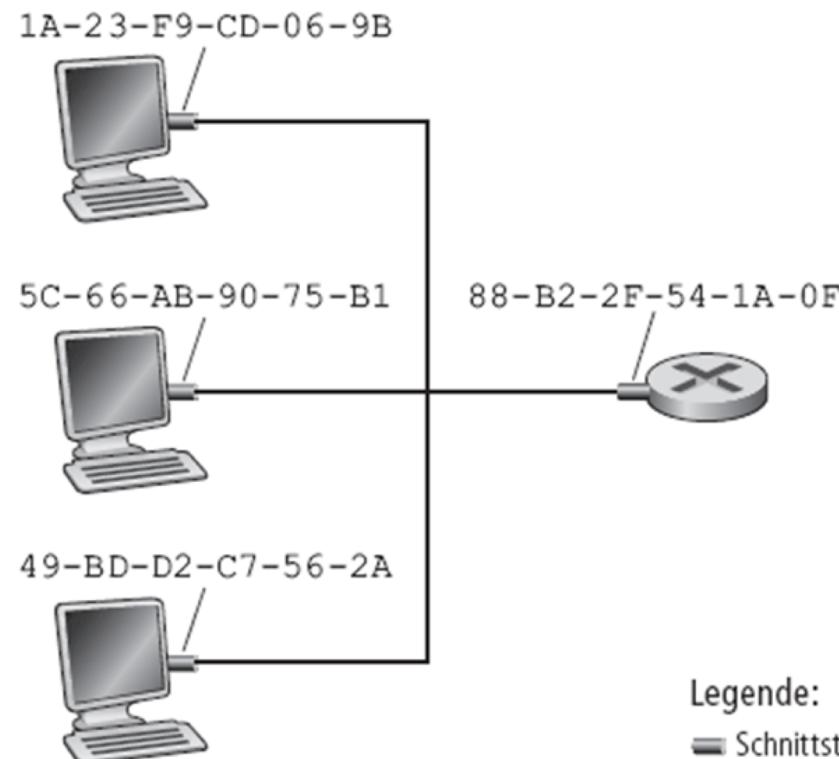
- Weltweit nur einmal vergeben
- Broadcast-Adresse: FF:FF:FF:FF:FF:FF

ARP



MAC-Adressen und ARP

- Jeder Adapter im LAN hat eine eindeutige MAC-Adresse



Wieviele unterschiedliche MAC-Adressen gibt es?

MAC-Adressen und ARP

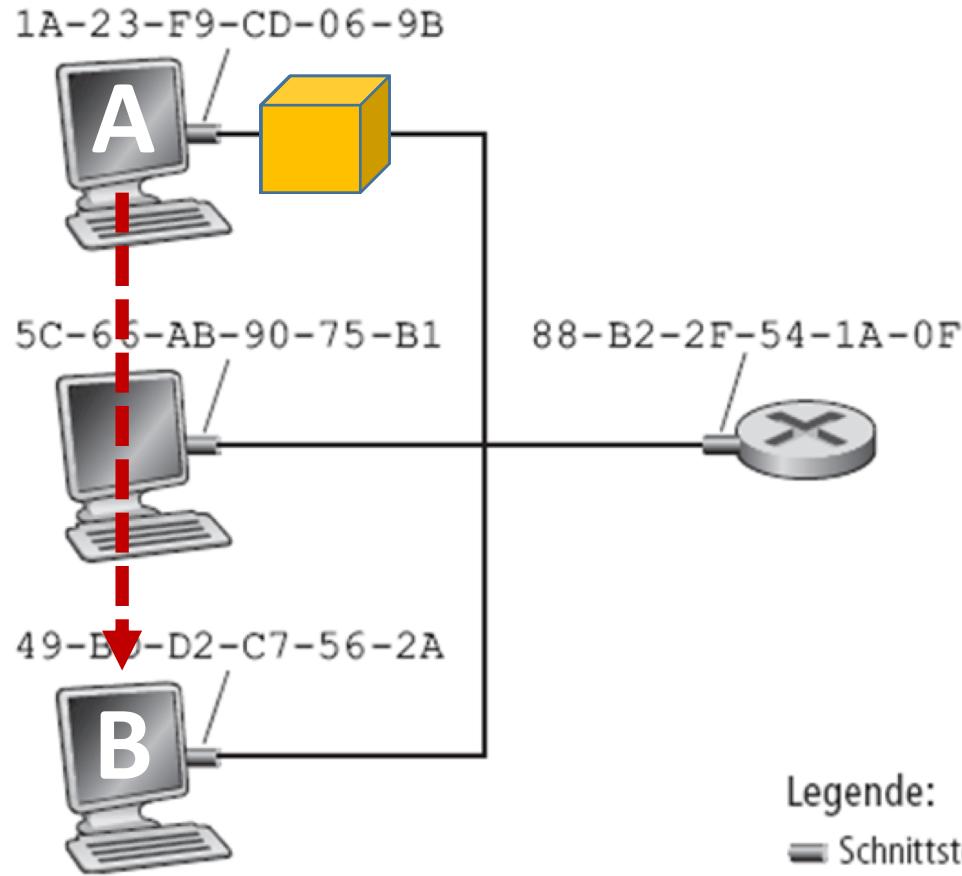
- Die Zuordnung von MAC-Adressen wird von der IEEE überwacht
- Hersteller kaufen einen Teil des Adressraums (um die Eindeutigkeit der Adressen sicherzustellen)
- Analogie:
 - MAC-Adresse: Rentenversicherungsnummer
 - IP-Adresse: Postanschrift
- MAC: flacher Adressraum → Portabilität
 - Eine Netzwerkkarte kann problemlos von einem LAN in ein anderes LAN bewegt werden
- IP: hierarchischer Adressraum → keine Portabilität
 - Adresse hängt vom Subnetz ab, kann nicht (problemlos) in einem anderen LAN verwendet werden

ARP: Address Resolution Protocol

Problem: Wie erfahre ich die MAC-Adr. von B, wenn ich die IP-Adr. von B kenne?

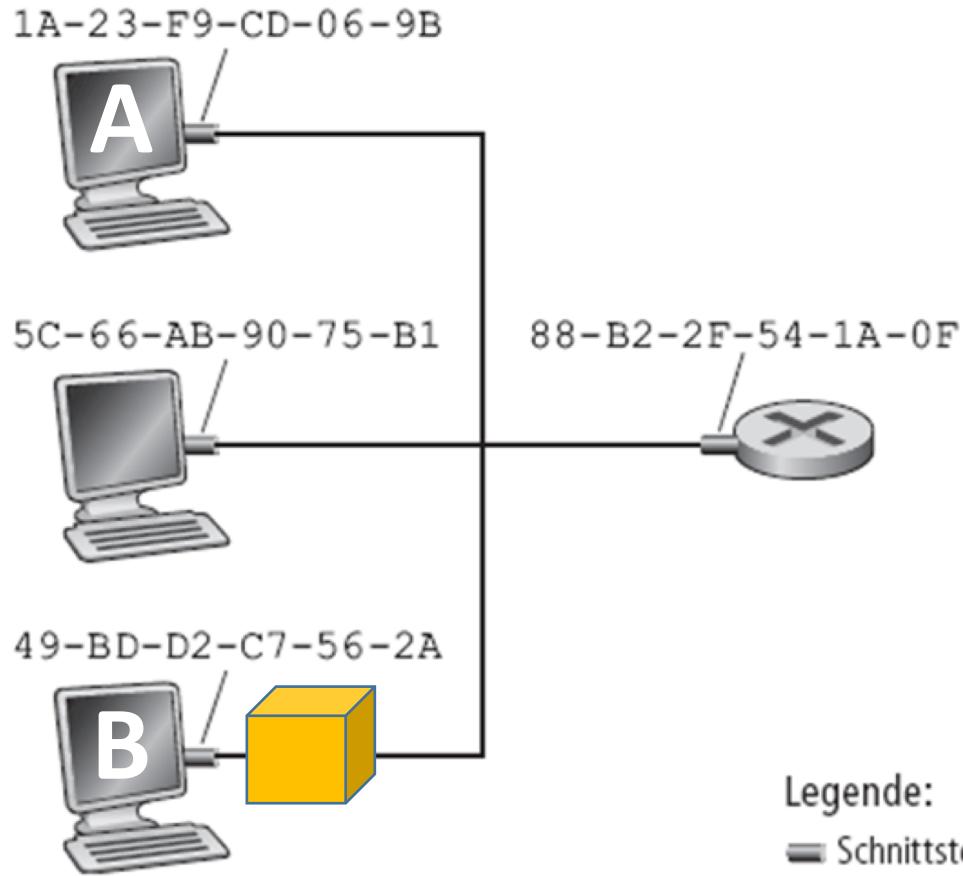
- Verwendung des Address Resolution Protocol (ARP)
- Jedes System in einem LAN hat einen ARP-Cache, in dem die Zuordnung von IP- zu MAC-Adressen gespeichert ist
- Jeder Eintrag ist mit einer Lebenszeit versehen, nach Ablauf der Lebenszeit wird der Eintrag gelöscht (typische Lebenszeit: 20 Minuten)
- Ansehen + Manipulieren des ARP-Caches mit dem Kommando **arp**

ARP: Funktionsweise



- A möchte ein Datagramm an B schicken, die MAC-Adresse von B ist nicht im ARP-Cache von A
- A schickt eine ARP-Query als Broadcast-Rahmen, die Query enthält die IP-Adresse von B
- Empfänger-MAC-Adresse = FF-FF-FF-FF-FF-FF
- Alle Systeme im LAN erhalten diese Anfrage

ARP: Funktionsweise

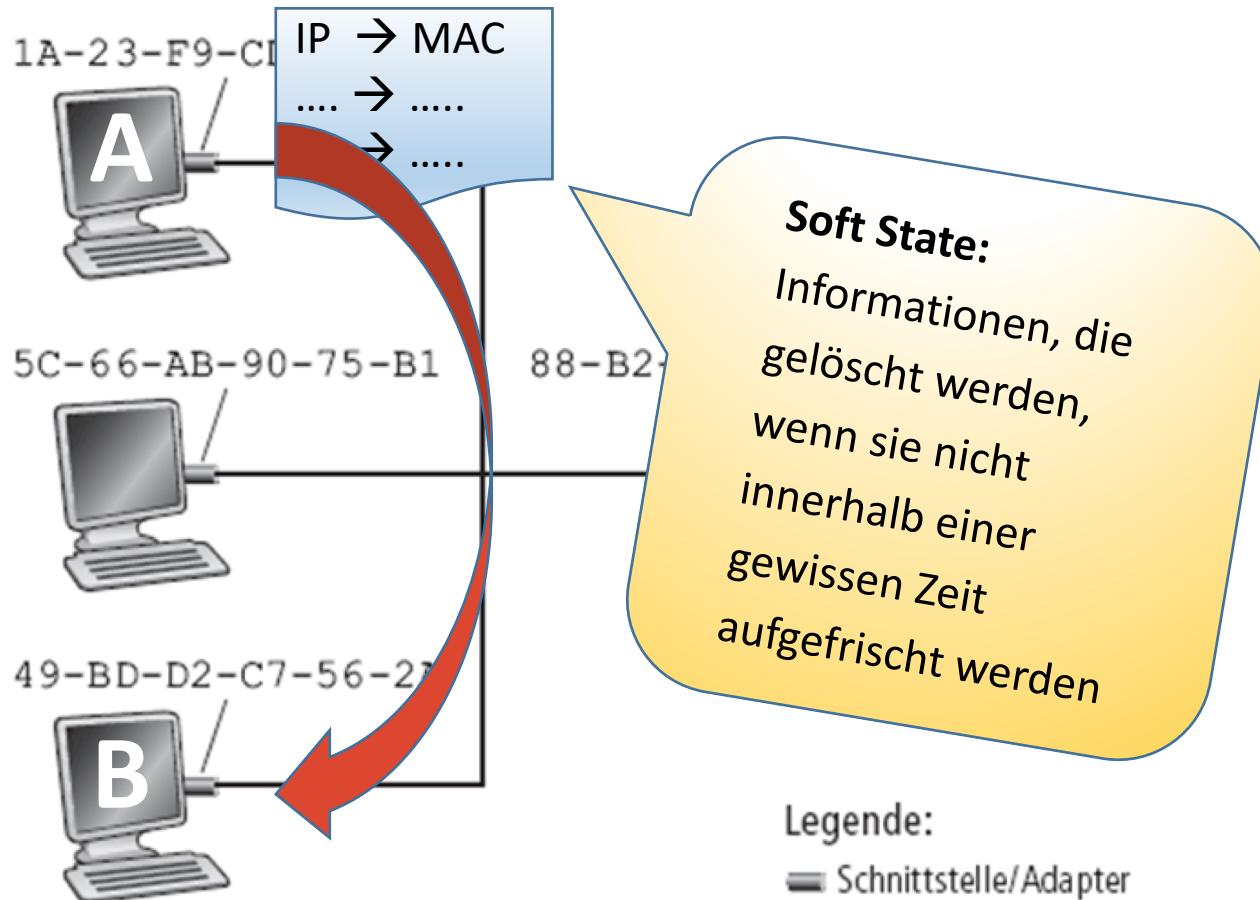


- B empfängt die ARP-Query, erkennt seine IP-Adresse und antwortet A mit seiner eigenen MAC-Adresse
- Empfänger-MAC-Adresse = MAC-Adresse von A

Legende:

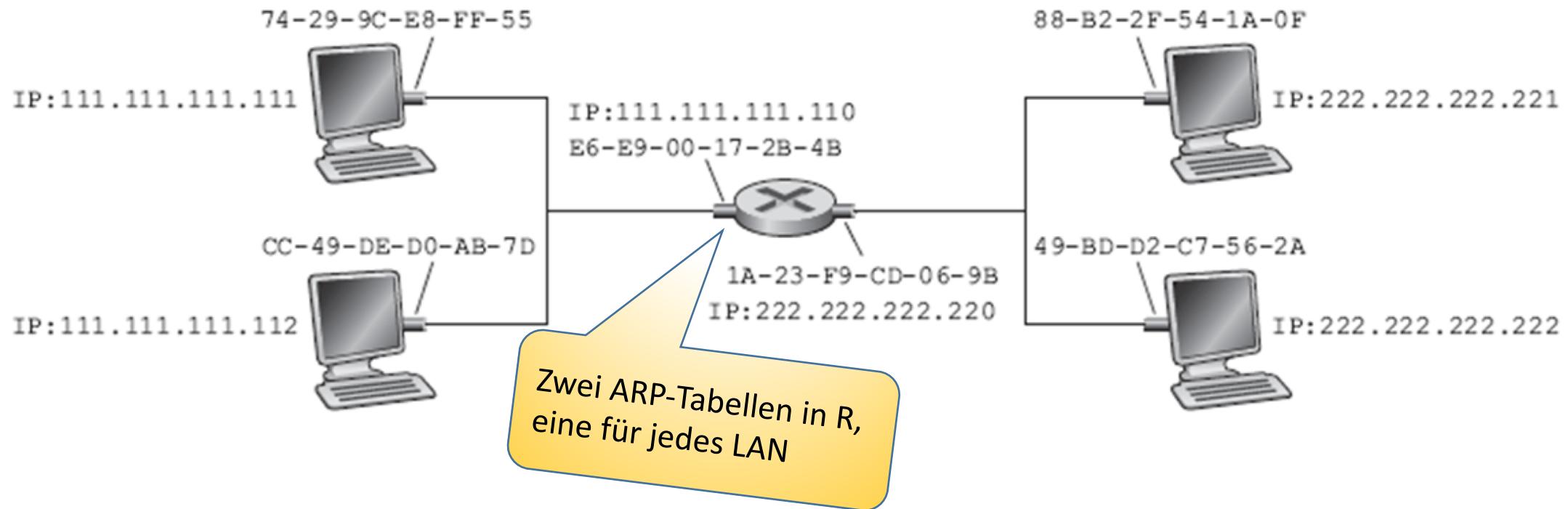
— Schnittstelle/Adapter

ARP: Funktionsweise



- A trägt die Abbildung der IP-Adresse von B auf die MAC-Adresse von B im ARP Cache ein
- A schickt den Datagrammrahmen, der die IP- und die MAC-Adresse von B enthält
- ARP ist “Plug-and-Play”:
- Keine manuelle Konfiguration notwendig

ARP: Routing zwischen zwei LANs



Szenario:

Wir senden ein Datagramm von 111.111.111.111 zu 222.222.222.222 über den Router R

ARP: Routing zwischen zwei LANs



- 111.111.111.111 erstellt ein IP-Datagramm mit dem Ziel 222.222.222.222
- 111.111.111.111 schlägt in seiner IP-Weiterleitungstabelle nach und stellt fest, dass dieses Paket über R (111.111.111.110) weitergeleitet werden muss
- 111.111.111.111 verwendet ARP, um die MAC-Adresse von 111.111.111.110 zu bestimmen
- 111.111.111.111 erstellt einen Rahmen der Sicherungsschicht mit E6-E9-00-17-2B-4B als Zieladresse
- Dieser Rahmen enthält das IP-Datagramm von 111.111.111.111 an 222.222.222.222
- Die Netzwerkkarte von 111.111.111.111 sendet den Rahmen
- Die Netzwerkkarte von 111.111.111.110 empfängt den Rahmen
- R packt das IP-Datagramm aus und stellt fest, dass es für 222.222.222.222 bestimmt ist
- Über die IP-Weiterleitungstabelle stellt R fest, dass er das Datagramm direkt an 222.222.222.222 ausliefern kann
- R verwendet ARP, um die MAC-Adresse von 222.222.222.222 zu erfahren
- R erstellt einen Rahmen, der das Datagramm von 111.111.111.111 an 222.222.222.222 enthält, und sendet es an die so ermittelte MAC-Adresse

Ethernet



Ethernet

- Erste weitverbreitete LAN-Technologie
- Marktbeherrschende LAN-Technologie auf CSMA/CD-Basis
- Billig (einfache Netzwerkkarten für < 10 €)
- Einfacher und billiger als Verfahren mit koordiniertem Kanalzugriff
- Datenrate hat sich über die Zeit stark erhöht:
10, 100, 1.000, 10.000, 40.000, 100.000 Mbit/s

Ethernet-Dienst

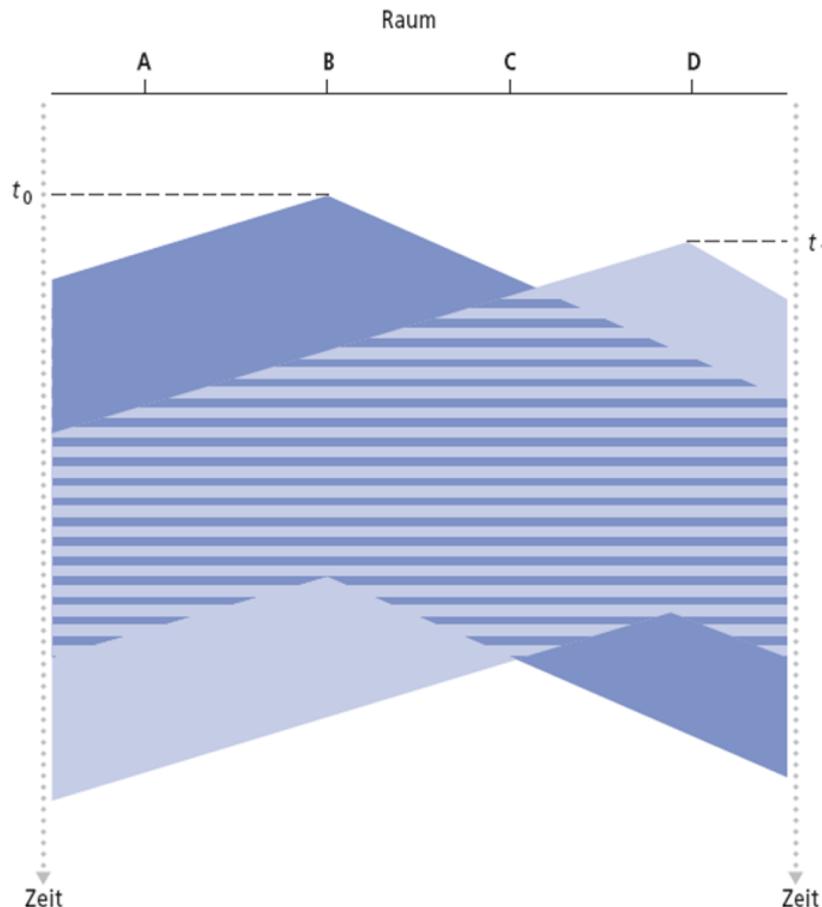
- Ethernet stellt einen unzuverlässigen und verbindungslosen Dienst zum Austausch von Daten zwischen Stationen in einem LAN zur Verfügung
- Verbindungslos: kein Verbindungsauf- und -abbau zwischen Sender und Empfänger
- Unzuverlässig: Wenn Übertragungsfehler (z.B. Bitfehler) vorkommen, werden die Pakete einfach verworfen, es erfolgt keine Übertragungswiederholung
 - Achtung: Kollisionen werden von Ethernet per Collision Detection erkannt und durch Übertragungswiederholung behoben!
 - Andere Rahmenverluste müssen auf höheren Schichten behoben werden oder der Inhalt des Rahmens geht verloren.

CSMA (Carrier Sense Multiple Access)

CSMA: Zuhören vor dem Übertragen

- Wenn der Kanal als leer erkannt wird: übertrage den Rahmen
- Wenn der Kanal als besetzt erkannt wird: Übertragung verschieben
- Analogie: nicht dazwischenreden, wenn jemand anderes gerade etwas sagt!

CSMA: Kollisionen



Kollisionen können immer noch auftreten:

- Die Ausbreitungsverzögerung kann dazu führen, dass man die Übertragung eines anderen Knotens nicht rechtzeitig erkennt

Kollision:

- Dauert die ganze Übertragungszeit
- Zeit wird verschwendet

Beachte:

- Die Auswirkung der Distanz und der Ausbreitungsgeschwindigkeit auf die Wahrscheinlichkeit einer Kollision

CSMA/CD (Collision Detection)

CSMA/CD: Carrier Sensing wie in CSMA

- Kollisionen werden schnell erkannt
- Übertragungen, die kollidieren, werden abgebrochen

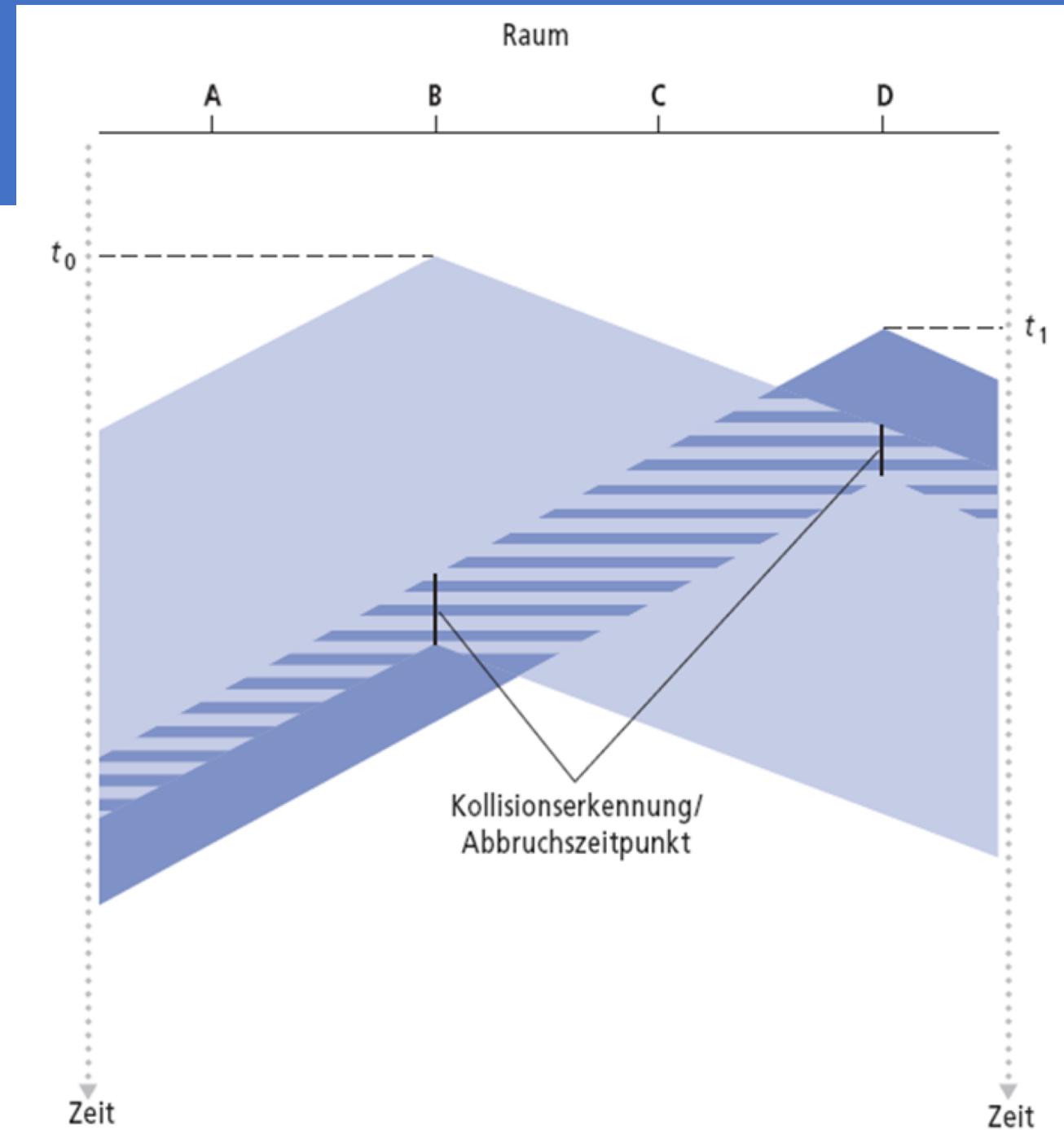
Kollisionserkennung:

- Einfach in drahtgebundenen LANs: messe die empfangene Signalstärke und vergleiche sie mit der gesendeten Signalstärke
- Schwierig in drahtlosen LANs: Die empfangene Signalstärke wird von der eigenen Übertragung dominiert

Analogie: der höfliche Diskussionsteilnehmer

CSMA/CD

Kollisionserkennung:



Effizienz von CSMA/CD

Hängt von der Signallaufzeit t_{prop} zwischen konkurrierenden Stationen ab.

- Wenn diese gegen 0 geht, dann geht auch die Wahrscheinlichkeit für eine Kollision gegen 0 und somit die Effizienz gegen 1.
- Wenn die Signallaufzeit groß wird, dann steigt das Risiko einer Kollision und die Effizienz sinkt.

Hängt von der durchschnittlichen Zeit zur Übertragung eines Paketes $t_{\text{übertragung}}$ (und damit von der Paketgröße) ab.

- Geht diese gegen unendlich, dann geht die Effizienz gegen 1

Bei Existenz vieler sendewilliger Stationen gilt:

- Effizienz $\approx 1/(1+5t_{\text{ausbreitung}}/t_{\text{übertragung}})$

Herleitung dazu in: S. Lam, „A Carrier Sense Multiple Access Protocol for Local Networks,“ Computer Networks, Vol. 4, pp. 21-32, 1980.

CSMA/CD im Ethernet

- Netzwerkkarte bekommt die zu sendenden Daten
- Wenn das Medium von der Netzwerkkarte als frei erkannt wird, dann überträgt sie die Daten in einem Ethernet-Rahmen. Wenn das Medium belegt ist, wartet die Netzwerkkarte, bis das Medium frei wird, und überträgt dann
- Wenn der Rahmen ohne Kollision übertragen wurde: Ende
- Wenn eine Netzwerkkarte eine Kollision feststellt, dann wird die Übertragung abgebrochen und ein Jam-Signal gesendet
- Danach wird „Exponential Backoff“ durchgeführt: Nach der m-ten Kollision zieht die Netzwerkkarte eine Zufallszahl K aus dem Bereich $\{0,1,2,\dots,2^m-1\}$.
- Die Netzwerkkarte wartet $K \cdot 512$ Bit-Zeiten (= Dauer der Übertragung eines Bits) und geht dann zum zweiten Schritt zurück

CSMA/CD im Ethernet

Jam-Signal:

- Sicherstellen, dass alle Sender die Kollision erkennen
- 48 Bit lang
- Illegale physikalische Werte

Bit-Zeit:

- 0,1 Mikrosekunden bei 10 MBit/s Ethernet
- Bei $m = 10$ beträgt die durchschnittliche Wartezeit ~ 50 ms

Exponential Backoff:

- Ziel: Frequenz der Übertragungswiederholung der aktuellen Lastsituation anpassen
- Bei hoher Last werden mehrere Kollisionen in Folge passieren, bis das richtige Intervall für die Zufallszahl gefunden ist
- Bei der ersten Kollision: wähle K aus $\{0,1\}$
- Bei der zweiten Kollision: wähle K aus $\{0,1,2,3\} \dots$
- Bei der zehnten Kollision: wähle K aus $\{0,1,2,3,4,\dots,1023\}$

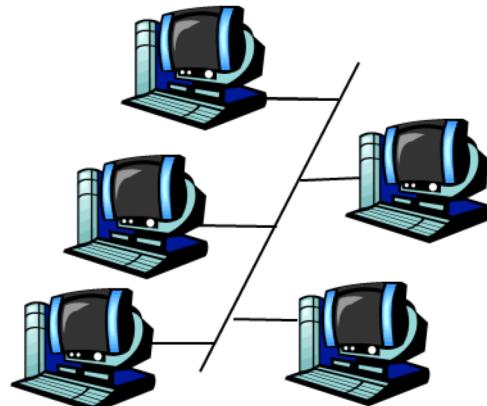
Netzwerk- Komponenten



Ethernet-Topologie

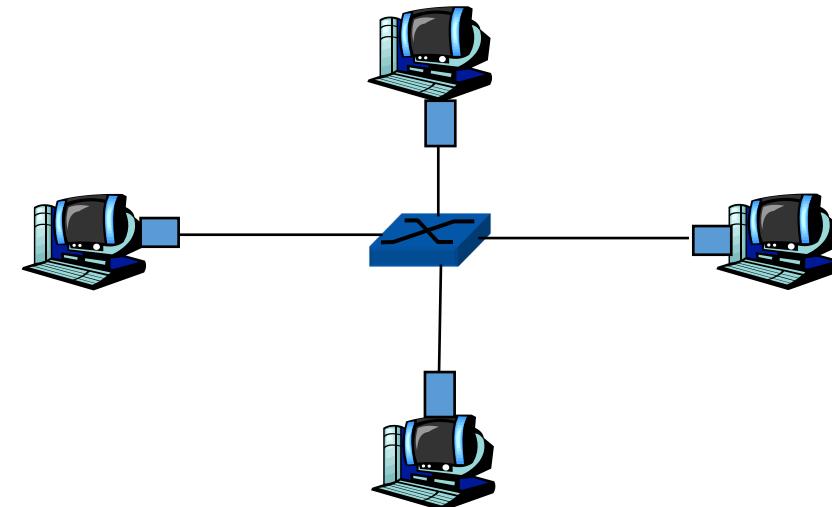
Bus-Topologie bis Mitte der 90er Jahre

- Alle Knoten in einer Kollisionsdomäne (die Übertragung eines Knotens konnte mit der Übertragung jedes anderen Knotens kollidieren)



Heute: Stern-Topologie

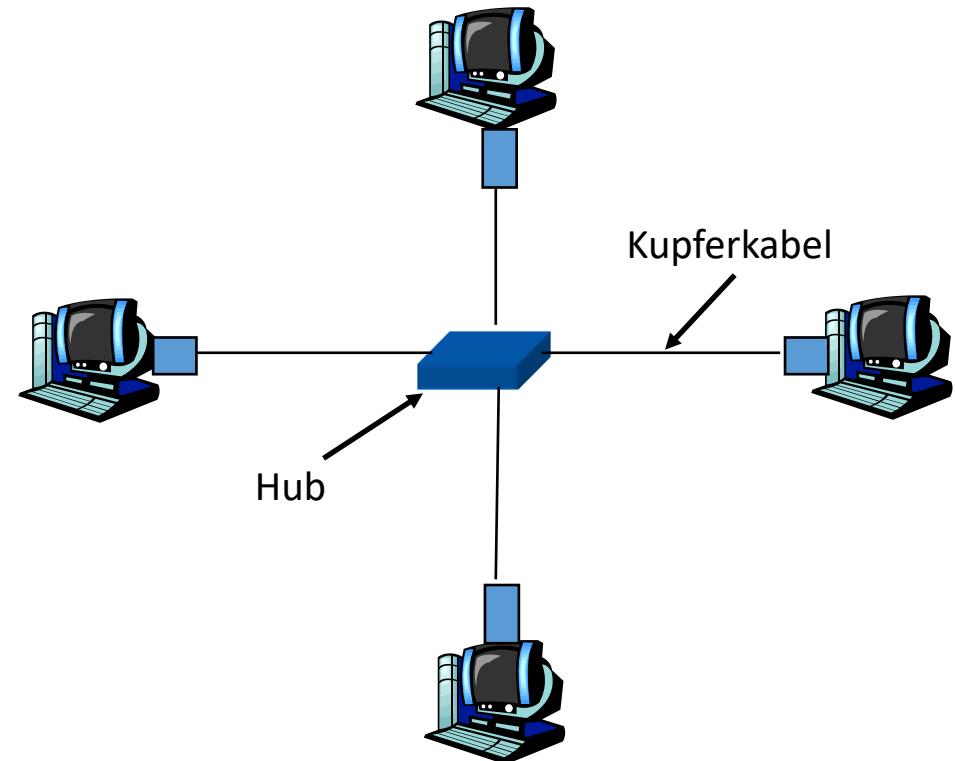
- Aktiver Switch im Zentrum
- Endsysteme sind an den Switch angeschlossen, ihre Übertragungen kollidieren nicht mehr miteinander



Hubs bzw. Repeater

... gehören zur **Bitübertragungsschicht** (Layer 1):

- Bits, die auf einem Link ankommen, werden auf alle anderen Links mit der Eingangsrate kopiert
- Die Übertragung aller über einen Hub verbundenen Knoten kann miteinander kollidieren
- Ein Hub puffert keine Rahmen
- Kein CSMA/CD im Hub: Die Netzwerkkarten der Hosts führen CSMA/CD aus (und erkennen Kollisionen)



Switch

Ein Switch arbeitet auf der **Sicherungsschicht** (Layer2):

- Empfängt Ethernet-Rahmen, puffert sie und leitet sie weiter
- Untersucht den Header eines Rahmens und leitet ihn gezielt anhand der Empfängeradresse auf eine Ausgangsleitung weiter
- Wenn ein Frame von einem Switch weitergeleitet wird, dann verwendet der Switch CSMA/CD

Transparent

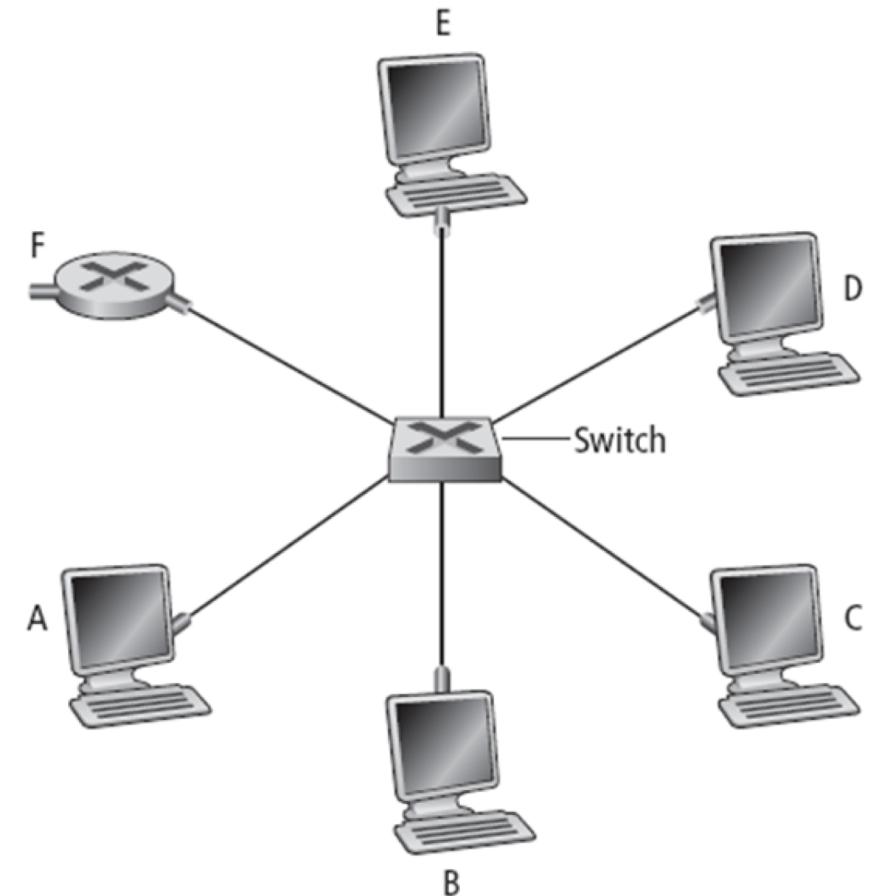
- Endsysteme wissen nichts über die Gegenwart eines Switches

Plug-and-Play, selbst lernend

- Switches müssen nicht konfiguriert werden

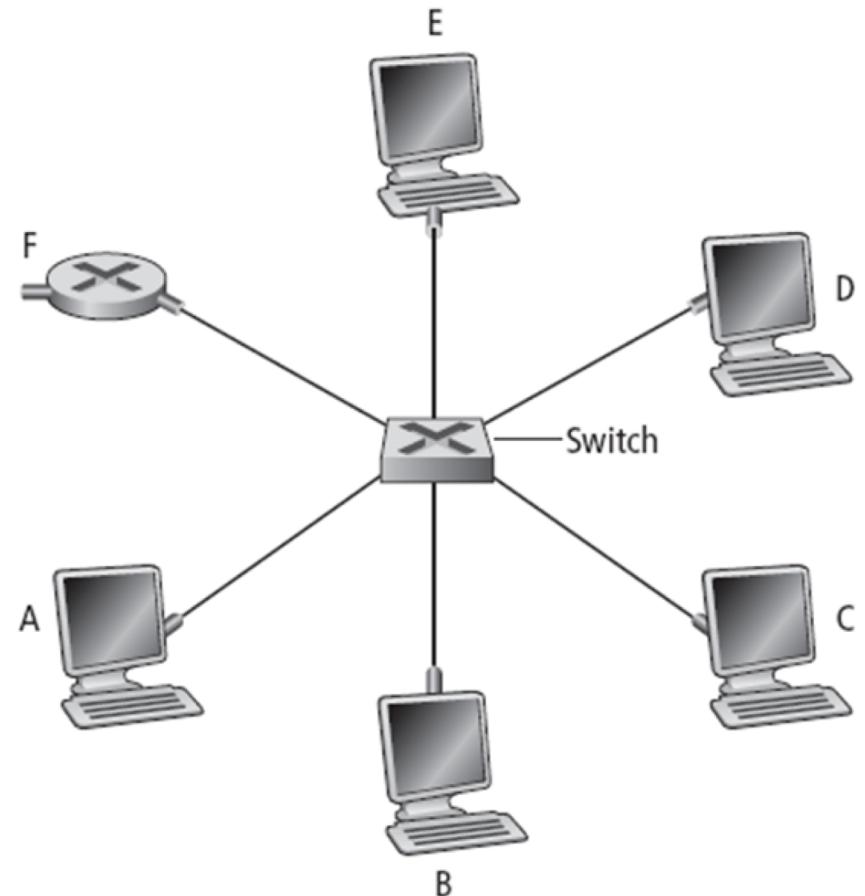
Switch: ermöglicht mehrere gleichzeitige Übertragungen

- Jeder Host hat einen eigenen Link zum Switch
- Ein Switch puffert Rahmen
- Das Ethernet-Protokoll wird auf jedem Link verwendet, es kann jedoch keine Kollisionen geben; Vollduplex
 - Jeder Link ist eine eigene Kollisionsdomäne
- Switching: E-nach-B und D-nach-A gleichzeitig ohne Kollisionen möglich
 - Geht nicht mit einem Hub!



Switch

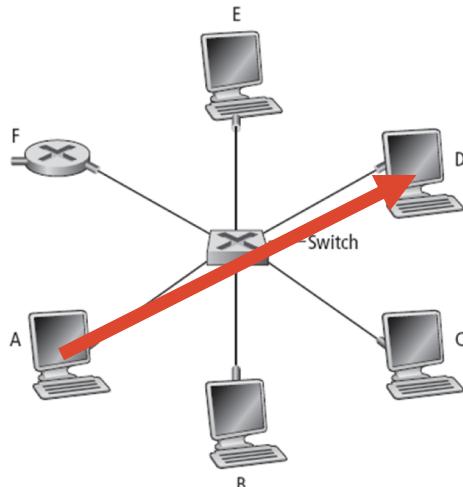
- Woher weiß der Switch, über welches Interface/welchen Port z.B. das Interface des Endsystems D erreichbar ist?



Switching-Tabelle

Jeder Switch besitzt eine Switch-Tabelle mit folgenden Einträgen:

- MAC-Adresse eines Hosts
- Schnittstelle, über die der Host erreicht werden kann
- Zeitstempel



Ein Switch lernt, welche Hosts er über eine gegebene Schnittstelle erreichen kann:

- Wenn er einen Rahmen empfängt, dann lernt der Switch, dass der Absender hinter dieser Schnittstelle liegen muss
- Er trägt diese Information in die Switch-Tabelle ein

Beispiel: A schickt einen Rahmen an D

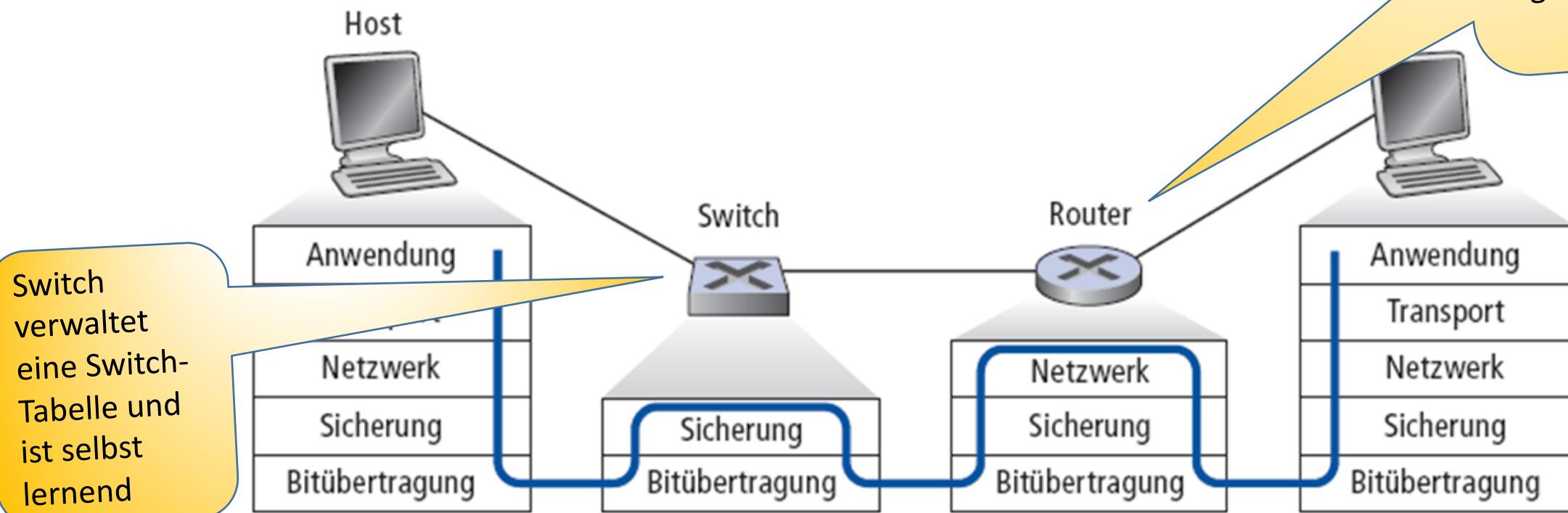
MAC-Adresse	Interface	TTL
A	5	60

Vergleich Switch vs. Router

Beide speichern Pakete und leiten diese weiter

- Router: auf der Netzwerkebene (verwendet IP-Adressen)
- Switch: gehört zur Sicherungsschicht (verwendet MAC-Adressen)

Router verwaltet eine Weiterleitungstabelle und führt Routingsalgorithmen aus



Zusammenfassender Vergleich

	Hubs	Router	Switches
Isolierung von Verkehr	nein	ja	ja
Plug-and-Play	ja	nein	ja
Optimales Routing	nein	ja	nein

Recherche: Layer2-/Layer2+-/Layer3-Switches?

Im Handel werden einige verschiedene Switches angeboten, u.a.:

- Layer2-Switch
- Layer2+-Switch
- Layer3-Switch

Welche Bedeutung haben diese Bezeichnungen? Wie unterscheiden sich die unterschiedlichen „Switch-Klassen“?

Virtuelle Netzwerke (VLAN)

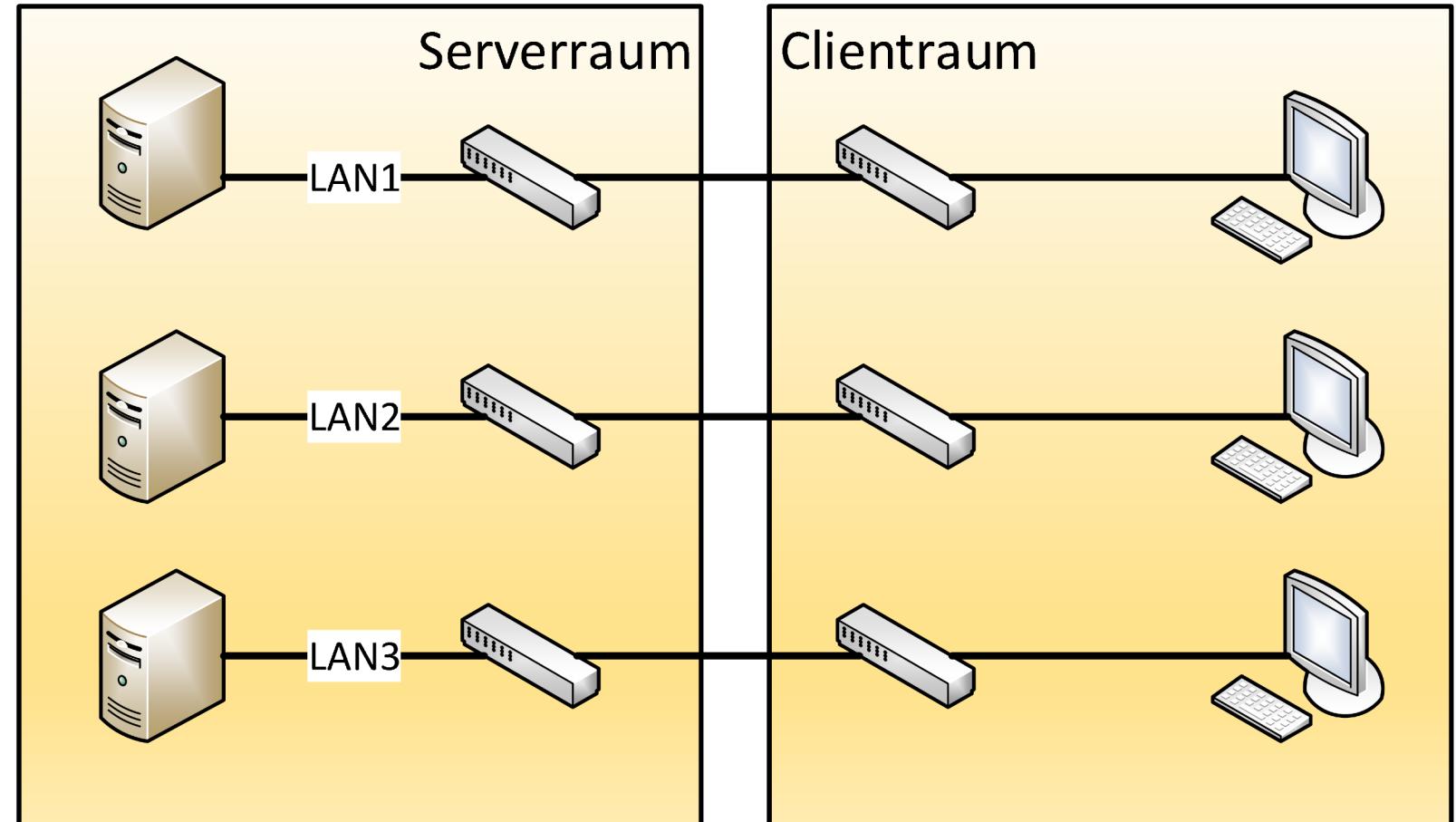


Abbildung von verschiedenen Netzstrukturen

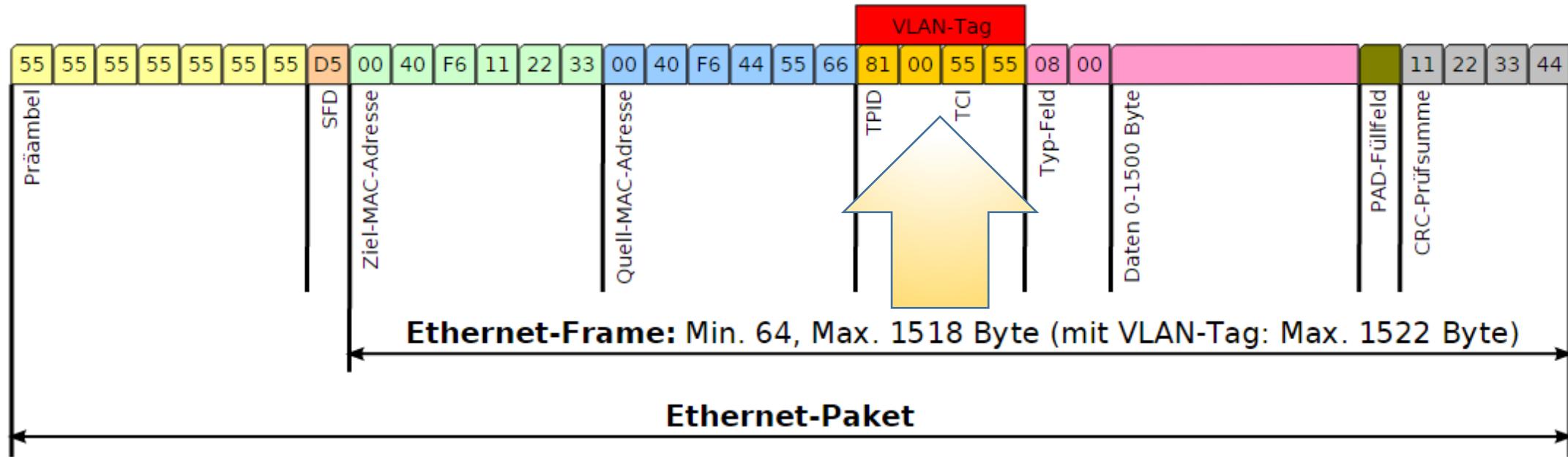
- 3 Netzwerke
- physikalisch getrennt
- eigene Komponenten pro Netz (Switches)

Layer 2 bietet dafür eine andere Lösung:

VLAN



VLAN (Virtual LAN)



- über das VLAN-Tag lassen sich Netze virtuell trennen
- VLAN kann Port-based auf einem Switch oder tagged im ganzen Netzwerk genutzt werden

Abbildung von verschiedenen Netzstrukturen

- 3 Netzwerke
- virtuell getrennt
- Einsatz von **VLANs**

