

Folien zur Veranstaltung Rechnernetze in der AI Wintersemester 2018 (Teil 6)

Prof. Dr. Franz Korf
Franz.Korf@haw-hamburg.de

Basierend auf der RN Vorlesung von M. Hübner

Kapitel 6: Sicherungsschicht & LAN

Gliederung

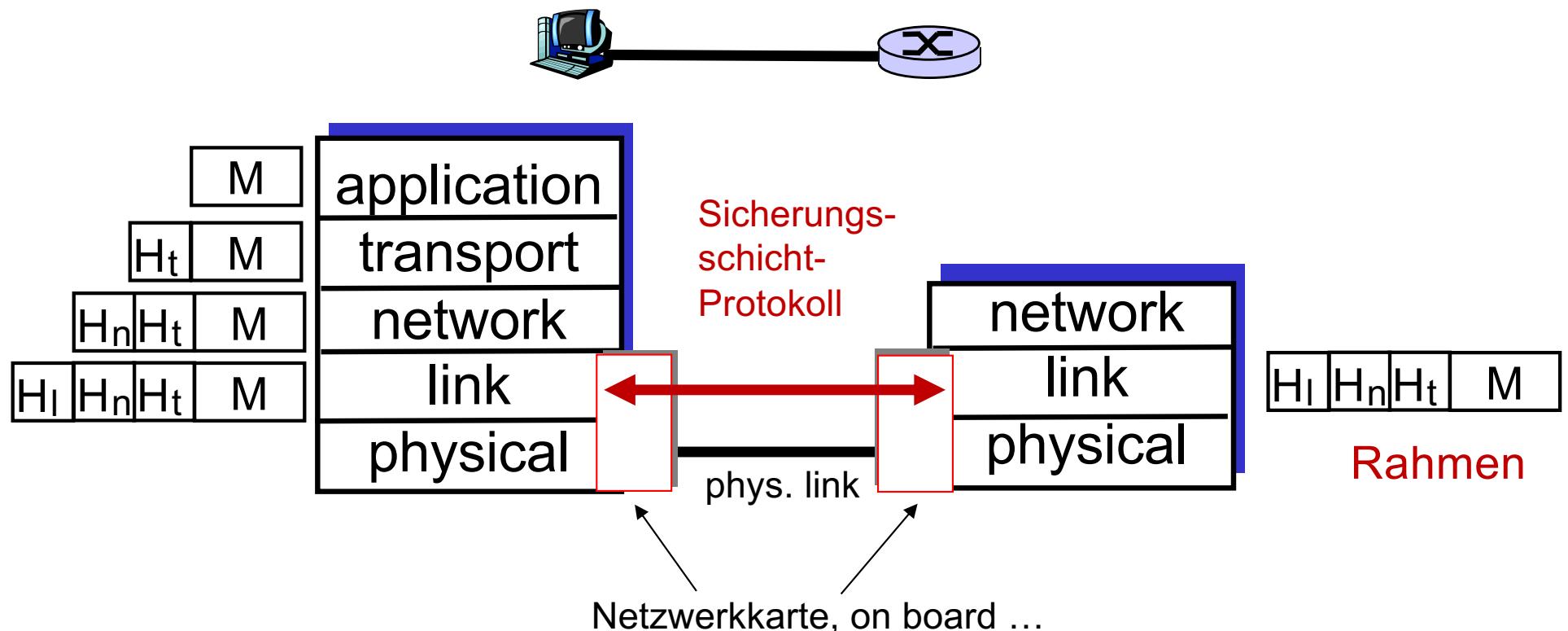
- Einführung und Grundlagen 
- Punkt-zu-Punkt-Protokolle
- Mehrfachzugriffsprotokolle (MAC)
- LAN-Adressen und ARP
- Ethernet
- Switches
- Zusammenfassung

Textbuch zu diesem Kapitel: J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz, Kapitel 5

**Folien und Abbildung teilweise aus:
J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz**

Sicherungsschicht: Kontext

- Verbindung zwischen zwei *physikalisch verbundene* Geräte:
 - Host-Router, Router-Router, Host-Host
- Dateneinheit: *Frame ("Rahmen")*



Dienste der Sicherungsschicht

Framing

- Kapselt die Datagramme in Rahmen, fügt Header, **Trailer** hinzu
 - Problem: Erkennung von Rahmengrenzen im Bitstrom

Medienzugriff

- Implementiert Kanalzugangsprotokoll (bei Broadcast-Medium muss der Zugriff koordiniert werden)

Zuverlässige Zustellung

- Garantiert eine fehlerfreie Übertragung über den Link
- Ist aus Kapitel 3 bekannt
- Bei einer hohen Fehlerrate wichtig, damit Fehler lokal korrigiert werden und eine erneute Übertragung erspart bleibt (Funknetze)
- Bei einer kleiner Fehlerrate entfällt dieser Dienst oftmals (Kabelnetze)

Dienste der Sicherungsschicht (Fortsetzung)

Fehlererkennung

- Fehler durch Signalabschwächung oder Störungen.
- Empfänger entdeckt Fehler:
 - Signalisiert Sender das Paket neu zu versenden oder verwirft es

Fehlerkorrektur

- Empfänger identifiziert und korrigiert Bitfehler ohne neue Paketanforderung

Flusskontrolle

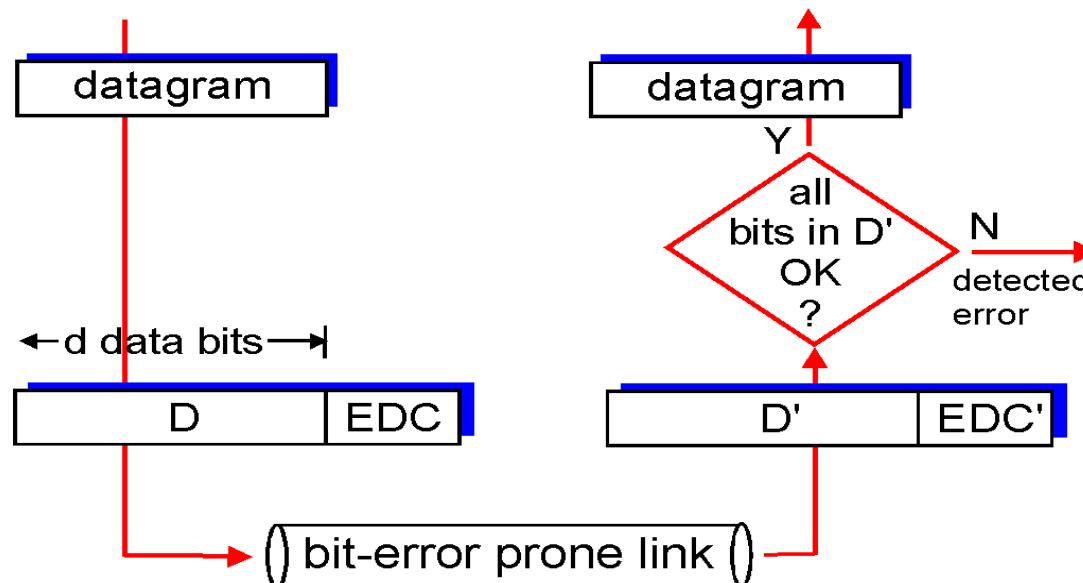
- Ausgleich der Datenrate zwischen Sender und Empfänger

Sicherungsschicht: Implementierung

- Implementiert in der HW Netzwerkkarte (“Adapter”)
 - z.B. Ethernet-Karte, WLAN-Adapter
 - Enthält typischerweise: RAM, Signalprozessor-Chips, Bus-Interface, Leitungs-Interface
 - 48 Bit-Adresse (“**LAN-Adresse**” oder “**MAC-Adresse**” oder “**physische Adresse**” oder “**Ethernet-Adresse**”) in der Netzwerkkarte einprogrammiert.
 - Die MAC Adresse ist weltweit eindeutig über MAC Adressbereich, der einem Herstellung zugewiesen wird.
- Implementierung in der SW / Treiber
 - Bereitstellung der Daten im Speicher (Header und Payload)
 - Fehlerbehandlung – Fehlererkennung in HW

Fehlerkennung auf Bitebene: Generelle Situation

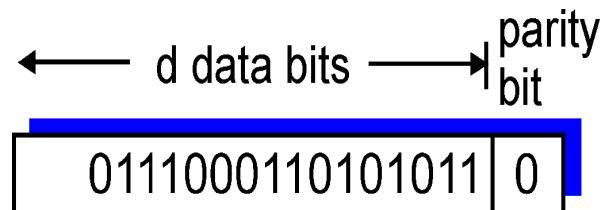
- Wird i.d.R. in HW realisiert
- **EDC** = Error Detection and Correction Bits (Redundanz)
- **D** = Daten, die durch Fehlererkennung geschützt werden
- Fehlererkennung nicht 100% verlässlich!
 - Auf Fehlerklassen optimiert
 - Das Protokoll könnte Fehler "übersehen" – sehr selten
 - größeres EDC-Feld ergibt sicherere Fehlererkennung und -korrektur



Verfahren: Paritätsprüfung

Single Bit Parity

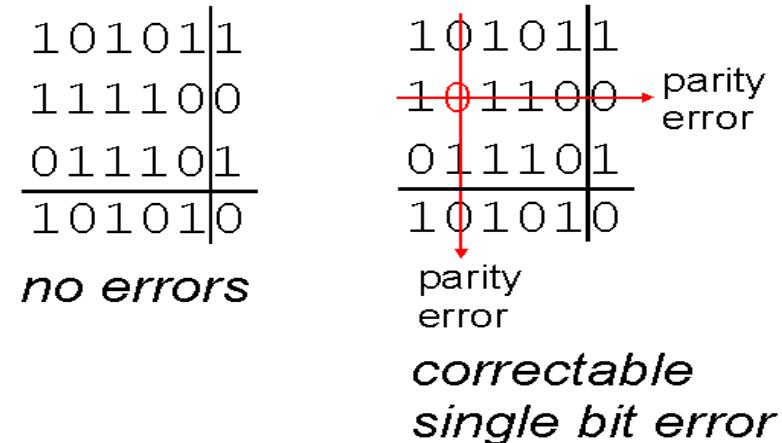
- Erkennt Einzelbitfehler



- Odd Parity: Die Gesamtzahl der 1 ist ungerade
- Even Parity: Die Gesamtzahl der 1 ist gerade
- Eine gerade Anzahl von Bitfehlern wird nicht erkannt.
 - Problem, wenn Fehler als Burst auftreten

Verfahren: Zweidimensionale Parity

- Ansatz: Die d zu übertragenden Datenbits wird in i Zeilen und j Spalten aufgeteilt.
- Für jeder Zeile und für jede Spalte wird ein Parity Bit hinzugefügt.
- 1 Bit Fehler werden korrigiert
- 2 Bit Fehler werden erkannt.
- **FEC:** Forward Error Correction



Verfahren: UDP-Prüfsumme

Ziel

- Entdecke Bit-Fehler im übertragenen UDP-Segment

Sender

- Behandelt Segmentinhalt als Folge von 16-Bit Integer-Zahlen, die aufsummiert werden.
- Prüfsumme: Addition (Einer-Komplement-Summe) des Segment-Inhalts
- Sender schreibt Prüfsumme in das UDP – Prüfsummenfeld

Empfänger

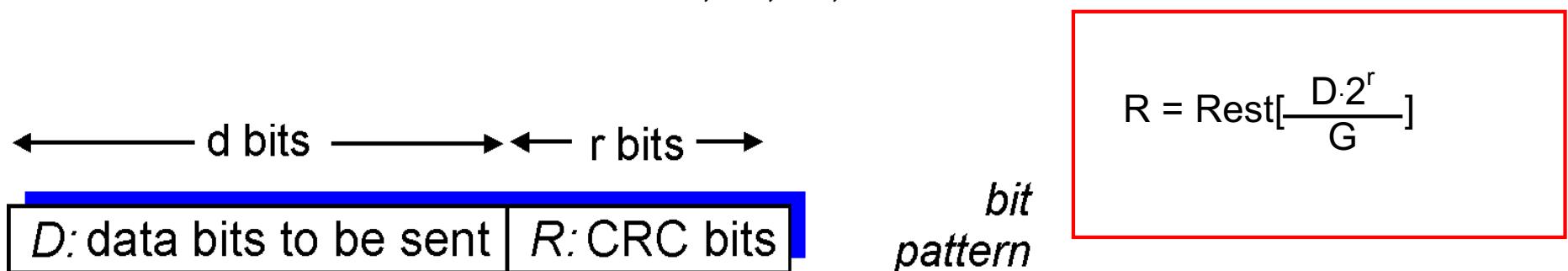
- Berechnet Prüfsumme des empfangenen Segments (inklusive Prüfsummenfeld)
- Ergebnis 0xFFFF ⇔ kein Fehler erkannt

Diskussion

- Erkennt wenig Fehler im Vergleich zu CRC
- Aber einfach in SW realisierbar

Verfahren: Cyclic Redundancy Check (CRC)

- Betrachte Datenbits, **D**, als eine binäre Zahl
- Wähle Bitmuster der Länge $r+1$ (Generator), **G**
- Ziel: Wähle r CRC-Bits **R**, so dass
 - $\langle D|R \rangle$ genau durch G teilbar ist ($\text{mod } 2 \rightarrow$ Addition ohne Übertrag = XOR)
 - Empfänger kennt G, teilt $\langle D|R \rangle$ durch G. Falls Rest bleibt: Fehler!
- Entdeckt alle aufeinander folgenden Fehler (“Burst-Fehler”) mit weniger als $r+1$ Bits und jede ungerade Zahl an Bitfehlern
- G ist international normiert für $r = 8, 12, 16, 32$



$$D * 2^r \quad \text{XOR} \quad R$$

*mathematical
formula*

Beispiel

$$G = 1001 \quad D = 101110 \quad r = 3$$

$$101110 / 1001 = 101011$$

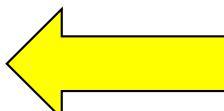
$$\begin{array}{r}
 101110 \\
 \underline{-} 1001 \\
 \hline
 101 \\
 -000 \\
 \hline
 1010 \\
 \underline{-} 1001 \\
 \hline
 110 \\
 -000 \\
 \hline
 1100 \\
 \underline{-} 1001 \\
 \hline
 1010 \\
 \underline{-} 1001 \\
 \hline
 011
 \end{array}
 = R$$

$$D \cdot R / G = 101110 \cdot 011 / 1001 =$$

$$\begin{array}{r}
 101110 \\
 \underline{-} 1001 \\
 \hline
 101 \\
 -000 \\
 \hline
 1010 \\
 \underline{-} 1001 \\
 \hline
 110 \\
 -000 \\
 \hline
 1100 \\
 \underline{-} 1001 \\
 \hline
 1010 \\
 \underline{-} 1001 \\
 \hline
 011
 \end{array}$$

Kapitel 6: Sicherungsschicht & LAN

Gliederung

- Einführung und Grundlagen
 - Punkt-zu-Punkt-Protokolle
 - Mehrfachzugriffsprotokolle (MAC)
 - LAN-Adressen und ARP
 - Ethernet
 - Switches
 - Zusammenfassung
- 

Textbuch zu diesem Kapitel: J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz, Kapitel 5

Folien und Abbildung teilweise aus:

J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz

Punkt zu Punkt Sicherungsschichtprotokolle

Ein Sender, ein Empfänger, eine Verbindung:

- einfacher als “Broadcast”-Medien:
- Kein Medium-Zugangsprotokoll (MAC)
- Explizite MAC-Adressen sind unnötig

- z.B.: Einwahlverbindung (Modem), ISDN, DSL

Populäre Punkt zu Punkt Protokolle:

- PPP (point-to-point protocol)
- HDLC: High level data link control
(Sicherungsschicht, war mal “high layer” im Protokollstack!)

PPP [RFC 1661/1662] Design-Anforderungen

Verpacken von Paketen:

- Einpacken des Netzwerkschichtdatagramms in den Rahmen der Sicherungsschicht
- Transportiert Netzwerkschichtdaten mehrerer Netzwerkschichtprotokolle (nicht nur IP)
 - Demultiplex-Fähigkeit zur Netzwerkschicht

Bit-Transparenz:

- Muss jedes Bitmuster im Datenfeld transportieren können

Fehlererkennung (keine Korrektur)

Verbindungsaktivität:

- entdeckt und meldet Verbindungsfehler zur Netzwerkschicht

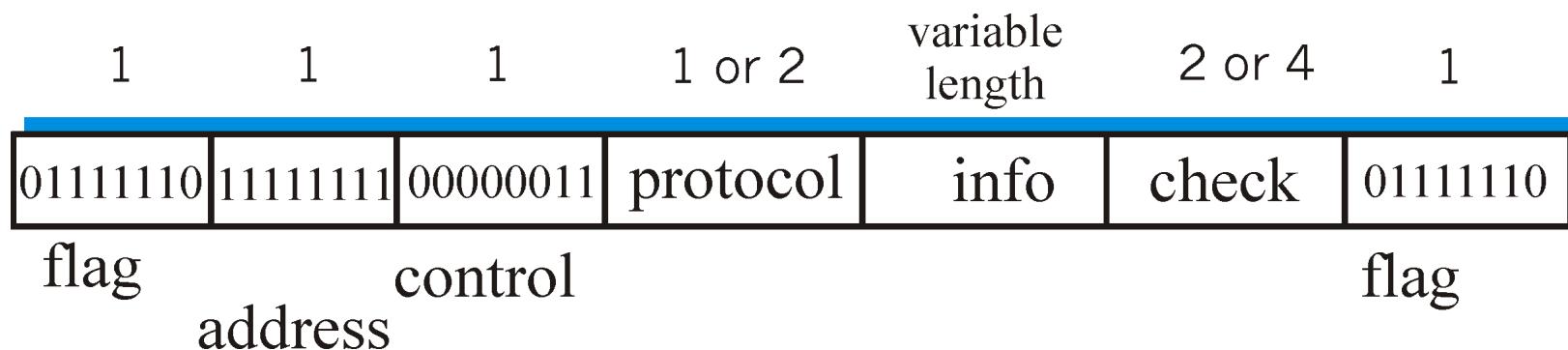
Netzwerkschicht-Adressverhandlung:

- Endpunkt kann die Netzwerkschicht-Adresse (IP, ..) des Kommunikationspartners lernen / konfigurieren

PPP unterstützt nicht

- Fehlerkorrektur
- Flusskontrolle
- “multipoint” Verbindungen (ein Master, N Slaves an einem Kabel)

PPP Datenrahmen



flag Begrenzung (Rahmenanfang/-ende)

address unnötig (ist eine Option)

control tut nichts; in Zukunft evtl. unterschiedliche Kontrollfelder

protocol Protokoll der nächsten Schicht (also PPP-LCP, IP, IPCP, IPX etc.)

info Daten der nächsthöheren Schicht

check CRC für Fehlererkennung

Byte Stuffing

Bit-Transparenz bedeutet: Datenfeld muss auch <01111110> enthalten können
(Anfangs-/ Endflagbyte)

Standard Technik, wenn ein Datenbyte den Wert eines Kontrollbytes haben kann.

Frage: Ist empfangenes <01111110> eine Rahmengrenze oder Teil der Nutzdaten?

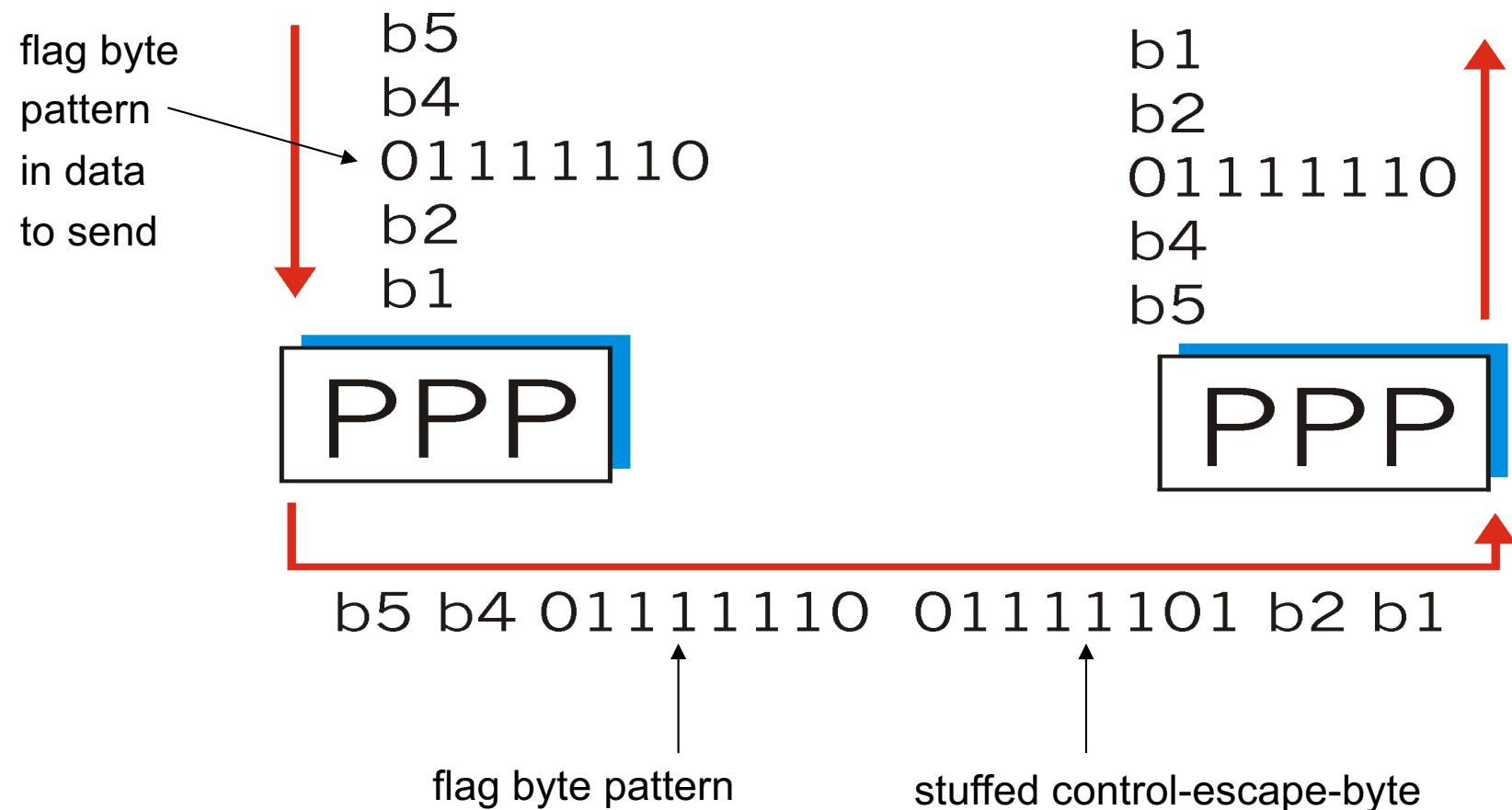
Sender

- Addiert (“stopft”) ein zusätzliches **Control-Escape-Byte** <01111101> vor jedes <01111110> und <01111101> Daten-Byte

Empfänger

- Wenn <01111101> <01111101> (Control-Escape/Control-Escape) oder <01111101> <01111110> (Control-Escape/Flag) im Datenstrom gefunden:
Verwirf zusätzliches <01111101> Control-Escape-Byte
(Flag- oder Control-Escape-Byte war zufällig im Originaldatenstrom enthalten)
- Wenn einzelnes <01111110> Flag-Byte im Datenstrom gefunden: Interpretation als Rahmengrenze ist eindeutig!

Beispiel

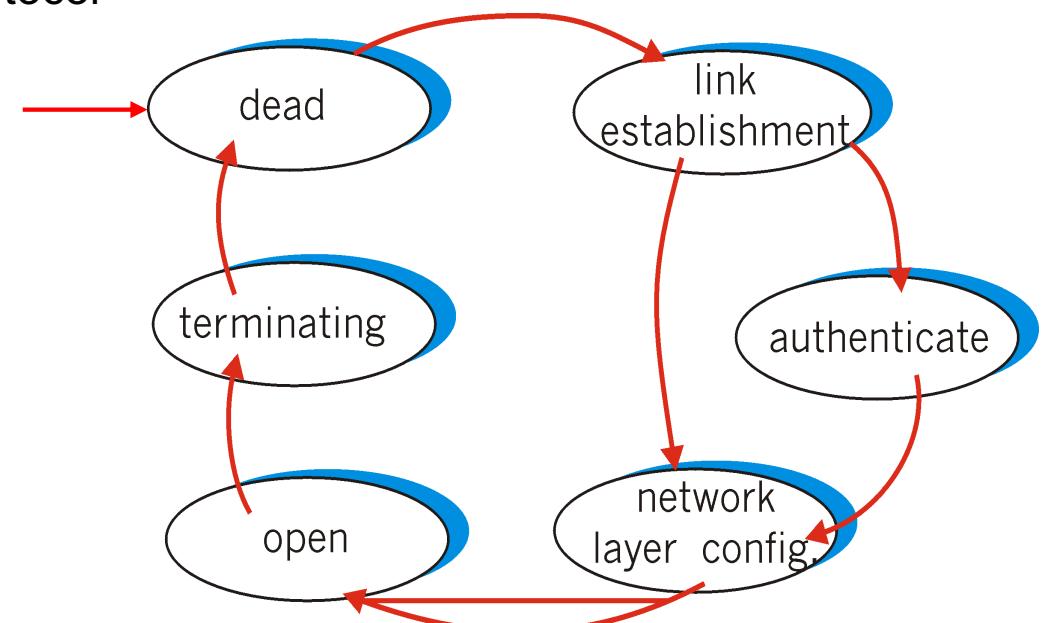


PPP: Escaped Byte wird mit XOR 0x20 verknüpft:
Einfaches Suchen von Rahmenanfang/Ende.

PPP Link Control Protocol (LCP)

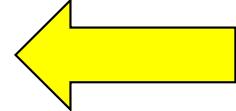
Vor Austausch von Daten der Netzwerkschicht muss die Sicherungsschicht die

- **PPP Verbindung konfigurieren** (max. Rahmenlänge, Authentifizierung)
- Dies geschieht über den Austausch von Frames
- **Netzwerkschicht-Info lernen/konfigurieren**
 - für IP: übertrage IP Control Protocol (IPCP) Nachricht, um IP-Adresse zu konfigurieren



Kapitel 6: Sicherungsschicht & LAN

Gliederung

- Einführung und Grundlagen
- Punkt-zu-Punkt-Protokolle
- Mehrfachzugriffsprotokolle (MAC) 
- LAN-Adressen und ARP
- Ethernet
- Switches
- Zusammenfassung

Textbuch zu diesem Kapitel: J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz, Kapitel 5

Folien und Abbildung teilweise aus:

J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz

Mehrfachzugriffsprotokolle (MAC Protokolle)

Situation

- Einzelner gemeinsam genutzter Kommunikationskanal
- Zwei oder mehr gleichzeitige Übertragungen: Interferenz → Daten unbrauchbar
 - Nur eine Station kann zu einem Zeitpunkt erfolgreich senden

Mehrfachzugriffsprotokolle

- Verteilter Algorithmus, der bestimmt, wie mehrere Stationen das Medium gemeinsam nutzen können, d.h.: er bestimmt, welche Station senden darf
- Die Kommunikation darüber, wer den Kommunikationskanal nutzen kann, muss ebenfalls über das Medium stattfinden!
- Aspekte der Mehrfachzugriffsprotokolle:
 - synchron oder asynchron
 - Welches Wissen wird über andere Stationen benötigt?
 - Preis / Aufwand
 - Robustheit (bei fehlerhaftem Kanal)
 - Performanz (Durchsatz pro Teilnehmer = R/n)

R: Datenrate des Kanals

n : Anzahl Teilnehmer

MAC Protokolle: 3 unterschiedliche Arten

Kanalaufteilung

- Teile den Kanal in kleinere “Teile” auf (Zeitscheiben /Frequenzauflaufteilung)
- Zuweisung eines “Teils” zur exklusiven Nutzung durch eine Station

Wahlfreier Zugriff (Random Access)

- Kollisionen kommen vor
- Wiederholung bei Kollisionen

Rotation (Taking Turns Protocol)

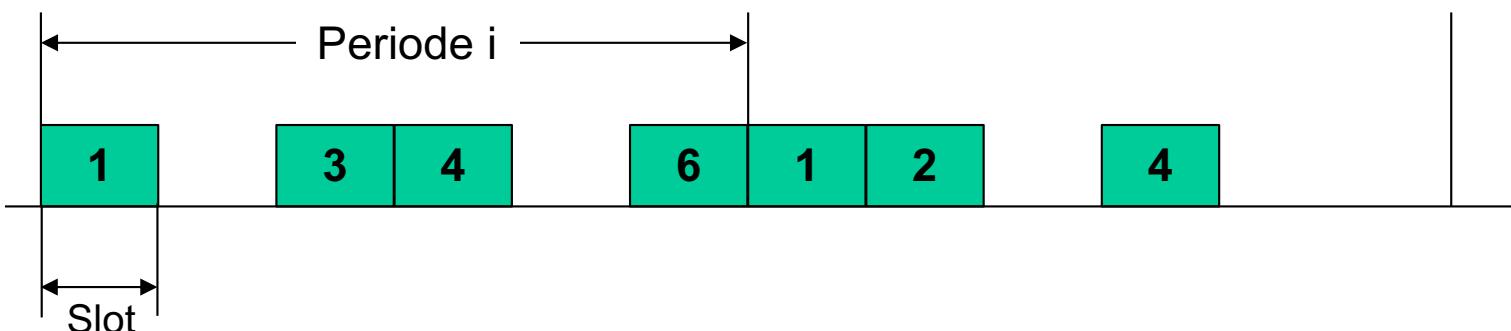
- Strenge Koordination über das gemeinsam genutzte Medium, um Kollisionen zu vermeiden
- Der Kanal wird einem Teilnehmer zugeordnet
 - Zugriff über “Token” geregelt
 - Zugriff über Master/Slave Ansatz: Master weist den Slaves den Kanal zu

Entwurfsziele: effizient, fair, einfach, dezentralisiert

Kanalaufteilungs-MAC-Protokolle: TDMA

TDMA: Time Division Multiple Access

- Periodischer Zugriff auf den Kanal
- Jede Station erhält Zeitschlitz ("Slot") fester Länge (Länge = Paketsendezeit) in jeder Runde
- Synchronisierte gemeinsame Uhrzeu
- Ungenutzte Slots bleiben leer
- Fair, aber ineffizient bei Nutzern mit stark unterschiedlichen Lastanforderungen

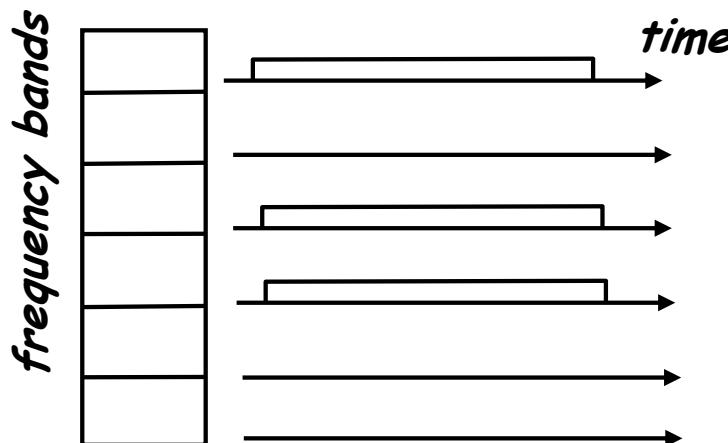


- Beispiel: 6 Stationen
 - Periode i: Station 2 und 5 nutzen Slot nicht: 1/3 der Datenrate ungenutzt
 - Periode i+1: 1/2 Datenrate ungenutzt

Kanalaufteilungs-MAC-Protokolle: FDMA

FDMA: Frequency Division Multiple Access

- Kanalspektrum wird in Frequenzbänder aufgeteilt
- Jeder Station wird ein festes Frequenzband zugewiesen
- Ungenutzte Übertragungszeit in einem Frequenzband geht verloren
- fair, aber ineffizient bei Nutzern mit stark unterschiedlichen Lastanforderungen



- Beispiel: 6 Stationen im LAN, 1,3,4 haben Paket, Frequenzbänder 2,5,6 ungenutzt

Wahlfreier Zugriff (Random Access)

Wenn eine Station ein Paket senden will

- übertrage mit gesamter möglicher Datenrate R des Kanals
- Keine a priori Koordination zwischen Stationen!

Zwei oder mehr gleichzeitige sendende Stationen → “Kollision”

Random Access MAC Protokolle spezifizieren:

- Wie Kollisionen entdeckt werden
- Wie nach Kollision wieder aufgesetzt wird (Recovery)

Beispiele für Zufallszugriffsprotokolle:

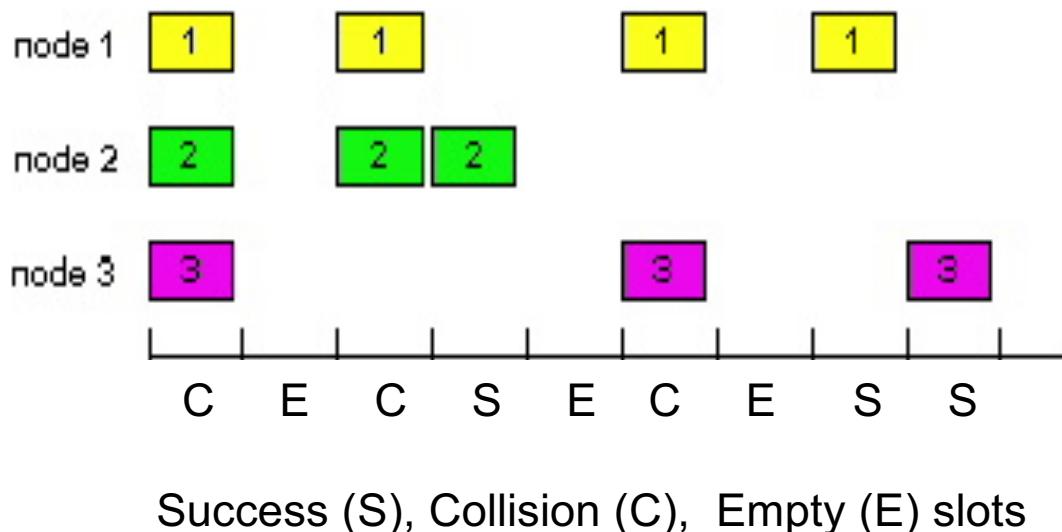
- Slotted ALOHA
- Pure ALOHA
- CSMA und CSMA/CD

Slotted Aloha

Ansatz

- Zeit ist in Zeitschlüsse (“Slots”) gleicher Größe aufgeteilt (= Paketübertragungszeit)
(Die Uhren der Teilnehmer **müssen** synchronisiert werden)
- Station mit Sendewunsch: Überträgt ab Beginn des nächsten Slots
- Bei Kollision: Wiederholung der Übertragung im einem späteren Slot mit Wahrscheinlichkeit p (solange, bis erfolgreich)

Beispiel



Effizienzbetrachtung:

Vereinfachende Annahme:

- n Stationen, jede will mit Wahrscheinlichkeit p senden

$P(\text{Erfolg für Station } x) =$

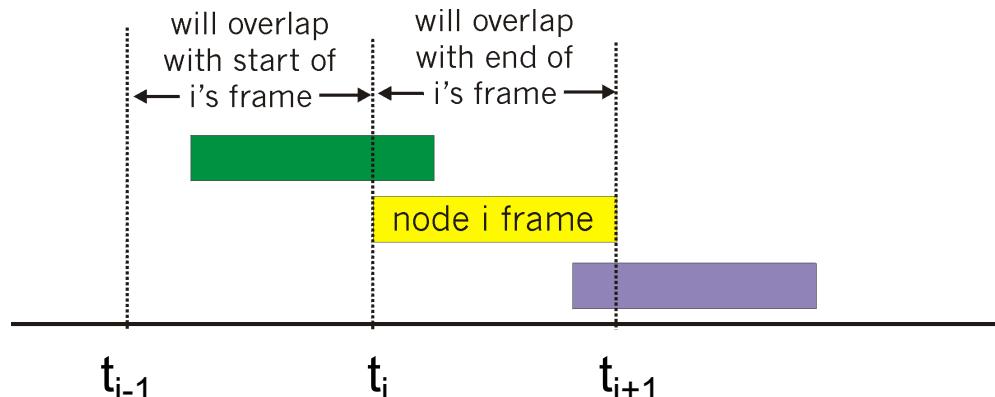
$$\begin{aligned} & P(x \text{ sendet}) * P(\text{andere senden nicht}) \\ &= p * (1-p)^{(n-1)} \end{aligned}$$

Was passiert bei großem n ?

(Pure) ALOHA

Ansatz

- Ansatz ohne Zeitslots => Uhrensynchronisation entfällt, aber weiterhin fest Zeitspanne für die Übertragung eines Rahmens
- Station mit Sendewunsch: sendet sofort
- Bei Kollision: Nachdem dem kollidierte Rahmen vollständig übertragen wurde, wird der Rahmen mit Wahrscheinlichkeit p erneut übertragen (bzw. es wird die Übertragungszeit eines Rahmen gewartet)



Effizienzbetrachtung:

Vereinfachende Annahme:

- n Stationen, jede will mit Wahrscheinlichkeit p senden

$P(\text{Erfolg für Station } x) =$

$P(x \text{ sendet}) *$

$P(\text{anderer senden nicht in } [t_{i-1}, t_i]) *$

$P(\text{anderer senden nicht in } [t_i, t_{i+1}])$

$$= p * (1-p)^{(n-1)} * (1-p)^{(n-1)}$$

Im Vergleich zu Slotted ALOHA steigt die Kollisionswahrscheinlichkeit an

CSMA: (Carrier Sense Multiple Access)

Vorgehen: CSMA: Lauschen vor der Übertragung:

- Wenn Kanal frei ist: übertrage gesamtes Paket
- Wenn Kanal belegt, verschiebe Übertragung
 - Persistentes CSMA: versuche sofort, wenn Kanal frei wird, neu zu übertragen
 - Nicht-persistentes CSMA: neuer Sendevorschuss nachdem der Kanal frei wurde und zusätzlich eine zufällige Wartezeit abgelaufen ist
- Analogie: Lasse Deine Mitmenschen im Gespräch ausreden

CSMA Kollisionen

Kollision kann passieren

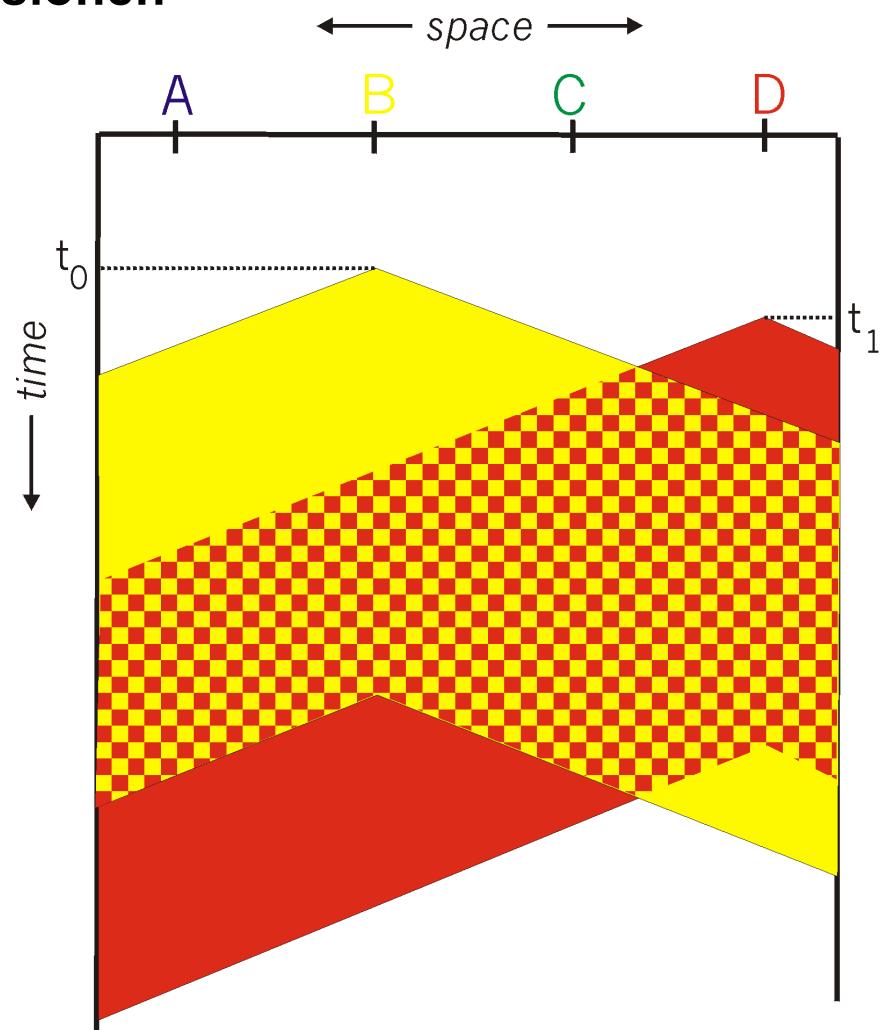
- Die Ausbreitungsverzögerung kann bewirken, dass zwei Stationen das Medium fälschlich für frei halten und senden

Wirkung einer Kollision

- Verschwendungen der **gesamten** Übertragungszeit – alle Sender senden das gesamte Paket, obwohl ein Kollision vorliegt

Beachte

- Die Rolle der Entfernung und die Ausbreitungsverzögerung bei der Kollisionswahrscheinlichkeit



Raum - Zeit - Diagramm: Station B und D senden

CSMA/CD (Collision Detection)

Vorgehen: CSMA/CD: Verhalten wie bei CSMA, aber Mithören der eigenen Übertragung

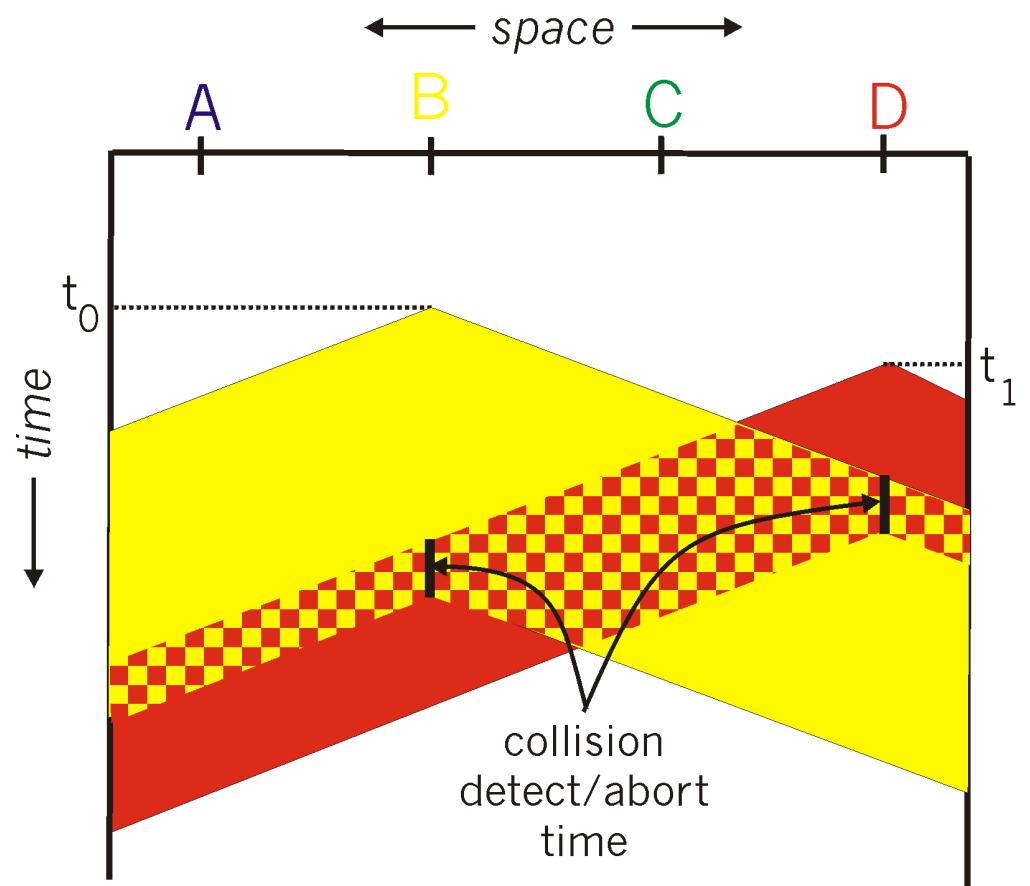
- Kollisionen werden schnell *entdeckt*
- Übertragung wird bei entdeckter Kollision abgebrochen, dadurch wird die verschwendete Belegung des Medium reduziert
- Persistente oder nicht-persistente Neuversendung nach Kollision
- Entdeckung einer Kollision:
 - leicht in “Draht” - LANs: Messen des Kabelsignals, Vergleich des gesendeten und gemessenen Signals
 - schwer in drahtlosen LANs (Funktechnik): Empfänger muss beim Sendevorgang abgeschaltet werden

Analogie: der höfliche Gesprächspartner

CSMA/CD Kollisionsentdeckung

Kollision wird frühzeitig erkannt

- Durch den Abbruch der Übertragung bei einer Kollision wird die durch die Kollision verschwendete Übertragungszeit reduziert.



Raum - Zeit - Diagramm: Station
B und D senden

Exponential Backoff

Frage: Wie lange soll nach einer Kollision gewartet werden, bis der nächste Sendeversuch unternommen wird?

Ziel: Adaption der neuen Sendeversuche an die aktuelle Last

- Bei hoher Last: zufälliges Warten wird länger

Verfahren: Exponential Backoff

- Verzögerung ist $K * x$ Bit-Sendezeiten (Ethernet $x = 512$)
 - Nach 1. Kollision: wähle K zufällig aus $\{0,.., 2^1-1\}$
 - Nach 2. Kollision: wähle K zufällig aus $\{0,1,.., 2^2-1\}$
 - ...
 - Nach 10 oder mehr Kollisionen, wähle K zufällig aus $\{0,1,2,3,4,\dots,2^{10}-1\}$
- Abbruch nach x Sendever suchen (Ethernet $x = 16$)

Bewertung

Kanalaufteilende MAC Protokolle

- Teilen die Gesamtkapazität des Kanals
- Effizient bei hoher Last (wenn die Last gleichverteilt ist)
- Ineffizient bei geringer Last:
 - Verzögerung beim Kanalzugriff
 - Geringe Bandbreite ($1/n$), obwohl nur eine Station aktiv ist !

Zufallszugriff MAC Protokolle

- Effizient bei geringer – mittlerer Last: einzelne Station erhält die gesamte Bandbreite des Kanals
- Hohe Last: viele Kollisionen, dadurch Overhead

Alternative (mit anderen Nachteilen)

- Rotationsprotokolle (“nach Reihenfolge”)
- Reservierungsbasierte MAC-Protokolle

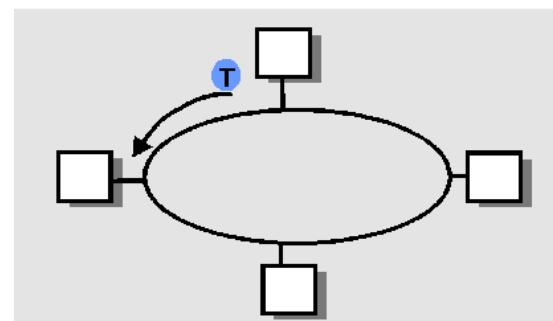
Rotationsprotokolle (“nach Reihenfolge”)

Polling (Abfrage):

- Master-Station teilt Slave-Station mit, wann sie mit der Übertragung dran ist
- Request-to-Send, Clear-to-Send Nachrichten
- Probleme:
 - Polling Overhead
 - Latenz
 - Single point of failure (Master)

Token Passing:

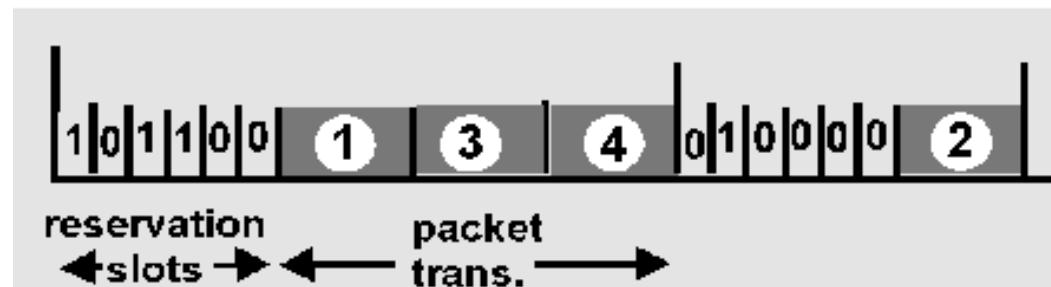
- Kontroll-Token läuft im Kreis von einer Station zum nächsten.
- Token-Nachricht ohne Daten
- Probleme:
 - Token Overhead
 - Latenz
 - Single point of failure (Token/Master)



Reservierungsbasierte Protokolle

Verteiltes Polling:

- Reservierungsphase + Datenübertragungsphase
- Zeit wird in Zeitschlüsse (“Slots”) aufgeteilt
- Zunächst gibt es N kurze Reservierungsslots
 - Reservierungsslot-Zeit hängt ab von der Länge des Übertragungsmediums
 - Stationen mit Sendewunsch belegen **ihren** Slot in den Reservierungsslots
 - Reservierung wird von allen Stationen gesehen und gemerkt
- Nach der Reservierungsphase senden die Stationen in festen “Datenslots”, die sie sich vorher per Reservierung angemeldet haben



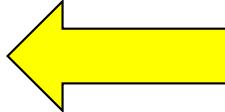
Zusammenfassung der MAC Protokolle

Aufteilung eines gemeinsam genutzten Mediums?

- Feste Kanalaufteilung, durch Zeit, Frequenz oder Code
 - Time Division, Code Division, Frequency Division
- Zufallsaufteilung (dynamisch),
 - ALOHA, Slotted ALOHA, CSMA, CSMA/CD
 - CSMA/CD wird bei Ethernet genutzt
- Rotation / Reihenfolgen
 - Durch Zuteilung über Master oder durch umlaufende Token
- Reservierungen
 - Reservierungsphase / Übertragungsphase

Kapitel 6: Sicherungsschicht & LAN

Gliederung

- Einführung und Grundlagen
- Punkt-zu-Punkt-Protokolle
- Mehrfachzugriffsprotokolle (MAC)
- LAN-Adressen und ARP 
- Ethernet
- Switches
- Zusammenfassung

Textbuch zu diesem Kapitel: J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz, Kapitel 5

Folien und Abbildung teilweise aus:

J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz

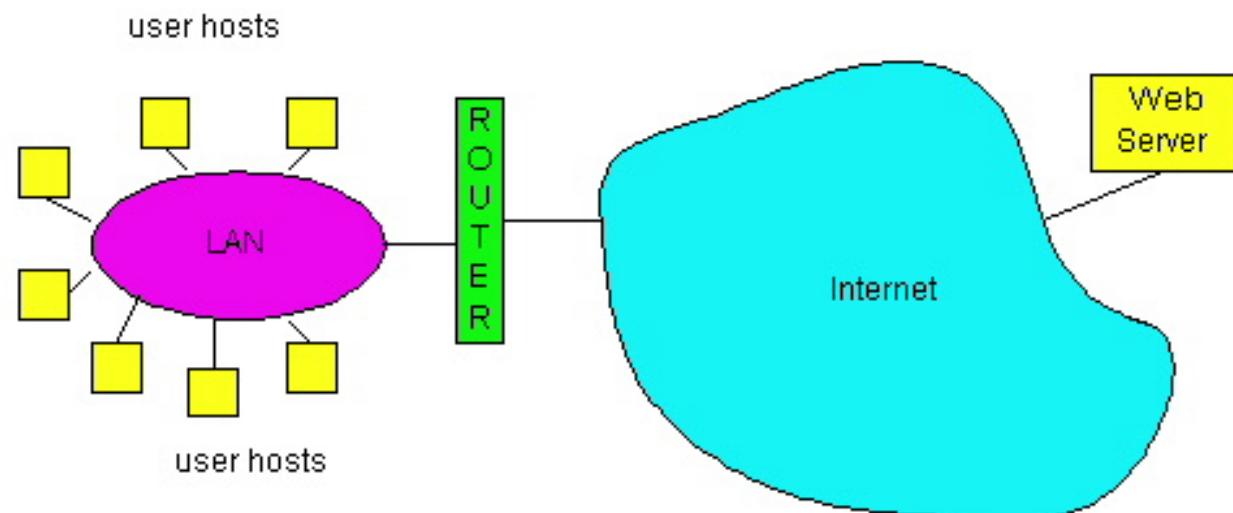
LAN Technologien

Bisher:

- Prinzipien der Sicherungsschicht
- Dienste, Fehlerentdeckung/Korrektur, Punkt-zu-Punkt-, Mehrfachzugriff

Jetzt: Local Area Networks (LAN)

- Alle Stationen sind über eine physikalische Verbindung erreichbar
- Aktuelle Technologien:
 - Adressierung über MAC Adressen & ARP-Protokoll
 - Ethernet
 - Switches
 - 802.11 (WLAN)



MAC (LAN) Adressen und ARP

32-bit / 128 bit - IP Adresse: Netzwerkschicht-Adresse

- wird benutzt, um das Datagramm zum Zielnetz zu transferieren

LAN- (oder MAC- oder physikalische) Adresse: Adresse der Sicherungsschicht

- wird benutzt, um das Datagramm von einem Interface zu einem anderen physikalisch verbundenen Interface zu transferieren (im selben Netzwerk)
- 48 Bit-Adresse (6 Byte), (fest) in der Netzwerkkarten einprogrammiert

- Beispiel: 3C-A9-F4-18-8F-45

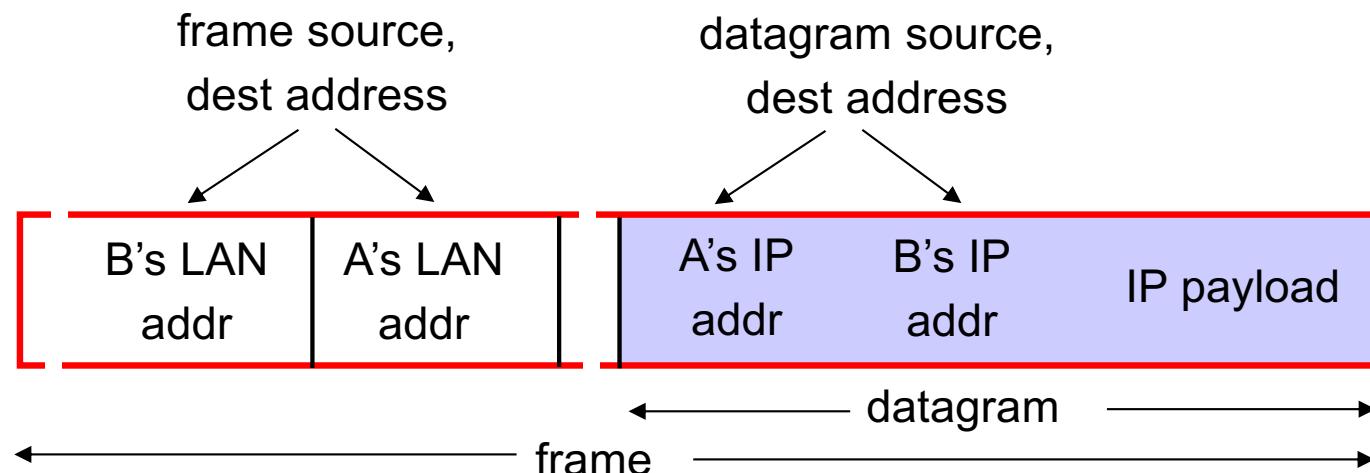
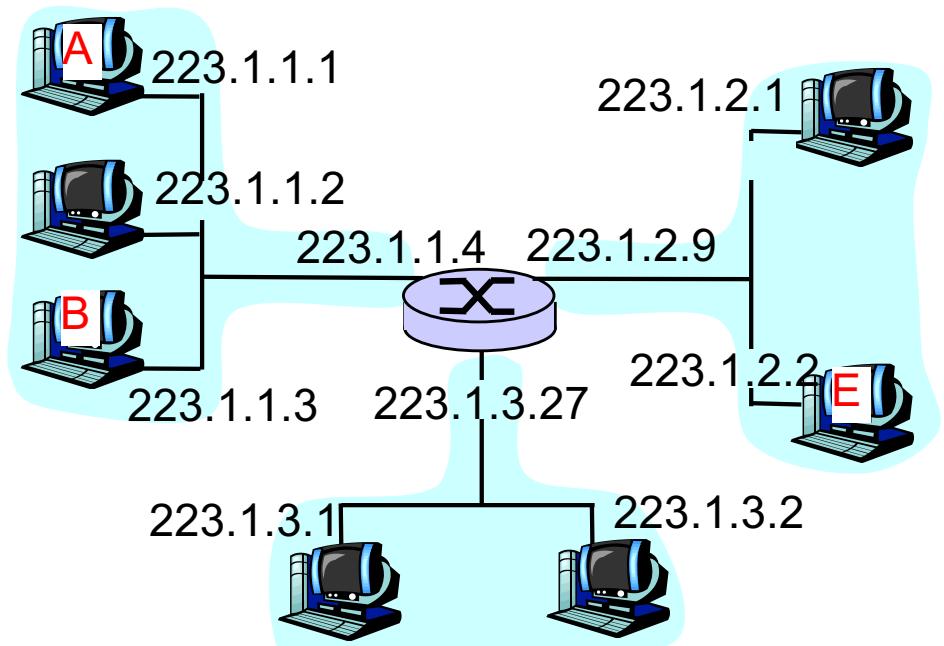
- Flache Adressstruktur → Portabilität
- Weltweit eindeutig:

- MAC-Adresszuteilung wird durch die IEEE verwaltet
 - Hersteller kaufen einen Teil des MAC-Adressraums (vorderen Bits sind fest)
 - Flash Tools beachten

ARP schließt die Lücke bei der bisherigen Routing-Diskussion!

A sendet IP-Datagramm an B:

- A sucht Netzwerkadresse
(Netzwerkteil der IP-Adresse) von B
in Routingtabelle, findet B in demselben
Netz wie A
- Sicherungsschicht von A sendet
Datagramm innerhalb eines Sicherungs-
schichtrahmens mit LAN-Adresse von B



**ARP liefert die
MAC Adr. zu
einer IP Adr.**

ARP: Address Resolution Protocol [RFC 826]

Frage: Wie wird die LAN-Adresse von B bestimmt bei bekannter IPv4-Adresse?

- Jeder IPv4-Knoten (Host, Router) im LAN hat ein **ARP**-Modul mit einer ARP-Tabelle:

IP Adr.	MAC Adr.	TTL

TTL: (Time To Live): Zeit, nach der dieser Eintrag verfällt (typisch 20 min)

- Über das ARP Protokoll wird B nach seiner MAC Adresse gefragt.
- IPv6: Neighbor Discovery Protocol (NDP) ersetzt ARP

ARP-Protokoll: Füllen der ARP-Tabelle

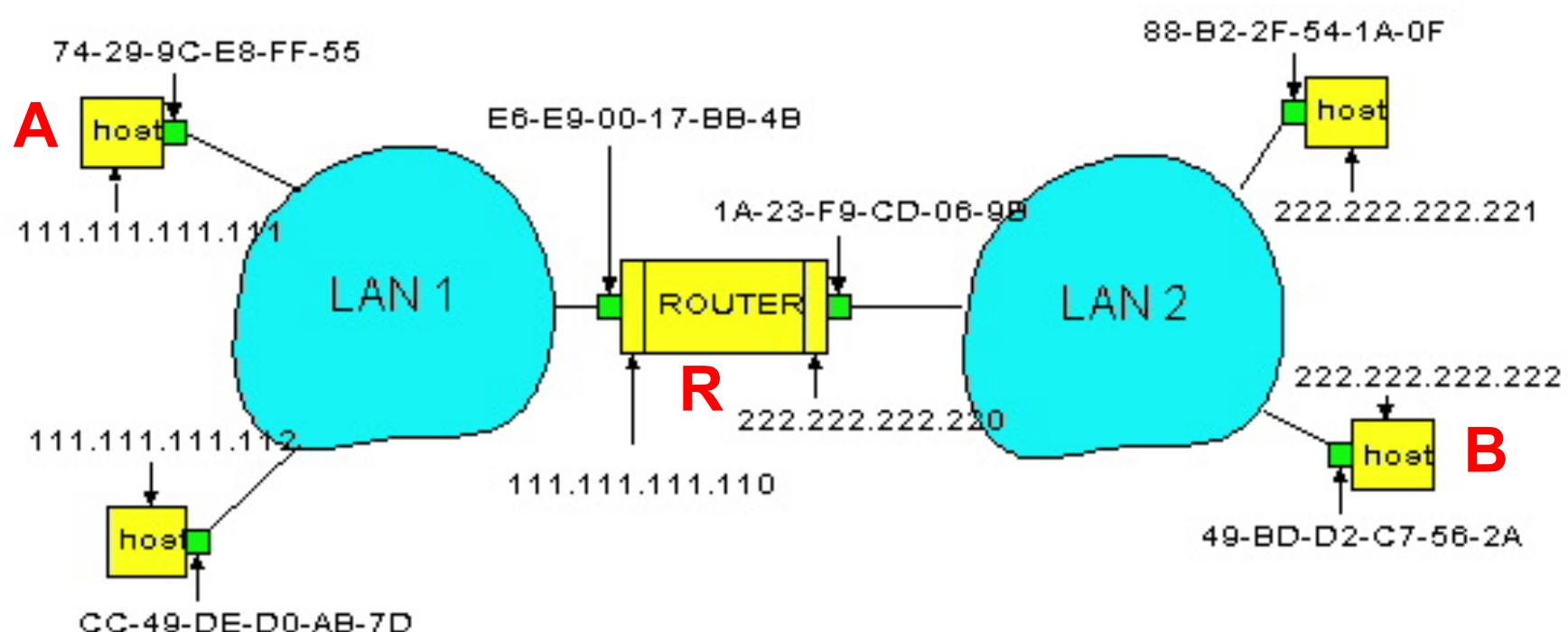
Situation: A kennt B's IPv4-Adresse und benötigt die LAN-Adresse von B

- A sendet an alle LAN-Stationen ein ARP-Anfragepaket, das die IPv4-Adresse von B enthält
 - “Broadcast”-Anfrage mit LAN-Adresse FF-FF-FF-FF-FF-FF
 - Alle Stationen im LAN empfangen die ARP-Anfrage
- B empfängt das ARP-Paket ebenfalls und antwortet A mit seiner (B's) LAN-Adresse
- A speichert das Tupel IPv4-/LAN-Adresse, bis die Information veraltet (wegen TTL)

Beispiel: Routing zu einem anderen LAN (1)

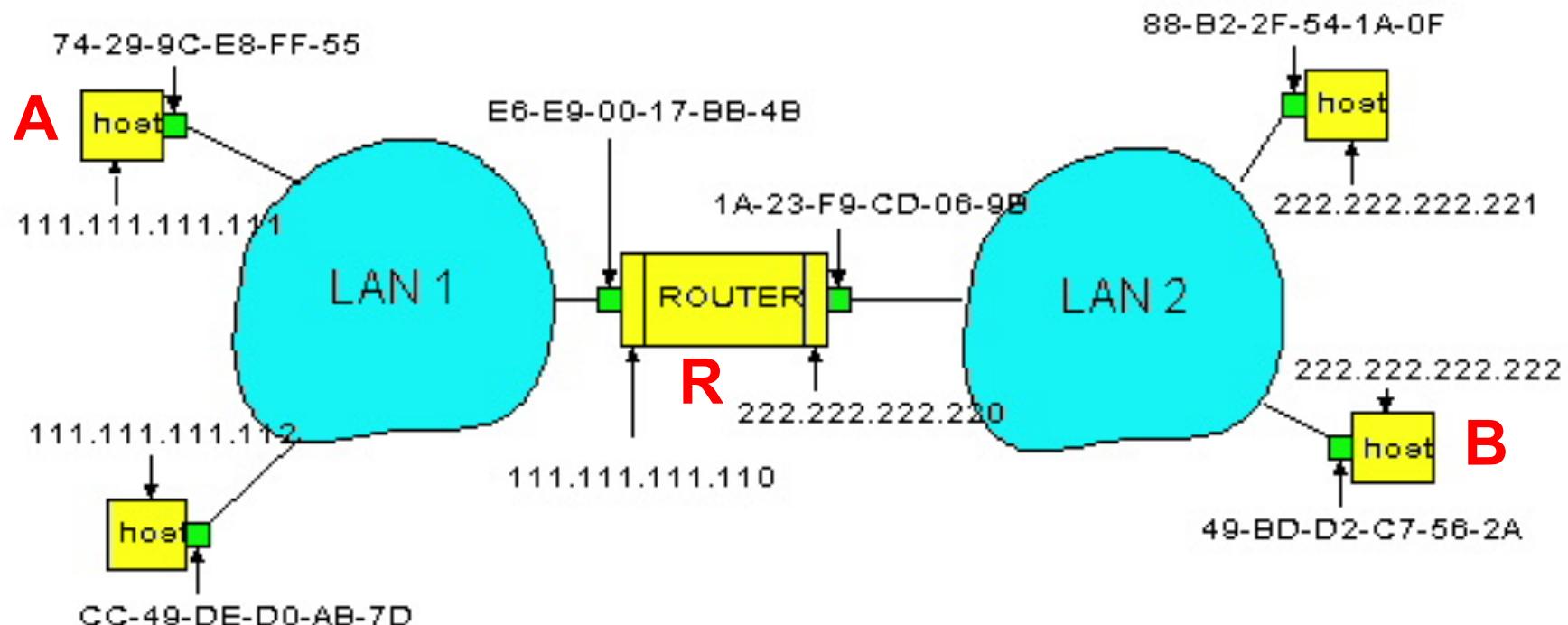
Aufgabe: Senden eines IP-Datagramms von der Quelle A zum Ziel B über R

- In der Routing-Tabelle von A wird der Router gefunden, Adresse: 111.111.111.110
- In der ARP-Tabelle von A wird zu 111.111.111.110 die LAN-Adresse E6-E9-00-17-BB-4B gefunden
- A erzeugt Ethernet-Rahmen mit R's LAN-Adresse als Ziel, Ethernet-Rahmen enthält A-nach-B IP-Datagramm



Beispiel: Routing zu einem anderen LAN (2)

- A's Sicherungsschicht sendet Ethernet-Rahmen
- R's Sicherungsschicht empfängt Ethernet-Rahmen
- R extrahiert IP-Datagramm aus dem Ethernet-Rahmen, sieht das Ziel B
- R benutzt ARP um B's LAN-Adresse 49-BD-D2-C7-56-2A zu erhalten
- R erzeugt Ethernet-Rahmen, der A-nach-B IP-Datagramm nach B sendet
- B extrahiert IP-Datagramm aus dem Ethernet-Rahmen und reicht die Daten hoch



Kapitel 6: Sicherungsschicht & LAN

Gliederung

- Einführung und Grundlagen
- Punkt-zu-Punkt-Protokolle
- Mehrfachzugriffsprotokolle (MAC)
- LAN-Adressen und ARP
- Ethernet 
- Switches
- Zusammenfassung

Textbuch zu diesem Kapitel: J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz, Kapitel 5

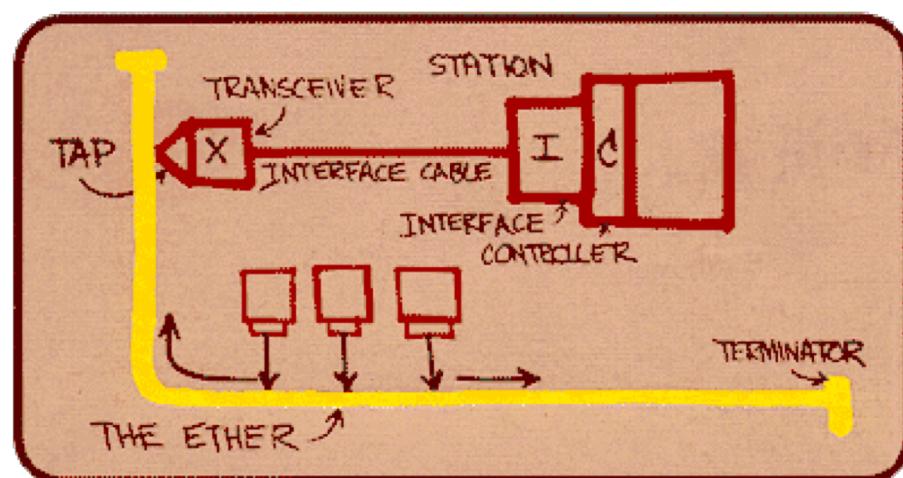
Folien und Abbildung teilweise aus:

J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz

Ethernet

“Dominierende” LAN Technologie, weil

- billig 8 € für 100 Mb/s, 10 € für 1.000 Mb/s
- erste breit genutzte LAN Technologie
- einfacher, billiger als Token LANs und ATM
- durch neue Physical Layer stets die Datenrate von Konkurrenzprodukten überboten wurde
- die Datenrate ständig steigt: 10, 100, 1.000, 10.000, 40.000, 100.000 Mb/s
- die Steigerung der Datenrate nahezu ohne Änderung der Layer 2 und höher erfolgt



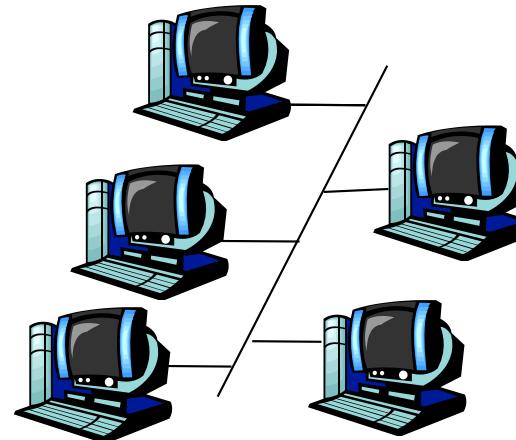
Metcalfe's
Ethernet
Skizze

Ethernet-Topologie

Bus-Topologie (“Standard”-

Ethernet-Betrieb):

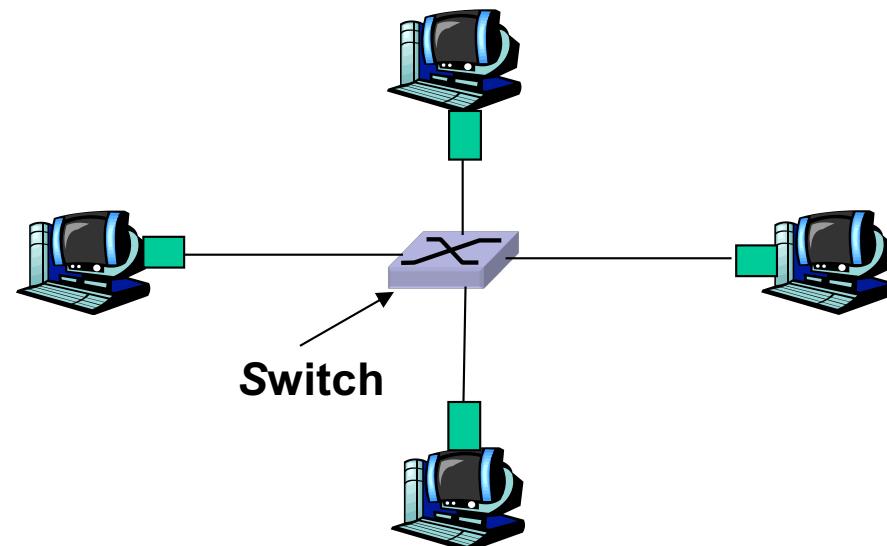
- Alle Stationen teilen sich dasselbe (Bus-)Medium, gleichzeitig gesendete Pakete kollidieren



Stern-Topologie (moderner de-

facto Ethernet-Standard)

- Ein Switch vermittelt zwischen allen Stationen
- Auf jeder einzelnen Verbindung wird ein separates Ethernet betrieben (daher kollisionsfrei!)



Ethernet-Rahmen Struktur (1)

Sendende Netzwerkkarte verpackt die Nutzdaten (IP-Datagramm oder anderes Netzwerk-Protokoll-Paket) in einen **Ethernet-Rahmen (Frame)**



Präambel (8 Byte)

- 7 Bytes mit Bitmuster 10101010 gefolgt von einem Byte mit 10101011
- Wird benutzt, um den Takt von Sender und Empfänger zu synchronisieren

Adressen (6 Byte pro Adresse)

- Wenn eine Netzwerkkarte einen Rahmen mit der eigenen Adresse oder der Broadcast-Adresse (= FF:FF:FF:FF:FF:FF) empfängt, dann werden die Daten an die nächsthöhere Schicht weitergegeben
- Sonst wird der Rahmen verworfen

Ethernet-Rahmen Struktur (2)



Typ (2 Byte)

- verweist auf das Protokoll der nächsthöheren Schicht, meist IP, aber z.B. auch Novell IPX, AppleTalk, ARP, ICMP, ... (2 Byte)

Data (46 – 1500 Byte)

- MTU (Maximum Transfer Unit) 1500 Byte
- Mindestgröße von 46 Byte (=> Mindestrahmenlänge)

CRC (4 Byte)

- wird beim Empfänger geprüft, bei Fehler Rahmen einfach wegwerfen

Paketende:

- Erkannt durch eine Ruheperiode von 9,6 Mikrosekunden

Ethernet - Dienstangebot

- 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
 - Kollisionen werden von Ethernet per Collision Detection erkannt und durch Übertragungswiederholung behoben (CSMA/CD)
 - Jam Signal: stellt sicher, dass alle Stationen im LAN die Kollision bemerken (48 Bits)
 - Andere Rahmenverluste müssen auf höheren Schichten behoben werden oder der Inhalt des Rahmens geht verloren

entfällt bei Switch basierten Ethernet

Ethernet – Technologien

10Base2

- 10: 10Mb/s, 2: 200 Meter max. Kabellänge
- Dünnes Koaxialkabel in einer Bustopologie

10BaseT und 100BaseT

- 10 Mb/s und 100 Mb/s Datenrate
- 100 Mb/s wird “Fast Ethernet” genannt
- T steht für Twisted Pair (verdrillter Draht) Switch basiert

Gigabit Ethernet

- 1 Gb/s und 10 Gb/s Datenrate
- Benutzt Standard Ethernet Paketformat
- Erlaubt Punkt-zu-Punkt-Verbindungen (→ Switches) und Broadcast-Medium-Verbindungen via Hub (shared mode)
- Voll-Duplex für Punkt-zu-Punkt Verbindungen
- Nur im “shared mode” wird CSMA/CD benutzt (benötigt kurze Abstände zwischen den Stationen)

Ethernet: Physikalische Medien

Koaxialkabel

- Zwei konzentrische Kupferleitungen
- Basisband-Übertragung:
 - Nur ein “Kanal” auf dem Kabel
 - Früher Ethernet-Standard
- Breitband-Übertragung:
 - Mehrere Kanäle gleichzeitig auf dem Kabel
 - Fernsehen (HFC)



Twisted Pair

- Paarweise verdrillter Kupferdraht
- Kategorie 3: traditionelle Telefonkabel, 10 Mbit/s Ethernet
- Kategorie 5:
100 Mbit/s - 1 Gbit/s Ethernet
- Kategorie 7:
10 Gbit/s Ethernet



Ethernet: Physikalische Medien

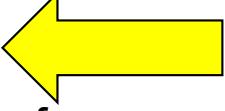
Glasfaserkabel

- Glasfaser überträgt Lichtimpulse
- Hohe Übertragungsraten (bis 100 Gbit/s)
- Niedrige Fehlerraten
- Große Abstände zwischen physikalischen Verstärkern möglich (keine Dämpfung)
- Keine EMV Probleme
- Teilweise mechanisch empfindlich (Biegeradius, Dehnung)



Kapitel 6: Sicherungsschicht & LAN

Gliederung

- Einführung und Grundlagen
- Punkt-zu-Punkt-Protokolle
- Mehrfachzugriffsprotokolle (MAC)
- LAN-Adressen und ARP
- Ethernet
- Switches 
- Zusammenfassung

Textbuch zu diesem Kapitel: J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz, Kapitel 5

Folien und Abbildung teilweise aus:

J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz

LAN-Verbindungen

Mögliche Topologien (für kabelgebundene LANs):

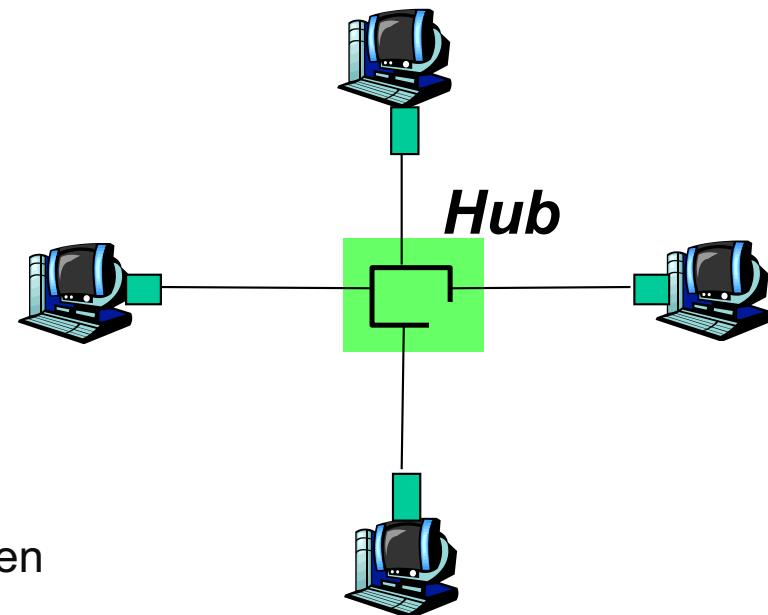
- Bus
- Ring
- Stern

Frage: Welche Geräte stehen zur Kopplung von einzelnen LAN-Segmenten auf Schicht 1 und 2 zur Verfügung?

- Hub
- Switch

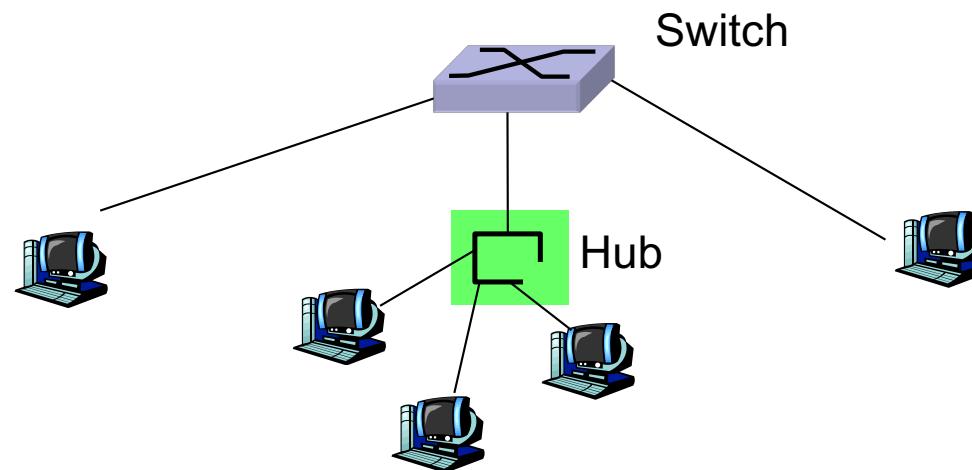
Hub

- Gerät der physikalischen Schicht: Einfacher Verstärker (Repeater)
- Alle auf einer Verbindung eingehenden **Bits** werden an alle übrigen Verbindungen weitergeleitet (Bus-Topologie im Hub implementiert)
 - Alle angeschlossenen Stationen befinden sich in einer einzigen CSMA/CD-Kollisionsdomäne
 - Unterschiedliche Ethernettypen (d.h. 10BaseT and 100baseT) können durch Hubs nicht verbunden werden
- Was bedeutet ein Hub für Sniffer wie Wireshark?



Switch (alter Begriff: Bridge)

- Gerät der **Sicherungsschicht**: Operiert auf Ethernet-Frames, prüft Frame-Header und sendet Frame **selektiv** weiter aufgrund der angegebenen Zieladresse
- Änderungen an den Netzwerkkarten der Hosts sind nicht notwendig – Plug & Play
- Switches **isolieren Kollisionsdomänen**, da sie die Rahmen puffern können
 - Rahmen mit Zieladresse im selben LAN –Segment werden nicht in andere Segmente versendet
 - Wie weiß der Switch, in welches LAN-Segment ein Rahmen weiterzugeben ist?



Switch-Filtertabelle

- Ein Switch **lernt**, welche Hosts durch welche Schnittstelle (Interface) erreicht werden können. Dazu pflegt er eine Filtertabelle
 - Wenn ein Rahmen empfangen wird, speichert der Switch in der Filtertabelle, an welcher Switch-Schnittstelle der Absender liegt - das LAN, durch das der Rahmen empfangen wurde
- Eintrag in der Filtertabelle:
 - LAN-Adresse (des Absenders)
 - Switch-Schnittstelle
 - Zeitstempel (TTL)
- Unbenutzte Einträge in der Tabelle verfallen (TTL ist typisch etwa 60 Minuten)

Switch: Weiterleiten/Filtern inkl. "Lern"-Algorithmus

Wenn ein Switch einen Rahmen erhält:

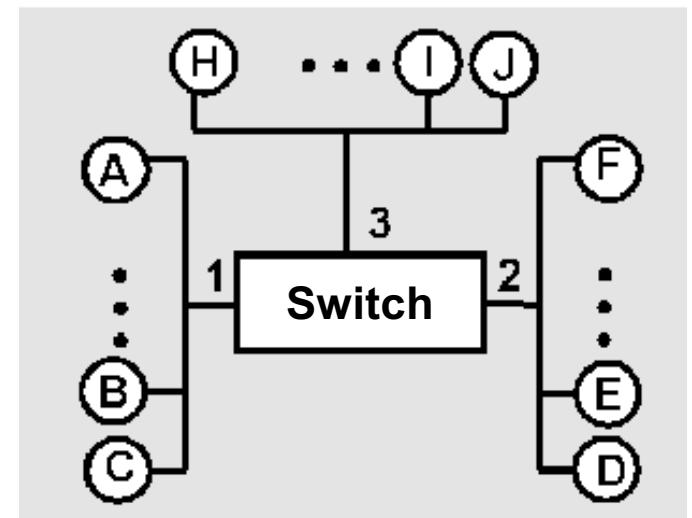
- Speichere die LAN-Absenderadresse + Eingangsschnittstelle in der Switch-Tabelle
- Suche über die LAN-Empfängeradresse die Ausgangsschnittstelle in der Switch-Tabelle
- **if** Eintrag gefunden **then** {
 - if** Ausgangs- und Eingangsschnittstelle identisch
 - then** Rahmen verwerfen // Warum?
 - else** Rahmen auf Ausgangsschnittstelle weiterleiten
- }
- else** "Fluten" /* Weitergabe auf alle Schnittstellen
 - außer der Eingangsschnittstelle*/

Switch Lernprozess: Beispiel

Situation: C sendet Rahmen nach D und
D antwortet mit einem Rahmen an C

Filtertabelle:

Address	Port	TTL
A	1	...
B	1	...
E	2	...
H	3	...
J	3	...

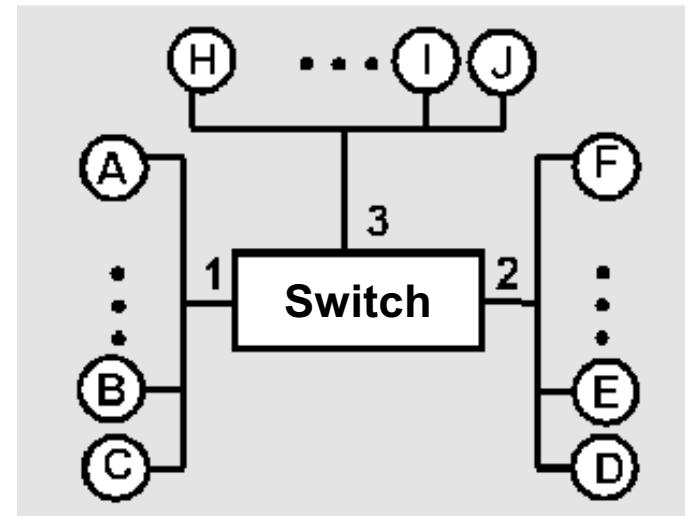


- C sendet Rahmen, Switch hat keine Info über D, folglich muss der Rahmen geflutet werden
 - Switch merkt sich, dass C über Schnittstelle 1 erreichbar ist
 - Rahmen wird im oberen LAN 3 ignoriert
 - Rahmen wird von D empfangen

Address	Port	TTL
A	1	...
B	1	...
C	1	...
E	2	...
H	3	...
J	3	...

Switch Lernprozess: Beispiel (Fortsetzung)

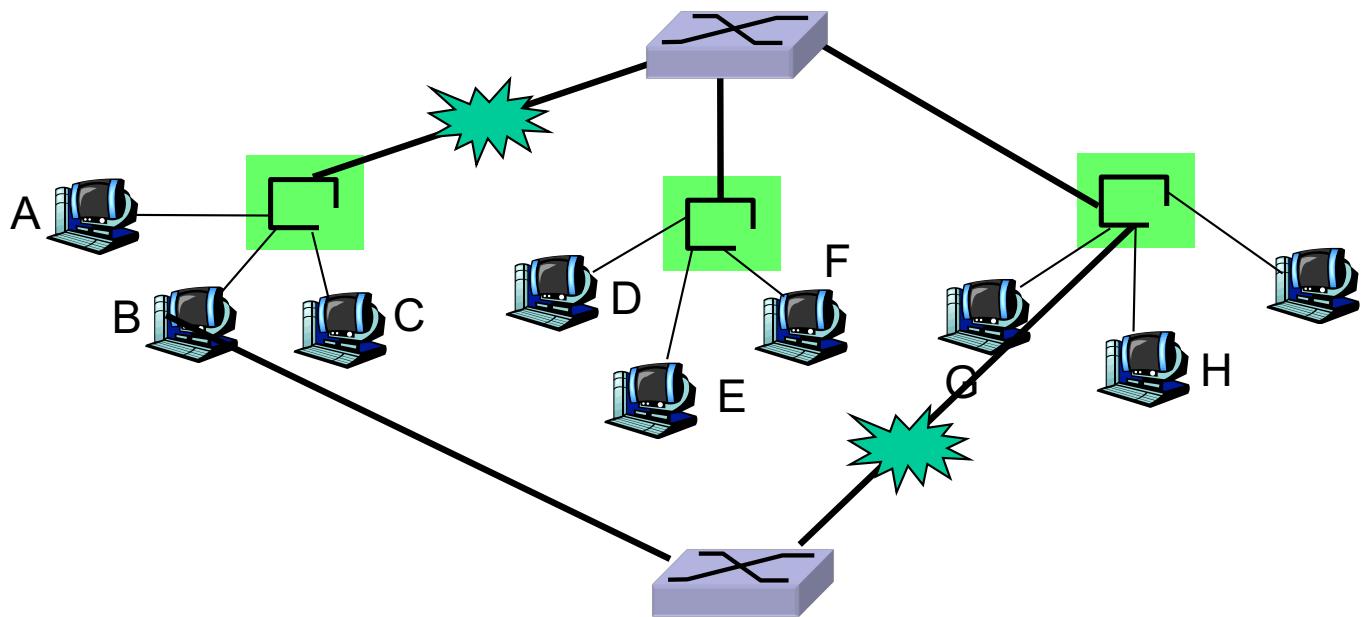
- D erzeugt Antwort an C und sendet Antwort-Rahmen
 - Switch sieht Rahmen von D
 - Switch notiert, dass D an Schnittstelle 2 liegt
 - Aus der Filtertabelle weiss der Switch, das C über Schnittstelle 1 erreichbar ist
 - Folglich sendet der Switch den Rahmen **selektiv** über Schnittstelle 1



Address	Port	TTL
A	1	...
B	1	...
C	1	...
D	2	...
E	2	...
H	3	...
J	3	...

Switch: “Spanning Tree” Protokoll

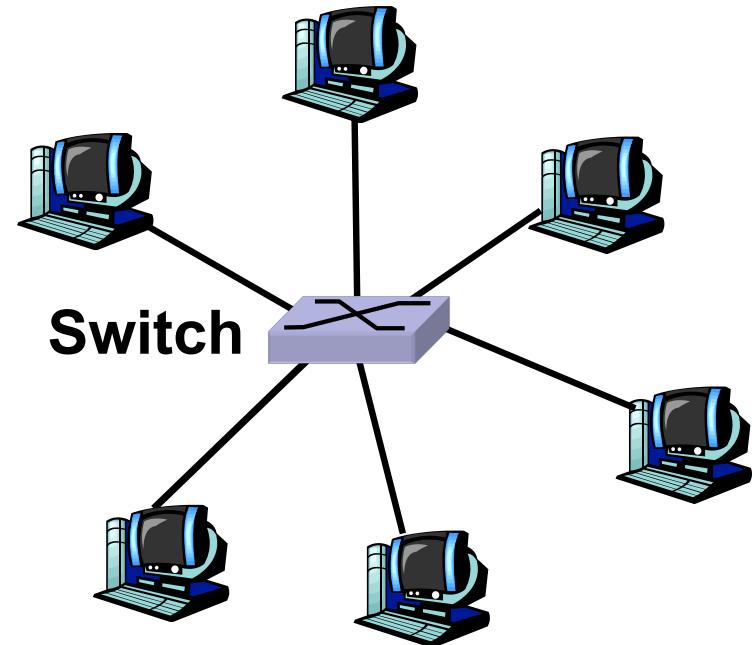
- Oft wünschenswert, redundante alternative Verbindungswege zwischen Quelle und Ziel
- Bei mehrfachen Pfaden entstehen Zyklen – die Switches könnten ständig Pakete im Kreis versenden (Welche Pakete werden im Kreis geschickt?)
Bei Routern ist dies aufgrund des Routing Algorithmus nicht der Fall!
- Lösung: Switches erkennen Topologie und organisieren sich in einer baumförmigen Struktur – zyklusfrei



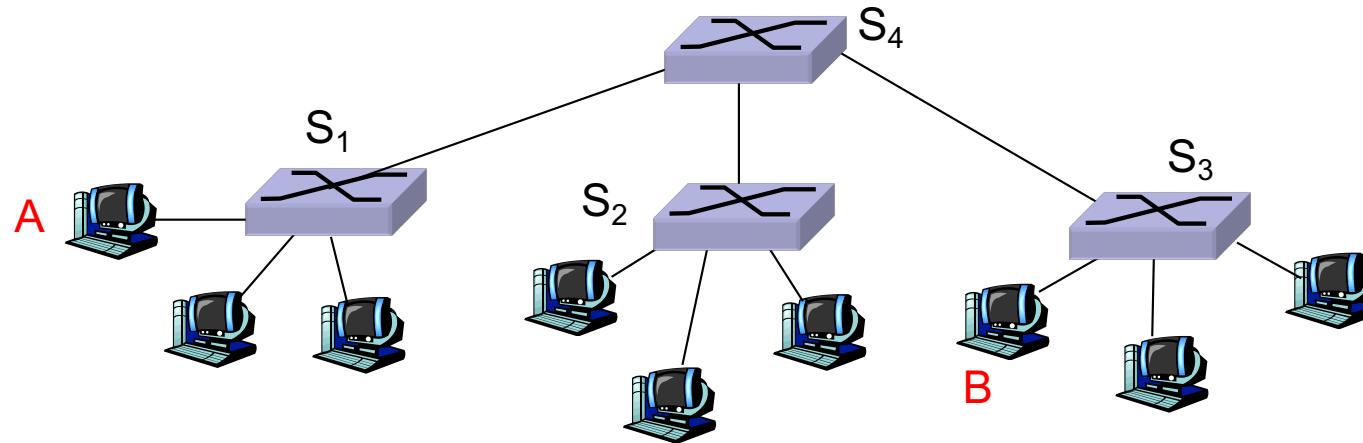
Switch - Anwendung

Aktueller Standard:

- Kein Einsatz von Hubs, sondern jeder einzelne Host ist direkt mit einer eigenen Switch-Schnittstelle verbunden, d.h.
 - keine Kollisionen!
- Viele Schnittstellen ("Ports")
 - Cisco: bis 384 pro Switch



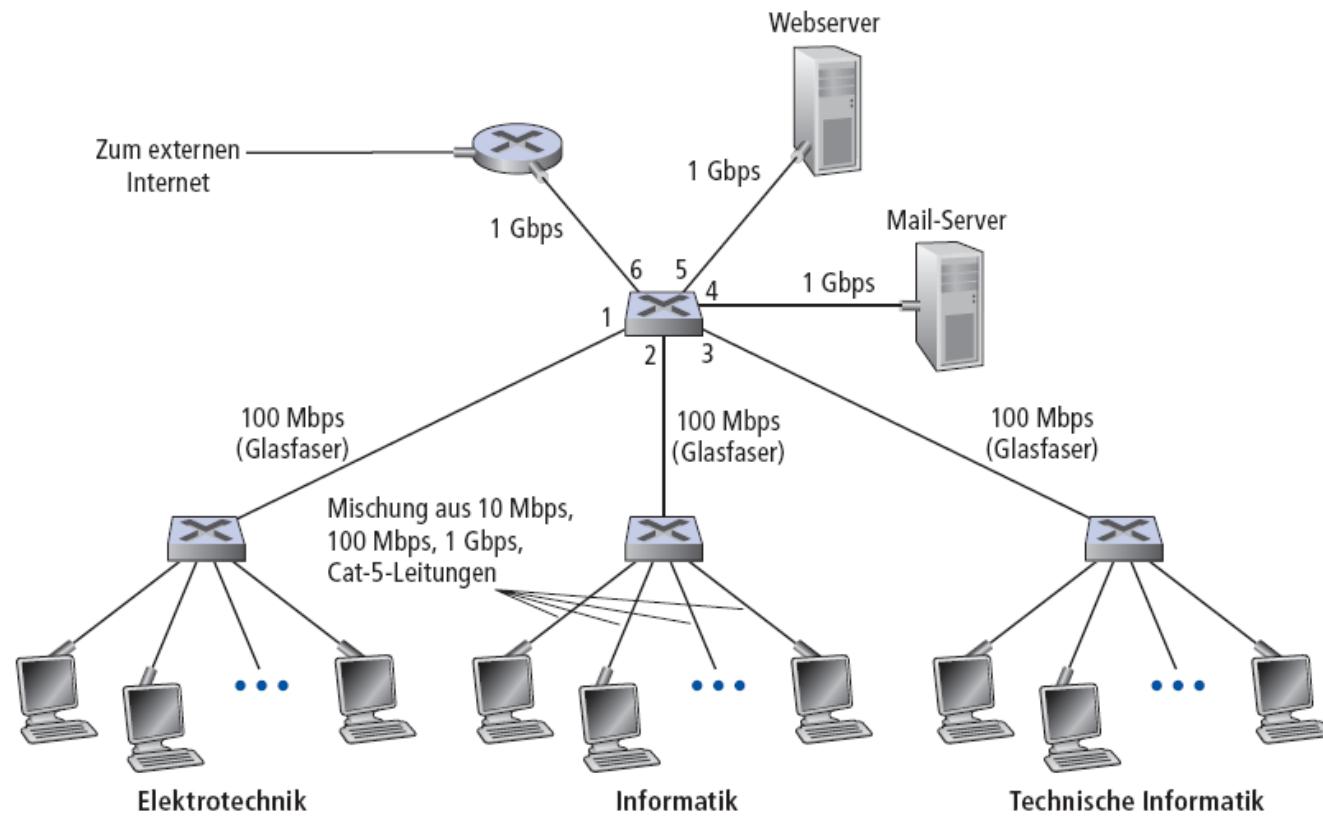
Switch-Verbindungen



Frage: Host A sendet einen Rahmen an Host B - woher wissen Switch S_1 / S_4 / S_3 , welche Ausgangsschnittstelle benutzt werden muss?

Antwort: Switch-Lernalgorithmus wird verwendet!

Switches in einer komplexeren Umgebung



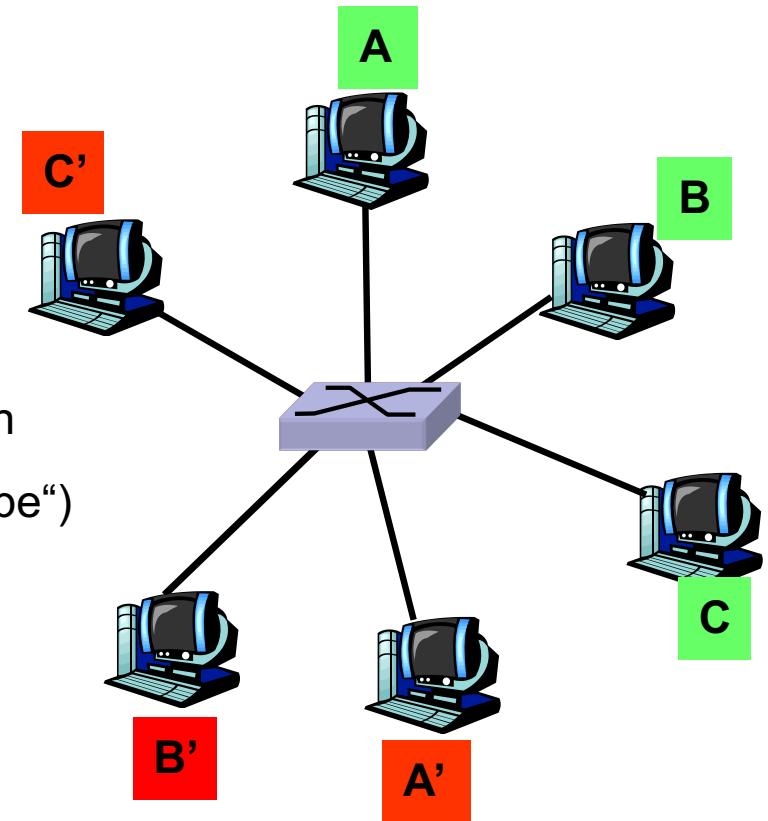
Problem: Im internen Netz keine komplette Verkehrsisolierung ohne Router möglich, d.h. bei Broadcast / Fluten wird ein Rahmen an **alle** Hosts weitergeleitet.

Lösung: Virtuelle LANS (VLANs)

VLAN: Logische Zusammenfassung von Hosts

zu einem „virtuellen“ LAN

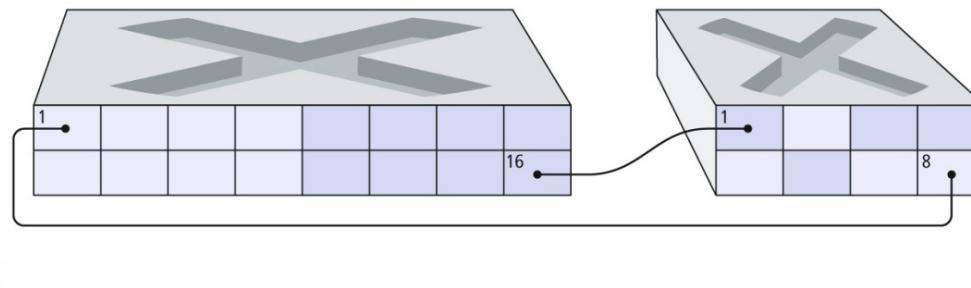
- Broadcasts / gegenseitige Erreichbarkeit nur innerhalb des VLAN gegeben
- Verwaltung über zusätzliche Konfigurationstabellen in den Switches mit Zuordnung der VLAN-ID („Farbe“)
- Ermittlung der VLAN-ID eines Rahmen über
 - ID der Eingangs-Schnittstelle oder
 - LAN-Adresse (Quelle / Ziel) oder
 - IP-Adresse oder
 - Protokoll IEEE 802.1Q
 - Erweiterung des Ethernet-Rahmenformats um VLAN-ID
 - Ziel: Identische VLAN-IDs über mehrere Switches hinweg



VLANs bei mehreren Switches

Statische VLAN-Zuordnung

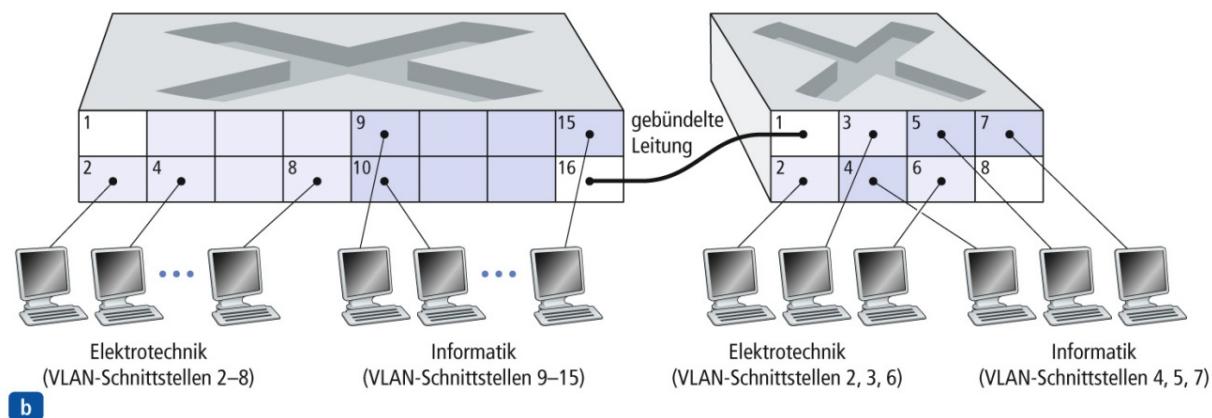
- erfordert für jedes VLAN eine eigene Leitung zwischen zwei Switches



a

VLAN-Trunking: Nutzung jeweils einer speziellen Switch-Schnittstelle für mehrere VLANs ("gebündelte Leitung")

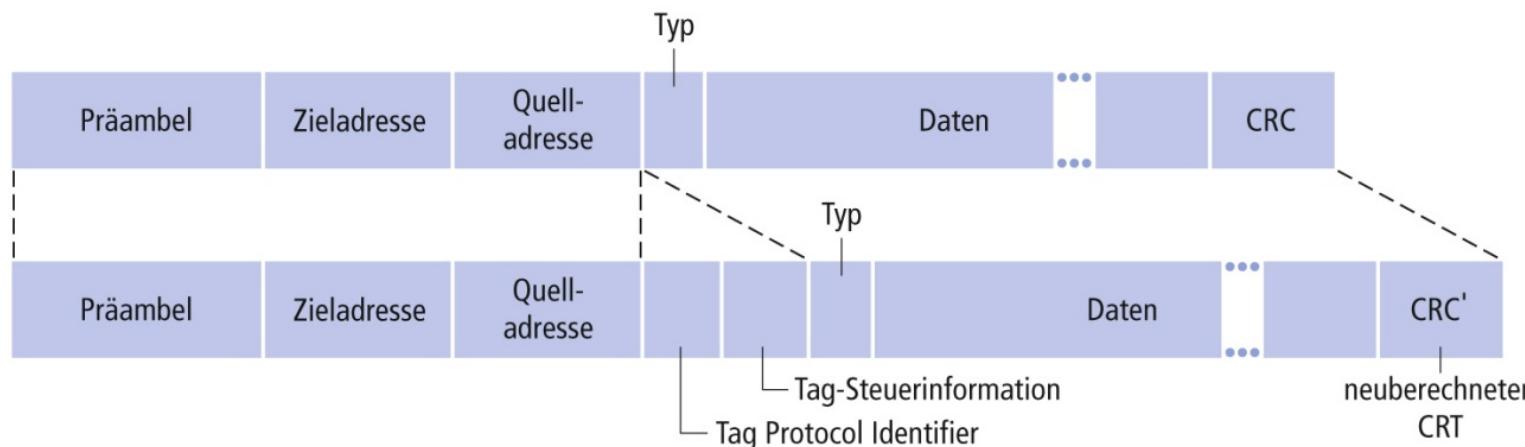
- erfordert für jedes VLAN eine eigene VLAN-ID (Protokoll IEEE 802.1Q)



b

IEEE 802.1Q -Protokoll

- Ethernet-Rahmen, die über eine **VLAN-Trunking-Schnittstelle** gesendet werden, erhalten im Header einen zusätzlichen "Tag" (4 Byte groß) mit einem Protokoll-Identifier (0x8100) und einer 12-Bit VLAN-ID als Steuerinformation



- Der Empfänger-Switch entfernt den Tag aus dem Header bei Weiterleitung an eine "normale" Schnittstelle
- Anmerkung: Im VLAN Tag codieren 3 Bits eine Priorität => Scheduling am Link

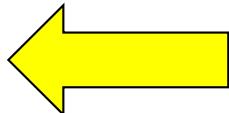
Vergleich zwischen Verbindungskomponenten

	Hub	Switch	Router
Schicht	Physikal. (1)	Sicherung (2)	Netzwerk (3)
Isolation des Netzwerkverkehrs	Nein	Ja	Ja
Plug and Play	Ja	Ja	Nein
Optimales Routing	Nein	Nein	Ja

Kapitel 6: Sicherungsschicht & LAN

Gliederung

- Einführung und Grundlagen
- Punkt-zu-Punkt-Protokolle
- Mehrfachzugriffsprotokolle (MAC)
- LAN-Adressen und ARP
- Ethernet
- Switches
- Zusammenfassung

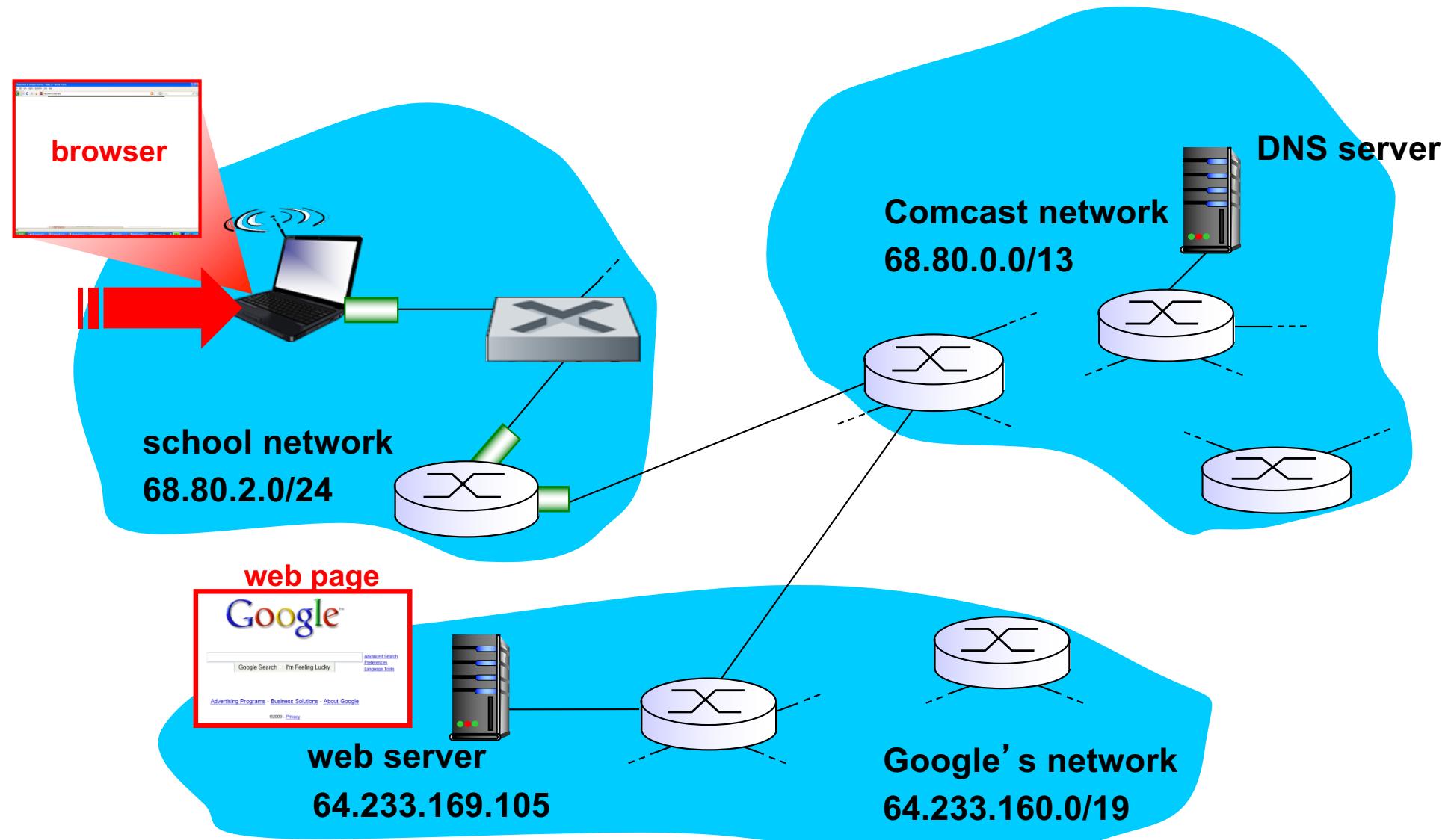


Textbuch zu diesem Kapitel: J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz, Kapitel 5

Folien und Abbildung teilweise aus:

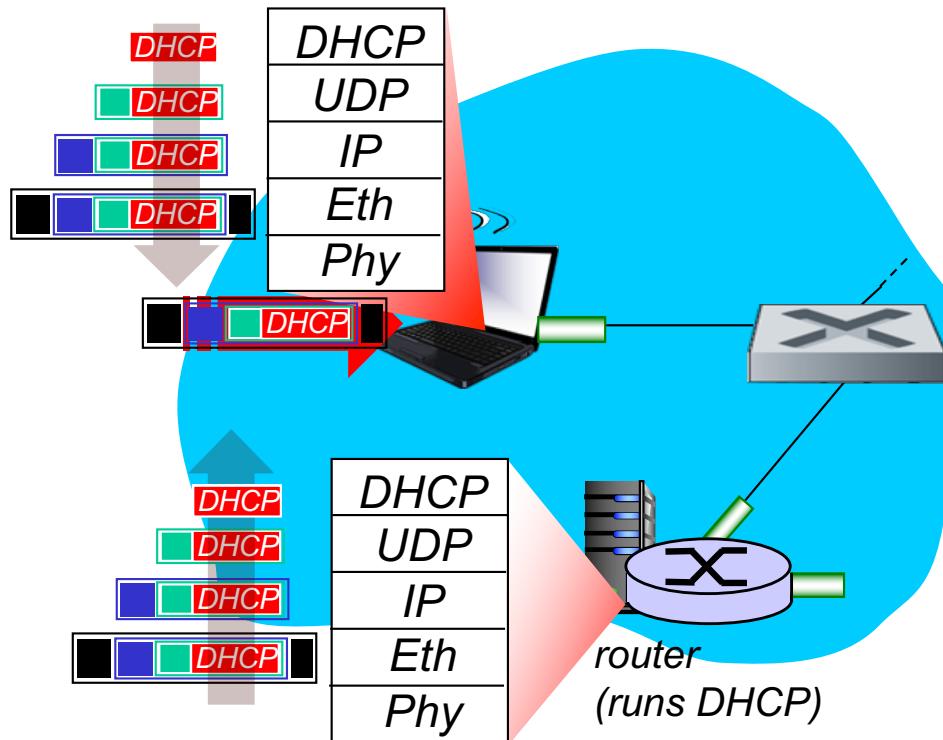
J. Kurose & K. Ross: Computernetzwerke – Der Top-Down-Ansatz

Die Reise einer Anfrage bei Google



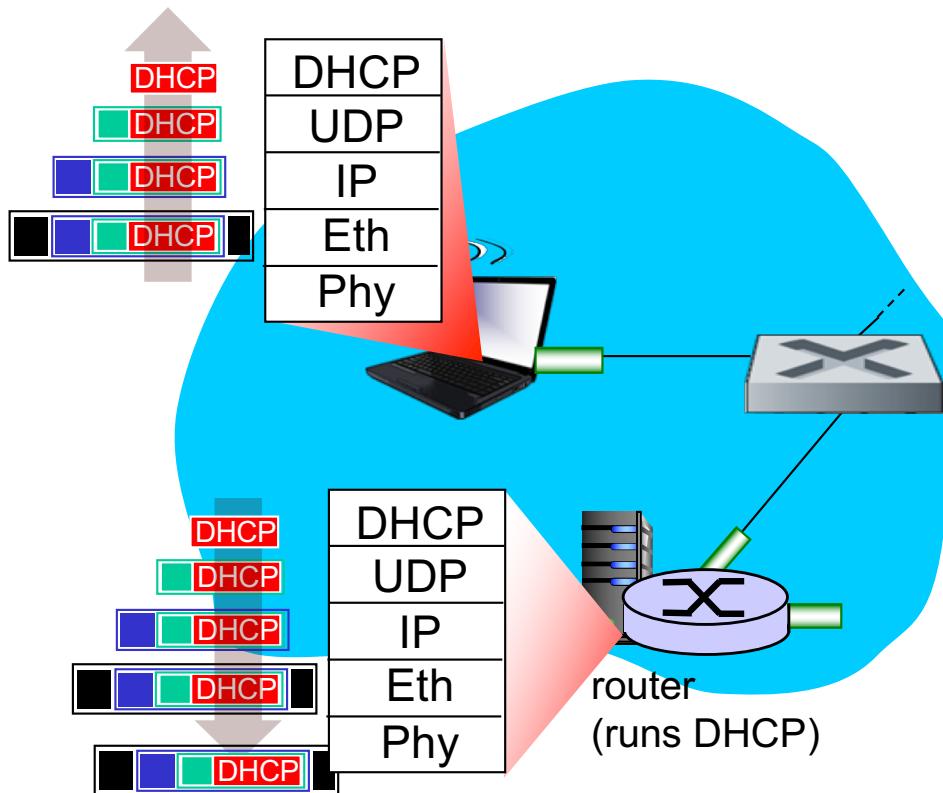
Quelle der Folien: Kurose & Ross: Computernetzwerke – Der Top-Down-Ansatz

connecting to the Internet



- connecting laptop needs to get its own IP address, addr of first-hop router, addr of DNS server: use **DHCP**
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.3 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet *demuxed* to IP demuxed, UDP demuxed to DHCP

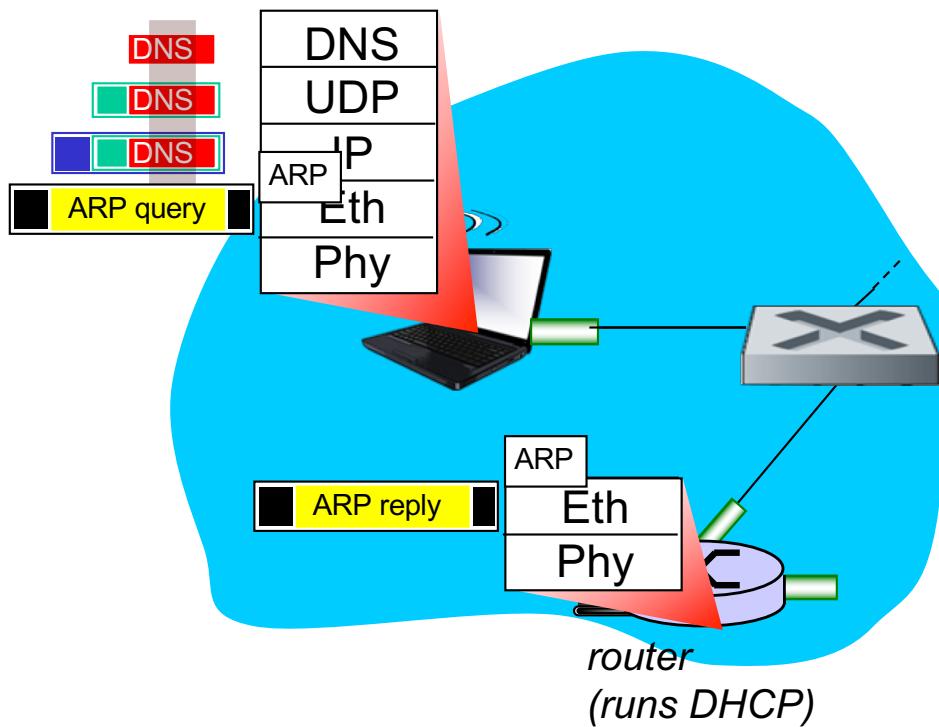
connecting to the Internet



- DHCP server formulates **DHCP ACK** containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- encapsulation at DHCP server, frame forwarded (switch learning) through LAN, demultiplexing at client
- ❖ DHCP client receives DHCP ACK reply

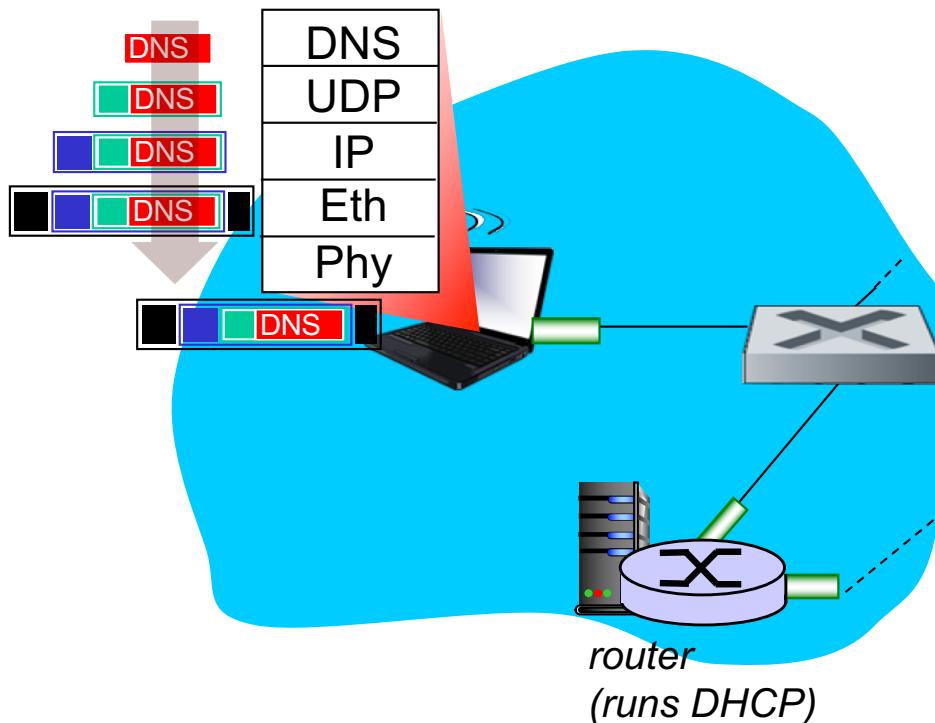
Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router

ARP (before DNS, before HTTP)

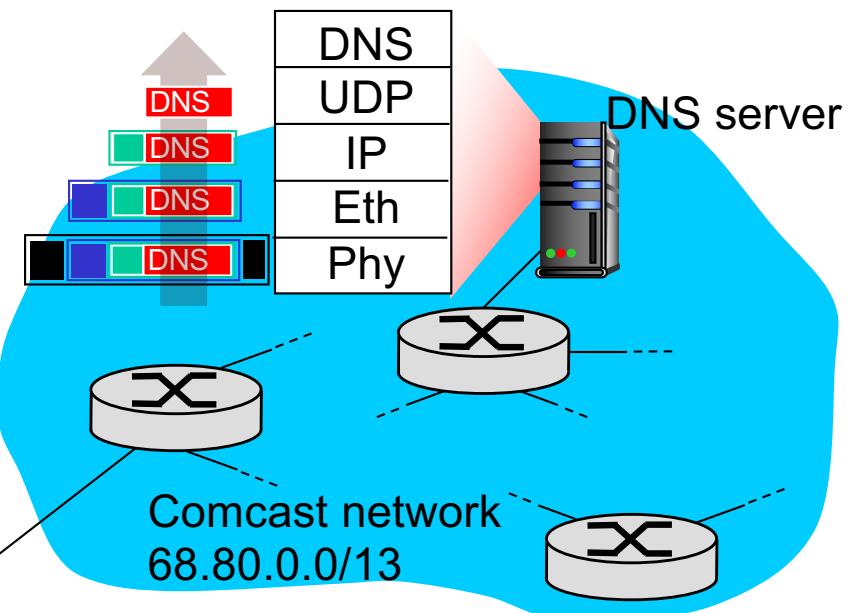


- before sending **HTTP** request, need IP address of www.google.com: **DNS**
- DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, need MAC address of router interface: **ARP**
- ARP query broadcast, received by router, which replies with ARP reply giving MAC address of router interface
- now knows MAC address of first hop router, so can now send frame containing DNS query

using DNS

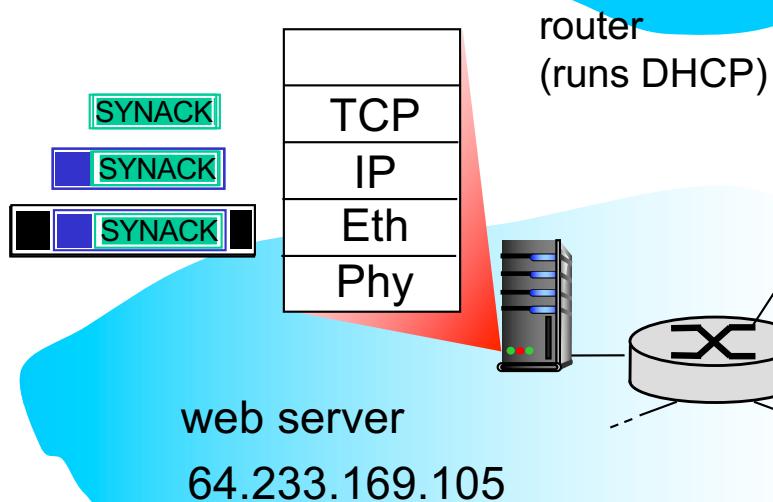
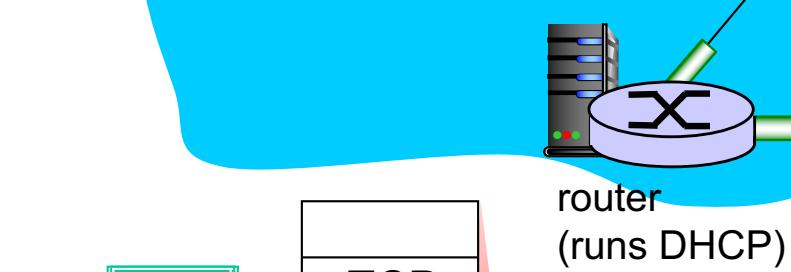
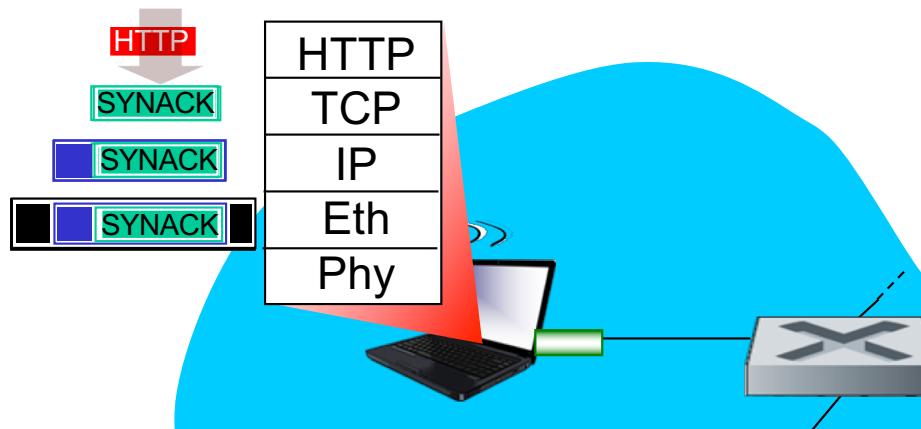


- IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router



- IP datagram forwarded from campus network into comcast network, routed (tables created by **RIP**, **OSPF**, **IS-IS** and/or **BGP** routing protocols) to DNS server
- demux'ed to DNS server
- DNS server replies to client with IP address of www.google.com

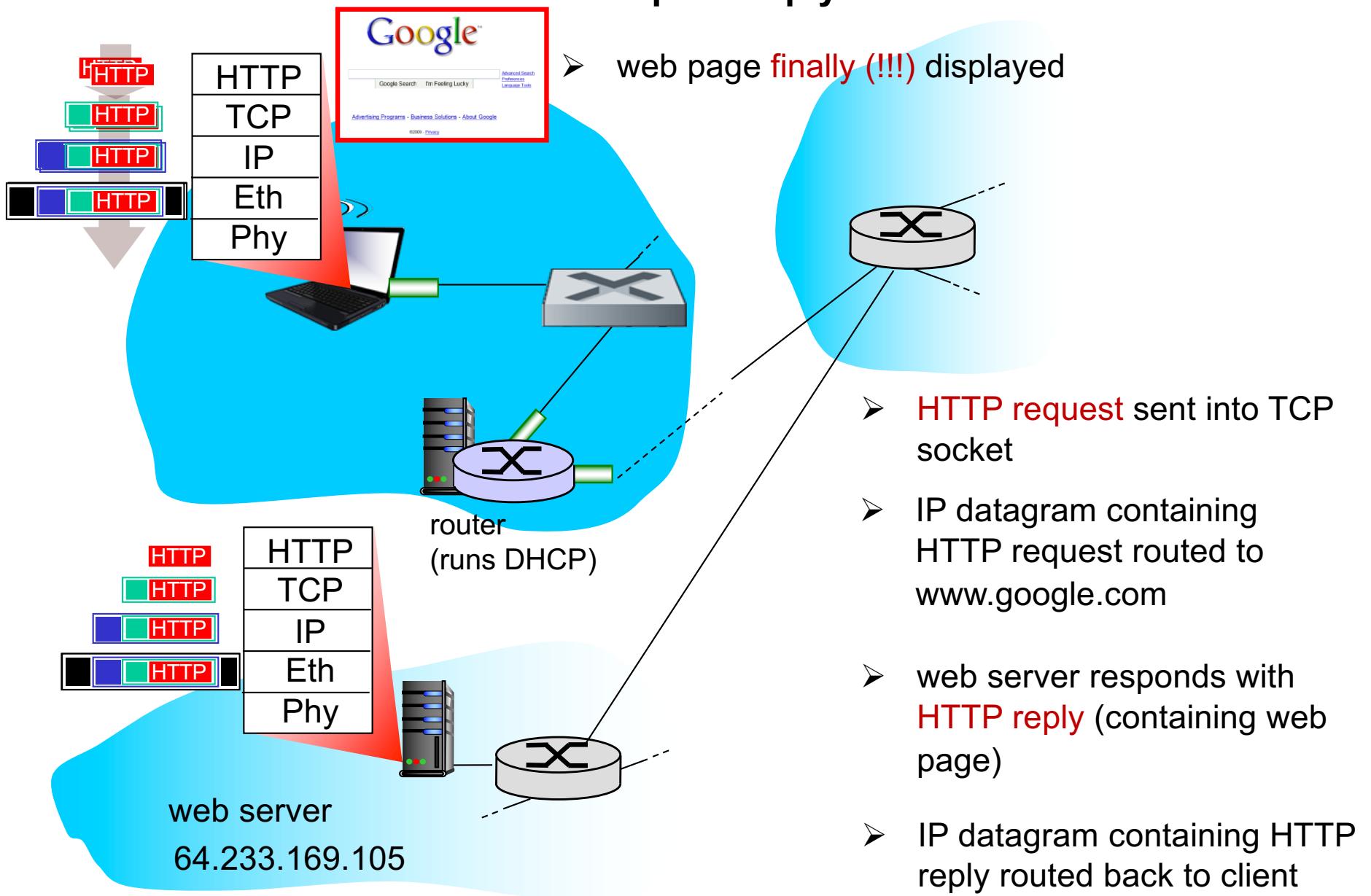
TCP connection carrying HTTP



web server
64.233.169.105

- to send HTTP request, client first opens **TCP socket** to web server
- TCP **SYN segment** (step 1 in 3-way handshake) inter-domain routed to web server
- web server responds with TCP **SYNACK** (step 2 in 3-way handshake)
- TCP **connection established!**

HTTP request/reply



Zusammenfassung

