Digitale Kommunikation und Internetdienste 1

Wintersemester 2004/2005 – Teil 4

Belegnummer Vorlesung: 39 30 02

Übungen: 39 30 05

Jan E. Hennig

AG Rechnernetze und Verteilte Systeme (RVS)
Technische Fakultät
Universität Bielefeld

jhennig@rvs.uni-bielefeld.de

basierend auf den Arbeiten von Michael Blume, Heiko Holtkamp, Marcel Holtmann und I Made Wiryana

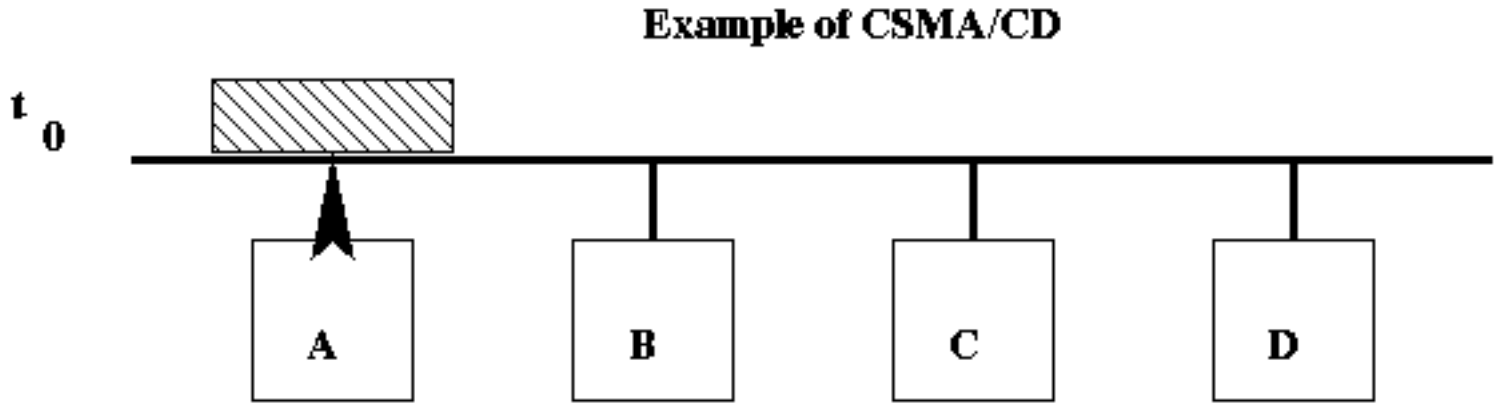
Übersicht

- Kollisionen
- binärer exponentieller „Backoff-Algorithmus”
- Ethernet-Geräte und deren OSI-Klassifikation
  - Repeater
  - Hub
  - Bridge
  - Switch
  - Router
  - Gateway

Erinnerung

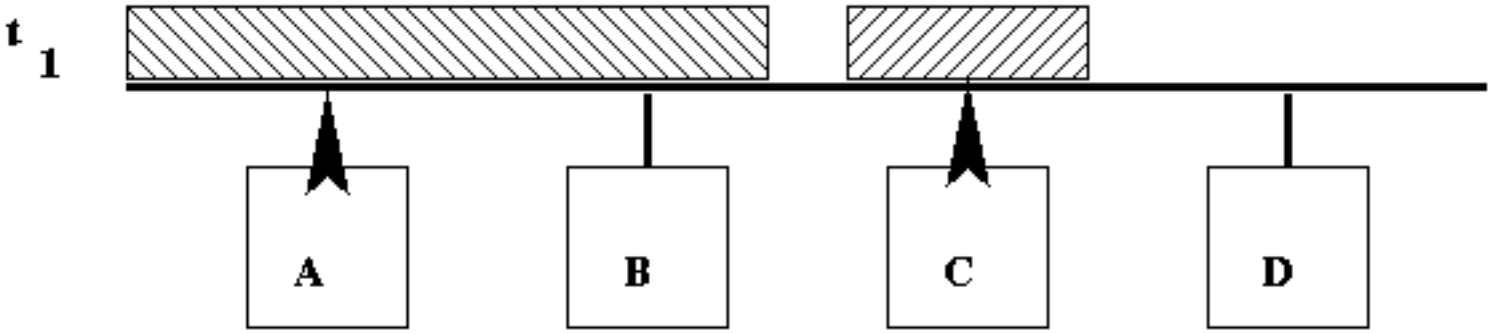
- mehrere Knoten an einem gemeinsamen Übertragungsmedium
- Konflikt (Kollision), wenn zwei Knoten gleichzeitig senden
- Ethernet arbeitet senderorientiert
- Vorgehen beim Senden:
  1. senden wenn „Leitung frei”
  2. sonst warten, bis frei
  3. falls Kollision während des Sendens, dann sofort stoppen und Warnsignal senden
  4. anschließend warten und dann nochmals versuchen
- Um Kollisionen erkennen zu können ist eine Mindestpaketgröße vorgeschrieben

Beispiel einer Kollision (1)



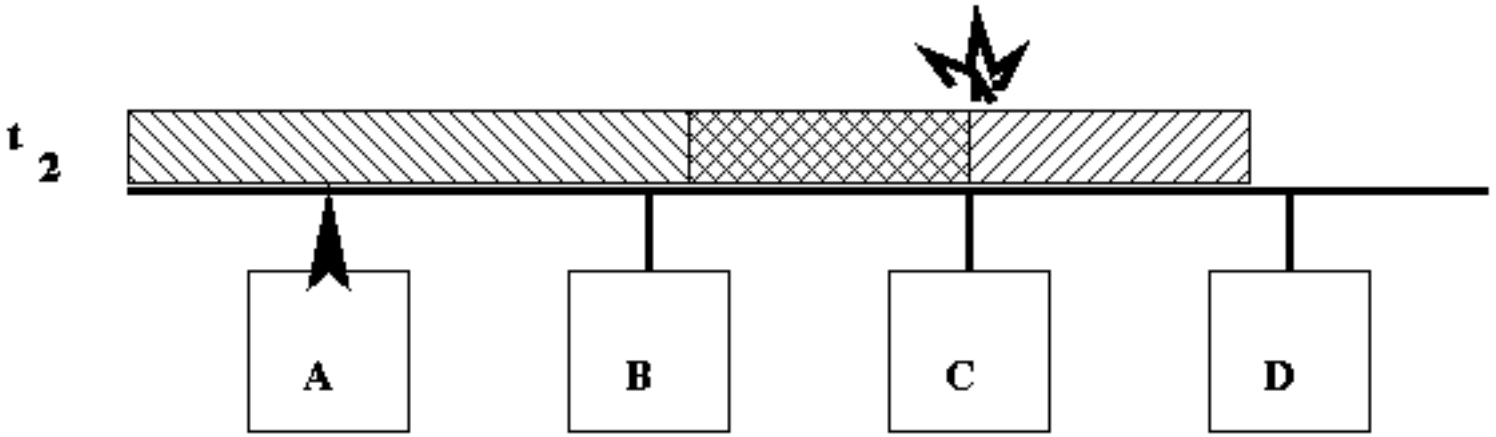
- mehrere Hosts sind im Netz eingebunden
- t_0: Host A stellt keinen Netzverkehr fest und beginnt mit dem Senden

Beispiel einer Kollision (2)



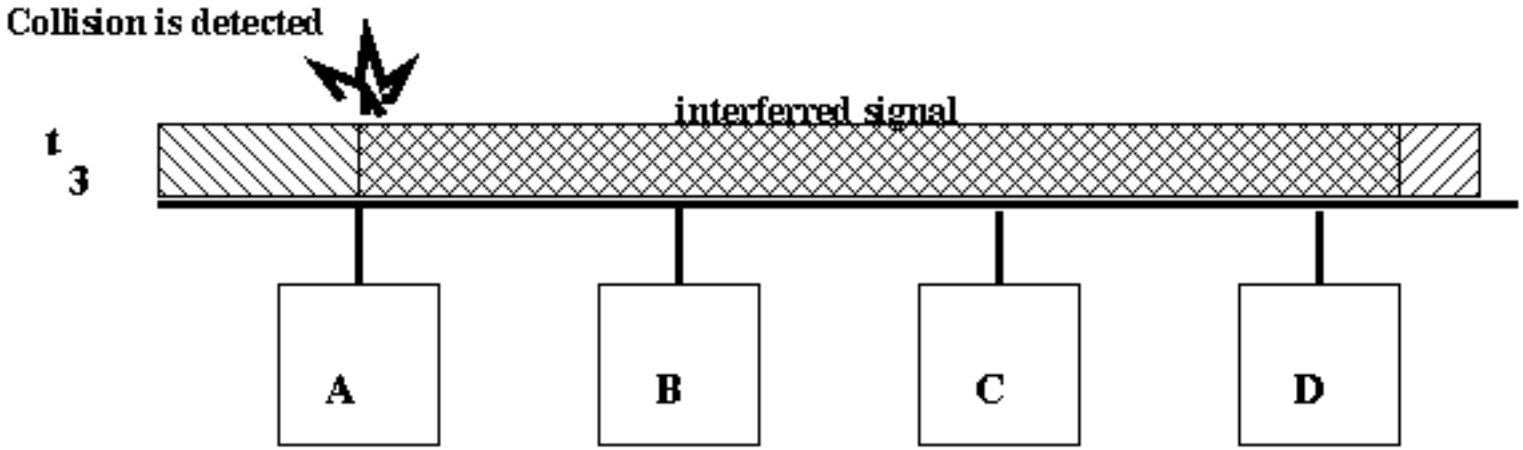
- endliche Ausbreitungsgeschwindigkeit elektromagnetischer Wellen
- t_1: Host C stellt keinen Netzverkehr fest und beginnt mit dem Senden
- obwohl Host A bereits sendet

Beispiel einer Kollision (3)



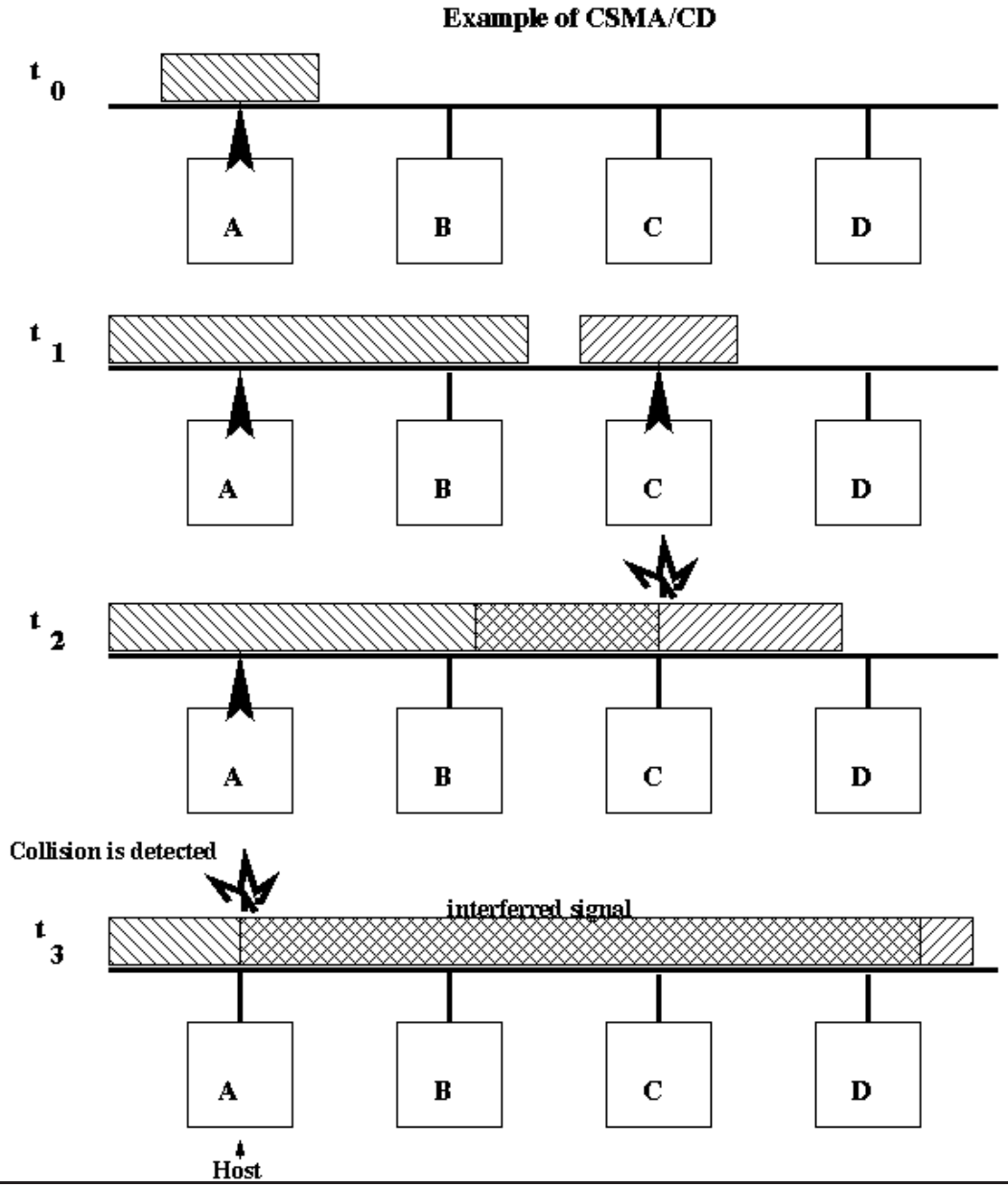
- t_2: die von Host A ausgesendeten Daten haben den Host C erreicht
- Host C erkennt die Kollision aufgrund der Interferrenz der Signale von Host A und C
- Host C unterbricht daraufhin seine Übertragung
- und sendet Warnsignal (auch JAM-Signal genannt)

Beispiel einer Kollision (4)



- t_3: das Kollisionsrauschen erreicht Host A
- Host A stellt nun ebenfalls die Übertragung ein

Beispiel: Übersicht



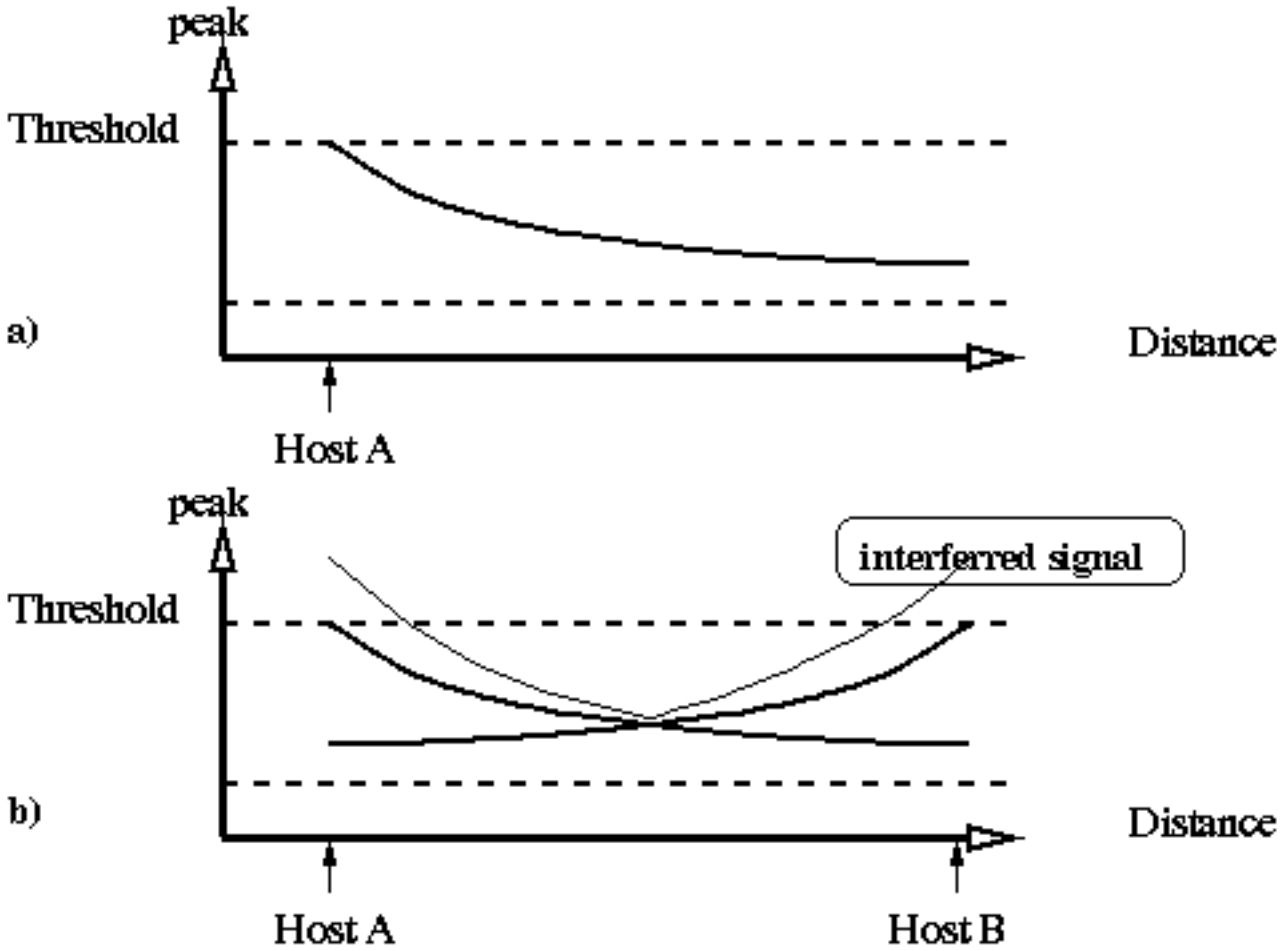
Folgerungen

- ein Host kann nur während seiner Datenübertragung eine Kollision feststellen
- die minimale Paketlänge ist nötig
  - wäre sie zu kurz, könnte Nachricht bereits übermittelt sein, bevor die Signale von C Host A erreichen
  - Host A würde dann von einer kollisionsfreien Übermittlung ausgehen
  - Eigenschaft des JAM-Signals: verlängert die Kollision
  - dient dem Vorbeugen gegen unerkannte Kollisionen
- die maximale Entfernung zweier Knoten im Netz (Netzausdehnung) muß begrenzt sein

Netzausdehnung

- maximale Netzausdehnung so gewählt, daß Übertragung eines Pakets mit Minimallänge mehr als die *doppelte Zeitspanne* einer einfachen Signalübertragung zwischen den Enden benötigt
- außerdem: Beachtung der Dämpfung
- Signalpegel werden mit der Entfernung zum Sender schwächer
- bei Coax-Verkabelung: Maximalwert wird bei Kollision überschritten
- bei Twisted-Pair-Verkabelung: Sende- und Empfangsleitungen getrennt: falls Signal auf Empfangsleitung während des Sendens → Kollision

Dämpfung


peak
Threshold
a)
Distance
Host A
peak
interferred signal
Threshold
b)
Distance
Host A
Host B

Kollisionsdomäne

- je mehr Knoten senden, desto mehr Kollisionen
- trifft alle Knoten in einem Netzwerksegment
- man spricht auch von der *Kollisionsdomäne (collision domain)*
- dies ist einen Bereich des Netzwerks, in welchem jeweils nur ein Knoten seine Daten auf den Daten-Kanal stellen kann, ohne daß es zu einer Kollision kommt
- bei ca. 30 Knoten: Übertragungsleistung von nur noch ca. 30-40% (Richtwert)

Wartezeit

- Falls Kollision erkannt: Übertragungsstop für zufällige Zeitspanne
- Wartezeit bestimmt sich durch aneinanderhängen fester Zeitintervalle
- Intervall korrespondiert mit maximaler Netzwerkausdehnung
- z.B. bei ThickEthernet beträgt ein Intervall $51.2\mu s$
- diese Zeit benötigt ein Paket minimaler Länge im „worst case”

Längenberechnung

- Beispiel: idealer Fall, nur zwei Knoten
- 10Mbps-Ethernet benutzt 10MHz-Frequenz zum Datenübertragen
- entspricht 10×10^6 Bits und Takte (Manchester: 1 Bit pro Takt)
- kleinste erlaubte Paketgröße: 64 Byte, entspricht $51,2\mu s$
- Ausbreitungsgeschwindigkeit:
  - Faktor $1,00$ im Vakuum
  - Faktor $0,77$ für Koaxialkabel
  - Faktor $0,60$ für Twisted-Pair-Kabel

Beispielrechnung

- Signal von $51,2\mu s$ im Koaxialkabel

$$0.77 \times 3 \times 10^8 = 231 \times 10^6 m/s \text{ (coax)}$$
$$231 \times 10^6 \times 51.2 \times 10^{-6} = 11827.20m = 11.82km$$

- bei ThickEthernet: maximale Länge 2500m
- $\rightarrow$ 64-Byte-Frame benötigt also für $2 \times 2,5km = 5km$ nur etwa die Hälfte der minimalen Übertragungsdauer
- dient als Reserve (hier: idealer Fall), z.B. für Verzögerung durch Repeater (Signalverstärker)

Bin. exp. Backoff-Algorithmus (1)

- Ethernet verwendet festen Algorithmus für Wartezeit
- den *binären exponentiellen „Backoff-Algorithmus”*
- Menge von Warteslots
- aus der Menge wird zufällig ein Slot ausgewählt
- bei erster Kollision: $\{0, 1\}$
- d.h. Host A und C warten entweder $0 \times 51,2\mu s$ oder $1 \times 51,2\mu s$

Bin. exp. Backoff-Algorithmus (2)

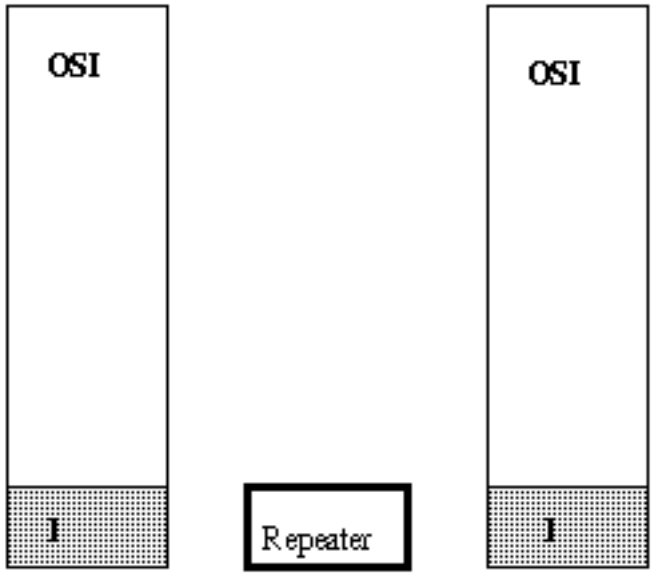
- falls zufällig gleicher Slot gewählt: erneute Kollision
- exponentielles Erweitern der Menge
- nun: $\{0, 1, 2, 3\}$, Kollisionswahrscheinlichkeit 0,25
- generell: nach K Kollisionen Menge von Slots zwischen 0 und 2^{K-1}
- zudem Maximalzahl 1023 (entspricht 10 Kollisionen)
- nach 16 Kollisionen Fehlermeldung und Aufgeben des Sendens

Ethernet-Geräte

- Repeater (Signalverstärker)
- Hub
- Bridge
- Switch
- Router
- Gateway

Repeater (1)

- reicht Signal „fast ohne Verzögerung” von einem Anschluß zum anderen weiter
- Gerät der OSI-Schicht 1
- dadurch für andere Knoten im Netzwerk „unsichtbar”



Repeater (2)

- verstärkt Signale, z.B. bei sehr großen Kabellängen
- teilt ein Netz in physikalisch unabhängige Segmente
- trotzdem bleibt die logische Topologie eines Busses erhalten
- erhöht somit nicht die Netzkapazität
- kann fehlerhafte elektrische Signale herausfiltern
- grenzt bestimmte Fehler (z.B. Kabelbruch) auf das jeweilige Segment ein

Medienkonverter

- Repeater werden oft als Medienkonverter eingesetzt
- es gibt aber auch „reine” Medienkonverter ohne Signalfilterung
- reine Medienkonverter erhöhen somit nicht die Netzwerksicherheit

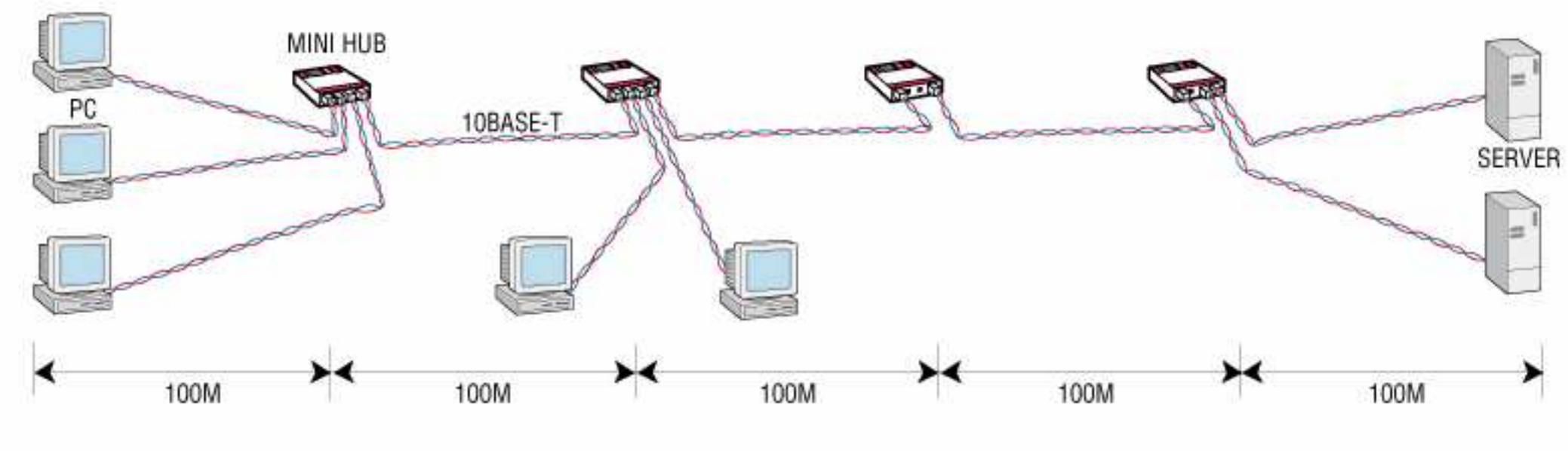
Regeln

- Anzahl und Einsatz von Repeatern ist nicht beliebig wählbar
- keine Ring- oder Schleifenanordnung erlaubt
- da Repeater eine (wenn auch kleine) Verzögerung mit sich bringen dürfen nicht zu viele Repeater hintereinander geschaltet sein
- direkter Schluß aus CSMA/CD-Eigenschaften
- dazu dient die 5-4-3-Repeater-Regel

5-4-3-Repeater-Regel

- Eine Netztopologie, die nur auf Repeatern beruht, darf aus **max. 5 Segmenten** bestehen.
- Es sind auf dem Übertragungsweg max. nur **4 Repeater** erlaubt.
- Bis zu **3 Segmente** dürfen **direkten Anschluß an Userknoten** haben. Der Rest müssen Punk-zu-Punkt-Verbindungen zwischen den Repeatern sein, sog. *Inter Repeater Links (IRL)*.

5-4-3-Repeater-Regel (Beispiel)

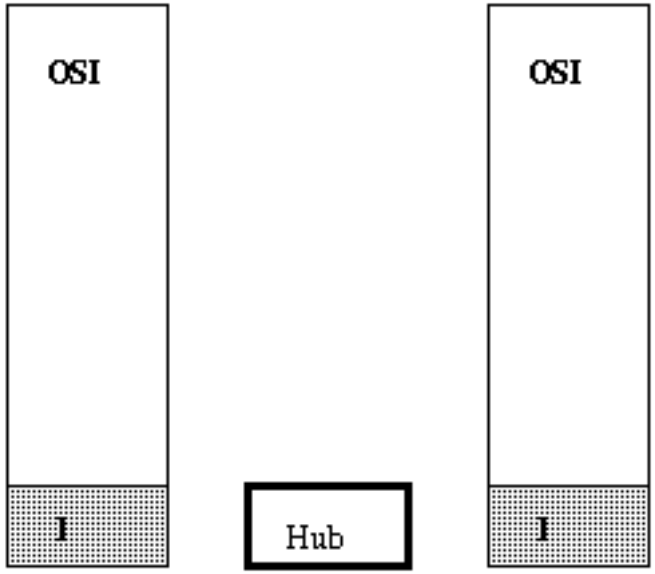


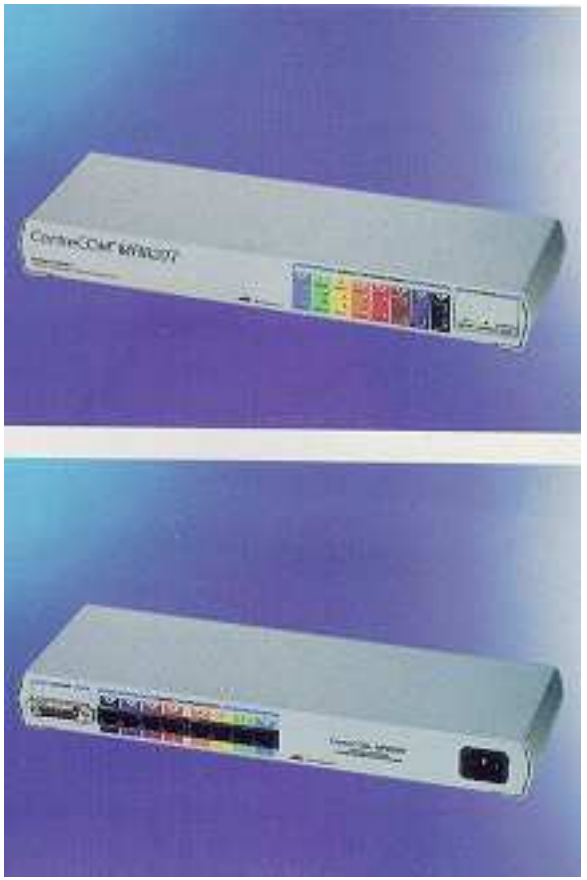
Network expansion with respect to the 5–4–3 Repeater rule

(5 Segmente, 4 Repeater, 3 Segmente mit direktem Anschluß an Userknoten)

Hub (1)

- *Hub* von engl. *Achse*
- auch *Multiport-Repeater* genannt
- Gerät der OSI-Schicht 1





Hub (2)

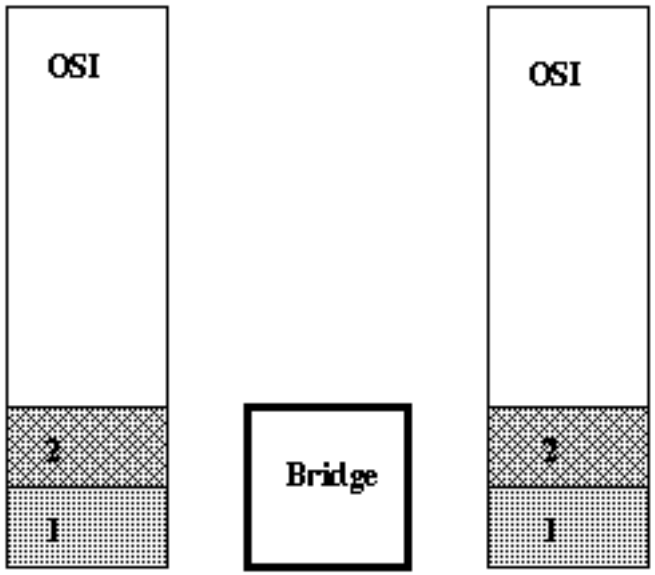
- gehorcht ebenfalls der Repeater-Regel
- Bezeichnung nicht einheitlich
- verteilt die an einem *Anschluß* (auch engl. *port*) ankommenden Signale auf alle weiteren benutzte Anschlüsse
- teilt ein Netz in physikalisch unabhängige Segmente
- trotzdem bleibt die logische Topologie eines Busses erhalten
- erhöht somit nicht die Netzkapazität

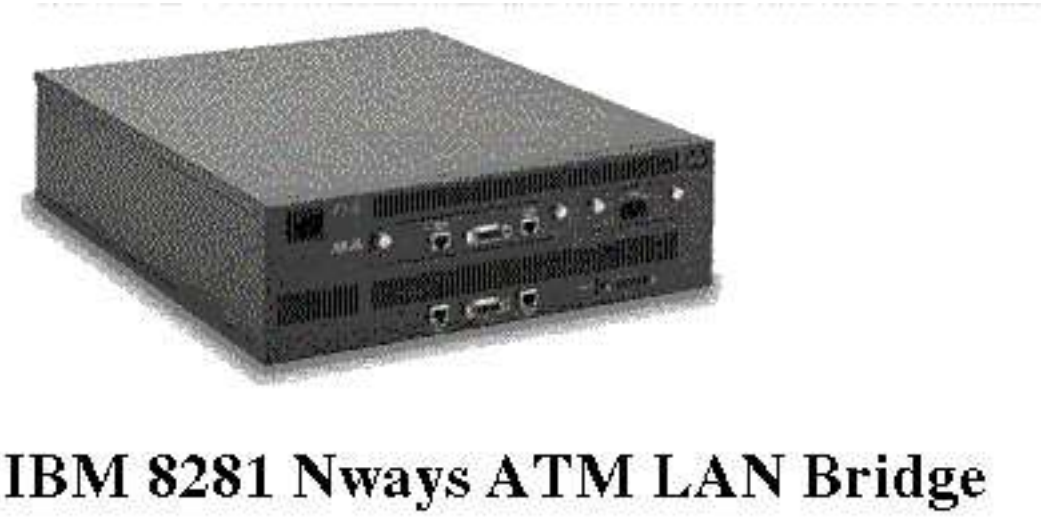
Hub (3)

- einige Hubs lassen sich zu einem Stack vereinen
- schnelle, hersteller-spezifische Anschlüsse
- dadurch leichte Erweiterbarkeit beim Wachsen eines Netzwerks
- derartig verbundene Hubs zählen als nur ein Repeater bei der Repeater-Regel
- nicht verwechseln mit „uplink port”
- dies ist ein „normaler” Anschluß mit anderer Pinbelegung

Bridge (1)

- Gerät der OSI-Schicht 2
- beschrieben in IEEE 802.1d
- Trennung von Kollisionsdomänen





IBM 8281 Nways ATM LAN Bridge

Bridge (2)

- kann LANs mit verschiedenen physikalischen Eigenschaften verbinden
- z.B. Coax- mit Twisted-Pair-Netzwerke
- dazu müssen jedoch alle Protokolle der höheren Ebenen 3-7 konform sein
- eine Bridge ist *protokolltransparent*
- im Netz muß die gleiche Adressierung vorliegen (MAC-Adressen)

Bridge (3)

- sorgt nicht (kaum) für eine logische Unterteilung
- sondern für eine physikalische Unterteilung
- interpretiert MAC-Adressen
- lernt, welche MAC-Adressen an welchem Anschluß auftreten

Bridge (4)

- Eigenschaft *Ausfallsicherheit*
  Störungen gelangen nicht von einer auf die andere Seite, Trennung von Kollisionsdomänen

- Eigenschaft *Datensicherheit*
  Informationen, die zwischen Knoten auf einer Seite der Bridge ausgetauscht werden, können nicht auf der anderen Seite der Bridge abgehört werden

- Eigenschaft *Durchsatzsteigerung*
  In den durch Bridges getrennten Netzsegmenten können unterschiedliche Daten gleichzeitig transferriert werden. Hierdurch wird die *Netzperformance* erhöht.

Bridge (5)

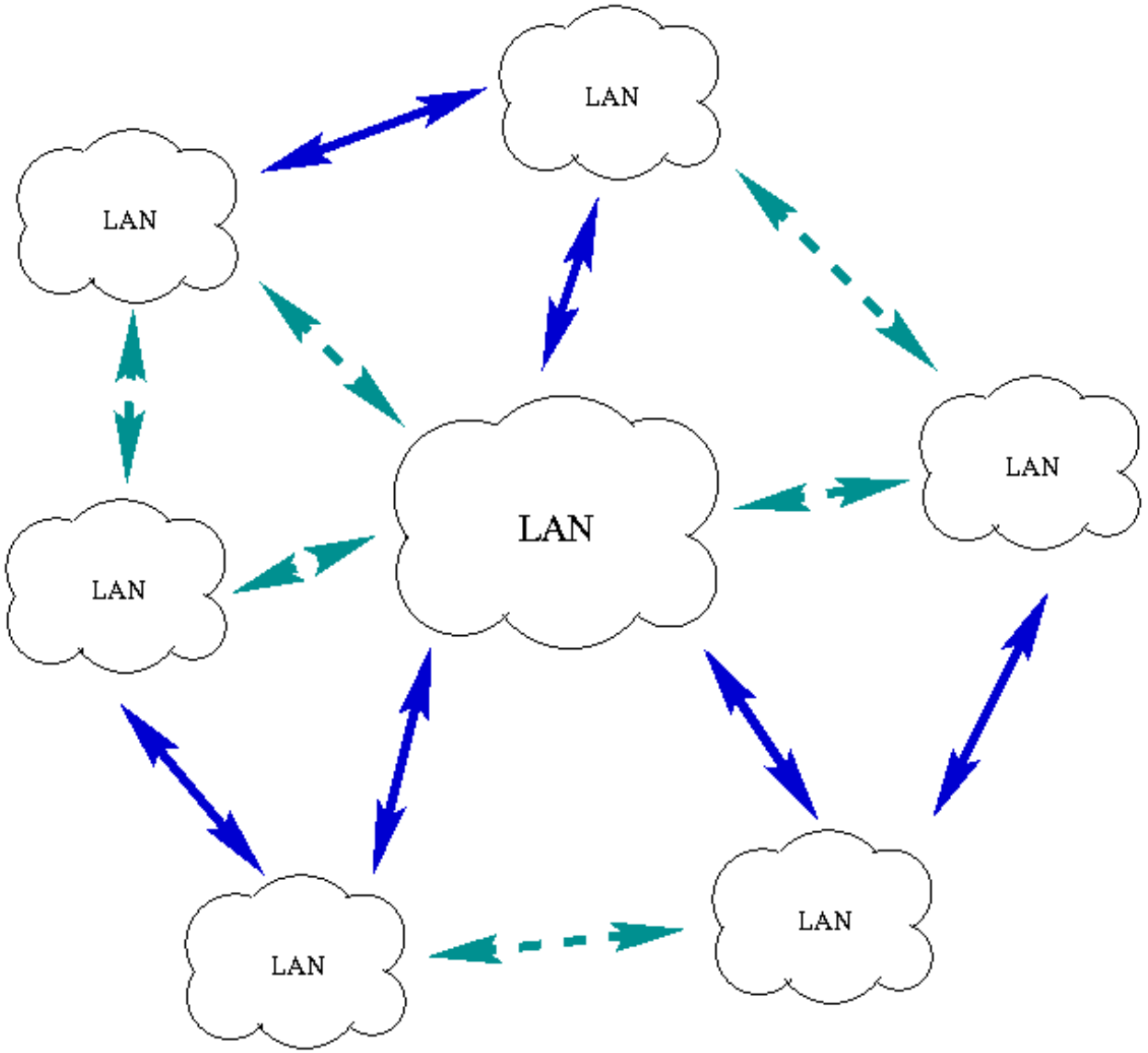
Eigenschaft *Vermeiden von Netzwerkschleifen*

- Mit dem sog. *Spanning Tree-Algorithmus* ist es möglich Schleifen- und Ringanordnungen (also redundante Verbindungen) sicher zu betreiben.
- Die Bridges im Netz kommunizieren miteinander,
- (im Gegensatz zu „dummen" Repeatern oder Hubs)
- stellen über den Algorithmus sicher, daß bei mehreren redundanten Verbindungen immer nur eine gerade aktiv ist.
- dies verhindert kreisende Pakete im Netz.

Spanning Tree-Algorithmus

- ist in IEEE 802.1d spezifiziert
- ersetzt redundante Pfade durch einen deterministischen logischen Pfad im Netz
- dadurch, daß ein Pfad aus mehreren gewählt wird
- dazu „beratschlagen” sich die Bridges im Netz
- und wählen schrittweise einen geeigneten Pfad

Spanning Tree: Beispiel



Example for the Spanning Tree Algorithm

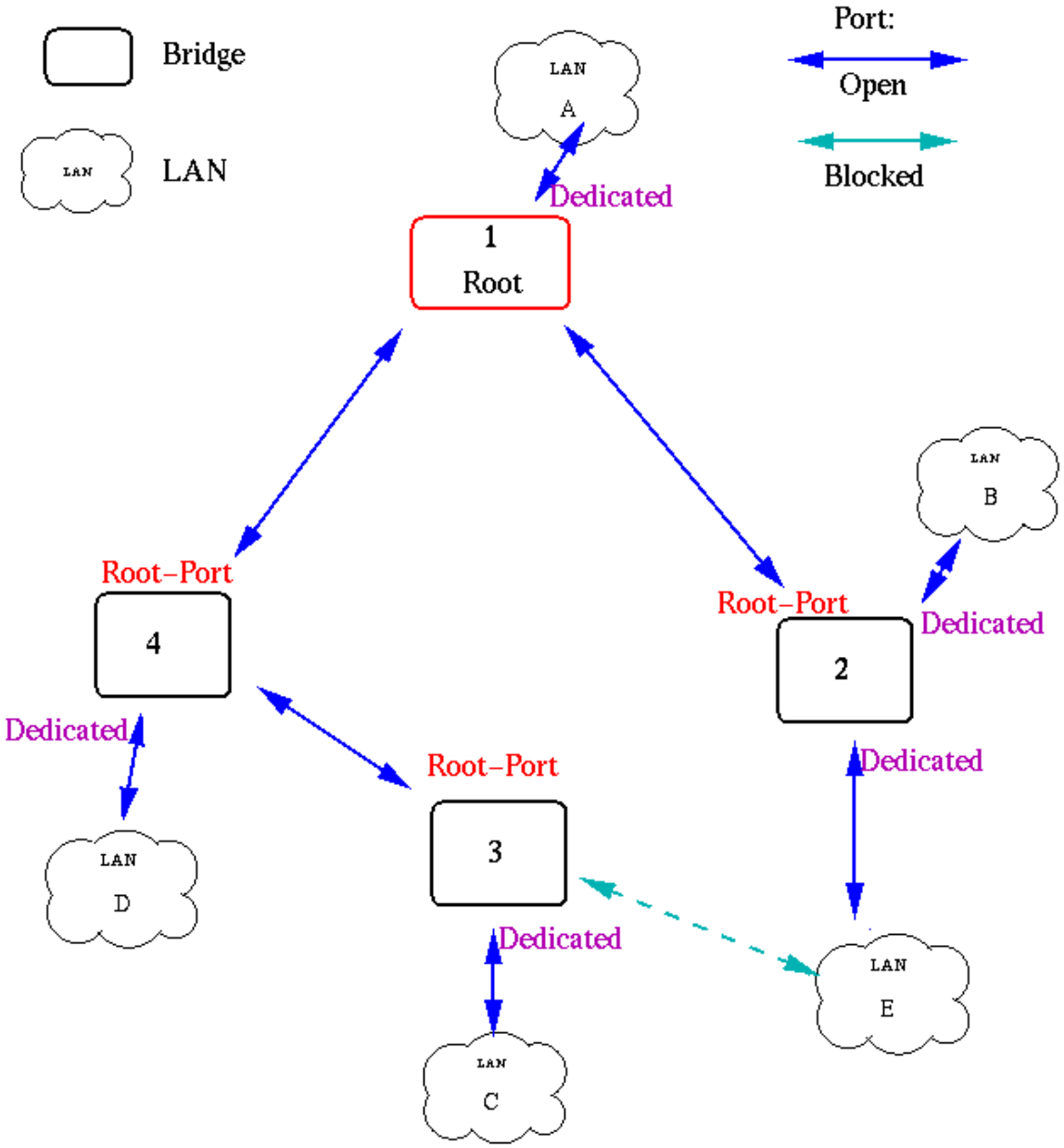
Spanning Tree: Details

- Bridges kommunizieren über sog. *Bridge Protocol Data Units (BPDUs)*
- Bridge: Eindeutige Bridge-ID
- Anschluß/Port: Eindeutige Port-ID
- Anschluß/Port: Relative Port Priorität
- Port: Kostenfaktor für jeden Port
  (je höher die Netzwerk-Performance im angeschlossenen LAN, desto geringer die Kosten)

Spanning Tree: Vorgehen

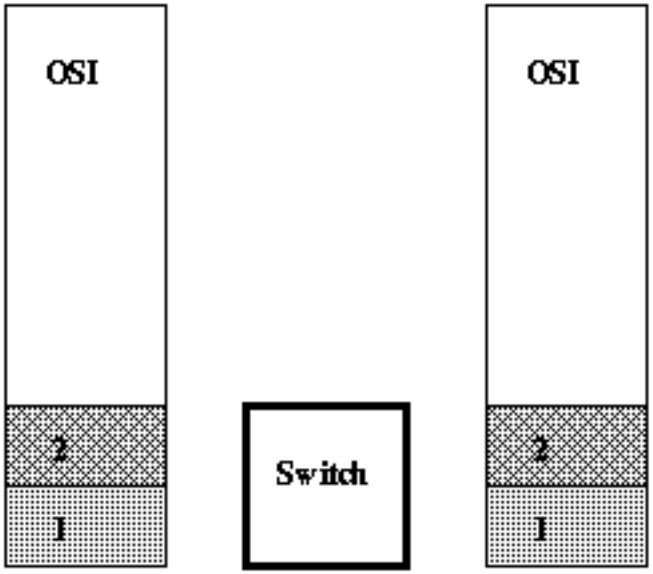
1. Auswahl der Root-Bridge
   - Bridge mit der kleinsten Bridge-ID
   - Bei gleicher ID wird diejenige mit der kleinsten MAC-Adresse gewählt
2. Auswahl eines Root-Ports pro Bridge
   - Ausnahme Root-Bridge, sonst bei jeder Bridge Festlegen eines Ports als Root-Port nach Kostenfaktor.
   - Verbindung mit geringstem Kostenfaktor zur Root-Bridge ist Root-Port.
3. Zuordnung einer Bridge pro LAN
   - Diese verhindert Schleifen.
   - Falls nur eine Bridge an einem LAN: der entsprechende Port wird dem LAN global zugeordnet.
   - Falls mehrere Bridges mit direktem Zugang zu einem LAN: Wahl des Ports mit den geringsten Kosten zur Root-Bridge.

Spanning Tree: Baum



Switch (1)

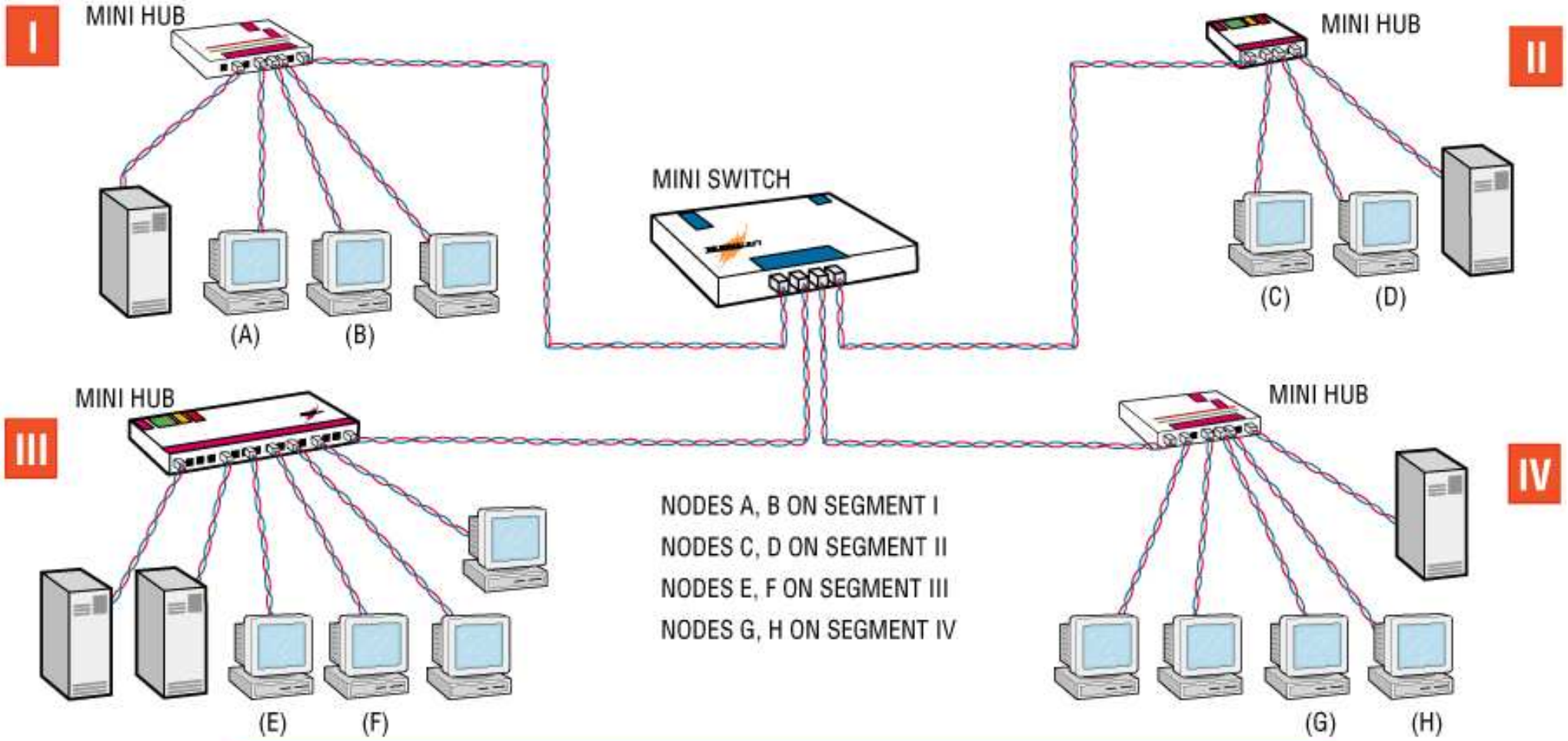
- Gerät der OSI-Schicht 2
- wird auch *Multiport-Bridge* genannt
- Begriff „Switch” wurde vom Hersteller Calpana eingeführt



Switch (2)

- kann LANs mit verschiedenen physikalischen Eigenschaften verbinden
- z.B. Coax- mit Twisted-Pair-Netzwerke
- dazu müssen jedoch alle Protokolle der höheren Ebenen 3-7 konform sein
- untersucht Datenpakete auf MAC-Adresse
- erhöht die Netzwerkperformance:
  - teilt Netzwerk in Segmente (jeweils eine Kollisionsdomäne)
  - kann seine Ports bei Bedarf miteinander verschalten, mehrere zur gleichen Zeit

Switch – Beispiel



TRAFFIC EXAMPLES	
NODE A to NODE H	Packet arrives in switch on segment I and is forwarded to segment IV ONLY
NODE E to NODE F	Packet arrives in switch on segment III and is filtered from the rest of the network (because the switch knows that F is on the same segment as E)

Switch (3)

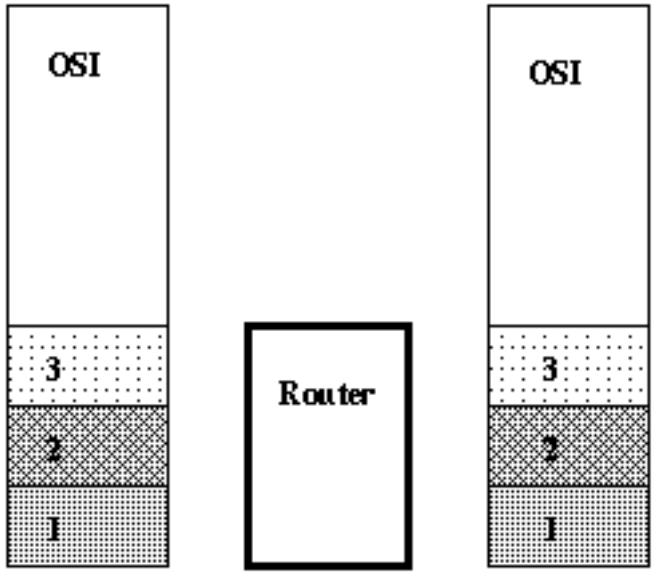
- Netzlast sollte möglichst gleichmäßig auf die Ports verteilt werden
- z.B. ein vielfrequentierter Knoten sollte an ein Einzelsegment (exklusives Segment) angeschlossen werden (alleine am Port)
- Ziel: Reduktion der Datenmenge, die mehr als ein Segment durchlaufen muß
- zwei etablierte Typen:
  - Cut-Through
  - Store-And-Forward

Switch-Typen

- Cut-Through
  - bietet sehr kurze Verweilzeit (Latenz)
  - nur Quell-/Zieladresse wird gelesen
  - jedoch: defekte bzw. ungültige Pakete passieren Switch
- Store-And-Forward
  - untersucht das gesamte Datenpaket
  - Pakete werden zwischengespeichert und CRCs verglichen
  - danach entweder verworfen oder weitergeleitet
  - kann bei häufig fehlerhaften Paketen Netzwerkperformance sehr verbessern
  - jedoch: höhere Latenz

Router (1)

- Gerät der OSI-Schicht 3
- häufig Begriffsverwechselung mit „Gateway”
- verknüpft unterschiedliche Protokolle bis zur OSI-Schicht 3



Router (2)

- Adressierung der OSI-Schicht 3 muß einheitlich sein (z.B. IP)
- verbindet so aber auch verschiedene Topologien miteinander
- untersucht Adressangaben im Datenpaket
- leitet Daten in Abhängigkeit seiner *Routing-Tabelle* weiter
- arbeitet nicht mit MAC-Adressen

Router (3)

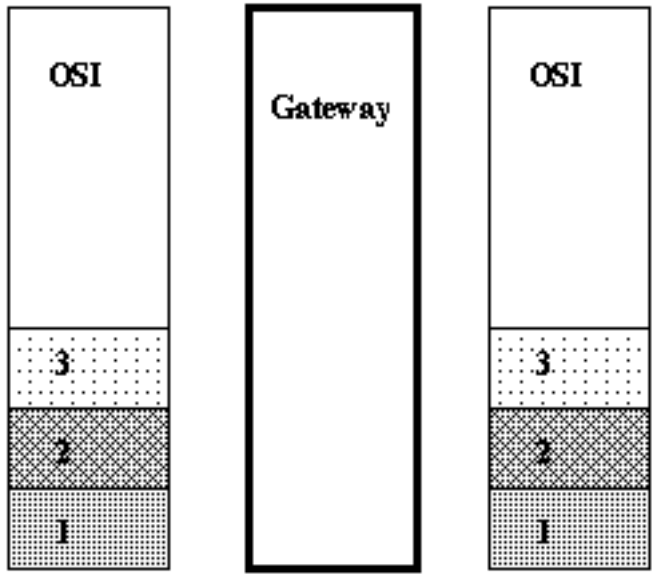
- durch ausführlichere Untersuchung höhere Latenzzeit
- dafür nur Adressen der Ebene 3 benötigt
- Wegfindung kann auch über Algorithmen (berechnet) erfolgen
- kann so bestmöglichen Weg für die Daten finden
- dieses Weiterleiten von Daten heißt *Routen (routing)*
- zwei Aussprachen gängig

Router (4)

- Router verstehen oft mehr als ein Protokoll der Ebene 3 (z.B. IP, IPX, AppleTalk)
- Es gibt Router mit zusätzlicher Bridge-Funktionalität
- Router oft umfangreich konfigurierbar
- Router unterstützen oft das sog. *Tunneln (tunneling)* von Protokollen (z.B. IPv6 über IPv4)
- Oft bieten Router auch eine Filterfunktion (z.B. die einer Paketfilter-*Firewall*)
- Broadcasts werden i.d.R. nicht weitergeleitet

Gateway

- Gerät der OSI-Schicht 7
- ermöglicht das Verbinden völlig unterschiedlicher Systeme
- z.B. TCP/IP-Systeme – DECnet-Hosts
- oft nicht nur reine Hardwarelösung sondern Softwaremodule
- unterstützt kein Tunneln, sondern setzt das jeweilige Protokoll real in ein anderes um



Netzwerkkarte

- Teil eines PCs
- heute seltener als Steckkarte, häufiger bereits direkt auf der Hauptplatine untergebracht
- für sich allein genommen ein Gerät der OSI-Schicht 1
- der Netzwerkkartentreiber entspricht grob OSI-Schicht 2
- mit entsprechender Software kann ein PC alle höheren Aufgaben bis hin zu OSI-Schicht 7 durchführen

Aussicht

Themenübersicht für die kommende Vorlesung:

- Address Resolution Protokoll (ARP)
- Token Ring
- Internet Layer
- Internet Protocol

Ende Teil 4. Danke für die Aufmerksamkeit.