Telematik

5. Brücken

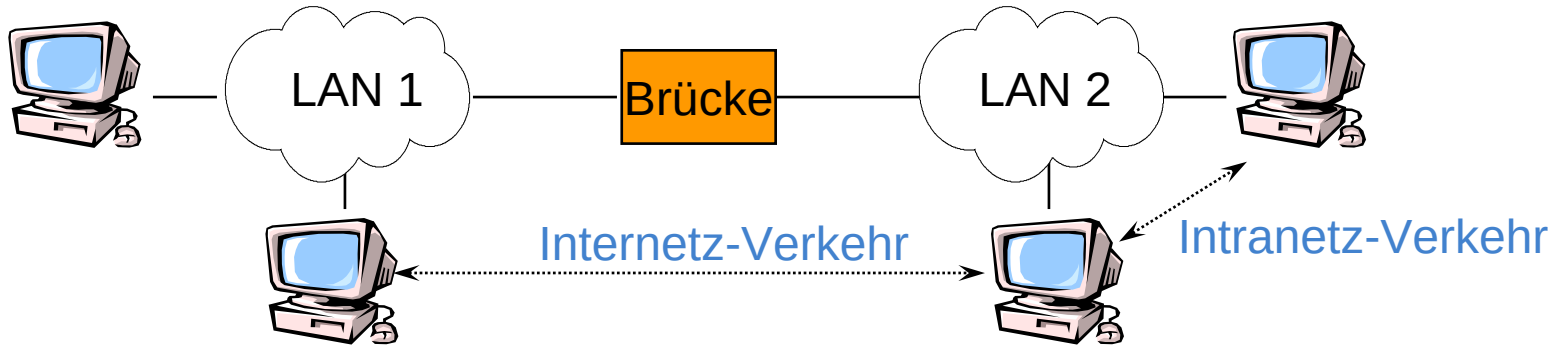
Prof. Dr. Martina Zitterbart
Dipl.-Inform. Thomas Gamer
Dipl.-Inform. Martin Röhricht
[zit | gamer | roehricht]@tm.uka.de

5. Brücken

Brücken

[Kesh97]

- Ziel
  - Kopplung von lokalen Netzen (LANs) auf Schicht 2
    - homogen: Netze vom gleichen Typ (z.B. 802.x mit 802.x)
    - heterogen: Netze unterschiedlichen Typs (z.B. 802.x mit 802.y ($x \neq y$))
- Eigenschaften
  - Filterfunktion
    - Trennen des Intranetz-Verkehrs in einem LAN von dem Internetz-Verkehr zu anderen LANs
  - Separierung des Verkehrs
    - Erhöhung der Netzkapazität großer Netze
- Schema



5.1 Kopplung verschiedener LANs mit Brücken

- Zwei Techniken können eingesetzt werden
  - Konvertierung der Datenformate
    - Dateneinheit wird in das Datenformat des „nächsten“ Teilnetzes konvertiert
    - LANs unterstützen verschiedene maximale Längen ihrer Dateneinheiten (z.B. 1500 Bytes im Ethernet, 4500 Bytes in FDDI)
      - Segmentieren wird notwendig. Wer reassembliert?
    - Die Köpfe der Dateneinheiten haben in verschiedenen LANs unterschiedliche Felder (z.B. Prioritätsfelder im Token Ring sind in Ethernet nicht vorhanden)
  - Einkapselung von Dateneinheiten
    - Empfangene Dateneinheit wird in das Datenfeld einer Dateneinheit für das „nächste“ Netz eingefügt
      - Informationsverluste können so vermieden werden. Aber Segmentierung …?
    - An beiden Enden des zu überbrückenden Netzes müssen gleiche Netze angeschlossen sein
    - Kommunikation mit Systemen, die direkt am zu überbrückenden Netz angeschlossen sind, ist nicht möglich

Überblick

- Source-Routing-Brücken
  - Endsystem fügt Information zur Wegewahl in die zu sendende Dateneinheit ein
    - Das sendende Endsystem fügt die Adressen aller Zwischensysteme in die zu sendende Dateneinheit ein
    - Brücken leiten die Dateneinheit anhand dieser Information weiter
    - Senden von Dateneinheiten ist nicht transparent für das Endsystem – es muss den Weg kennen
      - Senden von Explorer-Dateneinheit um mögliche Wege zu finden (vor dem Senden von Nutzdaten)
  - Wenig Aufgaben innerhalb der Brücke, daher einfache Realisierbarkeit
  - In der Praxis wenig eingesetzt
- Transparente Brücken
  - Weit verbreiteter Brückentyp in heutigen lokalen Netzen
  - Weiterleitungsentscheidung wird von der Brücke eigenständig getroffen
  - Brücke verwaltet in der Regel eine Tabelle (die Filterdatenbasis), in der sie Information über die Lokation von Endsystemen sammelt
    - Diese Information kann statisch angegeben oder dynamisch gelernt werden
  - Das Vorhandensein einer Brücke zum Zielsystem bleibt dem sendenden Endsystem verborgen
    - Endsystem ist nicht in die Wegewahl involviert – sendet Dateneinheiten wie bei „direkter Verbindung“

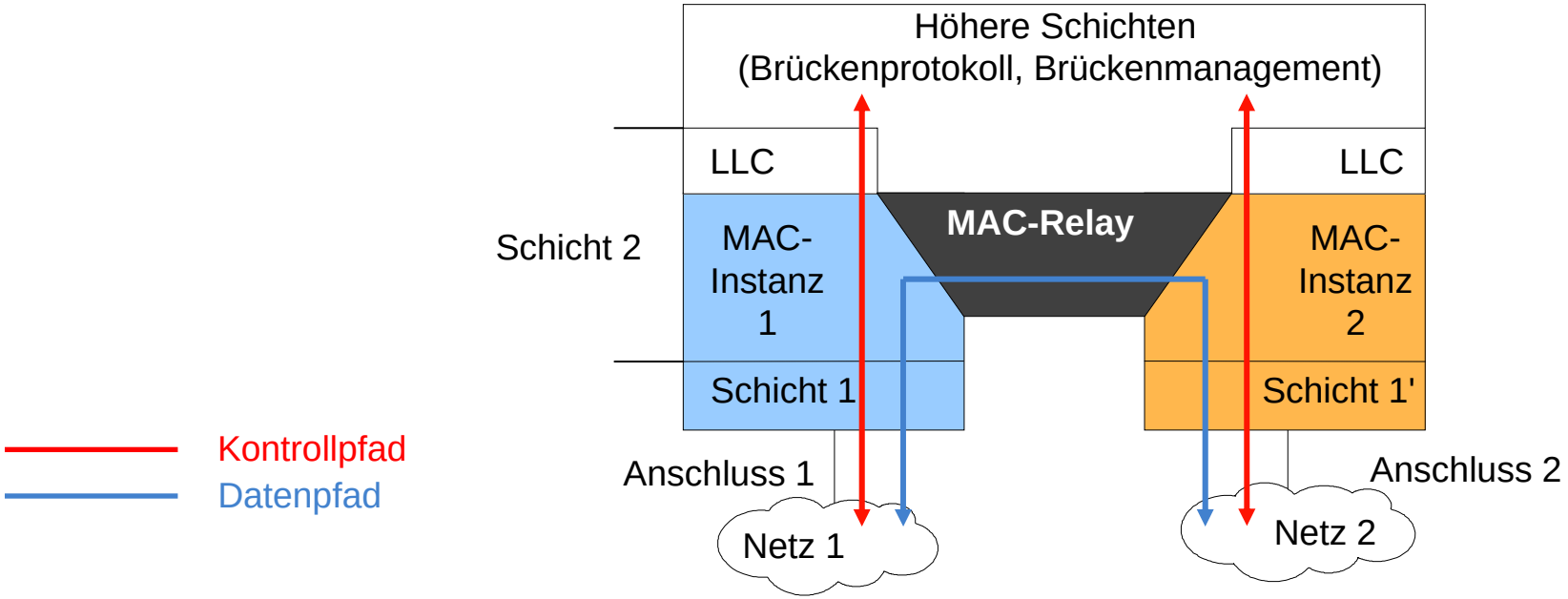
[Cisc06]

Zusammenfassung: Transparente Brücken vs. Source-Routing-Brücken

Eigenschaft	Transparente Brücken	Source-Routing-Brücken
Transparenz	✓	–
Verzögerung	gering	ggf. hoch
Routing	nicht optimal	optimal
Alternative Wege	–	✓
Kapazitätsausnutzung	schlecht	gut
Skalierbarkeit	schlecht	gut
Reihenfolgeerhaltung	✓	–

5.2 Transparente Brücken

- Wesentliche Merkmale
  - Für jeden Netzanschluss existieren eigene Schicht-1- und MAC-Instanzen
  - MAC-Relay implementiert die Weiterleitungs- und Filterfunktionen auf Schicht 2
  - LLC-Instanzen sind nur in den Kontrollpfad involviert (z.B. Brückenprotokoll, Brückenmanagement), nicht aber in den Datenpfad
- Teilweise auch als MAC-Layer-Brücke oder als Spanning-Tree-Brücke bezeichnet
  - Heute werden vor allem Schicht 2-Switches statt Brücken eingesetzt
- Aufbau einer transparenten Brücke:

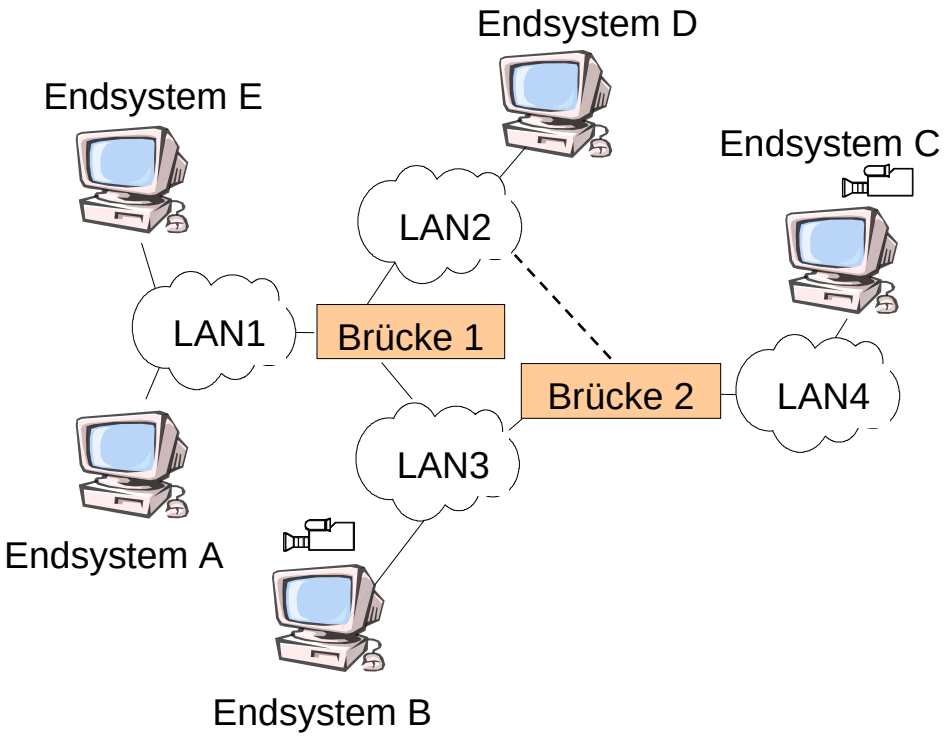


Aufgaben im Überblick

- Weiterleiten von Dateneinheiten
  - Lernen der Position von Endsystemen
    - Aufbau der Filterdatenbasis
  - Filtern bzw. Weiterleiten von Dateneinheiten
    - Auswertung der Information in der Filterdatenbasis, um Dateneinheiten gezielt weiterzuleiten
- „Kontrolle“ der Netztopologie
  - Etablierung einer schleifenfreien Topologie
    - Dateneinheiten dürfen nicht endlos im Netz kreisen
- ... Details auf den folgenden Folien

5.2.1 Lernen der Position von Endsystemen

- Annahme: Brücke neu gestartet
  - Noch keine Weiterleitungsinformation vorhanden
  - Keine statisch konfigurierte Weiterleitungsinformation
- Vorgehensweise am Beispiel
  - Brücke 1 empfängt Dateneinheit die von Endsystem A an Endsystem C gesendet wird
  - Brücke 1 lernt damit, dass Endsystem A über das entsprechende Interface (Port) erreichbar ist. Dies kann bei zukünftigen Dateneinheiten in Richtung Endsystem A genutzt werden
  - Kennt Brücke 1 Endsystem C, so leitet sie die Dateneinheit entweder über LAN2 oder LAN3 in Richtung Brücke 2 weiter
    - Brücke 1 hat vorher gelernt, an welchen Ausgangsport sie die Daten senden muss
  - Ist das Ziel-Endsystem nicht bekannt, so wird die empfangene Dateneinheit an alle angeschlossenen Ports außer dem Eingangsport geflutet



Filterdatenbasis

- Filterdatenbasis enthält erforderliche Information für das zielgerichtete Weiterleiten der Dateneinheiten
  - Zieladresse, Ausgangsport und Zeitgeber
  - Statische und dynamische Einträge
    - Statische Einträge werden vom Systemadministrator erstellt
    - Dynamische Einträge werden während des Betriebs gelernt bzw. verlernt
      - Lernen durch „durchlaufende“ Dateneinheiten
      - Verlernen durch Zeitgeber (soft-state)
- Filtern
  - Dateneinheiten, die lokale Ziele haben, werden nicht über die Brücke weitergeleitet (z.B. Daten von Endsystem A an Endsystem E)

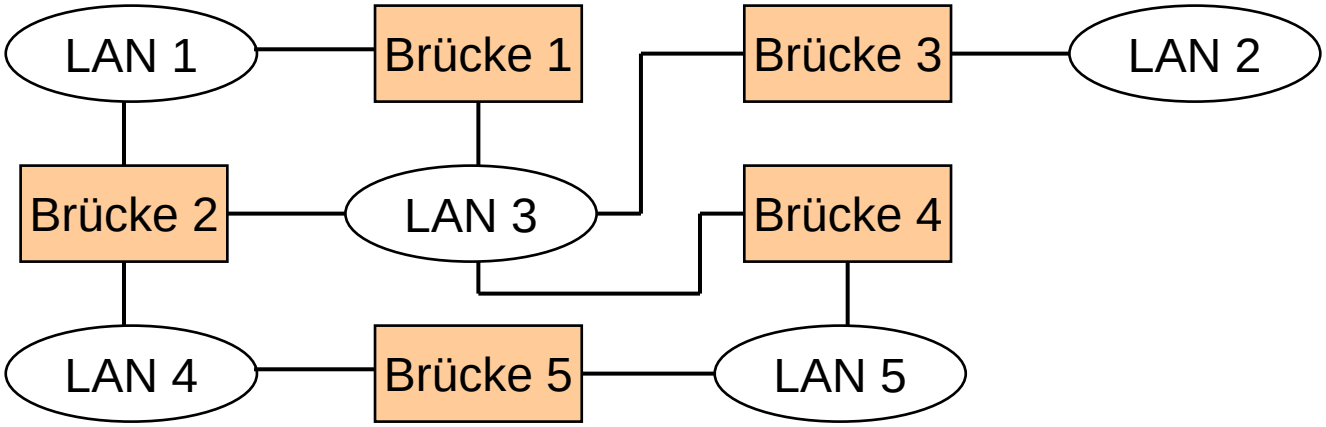
  → Separierung des Verkehrs ermöglicht eine höhere Skalierbarkeit
- Netztopologie
  - Eine Rekonfiguration hat Auswirkungen auf die Filterdatenbasis
    - Einträge müssen verlernt werden, da sie potenziell veraltet sind
    - Neue Einträge müssen erzeugt werden

5.2.2 Vermeiden von Schleifen

- Prinzipiell können Schleifen zwischen den im Netz konfigurierten Brücken entstehen (z.B. falls gestrichelte Verbindung im Beispielnetz vorhanden ist) Dies muss vermieden werden. Warum?
- Vermeidung von Schleifen durch Spanning-Tree-Algorithmus
  - Zwischen den Brücken wird eine Baumtopologie aufgebaut. Die Brücken bilden die Knoten des Baums, die lokalen Netze die Kanten.
  - Dateneinheiten können lediglich entlang des Baums weitergeleitet werden, womit keine Schleifen möglich sind
    - Aber: Ressourcen gegebenenfalls nicht optimal genutzt. Evtl. sind nicht alle physikalisch vorhandenen Brücken Bestandteil des Baums.
- Spanning-Tree-Algorithmus ist Bestandteil des Brückenprotokolls, das oberhalb der LLC-Schicht bearbeitet wird
  - Das Brückenprotokoll gehört zum Kontrollpfad, nicht zum Datenpfad
    - Stellt Informationen für die Weiterleitung von Dateneinheiten zur Verfügung (vgl. Routing)
    - Eigentliche Weiterleitung von Dateneinheiten operiert „unabhängig“ vom Brückenprotokoll
  - Austausch von Information zwischen den Brücken erfolgt durch Versenden sogenannter BPDUs (Bridge Protocol Data Units)

Beispielnetz und Anforderungen

- Beispielnetz



- Anforderungen, um eine schleifenfreie Topologie anhand des Spanning-Tree-Algorithmus aufbauen zu können
  - Gruppenadresse zur Adressierung aller im Netz konfigurierten Brücken muss definiert sein (MAC-Adresse!)
  - Eindeutige Brücken-Kennungen pro Brücke innerhalb des Netzes erforderlich
  - Eindeutige Anschluss-Kennungen pro Anschluss in jeder Brücke notwendig
  - Pfadkosten an allen Anschlüssen einer Brücke müssen bekannt sein

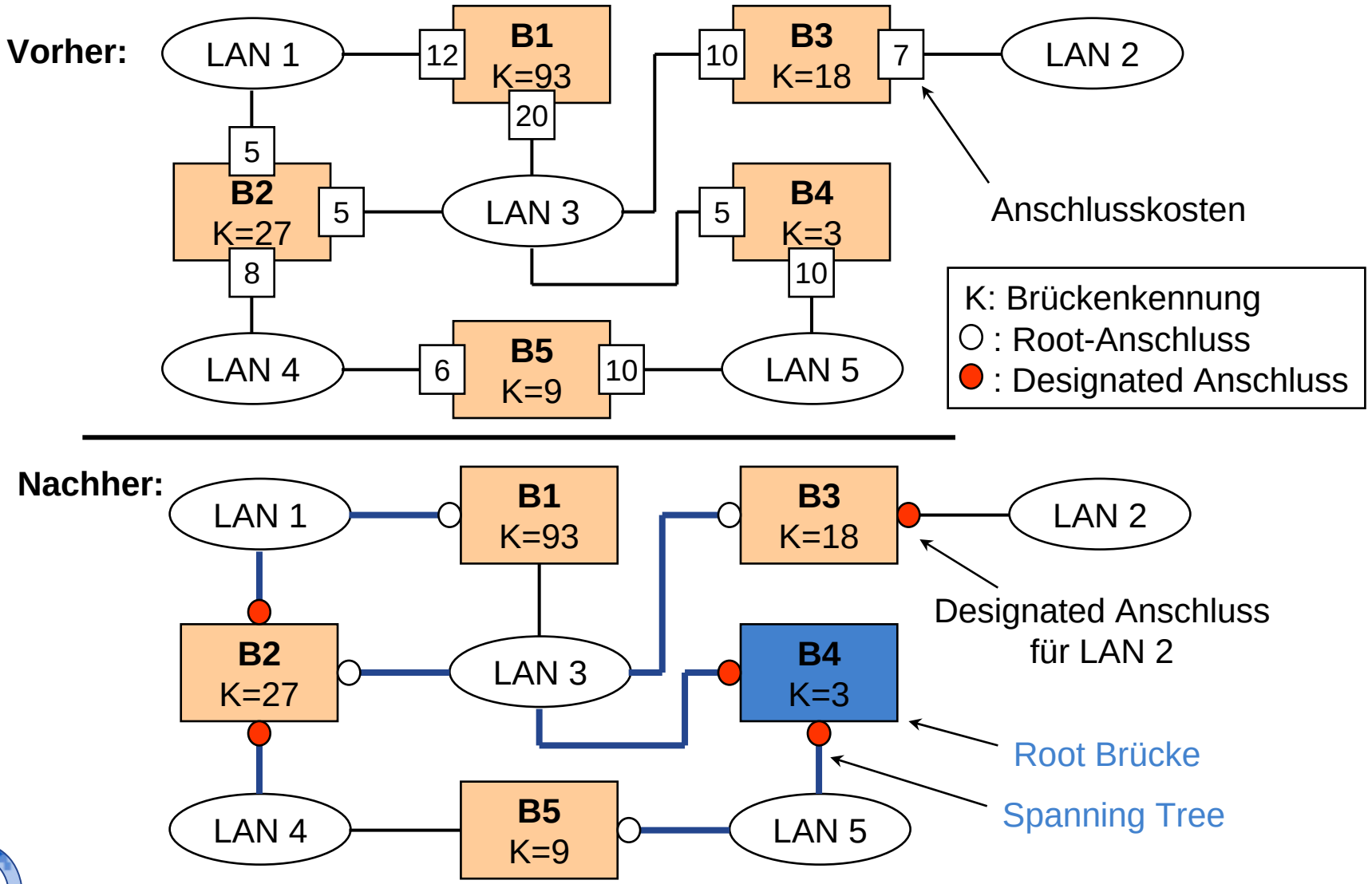
Spanning-Tree-Algorithmus – Ablauf

- Bestimmen der Root-Brücke als Wurzel des Baums
  - Brücke mit kleinstem Wert der Brücken-Kennung im Netz wird Root-Brücke
    - Brücken-Kennung: Prioritätsfeld und Teil der MAC-Adresse des Anschlusses
    - Systemadministrator kann Konfiguration über Prioritätsfeld beeinflussen
  - Bei der Initialisierung geht jede Brücke zunächst davon aus, dass sie Root-Brücke ist
    - Austausch der Brücken-Kennungen über regelmäßig gesendete Configuration-BPDUs
  - Sobald kleinere Brücken-Kennung empfangen wird als eigene Kennung, nicht mehr Root-Brücke

Spanning-Tree-Algorithmus – Ablauf

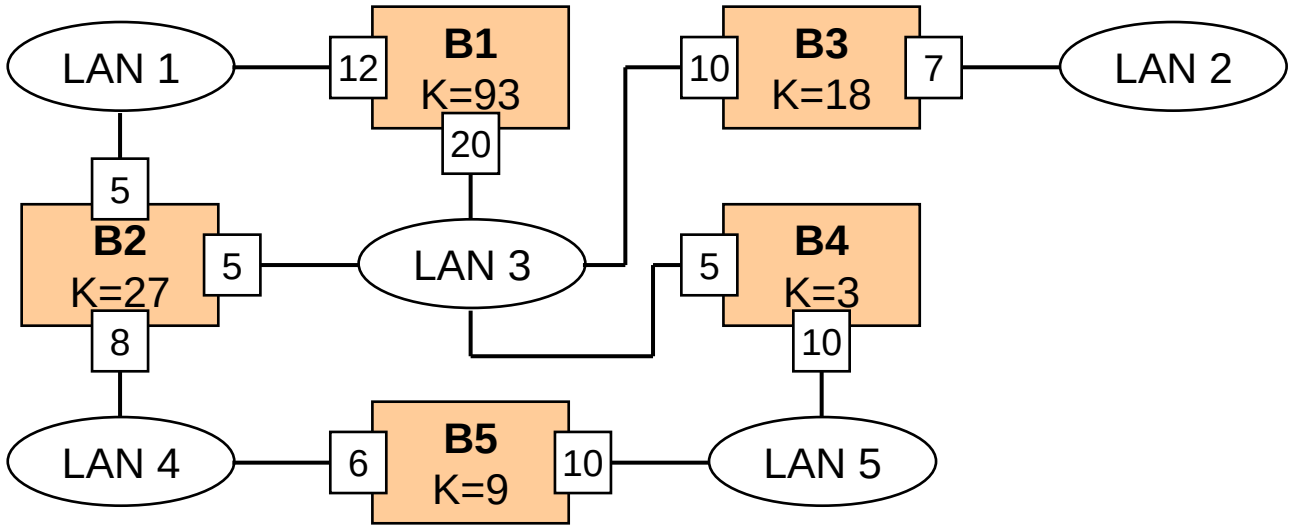
- Bestimmen der Root-Anschlüsse
  - Ist Brücke nicht Root-Brücke, so muss sie Anschluss (Port) in Richtung Root-Brücke bestimmen
    - Berechnung der Pfadkosten zur Root-Brücke
      - Summe über alle Anschlusskosten auf dem Weg zur Root-Brücke
      - Datenrate der angeschlossenen Übertragungsabschnitte kann als Kostenfunktion dienen
    - Auswahl des Anschlusses mit den geringsten Kosten
- Bestimmen der Designated-Brücke für jedes LAN (Schleifenfreiheit!)
  - Ein Netz kann mehrere Brücken mit Root-Anschlüssen besitzen. Es wird derjenige mit den geringsten Kosten als Designated-Anschluss des LANs gewählt. Die betroffene Brücke wird damit zur Designated-Brücke.
    - Auflösung gleicher Kosten über Brücken-Kennung

Spanning-Tree-Algorithmus: Beispiel



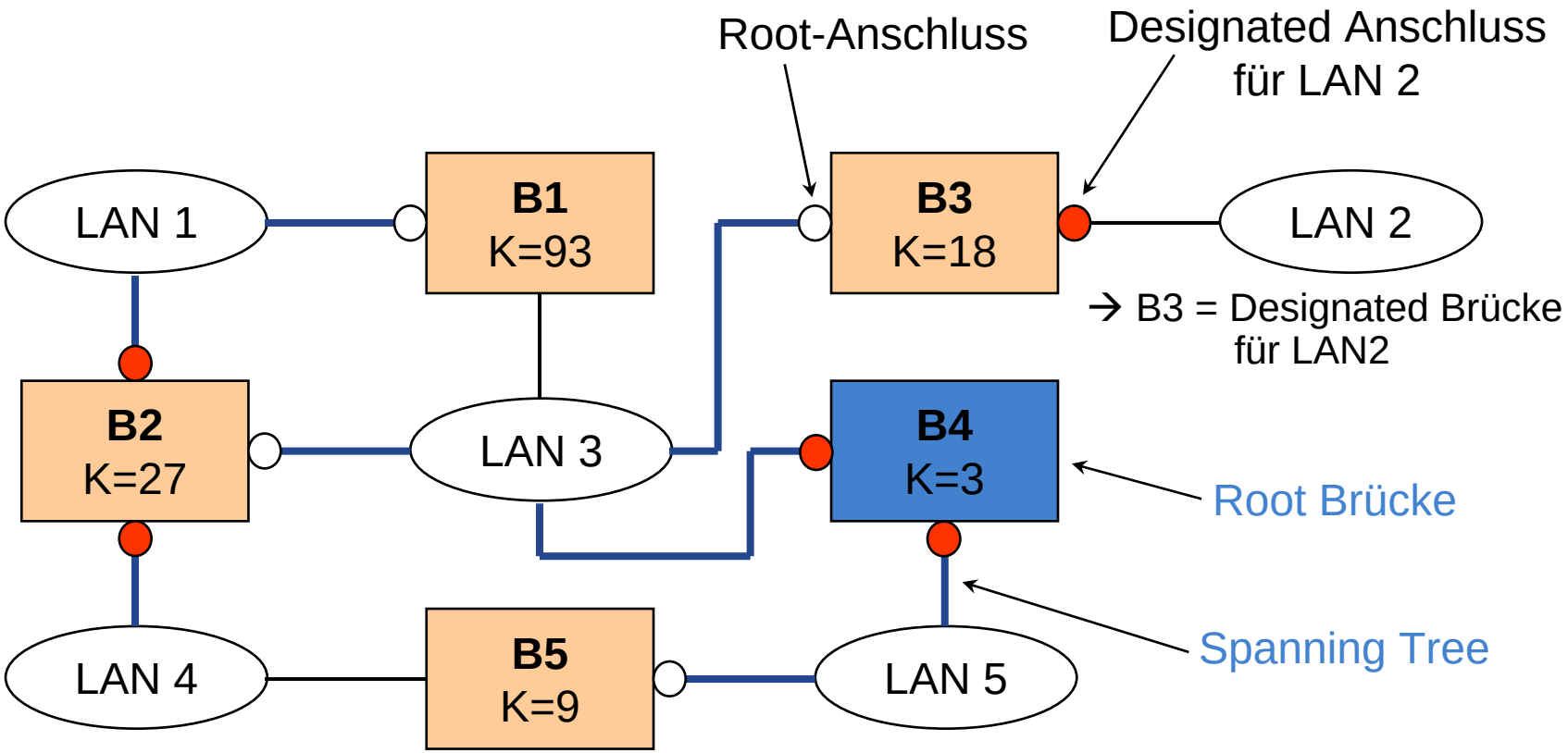
Berechnung Pfadkosten zur Wurzel

Vorher:

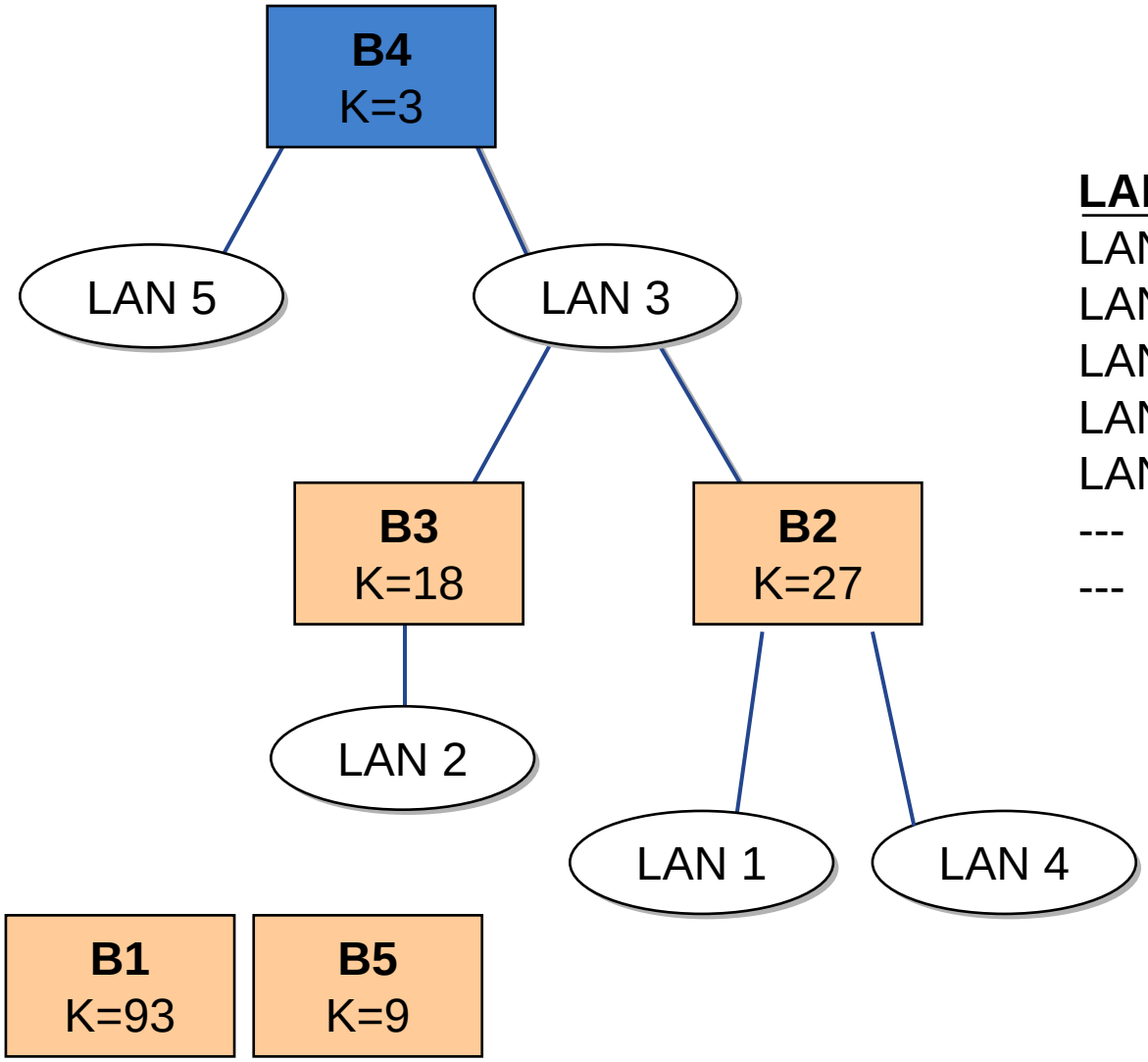


Brücke	Pfadkosten zur Wurzel (Root-Brücke)
B3	**10** (via LAN 3)
B1	20 (via LAN 3)
	17 = 12 + 5 (via LAN 1 & LAN 3)
B2	**5** (via LAN 3)
	18 = 8 + 10 (via LAN 4 & LAN 5)
	25 = 5 + 20 (via LAN 1 & LAN 3)
B5	**10** (via LAN 5)
	11 = 6 + 5 (via LAN 4 und LAN 3)

Bestimmung der Designated Brücken



Der resultierende Spanning Tree

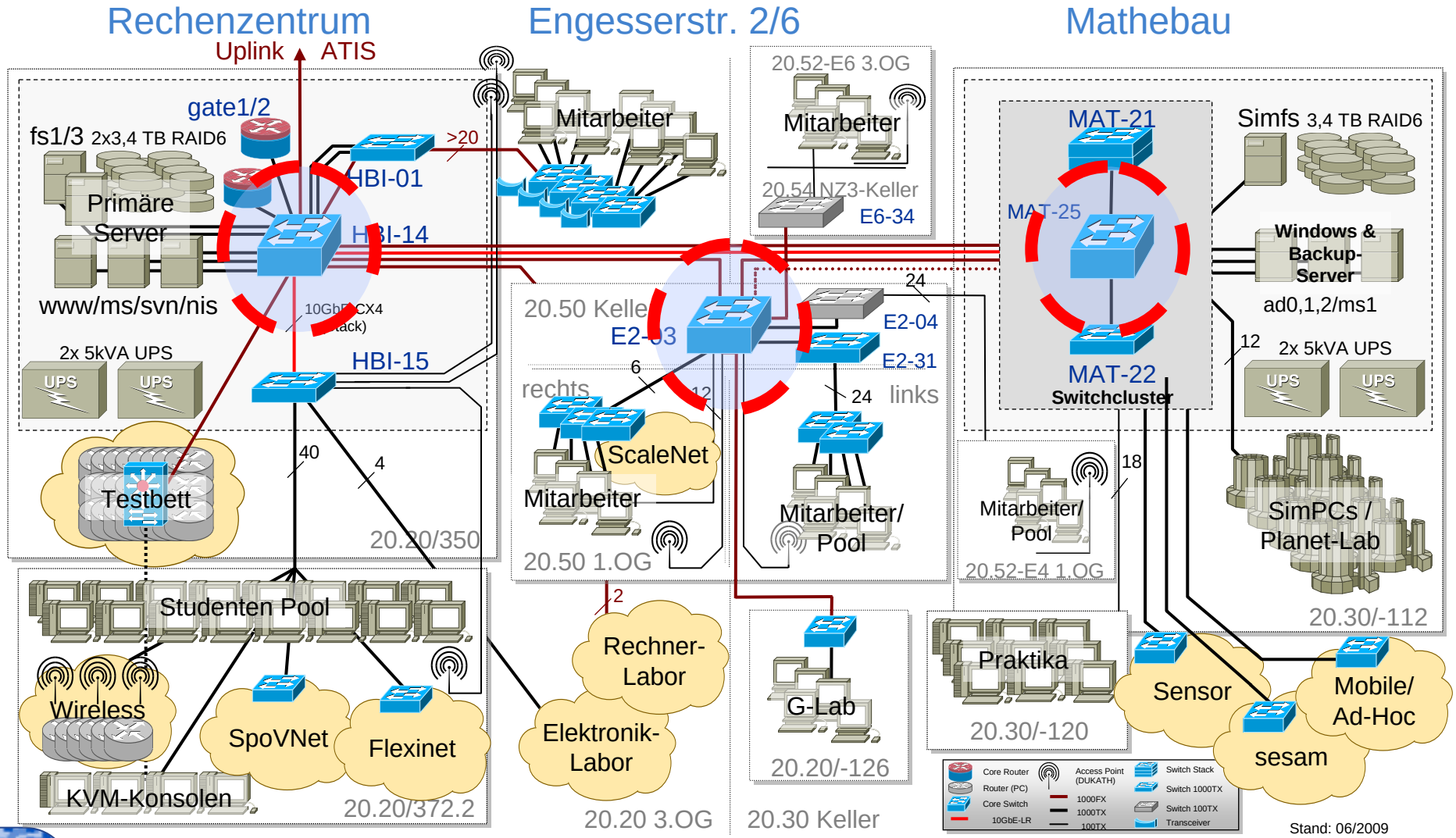


LAN	Designated Brücke
LAN 1	B2
LAN 4	B2
LAN 2	B3
LAN 3	B4 (Root Brücke)
LAN 5	B4 (Root Brücke)
---	B5
---	B1

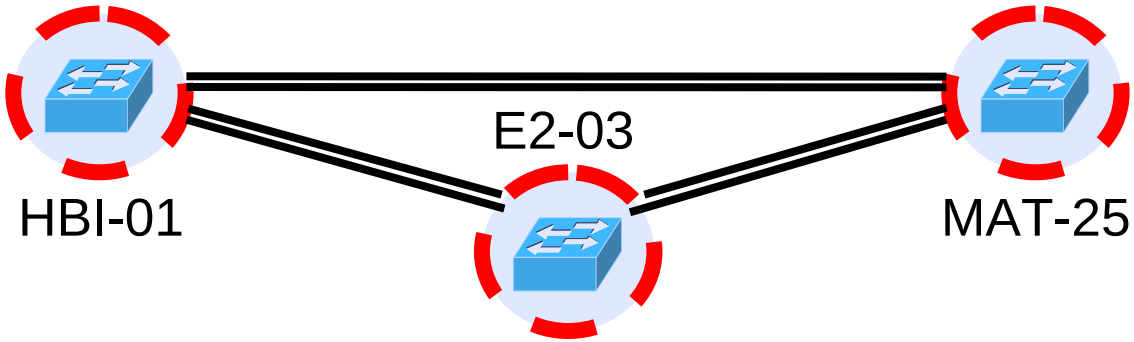
Einschub: Schicht 2-Switches

- Einsatz von Switches zur Kopplung von lokalen Netzen
  - Auch als „Multi-port Bridges“ bezeichnet
    - Arbeiten auf Schicht 2
    - Zeitgleiche Übertragung von Dateneinheiten zwischen verschiedenen Port-Paaren möglich
  - Jeder Port des Switches ist vergleichbar mit einem eigenen Netzsegment
    - Sternförmige Topologie
      - Jedes angeschlossene System erhält die volle Kapazität
    - Ermöglicht heterogene Links
      - z.B. 10Base-T an Port 1 und 100Base-FX an Port 2
  - Vollduplex-Betrieb der Punkt-zu-Punkt-Verbindung
    - Keine Kollisionen mehr möglich
  - Flusskontrolle findet im Switch statt
    - Senderate kann durch PAUSE-Dateneinheiten gedrosselt werden
  - Weitere Optimierungen, z.B. für effizientes IP-Multicast möglich
  - Ermöglicht den Aufbau von V-LANs, z.B. durch Aggregation mehrerer Ports

5.3 Switches – Einsatz am ITM



Switches am ITM



- Konfiguration
  - Jeder Switch ist redundant an seine Nachbar-Switches angebunden
- Switches arbeiten als transparente Brücken
  - Alle Switches sind in einer Spanning Tree-Domäne angesiedelt, d.h. es existiert genau eine Root-Brücke
  - Es existiert nur ein aktiver Datenpfad, d.h. redundante Anbindung wird nur im Fehlerfall verwendet!
  - Pro Sekunde wird eine Hello-Dateneinheit von einer Brücke versendet. Wenn 10 Sekunden keine Hello-Dateneinheit empfangen wurde, wird der Spanning-Tree-Algorithmus aktiv (Dauer ca. 5 Sekunden)

  ➔ Nach 15 Sekunden besteht wieder Konnektivität
- Anmerkung
  - Bei dieser Topologie könnte auch einfach auf den redundanten Link umgeschaltet werden

5.4 V-LANs

- Was ist ein V-LAN?
  - V-LAN = Virtuelles LAN
  - Auf Ethernet-Ebene wird der Datenverkehr logisch getrennt

  ➔ Virtuelle Leitung
- Wieso werden V-LANs eingesetzt?

[Cisc06a]

  - Sicherheit
    - Broadcast-Medium kann jedes angeschlossene System mithören
    - Trennung eines physikalischen Mediums in logische Medien ermöglicht gezielte Gruppierung von Systemen
    - Bessere Kontrolle über Größe und Zusammensetzung eines Netzes
  - Flexibilität
    - Einfache Reorganisation der logischen Medien möglich
      - Keine Änderung an physikalischem Medium, z.B. neue Verkabelung, notwendig
  - Performance
    - Broadcast-Last eines Netzes sinkt, wenn ein physikalisches Medium in mehrere logische Medien aufgeteilt wird

Konfiguration von V-LANs

- Ohne V-LAN Technik

  Ethernetkabel 1
  Ethernetkabel 2
  Ethernetkabel 3

- Mit V-LAN Technik

  Virtuelles Ethernetkabel 1
  Virtuelles Ethernetkabel 2
  Virtuelles Ethernetkabel 3

- Unterscheidung von V-LANs
  - Jedes V-LAN erhält eine eindeutige Kennung (ID)
  - Tagging von Ethernet-Frames mit der ID des angesprochenen V-LANs
  - Switches entfernen Tagging vor Auslieferung an Endsystem
  - Es existieren unterschiedliche Protokolle zur Unterstützung von V-LANs
    - IEEE 802.1q [IEEE03]
    - Cisco Inter-Switch Link (ISL)

V-LAN-Dateneinheit

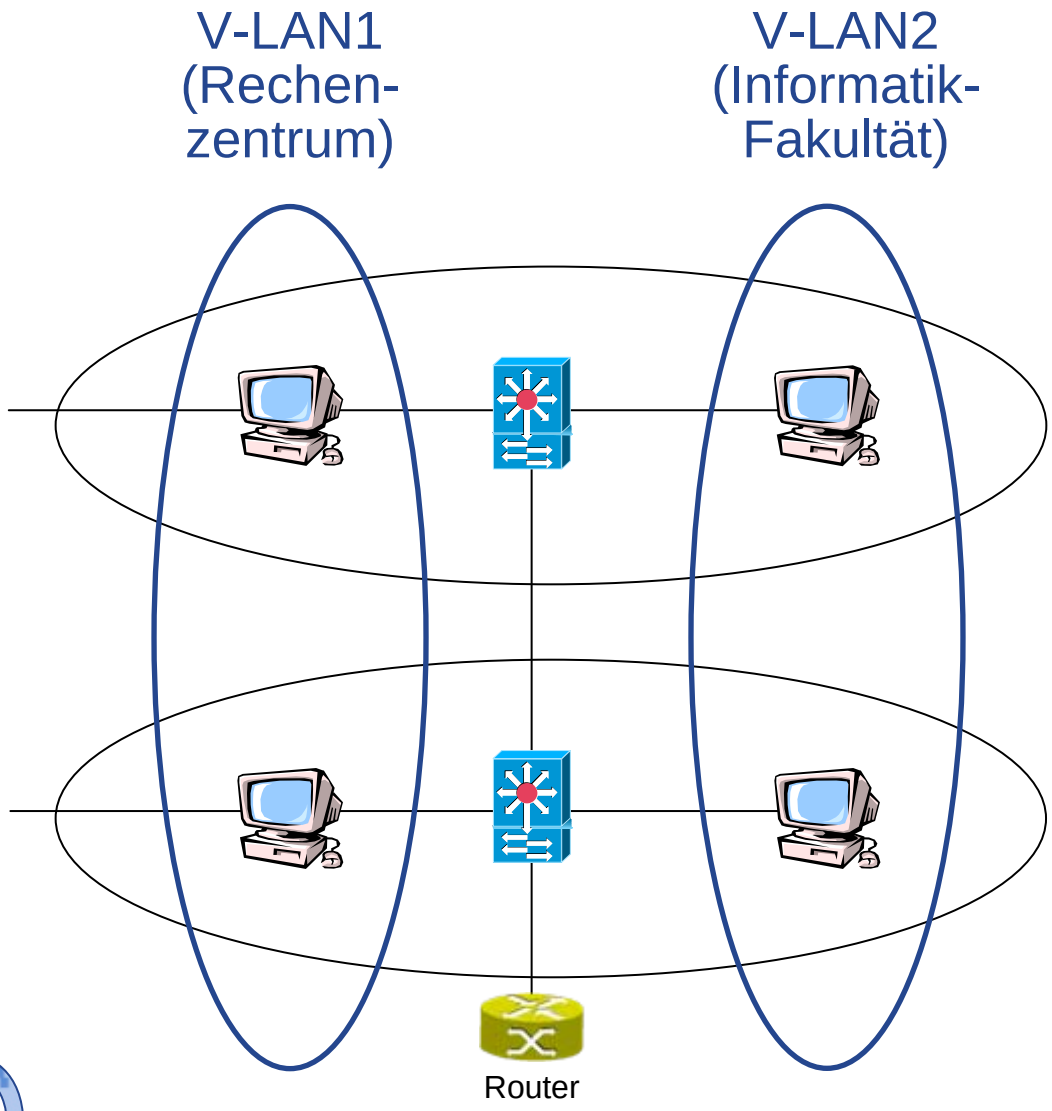
Ethernet-Dateneinheit

```
▷ Frame 52 (90 bytes on wire, 90 bytes captured)
▽ Ethernet II, Src: 00:07:e9:23:e7:07, Dst: 00:0c:6e:40:8d:0e
    Destination: 00:0c:6e:40:8d:0e (141.3.70.246)
    Source: 00:07:e9:23:e7:07 (141.3.71.126)
    Type: 802.1Q Virtual LAN (0x8100)
▽ 802.1q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0110 0110 = ID: 102
    Type: IPv6 (0x86dd)
▽ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: TCP (0x06)
    Hop limit: 63
    Source address: 2001:638:204:6:207:e9ff:fe17:3a1d (2001:638:204:6:207:e9ff:fe17:3a1d)
    Destination address: 2001:638:204:5:20c:6eff:fe40:8d0e (2001:638:204:5:20c:6eff:fe40:8d0e)
▷ Transmission Control Protocol, Src Port: 34183 (34183), Dst Port: ssh (22), Seq: 80, Ack: 208, Len: 0
```

V-LAN-ID

CFI – Canonical Format Identifier (bei Ethernet 0)

Konfiguration von V-LANs



LAN1 (Geb 20.20, 3. Stock)

LAN2 (Geb 20.20, 2. Stock)

Konfiguration unter Linux

- Laden des V-LAN Moduls:

```
modprobe 8021q
```

- Hinzufügen eines neuen V-LANs:

```
vconfig add lo 811
```

- Zuweisen der IP-Parameter:

```
ifconfig lo.811  10.11.1.1 netmask 255.255.0.0 broadcast 10.11.255.255
```

- Ergebnis: (`ifconfig lo.811`):

```
lo.811    Link encap:Local Loopback
          inet addr:10.11.1.1  Mask:255.255.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

5.5 Literatur

Bücher

[Kesh97] S. Keshav; An Engineering Approach to Computer Networking; Addison-Wesley, 1997

- Kapitel 11: Routing

[Stal06] W. Stallings; Data & Computer Communications; Pearson Prentice Hall, 8th Edition, 2006

- Kapitel 15

Vertiefende Literatur

[IEEE03] IEEE Standard 802.1Q: IEEE Standards for Local and metropolitan area networks – Virtual Bridged Local Area Networks; IEEE, 2003 Edition

Internet-Links

[Cisc06] Cisco; Source-Route Bridging; http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/srb.htm

[Cisc06a] Cisco; LAN-Switching; http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm

5.6 Aufgaben

1) Stellen Sie kurz Source-Routing Brücken und transparente Brücken gegenüber.
2) Woher kennen Source-Routing Brücken den Weg einer Dateneinheit?
3) Wie werden Schleifen bei transparenten Brücken verhindert?
4) Welche Unterschiede bestehen zwischen statischen und dynamischen Einträgen in der Filterdatenbasis transparenter Brücken?
5) Nutzen transparente Brücken die vorhandenen Ressourcen optimal aus?
6) Welche Schritte muss eine Brücke durchführen, um ein Token Ring-Netz mit einem Ethernet-LAN zu verbinden? Wo bestehen Einschränkungen?
8) Was ist ein V-LAN?
9) Erläutern Sie die Vorteile von V-LANs.