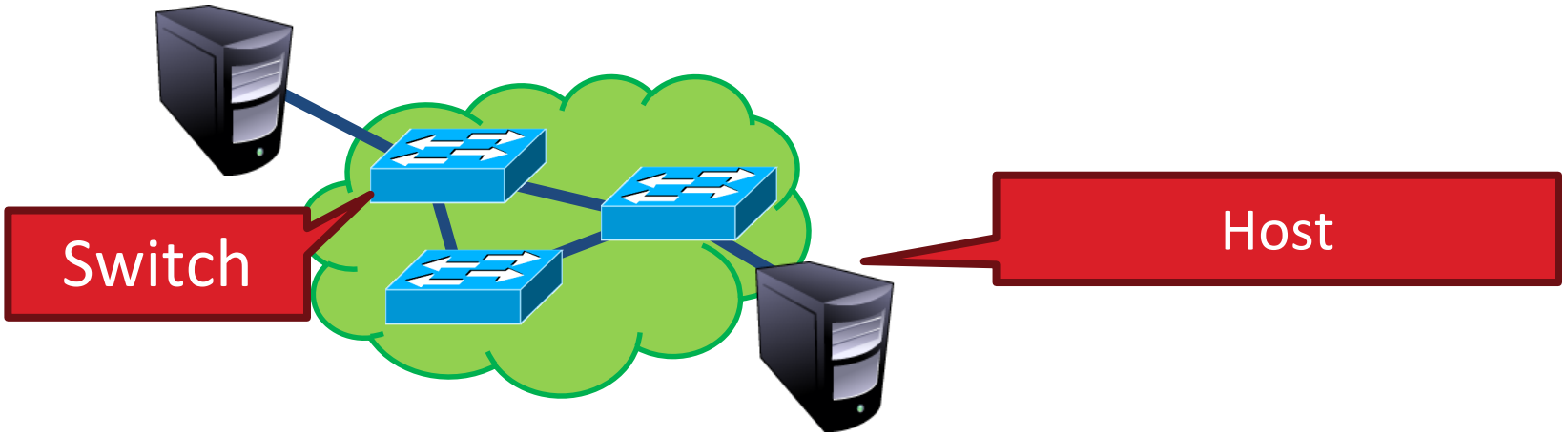
Kapitel 5: Verkehrslenkung im Internet

Verkehrslenkung im LAN

- Netzknoten werden in einem LAN über die MAC Adresse identifiziert
  - Der MAC (Medium Access Control) Layer ist ein Sublayer von Schicht 2
    - spezifiziert vor allem die Koordination von Übertragungen auf einem gemeinsam genutzten Übertragungsmedium
    - dazu zählen auch die Adressen
  - Netzknoten werden auch als Stationen bezeichnet
- MAC Adressen sind nicht strukturiert
  - Verwendung der gleichen MAC Adresse in allen LANs
  - Keine Konfiguration einer MAC Adresse bei Zutritt zu einem LAN
  - Verkehrslenkung muss flache Adresshierarchie mit kontinuierlicher Veränderung der MAC Adressen im Netz unterstützen

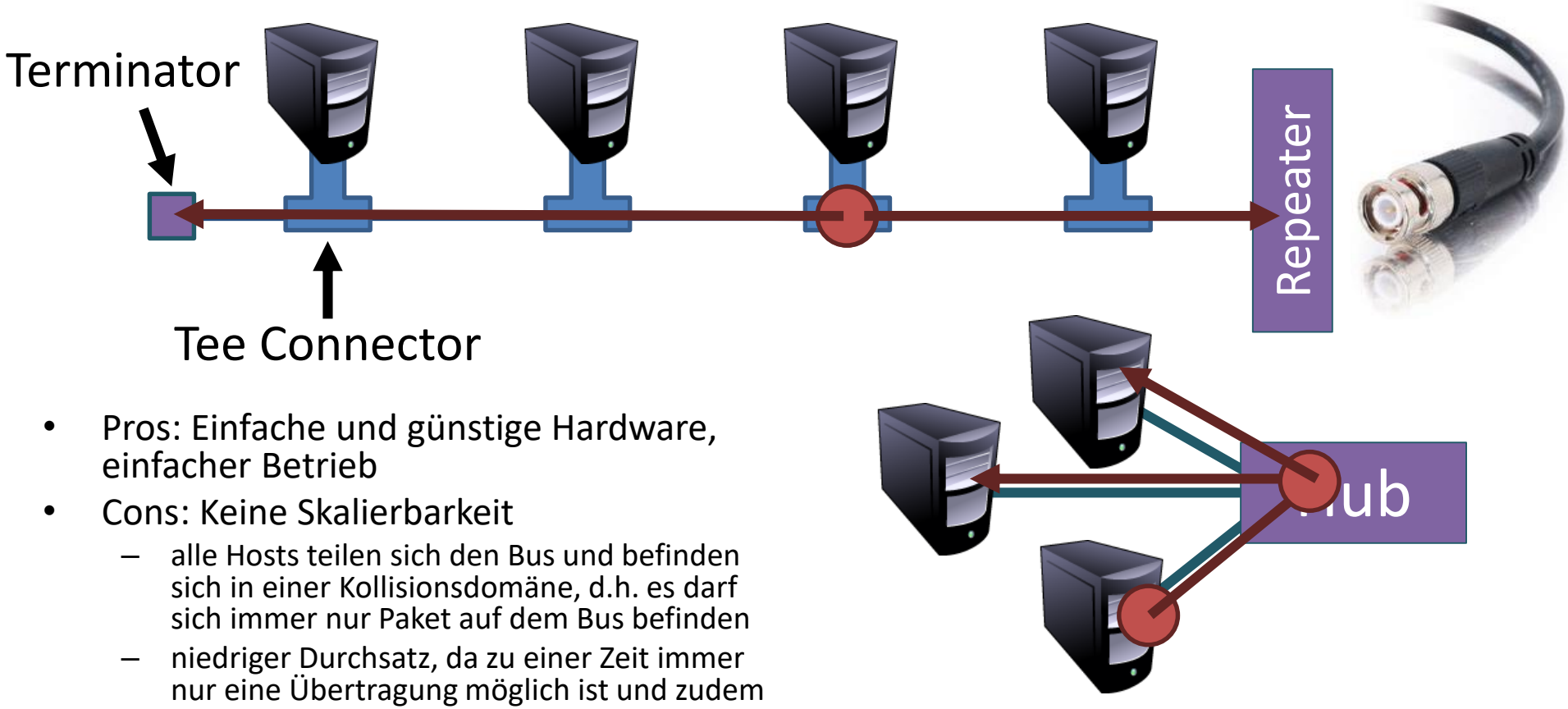
LAN (Local Area Network) - Netzknoten

- Hub: Einfacher Repeater
  - auf Schicht 1 (Physical Layer, Bitübertragungsschicht)
- Bridge: Verbindung von (heterogenen) LAN-Segmenten
  - auf Schicht 2 (Link/MAC Layer), Sicherungs-/Medienzugriffsschicht
- Switch: Spezielle Bridge mit nur einem Netzknoten pro Port
  - auf Schicht 2 (Link/MAC Layer), Sicherungs-/Medienzugriffsschicht



Ethernet Bus (eher historisch)

Ethernet wurde ursprünglich für einen Bus als geteiltes Medium entworfen, in dem alle Knoten alle Pakete hören. Mit einem Hub wurden mehrere Busse verbunden und Bits auf alle angeschlossenen Busse repliziert.

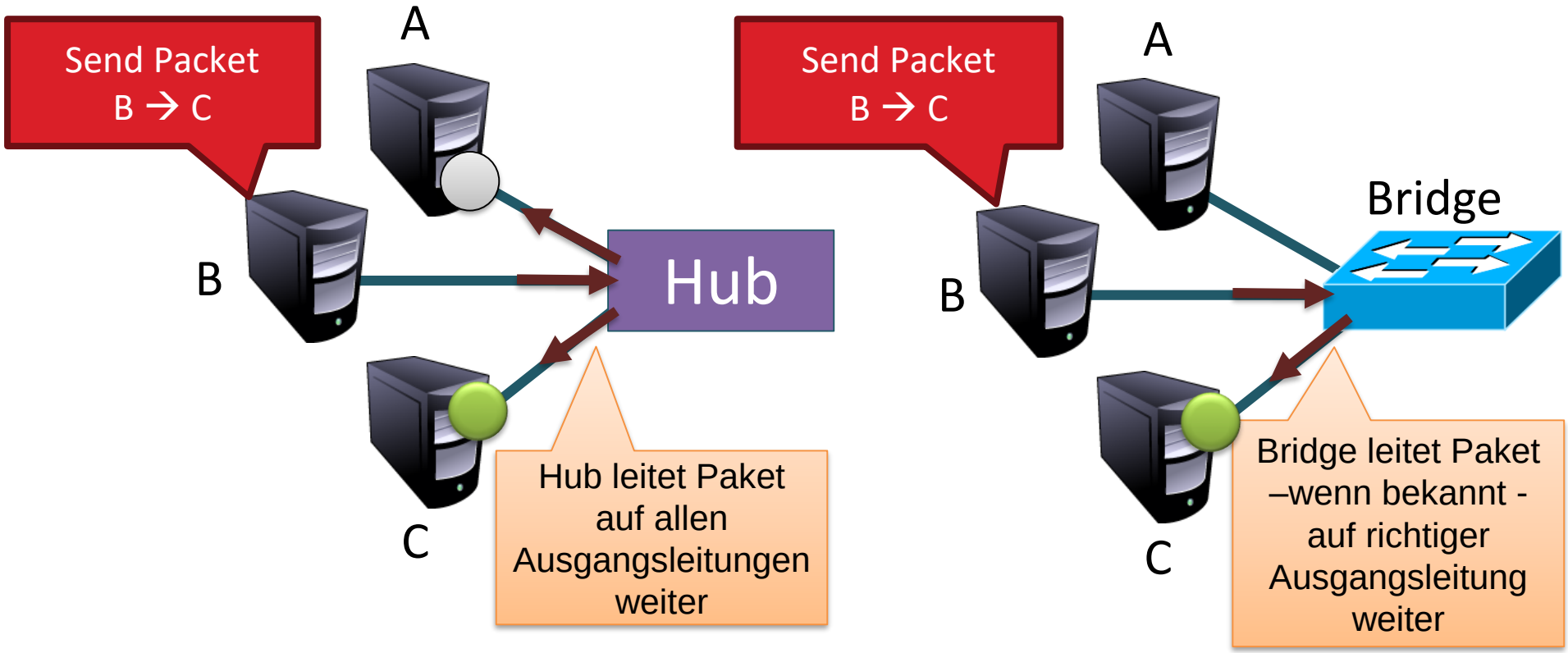


- Pros: Einfache und günstige Hardware, einfacher Betrieb
- Cons: Keine Skalierbarkeit
  - alle Hosts teilen sich den Bus und befinden sich in einer Kollisionsdomäne, d.h. es darf sich immer nur Paket auf dem Bus befinden
  - niedriger Durchsatz, da zu einer Zeit immer nur eine Übertragung möglich ist und zudem Kollisionen den Durchsatz weiter verringern

Hubs und Bridges

Hubs
- verbinden einzelne Stationen oder Busse
- durch Hubs verbundene Stationen gehören zum gleichen LAN Segment
- leiten Pakete auf allen Ausgangsleitungen weiter

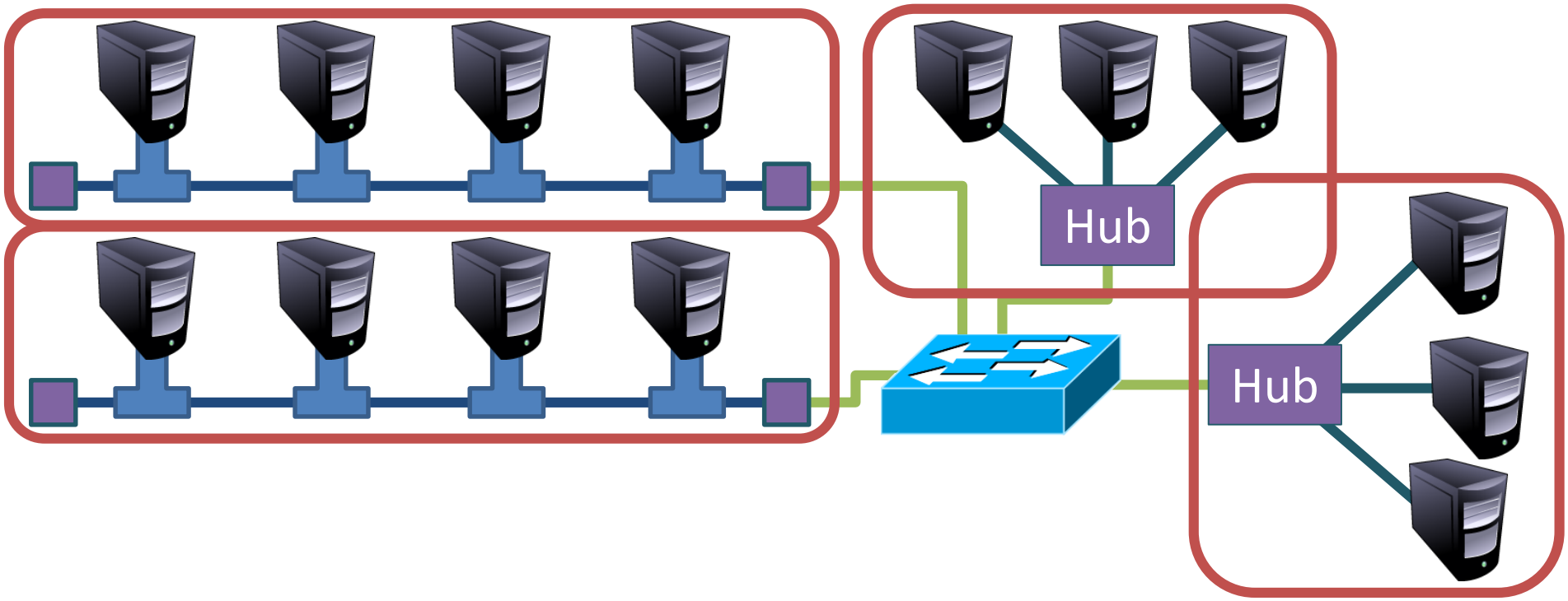
Bridges
- verbinden einzelne Stationen oder Busse
- durch Bridges verbundene Stationen gehören zu verschiedenen LAN Segmenten
- leitet Pakete nur auf der richtigen Ausgangsleitung weiter



Bridges zwischen LAN-Segmenten

Bridges verbinden LAN-Segmente um

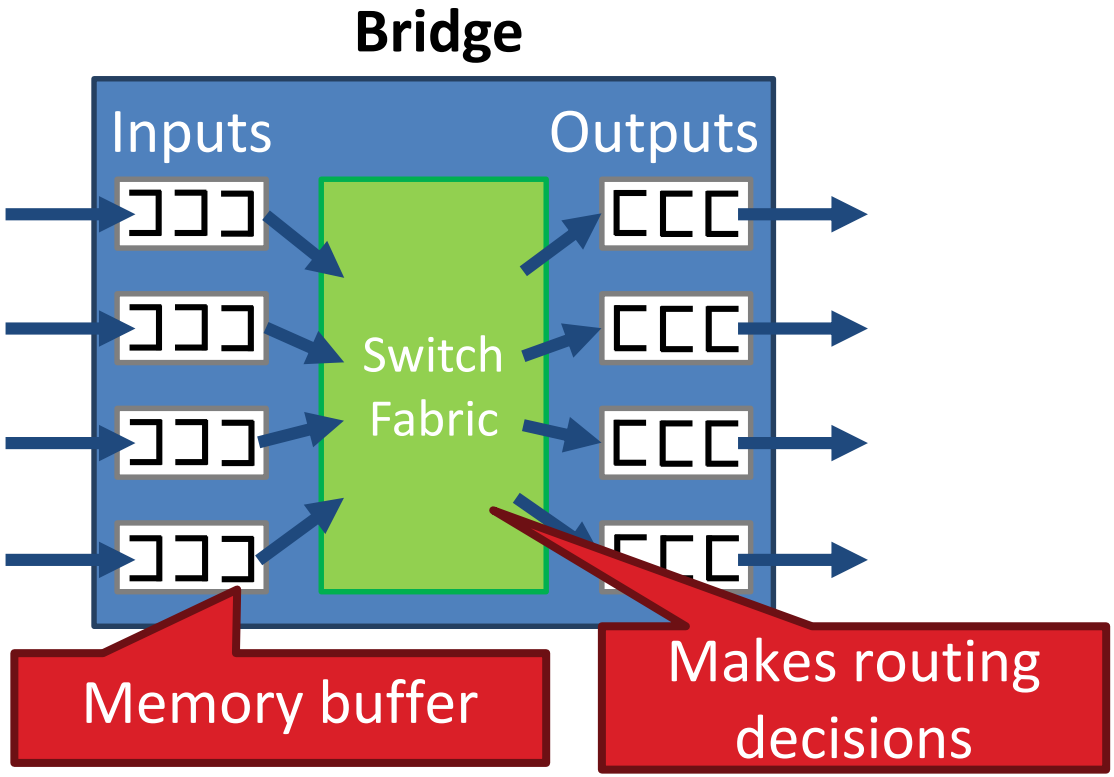
- Kollisionsdomänen (siehe Ethernet) aufzubrechen
  - gleichzeitige Übertragung in unterschiedlichen LAN-Segmenten möglich
  - Bridge speichert die Pakete und leitet sie in andere LAN-Segmente weiter
- LANs mit unterschiedlichen Technologien zu Verbinden
  - Access Point ist eine Bridge, die Ethernet LAN und WLAN verbindet



Kapitel 5: Verkehrslenkung im Internet

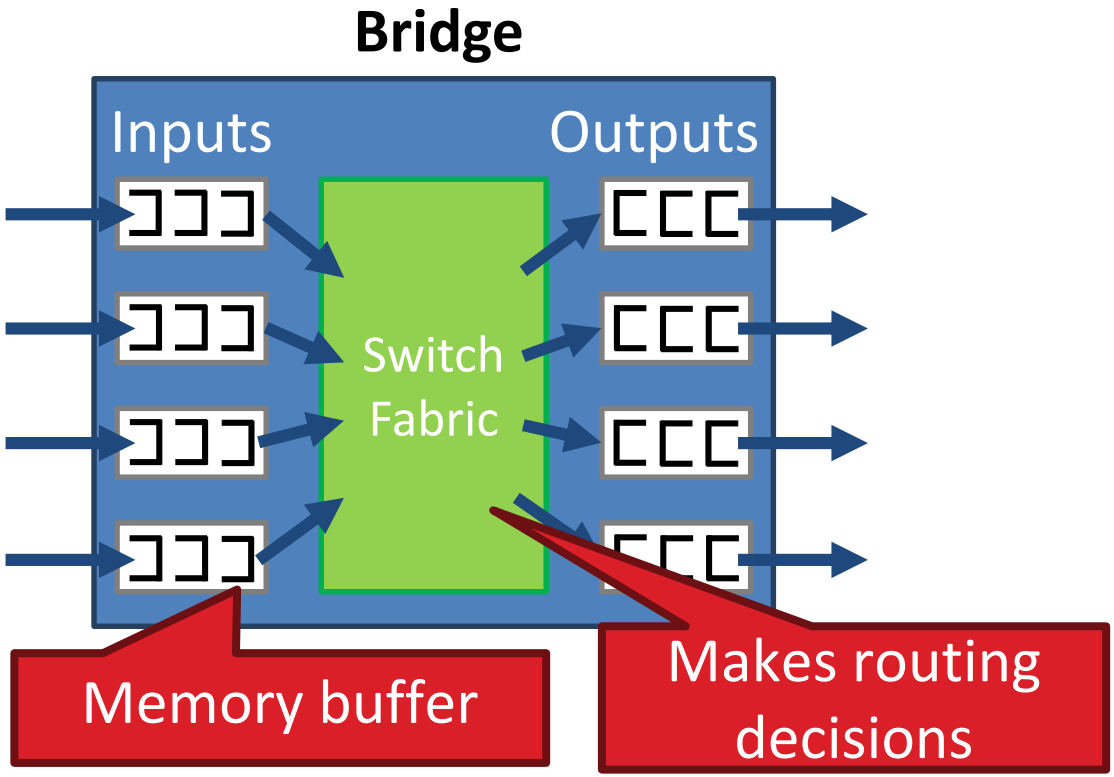
Aufbau einer Bridge

- Die Ein-/Ausgangsleitungen einer Bridge werden als Ports bezeichnet
- Eine Bridge speichert Pakete in Puffern am Eingangs- und Ausgangsport.
- Die Switching Fabric leitet Pakete aufgrund der Ziel-MAC-Adresse vom Eingangspuffer in den richtigen Ausgangspuffer



Aufgaben der Bridge

- Frames weiterleiten
- Ausgangsports von MAC Adressen lernen
- Spanning Tree Algorithm
- … und mittlerweile noch vieles mehr



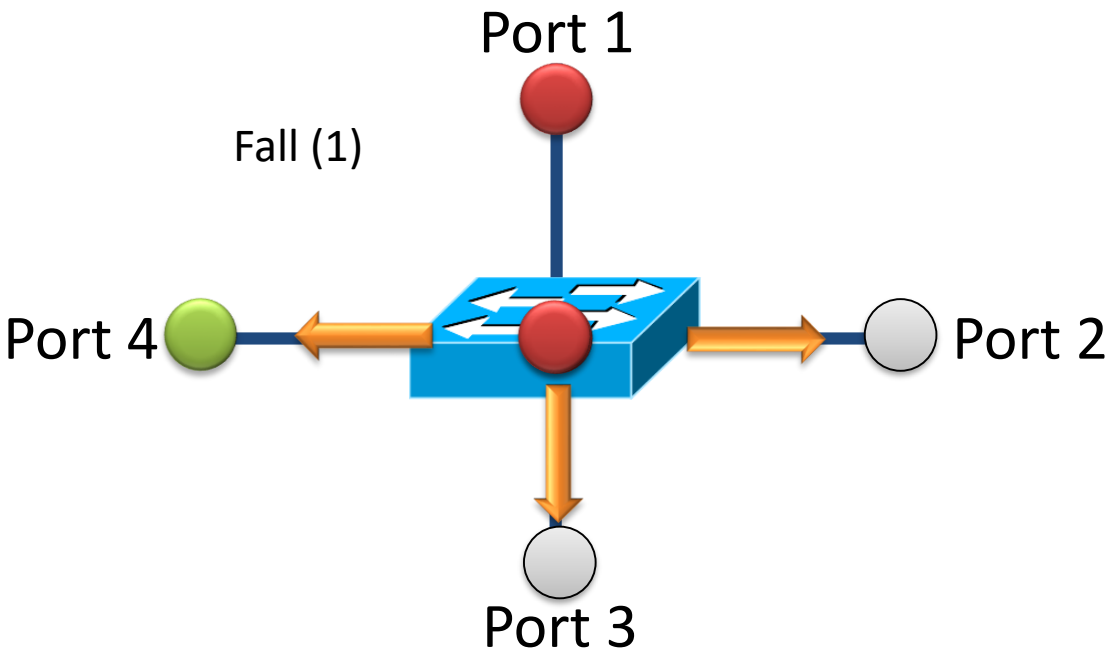
Frames weiterleiten - Frame Forwarding Table

- Die Frame Forwarding Table enthält für jede bekannte MAC-Adresse den Ausgangsport
- alle Einträge haben eine Gültigkeitsdauer
- Bridges **lernen** die Ports der MAC-Adressen und müssen nicht konfiguriert werden.

MAC Address	Port	Age
00:00:00:00:00:AA	1	1 minute
00:00:00:00:00:BB	2	7 minutes
00:00:00:00:00:CC	3	2 seconds
00:00:00:00:00:DD	1	3 minutes

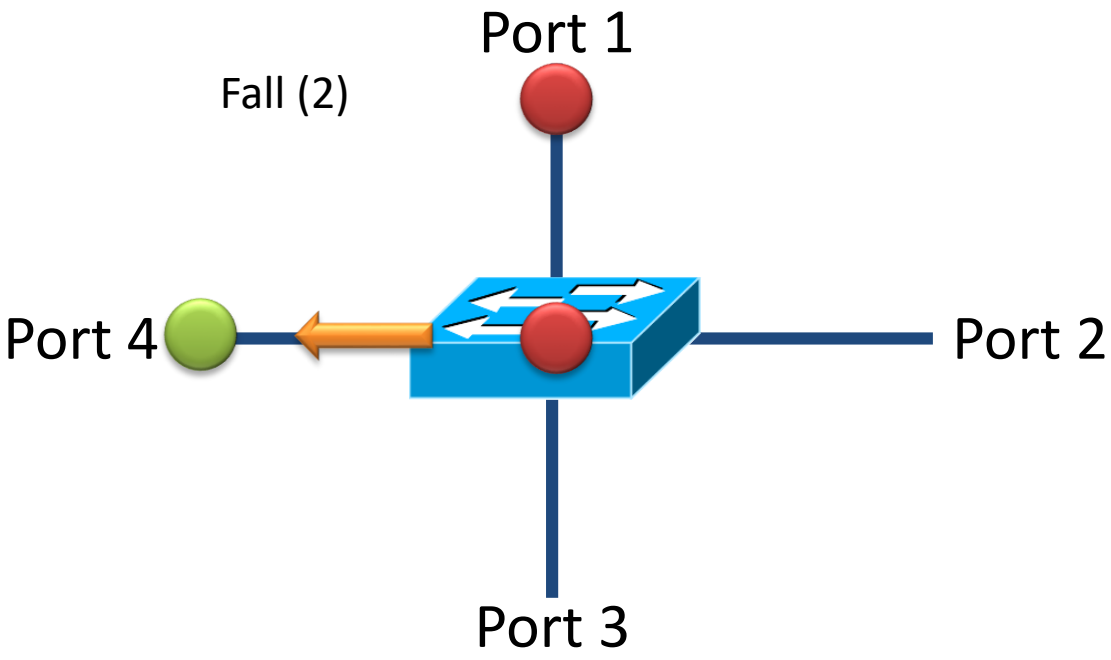
Bridges in Action

- Forwarding von Frames
  - (1) Port der Ziel-MAC-Adresse unbekannt:
    - Frame wird auf alle Ports geschickt (broadcast) außer dem Ursprungsport



Bridges in Action

- Forwarding von Frame
  - (1) Port der Ziel-MAC-Adresse unbekannt:
    - Frame wird auf alle Ports geschickt (broadcast) außer dem Ursprungsport
  - (2) Port der Ziel-MAC-Adresse bekannt:
    - Frame wird auf diesen Port geschickt

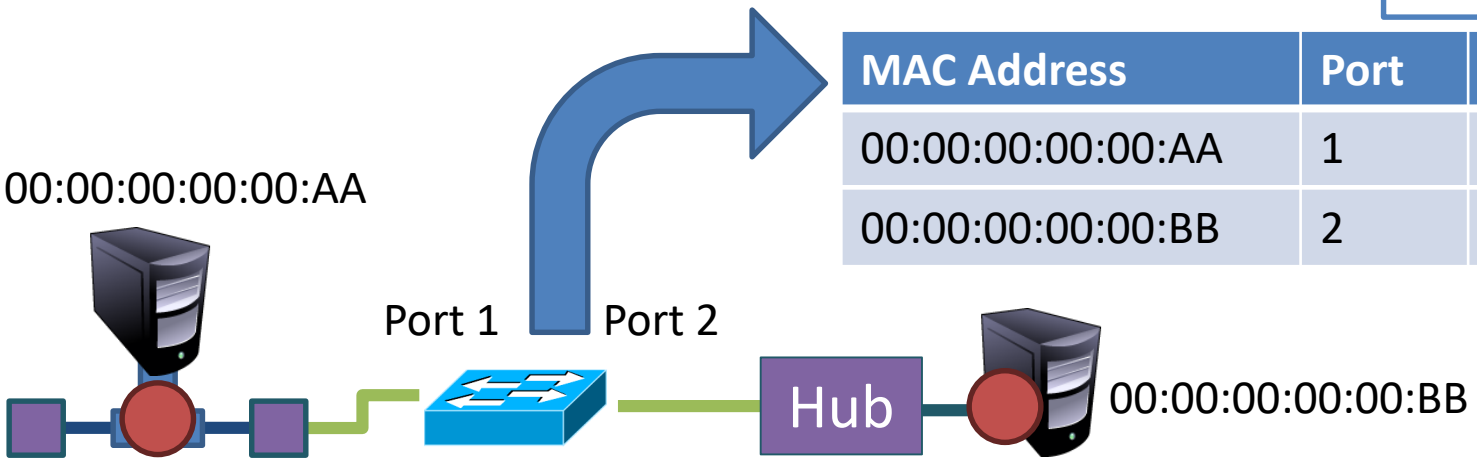


Adressen lernen

- Einfaches Prinzip
  - in jedem Frame befindet sich die Source-MAC-Address
  - Bridge merkt sich für jeden MAC-Frame
    - Ankunftsport
    - Source-MAC-Address
    - Zeit
  - Existierende Einträge werden upgedatet oder nach einiger Zeit gelöscht
    - Rechner können im LAN wandern
    - Rechner können das LAN verlassen

Alte Einträge nach Timeout löschen

MAC Address	Port	Age
00:00:00:00:00:AA	1	0 minutes
00:00:00:00:00:BB	2	0 minutes

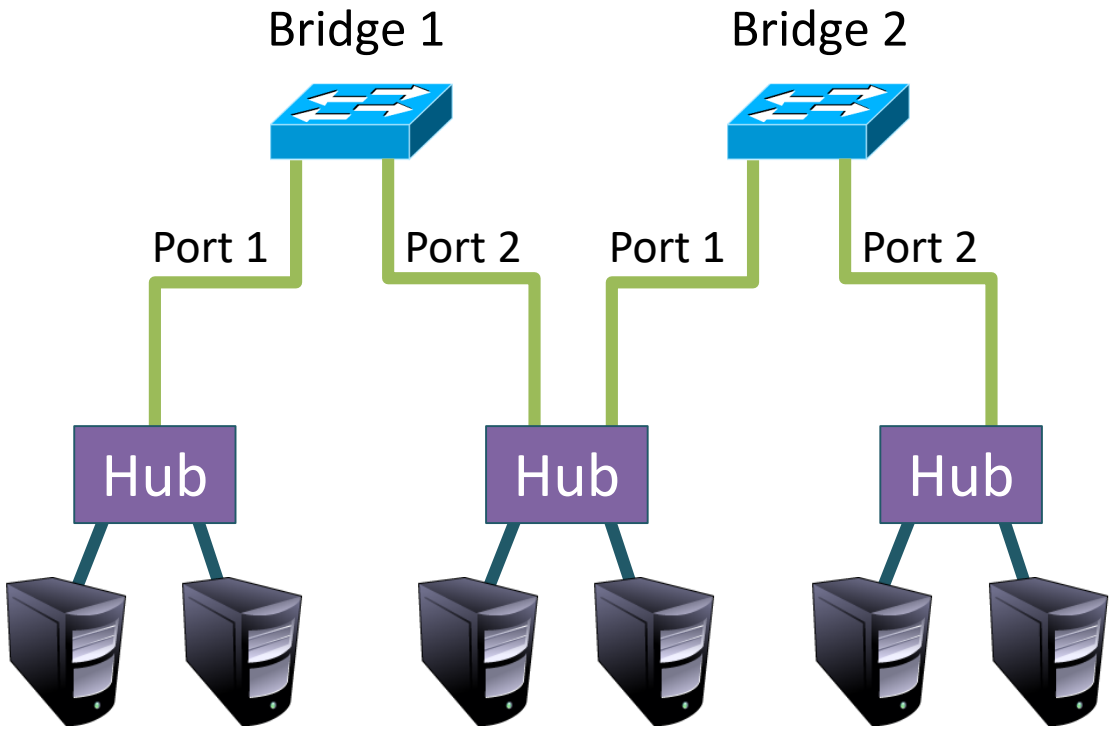


Komplexeres Beispiel

- Das Netz in diesem Beispiel besteht aus drei LAN Segmenten mit jeweils 2 Hosts, die über 2 Bridges miteinander verbunden sind.
  - Die MAC-Adressen der Hosts seien von links nach rechts AA-FF.
- Die Forwarding-Tabellen der Bridges sind zunächst leer.
- Drei Pakete werden von AA nach FF, von CC nach AA und von EE nach CC gesendet.

Paketsequenz:

1. **<Src=AA, Dest=FF>**
2. <Src=CC, Dest=AA>
3. <Src=EE, Dest=CC>



Komplexeres Beispiel

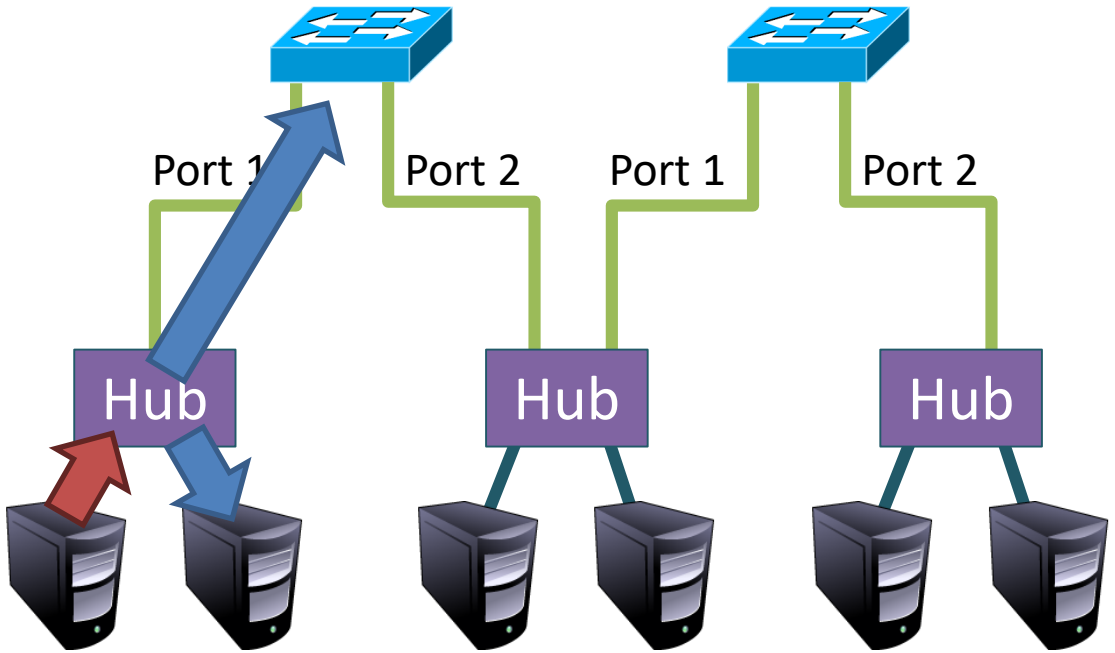
Paketsequenz:

1. **<Src=AA, Dest=FF>**

Bridge 1

AA	1

Bridge 2



Komplexeres Beispiel

Paketsequenz:

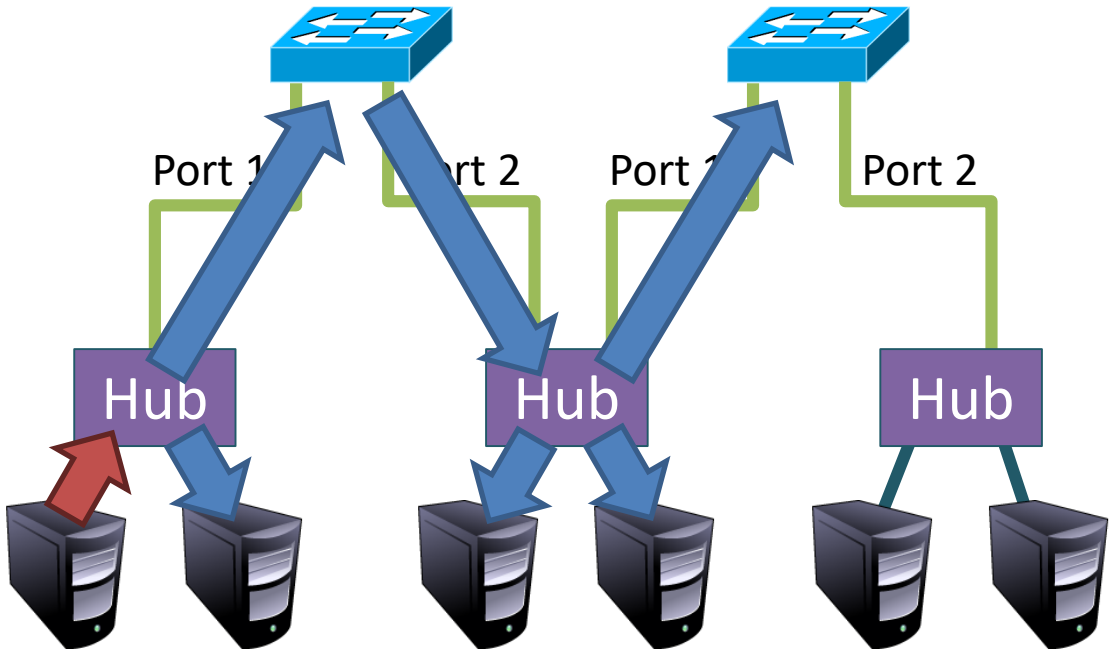
1. **<Src=AA, Dest=FF>**

Bridge 1

AA	1

Bridge 2

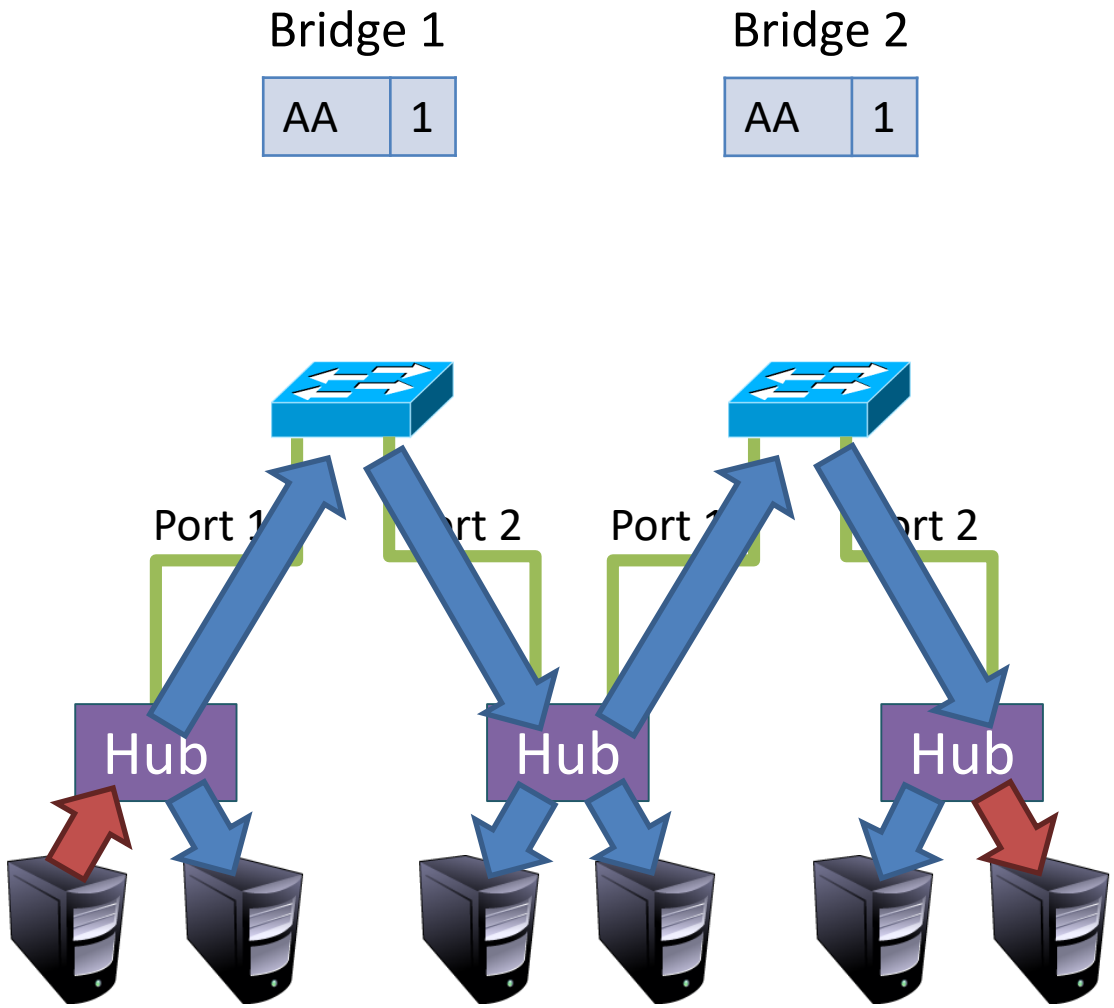
AA	1



Komplexeres Beispiel

Paketsequenz:

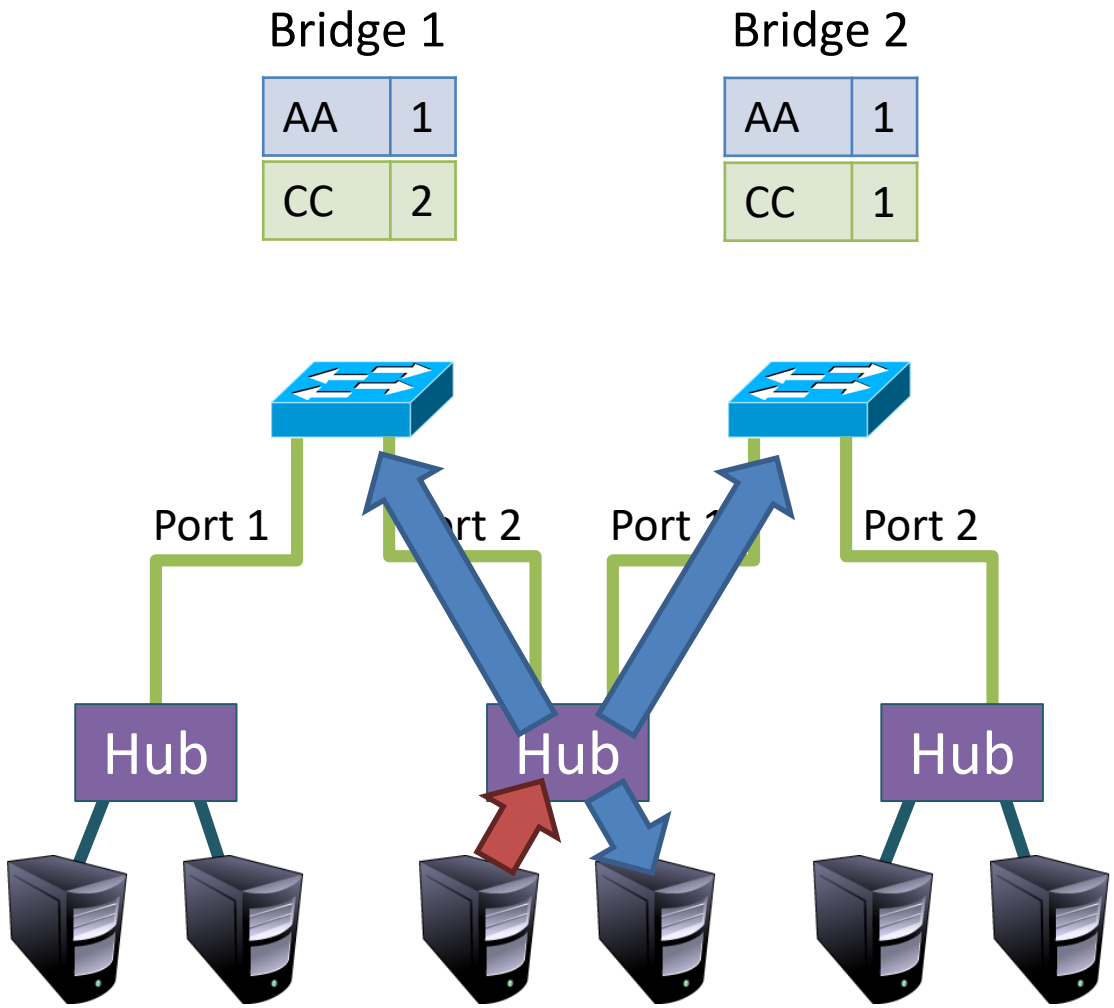
1. **<Src=AA, Dest=FF>**



Komplexeres Beispiel

Paketsequenz:

1. <Src=AA, Dest=FF>
2. **<Src=CC, Dest=AA>**



Komplexeres Beispiel

Paketsequenz:

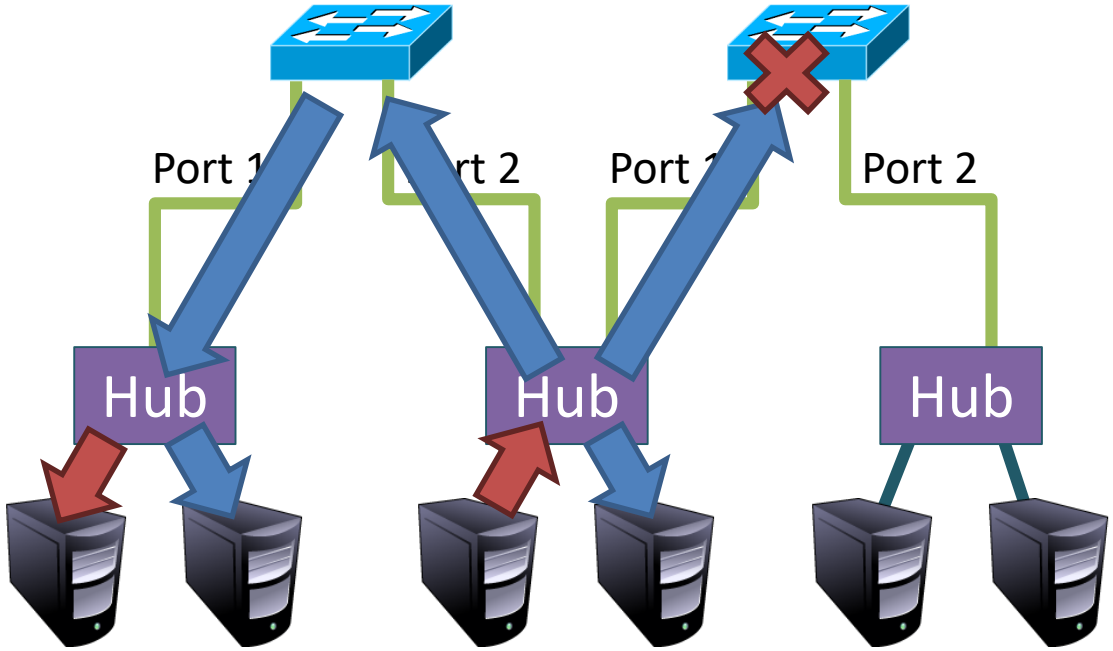
1. <Src=AA, Dest=FF>
2. **<Src=CC, Dest=AA>**

Bridge 1

AA	1
CC	2

Bridge 2

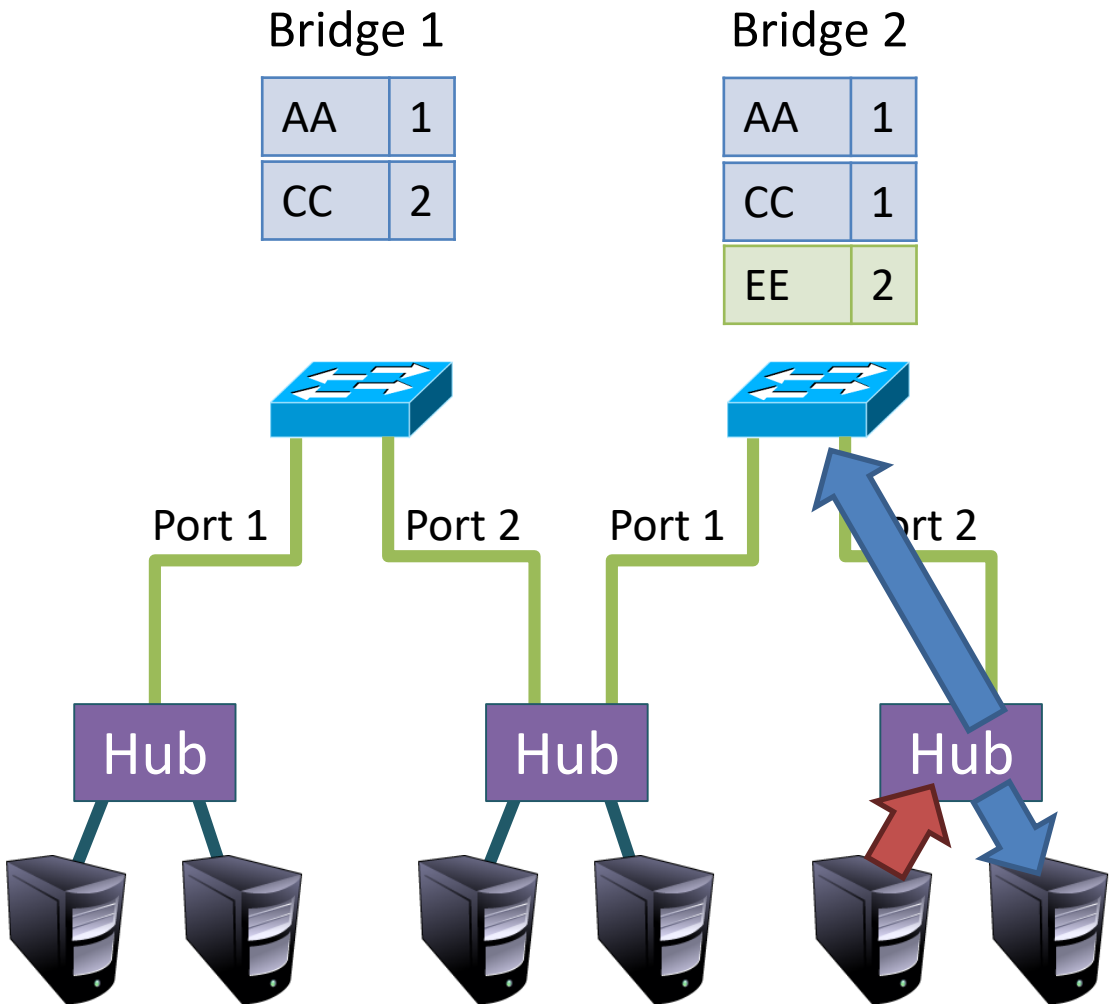
AA	1
CC	1



Komplexeres Beispiel

Paketsequenz:

1. <Src=AA, Dest=FF>
2. <Src=CC, Dest=AA>
3. **<Src=EE, Dest=CC>**

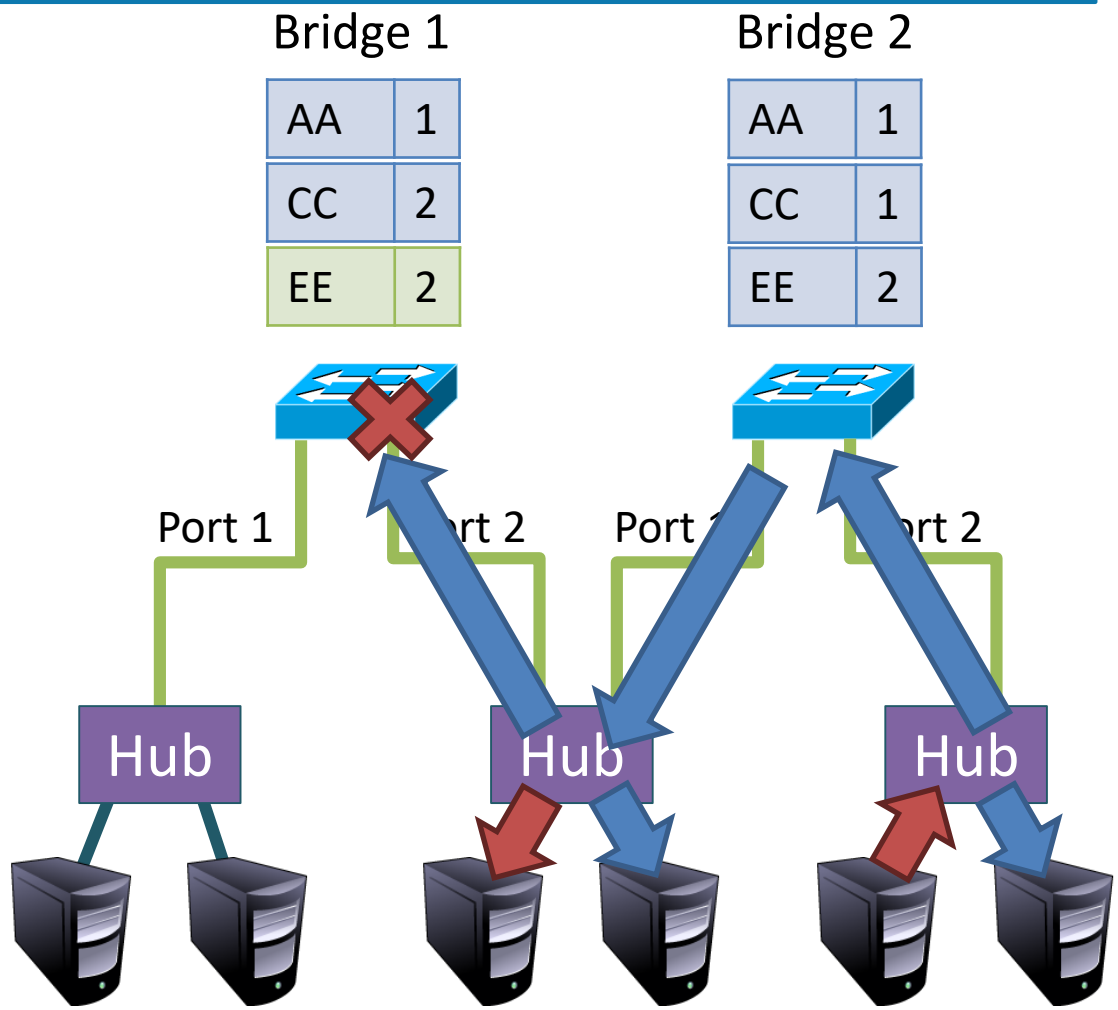


Komplexeres Beispiel

Die Erkenntnis aus dem Beispiel ist, dass eine Bridge einen Frame nicht weiterleitet, wenn bekannt ist, dass der Ziel-Host sich in dem Segment befindet, aus dem der Frame kommt.

Paketsequenz:

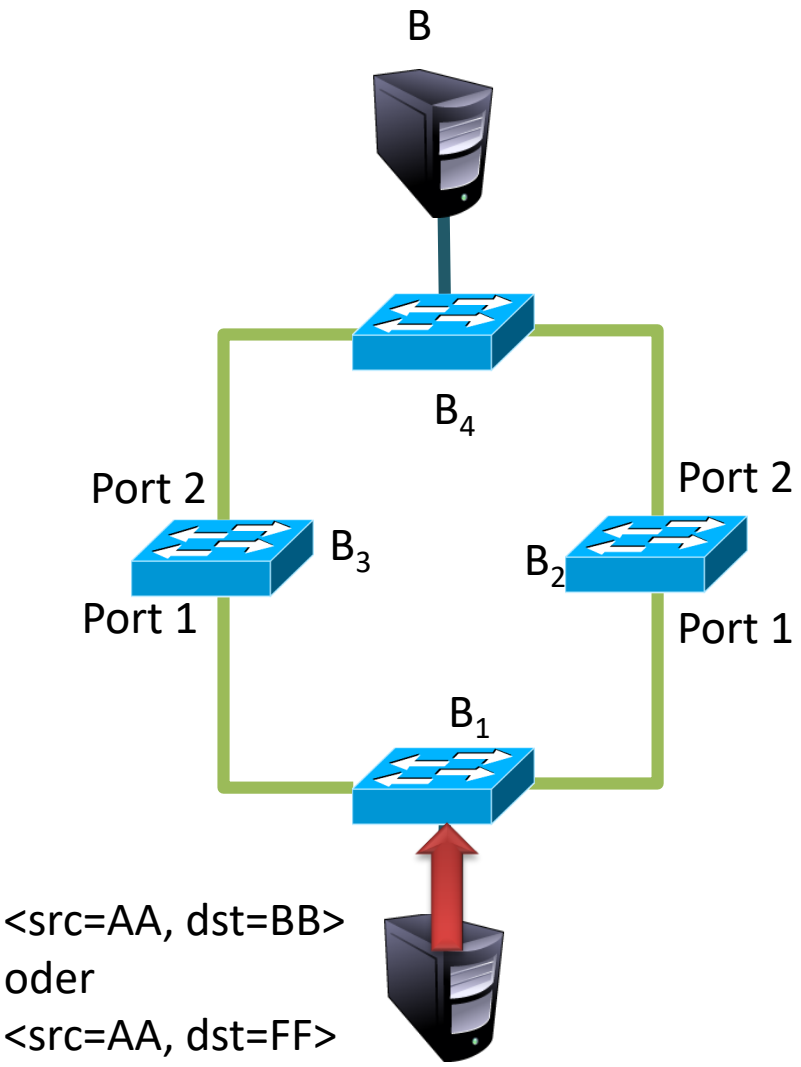
1. <Src=AA, Dest=FF>
2. <Src=CC, Dest=AA>
3. **<Src=EE, Dest=CC>**



Kapitel 5: Verkehrslenkung im Internet

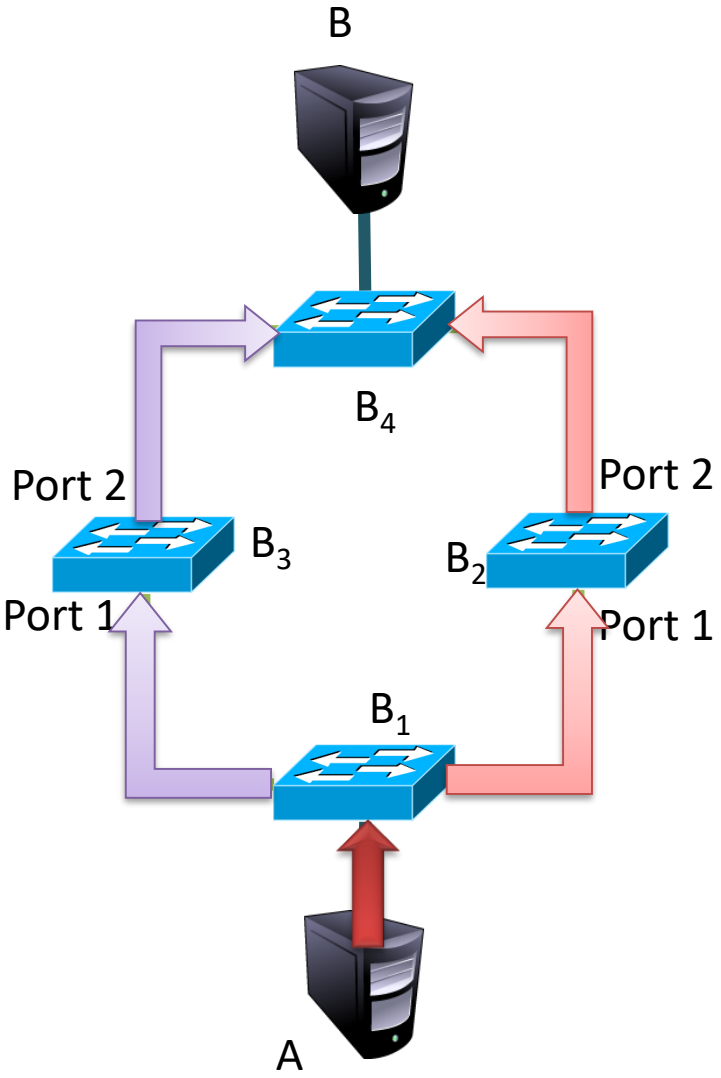
Loops – Der unendliche Broadcast

- Loops entstehen, wenn Bridges im Kreis geschaltet werden
  - im einfachsten Fall, wenn zwei Ports einer Bridge miteinander verbunden sind
- Betrachten den Fall mit vier zu einem Kreis geschalteten Bridges
- Host A schickt einen Frame mit Ziel
  - "unbekannter" Knoten B, d.h. ohne Eintrag in Forwarding Tables
  - Broadcast FF:FF:FF:FF:FF:FF



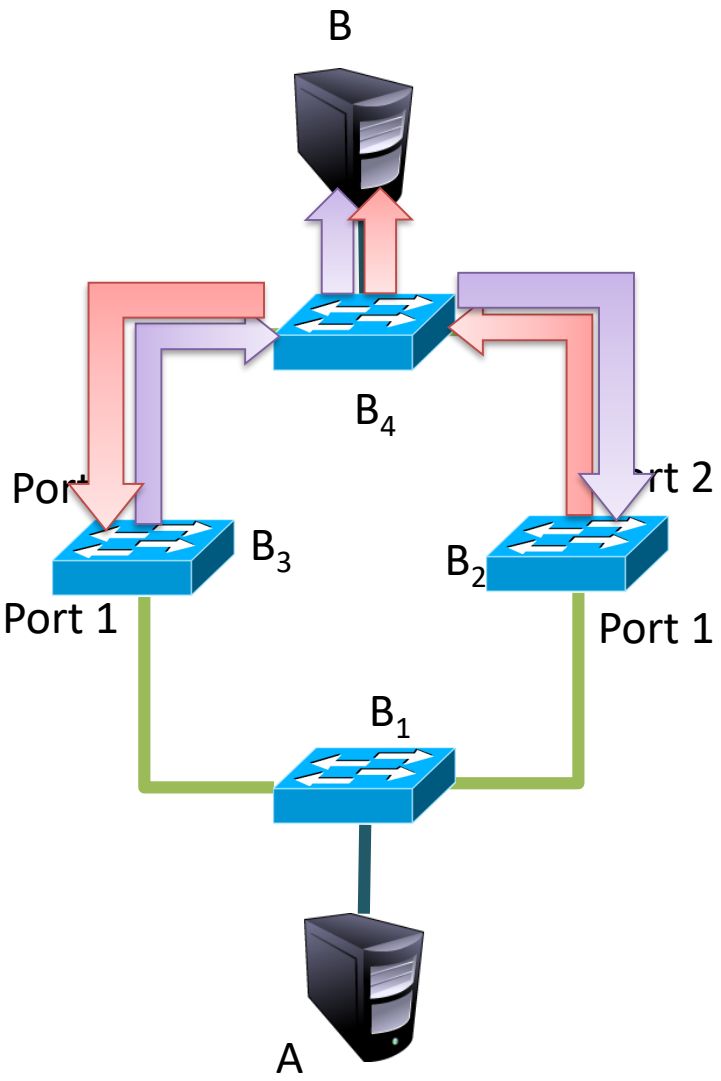
Loops – Der unendliche Broadcast

- Bridge B_1 erhält Frame mit unbekanntem Ziel und forwardet diesen auf alle Ports
- Bridges B_2 und B_3 erhalten den Frame und forwarden ihn auf allen Ports



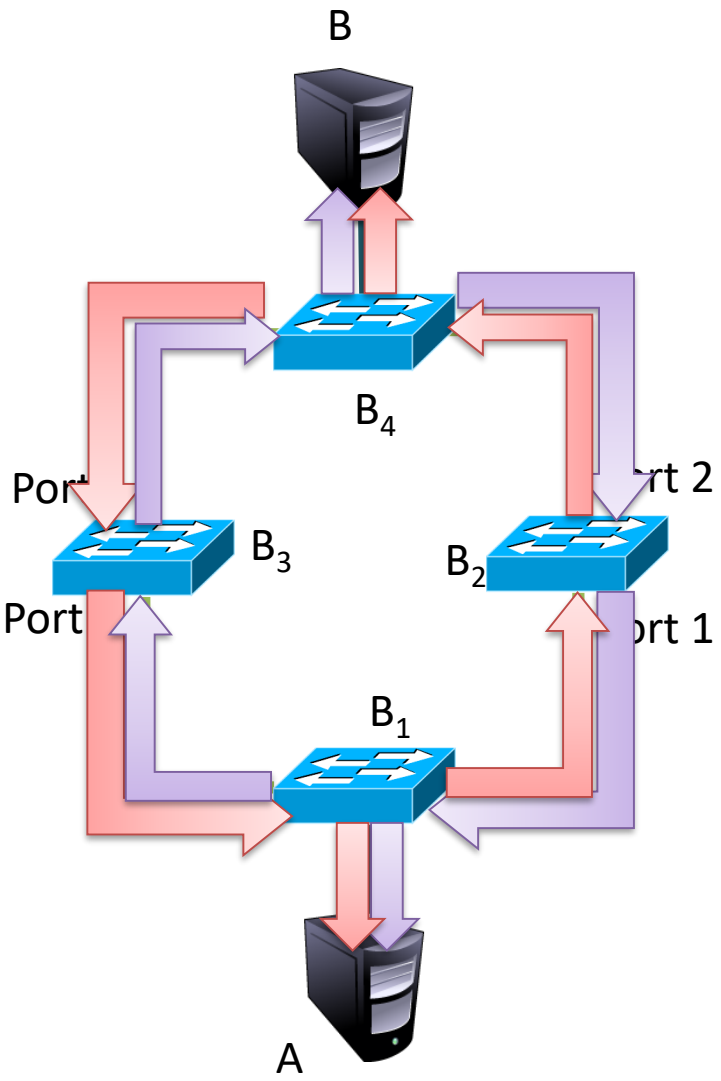
Loops – Der unendliche Broadcast

- Bridge B_1 erhält Frame mit unbekanntem Ziel und forwardet diesen auf alle Ports
- Bridges B_2 und B_3 erhalten den Frame und forwarden ihn auf allen Ports
- Bridge B_4 erhält den Frame zweimal mit unbekanntem Ziel und forwardet beide Kopien auf alle Ports
  - eine Bridge überprüft nicht, ob Frames mehrfach gesendet werden



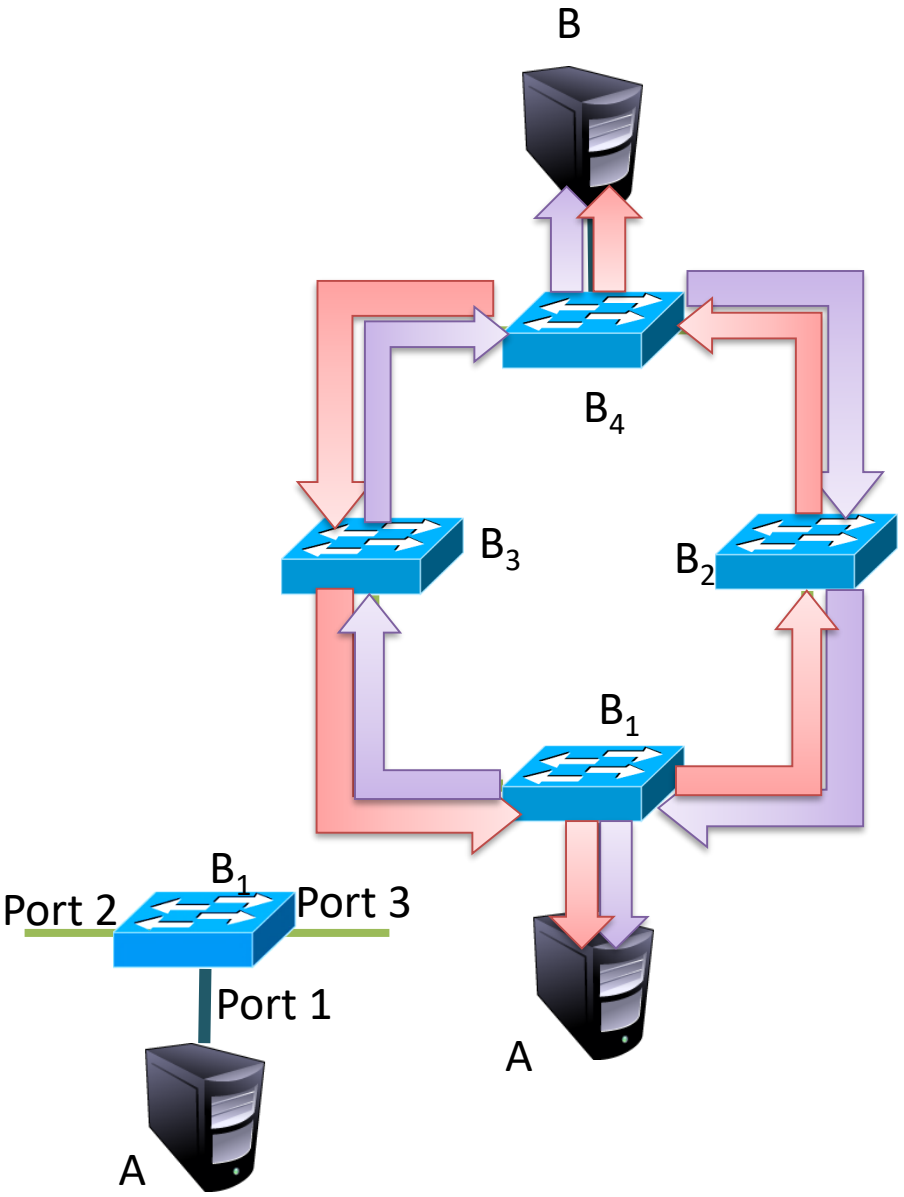
Loops – Der unendliche Broadcast

- Bridges B_2 und B_3 erhalten den Frame und forwarden ihn auf allen Ports
- Bridge B_1 erhält den Frame zweimal mit unbekanntem Ziel und forwardet beide Kopien auf alle Ports
- ...
- Der "Broadcast Storm" nimmt kein Ende, das Netz wird überlastet



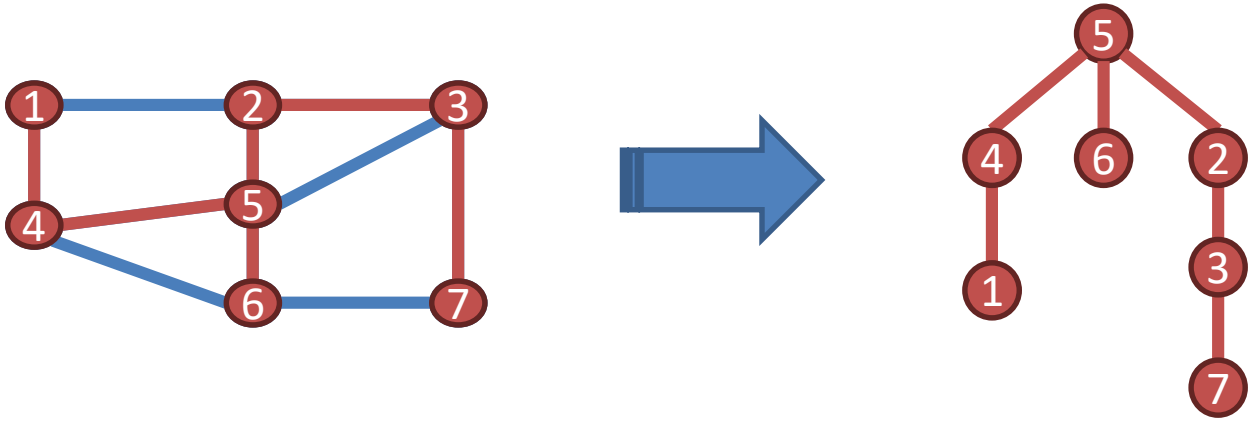
Loops – Der unendliche Broadcast

- Zusätzlich tritt das Problem auf, dass eine Bridge Pakete eines Absenders abwechselnd über mehrere Ports erhält und immer wieder ihre Forwarding Table updated
- Im Beispiel stehen in der Forwarding Table von Bridge B_1 als Ausgangsports für Station A abwechselnd Ports 2 und 3. Station A an Port 1 ist somit nicht mehr erreichbar.
- Abhilfen:
  - Loop Detection
  - Forwarden entlang eines Spannbaums
    - Spanning Tree Protocol



Lösung: Spanning Tree

- Bridges identifizieren über das Spanning-Tree-Protokoll einen Spannbaum
  - STP (Spanning Tree Protocol), IEEE 802.1D-1990
  - RSTP (Rapid Spanning Tree Protocol), IEEE 802.1D-2004
  - Spannbaum ist ein zyklenfreier Graph, der alle Netzknoten (Bridges) enthält

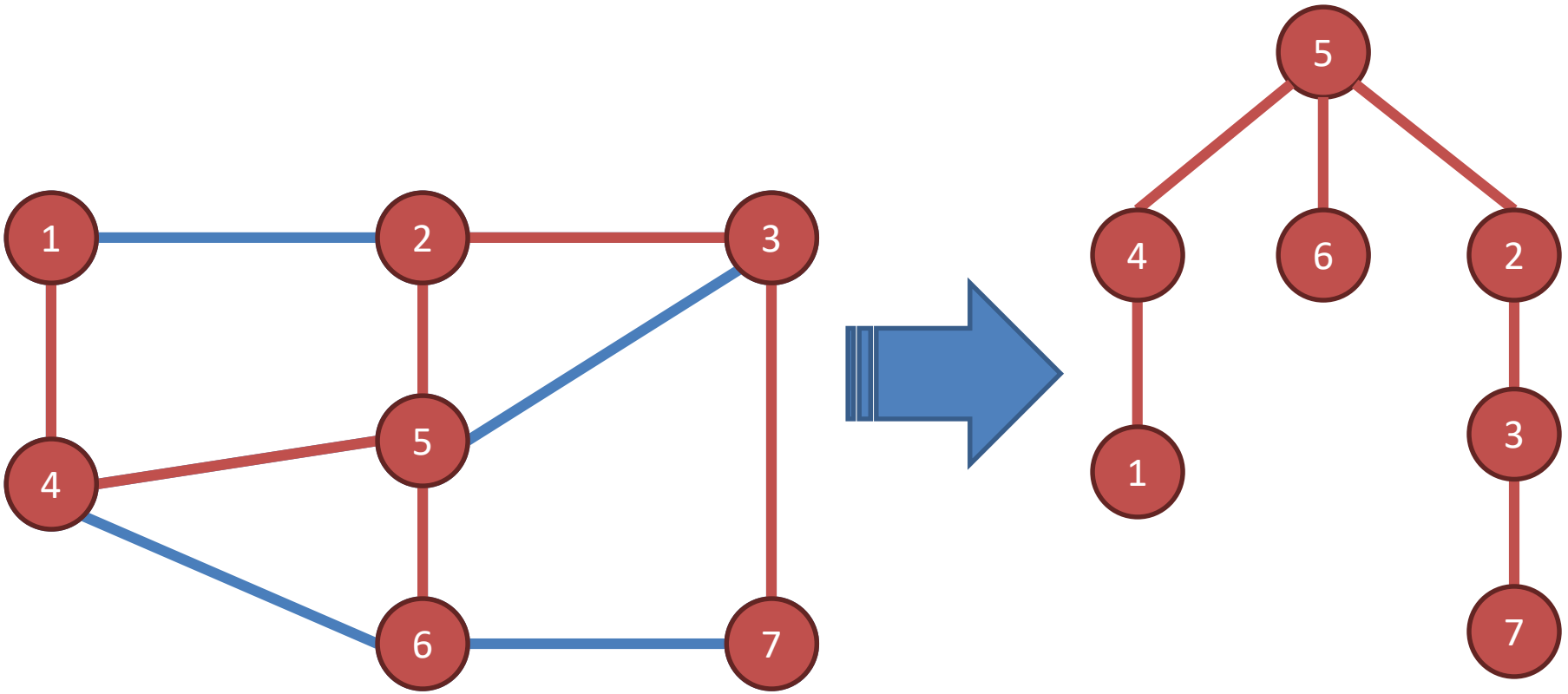


- Jede Bridge kennt die benachbarten Bridges im Spanning-Tree
- Paketweiterleitung (Broadcast) erfolgt nur entlang des Spanning-Trees
  - Zyklen werden vermieden

Spanning Tree (Spannbaum)

Info

- Spanning-Tree enthält alle Knoten und eine Teilmenge der Kanten, so dass alle Knoten verbunden sind
  - es gibt mehrere Spanning-Trees für einen Grafen
  - minimaler Spanning-Tree enthält die kleinst-mögliche Anzahl von Kanten
- Bridges finden einen Spanning-Tree über einen Spanning-Tree-Algorithmus



Spanning-Tree-Algorithmus (IEEE 802.1)

Info

1. Wähle eine Bridge als Wurzel
2. Jede Bridge findet einen kürzesten Weg zur Wurzel
3. Alle diese Pfade zusammen bilden den Spaning Tree

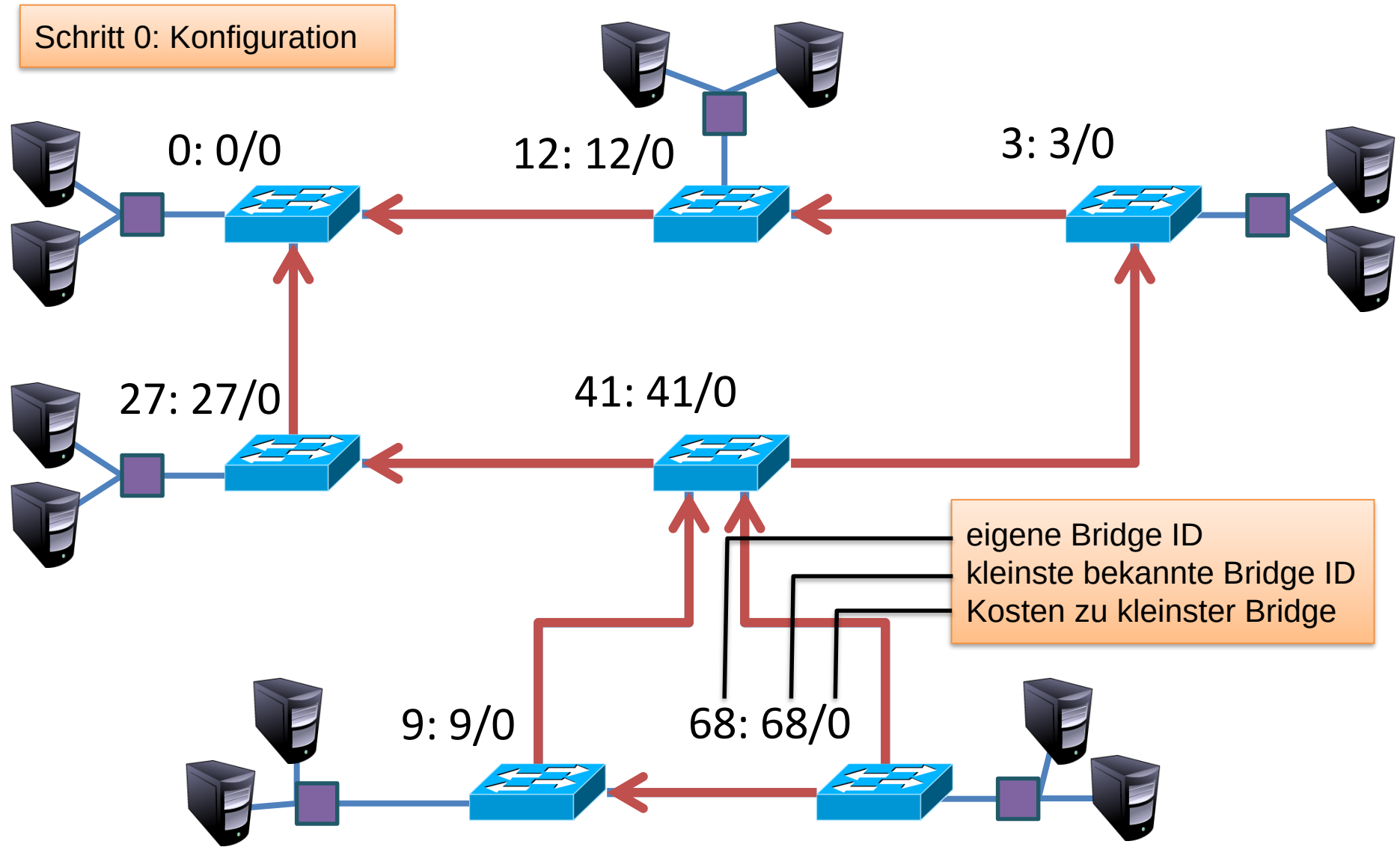
- Aufbau des Spanning Trees über Bridge Protocol Data Units (BPDU)

  - Auswahl der Root-Bridge (kleinste ID)
  - Berechnung des kürzesten Pfades
  - Nächster Hop zur Wurzel und dazugehöriger Port
  - Auswahl der Ports, die zum Spannbaum gehören

- Protokolle:
  - STP (Spanning Tree Protocol), IEEE 802.1D-1990
  - RSTP (Rapid Spanning Tree Protocol), IEEE 802.1D-2004

Aufbau eines Spannbaum

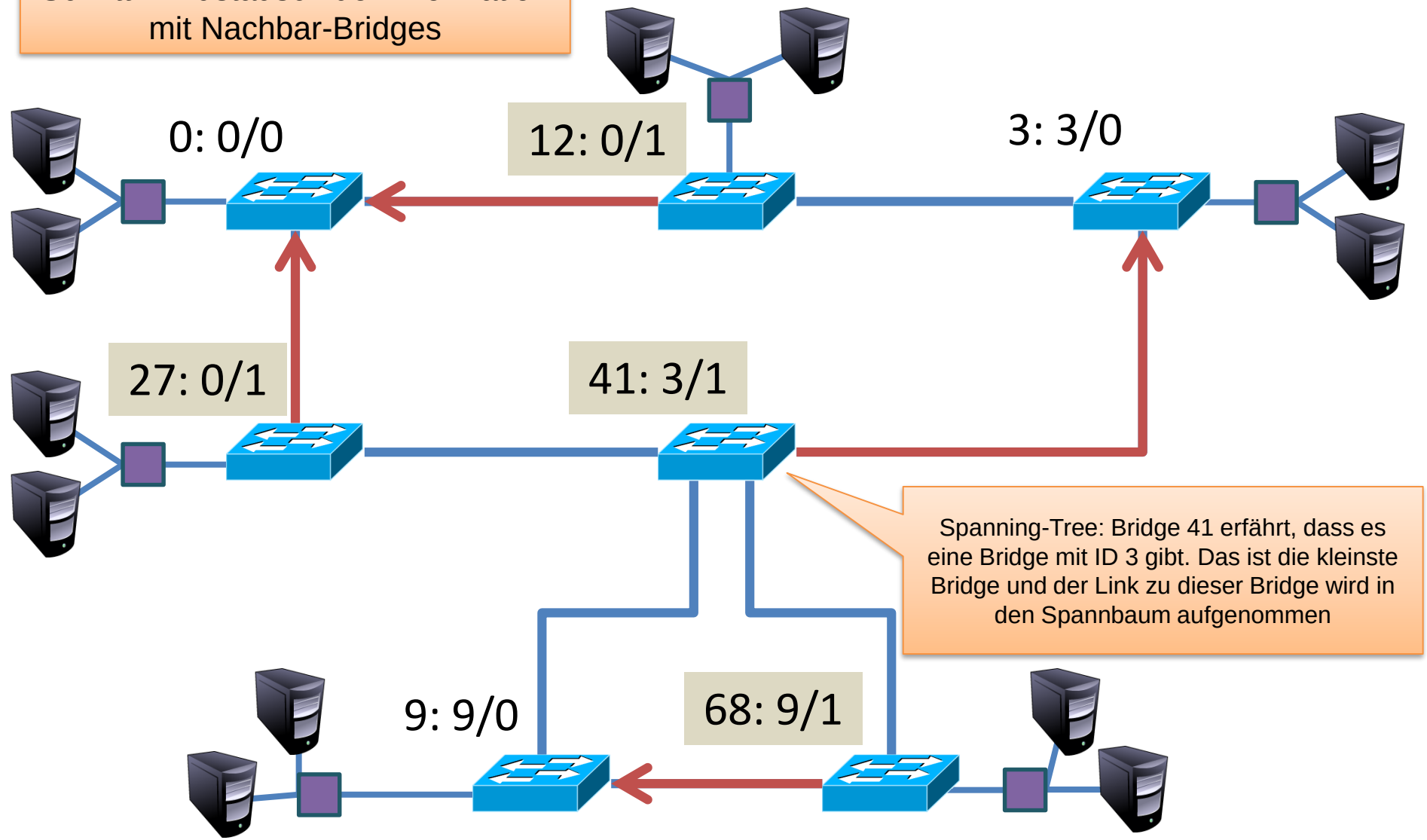
Info



Aufbau eines Spannbaum

Info

Schritt 1: Austausch der Information mit Nachbar-Bridges

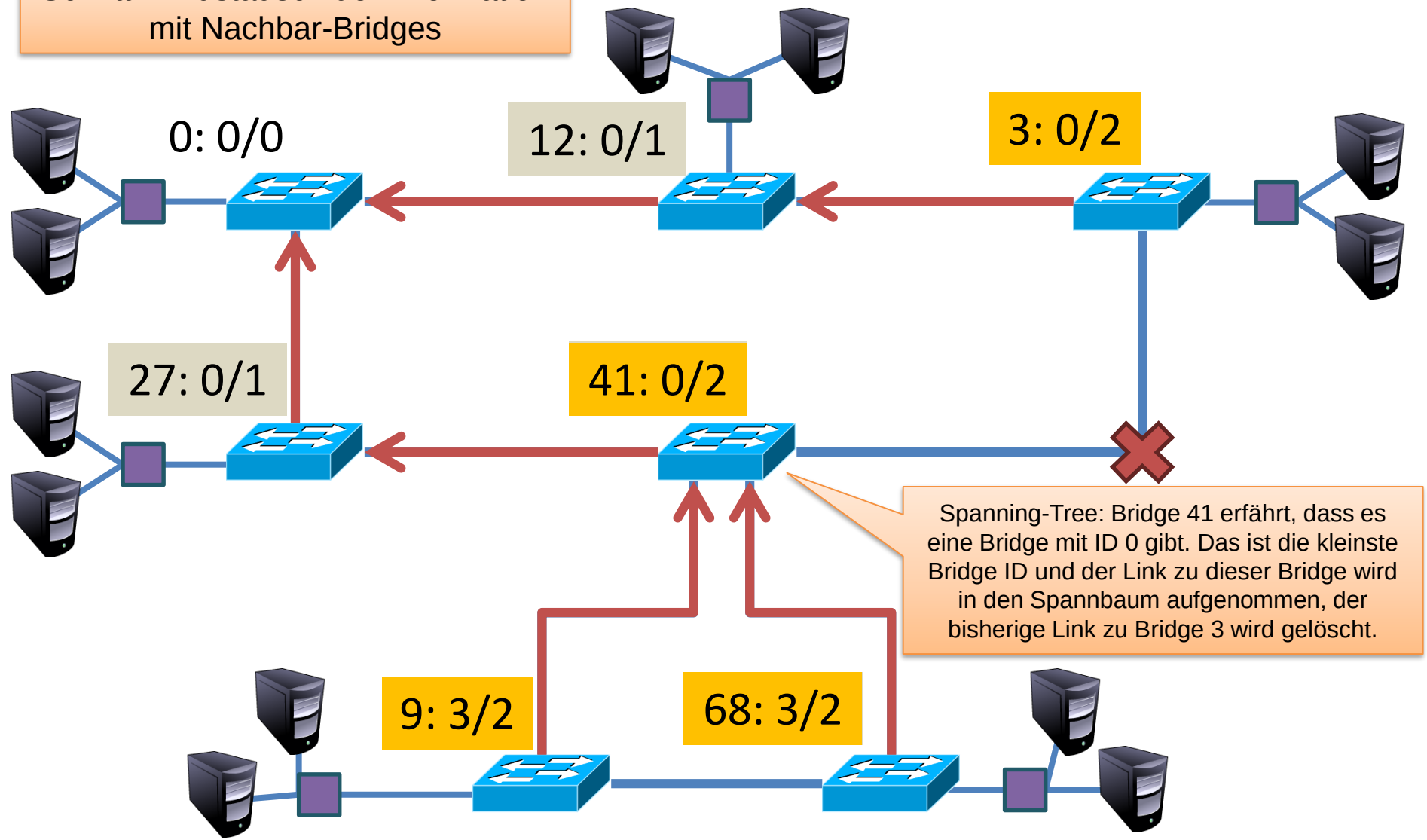


Spanning-Tree: Bridge 41 erfährt, dass es eine Bridge mit ID 3 gibt. Das ist die kleinste Bridge und der Link zu dieser Bridge wird in den Spannbaum aufgenommen

Aufbau eines Spannbaum

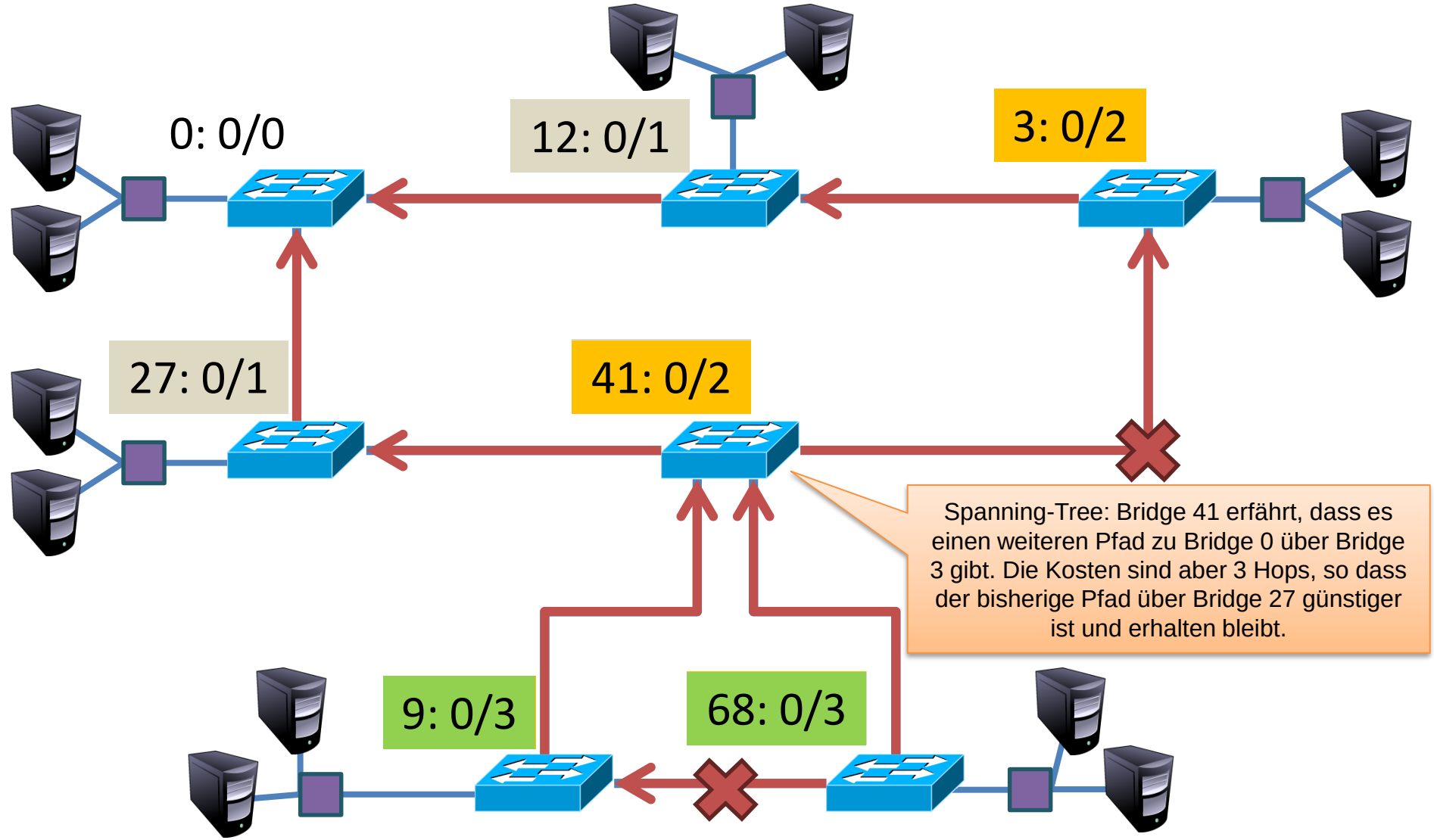
Info

Schritt 2: Austausch der Information mit Nachbar-Bridges



Aufbau eines Spannbaum

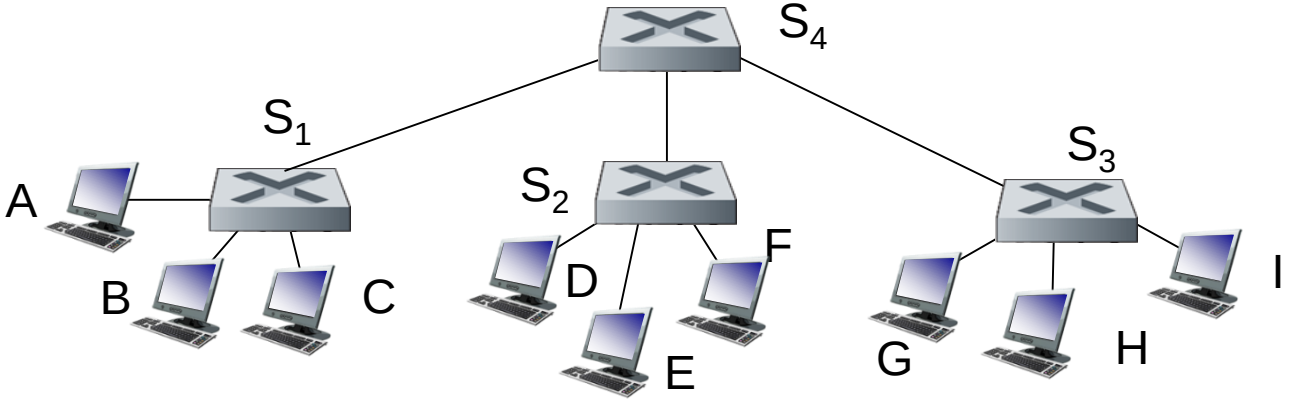
Info



Kapitel 5: Verkehrslenkung im Internet

Switches

- typisches Element in heutigen LANs
- Bridge mit nur einem Netzknoten (Host, Switch) pro LAN-Segment
  - Unterschied Bridge/Switch nicht genau definiert
  - Switches unterstützen VLANs (Virtual LANs)
- Verbindung zwischen Switch und Host oder Switch und Switch über Full-Duplex-Ethernet
  - im Switched Ethernet gibt es keine Kollisionen



Virtuelle LANs – Virtual Local Area Network (VLAN)

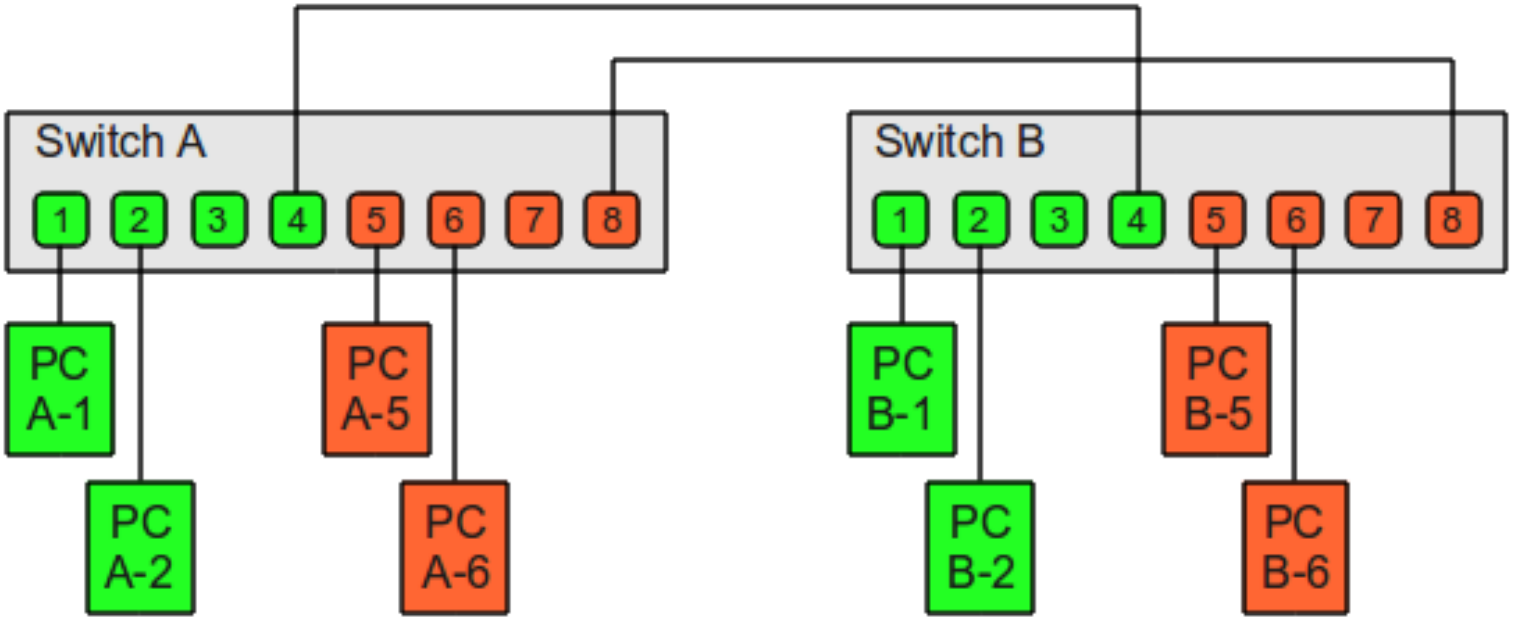
- VLANs sind eine Technik, um mehrere logische LANs auf einem physikalischen LAN zu betreiben
  - Broadcast Frames - und auch Frames mit unbekannter Zieladresse - werden dann nur im logischen LAN, dem VLAN, weitergeleitet
  - eine direkte Kommunikation zwischen Stationen in zwei unterschiedlichen VLANs eines physikalischen LANs ist nicht möglich
    - die VLANs müssen durch einen Router verbunden werden – die Paketweiterleitung erfolgt über die IP-Adresse
- Es gibt zwei Möglichkeiten Ports bzw. Frames einem VLAN zuzuweisen
  - Zuordnung eines Ports zu genau einem VLAN (port-basiert)
    - ein Switch ordnet die auf dem Port empfangenen Frames dem konfigurierten VLAN zu und leitet sie entsprechend weiter
  - Zuordnung mehrerer VLANs zu einem Port mittels VLAN-Tagging
    - der Port wird Trunk-Port genannt

VLANs – Tagging

- Frames, die zwischen Trunk-Ports übertragen werden, werden getaggt, d.h. die VLAN-ID wird im Frame-Header übertragen
  - dazu wird zwischen Trunk-Ports das IEEE 802.1q Protokoll verwendet, das den Ethernet-Header um das Feld VLAN-ID erweitert
  - Trunk-Ports können also nur mit Trunk-Ports verbunden sein
- ein Switch ordnet die auf einem Trunk-Port empfangenen Frames dem im Frame-Header spezifizierten VLAN zu und leitet sie entsprechend weiter
- die über einen Trunk-Port laufenden VLANs können konfiguriert werden
  - Frames, die zu nicht konfigurierten VLANs gehören, werden verworfen

Beispiel: Port-basiertes VLAN

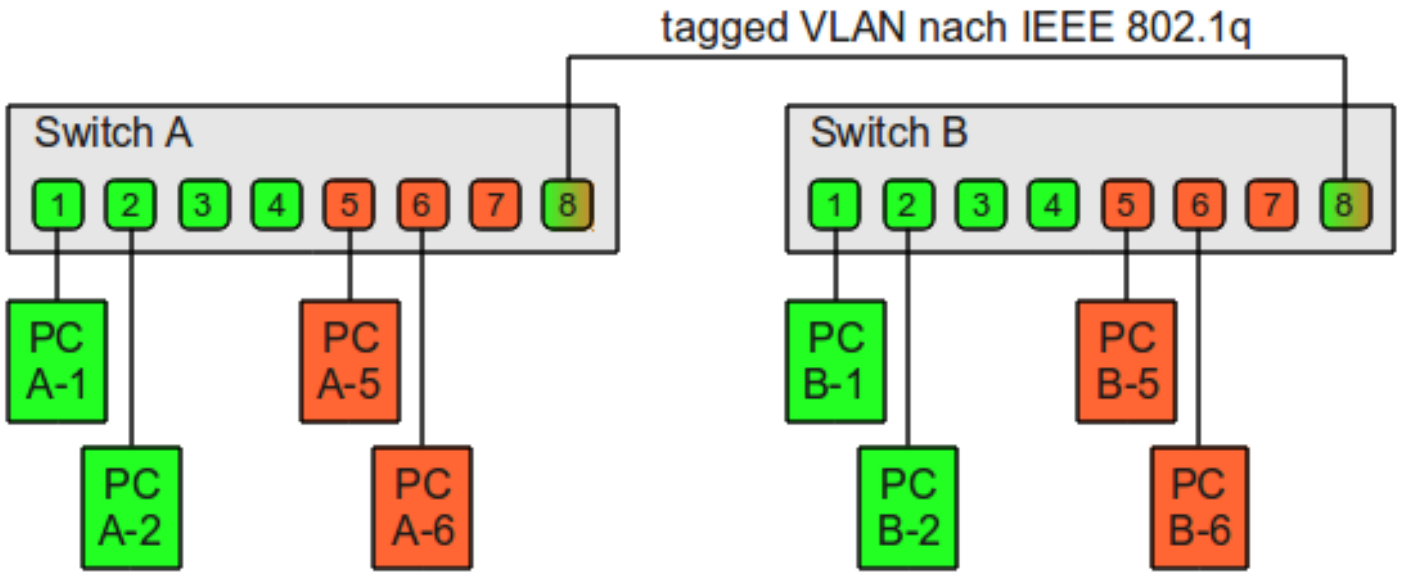
- Physikalisches LAN besteht aus zwei Switches mit jeweils 8 Ports
  - Ports 1-4 werden jeweils VLAN 1 zugeordnet
  - Ports 5-8 werden jeweils VLAN 2 zugeordnet
  - um die beiden logischen Switches eines VLANs zu verbinden, müssen zwei diesem VLAN zugeordnete Ports der beiden Switches verbunden werden
- Ein Broadcast-Frame von PC A-1 wird von Switch A nur auf Ports 2-4 weitergeleitet, Switch B erhält den Frame auf Port 4 und forwardet ihn auf Ports 1-3



source: http://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen

Beispiel: Tagged VLAN mit Trunk-Port

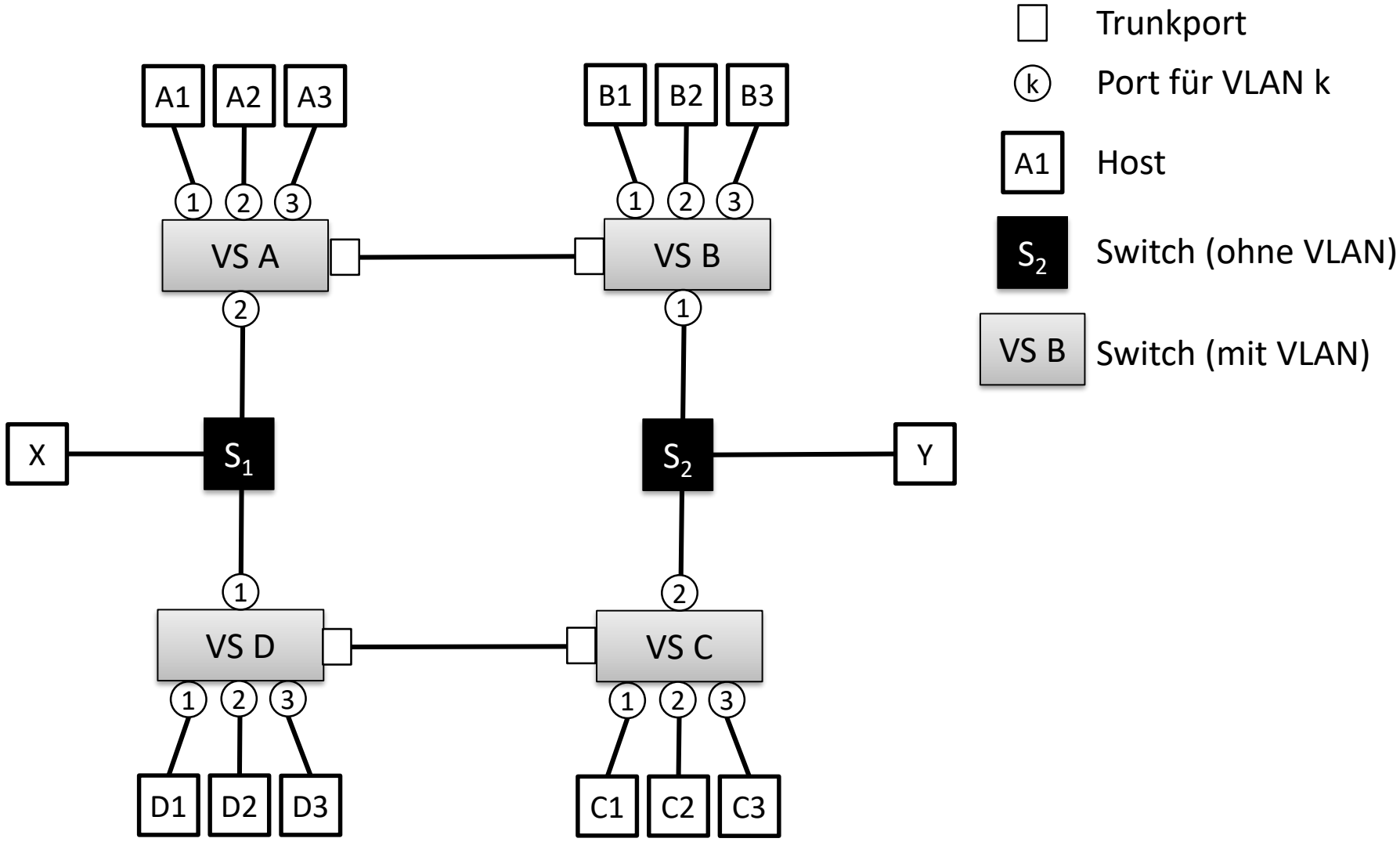
- Physikalisches LAN besteht aus zwei Switches mit jeweils 8 Ports
  - Ports 1-4 werden jeweils VLAN 1 zugeordnet
  - Ports 5-7 werden jeweils VLAN 2 zugeordnet
- Port 8 ist jeweils als Trunk-Port für VLANs 1 und 2 konfiguriert
- Ein Broadcast-Frame von PC A-1 wird von Switch A auf Ports 2-4 weitergeleitet
  - zusätzlich wird der Frame mit dem Tag **VLAN1** versehen auf Port 8 weitergeleitet
  - Switch B erhält den Frame auf Port 8, erkennt am Tag, dass er zu VLAN 1 gehört und forwardet ihn auf Ports 1-4



source: http://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen

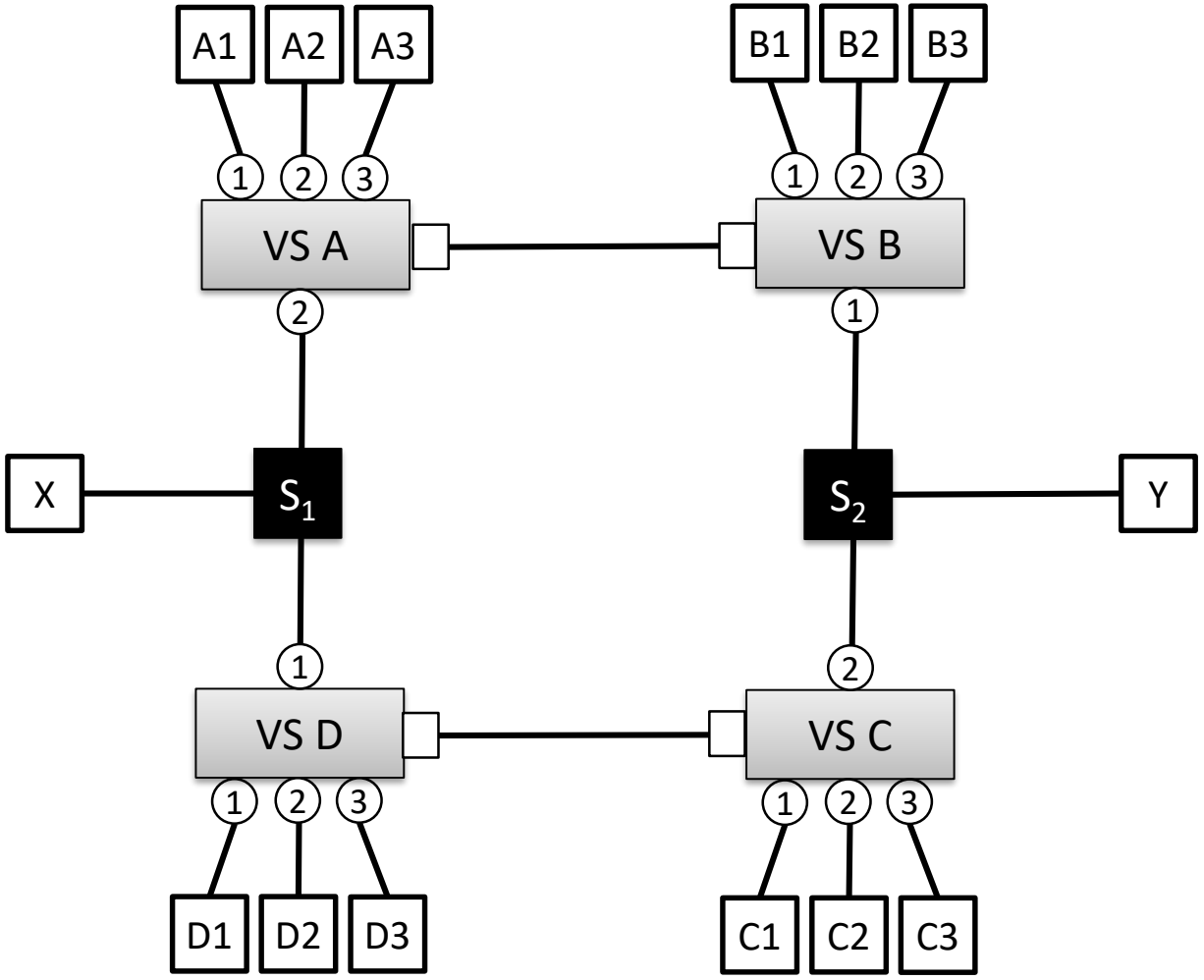
Beispiel zum Verständnis

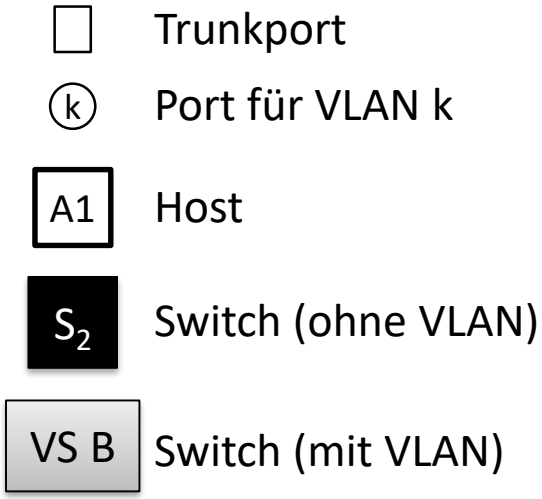
- Welche VLANs gibt es in diesem LAN?



Beispiel zum Verständnis

- Welche VLANs gibt es in diesem LAN?

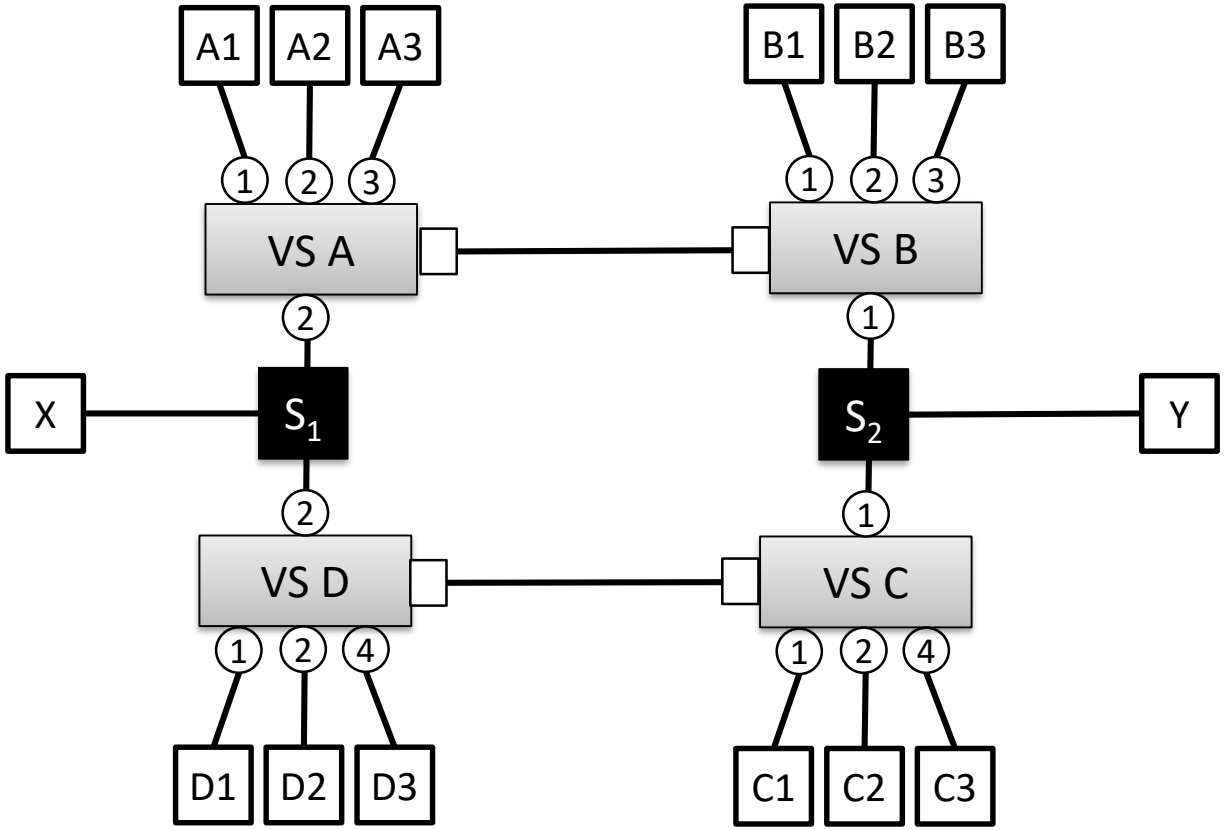




Liste der VLANs:
- A1, B1, Y, C2, D2
- A2, B2, X, D1, C1
- A3, B3
- D3, C3

Erklärung

- Die Zuweisung Port zu VLAN-ID wird in einem Switch lokal interpretiert, d.h. ein VLAN1-Port von Switch A kann mit einem VLAN2-Port von Switch B verbunden sein
- Eine solche Zuweisung ist zwar technisch möglich aber nicht sinnvoll, weil irreführend. Wird die Konfiguration der Ports mit einem Tool mit Netzsicht vorgenommen, wird eine derartige Konfiguration meist nicht unterstützt.
- Eine bessere Konfiguration mit identischen VLANs wäre die folgende:



Liste der VLANs:
- A1, B1, Y, C2, D2
- A2, B2, X, D1, C1
- A3, B3
- D3, C3

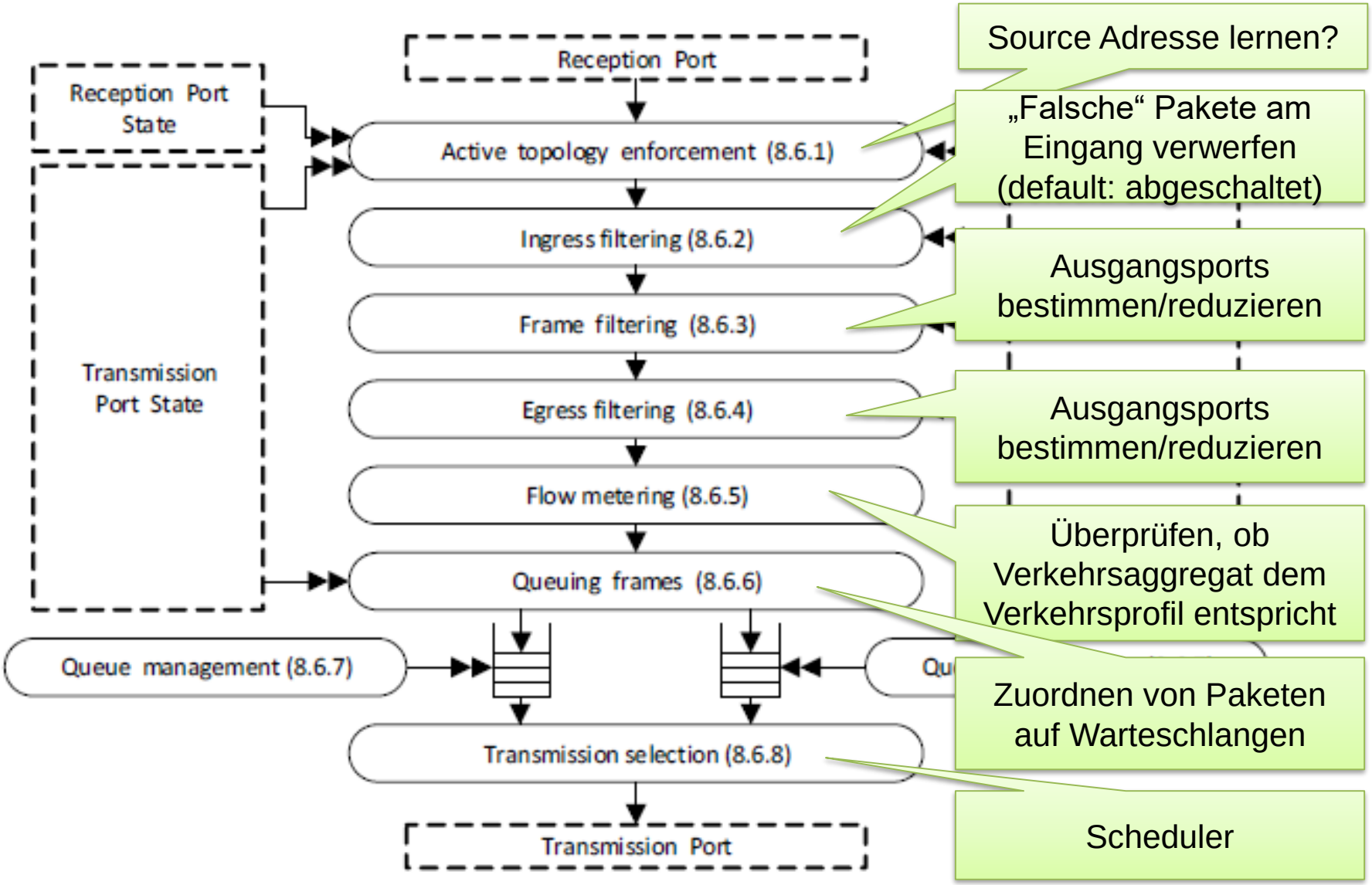
Einsatzszenarien für VLANs (1)

- Klassisch diesen VLANs zunächst dazu, auf einer physikalischen Infrastruktur, mehrere logische (virtuelle) LANs zu betreiben.
- Der unmittelbare Vorteil ist die Ersparnis von Hardware-Ressourcen, d.h. weniger Switches und eine einfachere Verkabelung.
- Weitere Gründe für das Betreiben von getrennten LANs sind
  - Einschränkung von LAN-Broadcasts z.B. von ARP-Pakete
  - Sicherheit: Vermeiden der unmittelbaren Erreichbarkeit von Geräten über die MAC-Adresse. VLANs sind durch Router evtl. mit Firewall getrennt.
    - Separieren eines Gäste WLANs als eigenes VLAN
    - Separieren von VLANs für Professoren und Studierende
- Einfachere Zuweisung von Geräten zu LANs
  - LAN: Gerät muss an bestimmten Switch angeschlossen werden
  - VLAN: Gerät wird an beliebigen Switch angeschlossen und VLAN wird konfiguriert

Einsatzszenarien für VLANs (2)

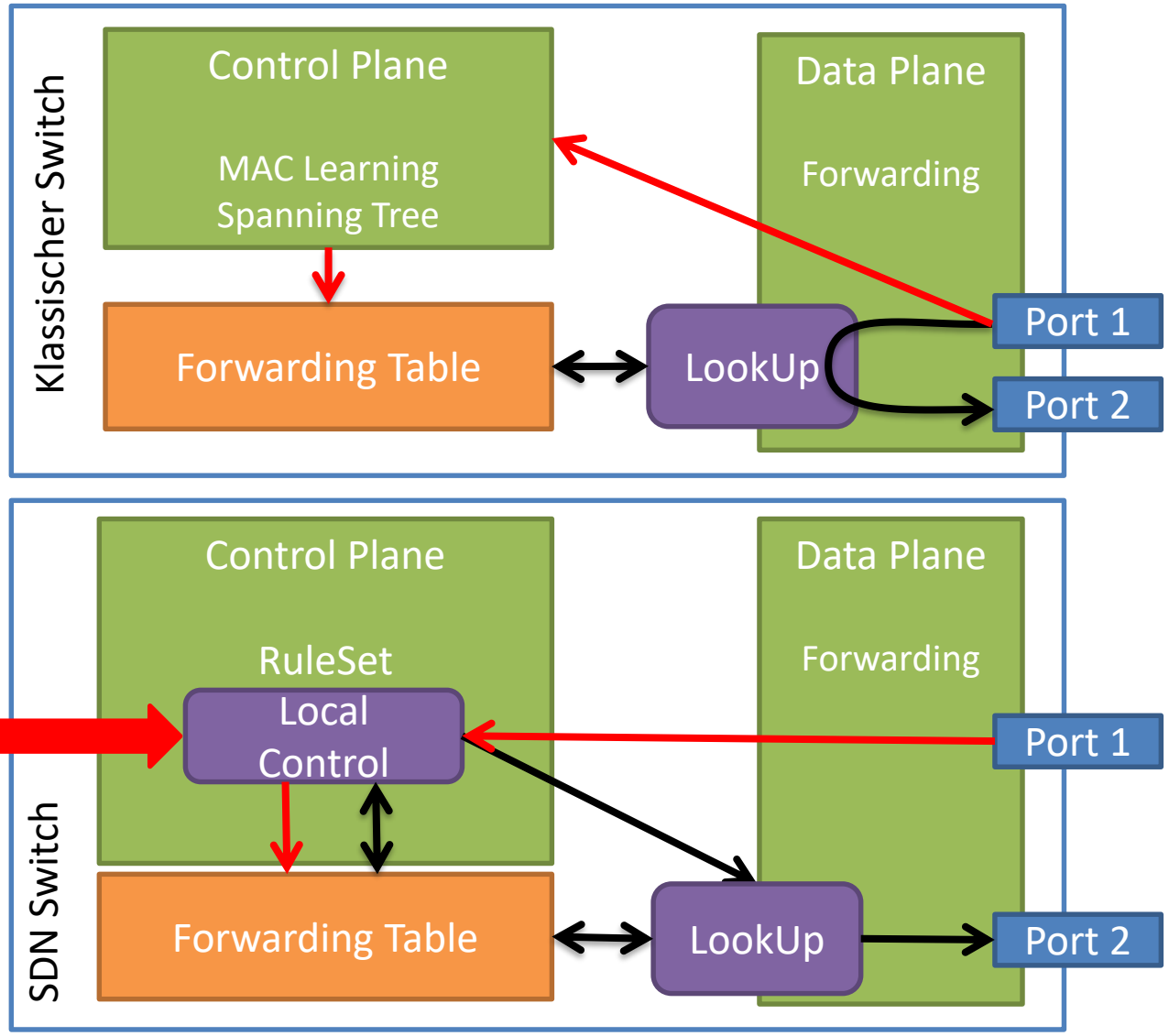
- Aufsplitten eines LANs in mehrere Netzwerksegmente mit eigenen IP Adressbereichen
  - siehe Netzwerksegmente im Kapitel zu Intra-Domain Routing
  - erlaubt Firewall-Regeln und andere Einschränkungen aufgrund der IP-Adresse
- Unterschiedliche Verkehrsbehandlung über VLAN
  - Priorisierung von Frames über die VLAN-ID
  - Beispiel VoIP:
    - alle VoIP-Geräte befinden sich in einem VLAN
    - Frames dieses VLANs werden priorisiert
- Virtualisierung:
  - VLAN-fähige Netzwerkkarten mit virtuellen Interfaces werden genutzt, um einen Host mit mehrere VLANs zu verbinden.
  - So können mehrere virtuelle Maschinen in unterschiedlichen VLANs betrieben werden.

Komplexität Bridge: Forwarding Process (802.1Q Standard)



Prinzip: Software Defined Networking

Prinzip von SDN:
Entscheidung über Verkehrslenkung nicht mehr lokal im Switch sondern in zentralem Controller mit zentraler Sicht und globalen Informationen



Zusammenfassung – Bridges und Switches

- Lokale Netze leiten Pakete aufgrund der MAC Adresse weiter
- MAC Adressen unstrukturiert und bilden einen flachen Adressraum
  - Vorteil: jeder Rechner kann mit seiner eigenen MAC Adresse in ein lokales Netz aufgenommen werden, ohne dass eine Konfiguration notwendig ist
  - Nachteil: jeder Switch muss sich in seiner Forwarding-Tabelle der Port für alle MAC Adressen im lokalen Netz merken. Bei großen Netzen kann die Forwarding-Tabelle sehr groß werden
- Bridges (und damit auch Switches) lernen die Zuordnung von MAC Adresse zu Port über die Source-MAC-Adresse ankommender Pakete
- In heutigen LANs existieren eigentlich nur noch Switches und damit kollisionsfreies Switched Ethernet.
  - heutige Switches unterstützen VLAN, um mehrere logische LANs in große physikalische LANs einzubetten.
- WLAN Access Points sind funktionell Bridges, die ein LAN und ein WLAN verbinden.
- Software Defined Networking (SDN) wird in vielen Netzen eingeführt, um klassische dezentrale Switching- und Routing-Entscheidungen durch einen zentralen Controller abzulösen
  - ermöglicht effizienteres Netzwerkmanagement