

Netztechnik-Vorlesung Teil-8

Inhalt

- Netzwerk-Komponenten
 - ◆ Repeater
 - ◆ Brücken
 - ◆ Switches
 - ◆ Router
 - ◆ Gateways

Einleitung

Bei der Übertragung von Daten in Netzwerken sind viele Anforderungen und Probleme zu bewältigen:

- Dämpfungsprobleme, die letztendlich Längenprobleme erzeugen können.
- Begrenzung der Anzahl der Teilnehmer auf einem Netzsegment.
- Räumliche Trennung
- Logische Trennung
- Lastprobleme
- Antwortzeiten
- Kollisionen
- Sicherheit
- Management

Für jedes dieser Probleme gibt es ein Heilmittel.
Je nach Problem werden die Komponenten eingesetzt.

Netzwerk-Komponenten

Repeater Teil-1

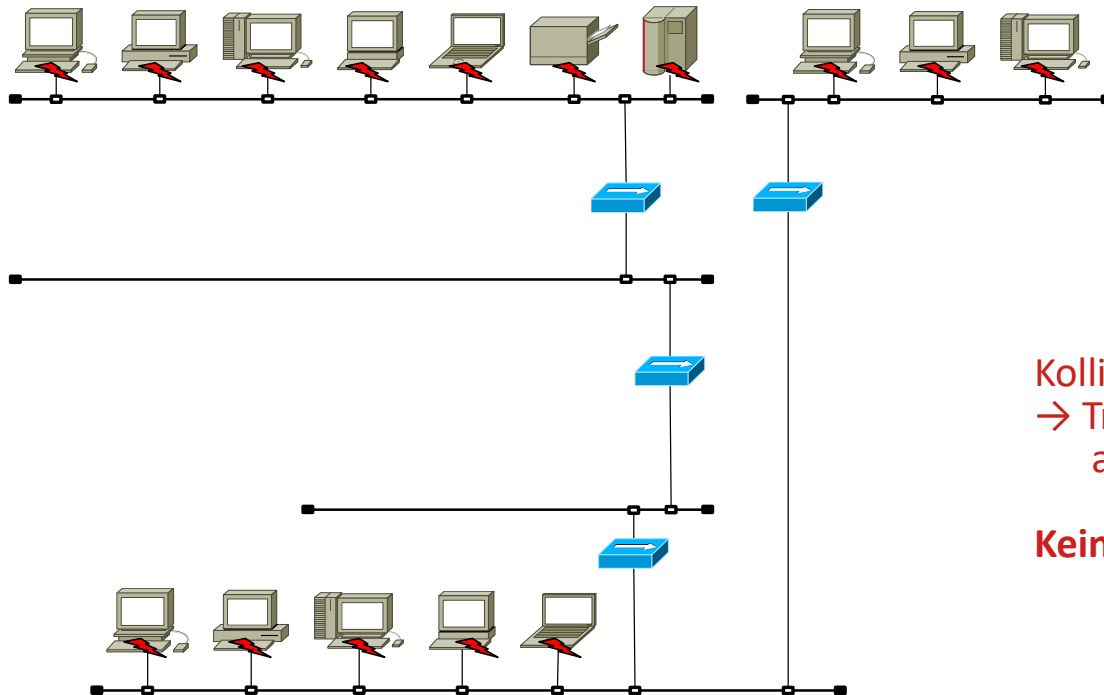


Verlängert Netzsegmente, die wg. Dämpfung an Grenzen stoßen

Überall die gleich Geschwindigkeit (10Mbps oder 100Mbps)

Repeater-Regeln

- Repeater-Regeln für 10 Mbps
 - ◆ Max. 5 Segmente
 - ◆ Max. 4 Repeater zwischen zwei Endgeräten
 - ◆ Max. 3 gleichzeitig genutzte Segmente (an 3 Segmenten dürfen gleichzeitig Stationen betrieben werden)
- Repeater-Regeln für 100 Mbps
 - ◆ Max. 4 Segmente
 - ◆ Max. 3 Repeater zwischen zwei Endgeräten
 - ◆ Max. 2 gleichzeitig genutzte Segmente (an 2 Segmenten dürfen gleichzeitig Stationen betrieben werden)

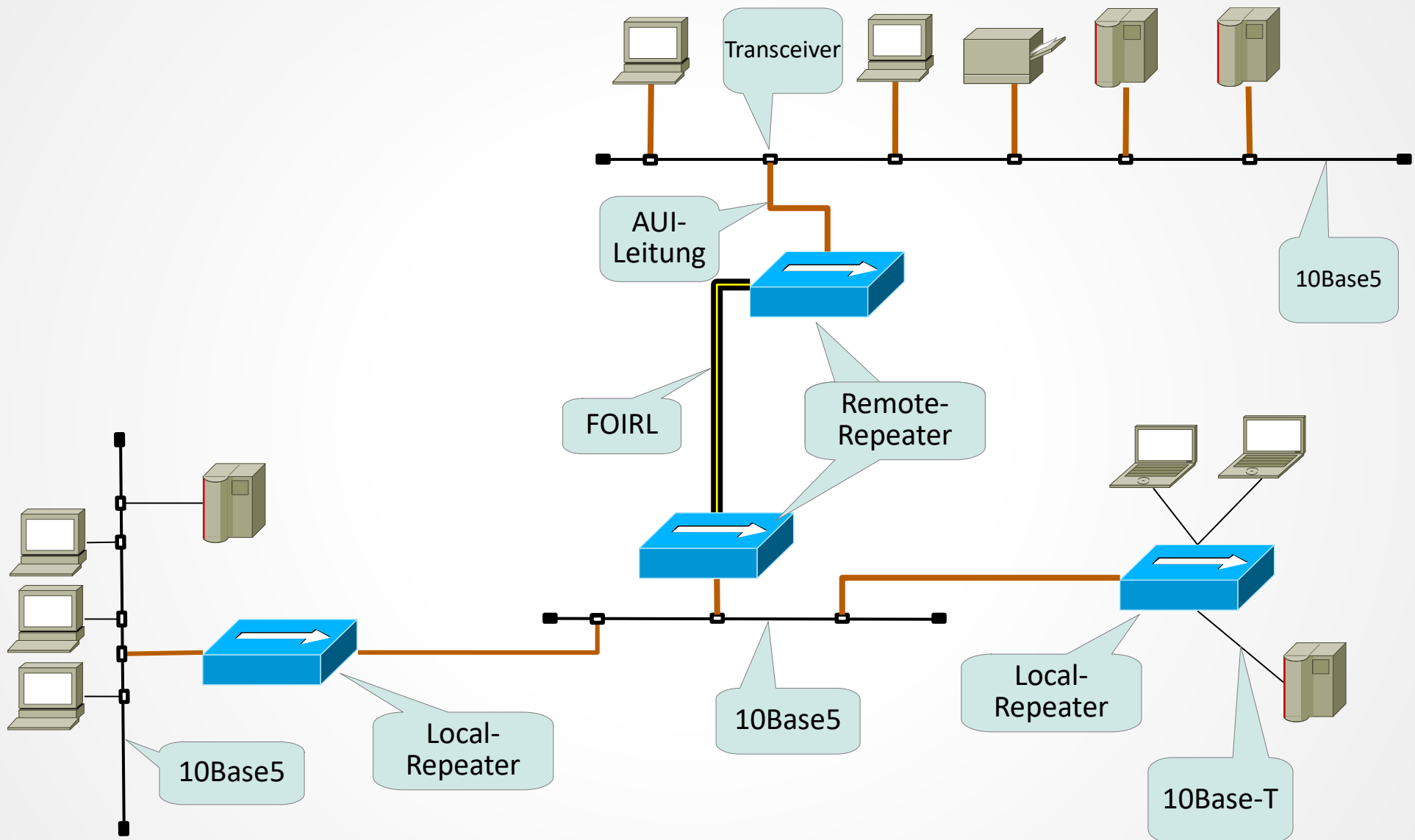


Kollisionen werden weiter geleitet!
→ Tritt in einem Segment eine Kollision auf, wird sie auch an die anderen Segmenten weiter geleitet!

Keine Begrenzung von Kollisionsdomänen

Netzwerk-Komponenten

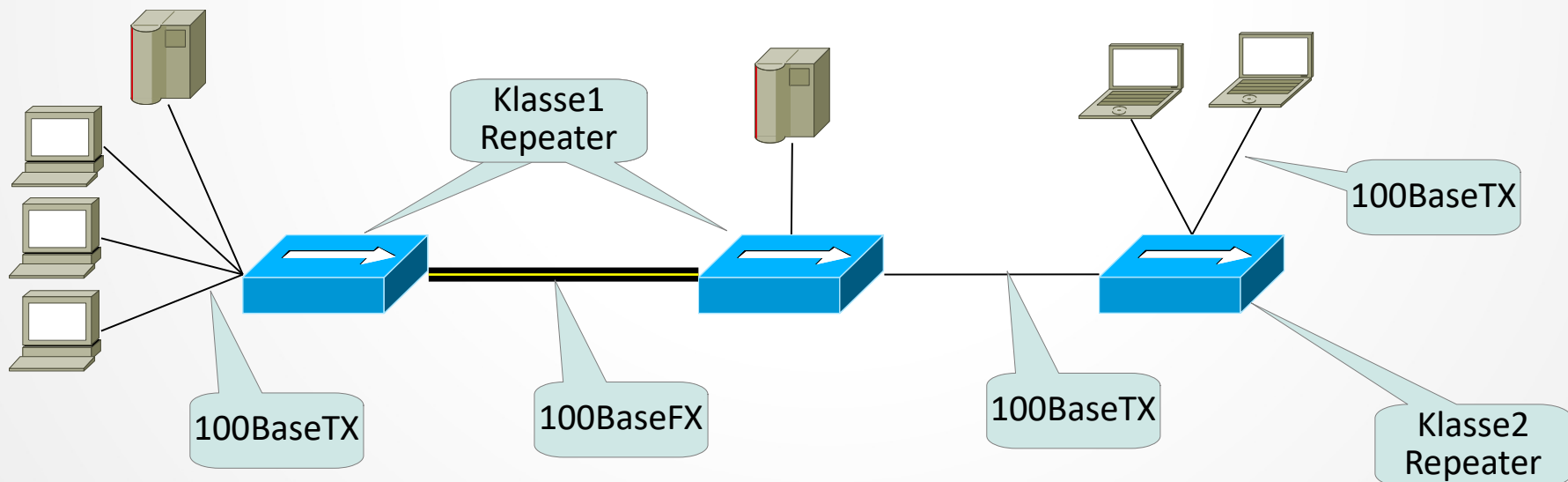
Repeater Teil-2



Netzwerk-Komponenten

Repeater Teil-3

Klasse	Bedeutung
1	Entspricht einem Media-Konverter. Es können unterschiedliche Medien miteinander verbunden werden. Z. B. kann 100Base-Tx mit 100Base-Fx verbunden werden. Ist somit langsamer als Repeater der Klasse II.
2	Diese Repeater verbinden immer nur Ports mit dem gleichen Medium



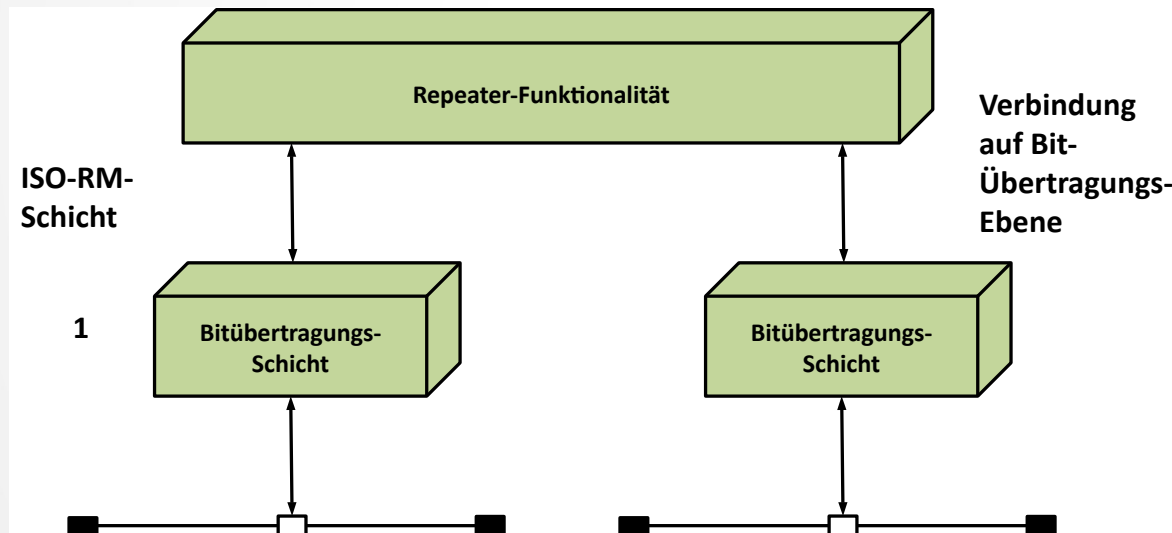
Netzwerk-Komponenten

Repeater Teil-4

Probleme, bei denen mit Repeatern geholfen werden kann:

- Längenbegrenzungen (Maximale Segmentlängen, je nach Topologie beachten)
- Anzahl von Teilnehmern (maximale Komponentenanzahl beachten)
Z.B. in einem Netzsegment ist die Anzahl der möglichen Teilnehmer begrenzt, z. B. 30 in einem 10Base2-Netzsegment.

Repeater im ISO-7-Schichten-Modell



Netzwerk-Komponenten

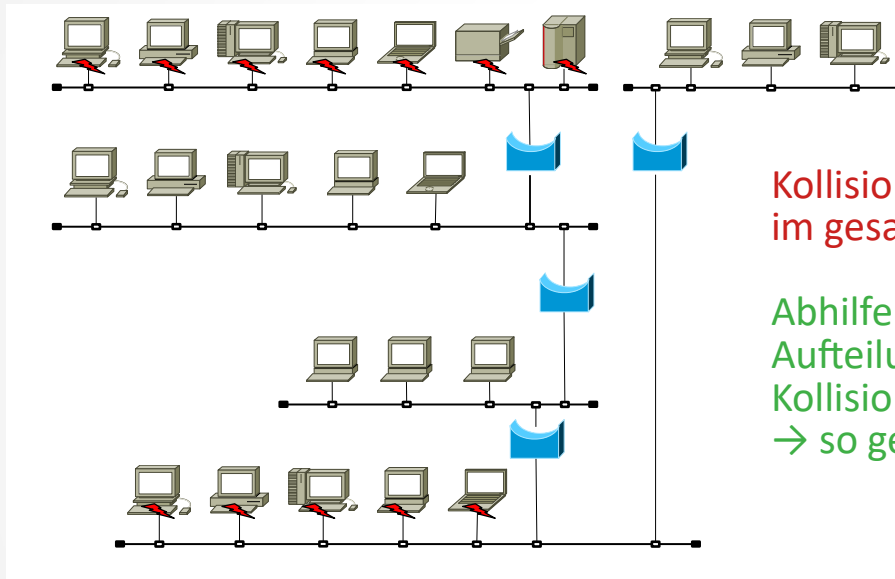
Repeater Teil-5

Repeater-Bauformen:

- Sternkoppler
- Hub
- Media-Konverter
- Switching-Hub

Netzwerk-Komponenten

Brücken Teil-1



Kollisionen treten im Repeaternetz
im gesamten Netzwerk auf.

Abhilfe:
Aufteilung eines Netzwerks in Segmente, in denen eventuelle
Kollisionen gekapselt bleiben
→ so genannte Kollisionsdomänen

Netzwerk-Komponenten

Brücken Teil-2

Damit Brücken ihre Funktion durchführen können müssen sie wissen welcher Netzwerkteilnehmer in welchem Netzwerk-Segment angeschlossen ist.

Dazu beobachten sie den gesamten Datenverkehr in den einzelnen Segmenten und merken sich den Anschlussport (an dem der Frame eingetroffen ist) und die Quell-MAC-Adresse des Frames in einer Tabelle.

Damit dies funktioniert müssen alle Brückenports im Promiscuous-Mode betrieben werden.

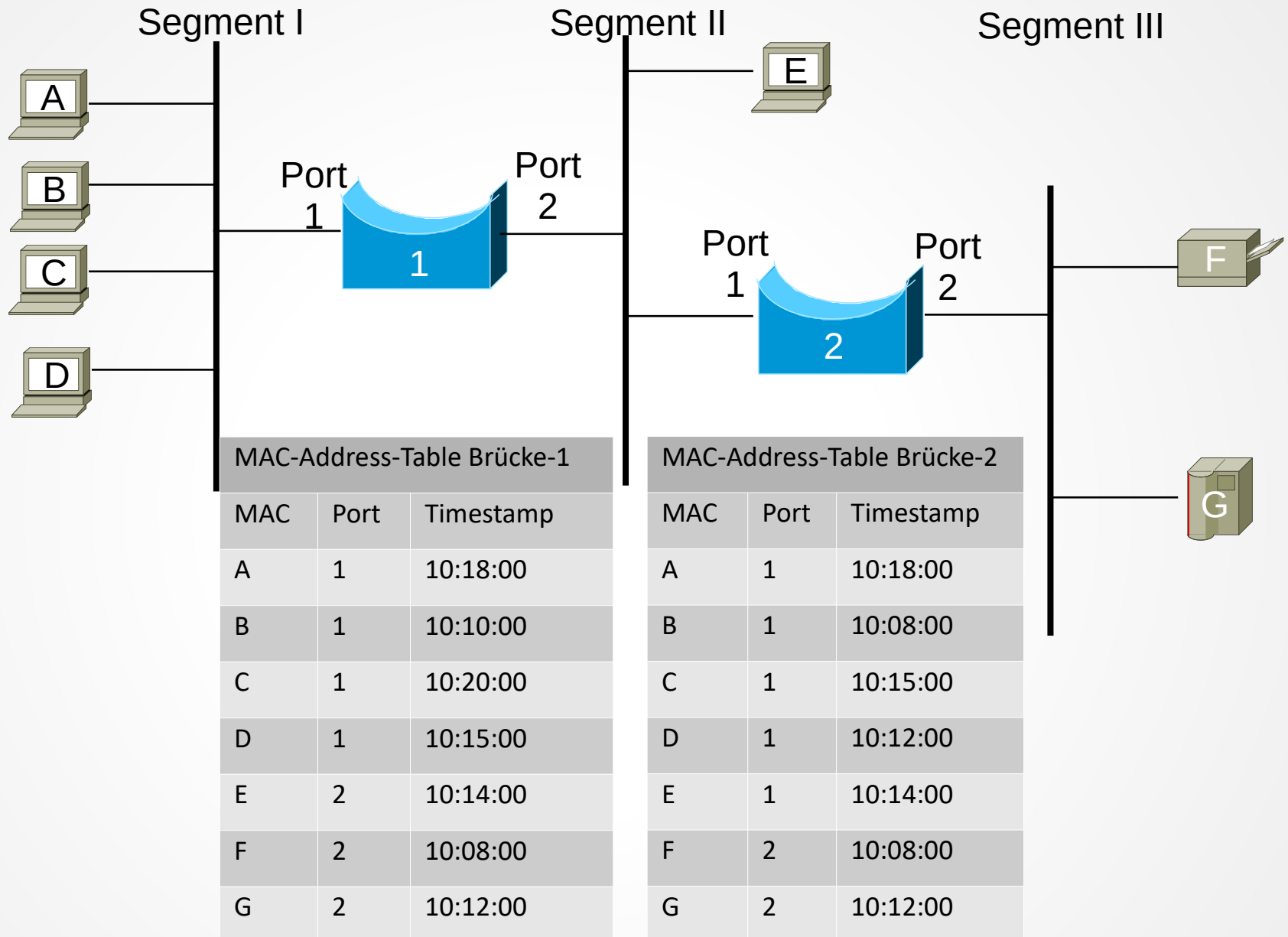
Kommt ein Frame an einem Port an wird die Ziel-MAC-Adresse des Frames untersucht. Und eine Forwarding-Decision getroffen:

- Liegt das Ziel im Netzwerk-Segment aus dem es kam, wird der Frame verworfen.
- Ist das Ziel an einem anderen Port angeschlossen, wird der Frame an diesen Port weiter geleitet.

Hier wird auch klar warum MAC-Adressen eindeutig sein müssen. Ist eine MAC-Adresse an mehreren Ports vorhanden, kann die Brücke keine vernünftige Forwarding-Decision treffen!

Netzwerk-Komponenten

Brücken Teil-3 (Adress-Tabellen)



Netzwerk-Komponenten

Adressbuchverwaltung Brücken Teil-4

Adressbuchverwaltung

- **Dynamisches Adressbuch**

Die MAC-Adressen werden während der Bearbeitung im Selbstlernmodus in einem dynamischen Adressbuch vermerkt. Die Einträge werden nach einem Aging-Mechanismus wieder aus dem Adressbuch entfernt.

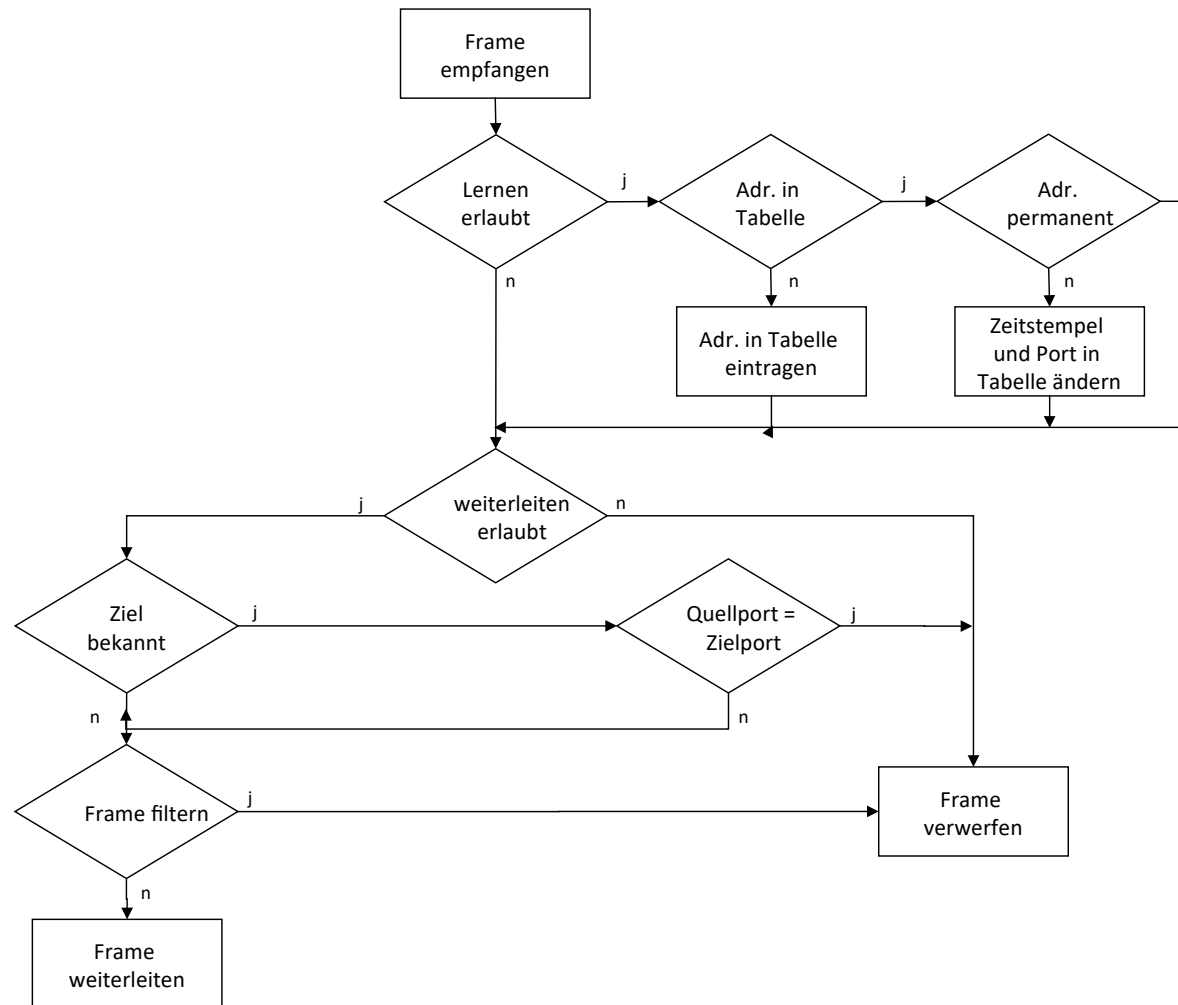
Typische Zeiten sind hierbei 5 Minuten (Cisco). Dies ist auch die Zeit die ein Notebook bei einem Switchport-Wechsel warten muss um wieder erreichbar sein.

- **Statisches Adressbuch**

Für Adressen, die nicht dem Alterungsmechanismus unterliegen sollen, besteht die Möglichkeit von manuellen statischen Einträgen.

Netzwerk-Komponenten

Ablauf der Forwarding-Decision Brücken Teil-5



Netzwerk-Komponenten

Filter Brücken Teil-6

Für den Administrator steht eine Vielzahl von Konfigurationsmöglichkeiten zur Verfügung.
So können Filter parametrisiert werden.
Damit können Rahmen, je nach gesetztem Filter, weiter geleitet, oder verworfen werden.

Es kann auf folgende Rahmenteile gefiltert werden:

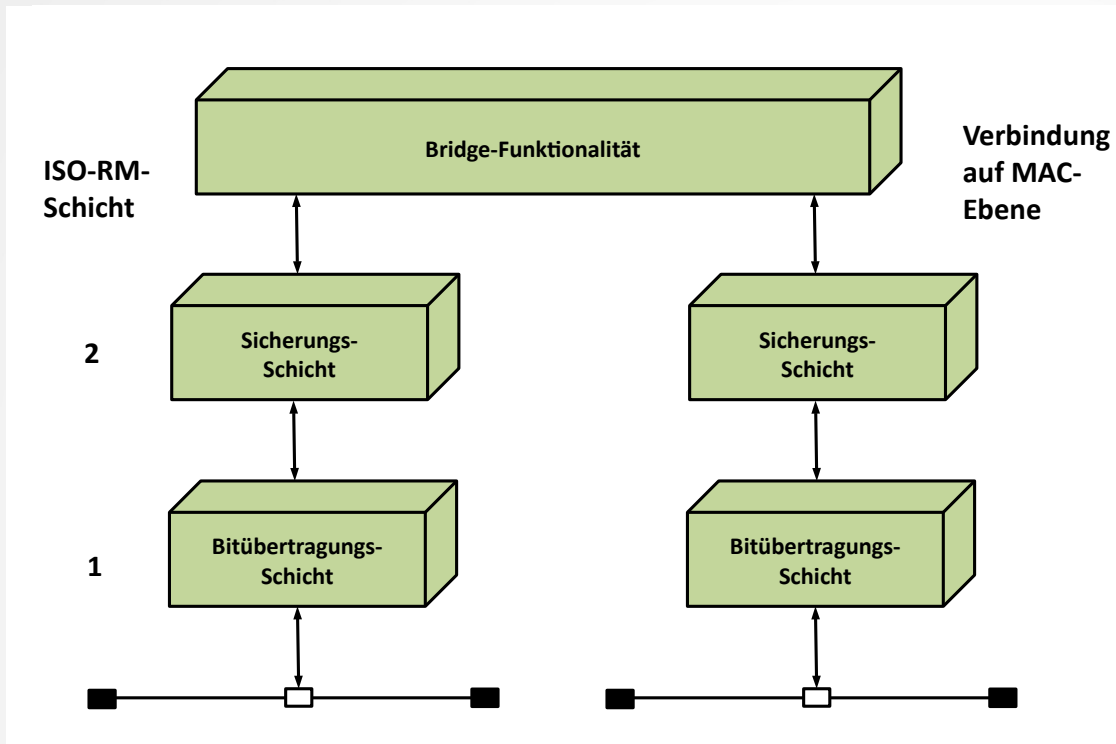
- Dedizierte Ziel-MAC-Adresse
- Dedizierte Quell-MAC-Adresse
- Eine Broadcast-Adresse
- Ein Typfeld
- Eine Maske

Die Filterung kann folgendermaßen erfolgen:

- Positiv mit einer Whitelist (Nur parametrisierte Rahmen werden transportiert)
- Negativ mit einer Blacklist (alle parametrisierten Rahmen werden verworfen)

Netzwerk-Komponenten

Brücken Teil-7 (Brücken im IOS-7-Schichten-Modell)



Brücken arbeiten mit Frames auf Ebene 2 mit den MAC-Adressen.

Die Frames selbst werden nicht verändert sondern nur weiter geleitet oder verworfen.

Deshalb sind Brücken für die Protokolle der höheren Ebenen (≥ 3) Transparent.

In einem Netzwerk dürfen nach IEEE802.1d maximal 7 Brücken verbaut sein um sicher zu stellen, dass die Grenzen der Frame-Laufzeit (max. 7 Sec.) eingehalten werden

Netzwerk-Komponenten

Brücken Teil-8

Probleme in Netzwerken, bei denen eine Brücke hilfreich ist:

- **Das, was schon von Repeatern erledigt werden konnte:**

- ◆ **Längenbegrenzung von Netzwerken**

- Je nach verwendeter Topologie sind die Netzsegmente in ihrer Länge begrenzt. Z. B. bei 10Base2 185 m.

- Bei einer Aufteilung eines Netzwerkes durch eine Brücke in zwei Subsegmente, steht in beiden Subsegmenten wieder die gesamte Längenausdehnung (Entsprechend den definierten Standards) zur Verfügung. Hier bei 10Base2 sind es 370 m.

- ◆ **Begrenzung der Stations-Anzahl**

- In einem Netzsegment ist die Anzahl der möglichen Teilnehmer begrenzt, z. B. 30 in einem 10Base2-Netzsegment.

- Bei einer Aufteilung eines Netzwerkes durch eine Brücke in zwei Subsegmente steht in beiden Subsegmenten wieder die maximale Stations-Anzahl zur Verfügung.
Hier bei 10Base2 sind es 60.

- **Ausbreitung fehlerhafter Pakete**

- Erkennt eine Brücke auf einem Subsegment ein fehlerhaftes Paket, wird es nicht auf das andere Subsegment übertragen. Genauso werden auch Kollisionen auf ein Subsegment begrenzt.

- **Große Netzlast innerhalb eines Netzsegments**

- Da nicht alle Rahmen von einer Bridge übertragen werden, ist die Netzlast in den einzelnen Subsegmenten geringer. Dies ist je nach Datenverkehr (Unicasts, Multicasts und Broadcasts) jedoch nur bedingt wirksam.

- **Kollisionen**

- Kollisionen bleiben bei einer Brücke auf den Port begrenzt an dem die auftreten.

Netzwerk-Komponenten

Brücken Teil-9 (Brückentypen)

Lokale Brücke:

Dieser Brückentyp stellt die Urform der Brücken dar und wurde dazu verwendet ein LAN-Segment in 2 Subsegmente aufzuteilen.

Remote-Brücke:

Remotebrücken verbinden Subsegmente über WAN-Strecken.

Sie treten immer paarweise auf. (Bei erhöhter Verfügbarkeit auch zu viert)

Remotebrücken können sowohl mehrere LAN-Ports als auch mehrere WAN-Ports haben.

Dies kann zur Erhöhung der Verfügbarkeit als auch der Erhöhung der Bandbreite durch Port-Aggregation genutzt werden.

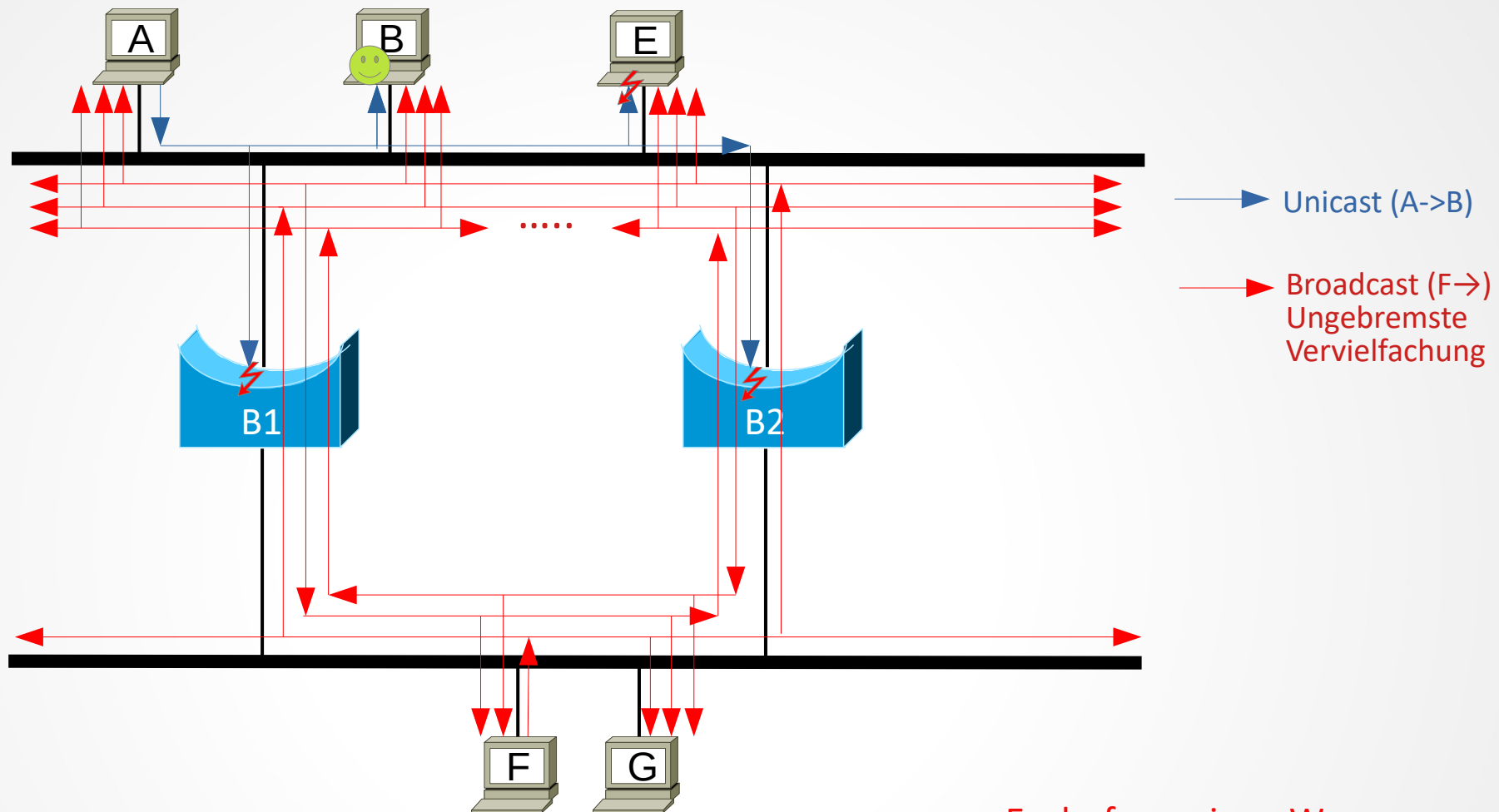
Multiport-Brücke:

Dieser Typ ist eine Weiterentwicklung der Remote-Brücken
(die oft mehr als 2 Ports haben)

Damit können auch mehr als 2 Subsegmente mit einer Brücke erstellt werden.

Netzwerk-Komponenten

Brücken Teil-10 (Redundanz und Zyklenfreiheit)



Es darf nur einen Weg
von a nach g geben!

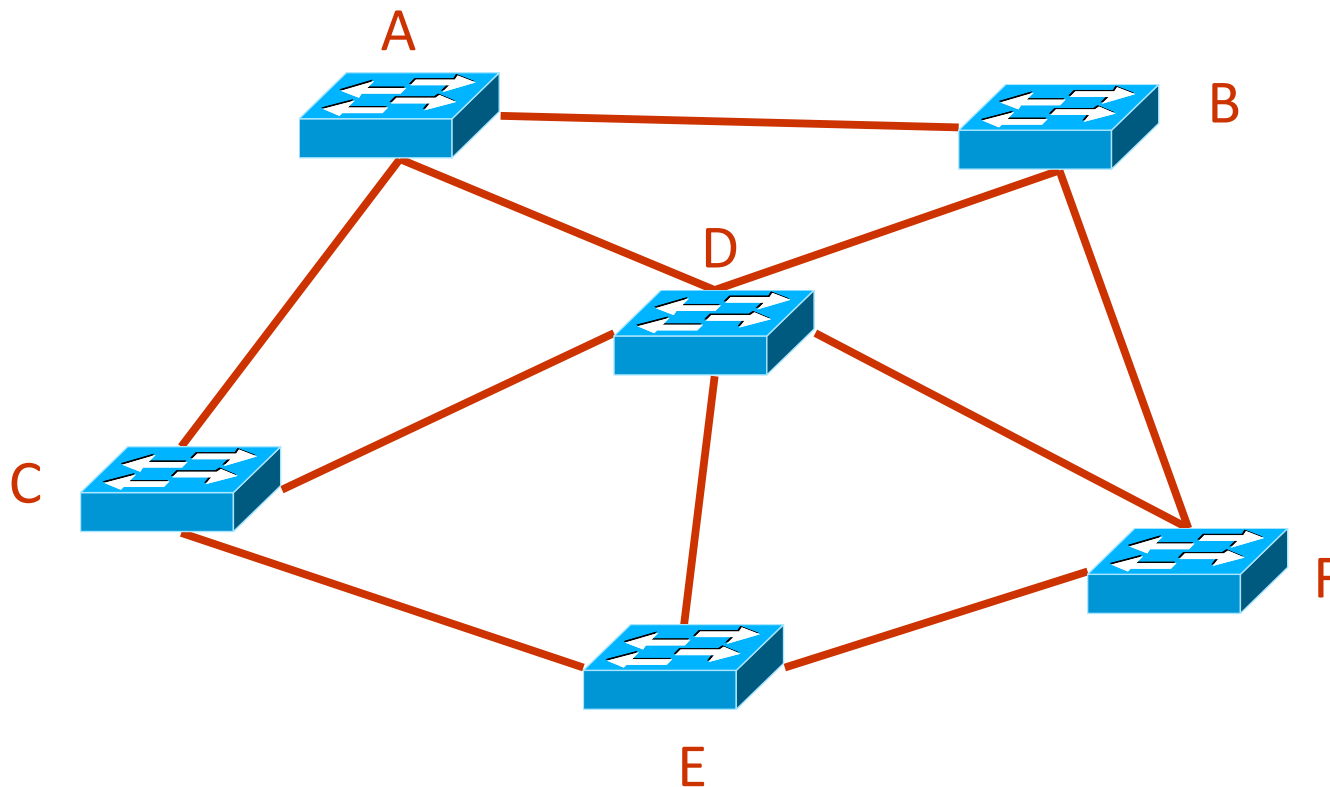
Lösung: Spanning Tree

Netzwerk-Komponenten

Brücken Teil-11 (Spanning Tree-1)

Ausgangs-Zustand:

Netzwerk-Segmente mit 6 Switches

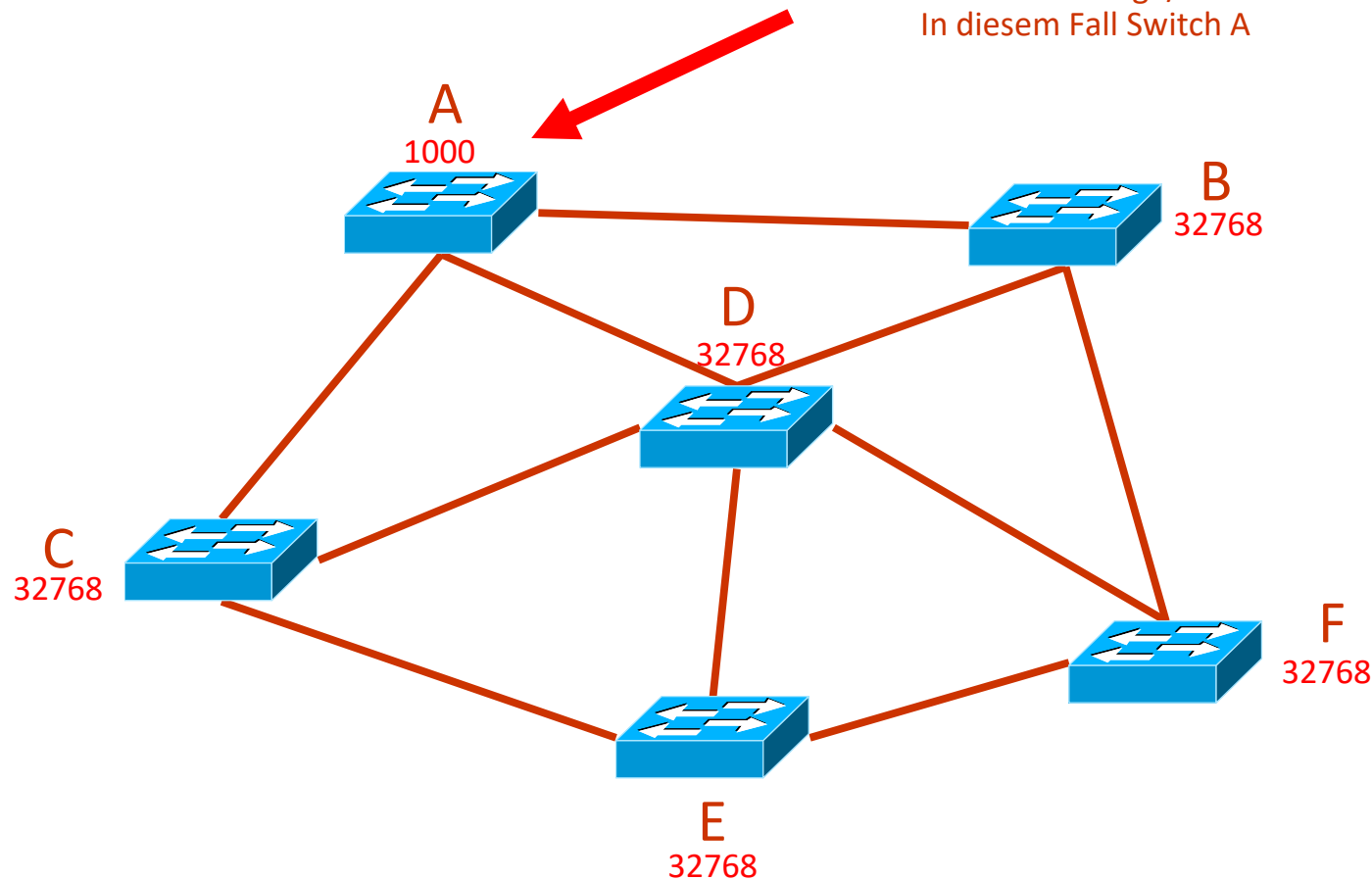


Netzwerk-Komponenten

Brücken Teil-12 (Spanning Tree-2)

Ermitteln des Root-Switches

Um eine hierarchische Struktur zu ermitteln, ist zuerst die Root-Brücke zu ermitteln. Die Brücke/Switch mit der höchsten Priorität wird Root-Bridge/Switch. In diesem Fall Switch A



Netzwerk-Komponenten

Brücken Teil-13 (Spanning Tree-3)

Pfadkosten = 1000/Bandbreitein [Mbps]

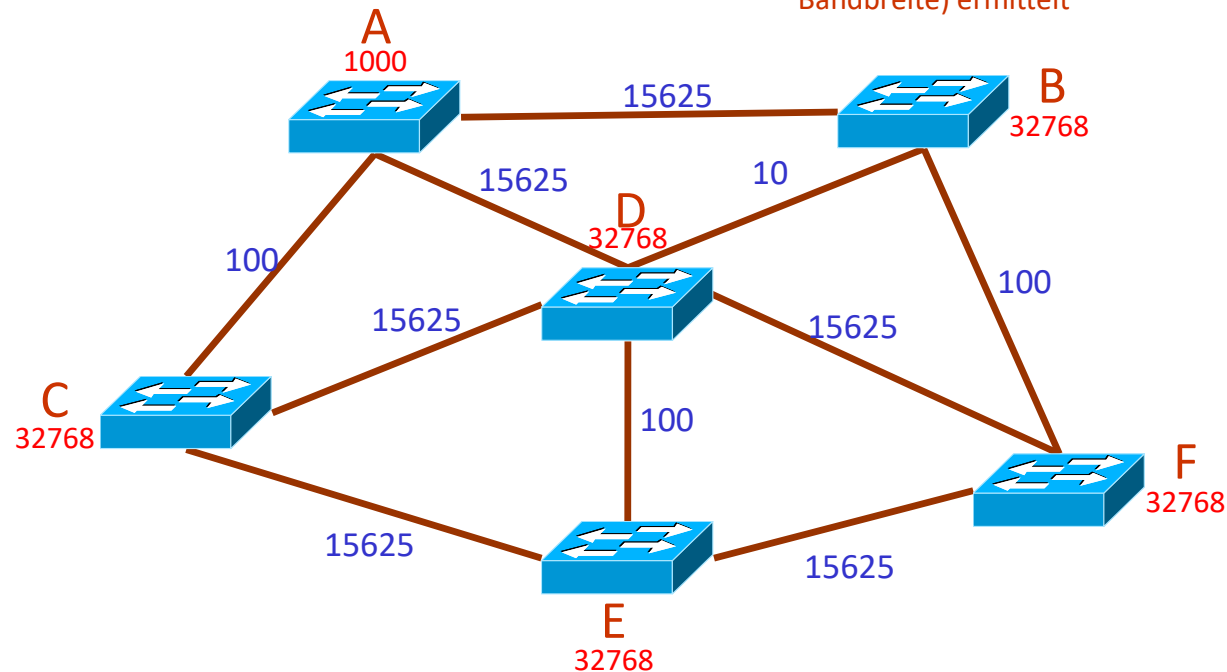
1	= 1000 Mbps Ethernet
10	= 100Mbps Ethernet
100	= 10Mbps Ethernet
250	= 4Mbps Token-Ring
15625	= 64k (ISDN)

Wegeermittlung

Nach dem Festlegen der Root-Bridge werden die Wege ermittelt.

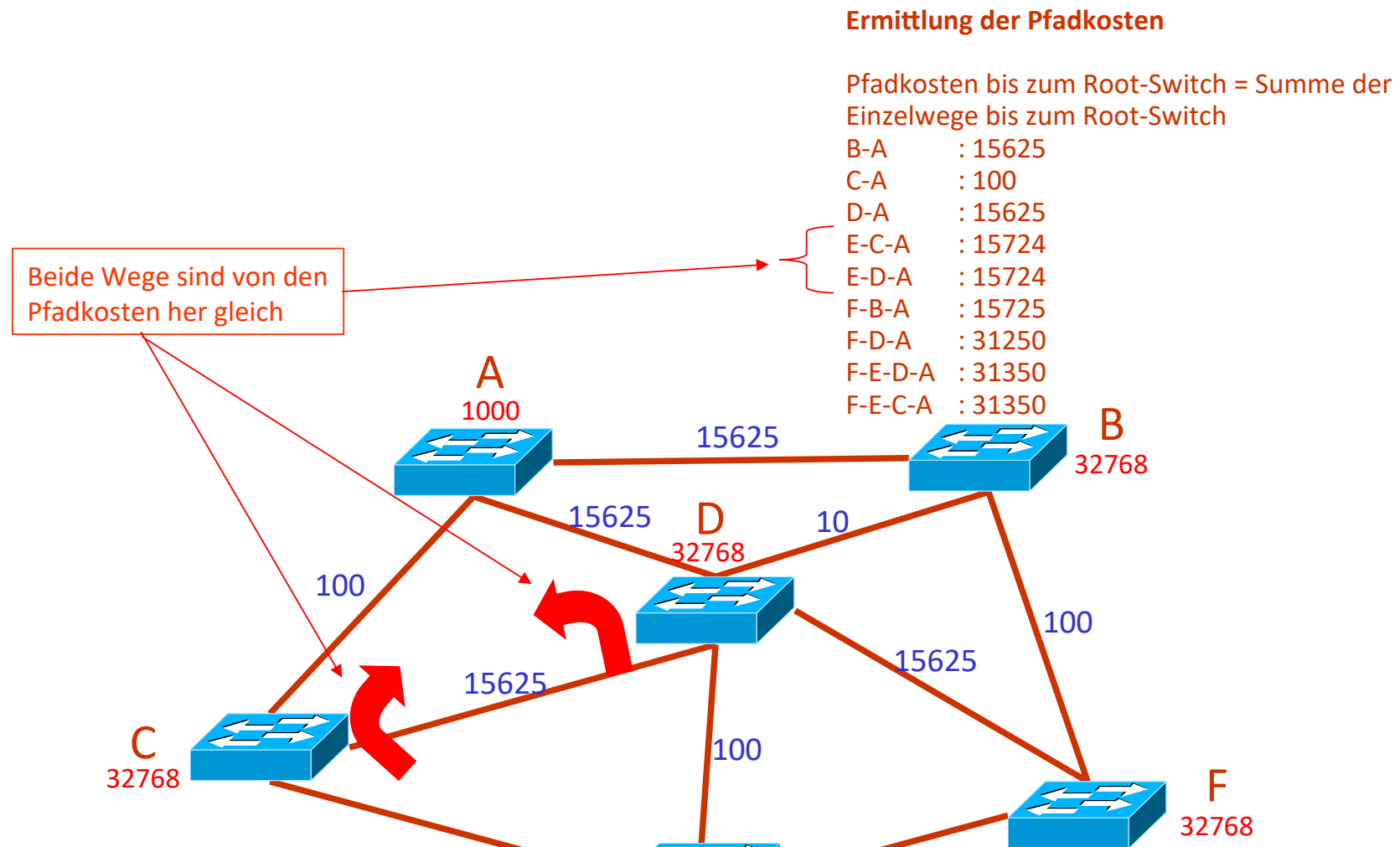
Zuerst müssen alle Switches/Brücken den günstigsten Weg zur Root-Bridge ermitteln

Dazu werden die Pfadkosten (proportional zur Bandbreite) ermittelt



Netzwerk-Komponenten

Brücken Teil-14 (Spanning Tree-4)



Netzwerk-Komponenten

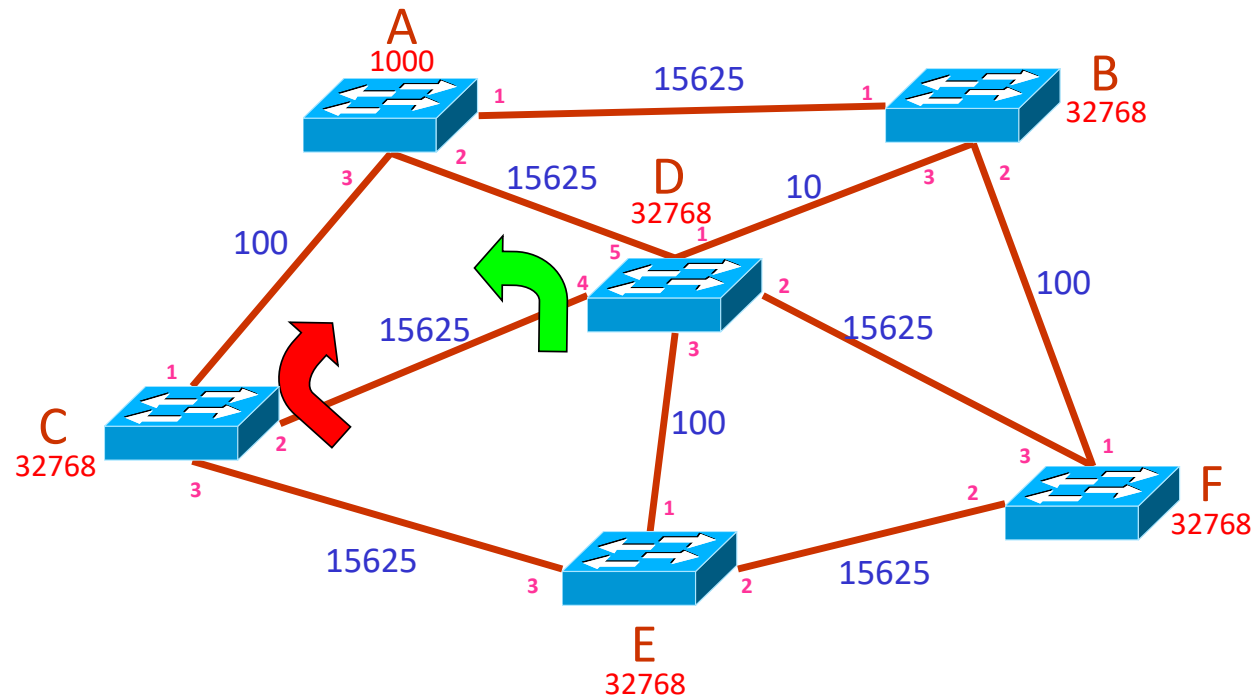
Brücken Teil-15 (Spanning Tree-5)

Die niedrigere Port-ID wird bevorzugt.

Daraus folgt für den Switch E der Pfad: E-D-A

Entscheidung bei gleichen Pfadkosten:

Bei gleichen Pfadkosten entscheidet die PortID



Netzwerk-Komponenten

Brücken Teil-16 (Spanning Tree-6)

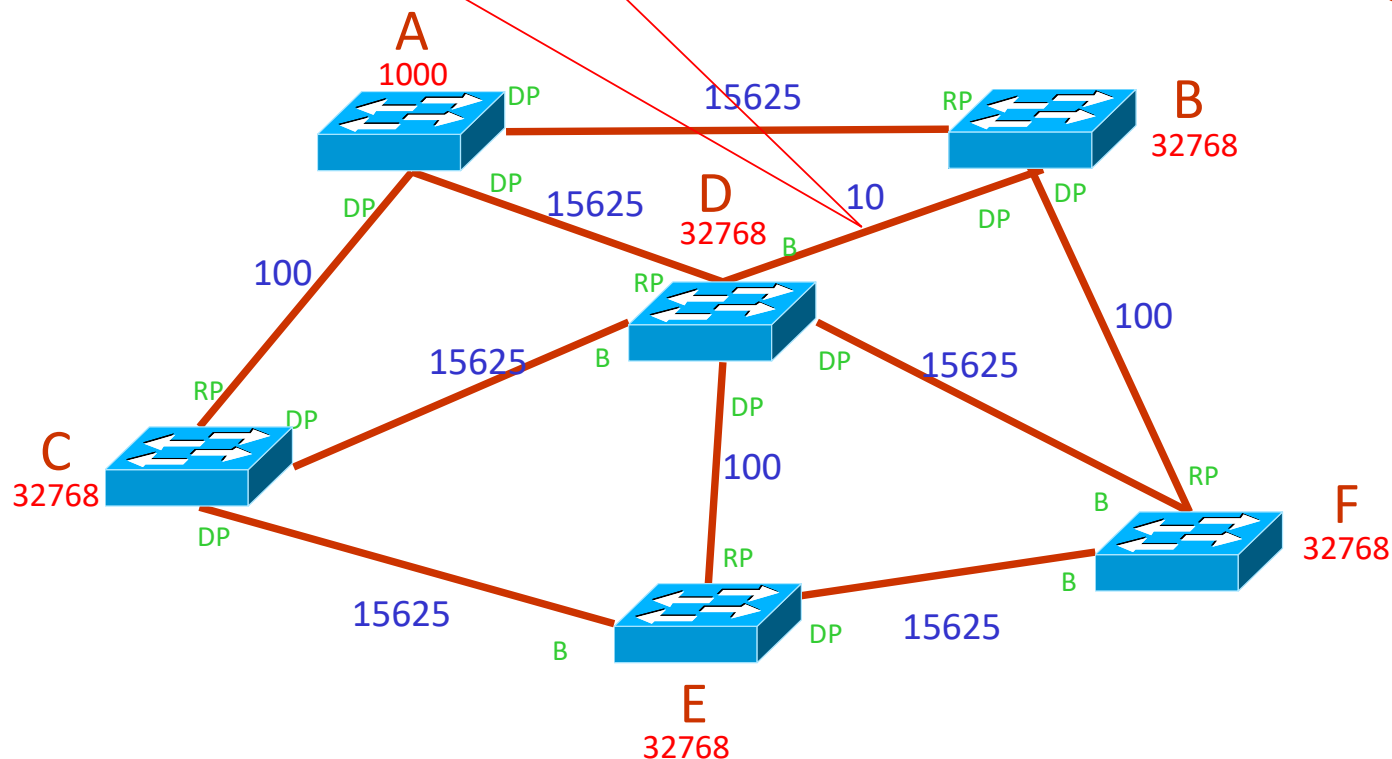
Die Verbindung zwischen D und B ist ein Ethernet-Segment!
Bei der Bestimmung des DP hat B wegen der Bridge-ID den Zuschlag bekommen.
Die in diesem Segment angeschlossenen Geräte senden ihre Pakete über B in andere Segmente

Port-Funktionszuordnung

In einem Switch ist der Port, der als nächster zum Root-Switch führt, der Root-Port (RP)

In jedem Netzwerk ist der Switchport, der zur Root-Switch führt, der designierte Port (DP)

Die anderen Ports sind im Blocking Modus (B)

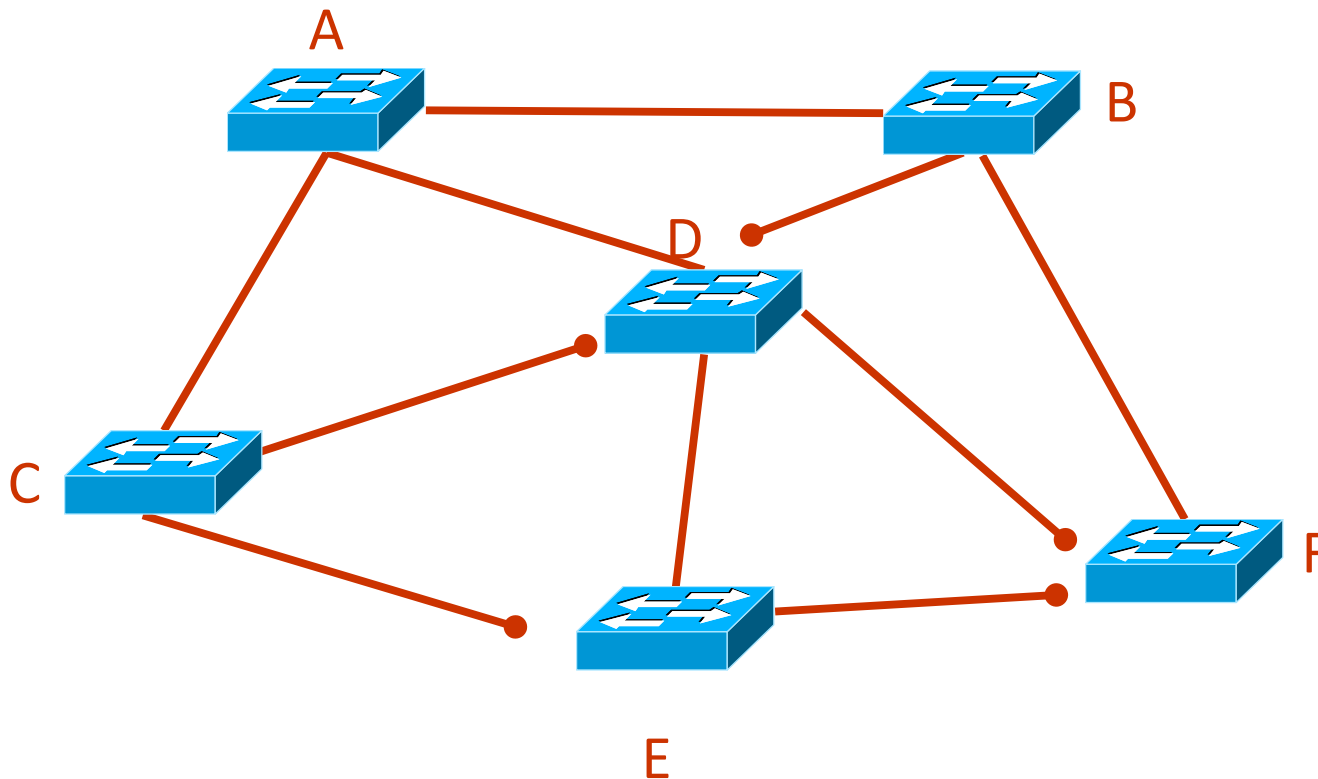


Netzwerk-Komponenten

Brücken Teil-17 (Spanning Tree-7)

Ergebnis:

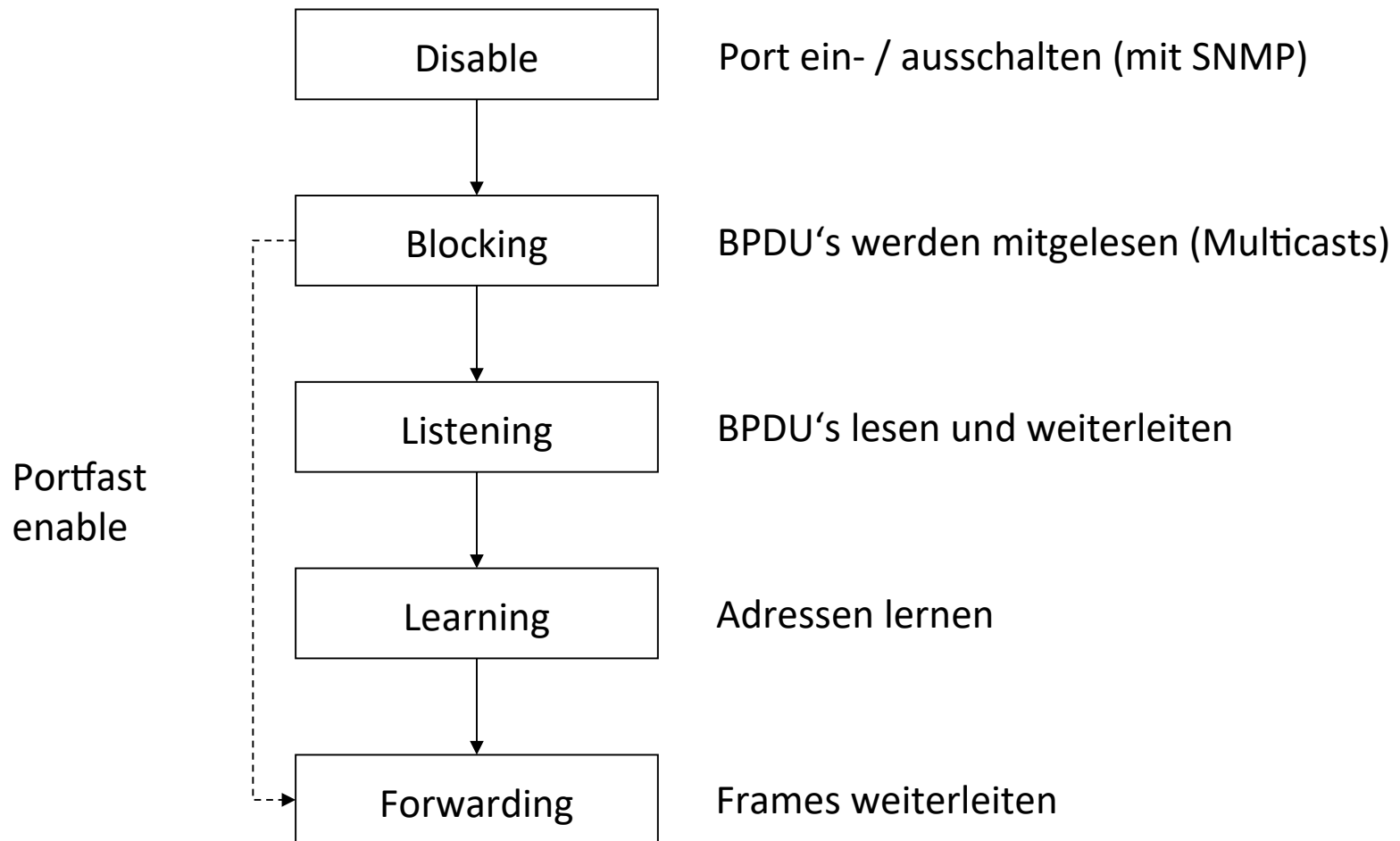
Damit ergibt sich nach dem Ablauf des Spanning-Tree-Algorithmus dieser Aufbau



Netzwerk-Komponenten

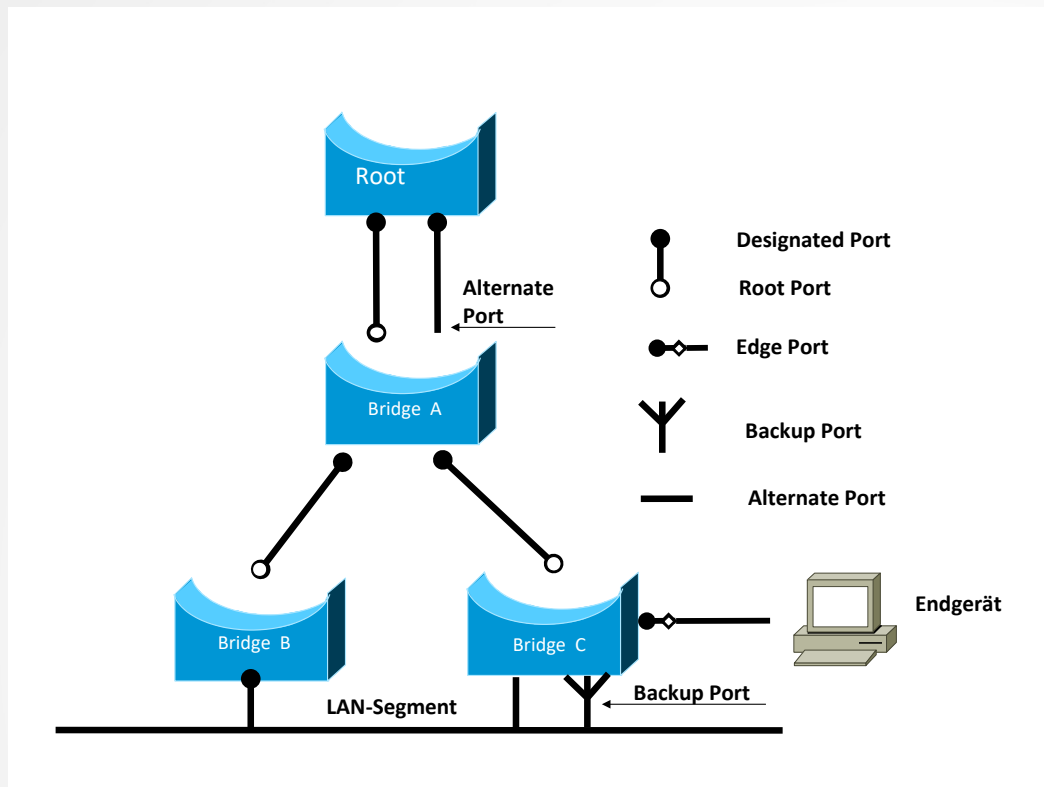
Brücken Teil-18 (Portzustände)

Portzustände beim Spanning Tree



Netzwerk-Komponenten

Brücken Teil-19 (RSTP = Rapid Reconfiguraton Spanning Tree)



Root Port

Der Root Port ist der Port eines Switches der zum Root Switch hin (upstream) aktiv, also im FORWARDING-Modus ist.

Auswahlverfahren:

Kosten zum Root

Port Priorität

Port ID

Designated Port

Der Designated Port ist der Port der downstream (also vom Root Switch weg) bestimmt werden. Es ist der Port der zur Designated Bridge gehört.

Edge Port

Der Edge Port ist ein Port an dem kein Switch mehr angebunden ist.

Alternate Port

Der Alternate Port ist ein Port, der einen Weg zum Root Port weist, jedoch aufgrund des Auswahlverfahrens nicht zum Root Port wurde.

Backup Port

Der Backup Port ist ein Port der wie ein Designated Port arbeiten könnte, jedoch aufgrund des Auswahlverfahrens nicht zum Designated Port wurde.

Netzwerk-Komponenten

Switches Teil-20 (RSTP = Rapid Reconfiguraton Spanning Tree)

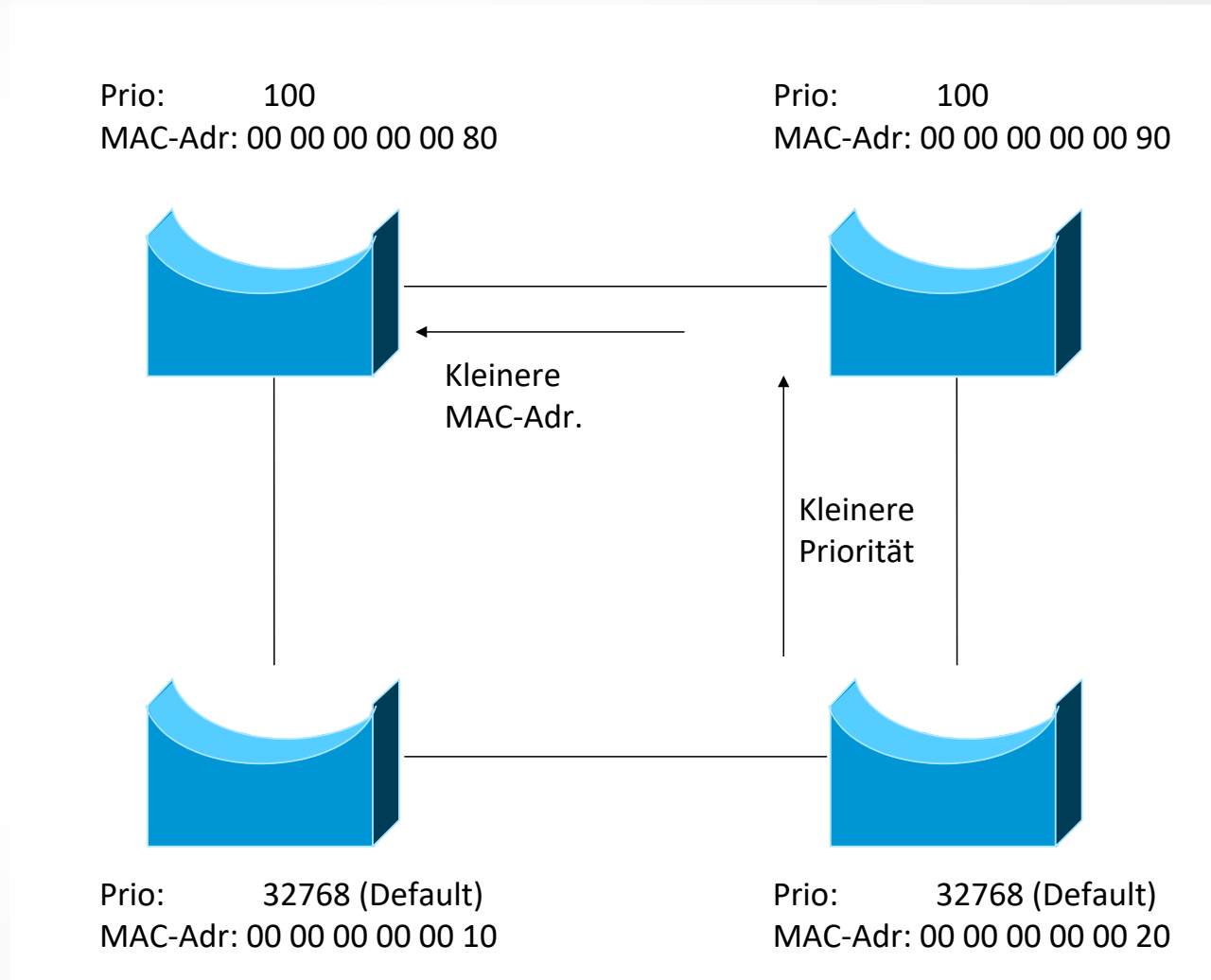
Port Status			
STP	RSTP	Active Topologie	Port Role
Disable	Discarding	Excluded	Disabled
Blocking	Discarding	Excluded	Alternate / Backup
Listening	Discarding	Included	Root, Designated, Edge
Learning	Learning	Included	Root, Designated
Forwarding	Forwarding	Included	Root, Designated, Edge

Netzwerk-Komponenten

Brücken Teil-21 (STP-Übersicht)

Bridge-ID = <Priorität> <MAC-Adresse>

Die Priorität ist per Default 32768



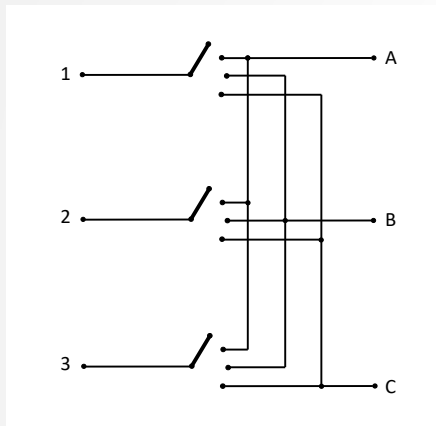
Netzwerk-Komponenten

Switches Teil-1 (Typen)

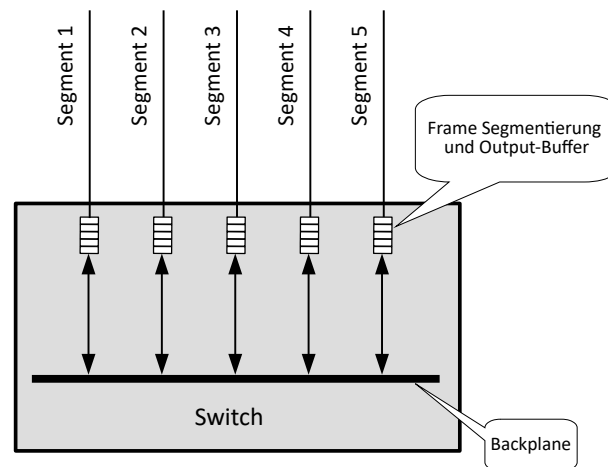


Switches entsprechen, von ihrer Funktionalität her, Multiport-Brücken. Brücken nutzen die CPU, um die Wegewahl der Rahmen durchzuführen.

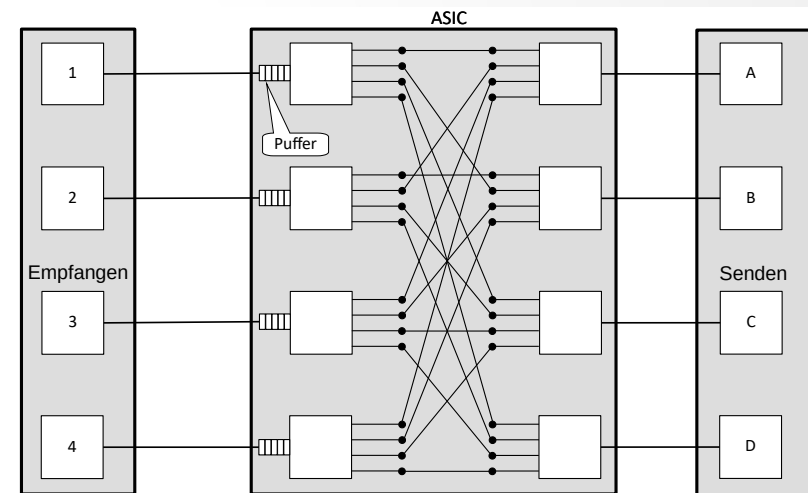
Bei Switches ist die Wegewahl in ASIC's (Application Specific Integrated Circuit), also in Hardware, realisiert.



Koppelfeld-Prinzip



Cell-Backplane-Switch



Matrix-Switch

Netzwerk-Komponenten

Switches Teil-2 (Strategien)

Store & Foreward

Frames werden komplett untersucht und gespeichert. Danach erfolgt die Forwarding-Entscheidung und der Frame wird auf den Ausgangsport geschaltet. Damit können fehlerhafte Frames anhand der CRC-Bearbeitung erkannt und aussortiert werden. Dies ist das sicherste, jedoch aber auch langsamste Verfahren.

Cut Through

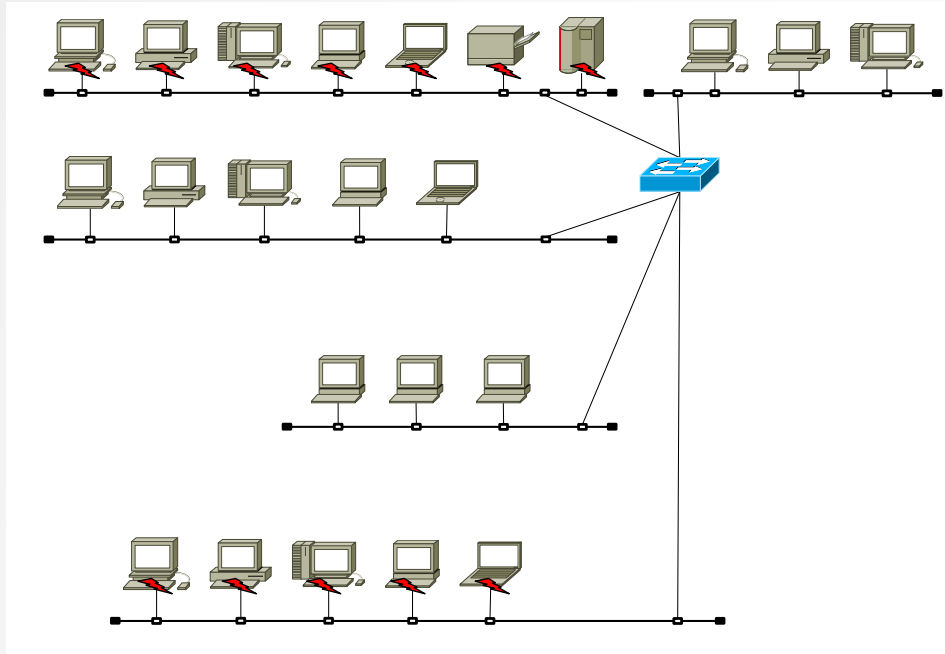
Sobald die Ziel-MAC-Adresse erkannt wurde wird der Frame auf den Ausgangsport weiter geleitet. Damit können jedoch fehlerhafte Frames nicht erkannt und aussortiert werden. Dies ist das unsicherste, jedoch auch das schnellste Verfahren.

Cut Through Collision Free

Frames werden während des Empfangs der ersten 64 Bytes auf eine Kollision hin untersucht und, falls bis dahin kein Fehler aufgetreten ist, auf den Ausgangsport weiter geleitet. Damit können fehlerhafte Frames nicht erkannt und aussortiert werden. Dies ist ein Kompromiss zwischen dem Cut Through- und Store & Forward-Verfahren.

Netzwerk-Komponenten

Switches Teil-3 (Layer-2)

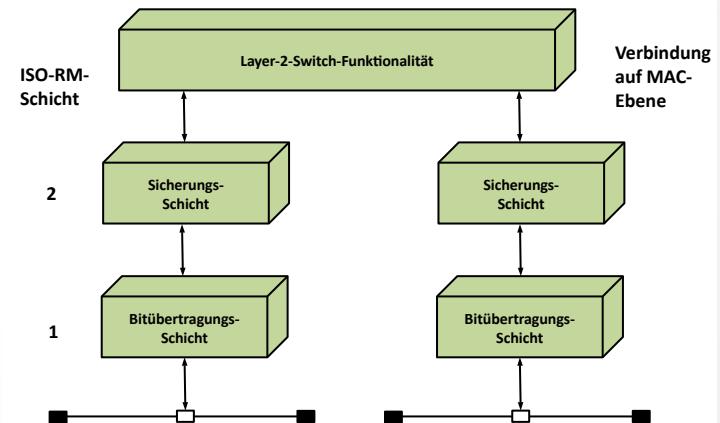


Alle Funktion und Randbedingungen wie bei den Brücken gelten hier auch!

Besonders

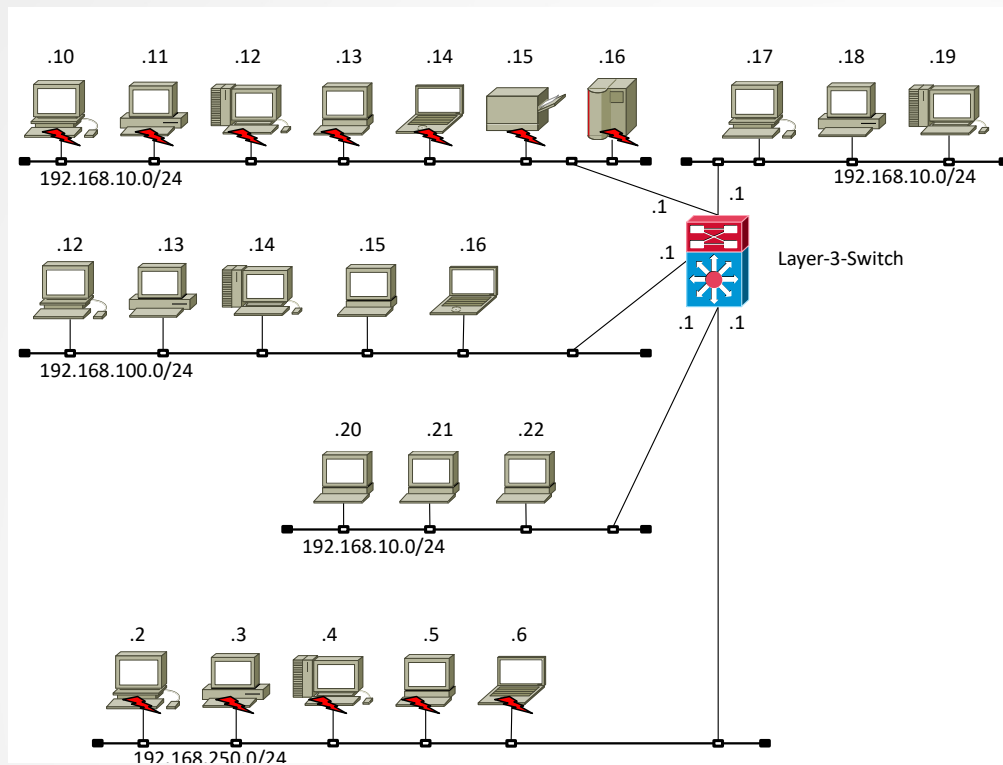
- **Kollisionen** bleiben auf das Segment begrenzt in dem sie auftreten
- **Unicasts** werden nur weiter geleitet, wenn das Ziel in einem anderen Segment liegt.
- **Multicasts und Broadcasts** werden an allen Ports weiter geleitet.

Ein Frame wird bis auf die Ebene 2 entpackt um mit der MAC-Adresse die Forwarding-Entscheidung zu treffen



Netzwerk-Komponenten

Switches Teil-4 (Layer-3 und höher)

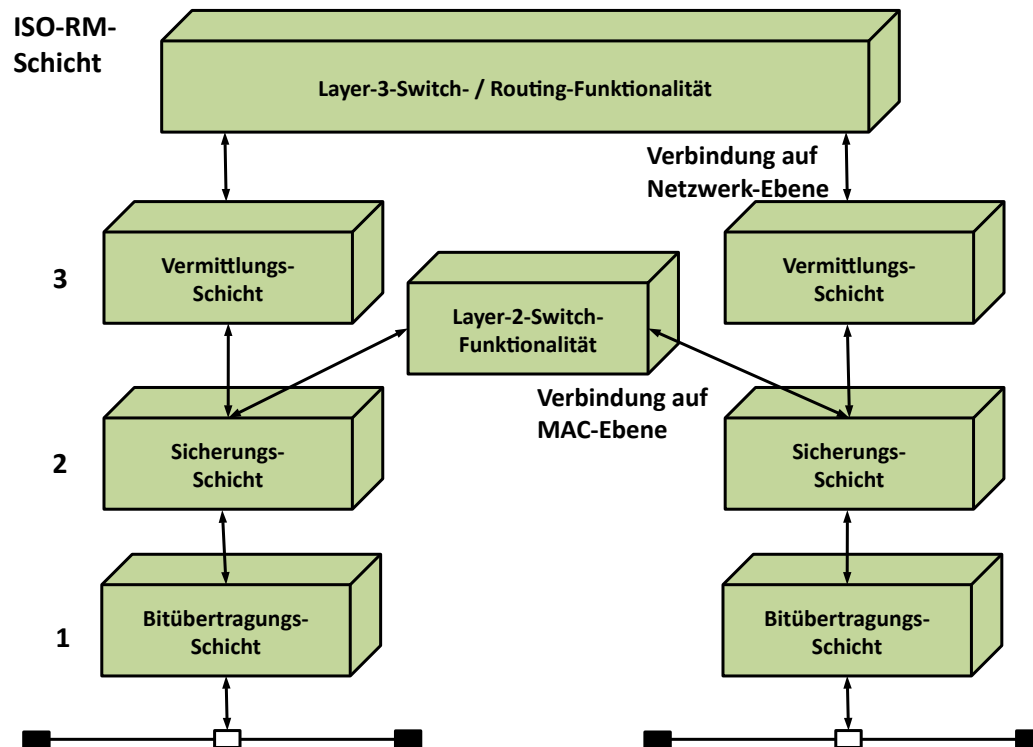


Vor allem wenn die Physik sich nicht ändert
kann ein Switch auch die Funktionalität
höherer Schichten (z. B. Routing der Ebene 3)
Übernehmen

Dies geht bis zur Ebene 7 (bei der die Applikation
die Wege-Entscheidung beeinflusst)

Netzwerk-Komponenten

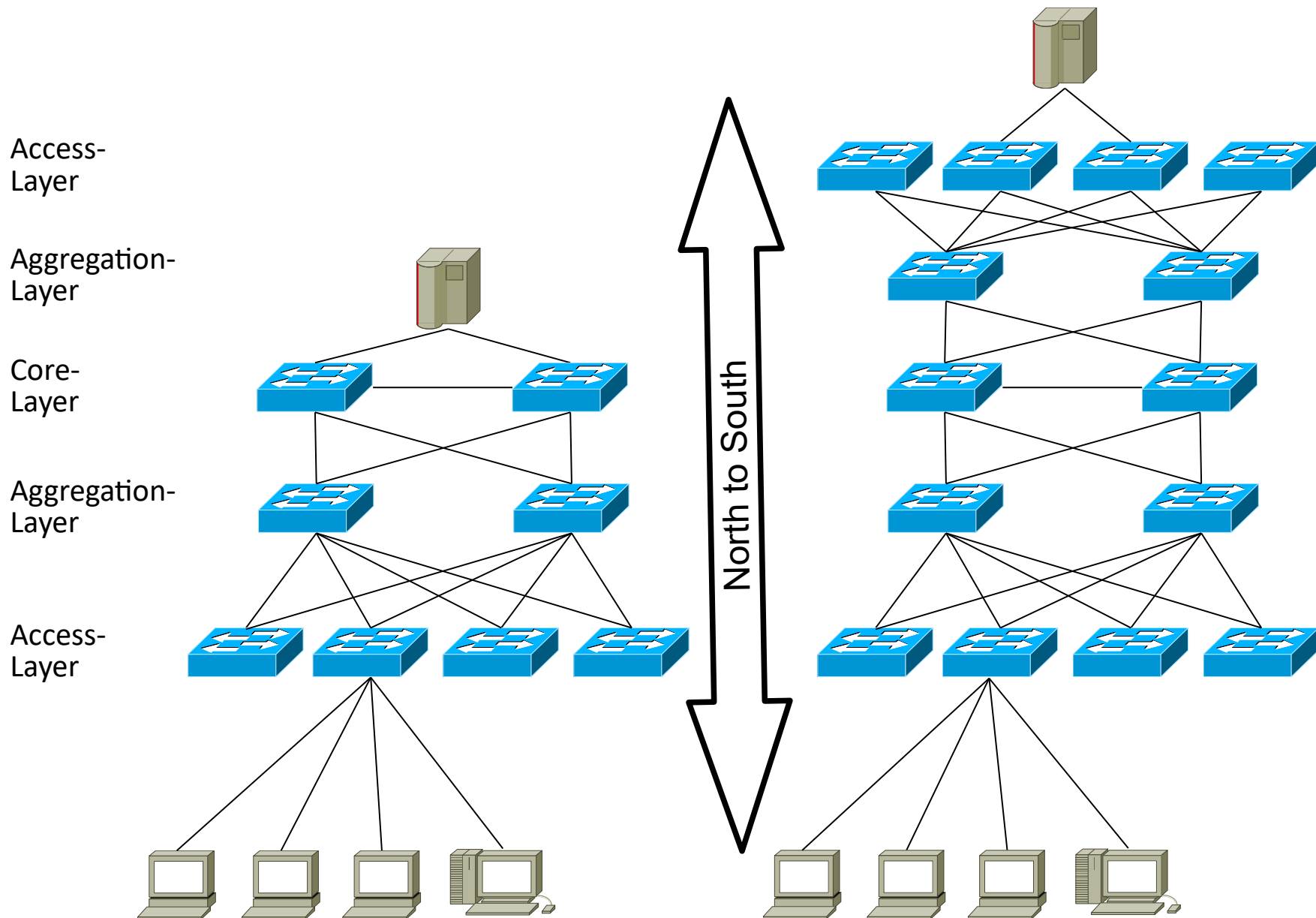
Switches Teil-5 (im ISO-7-Schichten-Modell)



Verfahren	
Layer-3-Switching	Überall routen
Layer-3-Cut-Through-Switching	Einmal routen danach switchen
Layer-2/3-Switching	Switchen wo möglich Routen wo unumgänglich
Layer-2-Switching	Überall switchen

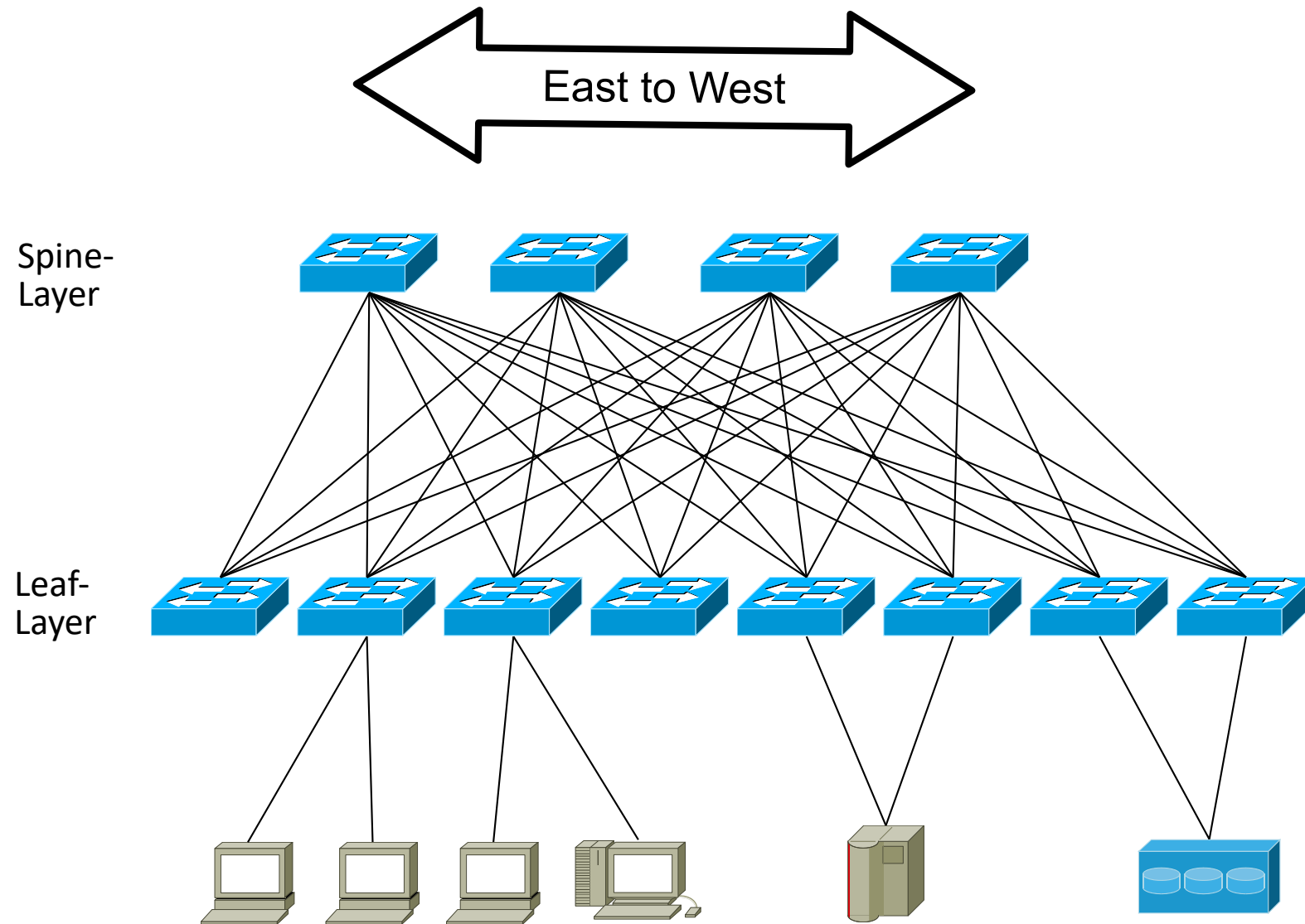
Netzwerk-Komponenten

Switches Teil-6 (Layer-2-Netzwerke)



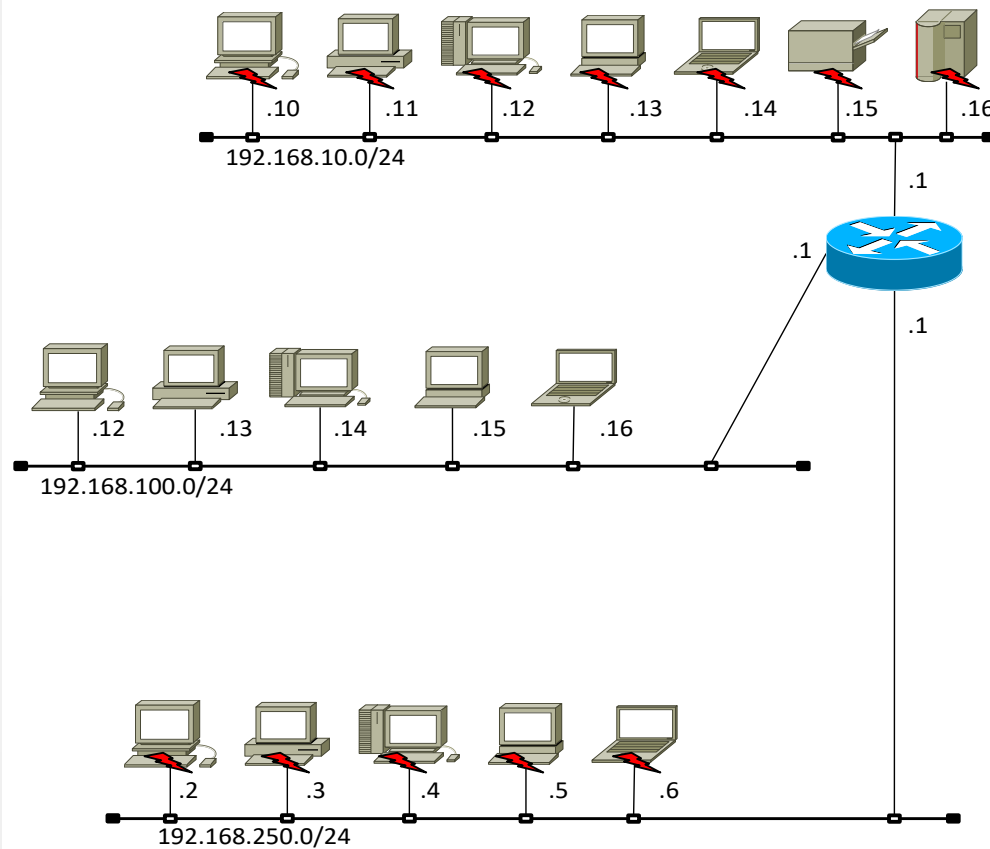
Netzwerk-Komponenten

Switches Teil-7 (Layer-2-Netzwerke)



Netzwerk-Komponenten

Router Teil-1



Router arbeiten auf ISO-RM-Ebene 3 (Netzwerk-Schicht) und verbinden somit zwei Netzwerke miteinander. Dafür haben Router eine Schnittstelle und eine Adresse in jedem Netzwerk

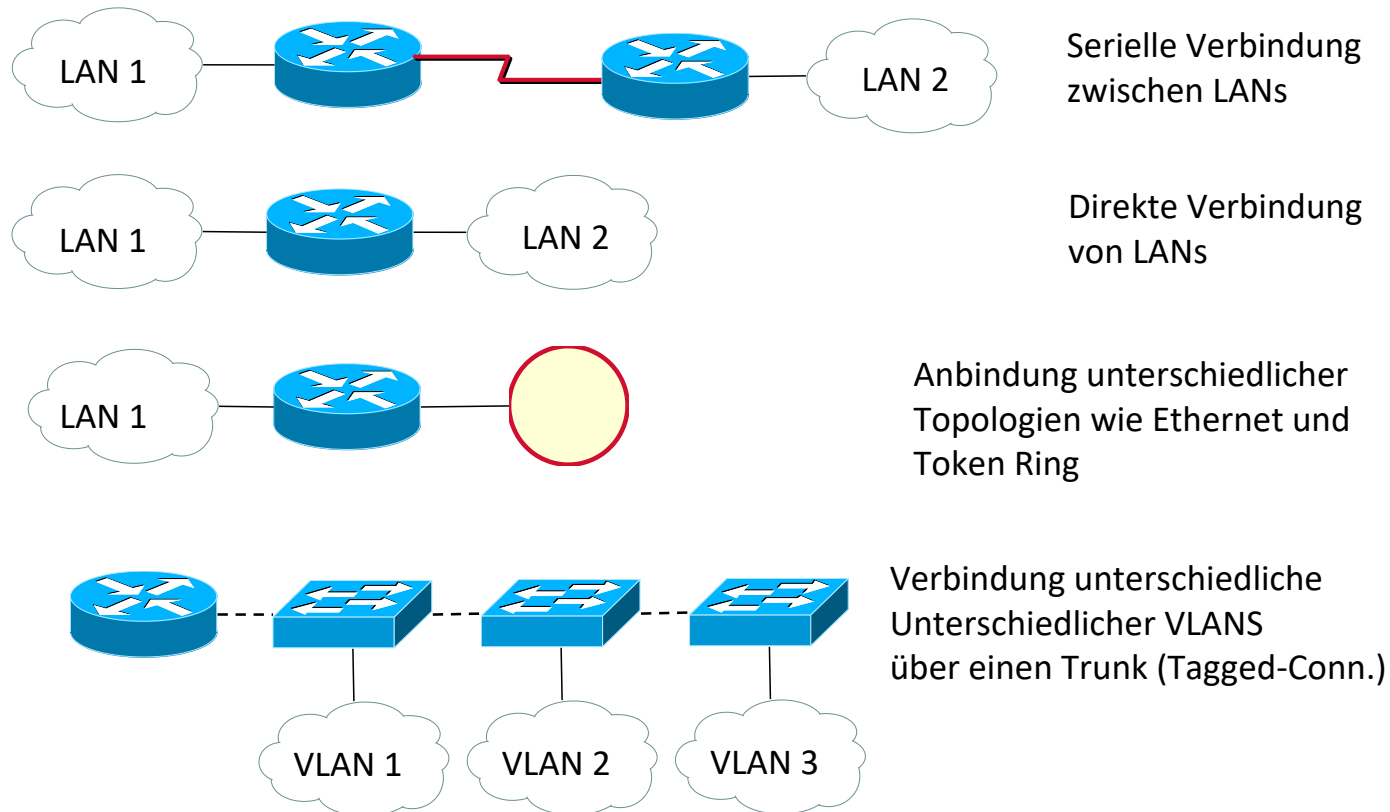
Broadcasts werden auf ISO-RM-Ebene 2 abgehandelt und werden von Routern somit nicht weitergeleitet.

Kollisionen werden auf ISO-RM-Ebene 1 abgehandelt und werden von Routern ebenfalls nicht weitergeleitet.

Somit begrenzen Router sowohl Broadcast- als auch Kollisions-Domänen.

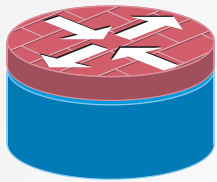
Netzwerk-Komponenten

Router Teil-2 (Verbindung unterschiedlicher Topologien)

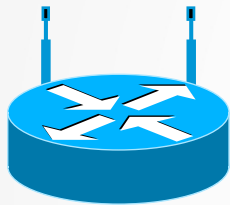


Netzwerk-Komponenten

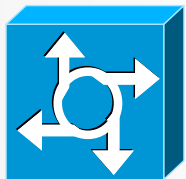
Router Teil-3 (Zusätzliche Funktionen)



Router können noch weitere Funktionen beinhalten.
So ist z. B. Eine Firewall in vielen Routern im SOHO-Bereich anzutreffen.



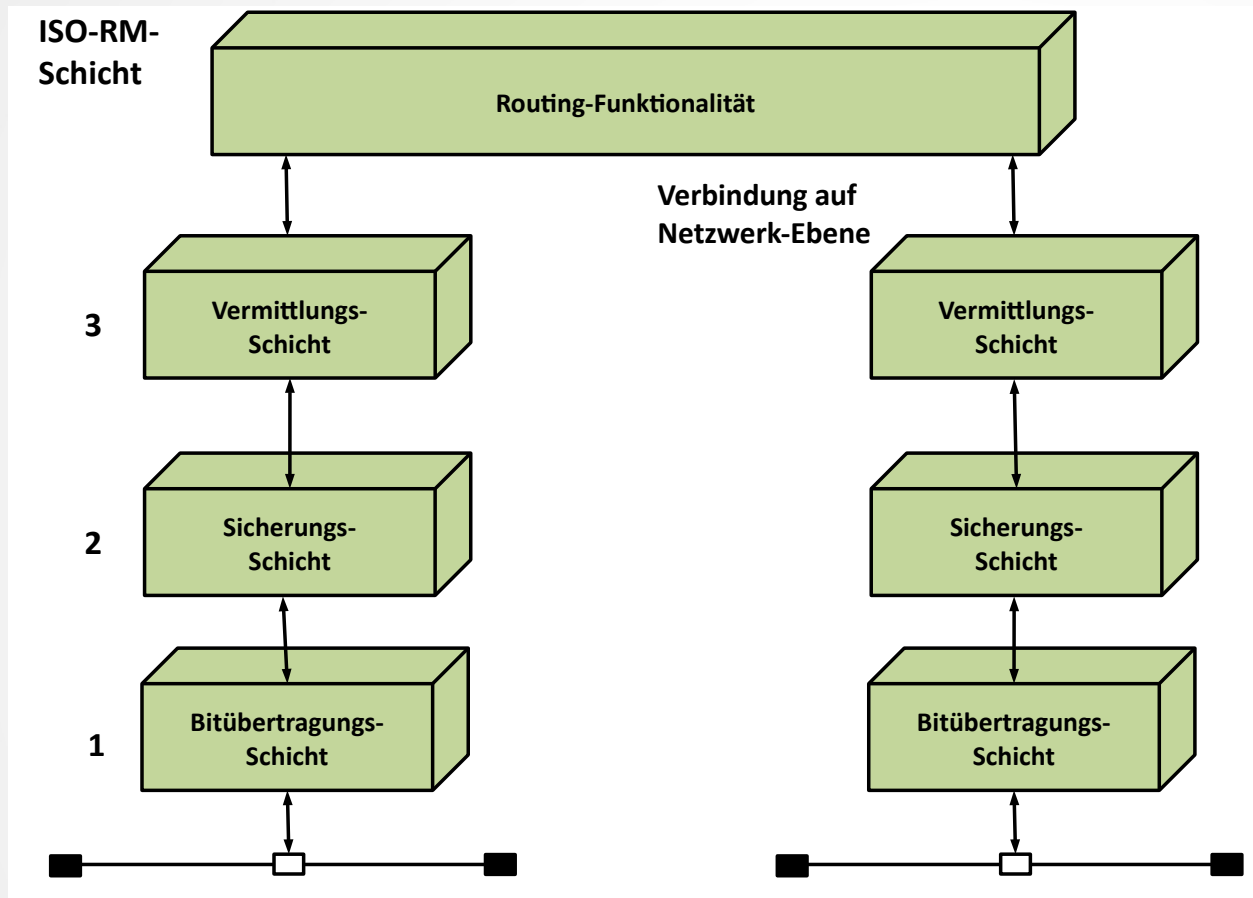
Router im SOHO-Bereich haben oft auch eine WLAN-Schnittstelle



Ist ein Router für eine Anbindung des Firmen-Ethernet an verschiedene Topologien wie ISDN oder analoge Leitung zuständig, spricht man auch von einem ACCESS-Server.

Netzwerk-Komponenten

Router Teil-4 (im ISO-7-Schichten-Modell)



Ein Paket ist bis auf die Ebene 3 zu entpacken, um mit der IP-Adresse, die Forwarding-Entscheidung zu treffen

Behandlung von Frames

- **Kollisionen** bleiben auf das Netzwerk begrenzt in dem sie auftreten.
- **Unicasts** werden nur weiter geleitet, wenn das Ziel in einem anderen Netzwerk liegt.
- **Multicasts und Broadcasts** bleiben auf das Netzwerk begrenzt in dem sie auftreten.

Netzwerk-Komponenten

Router Teil-5 (im Zusammenhang mit Protokollen)

Es gibt sowohl **routebare Protokolle**, als auch **Routingprotokolle**.

Bei den routebaren Protokollen handelt es sich um Protokolle, die von Routern weitergeleitet werden können.

Bei den Routingprotokollen handelt es sich um die Protokolle, welche die Router untereinander zur Abwicklung ihres Routing-Auftrages benützen. Dabei werden Informationen, wie z. B. Routingtabellen, dynamisch ausgetauscht. Damit können die Router auf Veränderungen der Netzwerk-Struktur, wie z. B. den Ausfall eines Routers, reagieren.

Routingprotokolle

- BGP (Border Gateway Protocol)
- HSRP (Hot Standby Router Protocol)
- IGRP/EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)

Routebare Protokolle

- IP (Internet Protocol)
- IPX (Internet Paket Exchange)
- OSI (Open Systems Interconnection)
- Apple Talk (Kommunikation zwischen Apple-Rechnern)

Nicht routebare Protokolle

(sind nicht routebare Protokolle, da sie auf Ebene 3 keine Informationen für die Vermittlung zur Verfügung stellen)

- NetBIOS
- NetBEUI
- LAT

Netzwerk-Komponenten

Router Teil-6 (Funktionsweise-1)

Routing-Tabelle PC1

Ziel	FLAG	Next Hop	Interface	Metrik
Default 0.0.0.0	AG	R1	N1-Adr	100
Selbst 127.0.0.0	A		Localhost 127.0.0.1	150
N1	A		N1-Adr	25

Routing-Tabelle R1

Ziel	FLAG	Next Hop	Interface	Metrik
N1	A		e0	25
N2	A		e1	25
N3	AG	R2	e1	100
N3	AG	R3	e1	200
N4	AG	R3	e1	100
N5	AG	R4	e1	100
S1	AGH	R2	e1	100
Default	AG	R3	e1	100

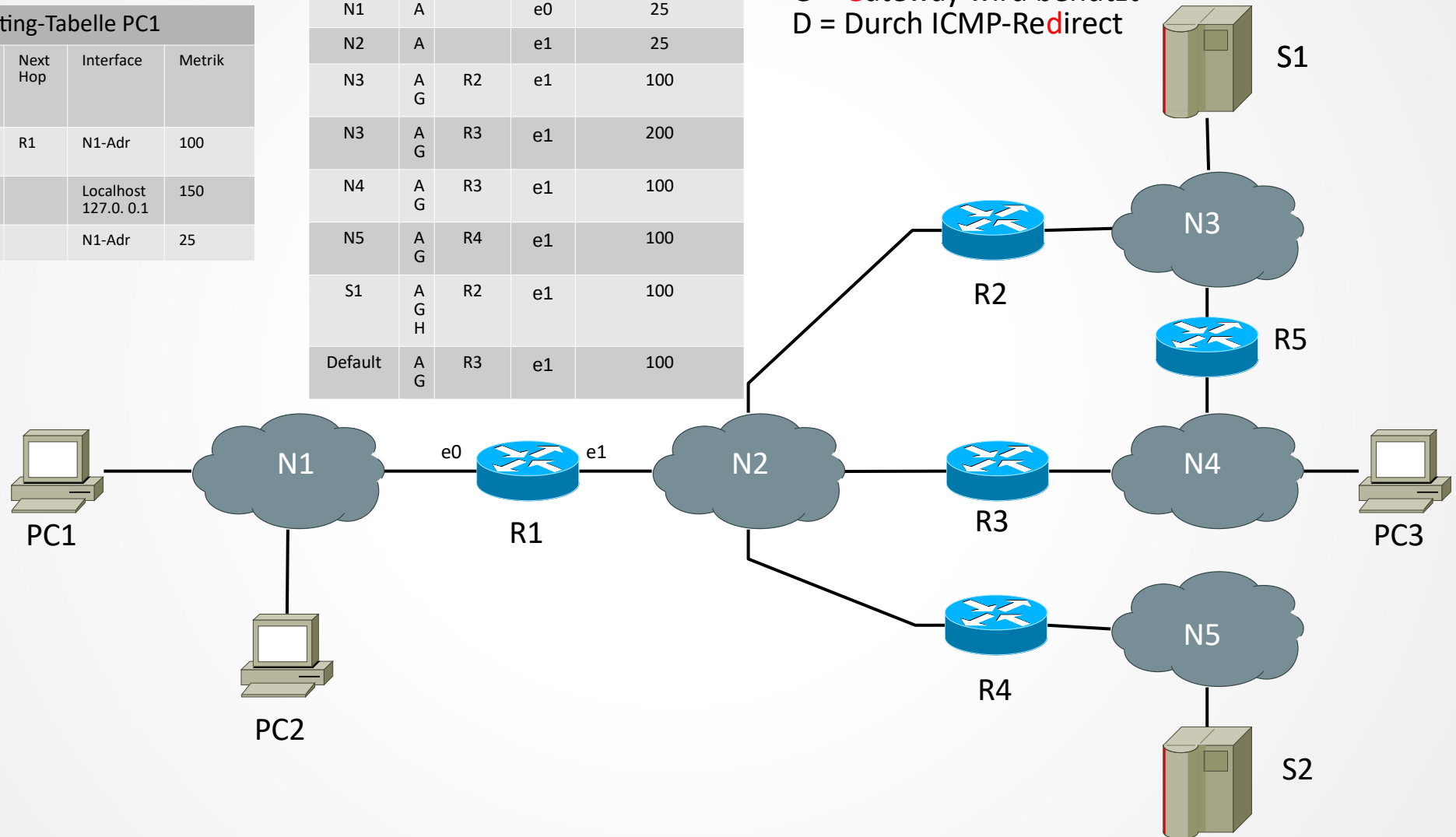
Flags:

U/A = In Use / Aktiv

H = Route führt direkt zum Host (Hostroute)

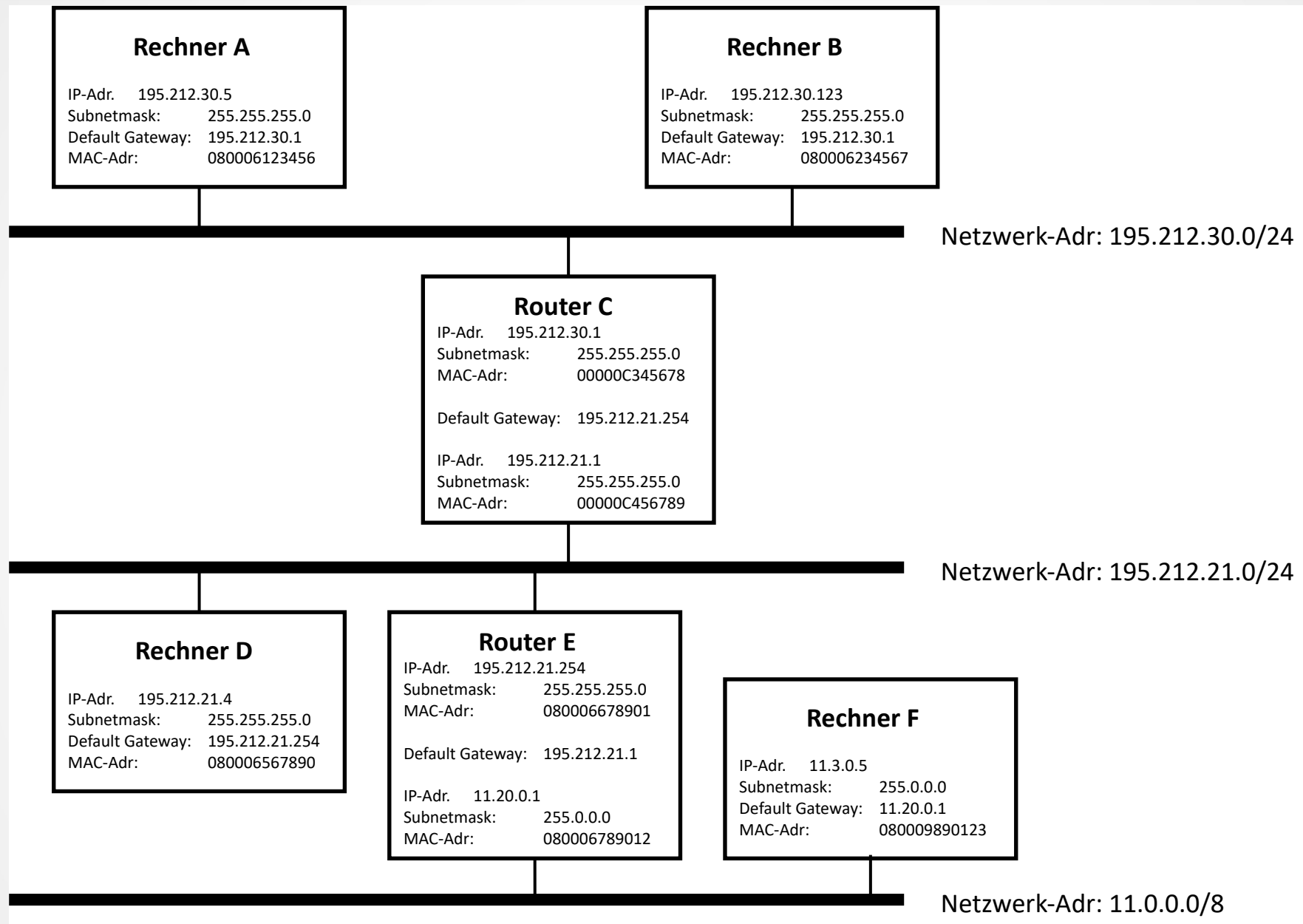
G = Gateway wird benutzt

D = Durch ICMP-Redirect



Netzwerk-Komponenten

Router Teil-6 (Funktionsweise-2)



Netzwerk-Komponenten

Router Teil-8 (Funktionsweise-3)

A -> B

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006234567	0800006123456	0x800	195.212.30.123	195.212.30.5

A -> D

A -> C

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
00000C345678	0800006123456	0x800	195.212.21.4	195.212.30.5

C -> D

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006567890	00000C456789	0x800	195.212.21.4	195.212.30.5

A -> F

A -> C

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
00000C345678	0800006123456	0x800	11.3.0.5	195.212.30.5

C -> E

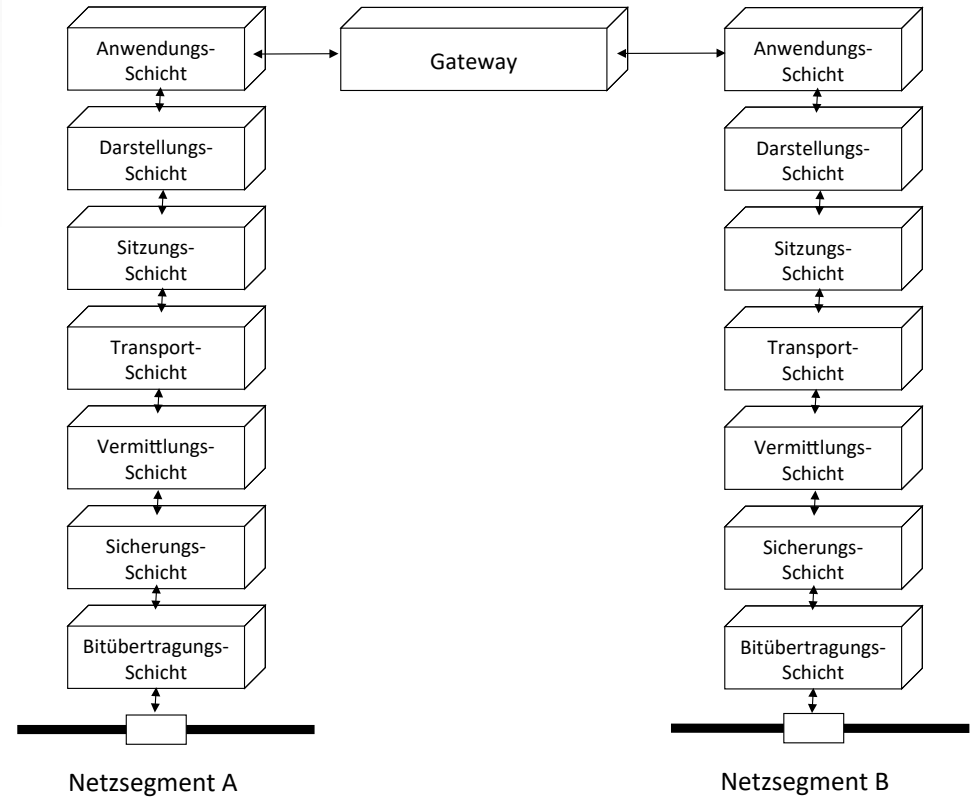
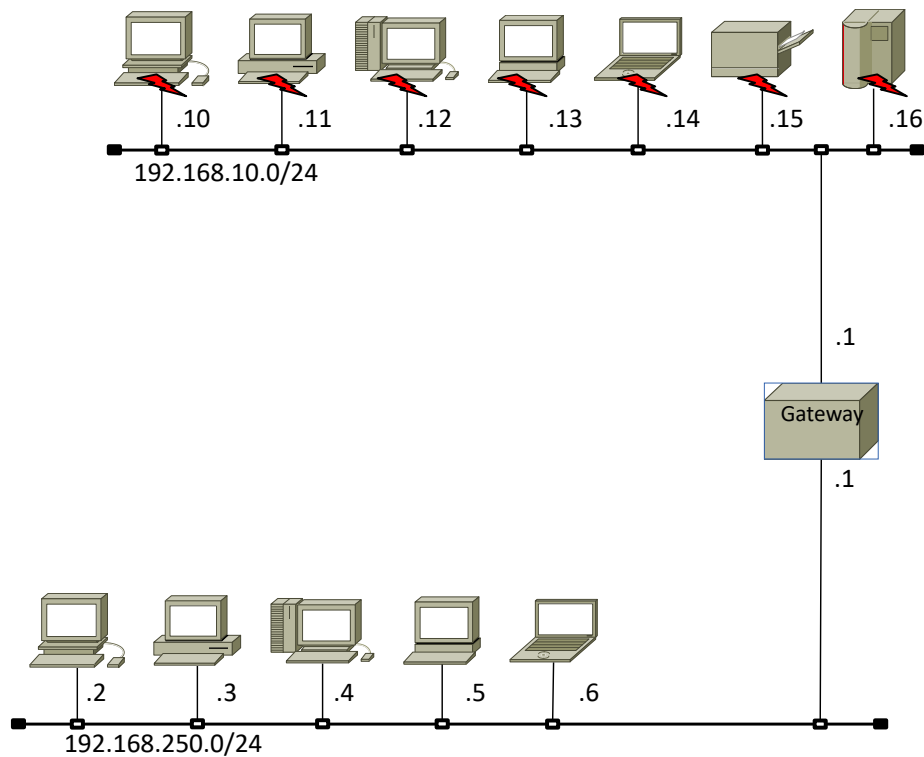
Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006678901	00000C456789	0x800	11.3.0.5	195.212.30.5

E -> F

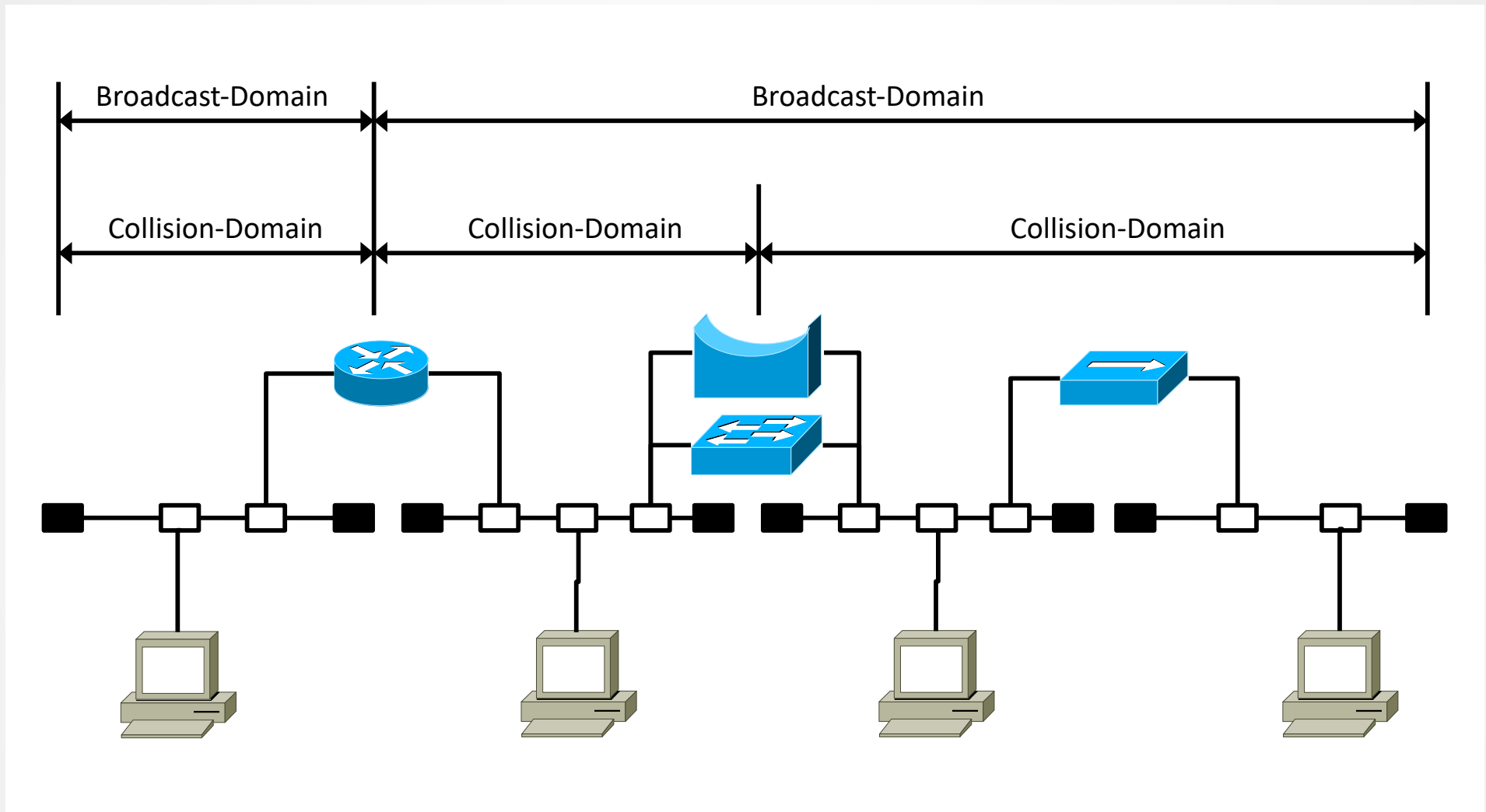
Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080009890123	080006789012	0x800	11.3.0.5	195.212.30.5

Netzwerk-Komponenten

Gateways



Netzwerk-Komponenten Zusammenfassung



Netztechnik-Vorlesung Teil-8

Inhalt

- Netzwerk-Komponenten
 - ◆ Repeater
 - ◆ Brücken
 - ◆ Switches
 - ◆ Router
 - ◆ Gateways

Netzwerk-Komponenten arbeiten auf verschiedenen Ebenen des OSI-RM.

Repeater → Ebene 1

Brücken, Switches → Ebene 2

Router → Ebene 3

Gateways → bis Ebene 7

Es gibt auch Ableitungen und Mischformen.

Dual-Speed-Hub (Entspricht 2 Hubs die mit einem Switch verbunden werden)

Layer-3-Switch (Router auf Ebene 3)

Default Gateway (Router auf Ebene 3)

...

Einleitung

Bei der Übertragung von Daten in Netzwerken sind viele Anforderungen und Probleme zu bewältigen:


- Dämpfungsprobleme, die letztendlich Längenprobleme erzeugen können.
- Begrenzung der Anzahl der Teilnehmer auf einem Netzsegment.
- Räumliche Trennung
- Logische Trennung
- Lastprobleme
- Antwortzeiten
- Kollisionen
- Sicherheit
- Management

Für jedes dieser Probleme gibt es ein Heilmittel.
Je nach Problem werden die Komponenten eingesetzt.

Die Probleme im LAN-Umfeld sind vielfältig und entstehen zum einen wenn die Netzwerke immer größer werden (Dämpfungsprobleme) und wenn immer mehr Netzteilnehmer dazu kommen (Kollisionsprobleme, Broadcast-Probleme)

Zum Anderen sollen die Netzwerke verwaltet / gemanagt werden. Das ist erforderlich um Bereiche voneinander abzutrennen / zu sichern

Netzwerk-Komponenten Repeater Teil-1



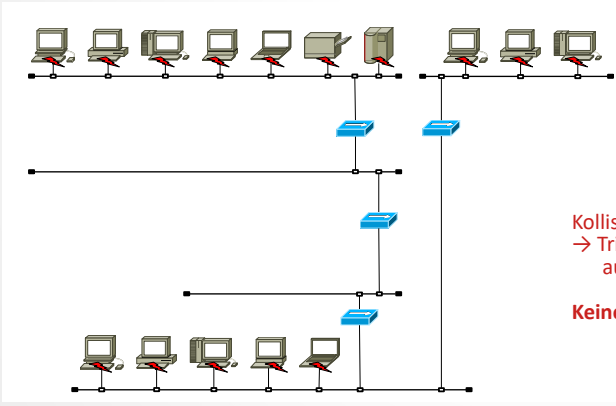
Verlängert Netzsegmente, die wg. Dämpfung an Grenzen stoßen
Überall die gleich Geschwindigkeit (10Mbps oder 100Mbps)

Repeater-Regeln

- Repeater-Regeln für 10 Mbps
 - ◆ Max. 5 Segmente
 - ◆ Max. 4 Repeater zwischen zwei Endgeräten
 - ◆ Max. 3 gleichzeitig genutzte Segmente (an 3 Segmenten dürfen gleichzeitig Stationen betrieben werden)
- Repeater-Regeln für 100 Mbps
 - ◆ Max. 4 Segmente
 - ◆ Max. 3 Repeater zwischen zwei Endgeräten
 - ◆ Max. 2 gleichzeitig genutzte Segmente (an 2 Segmenten dürfen gleichzeitig Stationen betrieben werden)

Kollisionen werden weiter geleitet!
→ Tritt in einem Segment eine Kollision auf, wird sie auch an die anderen Segmenten weiter geleitet!

Keine Begrenzung von Kollisionsdomänen



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 4:46

Repeater sind dafür gedacht die Längenrestriktion eines LAN.Segments zu erweitern.

Dazu funktioniert der Repeater wie ein dummer Verstärker.
Deshalb werden Kollisionen weiter geleitet und betreffen damit alle LAN Segmente

Es werden im Normalfall kein Frames untersucht.

In Luxus-Versionen gibt es Port-Management Collisions-Abtrennung und Filterung

Repeater-Regel für 10Mbps

5-4-3

Max. 5 Segmente

Max. 4 Repeatern

Max.3 Segmente dürfen „bevölkert sein“

Repeater-Regel für 100Mbps

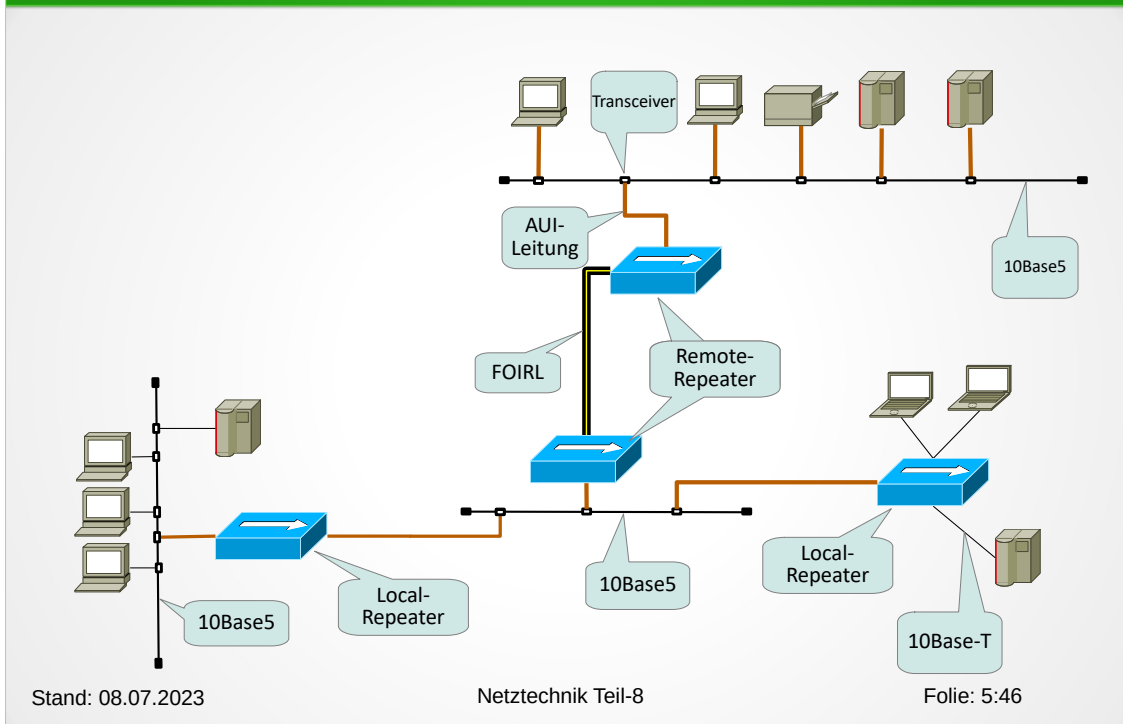
4-3-2

Max. 4 Segmente

Max. 3 Repeatern

Max. 2 Segmente dürfen „bevölkert sein“

Netzwerk-Komponenten Repeater Teil-2



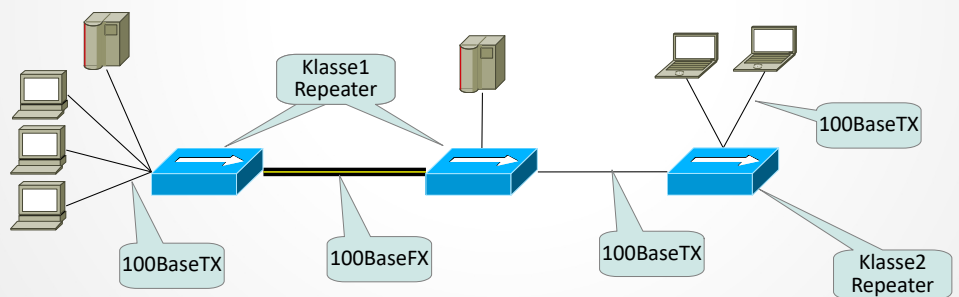
Grundsätzlich muss zwischen Local- und Remote-Repeatern unterschieden werden.

Local Repeater verlängern ein LAN-Seggment um ein weiteres Segment. Dafür werden die Spannungspegel und der Takt aufgefrischt.

Remote-Repeater können die Distanz zweier LAN-Segmente auf bis zu 1000m erweitern indem zwischen ihnen eine Glasfaser-Verbindung erstellt wird. Remote-Repeater bestehen aus zwei Komponenten die aus LAN-Segment-Sicht als ein Repeater gesehen werden.

Netzwerk-Komponenten Repeater Teil-3

Klasse	Bedeutung
1	Entspricht einem Media-Konverter. Es können unterschiedliche Medien miteinander verbunden werden. Z. B. kann 100Base-Tx mit 100Base-Fx verbunden werden. Ist somit langsamer als Repeater der Klasse II.
2	Diese Repeater verbinden immer nur Ports mit dem gleichen Medium



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 6:46

Eine weitere Unterteilung wurde mit der Einführung von 100Mbps vorgenommen.

Medienconverter (Repeater an denen unterschiedliche Medien angeschlossen sind) müssen Daten zwischenspeichern. Dafür benötigen sie Zeit und haben dadurch eine größere Latenzzeit.

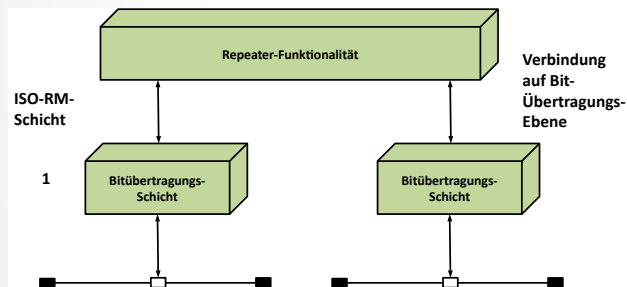
Repeater, die das Signal nur auffrischen, können schneller agieren und haben dadurch eine geringere Latenzzeit.

Netzwerk-Komponenten Repeater Teil-4

Probleme, bei denen mit Repeatern geholfen werden kann:

- Längenbegrenzungen (Maximale Segmentlängen, je nach Topologie beachten)
 - Anzahl von Teilnehmern (maximale Komponentenanzahl beachten)
- Z.B. in einem Netzsegment ist die Anzahl der möglichen Teilnehmer begrenzt, z. B. 30 in einem 10Base2-Netzsegment.

Repeater im ISO-7-Schichten-Modell



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 7:46

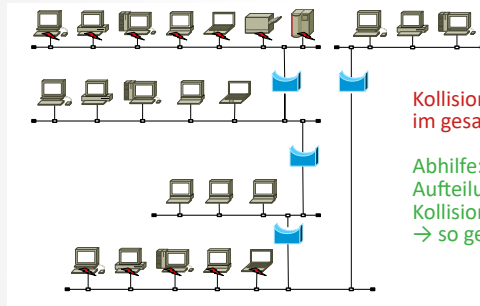
Repeater arbeiten mit den Informationen der Ebene 1
Dazu gehört die Präambel und evtl. der SFD (Start Frame Delimiter)
Diese werden vom Repeater „aufgefrischt“. D. h. Die Amplitude und der Takt wird regeneriert.

Netzwerk-Komponenten Repeater Teil-5

Repeater-Bauformen:

- Sternkoppler
- Hub
- Media-Konverter
- Switching-Hub

Netzwerk-Komponenten Brücken Teil-1



Kollisionen treten im Repeaternetz
im gesamten Netzwerk auf.

Abhilfe:
Aufteilung eines Netzwerks in Segmente, in denen eventuelle
Kollisionen gekapselt bleiben
→ so genannte Kollisionsdomänen

Auf einem LAN-Segment können sich alle Teilnehmer ständig gegenseitig sehen. Sowohl Kollisionen, Unicasts, Multicasts und Broadcasts werden an alle Teilnehmern gesendet.

Jeder, der das gerade ankommende Paket „brauchen“ kann bearbeitet es.

Dadurch haben die Stationen allerdings auch viel mit Kollisionen und Traffic zu tun, den sie nicht nutzen können und somit umsonst überprüfen müssen.

Abhilfe schafft eine Aufteilung in Subsegmente durch Brücken.

Kollisionen werden grundsätzlich nicht weiter geleitet. Alle Broadcasts und alle Multicasts werden von den Brücken an allen Ports weiter geleitet.

Unicasts werden nur an die Ports weiter geleitet, an denen die MAC-Adresse des Ziels angeschlossen ist.

Damit fällt in den Sub-Segmenten ein Teil des Unicast Traffics und die Kollisionen weg.

Netzwerk-Komponenten Brücken Teil-2

Damit Brücken ihre Funktion durchführen können müssen sie wissen welcher Netzwerkteilnehmer in welchem Netzwerk-Segment angeschlossen ist.

Dazu beobachten sie den gesamten Datenverkehr in den einzelnen Segmenten und merken sich den Anschlussport (an dem der Frame eingetroffen ist) und die Quell-MAC-Adresse des Frames in einer Tabelle.

Damit dies funktioniert müssen alle Brückenports im Promiscuous-Mode betrieben werden.

Kommt ein Frame an einem Port an wird die Ziel-MAC-Adresse des Frames untersucht. Und eine Forwarding-Decision getroffen:

- Liegt das Ziel im Netzwerk-Segment aus dem es kam, wird der Frame verworfen.
- Ist das Ziel an einem anderen Port angeschlossen, wird der Frame an diesen Port weiter geleitet.

Hier wird auch klar warum MAC-Adressen eindeutig sein müssen. Ist eine MAC-Adresse an mehreren Ports vorhanden, kann die Brücke keine vernünftige Forwarding-Decision treffen!

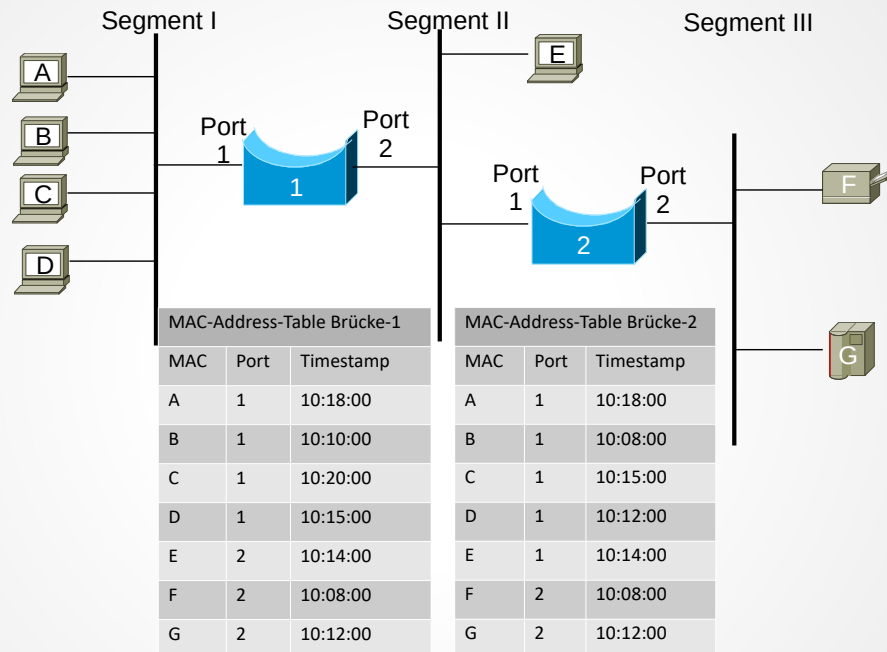
Dazu müssen die Brücken jedoch wissen, welche MAC-Adresse an welchem Port angeschlossen ist.

Dies „lernen“ die Brücken indem sie den Traffic an allen Ports im „Promiscuous-Mode“ abhören.

Sie entnehmen die Quell-MAC-Adressen den Frame-Headern und bauen damit eine Tabelle auf.

In der Tabelle werden die MAC-Adressen den zugehörigen Ports und einem Zeitstempel zugeordnet.

Netzwerk-Komponenten Brücken Teil-3 (Adress-Tabellen)



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 11:46

Ablauf:

1.

B sendet A einen Frame:

Die Brücke 1 macht nichts, denn sie hat gelernt dass A im gleichen Sub-Segment wie B liegt und damit den Frame auch schon bekommen hat.

2.

A zieht von Segment I nach Segment II um.

3.

B sendet A einen Frame:

Die Brücke 1 macht nichts, denn sie ist der Meinung, dass A im Segment I liegt.

Das ist falsch, denn damit bekommt A den Frame nicht mehr zugestellt.

Abhilfe:

Die Einträge in der Tabelle haben nur eine zeitlich begrenzte Gültigkeit.

Durch einen Aging-Algorithmus werden alte Einträge eliminiert.

Sobald eine Station nach einem Umzug wieder Daten sendet, kann die Tabelle aktualisiert werden.

Dies geschieht auch jedes mal wenn ein Switch einen Frame bekommt.

Netzwerk-Komponenten Adressbuchverwaltung Brücken Teil-4

Adressbuchverwaltung

- **Dynamisches Adressbuch**

Die MAC-Adressen werden während der Bearbeitung im Selbstlernmodus in einem dynamischen Adressbuch vermerkt. Die Einträge werden nach einem Aging-Mechanismus wieder aus dem Adressbuch entfernt.
Typische Zeiten sind hierbei 5 Minuten (Cisco). Dies ist auch die Zeit die ein Notebook bei einem Switchport-Wechsel warten muss um wieder erreichbar sein.

- **Statisches Adressbuch**

Für Adressen, die nicht dem Alterungsmechanismus unterliegen sollen, besteht die Möglichkeit von manuellen statischen Einträgen.

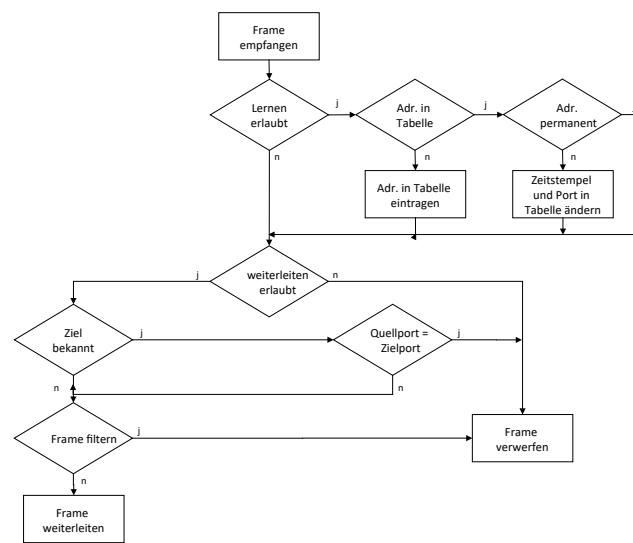
Der Administrator kann die Brücken (die MAC-Adressen) selbst lernen lassen. Dann unterliegen die Zuordnungen einem Aging-Algorithmus der dafür sorgt, dass alte Zuordnungen entfernt werden.

Dadurch wird dafür gesorgt, dass ein Umzug eines Geräts an einen anderen Port, oder das Ersetzen einer Netzwerk-Karte, sich nicht negativ (blockierend) auswirkt.

Der Administrator kann jedoch die Zuordnung von MAC-Adresse zu Port auch selbst vornehmen. Die Zuordnung ist dann statisch und wird nicht über einen Aging-Algorithmus entfernt und bleibt auch über einen Wiederanlauf erhalten.

Netzwerk-Komponenten

Ablauf der Forwarding-Decision Brücken Teil-5



Wird ein Frame an einem Port empfangen, wird der abgebildete Ablauf durchgeführt.

Im Normalfall ist das Lernen von MAC-Adressen erlaubt und es wird ein Eintrag in der Tabelle für die MAC-Adress-Port-Zuordnung vorgenommen oder aktualisiert.

Im Normalfall ist das weiterleiten erlaubt. Falls nicht, wird der Frame nicht weiter geleitet.

Ist das Ziel nicht bekannt, muss es an allen Ports weiter geleitet werden, falls nicht noch Filter eine Weiterleitung unterbinden.

Netzwerk-Komponenten Filter Brücken Teil-6

Für den Administrator steht eine Vielzahl von Konfigurationsmöglichkeiten zur Verfügung. So können Filter parametrisiert werden. Damit können Rahmen, je nach gesetztem Filter, weiter geleitet, oder verworfen werden.

Es kann auf folgende Rahmenteile gefiltert werden:

- Dedizierte Ziel-MAC-Adresse
- Dedizierte Quell-MAC-Adresse
- Eine Broadcast-Adresse
- Ein Typfeld
- Eine Maske

Die Filterung kann folgendermaßen erfolgen:

- Positiv mit einer Whitelist (Nur parametrisierte Rahmen werden transportiert)
- Negativ mit einer Blacklist (alle parametrisierten Rahmen werden verworfen)

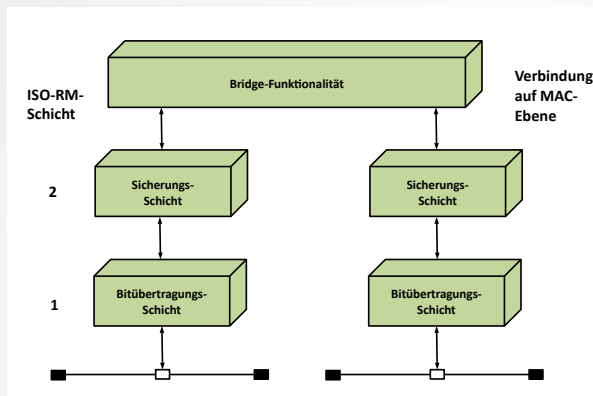
Es gibt einige Möglichkeiten Frame zu filtern.

Am augenscheinlichsten sind die MAC-Adressen (Quelle, Ziel, Multicast oder Broadcast).

Es können jedoch auch Einträge im Typfeld oder bestimmte Bitmuster weiter hinten im Frame bearbeitet werden.

Netzwerk-Komponenten

Brücken Teil-7 (Brücken im IOS-7-Schichten-Modell)



Brücken arbeiten mit Frames auf Ebene 2 mit den MAC-Adressen.

Die Frames selbst werden nicht verändert sondern nur weiter geleitet oder verworfen.

Deshalb sind Brücken für die Protokolle der höheren Ebenen (≥ 3) Transparent.

In einem Netzwerk dürfen nach IEEE802.1d maximal 7 Brücken verbaut sein um sicher zu stellen, dass die Grenzen der Frame-Laufzeit (max. 7 Sec.) eingehalten werden

Da Brücken MAC-Adressen zur Entscheidung für das Forwarding nutzen arbeiten sie auf Ebene 2.

Informationen der Ebene 3 (z. b. IP-Adressen) werden von der Brücke nicht ausgewertet.

Netzwerk-Komponenten Brücken Teil-8

Probleme in Netzwerken, bei denen eine Brücke hilfreich ist:

- **Das, was schon von Repeatern erledigt werden konnte:**

- ◆ **Längenbegrenzung von Netzwerken**

- Je nach verwendeter Topologie sind die Netzsegmente in ihrer Länge begrenzt. Z. B. bei 10Base2 185 m.

- Bei einer Aufteilung eines Netzwerkes durch eine Brücke in zwei Subsegmente, steht in beiden Subsegmenten wieder die gesamte Längenausdehnung (Entsprechend den definierten Standards) zur Verfügung. Hier bei 10Base2 sind es 370 m.

- ◆ **Begrenzung der Stations-Anzahl**

- In einem Netzsegment ist die Anzahl der möglichen Teilnehmer begrenzt, z. B. 30 in einem 10Base2-Netzsegment.

- Bei einer Aufteilung eines Netzwerkes durch eine Brücke in zwei Subsegmente steht in beiden Subsegmenten wieder die maximale Stations-Anzahl zur Verfügung.
Hier bei 10Base2 sind es 60.

- **Ausbreitung fehlerhafter Pakete**

- Erkennt eine Brücke auf einem Subsegment ein fehlerhaftes Paket, wird es nicht auf das andere Subsegment übertragen. Genauso werden auch Kollisionen auf ein Subsegment begrenzt.

- **Große Netzlast innerhalb eines Netzsegments**

- Da nicht alle Rahmen von einer Bridge übertragen werden, ist die Netzlast in den einzelnen Subsegmenten geringer. Dies ist je nach Datenverkehr (Unicasts, Multicasts und Broadcasts) jedoch nur bedingt wirksam.

- **Kollisionen**

- Kollisionen bleiben bei einer Brücke auf den Port begrenzt an dem die auftreten.

Stand: 08.07.2023

Netztechnik Teil-8

Folie: 16:46

Das was Geräte der unterlagerten Ebenen können wird von Brücken auch beherrscht.

Hinzu kommen die Begrenzungen von Kollisionsdomänen, die Eliminierung von fehlerhaften Frames und die Reduzierung der Netzlast durch Begrenzung der Unicasts auf den zugeordneten Ports.

Netzwerk-Komponenten

Brücken Teil-9 (Brückentypen)

Lokale Brücke:

Dieser Brückentyp stellt die Urform der Brücken dar und wurde dazu verwendet ein LAN-Segment in 2 Subsegmente aufzuteilen.

Remote-Brücke:

Remotebrücken verbinden Subsegmente über WAN-Strecken.

Sie treten immer paarweise auf. (Bei erhöhter Verfügbarkeit auch zu viert)

Remotebrücken können sowohl mehrere LAN-Ports als auch mehrere WAN-Ports haben.

Dies kann zur Erhöhung der Verfügbarkeit als auch der Erhöhung der Bandbreite durch Port-Aggregation genutzt werden.

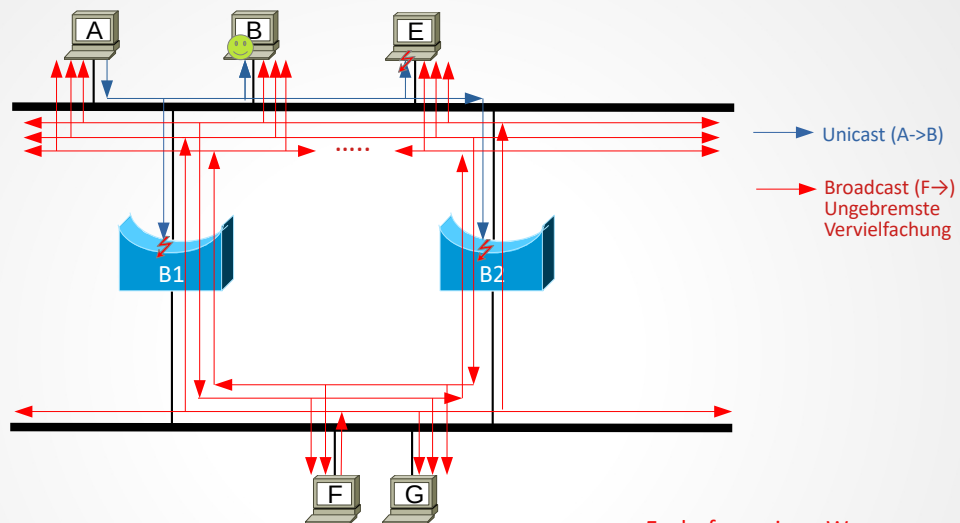
Multiport-Brücke:

Dieser Typ ist eine Weiterentwicklung der Remote-Brücken

(die oft mehr als 2 Ports haben)

Damit können auch mehr als 2 Subsegmente mit einer Brücke erstellt werden.

Netzwerk-Komponenten Brücken Teil-10 (Redundanz und Zyklenfreiheit)



Es darf nur einen Weg
von a nach g geben!

Lösung: Spanning Tree

Unicasts sind für Brücken kein Problem.

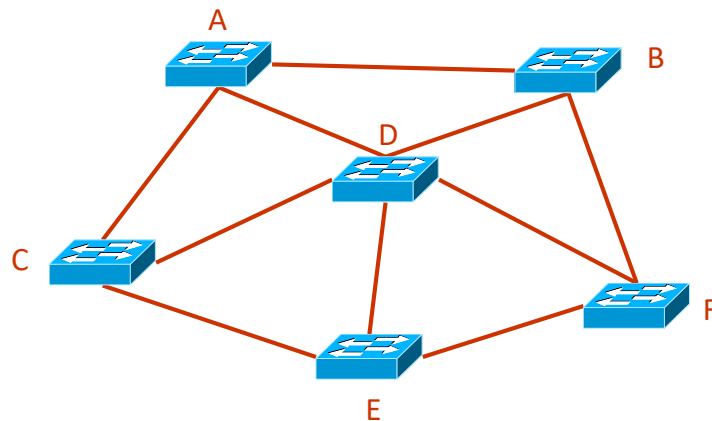
Probleme entstehen dann, wenn ein Frame an allen Ports immer weiter geleitet werden muss.

Dadurch können Schleifen entstehen die z. B. Zu Broadcast-Stürmen führen. Diese legen ein Netzwerk innerhalb kürzester Zeit lahm.

Netzwerk-Komponenten Brücken Teil-11 (Spanning Tree-1)

Ausgangs-Zustand:

Netzwerk-Segmente mit 6 Switches



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 19:46

Um eine Schleifenbildung zu vermeiden kann mit einem Spanning Tree dafür gesorgt werden, dass es immer nur einen Weg von A nach B gibt.

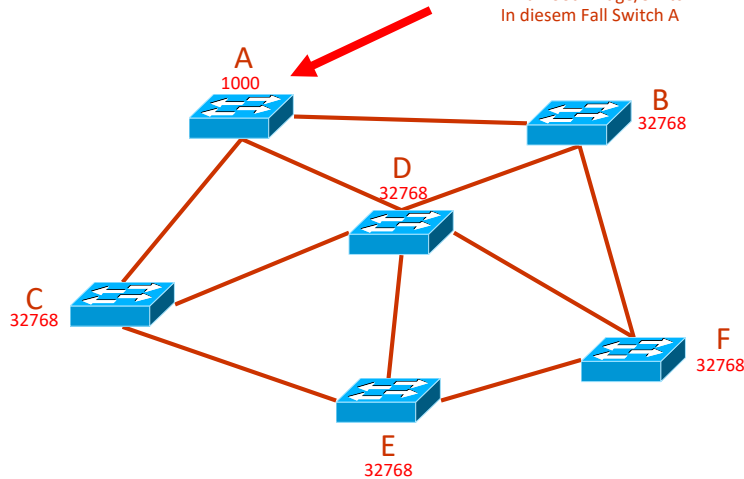
In der Folie ist ein beliebig zusammengeschaltetes Netzwerk dargestellt, welches sich mit dem Spanning Tree organisiert, so dass es eine Baumstruktur ergibt.

Die Bearbeitung des Spanning Tree läuft für Brücken und Switches gleich ab.

Netzwerk-Komponenten Brücken Teil-12 (Spanning Tree-2)

Ermitteln des Root-Switches

Um eine hierarchische Struktur zu ermitteln, ist zuerst die Root-Brücke zu ermitteln. Die Brücke/Switch mit der höchsten Priorität wird Root-Bridge/Switch. In diesem Fall Switch A



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 20:46

Als erstes ist ein Root-Switch zu bestimmen.

Dazu dient die Switch-ID welche sich aus der Priorität und der MAC-Adresse zusammensetzt:

Switch-ID = <Priorität><MAC-Adresse>

Der Switch mit der kleinsten Switch-ID wird der Root-Switch)

Die Priorität ist bei allen Switches per Default auf 32768 eingestellt. Ändert der Administrator nichts daran, wird der Switch mit der kleinsten MAC-Adresse zum Root-Switch.

Da das nicht unbedingt zu einem performanten Netzwerk führt, sollte der Administrator, sofern er den Spanning Tree verwendet, einen Root-Switch bestimmen, indem er die Priorität auf einen Wert kleiner 32768 setzt.

Netzwerk-Komponenten Brücken Teil-13 (Spanning Tree-3)

Pfadkosten = 1000/Bandbreite [Mbps]

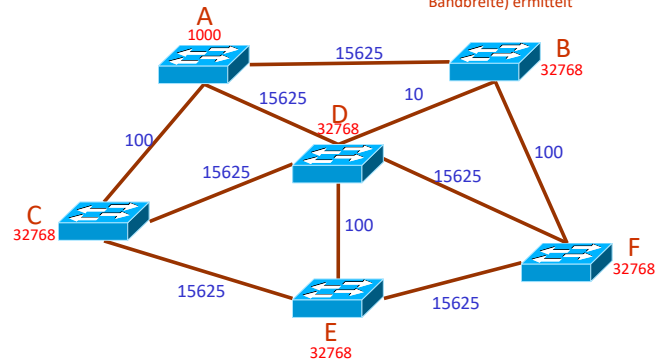
1 = 1000 Mbps Ethernet
10 = 100Mbps Ethernet
100 = 10Mbps Ethernet
250 = 4Mbps Token-Ring
15625 = 64k (ISDN)

Wegeermittlung

Nach dem Festlegen der Root-Bridge werden die Wege ermittelt.

Zuerst müssen alle Switches/Brücken den günstigsten Weg zur Root-Bridge ermitteln

Dazu werden die Pfadkosten (proportional zur Bandbreite) ermittelt

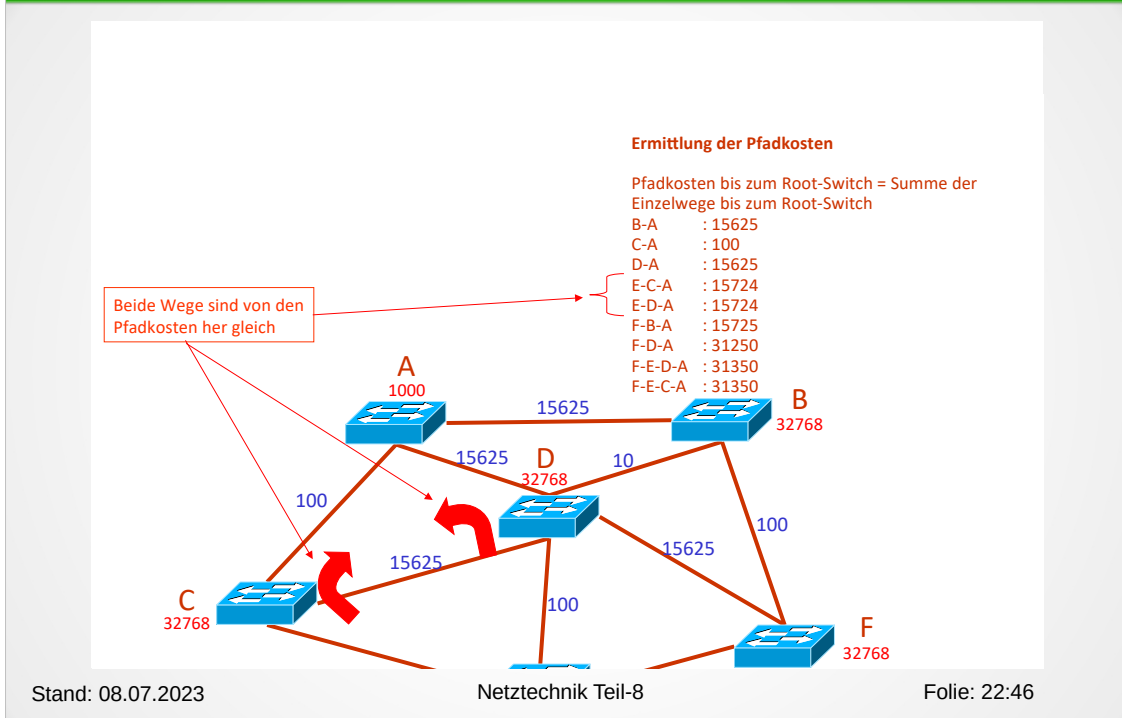


Ist der Root-Switch bestimmt, werden die Pfadkosten eines jeden Switches zum Root-Switch bestimmt.

Die Pfadkosten werden zwar aus der Datenübertragungsrate abgeleitet, können jedoch vom Administrator korrigiert werden.

Je größer die Datenübertragungsrate ist, desto kleiner sind die Pfadkosten.

Netzwerk-Komponenten Brücken Teil-14 (Spanning Tree-4)



Es kann den Fall geben, dass es mehrere Wege mit gleichen Pfadkosten von einem Switch zum Root-Switch.

Dies ist der Fall beim Switch E.

Es gibt einen Weg über den Switch C mit den Pfadkosten $15625 + 100$ und einen Weg über den Switch D mit den Pfadkosten $100 + 15625$.

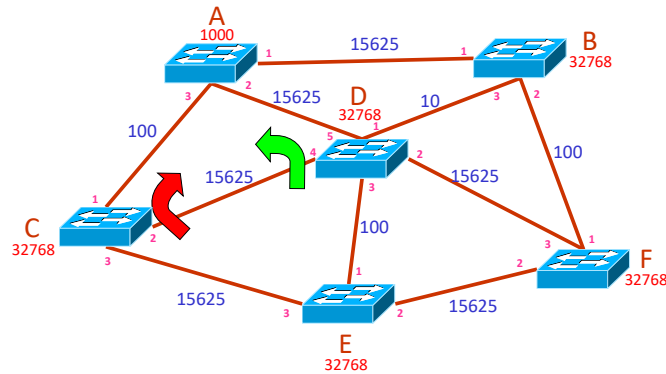
Da es nur einen Weg geben darf, muss einer der beiden Wege ausgewählt werden.

Netzwerk-Komponenten Brücken Teil-15 (Spanning Tree-5)

Die niedrigere Port-ID wird bevorzugt.
Daraus folgt für den Switch E der Pfad: E-D-A

Entscheidung bei gleichen Pfadkosten:

Bei gleichen Pfadkosten entscheidet die PortID



Die Lösung besteht darin, dass der Switch den Port mit der kleinsten Portnummer (im obigen Fall Port-1) für den Weg zum Root-Switch auswählt.

Netzwerk-Komponenten Brücken Teil-16 (Spanning Tree-6)

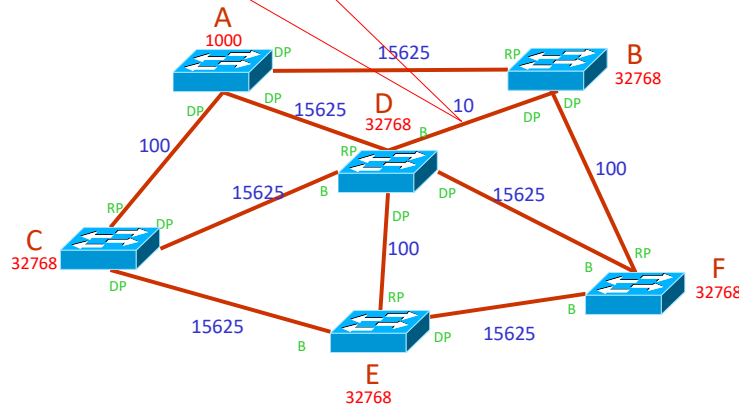
Die Verbindung zwischen D und B ist ein Ethernet-Segment!
Bei der Bestimmung des DP hat B wegen der Bridge-ID den Zuschlag bekommen.
Die in diesem Segment angeschlossenen Geräte senden ihre Pakete über B in andere Segmente

Port-Funktionszuordnung

In einem Switch ist der Port, der als nächster zum Root-Switch führt, der Root-Port (RP)

In jedem Netzwerk ist der Switchport, der zur Root-Switch führt, der designierte Port (DP)

Die anderen Ports sind im Blocking Modus (B)



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 24:46

Die Verbindungen zwischen den Switches sind Netzwerke und könnten theoretisch aus einem Bus bestehen, an dem weitere Geräte angeschlossen sind.

Dies ist der Fall bei der Verbindung zwischen dem Switch D und dem Switch B. Beide Switches haben die gleichen Pfadkosten zum Root-Switch.

In diesem Fall wird wieder die Switch-ID herangezogen, um zu bestimmen über welchen Switch die Geräte die am 10-Mbit-LAN hängen zum Root-Switch kommunizieren.

Im obigen Fall gewinnt der Switch B.

Danach können die Switch-Ports einer Funktion zugeordnet werden:

RP = Root-Port.

Das ist der Port eines Switches der zum Root-Switch führt.

DP = Designated Port.

Das ist der Port eines LANs (zwischen den Switches) welcher zum Root-Switch führt.

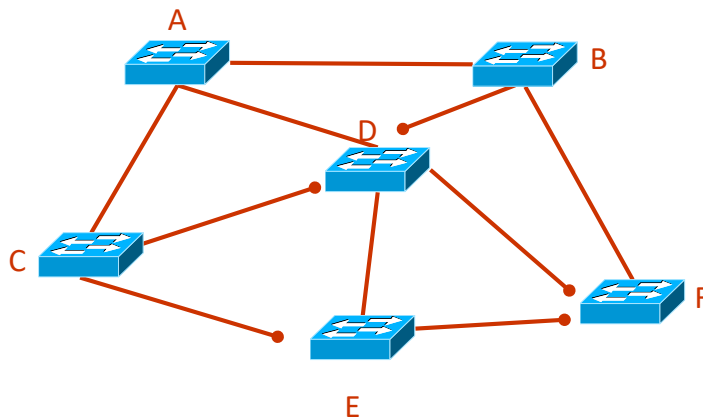
B = Blocking-Port.

Alle Ports, die nicht zum Root-Port oder Designated-Port gemacht wurden, werden geblockt (Blocking-Port).

Netzwerk-Komponenten Brücken Teil-17 (Spanning Tree-7)

Ergebnis:

Damit ergibt sich nach dem Ablauf des Spanning-Tree-Algorithmus dieser Aufbau



Stand: 08.07.2023

Netztechnik Teil-8

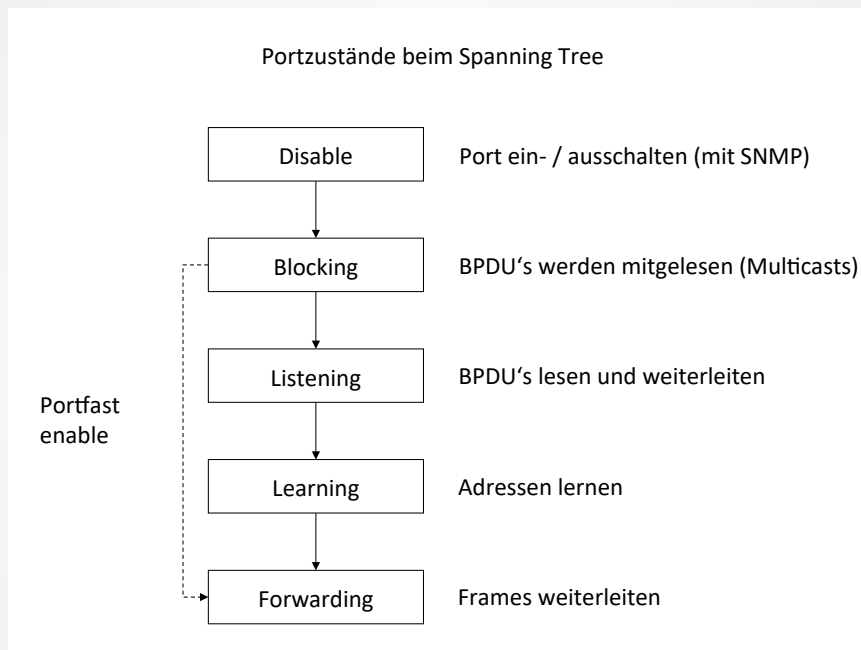
Folie: 25:46

Das Ergebnis ist die obige Baumstruktur.

Damit die Switches eventuelle Ausfälle einer Verbindung, oder eines Switches erkennen können, senden sie an allen Ports, an denen Switches hängen, Informationen in Form der BPDUs (Bridge-Protocol-Data-Units) aus.

Damit überwachen die Switches die gefundene Struktur und leiten gegebenenfalls eine Reorganisation ein, falls BPDUs für eine bestimmte Zeit ausbleiben.

Netzwerk-Komponenten Brücken Teil-18 (Portzustände)



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 26:46

Wird ein Switch hochgefahren, oder ein Port wird aktiviert (vom Status Disabled in den Status Active überführt), durchläuft er diverse Zustände bevor er eine Forwarding Decision treffen kann:

Blocking:

Es werden BPDUs empfangen.
Daten werden nicht weitergeleitet.

Listening:

Es werden BPDUs empfangen und gesendet um den Spanning Tree zu organisieren.
Daten werden nicht weitergeleitet.

Learning:

Der Spanning Tree ist organisiert und die Datenpakete, die empfangen werden dienen zum Aufbau der MAC-Tabelle.

Forwarding:

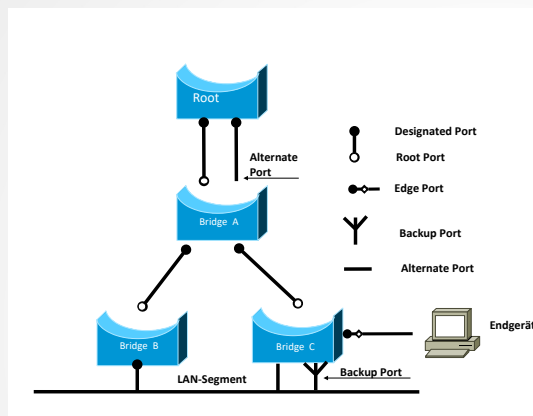
Frames werden weiter geleitet.

Da die einzelnen Zustände eine gewisse Zeit dauern, gibt es die Möglichkeit, eine Abkürzung zu nehmen damit die Frames weiter geleitet werden.

Dies kann z. B. bei Cisco-Switches mit dem CLI-Kommando „portfast enable“ für jeden Port einzeln eingeschaltet werden.

Netzwerk-Komponenten

Brücken Teil-19 (RSTP = Rapid Reconfiguraton Spanning Tree)



Root Port

Der Root Port ist der Port eines Switches der zum Root Switch hin (upstream) aktiv, also im FORWARDING-Modus ist.

Auswahlverfahren:

Kosten zum Root
Port Priorität
Port ID

Designated Port

Der Designated Port ist der Port der downstream (also vom Root Switch weg) bestimmt werden. Es ist der Port der zur Designated Bridge gehört.

Edge Port

Der Edge Port ist ein Port an dem kein Switch mehr angebunden ist.

Alternate Port

Der Alternate Port ist ein Port, der einen Weg zum Root Port weist, jedoch aufgrund des Auswahlverfahrens nicht zum Root Port wurde.

Backup Port

Der Backup Port ist ein Port der wie ein Designated Port arbeiten könnte, jedoch aufgrund des Auswahlverfahrens nicht zum Designated Port wurde.

Der Spanning Tree, in seiner ursprünglichen Form, hat eine lange Konvergenz-Zeit, was daran liegt, dass er Timer-getriggert ist. Erst wenn eine bestimmte Zeit keine BPDU eingetroffen ist, löst ein Switch die Reorganisation des Spanning Tree aus.

Das wurde in einem modifizierten Spanning Tree dem Rapid Reconfiguration Spanning Tree verbessert.

Grundsätzlich wird der Spanning Tree aufgebaut wie bisher. Allerdings wird bereits falls ein Port in den Zustand Down geht die Reorganisation des Spanning Trees durchgeführt.

Parallel zum Laufenden Spanning Tree ermitteln die Switches noch einen alternativen Spanning Tree, um im Reorganisations-Fall schneller zu einem Ergebnis zu kommen.

Netzwerk-Komponenten

Switches Teil-20 (RSTP = Rapid Reconfiguraton Spanning Tree)

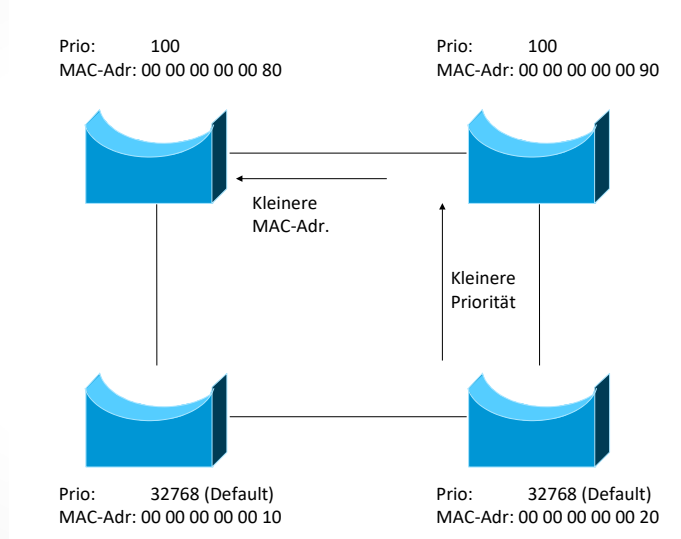
Port Status		Active Topologie	Port Role
STP	RSTP		
Disable	Discarding	Excluded	Disabled
Blocking	Discarding	Excluded	Alternate / Backup
Listening	Discarding	Included	Root, Designated, Edge
Learning	Learning	Included	Root, Designated
Forwarding	Forwarding	Included	Root, Designated, Edge

Mit dem neuen Spanning Tree wurden die Zustände überarbeitet und teilweise zusammengefasst.

Netzwerk-Komponenten Brücken Teil-21 (STP-Übersicht)

Bridge-ID = <Priorität> <MAC-Adresse>

Die Priorität ist per Default 32768



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 29:46

In der Folie ist nochmals dargestellt welche Faktoren dazu führen dass ein Switch zum Root-Switch gemacht wird.

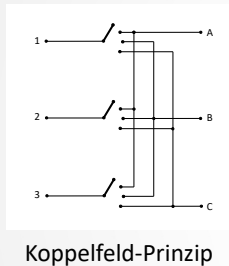
1.
Der Switch mit der kleinsten Switch-ID gewinnt.
2.
Per Default haben alle Switches die gleiche Priorität. Damit gewinnt der Switch mit der kleinsten MAC-Adresse.
3.
Um einen bestimmten Switch zum Root-Switch zu machen, sollte der Administrator dem Root-Switch die kleinste Priorität geben.

Netzwerk-Komponenten Switches Teil-1 (Typen)

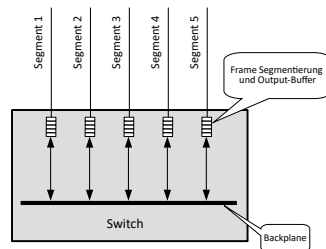


Switches entsprechen, von ihrer Funktionalität her, Multiport-Brücken. Brücken nutzen die CPU, um die Wegewahl der Rahmen durchzuführen.

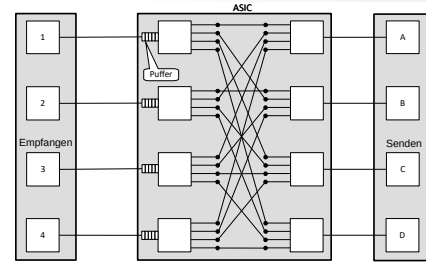
Bei Switches ist die Wegewahl in ASIC's (Application Specific Integrated Circuit), also in Hardware, realisiert.



Koppelfeld-Prinzip



Cell-Backplane-Switch



Matrix-Switch

Stand: 08.07.2023

Netztechnik Teil-8

Folie: 30:46

Funktional arbeiten Switches wie Brücken. Der Unterschied zu den Brücken besteht darin, dass die Bearbeitung weitestgehend in Hardware (ASICs) erfolgt.

Switches arbeiten nach dem Koppelfeld-Prinzip. Ein Frame, der an einem Port eintrifft, wird an einem bestimmten Port oder bei Broadcasts und Multicasts an allen Ports weiter geleitet.

Es gibt zwei Bauformen von Switches:

Cell-Backbone-Switch

Die Frames werden am Eingangsport gepuffert und in kleine Zellen aufgeteilt. Nach der Forwarding-Decision werden die Zellen an den Ausgangs-Port über die Backplane zum Zielp-Port transportiert. Dort wird der Frame zusammengebaut und gesendet.

Da die Zellen unterschiedlicher Ports auf der Backplane transportiert werden fühlt es sich für alle Ports so an, als ob sie gleichzeitig bearbeitet werden. Die Backplane-Kapazität des Switches ist hier ein wichtiges Performance-Kriterium.

Matrix Switch

Die Frames werden am Eingangsport gepuffert. Nachdem der Zielp-Port ermittelt wurde, wird der Frame an den Zielp-Port durchgeschaltet. Am Zielp-Port wird der Frame ausgesendet.

Netzwerk-Komponenten Switches Teil-2 (Strategien)

Store & Forward

Frames werden komplett untersucht und gespeichert. Danach erfolgt die Forwarding-Entscheidung und der Frame wird auf den Ausgangsport geschaltet. Damit können fehlerhafte Frames anhand der CRC-Bearbeitung erkannt und aussortiert werden. Dies ist das sicherste, jedoch aber auch langsamste Verfahren.

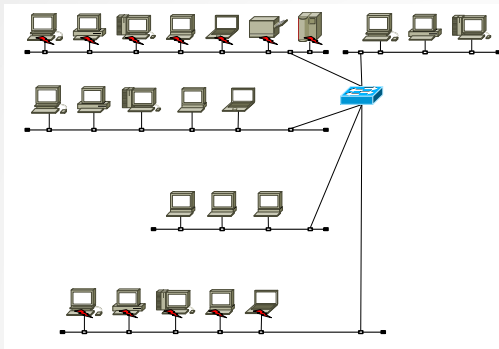
Cut Through

Sobald die Ziel-MAC-Adresse erkannt wurde wird der Frame auf den Ausgangsport weiter geleitet. Damit können jedoch fehlerhafte Frames nicht erkannt und aussortiert werden. Dies ist das unsicherste, jedoch auch das schnellste Verfahren.

Cut Through Collision Free

Frames werden während des Empfangs der ersten 64 Bytes auf eine Kollision hin untersucht und, falls bis dahin kein Fehler aufgetreten ist, auf den Ausgangsport weiter geleitet. Damit können fehlerhafte Frames nicht erkannt und aussortiert werden. Dies ist ein Kompromiss zwischen dem Cut Through- und Store & Forward-Verfahren.

Netzwerk-Komponenten Switches Teil-3 (Layer-2)

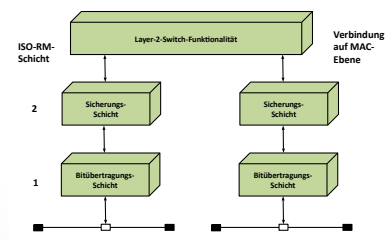


Alle Funktion und Randbedingungen wie bei den Brücken gelten hier auch!

Besonders

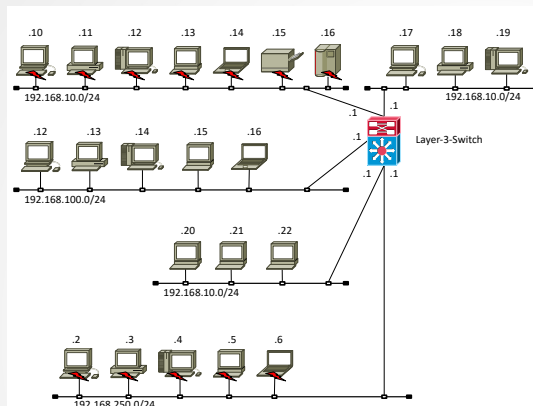
- **Kollisionen** bleiben auf das Segment begrenzt in dem sie auftreten
- **Unicasts** werden nur weiter geleitet, wenn das Ziel in einem anderen Segment liegt.
- **Multicasts und Broadcasts** werden an allen Ports weiter geleitet.

Ein Frame wird bis auf die Ebene 2 entpackt um mit der MAC-Adresse die Forwarding-Entscheidung zu treffen



Switches arbeiten normalerweise als Layer-2-Switches und somit auf Ebene 2 im OSI-RM, denn sie werten die MAC-Adresse für die Forwarding-Decision aus.

Netzwerk-Komponenten Switches Teil-4 (Layer-3 und höher)

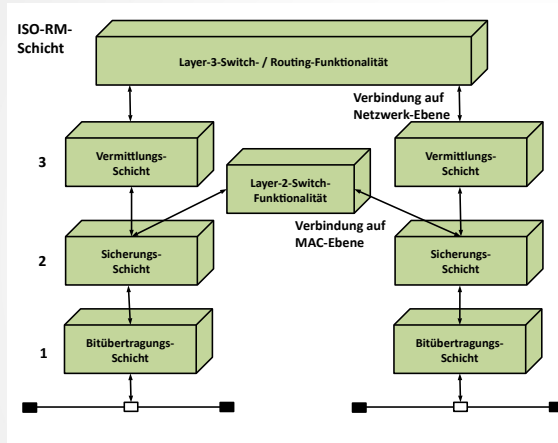


Vor allem wenn die Physik sich nicht ändert
kann ein Switch auch die Funktionalität
höherer Schichten (z. B. Routing der Ebene 3)
übernehmen

Dies geht bis zur Ebene 7 (bei der die Applikation
die Wege-Entscheidung beeinflusst)

Switches können allerdings auch auf Ebenen > Ebene-2 arbeiten. Dann erfüllen sie die Funktion eines Gerätes der entsprechenden Ebene.
z. B. agiert ein Layer-3-Switch als Router und somit auf Ebene 3.

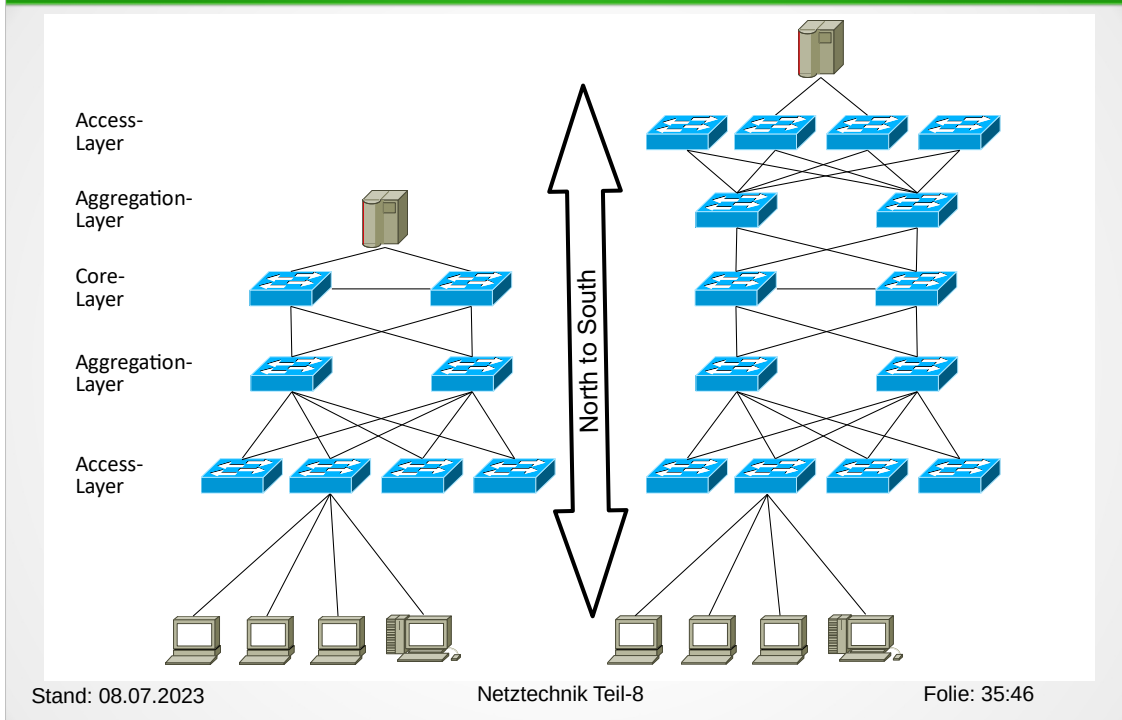
Netzwerk-Komponenten Switches Teil-5 (im ISO-7-Schichten-Modell)



Verfahren	
Layer-3-Switching	Überall routen
Layer-3-Cut-Through-Switching	Einmal routen danach switchen
Layer-2/3-Switching	Switchen wo möglich Routen wo unumgänglich
Layer-2-Switching	Überall switchen

Je nachdem auf welcher Ebene ein Switch agiert, kann er evtl. schon auf einer unterlagerten Ebene die Forwarding-Decision treffen und einen Frame weiter leiten.

Netzwerk-Komponenten Switches Teil-6 (Layer-2-Netzwerke)



Klassische Layer-2-Netzwerke können je nach Aufwand den in der Folie dargestellten hierarchischen Aufbau haben.

Die Endgeräte der User stehen in der Fläche und können über die Access-Layer-Switches mit einer Kupferverbindung angeschlossen werden.

Die Access-Layer-Switches sind wiederum redundant an die Aggregation-Layer-Switches angeschlossen. In der Aggregation-Layer werden zusammengehörende Netzwerke (VLANs) zusammengefasst.

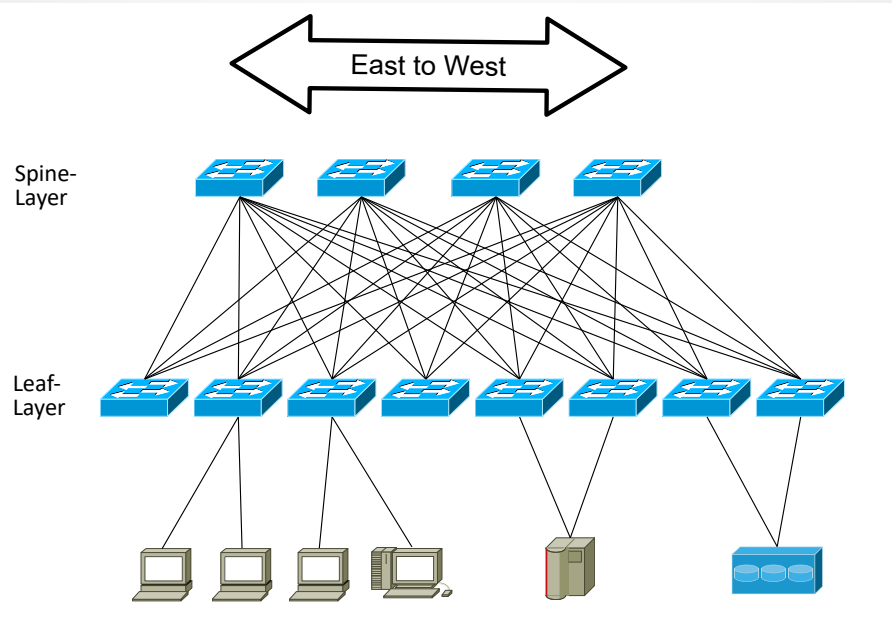
Die Aggregation-Layer-Switches stehen entweder bei den Etagenswitches oder im Rechenzentrum (RZ) und sind redundant an die Core-Layer-Switches im RZ angeschlossen.

Die Core-Layer-Switches im RZ sind oft Layer-3-Switches (also Router mit vielen Anschlüssen)

In kleinen RZ können die Server an die Core-Layer-Switches oder die Aggregation-Layer Switches (sofern sie im RZ stehen) angeschlossen werden.

In Großen Anlagen können die angeschlossenen Server über eine eigene Access-Layer und Aggregation-Layer angeschlossen werden.

Netzwerk-Komponenten Switches Teil-7 (Layer-2-Netzwerke)



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 36:46

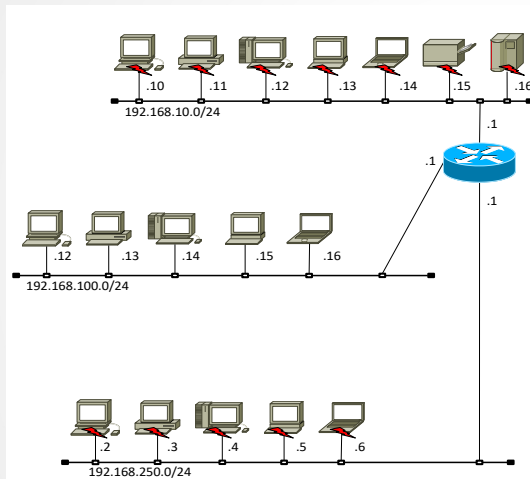
In modernen Installationen, vor allem bei Cloud-Realisierungen, gibt es kein hierarchisches System mehr.

Es gibt nur noch ein Spine-Layer, das alle Leaf-Switches redundant anbindet und der Leaf-Layer an den die Endgeräte und Server angeschlossen sind.

Damit müssen von jedem Endgerät immer nur 2 Switches genutzt werden um auf einen Server zuzugreifen.

Allerdings erfordert eine Solche Topologie eine Voll-Vermaschung.

Netzwerk-Komponenten Router Teil-1



Router arbeiten auf ISO-RM-Ebene 3 (Netzwerk-Schicht) und verbinden somit zwei Netzwerke miteinander. Dafür haben Router eine Schnittstelle und eine Adresse in jedem Netzwerk

Broadcasts werden auf ISO-RM-Ebene 2 abgehandelt und werden von Routern somit nicht weitergeleitet.

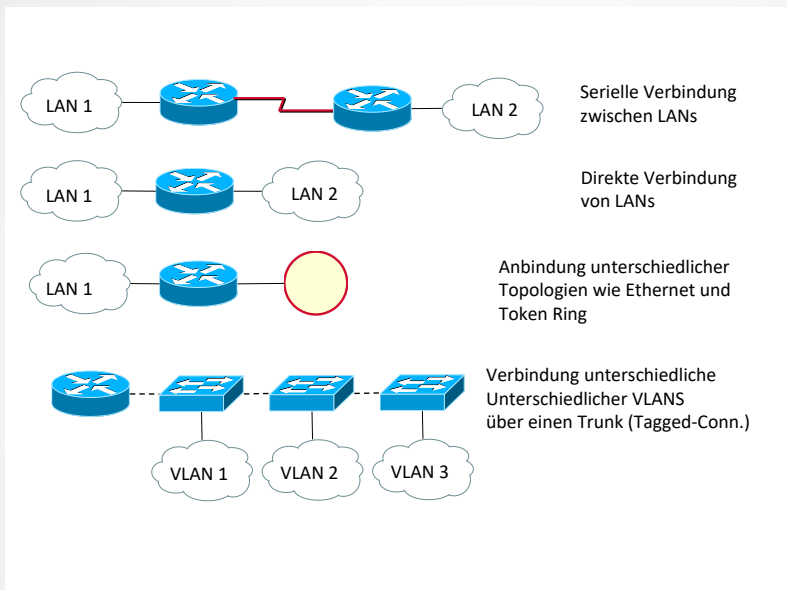
Kollisionen werden auf ISO-RM-Ebene 1 abgehandelt und werden von Routern ebenfalls nicht weitergeleitet.

Somit begrenzen Router sowohl Broadcast- als auch Kollisions-Domänen.

Router können eine Vielzahl von Funktionen vereinen. Allerdings ist das Routing (weiterleiten eines Paketes auf Ebene 3) als Grundfunktion vorhanden.

Netzwerk-Komponenten

Router Teil-2 (Verbindung unterschiedlicher Topologien)



Stand: 08.07.2023

Netztechnik Teil-8

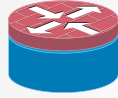
Folie: 38:46

Router können auch unterschiedliche Topologien miteinander verbinden.

Es müssen auch nicht immer 2 physikalische Anbindungen existieren. Bei einer Trunk-Verbindung werden mehrere VLANs über einen physikalischen Port angebunden. Jedes VLAN wird dann mit einem Subinterface im Router terminiert.

Netzwerk-Komponenten

Router Teil-3 (Zusätzliche Funktionen)



Router können noch weitere Funktionen beinhalten.
So ist z. B. Eine Firewall in vielen Routern im SOHO-Bereich anzutreffen.



Router im SOHO-Bereich haben oft auch eine WLAN-Schnittstelle



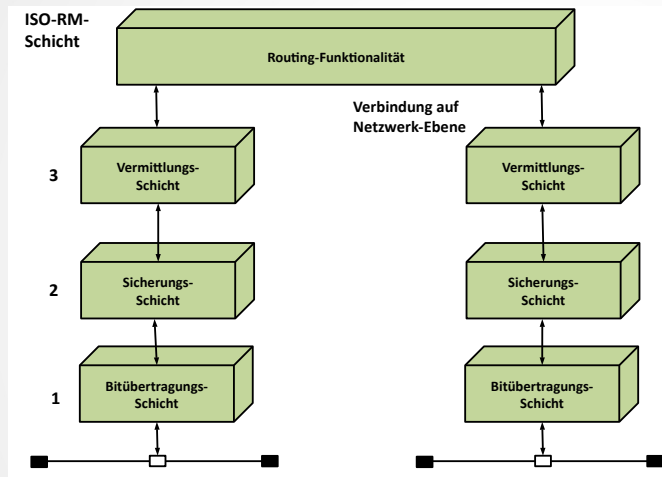
Ist ein Router für eine Anbindung des Firmen-Ethernet an verschiedene Topologien wie ISDN oder analoge Leitung zuständig, spricht man auch von einem ACCESS-Server.

Es gibt noch weitere Funktionen die Router wahrnehmen können.

Firewall
Accesspoint

...

Netzwerk-Komponenten Router Teil-4 (im ISO-7-Schichten-Modell)



Ein Paket ist bis auf die Ebene 3 zu entpacken, um mit der IP-Adresse, die Forwarding-Entscheidung zu treffen

Behandlung von Frames

- **Kollisionen** bleiben auf das Netzwerk begrenzt in dem sie auftreten.
- **Unicasts** werden nur weiter geleitet, wenn das Ziel in einem anderen Netzwerk liegt.
- **Multcasts und Broadcasts** bleiben auf das Netzwerk begrenzt in dem sie auftreten.

Router werten Informationen auf Ebene 3 zur Routing-Decision aus und arbeiten damit auf Ebene 3 im OSI-RM.

Netzwerk-Komponenten

Router Teil-5 (im Zusammenhang mit Protokollen)

Es gibt sowohl **routebare Protokolle**, als auch **Routingprotokolle**.

Bei den routebaren Protokollen handelt es sich um Protokolle, die von Routern weitergeleitet werden können.

Bei den Routingprotokollen handelt es sich um die Protokolle, welche die Router untereinander zur Abwicklung ihres Routing-Auftrages benützen. Dabei werden Informationen, wie z. B. Routingtabellen, dynamisch ausgetauscht. Damit können die Router auf Veränderungen der Netzwerk-Struktur, wie z. B. den Ausfall eines Routers, reagieren.

Routingprotokolle

- BGP (Border Gateway Protocol)
- HSRP (Hot Standby Router Protocol)
- IGRP/EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)

Routebare Protokolle

- IP (Internet Protocol)
- IPX (Internet Paket Exchange)
- OSI (Open Systems Interconnection)
- Apple Talk (Kommunikation zwischen Apple-Rechnern)

Nicht routebare Protokolle

(sind nicht routebare Protokolle, da sie auf Ebene 3 keine Informationen für die Vermittlung zur Verfügung stellen)

- NetBIOS
- NetBEUI
- LAT

Stand: 08.07.2023

Netztechnik Teil-8

Folie: 41:46

Unterscheidung

Routingprotokolle

Protokolle mit denen Router Informationen austauschen um die Routingtabellen aufzubauen und aktuell zu halten.

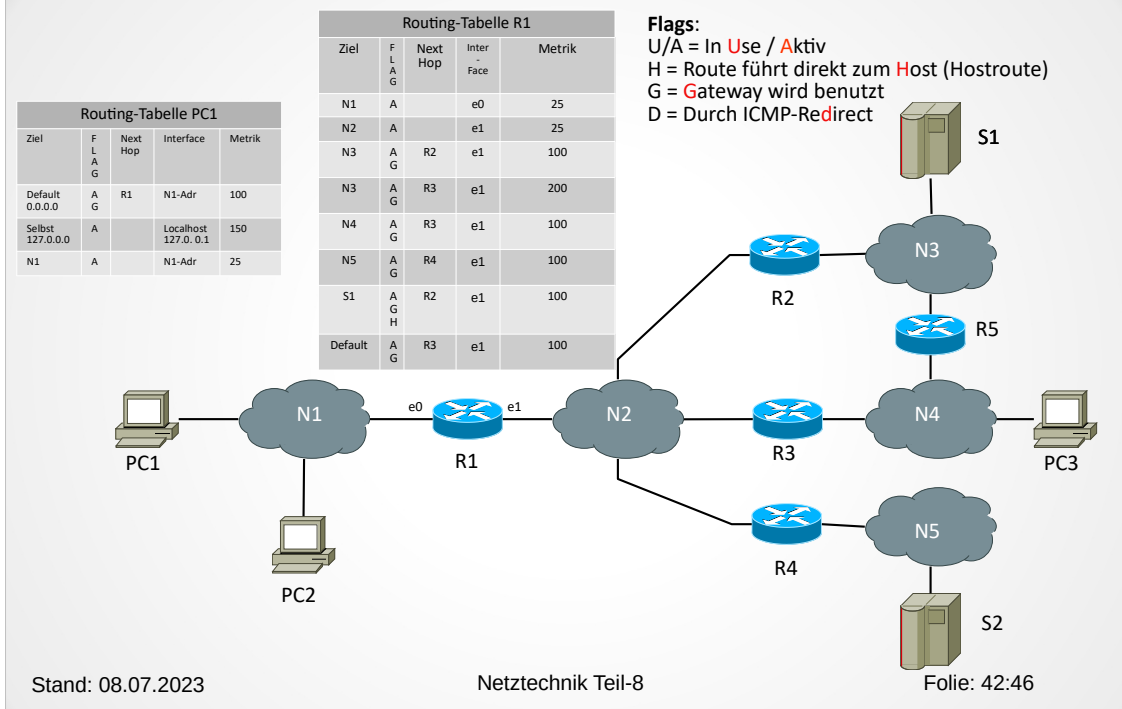
Routebare Protokolle

Das sind Protokolle die von Routern weiter geleitet werden können, da sie Informationen auf Ebene 3 zur Verfügung stellen. (z. B. IP-Adressen)

Nicht routebare Protokolle

Das sind Protokolle die auf Ebene 3 keine Information zur Verfügung stellen und somit nicht geroutet werden können (z. b. NetBEUI)

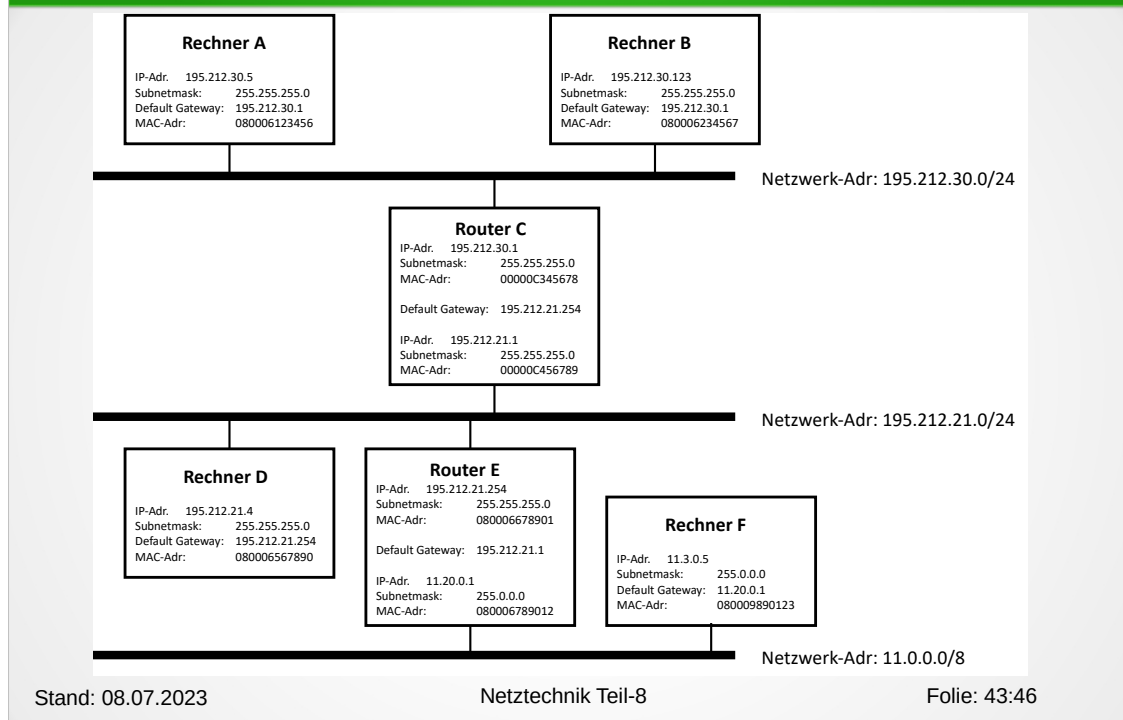
Netzwerk-Komponenten Router Teil-6 (Funktionsweise-1)



Alle Geräte (also nicht nur Router) haben eine Routingtabelle.

In Windows kann z. B. in einer DOS-Box mit dem Kommando `route print` die Routingtabelle ausgegeben werden..

Netzwerk-Komponenten Router Teil-6 (Funktionsweise-2)



Router werden in der Internet-Nomenklatur Gateways genannt. Daher sind die Default-Gateways bei Hosts in einem Netzwerk die Router, die den Weg in weitere Netzwerke kennen.

Beispiele:

A sendet ein Paket an B

A überprüft, ob B in seinem Netzwerk liegt. Das ist der Fall und so kann A sein Paket direkt an B senden.

A sendet ein Paket an D

A überprüft, ob D in seinem Netzwerk liegt. Das ist nicht der Fall, deshalb sendet A sein Paket an sein Default Gateway. Das ist der Router C. Der Router C überprüft, ob D in einem an ihn direkt angeschlossenen Netzwerk liegt. Das ist der Fall und so kann der Router C das Paket an den Rechner D senden.

A sendet ein Paket an F

A überprüft, ob F in seinem Netzwerk liegt. Das ist nicht der Fall, deshalb sendet A sein Paket an sein Default Gateway. Das ist der Router C. Der Router C überprüft, ob F in einem an ihn direkt angeschlossenen Netzwerk liegt. Das ist nicht der Fall, deshalb sendet der Router C das Paket an sein Default Gateway. Das ist der Router E. Der Router E überprüft, ob F in einem an ihn direkt angeschlossenen Netzwerk liegt. Das ist der Fall und so kann der Router E das Paket an den Rechner F senden.

Netzwerk-Komponenten Router Teil-8 (Funktionsweise-3)

A -> B

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006234567	0800006123456	0x800	195.212.30.123	195.212.30.5

A -> D

A -> C

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
00000C345678	0800006123456	0x800	195.212.21.4	195.212.30.5

C -> D

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006567890	00000C456789	0x800	195.212.21.4	195.212.30.5

A -> F

A -> C

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
00000C345678	0800006123456	0x800	11.3.0.5	195.212.30.5

C -> E

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006678901	00000C456789	0x800	11.3.0.5	195.212.30.5

E -> F

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080009890123	080006789012	0x800	11.3.0.5	195.212.30.5

Stand: 08.07.2023

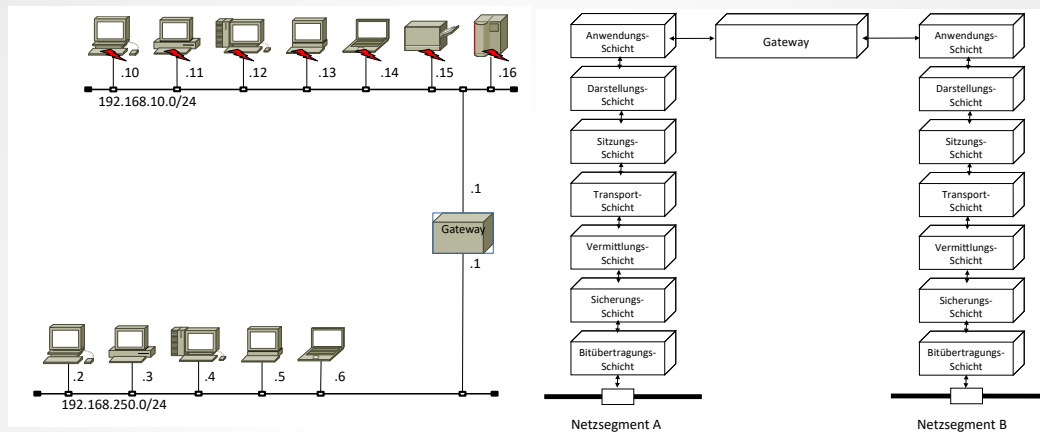
Netztechnik Teil-8

Folie: 44:46

In der Folie ist der Aufbau der Frames im Detail dargestellt.

Muss ein Paket über einen Router weiter geleitet werden. Werden im Router die MAC-Adressen ausgetauscht. Die IP-Adressen bleiben immer erhalten.

Netzwerk-Komponenten Gateways



Stand: 08.07.2023

Netztechnik Teil-8

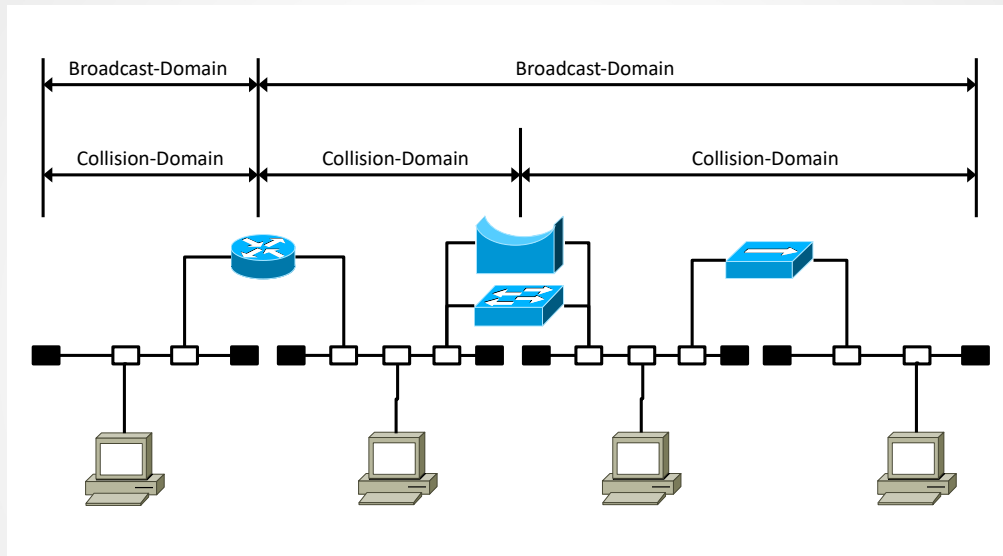
Folie: 45:46

Gateways verbinden Netzwerke auf Ebene 7.

Ein Fall für Gateways sind Firewalls.

Hier kann evtl. bis auf Applikationsebene untersucht ob der Datenverkehr stattfinden darf. (Application-Level-Firewalls)

Netzwerk-Komponenten Zusammenfassung



Stand: 08.07.2023

Netztechnik Teil-8

Folie: 46:46

Eine **Collisiondomain** (Kollisions-Bereich) ist der Netzwerkbereich, der von einer Kollision betroffen ist.

Da eine Kollision auf der ISO-RM-Ebene 1 stattfindet, wird sie von Repeatern weitergeleitet und von Brücken, Switches oder Routern nicht weitergeleitet.

Eine **Broadcastdomain** (Broadcast-Bereich) ist der Netzwerkbereich, der von einem Broadcast erreicht wird.

Da ein Broadcast auf der ISO-RM Ebene 2 oder 3 stattfindet, wird er von Repeatern, Brücken und Switches weitergeleitet, jedoch von Routern nicht weitergeleitet.

Deshalb gibt es sowohl für die Ebene 2 eine MAC-Broadcast-Adresse (FF:FF:FF:FF:FF:FF) als auch auf der Ebene 3 IP-Broadcast-Adresse (z. B. 192.168.178.255)