Netze

Modul 6: Netzwerksegmentierung

Prof. Dr. Hannes Tschofenig

6. November 2025

Semesterplanung — Vorlesungen

Modul	Dozent	Datum	Thema
1	Rademacher	2. Oktober 2025	Einführung, OSI-Referenzmodell und Topologien
2	Rademacher	9. Oktober 2025	Übertragungsmedien und Verkabelung
3	Rademacher	16. Oktober 2025	Ethernet und WLAN
4	Tschofenig	23. Oktober 2025	IPv4, Subnetze, ARP, ICMP
5	Tschofenig	30. Oktober 2025	IPv6 und Autokonfiguration
6	Tschofenig	6. November 2025	Netzwerksegmentierung
7	Tschofenig	13. November 2025	Routing
8	Rademacher	20. November 2025	Transportschicht und UDP
9	Rademacher	27. November 2025	TCP
10	Rademacher	4. Dezember 2025	DNS und HTTP 1
11	Tschofenig	11. Dezember 2025	HTTP 2 und QUIC
12	Tschofenig	18. Dezember 2025	TLS und VPN
/	/	8. Januar 2026	`Bei Bedarf / TBA`
13	Tschofenig	15. Januar 2026	Messaging
14	Rademacher	22. Januar 2026	Moderne Netzstrukturen

Semesterplanung — Übungen und Praktika

ID	KW	Art	Thema
	40	/	/
UE-1	41	Übung	Topologien und OSI
UE-2	42	Übung	Übertragungen bspw. Kabel
P-1	43	Praktikum	Laboreinführung und Netzwerktools
S-1	44	Video	IPv4
P-2	45	Praktikum	Adressierung
P-3	46	Praktikum	IPv4 und Autokonfiguration
P-4	47	Praktikum	IPv6 und Autokonfiguration
P-5	48	Praktikum	Routing
P-6	49	Praktikum	Switching
P-7	50	Praktikum	Transportprotokolle
S-2	51	Experiment	VPN
S-2	52	Experiment	VPN
	2	/	/
P-8	3	Praktikum	DNS
P-9	4	Praktikum	Webkommunikation

UE - Übung laut Stundenplan in den Seminarräumen

P - Praktikum in C055

S - Selbststudium KEINE Präsenz

Agenda

- Motivation: Warum Netzwerksegmentierung?
- Repeater (Layer 1)
- Switch (Layer 2)
- Spanning Tree Protokoll (STP / RSTP)
- VLAN (logische Segmentierung)
- Router (Layer 3)

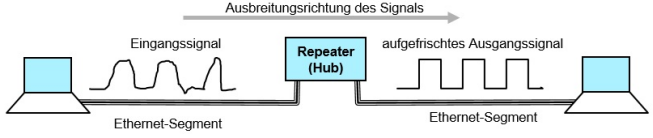
Warum Segmentierung?

- Begrenzung von Broadcast-Domänen → geringere Netzlast
- Reduzierung von Kollisionen durch Trennung von Kollisionsdomänen
- Erhöhung von Ausfallsicherheit und Redundanz:
  - Störungen bleiben auf einzelne Segmente begrenzt
  - Wartung und Änderungen ohne Beeinträchtigung anderer Segmente möglich
  - Redundante Pfade oder Systeme pro Segment realisierbar
- Verbesserung von Sicherheit
  - Schadsoftware oder Angriffe bleiben auf ein Segment begrenzt
  - Kontrolle des Verkehrs zwischen Segmenten durch Firewalls/ACLs nötig
  - Bestandteil einer „Defense-in-Depth"-Strategie

Repeater (Layer 1)

Repeater: Grundprinzip

- Arbeitet auf dem Physical Layer (Bitübertragungsschicht)
- Regeneriert / verstärkt eingehende Signale taktgerecht
- Sendet eingehende Signale an **alle** anderen Ports weiter
- Ein Ausfall eines Netzteils betrifft nur den jeweiligen Teil des Netzes
- Wichtig: Die Kollisionsdomäne wird **nicht** begrenzt!
- Ein Repeater verlängert ein Segment – er segmentiert nicht.
- Terminologie: Ein **Hub** ist ein Multiport-Repeater.



Switch (Layer 2)

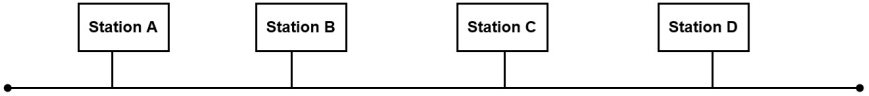
Switch – Einstieg

Switch[a]

[a] Natürlich sprechen wir hier nicht von der Nintendo Switch, https://de.wikipedia.org/wiki/Nintendo_Switch.

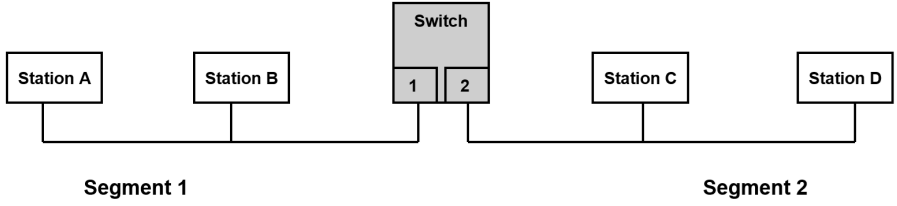
LAN ohne Switch

- Wie sieht die Netzlast aus?
- Wer hört mit, wer kollidiert mit wem?



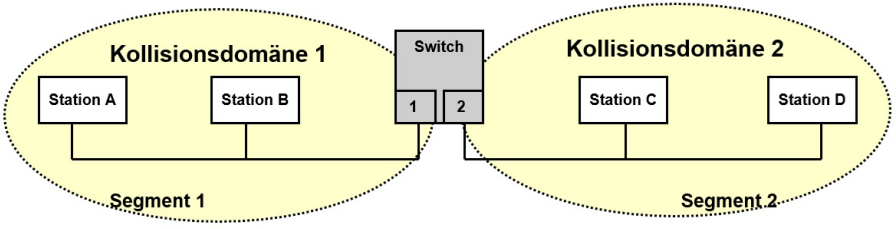
LAN mit Switch

- Wie verändert sich die Last?
- Welche Kommunikation läuft noch an alle? Welche nur Punkt-zu-Punkt?



Was macht ein Switch technisch?

- Filtert Frames anhand der **Ziel-MAC-Adresse**
- Verwirft fehlerhafte Frames (CRC-Prüfung)
- Trennt Kollisionsdomänen: Jeder Port ist eine eigene Kollisionsdomäne
- Broadcasts werden weiterhin an alle Ports desselben Layer-2-Segments weitergeleitet

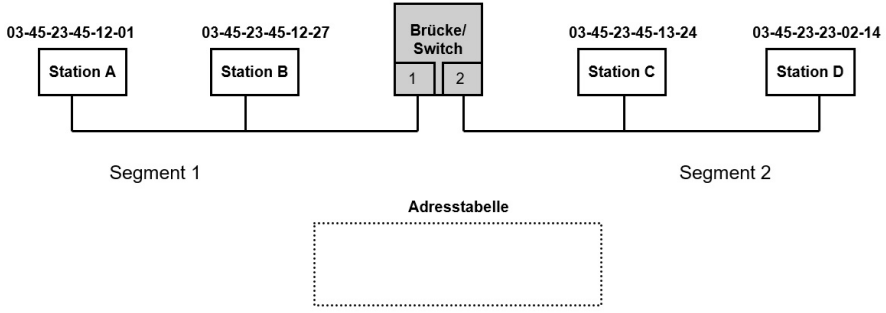


Lernende Adresstabellen

- Der Switch baut eine Tabelle **Port** $\rightarrow$ **MAC-Adresse** auf
- Lernen passiert anhand der **Absender**-MAC-Adresse eingehender Frames
- Weiterleitung passiert anhand der **Ziel**-MAC-Adresse
- Wenn Ziel unbekannt: Flooding (an alle Ports außer den Eingangsport)

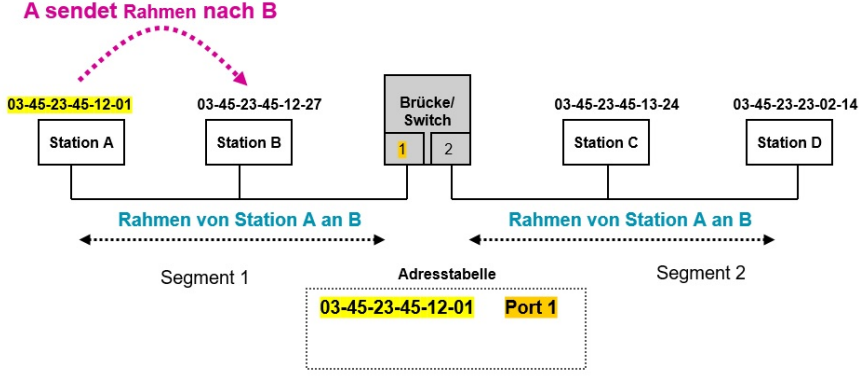
Aufbau der Adresstabelle (1)

- Start: Tabelle ist leer
- Switch beobachtet eingehende Frames



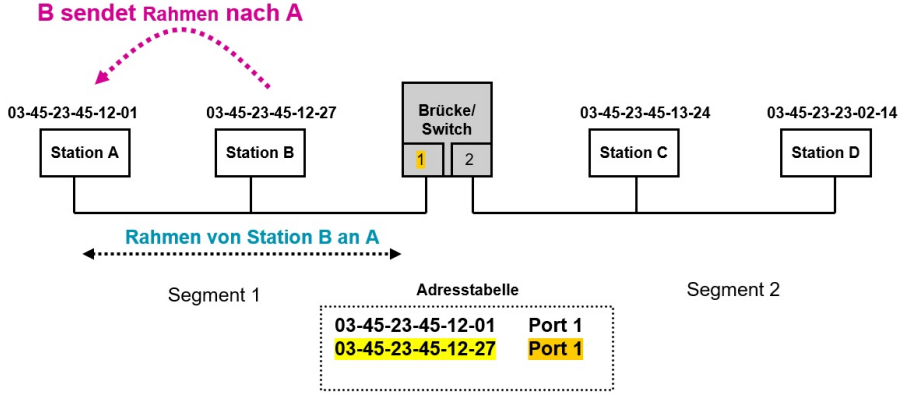
Aufbau der Adresstabelle (2)

- Erster Eintrag entsteht
- Für unbekannte Ziele: Frame wird ins andere Segment geflutet



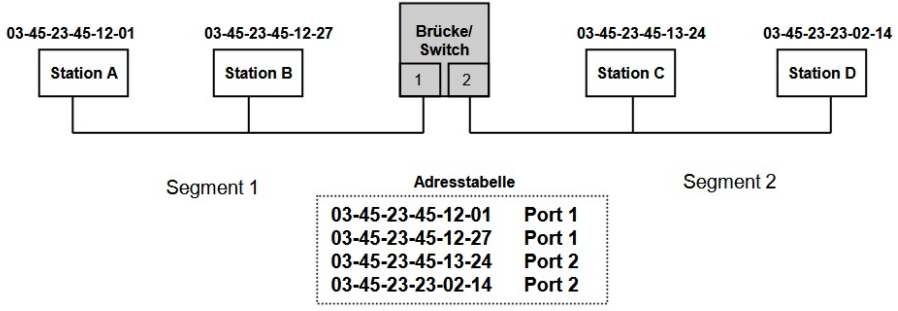
Aufbau der Adresstabelle (3)

- Mehr Geräte wurden gelernt
- Zum ersten Mal ist gezielte Weiterleitung möglich: kein Flooding mehr nötig



Aufbau der Adresstabelle (4)

- Nach einiger Zeit: vollständige Forwarding-Tabelle
- Kommunikation läuft gezielt Port-zu-Port



Grundfunktionen eines Switches

- Ein Switch ist eine Netzkomponente auf Schicht 2
- Lasttrennung durch Frame-Filterung
- Auftrennung von Kollisionsdomänen (jeder Port eigene Kollisionsdomäne)
- Für Endgeräte transparent (sie „merken“ den Switch nicht)
- **Broadcast- vs. Kollisionsdomäne:**
  - Kollisionsdomäne: durch Switch-Ports begrenzt
  - Broadcastdomäne: erst durch Router (Layer 3) begrenzt
- Selbstlernend: Der Algorithmus funktioniert in jeder schleifenfreien Topologie

Zwischenfazit: Switches

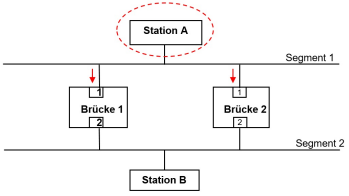
- Switches arbeiten auf **Layer 2**.
- Sie trennen Kollisionsdomänen und lernen MAC-Adressen.
- Broadcasts existieren weiterhin.
- ARP-Broadcasts oder DHCP-Discover-Nachrichten werden an alle angeschlossenen Rechner (also innerhalb derselben Broadcast-Domäne) weitergeleitet.

Nächster Schritt: Mehrere Switches mit Redundanz → Gefahr von Schleifen → Spanning Tree.

Spanning Tree Protokoll

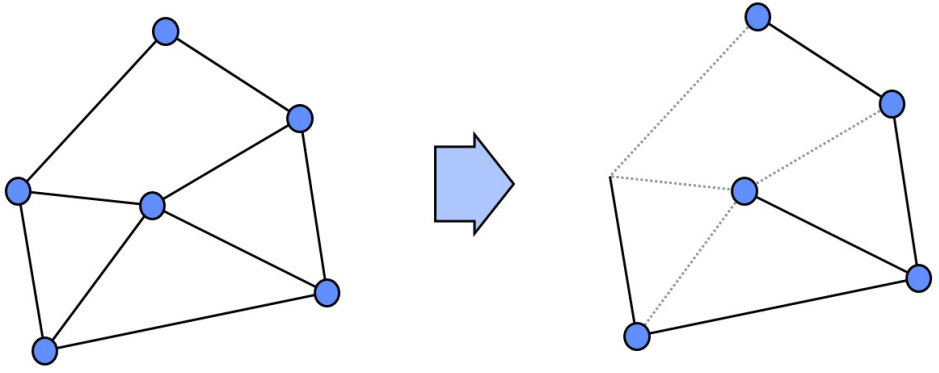
Motivation: Redundante Pfade

1. Redundante Verbindungen erhöhen Ausfallsicherheit
2. Aber: Schleifen zerstören die Forwarding-Tabellen
3. Frames können endlos im Kreis laufen (Broadcast Storm)
4. Ergebnis: Netz ist unbenutzbar



Idee des Spanning Tree Protokolls (STP)

- Switches einigen sich auf eine **logische, schleifenfreie Topologie**
- Bestimmte Ports werden in den Blockierzustand versetzt
- Ergebnis: Zwischen zwei beliebigen Knoten existiert genau **ein** aktiver Pfad
- Während der Neuberechnung werden Datenpfade kurz unterbrochen



Historischer Kontext

Radia Perlman entwickelte das Spanning Tree Protokoll [4].

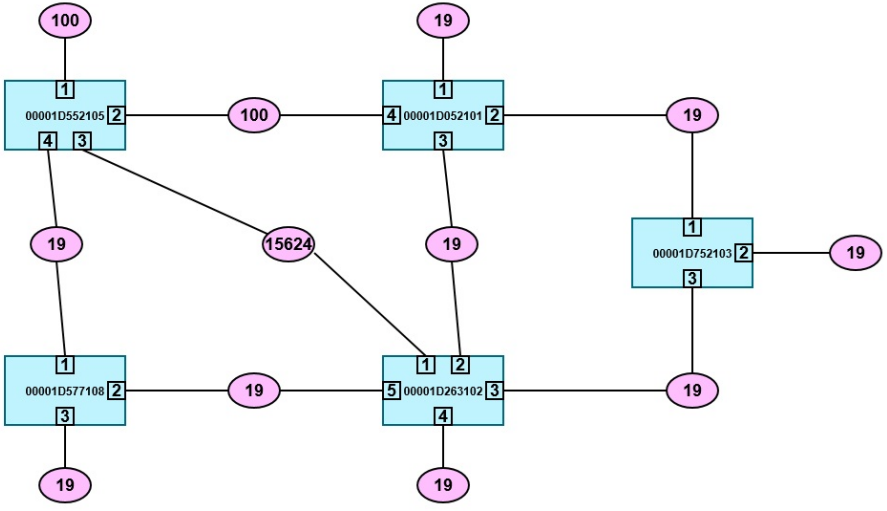
- Standardisiert in IEEE 802.1D [1]
- Grundlage für redundante Layer-2-Netze

Ablauf des Spanning Tree Algorithmus (Überblick)

1. Wahl einer **Root-Bridge** (Switch mit kleinster Bridge-ID = Priority + MAC)
2. Für jeden anderen Switch: Wahl eines **Root-Ports** (Pfad mit geringsten Kosten zur Root-Bridge)
3. Für jede Kollisionsdomäne: Bestimmung eines **Designated Ports** (Port mit besten Pfadkosten für dieses Segment)
4. Alle übrigen Ports werden **blockiert**

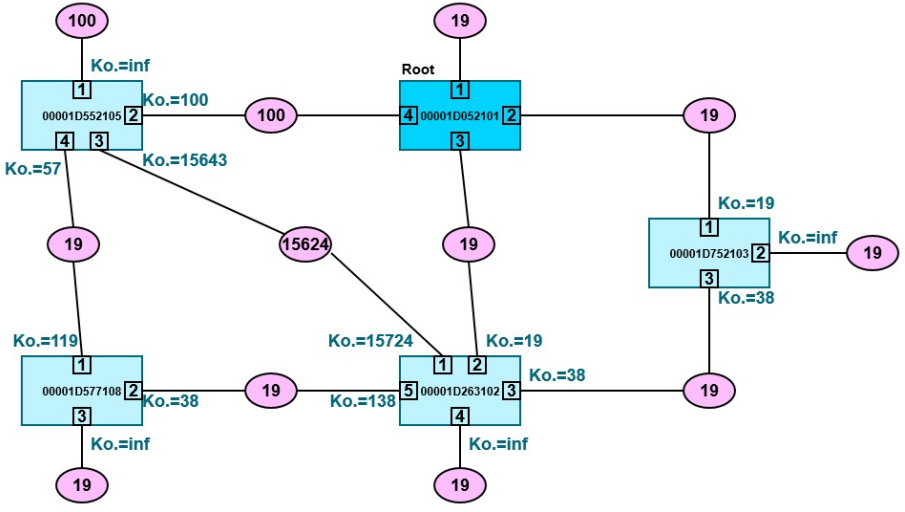
STP – Schritt 0: Topologie & Pfadkosten

- Pfadkosten orientieren sich an der Link-Geschwindigkeit (IEEE 802.1D)



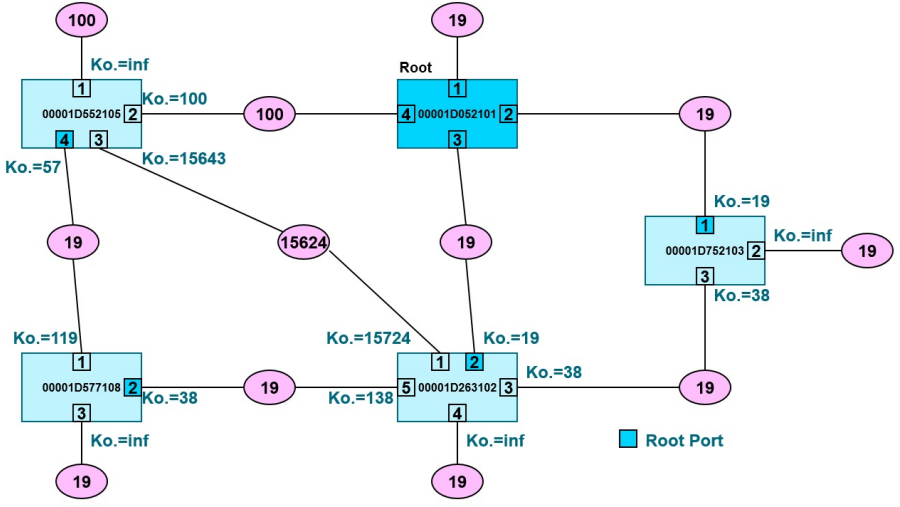
Schritt 1: Root-Bridge bestimmen

- Switch mit niedrigster Bridge-ID wird Root
- Alle Ports der Root-Bridge gelten als „designated“



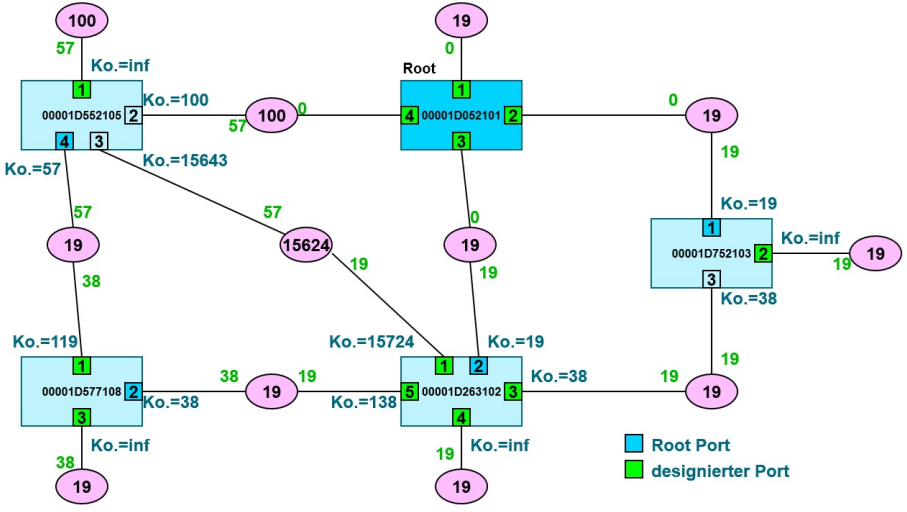
Schritt 2: Root-Ports wählen

- Jeder Nicht-Root-Switch bestimmt seinen besten Weg zur Root
- Dieser Port wird Root-Port



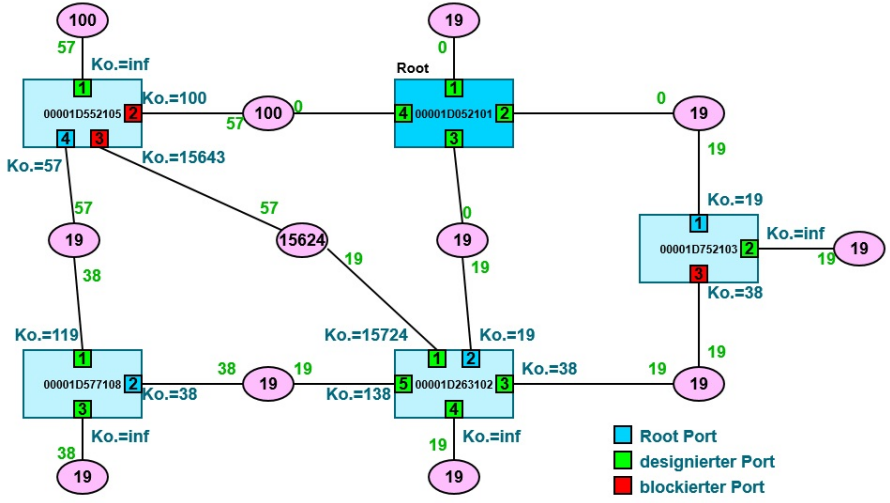
Schritt 3: Designated Ports wählen

- Pro Kollisionsdomäne genau ein aktiver Weiterleitungsport
- Der Port mit den geringsten Pfadkosten zur Root-Bridge gewinnt
- Falls Gleichstand: niedrigste Bridge-ID

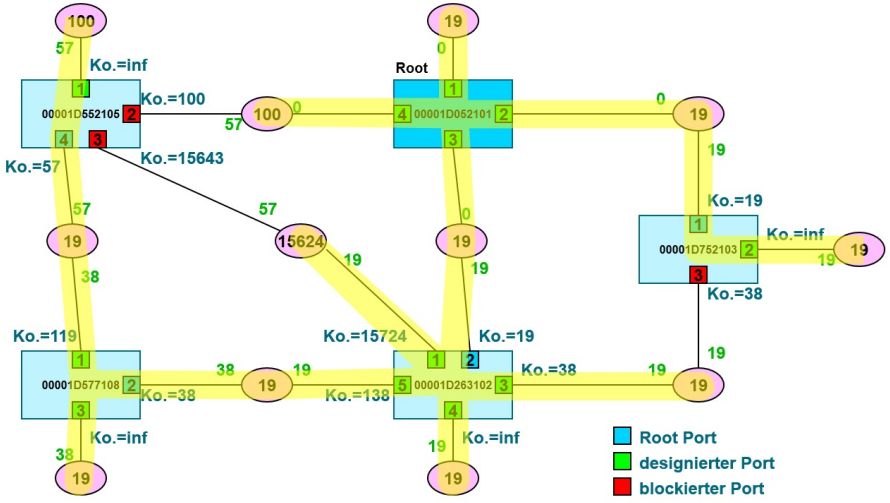


Schritt 4: Blockierte Ports

- Alle anderen Ports gehen in den Blockier-Zustand
- Schleifen sind damit entfernt



Ergebnis: Logischer Spannbaum



Von STP zu RSTP

- Klassisches STP (IEEE 802.1D): vergleichsweise langsam bei Topologieänderungen
- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w [2]):
  - Schnellere Konvergenz (typisch ≤ 6 Sekunden)
  - Schnelle Wiederherstellung bei Link- oder Switch-Ausfall
- Sicherheit:
  - Gefälschte STP-/BPDU-Frames können Neuberechnungen auslösen
  - Angriffsvektor: Netz kurzzeitig lahmlegbar

Zwischenfazit: Spanning Tree

- STP verhindert Layer-2-Schleifen durch Blockieren einzelner Ports.
- RSTP reagiert deutlich schneller auf Änderungen.
- Redundanz bleibt möglich, aber ohne Broadcast-Stürme.

Nächster Schritt: Wie trennen wir Netze logisch für Teams / Abteilungen? → VLAN.

VLAN (Virtuelle LANs)

VLAN: Grundidee

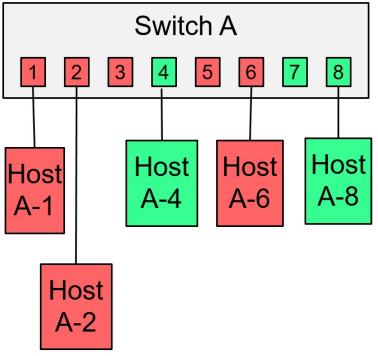
- Ein VLAN (Virtual LAN) ist ein **logisches** Layer-2-Netz
- Ein VLAN bildet eine eigene **Broadcastdomäne**
- Geräte können unabhängig von ihrer physischen Position logisch gruppiert werden
- Jedes VLAN benötigt einen eigenen IP-Adressbereich
- Kommunikation zwischen zwei VLANs erfolgt nur über einen Router / Layer-3-Switch

Warum VLANs?

- Flexibilität bei der Zuordnung von Endgeräten (z. B. Abteilungen, Stockwerke, VoIP)
- Trennung / Isolation von Verkehr (Security)
- Priorisierung von Datenverkehr (Quality of Service)
- Broadcast-Kontrolle

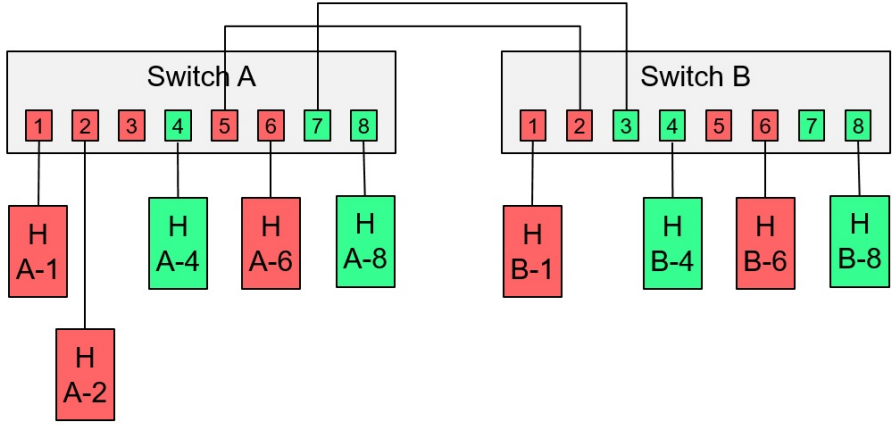
Mehrere VLANs auf einem Switch

1. Ein physischer Switch kann logisch in mehrere VLANs aufgeteilt werden
2. Ports werden VLANs zugewiesen
3. Beispiel: Ports 1, 2 und 6 = VLAN rot; Ports 4 und 8 = VLAN grün



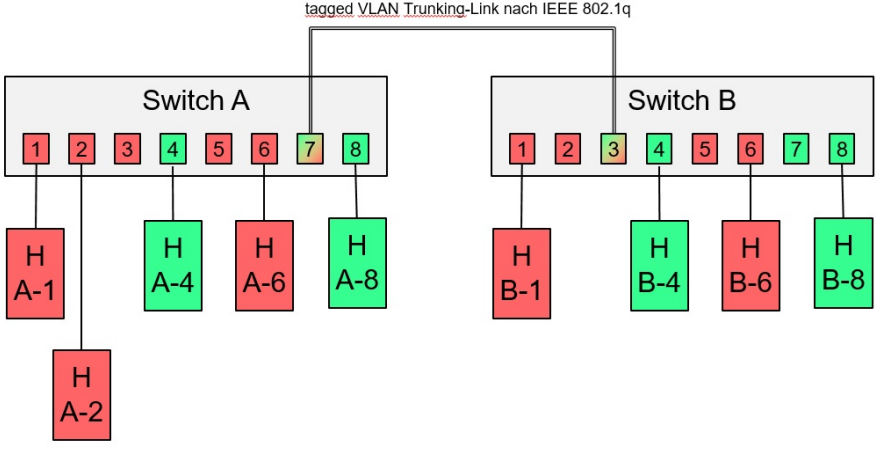
VLANs über mehrere Switches koppeln

- VLAN-rot und VLAN-grün sind logisch getrennt
- Hosts verschiedener VLANs liegen in unterschiedlichen IP-Netzen
- Ohne Router können diese VLANs **nicht** miteinander sprechen



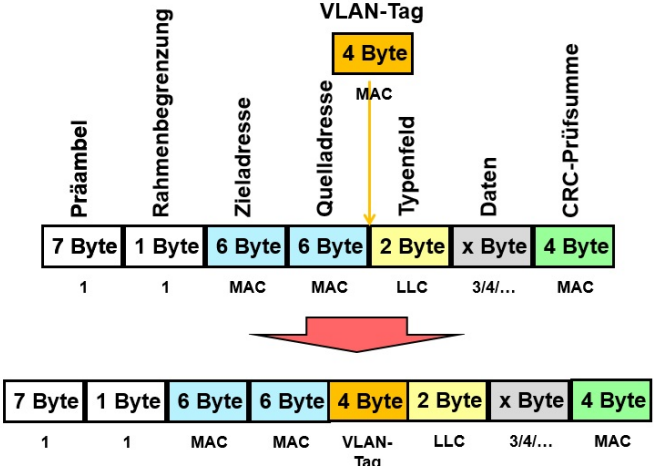
802.1Q-Trunking (Tagged VLANs)

- IEEE 802.1Q [3]: Frames werden mit einem VLAN-Tag versehen
- Ein **Trunk-Link** zwischen Switches trägt Frames aus mehreren VLANs gleichzeitig
- Auf dem Trunk laufen markierte Frames (z. B. VLAN-rot und VLAN-grün)



Ethernet-Frame mit VLAN-Tag (802.1Q)

- Tag enthält u. a. die VLAN-ID
- EtherType 0x8100 kennzeichnet getaggte Frames

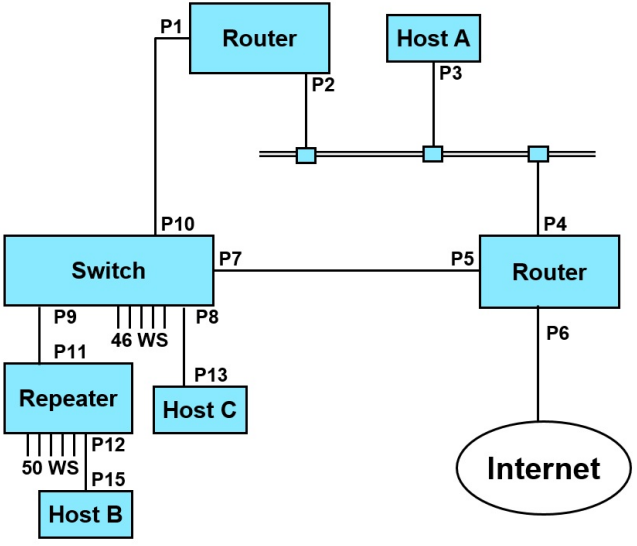


Quiz: Kollisions- vs. Broadcastdomänen

Fragen:

1. Welche Ports gehören zur selben Kollisionsdomäne?
2. Welche Ports gehören zur selben Broadcastdomäne?

Die Verbindung ins Internet wird nicht berücksichtigt.



Zwischenfazit: VLANs

- VLANs trennen Layer-2-Netze logisch statt physisch.
- Jedes VLAN ist eine eigene Broadcastdomäne & bekommt einen eigenen IP-Adressbereich.
- Kommunikation zwischen VLANs geht nur über Layer 3.

Nächster Schritt: Wer verbindet diese VLANs (und das Internet)? → Router.

Router (Layer 3)

Router – Rolle im Netz

Der Router als klassische Schicht-3-Komponente:

- Ein Router arbeitet auf Schicht 3 und wertet IP-Informationen aus
- Wichtigste Aufgabe: **Wegewahl** (Routing) zwischen Netzen
- Router begrenzen Broadcastdomänen
- Frage: Wie trifft ein Router Weiterleitungsentscheidungen?

Entscheidung des Routers

- Der Router sucht in der Routingtabelle nach dem besten Eintrag für das Zielpräfix
- Das Paket wird über das dazugehörige Ausgangs-Interface weitergeleitet
- Falls kein spezifischer Eintrag existiert:
  - Weiterleitung an das Standard-Gateway (Default Route)

Innere Architektur eines Routers

- Ein Router ähnelt einem spezialisierten Computer (ohne klassische Peripherie wie Monitor oder Tastatur)
- Wichtige Speicherarten:
  - **ROM** (Read-Only Memory) – enthält Bootloader und Grundfunktionen
  - **Flash** (nichtflüchtiger Speicher) – speichert das Betriebssystem und Konfigurationen
  - **RAM** (Random Access Memory) – Arbeitsspeicher für laufende Prozesse und Routingtabellen
- Ein interner Systembus (z. B. **PCIe**, Peripheral Component Interconnect Express) verbindet Interfaces mit CPU und Speicher
- Für hohe Performance: spezialisierte Hardware wie **ASICs** (Application-Specific Integrated Circuits) oder **FPGAs** (Field-Programmable Gate Arrays) für Paket-Forwarding
- Viele verschiedene Netzwerkinterfaces sind integraler Bestandteil des Designs

Konfiguration eines Routers (Überblick)

- Vergabe von IP-Adressen und Netzmasken für Interfaces
- Auswahl und Konfiguration der Routingprotokolle
- NAT / NAPT
- DHCP für angeschlossene Netze
- Paketfilterung / Firewall-Regeln

Zusammenfassung

- Layer 1: Repeater – Signale regenerieren, keine Segmentierung
- Layer 2: Switch – MAC-basiertes Forwarding, Kollisionsdomänen trennen
- STP / RSTP – verhindert Layer-2-Schleifen trotz Redundanz
- VLAN – logische Trennung in Broadcastdomänen
- Layer 3: Router – verbindet Netze und begrenzt Broadcast

Quellen I

[1] IEEE standard for local area network MAC (media access control) Bridges.
ANSI/IEEE Std 802.1D, 1998 Edition (1998), 1–373.

[2] IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Common Specifications – Part 3: Media Access Control (MAC) Bridges – Amendment 2 – Rapid Reconfiguration.
IEEE Std 802.1w-2001 (2001), 1–116.

[3] IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks.
IEEE Std 802.1Q-2022 (Revision of IEEE Std 802.1Q-2018) (2022), 1–2163.

[4] Perlman, R.
An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN.
Computer Communication Review - CCR 15 (09 1985), 44–53.