Ethernet VLAN/802.1q

mehr als nur ein geteilter Switch

Jörg Kinzebach <joerg@duck.franken.de>

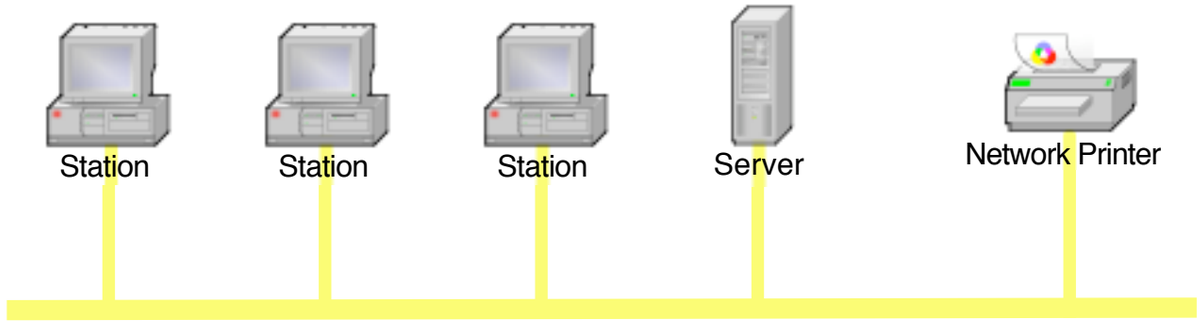
Ethernet VLAN/802.1q

- Ethernet (IEEE 802.3)
- Ethernet Switching
- Anwendung von VLANs
- 802.1q Framing
- Konfiguration
- Szenarien für VLAN-Nutzung
- Security

Gründe für den Einsatz der VLAN Technologie

- Vereinfachung des Netzes (weniger Geräte)
- Netzwerk-Sicherheit (Gruppierung)
- Abbildung der Organisations-Struktur auf die Netzwerk-Topologie
- Performance (Kontrolle von Broadcasts)
- Kostensenkung (Einsparung von Router-Interfaces)
- Transport von Layer3-Protokollen

Ethernet

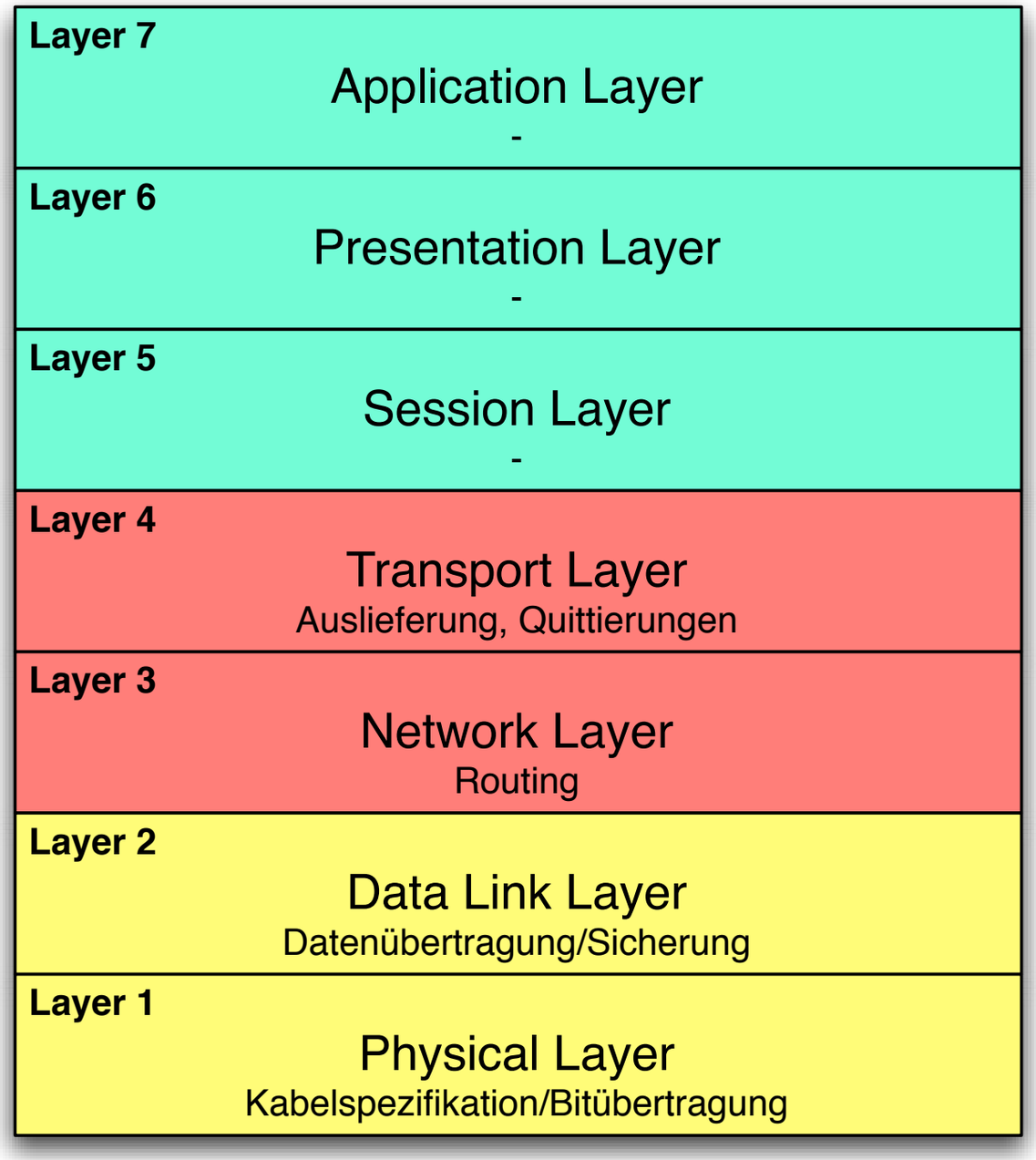


- IEEE 802.2 (IEEE = Institute of Electrical and Electronics Engineers)

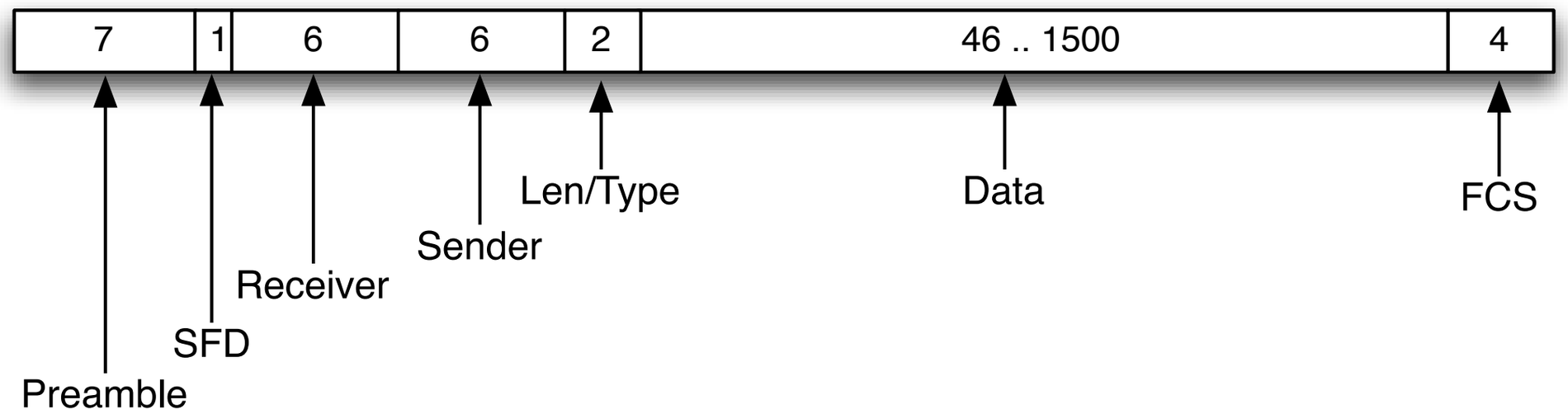
  Adressierung nach IEEE 802.1, Rahmenformate nach IEEE 802.2 und IEEE 802.3
- „Shared Medium“
- Ethernet Frames
- Koax (10Base5 - Thicknet, 10Base2 - Thinnet)
- Twisted Pair (10BaseT, 100BaseT, 1000BaseT, ...)
- Glasfaser (100BaseFX, 1000BaseFX, ...)
- Verbindungs-Los
- Leistung erhöht sich bisher kontinuierlich (3MBit/s, 10MBit/s, 100Mbit/s, 1GBit/s, 10Gbit/s, ...)

Ethernet im OSI Schichtmodell

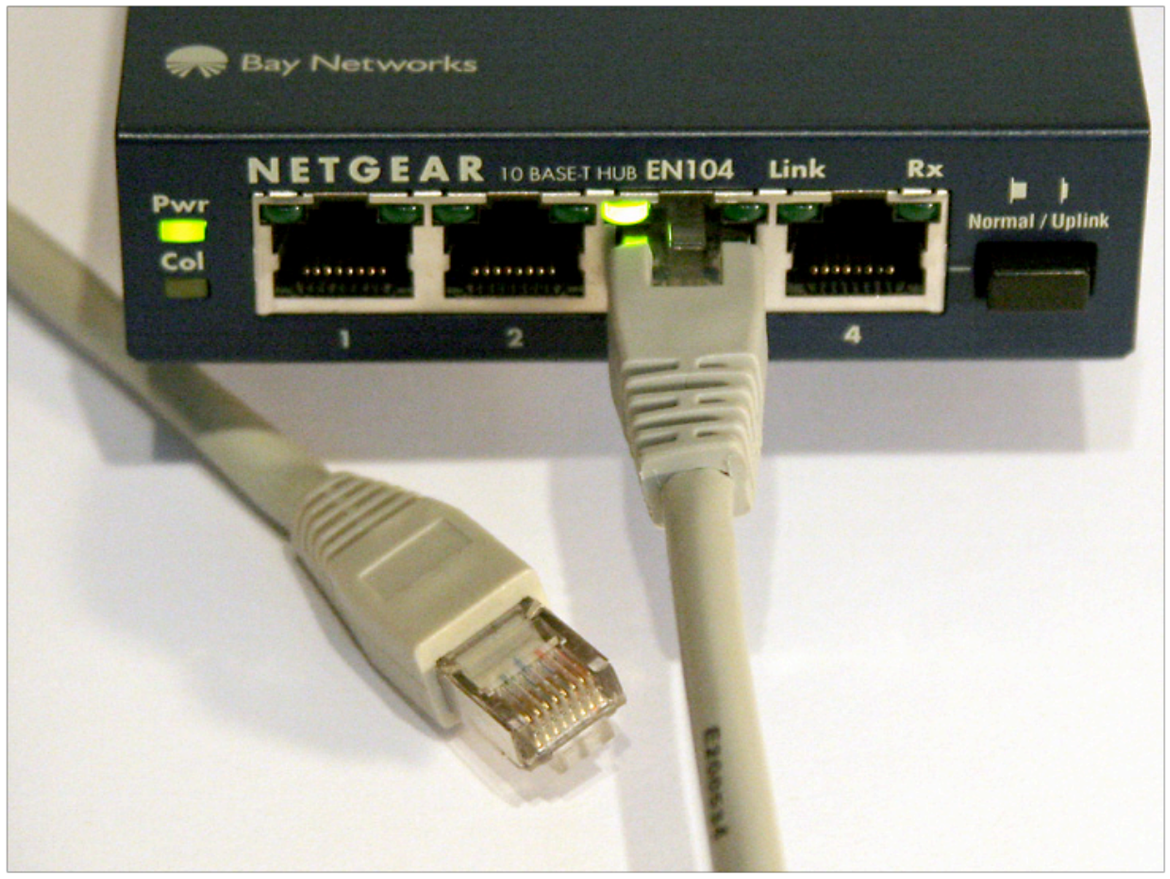
- CSMA/CD (Carrier Sense Multiple Access/Collision Detect)
- Logical Link Layer (LLC)
- Media Access Control (MAC)



Ethernet-Frame



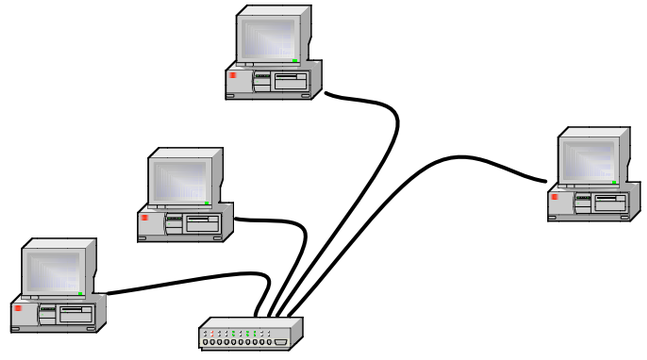
- Preamble + SFD: Synchronisation von Sender und Empfänger
- Receiver + Sender: Identifikation der Endpunkte (00:40:63:E7:29:16)
- Len/Type: Protokoll Typ oder Länge von Ethernet-Daten (DIX / Ethernet II)
- Data: bei Len/Type = 0x0800 ein IP-Paket
- FCS: 32 Bit Checksumme ohne Preamble und FCS

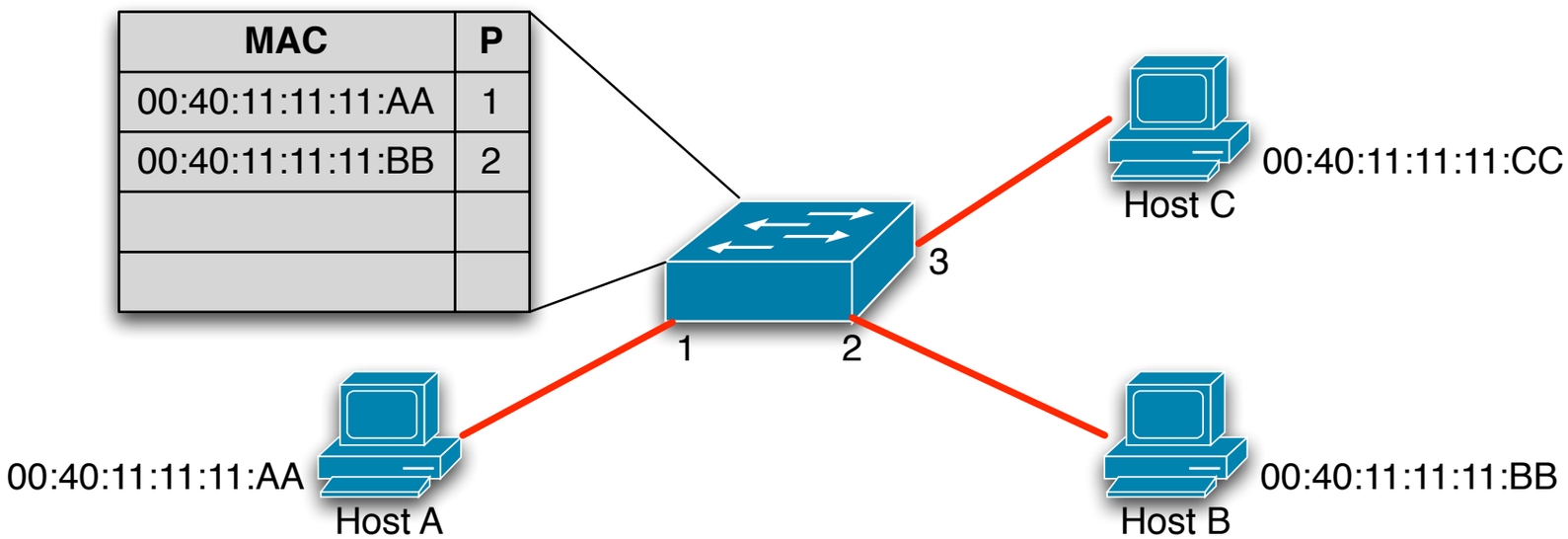


10Base2 und 10BaseT Vernetzung

Switched Ethernet LAN

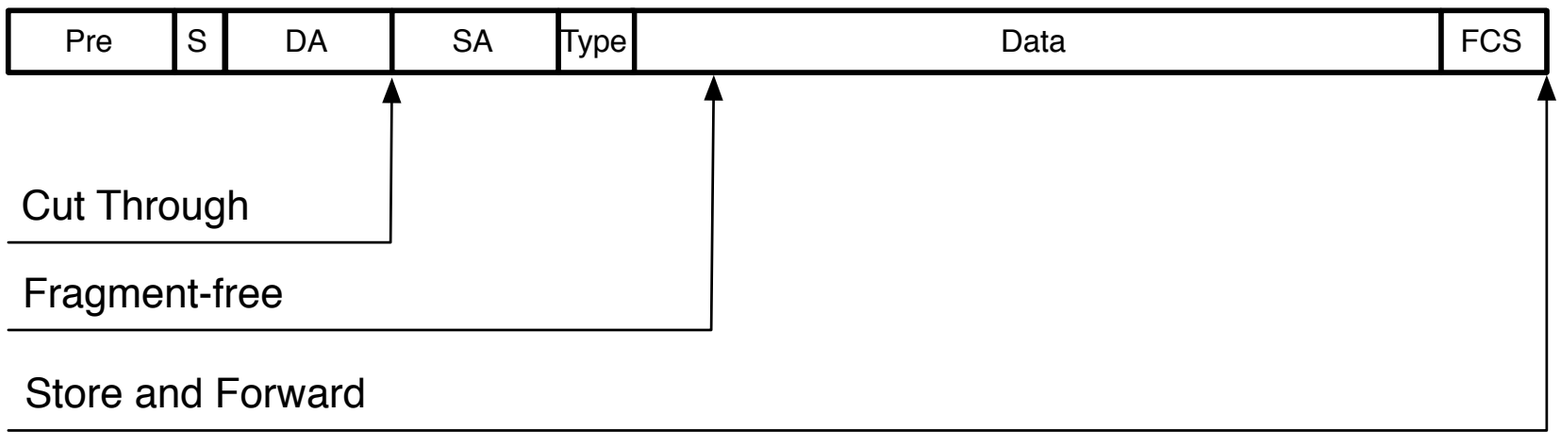
- Stern-Topologie
- physikalische Punkt zu Punkt Verbindung zwischen zwei Netzwerk-Nodes
- weiterhin „Shared Medium“
- mehrere Nodes können parallel kommunizieren
- Switch verwaltet MAC-Table mit Zuordnung von Adressen zu Ports



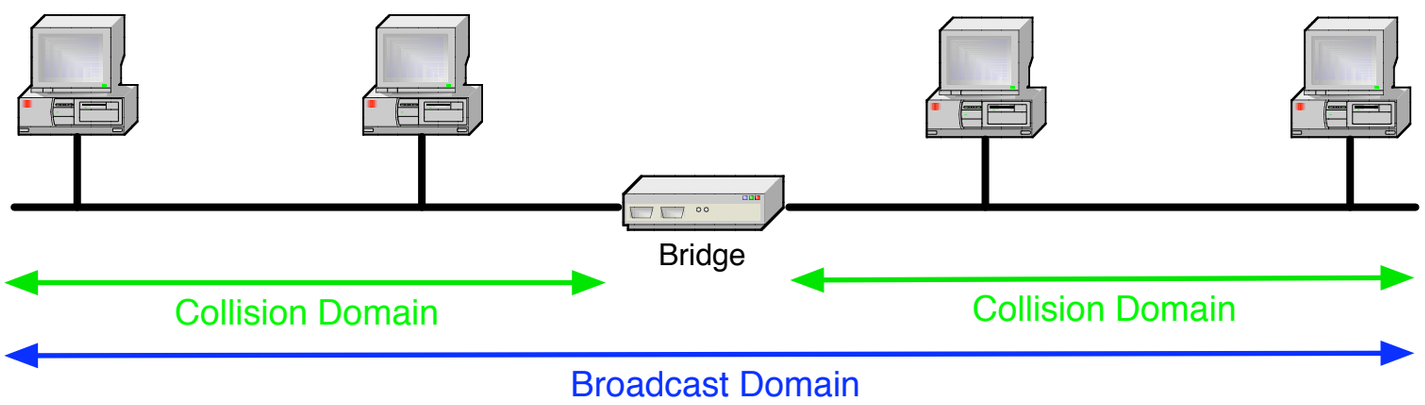


Switching

- Cut Through
  Weiterleitung sobald Empfängeradresse empfangen wurde
- Fragment-Free (Variante von Cut-Through)
  Weiterleitung nach Empfang der ersten 64 Octets wenn Destination-Port bereit
- Store and Forward
  Weiterleitung wird gestartet, wenn das komplette Frame empfangen und analysiert wurde



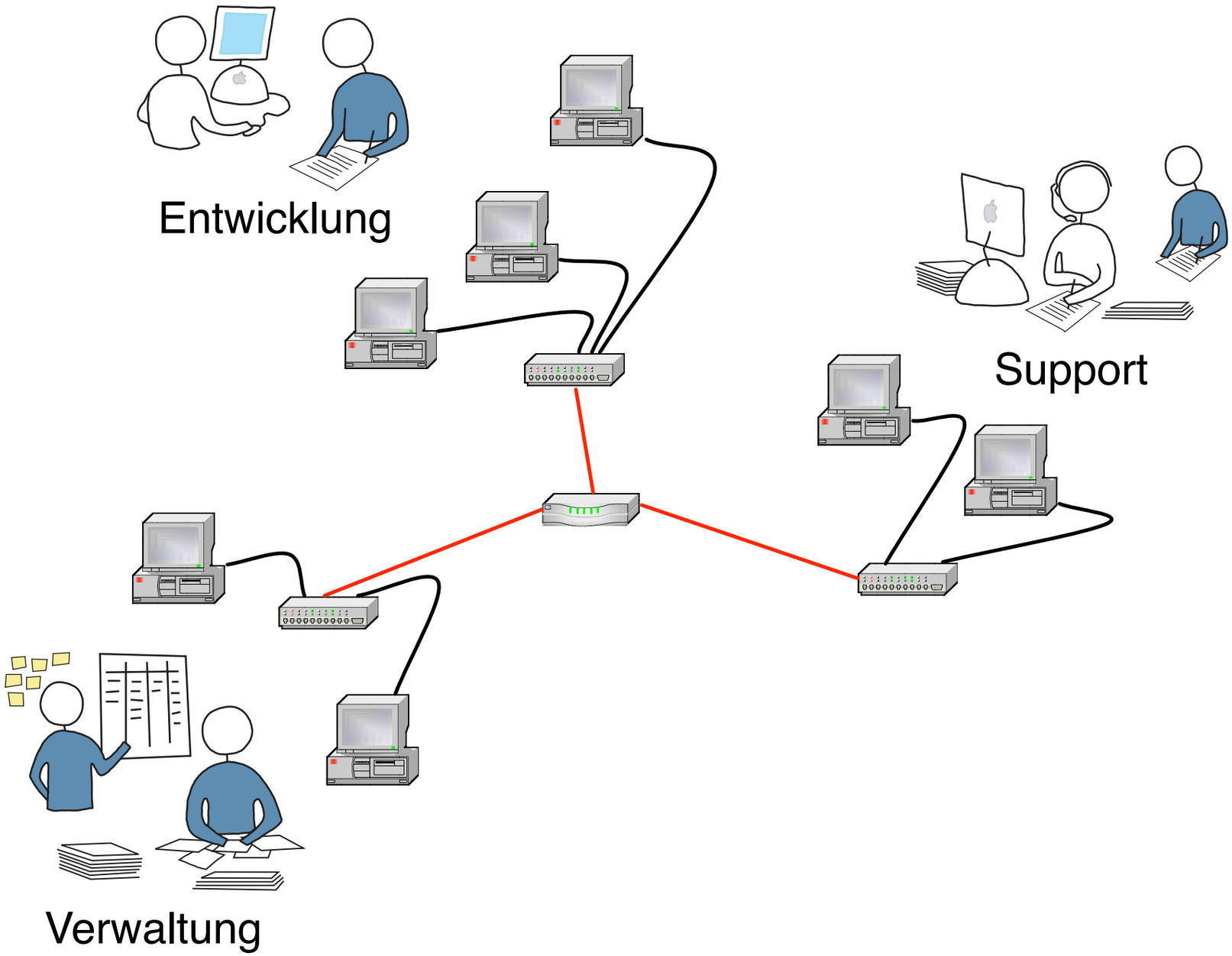
Collision und Broadcast



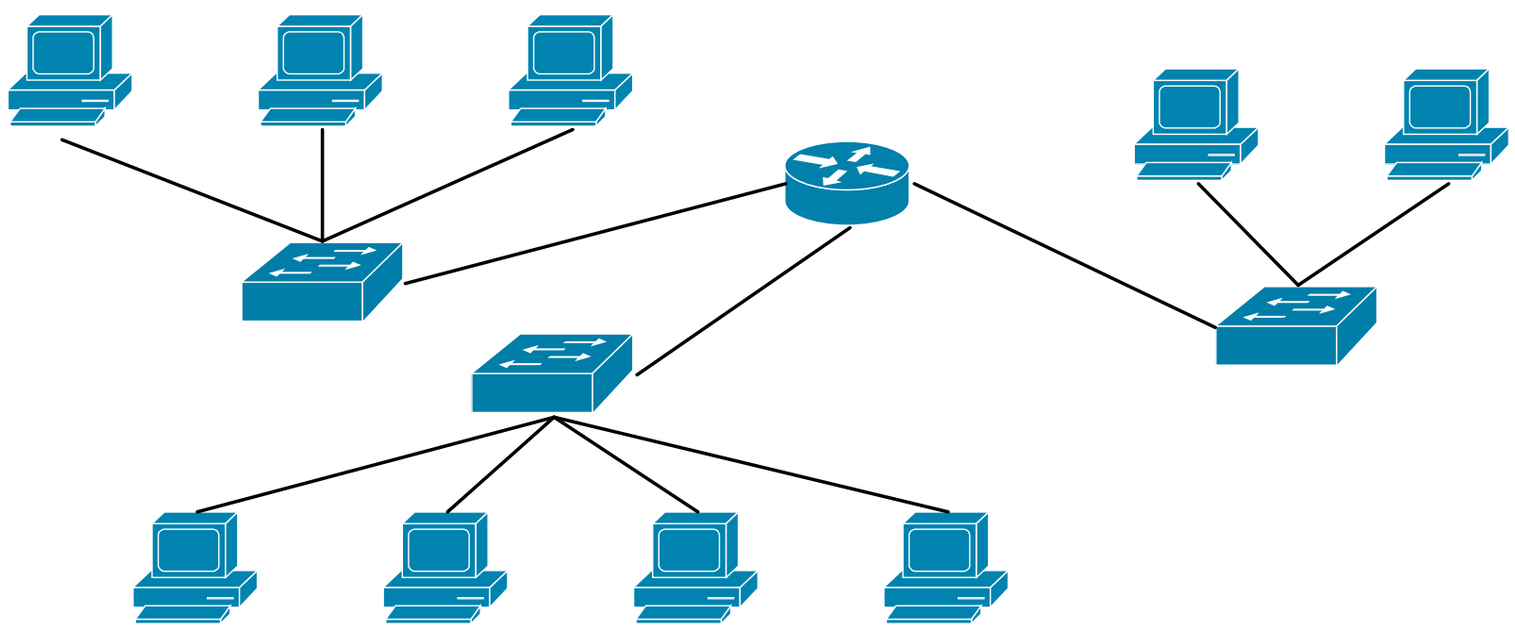
- Eine Collision Domain umfasst alle Rechner in einem physikalischen Segment

- Alle Rechner eines Ethernet oder IP-Subnetzes sind in einer Broadcast Domain, eine Broadcast-Domain kann aus vielen Collision Domains bestehen

Die Firma

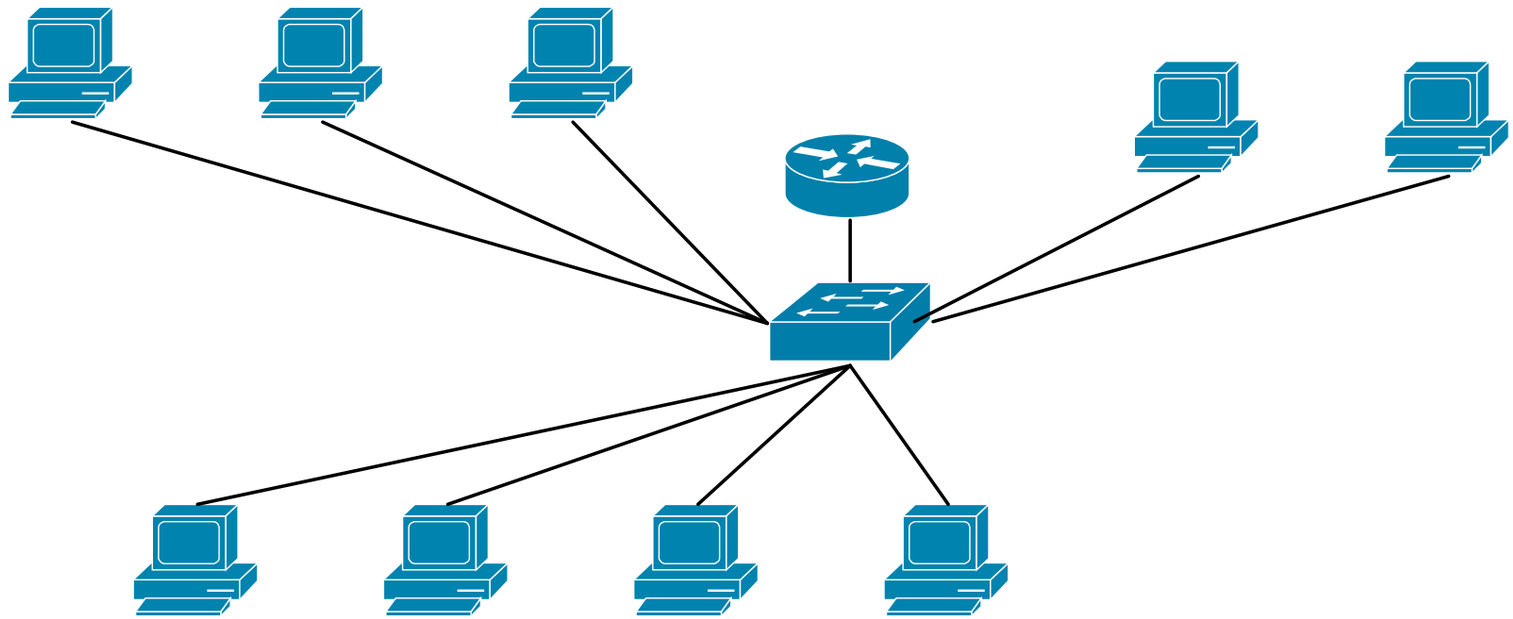


Das Netz mit vielen Switchen



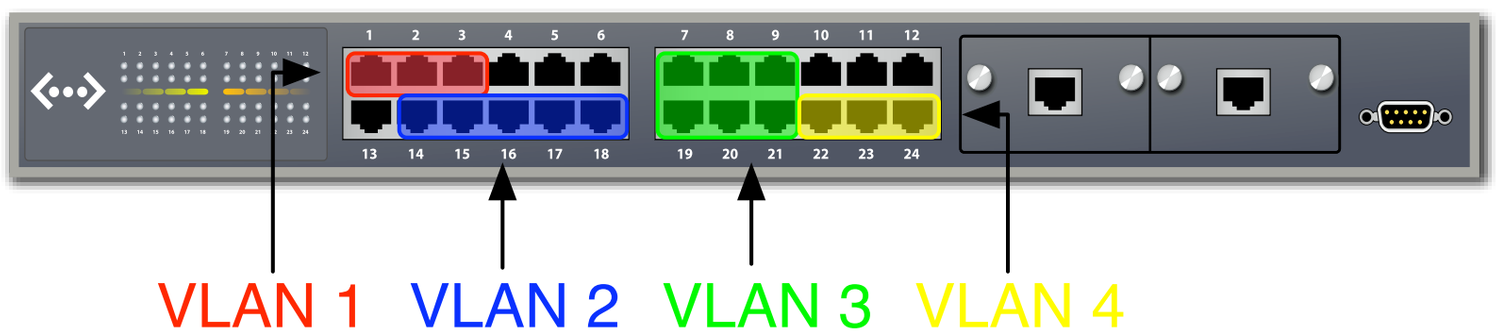
- Jede Abteilung besitzt eigenen Hub/Switch
- Switche sind mit zentralem Router verbunden

Das Netz mit VLANs zentralisiert



- Switch an zentraler, einfach auffindbarer Position
- Bessere Auslastung der Hardware
- Jeder Arbeitsplatz hat eine Leitung zum Switch
- Umzüge werden erleichtert

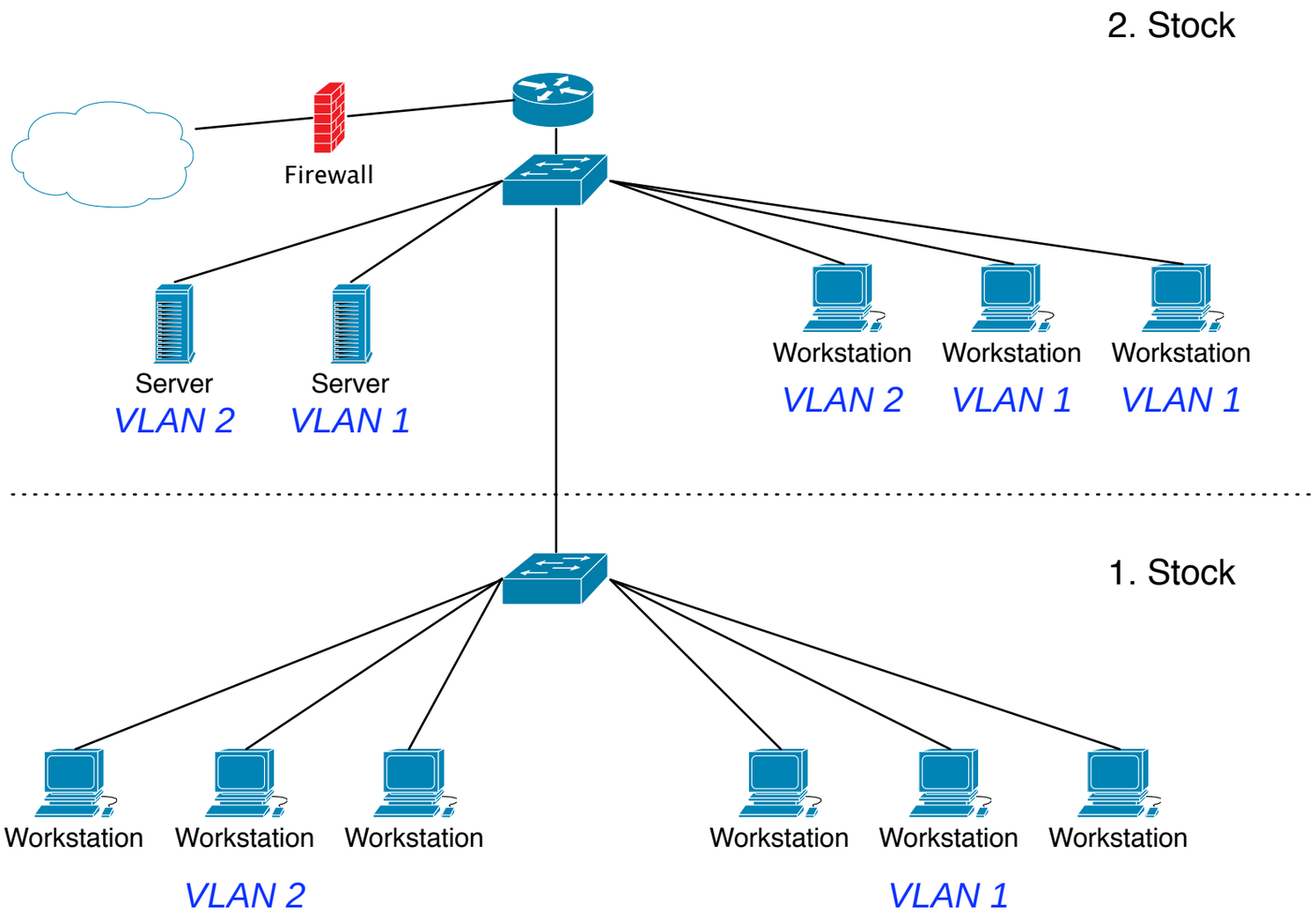
Der VLAN-Switch



- keine Verbindung im Switch zwischen VLANs
- eine Management und Monitoring-Schnittstelle

- port-based VLAN
- MAC based VLAN
- protocol-based VLAN
- IP-based VLAN

VLAN-Transport



- Transport mehrer VLANs zwischen zwei oder mehreren Switchen
- Verbindung zwischen Stockwerks-Verteilungen oder Gebäuden
- Routing zwischen VLANs

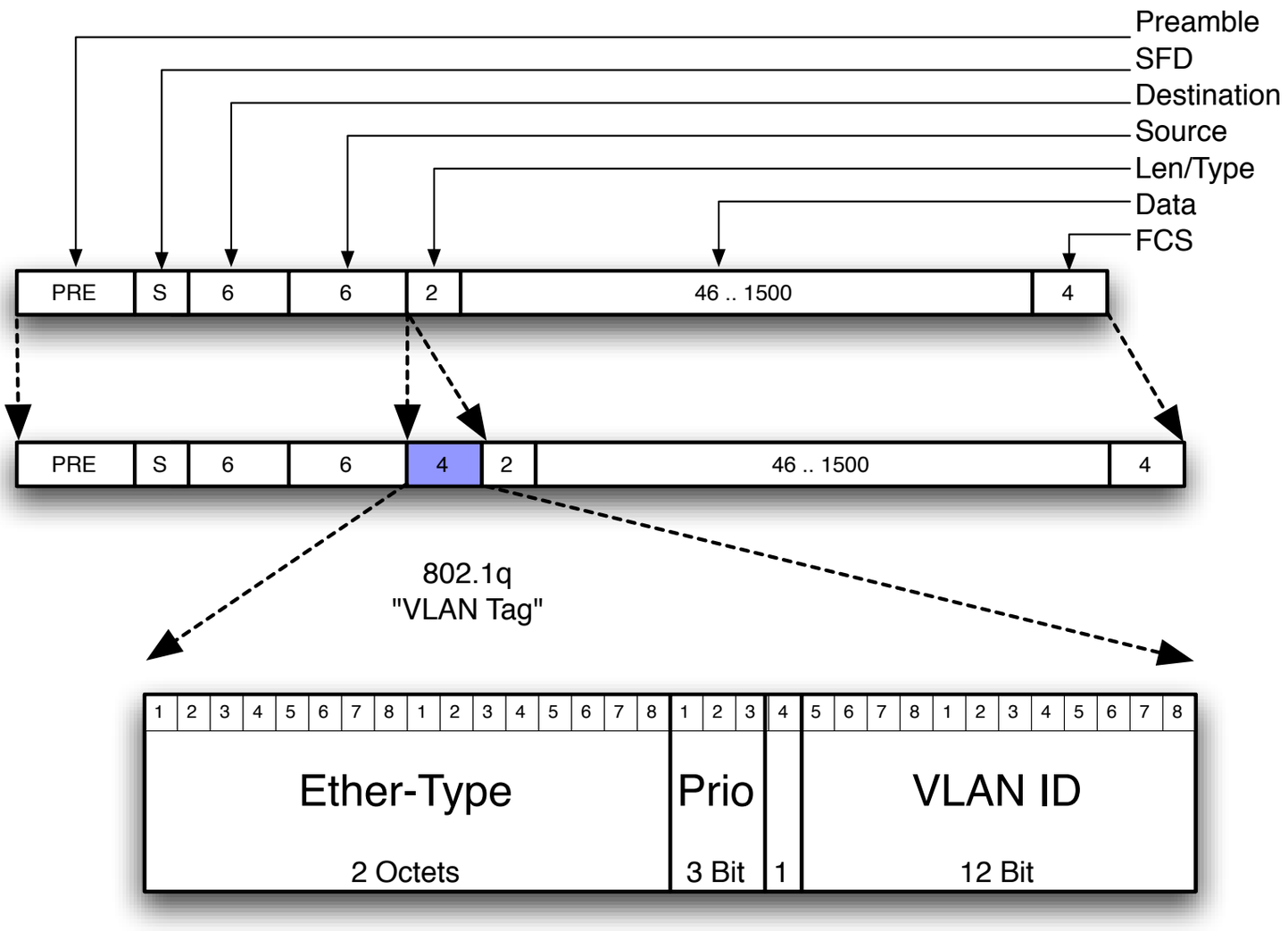
Kopplung von VLAN-fähigen Geräten

- Beim Transport von VLANs auf einem Link muß das Frame mit einer Markierung versehen werden, die es einem VLAN zuordnet („VLAN tagging“)
- ISL

  „Inter Switch Link“ (Cisco Proprietär)

  - nicht auf jeder Hardware verfügbar, auch von Cisco nicht mehr empfohlen
- IEEE 802.1Q
  - Herstellerunabhängiger interoperabler IEEE Standard
  - erlaubt CoS („Class of Service“) mit Hilfe von 802.1p
  - auch von Endgeräten unterstützt

IEEE 802.1q



- Ether Type: 802.1q
- Prio: CoS (Class of Service)
- VLAN ID: 0-4095

VLAN Konfiguration

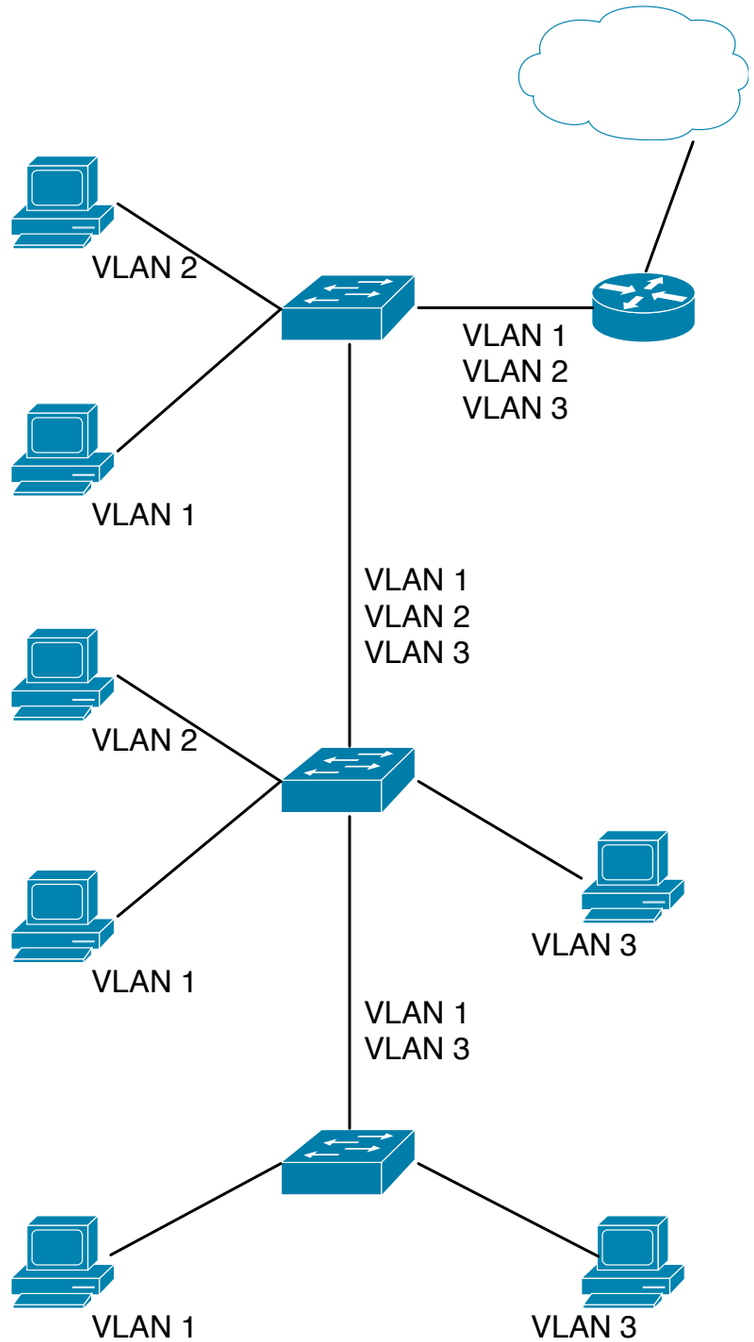
Port, Trunk, tagged, untagged

- Untagged Port entlässt Frames nach Entfernung der 802.1q Tags

- Tagged Port belässt 802.1q-Markierungen im Ethernet-Frame

- Trunk Port transportiert mehrere VLANs (tagged)

- PVID (Port VLAN Identifier) ist die Bezeichnung für das VLAN, dem eingehende Pakete ohne Tag zugewiesen werden



Konfigurationsbespiele

VLAN 1 + VLAN 3 auf Ethernet 2/1 tagged

CatOS

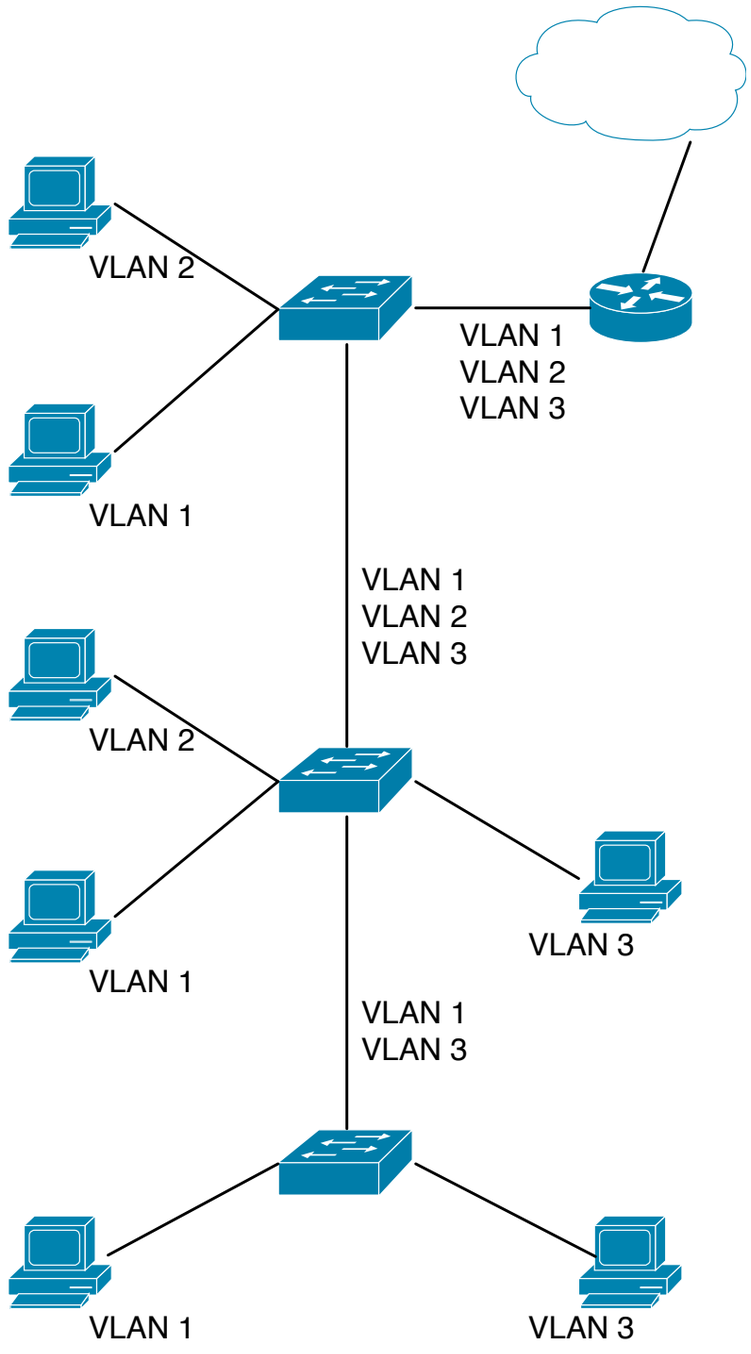
```
switch#(enable) set trunk 2/1 on dot1q 1,3
```

IOS

```
switch# interface FastEthernet2/1
switch(config-if)# switchport trunk encapsulation dot1q
switch(config-if)# switchport trunk allowed vlan 1,3
switch(config-if)# switchport mode trunk
```

Netgear

```
switch(config)# interface Ethernet 2/1
switch(config-if)# switchport access vlan tagged 1,3
```



VLAN 3 auf Ethernet 2/1 native (untagged)

CatOS

```
switch(enable)# set trunk Ethernet 2/2 off dot1q
switch(enable)# set vlan 3 2/1
switch(enable)# set vlan 3 name TestVLAN
```

IOS

```
switch(config)# vlan database
switch(config)# vlan 3
switch(config-vlan)# name TestVLAN
switch(config-vlan)# end
switch(config)# interface FastEthernet2/2
switch(config-if)# switchport access vlan 3
switch(config-if)# switchport mode access
```

Netgear

```
switch(config)# vlan database
switch(config-vlan)# vlan 3 TestVLAN
switch(config-vlan)# exit
switch(config)# interface Ethernet 2/2
switch(config-if)# switchport access vlan untagged 3
switch(config-if)# switchport access native 3
switch(config-if)# exit
```

NETGEAR® FSM700S Series Managed Stackable Switch

Support Help

UNIT 1

Navigation

- System
- Status
- Set-up
- Tools
- Security
- Advanced
  - Disable Advanced Alert
  - Port Mirroring
  - Port Trunking
  - Advanced Security
  - Advanced Tools
  - Traffic Management
  - VLANS
    - Primary VLAN
    - VLAN Ports
  - Spanning Tree
  - MAC
  - Multimedia Support
  - SNMP

Advanced > VLANS > VLAN Ports

Stack Unit 1:

Port	PVID	Port	PVID	Port	PVID	Port	PVID
1	1	2	195	3	2	4	195
5	2	6	195	7	1	8	2
9	2	10	2	11	2	12	2
13	2	14	2	15	2	16	2
17	666	18	1	19	666	20	3
21	1	22	1	23	2	24	2
25GbE	2	26GbE	2				

Apply Reload

To permanently save the configuration into non-volatile memory, click "**Apply**" on this page, followed by Tools > Save Configuration from the side navigation.

VLANs in Bunt

Management-Interface via Browser

VLAN unter Linux

- Anlegen eines VLAN auf eth0

```
# vconfig add eth0 2
```

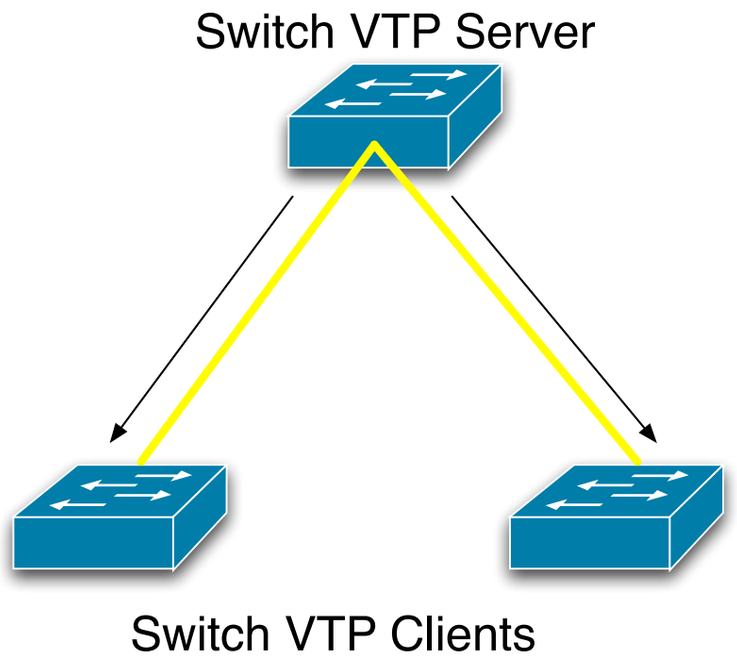
- Erzeugt neues Interface <pysdev>.<vlan id>

```
# ifconfig eth0.2 192.168.1.1 netmask 255.255.255.0
```

- kann auch zu einem Bridge-Interface (geswitchtes Netz) hinzugefügt werden um zwischen zwei VLANs zu switchen, ansonsten erfolgt „reguläres“ Routing zwischen den VLAN-Interfacen

```
# brctl addif br0 eth0.2
# brctl addif br0 eth0.4
```

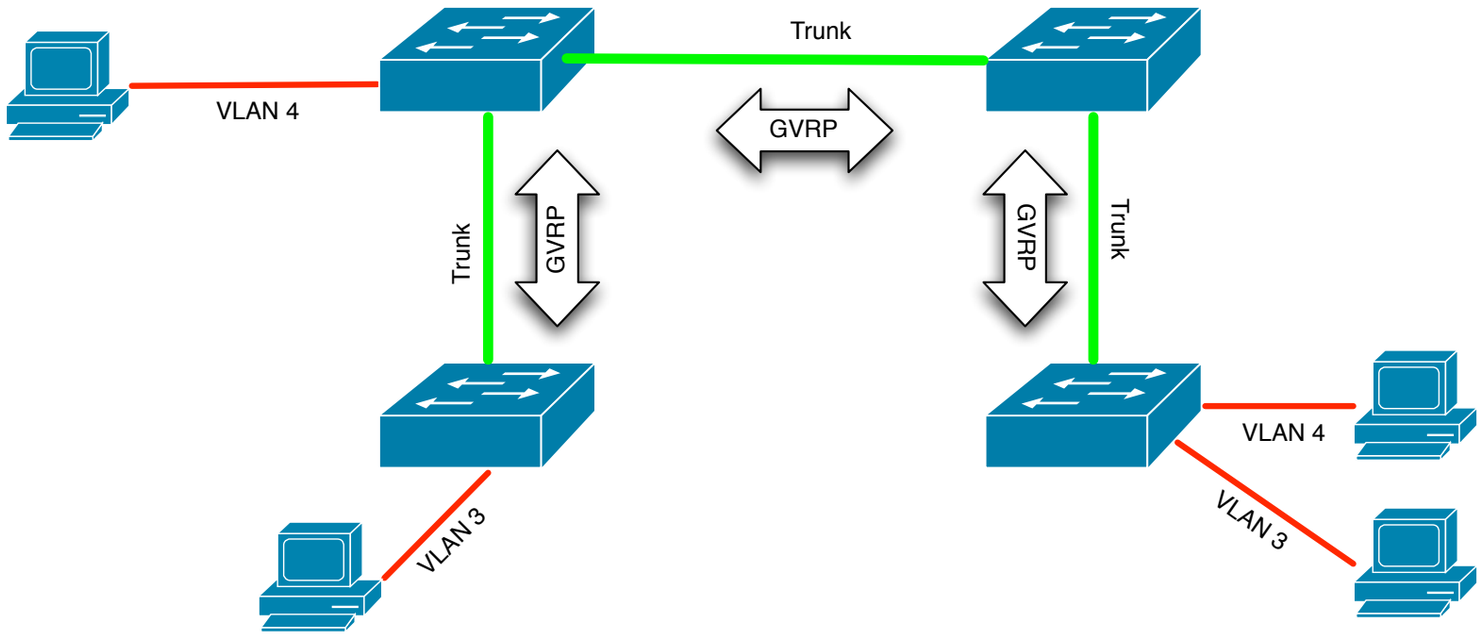
VLAN Trunk Protocol (VTP)



- VLANs werden nur noch auf VTP-Server in die Datenbank eingetragen
- Auf Clients brauchen und können VLANs nicht mehr angelegt und benannt zu werden, sie werden automatisch erzeugt

```
switch> (enable) set vtp domain franken
switch> (enable) set vtp mode client/server
switch> (enable) set vtp password ******
switch> (enable) set vtp pruning enable/disable
```

GVRP - Generic VLAN Registration Protocol



- Teil von GARP (Generic Attribute Registration Protocol)
- dynamische Erzeugung und Entfernung von VLANs auf Trunk-Ports

```
switch> (enable) set port 2/1 gvrp enable
switch> (enable) set gvrp dynamic-vlan-creation enable
```

VMPS - VLAN Management Policy Server

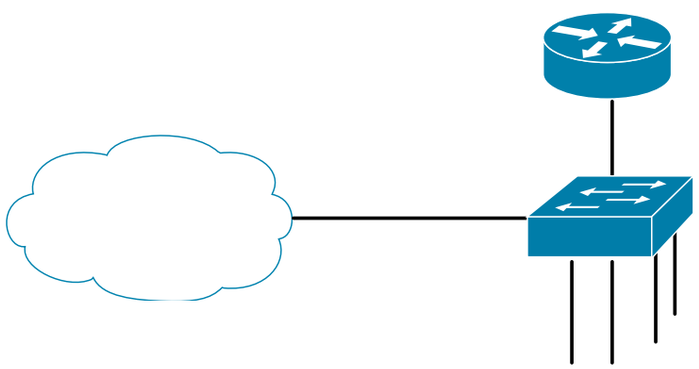
- Port erhält „dynamisch“ eine VLAN-Bindung aufgrund von MAC-Adresse
- VLAN Konfiguration liegt auf zentralem Server
- Periodischer „Download“ der aktuellen Konfiguration
- Konfiguration ist eine „Text“-Datei
- Transfer der Konfigurationsdatei via TFTP

```
!VMPS File Format, version 1.1
vmps domain Company
vmps mode open
!
vmps-mac-addrs
address 0012.2233.4455 vlan-name developement
address 0000.6509.a080 vlan-name sales
address aabb.ccdd.eeff vlan-name support
address 1223.5678.9abc vlan-name management
!
vmps-vlan-group Tech
vlan-name developement
vlan-name support
!
vmps-port-group Office1
device 10.1.1.20 port 3/1
device 10.1.1.20 port 3/2
device 10.1.1.21 all-ports
!
vmps-port-policies vlan-group Tech
port-group Office1
!
vmps-port-policies vlan-name sales
device 10.1.12 all-ports
```

```
switch> (enable) set vmps tftpserver 10.1.2.1
switch> (enable) set vmps state enable
switch> (enable) set port membership 3/1 dynamic
```

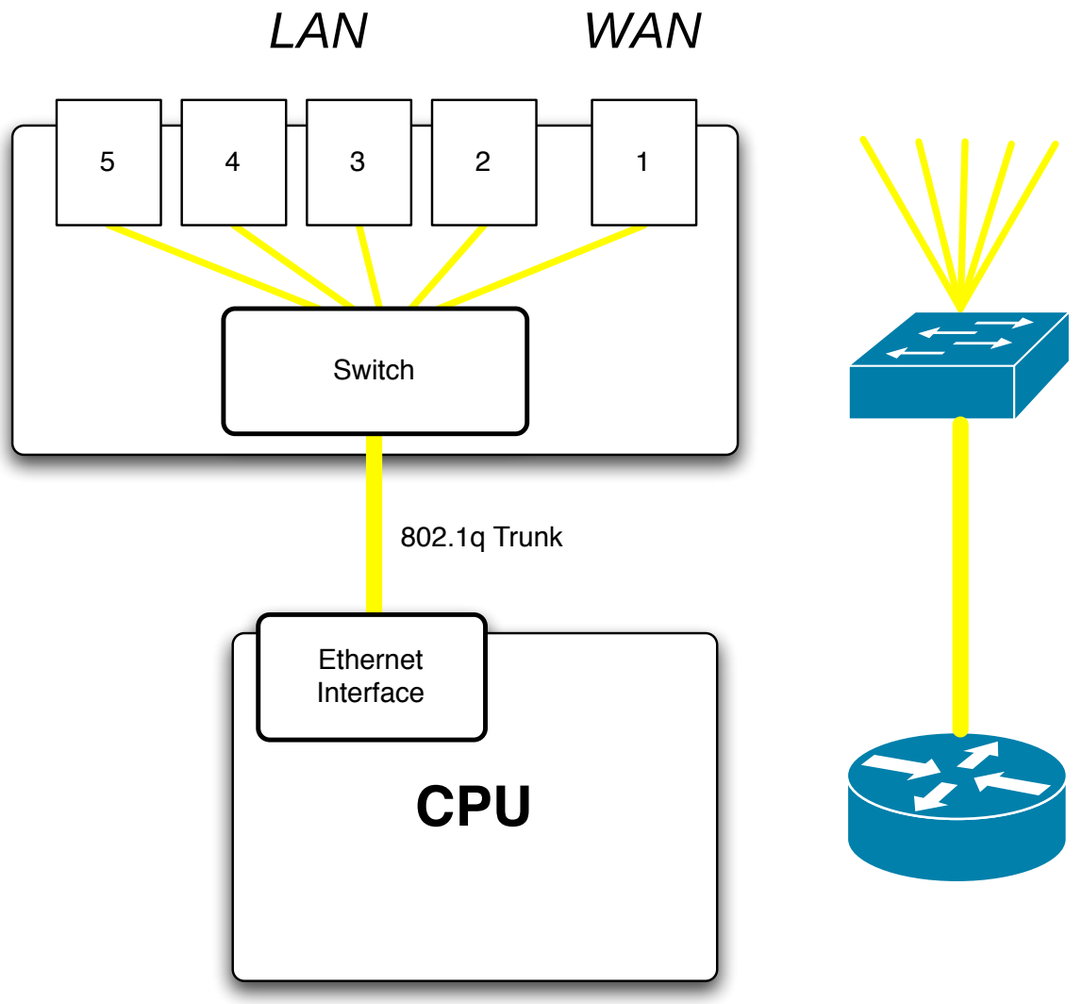
VLAN Szenarien

One Legged Router



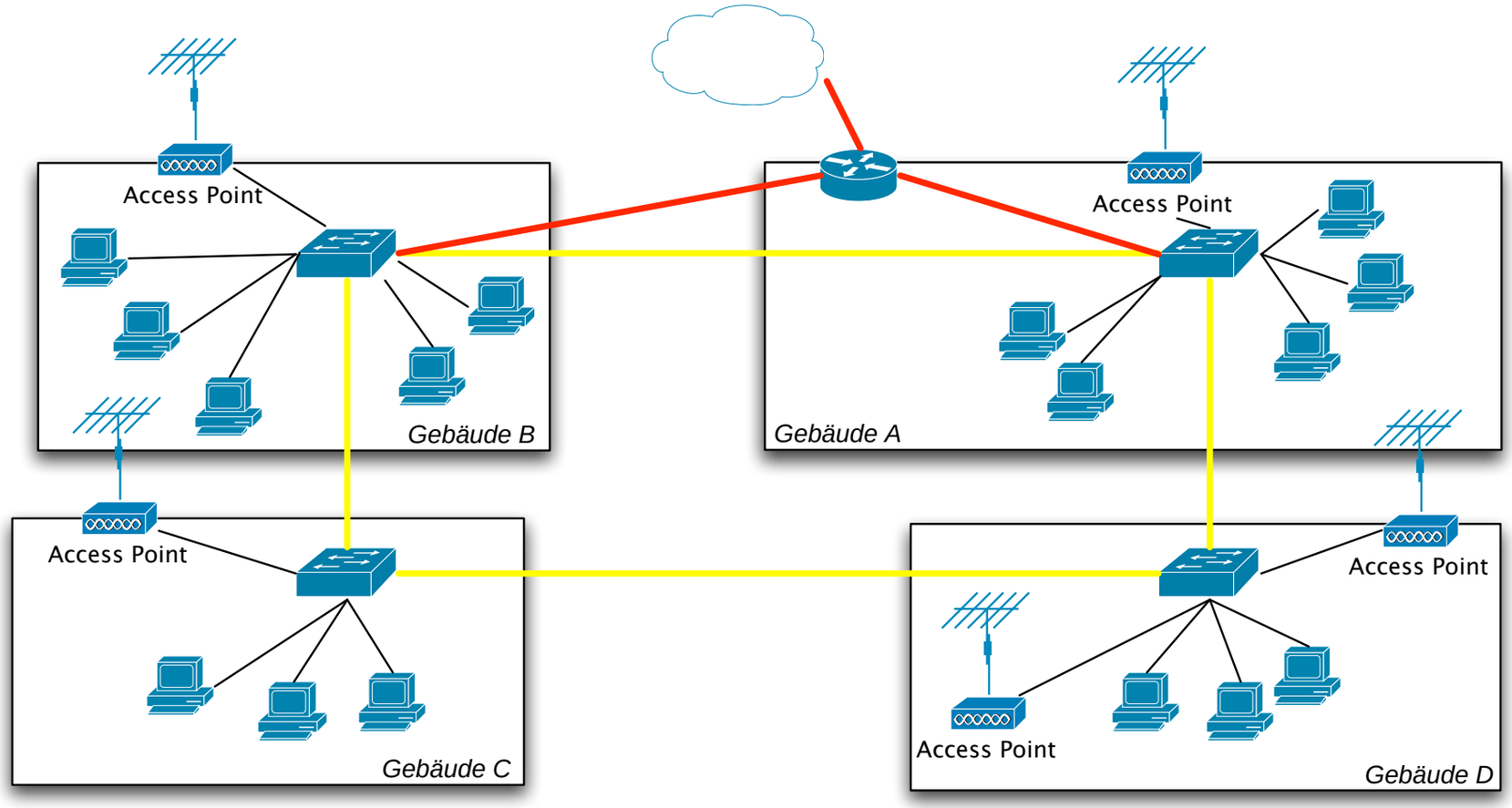
- Linecards für Router sehr teuer
- Switchports relativ günstig
- VLAN als Interface auf Router abbildbar

Embedded One Legged Router

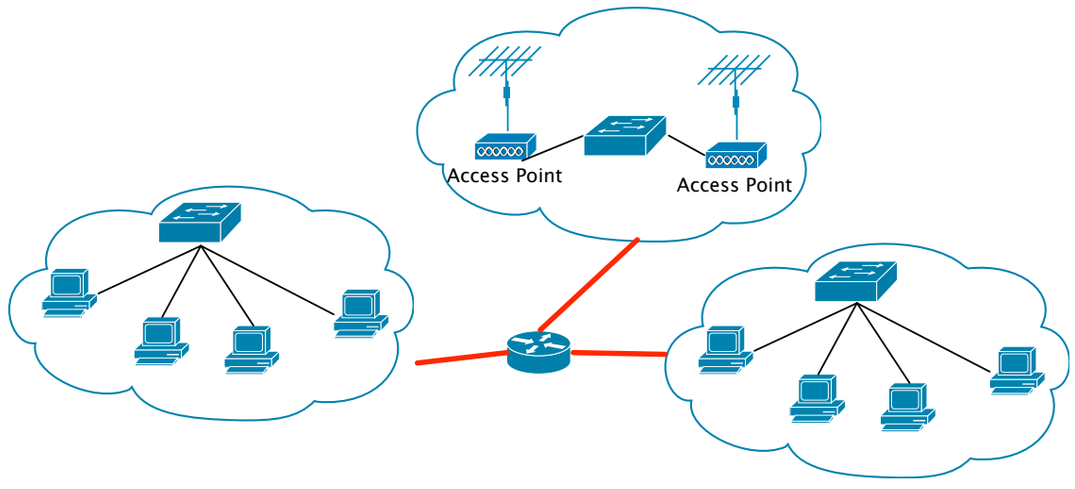


- Einsparung von Kosten & Platz
- variable Nutzung der vorhandenen Ethernet-Ports

Distributed Global Service

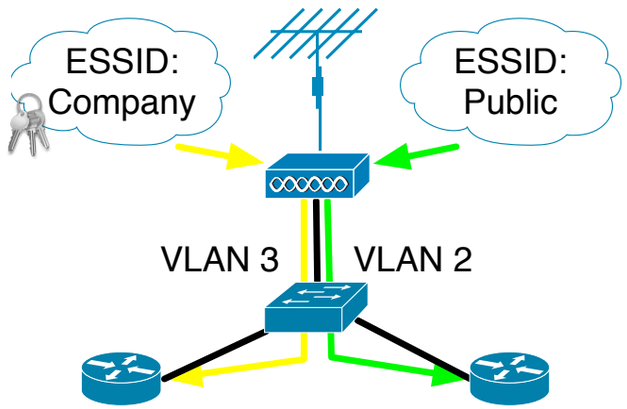


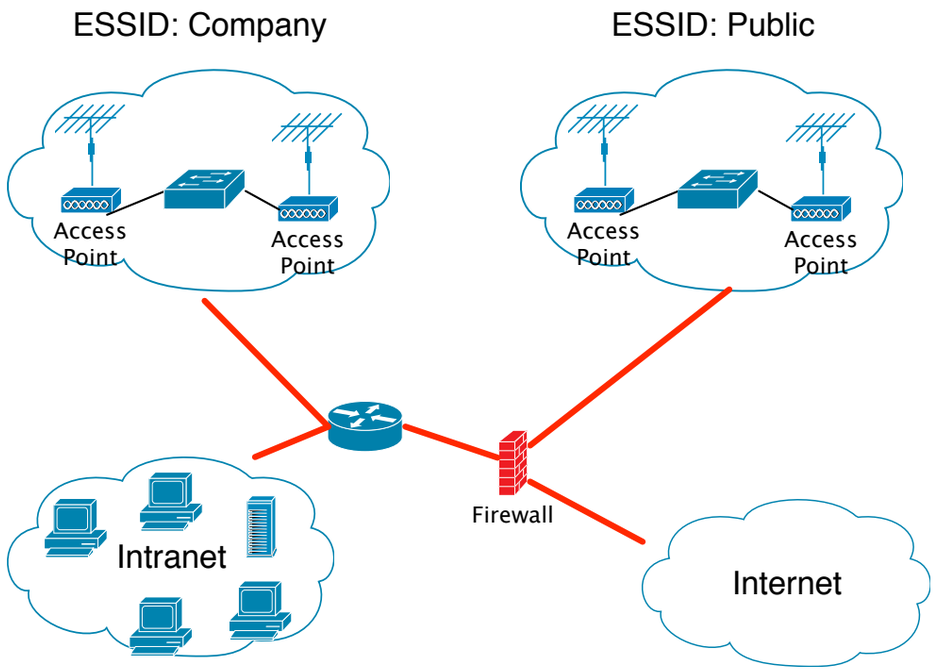
- WLAN Access an verschiedenen Standorten
- Zusammenführung zu einer WLAN-Wolke
- Routing mit Filterung zwischen den Wolken



WLAN Splitting

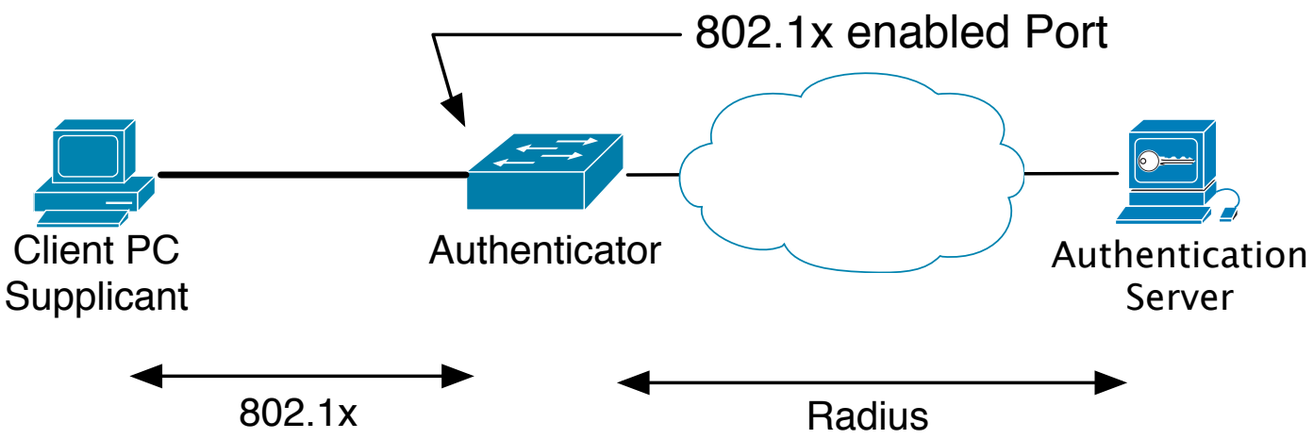
- Betrieb zweier ESSIDs auf einem AP
- Einsparung von Hardware und Frequenzen
- AP liefert Netzwerke auf LAN Interface mittels zweier VLANs
- VLANs trennen Trust oder Association
- VLANs werden dem zu der Policy gehörigen Router „übergeben“





802.1x mit VLAN Zuweisung

- Port-basierende Zugriffsbeschränkungen anhand von Authentisierung
- EAP (Extensible Authentication Protocol) über IEEE 802 Medium
  EAPOL (EAP over LAN)

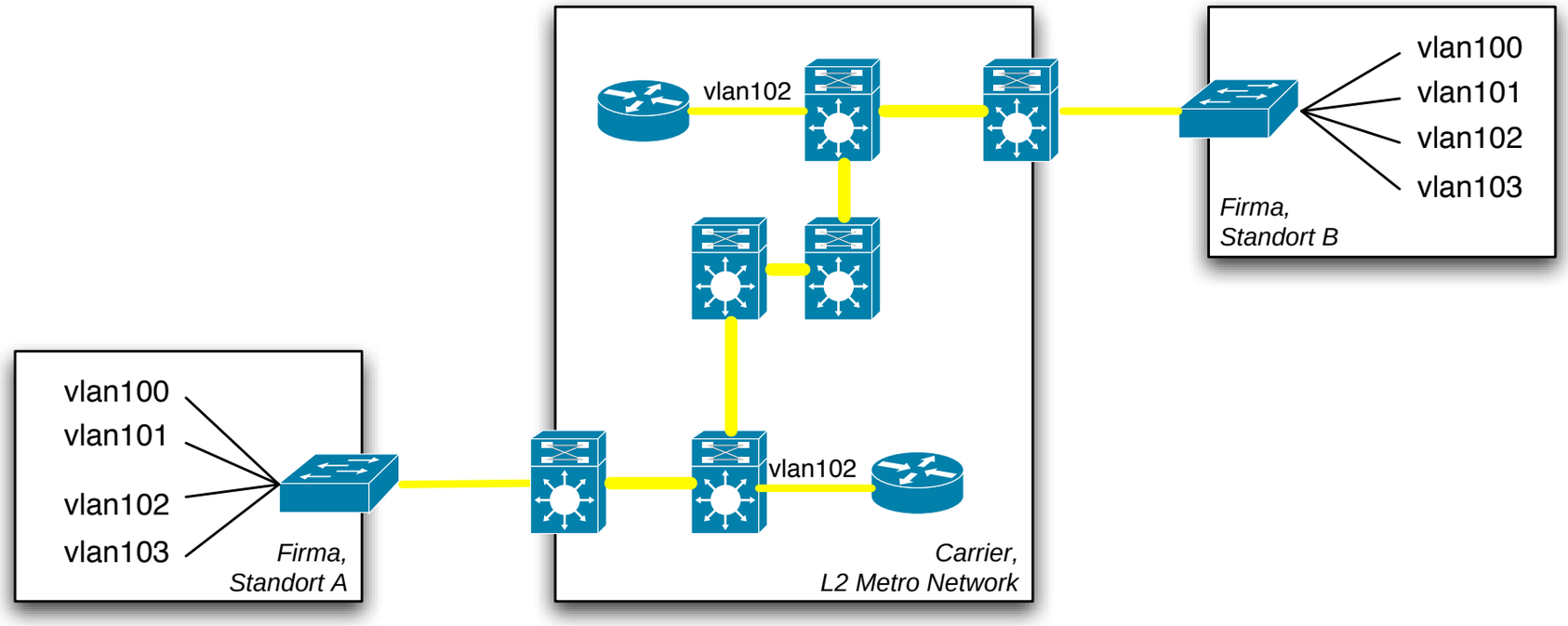



```
switch(config)# aaa authorization network default group radius
switch(config)# dot1x guest-vlan 10
switch(config)# dot1x auth-fail vlan 10
```

```
Radius AV Pairs
[64] Tunnel-type = „VLAN“ (13)
[65] Tunnel-medium-type = „802“ (6)
[81] Tunnel-Private-group = <VLAN Name>
```

- Zuweisung eines VLANs aus den Backend-Nutzer-Attributen
- Fallback auf Default-VLAN bei fehlender 802.1x Kommunikation
- Zuweisung eines VLANs bei fehlgeschlagener Authentisierung

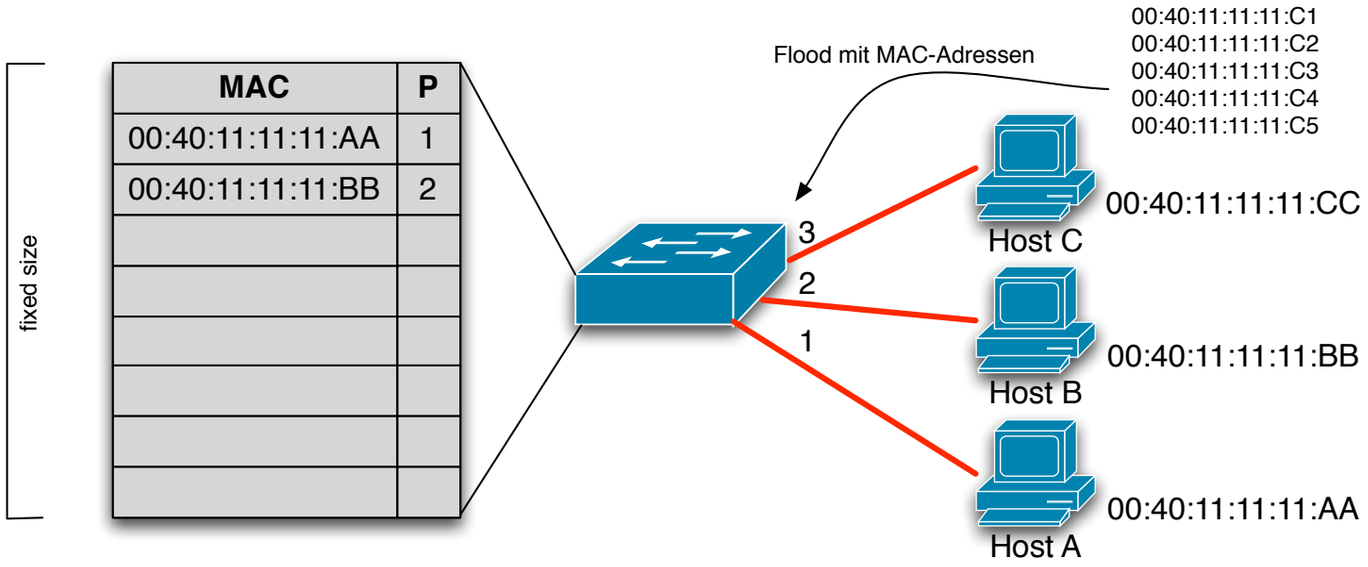
Double-Tagged, q-in-q, 802.1ad



- q-in-q
  - Zwei 802.1q Header folgen aufeinander
  - Switch analysiert äusseren Header und leitet Frame entsprechend weiter
- 802.1ad
  - IEEE Standard (November 2005)
  - Eigener Ether-Type für äusseren Frame-Header

Security

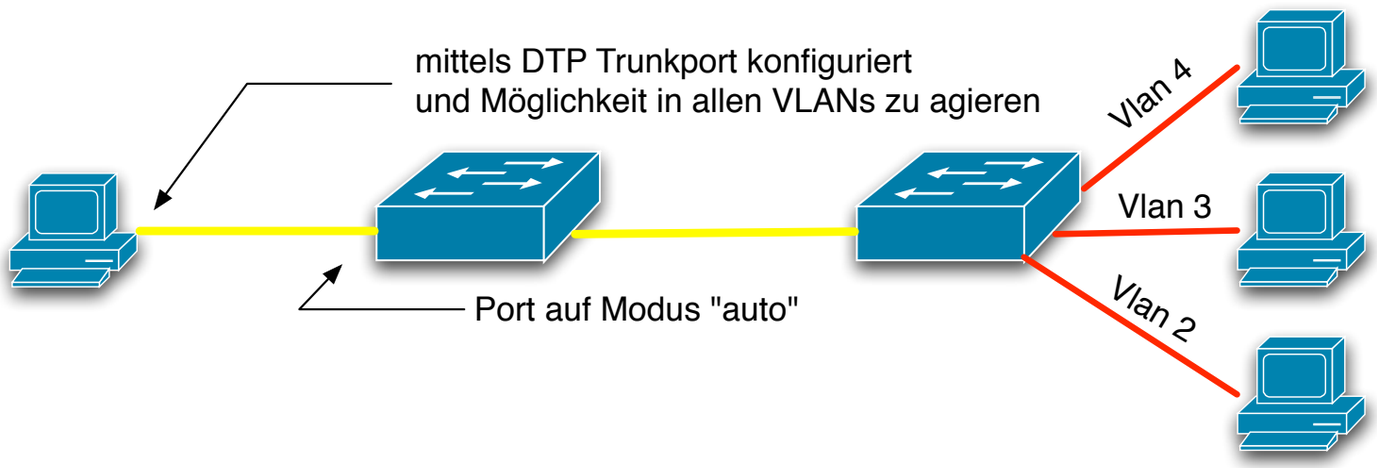
MAC-Flooding



- MAC/CAM-Table des Switches mit „erfundenen“ MAC-Adressen auffüllen um den Switch zum Flooden zu bewegen

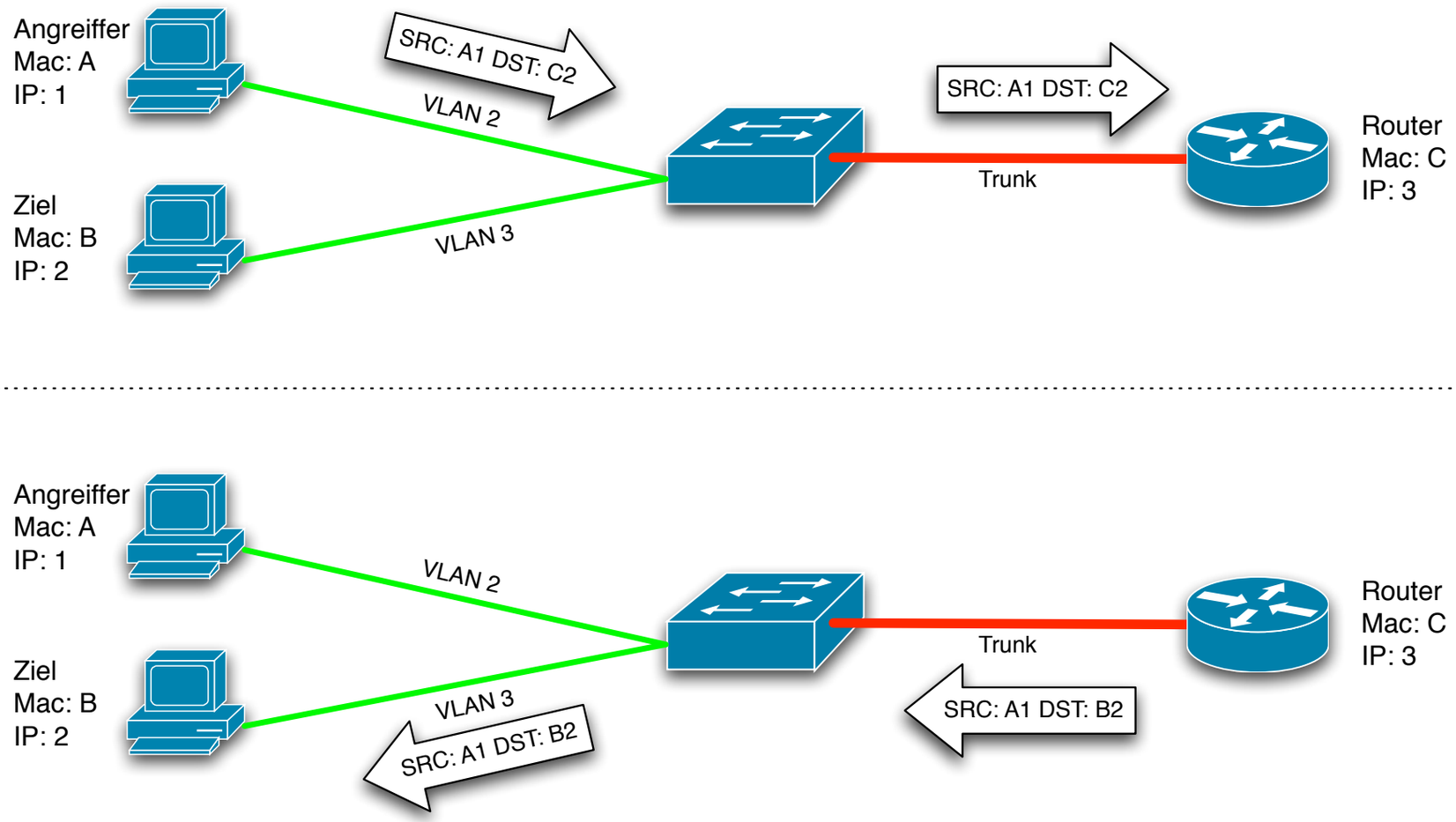
- Wenn Switch beim flooden nicht auf VLAN achtet, können Segmente überwunden werden

DTP - Switch Spoofing



- Port in Richtung Nutzer dynamisch konfigurierbar
- Nutzer kann sich Zugriff auf alle VLANs konfigurieren

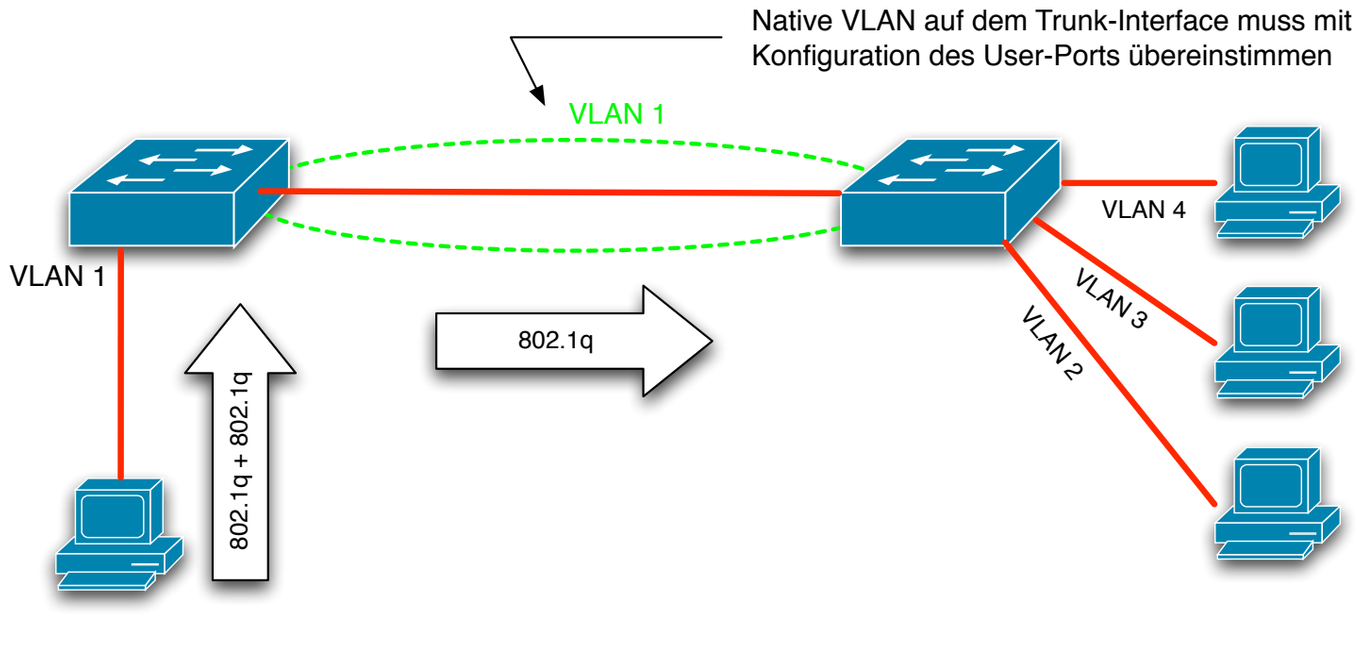
VLAN Hopping über Router



- Explizites Adressieren des Routers auf Layer 2, Ziel-Rechner auf Layer 3

- Kein VLAN-spezifisches Problem!

VLAN-Hopping mit q-in-q



- Trunk-Port hat gleiche native ID wie User-Access Port
- Quelle und Ziel müssen über mehr als einen Switch erreicht werden
- Erlaubt auf Layer2 nur das Senden zum Ziel-VLAN - nur unidirektionale Kommunikation, Layer3-Kommunikation potentiell bidirektional

⇨ Dummy ID für native VLAN (PVID) auf Trunk-Links

VLAN Sicherheit - Port Sicherheit

```
interface FastEthernet0/1
  description unused
  no ip address
  no cdp enable
  switchport mode access
  switchport nonegotiate
  shutdown
  spanning-tree portfast
  spanning-gree bpdufilter enable
```

```
interface FastEthernet2/1
  description Trunk Port
  no ip address
  no cdp enable
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk alloved vlan 2-10,1002-1005
  no shutdown
```

```
vtp mode transparent
```

- Auch unbenutzte Ports korrekt konfigurieren
- Access-Ports als solche konfigurieren
- Trunk ports in ein ungenutztes native VLAN konfigurieren
- keine „Sonderfeatures“ wenn sie nicht wirklich benötigt werden

Vielen Dank für die Aufmerksamkeit

noch Fragen?