

Thema: VLAN

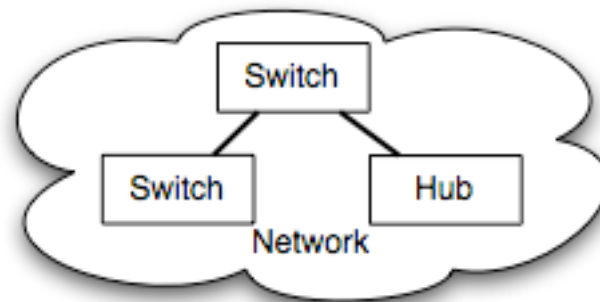
Virtual Local Area Network

Überblick

- Wie kam man auf VLAN?
- Wozu VLAN?
- Ansätze zu VLAN
- Wie funktioniert VLAN
- Wie setzt man VLAN ein

Wie kam man auf VLAN?

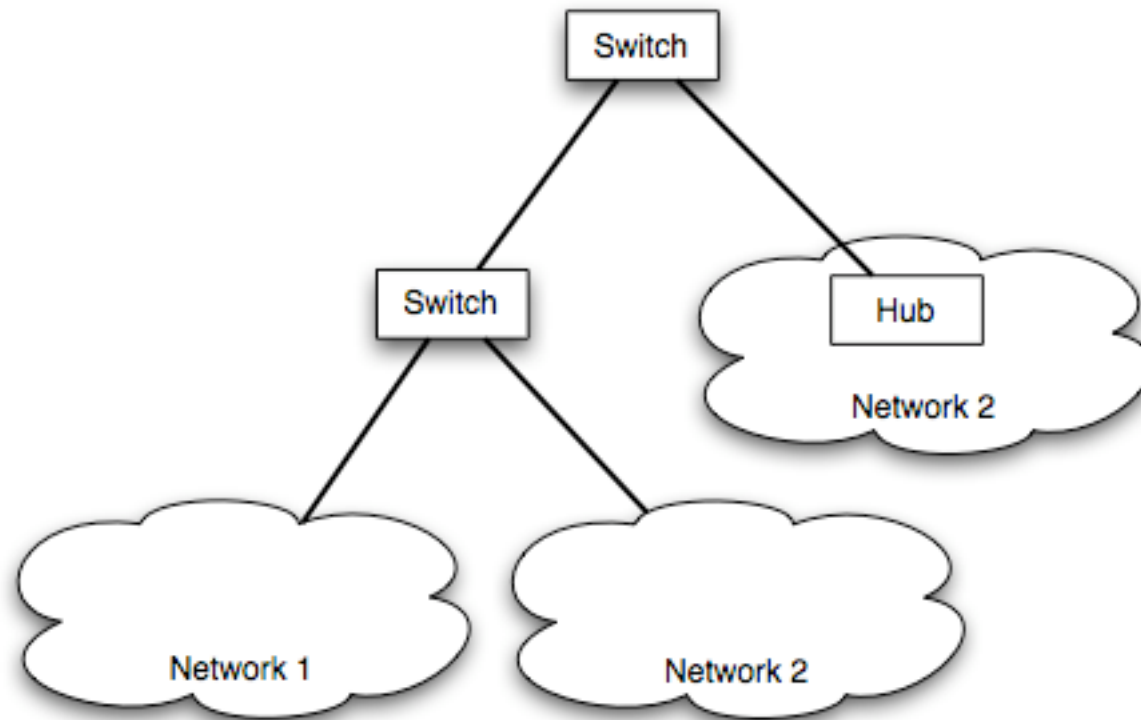
- Ursprünglich: flaches Netz
- ein Switch oder eine Reihe von zusammengeschalteten Switches



Wunsch nach unterteiltem Netz

- Schutz der Benutzer untereinander
- Unterteilung des Netzes nach Unternehmensstruktur
- besserer Durchsatz durch weniger Broadcast-Traffic (ein Subnet = eine Broadcast-Domain)

Wunsch nach unterteiltem Netz



Umsetzungsprobleme

- mühsam durch vorhandene Technologien umzusetzen
- jedes Netz benötigt einen extra Switch
- Netze müssen mit extra Routern verbunden werden
- Kabel müssen manuell umgesteckt werden
- Länge des Kabels zur Endstation begrenzt

Lösung durch VLAN

- mehrere virtuell voneinander getrennte Netze auf einem Switch
- Trennung der logischen Struktur von der physikalischen Struktur
- Durchschalten eines Netzes auf einen beliebigen Port
- benutztes LAN wird standortunabhängig
- kein Umstecken der Kabel
- eine Broadcast-Domain pro VLAN

Ansätze zu VLAN

- portbasiertes VLAN (Layer-1)
- protokollbasiertes VLAN
 - MAC (Layer-2)
 - Layer-3 Protokoll

Portbasiertes VLAN

- auf jedem Switch werden die VLANs fest konfiguriert
- jeder Port wird manuell zu einem VLAN zugehörig konfiguriert
- nur Traffic aus dem konfigurierten VLAN kommt auf dem Port an

Portbasiert Fazit

- Vorteile:
 - eindeutige Zuordnung der Ports zu einem VLAN
- Nachteile:
 - hoher administrativer Aufwand
 - Ports müssen manuell eingestellt werden
 - keine Mobilität der Endstationen möglich

Protokollbasiertes VLAN

- Vorteil gegenüber portbasiertem VLAN:
 - geringerer Administrationsaufwand
 - Rechner können ohne umkonfiguration umgestellt werden

MAC

- anhand der MAC-Adresse eines Frames wird entschieden zu welchem VLAN ein Frame gehört
- Vorteile:
 - Mobilität für Endstationen ist möglich
- Nachteile:
 - **unsicher!** MAC-Adressen können geändert werden
 - die MAC-Adressen müssen in den Switches konfiguriert werden
 - vor dem ersten Frame ist nicht klar zu welchem VLAN ein Port gehört

Layer-3

- zB. IP, IPX, AppleTalk
- auf Basis der Layer-3 Adresse wird entschieden zu welchem VLAN das Frame gehört

Layer-3

- Vorteile:
 - Mobilität möglich
 - Endstation kann in mehreren VLANs teilnehmen
- Nachteile:
 - vor dem ersten Frame ist nicht klar zu welchem VLAN ein Port gehört
 - **unsicher!** zB. IP-Adressen können noch einfacher als MAC-Adressen geändert werden
 - **unschön!** Verletzung des Schichtenmodells, der Switch *muss* Layer-3 verstehen
 - es gibt keinen Standard

Protokollbasiert Fazit

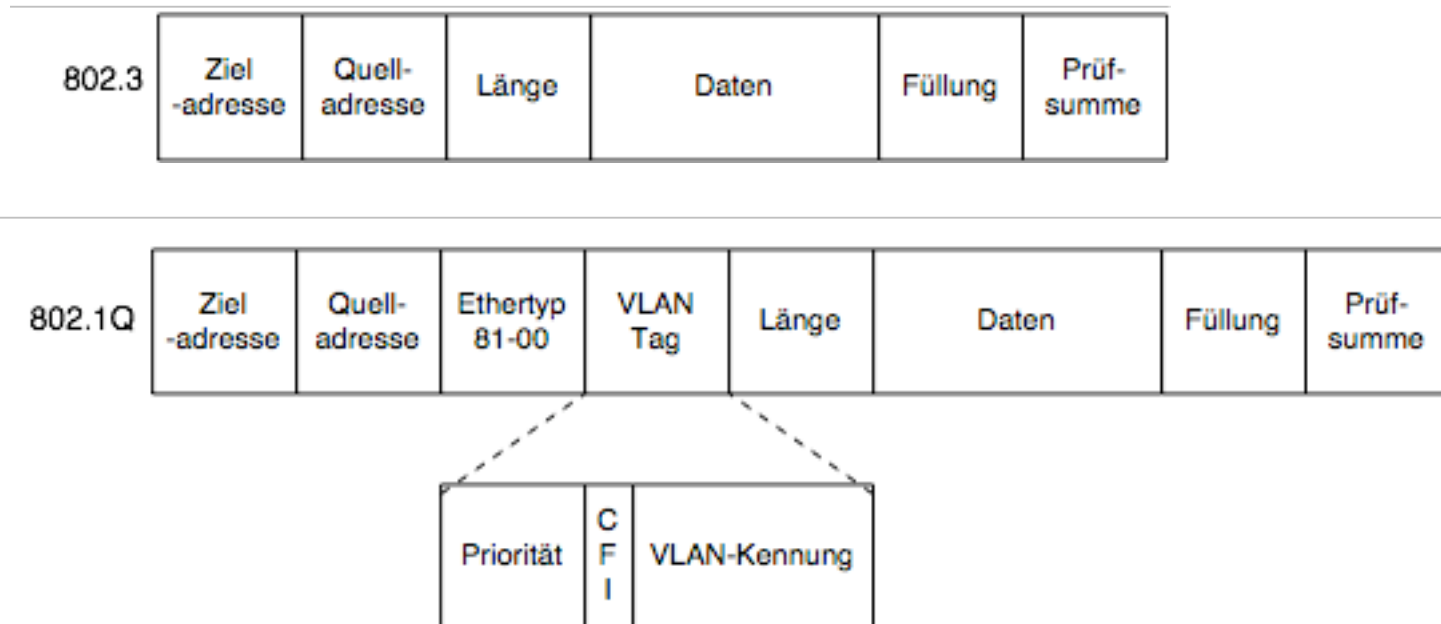
- Vorteile:
 - Mobilität für die Endstationen
- Nachteile:
 - massive Sicherheits- und Kontrolldefizite
 - Vorteil der Mobilität kann durch DHCP oder autoconfiguration (IPv6) erreicht werden

Wie funktioniert VLAN?

- Access Ports: untagged Frames
 - Endstationen
 - nicht VLAN fähige Switches
- Trunk Ports: tagged Frames
 - VLAN fähige Switches
 - VLAN fähige Endstationen
- Hybrid Ports: tagged und untagged Frames

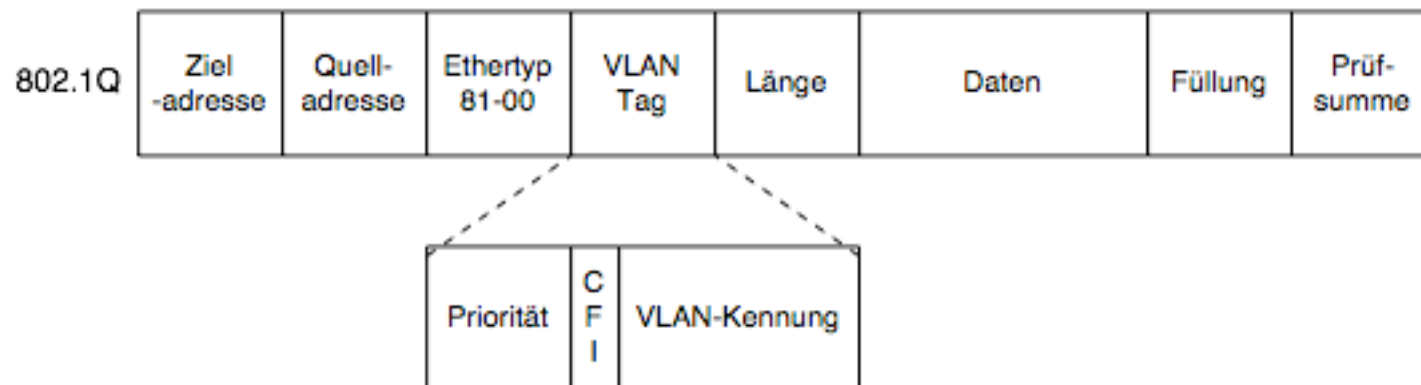
VLAN Tagging

- Standard: IEEE 802.1Q
- Layer-2 Ethernet-Frame wird mit zusätzlichen 4-Bytes “getagged”



VLAN Tagging

- 2-Byte Ethertype “81-00” (TPID - Tag Protocol Identifier)
- 2-Byte VLAN-Tag (TCI - Tag Control Information)
- 3-bit Prioritätsfeld (QoS nach IEEE 802.1p)
- 1-bit CFI (Canonical Format Indicator, gibt an ob ein RIF bei 802.3/ Ethernet benutzt wird oder welche Bitreihenfolge die Adresse bei FDDI/ TokenRing hat)
- 12-bit VLAN ID (4096 mögliche VLAN IDs, abzgl. ID 0)



Verbindung von VLAN Switches

- VLAN Trunks zwischen den Switches
- nur tagged Frames auf den Uplinkports
- verteilen der getaggten Frames auf verschiedene Switches

Verbindung von VLANs

- Inter-VLAN Routing
 - Routing
 - Layer-3 switching durch VLAN fähige Switches
 - auf dem Core-Switch oder in Edge-Switches

Wie setzt man es ein?

VLANs:

2-4: Network 2-4

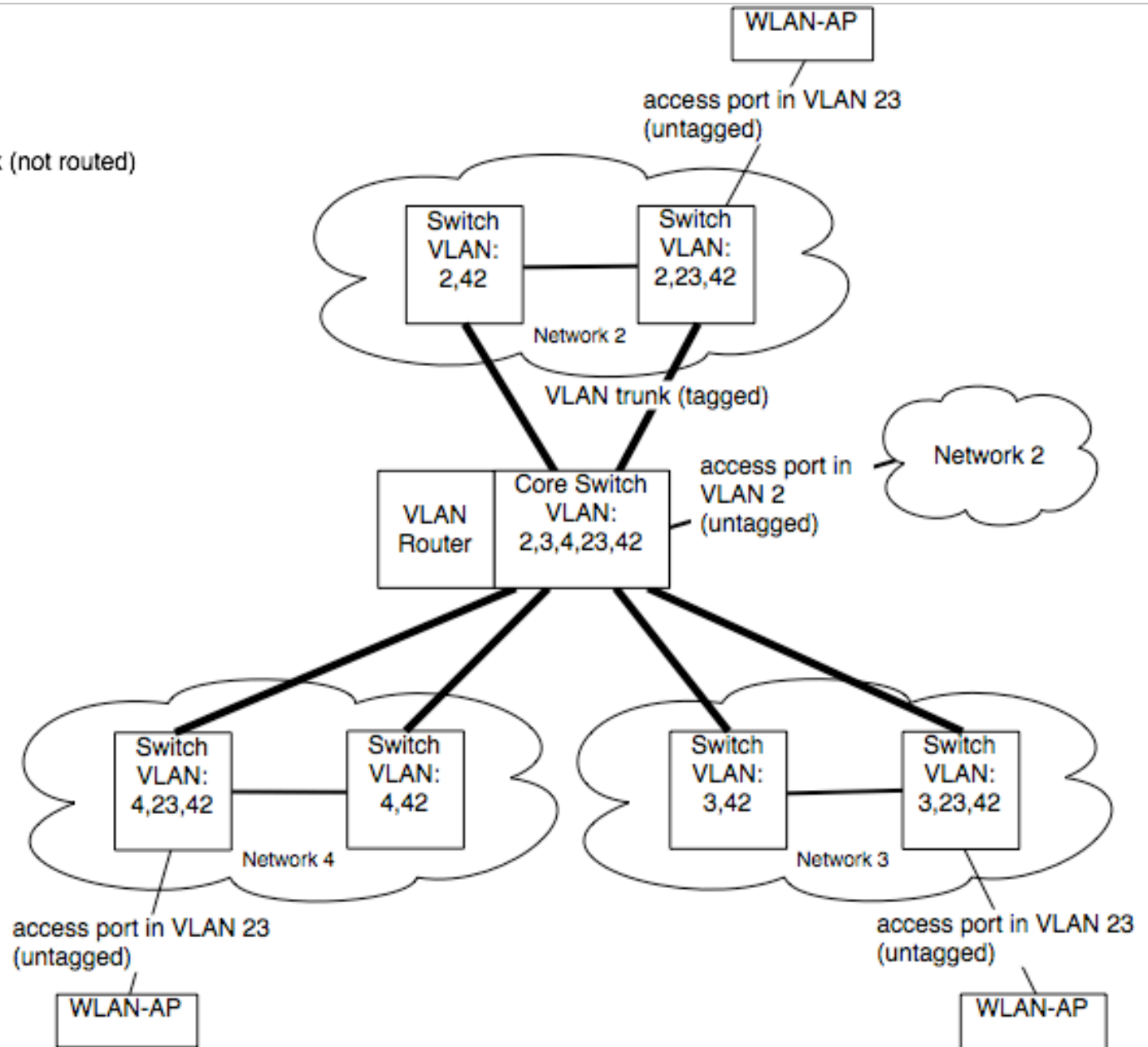
23: WLAN Network

42: Management-Network (not routed)

— 100 Mbit/s

== 1 Gbit/s

=== 2 Gbit/s



Quellen

- Computernetzwerke (A. Tanenbaum)
- Router, Bridges, Switches (R. Perlman)
- Wikipedia (<http://de.wikipedia.org/>)

Folien

<https://outpost.h3q.com/docu/VLAN.pdf>