zurück

VLANs – Grundlagen

VLANs (**V**irtual **LAN**) ermöglichen es, ein physisches Netzwerk logisch in mehrere, voneinander getrennte Netzwerke aufzuteilen.
So entsteht mehr Sicherheit, bessere Struktur und weniger Broadcast-Verkehr.

Warum VLANs?

- Trennung verschiedener Abteilungen (z. B. Verwaltung, Gäste, Technik)
- Sicherheit: weniger Angriffsfläche
- weniger Broadcasts → effizientere Netze
- Netzwerk logisch statt physisch trennen
- Grundlage für große Unternehmensnetze

Beispiel:

- VLAN 10 = Clients
- VLAN 20 = Server
- VLAN 30 = VoIP
- VLAN 40 = Gäste

VLAN-IDs

Jedes VLAN bekommt eine eindeutige Nummer:

- Bereich: **1 bis 4094**
- Sonderfälle:
  - VLAN 1 = Default
  - 1002–1005 = reserviert für alte Cisco-Techniken

Access-Port vs Trunk-Port

Access-Port

- gehört genau **einem VLAN**
- Geräte wie PCs, Drucker, Kameras

```
PC → Access-Port → VLAN 10
```

Trunk-Port

- transportiert **mehrere VLANs**
- Verbindung zwischen Switches / Switch → Router

```
Switch A === Trunk === Switch B
(VLANs 10,20,30)
```

802.1Q-Tagging

Trunk-Ports markieren Frames mit einem VLAN-Tag:

```
+--------+--------+--------+
| MACs   | EthTyp |  Tag   | Payload |
+--------+--------+--------+
```

Der Tag enthält:

- VLAN-ID
- Priorität (QoS)

Access-Ports hingegen **taggen nicht**.

ASCII-Diagramm: Access vs Trunk

```
    PC                      Switch                  Switch
    | (untagged)            |(tagged VLAN 10,20,30) |
    |                       |                       |
[Access Port] ----- VLAN10 | ---- [Trunk] -------- | VLANs 10-30
```

Inter-VLAN-Routing

VLANs **können nicht direkt** miteinander kommunizieren.

Verbindung erfolgt über:

- Router (Router-on-a-Stick)
- Layer-3-Switch (empfohlen in Unternehmen)

ASCII:

```
VLAN 10 → Router/L3-Switch → VLAN 20
```

Beispiel: Router-on-a-Stick

Ein physischer Router-Port wird in virtuelle Subinterfaces unterteilt:

```
Gi0/0.10  → VLAN 10 → 192.168.10.1
Gi0/0.20  → VLAN 20 → 192.168.20.1
```

Broadcast-Domains

Jedes VLAN ist eine **eigene Broadcast-Domain**.

Vorteil:

- ARP, DHCP, Broadcasts bleiben isoliert
- Netzlast sinkt

DHCP in VLANs

Option A: DHCP-Server pro VLAN
Option B: zentraler DHCP via **DHCP-Relay (IP Helper)**

```
Switch → DHCP Relay → DHCP Server
```

Praxisbeispiel (Unternehmen)

```
VLAN 10 – Clients (192.168.10.0/24)
VLAN 20 – Server  (192.168.20.0/24)
VLAN 30 – VoIP    (192.168.30.0/24)
```

```
VLAN 40 – Gäste   (192.168.40.0/24)
```

Trunk zwischen Core-Switch und Access-Switch:

```
Switch Core === VLANs 10,20,30,40 === Switch Access
```

VLAN-Mapping-Tabelle

VLAN	Name	Netz	Einsatzbereich
——	————-	——————-	————
10	Clients	192.168.10.0/24	Arbeitsplätze
20	Server	192.168.20.0/24	Backend-Dienste
30	VoIP	192.168.30.0/24	Telefone
40	Gäste	192.168.40.0/24	WLAN Gäste

Native VLAN

Auf Trunk-Ports:

- VLAN ohne Tag
- sollte **nicht** VLAN 1 sein
- Sicherheitsrisiko → am besten ein eigenes, unbenutztes VLAN verwenden

Sicherheitsaspekte

- niemals VLAN 1 produktiv nutzen
    - Native VLAN ändern
      * Access-Ports gegen ungewollte Tags schützen (DHCP Snooping, DAI)
      * Inter-VLAN-Firewall-Regeln setzen
      * nur benötigte VLANs auf Trunk freigeben

VLAN Hopping – Attacke

Bei falscher Konfiguration kann ein Angreifer:

- VLANs überspringen
  * fremde VLANs betreten

Schutz:

- Native VLAN sicher setzen
  * nur explizit erlaubte VLANs trunken
  * Access-Ports auf „Access“ setzen

Zusammenfassung

- VLANs trennen Netzwerke logisch auf einem Switch
  - Access-Ports → 1 VLAN
    * Trunk-Ports → viele VLANs, getaggt
    * 802.1Q = VLAN-Tag
    * Broadcast-Domains werden sauber getrennt
    * Kommunikation zwischen VLANs nur über Routing
    * wichtig für Sicherheit, Struktur und große Netzwerke