

VLAN

Inhaltsverzeichnis

- [1 Funktionsweise](#)
- [2 Typische Einsatzbereiche](#)
- [3 Wichtige Hinweise](#)
- [4 Fazit](#)

Ein VLAN (Virtual Local Area Network) teilt ein physisches Netzwerk logisch in getrennte Segmente. Geräte in unterschiedlichen VLANs kommunizieren nur über einen Router oder eine Firewall miteinander – das verbessert Übersicht, Sicherheit und Broadcast-Kontrolle.

1 Funktionsweise

Switches markieren Frames mit einer VLAN-ID (häufig IEEE 802.1Q). Ports gehören zu einem oder mehreren VLANs; Trunk-Links transportieren mehrere VLANs zwischen Switches.

- **Access-Port:** ein VLAN für Endgeräte
- **Trunk-Port:** mehrere VLANs zwischen Netzwerkgeräten
- **Inter-VLAN-Routing:** Kommunikation zwischen VLANs über Layer 3

2 Typische Einsatzbereiche

- Trennung von Clients, Servern, Gästen und Management
- VoIP, IoT oder Kameras in eigenen Segmenten
- Kleinere Broadcast-Domänen in größeren Netzen

3 Wichtige Hinweise

- VLAN allein ersetzt keine Firewall – Regeln zwischen Segmenten sind entscheidend.
- Native/untagged VLANs und falsch konfigurierte Trunks sind klassische Fehlerquellen.
- Dokumentation der VLAN-IDs und Zwecke spart späteren Betriebsaufwand.

4 Fazit

VLANs sind das Grundwerkzeug der Netzwerksegmentierung: Sie schaffen Ordnung und Sicherheit auf Layer 2 – wirksam vor allem in Kombination mit Routing- und [Firewall-Regeln](#).