# Netzwerk: VLAN Grundlagen

## Was ist ein VLAN?

Ein VLAN (Virtual Local Area Network) trennt Netzwerke logisch auf Layer-2-Ebene. Geräte in verschiedenen VLANs können sich nicht gegenseitig „sehen“, obwohl sie am gleichen physischen Switch angeschlossen sind.

## Tagged vs. Untagged

- **Tagged** : VLAN-ID bleibt im Ethernet-Frame erhalten. Wird meist bei Trunk-Ports verwendet (z. B. Router ↔ Switch).
- **Untagged**: VLAN-ID wird beim Senden entfernt. Wird meist bei Endgeräten genutzt, die keine VLANs verstehen (z. B. PCs).

## PVID – Port VLAN ID

Die PVID bestimmt, welchem VLAN ein ungetaggtes eingehendes Paket zugeordnet wird. Jeder Port kann nur **eine** PVID haben.

**Merksatz**: Wenn ein Port untagged in einem VLAN ist, muss seine PVID mit dieser VLAN-ID übereinstimmen.

## Access vs. Trunk Port

- **Access Port**: Akzeptiert nur ungetaggte Frames, ist einem einzigen VLAN zugeordnet
- **Trunk Port**: Unterstützt mehrere VLANs per Tagging (z. B. VLAN 1 + VLAN 2 über ein Kabel)

## Vorteile von VLANs

- Segmentierung von Netzen (z. B. Gäste, IoT, Management)
- Broadcast-Domänen trennen
- Sicherheit erhöhen
- Weniger Geräte für gleiche Funktionalität nötig

# Netzwerk:Switch Konfigurationen

## Beispiel: GS1200-8 (Zyxel) mit 2 VLANs

| Port | VLAN 1 | VLAN 2 | PVID | Beschreibung |
|---|---|---|---|---|
| 1 | Untagged | – | 1 | FritzBox (Internet) |
| 5 | – | Untagged | 2 | Zyxel LAN-Port (VLAN2) |
| 7 | – | Untagged | 2 | Client (z. B. PC) |
| 8 | Untagged | – | 1 | Zyxel WAN-Port (VLAN1) |

→ Wichtig: **PVID muss zur untagged VLAN-ID passen!**

## Best Practices

- Immer dokumentieren, welcher Port welchem VLAN zugeordnet ist
- „VLAN Leaks“ vermeiden (Ports nicht aus Versehen in beiden VLANs untagged!)
- Bei Trunk-Ports explizit markieren, welche VLANs erlaubt sind

# Fehlerbehebung: DHCP kommt nicht an

## Symptome

- Client bekommt keine IP-Adresse
- IP bleibt auf APIPA (169.254.x.x)

## Checkliste

- Switchport hat VLAN 2 als „untagged“? 
- PVID = VLAN 2? 
- DHCP-Server im richtigen Netzbereich aktiv? 
- DHCP-Range nicht erschöpft? 
- VLAN wird durch alle Zwischen-Switche korrekt weitergeleitet? 
- Firewall blockiert DHCP (UDP Port 67/68)? 

## Schnelltest

- Client mit statischer IP konfigurieren → Zugriff auf Gateway?
- DHCP mit Wireshark sniffen (filter: `bootp`)

# Projekte: Zyxel VLAN Setup

## Ausgangslage

- FritzBox liefert Internet über Port 1
- Zyxel-Router holt Internet auf Port 8 (VLAN 1 untagged)
- Zyxel-Router verteilt IPs über Port 5 (VLAN 2 untagged)
- Clients (Port 7) bekommen IP vom Zyxel, nicht von FritzBox

## VLAN-Konfiguration Switch (GS1200)

- VLAN 1: Ports 1 (U), 8 (U), Rest: Non-Member
- VLAN 2: Ports 5 (U), 7 (U), Rest: Non-Member
- PVID: Port 5 & 7 = 2, Port 1 & 8 = 1

## Testung

- DHCP funktioniert
- Gateway: 192.168.10.1 (Zyxel)
- Zugriff auf Internet über FritzBox (Routing korrekt)

# Projekte: VLAN Trunk vs Dual Cable

## Vergleich

| **Merkmal** | **Trunk-Port (1 Kabel)** | **Zwei Kabel (WAN/LAN getrennt)** |
|---|---|---|
| Geräteanzahl | 1 Port benötigt | 2 Ports benötigt |
| Konfig-Aufwand | Hoch – VLAN-Tagging nötig | Geringer |
| Fehleranfälligkeit | Höher (PVID/Tagging-Fehler) | Gering |
| VLAN-Flexibilität | Hoch | Eingeschränkt |
| Anfängerfreundlich |  |  |

## Empfehlung

- Für Heimumgebungen oder einfache Setups: **Zwei Kabel** sind robuster
- Für Profi-Setups oder Portmangel: **Trunk** mit sauberer Doku und VLAN-Disziplin

# Netzwerk: Glossar

- **VLAN** – Virtuelles LAN, logisch getrenntes Netzwerk auf Layer 2
- **PVID** – Port VLAN ID, bestimmt eingehende VLAN-Zuordnung
- **Tagged/Untagged** – Gibt an, ob VLAN-ID im Ethernet-Frame enthalten ist
- **Trunk Port** – Port, der mehrere VLANs getaggt transportiert
- **Access Port** – Port, der nur einem VLAN angehört (untagged)
- **DHCP Relay** – Weiterleitung von DHCP-Anfragen über Subnetze hinweg
- **Bridge Mode** – Gerät arbeitet auf Layer 2, ohne Routing
- **MAC Table** – Switch-internes Verzeichnis, welche MAC-Adresse an welchem Port erreichbar ist