

VLAN (Virtual Local Area Network)

Ein Virtual-Local-Area-Network (VLAN) ist ein logisches Teilnetz innerhalb eines physikalischen Netzwerks (IEEE 802.1Q).

VLANs trennen ein großes Netz in mehrere kleinere Netze auf.

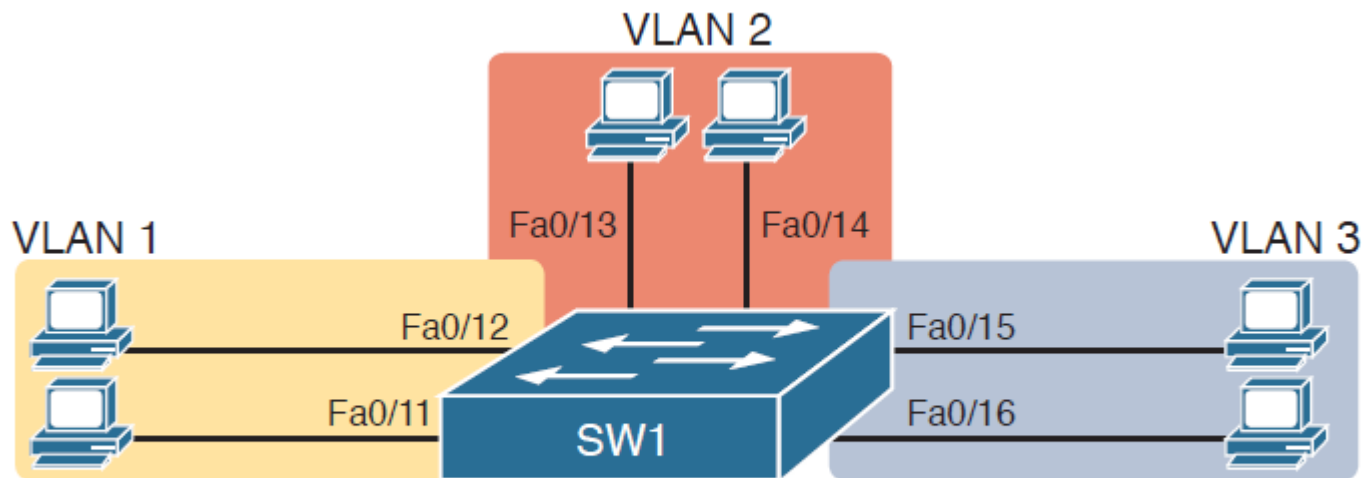
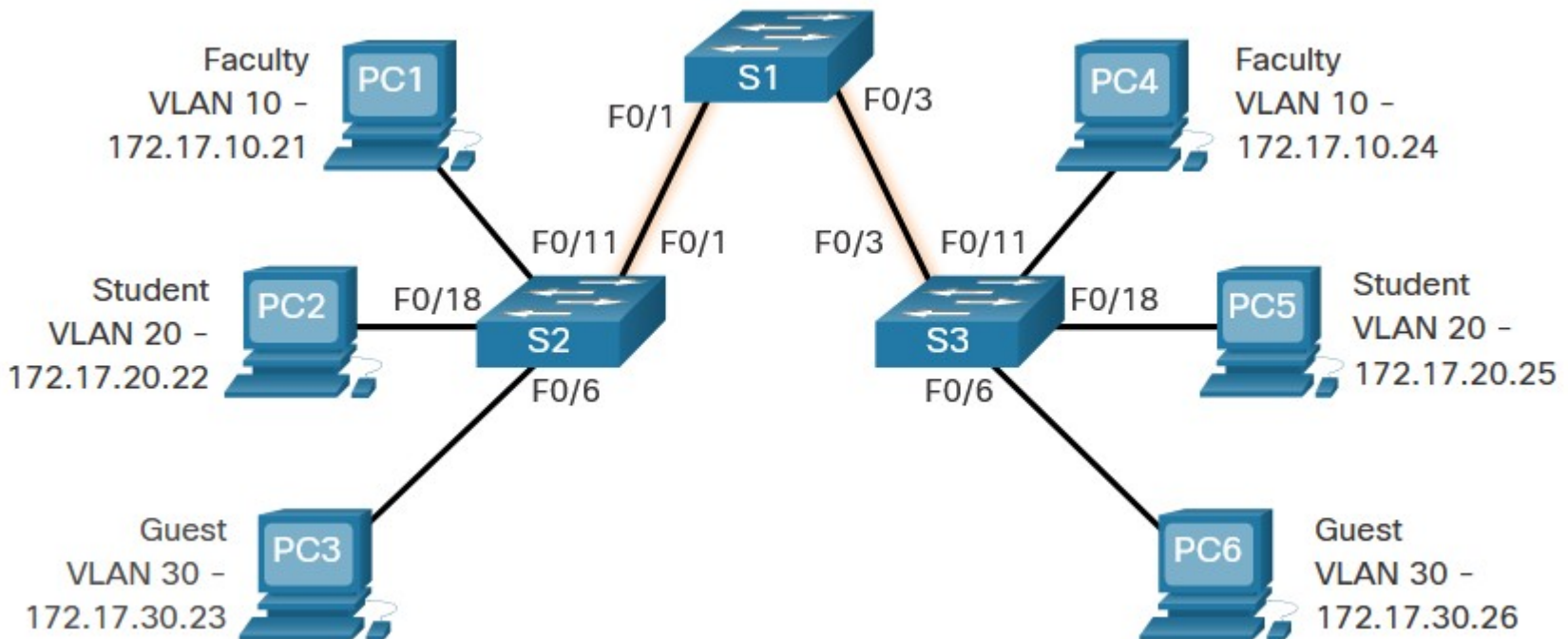


Figure 11-11 *Network with One Switch and Three VLANs*

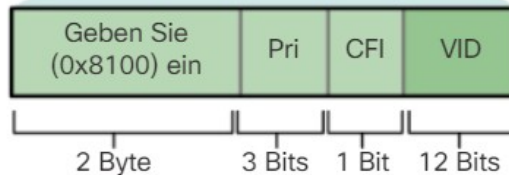
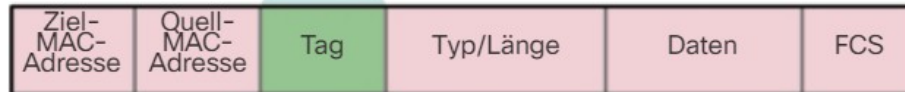
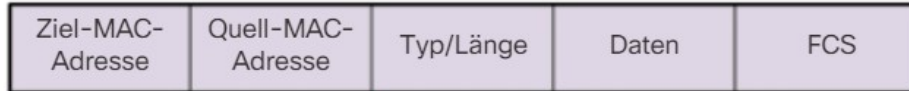
Quelle: CCENT/CCNA ICND1 100-105 Official Cert Guide

VLAN – Weshalb?



- Sicherheit – Gruppen mit sensiblen Daten können vom Rest des Netzwerks getrennt werden, um die Gefahr der Weitergabe vertraulicher Informationen zu reduzieren.
- Niedrigere Kosten – Kosteneinsparungen durch Minimierung teurer Netzwerkupgrades und effizientere Nutzung vorhandener Bandbreiten und Uplinks.
- Bessere Leistung – Durch die Aufteilung flacher Schicht-2-Netzwerke in mehrere logische Arbeitsgruppen (Broadcast-Domänen) wird unnötiger Datenverkehr im Netzwerk reduziert und die Leistung verbessert.
- je nach Konfiguration ggf. höherer Administrationsaufwand.

VLAN Tag



- 0x8100 → 802.1Q-Tag
- Pri → PCP (Priority Code Point): für die Priorisierung von Daten, z.B. Sprachdaten
- CFI = heute DEI (Drop Eligible Indicator) → bei Stau relevant
- **VID = VLAN-Identifizier / VLAN-Nummer (1 - 4094)**

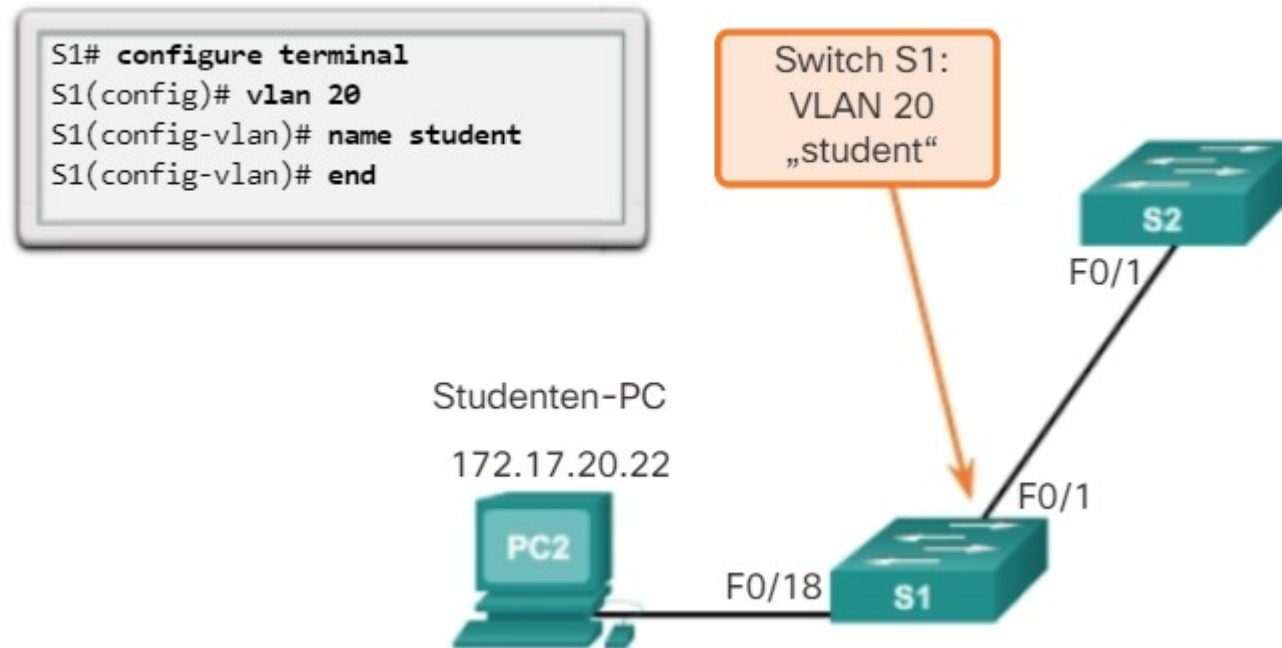
```
⊕ Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
⊕ Ethernet II, Src: Routerbo_4a:e8:1f (00:0c:42:4a:e8:1f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊖ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = CFI: Canonical (0)
    .... 0000 0000 0001 = ID: 1
    Type: IP (0x0800)
⊕ Internet Protocol
```

Statische VLANs werden auch **port-basierend** genannt. Die Zuordnung eines Ports zu einem VLAN erfolgt durch statische VLAN-Konfiguration. Wenn ein Gerät ans Netzwerk angeschlossen wird, nimmt es automatisch am VLAN „seines“ Ports teil. Wechselt der Benutzer die Ports, möchte aber im gleichen VLAN bleiben, dann muss der Administrator eine manuelle Zuweisung des neuen Ports zum gewünschten VLAN vornehmen.

Dynamische VLANs entstehen durch den Einsatz von Softwarelösungen. Mit Hilfe eines VMPS (VLAN Management Policy Server, Server für VLAN-Verwaltungsrichtlinien) können Sie Switch-Ports VLANs dynamisch basierend auf MAC-Adresse oder IP-Adresse etc. des Gerätes zuweisen, das an den Port angeschlossen ist.

VLAN Konfiguration (Switch)

VLANs erstellen und benennen:



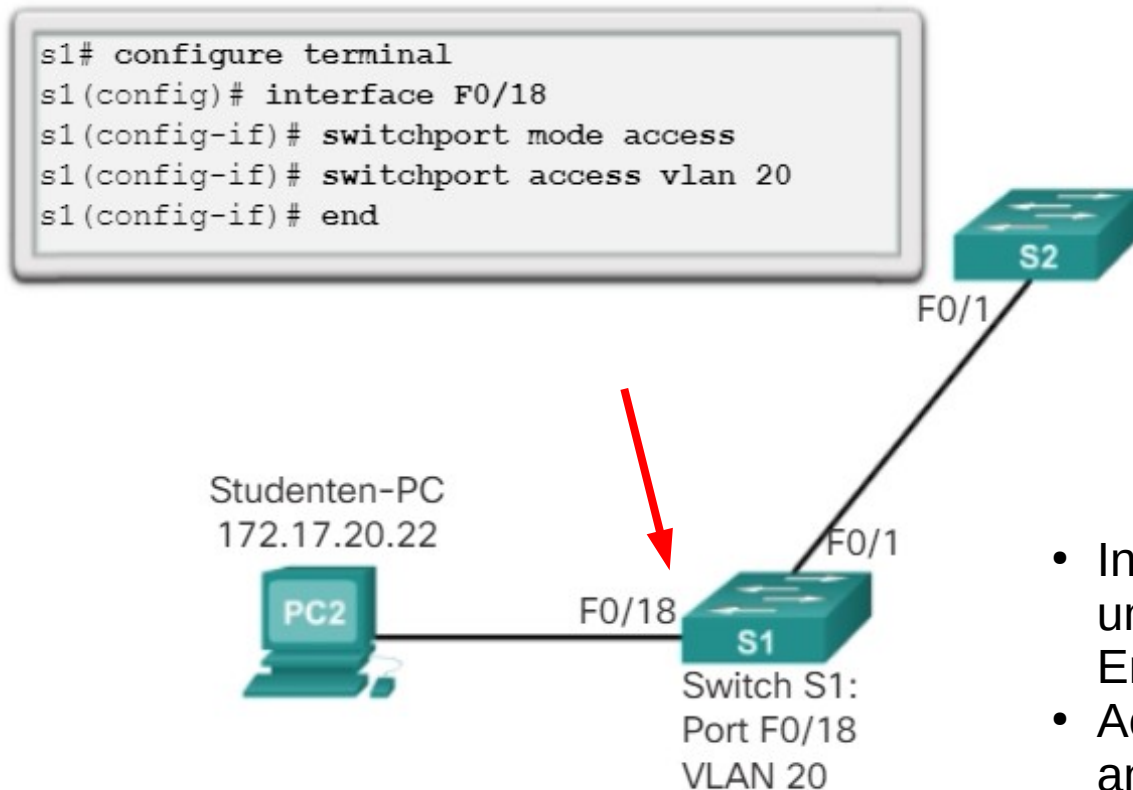
VLANs überprüfen:

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2,

VLAN Konfiguration (Switch)

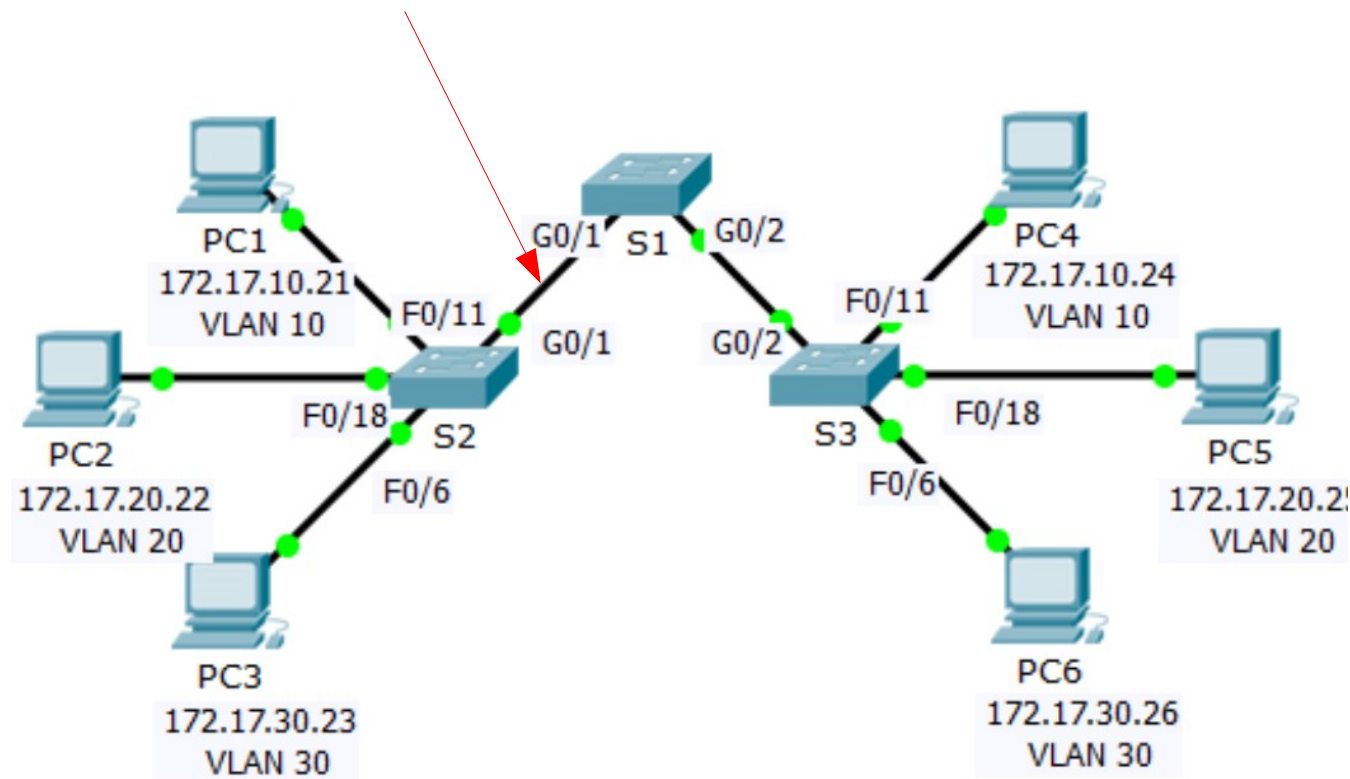
Access-Ports zuweisen:



- In der Regel handelt es sich um Ports mit angeschlossenen Endgeräten.
- Access-Ports werden bei anderen Herstellern Untagged-Ports genannt

Trunk-Port

Ein VLAN-Trunk ist ein OSI-Schicht-2-Link zwischen zwei Switches, der Daten für alle VLANs überträgt (es sei denn, die Liste der erlaubten VLANs wird manuell oder dynamisch eingeschränkt).



Trunk-Ports werden bei anderen Herstellern Tagged-Ports genannt.

Trunk-Port - Konfiguration

```
VLAN 10 - Faculty/Staff - 172.17.10.0/24  
VLAN 20 - Students - 172.17.20.0/24  
VLAN 30 - Guest - 172.17.30.0/24  
VLAN 99 - Native - 172.17.99.0/24
```

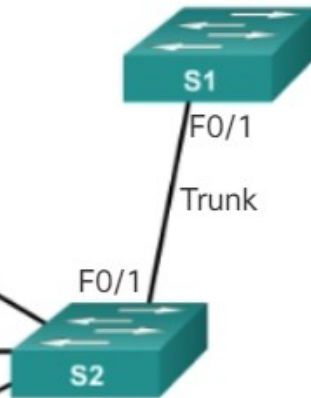
Faculty
VLAN 10
172.17.10.21



Student
VLAN 20
172.17.20.22



Guest
VLAN 30
172.17.30.23



```
S1(config)# interface FastEthernet0/1  
S1(config-if)# switchport mode trunk  
S1(config-if)# switchport trunk native vlan 99  
S1(config-if)# switchport trunk allowed vlan 10,20,30,99  
S1(config-if)# end
```

Native VLANs sind in der IEEE 802.1q-Spezifikation definiert, um die Abwärtskompatibilität mit *unmarkierten Daten* zu garantieren, die häufig in älteren LAN-Umgebungen auftreten. Ein natives VLAN dient als gemeinsamer Bezeichner an entgegengesetzten Enden eines Trunk-Links.