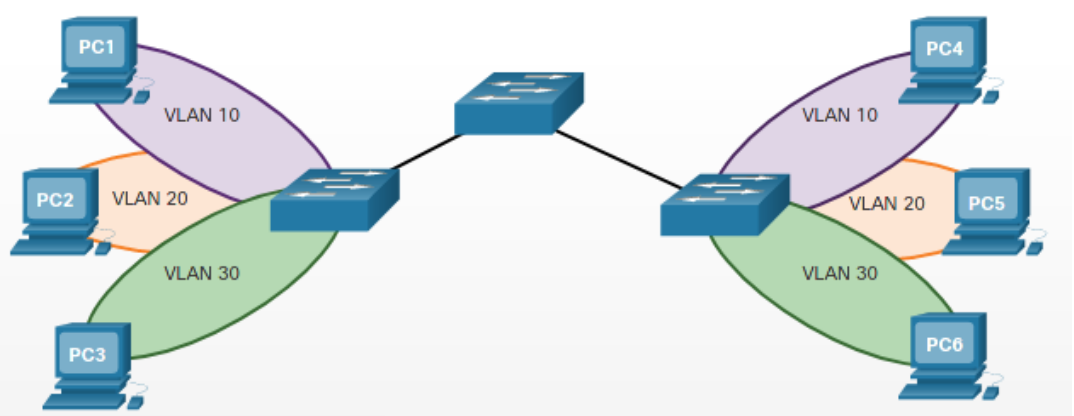
ZSL
Zentrum für Schulqualität
und Lehrerbildung
Baden-Württemberg

Networking Academy

VLANs



Andreas Grupp
andreas.grupp@zsl-rstue.de

Carina Haag
haag.c@lanz.schule

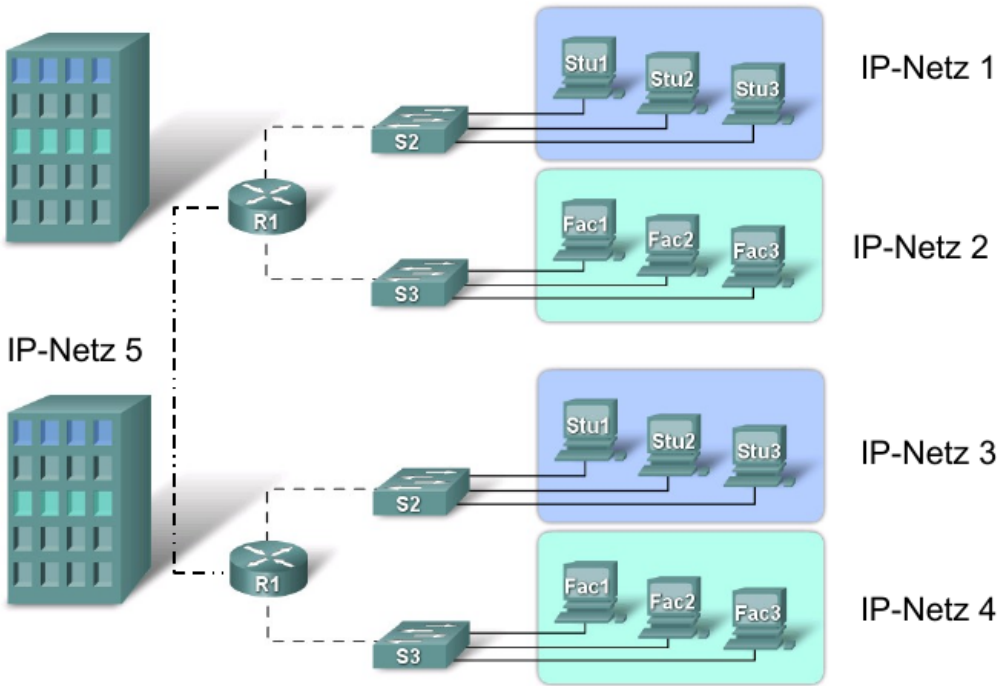
Tobias Heine
tobias.heine@springer-schule.de

Uwe Thiessat
uwe.thiessat@gbs-sha.de

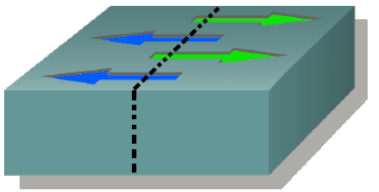
Warum VLANs – ein erster Einblick

Wie können wir „traditionell“ Netze trennen:

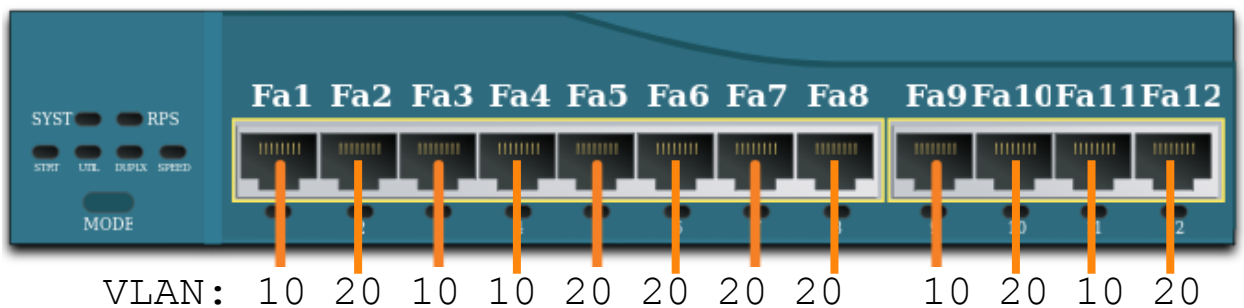
- **Beispiel**: Campus mit 2 Gebäuden in denen jeweils "Studenten-" und "Instructor-PC's" sind. Unmittelbarer Zugriff via Studenten- auf Lehrer-PC's soll nicht möglich sein. Trennung durch IP-Adressierung und Router
- **Nachteile**:
  - Einfacher Zugriff nur auf Ressourcen innerhalb eines Hauses
  - Hoher Bedarf an Geräten
  - Starres System



Lösung: Implementierung von VLANs



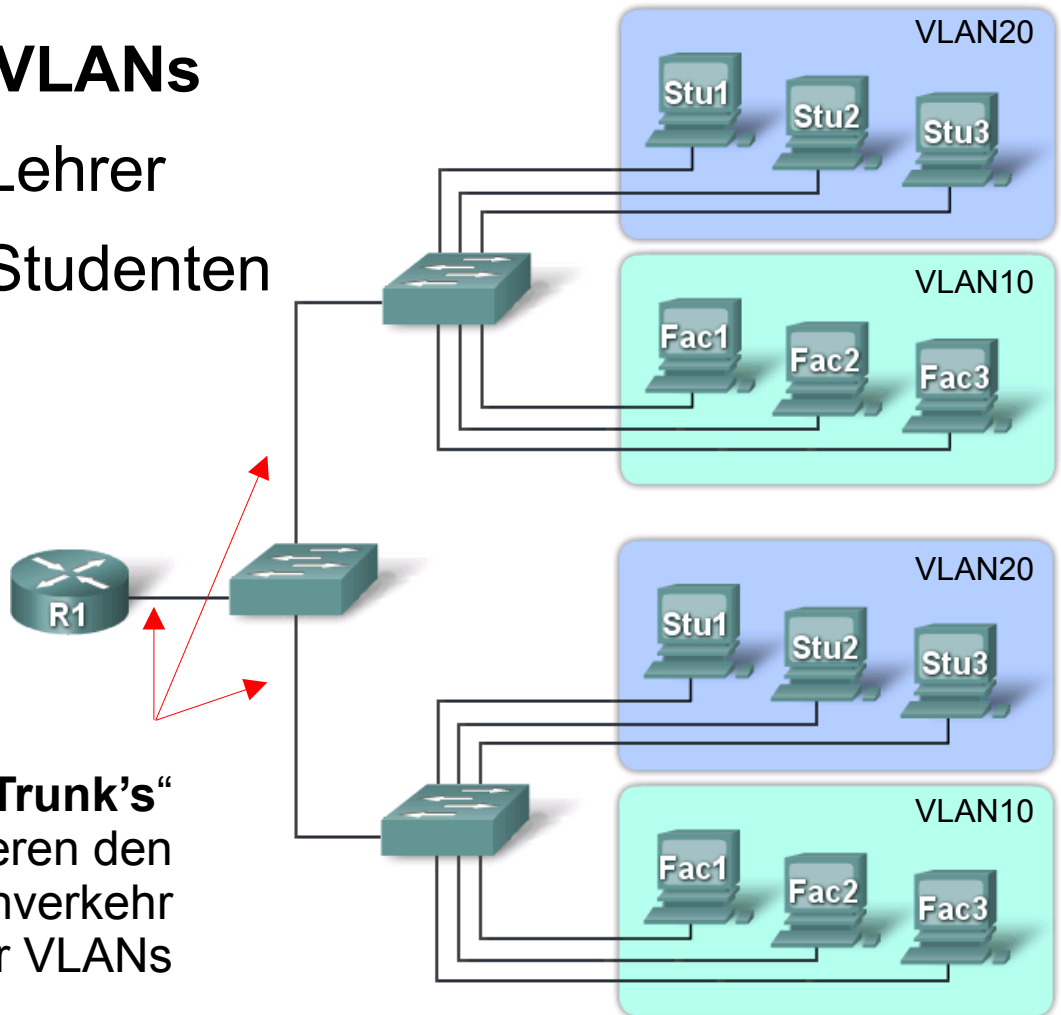
- VLANs (= Virtuelle LANs) sind **eigenständige Netzwerke**
- Studenten-PC's und Lehrer-PC's sind dadurch komplett getrennt obwohl sie die gleiche Infrastruktur benutzen (Geräte beider Gruppen hängen am gleichen Switch).
- VLANs trennen einen Switch logisch in eigenständige Geräte auf!
- Frames aus einem "logischen Gerät" können nicht in das andere "logische Gerät" gelangen.
- Das Gerät verhält sich wie zwei physikalisch eigene Geräte



Lösung: Implementierung von VLANs

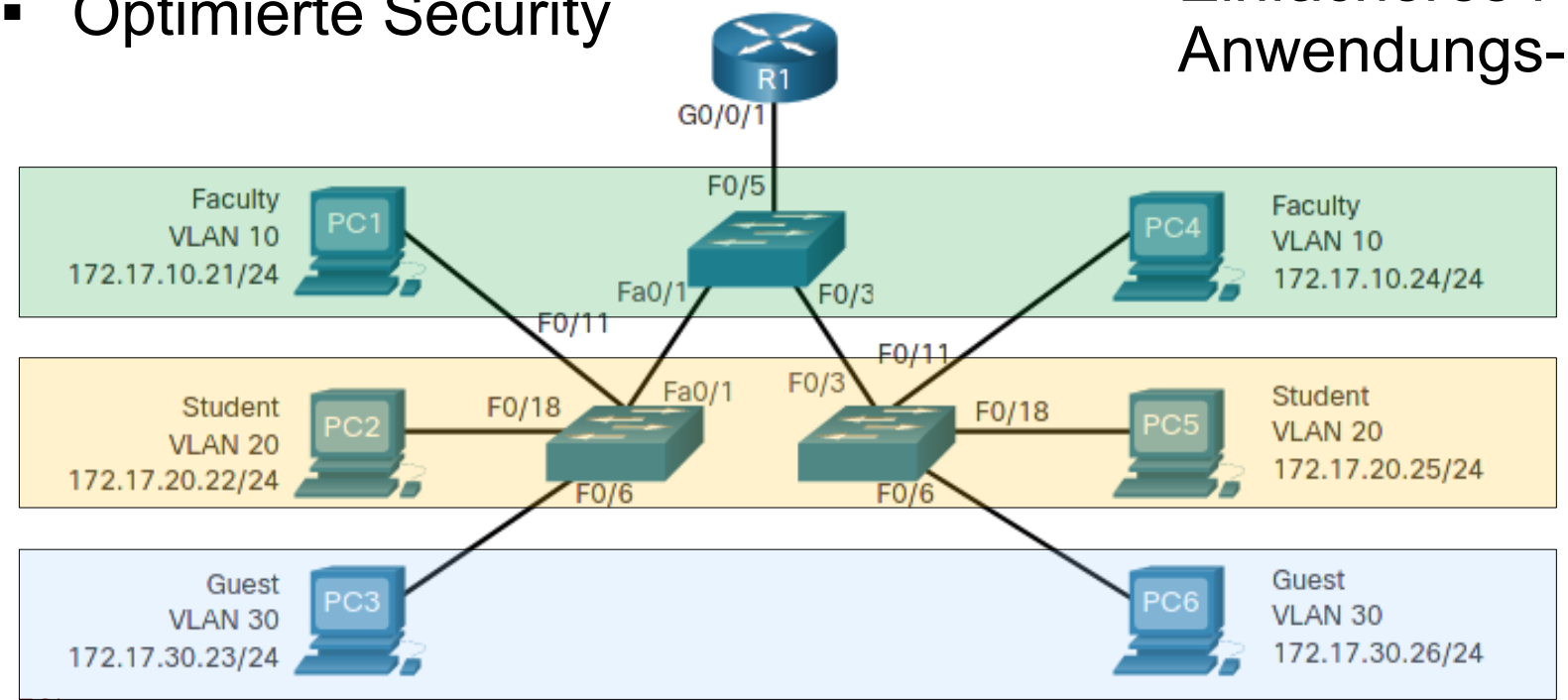
- Ein IP-Netz und VLAN 10 für Lehrer
- Ein IP-Netz und VLAN 20 für Studenten
- Zu beachten ist insbesondere:
  - Pro VLAN wird ein eigenes IP-Netz benötigt!
  - Traffic zwischen VLANs ist nur über einen Router (oder Layer-3-Switch) möglich!

„**Trunk's**“ transportieren den Datenverkehr mehrerer VLANs



Vorteile von VLAN-Umgebungen

- Kleinere Broadcast-Domänen
- Bessere Performance
- Optimierte Security
- Verbesserte Effizienz
- Günstiger
- Einfacheres Projekt- bzw. Anwendungs-Management

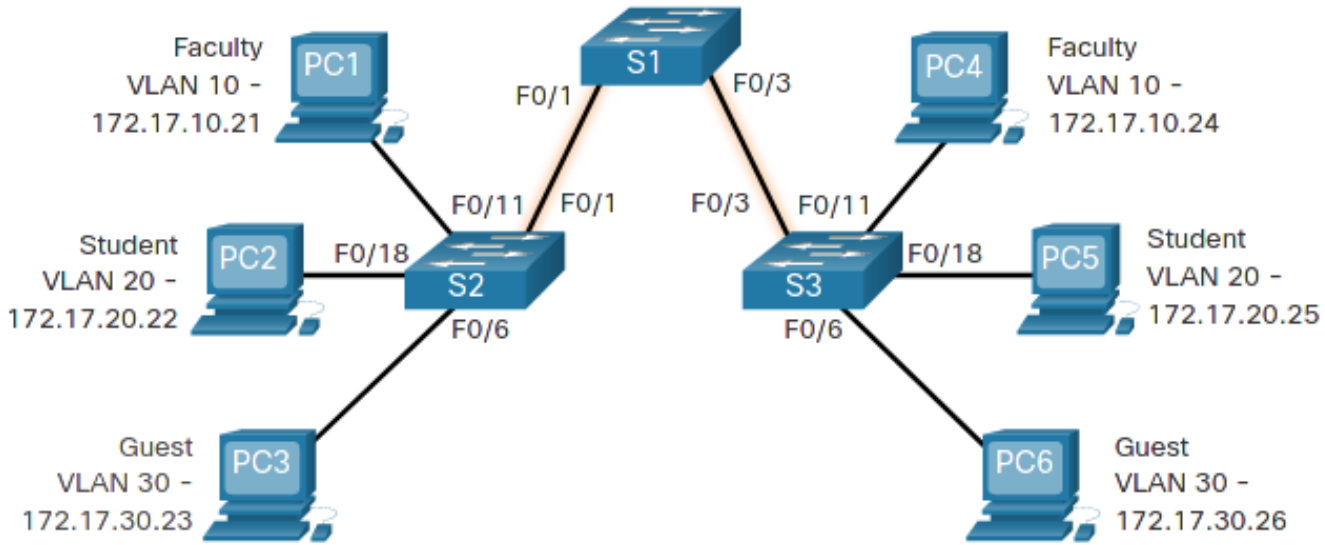


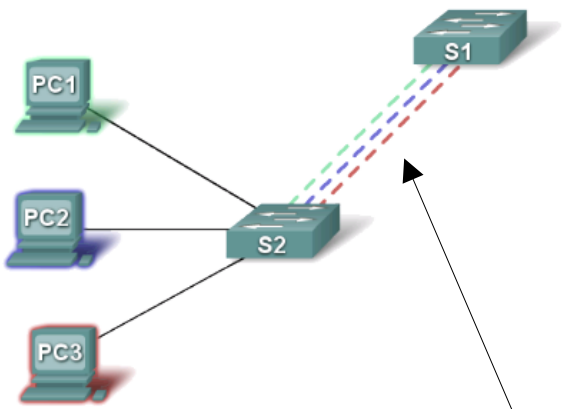
VLAN-Typen

- **Default VLAN:**
  - Alle Ports sind im Standard VLAN1 zugeordnet
  - Native und Management VLAN sind im Standard VLAN1
  - VLAN1 kann nicht umbenannt oder gelöscht werden
- **Data VLAN** / User VLAN → pro Verwendungszweck ein eigenes VLAN (siehe Bsp. oben)
- **Native VLAN** → wird für einen „unmarkierten“ (untagged) Traffic auf einem Trunk benötigt. Das Cisco Discovery Protokoll (CDP) nutzt dieses VLAN
- **Management VLAN** → eigenes VLAN für das Management und dafür verwendete Protokolle (SSH, SNMP, ...)
- **Voice VLAN** → eigenes VLAN das aufgrund der benötigten höheren Bandbreite der Sprachübertragung priorisiert werden kann.

VLAN Trunks definieren

- VLANs machen erst mit der Nutzung von Trunks Sinn
- Ein Trunk ist eine Punkt-zu-Punkt-Verbindung zwischen zwei Netzwerk-Geräten (Switches, Router, Server, ...) die Frames von mehr als einem VLAN transportieren.

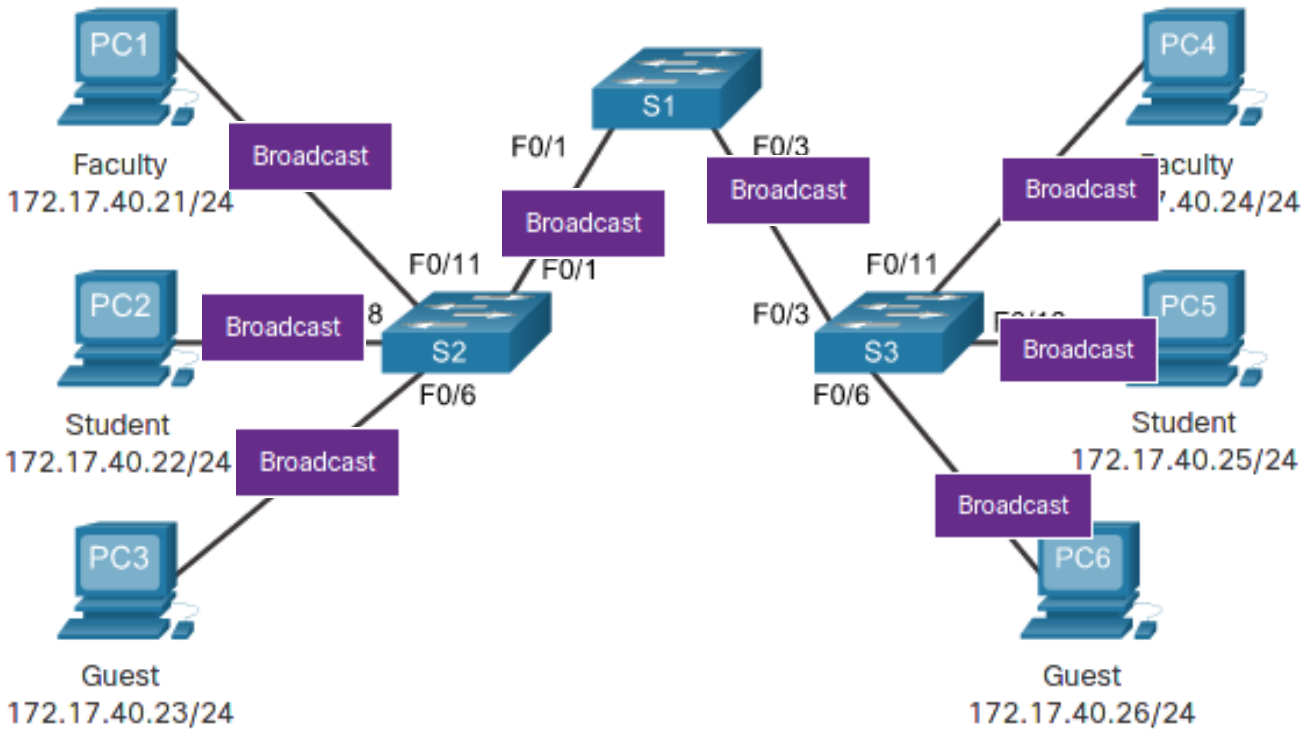




Das wäre Quatsch!!!

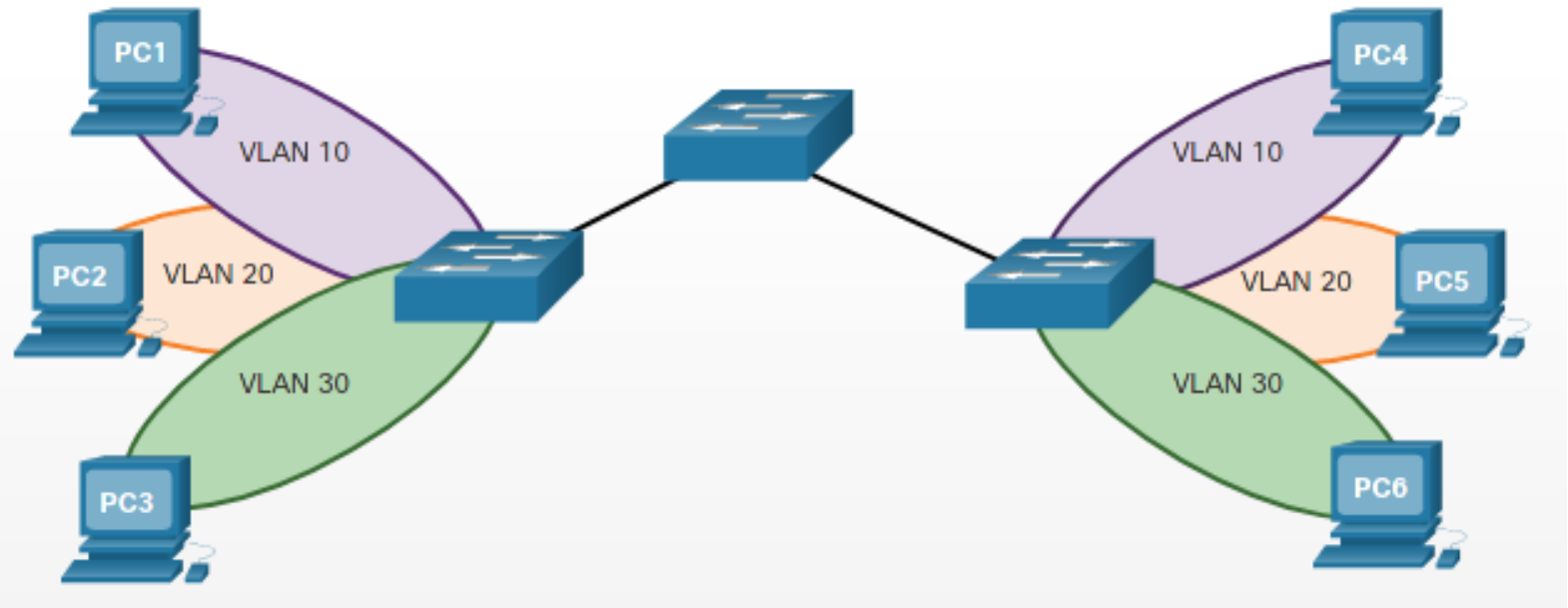
Netzwerke ohne VLANs

… verursachen je nach Größe des Netzwerkes ein relativ hohes Broadcast-Aufkommen.



Netzwerke mit VLANs …

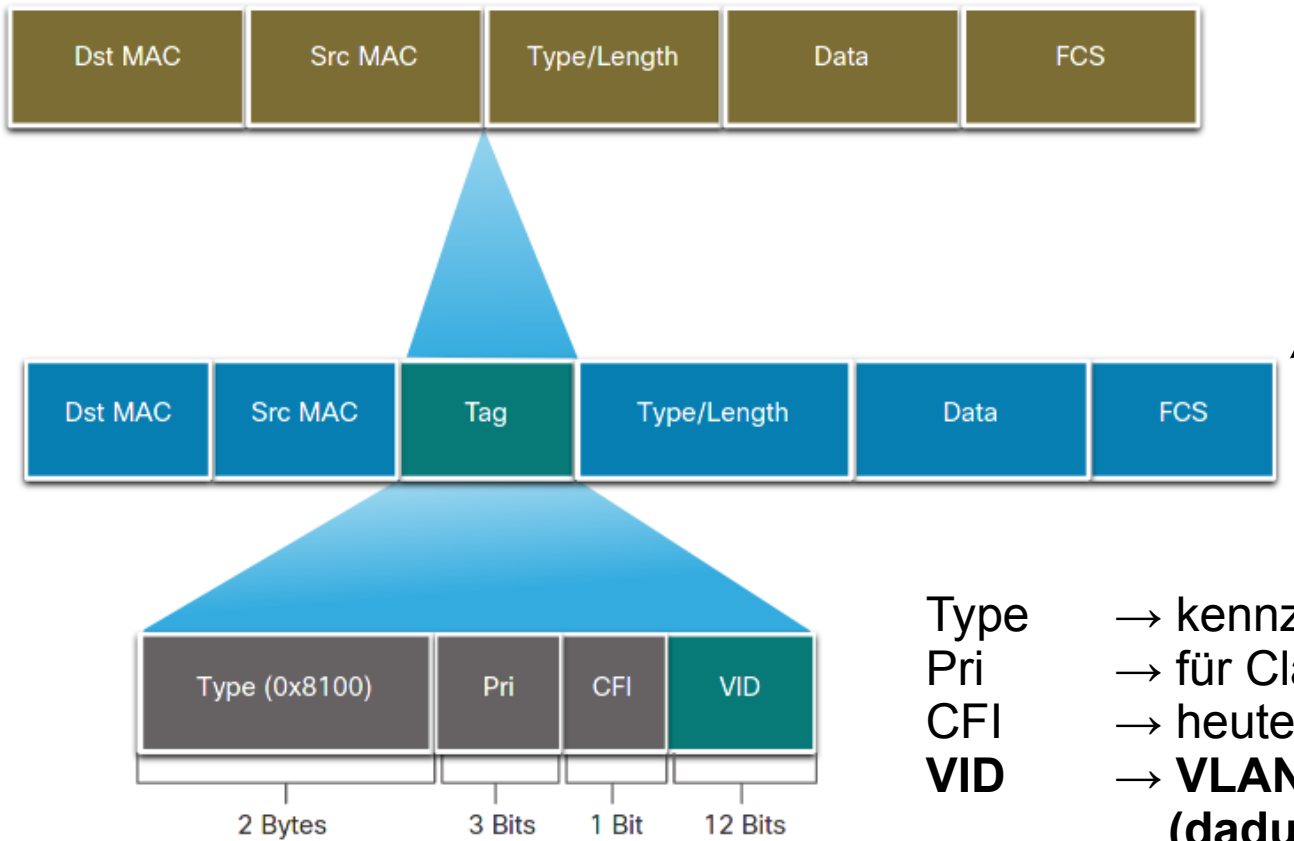
haben für jedes VLAN einen eigenen IP-Adress-Bereich. Broadcasts werden nur innerhalb eines VLANs von der Quelle zu möglichen Zielen versendet.



VLAN-Identifizierung

- Frames, die auf einem Trunk unterwegs sind, müssen irgendwie unterschieden werden.
- Dies erfolgt über eine Markierung (ein Tag)
- Das Standard-Ethernet-Frame hat **keine** Informationen über eine Zugehörigkeit zu einem VLAN.
- Daher erhält ein Frame, das auf einem Trunk platziert wird, weitere **4 Byte** im Header-Bereich (Tagging)
- Man spricht dann von einem **IEEE 802.1Q** Header

VLAN-Identifizierung

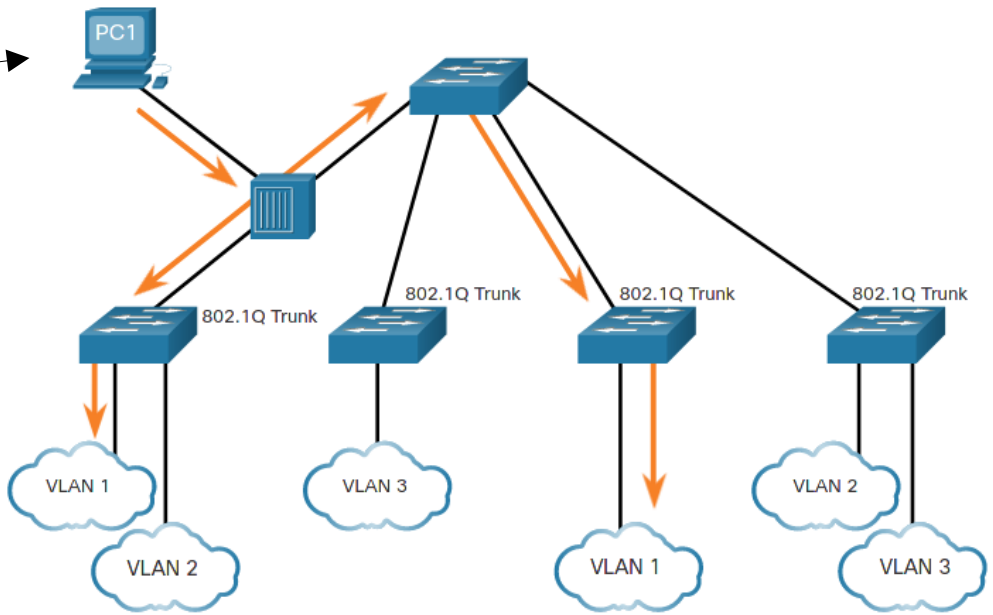


FCS wird neu berechnet

Type → kennzeichnet VLAN-tagged-Frame
Pri → für Class-of-Service-Abbildungen
CFI → heute DEI (Drop Eligible Indicator)
VID → VLAN-Identifier / VLAN-Nummer (dadurch max. 4096 VLANs theoretisch möglich)

Native VLANs and 802.1Q Tagging

Nicht sauber … aber theoretisch denkbar:
Ein PC hängt sich direkt an einen Trunk



Problem: Trunk ist nur für Tagged-Traffic gedacht. Die Netzwerkkarte des PCs schiebt ihre Frames aber untagged rein … was tun?

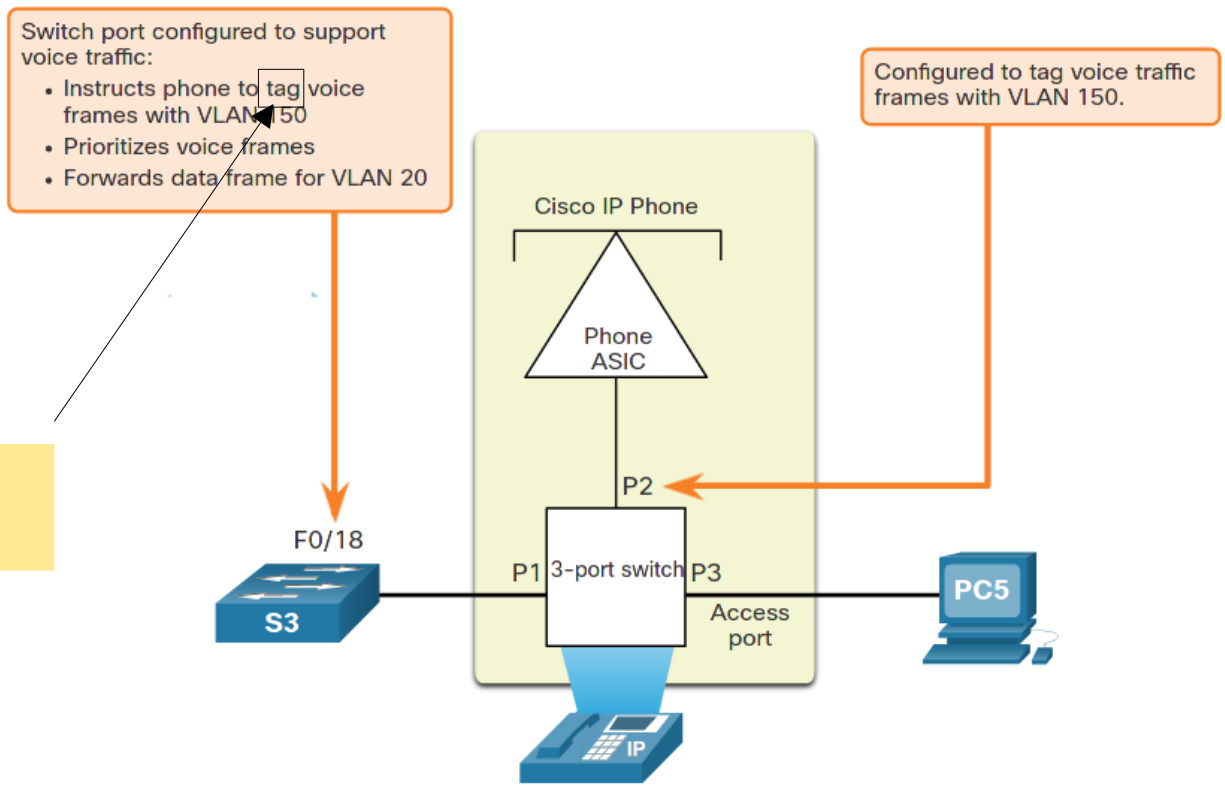
Lösung: Dafür ist das Native VLAN vorgesehen.

Beachte:
- Native VLAN soll nicht auf VLAN1 liegen
- Abänderung immer auf beiden Seiten des Trunks
- DTP nutzt das Native VLAN
- Fehlermeldungen im Fall eines Native-VLAN-Missmatches
- Tagged Frames auf Trunk mit Native VLAN-ID werden verworfen

Voice VLAN Tagging

- Auch für VoIP sollte ein eigenes VLAN erstellt werden. Ermöglicht:
  - Priorisierung (QoS)
  - Sicherheitsrichtlinien
- Besondere Anschluss- und Port-Konfiguration:

Data-VLAN: untagged
Voice-VLAN: tagged



Voice VLAN Tagging

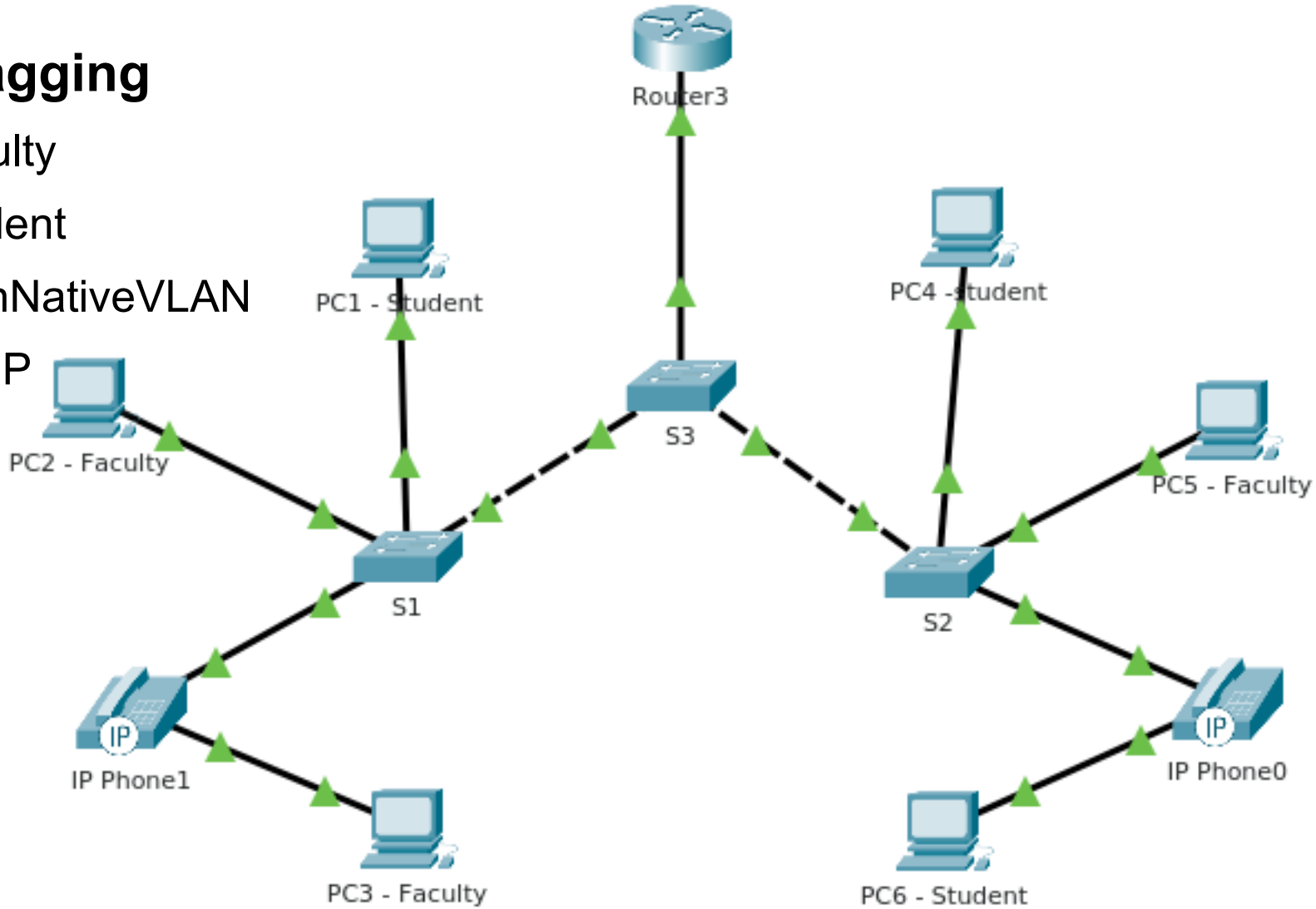
- Auch für VoIP sollte ein eigenes VLAN erstellt werden. Ermöglicht:
  - Priorisierung (QoS)
  - Sicherheitsrichtlinien
- Besondere Anschluss- und Port-Konfiguration:

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

VLANs in einer Multi-Switch-Umgebung

Voice VLAN Tagging

- VLAN 10: Faculty
- VLAN 20: Student
- VLAN 99: MeinNativeVLAN
- VLAN 150: VoIP



VLAN konfigurieren …

- VLAN (im verfügbaren Range) erzeugen
- VLAN einem oder mehreren Ports zuweisen
- Konfiguration überprüfen
- Voice-VLAN zuweisen
- Portzuweisung ändern
- VLANs löschen

VLAN Ranges auf einem Catalyst Switch:

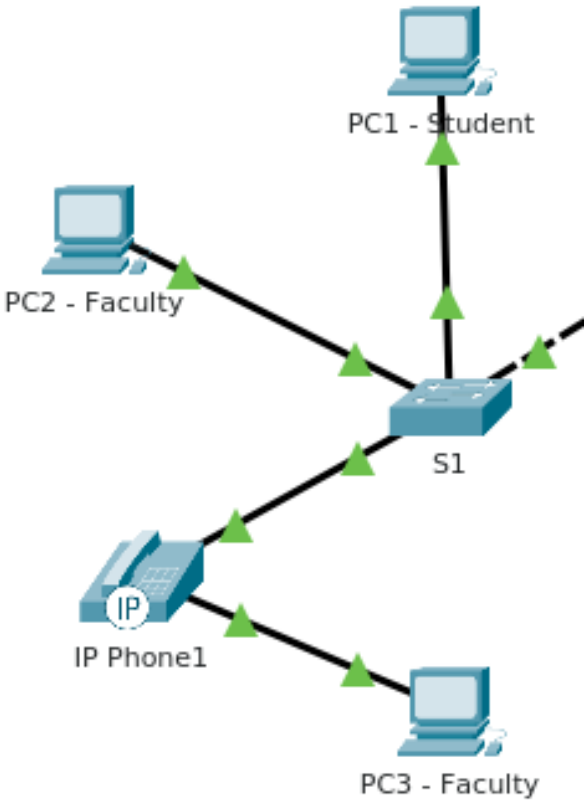
- VLAN 1 – 1005: Normal Range (für kleine bis große Netzwerke) **Zuordnung in vlan.dat gespeichert**
  - VLAN 1: Default VLAN (nicht löschbar): "Out of the box" sind alle Ports diesem VLAN zugeordnet
  - 1002 bis 1005 für legacy networks reserviert (nicht löschbar)
- 1006 bis 4094 – Extended Range (für ISPs und globale U-Netze) **Zuordnung in der running config gespeichert**

```
S1#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- ----------
1    default                          active    Fa0/1, Fa…
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

VLAN erstellen

```
S1#configure terminal
S1(config)#vlan 10
S1(config-vlan)#name faculty
S1(config-vlan)#end
```

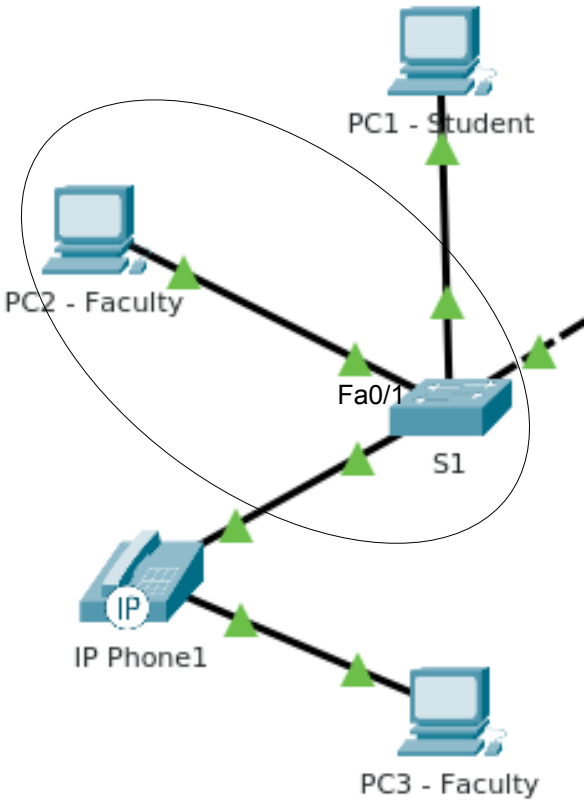
```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
1    default                           active    Fa0/1, Fa…
                                                 Fa0/5, Fa…
                                                 Fa0/9, Fa…
                                                 …
10   faculty                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```



Port einem VLAN zuordnen

```
S1#configure terminal
S1(config)#interface Fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#end
```

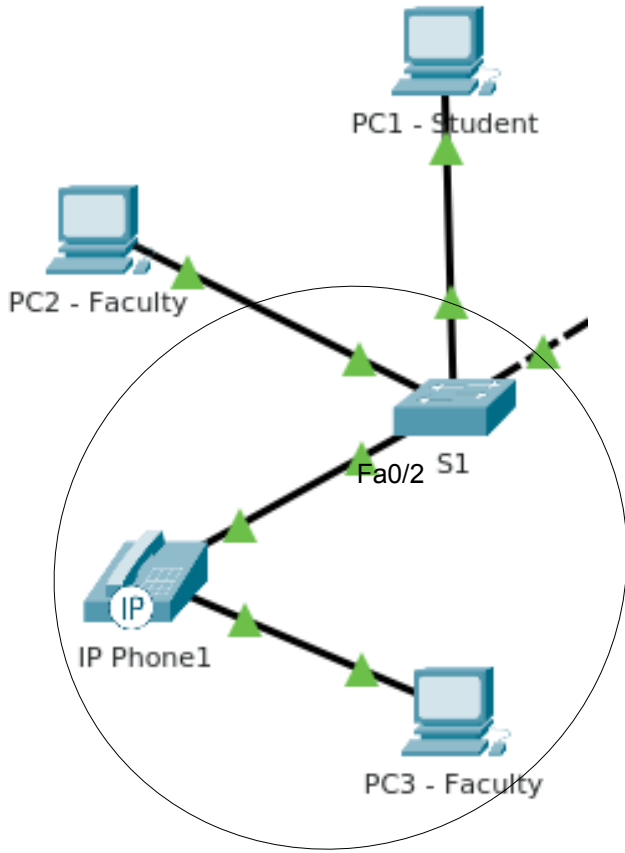
```
S1#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------
1    default                             active    Fa0/2, Fa…
                                                   Fa0/6, Fa…
                                                   Fa0/10, Fa…
                                                   …
10   faculty                             active    Fa0/1
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```



Port einem DATA- und einem Voice-VLAN zuordnen

```
S1#configure terminal
S1(config)#vlan 150
S1(config-vlan)#name Voice
S1(config-vlan)#exit
S1(config)#interface fa0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#mls qos trust cos
S1(config-if)#switchport voice vlan 150
```

```
S1#show interf fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (faculty)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 150
```



VLAN-Konfiguration überprüfen

```
S1#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
…
10   faculty                           active    Fa0/1, Fa0/2
150  Voice                             active    Fa0/2
```

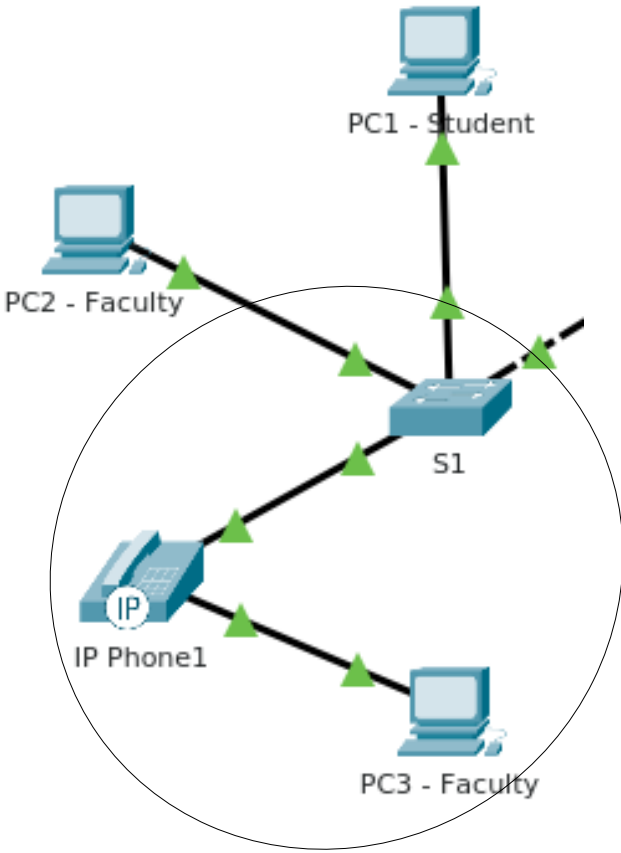
… jetzt auch Fa0/2 bei VLAN 10 und VLAN 150 eingetragen.

```
S1#show interfaces fa0/1 switchport
```

… Ausgaben: s. o.

```
S1#show vlan summary
Number of existing VLANs              : 9
 Number of existing VTP VLANs         : 9
 Number of existing extended VLANS    : 0
```

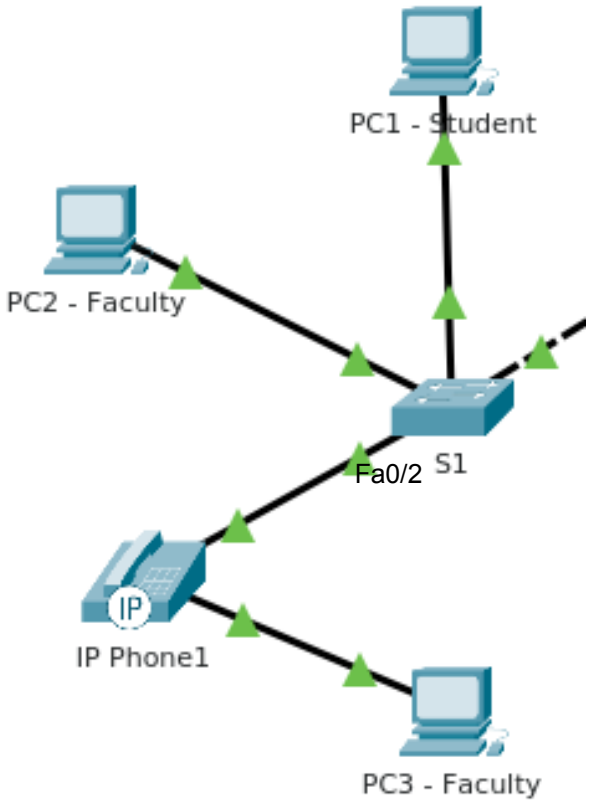
… Achtung: Dieser Befehl ist nicht in Packet Tracer verfügbar



VLAN Mitgliedschaft ändern

```
S1(config)#interf range fa0/1 - fa0/2
S1(config-if-range)#no switchport access vlan
S1(config-if-range)#end
```

```
S1#show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
```



VLANs löschen

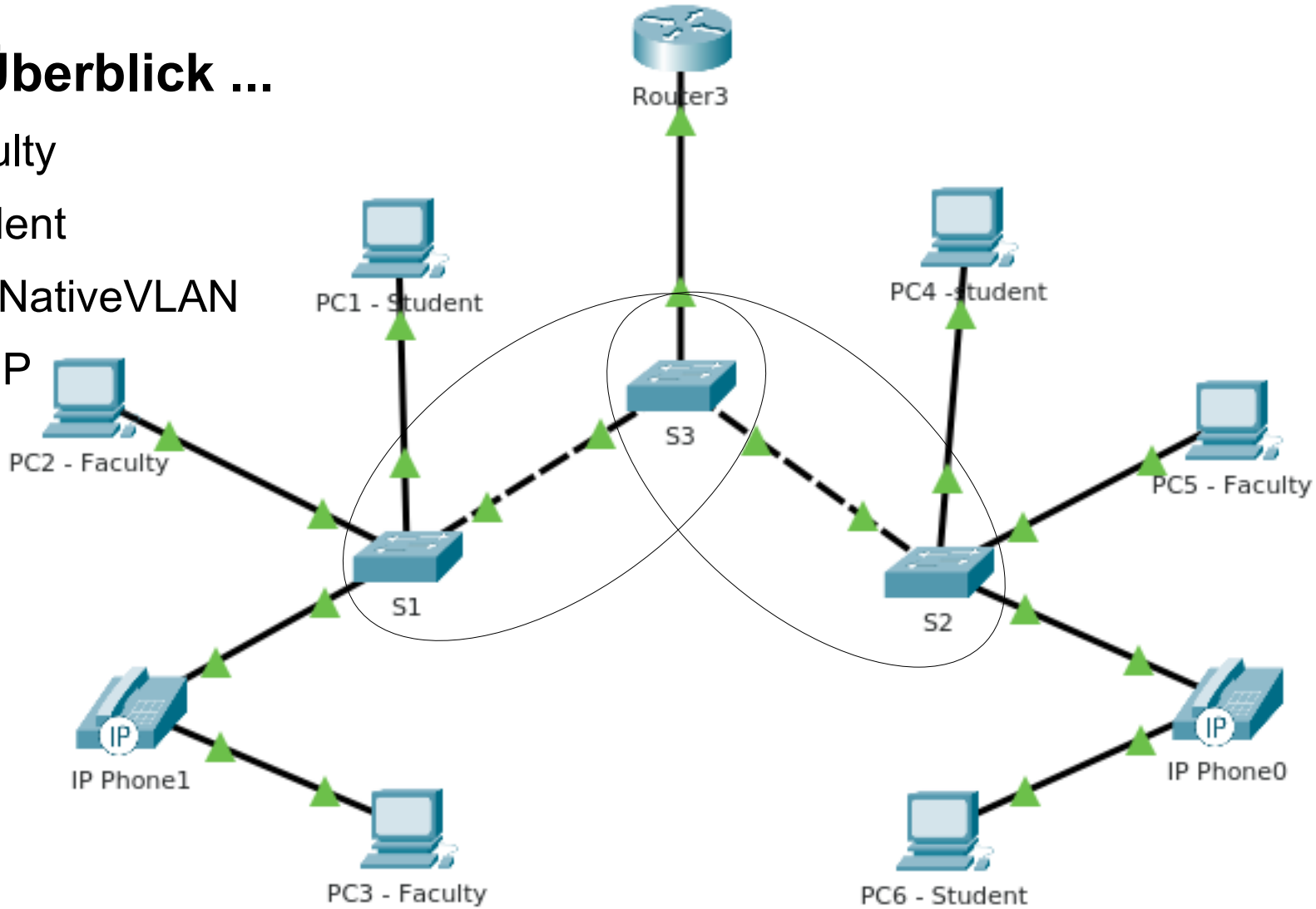
- Einzelnes VLAN löschen: `S1(config)# no vlan 20`
- Vorsicht: Vorher alle Port-Mitgliedschaften zur jeweiligen VLAN-ID aufheben. Sonst wird der Port unter `S1# show vlan brief` nicht aufgeführt
- Um alle VLANs zu löschen muss die vlan.dat gelöscht werden `S1# delete vlan.dat`
- Switch in den Auslieferungszustand setzen:

```
S1#erase startup-config
S1#delete vlan.dat
S1#reload
System configuration has been modified. Save? [yes/no]: no
```

VLAN Trunk Konfiguration

Nochmal der Überblick ...

- VLAN 10: Faculty
- VLAN 20: Student
- VLan 99: MeinNativeVLAN
- VLAN 150: VoIP

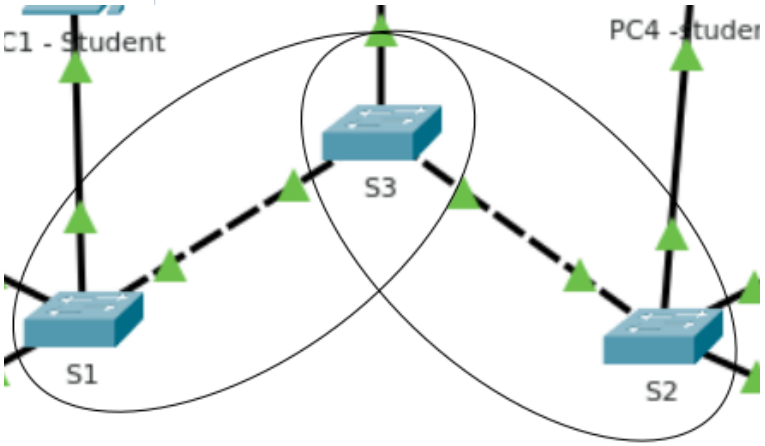


Trunk Konfiguration

```
S1#configure terminal
S1(config)#vlan 99
S1(config-vlan)#name MeinNativeVLAN
S1(config)#interf g0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switch trunk native vlan 99
S1(config-if)#switchport trunk allowed vlan 10,20,99,150
S1(config-if)#end
```

Vorsicht: Die Konfiguration **AUCH** auf dem gegenüberliegenden Port auf S3 ausführen

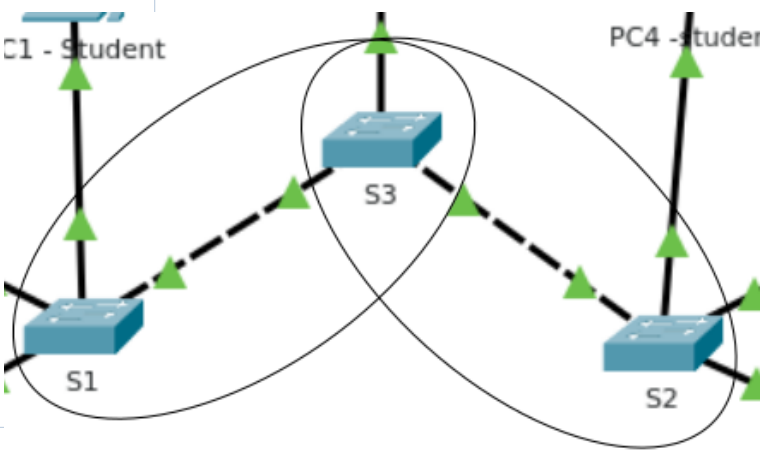
```
S1#show interfaces g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (MeinNativeVLAN)
[…]
Trunking VLANs Enabled: 10,20,99,150
```



Trunkeinstellungen auf Default-Werte setzen

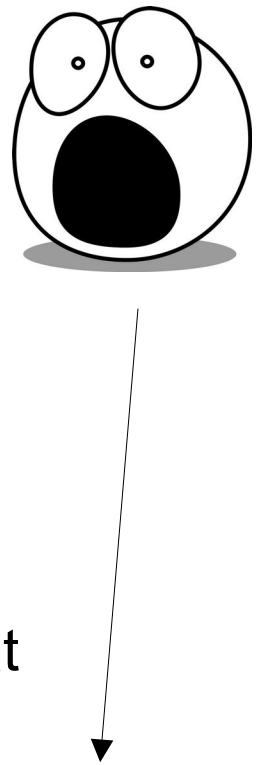
```
S1#configure terminal
S1(config)#interf g0/1
S1(config-if)#no switchport trunk allowed vlan
S1(config-if)#no switchport trunk native vlan
S1(config-if)#end
```

```
S1#show interfaces g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
[…]
Trunking VLANs Enabled: All
```



Grundlagen Dynamic Trunking Protocol (DTP)

- Cisco-propriäteres Protokoll
- **Ziel:** Konfiguration von Trunks beschleunigen
- **Idee:** Automatisches Aushandeln eines Trunks mit einem Nachbargerät
- Ein Interface kann …
  - … als Access-Port konfiguriert sein
  - … als Trunk-Port konfiguriert sein
  - … für eine dynamische Aushandlung mit dem Nachbargerät konfiguriert sein.
- DTP ist auf den Catalyst 2960-Switchen automatisch an (Autsch)



Grundlagen Dynamic Trunking Protocol (DTP)

- DTP abschalten:

```
S1#configure terminal
S1(config)#interf g0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

- DTP wieder aktivieren:

```
S1(config-if)# switchport mode dynamic auto
```

- DTP-Modes
  - **dynamic auto:** Trunk wird erzeugt wenn Nachbargerät als Trunk oder Dynamic Desireable gesetzt ist.
  - **dynamic desireable:** Trunk wird erzeugt wenn Nachbargerät als Trunk, Dynamic Desireable oder Dynamic Auto gesetzt ist.

DTP-Konfigurations-Ergebnisse:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

DTP-Konfiguration überprüfen

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
```

DTP ist IMHO ein Sicherheitsproblem. Daher sollten Trunks manuell konfiguriert werden und DTP abgeschaltet werden:

```
S1#configure terminal
Switch(config)#interf range f0/1 - f0/24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#interf rang g0/1 - g0/2
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport nonegotiate
```

Zum Abschluss nochmal ...

Best Practise bzgl. VLANs

- Native VLAN von Trunks nicht in VLAN1
- Management-VLAN nicht in VLAN 1 und nicht auf Native VLAN
- Kein Gerät in VLAN 1, Native VLAN und Management VLAN
- Ungenutzte Switch-Ports in „Black-Hole-VLAN“ und abschalten.
- Keine Ports mit Dynamic Trunking Modes (desirable, auto)
- DTP Verhandlungen abschalten
- Voice-Traffic in eigenes VLAN

Activites, Labs, PT-Übungen, etc.

- 3.1.4 PT: Who hears the Broadcast
- 3.2.8 PT: Investigate a VLAN Implementation
- **3.3.12 PT: VLAN Configuration**
- **3.4.5 PT: Configure Trunks**
- 3.4.6 Lab: Configure VLANs and Trunking
- 3.5.5 PT: Configure DTP
- 3.6.1 PT: Implement VLANs and Trunking
- **3.6.2 Lab: Configure VLANs and Trunking**
- **3.6.4 Module Quiz: VLANs**